



Microsoft Security Intelligence Report

Volume 19 | January through June, 2015

REGIONAL THREAT ASSESSMENT

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it.

Copyright © 2015 Microsoft Corporation. All rights reserved.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Contents

Albania	1
Algeria	11
Angola	21
Argentina	25
Australia	35
Austria.....	45
Bahamas, The	55
Bahrain	59
Bangladesh.....	69
Belarus.....	79
Belgium	89
Bolivia.....	99
Brazil	107
Bulgaria	117
Canada	127
Chile	137
China.....	147
Colombia	157
Costa Rica	167
Croatia.....	177
Cyprus	187
Czech Republic	197
Denmark	207
Dominican Republic.....	217
Ecuador	227
Egypt.....	237
El Salvador	247
Estonia	257
Finland.....	267

France.....	277
Georgia.....	287
Germany.....	297
Greece.....	307
Guatemala.....	317
Honduras.....	327
Hong Kong S.A.R.....	335
Hungary.....	345
Iceland.....	355
India.....	365
Indonesia.....	375
Iraq.....	385
Ireland.....	395
Israel.....	405
Italy.....	415
Jamaica.....	425
Japan.....	433
Jordan.....	443
Kazakhstan.....	453
Kenya.....	463
Korea.....	473
Kuwait.....	483
Latvia.....	493
Lebanon.....	503
Lithuania.....	511
Luxembourg.....	521
Macao S.A.R.....	527
Malaysia.....	533
Malta.....	543
Mexico.....	549
Moldova.....	559

Mongolia.....	569
Morocco.....	575
Nepal	585
Netherlands	595
New Zealand	605
Nicaragua	615
Nigeria.....	621
Norway.....	629
Oman.....	639
Pakistan	649
Palestinian Authority.....	659
Panama	669
Paraguay.....	679
Peru	685
Philippines	695
Poland	705
Portugal.....	715
Puerto Rico.....	725
Qatar	735
Romania.....	745
Russia	755
Saudi Arabia.....	765
Senegal.....	775
Serbia.....	785
Singapore	795
Slovakia	805
Slovenia.....	815
South Africa.....	825
Spain	835
Sri Lanka.....	845
Sweden.....	855

Switzerland.....	865
Taiwan	875
Tanzania	885
Thailand	891
Trinidad and Tobago	901
Tunisia	911
Turkey.....	921
Ukraine.....	931
United Arab Emirates.....	941
United Kingdom	951
United States	961
Uruguay	971
Venezuela	981
Vietnam.....	991
Zimbabwe	1001

Albania

The statistics presented here are generated by Microsoft security programs and services running on computers in Albania in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Albania

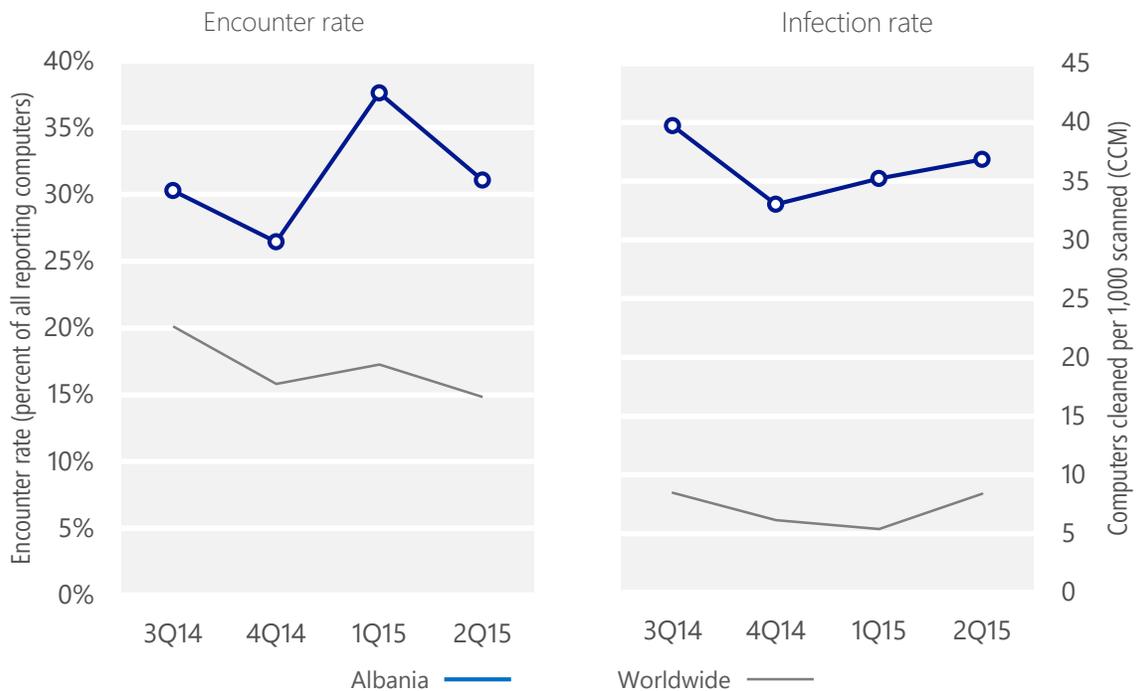
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Albania	30.3%	26.5%	37.6%	31.1%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Albania	39.7	33.0	35.2	36.8
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcote, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 31.1% of computers in Albania encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 36.8 of every 1,000 unique computers scanned in Albania in 2Q15 (a CCM score of 36.8, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Albania over the last four quarters, compared to the world as a whole.

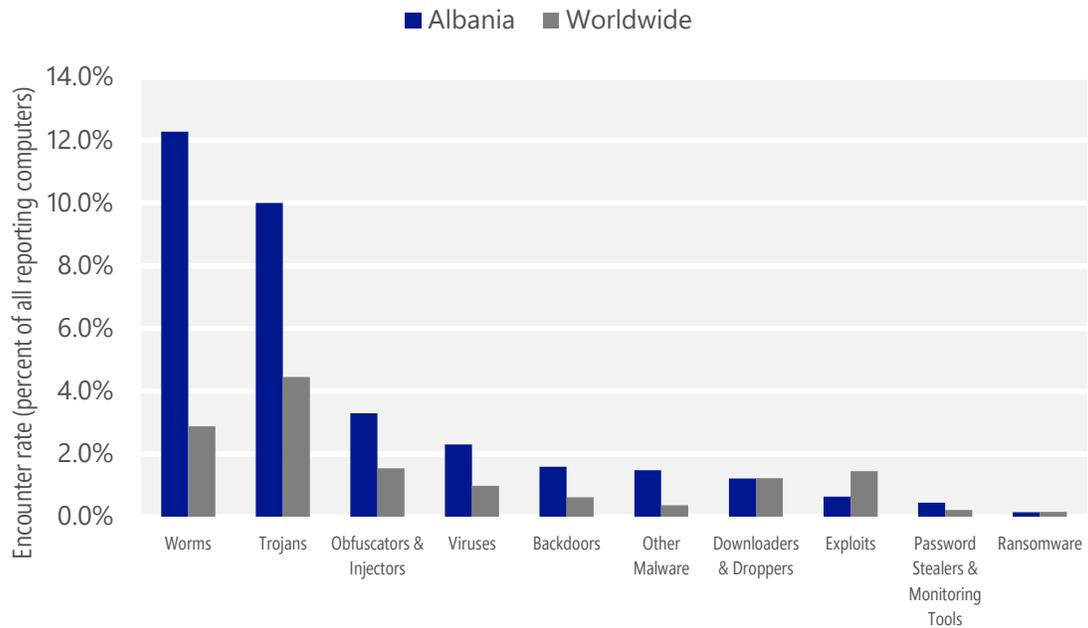
Malware encounter and infection rate trends in Albania and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in Albania and around the world, and for explanations of the methods and terms used here.

Malware categories

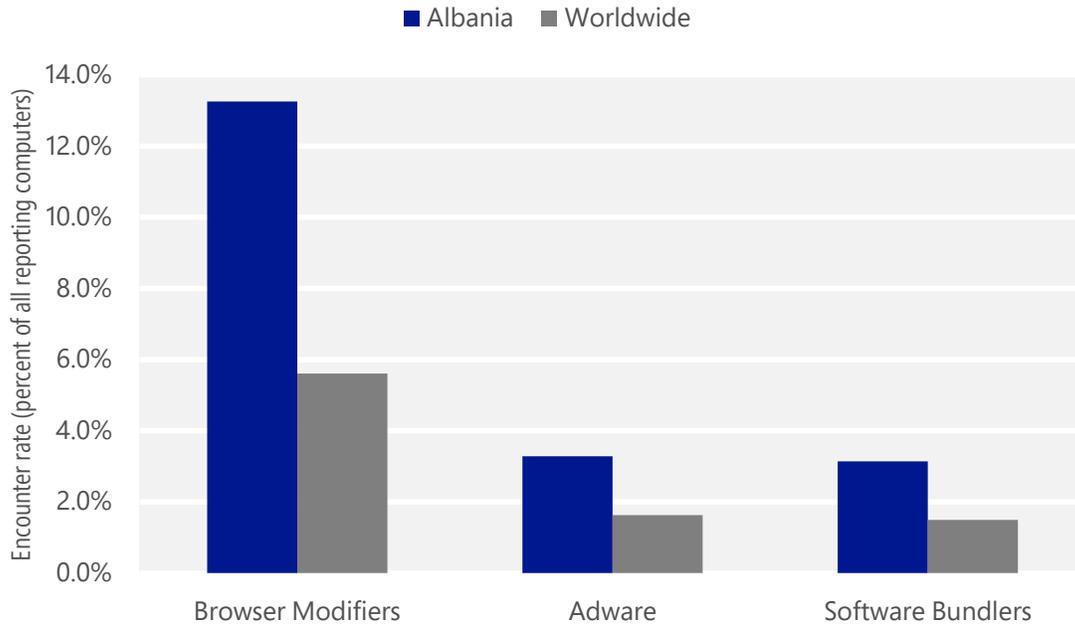
Malware encountered in Albania in 2Q15, by category



- The most common malware category in Albania in 2Q15 was Worms. It was encountered by 12.3 percent of all computers there, down from 13.3 percent in 1Q15.
- The second most common malware category in Albania in 2Q15 was Trojans. It was encountered by 10.0 percent of all computers there, up from 6.9 percent in 1Q15.
- The third most common malware category in Albania in 2Q15 was Obfuscators & Injectors, which was encountered by 3.3 percent of all computers there, down from 4.0 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Albania in 2Q15, by category



- The most common unwanted software category in Albania in 2Q15 was Browser Modifiers. It was encountered by 13.3 percent of all computers there, down from 19.4 percent in 1Q15.
- The second most common unwanted software category in Albania in 2Q15 was Adware. It was encountered by 3.3 percent of all computers there, down from 6.9 percent in 1Q15.
- The third most common unwanted software category in Albania in 2Q15 was Software Bundlers, which was encountered by 3.1 percent of all computers there, up from 2.1 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Albania in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Gamarue	Worms	7.0%
2	VBS/Jenxcus	Worms	3.3%
3	INF/Autorun	Obfuscators & Injectors	2.4%
4	Win32/Kilim	Trojans	2.4%
5	Win32/Sality	Viruses	1.9%
6	Win32/Helompy	Worms	1.5%
7	Win32/Skeeyah	Trojans	1.4%
8	Win32/Obfuscator	Obfuscators & Injectors	1.1%
9	Win32/Yeltminky	Worms	1.0%
10	Win32/Brontok	Worms	1.0%

- The most common malware family encountered in Albania in 2Q15 was [Win32/Gamarue](#), which was encountered by 7.0 percent of reporting computers there. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The second most common malware family encountered in Albania in 2Q15 was [VBS/Jenxcus](#), which was encountered by 3.3 percent of reporting computers there. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The third most common malware family encountered in Albania in 2Q15 was [INF/Autorun](#), which was encountered by 2.4 percent of reporting computers there. [INF/Autorun](#) is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The fourth most common malware family encountered in Albania in 2Q15 was [Win32/Kilim](#), which was encountered by 2.4 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Albania in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	7.2%
2	Win32/KipodToolsCby	Browser Modifiers	6.4%
3	Win32/InstalleRex	Software Bundlers	2.8%
4	Win32/SaverExtension	Adware	2.3%
5	Win32/AlterbookSP	Browser Modifiers	0.4%

- The most common unwanted software family encountered in Albania in 2Q15 was [Win32/CouponRuc](#), which was encountered by 7.2 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in Albania in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 6.4 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common unwanted software family encountered in Albania in 2Q15 was [Win32/InstalleRex](#), which was encountered by 2.8 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Albania in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/Gamarue	Worms	8.1
2	Win32/Sality	Viruses	8.0
3	Win32/IeEnablerCby	Browser Modifiers	6.8
4	VBS/Jenxcus	Worms	5.3
5	Win32/Helompy	Worms	2.9
6	Win32/Brontok	Worms	2.8
7	Win32/Kilim	Trojans	2.1
8	Win32/Pramro	Trojans	1.1
9	Win32/Yeltminky	Worms	1.0
10	Win32/Vobfus	Worms	0.7

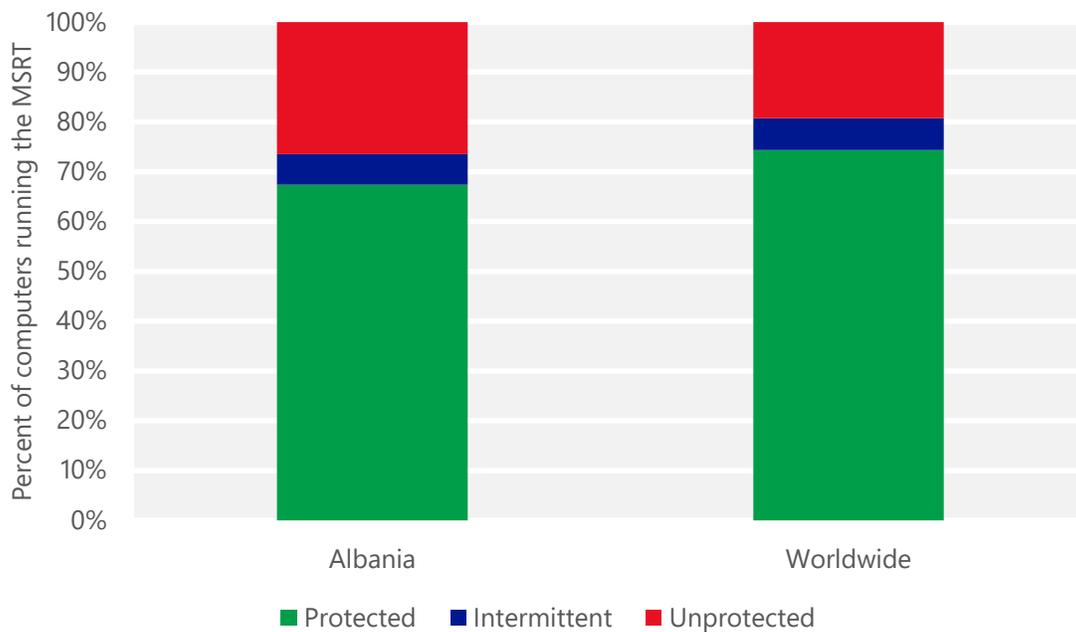
- The most common threat family infecting computers in Albania in 2Q15 was [Win32/Gamarue](#), which was detected and removed from 8.1 of every 1,000 unique computers scanned by the MSRT. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The second most common threat family infecting computers in Albania in 2Q15 was [Win32/Sality](#), which was detected and removed from 8.0 of every 1,000 unique computers scanned by the MSRT. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The third most common threat family infecting computers in Albania in 2Q15 was [Win32/IeEnablerCby](#), which was detected and removed from 6.8 of every 1,000 unique computers scanned by the MSRT. [Win32/IeEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The fourth most common threat family infecting computers in Albania in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 5.3 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Albania and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Albania

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	1.08 (0.28)	0.43 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	1.51 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	4.53 (16.7)	

Algeria

The statistics presented here are generated by Microsoft security programs and services running on computers in Algeria in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Algeria

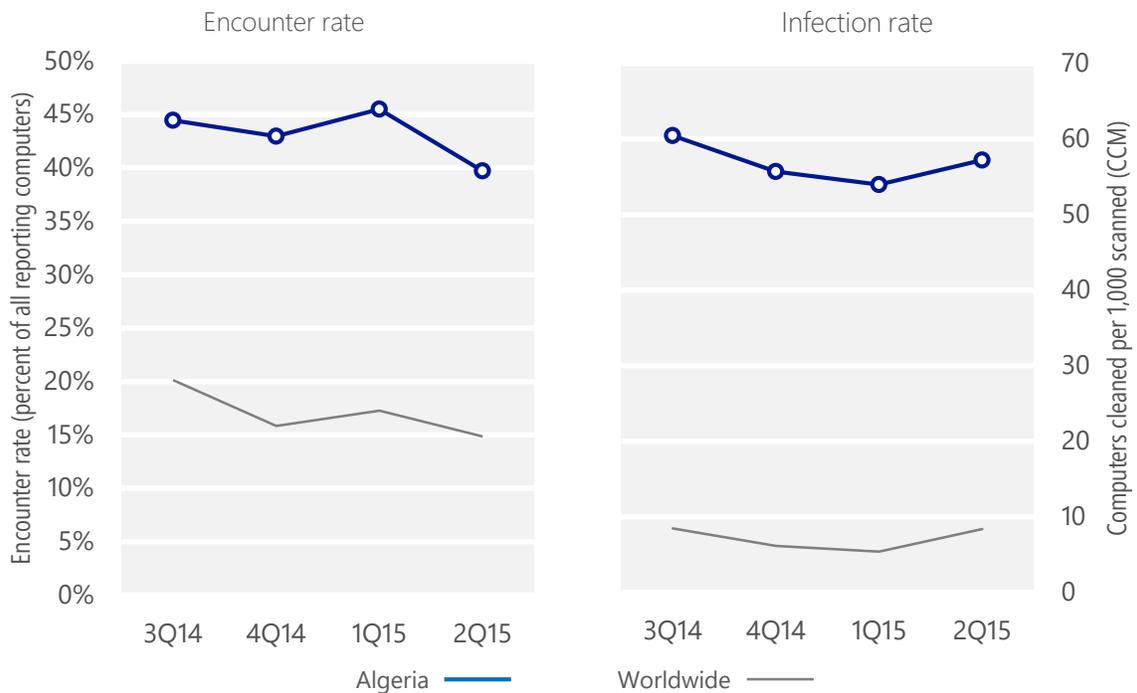
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Algeria	44.4%	43.0%	45.5%	39.7%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Algeria	60.5	55.7	54.0	57.2
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcote, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 39.7% of computers in Algeria encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 57.2 of every 1,000 unique computers scanned in Algeria in 2Q15 (a CCM score of 57.2, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Algeria over the last four quarters, compared to the world as a whole.

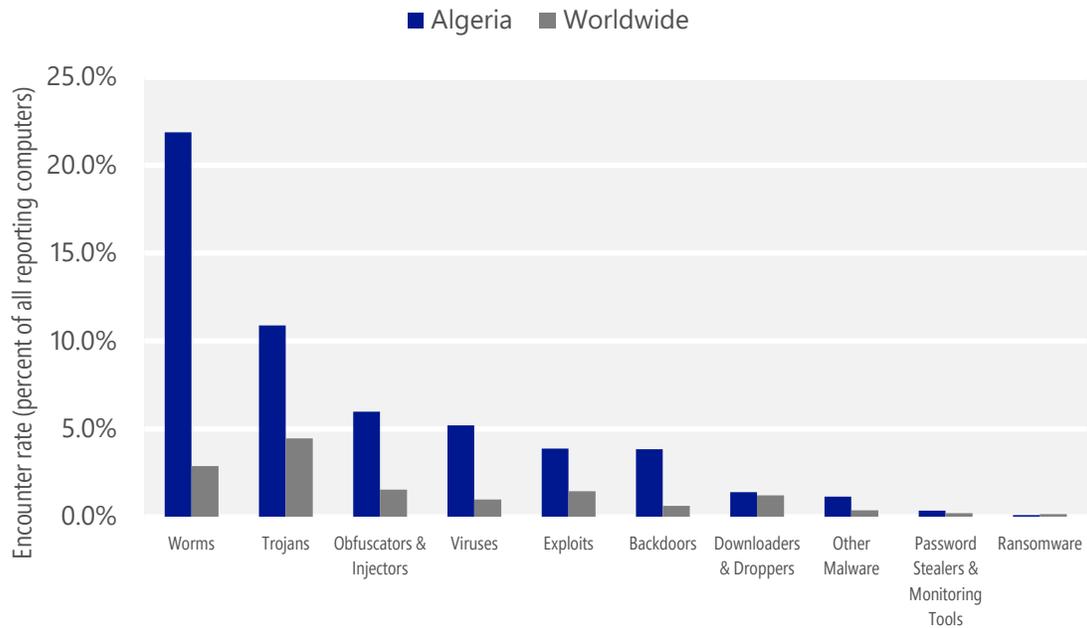
Malware encounter and infection rate trends in Algeria and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in Algeria and around the world, and for explanations of the methods and terms used here.

Malware categories

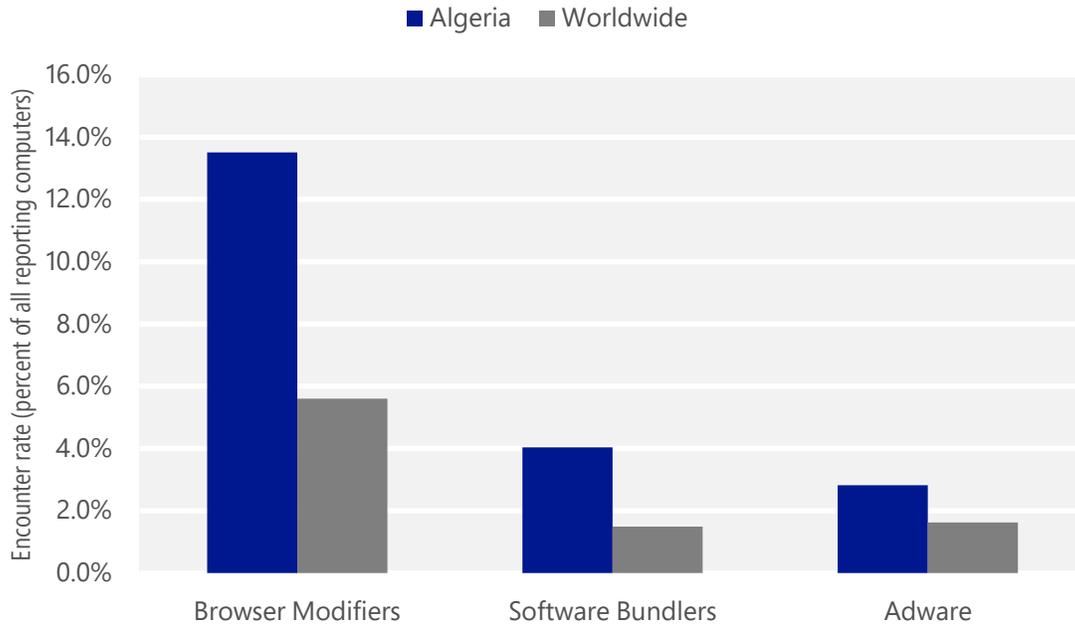
Malware encountered in Algeria in 2Q15, by category



- The most common malware category in Algeria in 2Q15 was Worms. It was encountered by 21.9 percent of all computers there, down from 22.4 percent in 1Q15.
- The second most common malware category in Algeria in 2Q15 was Trojans. It was encountered by 10.9 percent of all computers there, down from 12.3 percent in 1Q15.
- The third most common malware category in Algeria in 2Q15 was Obfuscators & Injectors, which was encountered by 6.0 percent of all computers there, down from 6.8 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Algeria in 2Q15, by category



- The most common unwanted software category in Algeria in 2Q15 was Browser Modifiers. It was encountered by 13.5 percent of all computers there, down from 21.4 percent in 1Q15.
- The second most common unwanted software category in Algeria in 2Q15 was Software Bundlers. It was encountered by 4.0 percent of all computers there, down from 5.6 percent in 1Q15.
- The third most common unwanted software category in Algeria in 2Q15 was Adware, which was encountered by 2.8 percent of all computers there, up from 2.3 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Algeria in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Ippedo	Worms	11.5%
2	VBS/Jenxcus	Worms	10.0%
3	INF/Autorun	Obfuscators & Injectors	5.6%
4	Win32/Gamarue	Worms	3.6%
5	Win32/Obfuscator	Obfuscators & Injectors	3.0%
6	Win32/Ramnit	Trojans	3.0%
7	Win32/CplLnk	Exploits	2.9%
8	Win32/Sality	Viruses	2.7%
9	MSIL/Bladabindi	Backdoors	2.4%
10	Win32/Macoute	Worms	1.9%

- The most common malware family encountered in Algeria in 2Q15 was [Win32/Ippedo](#), which was encountered by 11.5 percent of reporting computers there. [Win32/Ippedo](#) is a worm that can send sensitive information to a malicious hacker. It spreads through removable drives, such as USB flash drives.
- The second most common malware family encountered in Algeria in 2Q15 was [VBS/Jenxcus](#), which was encountered by 10.0 percent of reporting computers there. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The third most common malware family encountered in Algeria in 2Q15 was [INF/Autorun](#), which was encountered by 5.6 percent of reporting computers there. [INF/Autorun](#) is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The fourth most common malware family encountered in Algeria in 2Q15 was [Win32/Gamarue](#), which was encountered by 3.6 percent of reporting computers there. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Algeria in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/KipodToolsCby	Browser Modifiers	8.6%
2	Win32/CouponRuc	Browser Modifiers	5.4%
3	Win32/InstalleRex	Software Bundlers	3.8%
4	Win32/SaverExtension	Adware	1.6%
5	Win32/AlterbookSP	Browser Modifiers	0.5%

- The most common unwanted software family encountered in Algeria in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 8.6 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common unwanted software family encountered in Algeria in 2Q15 was [Win32/CouponRuc](#), which was encountered by 5.4 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The third most common unwanted software family encountered in Algeria in 2Q15 was [Win32/InstalleRex](#), which was encountered by 3.8 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Algeria in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	21.1
2	Win32/leEnablerCby	Browser Modifiers	8.0
3	Win32/Sality	Viruses	8.0
4	Win32/Gamarue	Worms	5.4
5	MSIL/Bladabindi	Backdoors	4.9
6	Win32/Ramnit	Trojans	4.4
7	Win32/Kilim	Trojans	3.5
8	Win32/Yeltminky	Worms	3.3
9	Win32/Virut	Viruses	1.7
10	Win32/Parite	Viruses	1.3

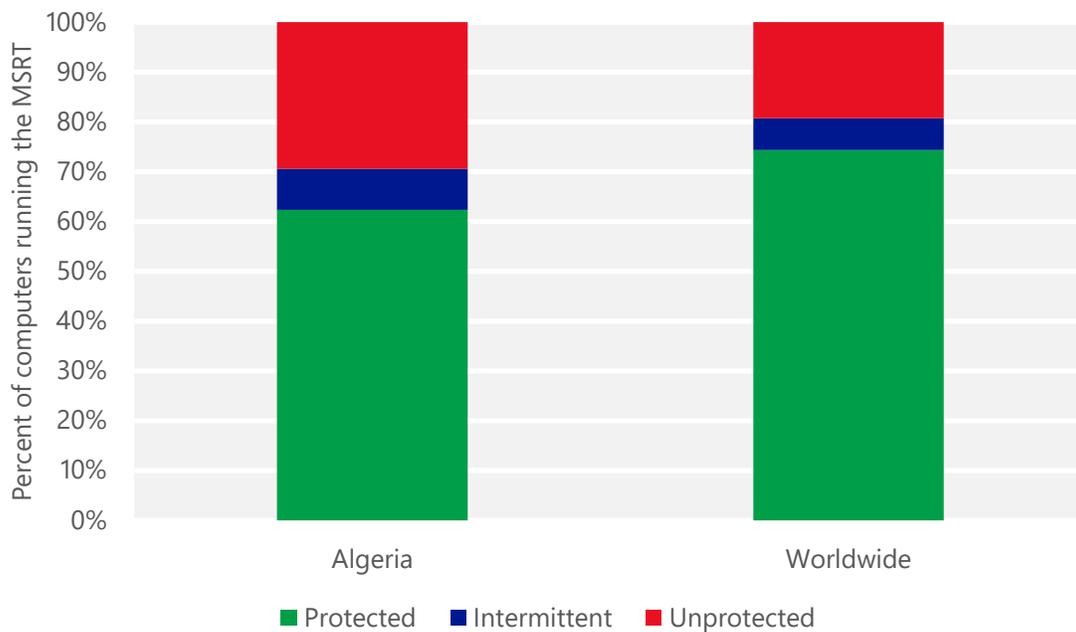
- The most common threat family infecting computers in Algeria in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 21.1 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Algeria in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 8.0 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common threat family infecting computers in Algeria in 2Q15 was [Win32/Sality](#), which was detected and removed from 8.0 of every 1,000 unique computers scanned by the MSRT. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The fourth most common threat family infecting computers in Algeria in 2Q15 was [Win32/Gamarue](#), which was detected and removed from 5.4 of every 1,000 unique computers scanned by the MSRT. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Algeria and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Algeria

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.07 (0.28)	0.07 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	2.26 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	4.51 (16.7)	

Angola

The statistics presented here are generated by Microsoft security programs and services running on computers in Angola in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Angola

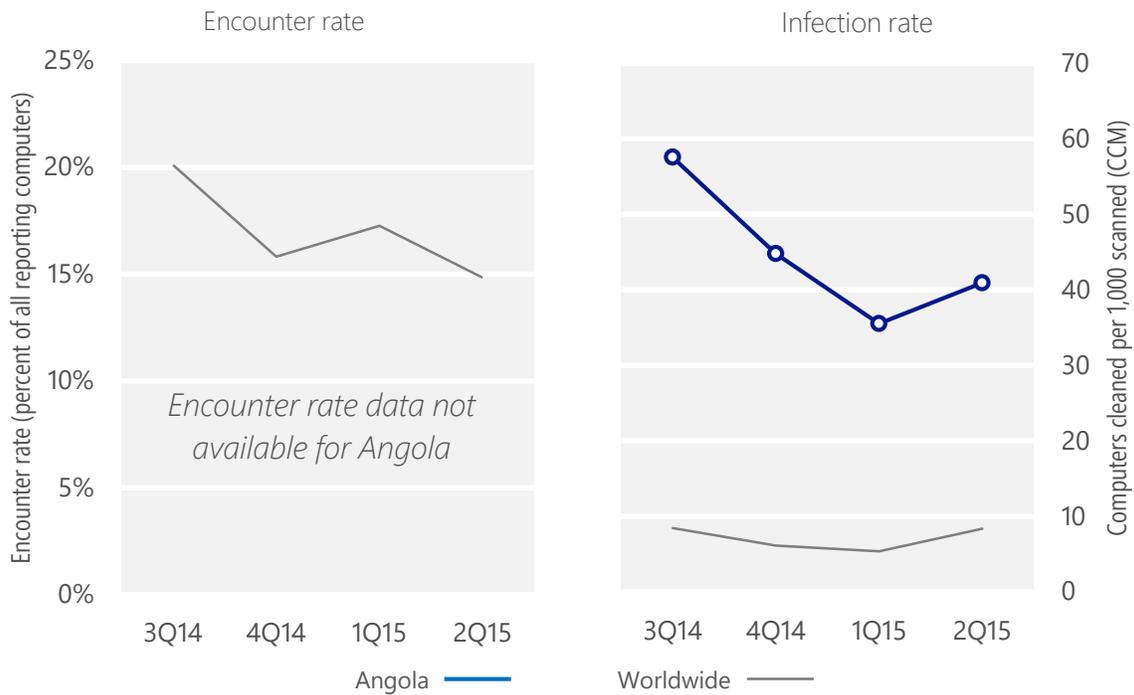
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Angola	N/A	N/A	N/A	N/A
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Angola	57.6	44.8	35.5	40.9
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcout, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, the MSRT detected and removed malware from 40.9 of every 1,000 unique computers scanned in Angola in 2Q15 (a CCM score of 40.9, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Angola over the last four quarters, compared to the world as a whole.

Malware encounter and infection rate trends in Angola and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in Angola and around the world, and for explanations of the methods and terms used here.

Top threat families by infection rate

The most common malware families by infection rate in Angola in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	19.5
2	Win32/Gamarue	Worms	7.5
3	Win32/leEnablerCby	Browser Modifiers	5.0
4	Win32/Nuqel	Worms	4.2
5	Win32/Chir	Viruses	2.6
6	Win32/Ramnit	Trojans	2.0
7	Win32/Vobfus	Worms	1.2
8	Win32/Virut	Viruses	1.0
9	Win32/Sality	Viruses	0.9
10	Win32/Tupym	Worms	0.7

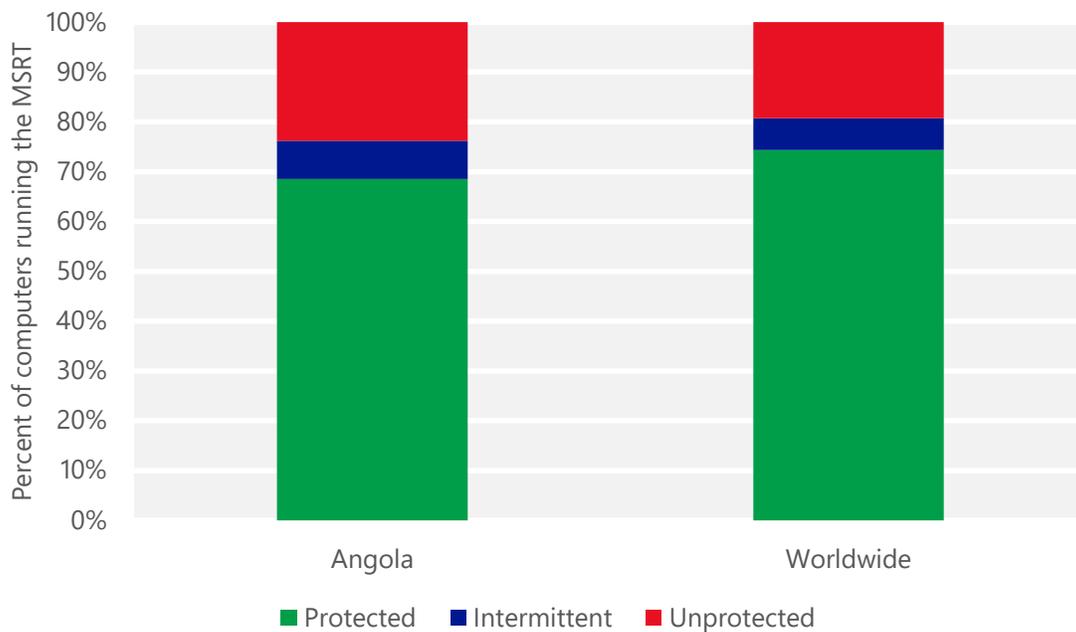
- The most common threat family infecting computers in Angola in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 19.5 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Angola in 2Q15 was [Win32/Gamarue](#), which was detected and removed from 7.5 of every 1,000 unique computers scanned by the MSRT. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The third most common threat family infecting computers in Angola in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 5.0 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The fourth most common threat family infecting computers in Angola in 2Q15 was [Win32/Nuqel](#), which was detected and removed from 4.2 of every 1,000 unique computers scanned by the MSRT. [Win32/Nuqel](#) is a worm that spreads via mapped drives and certain instant messaging applications. It may modify system settings, connect to certain websites, download arbitrary files, or take other malicious actions.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Angola and worldwide protected by real-time security software in 2Q15



Argentina

The statistics presented here are generated by Microsoft security programs and services running on computers in Argentina in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Argentina

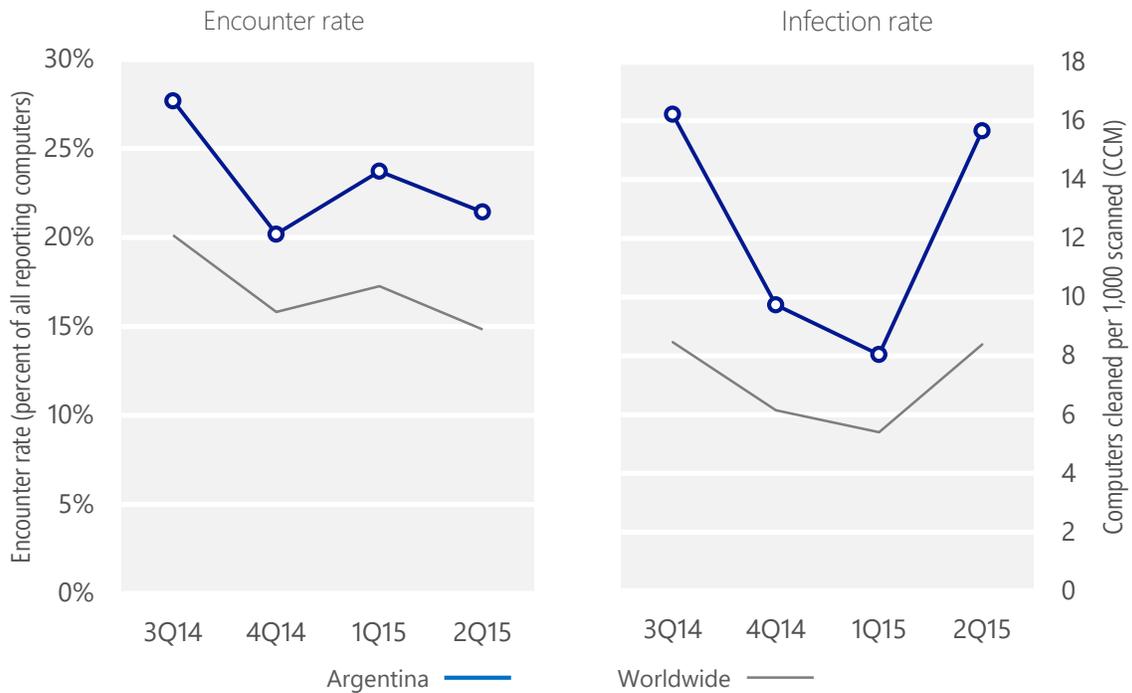
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Argentina	27.7%	20.2%	23.7%	21.4%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Argentina	16.2	9.7	8.0	15.7
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcoute, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 21.4% of computers in Argentina encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 15.7 of every 1,000 unique computers scanned in Argentina in 2Q15 (a CCM score of 15.7, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Argentina over the last four quarters, compared to the world as a whole.

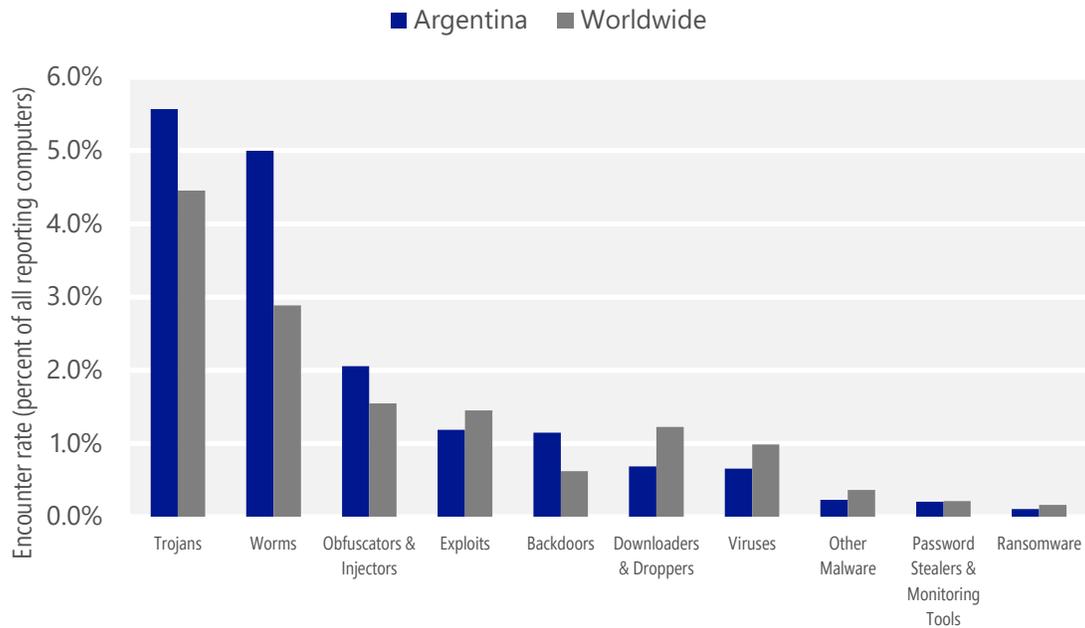
Malware encounter and infection rate trends in Argentina and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in Argentina and around the world, and for explanations of the methods and terms used here.

Malware categories

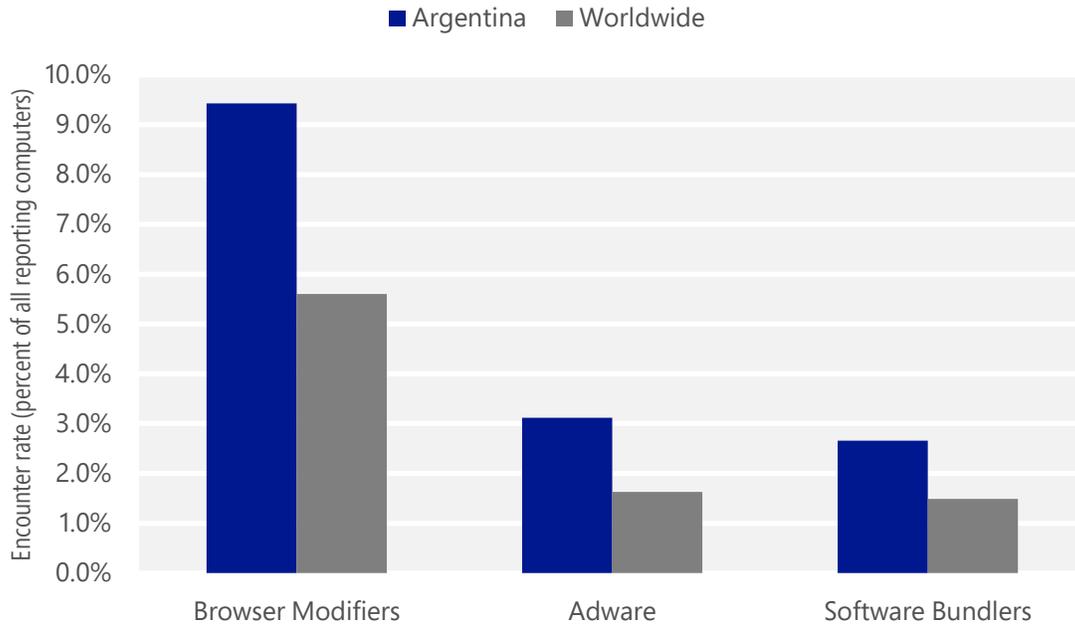
Malware encountered in Argentina in 2Q15, by category



- The most common malware category in Argentina in 2Q15 was Trojans. It was encountered by 5.6 percent of all computers there, up from 5.1 percent in 1Q15.
- The second most common malware category in Argentina in 2Q15 was Worms. It was encountered by 5.0 percent of all computers there, up from 3.8 percent in 1Q15.
- The third most common malware category in Argentina in 2Q15 was Obfuscators & Injectors, which was encountered by 2.1 percent of all computers there, down from 2.1 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Argentina in 2Q15, by category



- The most common unwanted software category in Argentina in 2Q15 was Browser Modifiers. It was encountered by 9.4 percent of all computers there, down from 12.1 percent in 1Q15.
- The second most common unwanted software category in Argentina in 2Q15 was Adware. It was encountered by 3.1 percent of all computers there, down from 6.5 percent in 1Q15.
- The third most common unwanted software category in Argentina in 2Q15 was Software Bundlers, which was encountered by 2.7 percent of all computers there, up from 0.6 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Argentina in 2Q15

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	1.4%
2	JS/Bondat	Worms	1.4%
3	Win32/Obfuscator	Obfuscators & Injectors	1.3%
4	Win32/Kilim	Trojans	1.3%
5	Win32/Skeeyah	Trojans	1.2%
6	Win32/Caphaw	Backdoors	0.7%
7	INF/Autorun	Obfuscators & Injectors	0.7%
8	JS/Axpergle	Exploits	0.6%
9	Win32/Dorkbot	Worms	0.6%
10	Win32/Conficker	Worms	0.5%

- The most common malware family encountered in Argentina in 2Q15 was [VBS/Jenxcus](#), which was encountered by 1.4 percent of reporting computers there. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common malware family encountered in Argentina in 2Q15 was [JS/Bondat](#), which was encountered by 1.4 percent of reporting computers there. [JS/Bondat](#) is a family of threats that collects information about the computer, infects removable drives, and tries to stop the user from accessing files. It spreads by infecting removable drives, such as USB thumb drives and flash drives.
- The third most common malware family encountered in Argentina in 2Q15 was [Win32/Obfuscator](#), which was encountered by 1.3 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The fourth most common malware family encountered in Argentina in 2Q15 was [Win32/Kilim](#), which was encountered by 1.3 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Argentina in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	5.2%
2	Win32/KipodToolsCby	Browser Modifiers	2.9%
3	Win32/InstalleRex	Software Bundlers	2.5%
4	Win32/SaverExtension	Adware	1.6%
5	Win32/AlterbookSP	Browser Modifiers	1.1%

- The most common unwanted software family encountered in Argentina in 2Q15 was [Win32/CouponRuc](#), which was encountered by 5.2 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in Argentina in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 2.9 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common unwanted software family encountered in Argentina in 2Q15 was [Win32/InstalleRex](#), which was encountered by 2.5 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Argentina in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	6.2
2	VBS/Jenxcus	Worms	2.5
3	Win32/Kilim	Trojans	1.7
4	Win32/CompromisedCert	Other Malware	1.0
5	Win32/Dorkbot	Worms	0.9
6	Win32/Sality	Viruses	0.8
7	Win32/Brontok	Worms	0.4
8	Win32/Ramnit	Trojans	0.4
9	Win32/Wysotot	Trojans	0.4
10	Win32/Lethic	Trojans	0.3

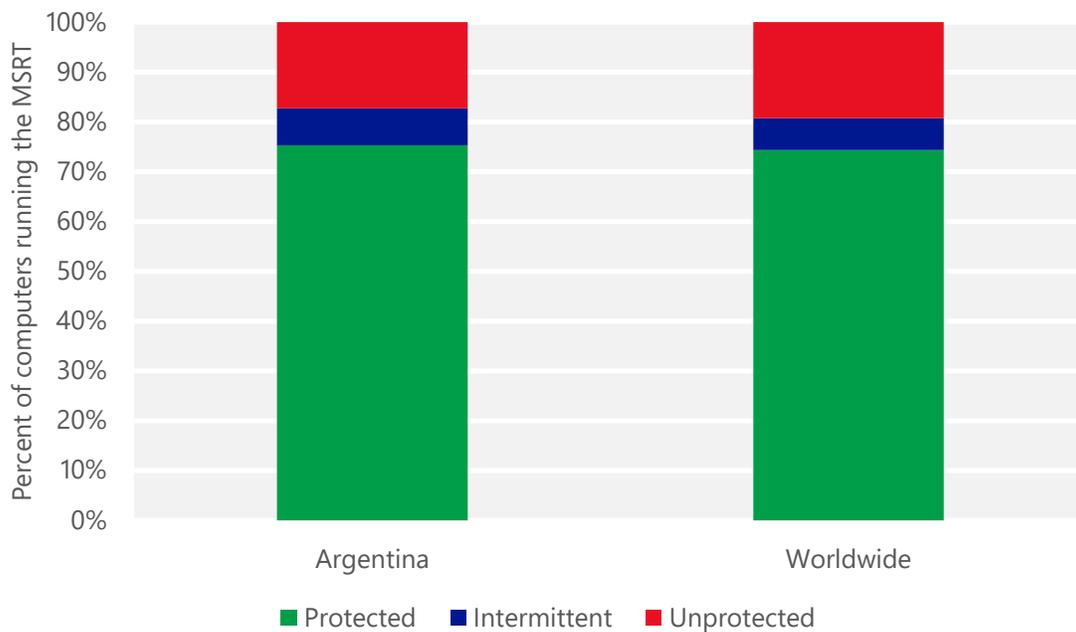
- The most common threat family infecting computers in Argentina in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 6.2 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Argentina in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 2.5 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The third most common threat family infecting computers in Argentina in 2Q15 was [Win32/Kilim](#), which was detected and removed from 1.7 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The fourth most common threat family infecting computers in Argentina in 2Q15 was [Win32/CompromisedCert](#), which was detected and removed from 1.0 of every 1,000 unique computers scanned by the MSRT. [Win32/CompromisedCert](#) is a detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Argentina and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Argentina

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.08 (0.28)	0.12 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	6.92 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	20.17 (16.7)	

Australia

The statistics presented here are generated by Microsoft security programs and services running on computers in Australia in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille, or CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Australia

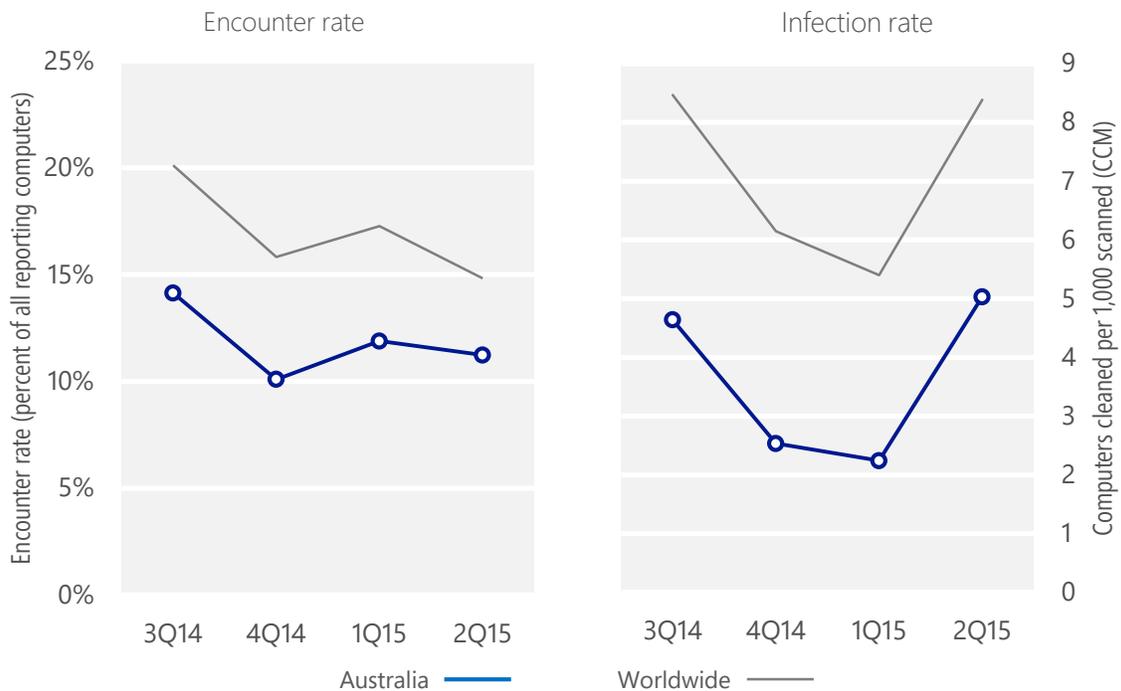
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Australia	14.1%	10.1%	11.9%	11.2%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Australia	4.6	2.5	2.2	5.0
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcote, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 11.2% of computers in Australia encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 5.0 of every 1,000 unique computers scanned in Australia in 2Q15 (a CCM score of 5.0, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Australia over the last four quarters, compared to the world as a whole.

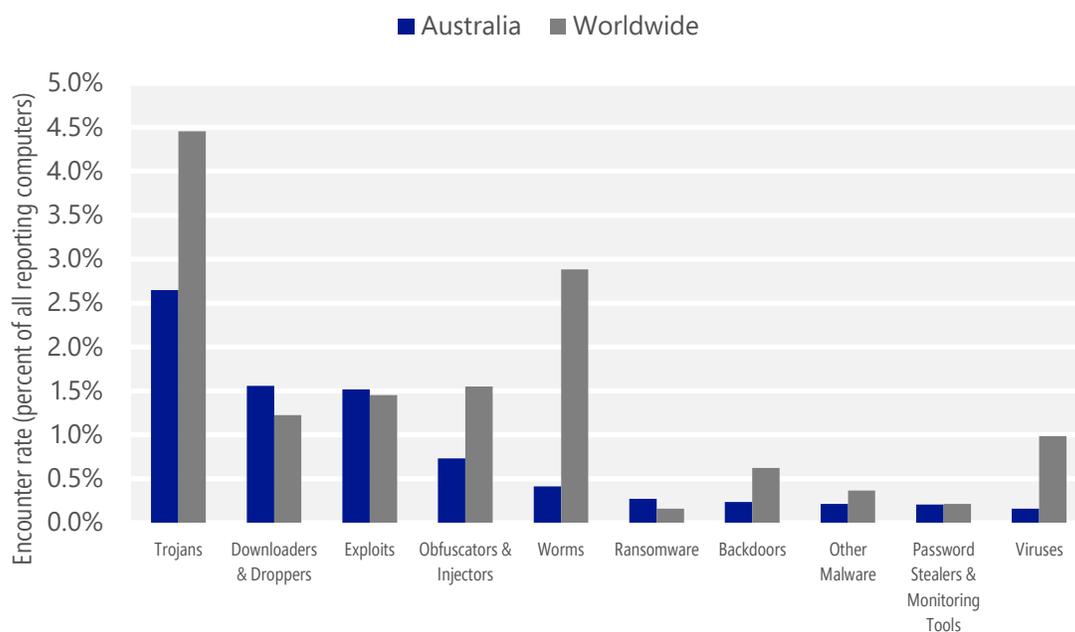
Malware encounter and infection rate trends in Australia and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in Australia and around the world, and for explanations of the methods and terms used here.

Malware categories

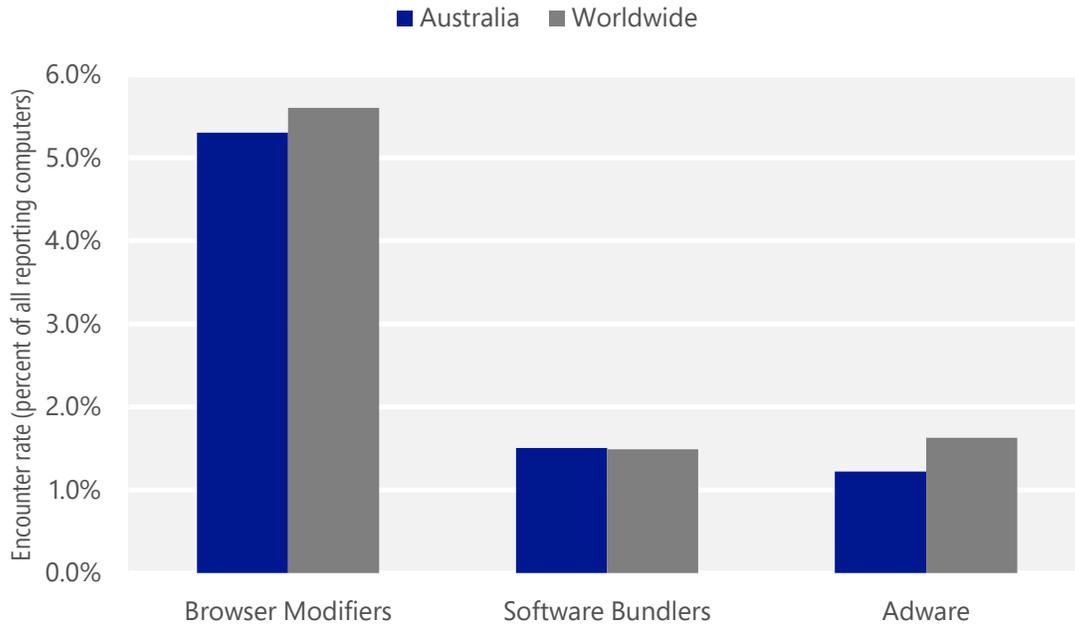
Malware encountered in Australia in 2Q15, by category



- The most common malware category in Australia in 2Q15 was Trojans. It was encountered by 2.6 percent of all computers there, up from 2.1 percent in 1Q15.
- The second most common malware category in Australia in 2Q15 was Downloaders & Droppers. It was encountered by 1.6 percent of all computers there, down from 1.9 percent in 1Q15.
- The third most common malware category in Australia in 2Q15 was Exploits, which was encountered by 1.5 percent of all computers there, up from 1.4 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Australia in 2Q15, by category



- The most common unwanted software category in Australia in 2Q15 was Browser Modifiers. It was encountered by 5.3 percent of all computers there, up from 4.7 percent in 1Q15.
- The second most common unwanted software category in Australia in 2Q15 was Software Bundlers. It was encountered by 1.5 percent of all computers there, down from 3.3 percent in 1Q15.
- The third most common unwanted software category in Australia in 2Q15 was Adware, which was encountered by 1.2 percent of all computers there, up from 0.8 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Australia in 2Q15

	Family	Most significant category	% of reporting computers
1	JS/Axpergle	Exploits	0.9%
2	Win32/Obfuscator	Obfuscators & Injectors	0.6%
3	Win32/Kilim	Trojans	0.6%
4	Win32/Skeeyah	Trojans	0.6%
5	Win32/Peals	Trojans	0.5%
6	Win32/Upatre	Downloaders & Droppers	0.3%
7	Win32/Sdbby	Exploits	0.2%
8	Win32/Dynamer	Trojans	0.2%
9	Win32/Crowti	Ransomware	0.2%
10	JS/Neclu	Exploits	0.2%

- The most common malware family encountered in Australia in 2Q15 was [JS/Axpergle](#), which was encountered by 0.9 percent of reporting computers there. [JS/Axpergle](#) is a detection for the Angler exploit kit, which exploits vulnerabilities in recent versions of Internet Explorer, Silverlight, Adobe Flash Player, and Java to install malware.
- The second most common malware family encountered in Australia in 2Q15 was [Win32/Obfuscator](#), which was encountered by 0.6 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The third most common malware family encountered in Australia in 2Q15 was [Win32/Kilim](#), which was encountered by 0.6 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The fourth most common malware family encountered in Australia in 2Q15 was [Win32/Skeeyah](#), which was encountered by 0.6 percent of reporting computers there. [Win32/Skeeyah](#) is a generic detection for various threats that display trojan characteristics.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Australia in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	2.3%
2	Win32/KipodToolsCby	Browser Modifiers	1.8%
3	Win32/InstalleRex	Software Bundlers	1.3%
4	Win32/AlterbookSP	Browser Modifiers	0.9%
5	Win32/SaverExtension	Adware	0.7%

- The most common unwanted software family encountered in Australia in 2Q15 was [Win32/CouponRuc](#), which was encountered by 2.3 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in Australia in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 1.8 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common unwanted software family encountered in Australia in 2Q15 was [Win32/InstalleRex](#), which was encountered by 1.3 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Australia in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	1.5
2	Win32/Kilim	Trojans	1.2
3	Win32/CompromisedCert	Other Malware	0.6
4	Win32/Simda	Trojans	0.2
5	Win32/Dyzap	Password Stealers & Monitoring Tools	0.2
6	Win32/Zbot	Password Stealers & Monitoring Tools	0.1
7	Win32/Alureon	Trojans	0.1
8	Win32/Carberp	Trojans	0.1
9	VBS/Jenxcus	Worms	0.1
10	Win32/Brontok	Worms	0.1

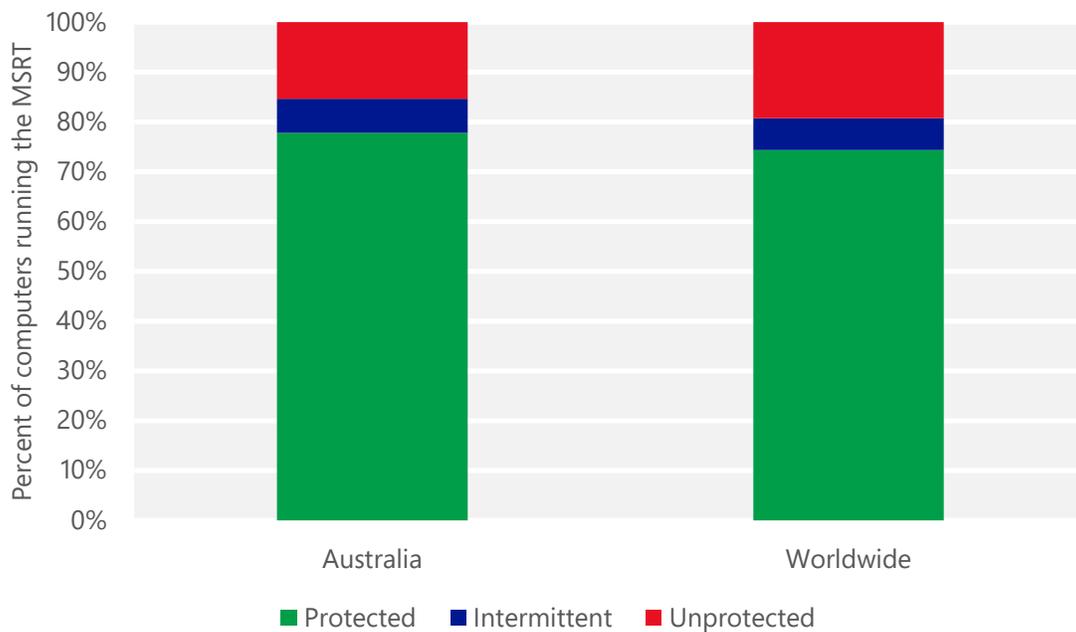
- The most common threat family infecting computers in Australia in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 1.5 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Australia in 2Q15 was [Win32/Kilim](#), which was detected and removed from 1.2 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The third most common threat family infecting computers in Australia in 2Q15 was [Win32/CompromisedCert](#), which was detected and removed from 0.6 of every 1,000 unique computers scanned by the MSRT. [Win32/CompromisedCert](#) is a detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.
- The fourth most common threat family infecting computers in Australia in 2Q15 was [Win32/Simda](#), which was detected and removed from 0.2 of every 1,000 unique computers scanned by the MSRT. [Win32/Simda](#) is a threat that can give an attacker backdoor access and control of an infected computer. It can then steal passwords and gather information about the computer to send to the attacker.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Australia and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Australia

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.05 (0.28)	0.11 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	7.33 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	16.77 (16.7)	

Austria

The statistics presented here are generated by Microsoft security programs and services running on computers in Austria in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Austria

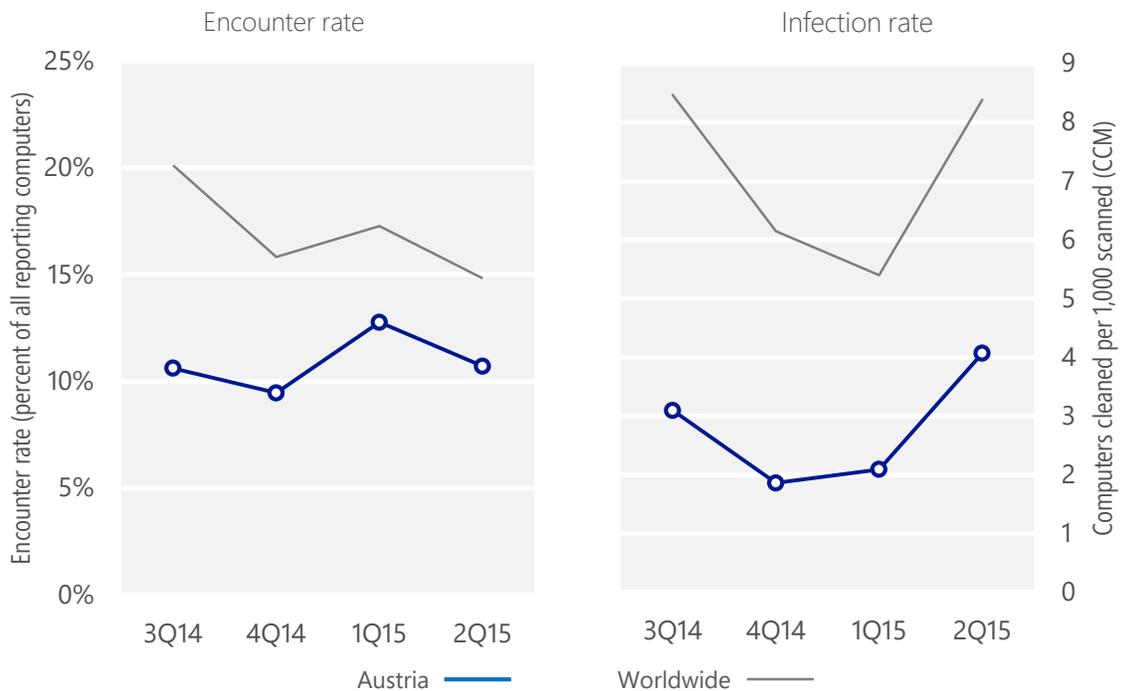
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Austria	10.6%	9.5%	12.8%	10.7%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Austria	3.1	1.9	2.1	4.1
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcout, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 10.7% of computers in Austria encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 4.1 of every 1,000 unique computers scanned in Austria in 2Q15 (a CCM score of 4.1, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Austria over the last four quarters, compared to the world as a whole.

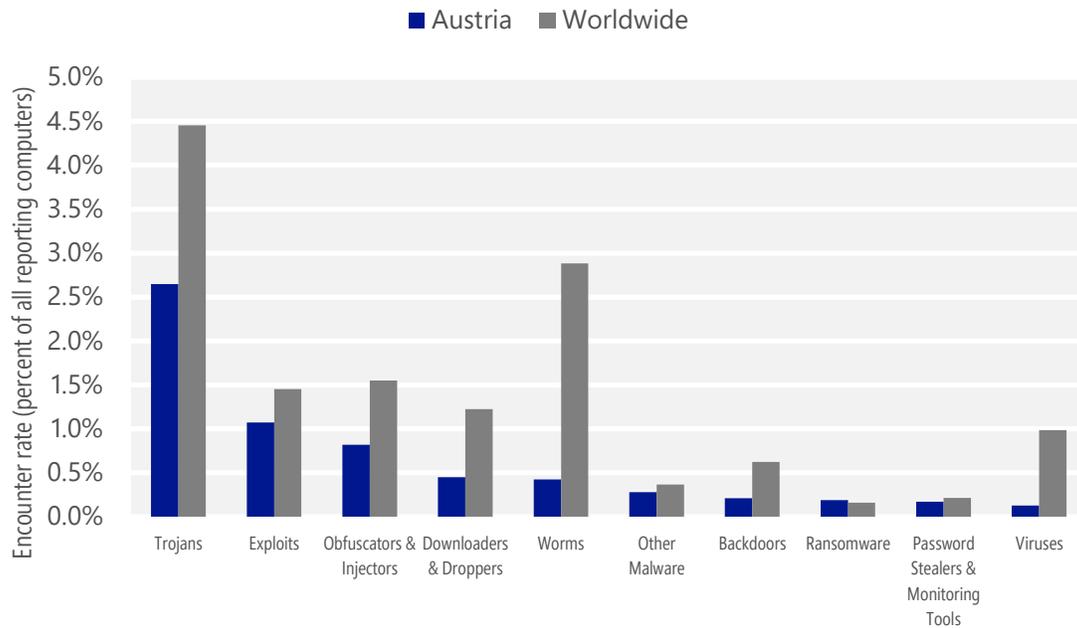
Malware encounter and infection rate trends in Austria and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in Austria and around the world, and for explanations of the methods and terms used here.

Malware categories

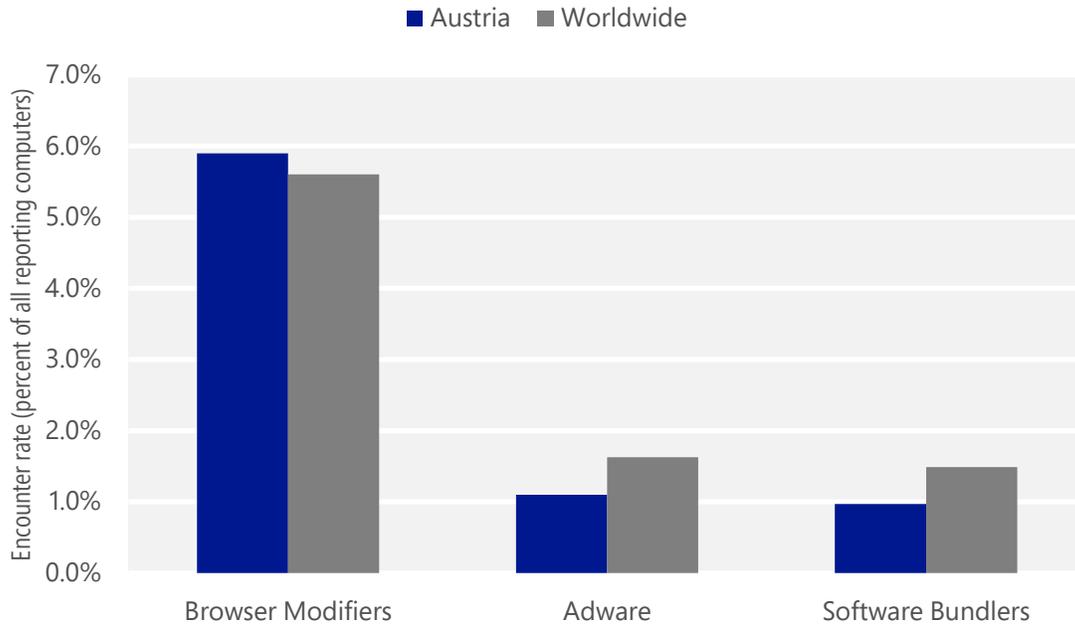
Malware encountered in Austria in 2Q15, by category



- The most common malware category in Austria in 2Q15 was Trojans. It was encountered by 2.6 percent of all computers there, up from 2.2 percent in 1Q15.
- The second most common malware category in Austria in 2Q15 was Exploits. It was encountered by 1.1 percent of all computers there, down from 2.0 percent in 1Q15.
- The third most common malware category in Austria in 2Q15 was Obfuscators & Injectors, which was encountered by 0.8 percent of all computers there, down from 1.0 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Austria in 2Q15, by category



- The most common unwanted software category in Austria in 2Q15 was Browser Modifiers. It was encountered by 5.9 percent of all computers there, down from 6.2 percent in 1Q15.
- The second most common unwanted software category in Austria in 2Q15 was Adware. It was encountered by 1.1 percent of all computers there, down from 3.2 percent in 1Q15.
- The third most common unwanted software category in Austria in 2Q15 was Software Bundlers, which was encountered by 1.0 percent of all computers there, up from 0.3 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Austria in 2Q15

	Family	Most significant category	% of reporting computers
1	JS/Axpergle	Exploits	0.7%
2	Win32/Skeeyah	Trojans	0.5%
3	Win32/Peals	Trojans	0.5%
4	Win32/Obfuscator	Obfuscators & Injectors	0.5%
5	Win32/Kilim	Trojans	0.4%
6	Win32/Emotet	Trojans	0.4%
7	Win32/Dynamer	Trojans	0.2%
8	Win32/CeelInject	Obfuscators & Injectors	0.2%
9	JS/Neclu	Exploits	0.1%
10	Win32/Conficker	Worms	0.1%

- The most common malware family encountered in Austria in 2Q15 was [JS/Axpergle](#), which was encountered by 0.7 percent of reporting computers there. [JS/Axpergle](#) is a detection for the Angler exploit kit, which exploits vulnerabilities in recent versions of Internet Explorer, Silverlight, Adobe Flash Player, and Java to install malware.
- The second most common malware family encountered in Austria in 2Q15 was [Win32/Skeeyah](#), which was encountered by 0.5 percent of reporting computers there. [Win32/Skeeyah](#) is a generic detection for various threats that display trojan characteristics.
- The third most common malware family encountered in Austria in 2Q15 was [Win32/Peals](#), which was encountered by 0.5 percent of reporting computers there. [Win32/Peals](#) is a generic detection for various threats that display trojan characteristics.
- The fourth most common malware family encountered in Austria in 2Q15 was [Win32/Obfuscator](#), which was encountered by 0.5 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Austria in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/KipodToolsCby	Browser Modifiers	2.6%
2	Win32/CouponRuc	Browser Modifiers	2.3%
3	Win32/AlterbookSP	Browser Modifiers	1.0%
4	Win32/InstalleRex	Software Bundlers	0.9%
5	Win32/SaverExtension	Adware	0.8%

- The most common unwanted software family encountered in Austria in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 2.6 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common unwanted software family encountered in Austria in 2Q15 was [Win32/CouponRuc](#), which was encountered by 2.3 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The third most common unwanted software family encountered in Austria in 2Q15 was [Win32/AlterbookSP](#), which was encountered by 1.0 percent of reporting computers there. [Win32/AlterbookSP](#) is a browser add-on that formerly displayed behaviors of unwanted software. Recent versions of the add-on no longer meet Microsoft detection criteria, and are no longer considered unwanted software.

Top threat families by infection rate

The most common malware families by infection rate in Austria in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	1.2
2	Win32/Kilim	Trojans	0.8
3	Win32/CompromisedCert	Other Malware	0.5
4	Win32/Emotet	Trojans	0.4
5	Win32/Nitol	Other Malware	0.1
6	Win32/Zbot	Password Stealers & Monitoring Tools	0.1
7	Win32/Sality	Viruses	0.1
8	MSIL/Bladabindi	Backdoors	0.1
9	Win32/Simda	Trojans	0.1
10	Win32/Alureon	Trojans	0.1

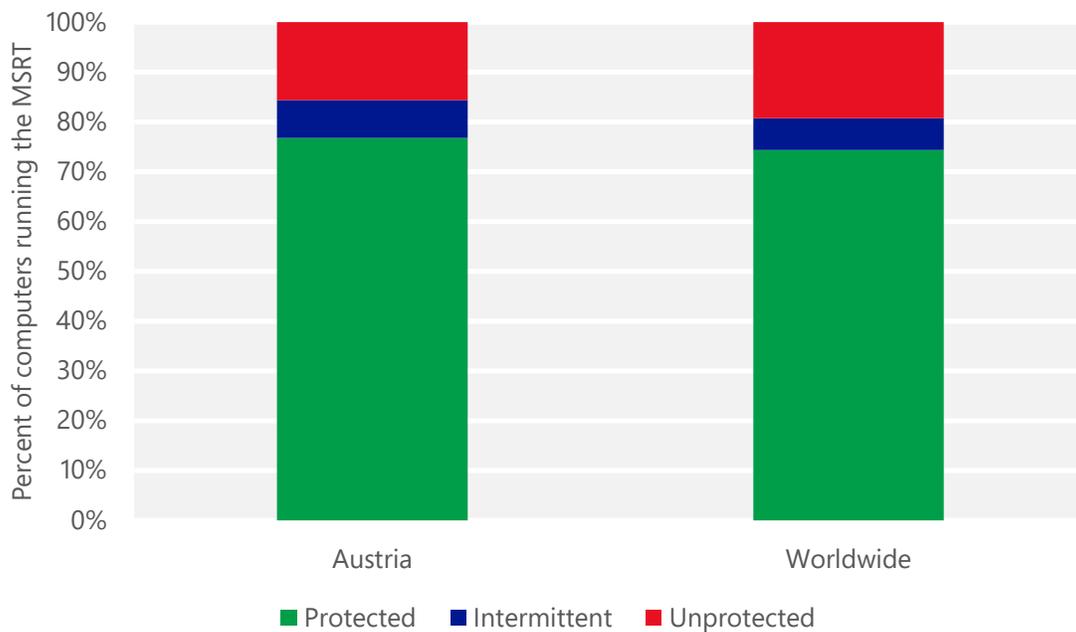
- The most common threat family infecting computers in Austria in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 1.2 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Austria in 2Q15 was [Win32/Kilim](#), which was detected and removed from 0.8 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The third most common threat family infecting computers in Austria in 2Q15 was [Win32/CompromisedCert](#), which was detected and removed from 0.5 of every 1,000 unique computers scanned by the MSRT. [Win32/CompromisedCert](#) is a detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.
- The fourth most common threat family infecting computers in Austria in 2Q15 was [Win32/Emotet](#), which was detected and removed from 0.4 of every 1,000 unique computers scanned by the MSRT. [Win32/Emotet](#) is a threat that can steal personal information, including banking user names and passwords. It is usually installed when the user opens a spam email attachment.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Austria and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Austria

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.04 (0.28)	0.03 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	3.10 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	12.92 (16.7)	

Bahamas, The

The statistics presented here are generated by Microsoft security programs and services running on computers in the Bahamas in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for the Bahamas

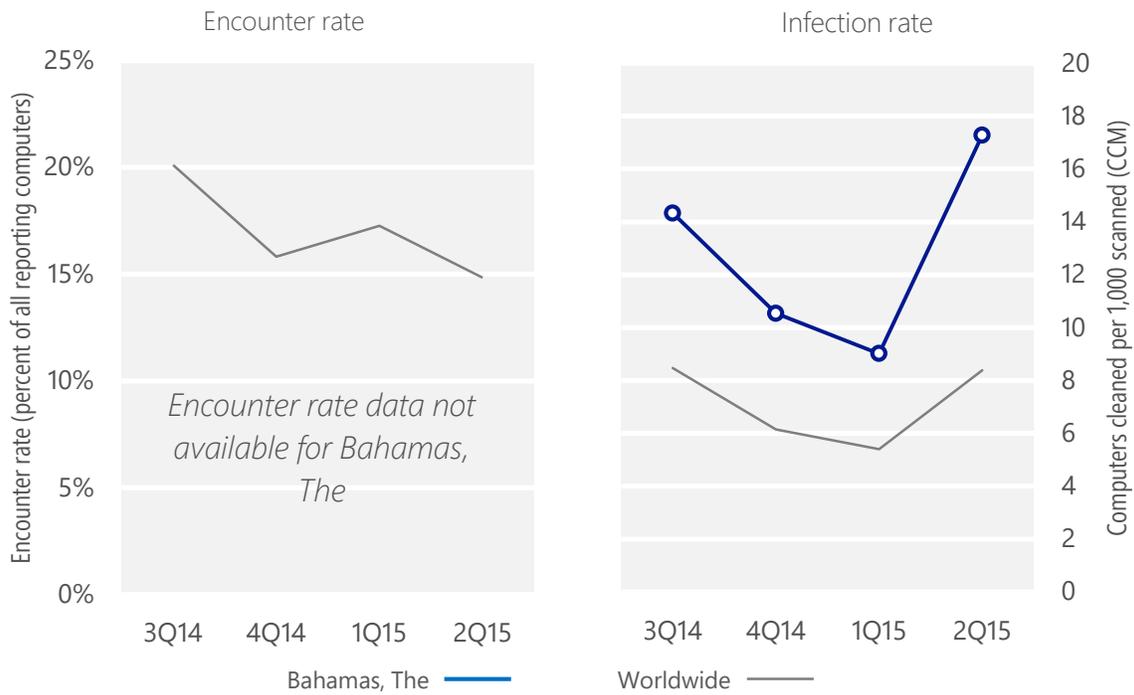
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Bahamas, The	N/A	N/A	N/A	N/A
<i>Worldwide encounter rate</i>	20.1%	15.8%	17.3%	14.8%
CCM, Bahamas, The	14.3	10.5	9.0	17.3
<i>Worldwide CCM</i>	8.5	6.1	5.4	8.4

Encounter and infection rates reported here do not include totals for the Brantall, Filcout, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, the MSRT detected and removed malware from 17.3 of every 1,000 unique computers scanned in the Bahamas in 2Q15 (a CCM score of 17.3, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for the Bahamas over the last four quarters, compared to the world as a whole.

Malware encounter and infection rate trends in the Bahamas and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in the Bahamas and around the world, and for explanations of the methods and terms used here.

Top threat families by infection rate

The most common malware families by infection rate in the Bahamas in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	8.2
2	VBS/Jenxcus	Worms	2.4
3	Win32/Kilim	Trojans	2.0
4	Win32/Vobfus	Worms	1.2
5	Win32/Brontok	Worms	1.0
6	Win32/Sality	Viruses	0.5
7	Win32/CompromisedCert	Other Malware	0.4
8	Win32/Dorkbot	Worms	0.3
9	Win32/Simda	Trojans	0.2
10	Win32/Dyzap	Password Stealers & Monitoring Tools	0.2

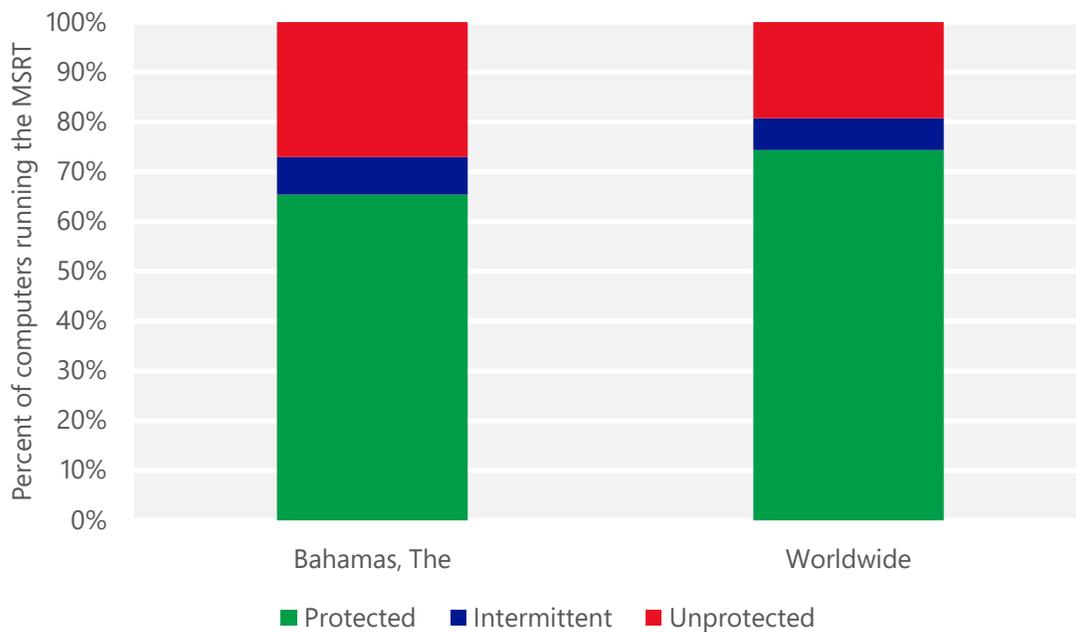
- The most common threat family infecting computers in the Bahamas in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 8.2 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in the Bahamas in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 2.4 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The third most common threat family infecting computers in the Bahamas in 2Q15 was [Win32/Kilim](#), which was detected and removed from 2.0 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The fourth most common threat family infecting computers in the Bahamas in 2Q15 was [Win32/Vobfus](#), which was detected and removed from 1.2 of every 1,000 unique computers scanned by the MSRT. [Win32/Vobfus](#) is a family of worms that spreads via network drives and removable drives and download/executes arbitrary files. Downloaded files may include additional malware.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in the Bahamas and worldwide protected by real-time security software in 2Q15



Bahrain

The statistics presented here are generated by Microsoft security programs and services running on computers in Bahrain in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Bahrain

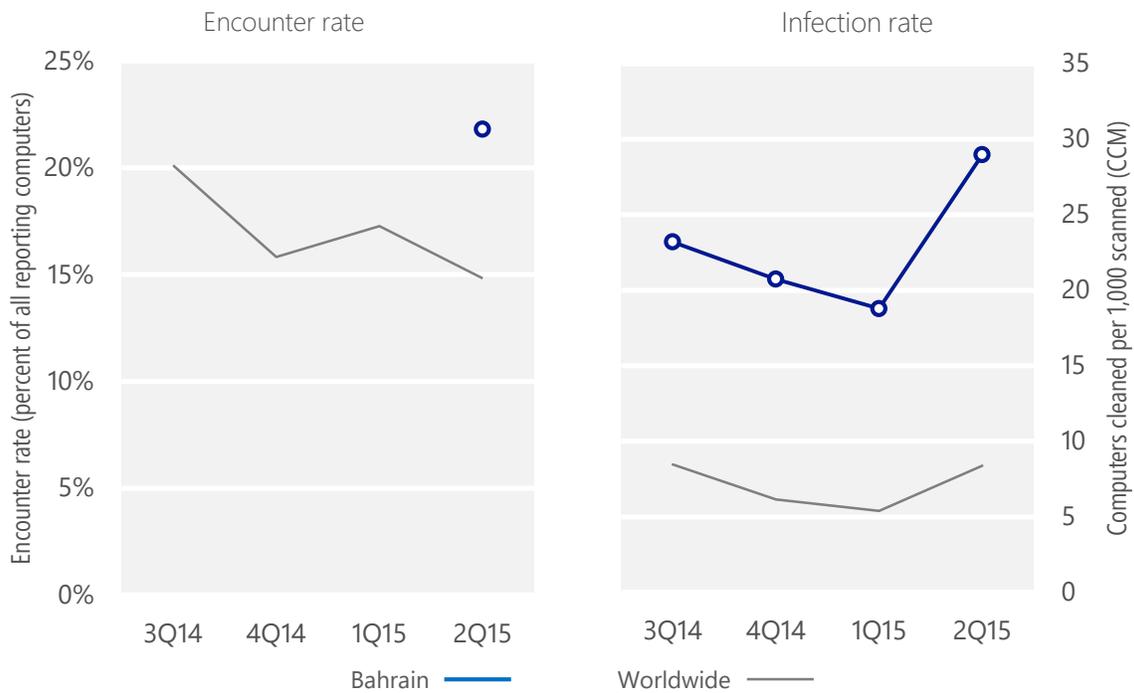
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Bahrain	N/A	N/A	N/A	21.8%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Bahrain	23.2	20.7	18.8	29.0
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcote, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 21.8% of computers in Bahrain encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 29.0 of every 1,000 unique computers scanned in Bahrain in 2Q15 (a CCM score of 29.0, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Bahrain over the last four quarters, compared to the world as a whole.

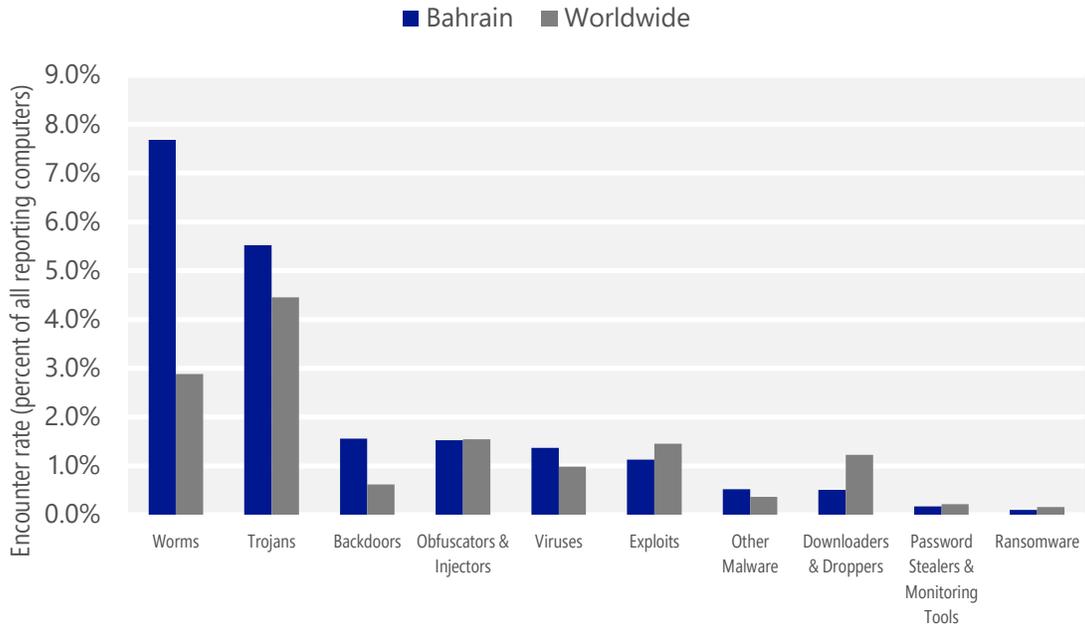
Malware encounter and infection rate trends in Bahrain and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in Bahrain and around the world, and for explanations of the methods and terms used here.

Malware categories

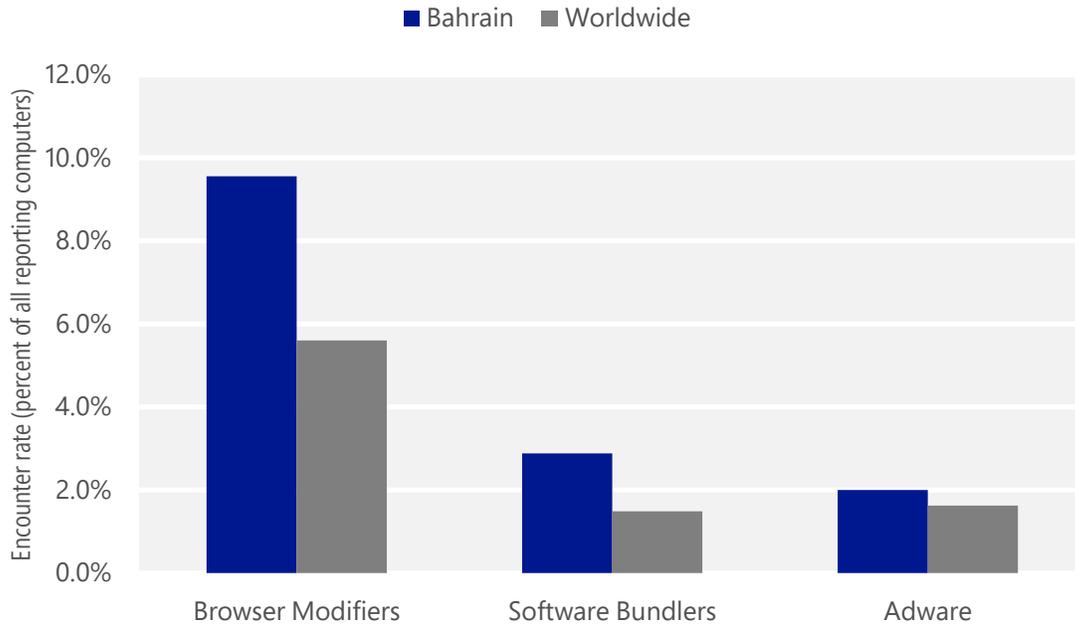
Malware encountered in Bahrain in 2Q15, by category



- The most common malware category in Bahrain in 2Q15 was Worms. It was encountered by 7.7 percent of all computers there, up from N/A percent in 1Q15.
- The second most common malware category in Bahrain in 2Q15 was Trojans. It was encountered by 5.5 percent of all computers there, up from N/A percent in 1Q15.
- The third most common malware category in Bahrain in 2Q15 was Backdoors, which was encountered by 1.6 percent of all computers there, up from N/A percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Bahrain in 2Q15, by category



- The most common unwanted software category in Bahrain in 2Q15 was Browser Modifiers. It was encountered by 9.6 percent of all computers there, up from N/A percent in 1Q15.
- The second most common unwanted software category in Bahrain in 2Q15 was Software Bundlers. It was encountered by 2.9 percent of all computers there, up from N/A percent in 1Q15.
- The third most common unwanted software category in Bahrain in 2Q15 was Adware, which was encountered by 2.0 percent of all computers there, up from N/A percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Bahrain in 2Q15

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	<0.1%
2	INF/Autorun	Obfuscators & Injectors	<0.1%
3	Win32/Skeeyah	Trojans	<0.1%
4	Win32/Kilim	Trojans	<0.1%
5	Win32/Gamarue	Worms	<0.1%
6	Win32/Obfuscator	Obfuscators & Injectors	<0.1%
7	MSIL/Bladabindi	Backdoors	<0.1%
8	Win32/Nuqel	Worms	<0.1%
9	Win32/Peals	Trojans	<0.1%
10	Win32/Caphaw	Backdoors	<0.1%

- The most common malware family encountered in Bahrain in 2Q15 was [VBS/Jenxcus](#), which was encountered by <0.1 percent of reporting computers there. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common malware family encountered in Bahrain in 2Q15 was [INF/Autorun](#), which was encountered by <0.1 percent of reporting computers there. [INF/Autorun](#) is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The third most common malware family encountered in Bahrain in 2Q15 was [Win32/Skeeyah](#), which was encountered by <0.1 percent of reporting computers there. [Win32/Skeeyah](#) is a generic detection for various threats that display trojan characteristics.
- The fourth most common malware family encountered in Bahrain in 2Q15 was [Win32/Kilim](#), which was encountered by <0.1 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Bahrain in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/KipodToolsCby	Browser Modifiers	<0.1%
2	Win32/CouponRuc	Browser Modifiers	<0.1%
3	Win32/InstalleRex	Software Bundlers	<0.1%
4	Win32/SaverExtension	Adware	<0.1%
5	Win32/Vonteera	Browser Modifiers	<0.1%

- The most common unwanted software family encountered in Bahrain in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by <0.1 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common unwanted software family encountered in Bahrain in 2Q15 was [Win32/CouponRuc](#), which was encountered by <0.1 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The third most common unwanted software family encountered in Bahrain in 2Q15 was [Win32/InstalleRex](#), which was encountered by <0.1 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Bahrain in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	7.4
2	VBS/Jenxcus	Worms	7.1
3	Win32/CompromisedCert	Other Malware	4.1
4	Win32/Sality	Viruses	1.9
5	Win32/Nuqel	Worms	1.8
6	Win32/Gamarue	Worms	1.5
7	Win32/Kilim	Trojans	1.5
8	MSIL/Bladabindi	Backdoors	1.3
9	Win32/Dorkbot	Worms	1.0
10	Win32/Ramnit	Trojans	0.9

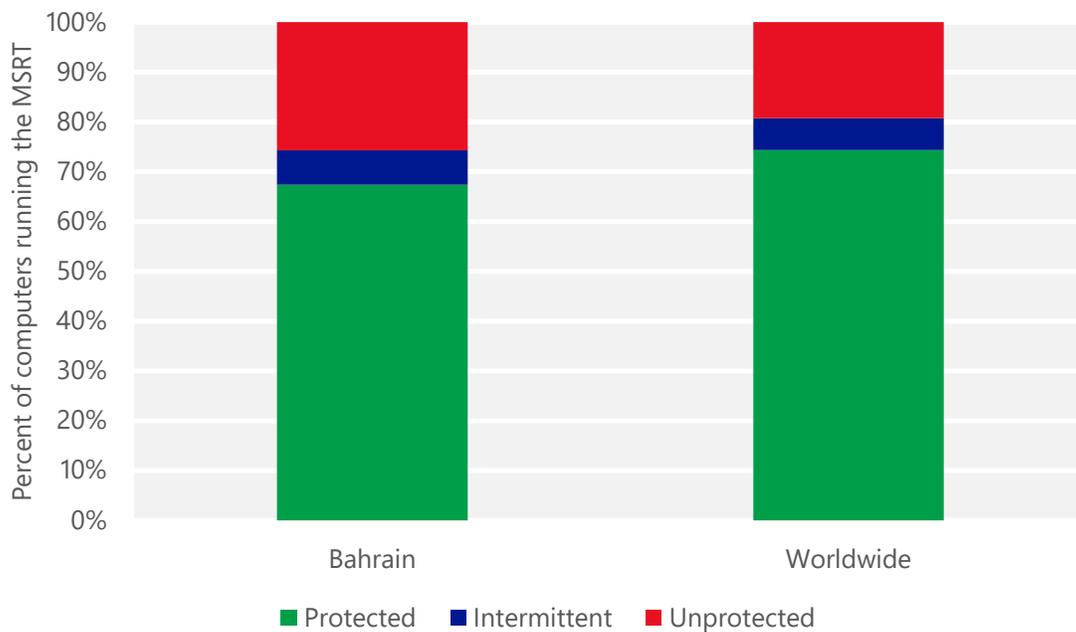
- The most common threat family infecting computers in Bahrain in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 7.4 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Bahrain in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 7.1 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The third most common threat family infecting computers in Bahrain in 2Q15 was [Win32/CompromisedCert](#), which was detected and removed from 4.1 of every 1,000 unique computers scanned by the MSRT. [Win32/CompromisedCert](#) is a detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.
- The fourth most common threat family infecting computers in Bahrain in 2Q15 was [Win32/Sality](#), which was detected and removed from 1.9 of every 1,000 unique computers scanned by the MSRT. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Bahrain and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Bahrain

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.00 (0.28)	0.00 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	N/A (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	4.64 (16.7)	

Bangladesh

The statistics presented here are generated by Microsoft security programs and services running on computers in Bangladesh in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Bangladesh

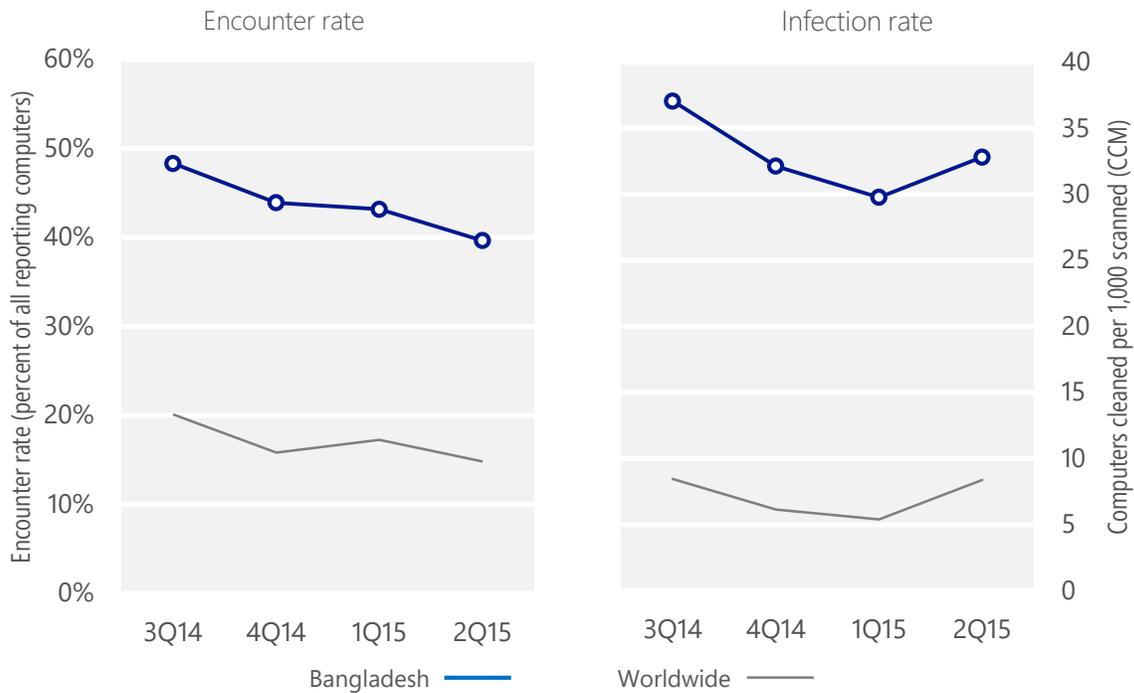
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Bangladesh	48.3%	43.9%	43.2%	39.7%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Bangladesh	37.1	32.1	29.8	32.8
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcote, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 39.7% of computers in Bangladesh encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 32.8 of every 1,000 unique computers scanned in Bangladesh in 2Q15 (a CCM score of 32.8, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Bangladesh over the last four quarters, compared to the world as a whole.

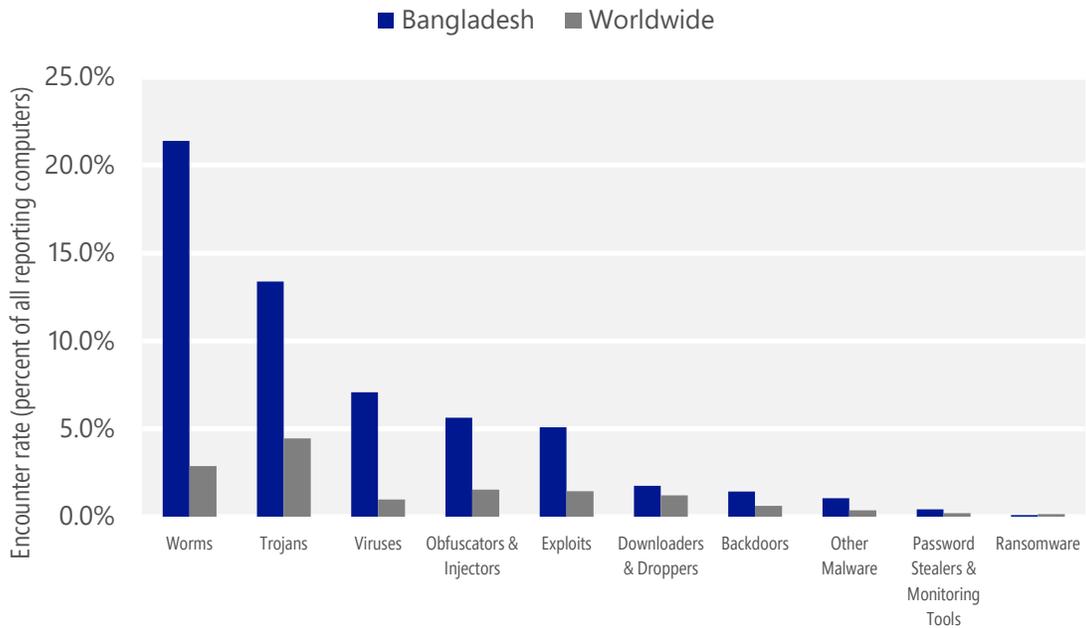
Malware encounter and infection rate trends in Bangladesh and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in Bangladesh and around the world, and for explanations of the methods and terms used here.

Malware categories

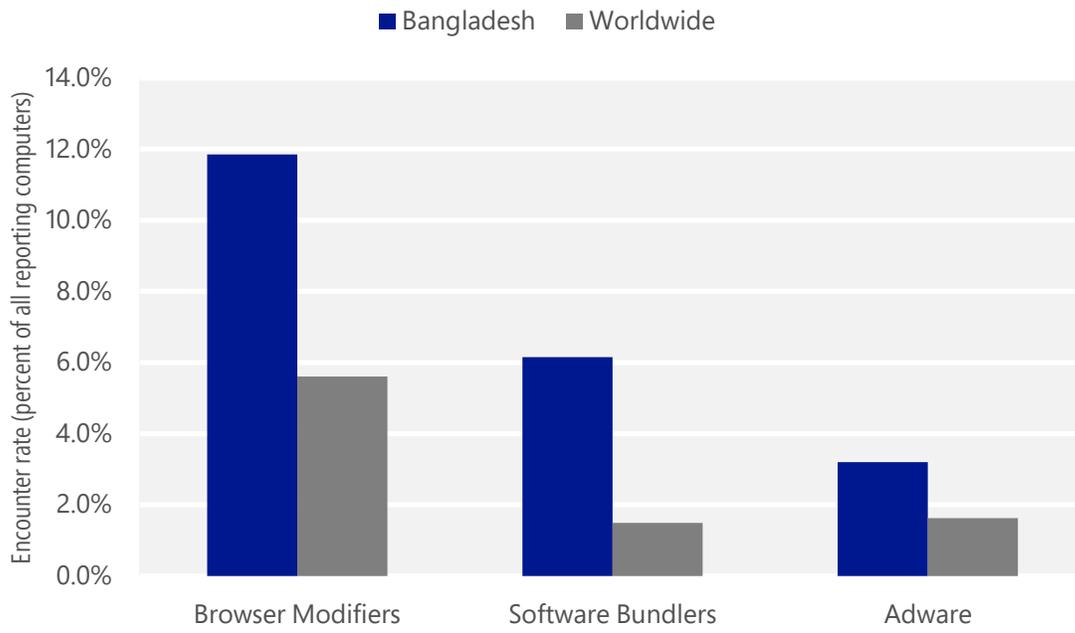
Malware encountered in Bangladesh in 2Q15, by category



- The most common malware category in Bangladesh in 2Q15 was Worms. It was encountered by 21.4 percent of all computers there, down from 22.0 percent in 1Q15.
- The second most common malware category in Bangladesh in 2Q15 was Trojans. It was encountered by 13.4 percent of all computers there, down from 13.9 percent in 1Q15.
- The third most common malware category in Bangladesh in 2Q15 was Viruses, which was encountered by 7.1 percent of all computers there, down from 9.0 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Bangladesh in 2Q15, by category



- The most common unwanted software category in Bangladesh in 2Q15 was Browser Modifiers. It was encountered by 11.9 percent of all computers there, down from 16.0 percent in 1Q15.
- The second most common unwanted software category in Bangladesh in 2Q15 was Software Bundlers. It was encountered by 6.2 percent of all computers there, down from 7.8 percent in 1Q15.
- The third most common unwanted software category in Bangladesh in 2Q15 was Adware, which was encountered by 3.2 percent of all computers there, up from 1.6 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Bangladesh in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Ippedo	Worms	13.6%
2	INF/Autorun	Obfuscators & Injectors	6.9%
3	Win32/Gamarue	Worms	6.3%
4	Win32/Ramnit	Trojans	5.4%
5	VBS/Jenxcus	Worms	5.4%
6	Win32/CplLnk	Exploits	4.4%
7	Win32/Sality	Viruses	3.3%
8	Win32/Obfuscator	Obfuscators & Injectors	3.1%
9	Win32/Virut	Viruses	1.9%
10	Win32/Skeeyah	Trojans	1.5%

- The most common malware family encountered in Bangladesh in 2Q15 was [Win32/Ippedo](#), which was encountered by 13.6 percent of reporting computers there. [Win32/Ippedo](#) is a worm that can send sensitive information to a malicious hacker. It spreads through removable drives, such as USB flash drives.
- The second most common malware family encountered in Bangladesh in 2Q15 was [INF/Autorun](#), which was encountered by 6.9 percent of reporting computers there. [INF/Autorun](#) is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The third most common malware family encountered in Bangladesh in 2Q15 was [Win32/Gamarue](#), which was encountered by 6.3 percent of reporting computers there. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The fourth most common malware family encountered in Bangladesh in 2Q15 was [Win32/Ramnit](#), which was encountered by 5.4 percent of reporting computers there. [Win32/Ramnit](#) is a family of multi-component malware that infects executable files, Microsoft Office files, and HTML files. [Win32/Ramnit](#) spreads to removable drives and steals sensitive information such as saved FTP credentials and browser cookies. It may also open a backdoor to await instructions from a remote attacker.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Bangladesh in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	7.2%
2	Win32/InstalleRex	Software Bundlers	6.0%
3	Win32/KipodToolsCby	Browser Modifiers	5.2%
4	Win32/SaverExtension	Adware	2.3%
5	Win32/AlterbookSP	Browser Modifiers	0.5%

- The most common unwanted software family encountered in Bangladesh in 2Q15 was [Win32/CouponRuc](#), which was encountered by 7.2 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in Bangladesh in 2Q15 was [Win32/InstalleRex](#), which was encountered by 6.0 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own “Installed On” date in Programs and Features to make it more difficult for a user to locate it and remove it.
- The third most common unwanted software family encountered in Bangladesh in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 5.2 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user’s consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.

Top threat families by infection rate

The most common malware families by infection rate in Bangladesh in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/Ramnit	Trojans	7.6
2	Win32/Sality	Viruses	7.5
3	VBS/Jenxcus	Worms	6.7
4	Win32/Gamarue	Worms	5.8
5	Win32/leEnablerCby	Browser Modifiers	3.6
6	Win32/Kilim	Trojans	1.5
7	Win32/Virut	Viruses	1.2
8	Win32/Chir	Viruses	0.7
9	Win32/Pramro	Trojans	0.7
10	Win32/CompromisedCert	Other Malware	0.7

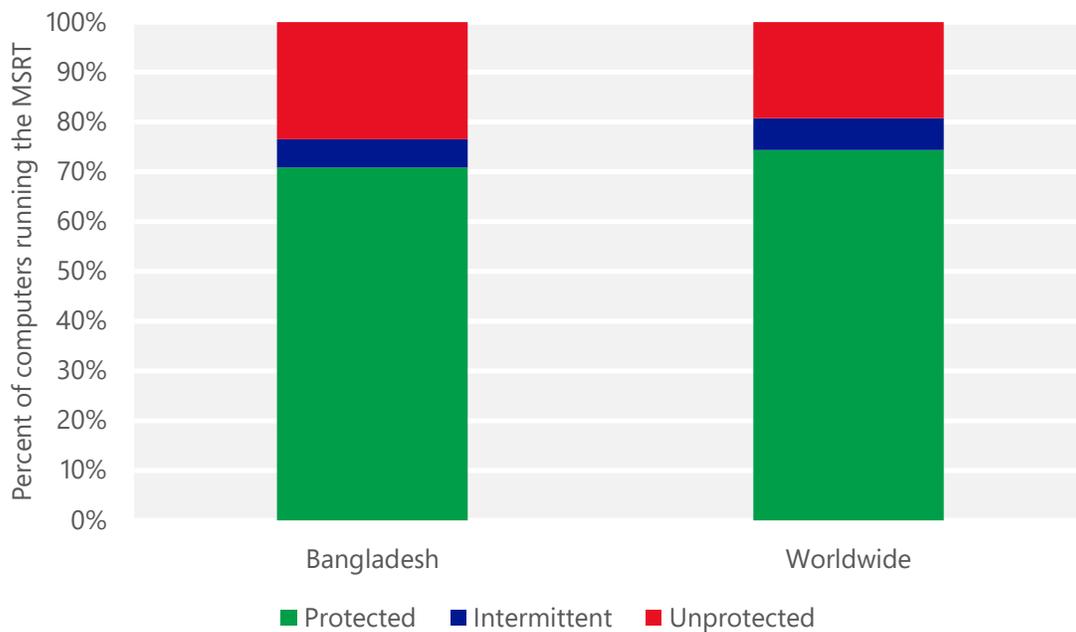
- The most common threat family infecting computers in Bangladesh in 2Q15 was [Win32/Ramnit](#), which was detected and removed from 7.6 of every 1,000 unique computers scanned by the MSRT. [Win32/Ramnit](#) is a family of multi-component malware that infects executable files, Microsoft Office files, and HTML files. Win32/Ramnit spreads to removable drives and steals sensitive information such as saved FTP credentials and browser cookies. It may also open a backdoor to await instructions from a remote attacker.
- The second most common threat family infecting computers in Bangladesh in 2Q15 was [Win32/Sality](#), which was detected and removed from 7.5 of every 1,000 unique computers scanned by the MSRT. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The third most common threat family infecting computers in Bangladesh in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 6.7 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The fourth most common threat family infecting computers in Bangladesh in 2Q15 was [Win32/Gamarue](#), which was detected and removed from 5.8 of every 1,000 unique computers scanned by the MSRT. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Bangladesh and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Bangladesh

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	3.96 (0.28)	0.03 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	4.42 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	9.60 (16.7)	

Belarus

The statistics presented here are generated by Microsoft security programs and services running on computers in Belarus in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Belarus

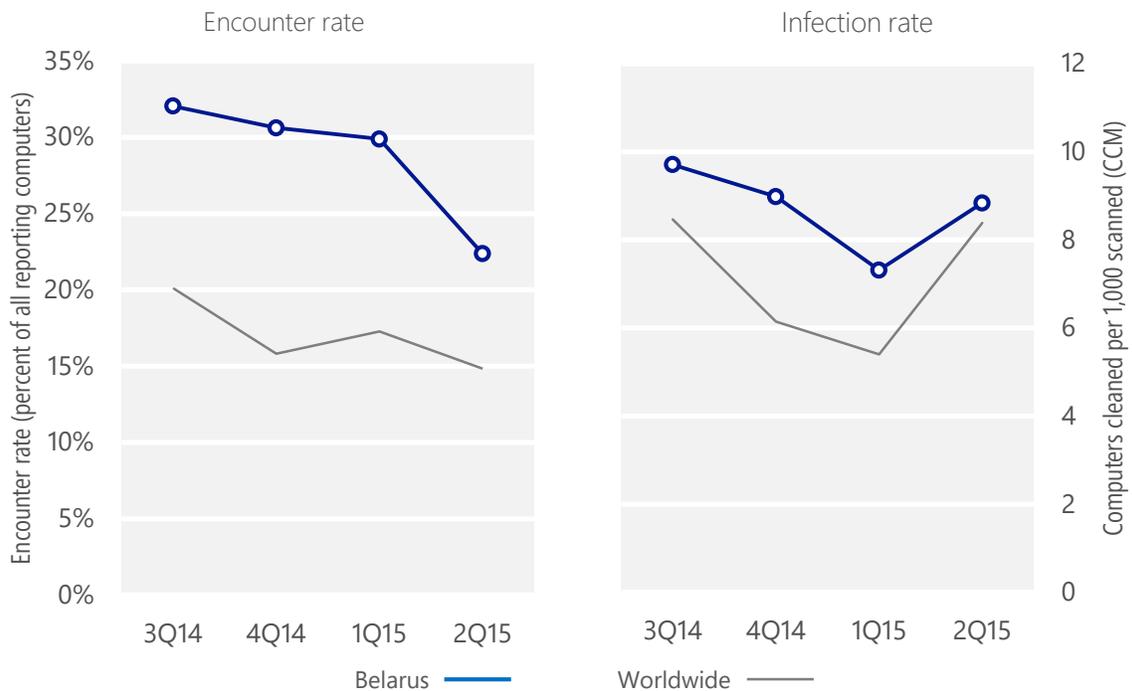
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Belarus	32.1%	30.6%	29.9%	22.4%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Belarus	9.7	9.0	7.3	8.8
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcote, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 22.4% of computers in Belarus encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 8.8 of every 1,000 unique computers scanned in Belarus in 2Q15 (a CCM score of 8.8, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Belarus over the last four quarters, compared to the world as a whole.

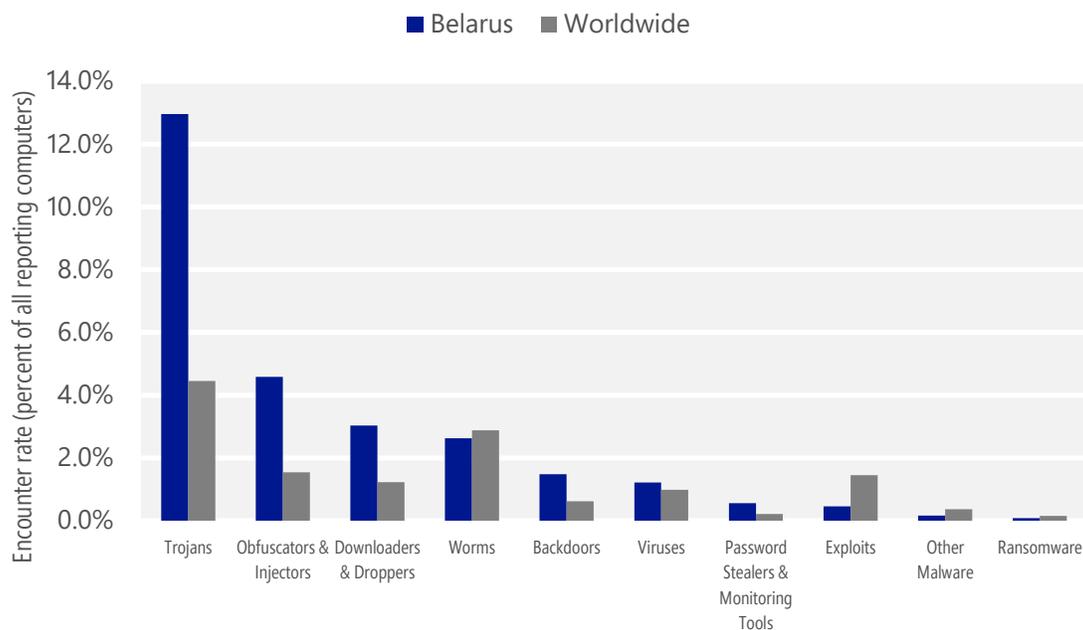
Malware encounter and infection rate trends in Belarus and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in Belarus and around the world, and for explanations of the methods and terms used here.

Malware categories

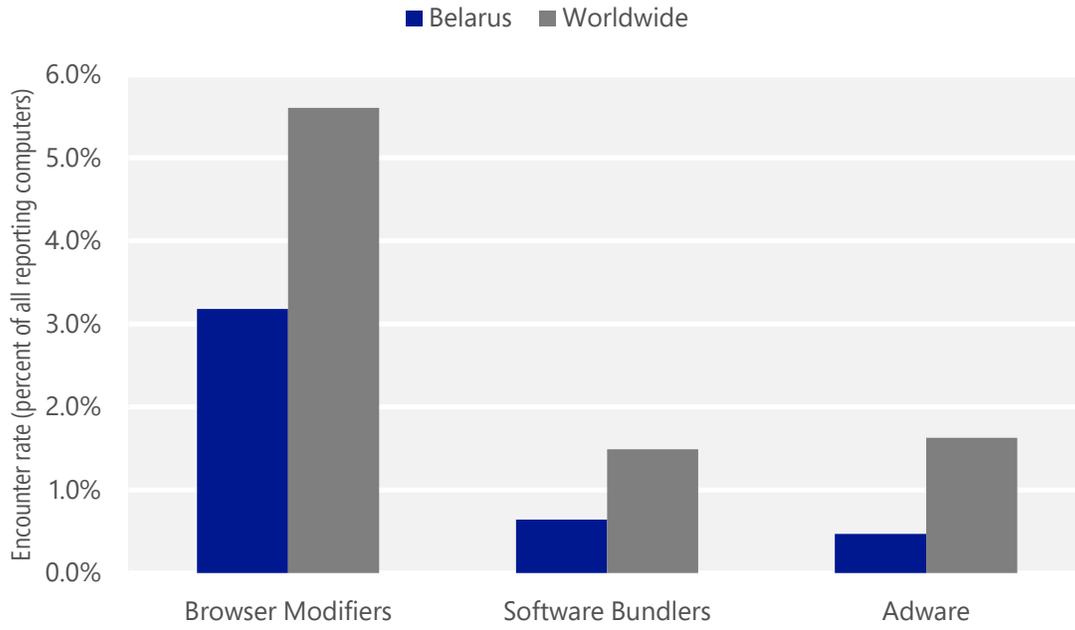
Malware encountered in Belarus in 2Q15, by category



- The most common malware category in Belarus in 2Q15 was Trojans. It was encountered by 13.0 percent of all computers there, down from 15.3 percent in 1Q15.
- The second most common malware category in Belarus in 2Q15 was Obfuscators & Injectors. It was encountered by 4.6 percent of all computers there, down from 7.4 percent in 1Q15.
- The third most common malware category in Belarus in 2Q15 was Downloaders & Droppers, which was encountered by 3.0 percent of all computers there, down from 5.1 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Belarus in 2Q15, by category



- The most common unwanted software category in Belarus in 2Q15 was Browser Modifiers. It was encountered by 3.2 percent of all computers there, down from 6.7 percent in 1Q15.
- The second most common unwanted software category in Belarus in 2Q15 was Software Bundlers. It was encountered by 0.6 percent of all computers there, down from 1.1 percent in 1Q15.
- The third most common unwanted software category in Belarus in 2Q15 was Adware, which was encountered by 0.5 percent of all computers there, up from 0.2 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Belarus in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Peals	Trojans	5.2%
2	Win32/Obfuscator	Obfuscators & Injectors	4.2%
3	Win32/Ogimant	Downloaders & Droppers	1.2%
4	Win32/Skeeyah	Trojans	1.1%
5	Win32/Dynamer	Trojans	1.1%
6	Win32/Gamarue	Worms	1.0%
7	Win32/Radonskra	Trojans	0.8%
8	Win32/Anaki	Trojans	0.6%
9	Win32/Caphaw	Backdoors	0.4%
10	INF/Autorun	Obfuscators & Injectors	0.4%

- The most common malware family encountered in Belarus in 2Q15 was [Win32/Peals](#), which was encountered by 5.2 percent of reporting computers there. [Win32/Peals](#) is a generic detection for various threats that display trojan characteristics.
- The second most common malware family encountered in Belarus in 2Q15 was [Win32/Obfuscator](#), which was encountered by 4.2 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The third most common malware family encountered in Belarus in 2Q15 was [Win32/Ogimant](#), which was encountered by 1.2 percent of reporting computers there. [Win32/Ogimant](#) is a threat that claims to help download items from the Internet, but actually downloads and runs files that are specified by a remote attacker.
- The fourth most common malware family encountered in Belarus in 2Q15 was [Win32/Skeeyah](#), which was encountered by 1.1 percent of reporting computers there. [Win32/Skeeyah](#) is a generic detection for various threats that display trojan characteristics.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Belarus in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/KipodToolsCby	Browser Modifiers	2.1%
2	Win32/CouponRuc	Browser Modifiers	0.8%
3	Win32/InstalleRex	Software Bundlers	0.6%
4	Win32/SaverExtension	Adware	0.3%
5	Win32/AlterbookSP	Browser Modifiers	0.2%

- The most common unwanted software family encountered in Belarus in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 2.1 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common unwanted software family encountered in Belarus in 2Q15 was [Win32/CouponRuc](#), which was encountered by 0.8 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The third most common unwanted software family encountered in Belarus in 2Q15 was [Win32/InstalleRex](#), which was encountered by 0.6 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Belarus in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	2.8
2	Win32/Gamarue	Worms	1.4
3	Win32/Ramnit	Trojans	0.8
4	Win32/CompromisedCert	Other Malware	0.6
5	Win32/Dorkbot	Worms	0.6
6	Win32/Sality	Viruses	0.4
7	Win32/Kilim	Trojans	0.4
8	Win32/Tofsee	Backdoors	0.2
9	Win32/Deminnix	Trojans	0.2
10	Win32/Lethic	Trojans	0.2

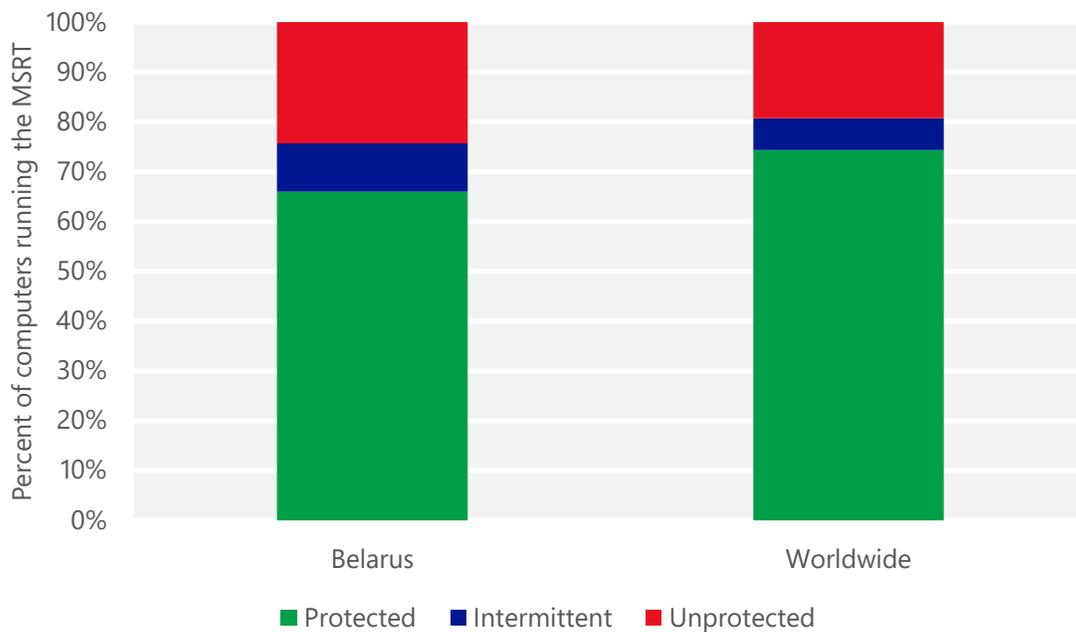
- The most common threat family infecting computers in Belarus in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 2.8 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Belarus in 2Q15 was [Win32/Gamarue](#), which was detected and removed from 1.4 of every 1,000 unique computers scanned by the MSRT. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The third most common threat family infecting computers in Belarus in 2Q15 was [Win32/Ramnit](#), which was detected and removed from 0.8 of every 1,000 unique computers scanned by the MSRT. [Win32/Ramnit](#) is a family of multi-component malware that infects executable files, Microsoft Office files, and HTML files. Win32/Ramnit spreads to removable drives and steals sensitive information such as saved FTP credentials and browser cookies. It may also open a backdoor to await instructions from a remote attacker.
- The fourth most common threat family infecting computers in Belarus in 2Q15 was [Win32/CompromisedCert](#), which was detected and removed from 0.6 of every 1,000 unique computers scanned by the MSRT. [Win32/CompromisedCert](#) is a detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Belarus and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Belarus

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.86 (0.28)	0.64 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	13.67 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	11.94 (16.7)	

Belgium

The statistics presented here are generated by Microsoft security programs and services running on computers in Belgium in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Belgium

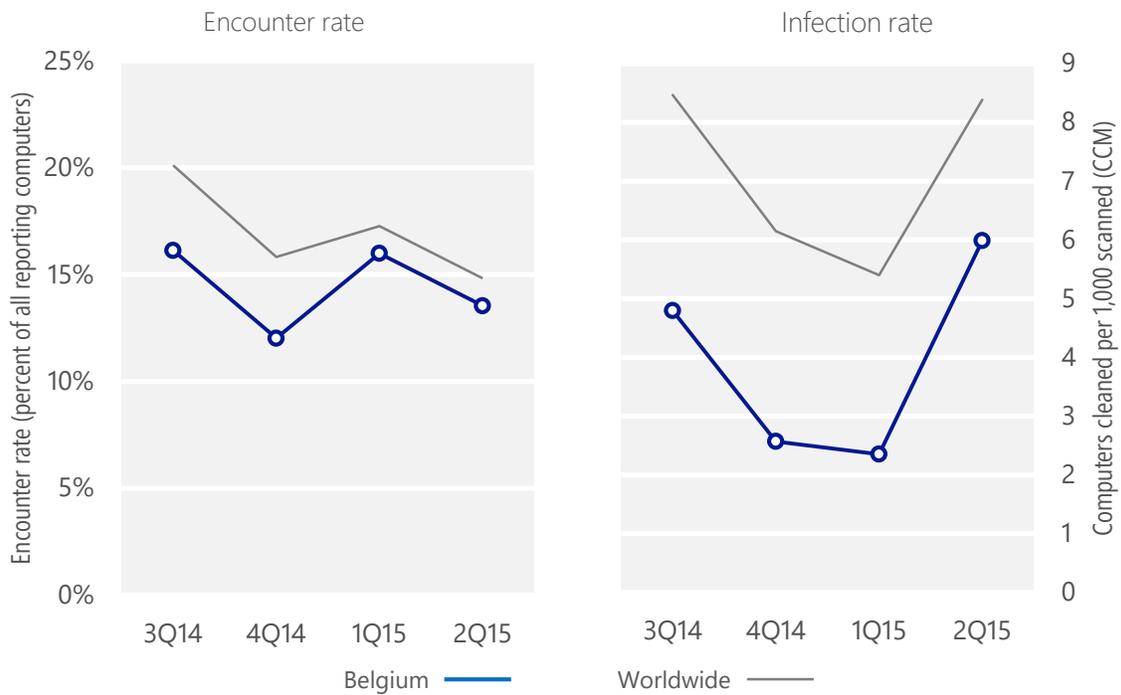
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Belgium	16.1%	12.0%	16.0%	13.5%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Belgium	4.8	2.6	2.4	6.0
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcoute, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 13.5% of computers in Belgium encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 6.0 of every 1,000 unique computers scanned in Belgium in 2Q15 (a CCM score of 6.0, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Belgium over the last four quarters, compared to the world as a whole.

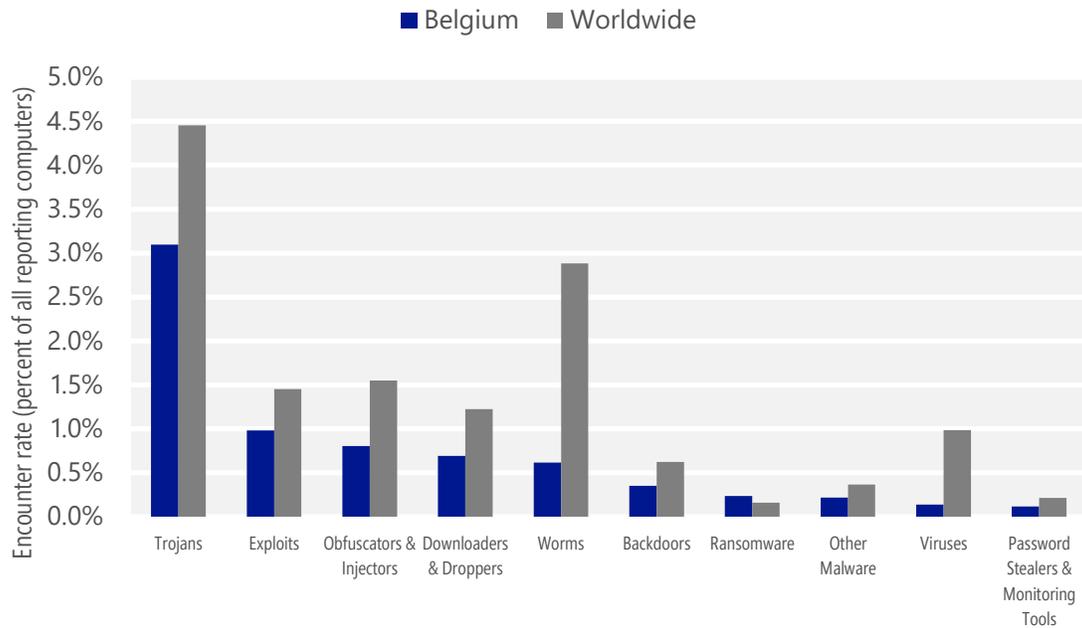
Malware encounter and infection rate trends in Belgium and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in Belgium and around the world, and for explanations of the methods and terms used here.

Malware categories

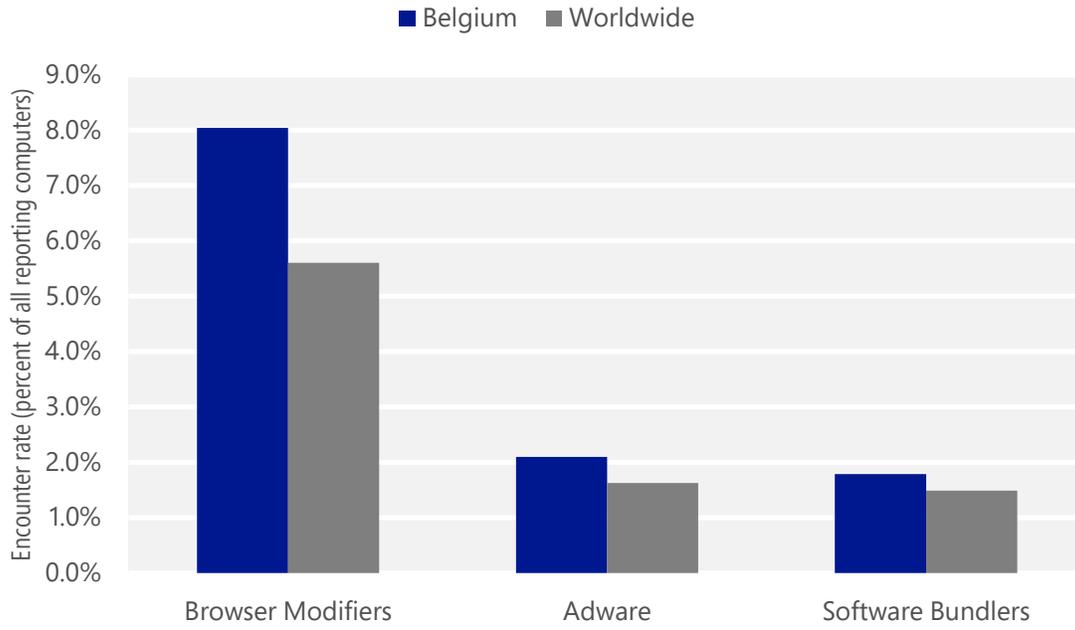
Malware encountered in Belgium in 2Q15, by category



- The most common malware category in Belgium in 2Q15 was Trojans. It was encountered by 3.1 percent of all computers there, up from 2.0 percent in 1Q15.
- The second most common malware category in Belgium in 2Q15 was Exploits. It was encountered by 1.0 percent of all computers there, down from 1.7 percent in 1Q15.
- The third most common malware category in Belgium in 2Q15 was Obfuscators & Injectors, which was encountered by 0.8 percent of all computers there, down from 1.0 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Belgium in 2Q15, by category



- The most common unwanted software category in Belgium in 2Q15 was Browser Modifiers. It was encountered by 8.0 percent of all computers there, down from 9.2 percent in 1Q15.
- The second most common unwanted software category in Belgium in 2Q15 was Adware. It was encountered by 2.1 percent of all computers there, down from 5.1 percent in 1Q15.
- The third most common unwanted software category in Belgium in 2Q15 was Software Bundlers, which was encountered by 1.8 percent of all computers there, up from 0.6 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Belgium in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Kilim	Trojans	1.1%
2	Win32/Skeeyah	Trojans	0.7%
3	Win32/Obfuscator	Obfuscators & Injectors	0.6%
4	JS/Axpergle	Exploits	0.5%
5	Win32/Peals	Trojans	0.3%
6	ASX/Wimad	Downloaders & Droppers	0.2%
7	VBS/Jenxcus	Worms	0.1%
8	INF/Autorun	Obfuscators & Injectors	0.1%
9	Win32/Dynamer	Trojans	0.1%
10	Win32/Sdbby	Exploits	0.1%

- The most common malware family encountered in Belgium in 2Q15 was [Win32/Kilim](#), which was encountered by 1.1 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The second most common malware family encountered in Belgium in 2Q15 was [Win32/Skeeyah](#), which was encountered by 0.7 percent of reporting computers there. [Win32/Skeeyah](#) is a generic detection for various threats that display trojan characteristics.
- The third most common malware family encountered in Belgium in 2Q15 was [Win32/Obfuscator](#), which was encountered by 0.6 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The fourth most common malware family encountered in Belgium in 2Q15 was [JS/Axpergle](#), which was encountered by 0.5 percent of reporting computers there. [JS/Axpergle](#) is a detection for the Angler exploit kit, which exploits vulnerabilities in recent versions of Internet Explorer, Silverlight, Adobe Flash Player, and Java to install malware.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Belgium in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	3.6%
2	Win32/KipodToolsCby	Browser Modifiers	3.2%
3	Win32/InstalleRex	Software Bundlers	1.7%
4	Win32/AlterbookSP	Browser Modifiers	1.3%
5	Win32/SaverExtension	Adware	1.3%

- The most common unwanted software family encountered in Belgium in 2Q15 was [Win32/CouponRuc](#), which was encountered by 3.6 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in Belgium in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 3.2 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common unwanted software family encountered in Belgium in 2Q15 was [Win32/InstalleRex](#), which was encountered by 1.7 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Belgium in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	2.2
2	Win32/Kilim	Trojans	1.6
3	Win32/CompromisedCert	Other Malware	0.7
4	VBS/Jenxcus	Worms	0.2
5	Win32/Simda	Trojans	0.1
6	Win32/Alureon	Trojans	0.1
7	MSIL/Bladabindi	Backdoors	0.1
8	Win32/Sality	Viruses	0.1
9	Win32/Brontok	Worms	0.1
10	Win32/Wysotot	Trojans	0.1

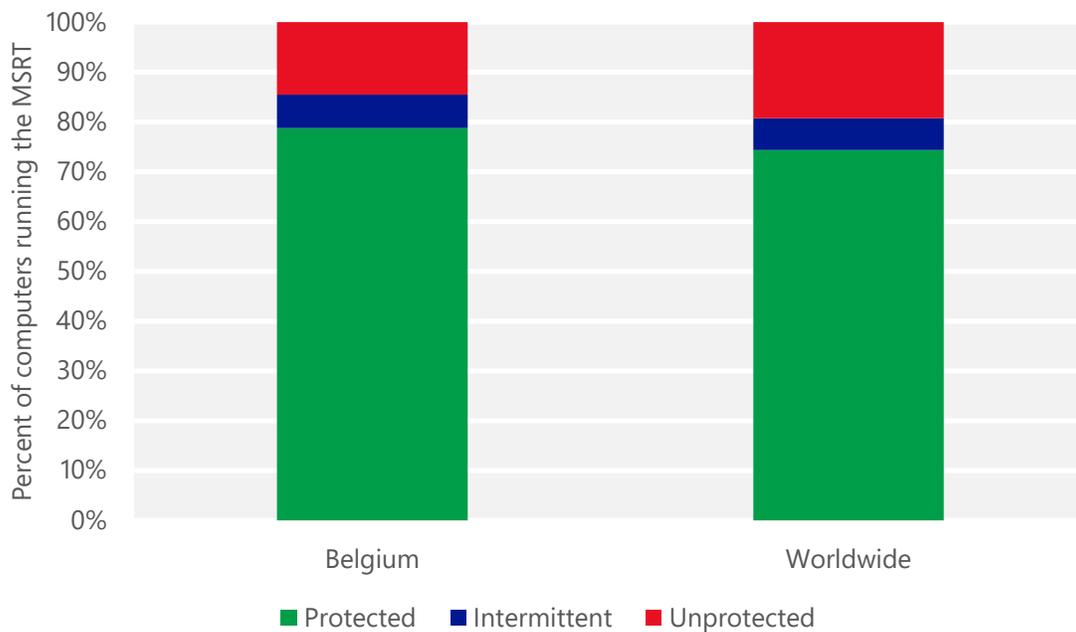
- The most common threat family infecting computers in Belgium in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 2.2 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Belgium in 2Q15 was [Win32/Kilim](#), which was detected and removed from 1.6 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The third most common threat family infecting computers in Belgium in 2Q15 was [Win32/CompromisedCert](#), which was detected and removed from 0.7 of every 1,000 unique computers scanned by the MSRT. [Win32/CompromisedCert](#) is a detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.
- The fourth most common threat family infecting computers in Belgium in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 0.2 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Belgium and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Belgium

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.13 (0.28)	0.41 (0.24)
Phishing sites per 1,000 hosts (Worldwide)		3.08 (5.0)
Malware hosting sites per 1,000 hosts (Worldwide)		8.09 (16.7)

Bolivia

The statistics presented here are generated by Microsoft security programs and services running on computers in Bolivia in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Bolivia

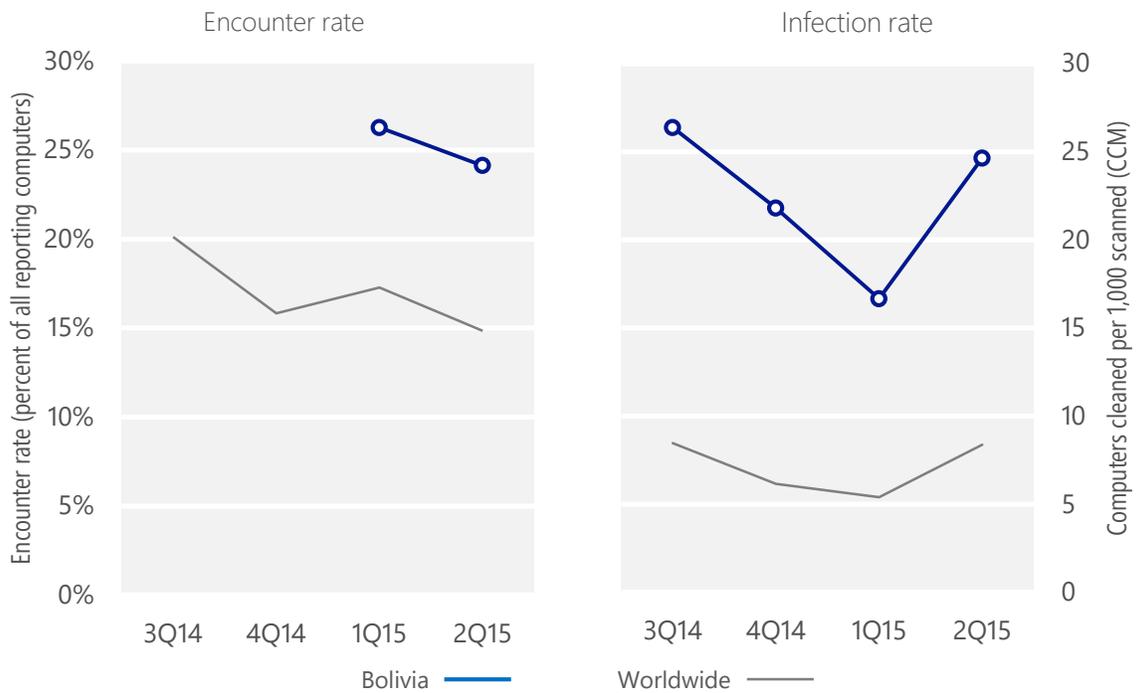
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Bolivia	N/A	N/A	26.3%	24.1%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Bolivia	26.4	21.8	16.7	24.6
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcoute, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 24.1% of computers in Bolivia encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 24.6 of every 1,000 unique computers scanned in Bolivia in 2Q15 (a CCM score of 24.6, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Bolivia over the last four quarters, compared to the world as a whole.

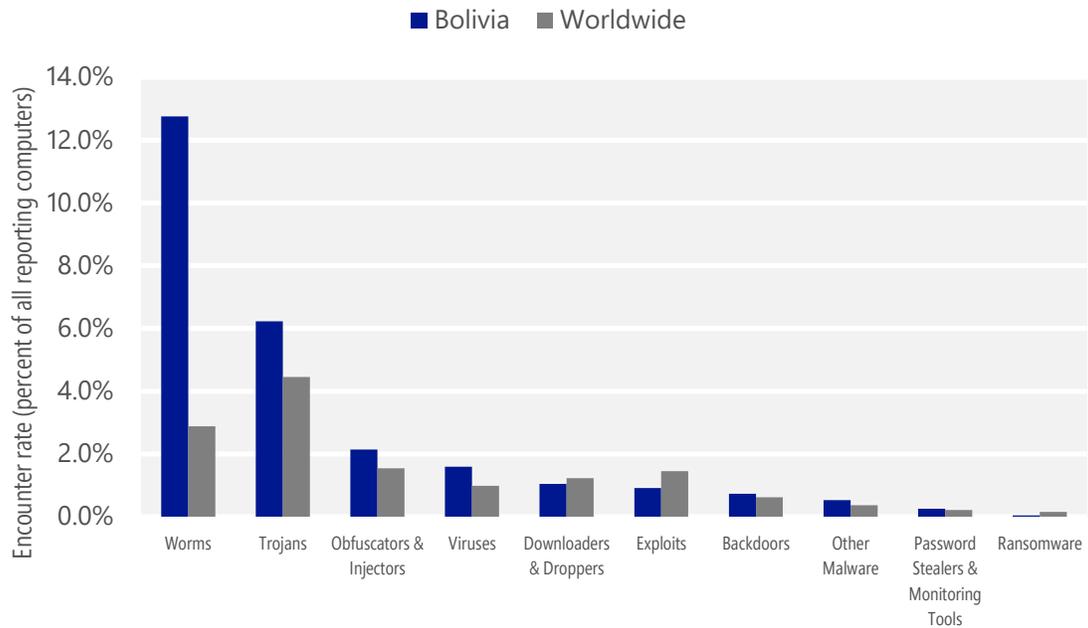
Malware encounter and infection rate trends in Bolivia and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in Bolivia and around the world, and for explanations of the methods and terms used here.

Malware categories

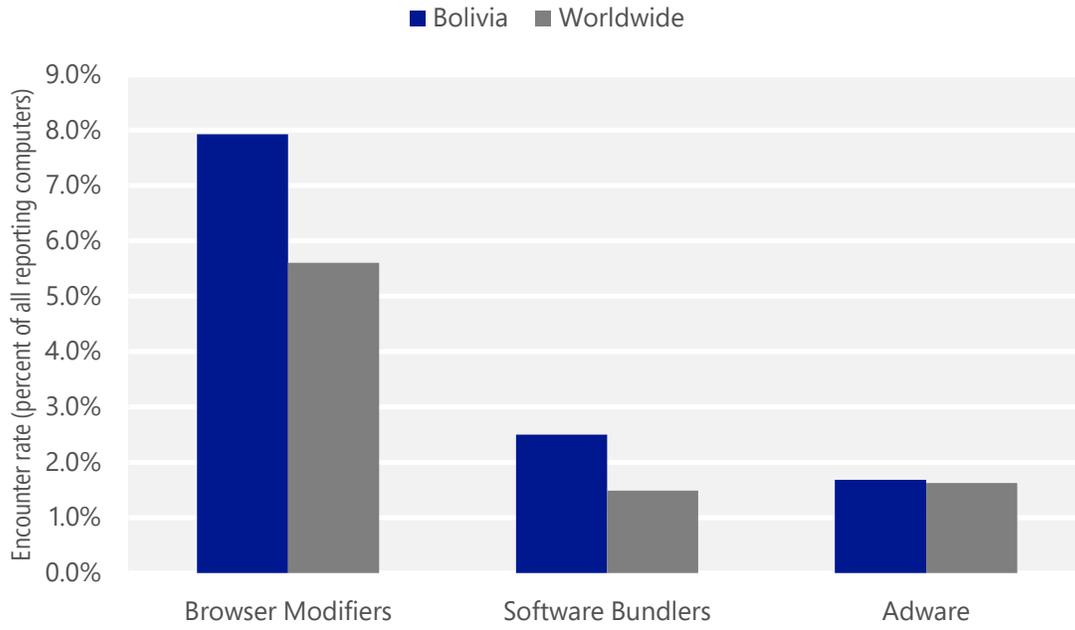
Malware encountered in Bolivia in 2Q15, by category



- The most common malware category in Bolivia in 2Q15 was Worms. It was encountered by 12.8 percent of all computers there, up from 11.9 percent in 1Q15.
- The second most common malware category in Bolivia in 2Q15 was Trojans. It was encountered by 6.2 percent of all computers there, up from 4.5 percent in 1Q15.
- The third most common malware category in Bolivia in 2Q15 was Obfuscators & Injectors, which was encountered by 2.1 percent of all computers there, down from 2.5 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Bolivia in 2Q15, by category



- The most common unwanted software category in Bolivia in 2Q15 was Browser Modifiers. It was encountered by 7.9 percent of all computers there, down from 11.0 percent in 1Q15.
- The second most common unwanted software category in Bolivia in 2Q15 was Software Bundlers. It was encountered by 2.5 percent of all computers there, down from 4.4 percent in 1Q15.
- The third most common unwanted software category in Bolivia in 2Q15 was Adware, which was encountered by 1.7 percent of all computers there, up from 0.8 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Bolivia in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Gamarue	Worms	0.1%
2	JS/Bondat	Worms	0.1%
3	VBS/Jenxcus	Worms	<0.1%
4	Win32/Obfuscator	Obfuscators & Injectors	<0.1%
5	Win32/Sohanad	Worms	<0.1%
6	Win32/Sality	Viruses	<0.1%
7	INF/Autorun	Obfuscators & Injectors	<0.1%
8	Win32/Peals	Trojans	<0.1%
9	Win32/Kilim	Trojans	<0.1%
10	Win32/Vobfus	Worms	<0.1%

- The most common malware family encountered in Bolivia in 2Q15 was [Win32/Gamarue](#), which was encountered by 0.1 percent of reporting computers there. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The second most common malware family encountered in Bolivia in 2Q15 was [JS/Bondat](#), which was encountered by 0.1 percent of reporting computers there. [JS/Bondat](#) is a family of threats that collects information about the computer, infects removable drives, and tries to stop the user from accessing files. It spreads by infecting removable drives, such as USB thumb drives and flash drives.
- The third most common malware family encountered in Bolivia in 2Q15 was [VBS/Jenxcus](#), which was encountered by <0.1 percent of reporting computers there. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The fourth most common malware family encountered in Bolivia in 2Q15 was [Win32/Obfuscator](#), which was encountered by <0.1 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Bolivia in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/KipodToolsCby	Browser Modifiers	<0.1%
2	Win32/CouponRuc	Browser Modifiers	<0.1%
3	Win32/InstalleRex	Software Bundlers	<0.1%
4	Win32/SaverExtension	Adware	<0.1%
5	Win32/AlterbookSP	Browser Modifiers	<0.1%

- The most common unwanted software family encountered in Bolivia in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by <0.1 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user’s consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common unwanted software family encountered in Bolivia in 2Q15 was [Win32/CouponRuc](#), which was encountered by <0.1 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The third most common unwanted software family encountered in Bolivia in 2Q15 was [Win32/InstalleRex](#), which was encountered by <0.1 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own “Installed On” date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Bolivia in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	7.7
2	VBS/Jenxcus	Worms	5.8
3	Win32/Gamarue	Worms	5.3
4	Win32/Sality	Viruses	1.9
5	Win32/Kilim	Trojans	1.6
6	Win32/Vobfus	Worms	0.6
7	Win32/Yeltminky	Worms	0.5
8	Win32/Ramnit	Trojans	0.5
9	Win32/Dorkbot	Worms	0.4
10	Win32/CompromisedCert	Other Malware	0.3

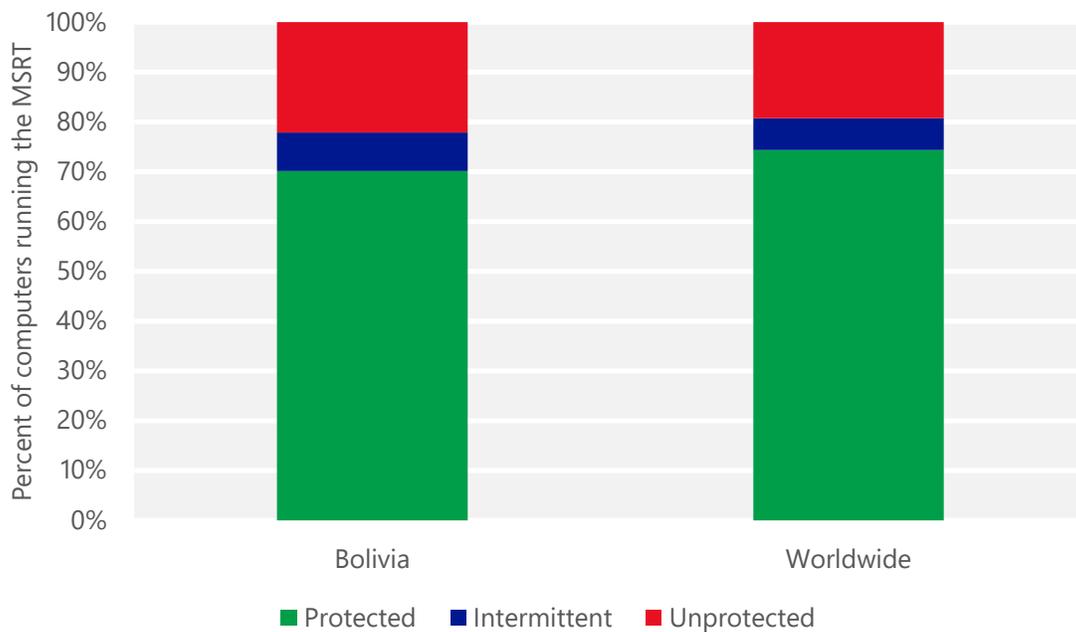
- The most common threat family infecting computers in Bolivia in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 7.7 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Bolivia in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 5.8 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The third most common threat family infecting computers in Bolivia in 2Q15 was [Win32/Gamarue](#), which was detected and removed from 5.3 of every 1,000 unique computers scanned by the MSRT. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The fourth most common threat family infecting computers in Bolivia in 2Q15 was [Win32/Sality](#), which was detected and removed from 1.9 of every 1,000 unique computers scanned by the MSRT. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Bolivia and worldwide protected by real-time security software in 2Q15



Brazil

The statistics presented here are generated by Microsoft security programs and services running on computers in Brazil in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Brazil

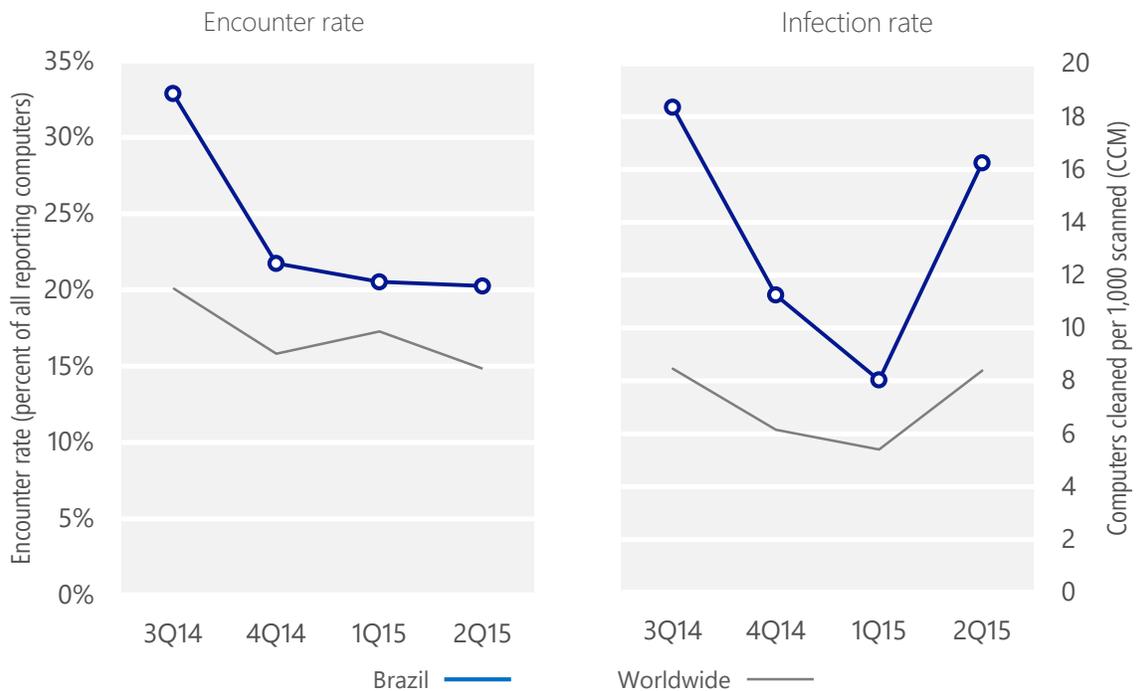
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Brazil	32.9%	21.7%	20.5%	20.2%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Brazil	18.4	11.2	8.0	16.2
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcoute, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 20.2% of computers in Brazil encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 16.2 of every 1,000 unique computers scanned in Brazil in 2Q15 (a CCM score of 16.2, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Brazil over the last four quarters, compared to the world as a whole.

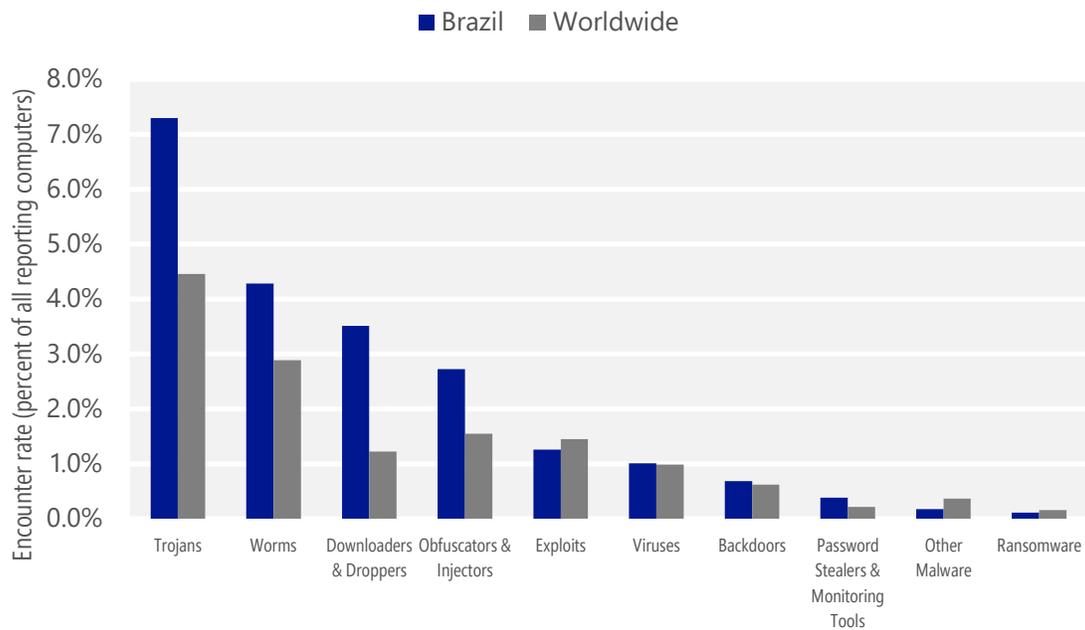
Malware encounter and infection rate trends in Brazil and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in Brazil and around the world, and for explanations of the methods and terms used here.

Malware categories

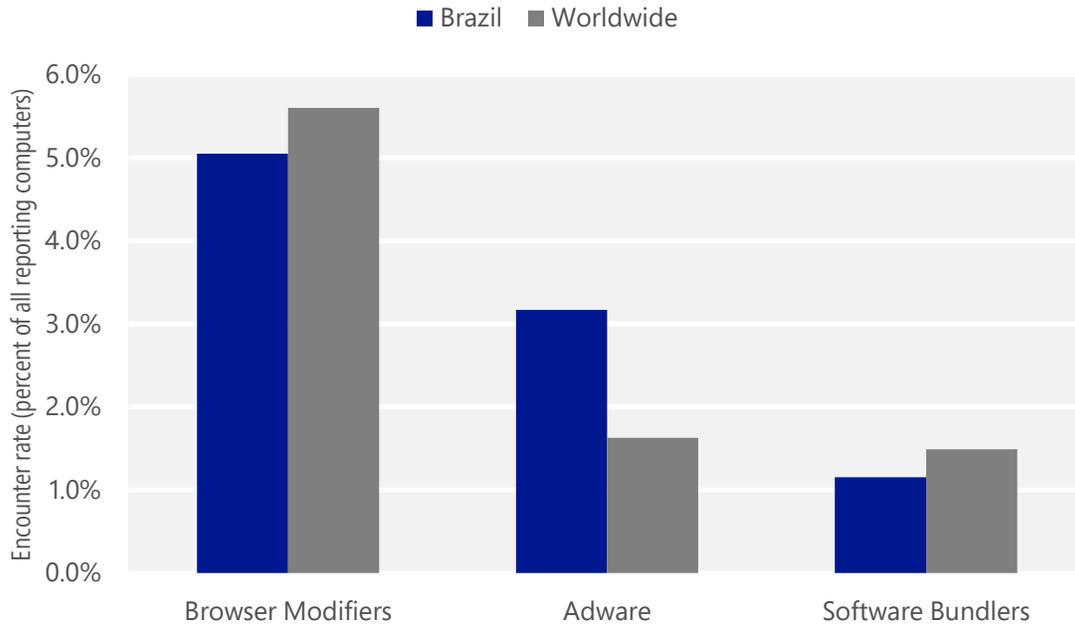
Malware encountered in Brazil in 2Q15, by category



- The most common malware category in Brazil in 2Q15 was Trojans. It was encountered by 7.3 percent of all computers there, up from 5.3 percent in 1Q15.
- The second most common malware category in Brazil in 2Q15 was Worms. It was encountered by 4.3 percent of all computers there, down from 4.6 percent in 1Q15.
- The third most common malware category in Brazil in 2Q15 was Downloaders & Droppers, which was encountered by 3.5 percent of all computers there, up from 2.9 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Brazil in 2Q15, by category



- The most common unwanted software category in Brazil in 2Q15 was Browser Modifiers. It was encountered by 5.1 percent of all computers there, down from 6.6 percent in 1Q15.
- The second most common unwanted software category in Brazil in 2Q15 was Adware. It was encountered by 3.2 percent of all computers there, down from 3.8 percent in 1Q15.
- The third most common unwanted software category in Brazil in 2Q15 was Software Bundlers, which was encountered by 1.2 percent of all computers there, up from 0.4 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Brazil in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Banload	Downloaders & Droppers	2.1%
2	Win32/Obfuscator	Obfuscators & Injectors	1.8%
3	VBS/Jenxcus	Worms	1.7%
4	Win32/Skeeyah	Trojans	1.6%
5	JS/Bondat	Worms	1.2%
6	Win32/Banker	Trojans	1.1%
7	Win32/Peals	Trojans	0.8%
8	Win32/Kilim	Trojans	0.6%
9	INF/Autorun	Obfuscators & Injectors	0.6%
10	Win32/Dynamer	Trojans	0.6%

- The most common malware family encountered in Brazil in 2Q15 was [Win32/Banload](#), which was encountered by 2.1 percent of reporting computers there. [Win32/Banload](#) is a family of trojans that download other malware. Banload usually downloads [Win32/Banker](#), which steals banking credentials and other sensitive data and sends it back to a remote attacker.
- The second most common malware family encountered in Brazil in 2Q15 was [Win32/Obfuscator](#), which was encountered by 1.8 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The third most common malware family encountered in Brazil in 2Q15 was [VBS/Jenxcus](#), which was encountered by 1.7 percent of reporting computers there. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The fourth most common malware family encountered in Brazil in 2Q15 was [Win32/Skeeyah](#), which was encountered by 1.6 percent of reporting computers there. [Win32/Skeeyah](#) is a generic detection for various threats that display trojan characteristics.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Brazil in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/KipodToolsCby	Browser Modifiers	2.1%
2	Win32/CouponRuc	Browser Modifiers	2.0%
3	Win32/EoRezo	Adware	1.9%
4	Win32/InstalleRex	Software Bundlers	1.1%
5	Win32/AlterbookSP	Browser Modifiers	0.6%

- The most common unwanted software family encountered in Brazil in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 2.1 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common unwanted software family encountered in Brazil in 2Q15 was [Win32/CouponRuc](#), which was encountered by 2.0 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The third most common unwanted software family encountered in Brazil in 2Q15 was [Win32/EoRezo](#), which was encountered by 1.9 percent of reporting computers there. [Win32/EoRezo](#) is adware that displays targeted advertising to affected users while browsing the Internet, based on downloaded pre-configured information.

Top threat families by infection rate

The most common malware families by infection rate in Brazil in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	6.1
2	VBS/Jenxcus	Worms	2.6
3	Win32/Banker	Trojans	1.3
4	Win32/Banload	Downloaders & Droppers	1.1
5	Win32/Sality	Viruses	0.9
6	Win32/Kilim	Trojans	0.8
7	Win32/Ramnit	Trojans	0.6
8	MSIL/Bladabindi	Backdoors	0.5
9	Win32/CompromisedCert	Other Malware	0.4
10	Win32/Wysotot	Trojans	0.4

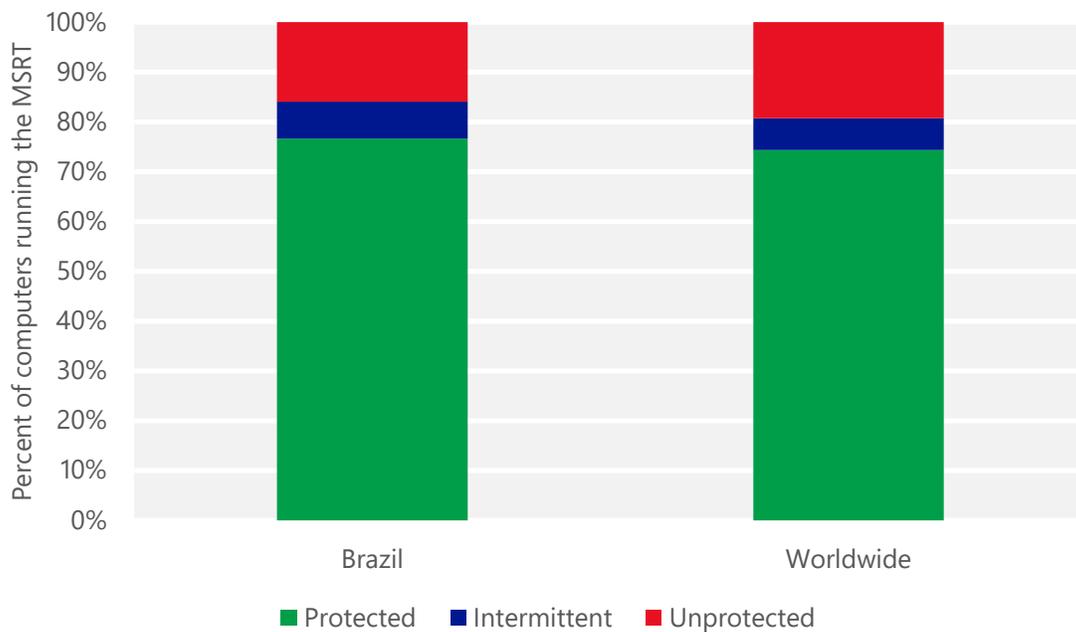
- The most common threat family infecting computers in Brazil in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 6.1 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Brazil in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 2.6 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The third most common threat family infecting computers in Brazil in 2Q15 was [Win32/Banker](#), which was detected and removed from 1.3 of every 1,000 unique computers scanned by the MSRT. [Win32/Banker](#) is a family of data-stealing Trojans that captures banking credentials such as account numbers and passwords from computer users and relays them to the attacker. Most variants target customers of Brazilian banks; some variants target customers of other banks.
- The fourth most common threat family infecting computers in Brazil in 2Q15 was [Win32/Banload](#), which was detected and removed from 1.1 of every 1,000 unique computers scanned by the MSRT. [Win32/Banload](#) is a family of trojans that download other malware. Banload usually downloads Win32/Banker, which steals banking credentials and other sensitive data and sends it back to a remote attacker.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Brazil and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Brazil

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.16 (0.28)	0.12 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	8.18 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	40.97 (16.7)	

Bulgaria

The statistics presented here are generated by Microsoft security programs and services running on computers in Bulgaria in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Bulgaria

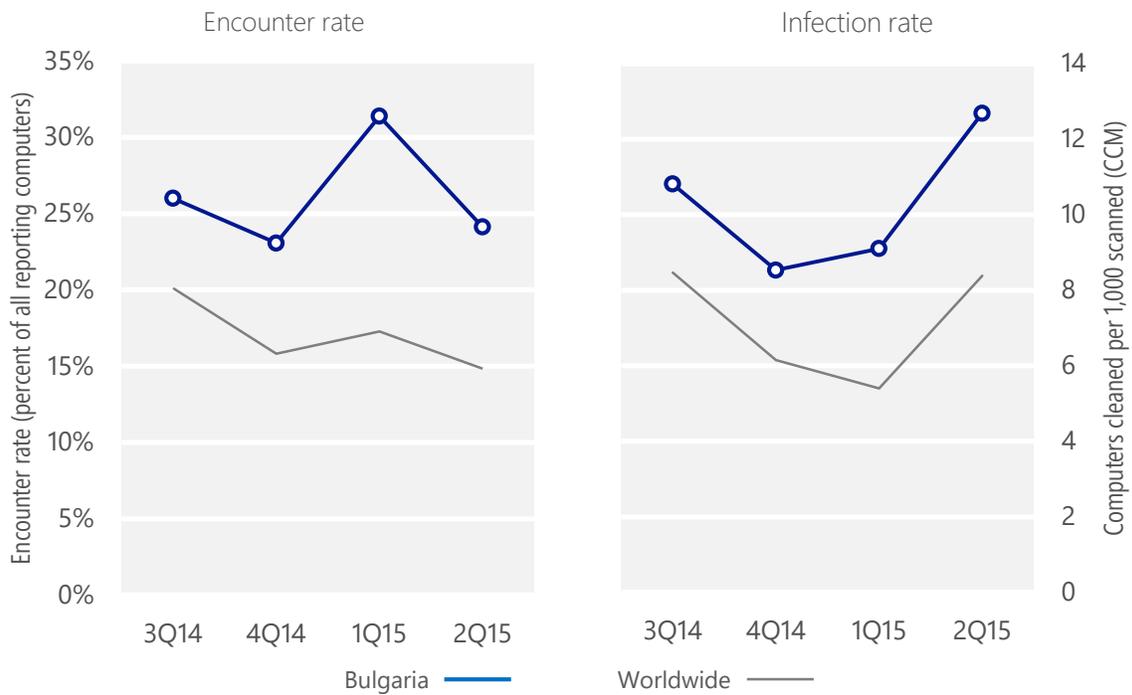
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Bulgaria	26.0%	23.1%	31.4%	24.1%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Bulgaria	10.8	8.5	9.1	12.7
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcote, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 24.1% of computers in Bulgaria encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 12.7 of every 1,000 unique computers scanned in Bulgaria in 2Q15 (a CCM score of 12.7, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Bulgaria over the last four quarters, compared to the world as a whole.

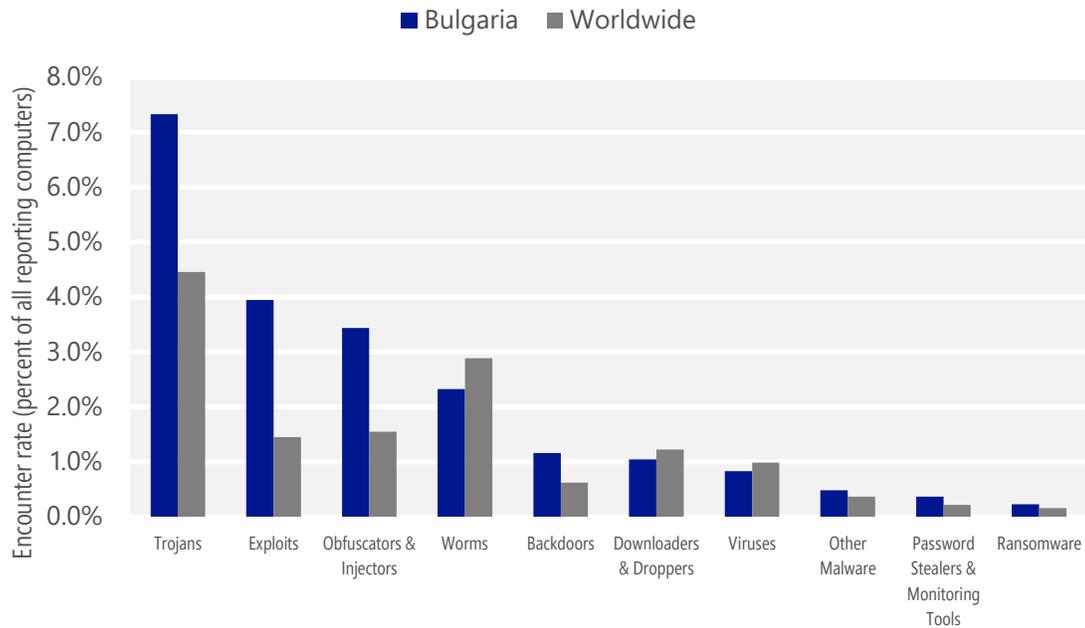
Malware encounter and infection rate trends in Bulgaria and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in Bulgaria and around the world, and for explanations of the methods and terms used here.

Malware categories

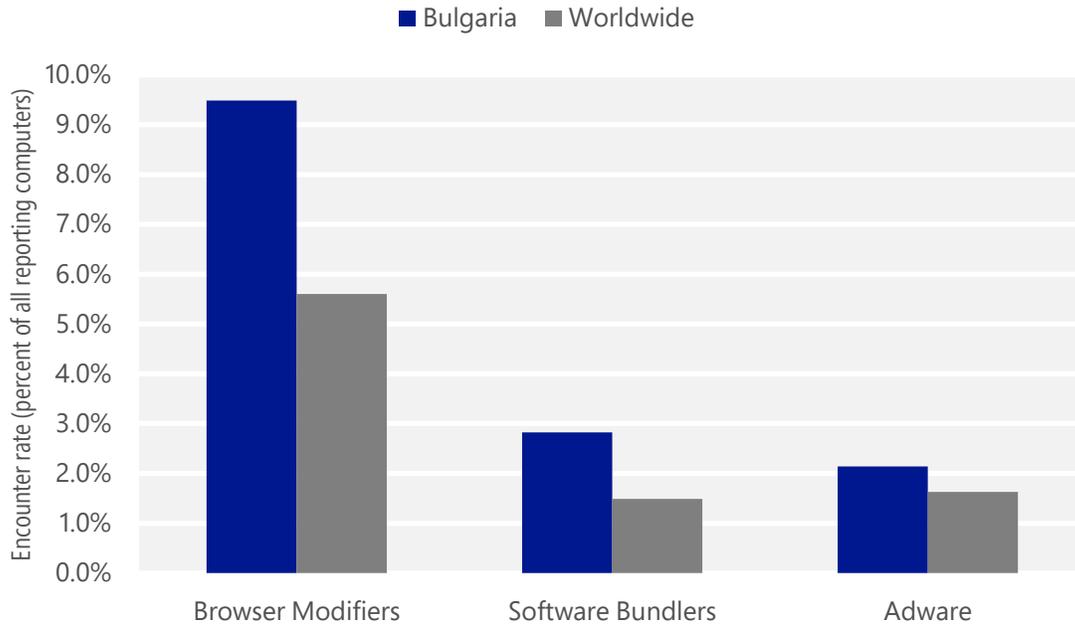
Malware encountered in Bulgaria in 2Q15, by category



- The most common malware category in Bulgaria in 2Q15 was Trojans. It was encountered by 7.3 percent of all computers there, down from 8.2 percent in 1Q15.
- The second most common malware category in Bulgaria in 2Q15 was Exploits. It was encountered by 3.9 percent of all computers there, down from 4.4 percent in 1Q15.
- The third most common malware category in Bulgaria in 2Q15 was Obfuscators & Injectors, which was encountered by 3.4 percent of all computers there, up from 3.4 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Bulgaria in 2Q15, by category



- The most common unwanted software category in Bulgaria in 2Q15 was Browser Modifiers. It was encountered by 9.5 percent of all computers there, down from 15.3 percent in 1Q15.
- The second most common unwanted software category in Bulgaria in 2Q15 was Software Bundlers. It was encountered by 2.8 percent of all computers there, down from 5.5 percent in 1Q15.
- The third most common unwanted software category in Bulgaria in 2Q15 was Adware, which was encountered by 2.1 percent of all computers there, up from 1.1 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Bulgaria in 2Q15

	Family	Most significant category	% of reporting computers
1	JS/Axpergle	Exploits	2.7%
2	Win32/Obfuscator	Obfuscators & Injectors	2.5%
3	JS/Neclu	Exploits	1.7%
4	Win32/Kilim	Trojans	1.7%
5	Win32/Skeeyah	Trojans	1.0%
6	Win32/Peals	Trojans	0.8%
7	INF/Autorun	Obfuscators & Injectors	0.7%
8	Win32/Gamarue	Worms	0.6%
9	Win32/Conficker	Worms	0.5%
10	Win32/Fynloski	Backdoors	0.4%

- The most common malware family encountered in Bulgaria in 2Q15 was [JS/Axpergle](#), which was encountered by 2.7 percent of reporting computers there. [JS/Axpergle](#) is a detection for the Angler exploit kit, which exploits vulnerabilities in recent versions of Internet Explorer, Silverlight, Adobe Flash Player, and Java to install malware.
- The second most common malware family encountered in Bulgaria in 2Q15 was [Win32/Obfuscator](#), which was encountered by 2.5 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The third most common malware family encountered in Bulgaria in 2Q15 was [JS/Neclu](#), which was encountered by 1.7 percent of reporting computers there. [JS/Neclu](#) is a detection for the Nuclear exploit kit, which attempts to exploit vulnerabilities in programs such as Java and Adobe Reader to install other malware.
- The fourth most common malware family encountered in Bulgaria in 2Q15 was [Win32/Kilim](#), which was encountered by 1.7 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Bulgaria in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	5.3%
2	Win32/KipodToolsCby	Browser Modifiers	3.6%
3	Win32/InstalleRex	Software Bundlers	2.7%
4	Win32/SaverExtension	Adware	1.6%
5	Win32/AlterbookSP	Browser Modifiers	0.8%

- The most common unwanted software family encountered in Bulgaria in 2Q15 was [Win32/CouponRuc](#), which was encountered by 5.3 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in Bulgaria in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 3.6 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common unwanted software family encountered in Bulgaria in 2Q15 was [Win32/InstalleRex](#), which was encountered by 2.7 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Bulgaria in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	3.1
2	Win32/CompromisedCert	Other Malware	2.1
3	Win32/Sality	Viruses	1.9
4	Win32/Kilim	Trojans	1.6
5	Win32/Brontok	Worms	0.5
6	Win32/Carberp	Trojans	0.4
7	MSIL/Bladabindi	Backdoors	0.3
8	Win32/Gamarue	Worms	0.3
9	VBS/Jenxcus	Worms	0.3
10	Win32/Helompy	Worms	0.3

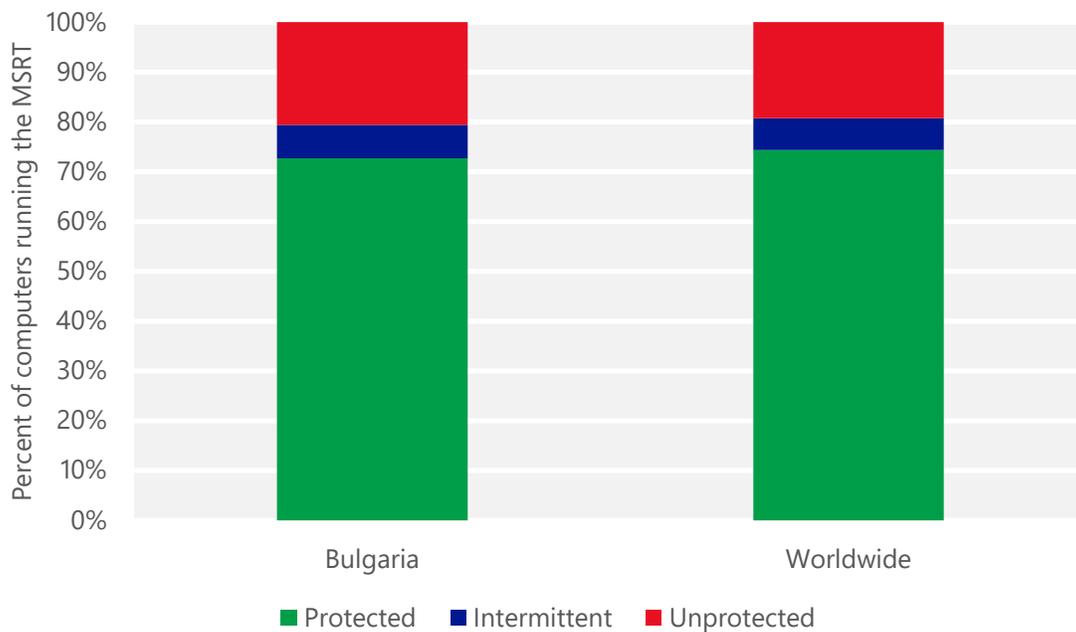
- The most common threat family infecting computers in Bulgaria in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 3.1 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Bulgaria in 2Q15 was [Win32/CompromisedCert](#), which was detected and removed from 2.1 of every 1,000 unique computers scanned by the MSRT. [Win32/CompromisedCert](#) is a detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.
- The third most common threat family infecting computers in Bulgaria in 2Q15 was [Win32/Sality](#), which was detected and removed from 1.9 of every 1,000 unique computers scanned by the MSRT. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The fourth most common threat family infecting computers in Bulgaria in 2Q15 was [Win32/Kilim](#), which was detected and removed from 1.6 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Bulgaria and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Bulgaria

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.28 (0.28)	1.35 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	98.52 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	10.82 (16.7)	

Canada

The statistics presented here are generated by Microsoft security programs and services running on computers in Canada in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Canada

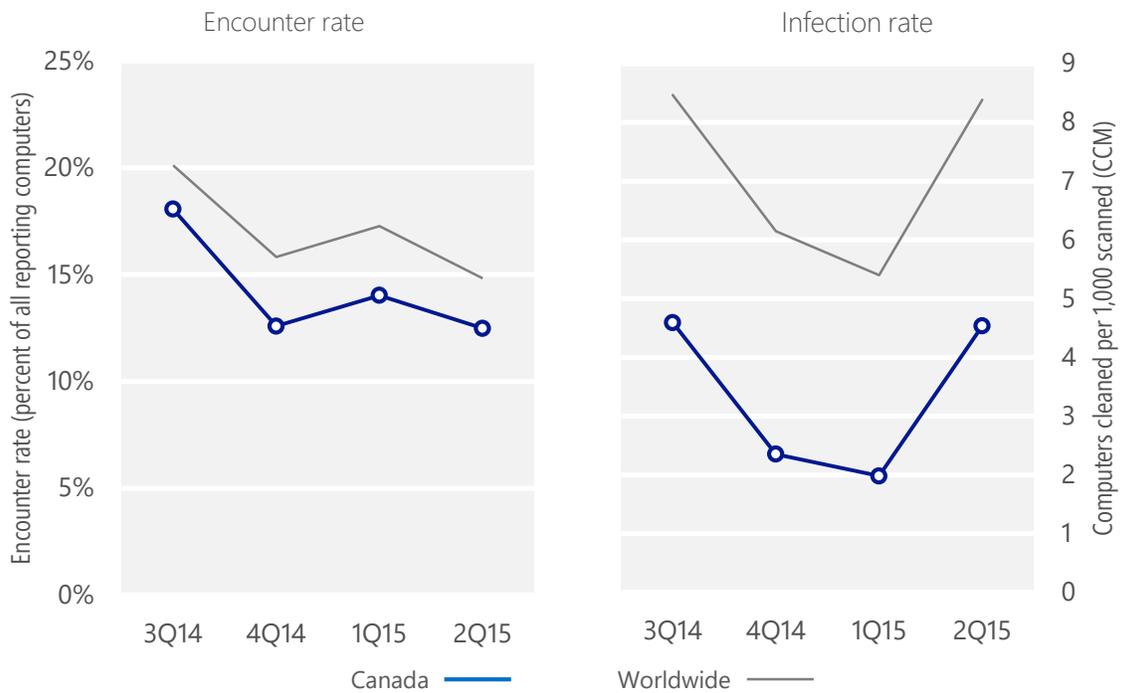
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Canada	18.1%	12.6%	14.0%	12.5%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Canada	4.6	2.4	2.0	4.5
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcote, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 12.5% of computers in Canada encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 4.5 of every 1,000 unique computers scanned in Canada in 2Q15 (a CCM score of 4.5, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Canada over the last four quarters, compared to the world as a whole.

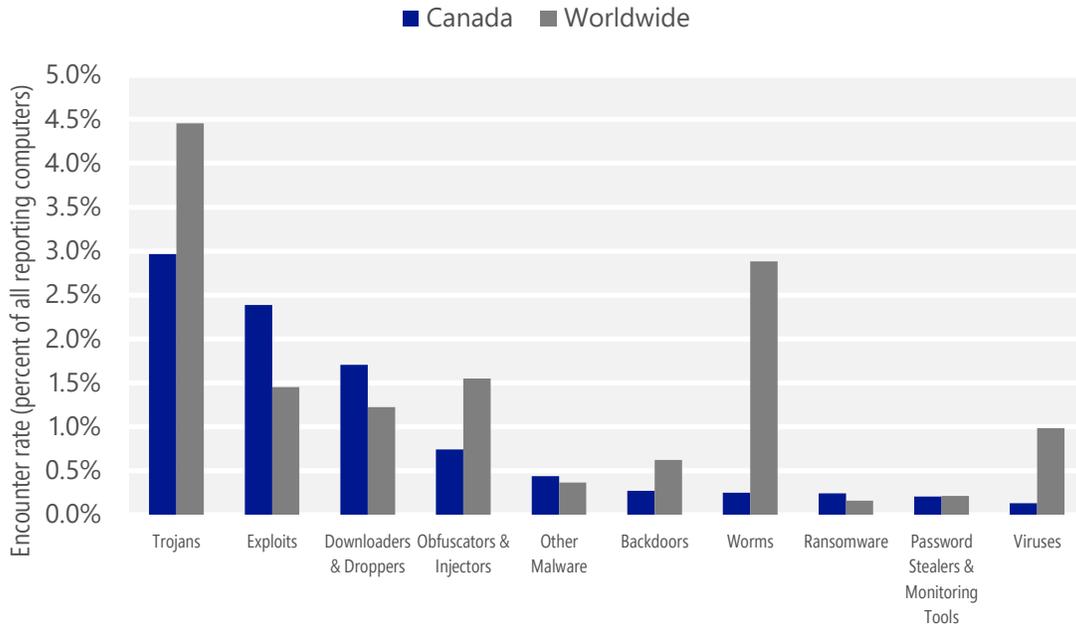
Malware encounter and infection rate trends in Canada and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in Canada and around the world, and for explanations of the methods and terms used here.

Malware categories

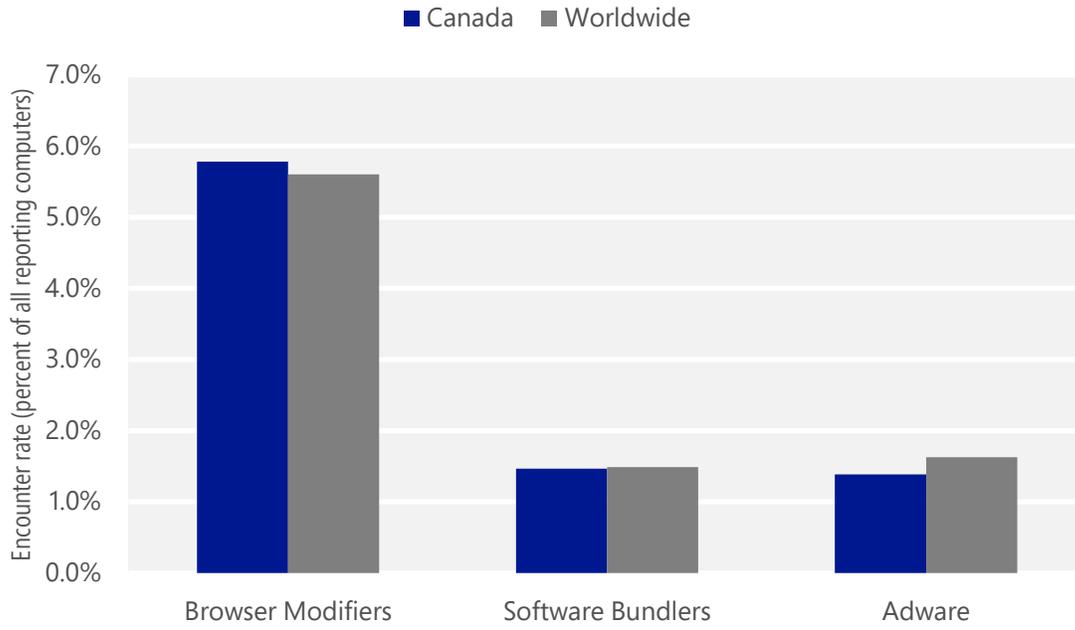
Malware encountered in Canada in 2Q15, by category



- The most common malware category in Canada in 2Q15 was Trojans. It was encountered by 3.0 percent of all computers there, down from 3.2 percent in 1Q15.
- The second most common malware category in Canada in 2Q15 was Exploits. It was encountered by 2.4 percent of all computers there, up from 2.1 percent in 1Q15.
- The third most common malware category in Canada in 2Q15 was Downloaders & Droppers, which was encountered by 1.7 percent of all computers there, up from 1.6 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Canada in 2Q15, by category



- The most common unwanted software category in Canada in 2Q15 was Browser Modifiers. It was encountered by 5.8 percent of all computers there, up from 5.5 percent in 1Q15.
- The second most common unwanted software category in Canada in 2Q15 was Software Bundlers. It was encountered by 1.5 percent of all computers there, down from 3.9 percent in 1Q15.
- The third most common unwanted software category in Canada in 2Q15 was Adware, which was encountered by 1.4 percent of all computers there, up from 1.0 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Canada in 2Q15

	Family	Most significant category	% of reporting computers
1	JS/Axpergle	Exploits	1.5%
2	Win32/Kilim	Trojans	0.7%
3	Win32/Obfuscator	Obfuscators & Injectors	0.7%
4	Win32/Peals	Trojans	0.6%
5	Win32/Skeeyah	Trojans	0.5%
6	Win32/Upatre	Downloaders & Droppers	0.2%
7	JS/Fiexp	Exploits	0.2%
8	JS/Neclu	Exploits	0.2%
9	Win32/Crowti	Ransomware	0.2%
10	Win32/Dynamer	Trojans	0.2%

- The most common malware family encountered in Canada in 2Q15 was [JS/Axpergle](#), which was encountered by 1.5 percent of reporting computers there. [JS/Axpergle](#) is a detection for the Angler exploit kit, which exploits vulnerabilities in recent versions of Internet Explorer, Silverlight, Adobe Flash Player, and Java to install malware.
- The second most common malware family encountered in Canada in 2Q15 was [Win32/Kilim](#), which was encountered by 0.7 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The third most common malware family encountered in Canada in 2Q15 was [Win32/Obfuscator](#), which was encountered by 0.7 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The fourth most common malware family encountered in Canada in 2Q15 was [Win32/Peals](#), which was encountered by 0.6 percent of reporting computers there. [Win32/Peals](#) is a generic detection for various threats that display trojan characteristics.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Canada in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	2.2%
2	Win32/KipodToolsCby	Browser Modifiers	1.6%
3	Win32/InstalleRex	Software Bundlers	1.2%
4	Win32/AlterbookSP	Browser Modifiers	1.0%
5	Win32/SaverExtension	Adware	0.7%

- The most common unwanted software family encountered in Canada in 2Q15 was [Win32/CouponRuc](#), which was encountered by 2.2 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in Canada in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 1.6 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common unwanted software family encountered in Canada in 2Q15 was [Win32/InstalleRex](#), which was encountered by 1.2 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Canada in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	1.5
2	Win32/Kilim	Trojans	1.2
3	Win32/CompromisedCert	Other Malware	0.4
4	Win32/Simda	Trojans	0.3
5	Win32/Alureon	Trojans	0.2
6	Win32/Dyzap	Password Stealers & Monitoring Tools	0.2
7	Win32/Nitol	Other Malware	0.1
8	Win32/Zbot	Password Stealers & Monitoring Tools	0.1
9	VBS/Jenxcus	Worms	0.1
10	MSIL/Bladabindi	Backdoors	0.1

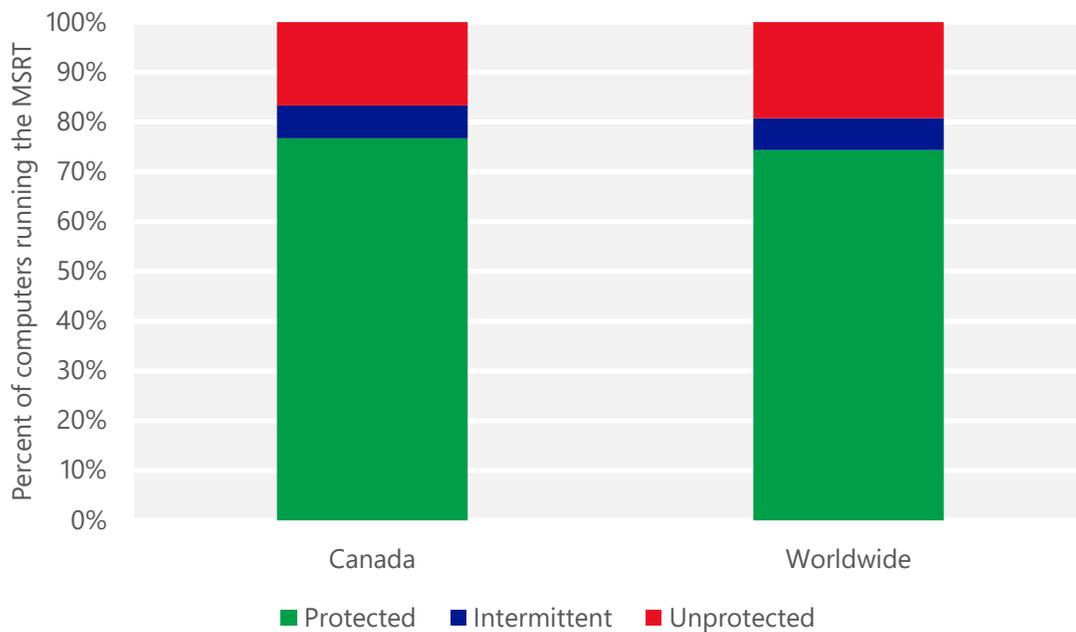
- The most common threat family infecting computers in Canada in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 1.5 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Canada in 2Q15 was [Win32/Kilim](#), which was detected and removed from 1.2 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The third most common threat family infecting computers in Canada in 2Q15 was [Win32/CompromisedCert](#), which was detected and removed from 0.4 of every 1,000 unique computers scanned by the MSRT. [Win32/CompromisedCert](#) is a detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.
- The fourth most common threat family infecting computers in Canada in 2Q15 was [Win32/Simda](#), which was detected and removed from 0.3 of every 1,000 unique computers scanned by the MSRT. [Win32/Simda](#) is a threat that can give an attacker backdoor access and control of an infected computer. It can then steal passwords and gather information about the computer to send to the attacker.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Canada and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Canada

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.17 (0.28)	0.13 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	5.22 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	17.33 (16.7)	

Chile

The statistics presented here are generated by Microsoft security programs and services running on computers in Chile in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Chile

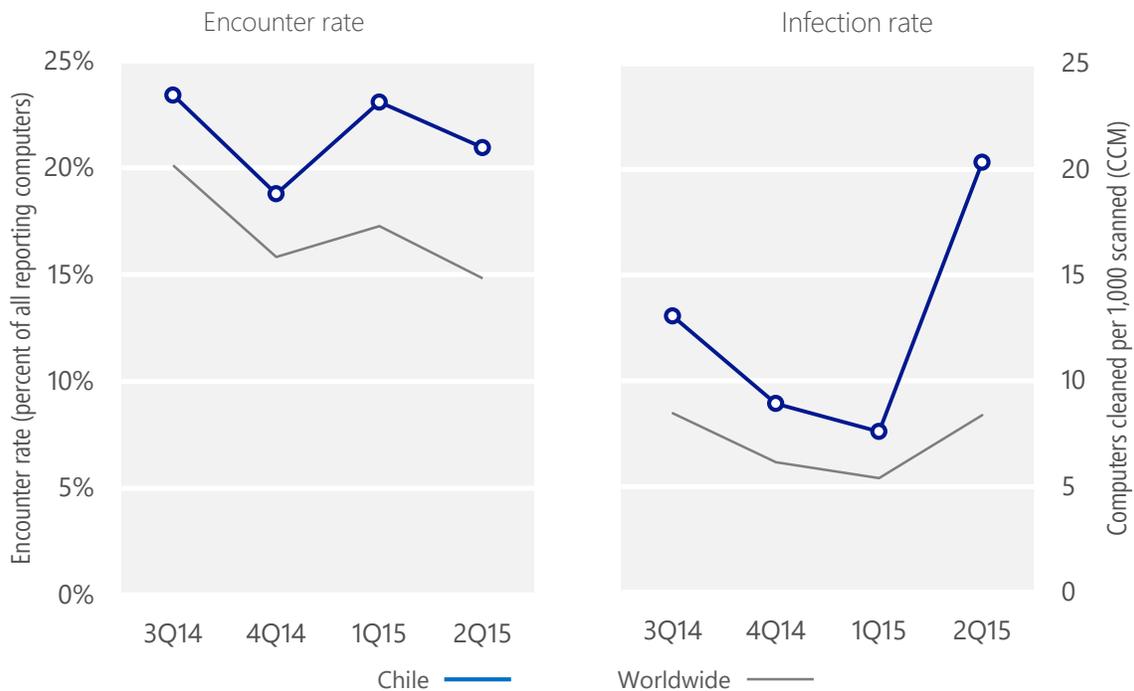
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Chile	23.4%	18.8%	23.1%	20.9%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Chile	13.1	8.9	7.6	20.3
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcote, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 20.9% of computers in Chile encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 20.3 of every 1,000 unique computers scanned in Chile in 2Q15 (a CCM score of 20.3, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Chile over the last four quarters, compared to the world as a whole.

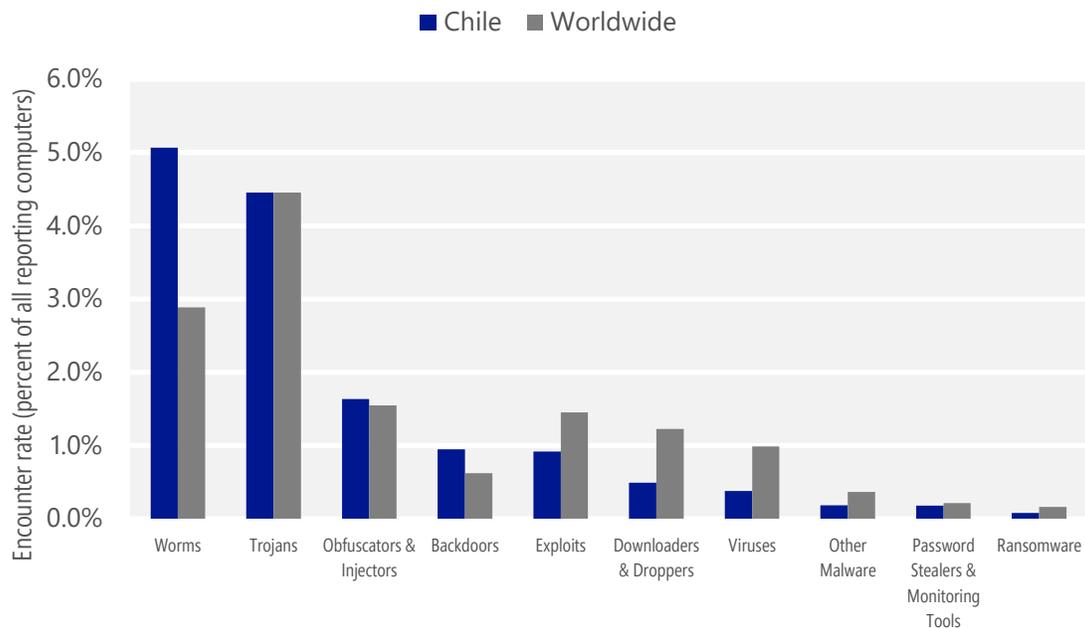
Malware encounter and infection rate trends in Chile and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in Chile and around the world, and for explanations of the methods and terms used here.

Malware categories

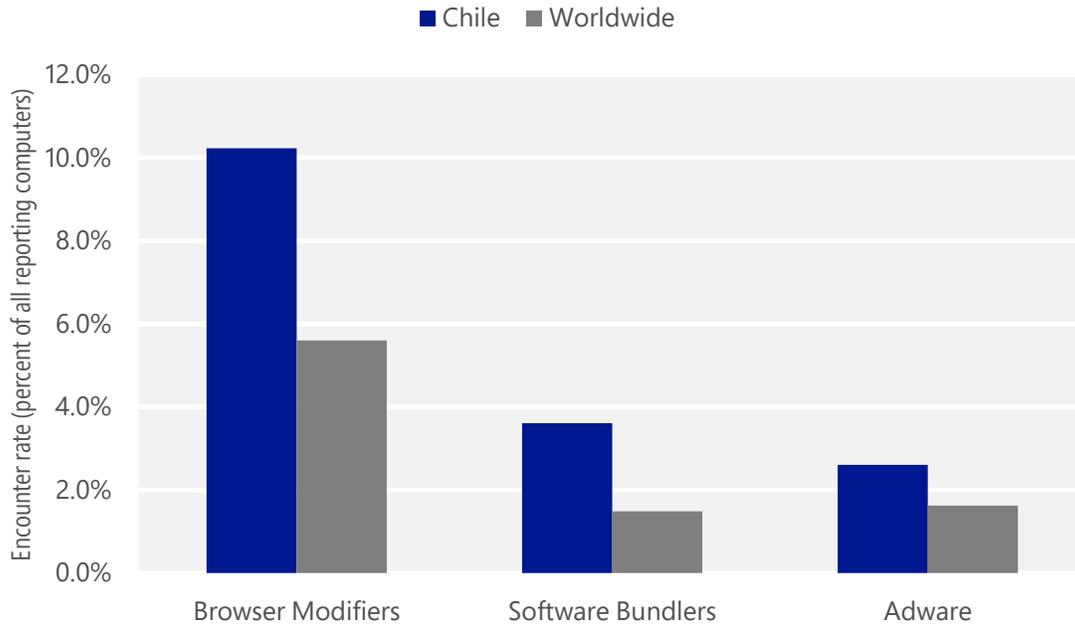
Malware encountered in Chile in 2Q15, by category



- The most common malware category in Chile in 2Q15 was Worms. It was encountered by 5.1 percent of all computers there, up from 4.4 percent in 1Q15.
- The second most common malware category in Chile in 2Q15 was Trojans. It was encountered by 4.5 percent of all computers there, up from 2.6 percent in 1Q15.
- The third most common malware category in Chile in 2Q15 was Obfuscators & Injectors, which was encountered by 1.6 percent of all computers there, down from 1.8 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Chile in 2Q15, by category



- The most common unwanted software category in Chile in 2Q15 was Browser Modifiers. It was encountered by 10.2 percent of all computers there, down from 13.8 percent in 1Q15.
- The second most common unwanted software category in Chile in 2Q15 was Software Bundlers. It was encountered by 3.6 percent of all computers there, down from 6.2 percent in 1Q15.
- The third most common unwanted software category in Chile in 2Q15 was Adware, which was encountered by 2.6 percent of all computers there, up from 0.7 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Chile in 2Q15

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	1.8%
2	JS/Bondat	Worms	1.8%
3	Win32/Kilim	Trojans	1.2%
4	Win32/Obfuscator	Obfuscators & Injectors	1.0%
5	Win32/Skeeyah	Trojans	0.8%
6	INF/Autorun	Obfuscators & Injectors	0.6%
7	Win32/Vermis	Worms	0.5%
8	Win32/Caphaw	Backdoors	0.5%
9	JS/Axpergle	Exploits	0.4%
10	Win32/Dorkbot	Worms	0.4%

- The most common malware family encountered in Chile in 2Q15 was [VBS/Jenxcus](#), which was encountered by 1.8 percent of reporting computers there. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common malware family encountered in Chile in 2Q15 was [JS/Bondat](#), which was encountered by 1.8 percent of reporting computers there. [JS/Bondat](#) is a family of threats that collects information about the computer, infects removable drives, and tries to stop the user from accessing files. It spreads by infecting removable drives, such as USB thumb drives and flash drives.
- The third most common malware family encountered in Chile in 2Q15 was [Win32/Kilim](#), which was encountered by 1.2 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The fourth most common malware family encountered in Chile in 2Q15 was [Win32/Obfuscator](#), which was encountered by 1.0 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Chile in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	5.6%
2	Win32/KipodToolsCby	Browser Modifiers	4.0%
3	Win32/InstalleRex	Software Bundlers	3.5%
4	Win32/SaverExtension	Adware	1.8%
5	Win32/AlterbookSP	Browser Modifiers	0.6%

- The most common unwanted software family encountered in Chile in 2Q15 was [Win32/CouponRuc](#), which was encountered by 5.6 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in Chile in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 4.0 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common unwanted software family encountered in Chile in 2Q15 was [Win32/InstalleRex](#), which was encountered by 3.5 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Chile in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	9.2
2	VBS/Jenxcus	Worms	3.6
3	Win32/CompromisedCert	Other Malware	2.0
4	Win32/Kilim	Trojans	1.8
5	Win32/Dorkbot	Worms	1.1
6	Win32/Brontok	Worms	0.5
7	Win32/Sality	Viruses	0.4
8	Win32/Lethic	Trojans	0.3
9	Win32/Ramnit	Trojans	0.3
10	Win32/Conficker	Worms	0.2

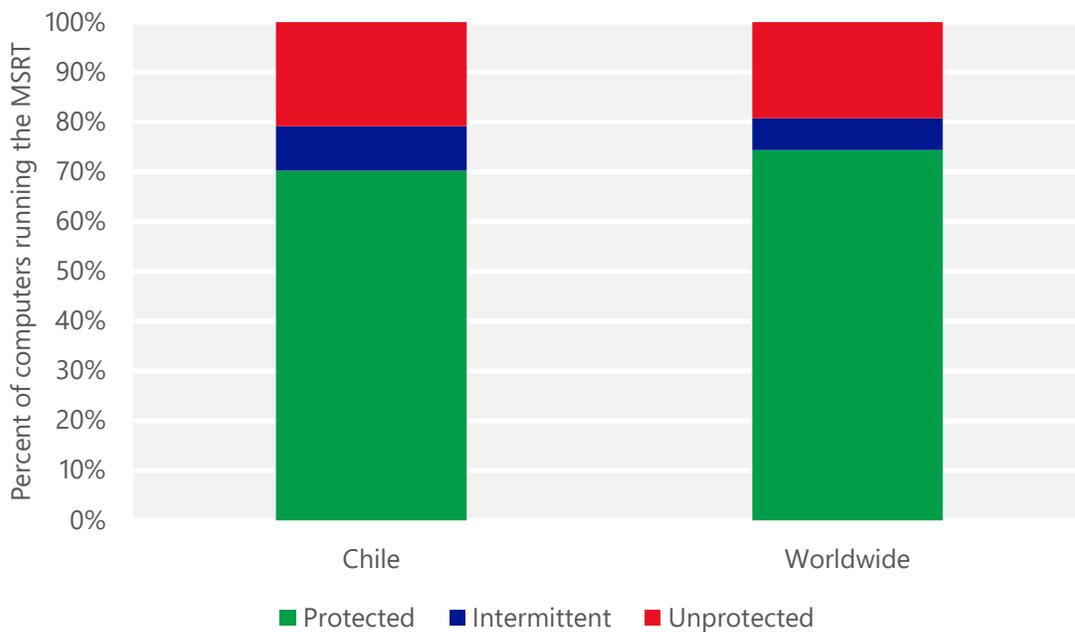
- The most common threat family infecting computers in Chile in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 9.2 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Chile in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 3.6 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The third most common threat family infecting computers in Chile in 2Q15 was [Win32/CompromisedCert](#), which was detected and removed from 2.0 of every 1,000 unique computers scanned by the MSRT. [Win32/CompromisedCert](#) is a detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.
- The fourth most common threat family infecting computers in Chile in 2Q15 was [Win32/Kilim](#), which was detected and removed from 1.8 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Chile and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Chile

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.25 (0.28)	0.47 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	8.54 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	7.44 (16.7)	

China

The statistics presented here are generated by Microsoft security programs and services running on computers in China in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for China

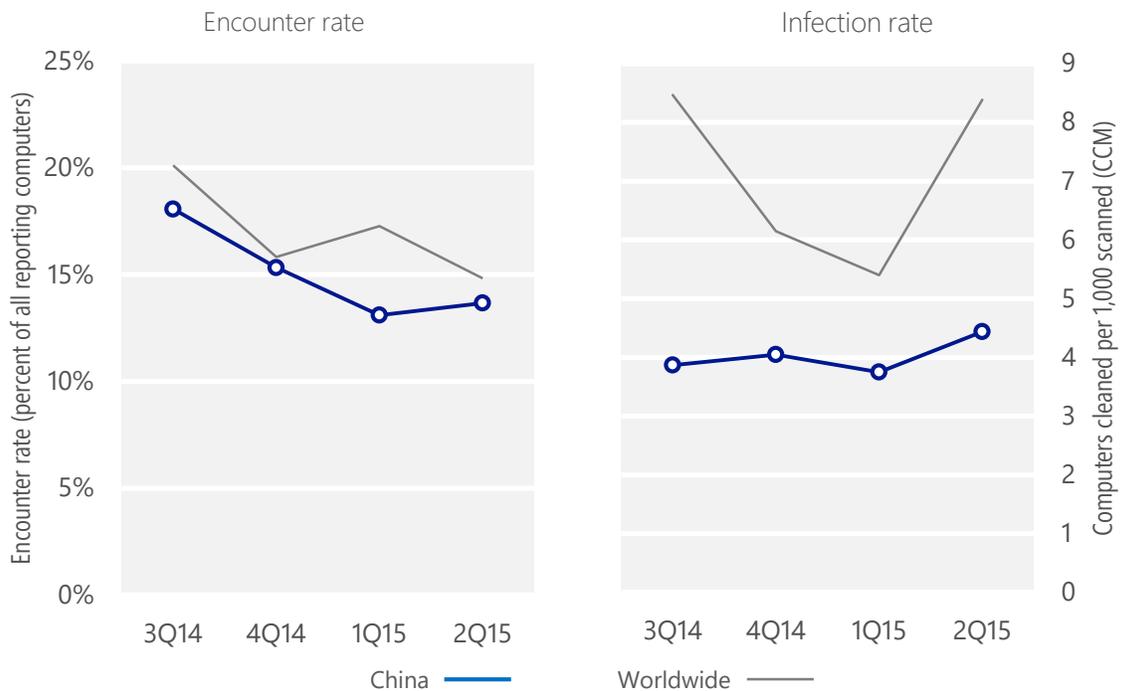
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, China	18.1%	15.3%	13.1%	13.7%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, China	3.9	4.0	3.8	4.4
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcote, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 13.7% of computers in China encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 4.4 of every 1,000 unique computers scanned in China in 2Q15 (a CCM score of 4.4, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for China over the last four quarters, compared to the world as a whole.

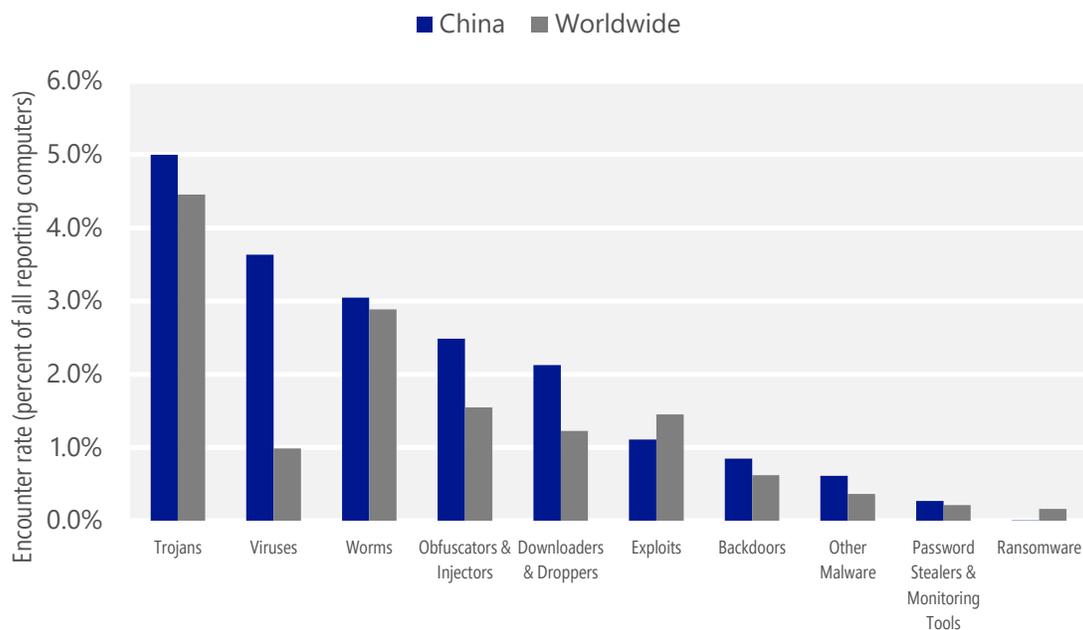
Malware encounter and infection rate trends in China and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in China and around the world, and for explanations of the methods and terms used here.

Malware categories

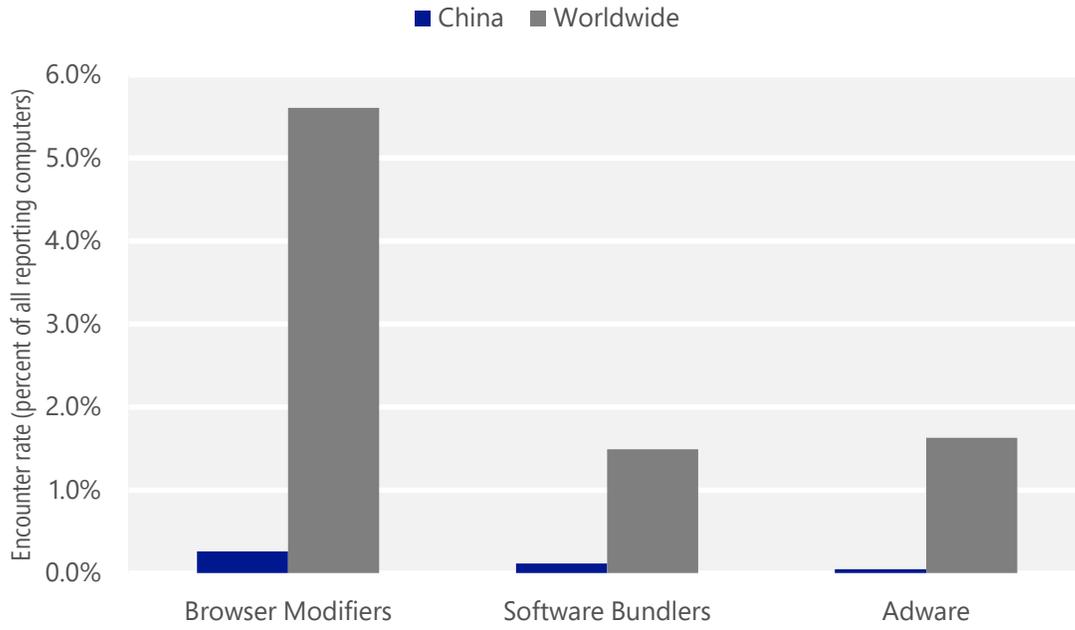
Malware encountered in China in 2Q15, by category



- The most common malware category in China in 2Q15 was Trojans. It was encountered by 5.0 percent of all computers there, down from 5.2 percent in 1Q15.
- The second most common malware category in China in 2Q15 was Viruses. It was encountered by 3.6 percent of all computers there, down from 3.8 percent in 1Q15.
- The third most common malware category in China in 2Q15 was Worms, which was encountered by 3.0 percent of all computers there, up from 2.6 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in China in 2Q15, by category



- The most common unwanted software category in China in 2Q15 was Browser Modifiers. It was encountered by 0.3 percent of all computers there, down from 0.3 percent in 1Q15.
- The second most common unwanted software category in China in 2Q15 was Software Bundlers. It was encountered by 0.1 percent of all computers there, down from 0.1 percent in 1Q15.
- The third most common unwanted software category in China in 2Q15 was Adware, which was encountered by 0.0 percent of all computers there, down from 0.1 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in China in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Obfuscator	Obfuscators & Injectors	2.0%
2	HTML/Adodb	Downloaders & Droppers	1.1%
3	DOS/JackTheRipper	Viruses	0.8%
4	VBS/CVE-2014-6332	Exploits	0.8%
5	Win32/Ramnit	Trojans	0.7%
6	INF/Autorun	Obfuscators & Injectors	0.7%
7	ALisp/Kenilfe	Worms	0.6%
8	Win32/Skeeyah	Trojans	0.5%
9	ALisp/Bursted	Viruses	0.5%
10	Win32/Nitol	Other Malware	0.5%

- The most common malware family encountered in China in 2Q15 was [Win32/Obfuscator](#), which was encountered by 2.0 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The second most common malware family encountered in China in 2Q15 was [HTML/Adodb](#), which was encountered by 1.1 percent of reporting computers there. [HTML/Adodb](#) is a generic detection for script trojans that exploit a vulnerability in Microsoft Data Access Components (MDAC) that allows remote code execution. Microsoft released Security Bulletin MS06-014 in April 2006 to address the vulnerability.
- The third most common malware family encountered in China in 2Q15 was [DOS/JackTheRipper](#), which was encountered by 0.8 percent of reporting computers there. [DOS/JackTheRipper](#) is a virus that can stop some files from working correctly in Windows XP and earlier operating systems. It spreads by infecting the master boot record (MBR) on connected hard disks and floppy disks.
- The fourth most common malware family encountered in China in 2Q15 was [VBS/CVE-2014-6332](#), which was encountered by 0.8 percent of reporting computers there. [VBS/CVE-2014-6332](#) is a detection for threats that use a vulnerability in Windows to download and run files on the computer, including other malware. Microsoft addressed the vulnerability with Security Bulletin MS14-064 in November 2014.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in China in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	0.1%
2	Win32/InstalleRex	Software Bundlers	0.1%
3	Win32/KipodToolsCby	Browser Modifiers	0.1%
4	Win32/AlterbookSP	Browser Modifiers	<0.1%
5	Win32/SaverExtension	Adware	<0.1%

- The most common unwanted software family encountered in China in 2Q15 was [Win32/CouponRuc](#), which was encountered by 0.1 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in China in 2Q15 was [Win32/InstalleRex](#), which was encountered by 0.1 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own “Installed On” date in Programs and Features to make it more difficult for a user to locate it and remove it.
- The third most common unwanted software family encountered in China in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 0.1 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user’s consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.

Top threat families by infection rate

The most common malware families by infection rate in China in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/Nitol	Other Malware	1.2
2	Win32/Ramnit	Trojans	1.1
3	Win32/Frethog	Password Stealers & Monitoring Tools	0.5
4	Win32/Sality	Viruses	0.3
5	VBS/Jenxcus	Worms	0.2
6	Win32/Conficker	Worms	0.2
7	Win32/Virut	Viruses	0.2
8	Win32/Parite	Viruses	0.1
9	Win32/Gamarue	Worms	0.1
10	Win32/Yeltminky	Worms	0.1

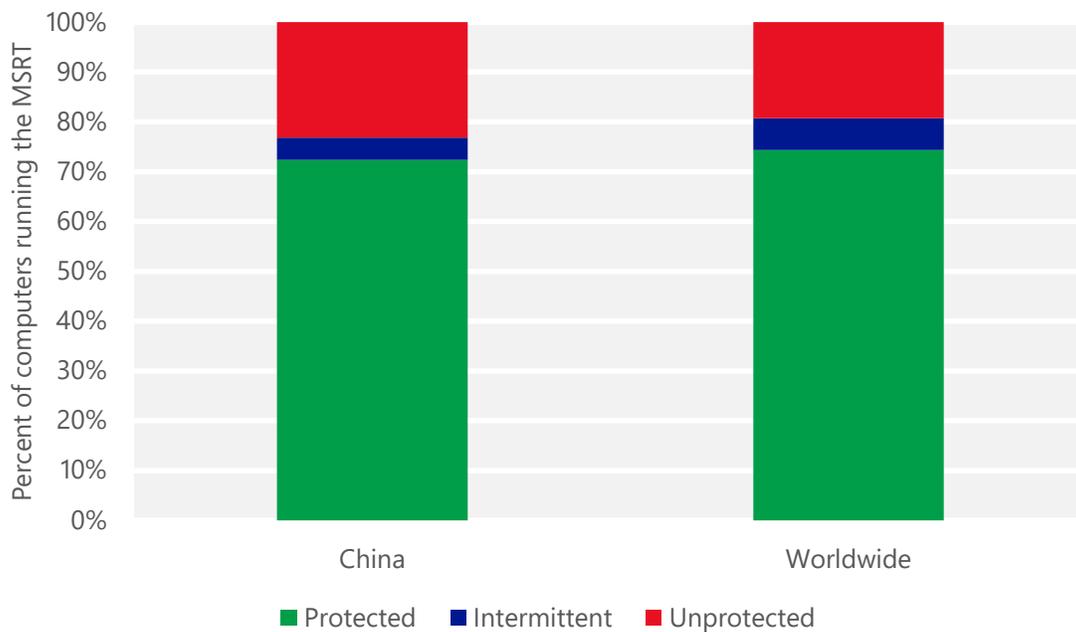
- The most common threat family infecting computers in China in 2Q15 was [Win32/Nitol](#), which was detected and removed from 1.2 of every 1,000 unique computers scanned by the MSRT. [Win32/Nitol](#) is a family of trojans that perform DDoS (distributed denial of service) attacks, allow backdoor access and control, download and run files, and perform a number of other malicious activities on the computer.
- The second most common threat family infecting computers in China in 2Q15 was [Win32/Ramnit](#), which was detected and removed from 1.1 of every 1,000 unique computers scanned by the MSRT. [Win32/Ramnit](#) is a family of multi-component malware that infects executable files, Microsoft Office files, and HTML files. Win32/Ramnit spreads to removable drives and steals sensitive information such as saved FTP credentials and browser cookies. It may also open a backdoor to await instructions from a remote attacker.
- The third most common threat family infecting computers in China in 2Q15 was [Win32/Frethog](#), which was detected and removed from 0.5 of every 1,000 unique computers scanned by the MSRT. [Win32/Frethog](#) is a large family of password-stealing trojans that targets confidential data, such as account information, from massively multiplayer online games.
- The fourth most common threat family infecting computers in China in 2Q15 was [Win32/Sality](#), which was detected and removed from 0.3 of every 1,000 unique computers scanned by the MSRT. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in China and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for China

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.15 (0.28)	0.19 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	1.64 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	10.31 (16.7)	

Colombia

The statistics presented here are generated by Microsoft security programs and services running on computers in Colombia in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Colombia

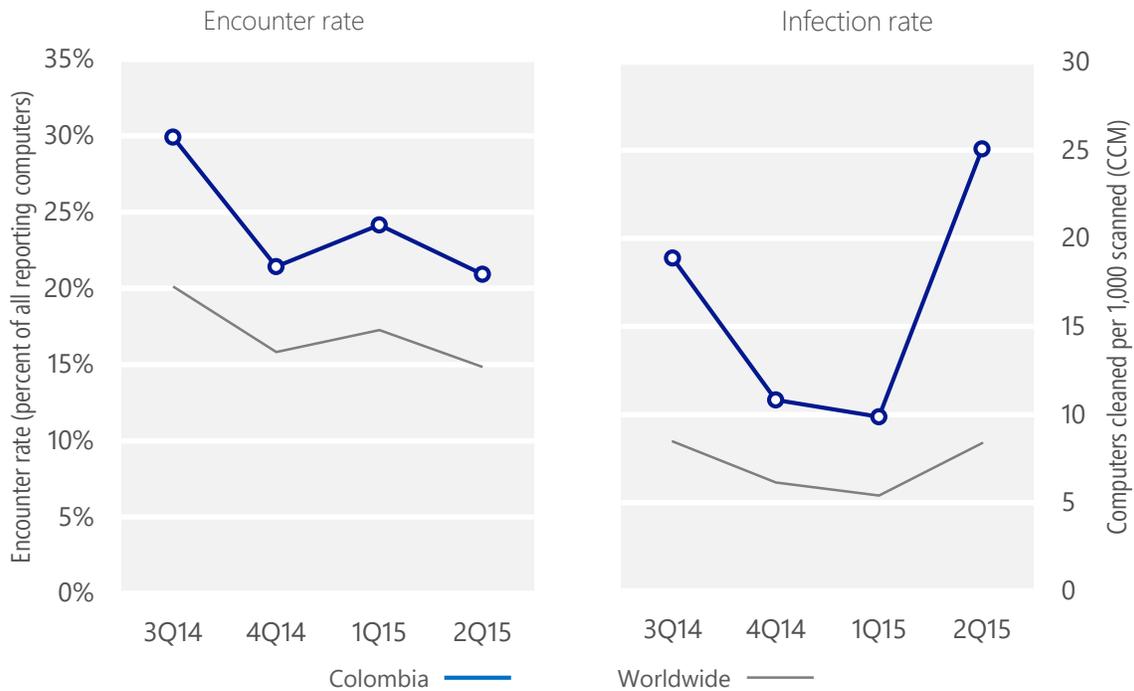
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Colombia	29.9%	21.4%	24.2%	20.9%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Colombia	18.9	10.8	9.9	25.1
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcoute, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 20.9% of computers in Colombia encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 25.1 of every 1,000 unique computers scanned in Colombia in 2Q15 (a CCM score of 25.1, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Colombia over the last four quarters, compared to the world as a whole.

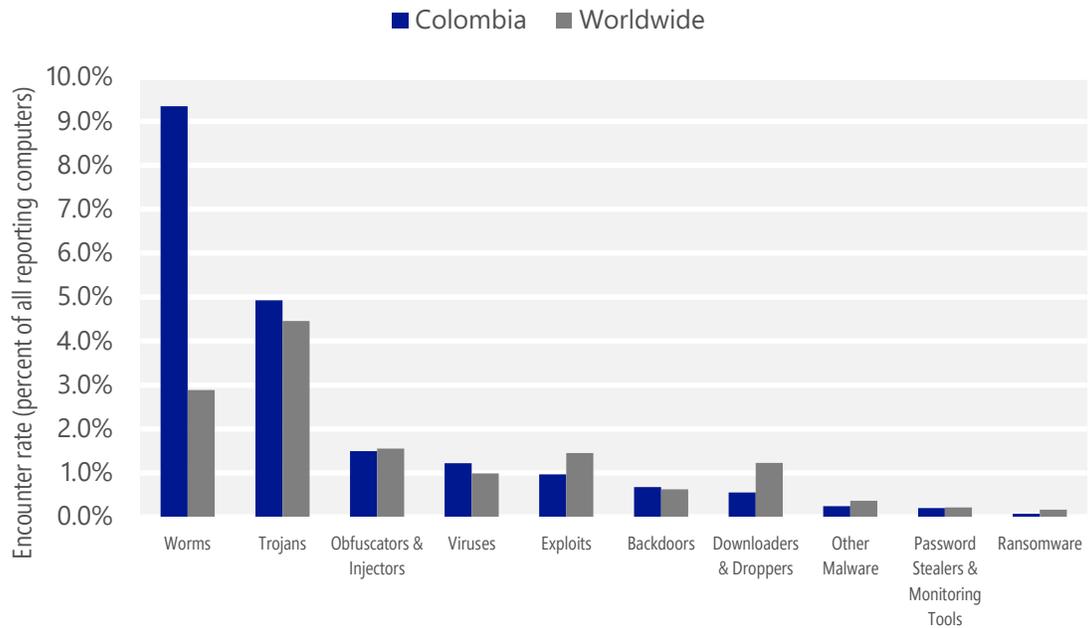
Malware encounter and infection rate trends in Colombia and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in Colombia and around the world, and for explanations of the methods and terms used here.

Malware categories

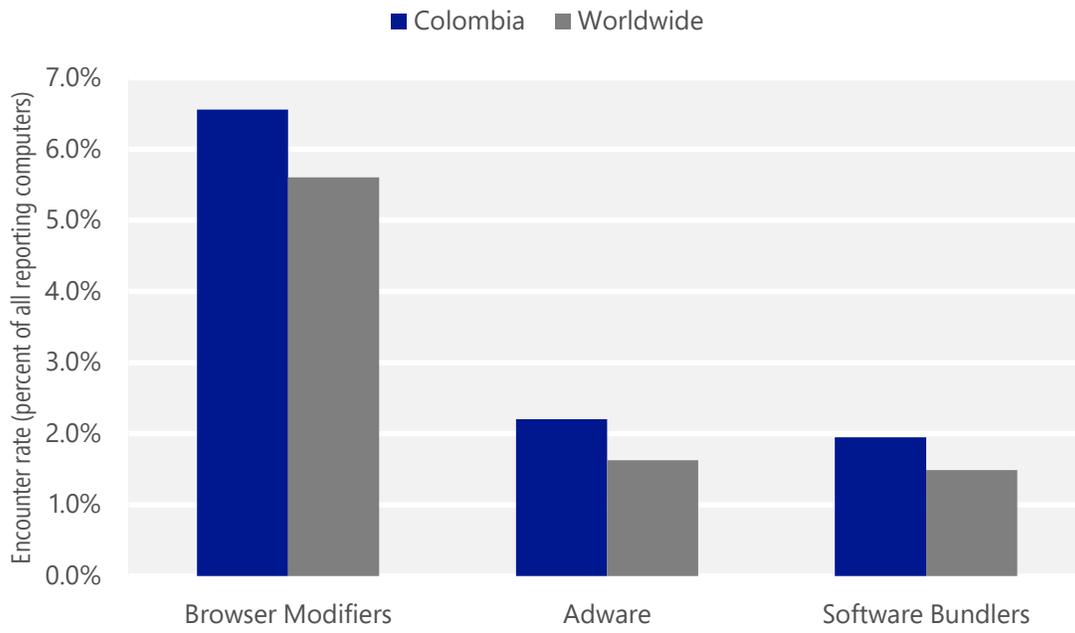
Malware encountered in Colombia in 2Q15, by category



- The most common malware category in Colombia in 2Q15 was Worms. It was encountered by 9.3 percent of all computers there, up from 8.9 percent in 1Q15.
- The second most common malware category in Colombia in 2Q15 was Trojans. It was encountered by 4.9 percent of all computers there, up from 4.2 percent in 1Q15.
- The third most common malware category in Colombia in 2Q15 was Obfuscators & Injectors, which was encountered by 1.5 percent of all computers there, down from 1.7 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Colombia in 2Q15, by category



- The most common unwanted software category in Colombia in 2Q15 was Browser Modifiers. It was encountered by 6.6 percent of all computers there, down from 10.5 percent in 1Q15.
- The second most common unwanted software category in Colombia in 2Q15 was Adware. It was encountered by 2.2 percent of all computers there, down from 4.4 percent in 1Q15.
- The third most common unwanted software category in Colombia in 2Q15 was Software Bundlers, which was encountered by 1.9 percent of all computers there, up from 0.5 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Colombia in 2Q15

	Family	Most significant category	% of reporting computers
1	JS/Bondat	Worms	4.8%
2	VBS/Jenxcus	Worms	4.1%
3	Win32/Kilim	Trojans	1.1%
4	Win32/Skeeyah	Trojans	0.9%
5	INF/Autorun	Obfuscators & Injectors	0.8%
6	Win32/Obfuscator	Obfuscators & Injectors	0.8%
7	Win32/Gamarue	Worms	0.7%
8	Win32/Peals	Trojans	0.5%
9	Win32/Sality	Viruses	0.4%
10	Win32/Ramnit	Trojans	0.4%

- The most common malware family encountered in Colombia in 2Q15 was [JS/Bondat](#), which was encountered by 4.8 percent of reporting computers there. [JS/Bondat](#) is a family of threats that collects information about the computer, infects removable drives, and tries to stop the user from accessing files. It spreads by infecting removable drives, such as USB thumb drives and flash drives.
- The second most common malware family encountered in Colombia in 2Q15 was [VBS/Jenxcus](#), which was encountered by 4.1 percent of reporting computers there. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The third most common malware family encountered in Colombia in 2Q15 was [Win32/Kilim](#), which was encountered by 1.1 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The fourth most common malware family encountered in Colombia in 2Q15 was [Win32/Skeeyah](#), which was encountered by 0.9 percent of reporting computers there. [Win32/Skeeyah](#) is a generic detection for various threats that display trojan characteristics.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Colombia in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	3.4%
2	Win32/KipodToolsCby	Browser Modifiers	2.3%
3	Win32/InstalleRex	Software Bundlers	1.8%
4	Win32/SaverExtension	Adware	1.0%
5	Win32/AlterbookSP	Browser Modifiers	0.6%

- The most common unwanted software family encountered in Colombia in 2Q15 was [Win32/CouponRuc](#), which was encountered by 3.4 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in Colombia in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 2.3 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common unwanted software family encountered in Colombia in 2Q15 was [Win32/InstalleRex](#), which was encountered by 1.8 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Colombia in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	10.3
2	Win32/leEnablerCby	Browser Modifiers	8.8
3	Win32/CompromisedCert	Other Malware	1.9
4	Win32/Kilim	Trojans	1.1
5	Win32/Sality	Viruses	0.9
6	Win32/Ramnit	Trojans	0.7
7	Win32/Gamarue	Worms	0.4
8	Win32/Dorkbot	Worms	0.3
9	Win32/Yeltminky	Worms	0.2
10	MSIL/Bladabindi	Backdoors	0.2

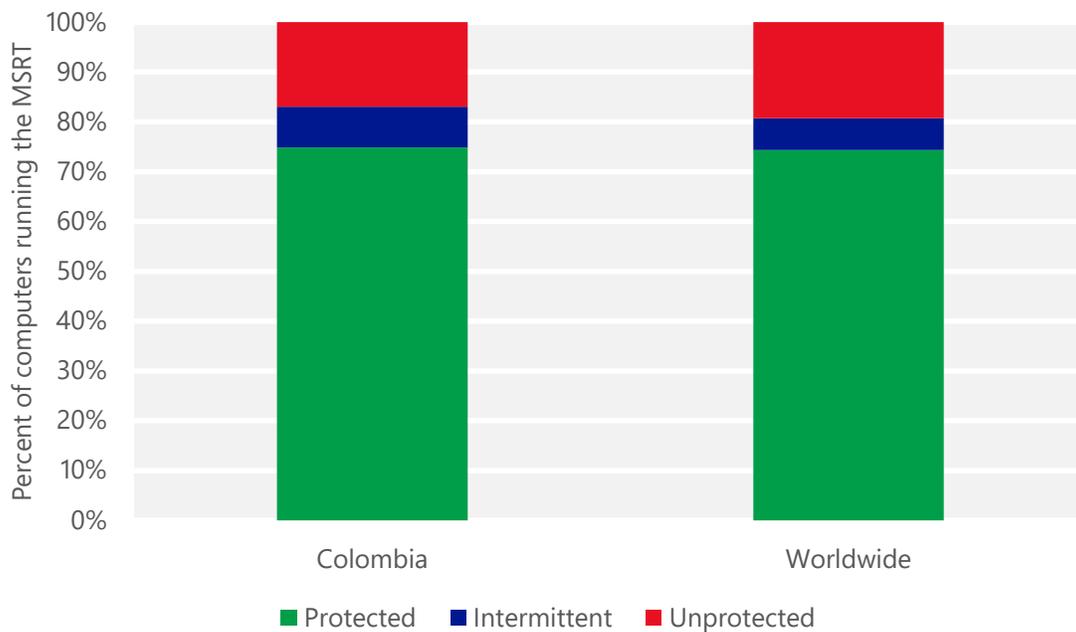
- The most common threat family infecting computers in Colombia in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 10.3 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Colombia in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 8.8 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common threat family infecting computers in Colombia in 2Q15 was [Win32/CompromisedCert](#), which was detected and removed from 1.9 of every 1,000 unique computers scanned by the MSRT. [Win32/CompromisedCert](#) is a detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.
- The fourth most common threat family infecting computers in Colombia in 2Q15 was [Win32/Kilim](#), which was detected and removed from 1.1 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Colombia and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Colombia

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.35 (0.28)	0.03 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	6.31 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	4.35 (16.7)	

Costa Rica

The statistics presented here are generated by Microsoft security programs and services running on computers in Costa Rica in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Costa Rica

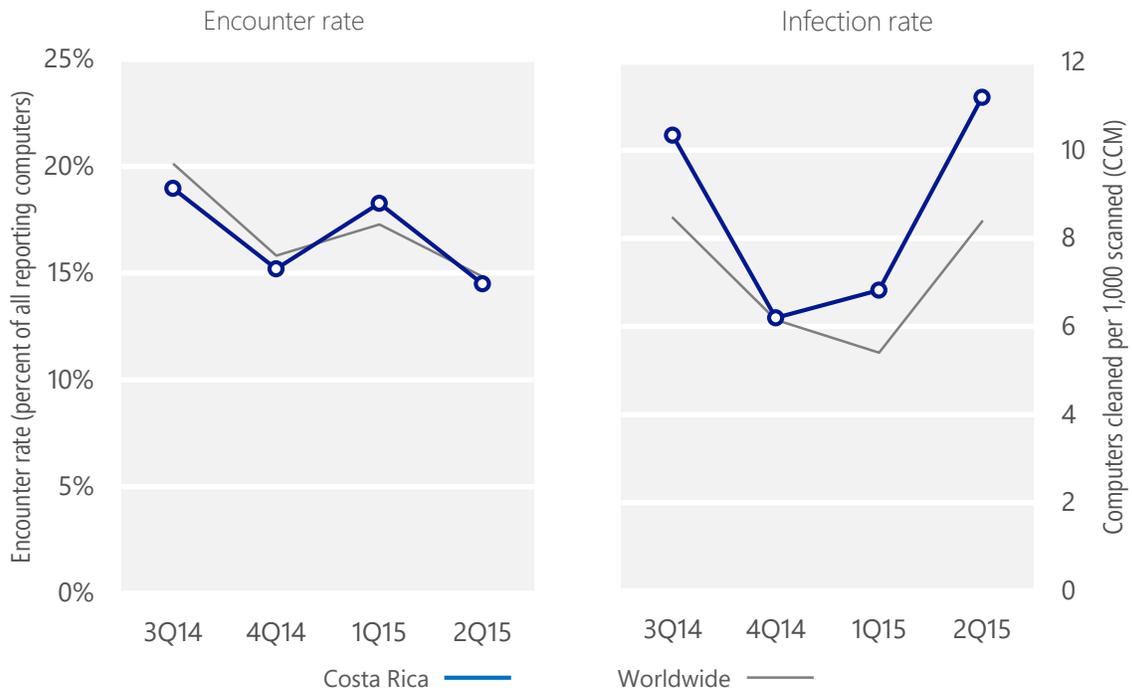
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Costa Rica	19.0%	15.2%	18.3%	14.5%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Costa Rica	10.3	6.2	6.8	11.2
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcoute, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 14.5% of computers in Costa Rica encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 11.2 of every 1,000 unique computers scanned in Costa Rica in 2Q15 (a CCM score of 11.2, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Costa Rica over the last four quarters, compared to the world as a whole.

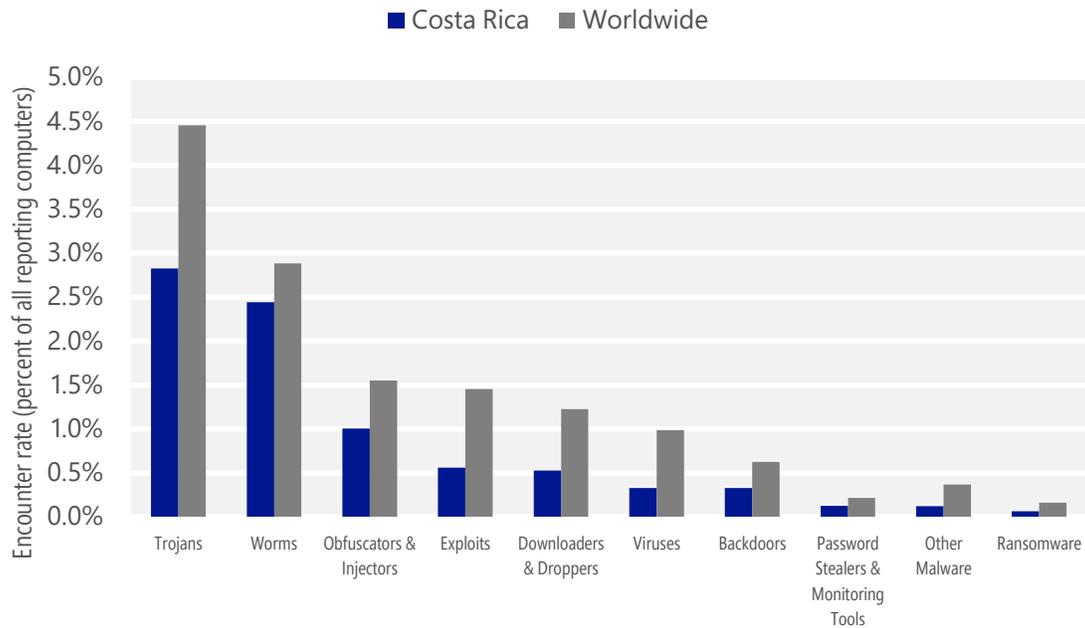
Malware encounter and infection rate trends in Costa Rica and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in Costa Rica and around the world, and for explanations of the methods and terms used here.

Malware categories

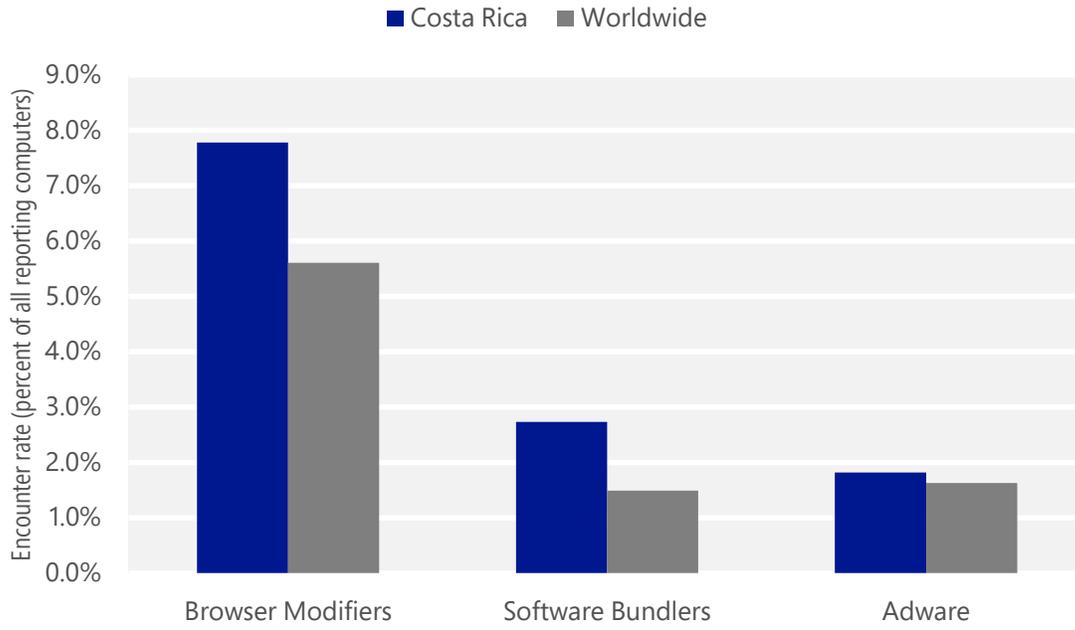
Malware encountered in Costa Rica in 2Q15, by category



- The most common malware category in Costa Rica in 2Q15 was Trojans. It was encountered by 2.8 percent of all computers there, down from 3.2 percent in 1Q15.
- The second most common malware category in Costa Rica in 2Q15 was Worms. It was encountered by 2.4 percent of all computers there, up from 2.1 percent in 1Q15.
- The third most common malware category in Costa Rica in 2Q15 was Obfuscators & Injectors, which was encountered by 1.0 percent of all computers there, down from 1.1 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Costa Rica in 2Q15, by category



- The most common unwanted software category in Costa Rica in 2Q15 was Browser Modifiers. It was encountered by 7.8 percent of all computers there, down from 11.3 percent in 1Q15.
- The second most common unwanted software category in Costa Rica in 2Q15 was Software Bundlers. It was encountered by 2.7 percent of all computers there, down from 4.3 percent in 1Q15.
- The third most common unwanted software category in Costa Rica in 2Q15 was Adware, which was encountered by 1.8 percent of all computers there, up from 0.6 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Costa Rica in 2Q15

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	1.4%
2	Win32/Kilim	Trojans	0.9%
3	Win32/Obfuscator	Obfuscators & Injectors	0.6%
4	Win32/Skeeyah	Trojans	0.5%
5	INF/Autorun	Obfuscators & Injectors	0.4%
6	JS/Axpergle	Exploits	0.3%
7	Win32/Peals	Trojans	0.2%
8	Win32/Vermis	Worms	0.2%
9	Win32/Conficker	Worms	0.2%
10	Win32/Dynamer	Trojans	0.1%

- The most common malware family encountered in Costa Rica in 2Q15 was [VBS/Jenxcus](#), which was encountered by 1.4 percent of reporting computers there. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common malware family encountered in Costa Rica in 2Q15 was [Win32/Kilim](#), which was encountered by 0.9 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The third most common malware family encountered in Costa Rica in 2Q15 was [Win32/Obfuscator](#), which was encountered by 0.6 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The fourth most common malware family encountered in Costa Rica in 2Q15 was [Win32/Skeeyah](#), which was encountered by 0.5 percent of reporting computers there. [Win32/Skeeyah](#) is a generic detection for various threats that display trojan characteristics.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Costa Rica in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	4.0%
2	Win32/KipodToolsCby	Browser Modifiers	3.2%
3	Win32/InstalleRex	Software Bundlers	2.6%
4	Win32/SaverExtension	Adware	1.3%
5	Win32/AlterbookSP	Browser Modifiers	0.4%

- The most common unwanted software family encountered in Costa Rica in 2Q15 was [Win32/CouponRuc](#), which was encountered by 4.0 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in Costa Rica in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 3.2 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common unwanted software family encountered in Costa Rica in 2Q15 was [Win32/InstalleRex](#), which was encountered by 2.6 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Costa Rica in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	5.7
2	VBS/Jenxcus	Worms	2.4
3	Win32/Kilim	Trojans	1.2
4	Win32/CompromisedCert	Other Malware	0.3
5	Win32/Sality	Viruses	0.2
6	Win32/Conficker	Worms	0.2
7	Win32/Dorkbot	Worms	0.2
8	Win32/Brontok	Worms	0.2
9	MSIL/Spacekito	Trojans	0.1
10	Win32/Ramnit	Trojans	0.1

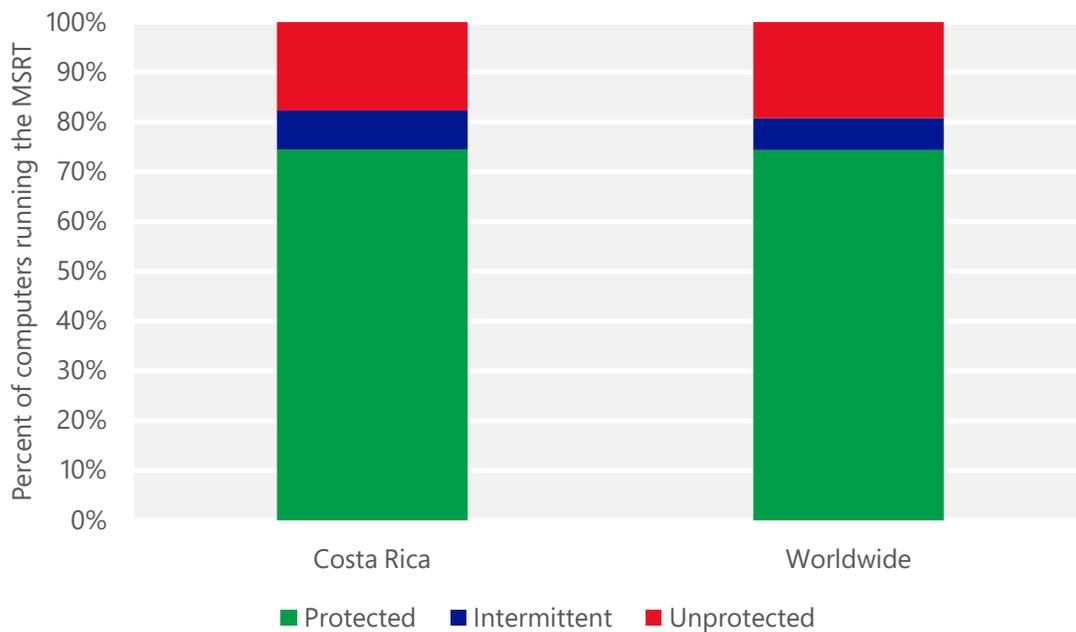
- The most common threat family infecting computers in Costa Rica in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 5.7 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Costa Rica in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 2.4 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The third most common threat family infecting computers in Costa Rica in 2Q15 was [Win32/Kilim](#), which was detected and removed from 1.2 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The fourth most common threat family infecting computers in Costa Rica in 2Q15 was [Win32/CompromisedCert](#), which was detected and removed from 0.3 of every 1,000 unique computers scanned by the MSRT. [Win32/CompromisedCert](#) is a detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Costa Rica and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Costa Rica

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.01 (0.28)	0.04 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	3.77 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	38.84 (16.7)	

Croatia

The statistics presented here are generated by Microsoft security programs and services running on computers in Croatia in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Croatia

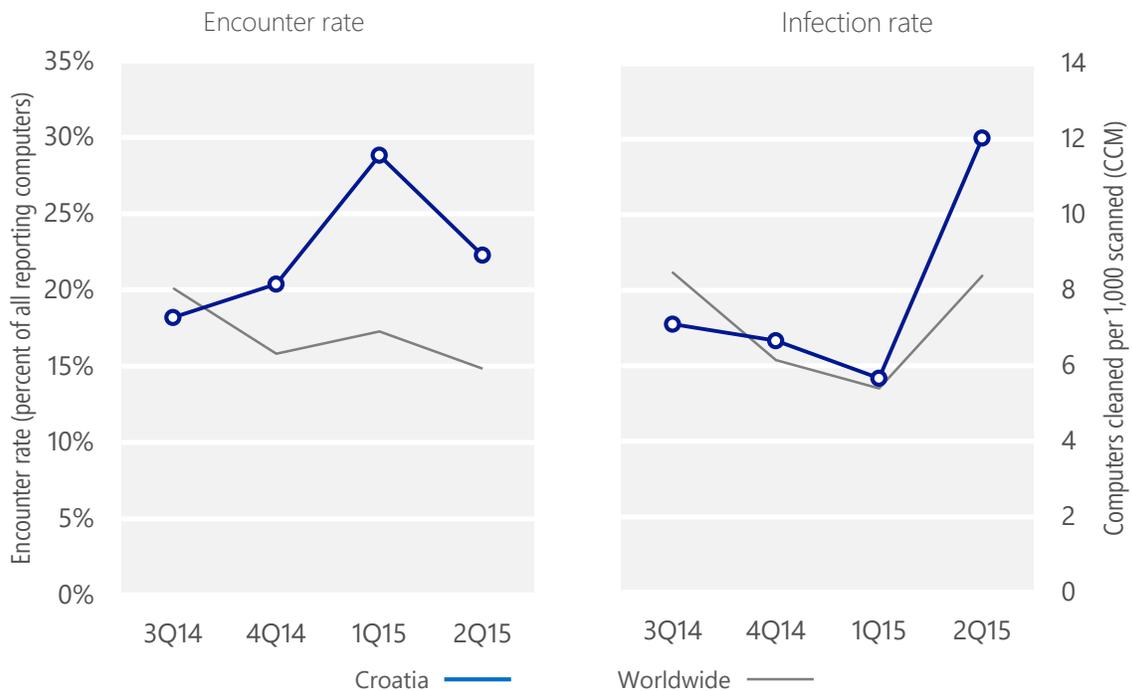
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Croatia	18.2%	20.4%	28.8%	22.3%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Croatia	7.1	6.7	5.7	12.0
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcout, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 22.3% of computers in Croatia encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 12.0 of every 1,000 unique computers scanned in Croatia in 2Q15 (a CCM score of 12.0, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Croatia over the last four quarters, compared to the world as a whole.

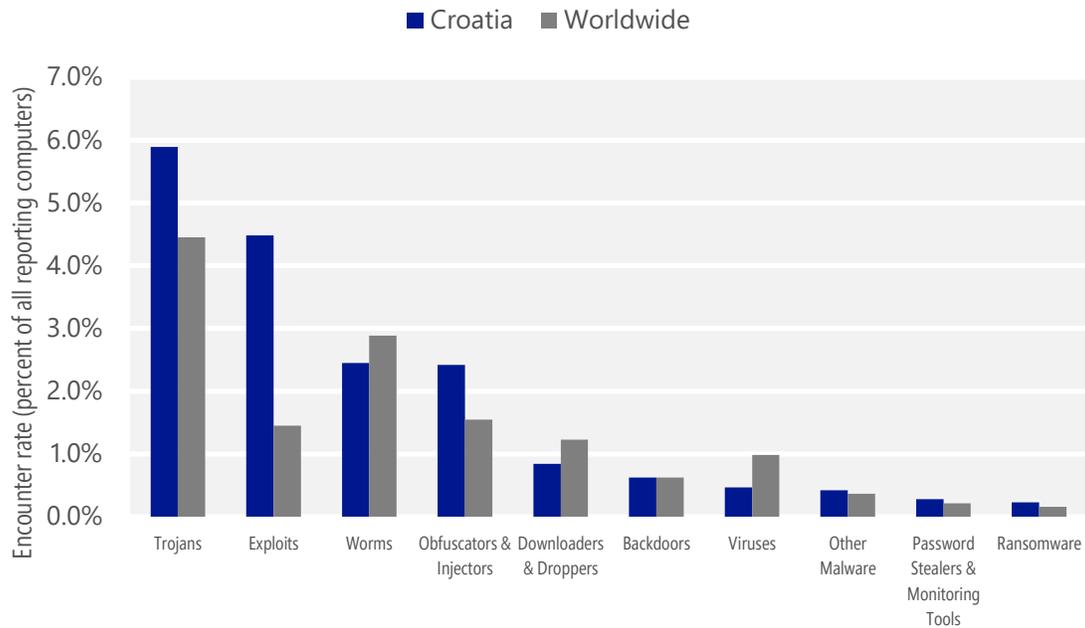
Malware encounter and infection rate trends in Croatia and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in Croatia and around the world, and for explanations of the methods and terms used here.

Malware categories

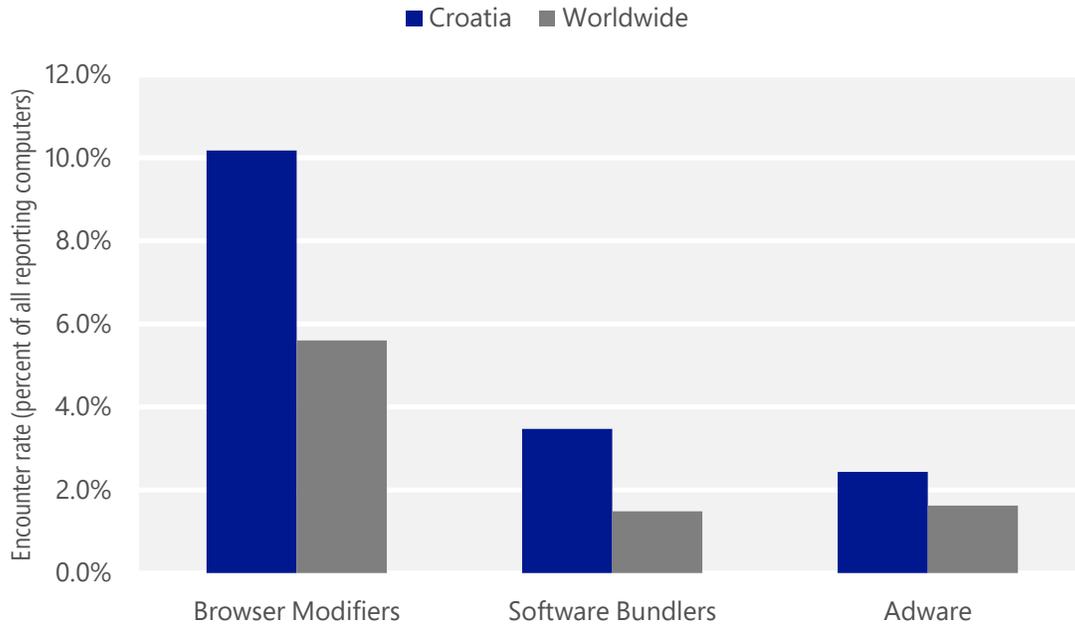
Malware encountered in Croatia in 2Q15, by category



- The most common malware category in Croatia in 2Q15 was Trojans. It was encountered by 5.9 percent of all computers there, up from 5.4 percent in 1Q15.
- The second most common malware category in Croatia in 2Q15 was Exploits. It was encountered by 4.5 percent of all computers there, down from 4.8 percent in 1Q15.
- The third most common malware category in Croatia in 2Q15 was Worms, which was encountered by 2.5 percent of all computers there, down from 3.3 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Croatia in 2Q15, by category



- The most common unwanted software category in Croatia in 2Q15 was Browser Modifiers. It was encountered by 10.2 percent of all computers there, down from 15.1 percent in 1Q15.
- The second most common unwanted software category in Croatia in 2Q15 was Software Bundlers. It was encountered by 3.5 percent of all computers there, down from 6.7 percent in 1Q15.
- The third most common unwanted software category in Croatia in 2Q15 was Adware, which was encountered by 2.4 percent of all computers there, up from 1.3 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Croatia in 2Q15

	Family	Most significant category	% of reporting computers
1	JS/Axpergle	Exploits	2.1%
2	Win32/Obfuscator	Obfuscators & Injectors	2.0%
3	Win32/Kilim	Trojans	1.7%
4	JS/Neclu	Exploits	1.6%
5	Win32/Skeeyah	Trojans	1.0%
6	Win32/Gamarue	Worms	0.9%
7	Win32/Peals	Trojans	0.8%
8	Win32/Pdfjsc	Exploits	0.5%
9	Win32/Sdbby	Exploits	0.5%
10	INF/Autorun	Obfuscators & Injectors	0.5%

- The most common malware family encountered in Croatia in 2Q15 was [JS/Axpergle](#), which was encountered by 2.1 percent of reporting computers there. [JS/Axpergle](#) is a detection for the Angler exploit kit, which exploits vulnerabilities in recent versions of Internet Explorer, Silverlight, Adobe Flash Player, and Java to install malware.
- The second most common malware family encountered in Croatia in 2Q15 was [Win32/Obfuscator](#), which was encountered by 2.0 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The third most common malware family encountered in Croatia in 2Q15 was [Win32/Kilim](#), which was encountered by 1.7 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The fourth most common malware family encountered in Croatia in 2Q15 was [JS/Neclu](#), which was encountered by 1.6 percent of reporting computers there. [JS/Neclu](#) is a detection for the Nuclear exploit kit, which attempts to exploit vulnerabilities in programs such as Java and Adobe Reader to install other malware.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Croatia in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	6.1%
2	Win32/KipodToolsCby	Browser Modifiers	3.8%
3	Win32/InstalleRex	Software Bundlers	3.3%
4	Win32/SaverExtension	Adware	1.9%
5	Win32/AlterbookSP	Browser Modifiers	0.7%

- The most common unwanted software family encountered in Croatia in 2Q15 was [Win32/CouponRuc](#), which was encountered by 6.1 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in Croatia in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 3.8 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common unwanted software family encountered in Croatia in 2Q15 was [Win32/InstalleRex](#), which was encountered by 3.3 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Croatia in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	4.4
2	Win32/Kilim	Trojans	1.7
3	Win32/CompromisedCert	Other Malware	1.6
4	Win32/Sality	Viruses	0.6
5	Win32/Carberp	Trojans	0.5
6	Win32/Gamarue	Worms	0.5
7	Win32/Helompy	Worms	0.5
8	VBS/Jenxcus	Worms	0.4
9	Win32/Simda	Trojans	0.4
10	Win32/Brontok	Worms	0.4

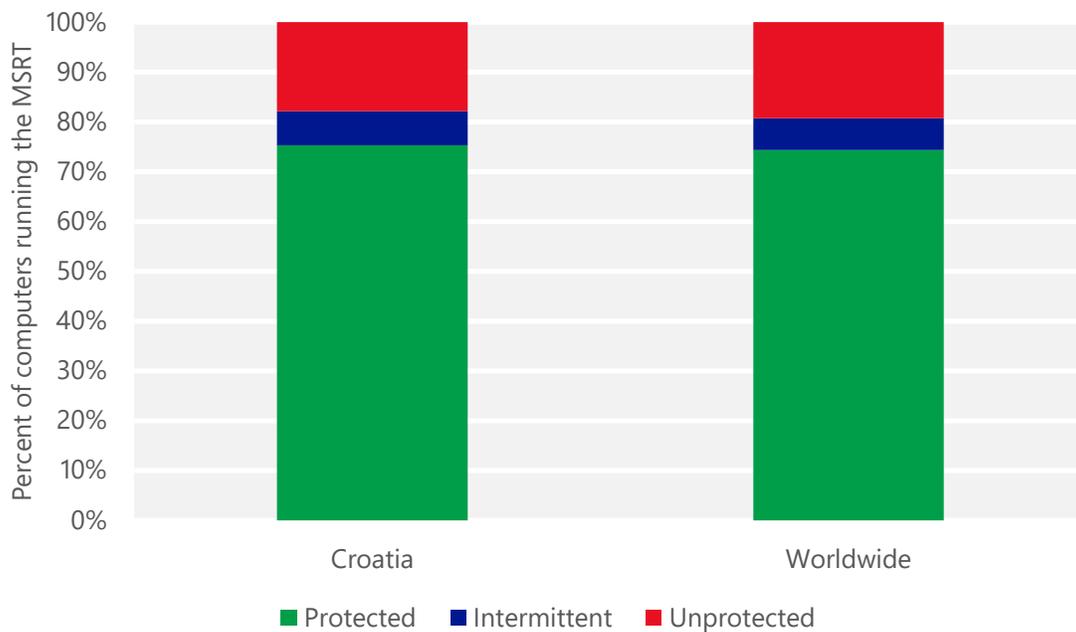
- The most common threat family infecting computers in Croatia in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 4.4 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Croatia in 2Q15 was [Win32/Kilim](#), which was detected and removed from 1.7 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The third most common threat family infecting computers in Croatia in 2Q15 was [Win32/CompromisedCert](#), which was detected and removed from 1.6 of every 1,000 unique computers scanned by the MSRT. [Win32/CompromisedCert](#) is a detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.
- The fourth most common threat family infecting computers in Croatia in 2Q15 was [Win32/Sality](#), which was detected and removed from 0.6 of every 1,000 unique computers scanned by the MSRT. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Croatia and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Croatia

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.06 (0.28)	0.08 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	5.41 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	13.47 (16.7)	

Cyprus

The statistics presented here are generated by Microsoft security programs and services running on computers in Cyprus in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille, or CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Cyprus

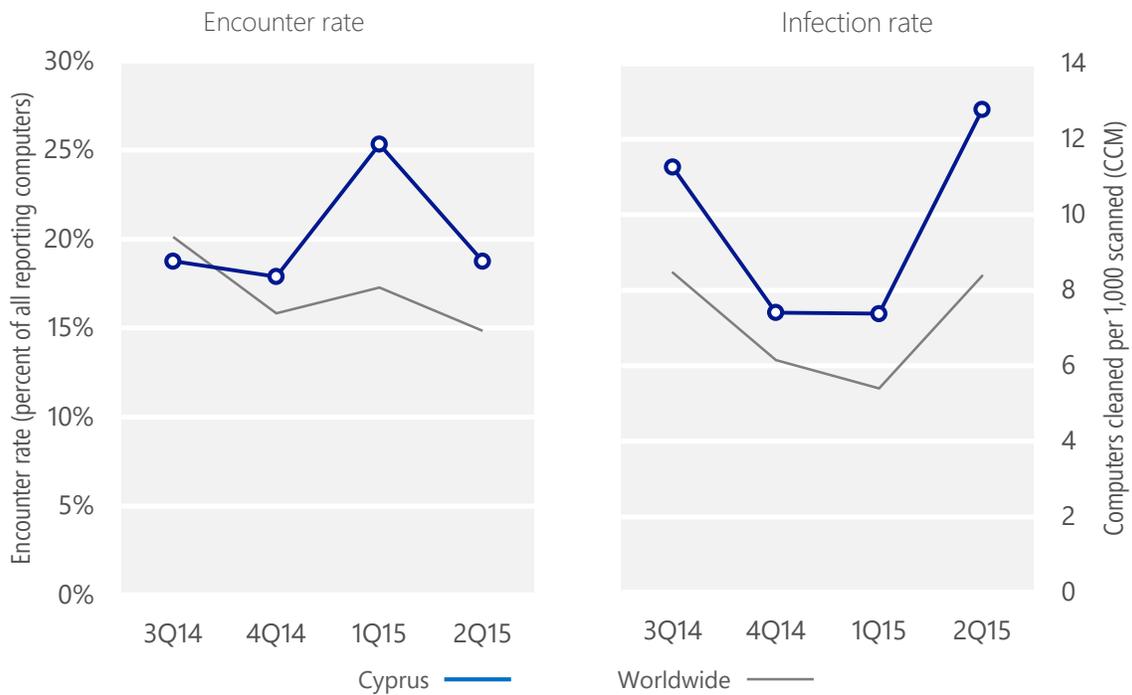
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Cyprus	18.8%	17.9%	25.3%	18.8%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Cyprus	11.3	7.4	7.4	12.8
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcote, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 18.8% of computers in Cyprus encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 12.8 of every 1,000 unique computers scanned in Cyprus in 2Q15 (a CCM score of 12.8, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Cyprus over the last four quarters, compared to the world as a whole.

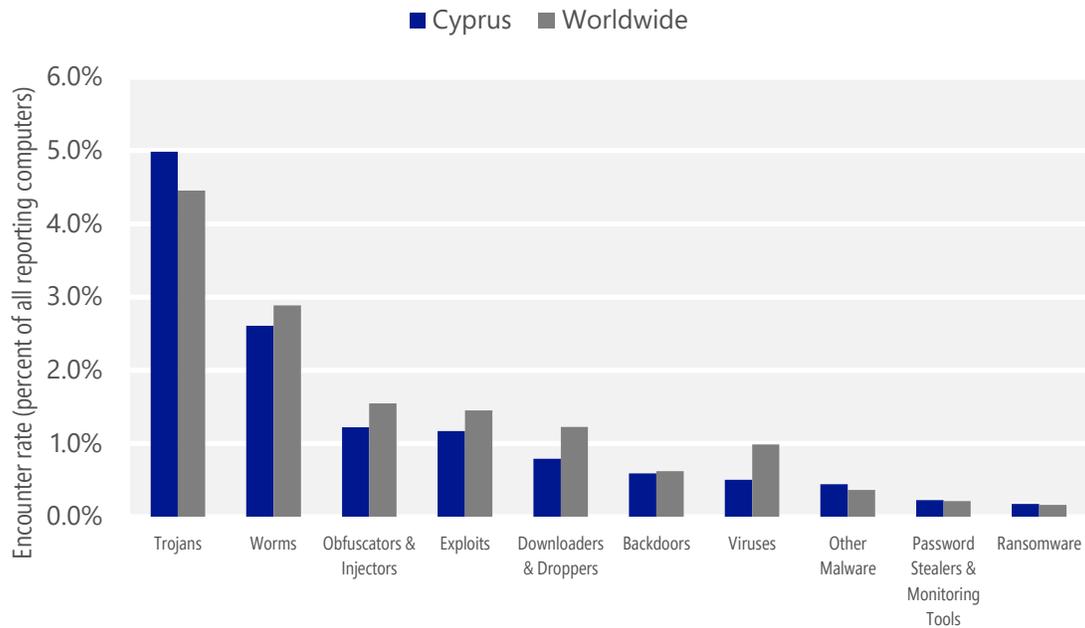
Malware encounter and infection rate trends in Cyprus and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in Cyprus and around the world, and for explanations of the methods and terms used here.

Malware categories

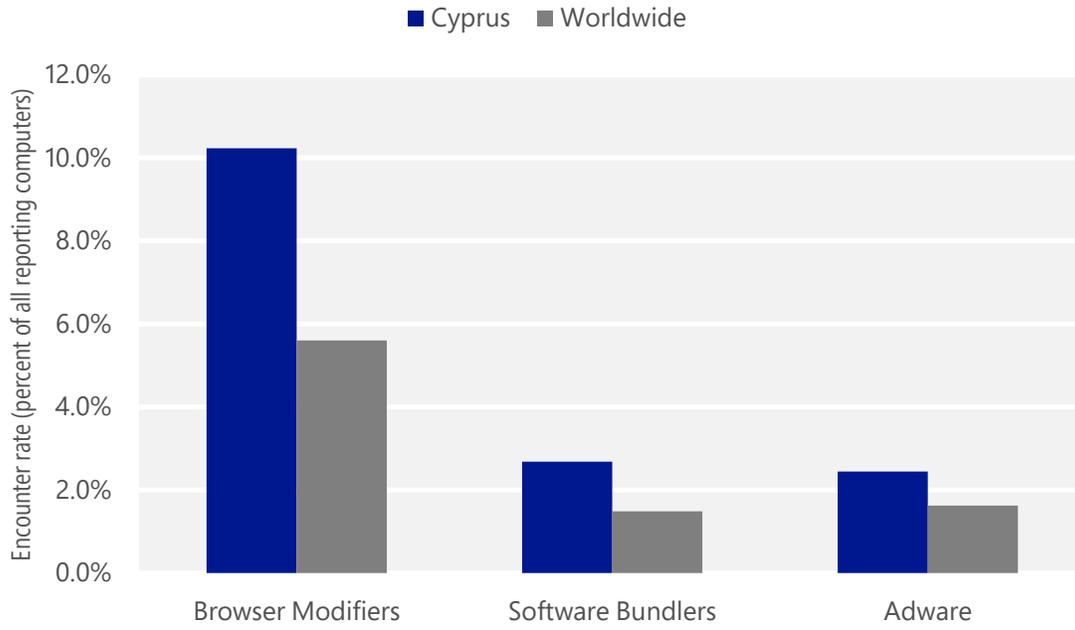
Malware encountered in Cyprus in 2Q15, by category



- The most common malware category in Cyprus in 2Q15 was Trojans. It was encountered by 5.0 percent of all computers there, up from 4.1 percent in 1Q15.
- The second most common malware category in Cyprus in 2Q15 was Worms. It was encountered by 2.6 percent of all computers there, down from 3.4 percent in 1Q15.
- The third most common malware category in Cyprus in 2Q15 was Obfuscators & Injectors, which was encountered by 1.2 percent of all computers there, down from 1.7 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Cyprus in 2Q15, by category



- The most common unwanted software category in Cyprus in 2Q15 was Browser Modifiers. It was encountered by 10.2 percent of all computers there, down from 15.9 percent in 1Q15.
- The second most common unwanted software category in Cyprus in 2Q15 was Software Bundlers. It was encountered by 2.7 percent of all computers there, down from 5.9 percent in 1Q15.
- The third most common unwanted software category in Cyprus in 2Q15 was Adware, which was encountered by 2.4 percent of all computers there, up from 1.0 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Cyprus in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Kilim	Trojans	1.5%
2	Win32/Gamarue	Worms	1.2%
3	Win32/Skeeyah	Trojans	0.8%
4	Win32/Obfuscator	Obfuscators & Injectors	0.8%
5	Win32/Peals	Trojans	0.6%
6	INF/Autorun	Obfuscators & Injectors	0.5%
7	JS/Axpergle	Exploits	0.5%
8	VBS/Jenxcus	Worms	0.3%
9	Win32/Sdbby	Exploits	0.3%
10	Win32/Conficker	Worms	0.2%

- The most common malware family encountered in Cyprus in 2Q15 was [Win32/Kilim](#), which was encountered by 1.5 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The second most common malware family encountered in Cyprus in 2Q15 was [Win32/Gamarue](#), which was encountered by 1.2 percent of reporting computers there. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The third most common malware family encountered in Cyprus in 2Q15 was [Win32/Skeeyah](#), which was encountered by 0.8 percent of reporting computers there. [Win32/Skeeyah](#) is a generic detection for various threats that display trojan characteristics.
- The fourth most common malware family encountered in Cyprus in 2Q15 was [Win32/Obfuscator](#), which was encountered by 0.8 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Cyprus in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	5.2%
2	Win32/KipodToolsCby	Browser Modifiers	4.8%
3	Win32/InstalleRex	Software Bundlers	2.5%
4	Win32/SaverExtension	Adware	1.9%
5	Win32/AlterbookSP	Browser Modifiers	0.7%

- The most common unwanted software family encountered in Cyprus in 2Q15 was [Win32/CouponRuc](#), which was encountered by 5.2 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in Cyprus in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 4.8 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common unwanted software family encountered in Cyprus in 2Q15 was [Win32/InstalleRex](#), which was encountered by 2.5 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Cyprus in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	4.5
2	Win32/Kilim	Trojans	1.7
3	Win32/CompromisedCert	Other Malware	1.4
4	Win32/Gamarue	Worms	1.2
5	Win32/Sality	Viruses	0.6
6	VBS/Jenxcus	Worms	0.5
7	Win32/Brontok	Worms	0.4
8	Win32/Ramnit	Trojans	0.3
9	MSIL/Bladabindi	Backdoors	0.2
10	Win32/Dyzap	Password Stealers & Monitoring Tools	0.2

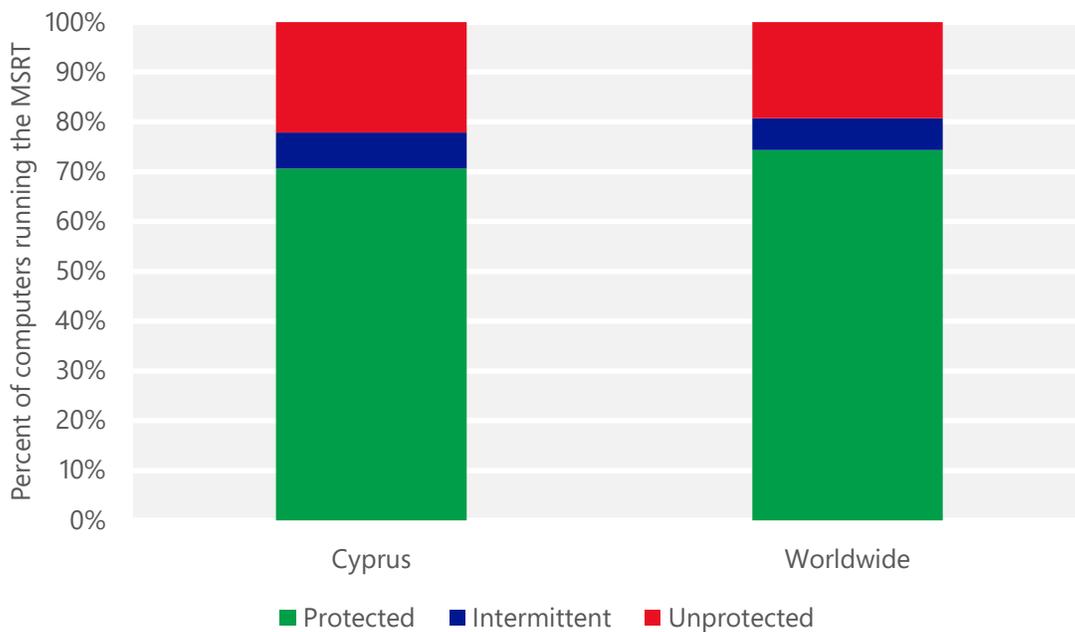
- The most common threat family infecting computers in Cyprus in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 4.5 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Cyprus in 2Q15 was [Win32/Kilim](#), which was detected and removed from 1.7 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The third most common threat family infecting computers in Cyprus in 2Q15 was [Win32/CompromisedCert](#), which was detected and removed from 1.4 of every 1,000 unique computers scanned by the MSRT. [Win32/CompromisedCert](#) is a detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.
- The fourth most common threat family infecting computers in Cyprus in 2Q15 was [Win32/Gamarue](#), which was detected and removed from 1.2 of every 1,000 unique computers scanned by the MSRT. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Cyprus and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Cyprus

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.67 (0.28)	3.35 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	13.10 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	32.74 (16.7)	

Czech Republic

The statistics presented here are generated by Microsoft security programs and services running on computers in the Czech Republic in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for the Czech Republic

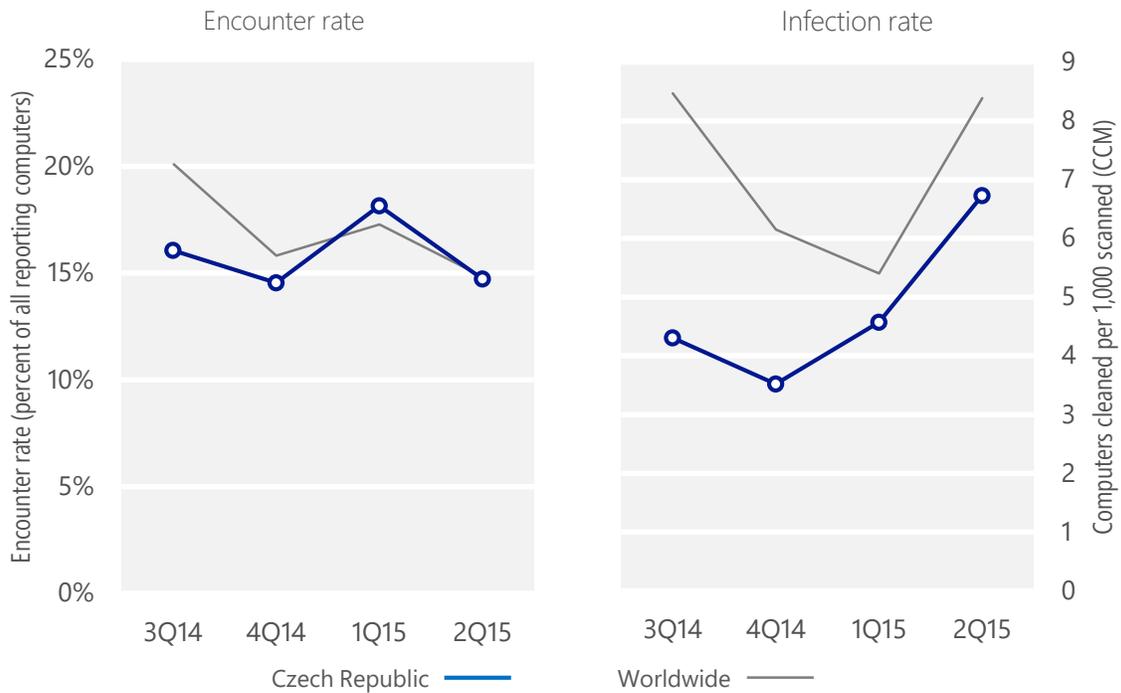
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Czech Republic	16.1%	14.5%	18.1%	14.7%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Czech Republic	4.3	3.5	4.6	6.7
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcoute, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 14.7% of computers in the Czech Republic encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 6.7 of every 1,000 unique computers scanned in the Czech Republic in 2Q15 (a CCM score of 6.7, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for the Czech Republic over the last four quarters, compared to the world as a whole.

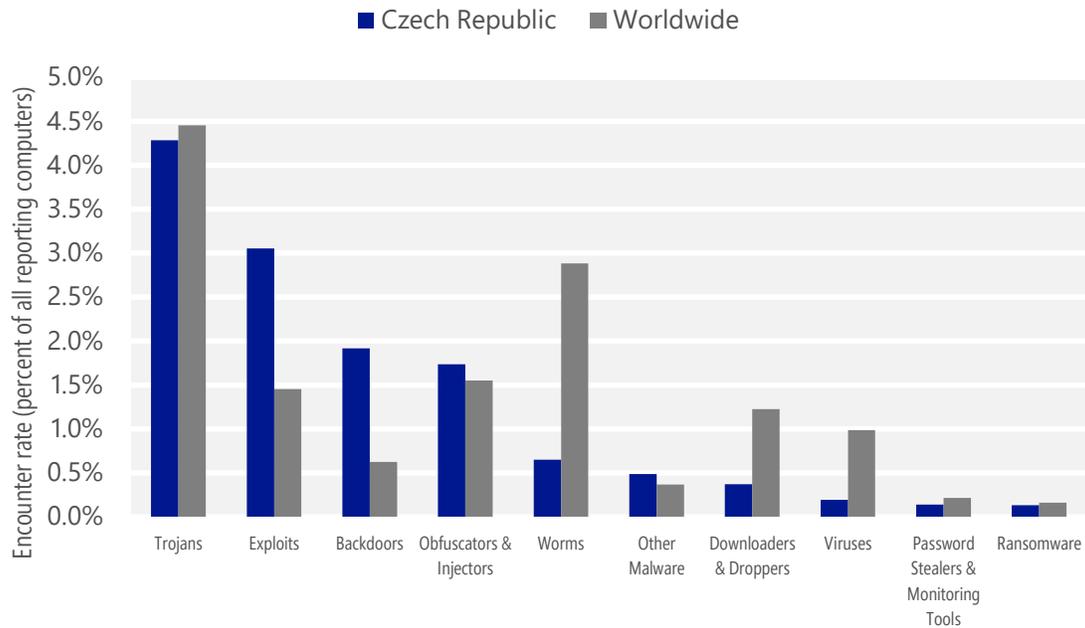
Malware encounter and infection rate trends in the Czech Republic and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in the Czech Republic and around the world, and for explanations of the methods and terms used here.

Malware categories

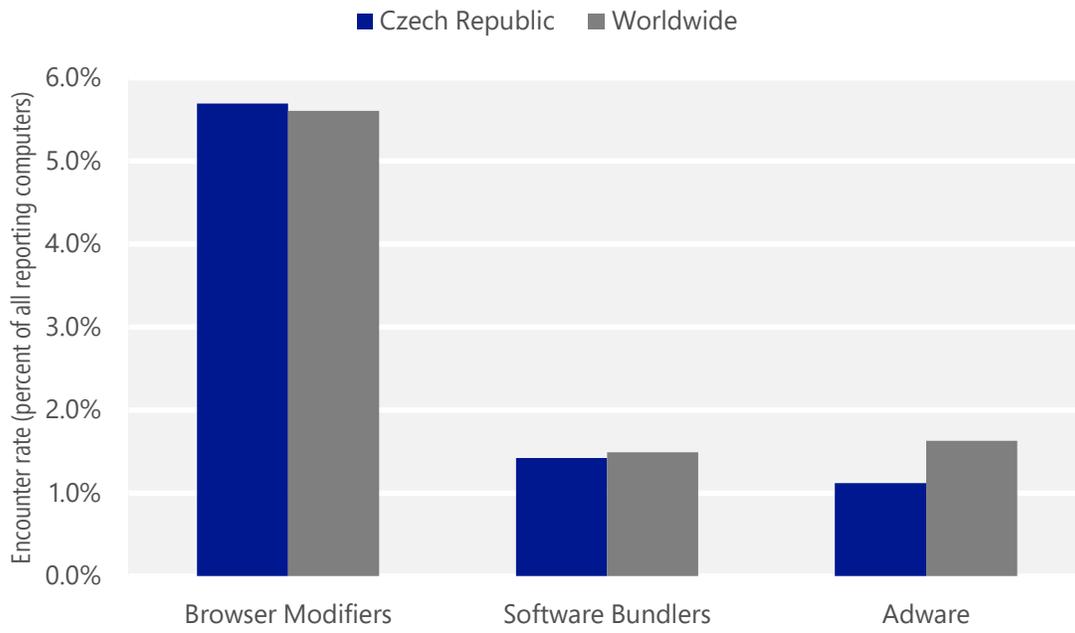
Malware encountered in the Czech Republic in 2Q15, by category



- The most common malware category in the Czech Republic in 2Q15 was Trojans. It was encountered by 4.3 percent of all computers there, up from 4.2 percent in 1Q15.
- The second most common malware category in the Czech Republic in 2Q15 was Exploits. It was encountered by 3.1 percent of all computers there, down from 4.1 percent in 1Q15.
- The third most common malware category in the Czech Republic in 2Q15 was Backdoors, which was encountered by 1.9 percent of all computers there, down from 2.1 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in the Czech Republic in 2Q15, by category



- The most common unwanted software category in the Czech Republic in 2Q15 was Browser Modifiers. It was encountered by 5.7 percent of all computers there, down from 6.7 percent in 1Q15.
- The second most common unwanted software category in the Czech Republic in 2Q15 was Software Bundlers. It was encountered by 1.4 percent of all computers there, down from 2.9 percent in 1Q15.
- The third most common unwanted software category in the Czech Republic in 2Q15 was Adware, which was encountered by 1.1 percent of all computers there, up from 0.5 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in the Czech Republic in 2Q15

	Family	Most significant category	% of reporting computers
1	JS/Axpergle	Exploits	2.1%
2	MSIL/Bladabindi	Backdoors	1.7%
3	Win32/Obfuscator	Obfuscators & Injectors	1.6%
4	JS/Neclu	Exploits	0.9%
5	Win32/Peals	Trojans	0.7%
6	Win32/Kilim	Trojans	0.7%
7	Win32/Skeeyah	Trojans	0.6%
8	Win32/Dynamer	Trojans	0.3%
9	Win32/Anaki	Trojans	0.3%
10	VBS/Jenxcus	Worms	0.3%

- The most common malware family encountered in the Czech Republic in 2Q15 was [JS/Axpergle](#), which was encountered by 2.1 percent of reporting computers there. [JS/Axpergle](#) is a detection for the Angler exploit kit, which exploits vulnerabilities in recent versions of Internet Explorer, Silverlight, Adobe Flash Player, and Java to install malware.
- The second most common malware family encountered in the Czech Republic in 2Q15 was [MSIL/Bladabindi](#), which was encountered by 1.7 percent of reporting computers there. [MSIL/Bladabindi](#) is a family of backdoors created by a malicious hacker tool called NJ Rat. The can steal sensitive information, download other malware, and allow backdoor access to an infected computer.
- The third most common malware family encountered in the Czech Republic in 2Q15 was [Win32/Obfuscator](#), which was encountered by 1.6 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The fourth most common malware family encountered in the Czech Republic in 2Q15 was [JS/Neclu](#), which was encountered by 0.9 percent of reporting computers there. [JS/Neclu](#) is a detection for the Nuclear exploit kit, which attempts to exploit vulnerabilities in programs such as Java and Adobe Reader to install other malware.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in the Czech Republic in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	2.5%
2	Win32/KipodToolsCby	Browser Modifiers	1.8%
3	Win32/AlterbookSP	Browser Modifiers	1.4%
4	Win32/InstalleRex	Software Bundlers	1.4%
5	Win32/SaverExtension	Adware	0.8%

- The most common unwanted software family encountered in the Czech Republic in 2Q15 was [Win32/CouponRuc](#), which was encountered by 2.5 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in the Czech Republic in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 1.8 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common unwanted software family encountered in the Czech Republic in 2Q15 was [Win32/AlterbookSP](#), which was encountered by 1.4 percent of reporting computers there. [Win32/AlterbookSP](#) is a browser add-on that formerly displayed behaviors of unwanted software. Recent versions of the add-on no longer meet Microsoft detection criteria, and are no longer considered unwanted software.

Top threat families by infection rate

The most common malware families by infection rate in the Czech Republic in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	2.1
2	MSIL/Bladabindi	Backdoors	1.5
3	Win32/CompromisedCert	Other Malware	1.2
4	Win32/Kilim	Trojans	0.6
5	VBS/Jenxcus	Worms	0.6
6	Win32/Simda	Trojans	0.2
7	Win32/Sality	Viruses	0.1
8	Win32/Ramnit	Trojans	0.1
9	Win32/Brontok	Worms	0.1
10	Win32/Conficker	Worms	<0.1

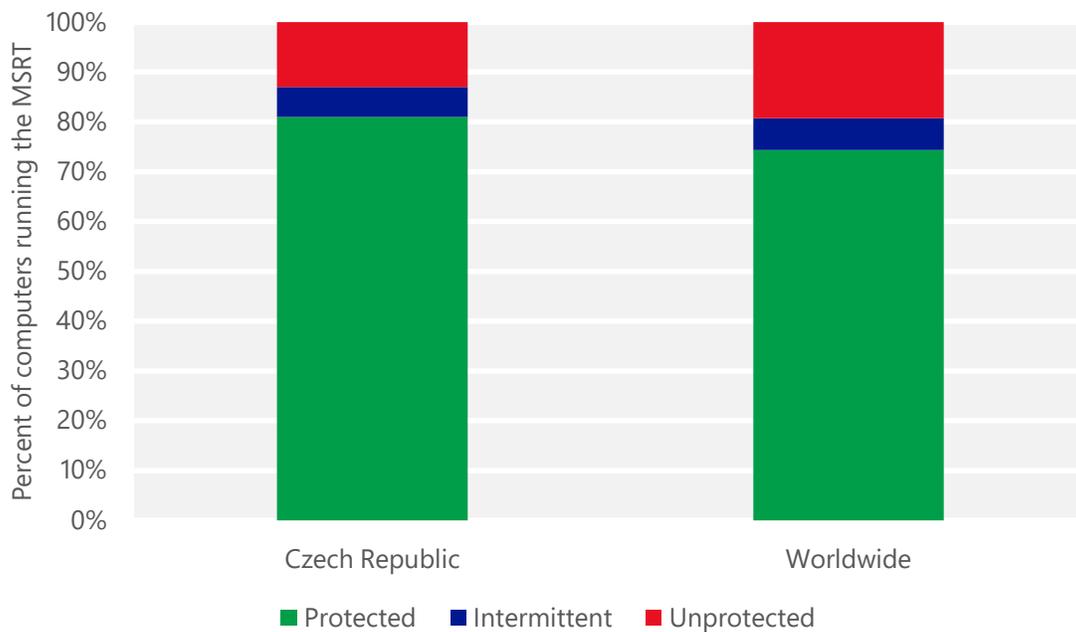
- The most common threat family infecting computers in the Czech Republic in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 2.1 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in the Czech Republic in 2Q15 was [MSIL/Bladabindi](#), which was detected and removed from 1.5 of every 1,000 unique computers scanned by the MSRT. [MSIL/Bladabindi](#) is a family of backdoors created by a malicious hacker tool called NJ Rat. The can steal sensitive information, download other malware, and allow backdoor access to an infected computer.
- The third most common threat family infecting computers in the Czech Republic in 2Q15 was [Win32/CompromisedCert](#), which was detected and removed from 1.2 of every 1,000 unique computers scanned by the MSRT. [Win32/CompromisedCert](#) is a detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.
- The fourth most common threat family infecting computers in the Czech Republic in 2Q15 was [Win32/Kilim](#), which was detected and removed from 0.6 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in the Czech Republic and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for the Czech Republic

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.46 (0.28)	1.05 (0.24)
Phishing sites per 1,000 hosts (Worldwide)		3.09 (5.0)
Malware hosting sites per 1,000 hosts (Worldwide)		8.61 (16.7)

Denmark

The statistics presented here are generated by Microsoft security programs and services running on computers in Denmark in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Denmark

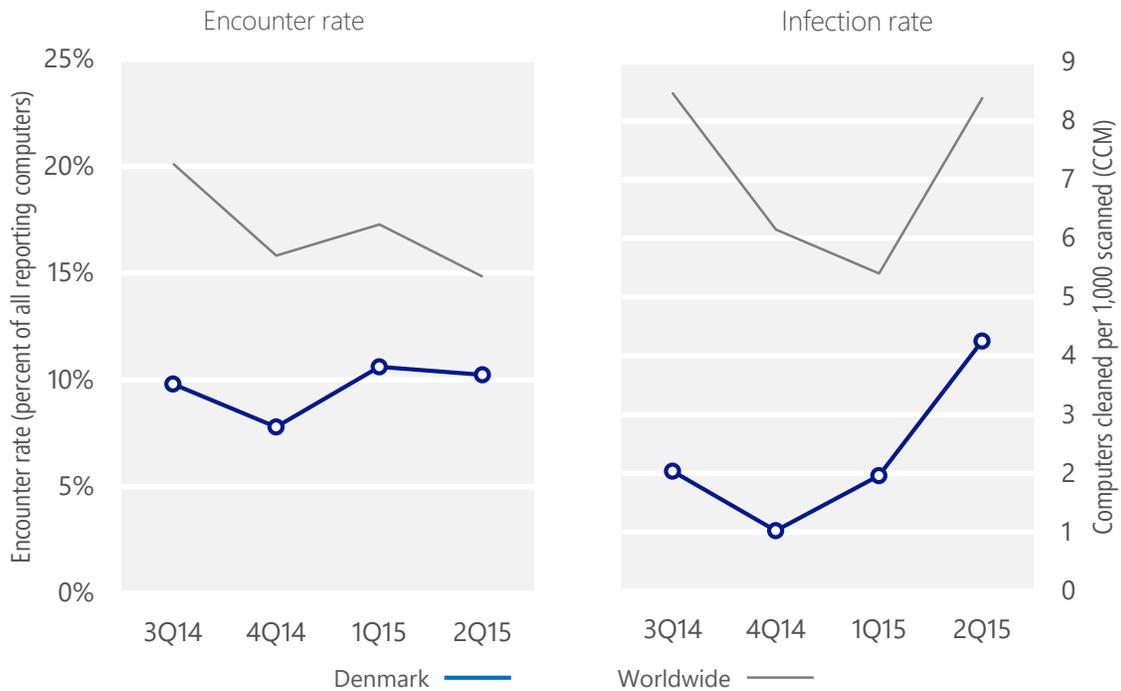
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Denmark	9.8%	7.8%	10.6%	10.2%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Denmark	2.0	1.0	2.0	4.2
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcoute, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 10.2% of computers in Denmark encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 4.2 of every 1,000 unique computers scanned in Denmark in 2Q15 (a CCM score of 4.2, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Denmark over the last four quarters, compared to the world as a whole.

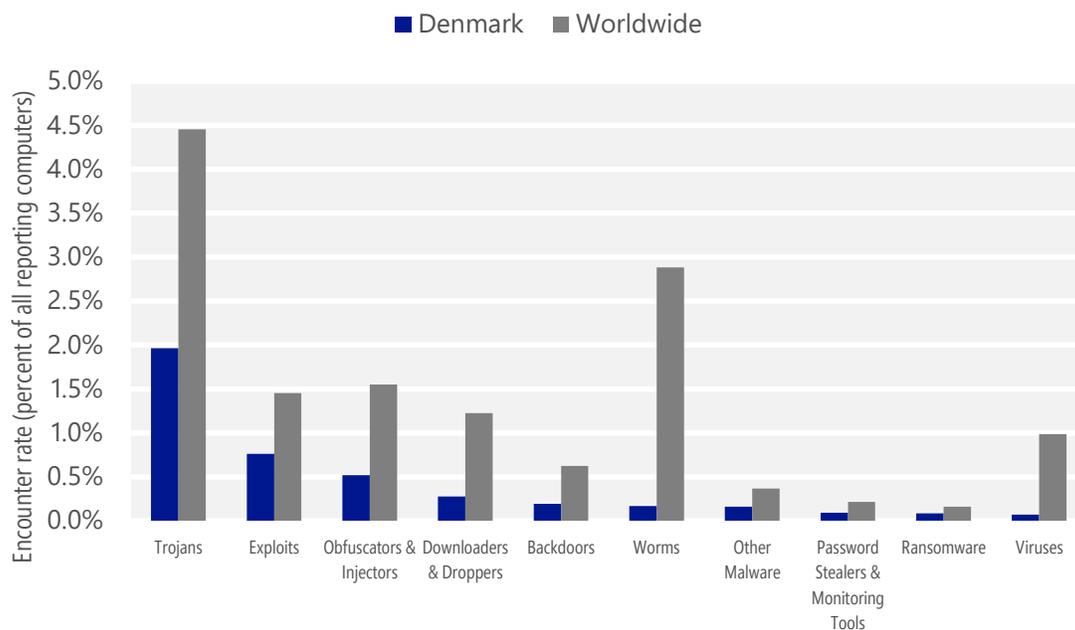
Malware encounter and infection rate trends in Denmark and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in Denmark and around the world, and for explanations of the methods and terms used here.

Malware categories

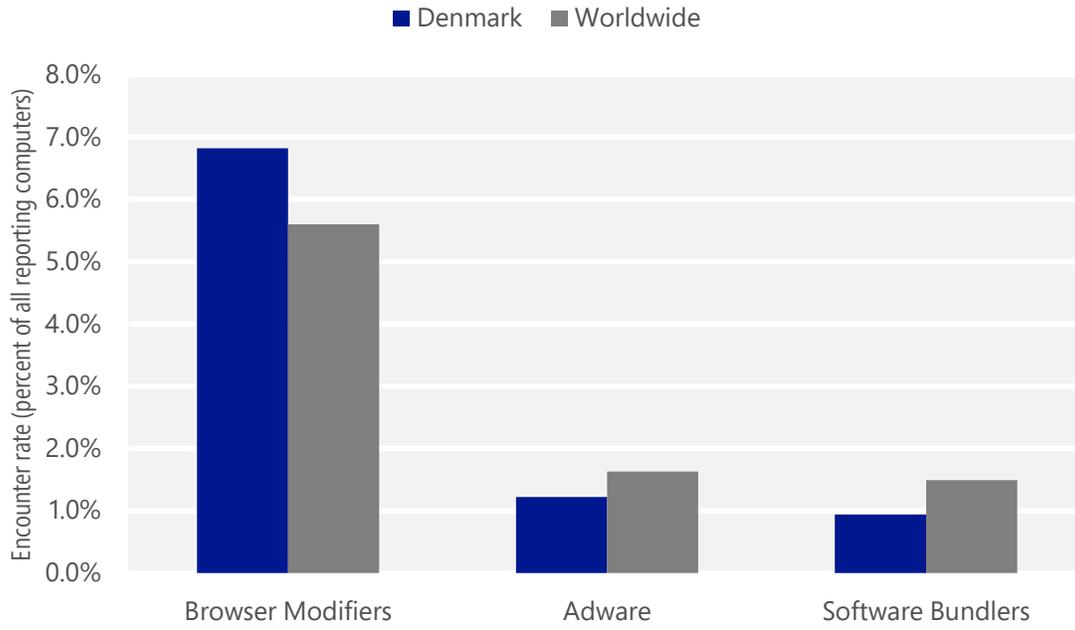
Malware encountered in Denmark in 2Q15, by category



- The most common malware category in Denmark in 2Q15 was Trojans. It was encountered by 2.0 percent of all computers there, up from 1.6 percent in 1Q15.
- The second most common malware category in Denmark in 2Q15 was Exploits. It was encountered by 0.8 percent of all computers there, down from 1.2 percent in 1Q15.
- The third most common malware category in Denmark in 2Q15 was Obfuscators & Injectors, which was encountered by 0.5 percent of all computers there, down from 0.7 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Denmark in 2Q15, by category



- The most common unwanted software category in Denmark in 2Q15 was Browser Modifiers. It was encountered by 6.8 percent of all computers there, up from 5.3 percent in 1Q15.
- The second most common unwanted software category in Denmark in 2Q15 was Adware. It was encountered by 1.2 percent of all computers there, down from 3.5 percent in 1Q15.
- The third most common unwanted software category in Denmark in 2Q15 was Software Bundlers, which was encountered by 0.9 percent of all computers there, up from 0.3 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Denmark in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Kilim	Trojans	0.6%
2	Win32/Skeeyah	Trojans	0.5%
3	JS/Axpergle	Exploits	0.5%
4	Win32/Obfuscator	Obfuscators & Injectors	0.4%
5	Win32/Peals	Trojans	0.2%
6	JS/Faceliker	Trojans	0.1%
7	Win32/Dynamer	Trojans	0.1%
8	JS/Neclu	Exploits	0.1%
9	Win32/Sdbby	Exploits	0.1%
10	Win32/Malagent	Trojans	0.1%

- The most common malware family encountered in Denmark in 2Q15 was [Win32/Kilim](#), which was encountered by 0.6 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The second most common malware family encountered in Denmark in 2Q15 was [Win32/Skeeyah](#), which was encountered by 0.5 percent of reporting computers there. [Win32/Skeeyah](#) is a generic detection for various threats that display trojan characteristics.
- The third most common malware family encountered in Denmark in 2Q15 was [JS/Axpergle](#), which was encountered by 0.5 percent of reporting computers there. [JS/Axpergle](#) is a detection for the Angler exploit kit, which exploits vulnerabilities in recent versions of Internet Explorer, Silverlight, Adobe Flash Player, and Java to install malware.
- The fourth most common malware family encountered in Denmark in 2Q15 was [Win32/Obfuscator](#), which was encountered by 0.4 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Denmark in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/AlterbookSP	Browser Modifiers	2.5%
2	Win32/CouponRuc	Browser Modifiers	2.5%
3	Win32/KipodToolsCby	Browser Modifiers	1.8%
4	Win32/InstalleRex	Software Bundlers	0.9%
5	Win32/SaverExtension	Adware	0.9%

- The most common unwanted software family encountered in Denmark in 2Q15 was [Win32/AlterbookSP](#), which was encountered by 2.5 percent of reporting computers there. [Win32/AlterbookSP](#) is a browser add-on that formerly displayed behaviors of unwanted software. Recent versions of the add-on no longer meet Microsoft detection criteria, and are no longer considered unwanted software.
- The second most common unwanted software family encountered in Denmark in 2Q15 was [Win32/CouponRuc](#), which was encountered by 2.5 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The third most common unwanted software family encountered in Denmark in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 1.8 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.

Top threat families by infection rate

The most common malware families by infection rate in Denmark in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/CompromisedCert	Other Malware	1.9
2	Win32/Kilim	Trojans	0.9
3	Win32/leEnablerCby	Browser Modifiers	0.9
4	MSIL/Bladabindi	Backdoors	0.1
5	Win32/Simda	Trojans	0.1
6	Win32/Alureon	Trojans	0.1
7	Win32/Nitol	Other Malware	<0.1
8	Win32/Zbot	Password Stealers & Monitoring Tools	<0.1
9	VBS/Jenxcus	Worms	<0.1
10	Win32/Emotet	Trojans	<0.1

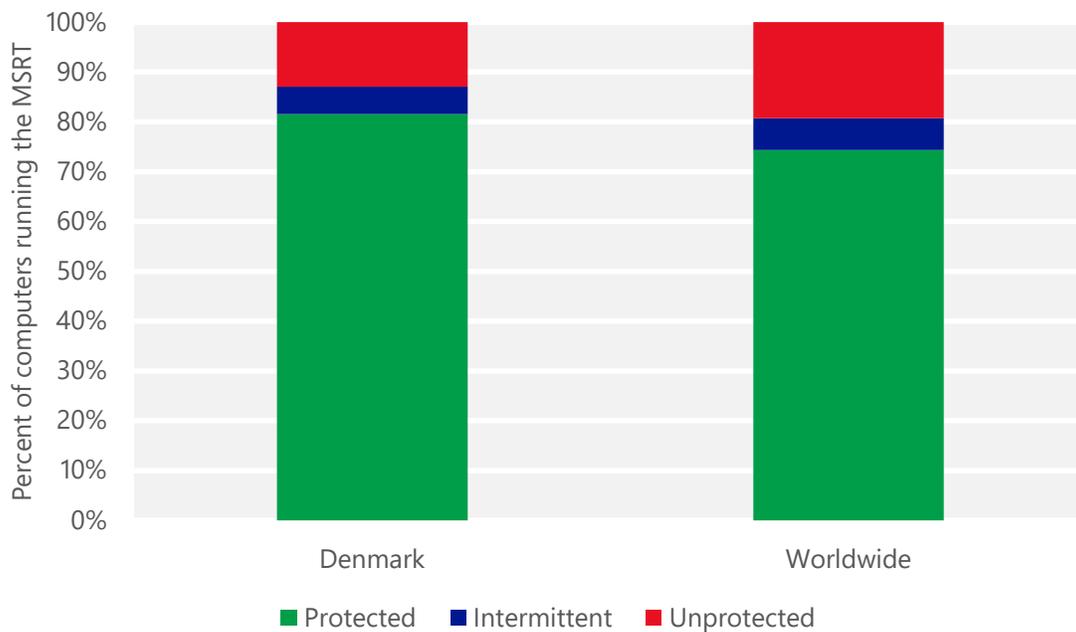
- The most common threat family infecting computers in Denmark in 2Q15 was [Win32/CompromisedCert](#), which was detected and removed from 1.9 of every 1,000 unique computers scanned by the MSRT. [Win32/CompromisedCert](#) is a detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.
- The second most common threat family infecting computers in Denmark in 2Q15 was [Win32/Kilim](#), which was detected and removed from 0.9 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The third most common threat family infecting computers in Denmark in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 0.9 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The fourth most common threat family infecting computers in Denmark in 2Q15 was [MSIL/Bladabindi](#), which was detected and removed from 0.1 of every 1,000 unique computers scanned by the MSRT. [MSIL/Bladabindi](#) is a family of backdoors created by a malicious hacker tool called NJ Rat. The can steal sensitive information, download other malware, and allow backdoor access to an infected computer.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Denmark and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Denmark

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.17 (0.28)	0.11 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	4.97 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	15.57 (16.7)	

Dominican Republic

The statistics presented here are generated by Microsoft security programs and services running on computers in the Dominican Republic in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for the Dominican Republic

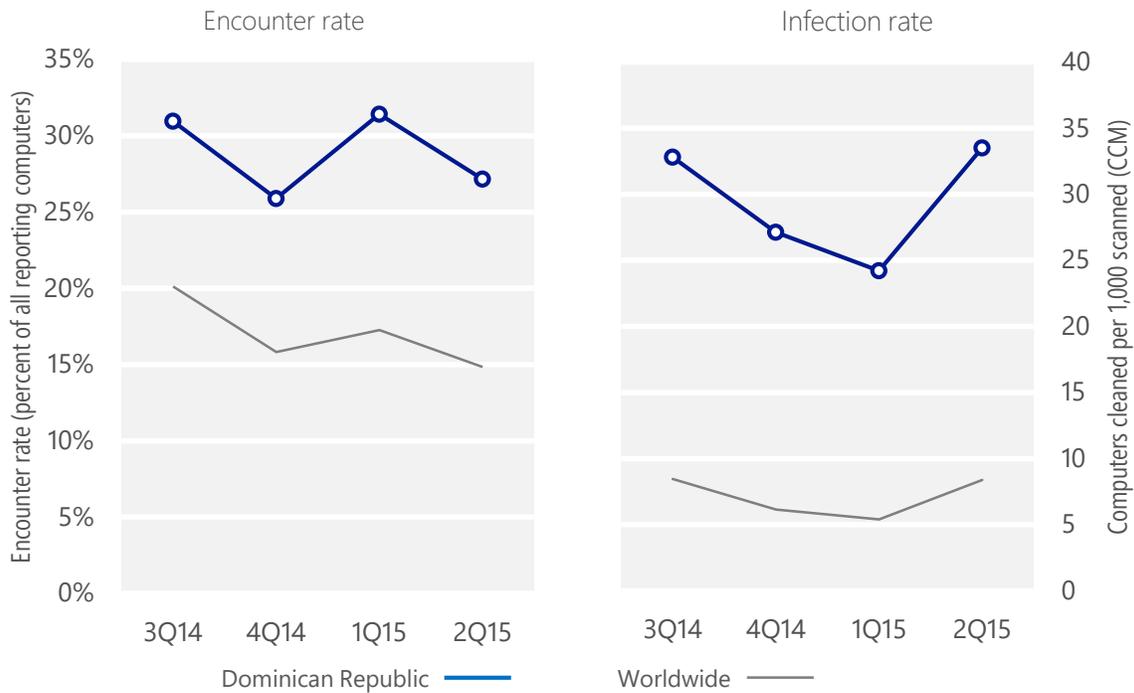
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Dominican Republic	31.0%	25.9%	31.4%	27.2%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Dominican Republic	32.8	27.1	24.2	33.5
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcoute, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 27.2% of computers in the Dominican Republic encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 33.5 of every 1,000 unique computers scanned in the Dominican Republic in 2Q15 (a CCM score of 33.5, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for the Dominican Republic over the last four quarters, compared to the world as a whole.

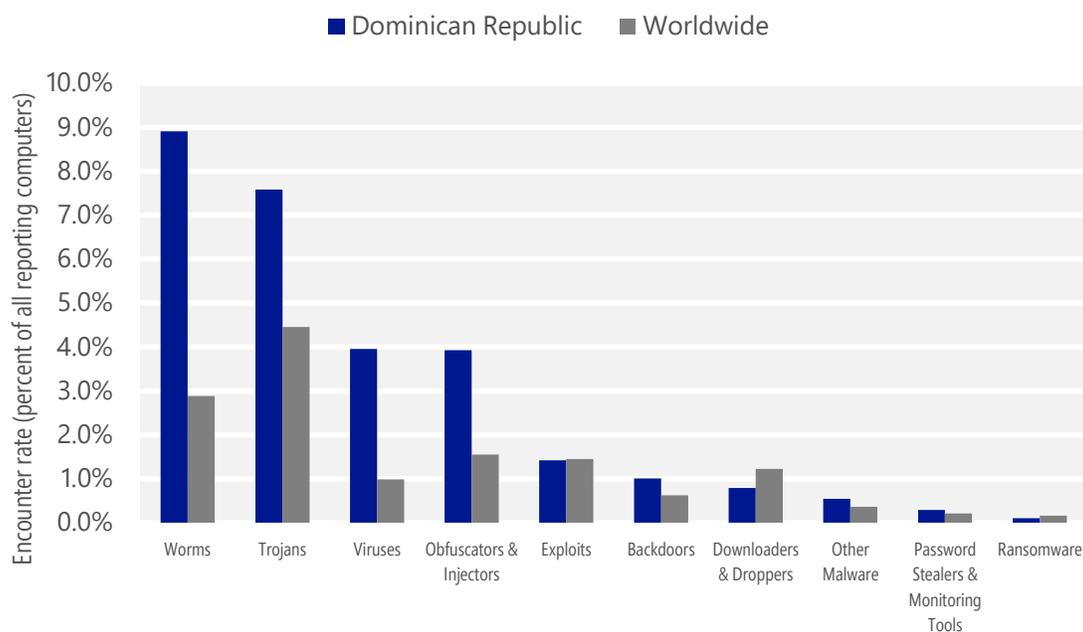
Malware encounter and infection rate trends in the Dominican Republic and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in the Dominican Republic and around the world, and for explanations of the methods and terms used here.

Malware categories

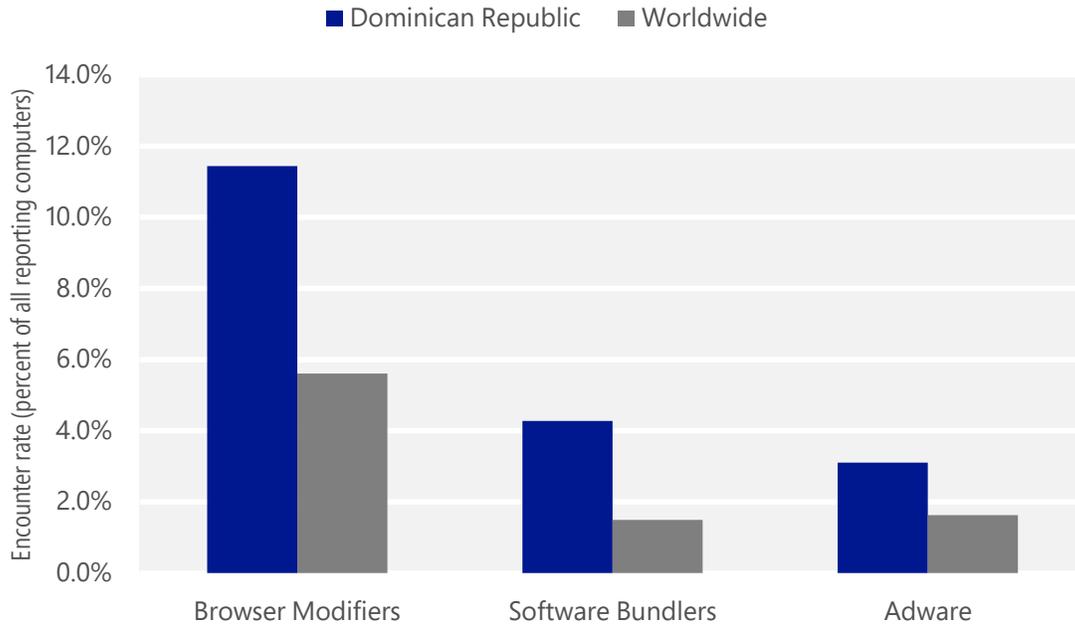
Malware encountered in the Dominican Republic in 2Q15, by category



- The most common malware category in the Dominican Republic in 2Q15 was Worms. It was encountered by 8.9 percent of all computers there, down from 9.2 percent in 1Q15.
- The second most common malware category in the Dominican Republic in 2Q15 was Trojans. It was encountered by 7.6 percent of all computers there, up from 5.4 percent in 1Q15.
- The third most common malware category in the Dominican Republic in 2Q15 was Viruses, which was encountered by 4.0 percent of all computers there, down from 4.8 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in the Dominican Republic in 2Q15, by category



- The most common unwanted software category in the Dominican Republic in 2Q15 was Browser Modifiers. It was encountered by 11.4 percent of all computers there, down from 16.9 percent in 1Q15.
- The second most common unwanted software category in the Dominican Republic in 2Q15 was Software Bundlers. It was encountered by 4.3 percent of all computers there, down from 7.2 percent in 1Q15.
- The third most common unwanted software category in the Dominican Republic in 2Q15 was Adware, which was encountered by 3.1 percent of all computers there, up from 1.1 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in the Dominican Republic in 2Q15

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	3.6%
2	Win32/Sality	Viruses	3.1%
3	INF/Autorun	Obfuscators & Injectors	3.0%
4	Win32/Gamarue	Worms	2.8%
5	Win32/Kilim	Trojans	1.7%
6	Win32/Obfuscator	Obfuscators & Injectors	1.1%
7	Win32/Brontok	Worms	1.1%
8	Win32/Skeeyah	Trojans	0.9%
9	Win32/Dynamer	Trojans	0.7%
10	Win32/Nuqel	Worms	0.7%

- The most common malware family encountered in the Dominican Republic in 2Q15 was [VBS/Jenxcus](#), which was encountered by 3.6 percent of reporting computers there. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common malware family encountered in the Dominican Republic in 2Q15 was [Win32/Sality](#), which was encountered by 3.1 percent of reporting computers there. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The third most common malware family encountered in the Dominican Republic in 2Q15 was [INF/Autorun](#), which was encountered by 3.0 percent of reporting computers there. [INF/Autorun](#) is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The fourth most common malware family encountered in the Dominican Republic in 2Q15 was [Win32/Gamarue](#), which was encountered by 2.8 percent of reporting computers there. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in the Dominican Republic in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	6.4%
2	Win32/KipodToolsCby	Browser Modifiers	4.8%
3	Win32/InstalleRex	Software Bundlers	4.1%
4	Win32/SaverExtension	Adware	2.3%
5	Win32/AlterbookSP	Browser Modifiers	0.5%

- The most common unwanted software family encountered in the Dominican Republic in 2Q15 was [Win32/CouponRuc](#), which was encountered by 6.4 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in the Dominican Republic in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 4.8 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common unwanted software family encountered in the Dominican Republic in 2Q15 was [Win32/InstalleRex](#), which was encountered by 4.1 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in the Dominican Republic in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	9.3
2	Win32/Sality	Viruses	9.1
3	VBS/Jenxcus	Worms	6.5
4	Win32/Gamarue	Worms	2.3
5	Win32/Kilim	Trojans	2.3
6	Win32/Brontok	Worms	1.7
7	Win32/Helompy	Worms	1.1
8	Win32/Nuqel	Worms	0.6
9	Win32/Chir	Viruses	0.6
10	Win32/Pramro	Trojans	0.6

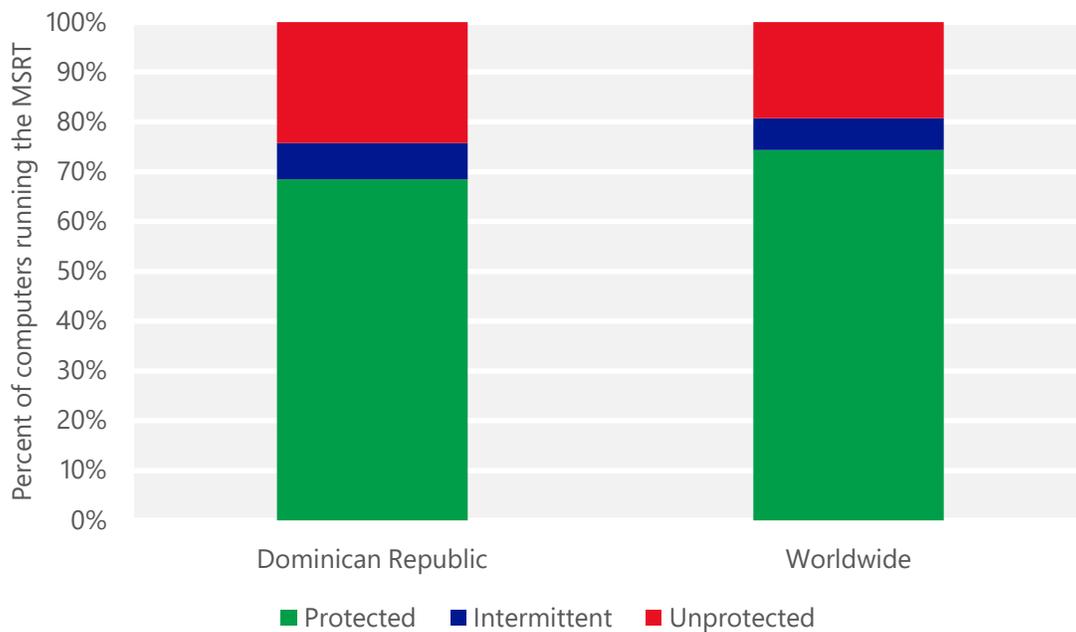
- The most common threat family infecting computers in the Dominican Republic in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 9.3 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in the Dominican Republic in 2Q15 was [Win32/Sality](#), which was detected and removed from 9.1 of every 1,000 unique computers scanned by the MSRT. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The third most common threat family infecting computers in the Dominican Republic in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 6.5 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The fourth most common threat family infecting computers in the Dominican Republic in 2Q15 was [Win32/Gamarue](#), which was detected and removed from 2.3 of every 1,000 unique computers scanned by the MSRT. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in the Dominican Republic and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for the Dominican Republic

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.50 (0.28)	0.07 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	6.77 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	11.19 (16.7)	

Ecuador

The statistics presented here are generated by Microsoft security programs and services running on computers in Ecuador in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Ecuador

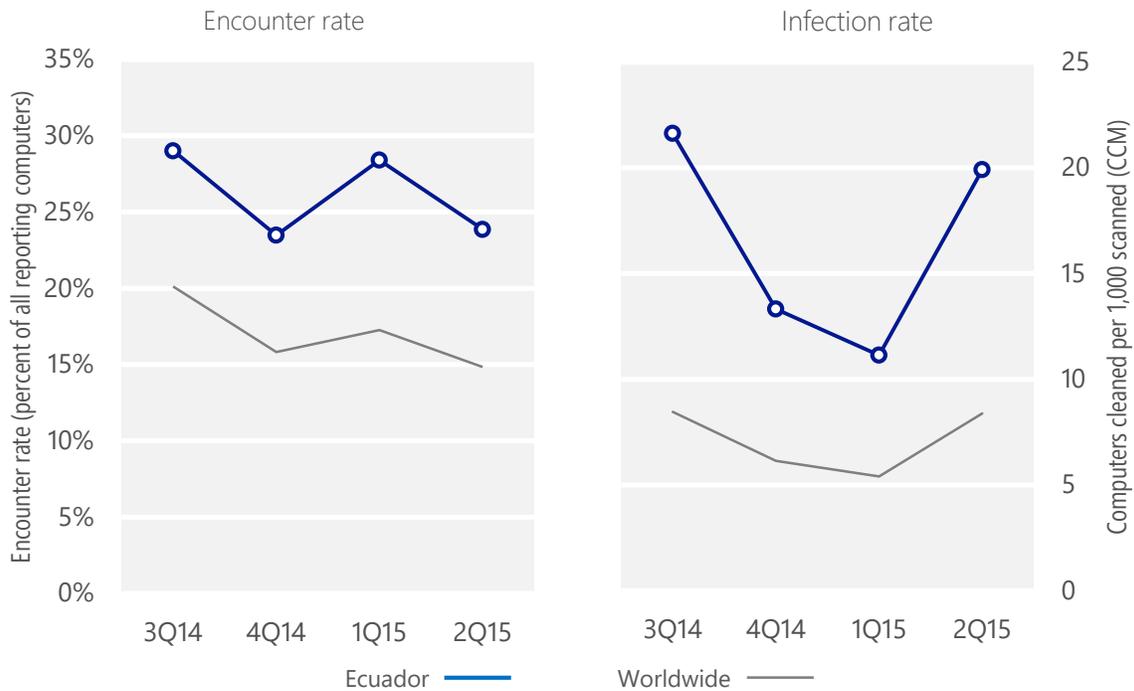
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Ecuador	29.0%	23.5%	28.4%	23.9%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Ecuador	21.6	13.3	11.1	19.9
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcout, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 23.9% of computers in Ecuador encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 19.9 of every 1,000 unique computers scanned in Ecuador in 2Q15 (a CCM score of 19.9, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Ecuador over the last four quarters, compared to the world as a whole.

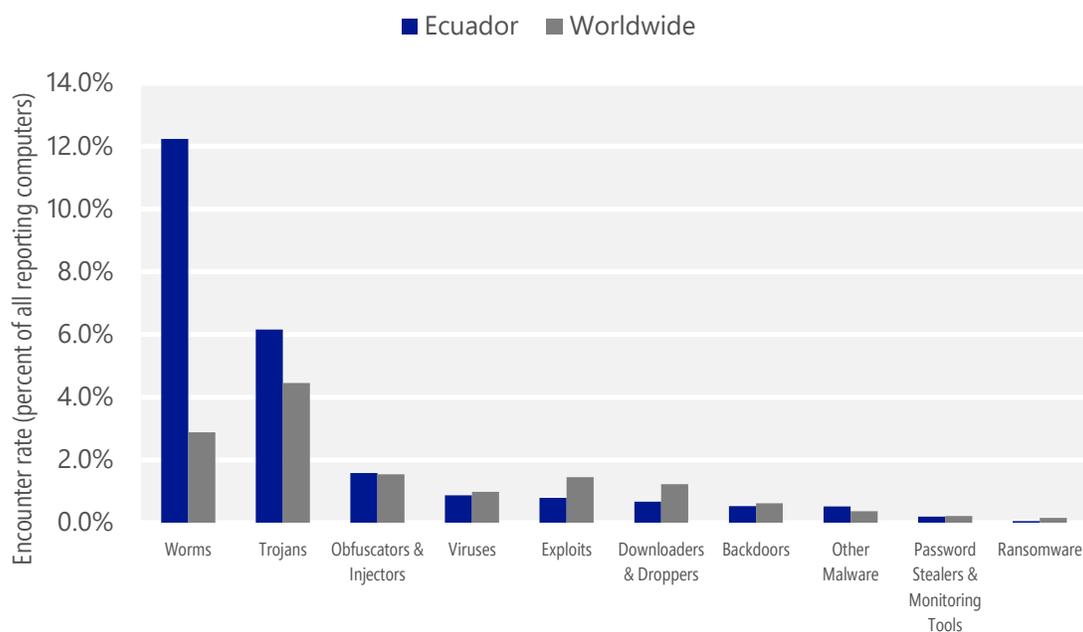
Malware encounter and infection rate trends in Ecuador and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in Ecuador and around the world, and for explanations of the methods and terms used here.

Malware categories

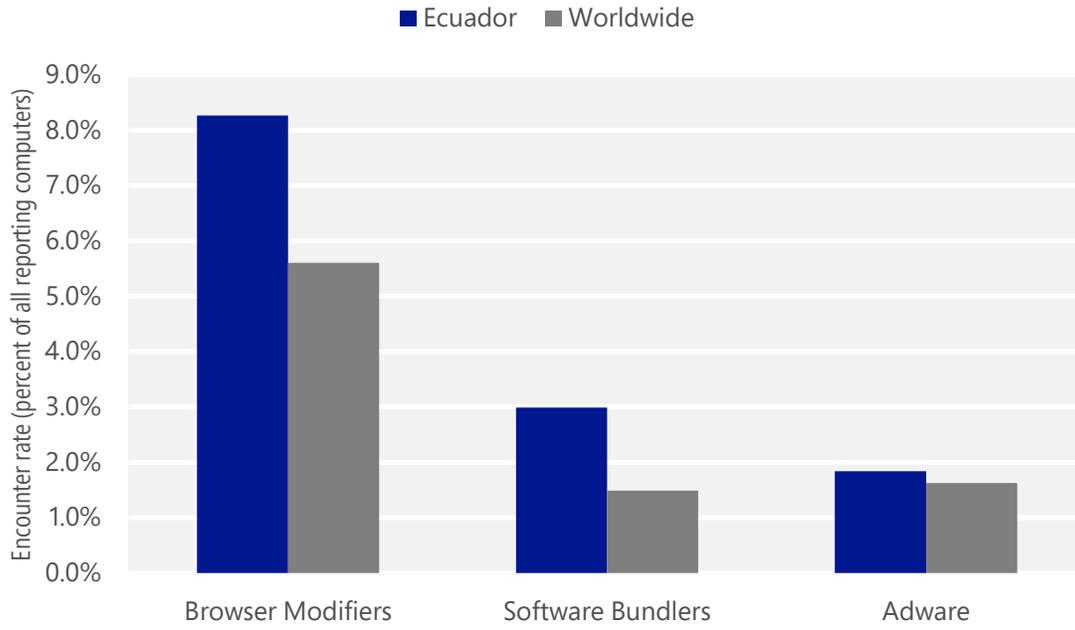
Malware encountered in Ecuador in 2Q15, by category



- The most common malware category in Ecuador in 2Q15 was Worms. It was encountered by 12.2 percent of all computers there, down from 12.9 percent in 1Q15.
- The second most common malware category in Ecuador in 2Q15 was Trojans. It was encountered by 6.2 percent of all computers there, up from 4.9 percent in 1Q15.
- The third most common malware category in Ecuador in 2Q15 was Obfuscators & Injectors, which was encountered by 1.6 percent of all computers there, down from 2.0 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Ecuador in 2Q15, by category



- The most common unwanted software category in Ecuador in 2Q15 was Browser Modifiers. It was encountered by 8.3 percent of all computers there, down from 13.3 percent in 1Q15.
- The second most common unwanted software category in Ecuador in 2Q15 was Software Bundlers. It was encountered by 3.0 percent of all computers there, down from 4.6 percent in 1Q15.
- The third most common unwanted software category in Ecuador in 2Q15 was Adware, which was encountered by 1.8 percent of all computers there, up from 0.8 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Ecuador in 2Q15

	Family	Most significant category	% of reporting computers
1	JS/Bondat	Worms	7.5%
2	Win32/Gamarue	Worms	3.9%
3	VBS/Jenxcus	Worms	2.5%
4	Win32/Kilim	Trojans	1.2%
5	Win32/Obfuscator	Obfuscators & Injectors	0.9%
6	Win32/Skeeyah	Trojans	0.7%
7	INF/Autorun	Obfuscators & Injectors	0.6%
8	Win32/Peals	Trojans	0.6%
9	Win32/Vobfus	Worms	0.5%
10	Win32/Ramnit	Trojans	0.4%

- The most common malware family encountered in Ecuador in 2Q15 was [JS/Bondat](#), which was encountered by 7.5 percent of reporting computers there. [JS/Bondat](#) is a family of threats that collects information about the computer, infects removable drives, and tries to stop the user from accessing files. It spreads by infecting removable drives, such as USB thumb drives and flash drives.
- The second most common malware family encountered in Ecuador in 2Q15 was [Win32/Gamarue](#), which was encountered by 3.9 percent of reporting computers there. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The third most common malware family encountered in Ecuador in 2Q15 was [VBS/Jenxcus](#), which was encountered by 2.5 percent of reporting computers there. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The fourth most common malware family encountered in Ecuador in 2Q15 was [Win32/Kilim](#), which was encountered by 1.2 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Ecuador in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	4.0%
2	Win32/KipodToolsCby	Browser Modifiers	3.4%
3	Win32/InstalleRex	Software Bundlers	2.9%
4	Win32/SaverExtension	Adware	1.3%
5	Win32/AlterbookSP	Browser Modifiers	0.8%

- The most common unwanted software family encountered in Ecuador in 2Q15 was [Win32/CouponRuc](#), which was encountered by 4.0 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in Ecuador in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 3.4 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common unwanted software family encountered in Ecuador in 2Q15 was [Win32/InstalleRex](#), which was encountered by 2.9 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Ecuador in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	8.9
2	VBS/Jenxcus	Worms	3.1
3	Win32/Gamarue	Worms	2.8
4	Win32/Kilim	Trojans	1.8
5	Win32/Sality	Viruses	0.8
6	Win32/CompromisedCert	Other Malware	0.7
7	Win32/Ramnit	Trojans	0.5
8	Win32/Vobfus	Worms	0.4
9	Win32/Dorkbot	Worms	0.3
10	Win32/Brontok	Worms	0.3

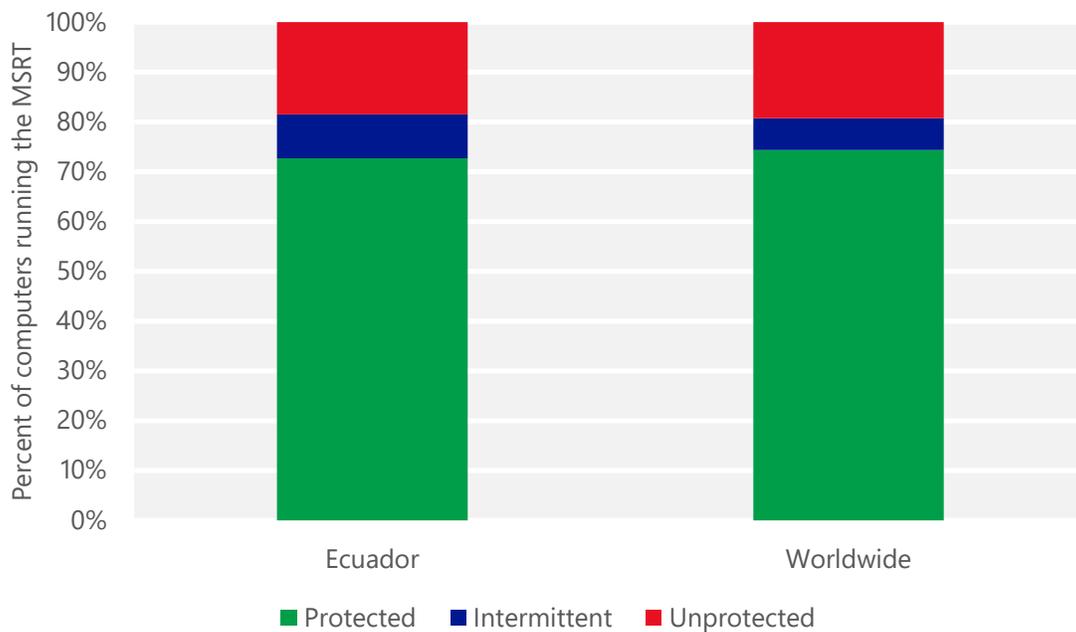
- The most common threat family infecting computers in Ecuador in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 8.9 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Ecuador in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 3.1 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The third most common threat family infecting computers in Ecuador in 2Q15 was [Win32/Gamarue](#), which was detected and removed from 2.8 of every 1,000 unique computers scanned by the MSRT. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The fourth most common threat family infecting computers in Ecuador in 2Q15 was [Win32/Kilim](#), which was detected and removed from 1.8 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Ecuador and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Ecuador

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.31 (0.28)	0.09 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	2.31 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	9.70 (16.7)	

Egypt

The statistics presented here are generated by Microsoft security programs and services running on computers in Egypt in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Egypt

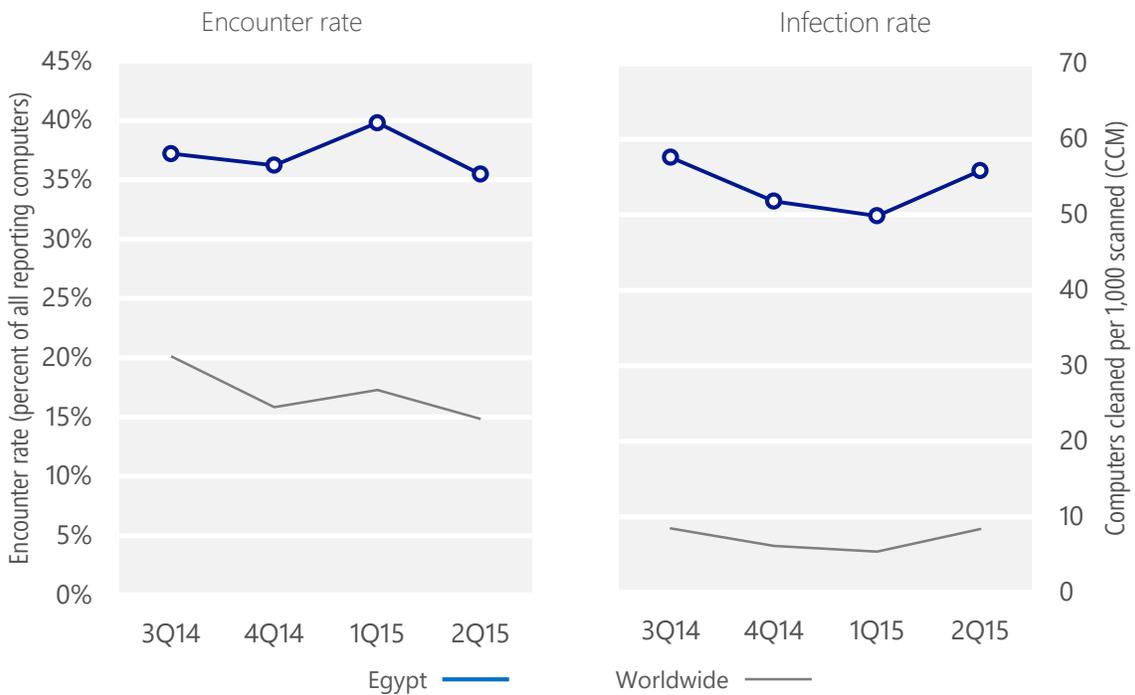
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Egypt	37.2%	36.2%	39.8%	35.5%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Egypt	57.6	51.8	49.8	55.8
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcout, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 35.5% of computers in Egypt encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 55.8 of every 1,000 unique computers scanned in Egypt in 2Q15 (a CCM score of 55.8, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Egypt over the last four quarters, compared to the world as a whole.

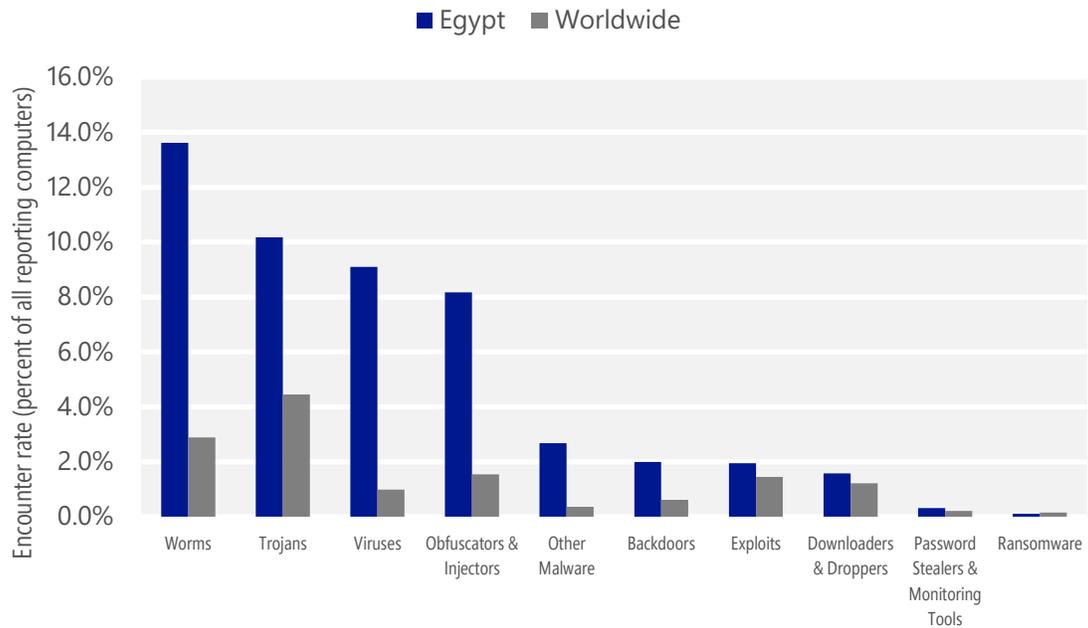
Malware encounter and infection rate trends in Egypt and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in Egypt and around the world, and for explanations of the methods and terms used here.

Malware categories

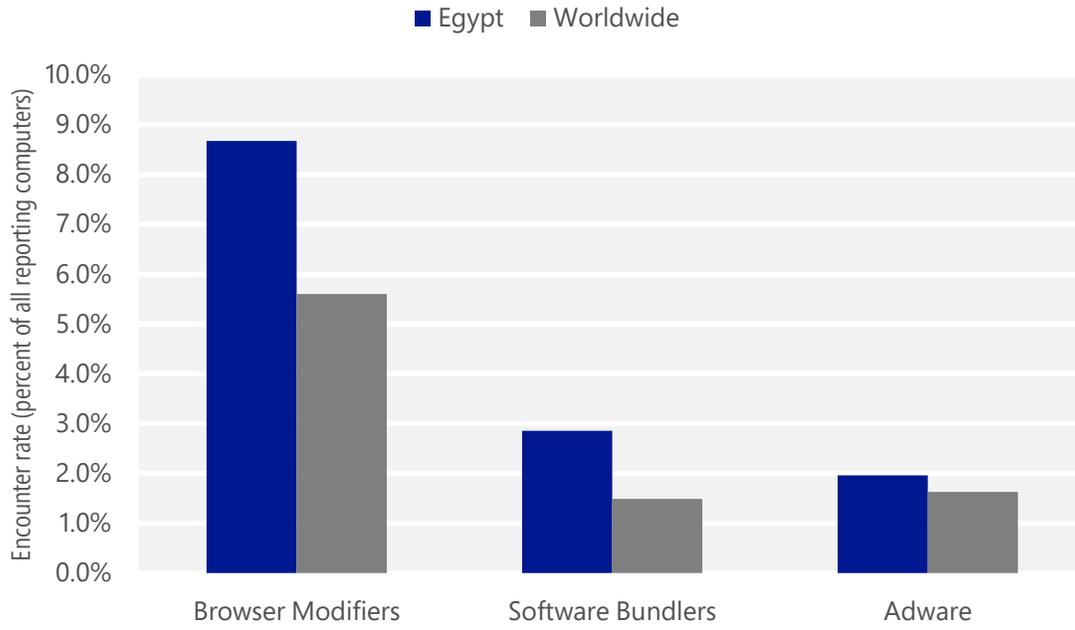
Malware encountered in Egypt in 2Q15, by category



- The most common malware category in Egypt in 2Q15 was Worms. It was encountered by 13.6 percent of all computers there, down from 15.4 percent in 1Q15.
- The second most common malware category in Egypt in 2Q15 was Trojans. It was encountered by 10.2 percent of all computers there, down from 10.2 percent in 1Q15.
- The third most common malware category in Egypt in 2Q15 was Viruses, which was encountered by 9.1 percent of all computers there, down from 9.5 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Egypt in 2Q15, by category



- The most common unwanted software category in Egypt in 2Q15 was Browser Modifiers. It was encountered by 8.7 percent of all computers there, down from 12.5 percent in 1Q15.
- The second most common unwanted software category in Egypt in 2Q15 was Software Bundlers. It was encountered by 2.9 percent of all computers there, down from 4.1 percent in 1Q15.
- The third most common unwanted software category in Egypt in 2Q15 was Adware, which was encountered by 2.0 percent of all computers there, up from 1.9 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Egypt in 2Q15

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	5.4%
2	JS/Bondat	Worms	5.3%
3	Win32/Obfuscator	Obfuscators & Injectors	4.8%
4	Win32/Sality	Viruses	4.6%
5	INF/Autorun	Obfuscators & Injectors	4.0%
6	Win32/Virut	Viruses	3.6%
7	Win32/Ramnit	Trojans	2.0%
8	Win32/Nitol	Other Malware	1.9%
9	Win32/Peals	Trojans	1.6%
10	Win32/Nuqel	Worms	1.4%

- The most common malware family encountered in Egypt in 2Q15 was [VBS/Jenxcus](#), which was encountered by 5.4 percent of reporting computers there. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common malware family encountered in Egypt in 2Q15 was [JS/Bondat](#), which was encountered by 5.3 percent of reporting computers there. [JS/Bondat](#) is a family of threats that collects information about the computer, infects removable drives, and tries to stop the user from accessing files. It spreads by infecting removable drives, such as USB thumb drives and flash drives.
- The third most common malware family encountered in Egypt in 2Q15 was [Win32/Obfuscator](#), which was encountered by 4.8 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The fourth most common malware family encountered in Egypt in 2Q15 was [Win32/Sality](#), which was encountered by 4.6 percent of reporting computers there. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Egypt in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/KipodToolsCby	Browser Modifiers	4.5%
2	Win32/CouponRuc	Browser Modifiers	3.9%
3	Win32/InstalleRex	Software Bundlers	2.7%
4	Win32/SaverExtension	Adware	1.2%
5	Win32/AlterbookSP	Browser Modifiers	0.4%

- The most common unwanted software family encountered in Egypt in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 4.5 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common unwanted software family encountered in Egypt in 2Q15 was [Win32/CouponRuc](#), which was encountered by 3.9 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The third most common unwanted software family encountered in Egypt in 2Q15 was [Win32/InstalleRex](#), which was encountered by 2.7 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Egypt in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/Sality	Viruses	18.5
2	VBS/Jenxcus	Worms	14.7
3	Win32/Virut	Viruses	6.4
4	Win32/Nitol	Other Malware	6.2
5	Win32/leEnablerCby	Browser Modifiers	5.4
6	Win32/Ramnit	Trojans	4.4
7	Win32/Nuqel	Worms	2.7
8	MSIL/Bladabindi	Backdoors	2.3
9	Win32/Kilim	Trojans	1.8
10	Win32/Gamarue	Worms	1.7

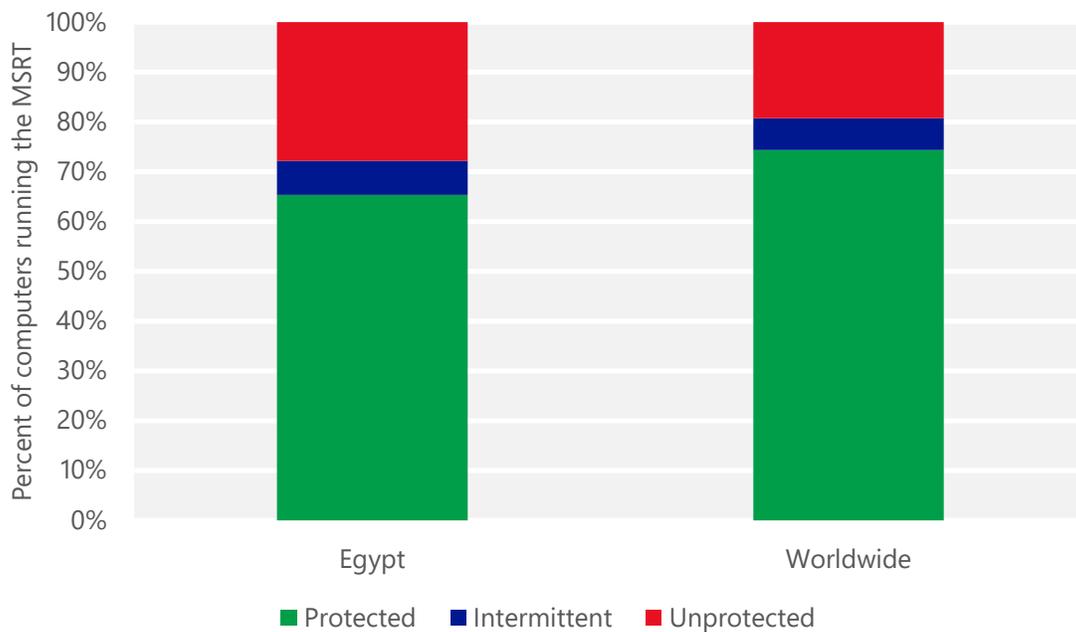
- The most common threat family infecting computers in Egypt in 2Q15 was [Win32/Sality](#), which was detected and removed from 18.5 of every 1,000 unique computers scanned by the MSRT. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The second most common threat family infecting computers in Egypt in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 14.7 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The third most common threat family infecting computers in Egypt in 2Q15 was [Win32/Virut](#), which was detected and removed from 6.4 of every 1,000 unique computers scanned by the MSRT. [Win32/Virut](#) is a family of file-infecting viruses that target and infect .exe and .scr files accessed on infected systems. Win32/Virut also opens a backdoor by connecting to an IRC server.
- The fourth most common threat family infecting computers in Egypt in 2Q15 was [Win32/Nitol](#), which was detected and removed from 6.2 of every 1,000 unique computers scanned by the MSRT. [Win32/Nitol](#) is a family of trojans that perform DDoS (distributed denial of service) attacks, allow backdoor access and control, download and run files, and perform a number of other malicious activities on the computer.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Egypt and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Egypt

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	1.05 (0.28)	1.39 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	2.07 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	6.94 (16.7)	

El Salvador

The statistics presented here are generated by Microsoft security programs and services running on computers in El Salvador in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for El Salvador

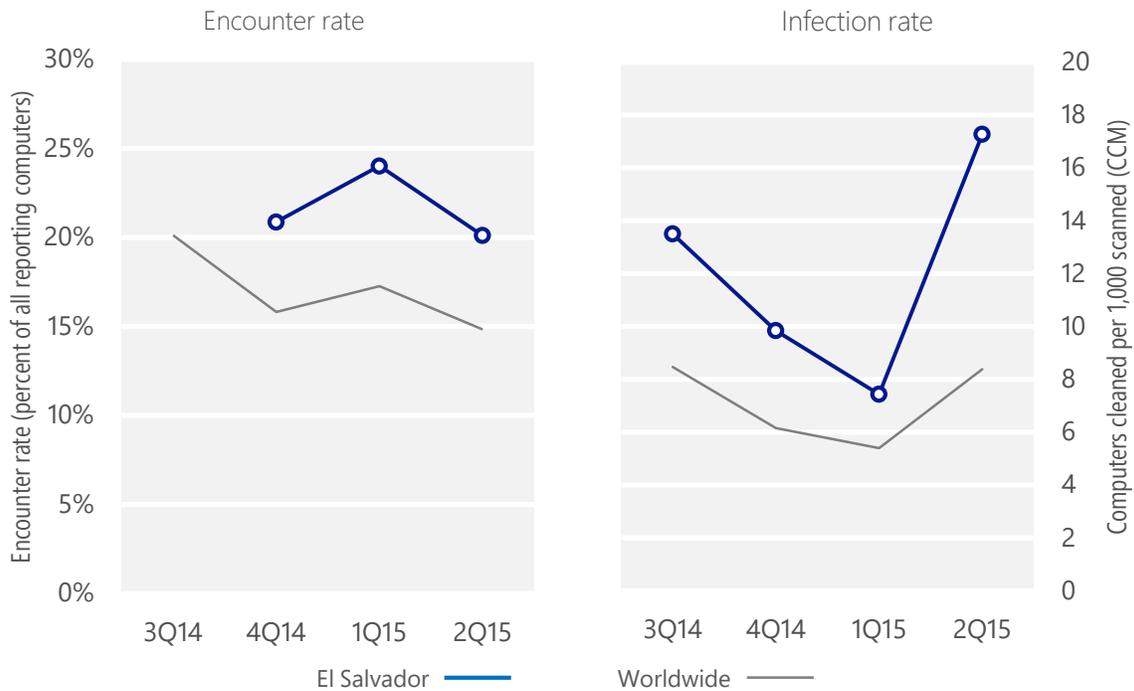
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, El Salvador	N/A	20.9%	24.0%	20.1%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, El Salvador	13.5	9.8	7.4	17.3
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcout, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 20.1% of computers in El Salvador encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 17.3 of every 1,000 unique computers scanned in El Salvador in 2Q15 (a CCM score of 17.3, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for El Salvador over the last four quarters, compared to the world as a whole.

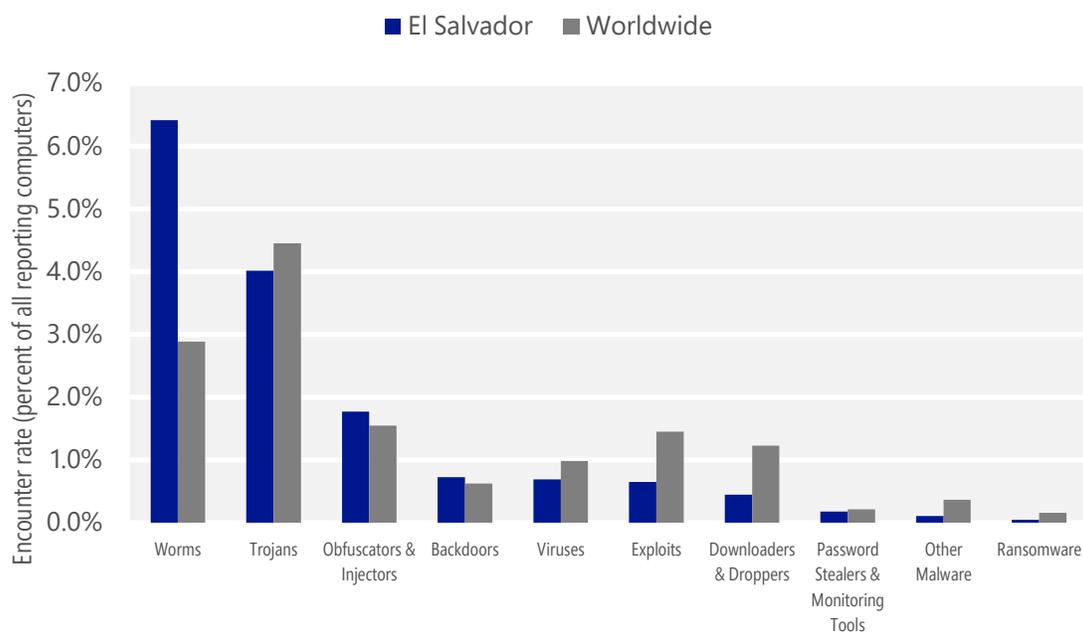
Malware encounter and infection rate trends in El Salvador and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in El Salvador and around the world, and for explanations of the methods and terms used here.

Malware categories

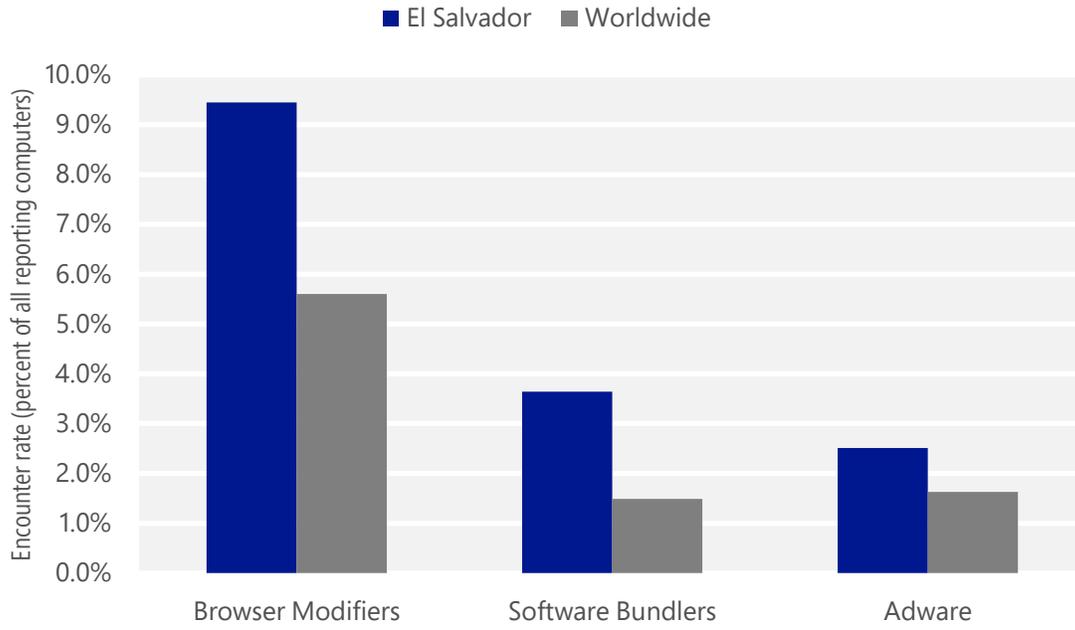
Malware encountered in El Salvador in 2Q15, by category



- The most common malware category in El Salvador in 2Q15 was Worms. It was encountered by 6.4 percent of all computers there, down from 6.5 percent in 1Q15.
- The second most common malware category in El Salvador in 2Q15 was Trojans. It was encountered by 4.0 percent of all computers there, up from 3.1 percent in 1Q15.
- The third most common malware category in El Salvador in 2Q15 was Obfuscators & Injectors, which was encountered by 1.8 percent of all computers there, down from 2.0 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in El Salvador in 2Q15, by category



- The most common unwanted software category in El Salvador in 2Q15 was Browser Modifiers. It was encountered by 9.4 percent of all computers there, down from 13.8 percent in 1Q15.
- The second most common unwanted software category in El Salvador in 2Q15 was Software Bundlers. It was encountered by 3.6 percent of all computers there, down from 5.9 percent in 1Q15.
- The third most common unwanted software category in El Salvador in 2Q15 was Adware, which was encountered by 2.5 percent of all computers there, up from 0.9 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in El Salvador in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Ippedo	Worms	2.4%
2	VBS/Jenxcus	Worms	1.6%
3	INF/Autorun	Obfuscators & Injectors	1.5%
4	Win32/Kilim	Trojans	1.3%
5	Win32/Obfuscator	Obfuscators & Injectors	0.8%
6	Win32/Brontok	Worms	0.7%
7	Win32/Skeeyah	Trojans	0.6%
8	Win32/Conficker	Worms	0.6%
9	Win32/Vermis	Worms	0.5%
10	Win32/Sality	Viruses	0.4%

- The most common malware family encountered in El Salvador in 2Q15 was [Win32/Ippedo](#), which was encountered by 2.4 percent of reporting computers there. [Win32/Ippedo](#) is a worm that can send sensitive information to a malicious hacker. It spreads through removable drives, such as USB flash drives.
- The second most common malware family encountered in El Salvador in 2Q15 was [VBS/Jenxcus](#), which was encountered by 1.6 percent of reporting computers there. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The third most common malware family encountered in El Salvador in 2Q15 was [INF/Autorun](#), which was encountered by 1.5 percent of reporting computers there. [INF/Autorun](#) is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The fourth most common malware family encountered in El Salvador in 2Q15 was [Win32/Kilim](#), which was encountered by 1.3 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in El Salvador in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	5.3%
2	Win32/KipodToolsCby	Browser Modifiers	3.8%
3	Win32/InstalleRex	Software Bundlers	3.5%
4	Win32/SaverExtension	Adware	1.9%
5	Win32/AlterbookSP	Browser Modifiers	0.4%

- The most common unwanted software family encountered in El Salvador in 2Q15 was [Win32/CouponRuc](#), which was encountered by 5.3 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in El Salvador in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 3.8 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common unwanted software family encountered in El Salvador in 2Q15 was [Win32/InstalleRex](#), which was encountered by 3.5 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in El Salvador in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	9.2
2	VBS/Jenxcus	Worms	2.2
3	Win32/Kilim	Trojans	2.0
4	Win32/Brontok	Worms	1.0
5	Win32/Sality	Viruses	0.7
6	Win32/Dorkbot	Worms	0.7
7	MSIL/Bladabindi	Backdoors	0.3
8	Win32/Vobfus	Worms	0.2
9	Win32/Gamarue	Worms	0.2
10	MSIL/Spacekito	Trojans	0.2

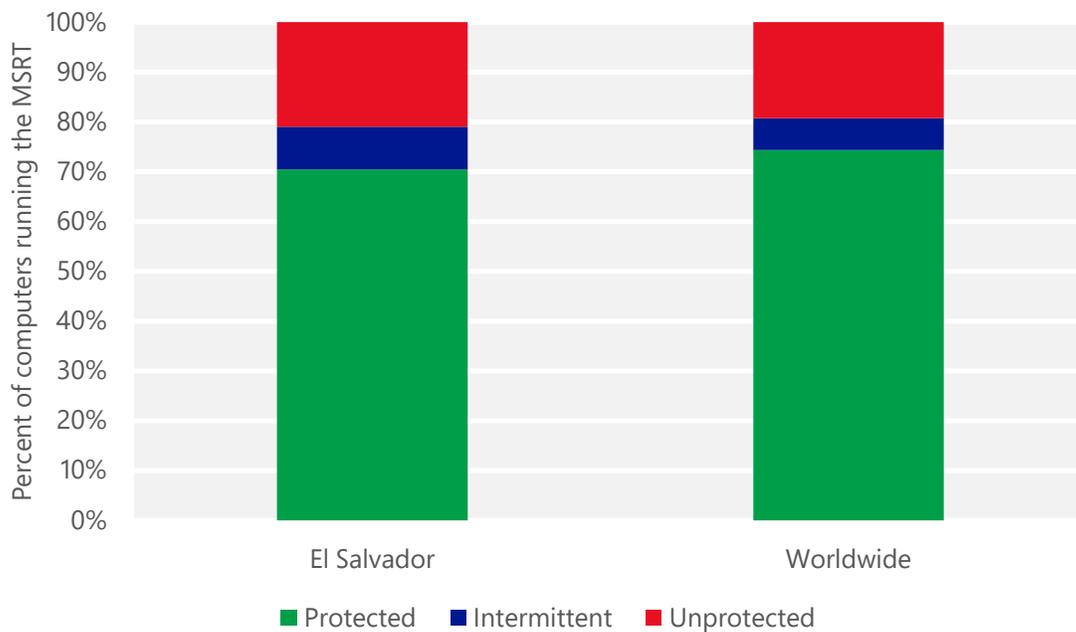
- The most common threat family infecting computers in El Salvador in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 9.2 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in El Salvador in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 2.2 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The third most common threat family infecting computers in El Salvador in 2Q15 was [Win32/Kilim](#), which was detected and removed from 2.0 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The fourth most common threat family infecting computers in El Salvador in 2Q15 was [Win32/Brontok](#), which was detected and removed from 1.0 of every 1,000 unique computers scanned by the MSRT. [Win32/Brontok](#) is a mass-mailing email worm that spreads by sending copies of itself as email attachments to addresses gathered from files on the infected computer, and by copying itself to removable volumes. Brontok can disable security software, and may conduct DoS attacks against certain websites.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in El Salvador and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for El Salvador

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.10 (0.28)	4.58 (0.24)
Phishing sites per 1,000 hosts (Worldwide)		0.84 (5.0)
Malware hosting sites per 1,000 hosts (Worldwide)		3.07 (16.7)

Estonia

The statistics presented here are generated by Microsoft security programs and services running on computers in Estonia in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Estonia

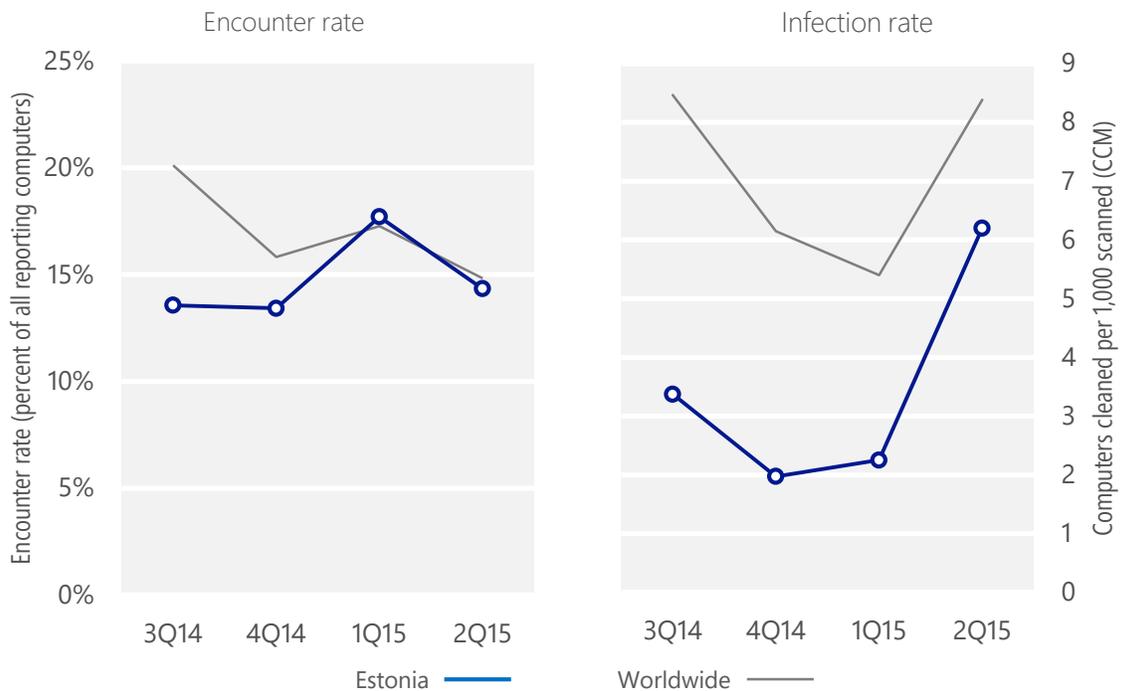
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Estonia	13.6%	13.4%	17.7%	14.3%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Estonia	3.4	2.0	2.3	6.2
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcout, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 14.3% of computers in Estonia encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 6.2 of every 1,000 unique computers scanned in Estonia in 2Q15 (a CCM score of 6.2, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Estonia over the last four quarters, compared to the world as a whole.

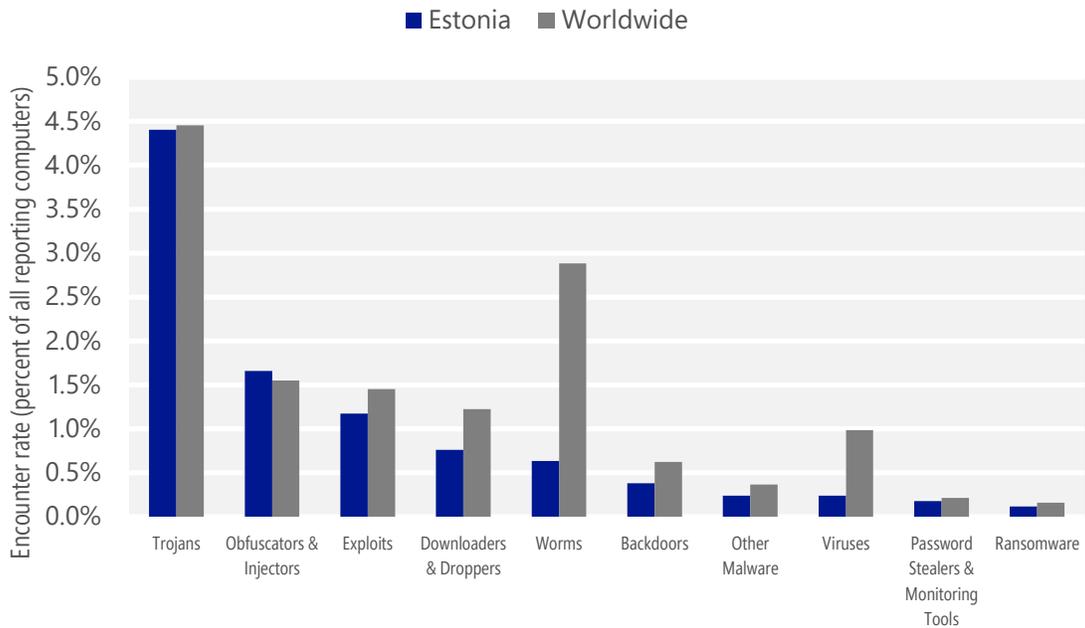
Malware encounter and infection rate trends in Estonia and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in Estonia and around the world, and for explanations of the methods and terms used here.

Malware categories

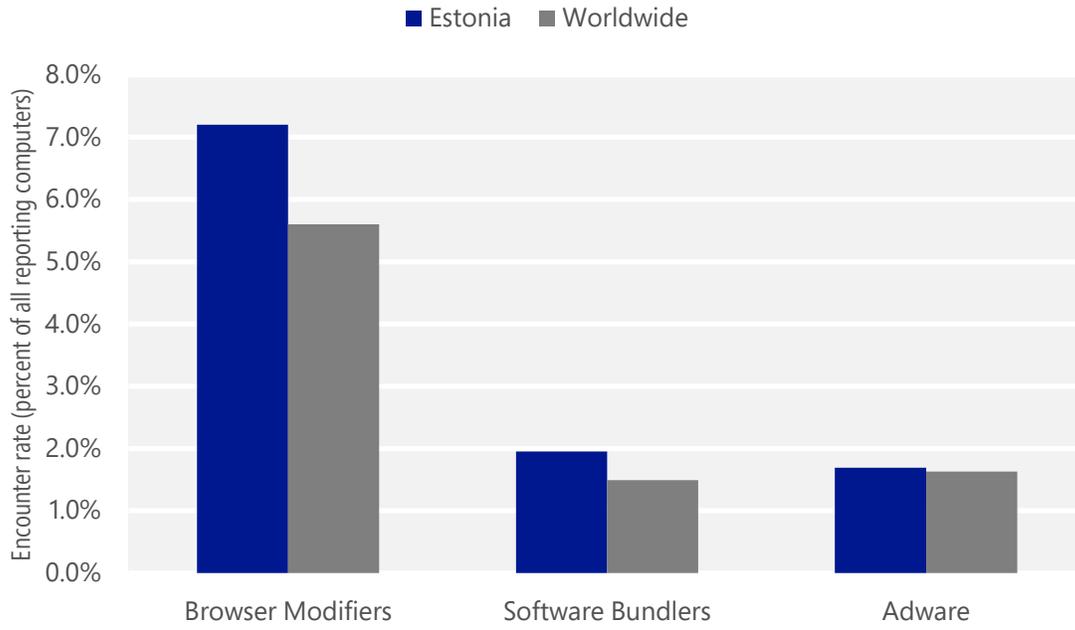
Malware encountered in Estonia in 2Q15, by category



- The most common malware category in Estonia in 2Q15 was Trojans. It was encountered by 4.4 percent of all computers there, up from 3.7 percent in 1Q15.
- The second most common malware category in Estonia in 2Q15 was Obfuscators & Injectors. It was encountered by 1.7 percent of all computers there, up from 1.6 percent in 1Q15.
- The third most common malware category in Estonia in 2Q15 was Exploits, which was encountered by 1.2 percent of all computers there, down from 1.4 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Estonia in 2Q15, by category



- The most common unwanted software category in Estonia in 2Q15 was Browser Modifiers. It was encountered by 7.2 percent of all computers there, down from 10.1 percent in 1Q15.
- The second most common unwanted software category in Estonia in 2Q15 was Software Bundlers. It was encountered by 2.0 percent of all computers there, down from 4.7 percent in 1Q15.
- The third most common unwanted software category in Estonia in 2Q15 was Adware, which was encountered by 1.7 percent of all computers there, up from 0.8 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Estonia in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Obfuscator	Obfuscators & Injectors	1.5%
2	Win32/Kilim	Trojans	1.1%
3	Win32/Peals	Trojans	0.9%
4	Win32/Skeeyah	Trojans	0.8%
5	JS/Axpergle	Exploits	0.6%
6	Win32/Sdbby	Exploits	0.3%
7	Win32/Dynamer	Trojans	0.3%
8	Win32/Gamarue	Worms	0.2%
9	Win32/Dalexis	Downloaders & Droppers	0.1%
10	JS/Neclu	Exploits	0.1%

- The most common malware family encountered in Estonia in 2Q15 was [Win32/Obfuscator](#), which was encountered by 1.5 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The second most common malware family encountered in Estonia in 2Q15 was [Win32/Kilim](#), which was encountered by 1.1 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The third most common malware family encountered in Estonia in 2Q15 was [Win32/Peals](#), which was encountered by 0.9 percent of reporting computers there. [Win32/Peals](#) is a generic detection for various threats that display trojan characteristics.
- The fourth most common malware family encountered in Estonia in 2Q15 was [Win32/Skeeyah](#), which was encountered by 0.8 percent of reporting computers there. [Win32/Skeeyah](#) is a generic detection for various threats that display trojan characteristics.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Estonia in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	3.8%
2	Win32/KipodToolsCby	Browser Modifiers	2.3%
3	Win32/InstalleRex	Software Bundlers	1.9%
4	Win32/SaverExtension	Adware	1.4%
5	Win32/AlterbookSP	Browser Modifiers	1.2%

- The most common unwanted software family encountered in Estonia in 2Q15 was [Win32/CouponRuc](#), which was encountered by 3.8 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in Estonia in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 2.3 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common unwanted software family encountered in Estonia in 2Q15 was [Win32/InstalleRex](#), which was encountered by 1.9 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Estonia in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	2.0
2	Win32/CompromisedCert	Other Malware	1.3
3	Win32/Kilim	Trojans	1.3
4	Win32/Gamarue	Worms	0.3
5	Win32/Ramnit	Trojans	0.2
6	Win32/Simda	Trojans	0.2
7	Win32/Sality	Viruses	0.1
8	MSIL/Bladabindi	Backdoors	0.1
9	Win32/Nuqel	Worms	0.1
10	Win32/Zbot	Password Stealers & Monitoring Tools	0.1

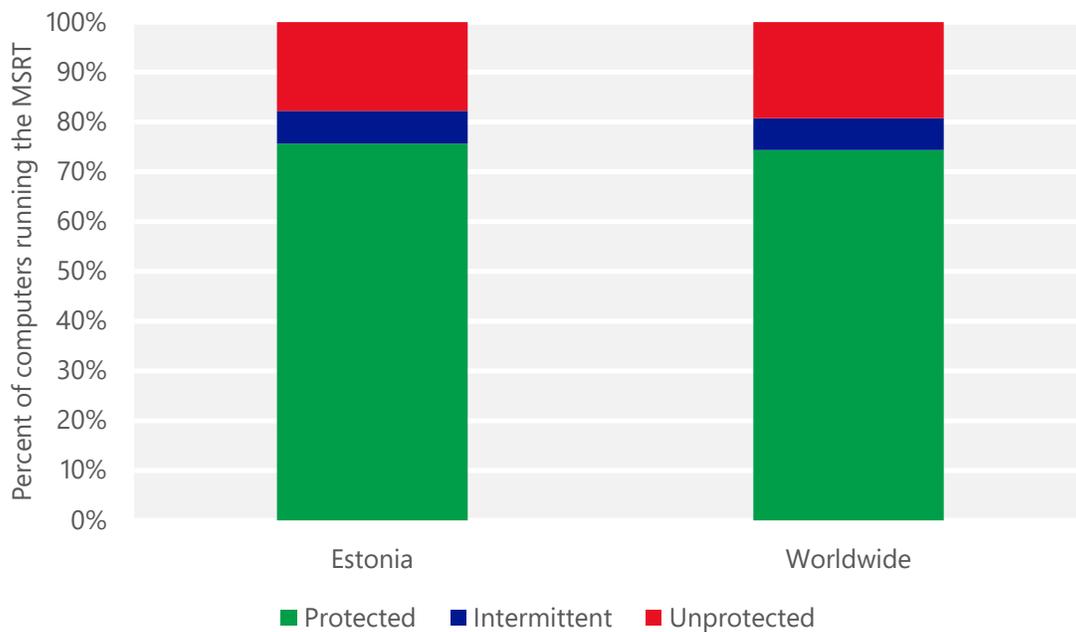
- The most common threat family infecting computers in Estonia in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 2.0 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Estonia in 2Q15 was [Win32/CompromisedCert](#), which was detected and removed from 1.3 of every 1,000 unique computers scanned by the MSRT. [Win32/CompromisedCert](#) is a detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.
- The third most common threat family infecting computers in Estonia in 2Q15 was [Win32/Kilim](#), which was detected and removed from 1.3 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The fourth most common threat family infecting computers in Estonia in 2Q15 was [Win32/Gamarue](#), which was detected and removed from 0.3 of every 1,000 unique computers scanned by the MSRT. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Estonia and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Estonia

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.18 (0.28)	0.05 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	4.06 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	11.65 (16.7)	

Finland

The statistics presented here are generated by Microsoft security programs and services running on computers in Finland in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Finland

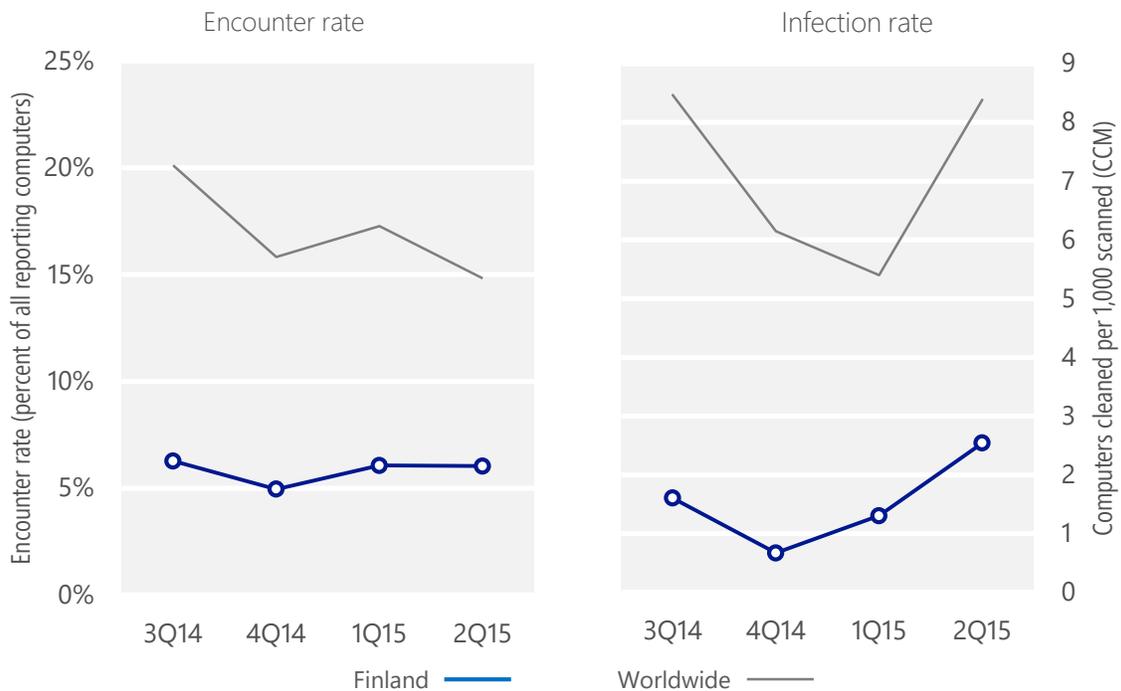
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Finland	6.3%	5.0%	6.1%	6.0%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Finland	1.6	0.7	1.3	2.5
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcote, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 6.0% of computers in Finland encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 2.5 of every 1,000 unique computers scanned in Finland in 2Q15 (a CCM score of 2.5, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Finland over the last four quarters, compared to the world as a whole.

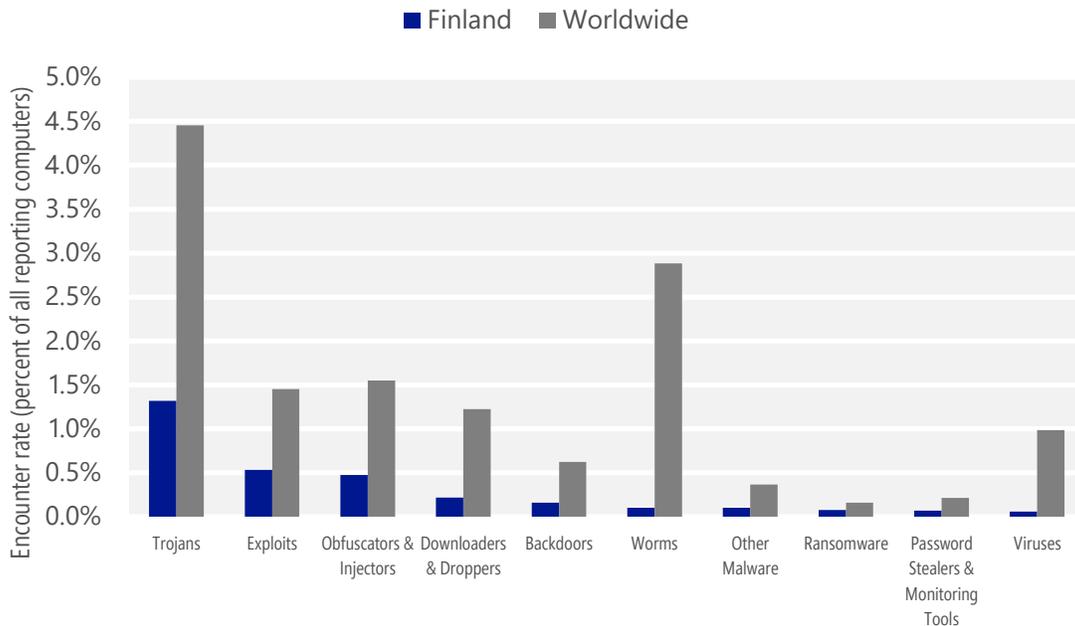
Malware encounter and infection rate trends in Finland and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in Finland and around the world, and for explanations of the methods and terms used here.

Malware categories

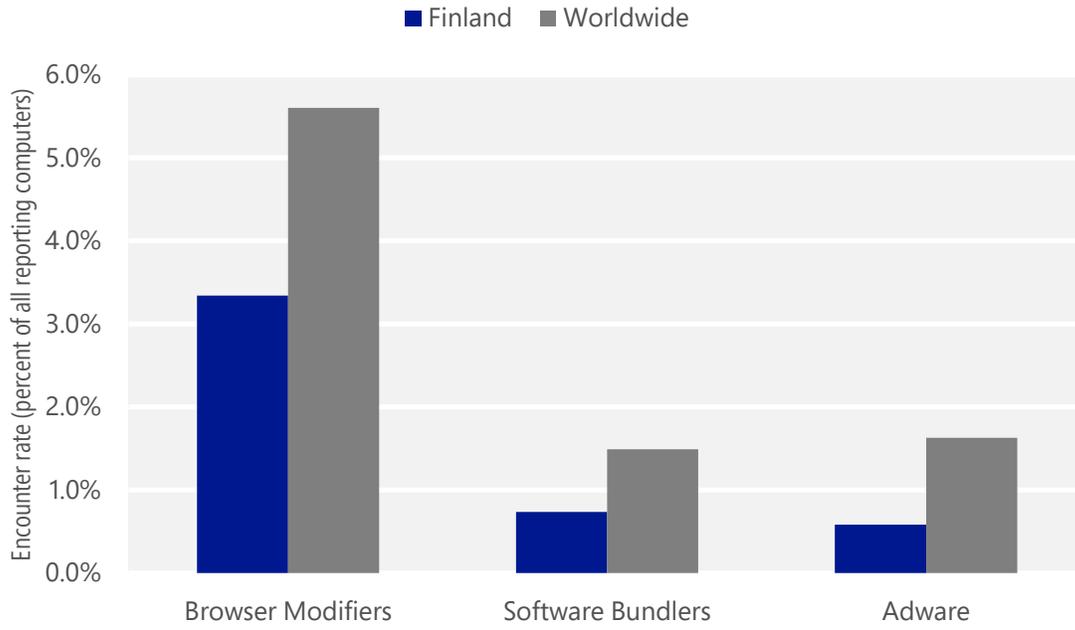
Malware encountered in Finland in 2Q15, by category



- The most common malware category in Finland in 2Q15 was Trojans. It was encountered by 1.3 percent of all computers there, up from 0.9 percent in 1Q15.
- The second most common malware category in Finland in 2Q15 was Exploits. It was encountered by 0.5 percent of all computers there, down from 0.7 percent in 1Q15.
- The third most common malware category in Finland in 2Q15 was Obfuscators & Injectors, which was encountered by 0.5 percent of all computers there, down from 0.6 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Finland in 2Q15, by category



- The most common unwanted software category in Finland in 2Q15 was Browser Modifiers. It was encountered by 3.3 percent of all computers there, up from 2.8 percent in 1Q15.
- The second most common unwanted software category in Finland in 2Q15 was Software Bundlers. It was encountered by 0.7 percent of all computers there, down from 1.5 percent in 1Q15.
- The third most common unwanted software category in Finland in 2Q15 was Adware, which was encountered by 0.6 percent of all computers there, up from 0.3 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Finland in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Obfuscator	Obfuscators & Injectors	0.4%
2	Win32/Kilim	Trojans	0.3%
3	JS/Axpergle	Exploits	0.2%
4	Win32/Skeeyah	Trojans	0.2%
5	Win32/Peals	Trojans	0.2%
6	Win32/Sdbby	Exploits	0.1%
7	Win32/Dynamer	Trojans	0.1%
8	MSIL/Bladabindi	Backdoors	<0.1%
9	Win32/Crowti	Ransomware	<0.1%
10	Win32/Fynloski	Backdoors	<0.1%

- The most common malware family encountered in Finland in 2Q15 was [Win32/Obfuscator](#), which was encountered by 0.4 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The second most common malware family encountered in Finland in 2Q15 was [Win32/Kilim](#), which was encountered by 0.3 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The third most common malware family encountered in Finland in 2Q15 was [JS/Axpergle](#), which was encountered by 0.2 percent of reporting computers there. [JS/Axpergle](#) is a detection for the Angler exploit kit, which exploits vulnerabilities in recent versions of Internet Explorer, Silverlight, Adobe Flash Player, and Java to install malware.
- The fourth most common malware family encountered in Finland in 2Q15 was [Win32/Skeeyah](#), which was encountered by 0.2 percent of reporting computers there. [Win32/Skeeyah](#) is a generic detection for various threats that display trojan characteristics.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Finland in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	1.2%
2	Win32/AlterbookSP	Browser Modifiers	1.2%
3	Win32/KipodToolsCby	Browser Modifiers	0.7%
4	Win32/InstalleRex	Software Bundlers	0.7%
5	Win32/SaverExtension	Adware	0.4%

- The most common unwanted software family encountered in Finland in 2Q15 was [Win32/CouponRuc](#), which was encountered by 1.2 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in Finland in 2Q15 was [Win32/AlterbookSP](#), which was encountered by 1.2 percent of reporting computers there. [Win32/AlterbookSP](#) is a browser add-on that formerly displayed behaviors of unwanted software. Recent versions of the add-on no longer meet Microsoft detection criteria, and are no longer considered unwanted software.
- The third most common unwanted software family encountered in Finland in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 0.7 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.

Top threat families by infection rate

The most common malware families by infection rate in Finland in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/CompromisedCert	Other Malware	1.1
2	Win32/leEnablerCby	Browser Modifiers	0.6
3	Win32/Kilim	Trojans	0.4
4	MSIL/Bladabindi	Backdoors	0.1
5	Win32/Alureon	Trojans	<0.1
6	Win32/Simda	Trojans	<0.1
7	Win32/Nitol	Other Malware	<0.1
8	Win32/Sality	Viruses	<0.1
9	Win32/Ramnit	Trojans	<0.1
10	Win32/Wysotot	Trojans	<0.1

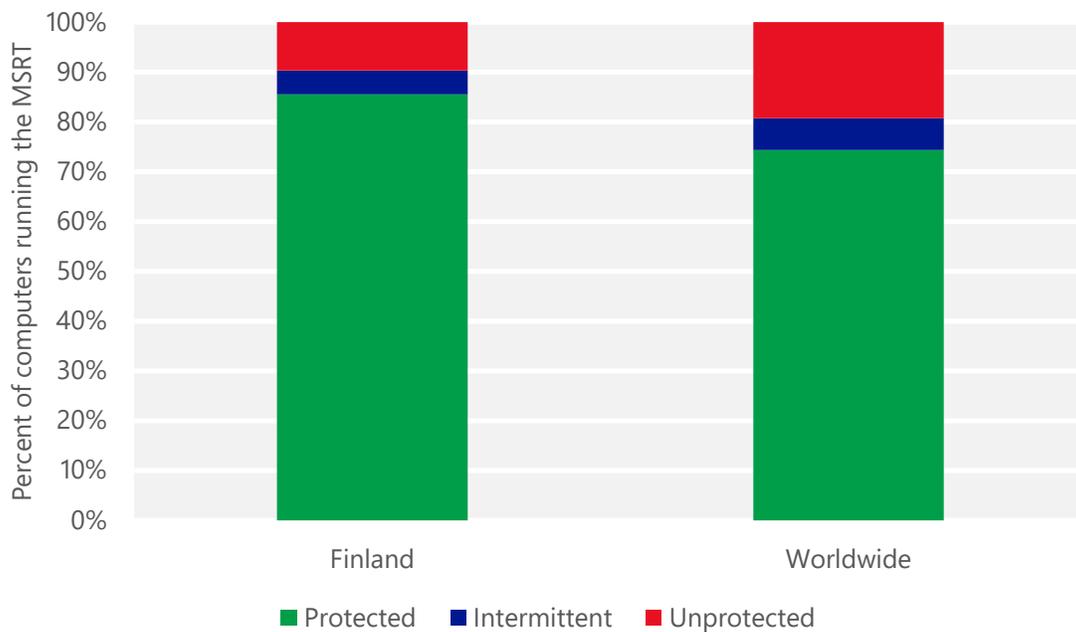
- The most common threat family infecting computers in Finland in 2Q15 was [Win32/CompromisedCert](#), which was detected and removed from 1.1 of every 1,000 unique computers scanned by the MSRT. [Win32/CompromisedCert](#) is a detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.
- The second most common threat family infecting computers in Finland in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 0.6 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common threat family infecting computers in Finland in 2Q15 was [Win32/Kilim](#), which was detected and removed from 0.4 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The fourth most common threat family infecting computers in Finland in 2Q15 was [MSIL/Bladabindi](#), which was detected and removed from 0.1 of every 1,000 unique computers scanned by the MSRT. [MSIL/Bladabindi](#) is a family of backdoors created by a malicious hacker tool called NJ Rat. The can steal sensitive information, download other malware, and allow backdoor access to an infected computer.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Finland and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Finland

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.05 (0.28)	0.01 (0.24)
Phishing sites per 1,000 hosts (Worldwide)		2.69 (5.0)
Malware hosting sites per 1,000 hosts (Worldwide)		4.42 (16.7)

France

The statistics presented here are generated by Microsoft security programs and services running on computers in France in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for France

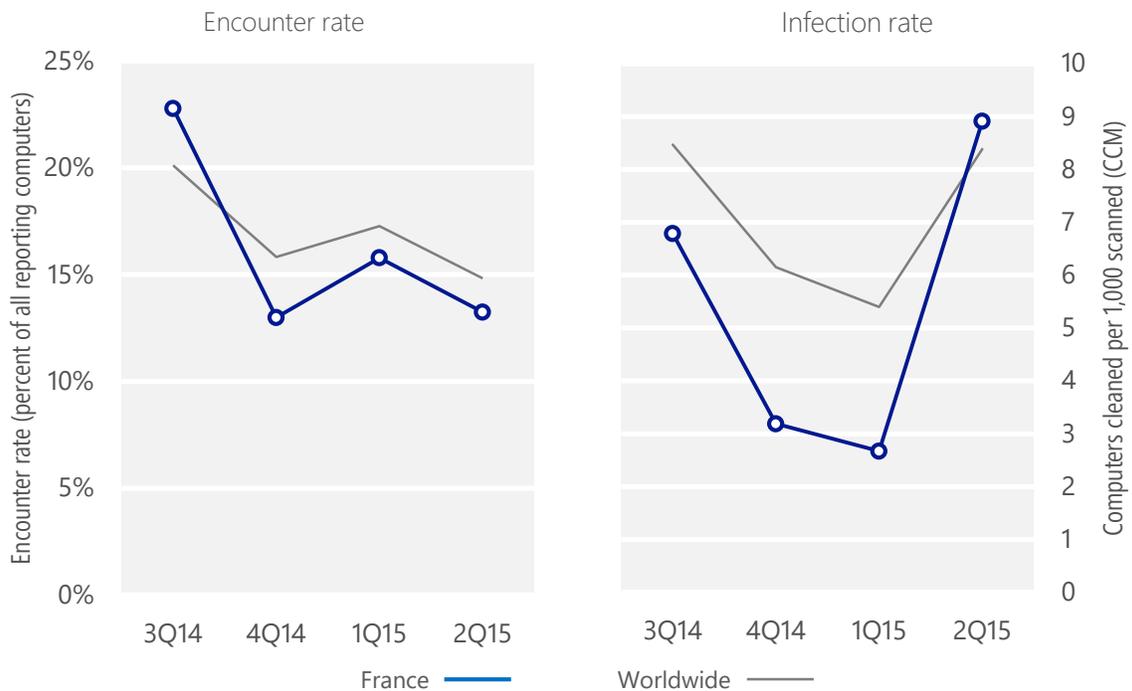
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, France	22.8%	13.0%	15.8%	13.2%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, France	6.8	3.2	2.7	8.9
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcoute, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 13.2% of computers in France encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 8.9 of every 1,000 unique computers scanned in France in 2Q15 (a CCM score of 8.9, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for France over the last four quarters, compared to the world as a whole.

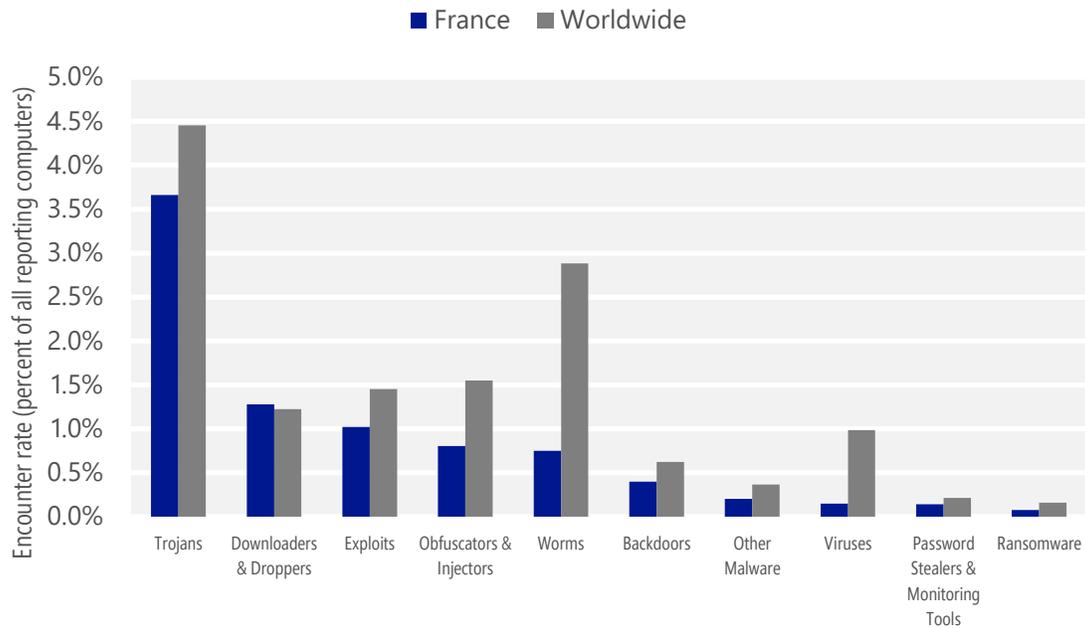
Malware encounter and infection rate trends in France and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in France and around the world, and for explanations of the methods and terms used here.

Malware categories

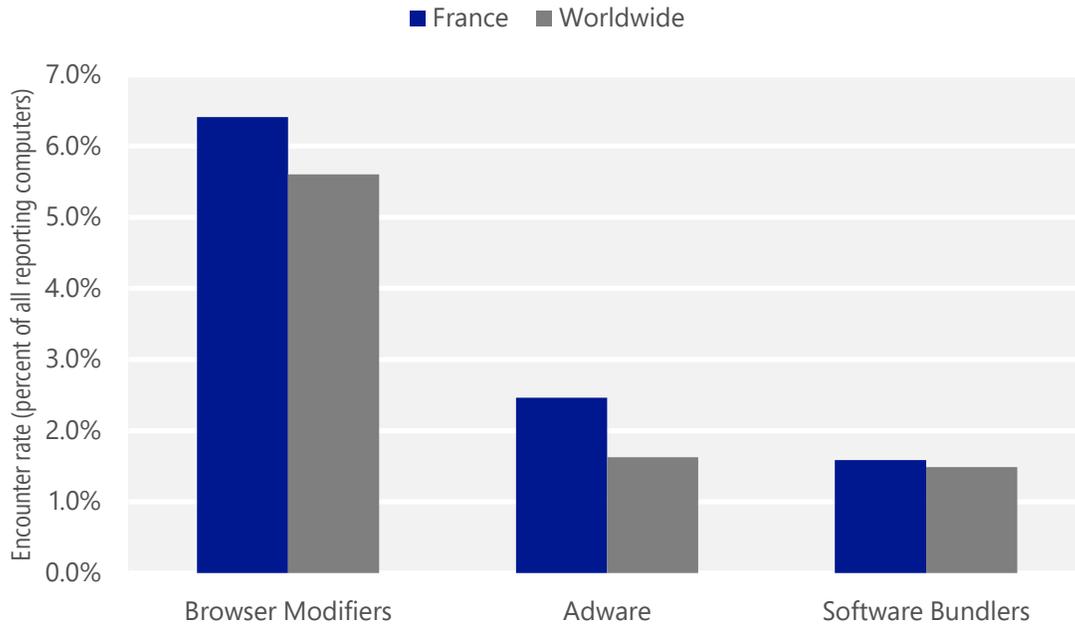
Malware encountered in France in 2Q15, by category



- The most common malware category in France in 2Q15 was Trojans. It was encountered by 3.7 percent of all computers there, up from 2.0 percent in 1Q15.
- The second most common malware category in France in 2Q15 was Downloaders & Droppers. It was encountered by 1.3 percent of all computers there, down from 1.5 percent in 1Q15.
- The third most common malware category in France in 2Q15 was Exploits, which was encountered by 1.0 percent of all computers there, down from 1.5 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in France in 2Q15, by category



- The most common unwanted software category in France in 2Q15 was Browser Modifiers. It was encountered by 6.4 percent of all computers there, down from 7.8 percent in 1Q15.
- The second most common unwanted software category in France in 2Q15 was Adware. It was encountered by 2.5 percent of all computers there, down from 5.3 percent in 1Q15.
- The third most common unwanted software category in France in 2Q15 was Software Bundlers, which was encountered by 1.6 percent of all computers there, up from 0.6 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in France in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Kilim	Trojans	1.0%
2	Win32/Skeeyah	Trojans	0.9%
3	JS/Axpergle	Exploits	0.6%
4	Win32/Obfuscator	Obfuscators & Injectors	0.6%
5	Win32/Peals	Trojans	0.3%
6	Win32/Tugspay	Downloaders & Droppers	0.2%
7	INF/Autorun	Obfuscators & Injectors	0.2%
8	VBS/Jenxcus	Worms	0.2%
9	Win32/Dynamer	Trojans	0.2%
10	ASX/Wimad	Downloaders & Droppers	0.1%

- The most common malware family encountered in France in 2Q15 was [Win32/Kilim](#), which was encountered by 1.0 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The second most common malware family encountered in France in 2Q15 was [Win32/Skeeyah](#), which was encountered by 0.9 percent of reporting computers there. [Win32/Skeeyah](#) is a generic detection for various threats that display trojan characteristics.
- The third most common malware family encountered in France in 2Q15 was [JS/Axpergle](#), which was encountered by 0.6 percent of reporting computers there. [JS/Axpergle](#) is a detection for the Angler exploit kit, which exploits vulnerabilities in recent versions of Internet Explorer, Silverlight, Adobe Flash Player, and Java to install malware.
- The fourth most common malware family encountered in France in 2Q15 was [Win32/Obfuscator](#), which was encountered by 0.6 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in France in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	3.2%
2	Win32/KipodToolsCby	Browser Modifiers	2.2%
3	Win32/InstalleRex	Software Bundlers	1.5%
4	Win32/EoRezo	Adware	1.1%
5	Win32/SaverExtension	Adware	1.0%

- The most common unwanted software family encountered in France in 2Q15 was [Win32/CouponRuc](#), which was encountered by 3.2 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in France in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 2.2 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common unwanted software family encountered in France in 2Q15 was [Win32/InstalleRex](#), which was encountered by 1.5 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in France in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	4.8
2	Win32/Kilim	Trojans	1.4
3	Win32/CompromisedCert	Other Malware	1.2
4	VBS/Jenxcus	Worms	0.2
5	Win32/Nitol	Other Malware	0.1
6	Win32/Brontok	Worms	0.1
7	Win32/Dyzap	Password Stealers & Monitoring Tools	0.1
8	MSIL/Bladabindi	Backdoors	0.1
9	Win32/Simda	Trojans	0.1
10	Win32/Wysotot	Trojans	0.1

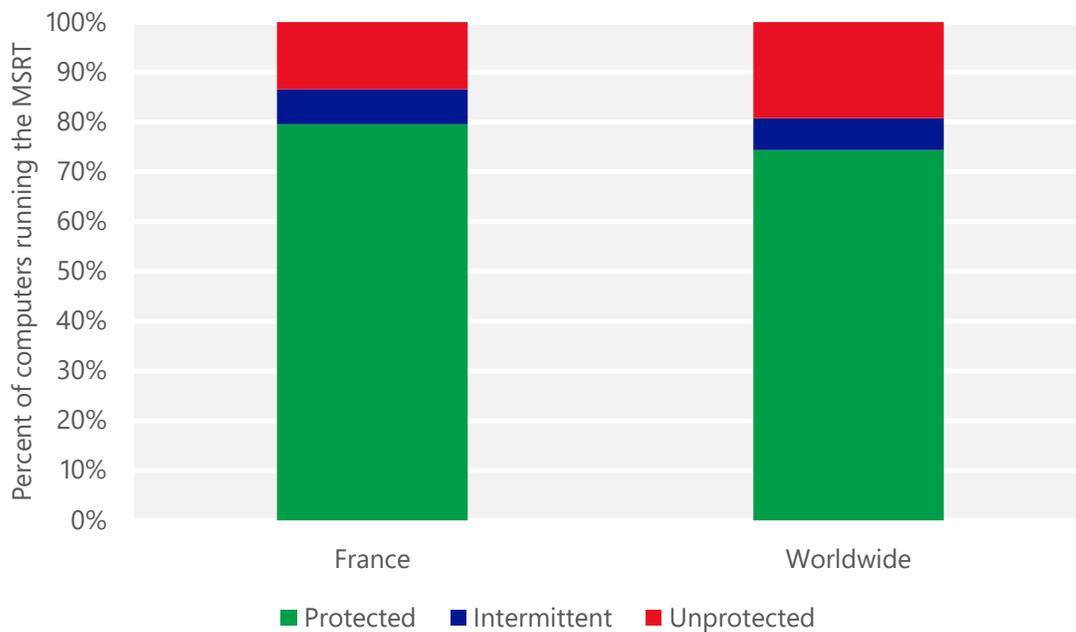
- The most common threat family infecting computers in France in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 4.8 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in France in 2Q15 was [Win32/Kilim](#), which was detected and removed from 1.4 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The third most common threat family infecting computers in France in 2Q15 was [Win32/CompromisedCert](#), which was detected and removed from 1.2 of every 1,000 unique computers scanned by the MSRT. [Win32/CompromisedCert](#) is a detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.
- The fourth most common threat family infecting computers in France in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 0.2 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in France and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for France

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.12 (0.28)	0.10 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	5.97 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	19.25 (16.7)	

Georgia

The statistics presented here are generated by Microsoft security programs and services running on computers in Georgia in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Georgia

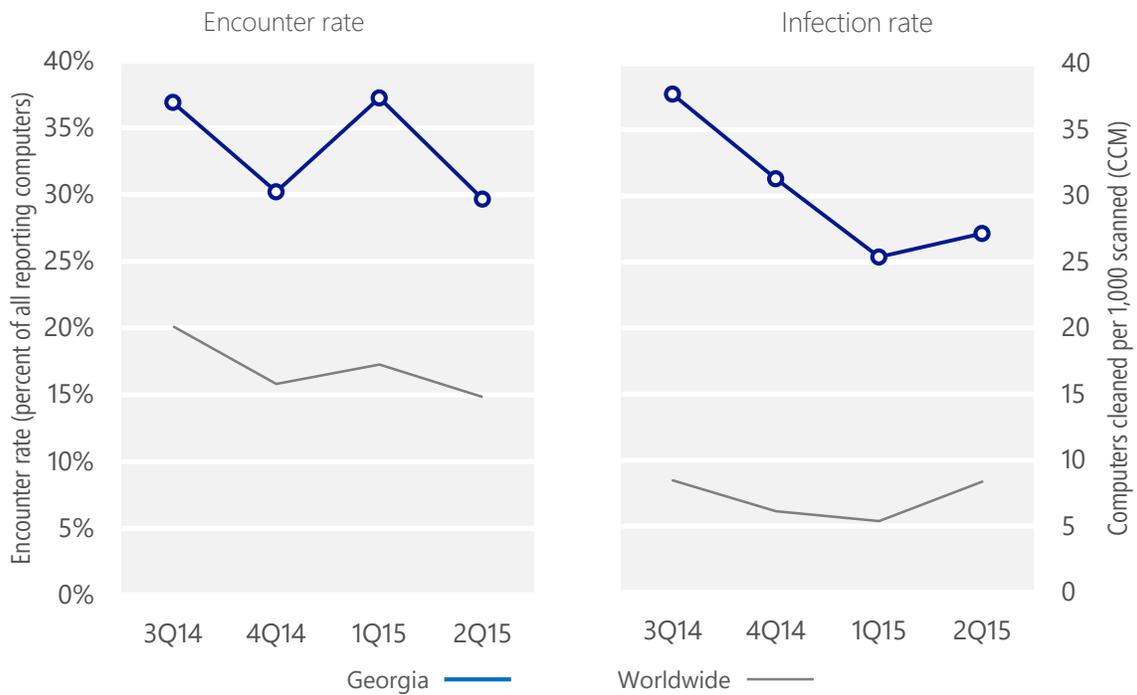
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Georgia	36.9%	30.2%	37.2%	29.7%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Georgia	37.7	31.3	25.4	27.2
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcoute, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 29.7% of computers in Georgia encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 27.2 of every 1,000 unique computers scanned in Georgia in 2Q15 (a CCM score of 27.2, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Georgia over the last four quarters, compared to the world as a whole.

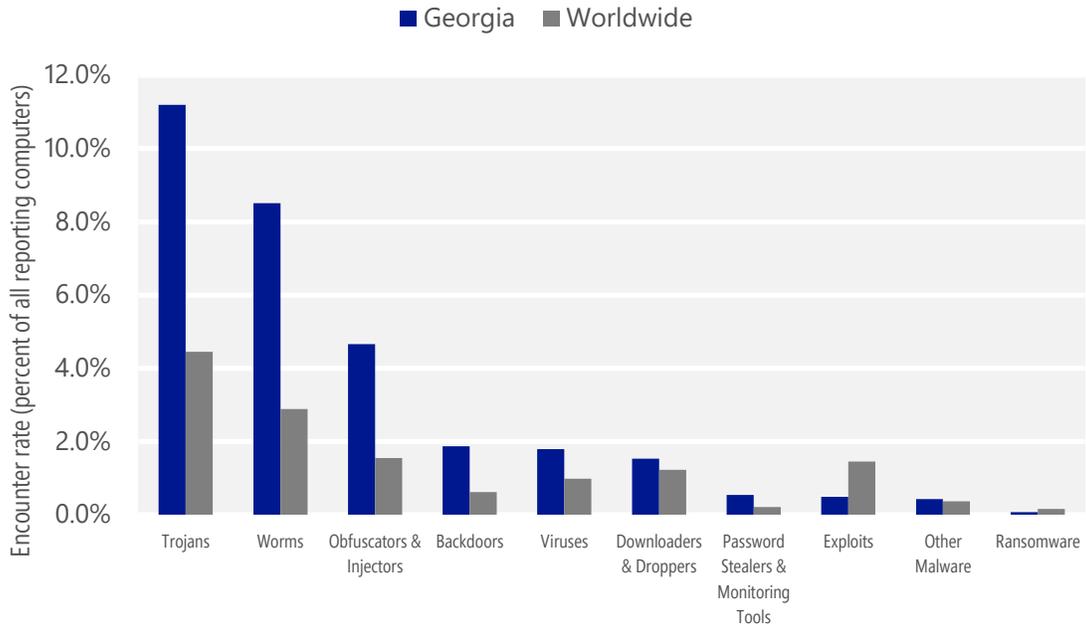
Malware encounter and infection rate trends in Georgia and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in Georgia and around the world, and for explanations of the methods and terms used here.

Malware categories

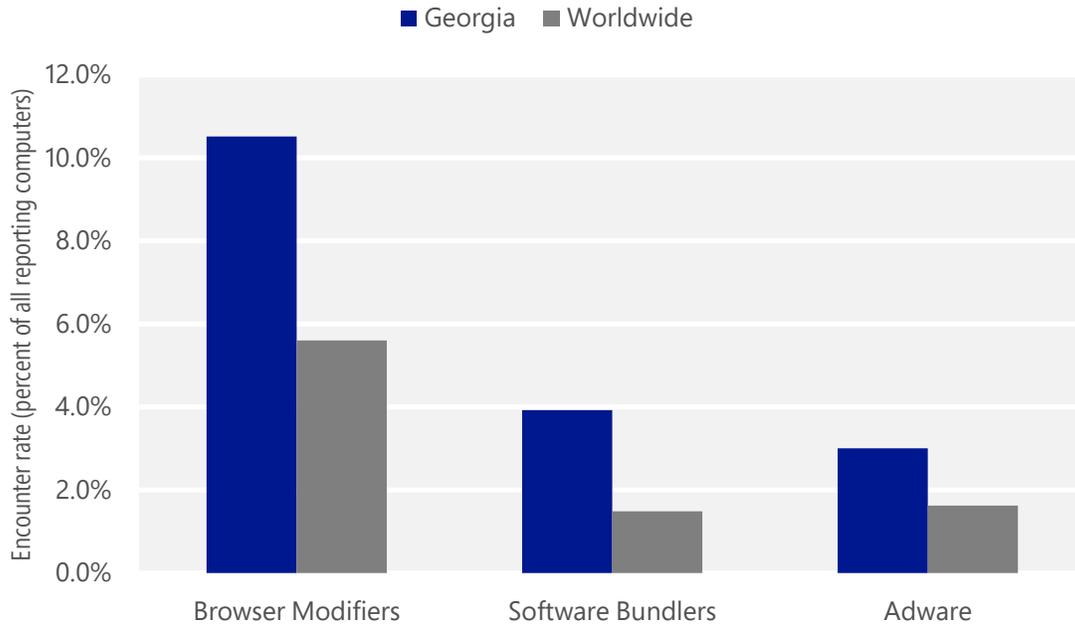
Malware encountered in Georgia in 2Q15, by category



- The most common malware category in Georgia in 2Q15 was Trojans. It was encountered by 11.2 percent of all computers there, down from 11.8 percent in 1Q15.
- The second most common malware category in Georgia in 2Q15 was Worms. It was encountered by 8.5 percent of all computers there, down from 11.6 percent in 1Q15.
- The third most common malware category in Georgia in 2Q15 was Obfuscators & Injectors, which was encountered by 4.7 percent of all computers there, down from 4.9 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Georgia in 2Q15, by category



- The most common unwanted software category in Georgia in 2Q15 was Browser Modifiers. It was encountered by 10.5 percent of all computers there, down from 16.6 percent in 1Q15.
- The second most common unwanted software category in Georgia in 2Q15 was Software Bundlers. It was encountered by 3.9 percent of all computers there, down from 6.4 percent in 1Q15.
- The third most common unwanted software category in Georgia in 2Q15 was Adware, which was encountered by 3.0 percent of all computers there, up from 1.3 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Georgia in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Obfuscator	Obfuscators & Injectors	3.7%
2	Win32/Kilim	Trojans	3.3%
3	Win32/Gamarue	Worms	2.8%
4	Win32/Skeeyah	Trojans	1.8%
5	Win32/Peals	Trojans	1.7%
6	Win32/Tophos	Worms	1.7%
7	Win32/Brontok	Worms	1.4%
8	INF/Autorun	Obfuscators & Injectors	1.1%
9	Win32/Caphaw	Backdoors	1.1%
10	Win32/Nuqel	Worms	0.9%

- The most common malware family encountered in Georgia in 2Q15 was [Win32/Obfuscator](#), which was encountered by 3.7 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The second most common malware family encountered in Georgia in 2Q15 was [Win32/Kilim](#), which was encountered by 3.3 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The third most common malware family encountered in Georgia in 2Q15 was [Win32/Gamarue](#), which was encountered by 2.8 percent of reporting computers there. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The fourth most common malware family encountered in Georgia in 2Q15 was [Win32/Skeeyah](#), which was encountered by 1.8 percent of reporting computers there. [Win32/Skeeyah](#) is a generic detection for various threats that display trojan characteristics.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Georgia in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	6.7%
2	Win32/KipodToolsCby	Browser Modifiers	4.0%
3	Win32/InstalleRex	Software Bundlers	3.8%
4	Win32/SaverExtension	Adware	2.4%
5	Win32/AlterbookSP	Browser Modifiers	0.3%

- The most common unwanted software family encountered in Georgia in 2Q15 was [Win32/CouponRuc](#), which was encountered by 6.7 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in Georgia in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 4.0 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common unwanted software family encountered in Georgia in 2Q15 was [Win32/InstalleRex](#), which was encountered by 3.8 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Georgia in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/Gamarue	Worms	4.9
2	Win32/leEnablerCby	Browser Modifiers	4.4
3	Win32/Kilim	Trojans	3.9
4	Win32/Sality	Viruses	3.2
5	Win32/Brontok	Worms	2.6
6	Win32/Ramnit	Trojans	2.2
7	Win32/Dorkbot	Worms	1.4
8	Win32/Nuqel	Worms	1.4
9	Win32/Helompy	Worms	1.3
10	Win32/Jeefo	Viruses	1.0

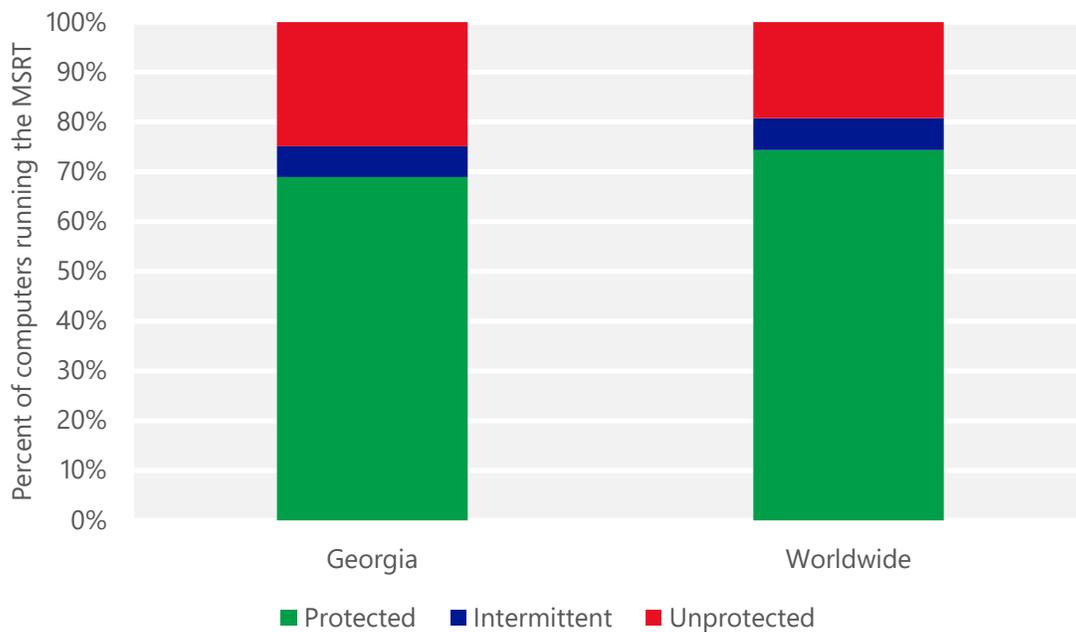
- The most common threat family infecting computers in Georgia in 2Q15 was [Win32/Gamarue](#), which was detected and removed from 4.9 of every 1,000 unique computers scanned by the MSRT. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The second most common threat family infecting computers in Georgia in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 4.4 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common threat family infecting computers in Georgia in 2Q15 was [Win32/Kilim](#), which was detected and removed from 3.9 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The fourth most common threat family infecting computers in Georgia in 2Q15 was [Win32/Sality](#), which was detected and removed from 3.2 of every 1,000 unique computers scanned by the MSRT. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Georgia and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Georgia

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.59 (0.28)	0.67 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	11.52 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	19.98 (16.7)	

Germany

The statistics presented here are generated by Microsoft security programs and services running on computers in Germany in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Germany

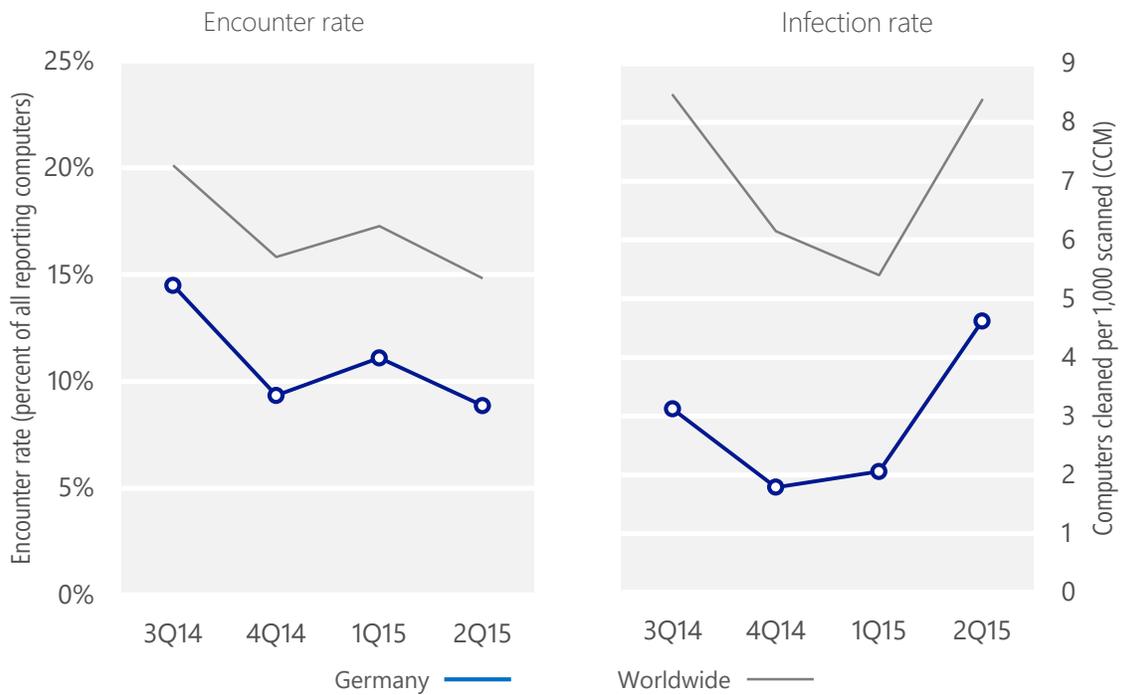
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Germany	14.5%	9.3%	11.1%	8.9%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Germany	3.1	1.8	2.1	4.6
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcote, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 8.9% of computers in Germany encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 4.6 of every 1,000 unique computers scanned in Germany in 2Q15 (a CCM score of 4.6, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Germany over the last four quarters, compared to the world as a whole.

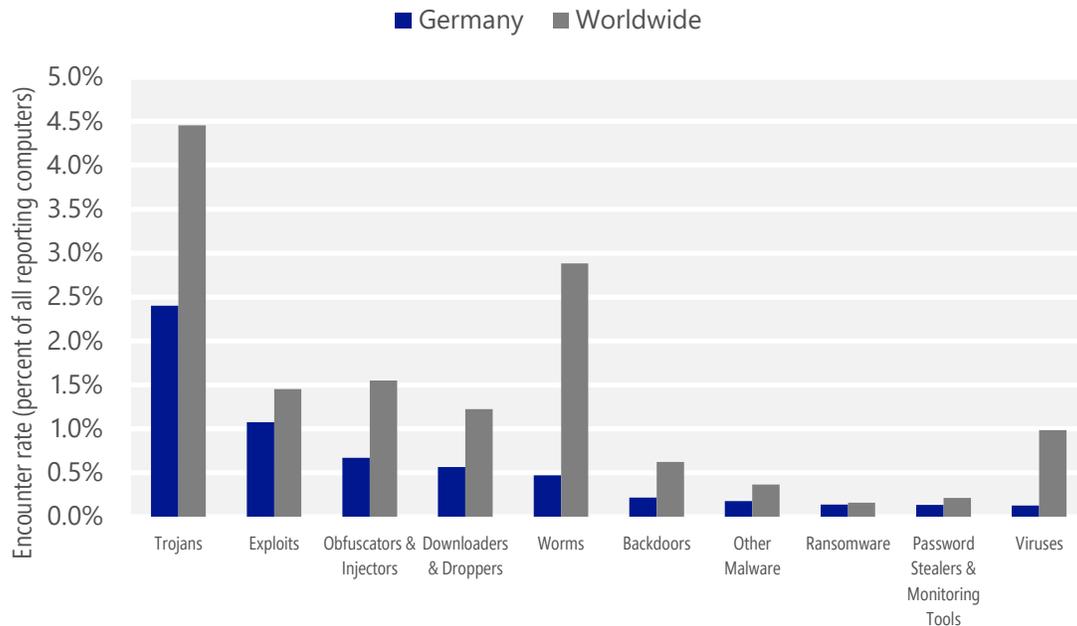
Malware encounter and infection rate trends in Germany and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in Germany and around the world, and for explanations of the methods and terms used here.

Malware categories

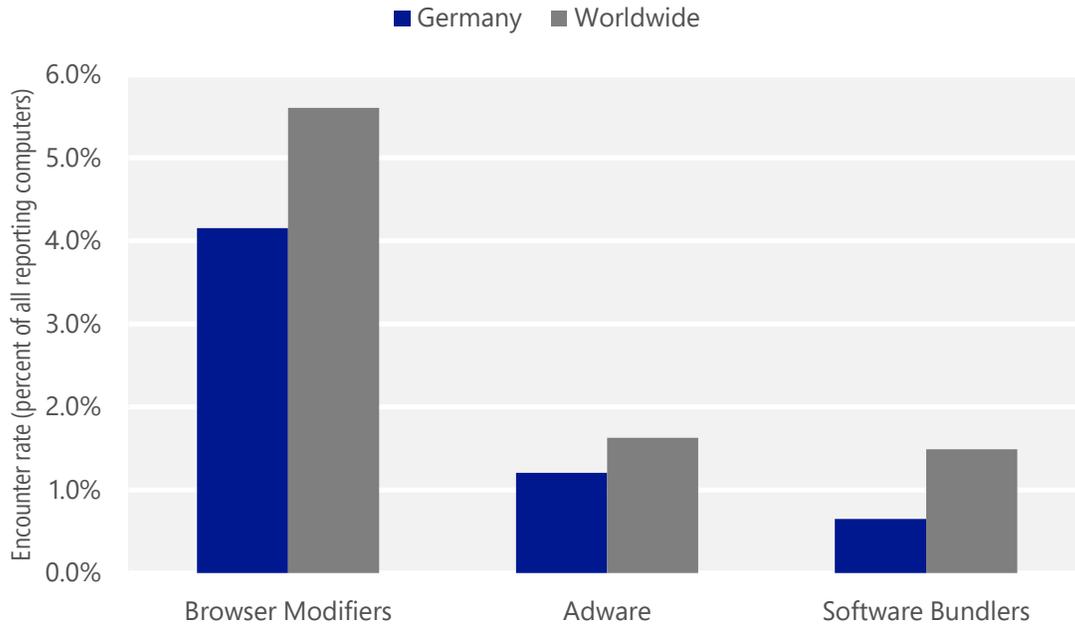
Malware encountered in Germany in 2Q15, by category



- The most common malware category in Germany in 2Q15 was Trojans. It was encountered by 2.4 percent of all computers there, up from 2.1 percent in 1Q15.
- The second most common malware category in Germany in 2Q15 was Exploits. It was encountered by 1.1 percent of all computers there, down from 1.9 percent in 1Q15.
- The third most common malware category in Germany in 2Q15 was Obfuscators & Injectors, which was encountered by 0.7 percent of all computers there, down from 1.0 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Germany in 2Q15, by category



- The most common unwanted software category in Germany in 2Q15 was Browser Modifiers. It was encountered by 4.2 percent of all computers there, down from 4.5 percent in 1Q15.
- The second most common unwanted software category in Germany in 2Q15 was Adware. It was encountered by 1.2 percent of all computers there, down from 2.8 percent in 1Q15.
- The third most common unwanted software category in Germany in 2Q15 was Software Bundlers, which was encountered by 0.7 percent of all computers there, up from 0.3 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Germany in 2Q15

	Family	Most significant category	% of reporting computers
1	JS/Axpergle	Exploits	0.7%
2	Win32/Obfuscator	Obfuscators & Injectors	0.6%
3	Win32/Skeeyah	Trojans	0.5%
4	Win32/Kilim	Trojans	0.4%
5	Win32/Peals	Trojans	0.4%
6	Win32/Dynamer	Trojans	0.2%
7	Win32/Conficker	Worms	0.2%
8	Win32/Emotet	Trojans	0.2%
9	Win32/Tugspay	Downloaders & Droppers	0.1%
10	JS/Neclu	Exploits	0.1%

- The most common malware family encountered in Germany in 2Q15 was [JS/Axpergle](#), which was encountered by 0.7 percent of reporting computers there. [JS/Axpergle](#) is a detection for the Angler exploit kit, which exploits vulnerabilities in recent versions of Internet Explorer, Silverlight, Adobe Flash Player, and Java to install malware.
- The second most common malware family encountered in Germany in 2Q15 was [Win32/Obfuscator](#), which was encountered by 0.6 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The third most common malware family encountered in Germany in 2Q15 was [Win32/Skeeyah](#), which was encountered by 0.5 percent of reporting computers there. [Win32/Skeeyah](#) is a generic detection for various threats that display trojan characteristics.
- The fourth most common malware family encountered in Germany in 2Q15 was [Win32/Kilim](#), which was encountered by 0.4 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Germany in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	1.8%
2	Win32/KipodToolsCby	Browser Modifiers	1.5%
3	Win32/InstalleRex	Software Bundlers	0.6%
4	Win32/AlterbookSP	Browser Modifiers	0.6%
5	Win32/SaverExtension	Adware	0.6%

- The most common unwanted software family encountered in Germany in 2Q15 was [Win32/CouponRuc](#), which was encountered by 1.8 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in Germany in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 1.5 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common unwanted software family encountered in Germany in 2Q15 was [Win32/InstalleRex](#), which was encountered by 0.6 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Germany in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	1.9
2	Win32/CompromisedCert	Other Malware	0.8
3	Win32/Kilim	Trojans	0.6
4	Win32/Emotet	Trojans	0.2
5	Win32/Matsnu	Trojans	0.1
6	Win32/Ramnit	Trojans	0.1
7	Win32/Zbot	Password Stealers & Monitoring Tools	0.1
8	Win32/Alureon	Trojans	0.1
9	Win32/Nitol	Other Malware	0.1
10	Win32/Dyzap	Password Stealers & Monitoring Tools	0.1

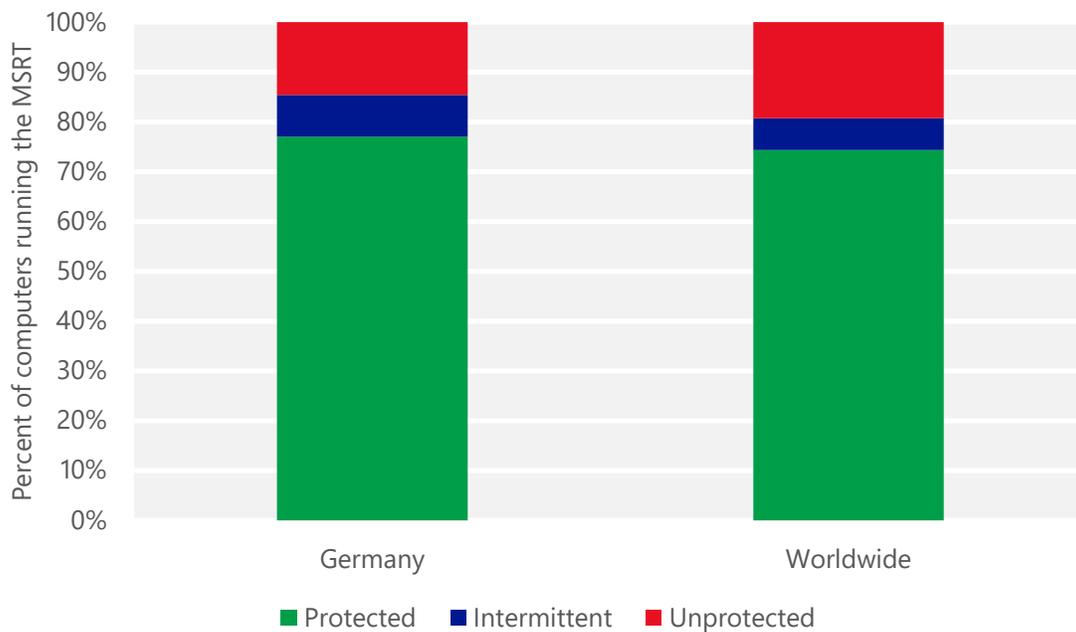
- The most common threat family infecting computers in Germany in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 1.9 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Germany in 2Q15 was [Win32/CompromisedCert](#), which was detected and removed from 0.8 of every 1,000 unique computers scanned by the MSRT. [Win32/CompromisedCert](#) is a detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.
- The third most common threat family infecting computers in Germany in 2Q15 was [Win32/Kilim](#), which was detected and removed from 0.6 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The fourth most common threat family infecting computers in Germany in 2Q15 was [Win32/Emotet](#), which was detected and removed from 0.2 of every 1,000 unique computers scanned by the MSRT. [Win32/Emotet](#) is a threat that can steal personal information, including banking user names and passwords. It is usually installed when the user opens a spam email attachment.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Germany and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Germany

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.17 (0.28)	0.13 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	4.35 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	15.23 (16.7)	

Greece

The statistics presented here are generated by Microsoft security programs and services running on computers in Greece in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Greece

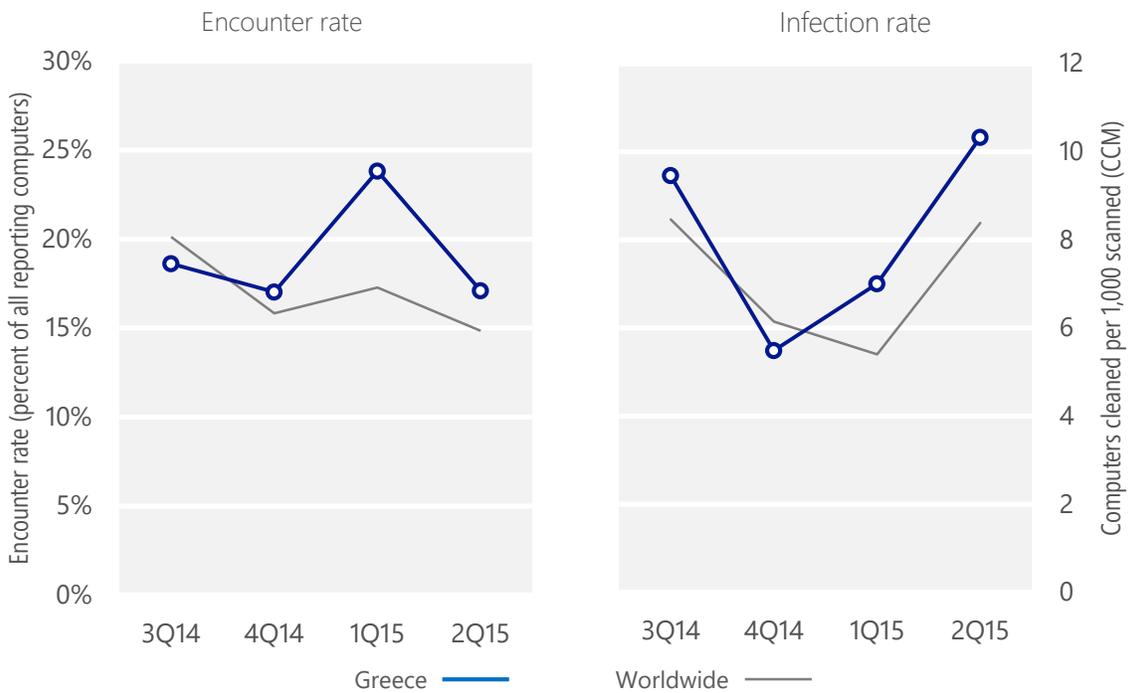
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Greece	18.6%	17.0%	23.8%	17.1%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Greece	9.5	5.5	7.0	10.3
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcote, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 17.1% of computers in Greece encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 10.3 of every 1,000 unique computers scanned in Greece in 2Q15 (a CCM score of 10.3, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Greece over the last four quarters, compared to the world as a whole.

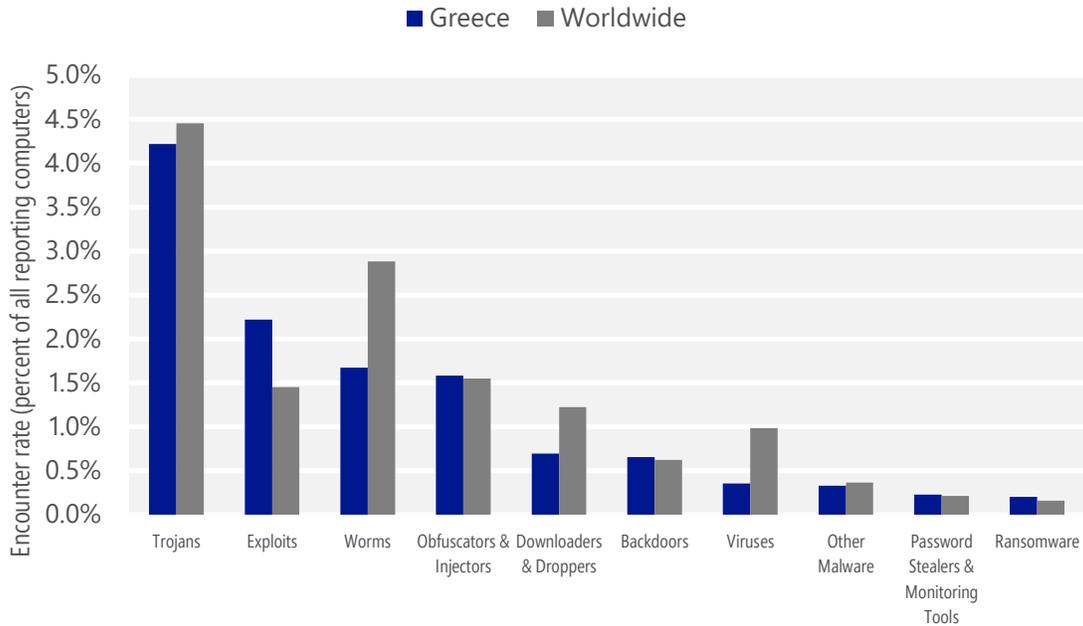
Malware encounter and infection rate trends in Greece and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in Greece and around the world, and for explanations of the methods and terms used here.

Malware categories

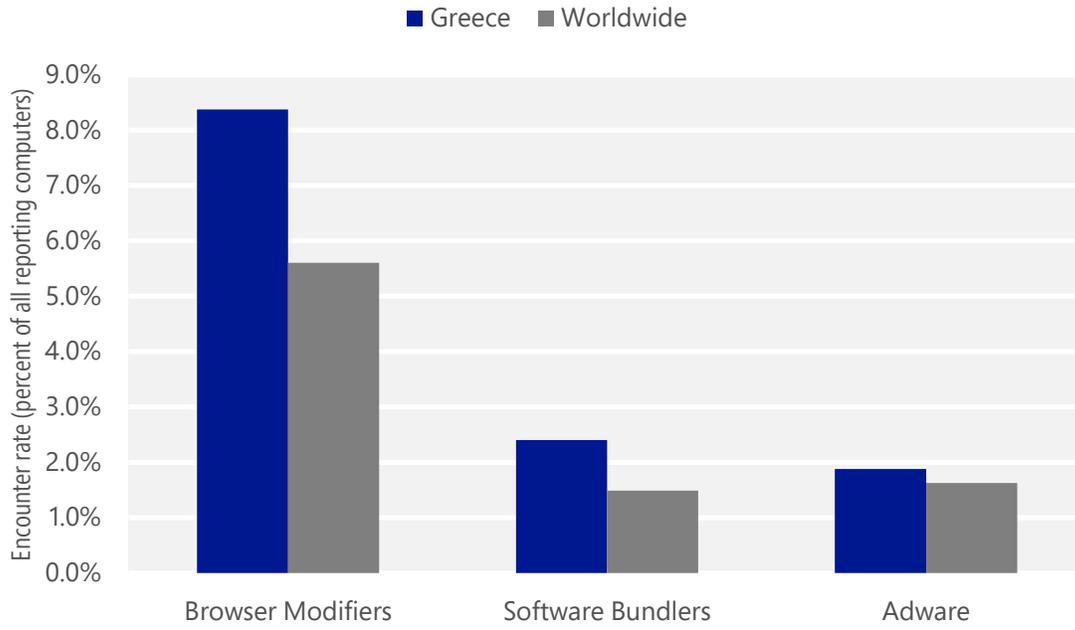
Malware encountered in Greece in 2Q15, by category



- The most common malware category in Greece in 2Q15 was Trojans. It was encountered by 4.2 percent of all computers there, up from 4.1 percent in 1Q15.
- The second most common malware category in Greece in 2Q15 was Exploits. It was encountered by 2.2 percent of all computers there, down from 2.6 percent in 1Q15.
- The third most common malware category in Greece in 2Q15 was Worms, which was encountered by 1.7 percent of all computers there, down from 2.1 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Greece in 2Q15, by category



- The most common unwanted software category in Greece in 2Q15 was Browser Modifiers. It was encountered by 8.4 percent of all computers there, down from 14.1 percent in 1Q15.
- The second most common unwanted software category in Greece in 2Q15 was Software Bundlers. It was encountered by 2.4 percent of all computers there, down from 5.1 percent in 1Q15.
- The third most common unwanted software category in Greece in 2Q15 was Adware, which was encountered by 1.9 percent of all computers there, up from 0.9 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Greece in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Kilim	Trojans	1.4%
2	JS/Axpergle	Exploits	1.2%
3	Win32/Obfuscator	Obfuscators & Injectors	1.2%
4	Win32/Skeeyah	Trojans	0.8%
5	INF/Autorun	Obfuscators & Injectors	0.6%
6	JS/Neclu	Exploits	0.5%
7	Win32/Peals	Trojans	0.4%
8	Win32/Sdbby	Exploits	0.4%
9	Win32/Gamarue	Worms	0.3%
10	Win32/Conficker	Worms	0.3%

- The most common malware family encountered in Greece in 2Q15 was [Win32/Kilim](#), which was encountered by 1.4 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The second most common malware family encountered in Greece in 2Q15 was [JS/Axpergle](#), which was encountered by 1.2 percent of reporting computers there. [JS/Axpergle](#) is a detection for the Angler exploit kit, which exploits vulnerabilities in recent versions of Internet Explorer, Silverlight, Adobe Flash Player, and Java to install malware.
- The third most common malware family encountered in Greece in 2Q15 was [Win32/Obfuscator](#), which was encountered by 1.2 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The fourth most common malware family encountered in Greece in 2Q15 was [Win32/Skeeyah](#), which was encountered by 0.8 percent of reporting computers there. [Win32/Skeeyah](#) is a generic detection for various threats that display trojan characteristics.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Greece in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	4.7%
2	Win32/KipodToolsCby	Browser Modifiers	3.2%
3	Win32/InstalleRex	Software Bundlers	2.3%
4	Win32/SaverExtension	Adware	1.4%
5	Win32/AlterbookSP	Browser Modifiers	0.6%

- The most common unwanted software family encountered in Greece in 2Q15 was [Win32/CouponRuc](#), which was encountered by 4.7 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in Greece in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 3.2 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common unwanted software family encountered in Greece in 2Q15 was [Win32/InstalleRex](#), which was encountered by 2.3 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Greece in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	3.2
2	Win32/CompromisedCert	Other Malware	2.5
3	Win32/Kilim	Trojans	1.5
4	Win32/Sality	Viruses	0.5
5	Win32/Brontok	Worms	0.3
6	Win32/Simda	Trojans	0.2
7	Win32/Gamarue	Worms	0.2
8	VBS/Jenxcus	Worms	0.2
9	Win32/Vobfus	Worms	0.2
10	MSIL/Bladabindi	Backdoors	0.2

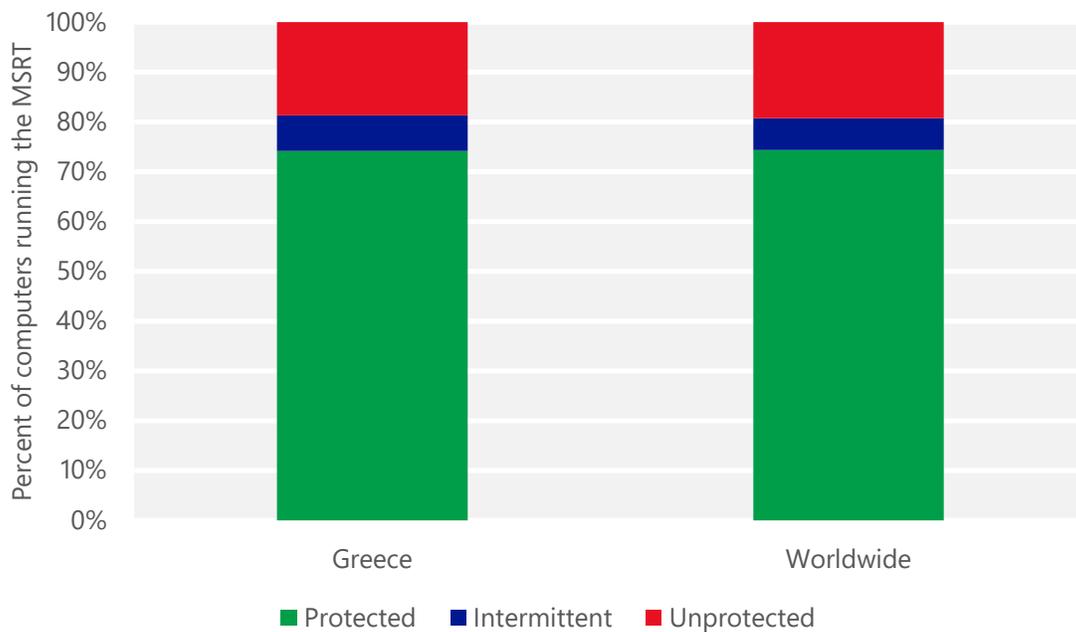
- The most common threat family infecting computers in Greece in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 3.2 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Greece in 2Q15 was [Win32/CompromisedCert](#), which was detected and removed from 2.5 of every 1,000 unique computers scanned by the MSRT. [Win32/CompromisedCert](#) is a detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.
- The third most common threat family infecting computers in Greece in 2Q15 was [Win32/Kilim](#), which was detected and removed from 1.5 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The fourth most common threat family infecting computers in Greece in 2Q15 was [Win32/Sality](#), which was detected and removed from 0.5 of every 1,000 unique computers scanned by the MSRT. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Greece and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Greece

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.26 (0.28)	0.12 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	4.47 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	6.61 (16.7)	

Guatemala

The statistics presented here are generated by Microsoft security programs and services running on computers in Guatemala in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Guatemala

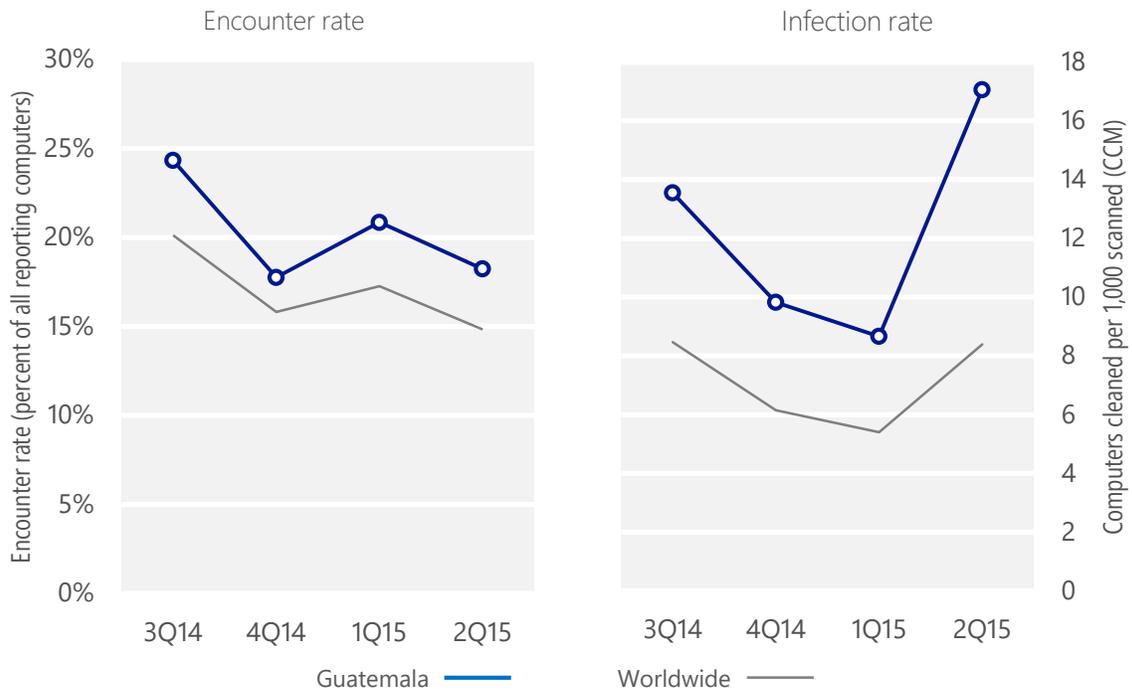
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Guatemala	24.3%	17.8%	20.9%	18.2%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Guatemala	13.5	9.8	8.7	17.1
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcout, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 18.2% of computers in Guatemala encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 17.1 of every 1,000 unique computers scanned in Guatemala in 2Q15 (a CCM score of 17.1, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Guatemala over the last four quarters, compared to the world as a whole.

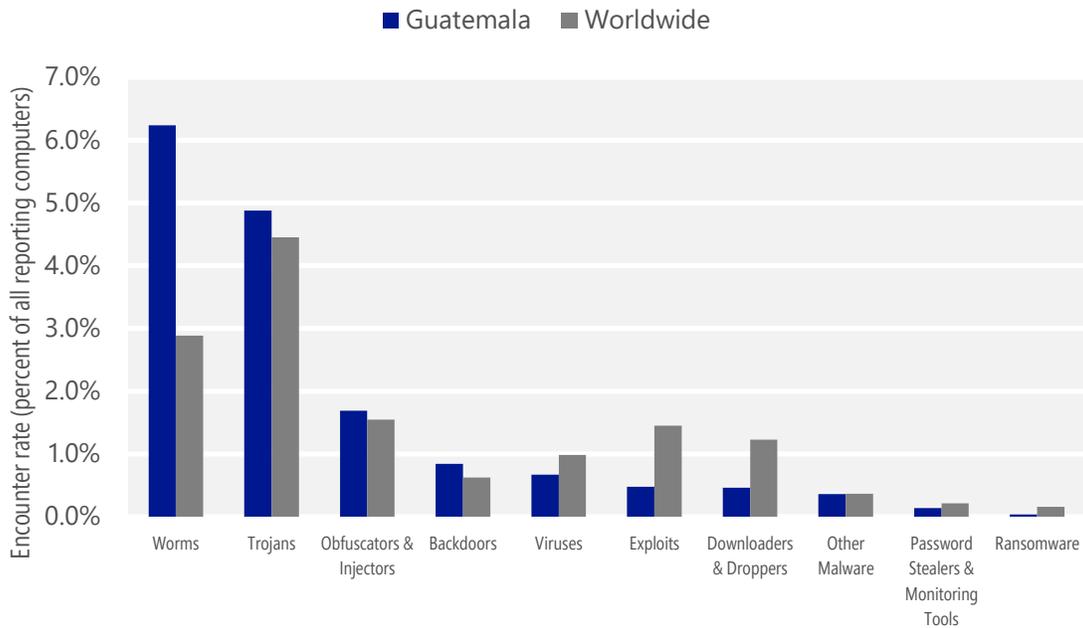
Malware encounter and infection rate trends in Guatemala and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in Guatemala and around the world, and for explanations of the methods and terms used here.

Malware categories

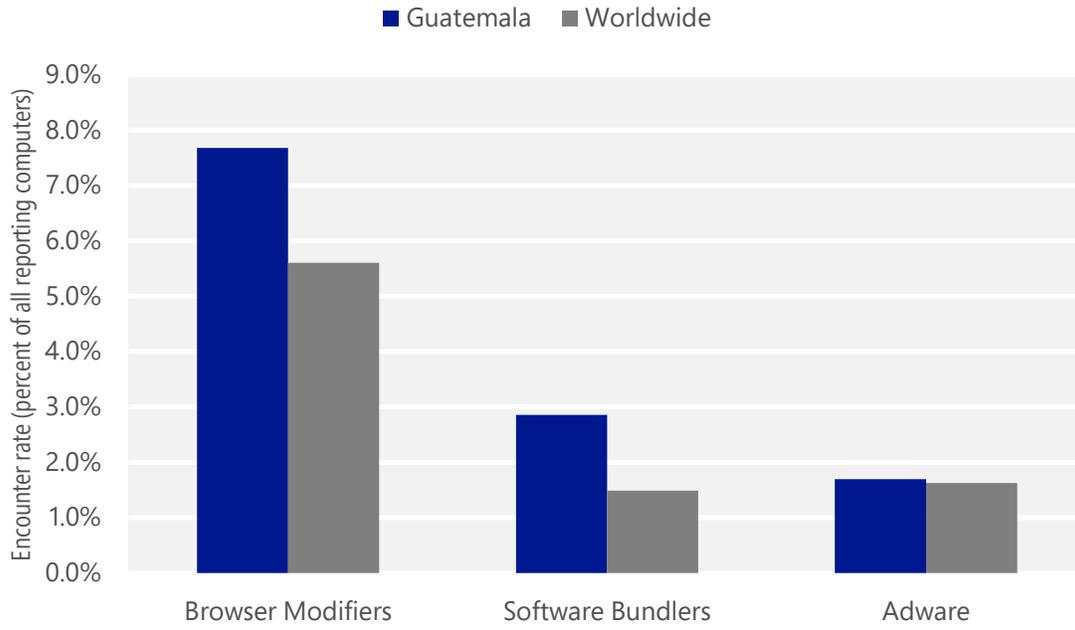
Malware encountered in Guatemala in 2Q15, by category



- The most common malware category in Guatemala in 2Q15 was Worms. It was encountered by 6.2 percent of all computers there, down from 6.4 percent in 1Q15.
- The second most common malware category in Guatemala in 2Q15 was Trojans. It was encountered by 4.9 percent of all computers there, up from 3.0 percent in 1Q15.
- The third most common malware category in Guatemala in 2Q15 was Obfuscators & Injectors, which was encountered by 1.7 percent of all computers there, down from 2.1 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Guatemala in 2Q15, by category



- The most common unwanted software category in Guatemala in 2Q15 was Browser Modifiers. It was encountered by 7.7 percent of all computers there, down from 10.8 percent in 1Q15.
- The second most common unwanted software category in Guatemala in 2Q15 was Software Bundlers. It was encountered by 2.9 percent of all computers there, down from 4.2 percent in 1Q15.
- The third most common unwanted software category in Guatemala in 2Q15 was Adware, which was encountered by 1.7 percent of all computers there, up from 0.7 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Guatemala in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Gamarue	Worms	2.0%
2	VBS/Jenxcus	Worms	1.4%
3	INF/Autorun	Obfuscators & Injectors	1.0%
4	Win32/Vobfus	Worms	1.0%
5	JS/Proslikefan	Worms	1.0%
6	Win32/Kilim	Trojans	0.9%
7	Win32/Obfuscator	Obfuscators & Injectors	0.7%
8	Win32/Skeeyah	Trojans	0.5%
9	Win32/Caphaw	Backdoors	0.5%
10	Win32/Vermis	Worms	0.5%

- The most common malware family encountered in Guatemala in 2Q15 was [Win32/Gamarue](#), which was encountered by 2.0 percent of reporting computers there. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The second most common malware family encountered in Guatemala in 2Q15 was [VBS/Jenxcus](#), which was encountered by 1.4 percent of reporting computers there. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The third most common malware family encountered in Guatemala in 2Q15 was [INF/Autorun](#), which was encountered by 1.0 percent of reporting computers there. [INF/Autorun](#) is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The fourth most common malware family encountered in Guatemala in 2Q15 was [Win32/Vobfus](#), which was encountered by 1.0 percent of reporting computers there. [Win32/Vobfus](#) is a family of worms that spreads via network drives and removable drives and download/executes arbitrary files. Downloaded files may include additional malware.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Guatemala in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	4.0%
2	Win32/KipodToolsCby	Browser Modifiers	3.4%
3	Win32/InstalleRex	Software Bundlers	2.7%
4	Win32/SaverExtension	Adware	1.3%
5	Win32/AlterbookSP	Browser Modifiers	0.3%

- The most common unwanted software family encountered in Guatemala in 2Q15 was [Win32/CouponRuc](#), which was encountered by 4.0 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in Guatemala in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 3.4 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common unwanted software family encountered in Guatemala in 2Q15 was [Win32/InstalleRex](#), which was encountered by 2.7 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Guatemala in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	6.8
2	VBS/Jenxcus	Worms	2.4
3	Win32/Gamarue	Worms	2.0
4	Win32/Kilim	Trojans	1.4
5	Win32/Vobfus	Worms	1.4
6	Win32/Dorkbot	Worms	0.8
7	Win32/Sality	Viruses	0.8
8	Win32/Brontok	Worms	0.6
9	Win32/Lethic	Trojans	0.2
10	Win32/CompromisedCert	Other Malware	0.2

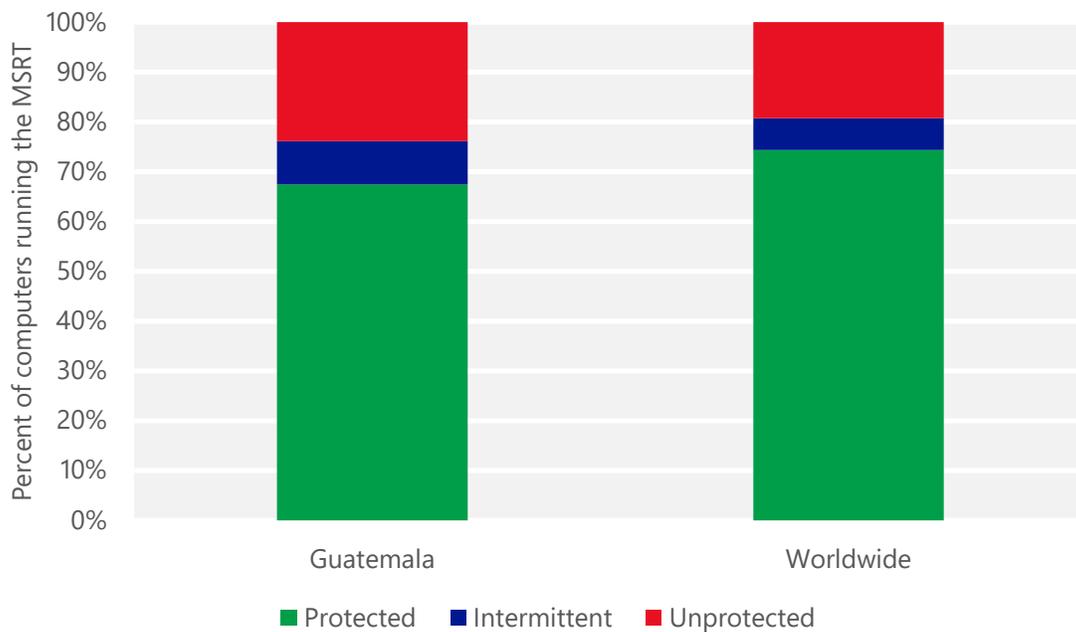
- The most common threat family infecting computers in Guatemala in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 6.8 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Guatemala in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 2.4 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The third most common threat family infecting computers in Guatemala in 2Q15 was [Win32/Gamarue](#), which was detected and removed from 2.0 of every 1,000 unique computers scanned by the MSRT. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The fourth most common threat family infecting computers in Guatemala in 2Q15 was [Win32/Kilim](#), which was detected and removed from 1.4 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Guatemala and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Guatemala

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.00 (0.28)	0.36 (0.24)
Phishing sites per 1,000 hosts (Worldwide)		2.08 (5.0)
Malware hosting sites per 1,000 hosts (Worldwide)		6.23 (16.7)

Honduras

The statistics presented here are generated by Microsoft security programs and services running on computers in Honduras in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Honduras

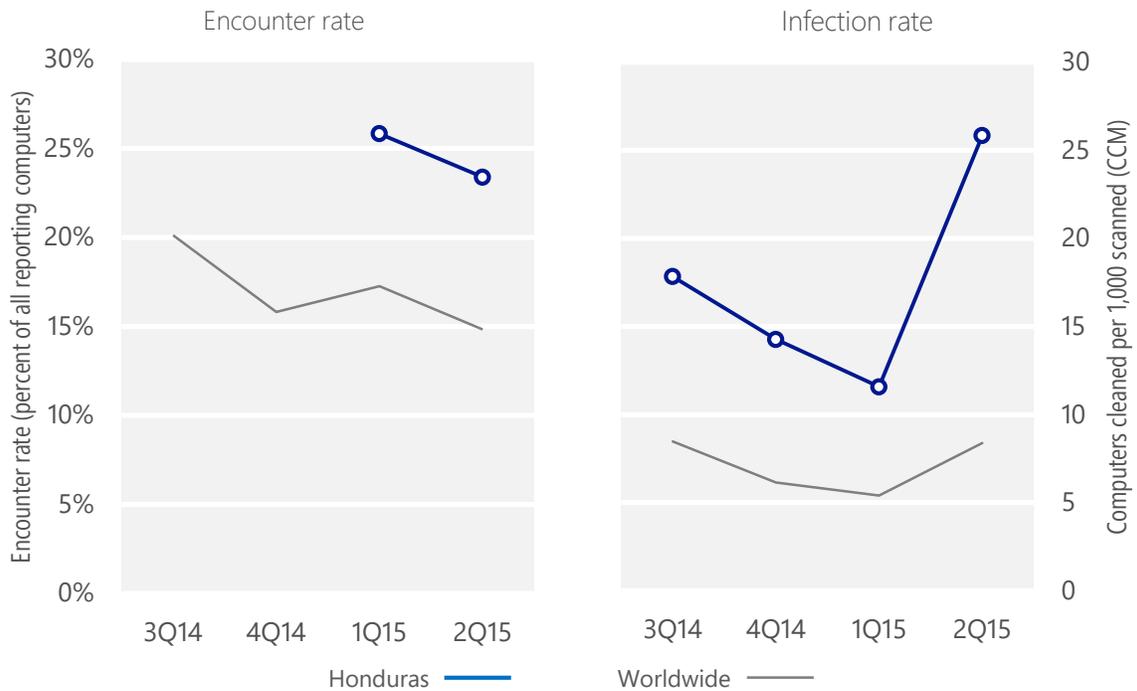
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Honduras	N/A	N/A	25.8%	23.4%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Honduras	17.8	14.3	11.6	25.8
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcote, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 23.4% of computers in Honduras encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 25.8 of every 1,000 unique computers scanned in Honduras in 2Q15 (a CCM score of 25.8, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Honduras over the last four quarters, compared to the world as a whole.

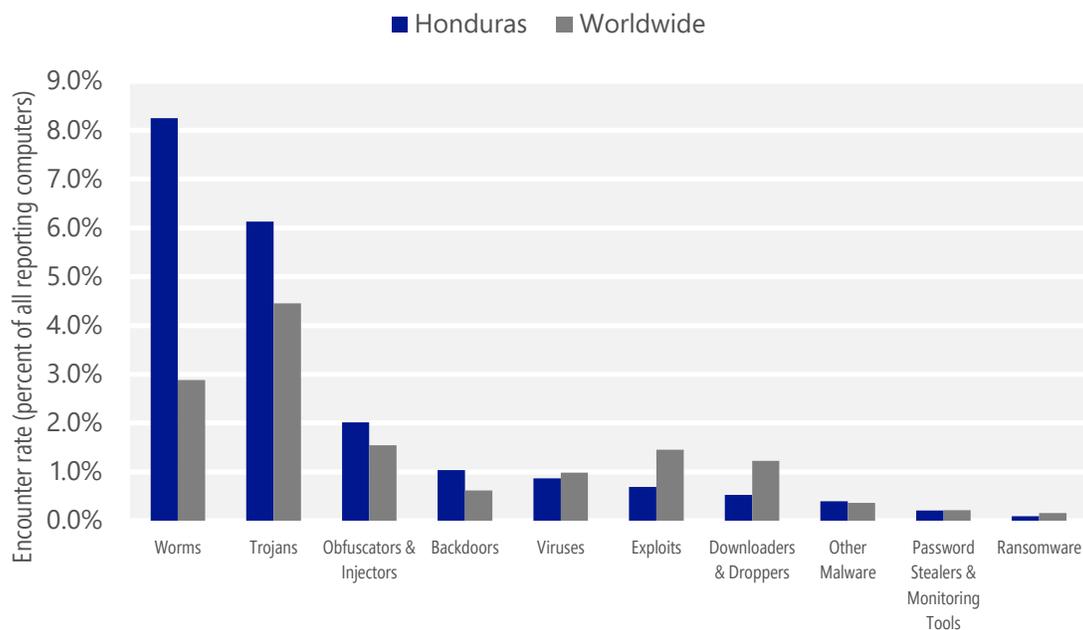
Malware encounter and infection rate trends in Honduras and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in Honduras and around the world, and for explanations of the methods and terms used here.

Malware categories

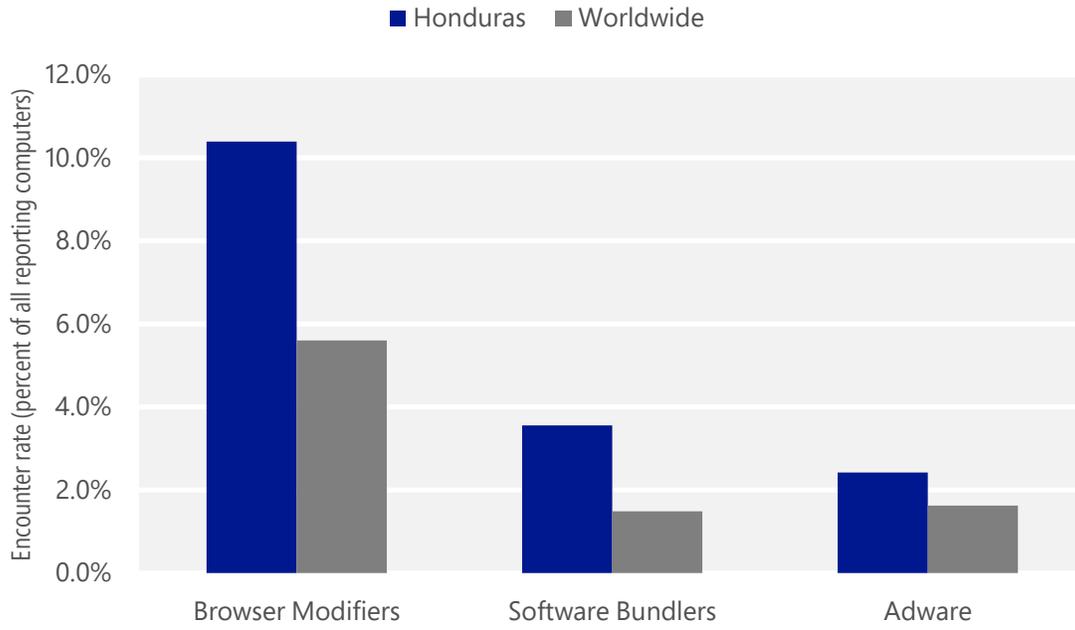
Malware encountered in Honduras in 2Q15, by category



- The most common malware category in Honduras in 2Q15 was Worms. It was encountered by 8.2 percent of all computers there, up from 7.6 percent in 1Q15.
- The second most common malware category in Honduras in 2Q15 was Trojans. It was encountered by 6.1 percent of all computers there, up from 3.5 percent in 1Q15.
- The third most common malware category in Honduras in 2Q15 was Obfuscators & Injectors, which was encountered by 2.0 percent of all computers there, down from 2.4 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Honduras in 2Q15, by category



- The most common unwanted software category in Honduras in 2Q15 was Browser Modifiers. It was encountered by 10.4 percent of all computers there, down from 14.8 percent in 1Q15.
- The second most common unwanted software category in Honduras in 2Q15 was Software Bundlers. It was encountered by 3.6 percent of all computers there, down from 5.8 percent in 1Q15.
- The third most common unwanted software category in Honduras in 2Q15 was Adware, which was encountered by 2.4 percent of all computers there, up from 0.9 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Honduras in 2Q15

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	<0.1%
2	Win32/Gamarue	Worms	<0.1%
3	INF/Autorun	Obfuscators & Injectors	<0.1%
4	Win32/Kilim	Trojans	<0.1%
5	Win32/Obfuscator	Obfuscators & Injectors	<0.1%
6	Win32/Skeeyah	Trojans	<0.1%
7	Win32/Nuqel	Worms	<0.1%
8	Win32/Caphaw	Backdoors	<0.1%
9	Win32/Yeltminky	Worms	<0.1%
10	Win32/Dorkbot	Worms	<0.1%

- The most common malware family encountered in Honduras in 2Q15 was [VBS/Jenxcus](#), which was encountered by <0.1 percent of reporting computers there. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common malware family encountered in Honduras in 2Q15 was [Win32/Gamarue](#), which was encountered by <0.1 percent of reporting computers there. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The third most common malware family encountered in Honduras in 2Q15 was [INF/Autorun](#), which was encountered by <0.1 percent of reporting computers there. [INF/Autorun](#) is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The fourth most common malware family encountered in Honduras in 2Q15 was [Win32/Kilim](#), which was encountered by <0.1 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Honduras in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	0.1%
2	Win32/KipodToolsCby	Browser Modifiers	0.1%
3	Win32/InstalleRex	Software Bundlers	<0.1%
4	Win32/SaverExtension	Adware	<0.1%
5	Win32/AlterbookSP	Browser Modifiers	<0.1%

- The most common unwanted software family encountered in Honduras in 2Q15 was [Win32/CouponRuc](#), which was encountered by 0.1 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in Honduras in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 0.1 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common unwanted software family encountered in Honduras in 2Q15 was [Win32/InstalleRex](#), which was encountered by <0.1 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Honduras in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	8.8
2	Win32/leEnablerCby	Browser Modifiers	8.6
3	Win32/Gamarue	Worms	1.9
4	Win32/Kilim	Trojans	1.7
5	Win32/Sality	Viruses	1.0
6	Win32/Dorkbot	Worms	0.9
7	Win32/Yeltminky	Worms	0.8
8	Win32/Nuqel	Worms	0.7
9	Win32/Brontok	Worms	0.5
10	Win32/Vobfus	Worms	0.5

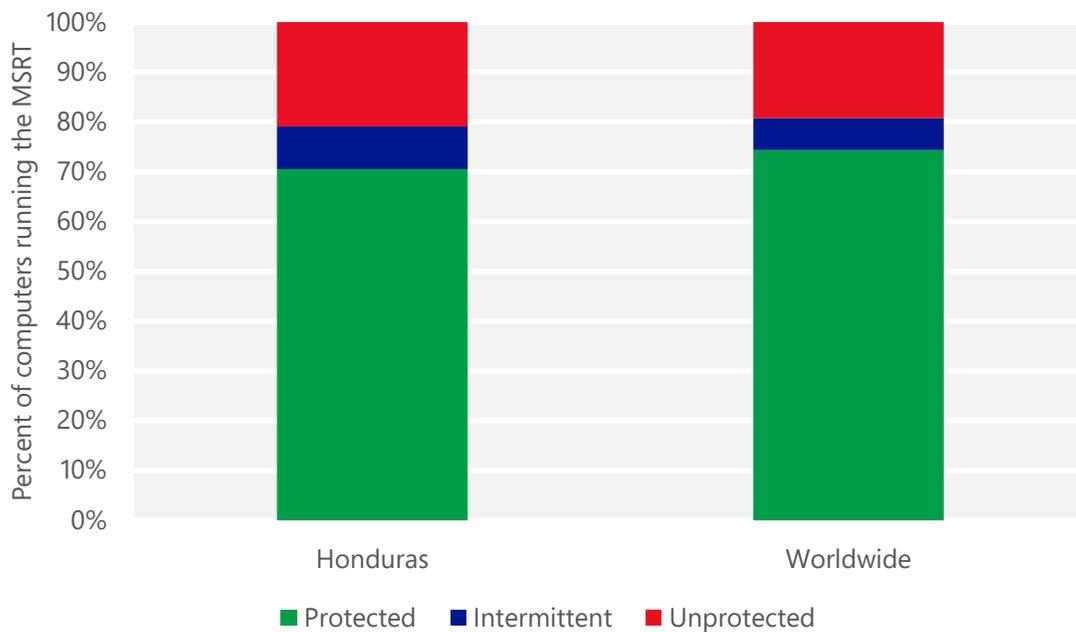
- The most common threat family infecting computers in Honduras in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 8.8 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Honduras in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 8.6 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common threat family infecting computers in Honduras in 2Q15 was [Win32/Gamarue](#), which was detected and removed from 1.9 of every 1,000 unique computers scanned by the MSRT. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The fourth most common threat family infecting computers in Honduras in 2Q15 was [Win32/Kilim](#), which was detected and removed from 1.7 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Honduras and worldwide protected by real-time security software in 2Q15



Hong Kong S.A.R.

The statistics presented here are generated by Microsoft security programs and services running on computers in Hong Kong S.A.R. in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Hong Kong S.A.R.

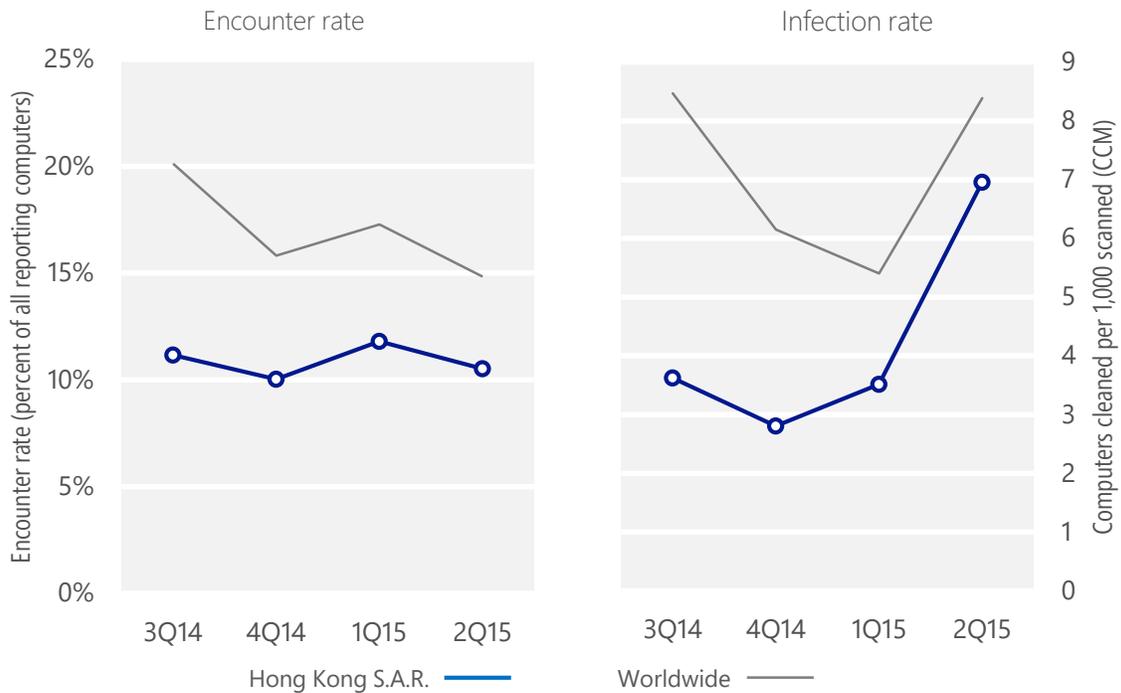
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Hong Kong S.A.R.	11.2%	10.0%	11.8%	10.5%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Hong Kong S.A.R.	3.6	2.8	3.5	7.0
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcoute, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 10.5% of computers in Hong Kong S.A.R. encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 7.0 of every 1,000 unique computers scanned in Hong Kong S.A.R. in 2Q15 (a CCM score of 7.0, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Hong Kong S.A.R. over the last four quarters, compared to the world as a whole.

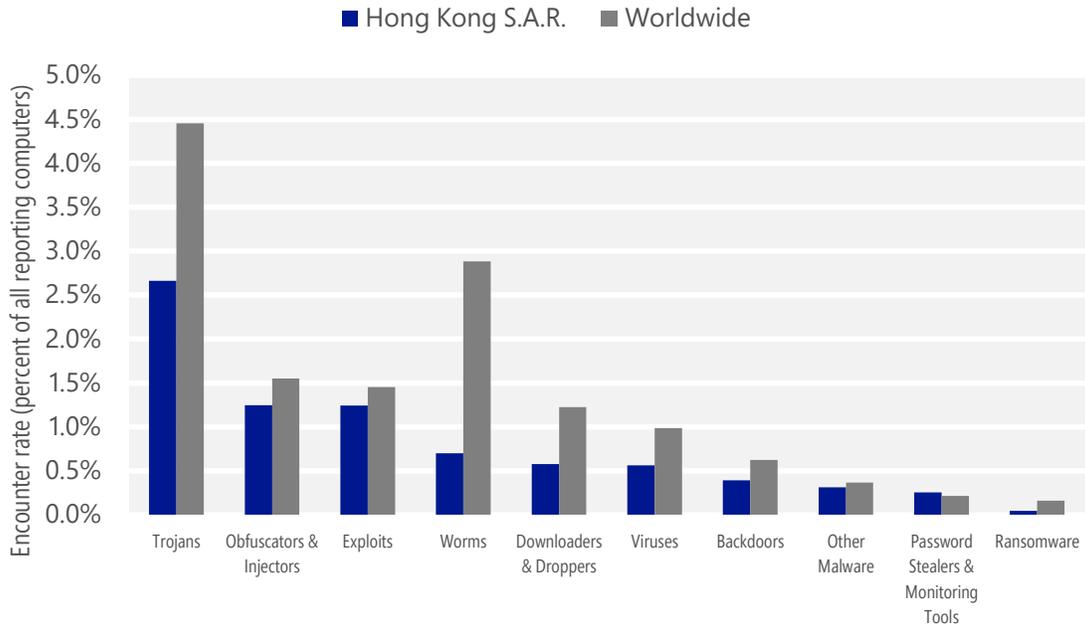
Malware encounter and infection rate trends in Hong Kong S.A.R. and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in Hong Kong S.A.R. and around the world, and for explanations of the methods and terms used here.

Malware categories

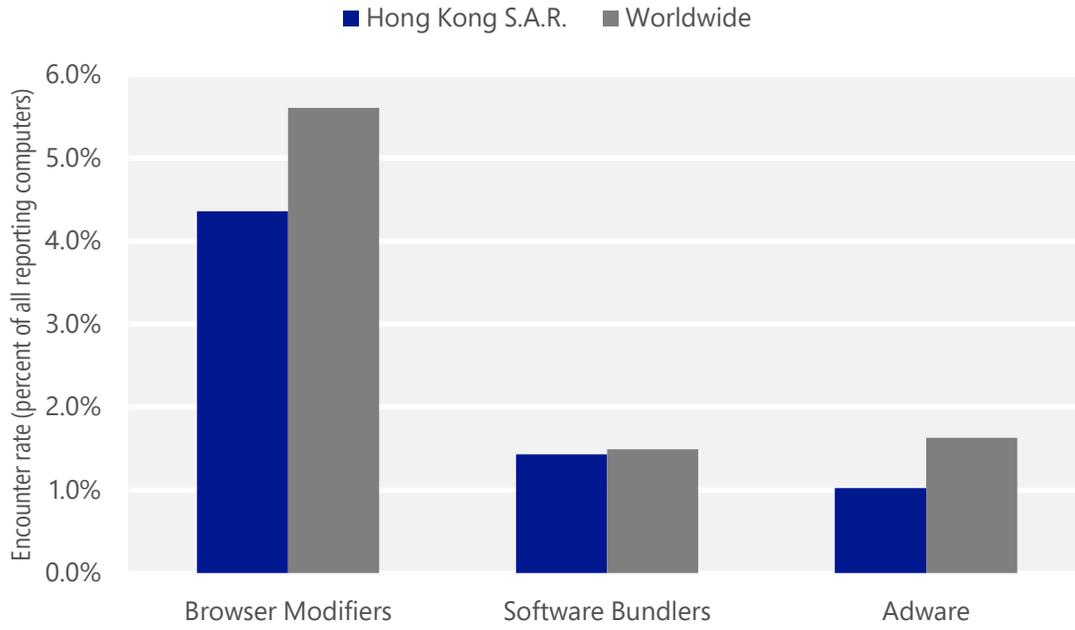
Malware encountered in Hong Kong S.A.R. in 2Q15, by category



- The most common malware category in Hong Kong S.A.R. in 2Q15 was Trojans. It was encountered by 2.7 percent of all computers there, up from 2.0 percent in 1Q15.
- The second most common malware category in Hong Kong S.A.R. in 2Q15 was Obfuscators & Injectors. It was encountered by 1.2 percent of all computers there, down from 1.3 percent in 1Q15.
- The third most common malware category in Hong Kong S.A.R. in 2Q15 was Exploits, which was encountered by 1.2 percent of all computers there, up from 1.0 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Hong Kong S.A.R. in 2Q15, by category



- The most common unwanted software category in Hong Kong S.A.R. in 2Q15 was Browser Modifiers. It was encountered by 4.4 percent of all computers there, down from 6.0 percent in 1Q15.
- The second most common unwanted software category in Hong Kong S.A.R. in 2Q15 was Software Bundlers. It was encountered by 1.4 percent of all computers there, down from 2.6 percent in 1Q15.
- The third most common unwanted software category in Hong Kong S.A.R. in 2Q15 was Adware, which was encountered by 1.0 percent of all computers there, up from 0.4 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Hong Kong S.A.R. in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Obfuscator	Obfuscators & Injectors	0.9%
2	JS/Neclu	Exploits	0.6%
3	Win32/Kilim	Trojans	0.5%
4	JS/Axpergle	Exploits	0.5%
5	Win32/Skeeyah	Trojans	0.5%
6	INF/Autorun	Obfuscators & Injectors	0.3%
7	Win32/Peals	Trojans	0.2%
8	Win32/Dynamer	Trojans	0.2%
9	Win32/Ramnit	Trojans	0.2%
10	Win32/CompromisedCert	Other Malware	0.1%

- The most common malware family encountered in Hong Kong S.A.R. in 2Q15 was [Win32/Obfuscator](#), which was encountered by 0.9 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The second most common malware family encountered in Hong Kong S.A.R. in 2Q15 was [JS/Neclu](#), which was encountered by 0.6 percent of reporting computers there. [JS/Neclu](#) is a detection for the Nuclear exploit kit, which attempts to exploit vulnerabilities in programs such as Java and Adobe Reader to install other malware.
- The third most common malware family encountered in Hong Kong S.A.R. in 2Q15 was [Win32/Kilim](#), which was encountered by 0.5 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The fourth most common malware family encountered in Hong Kong S.A.R. in 2Q15 was [JS/Axpergle](#), which was encountered by 0.5 percent of reporting computers there. [JS/Axpergle](#) is a detection for the Angler exploit kit, which exploits vulnerabilities in recent versions of Internet Explorer, Silverlight, Adobe Flash Player, and Java to install malware.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Hong Kong S.A.R. in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	2.3%
2	Win32/KipodToolsCby	Browser Modifiers	1.5%
3	Win32/InstalleRex	Software Bundlers	1.4%
4	Win32/SaverExtension	Adware	0.8%
5	Win32/AlterbookSP	Browser Modifiers	0.5%

- The most common unwanted software family encountered in Hong Kong S.A.R. in 2Q15 was [Win32/CouponRuc](#), which was encountered by 2.3 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in Hong Kong S.A.R. in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 1.5 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common unwanted software family encountered in Hong Kong S.A.R. in 2Q15 was [Win32/InstalleRex](#), which was encountered by 1.4 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Hong Kong S.A.R. in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	1.8
2	Win32/Kilim	Trojans	1.5
3	Win32/CompromisedCert	Other Malware	1.0
4	Win32/Winnti	Trojans	0.4
5	Win32/Ramnit	Trojans	0.3
6	Win32/Nitol	Other Malware	0.3
7	Win32/Dyzap	Password Stealers & Monitoring Tools	0.1
8	Win32/Sality	Viruses	0.1
9	Win32/Conficker	Worms	0.1
10	Win32/Parite	Viruses	0.1

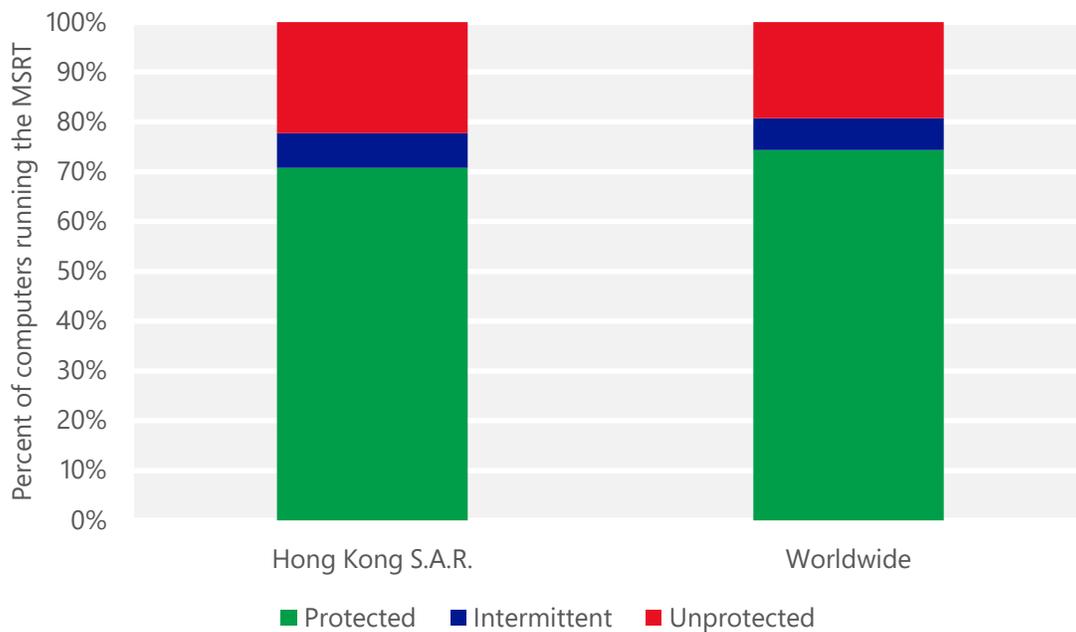
- The most common threat family infecting computers in Hong Kong S.A.R. in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 1.8 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Hong Kong S.A.R. in 2Q15 was [Win32/Kilim](#), which was detected and removed from 1.5 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The third most common threat family infecting computers in Hong Kong S.A.R. in 2Q15 was [Win32/CompromisedCert](#), which was detected and removed from 1.0 of every 1,000 unique computers scanned by the MSRT. [Win32/CompromisedCert](#) is a detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.
- The fourth most common threat family infecting computers in Hong Kong S.A.R. in 2Q15 was [Win32/Winnti](#), which was detected and removed from 0.4 of every 1,000 unique computers scanned by the MSRT. [Win32/Winnti](#) is a trojan that opens a remote connection to an attacker, who can execute remote commands on the computer, download and run other malware, delete files, and perform other malicious activities.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Hong Kong S.A.R. and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Hong Kong S.A.R.

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.22 (0.28)	0.19 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	7.02 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	6.38 (16.7)	

Hungary

The statistics presented here are generated by Microsoft security programs and services running on computers in Hungary in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Hungary

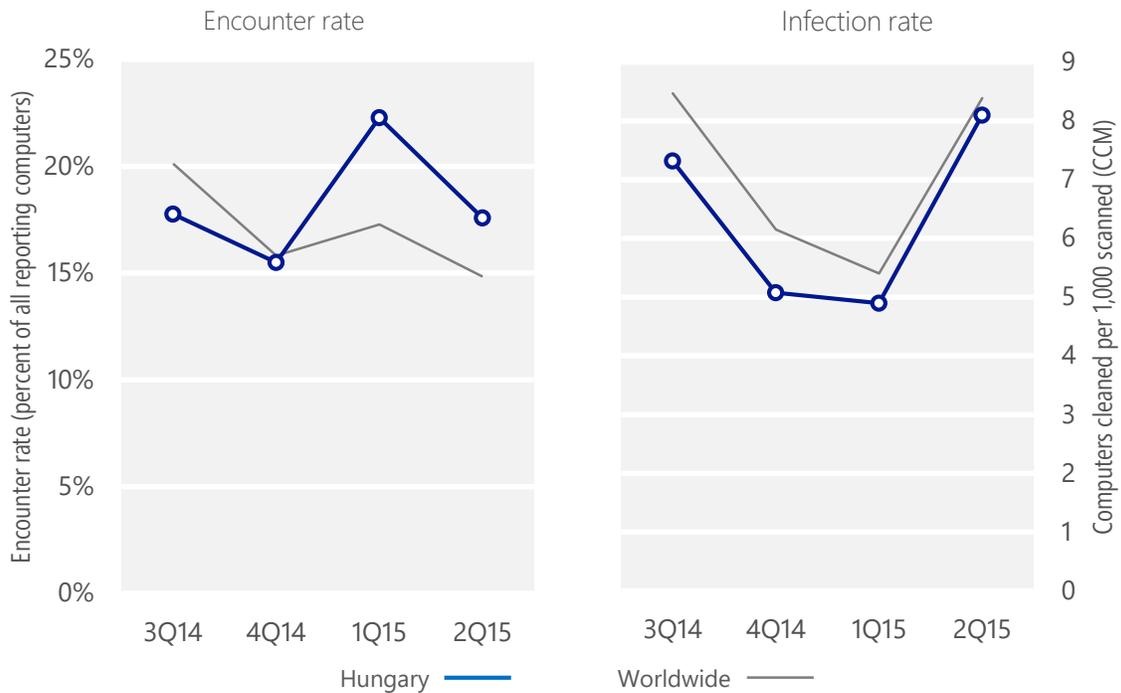
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Hungary	17.8%	15.5%	22.3%	17.6%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Hungary	7.3	5.1	4.9	8.1
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcote, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 17.6% of computers in Hungary encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 8.1 of every 1,000 unique computers scanned in Hungary in 2Q15 (a CCM score of 8.1, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Hungary over the last four quarters, compared to the world as a whole.

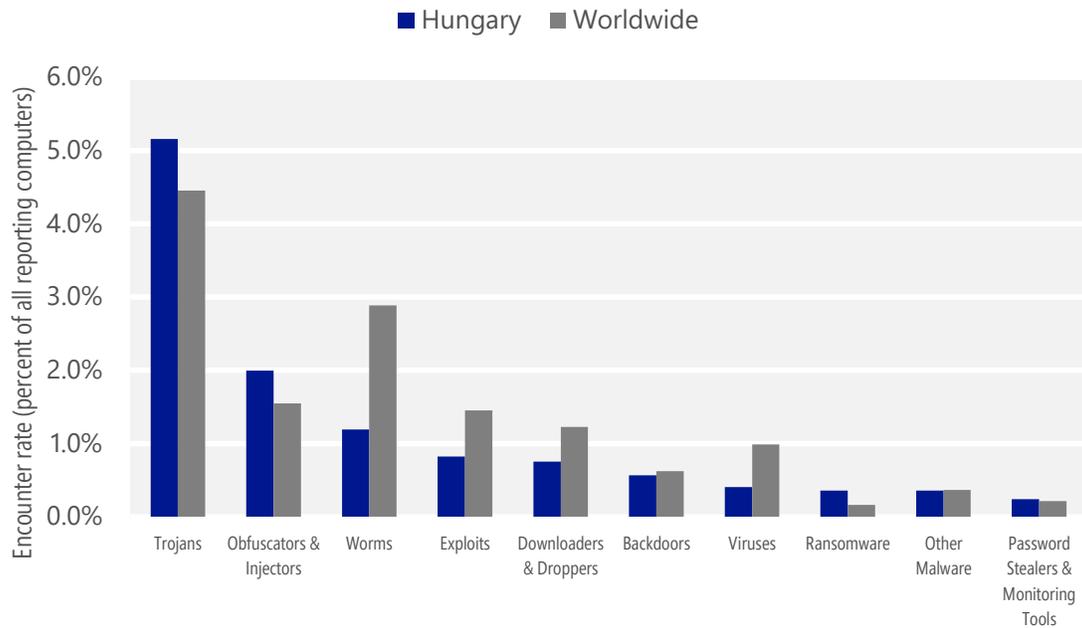
Malware encounter and infection rate trends in Hungary and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in Hungary and around the world, and for explanations of the methods and terms used here.

Malware categories

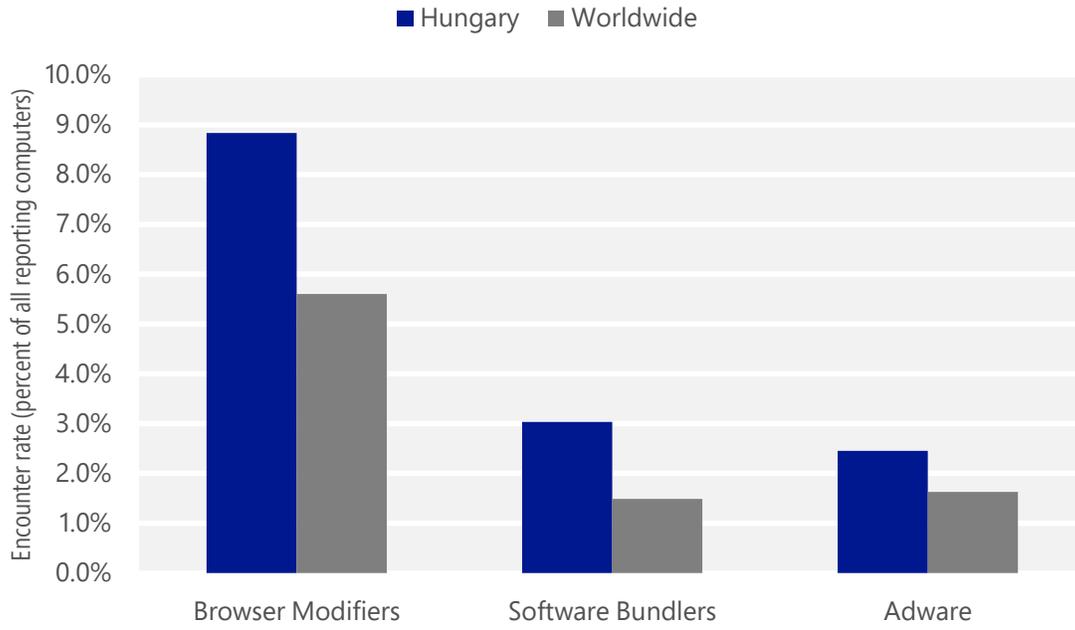
Malware encountered in Hungary in 2Q15, by category



- The most common malware category in Hungary in 2Q15 was Trojans. It was encountered by 5.2 percent of all computers there, up from 4.2 percent in 1Q15.
- The second most common malware category in Hungary in 2Q15 was Obfuscators & Injectors. It was encountered by 2.0 percent of all computers there, down from 2.2 percent in 1Q15.
- The third most common malware category in Hungary in 2Q15 was Worms, which was encountered by 1.2 percent of all computers there, down from 1.9 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Hungary in 2Q15, by category



- The most common unwanted software category in Hungary in 2Q15 was Browser Modifiers. It was encountered by 8.8 percent of all computers there, down from 12.9 percent in 1Q15.
- The second most common unwanted software category in Hungary in 2Q15 was Software Bundlers. It was encountered by 3.0 percent of all computers there, down from 5.3 percent in 1Q15.
- The third most common unwanted software category in Hungary in 2Q15 was Adware, which was encountered by 2.5 percent of all computers there, up from 0.9 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Hungary in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Obfuscator	Obfuscators & Injectors	1.6%
2	Win32/Kilim	Trojans	1.3%
3	Win32/Skeeyah	Trojans	1.0%
4	Win32/Peals	Trojans	0.4%
5	INF/Autorun	Obfuscators & Injectors	0.4%
6	JS/Axpergle	Exploits	0.4%
7	Win32/Dynamer	Trojans	0.3%
8	Win32/Crowti	Ransomware	0.3%
9	Win32/Conficker	Worms	0.3%
10	Win32/Brontok	Worms	0.3%

- The most common malware family encountered in Hungary in 2Q15 was [Win32/Obfuscator](#), which was encountered by 1.6 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The second most common malware family encountered in Hungary in 2Q15 was [Win32/Kilim](#), which was encountered by 1.3 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The third most common malware family encountered in Hungary in 2Q15 was [Win32/Skeeyah](#), which was encountered by 1.0 percent of reporting computers there. [Win32/Skeeyah](#) is a generic detection for various threats that display trojan characteristics.
- The fourth most common malware family encountered in Hungary in 2Q15 was [Win32/Peals](#), which was encountered by 0.4 percent of reporting computers there. [Win32/Peals](#) is a generic detection for various threats that display trojan characteristics.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Hungary in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	4.5%
2	Win32/KipodToolsCby	Browser Modifiers	3.3%
3	Win32/InstalleRex	Software Bundlers	3.0%
4	Win32/SaverExtension	Adware	1.4%
5	Win32/AlterbookSP	Browser Modifiers	1.3%

- The most common unwanted software family encountered in Hungary in 2Q15 was [Win32/CouponRuc](#), which was encountered by 4.5 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in Hungary in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 3.3 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common unwanted software family encountered in Hungary in 2Q15 was [Win32/InstalleRex](#), which was encountered by 3.0 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Hungary in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	3.0
2	Win32/Kilim	Trojans	1.3
3	Win32/Sality	Viruses	0.9
4	Win32/CompromisedCert	Other Malware	0.6
5	Win32/Brontok	Worms	0.6
6	Win32/Ramnit	Trojans	0.2
7	MSIL/Bladabindi	Backdoors	0.2
8	Win32/Simda	Trojans	0.2
9	Win32/Jeefo	Viruses	0.1
10	VBS/Jenxcus	Worms	0.1

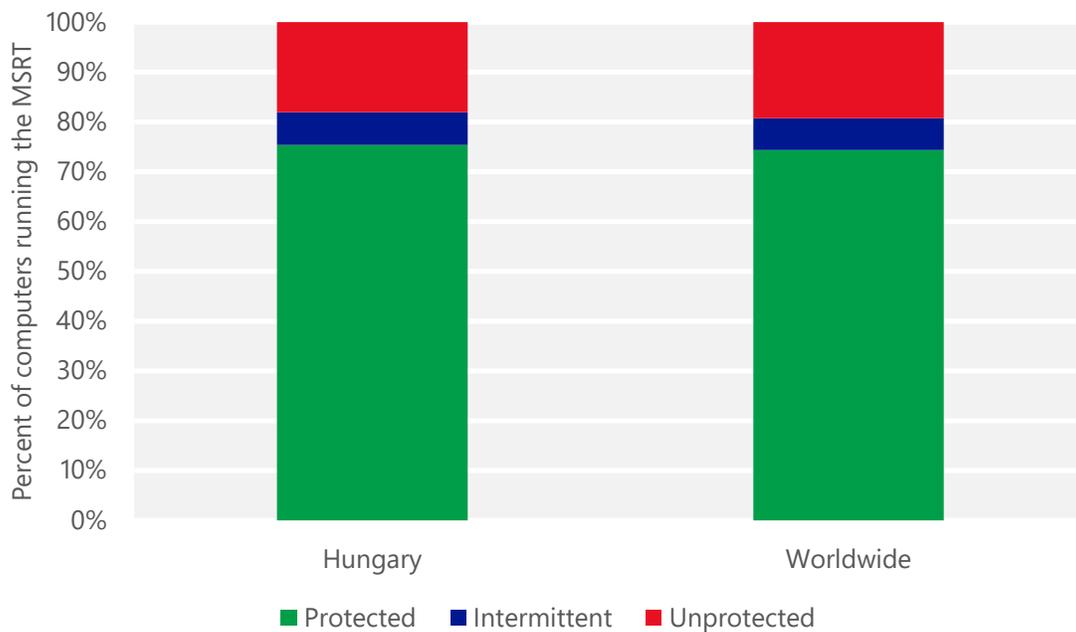
- The most common threat family infecting computers in Hungary in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 3.0 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Hungary in 2Q15 was [Win32/Kilim](#), which was detected and removed from 1.3 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The third most common threat family infecting computers in Hungary in 2Q15 was [Win32/Sality](#), which was detected and removed from 0.9 of every 1,000 unique computers scanned by the MSRT. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The fourth most common threat family infecting computers in Hungary in 2Q15 was [Win32/CompromisedCert](#), which was detected and removed from 0.6 of every 1,000 unique computers scanned by the MSRT. [Win32/CompromisedCert](#) is a detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Hungary and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Hungary

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.27 (0.28)	0.18 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	6.00 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	6.61 (16.7)	

Iceland

The statistics presented here are generated by Microsoft security programs and services running on computers in Iceland in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Iceland

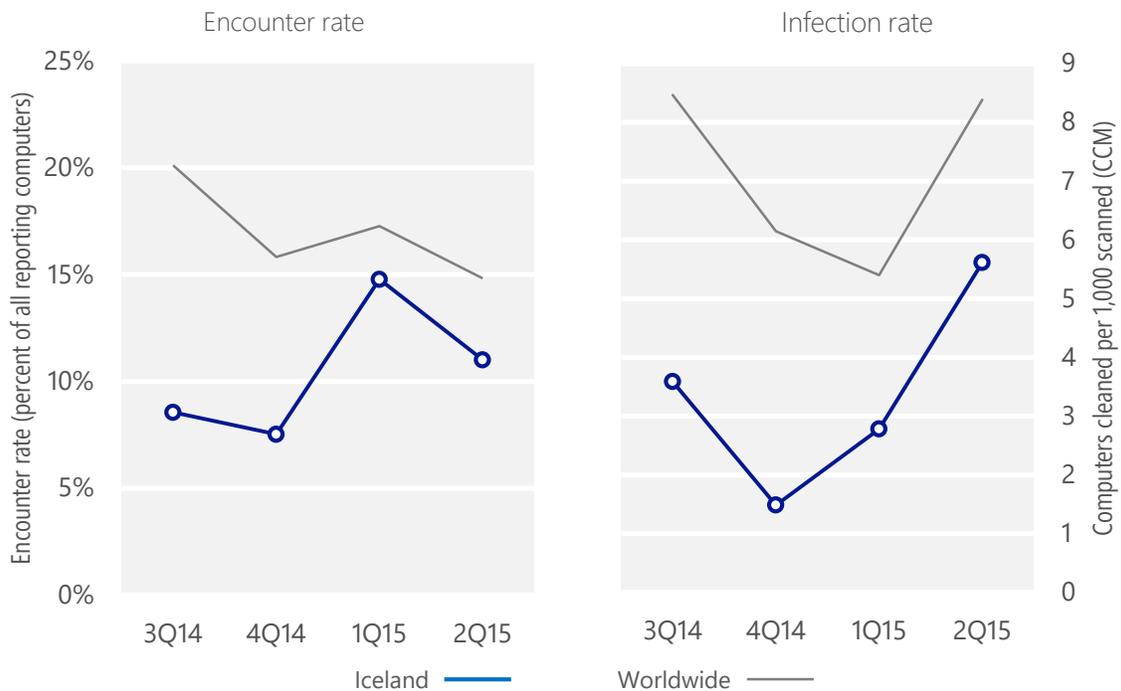
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Iceland	8.5%	7.5%	14.8%	11.0%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Iceland	3.6	1.5	2.8	5.6
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcout, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 11.0% of computers in Iceland encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 5.6 of every 1,000 unique computers scanned in Iceland in 2Q15 (a CCM score of 5.6, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Iceland over the last four quarters, compared to the world as a whole.

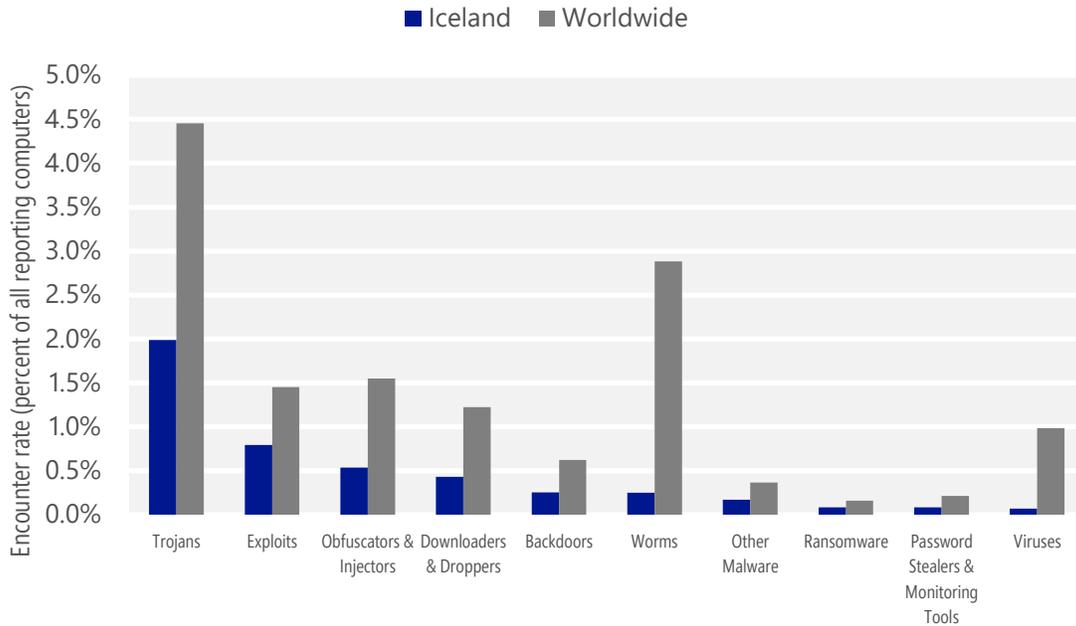
Malware encounter and infection rate trends in Iceland and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in Iceland and around the world, and for explanations of the methods and terms used here.

Malware categories

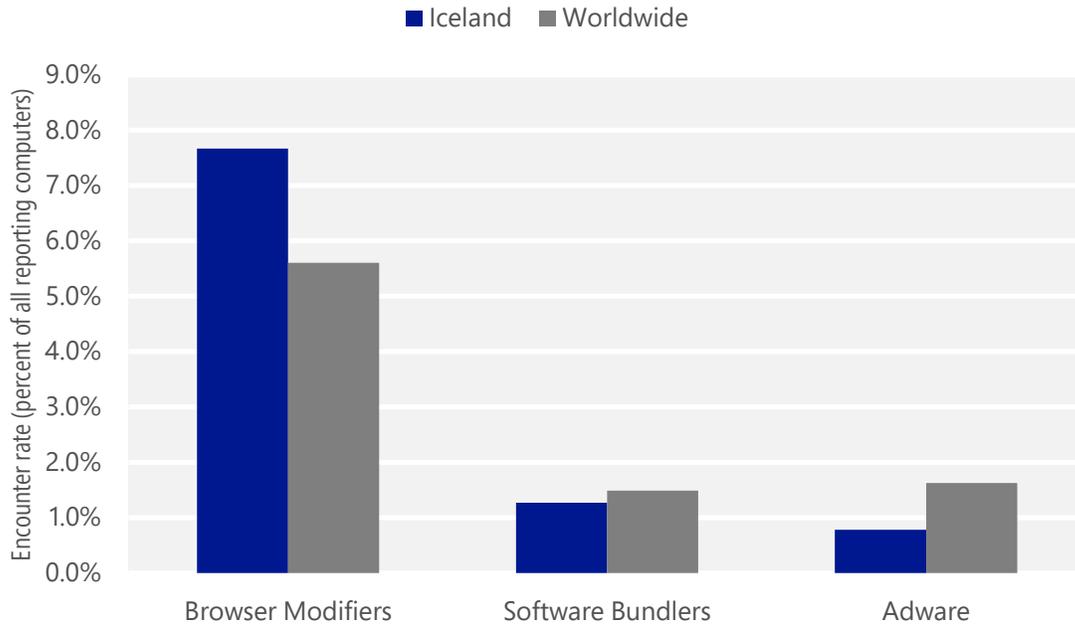
Malware encountered in Iceland in 2Q15, by category



- The most common malware category in Iceland in 2Q15 was Trojans. It was encountered by 2.0 percent of all computers there, up from 1.7 percent in 1Q15.
- The second most common malware category in Iceland in 2Q15 was Exploits. It was encountered by 0.8 percent of all computers there, down from 0.8 percent in 1Q15.
- The third most common malware category in Iceland in 2Q15 was Obfuscators & Injectors, which was encountered by 0.5 percent of all computers there, down from 0.7 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Iceland in 2Q15, by category



- The most common unwanted software category in Iceland in 2Q15 was Browser Modifiers. It was encountered by 7.7 percent of all computers there, down from 10.8 percent in 1Q15.
- The second most common unwanted software category in Iceland in 2Q15 was Software Bundlers. It was encountered by 1.3 percent of all computers there, down from 2.2 percent in 1Q15.
- The third most common unwanted software category in Iceland in 2Q15 was Adware, which was encountered by 0.8 percent of all computers there, up from 0.6 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Iceland in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Kilim	Trojans	0.7%
2	Win32/Skeeyah	Trojans	0.5%
3	Win32/Obfuscator	Obfuscators & Injectors	0.4%
4	Win32/Sdbby	Exploits	0.3%
5	JS/Axpergle	Exploits	0.3%
6	Win32/Peals	Trojans	0.2%
7	Win32/Dynamer	Trojans	0.1%
8	Win32/Fynloski	Backdoors	0.1%
9	Win32/Crowti	Ransomware	0.1%
10	Win32/Dalexis	Downloaders & Droppers	0.1%

- The most common malware family encountered in Iceland in 2Q15 was [Win32/Kilim](#), which was encountered by 0.7 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The second most common malware family encountered in Iceland in 2Q15 was [Win32/Skeeyah](#), which was encountered by 0.5 percent of reporting computers there. [Win32/Skeeyah](#) is a generic detection for various threats that display trojan characteristics.
- The third most common malware family encountered in Iceland in 2Q15 was [Win32/Obfuscator](#), which was encountered by 0.4 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The fourth most common malware family encountered in Iceland in 2Q15 was [Win32/Sdbby](#), which was encountered by 0.3 percent of reporting computers there. [Win32/Sdbby](#) is a threat that exploits a bypass to gain administrative privileges on a machine without going through a User Access Control prompt.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Iceland in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/KipodToolsCby	Browser Modifiers	4.9%
2	Win32/CouponRuc	Browser Modifiers	2.2%
3	Win32/InstalleRex	Software Bundlers	1.2%
4	Win32/SaverExtension	Adware	0.6%
5	Win32/AlterbookSP	Browser Modifiers	0.4%

- The most common unwanted software family encountered in Iceland in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 4.9 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common unwanted software family encountered in Iceland in 2Q15 was [Win32/CouponRuc](#), which was encountered by 2.2 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The third most common unwanted software family encountered in Iceland in 2Q15 was [Win32/InstalleRex](#), which was encountered by 1.2 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Iceland in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	2.1
2	Win32/CompromisedCert	Other Malware	1.6
3	Win32/Kilim	Trojans	1.1
4	Win32/Simda	Trojans	0.1
5	Win32/Alureon	Trojans	0.1
6	MSIL/Bladabindi	Backdoors	0.1
7	Win32/Conficker	Worms	<0.1
8	Win32/Sality	Viruses	<0.1
9	Win32/Carberp	Trojans	<0.1
10	Win32/Gamarue	Worms	<0.1

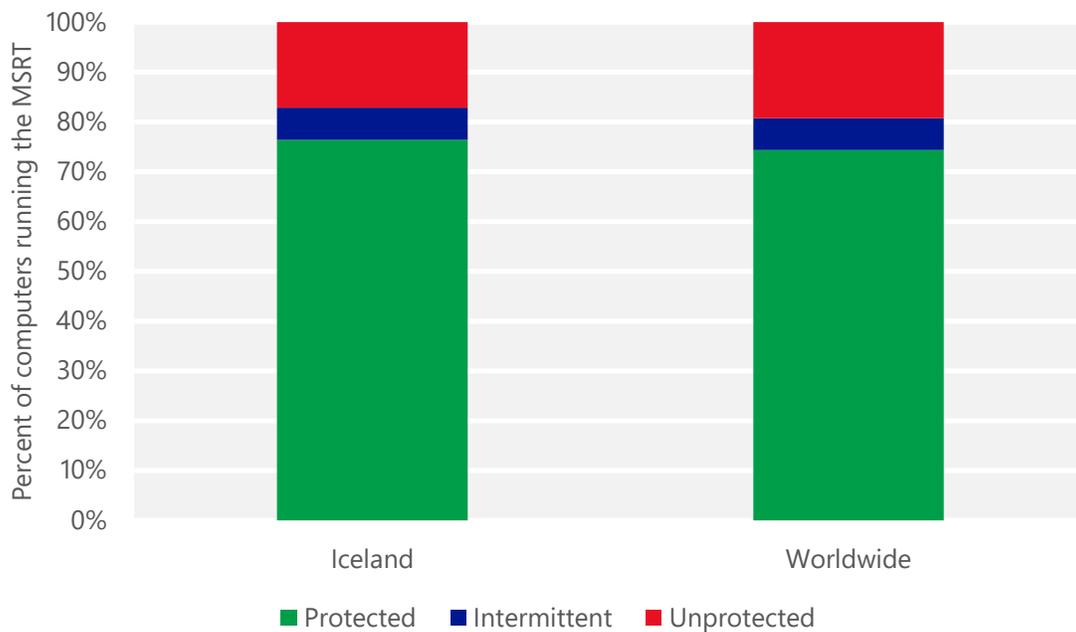
- The most common threat family infecting computers in Iceland in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 2.1 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Iceland in 2Q15 was [Win32/CompromisedCert](#), which was detected and removed from 1.6 of every 1,000 unique computers scanned by the MSRT. [Win32/CompromisedCert](#) is a detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.
- The third most common threat family infecting computers in Iceland in 2Q15 was [Win32/Kilim](#), which was detected and removed from 1.1 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The fourth most common threat family infecting computers in Iceland in 2Q15 was [Win32/Simda](#), which was detected and removed from 0.1 of every 1,000 unique computers scanned by the MSRT. [Win32/Simda](#) is a threat that can give an attacker backdoor access and control of an infected computer. It can then steal passwords and gather information about the computer to send to the attacker.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Iceland and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Iceland

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.15 (0.28)	0.13 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	5.03 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	6.81 (16.7)	

India

The statistics presented here are generated by Microsoft security programs and services running on computers in India in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for India

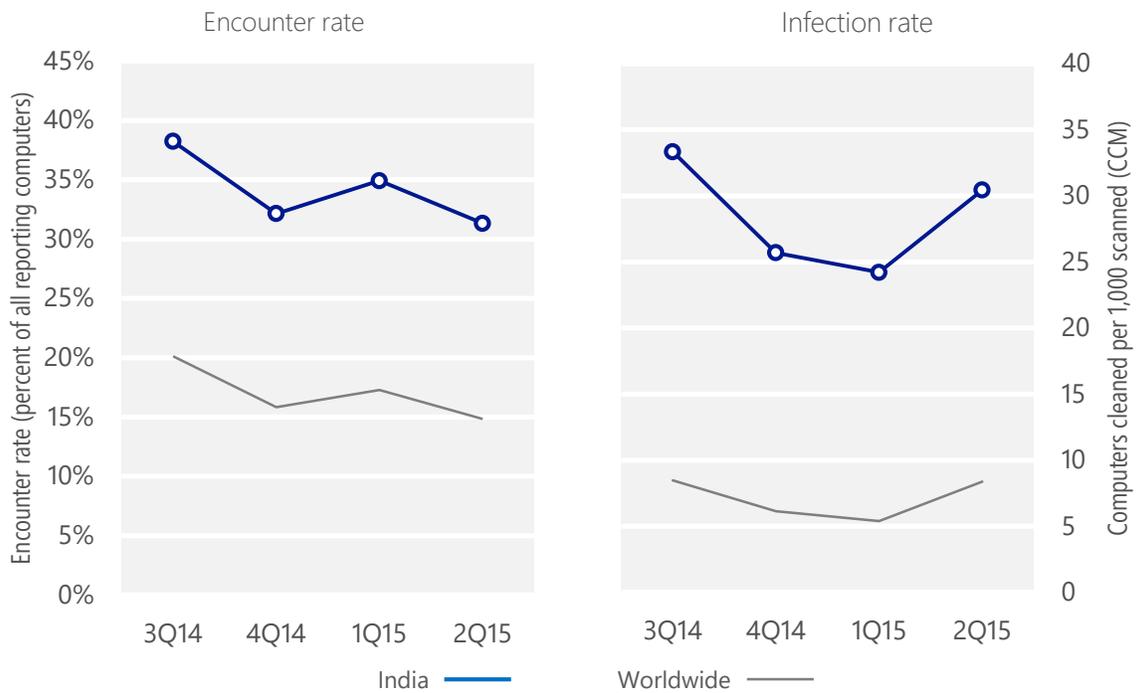
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, India	38.2%	32.1%	34.9%	31.3%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, India	33.3	25.7	24.2	30.4
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcoute, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 31.3% of computers in India encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 30.4 of every 1,000 unique computers scanned in India in 2Q15 (a CCM score of 30.4, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for India over the last four quarters, compared to the world as a whole.

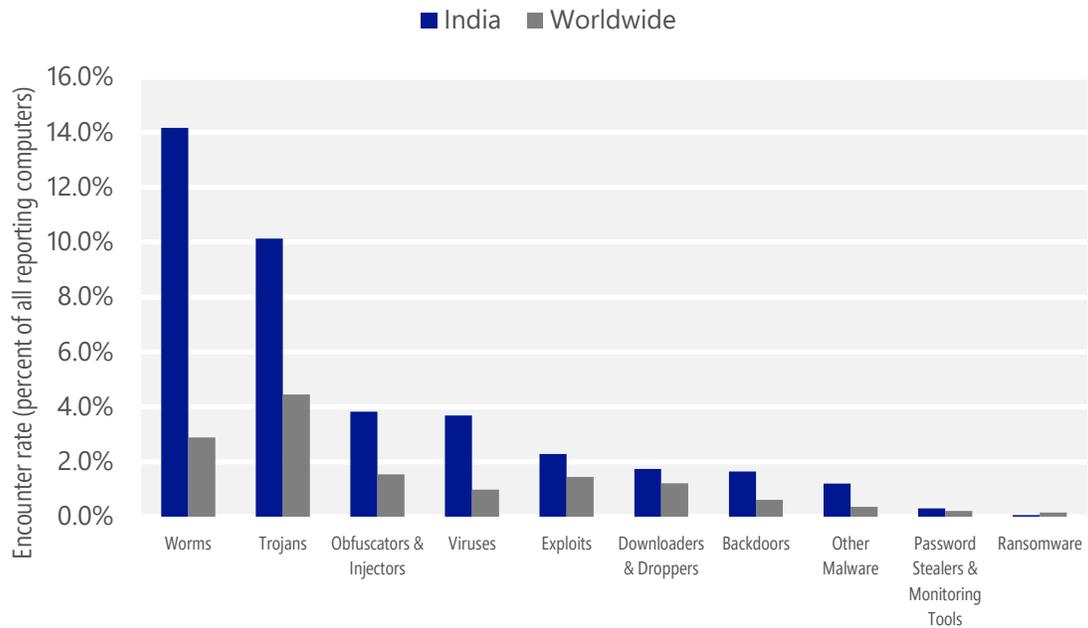
Malware encounter and infection rate trends in India and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in India and around the world, and for explanations of the methods and terms used here.

Malware categories

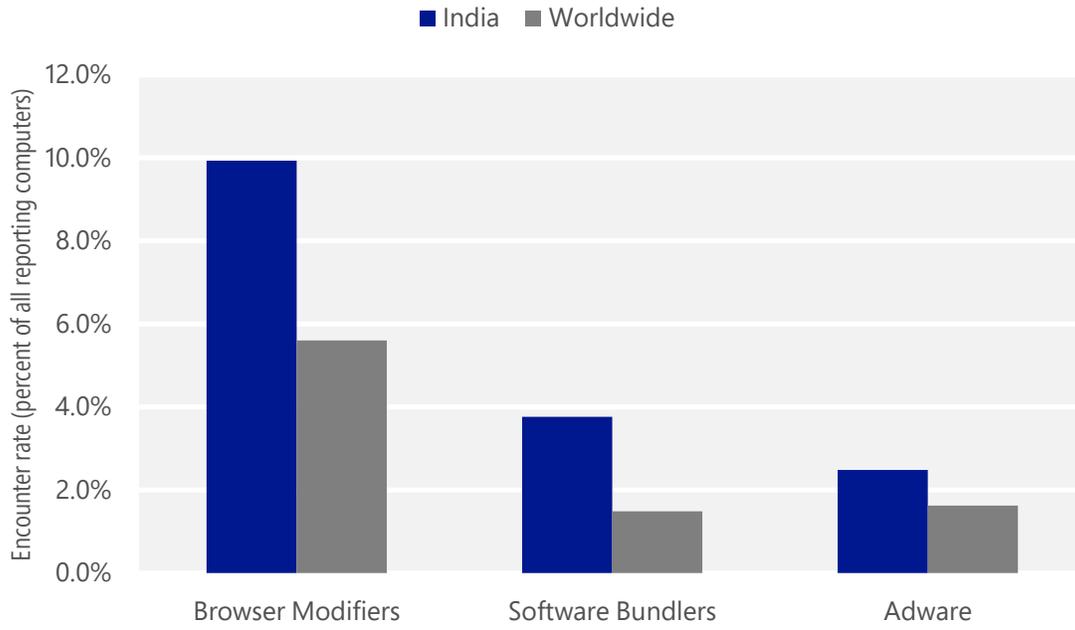
Malware encountered in India in 2Q15, by category



- The most common malware category in India in 2Q15 was Worms. It was encountered by 14.2 percent of all computers there, down from 17.0 percent in 1Q15.
- The second most common malware category in India in 2Q15 was Trojans. It was encountered by 10.1 percent of all computers there, up from 7.8 percent in 1Q15.
- The third most common malware category in India in 2Q15 was Obfuscators & Injectors, which was encountered by 3.8 percent of all computers there, down from 4.6 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in India in 2Q15, by category



- The most common unwanted software category in India in 2Q15 was Browser Modifiers. It was encountered by 9.9 percent of all computers there, down from 12.4 percent in 1Q15.
- The second most common unwanted software category in India in 2Q15 was Software Bundlers. It was encountered by 3.8 percent of all computers there, down from 5.7 percent in 1Q15.
- The third most common unwanted software category in India in 2Q15 was Adware, which was encountered by 2.5 percent of all computers there, up from 1.4 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in India in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Gamarue	Worms	6.1%
2	VBS/Jenxcus	Worms	3.6%
3	INF/Autorun	Obfuscators & Injectors	2.8%
4	Win32/Sality	Viruses	2.1%
5	Win32/Obfuscator	Obfuscators & Injectors	1.8%
6	Win32/Kilim	Trojans	1.3%
7	Win32/Peals	Trojans	1.3%
8	Win32/CplLnk	Exploits	1.2%
9	MSIL/Mofin	Worms	1.2%
10	Win32/Nuqel	Worms	1.2%

- The most common malware family encountered in India in 2Q15 was [Win32/Gamarue](#), which was encountered by 6.1 percent of reporting computers there. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The second most common malware family encountered in India in 2Q15 was [VBS/Jenxcus](#), which was encountered by 3.6 percent of reporting computers there. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The third most common malware family encountered in India in 2Q15 was [INF/Autorun](#), which was encountered by 2.8 percent of reporting computers there. [INF/Autorun](#) is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The fourth most common malware family encountered in India in 2Q15 was [Win32/Sality](#), which was encountered by 2.1 percent of reporting computers there. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in India in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	5.5%
2	Win32/KipodToolsCby	Browser Modifiers	4.3%
3	Win32/InstalleRex	Software Bundlers	3.6%
4	Win32/SaverExtension	Adware	1.4%
5	Win32/AlterbookSP	Browser Modifiers	0.4%

- The most common unwanted software family encountered in India in 2Q15 was [Win32/CouponRuc](#), which was encountered by 5.5 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in India in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 4.3 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common unwanted software family encountered in India in 2Q15 was [Win32/InstalleRex](#), which was encountered by 3.6 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in India in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/Gamarue	Worms	7.3
2	Win32/leEnablerCby	Browser Modifiers	5.5
3	VBS/Jenxcus	Worms	4.8
4	Win32/Sality	Viruses	4.0
5	Win32/CompromisedCert	Other Malware	1.8
6	Win32/Kilim	Trojans	1.8
7	Win32/Nuqel	Worms	1.8
8	Win32/Ramnit	Trojans	1.1
9	Win32/Virut	Viruses	0.7
10	MSIL/Bladabindi	Backdoors	0.6

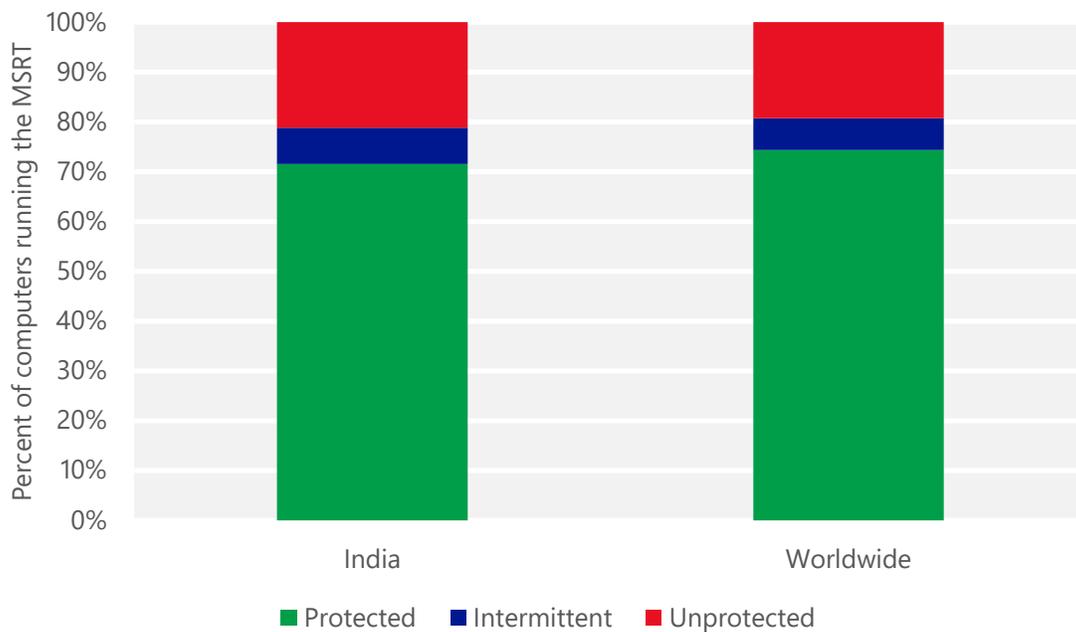
- The most common threat family infecting computers in India in 2Q15 was [Win32/Gamarue](#), which was detected and removed from 7.3 of every 1,000 unique computers scanned by the MSRT. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The second most common threat family infecting computers in India in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 5.5 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common threat family infecting computers in India in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 4.8 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The fourth most common threat family infecting computers in India in 2Q15 was [Win32/Sality](#), which was detected and removed from 4.0 of every 1,000 unique computers scanned by the MSRT. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in India and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for India

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.21 (0.28)	0.15 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	4.02 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	21.00 (16.7)	

Indonesia

The statistics presented here are generated by Microsoft security programs and services running on computers in Indonesia in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Indonesia

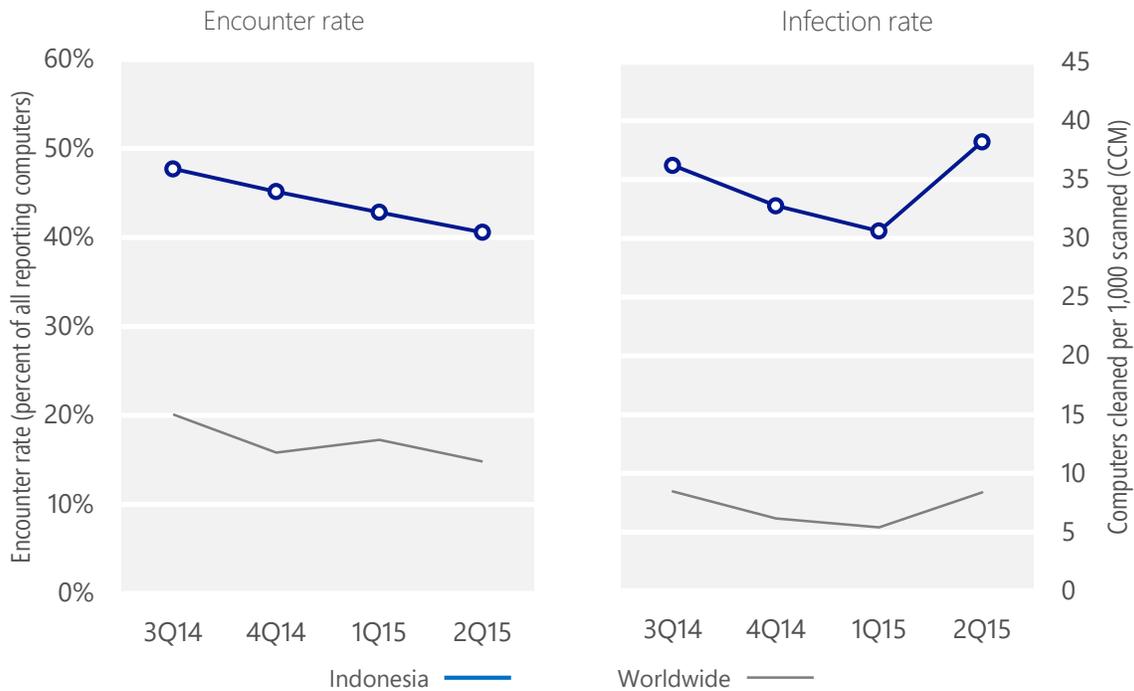
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Indonesia	47.7%	45.1%	42.8%	40.6%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Indonesia	36.2	32.8	30.6	38.2
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcoute, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 40.6% of computers in Indonesia encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 38.2 of every 1,000 unique computers scanned in Indonesia in 2Q15 (a CCM score of 38.2, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Indonesia over the last four quarters, compared to the world as a whole.

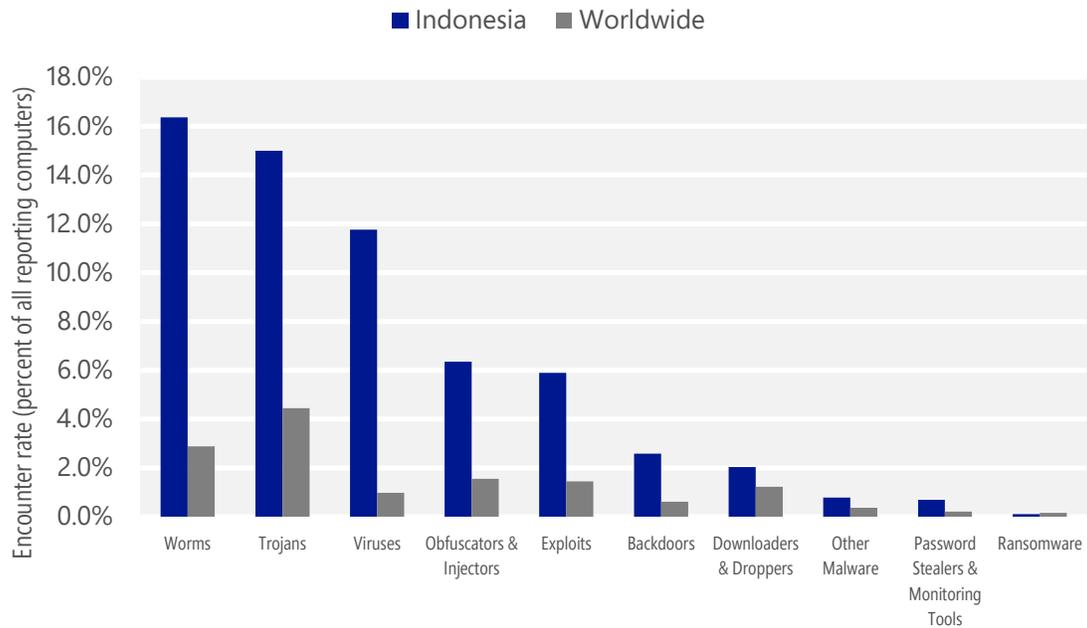
Malware encounter and infection rate trends in Indonesia and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in Indonesia and around the world, and for explanations of the methods and terms used here.

Malware categories

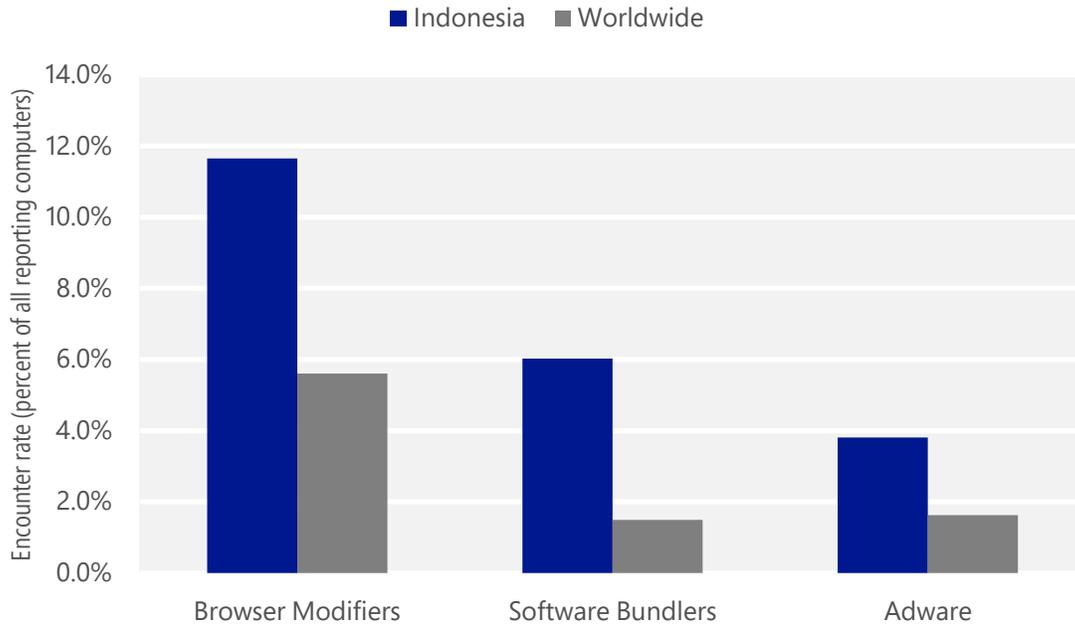
Malware encountered in Indonesia in 2Q15, by category



- The most common malware category in Indonesia in 2Q15 was Worms. It was encountered by 16.4 percent of all computers there, down from 19.0 percent in 1Q15.
- The second most common malware category in Indonesia in 2Q15 was Trojans. It was encountered by 15.0 percent of all computers there, up from 13.4 percent in 1Q15.
- The third most common malware category in Indonesia in 2Q15 was Viruses, which was encountered by 11.8 percent of all computers there, down from 12.3 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Indonesia in 2Q15, by category



- The most common unwanted software category in Indonesia in 2Q15 was Browser Modifiers. It was encountered by 11.7 percent of all computers there, down from 13.7 percent in 1Q15.
- The second most common unwanted software category in Indonesia in 2Q15 was Software Bundlers. It was encountered by 6.0 percent of all computers there, down from 7.9 percent in 1Q15.
- The third most common unwanted software category in Indonesia in 2Q15 was Adware, which was encountered by 3.8 percent of all computers there, up from 1.9 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Indonesia in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Gamarue	Worms	7.8%
2	Win32/Ramnit	Trojans	6.5%
3	Win32/CplLnk	Exploits	4.8%
4	Win32/Virut	Viruses	4.3%
5	INF/Autorun	Obfuscators & Injectors	3.7%
6	VBS/Jenxcus	Worms	3.6%
7	Win32/Sality	Viruses	3.5%
8	Win32/Obfuscator	Obfuscators & Injectors	3.2%
9	Win32/Peals	Trojans	2.1%
10	Win32/Slugin	Viruses	2.1%

- The most common malware family encountered in Indonesia in 2Q15 was [Win32/Gamarue](#), which was encountered by 7.8 percent of reporting computers there. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The second most common malware family encountered in Indonesia in 2Q15 was [Win32/Ramnit](#), which was encountered by 6.5 percent of reporting computers there. [Win32/Ramnit](#) is a family of multi-component malware that infects executable files, Microsoft Office files, and HTML files. Win32/Ramnit spreads to removable drives and steals sensitive information such as saved FTP credentials and browser cookies. It may also open a backdoor to await instructions from a remote attacker.
- The third most common malware family encountered in Indonesia in 2Q15 was [Win32/CplLnk](#), which was encountered by 4.8 percent of reporting computers there. [Win32/CplLnk](#) is a generic detection for specially-crafted malicious shortcut files that attempt to exploit the vulnerability addressed by Microsoft Security Bulletin MS10-046.
- The fourth most common malware family encountered in Indonesia in 2Q15 was [Win32/Virut](#), which was encountered by 4.3 percent of reporting computers there. [Win32/Virut](#) is a family of file-infecting viruses that target and infect .exe and .scr files accessed on infected systems. Win32/Virut also opens a backdoor by connecting to an IRC server.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Indonesia in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	7.2%
2	Win32/InstalleRex	Software Bundlers	5.8%
3	Win32/KipodToolsCby	Browser Modifiers	5.1%
4	Win32/SaverExtension	Adware	2.4%
5	Win32/EoRezo	Adware	0.6%

- The most common unwanted software family encountered in Indonesia in 2Q15 was [Win32/CouponRuc](#), which was encountered by 7.2 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in Indonesia in 2Q15 was [Win32/InstalleRex](#), which was encountered by 5.8 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own “Installed On” date in Programs and Features to make it more difficult for a user to locate it and remove it.
- The third most common unwanted software family encountered in Indonesia in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 5.1 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user’s consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.

Top threat families by infection rate

The most common malware families by infection rate in Indonesia in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/Ramnit	Trojans	7.1
2	Win32/leEnablerCby	Browser Modifiers	6.7
3	Win32/Gamarue	Worms	6.5
4	Win32/Sality	Viruses	6.1
5	VBS/Jenxcus	Worms	3.8
6	Win32/Virut	Viruses	2.9
7	Win32/Kilim	Trojans	2.8
8	Win32/CompromisedCert	Other Malware	1.0
9	Win32/Chir	Viruses	0.9
10	Win32/Dorkbot	Worms	0.9

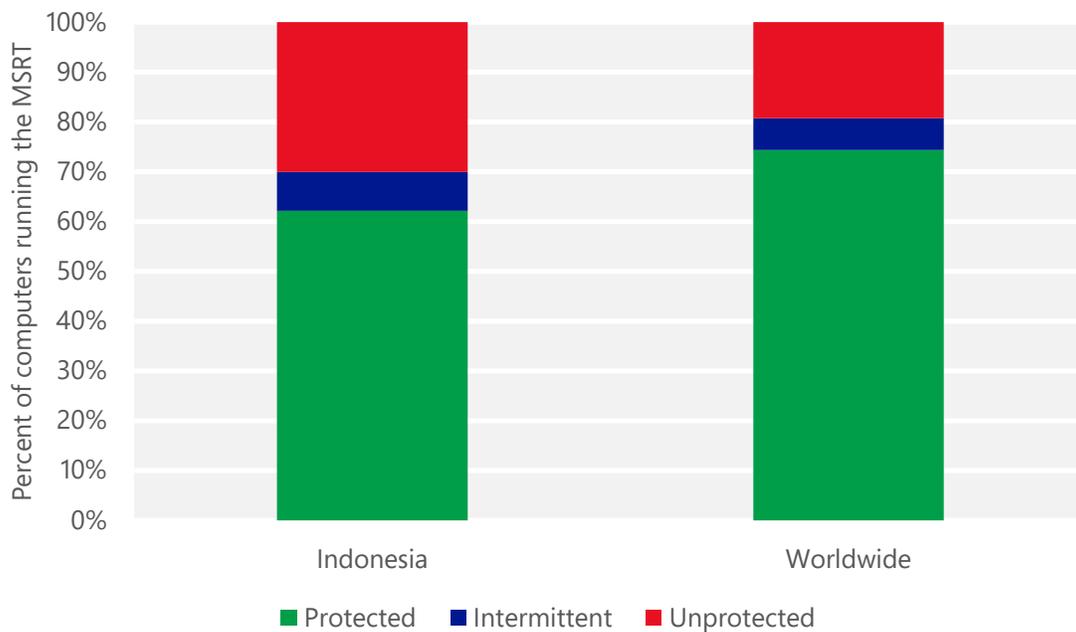
- The most common threat family infecting computers in Indonesia in 2Q15 was [Win32/Ramnit](#), which was detected and removed from 7.1 of every 1,000 unique computers scanned by the MSRT. [Win32/Ramnit](#) is a family of multi-component malware that infects executable files, Microsoft Office files, and HTML files. Win32/Ramnit spreads to removable drives and steals sensitive information such as saved FTP credentials and browser cookies. It may also open a backdoor to await instructions from a remote attacker.
- The second most common threat family infecting computers in Indonesia in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 6.7 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common threat family infecting computers in Indonesia in 2Q15 was [Win32/Gamarue](#), which was detected and removed from 6.5 of every 1,000 unique computers scanned by the MSRT. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The fourth most common threat family infecting computers in Indonesia in 2Q15 was [Win32/Sality](#), which was detected and removed from 6.1 of every 1,000 unique computers scanned by the MSRT. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Indonesia and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Indonesia

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	1.38 (0.28)	0.72 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	11.16 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	7.16 (16.7)	

Iraq

The statistics presented here are generated by Microsoft security programs and services running on computers in Iraq in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Iraq

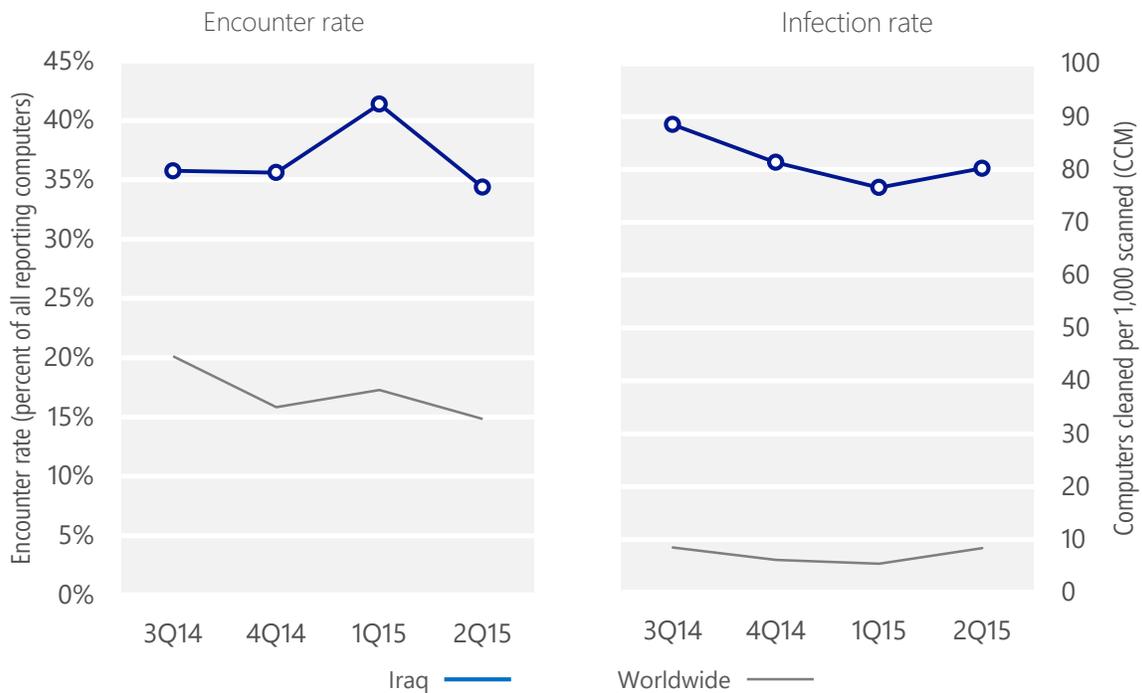
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Iraq	35.7%	35.6%	41.4%	34.4%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Iraq	88.5	81.3	76.6	80.2
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcout, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 34.4% of computers in Iraq encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 80.2 of every 1,000 unique computers scanned in Iraq in 2Q15 (a CCM score of 80.2, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Iraq over the last four quarters, compared to the world as a whole.

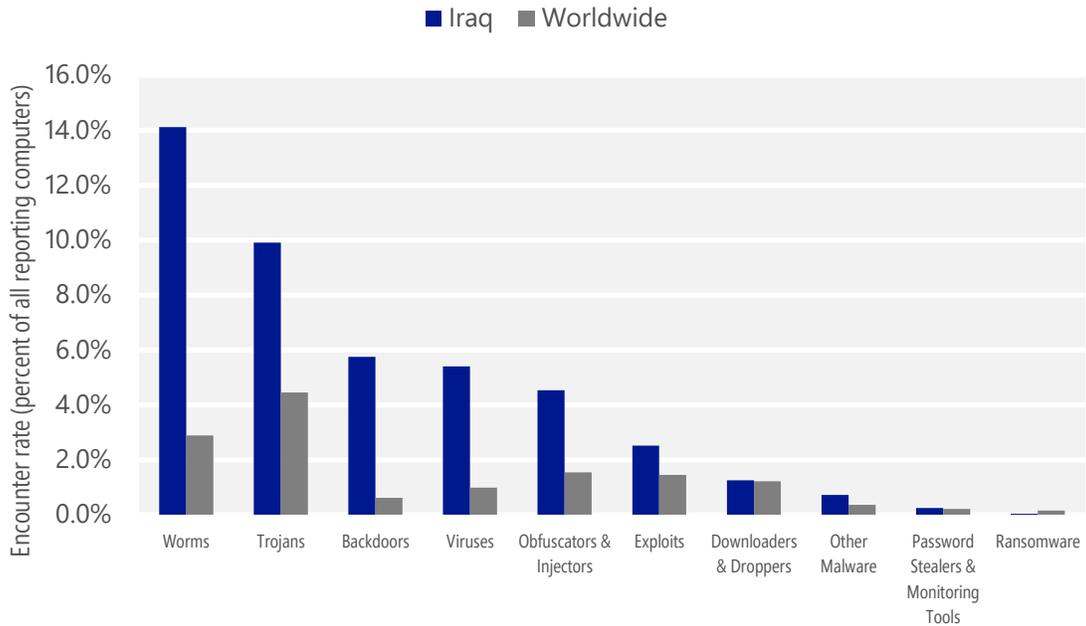
Malware encounter and infection rate trends in Iraq and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in Iraq and around the world, and for explanations of the methods and terms used here.

Malware categories

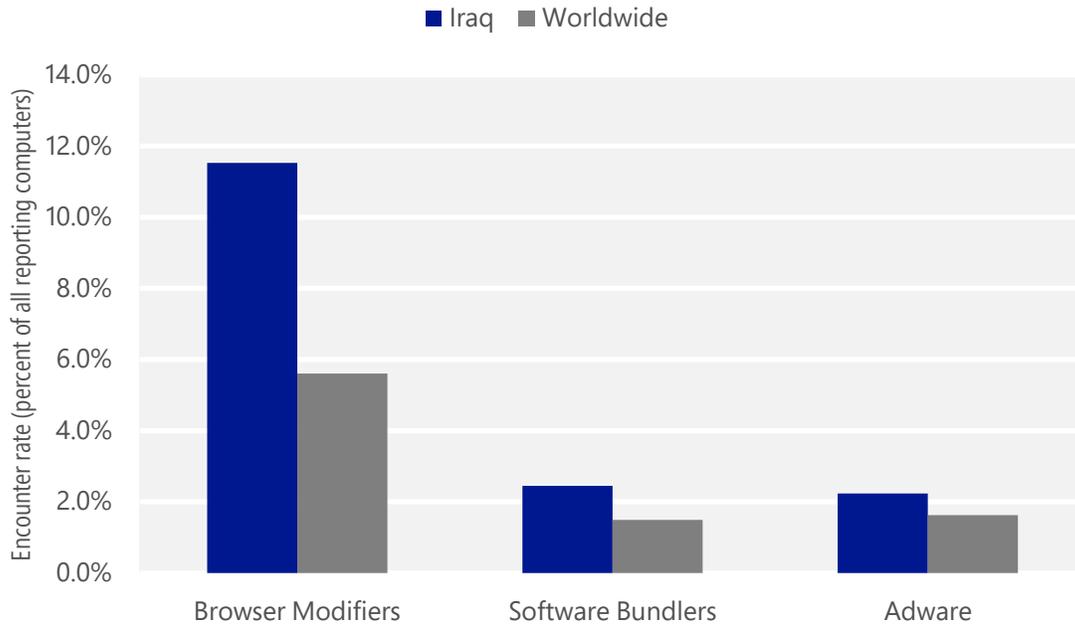
Malware encountered in Iraq in 2Q15, by category



- The most common malware category in Iraq in 2Q15 was Worms. It was encountered by 14.1 percent of all computers there, down from 16.7 percent in 1Q15.
- The second most common malware category in Iraq in 2Q15 was Trojans. It was encountered by 9.9 percent of all computers there, down from 10.0 percent in 1Q15.
- The third most common malware category in Iraq in 2Q15 was Backdoors, which was encountered by 5.8 percent of all computers there, down from 6.5 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Iraq in 2Q15, by category



- The most common unwanted software category in Iraq in 2Q15 was Browser Modifiers. It was encountered by 11.5 percent of all computers there, down from 17.9 percent in 1Q15.
- The second most common unwanted software category in Iraq in 2Q15 was Software Bundlers. It was encountered by 2.5 percent of all computers there, down from 4.8 percent in 1Q15.
- The third most common unwanted software category in Iraq in 2Q15 was Adware, which was encountered by 2.2 percent of all computers there, up from 1.1 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Iraq in 2Q15

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	7.7%
2	INF/Autorun	Obfuscators & Injectors	4.8%
3	MSIL/Bladabindi	Backdoors	4.0%
4	Win32/Wecykler	Worms	3.4%
5	Win32/Sality	Viruses	2.7%
6	Win32/Gamarue	Worms	2.1%
7	Win32/Obfuscator	Obfuscators & Injectors	2.1%
8	Win32/Ramnit	Trojans	2.0%
9	Win32/CplLnk	Exploits	1.9%
10	Win32/Peals	Trojans	1.4%

- The most common malware family encountered in Iraq in 2Q15 was [VBS/Jenxcus](#), which was encountered by 7.7 percent of reporting computers there. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common malware family encountered in Iraq in 2Q15 was [INF/Autorun](#), which was encountered by 4.8 percent of reporting computers there. [INF/Autorun](#) is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The third most common malware family encountered in Iraq in 2Q15 was [MSIL/Bladabindi](#), which was encountered by 4.0 percent of reporting computers there. [MSIL/Bladabindi](#) is a family of backdoors created by a malicious hacker tool called NJ Rat. The can steal sensitive information, download other malware, and allow backdoor access to an infected computer.
- The fourth most common malware family encountered in Iraq in 2Q15 was [Win32/Wecykler](#), which was encountered by 3.4 percent of reporting computers there. [Win32/Wecykler](#) is a family of worms that spread via removable drives, such as USB drives; they may stop security processes and other processes on the computer, and log keystrokes which they later send to a remote attacker.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Iraq in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/KipodToolsCby	Browser Modifiers	7.2%
2	Win32/CouponRuc	Browser Modifiers	4.3%
3	Win32/InstalleRex	Software Bundlers	2.3%
4	Win32/SaverExtension	Adware	1.4%
5	Win32/AlterbookSP	Browser Modifiers	0.6%

- The most common unwanted software family encountered in Iraq in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 7.2 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common unwanted software family encountered in Iraq in 2Q15 was [Win32/CouponRuc](#), which was encountered by 4.3 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The third most common unwanted software family encountered in Iraq in 2Q15 was [Win32/InstalleRex](#), which was encountered by 2.3 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Iraq in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	22.7
2	Win32/Sality	Viruses	15.4
3	MSIL/Bladabindi	Backdoors	13.1
4	Win32/Wecykler	Worms	9.9
5	Win32/Ramnit	Trojans	7.1
6	Win32/IeEnablerCby	Browser Modifiers	6.3
7	Win32/Gamarue	Worms	4.8
8	Win32/Brontok	Worms	3.2
9	Win32/Dorkbot	Worms	2.9
10	Win32/Kilim	Trojans	2.8

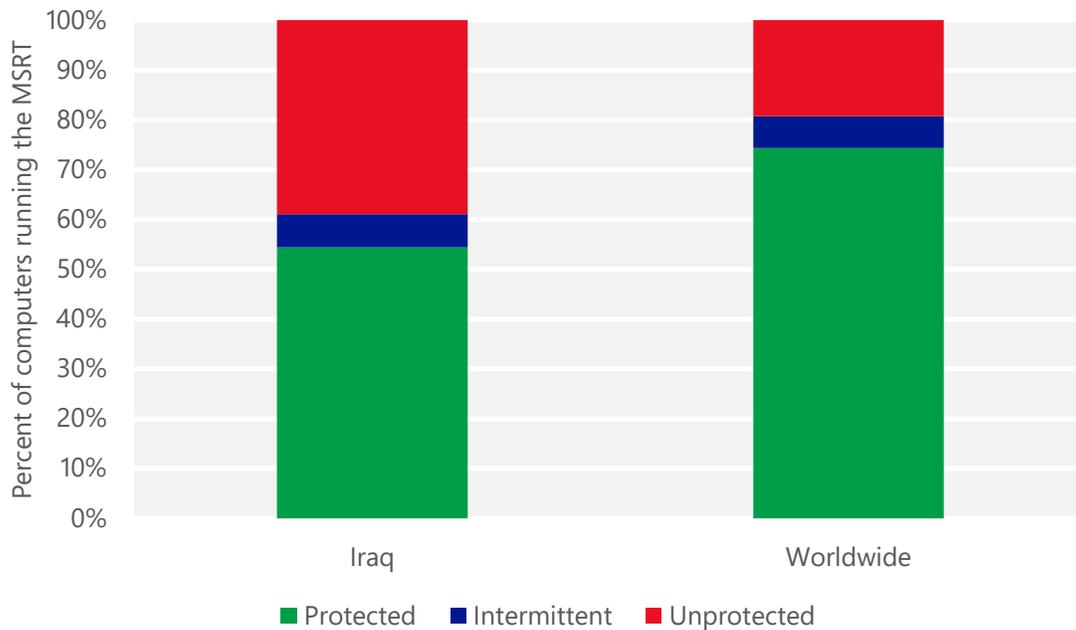
- The most common threat family infecting computers in Iraq in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 22.7 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Iraq in 2Q15 was [Win32/Sality](#), which was detected and removed from 15.4 of every 1,000 unique computers scanned by the MSRT. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The third most common threat family infecting computers in Iraq in 2Q15 was [MSIL/Bladabindi](#), which was detected and removed from 13.1 of every 1,000 unique computers scanned by the MSRT. [MSIL/Bladabindi](#) is a family of backdoors created by a malicious hacker tool called NJ Rat. The can steal sensitive information, download other malware, and allow backdoor access to an infected computer.
- The fourth most common threat family infecting computers in Iraq in 2Q15 was [Win32/Wecykler](#), which was detected and removed from 9.9 of every 1,000 unique computers scanned by the MSRT. [Win32/Wecykler](#) is a family of worms that spread via removable drives, such as USB drives; they may stop security processes and other processes on the computer, and log keystrokes which they later send to a remote attacker.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Iraq and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Iraq

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.13 (0.28)	0.06 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	4.41 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	20.58 (16.7)	

Ireland

The statistics presented here are generated by Microsoft security programs and services running on computers in Ireland in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Ireland

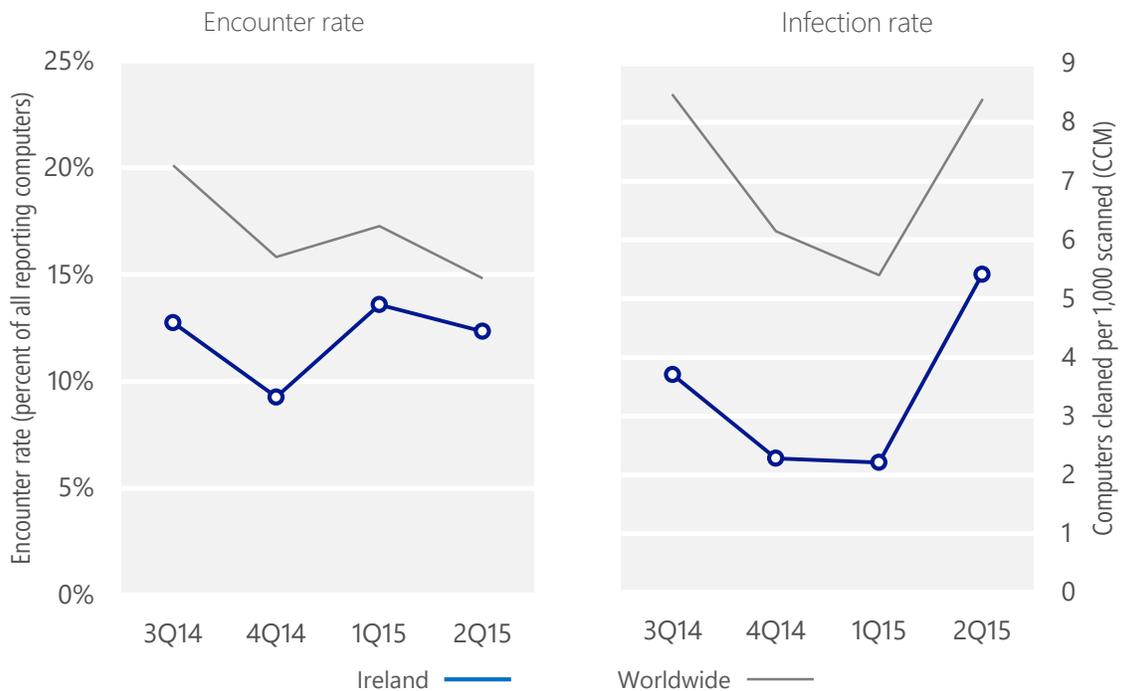
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Ireland	12.8%	9.3%	13.6%	12.3%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Ireland	3.7	2.3	2.2	5.4
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcout, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 12.3% of computers in Ireland encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 5.4 of every 1,000 unique computers scanned in Ireland in 2Q15 (a CCM score of 5.4, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Ireland over the last four quarters, compared to the world as a whole.

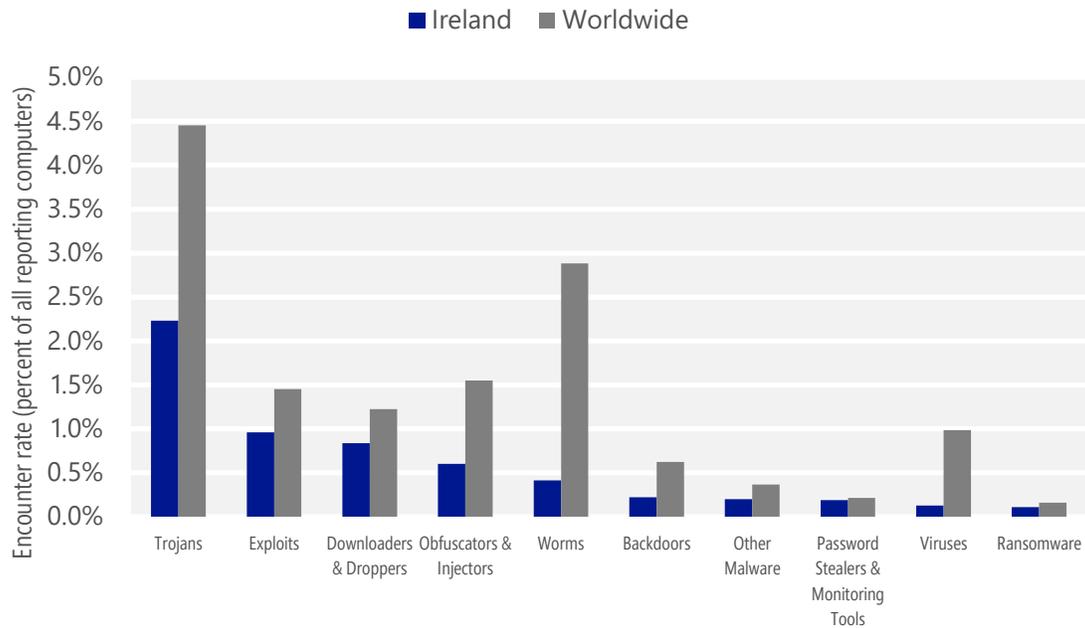
Malware encounter and infection rate trends in Ireland and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in Ireland and around the world, and for explanations of the methods and terms used here.

Malware categories

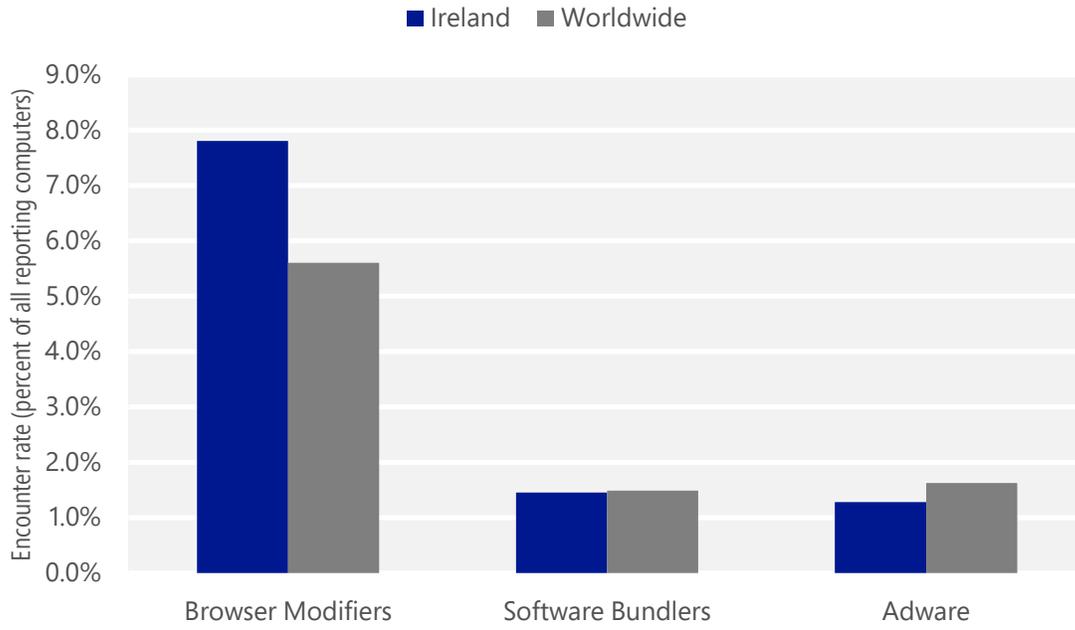
Malware encountered in Ireland in 2Q15, by category



- The most common malware category in Ireland in 2Q15 was Trojans. It was encountered by 2.2 percent of all computers there, up from 1.4 percent in 1Q15.
- The second most common malware category in Ireland in 2Q15 was Exploits. It was encountered by 1.0 percent of all computers there, down from 1.3 percent in 1Q15.
- The third most common malware category in Ireland in 2Q15 was Downloaders & Droppers, which was encountered by 0.8 percent of all computers there, down from 1.2 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Ireland in 2Q15, by category



- The most common unwanted software category in Ireland in 2Q15 was Browser Modifiers. It was encountered by 7.8 percent of all computers there, up from 7.8 percent in 1Q15.
- The second most common unwanted software category in Ireland in 2Q15 was Software Bundlers. It was encountered by 1.5 percent of all computers there, down from 3.5 percent in 1Q15.
- The third most common unwanted software category in Ireland in 2Q15 was Adware, which was encountered by 1.3 percent of all computers there, up from 0.5 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Ireland in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Kilim	Trojans	0.7%
2	Win32/Obfuscator	Obfuscators & Injectors	0.5%
3	JS/Axpergle	Exploits	0.4%
4	Win32/Skeeyah	Trojans	0.4%
5	Win32/Upatre	Downloaders & Droppers	0.3%
6	Win32/Peals	Trojans	0.3%
7	Win32/Sdbby	Exploits	0.3%
8	INF/Autorun	Obfuscators & Injectors	0.1%
9	Win32/Dynamer	Trojans	0.1%
10	Win32/Dyzap	Password Stealers & Monitoring Tools	0.1%

- The most common malware family encountered in Ireland in 2Q15 was [Win32/Kilim](#), which was encountered by 0.7 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The second most common malware family encountered in Ireland in 2Q15 was [Win32/Obfuscator](#), which was encountered by 0.5 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The third most common malware family encountered in Ireland in 2Q15 was [JS/Axpergle](#), which was encountered by 0.4 percent of reporting computers there. [JS/Axpergle](#) is a detection for the Angler exploit kit, which exploits vulnerabilities in recent versions of Internet Explorer, Silverlight, Adobe Flash Player, and Java to install malware.
- The fourth most common malware family encountered in Ireland in 2Q15 was [Win32/Skeeyah](#), which was encountered by 0.4 percent of reporting computers there. [Win32/Skeeyah](#) is a generic detection for various threats that display trojan characteristics.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Ireland in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/KipodToolsCby	Browser Modifiers	3.8%
2	Win32/CouponRuc	Browser Modifiers	2.8%
3	Win32/InstalleRex	Software Bundlers	1.4%
4	Win32/AlterbookSP	Browser Modifiers	1.3%
5	Win32/SaverExtension	Adware	1.0%

- The most common unwanted software family encountered in Ireland in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 3.8 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common unwanted software family encountered in Ireland in 2Q15 was [Win32/CouponRuc](#), which was encountered by 2.8 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The third most common unwanted software family encountered in Ireland in 2Q15 was [Win32/InstalleRex](#), which was encountered by 1.4 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Ireland in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	2.2
2	Win32/Kilim	Trojans	1.1
3	Win32/CompromisedCert	Other Malware	0.6
4	Win32/Dyzap	Password Stealers & Monitoring Tools	0.2
5	Win32/Simda	Trojans	0.1
6	Win32/Alureon	Trojans	0.1
7	VBS/Jenxcus	Worms	0.1
8	Win32/Sality	Viruses	0.1
9	Win32/Conficker	Worms	0.1
10	Win32/Zbot	Password Stealers & Monitoring Tools	0.1

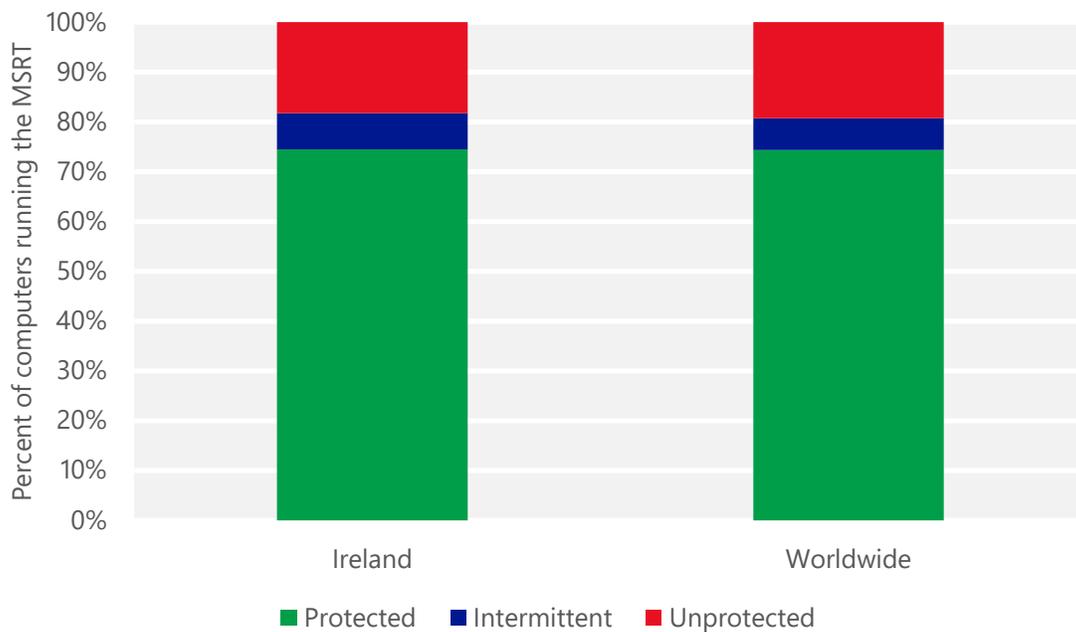
- The most common threat family infecting computers in Ireland in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 2.2 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Ireland in 2Q15 was [Win32/Kilim](#), which was detected and removed from 1.1 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The third most common threat family infecting computers in Ireland in 2Q15 was [Win32/CompromisedCert](#), which was detected and removed from 0.6 of every 1,000 unique computers scanned by the MSRT. [Win32/CompromisedCert](#) is a detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.
- The fourth most common threat family infecting computers in Ireland in 2Q15 was [Win32/Dyzap](#), which was detected and removed from 0.2 of every 1,000 unique computers scanned by the MSRT. [Win32/Dyzap](#) is a threat that steals login credentials for a long list of banking websites using man-in-the-browser (MITB) attacks. It is usually installed on the infected computer by TrojanDownloader:Win32/Upatre.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Ireland and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Ireland

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.05 (0.28)	0.02 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	4.49 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	9.80 (16.7)	

Israel

The statistics presented here are generated by Microsoft security programs and services running on computers in Israel in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Israel

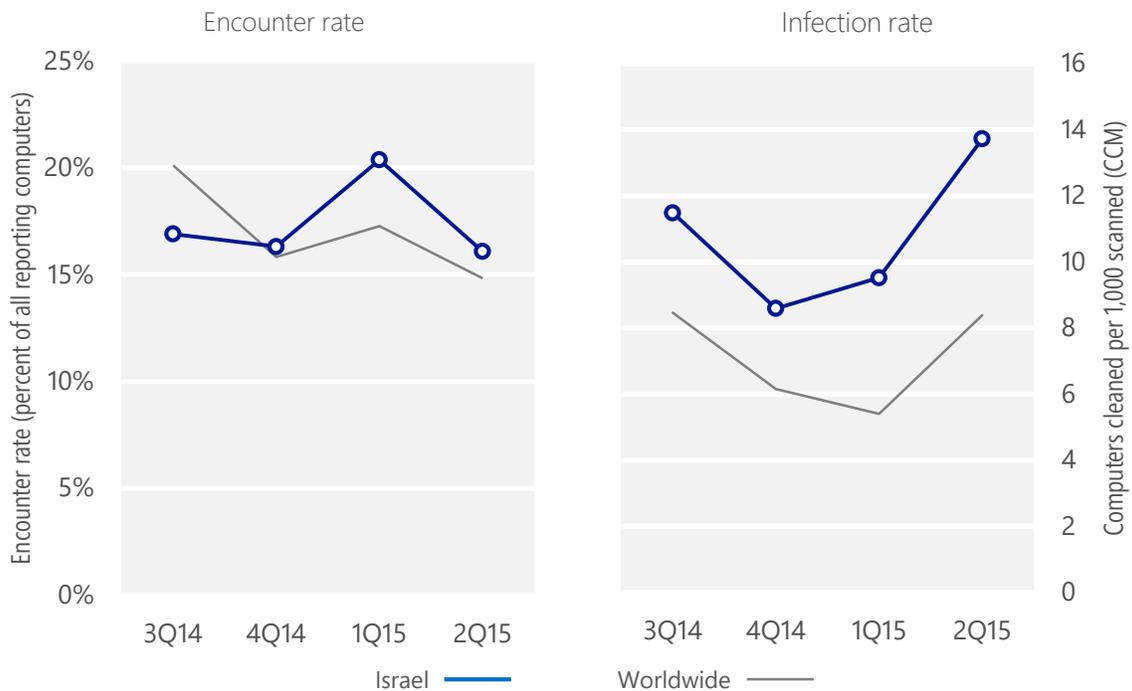
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Israel	16.9%	16.3%	20.4%	16.1%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Israel	11.5	8.6	9.5	13.7
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcout, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 16.1% of computers in Israel encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 13.7 of every 1,000 unique computers scanned in Israel in 2Q15 (a CCM score of 13.7, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Israel over the last four quarters, compared to the world as a whole.

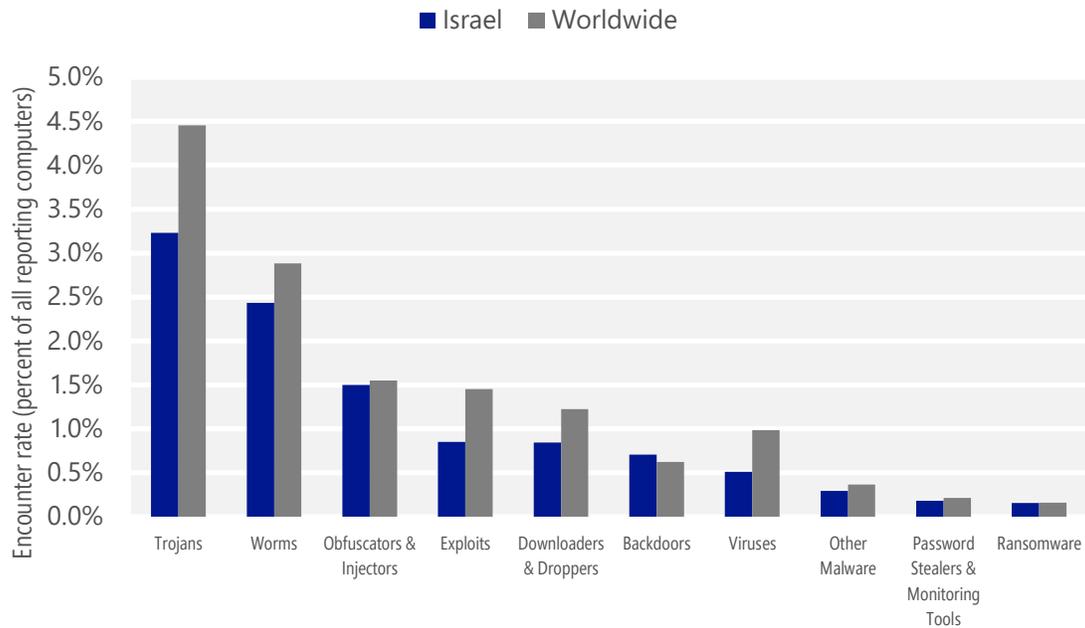
Malware encounter and infection rate trends in Israel and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in Israel and around the world, and for explanations of the methods and terms used here.

Malware categories

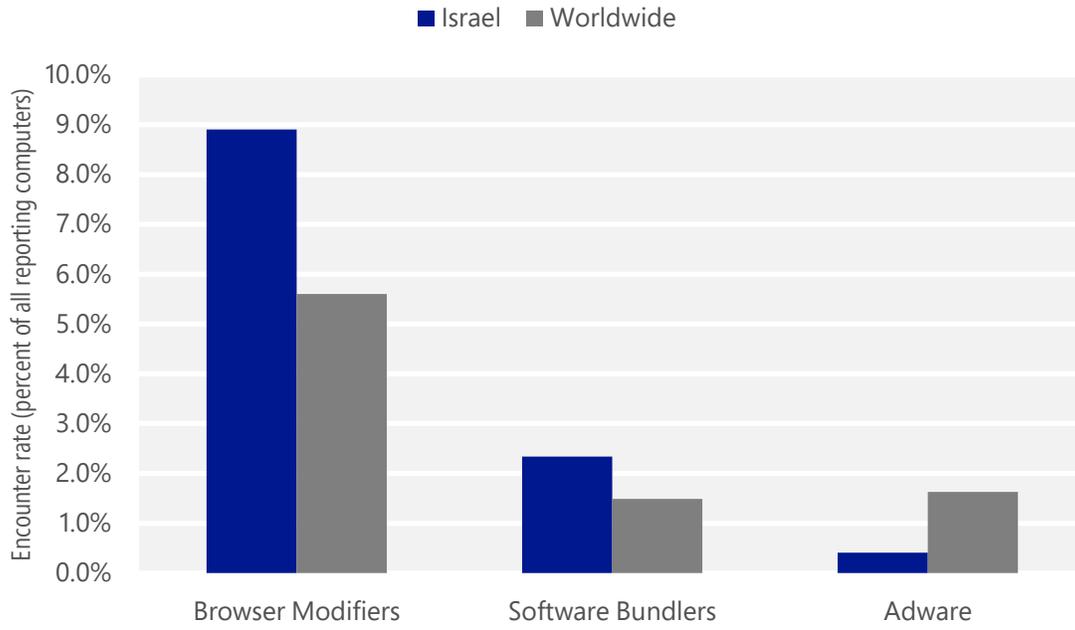
Malware encountered in Israel in 2Q15, by category



- The most common malware category in Israel in 2Q15 was Trojans. It was encountered by 3.2 percent of all computers there, down from 3.3 percent in 1Q15.
- The second most common malware category in Israel in 2Q15 was Worms. It was encountered by 2.4 percent of all computers there, down from 3.3 percent in 1Q15.
- The third most common malware category in Israel in 2Q15 was Obfuscators & Injectors, which was encountered by 1.5 percent of all computers there, down from 1.7 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Israel in 2Q15, by category



- The most common unwanted software category in Israel in 2Q15 was Browser Modifiers. It was encountered by 8.9 percent of all computers there, down from 13.1 percent in 1Q15.
- The second most common unwanted software category in Israel in 2Q15 was Software Bundlers. It was encountered by 2.3 percent of all computers there, up from 0.7 percent in 1Q15.
- The third most common unwanted software category in Israel in 2Q15 was Adware, which was encountered by 0.4 percent of all computers there, up from 0.4 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Israel in 2Q15

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	1.1%
2	Win32/Obfuscator	Obfuscators & Injectors	1.1%
3	Win32/Skeeyah	Trojans	0.6%
4	INF/Autorun	Obfuscators & Injectors	0.5%
5	Win32/Peals	Trojans	0.5%
6	JS/Axpergle	Exploits	0.5%
7	Win32/Brontok	Worms	0.3%
8	MSIL/Bladabindi	Backdoors	0.3%
9	Win32/Dynamer	Trojans	0.2%
10	Win32/Sality	Viruses	0.2%

- The most common malware family encountered in Israel in 2Q15 was [VBS/Jenxcus](#), which was encountered by 1.1 percent of reporting computers there. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common malware family encountered in Israel in 2Q15 was [Win32/Obfuscator](#), which was encountered by 1.1 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The third most common malware family encountered in Israel in 2Q15 was [Win32/Skeeyah](#), which was encountered by 0.6 percent of reporting computers there. [Win32/Skeeyah](#) is a generic detection for various threats that display trojan characteristics.
- The fourth most common malware family encountered in Israel in 2Q15 was [INF/Autorun](#), which was encountered by 0.5 percent of reporting computers there. [INF/Autorun](#) is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Israel in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/KipodToolsCby	Browser Modifiers	4.7%
2	Win32/CouponRuc	Browser Modifiers	2.8%
3	Win32/InstalleRex	Software Bundlers	2.2%
4	Win32/AlterbookSP	Browser Modifiers	1.5%
5	Win32/DefaultTab	Browser Modifiers	0.3%

- The most common unwanted software family encountered in Israel in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 4.7 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common unwanted software family encountered in Israel in 2Q15 was [Win32/CouponRuc](#), which was encountered by 2.8 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The third most common unwanted software family encountered in Israel in 2Q15 was [Win32/InstalleRex](#), which was encountered by 2.2 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Israel in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	5.4
2	VBS/Jenxcus	Worms	2.1
3	Win32/CompromisedCert	Other Malware	1.3
4	Win32/Brontok	Worms	1.2
5	Win32/Sality	Viruses	0.9
6	MSIL/Bladabindi	Backdoors	0.5
7	Win32/Ramnit	Trojans	0.5
8	Win32/Kilim	Trojans	0.3
9	Win32/Dorkbot	Worms	0.2
10	Win32/Simda	Trojans	0.2

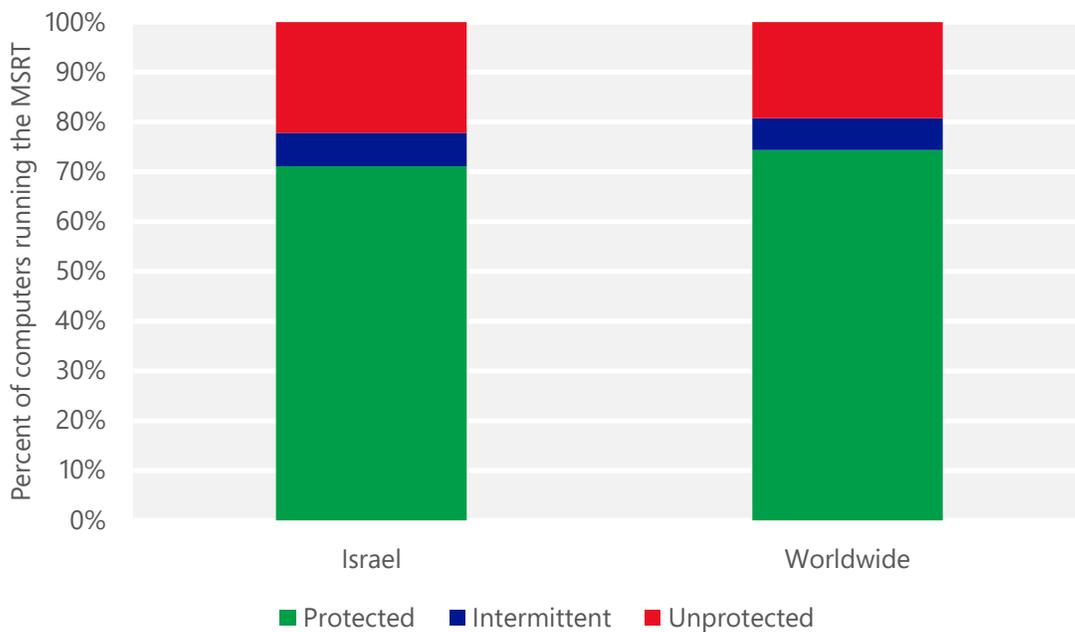
- The most common threat family infecting computers in Israel in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 5.4 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Israel in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 2.1 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The third most common threat family infecting computers in Israel in 2Q15 was [Win32/CompromisedCert](#), which was detected and removed from 1.3 of every 1,000 unique computers scanned by the MSRT. [Win32/CompromisedCert](#) is a detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.
- The fourth most common threat family infecting computers in Israel in 2Q15 was [Win32/Brontok](#), which was detected and removed from 1.2 of every 1,000 unique computers scanned by the MSRT. [Win32/Brontok](#) is a mass-mailing email worm that spreads by sending copies of itself as email attachments to addresses gathered from files on the infected computer, and by copying itself to removable volumes. Brontok can disable security software, and may conduct DoS attacks against certain websites.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Israel and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Israel

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.13 (0.28)	0.08 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	5.09 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	12.57 (16.7)	

Italy

The statistics presented here are generated by Microsoft security programs and services running on computers in Italy in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Italy

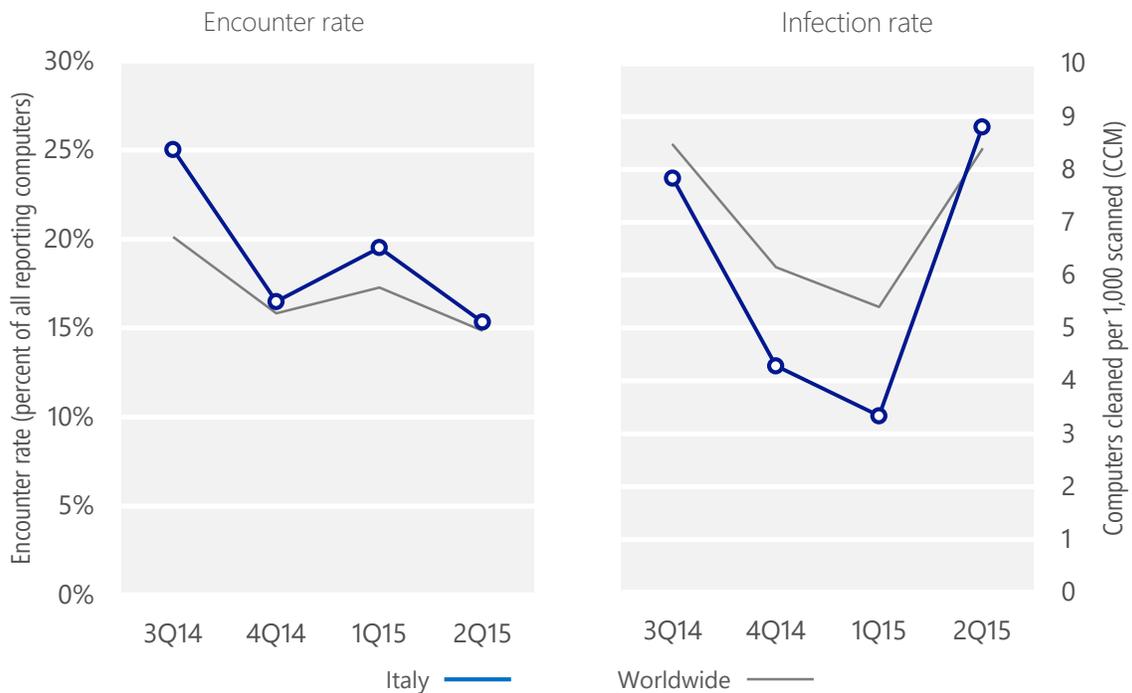
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Italy	25.0%	16.5%	19.5%	15.3%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Italy	7.8	4.3	3.3	8.8
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcout, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 15.3% of computers in Italy encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 8.8 of every 1,000 unique computers scanned in Italy in 2Q15 (a CCM score of 8.8, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Italy over the last four quarters, compared to the world as a whole.

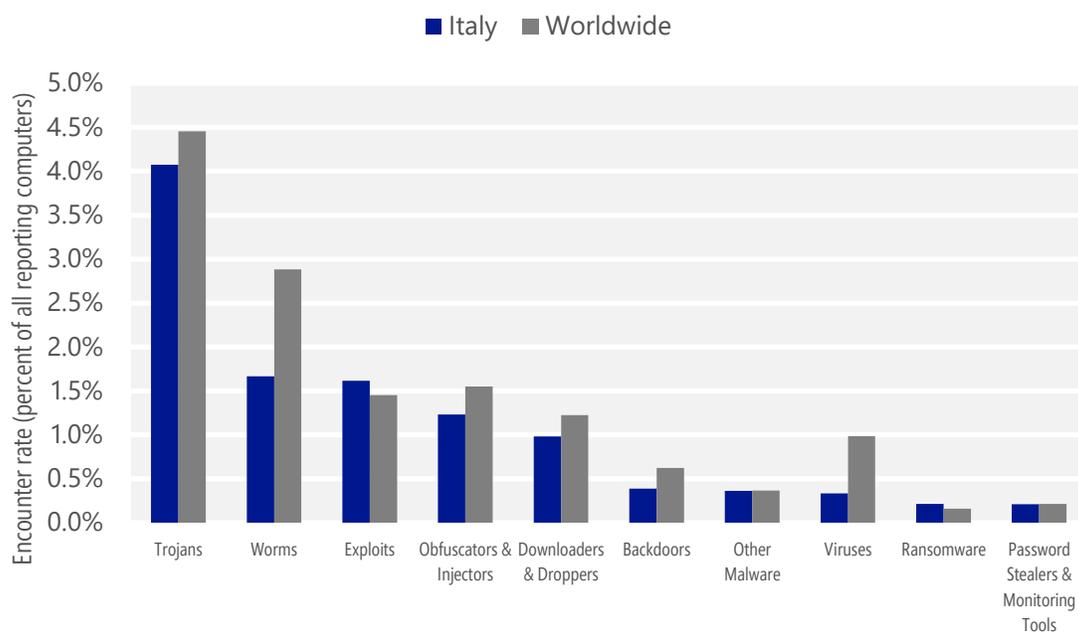
Malware encounter and infection rate trends in Italy and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in Italy and around the world, and for explanations of the methods and terms used here.

Malware categories

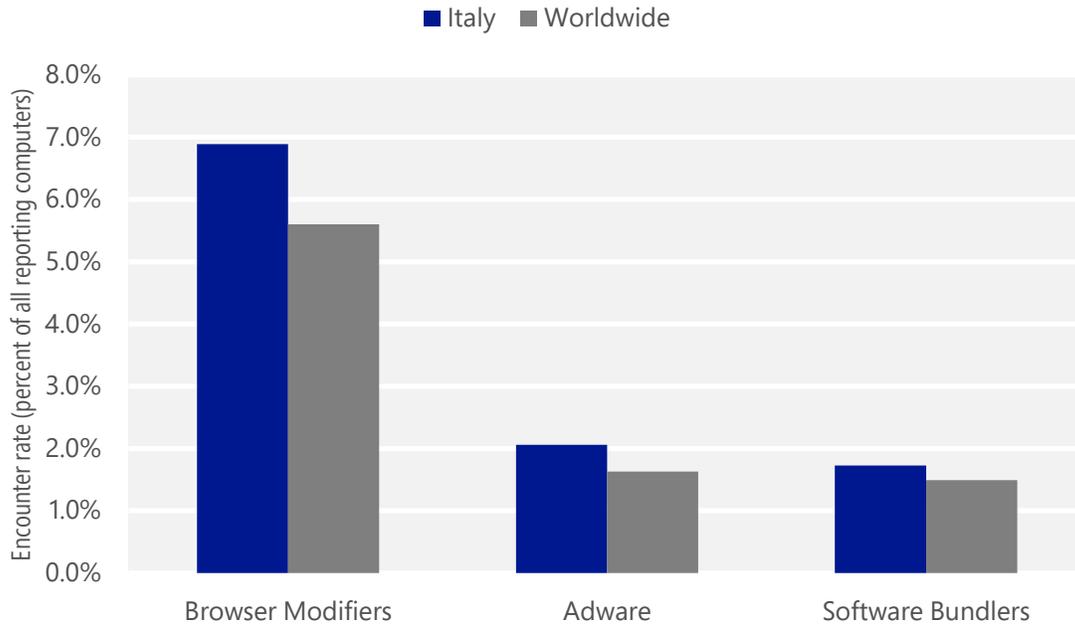
Malware encountered in Italy in 2Q15, by category



- The most common malware category in Italy in 2Q15 was Trojans. It was encountered by 4.1 percent of all computers there, up from 2.9 percent in 1Q15.
- The second most common malware category in Italy in 2Q15 was Worms. It was encountered by 1.7 percent of all computers there, down from 2.6 percent in 1Q15.
- The third most common malware category in Italy in 2Q15 was Exploits, which was encountered by 1.6 percent of all computers there, down from 2.2 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Italy in 2Q15, by category



- The most common unwanted software category in Italy in 2Q15 was Browser Modifiers. It was encountered by 6.9 percent of all computers there, down from 8.3 percent in 1Q15.
- The second most common unwanted software category in Italy in 2Q15 was Adware. It was encountered by 2.1 percent of all computers there, down from 5.1 percent in 1Q15.
- The third most common unwanted software category in Italy in 2Q15 was Software Bundlers, which was encountered by 1.7 percent of all computers there, up from 0.7 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Italy in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Kilim	Trojans	1.1%
2	JS/Axpergle	Exploits	0.9%
3	Win32/Obfuscator	Obfuscators & Injectors	0.9%
4	Win32/Skeeyah	Trojans	0.7%
5	Win32/Peals	Trojans	0.5%
6	Win32/Conficker	Worms	0.5%
7	INF/Autorun	Obfuscators & Injectors	0.4%
8	Win32/Dynamer	Trojans	0.4%
9	ASX/Wimad	Downloaders & Droppers	0.3%
10	Win32/Gamarue	Worms	0.3%

- The most common malware family encountered in Italy in 2Q15 was [Win32/Kilim](#), which was encountered by 1.1 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The second most common malware family encountered in Italy in 2Q15 was [JS/Axpergle](#), which was encountered by 0.9 percent of reporting computers there. [JS/Axpergle](#) is a detection for the Angler exploit kit, which exploits vulnerabilities in recent versions of Internet Explorer, Silverlight, Adobe Flash Player, and Java to install malware.
- The third most common malware family encountered in Italy in 2Q15 was [Win32/Obfuscator](#), which was encountered by 0.9 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The fourth most common malware family encountered in Italy in 2Q15 was [Win32/Skeeyah](#), which was encountered by 0.7 percent of reporting computers there. [Win32/Skeeyah](#) is a generic detection for various threats that display trojan characteristics.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Italy in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	3.1%
2	Win32/KipodToolsCby	Browser Modifiers	2.8%
3	Win32/InstalleRex	Software Bundlers	1.6%
4	Win32/SaverExtension	Adware	1.0%
5	Win32/AlterbookSP	Browser Modifiers	0.6%

- The most common unwanted software family encountered in Italy in 2Q15 was [Win32/CouponRuc](#), which was encountered by 3.1 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in Italy in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 2.8 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common unwanted software family encountered in Italy in 2Q15 was [Win32/InstalleRex](#), which was encountered by 1.6 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Italy in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	4.0
2	Win32/Kilim	Trojans	1.2
3	Win32/CompromisedCert	Other Malware	1.0
4	VBS/Jenxcus	Worms	0.4
5	Win32/Simda	Trojans	0.2
6	Win32/Ramnit	Trojans	0.2
7	Win32/Conficker	Worms	0.2
8	Win32/Carberp	Trojans	0.2
9	Win32/Alureon	Trojans	0.2
10	Win32/Sality	Viruses	0.2

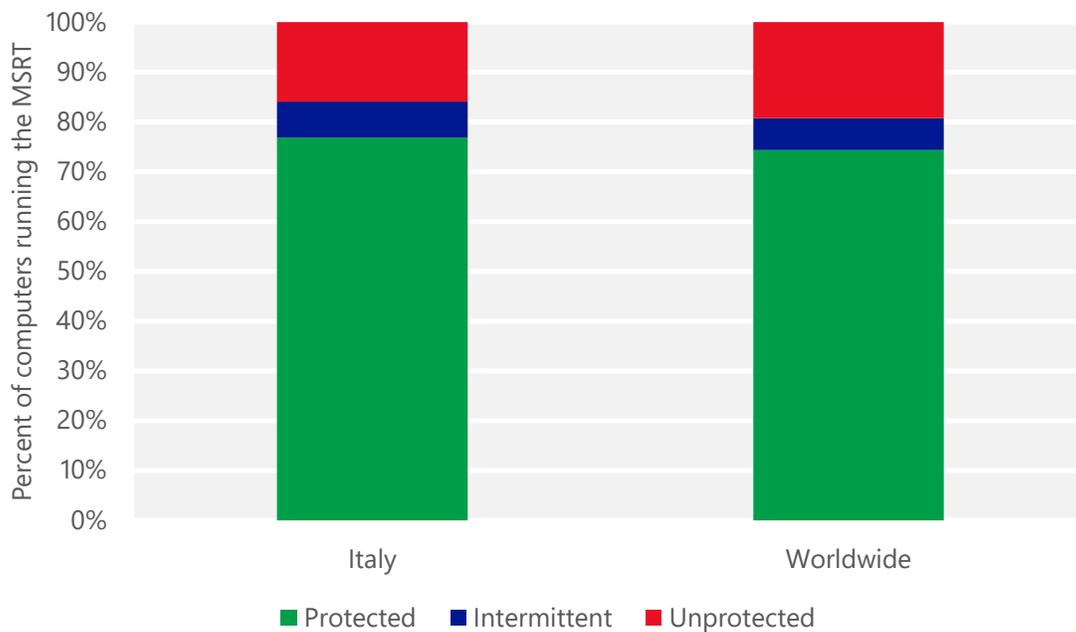
- The most common threat family infecting computers in Italy in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 4.0 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Italy in 2Q15 was [Win32/Kilim](#), which was detected and removed from 1.2 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The third most common threat family infecting computers in Italy in 2Q15 was [Win32/CompromisedCert](#), which was detected and removed from 1.0 of every 1,000 unique computers scanned by the MSRT. [Win32/CompromisedCert](#) is a detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.
- The fourth most common threat family infecting computers in Italy in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 0.4 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Italy and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Italy

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.23 (0.28)	0.18 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	4.75 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	16.04 (16.7)	

Jamaica

The statistics presented here are generated by Microsoft security programs and services running on computers in Jamaica in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Jamaica

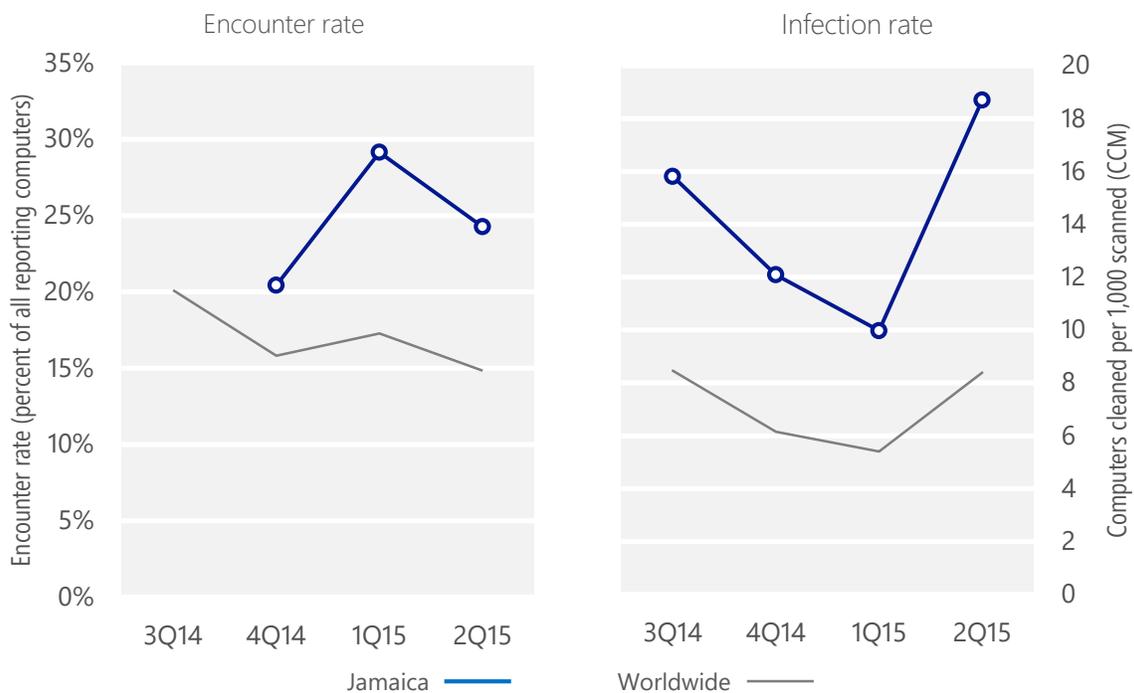
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Jamaica	N/A	20.4%	29.1%	24.3%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Jamaica	15.8	12.1	10.0	18.7
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcote, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 24.3% of computers in Jamaica encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 18.7 of every 1,000 unique computers scanned in Jamaica in 2Q15 (a CCM score of 18.7, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Jamaica over the last four quarters, compared to the world as a whole.

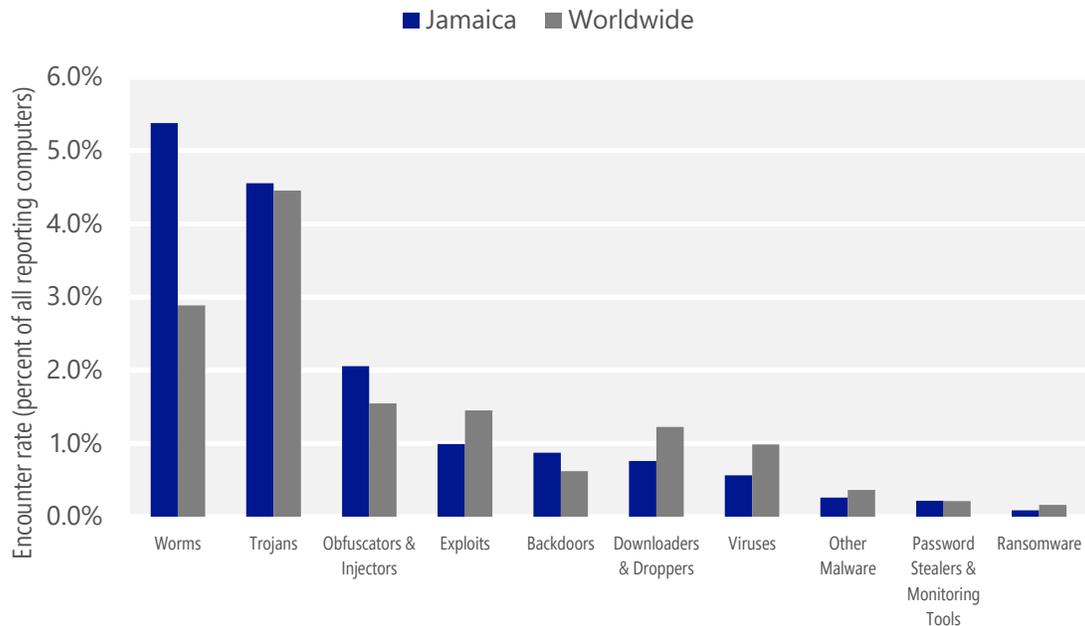
Malware encounter and infection rate trends in Jamaica and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in Jamaica and around the world, and for explanations of the methods and terms used here.

Malware categories

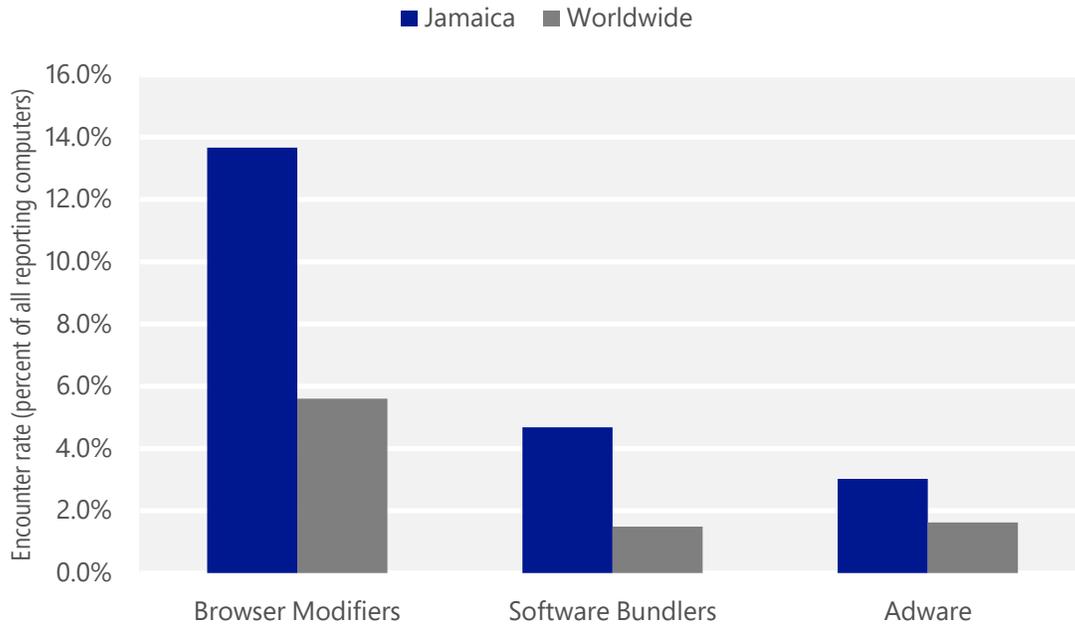
Malware encountered in Jamaica in 2Q15, by category



- The most common malware category in Jamaica in 2Q15 was Worms. It was encountered by 5.4 percent of all computers there, down from 7.2 percent in 1Q15.
- The second most common malware category in Jamaica in 2Q15 was Trojans. It was encountered by 4.6 percent of all computers there, up from 2.7 percent in 1Q15.
- The third most common malware category in Jamaica in 2Q15 was Obfuscators & Injectors, which was encountered by 2.1 percent of all computers there, down from 2.2 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Jamaica in 2Q15, by category



- The most common unwanted software category in Jamaica in 2Q15 was Browser Modifiers. It was encountered by 13.7 percent of all computers there, down from 19.1 percent in 1Q15.
- The second most common unwanted software category in Jamaica in 2Q15 was Software Bundlers. It was encountered by 4.7 percent of all computers there, down from 6.2 percent in 1Q15.
- The third most common unwanted software category in Jamaica in 2Q15 was Adware, which was encountered by 3.0 percent of all computers there, up from 1.4 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Jamaica in 2Q15

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	2.6%
2	Win32/Obfuscator	Obfuscators & Injectors	1.4%
3	Win32/Kilim	Trojans	1.4%
4	Win32/Skeeyah	Trojans	1.0%
5	Win32/Ippedo	Worms	0.9%
6	Win32/Gamarue	Worms	0.8%
7	INF/Autorun	Obfuscators & Injectors	0.7%
8	Win32/Brontok	Worms	0.6%
9	JS/Proslifean	Worms	0.4%
10	Win32/Peals	Trojans	0.4%

- The most common malware family encountered in Jamaica in 2Q15 was [VBS/Jenxcus](#), which was encountered by 2.6 percent of reporting computers there. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common malware family encountered in Jamaica in 2Q15 was [Win32/Obfuscator](#), which was encountered by 1.4 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The third most common malware family encountered in Jamaica in 2Q15 was [Win32/Kilim](#), which was encountered by 1.4 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The fourth most common malware family encountered in Jamaica in 2Q15 was [Win32/Skeeyah](#), which was encountered by 1.0 percent of reporting computers there. [Win32/Skeeyah](#) is a generic detection for various threats that display trojan characteristics.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Jamaica in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/KipodToolsCby	Browser Modifiers	7.6%
2	Win32/CouponRuc	Browser Modifiers	6.1%
3	Win32/InstalleRex	Software Bundlers	4.5%
4	Win32/SaverExtension	Adware	2.2%
5	Win32/AlterbookSP	Browser Modifiers	0.7%

- The most common unwanted software family encountered in Jamaica in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 7.6 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common unwanted software family encountered in Jamaica in 2Q15 was [Win32/CouponRuc](#), which was encountered by 6.1 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The third most common unwanted software family encountered in Jamaica in 2Q15 was [Win32/InstalleRex](#), which was encountered by 4.5 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Jamaica in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	8.1
2	VBS/Jenxcus	Worms	4.1
3	Win32/Kilim	Trojans	2.0
4	Win32/Brontok	Worms	0.9
5	Win32/Gamarue	Worms	0.9
6	Win32/CompromisedCert	Other Malware	0.5
7	Win32/Vobfus	Worms	0.5
8	MSIL/Bladabindi	Backdoors	0.4
9	Win32/Sality	Viruses	0.4
10	Win32/Virut	Viruses	0.3

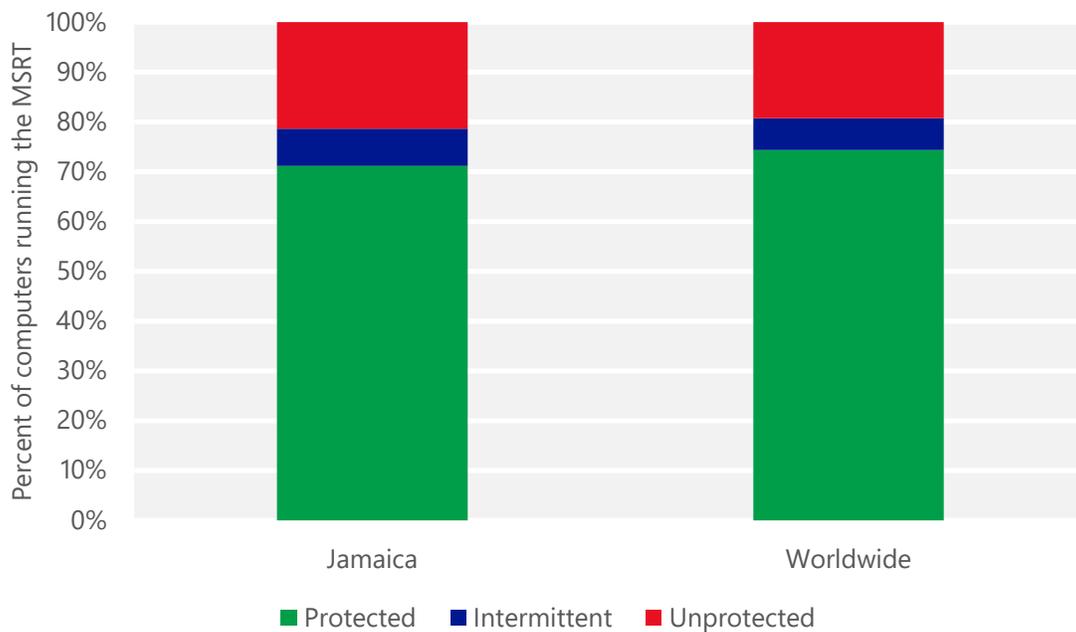
- The most common threat family infecting computers in Jamaica in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 8.1 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Jamaica in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 4.1 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The third most common threat family infecting computers in Jamaica in 2Q15 was [Win32/Kilim](#), which was detected and removed from 2.0 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The fourth most common threat family infecting computers in Jamaica in 2Q15 was [Win32/Brontok](#), which was detected and removed from 0.9 of every 1,000 unique computers scanned by the MSRT. [Win32/Brontok](#) is a mass-mailing email worm that spreads by sending copies of itself as email attachments to addresses gathered from files on the infected computer, and by copying itself to removable volumes. Brontok can disable security software, and may conduct DoS attacks against certain websites.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Jamaica and worldwide protected by real-time security software in 2Q15



Japan

The statistics presented here are generated by Microsoft security programs and services running on computers in Japan in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Japan

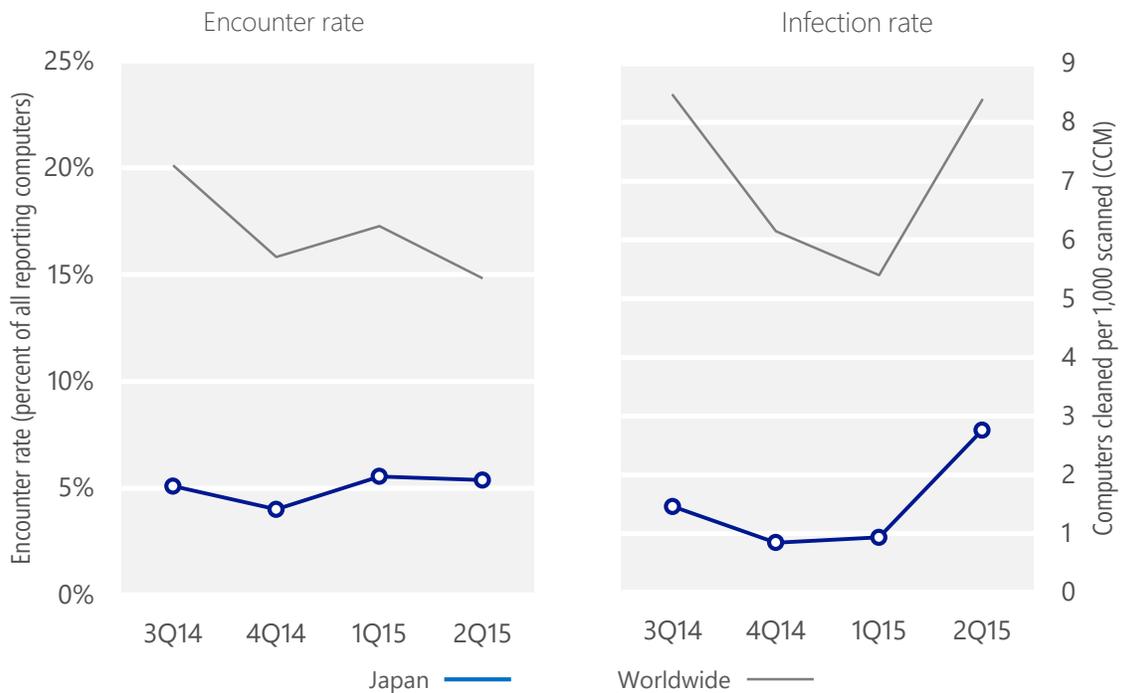
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Japan	5.1%	4.0%	5.5%	5.4%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Japan	1.5	0.8	0.9	2.8
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcout, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 5.4% of computers in Japan encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 2.8 of every 1,000 unique computers scanned in Japan in 2Q15 (a CCM score of 2.8, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Japan over the last four quarters, compared to the world as a whole.

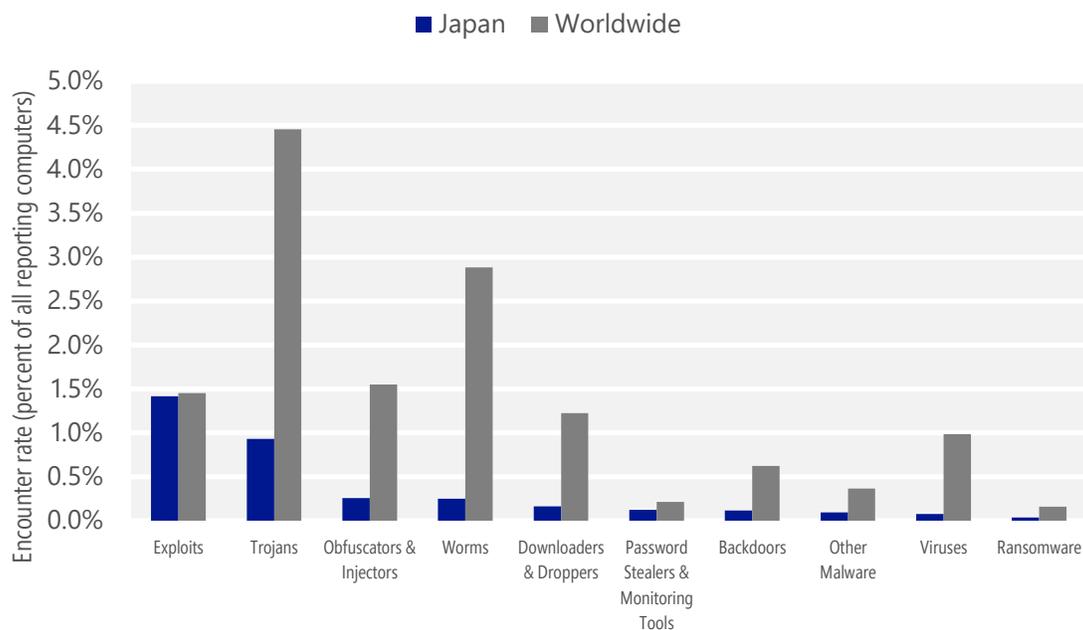
Malware encounter and infection rate trends in Japan and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in Japan and around the world, and for explanations of the methods and terms used here.

Malware categories

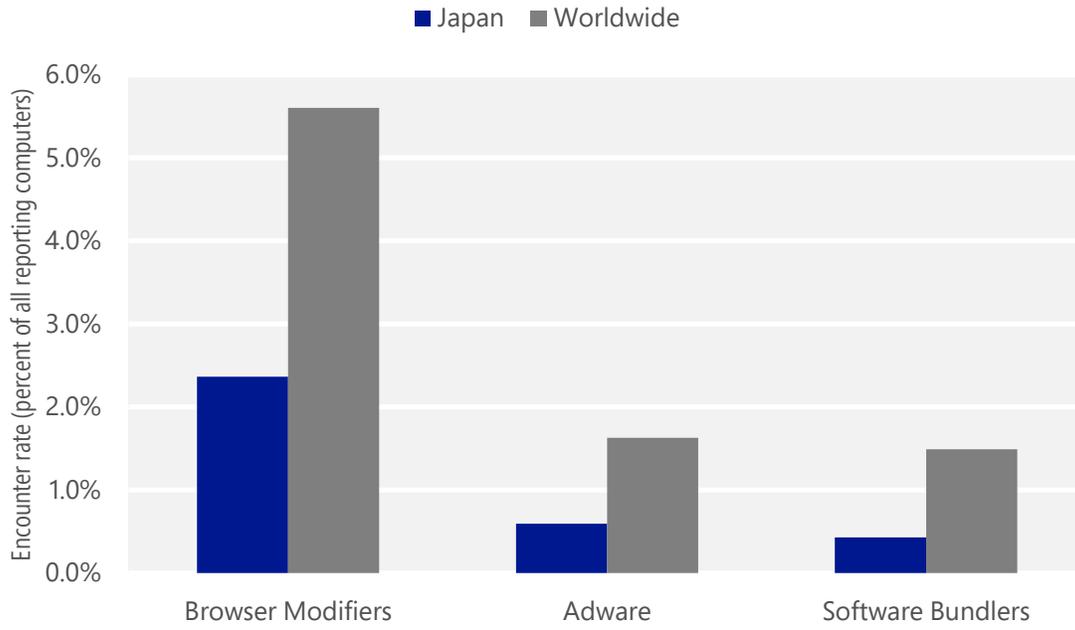
Malware encountered in Japan in 2Q15, by category



- The most common malware category in Japan in 2Q15 was Exploits. It was encountered by 1.4 percent of all computers there, down from 1.8 percent in 1Q15.
- The second most common malware category in Japan in 2Q15 was Trojans. It was encountered by 0.9 percent of all computers there, up from 0.5 percent in 1Q15.
- The third most common malware category in Japan in 2Q15 was Obfuscators & Injectors, which was encountered by 0.3 percent of all computers there, down from 0.4 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Japan in 2Q15, by category



- The most common unwanted software category in Japan in 2Q15 was Browser Modifiers. It was encountered by 2.4 percent of all computers there, up from 1.8 percent in 1Q15.
- The second most common unwanted software category in Japan in 2Q15 was Adware. It was encountered by 0.6 percent of all computers there, down from 1.4 percent in 1Q15.
- The third most common unwanted software category in Japan in 2Q15 was Software Bundlers, which was encountered by 0.4 percent of all computers there, up from 0.1 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Japan in 2Q15

	Family	Most significant category	% of reporting computers
1	JS/Axpergle	Exploits	1.1%
2	Win32/Skeeyah	Trojans	0.2%
3	JS/Neclu	Exploits	0.2%
4	Win32/Obfuscator	Obfuscators & Injectors	0.2%
5	Win32/Kilim	Trojans	0.2%
6	Win32/Peals	Trojans	0.2%
7	INF/Autorun	Obfuscators & Injectors	0.1%
8	Win32/Zbot	Password Stealers & Monitoring Tools	0.1%
9	Win32/Conficker	Worms	0.1%
10	Win32/Dynamer	Trojans	0.1%

- The most common malware family encountered in Japan in 2Q15 was [JS/Axpergle](#), which was encountered by 1.1 percent of reporting computers there. [JS/Axpergle](#) is a detection for the Angler exploit kit, which exploits vulnerabilities in recent versions of Internet Explorer, Silverlight, Adobe Flash Player, and Java to install malware.
- The second most common malware family encountered in Japan in 2Q15 was [Win32/Skeeyah](#), which was encountered by 0.2 percent of reporting computers there. [Win32/Skeeyah](#) is a generic detection for various threats that display trojan characteristics.
- The third most common malware family encountered in Japan in 2Q15 was [JS/Neclu](#), which was encountered by 0.2 percent of reporting computers there. [JS/Neclu](#) is a detection for the Nuclear exploit kit, which attempts to exploit vulnerabilities in programs such as Java and Adobe Reader to install other malware.
- The fourth most common malware family encountered in Japan in 2Q15 was [Win32/Obfuscator](#), which was encountered by 0.2 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Japan in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/AlterbookSP	Browser Modifiers	0.9%
2	Win32/CouponRuc	Browser Modifiers	0.8%
3	Win32/InstalleRex	Software Bundlers	0.4%
4	Win32/KipodToolsCby	Browser Modifiers	0.3%
5	Win32/SaverExtension	Adware	0.3%

- The most common unwanted software family encountered in Japan in 2Q15 was [Win32/AlterbookSP](#), which was encountered by 0.9 percent of reporting computers there. [Win32/AlterbookSP](#) is a browser add-on that formerly displayed behaviors of unwanted software. Recent versions of the add-on no longer meet Microsoft detection criteria, and are no longer considered unwanted software.
- The second most common unwanted software family encountered in Japan in 2Q15 was [Win32/CouponRuc](#), which was encountered by 0.8 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The third most common unwanted software family encountered in Japan in 2Q15 was [Win32/InstalleRex](#), which was encountered by 0.4 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own “Installed On” date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Japan in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/Zbot	Password Stealers & Monitoring Tools	0.8
2	Win32/leEnablerCby	Browser Modifiers	0.5
3	Win32/CompromisedCert	Other Malware	0.5
4	Win32/Kilim	Trojans	0.4
5	Win32/Nitol	Other Malware	0.1
6	Win32/Alureon	Trojans	0.1
7	Win32/Carberp	Trojans	<0.1
8	Win32/Simda	Trojans	<0.1
9	Win32/Sality	Viruses	<0.1
10	Win32/Conficker	Worms	<0.1

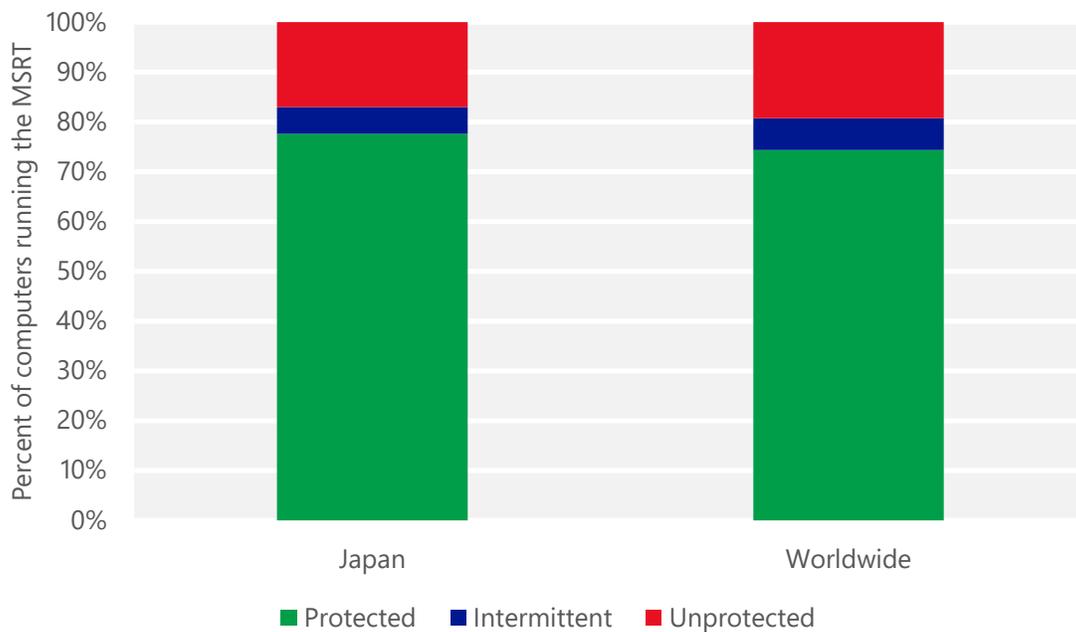
- The most common threat family infecting computers in Japan in 2Q15 was [Win32/Zbot](#), which was detected and removed from 0.8 of every 1,000 unique computers scanned by the MSRT. [Win32/Zbot](#) is a family of password stealing trojans that also contains backdoor functionality allowing unauthorized access and control of an affected computer.
- The second most common threat family infecting computers in Japan in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 0.5 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common threat family infecting computers in Japan in 2Q15 was [Win32/CompromisedCert](#), which was detected and removed from 0.5 of every 1,000 unique computers scanned by the MSRT. [Win32/CompromisedCert](#) is a detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.
- The fourth most common threat family infecting computers in Japan in 2Q15 was [Win32/Kilim](#), which was detected and removed from 0.4 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Japan and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Japan

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.06 (0.28)	0.05 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	1.55 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	14.72 (16.7)	

Jordan

The statistics presented here are generated by Microsoft security programs and services running on computers in Jordan in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Jordan

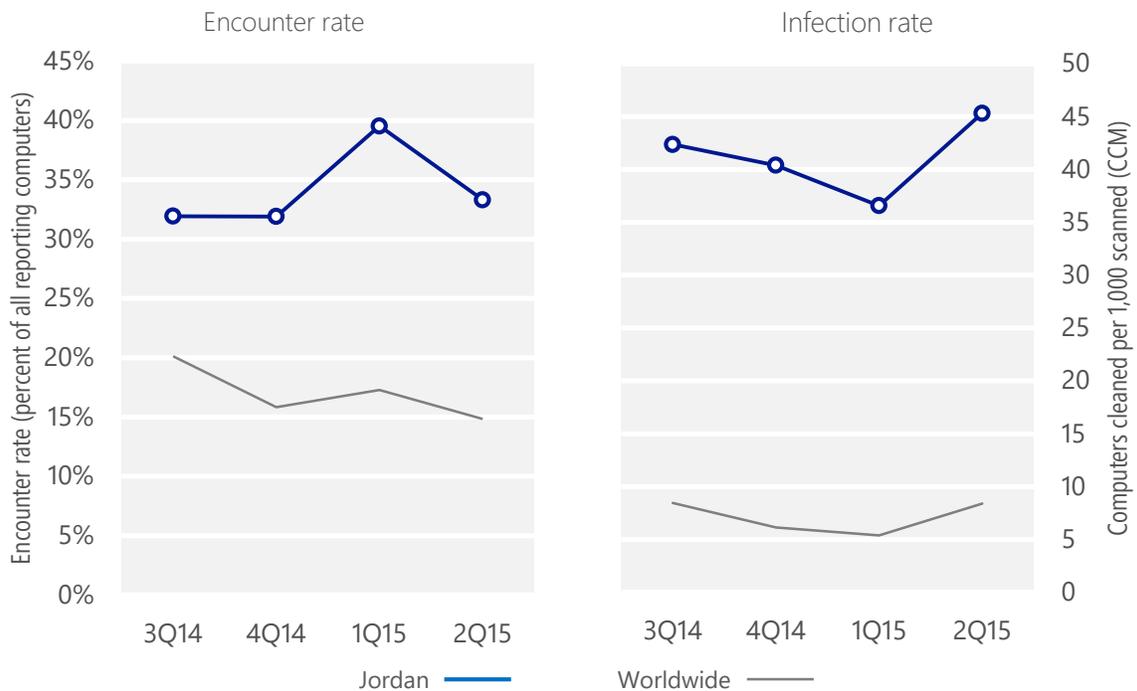
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Jordan	31.9%	31.9%	39.5%	33.3%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Jordan	42.4	40.4	36.6	45.3
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcote, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 33.3% of computers in Jordan encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 45.3 of every 1,000 unique computers scanned in Jordan in 2Q15 (a CCM score of 45.3, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Jordan over the last four quarters, compared to the world as a whole.

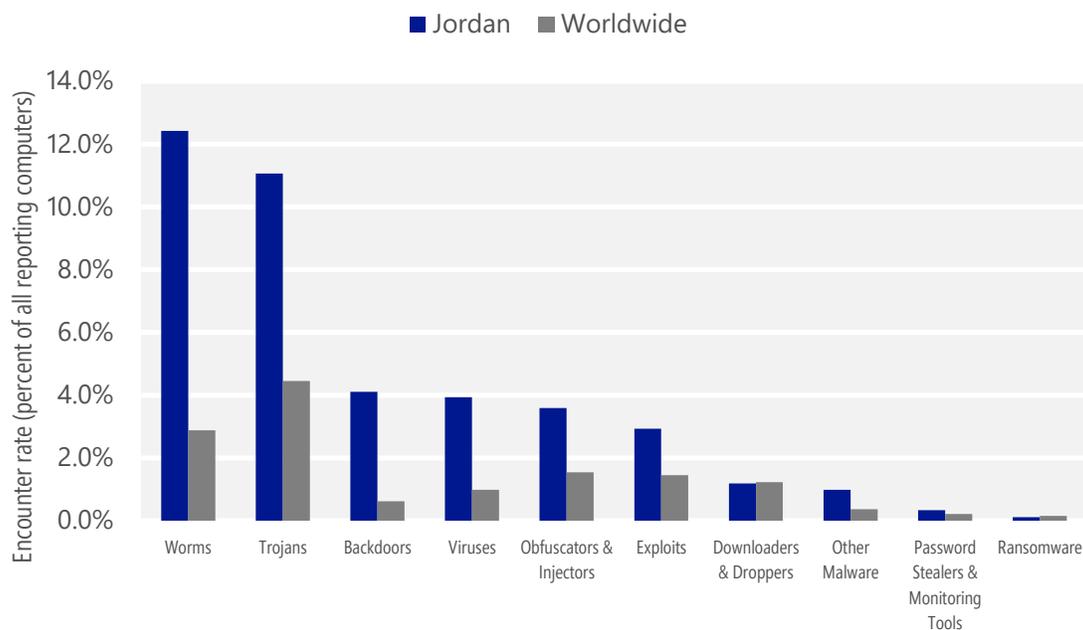
Malware encounter and infection rate trends in Jordan and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in Jordan and around the world, and for explanations of the methods and terms used here.

Malware categories

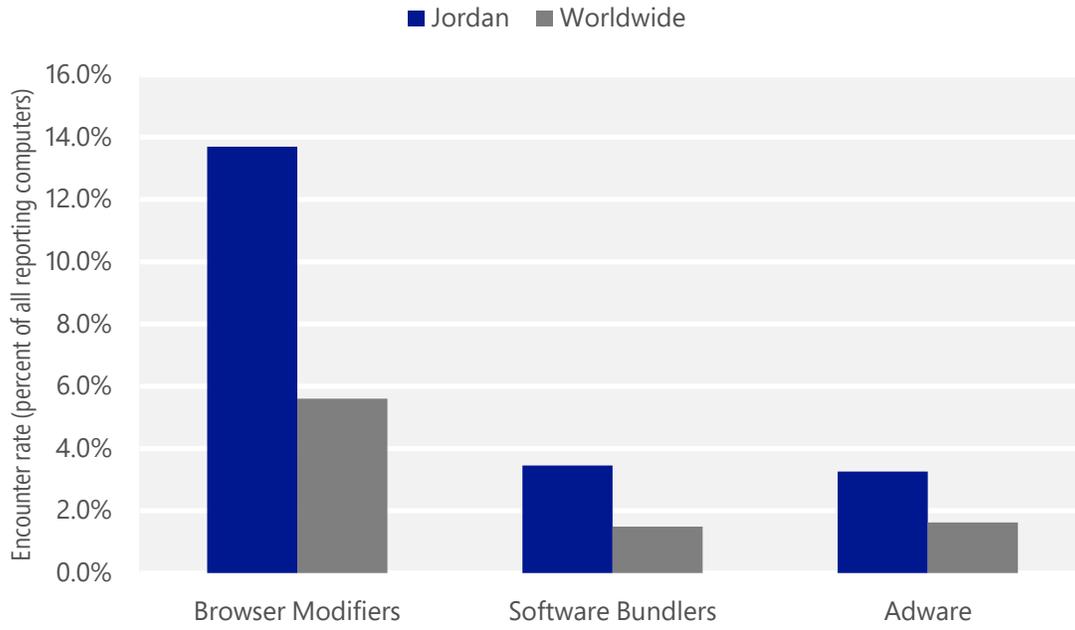
Malware encountered in Jordan in 2Q15, by category



- The most common malware category in Jordan in 2Q15 was Worms. It was encountered by 12.4 percent of all computers there, down from 13.2 percent in 1Q15.
- The second most common malware category in Jordan in 2Q15 was Trojans. It was encountered by 11.1 percent of all computers there, up from 8.9 percent in 1Q15.
- The third most common malware category in Jordan in 2Q15 was Backdoors, which was encountered by 4.1 percent of all computers there, down from 4.5 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Jordan in 2Q15, by category



- The most common unwanted software category in Jordan in 2Q15 was Browser Modifiers. It was encountered by 13.7 percent of all computers there, down from 21.0 percent in 1Q15.
- The second most common unwanted software category in Jordan in 2Q15 was Software Bundlers. It was encountered by 3.5 percent of all computers there, down from 7.0 percent in 1Q15.
- The third most common unwanted software category in Jordan in 2Q15 was Adware, which was encountered by 3.3 percent of all computers there, up from 2.0 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Jordan in 2Q15

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	6.9%
2	Win32/Gamarue	Worms	3.8%
3	Win32/Caphaw	Backdoors	2.5%
4	INF/Autorun	Obfuscators & Injectors	2.4%
5	Win32/Sality	Viruses	2.2%
6	Win32/CplLnk	Exploits	2.0%
7	Win32/Ramnit	Trojans	2.0%
8	Win32/Obfuscator	Obfuscators & Injectors	1.7%
9	Win32/Kilim	Trojans	1.6%
10	Win32/Sulunch	Trojans	1.5%

- The most common malware family encountered in Jordan in 2Q15 was [VBS/Jenxcus](#), which was encountered by 6.9 percent of reporting computers there. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common malware family encountered in Jordan in 2Q15 was [Win32/Gamarue](#), which was encountered by 3.8 percent of reporting computers there. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The third most common malware family encountered in Jordan in 2Q15 was [Win32/Caphaw](#), which was encountered by 2.5 percent of reporting computers there. [Win32/Caphaw](#) is a family of backdoors that spread via Facebook, YouTube, Skype, removable drives, and drive-by download. It can make Facebook posts via the user's account, and may steal online banking details.
- The fourth most common malware family encountered in Jordan in 2Q15 was [INF/Autorun](#), which was encountered by 2.4 percent of reporting computers there. [INF/Autorun](#) is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Jordan in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/KipodToolsCby	Browser Modifiers	6.9%
2	Win32/CouponRuc	Browser Modifiers	6.7%
3	Win32/InstalleRex	Software Bundlers	3.2%
4	Win32/SaverExtension	Adware	2.2%
5	Win32/AlterbookSP	Browser Modifiers	0.7%

- The most common unwanted software family encountered in Jordan in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 6.9 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common unwanted software family encountered in Jordan in 2Q15 was [Win32/CouponRuc](#), which was encountered by 6.7 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The third most common unwanted software family encountered in Jordan in 2Q15 was [Win32/InstalleRex](#), which was encountered by 3.2 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Jordan in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	13.0
2	Win32/leEnablerCby	Browser Modifiers	7.6
3	Win32/Sality	Viruses	6.8
4	Win32/Gamarue	Worms	6.8
5	Win32/Ramnit	Trojans	3.5
6	MSIL/Bladabindi	Backdoors	2.5
7	Win32/Kilim	Trojans	2.4
8	Win32/Dorkbot	Worms	2.4
9	Win32/Virut	Viruses	1.5
10	Win32/CompromisedCert	Other Malware	1.1

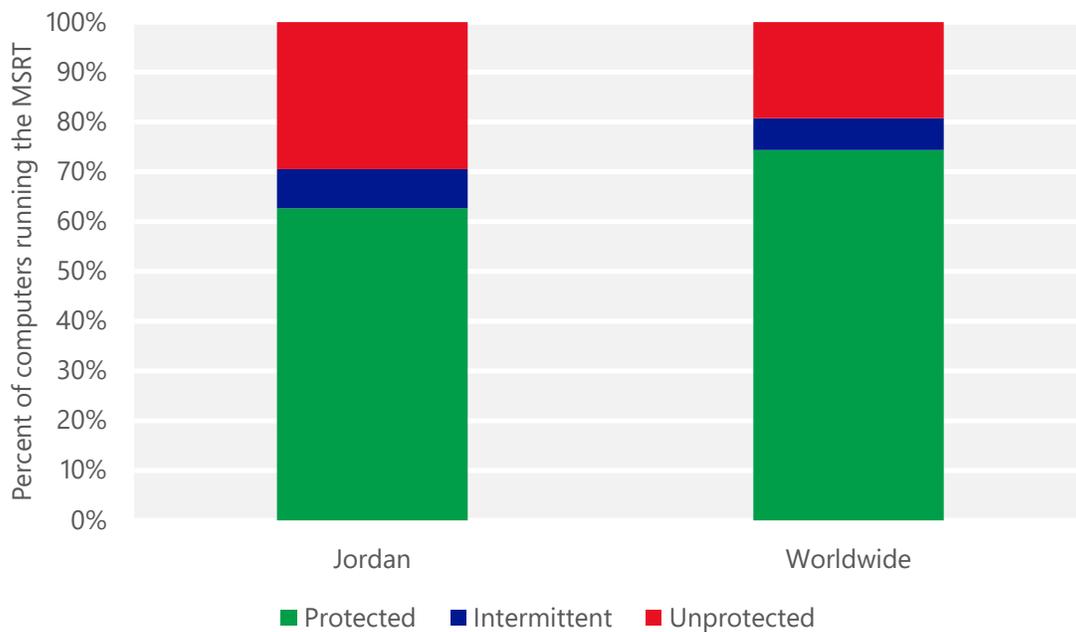
- The most common threat family infecting computers in Jordan in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 13.0 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Jordan in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 7.6 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common threat family infecting computers in Jordan in 2Q15 was [Win32/Sality](#), which was detected and removed from 6.8 of every 1,000 unique computers scanned by the MSRT. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The fourth most common threat family infecting computers in Jordan in 2Q15 was [Win32/Gamarue](#), which was detected and removed from 6.8 of every 1,000 unique computers scanned by the MSRT. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Jordan and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Jordan

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.54 (0.28)	0.17 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	5.40 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	11.09 (16.7)	

Kazakhstan

The statistics presented here are generated by Microsoft security programs and services running on computers in Kazakhstan in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Kazakhstan

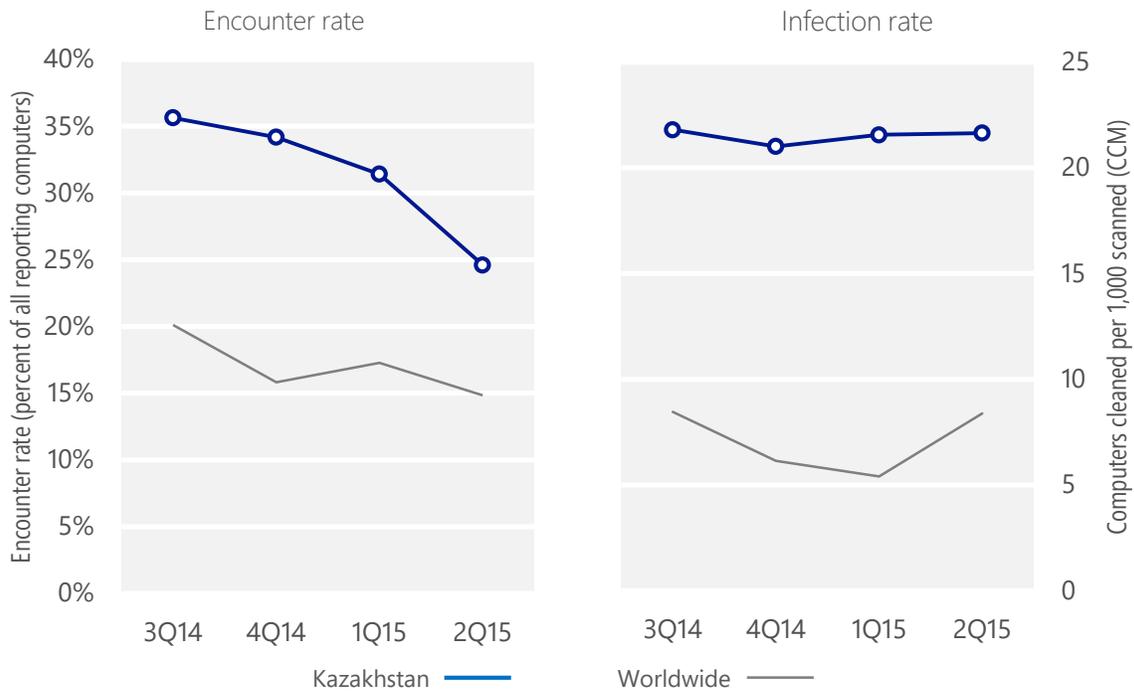
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Kazakhstan	35.6%	34.2%	31.4%	24.6%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Kazakhstan	21.8	21.0	21.6	21.6
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcoute, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 24.6% of computers in Kazakhstan encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 21.6 of every 1,000 unique computers scanned in Kazakhstan in 2Q15 (a CCM score of 21.6, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Kazakhstan over the last four quarters, compared to the world as a whole.

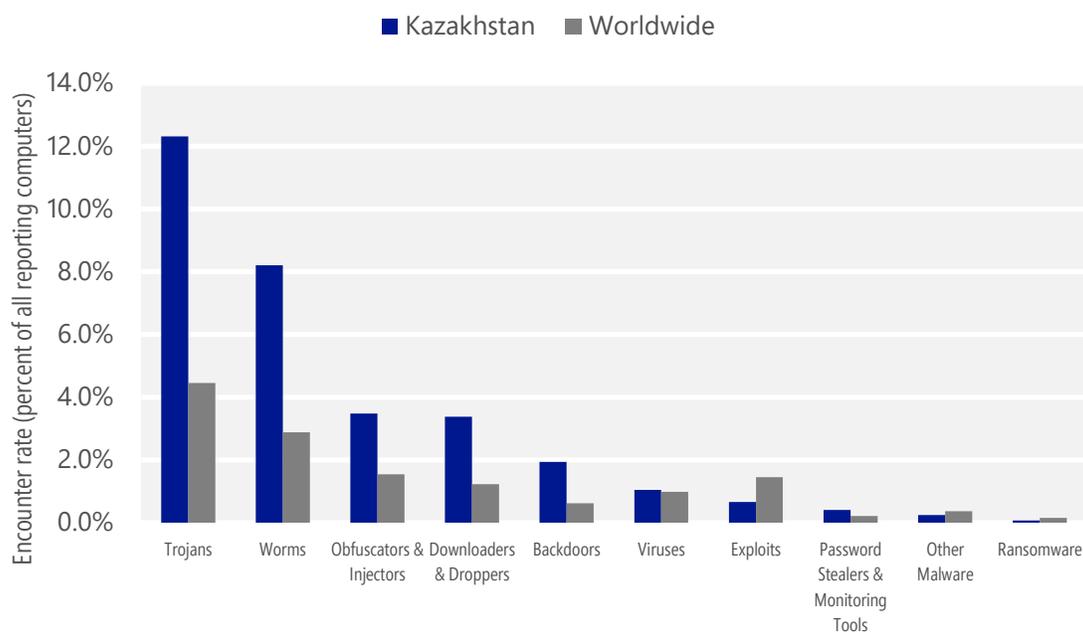
Malware encounter and infection rate trends in Kazakhstan and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in Kazakhstan and around the world, and for explanations of the methods and terms used here.

Malware categories

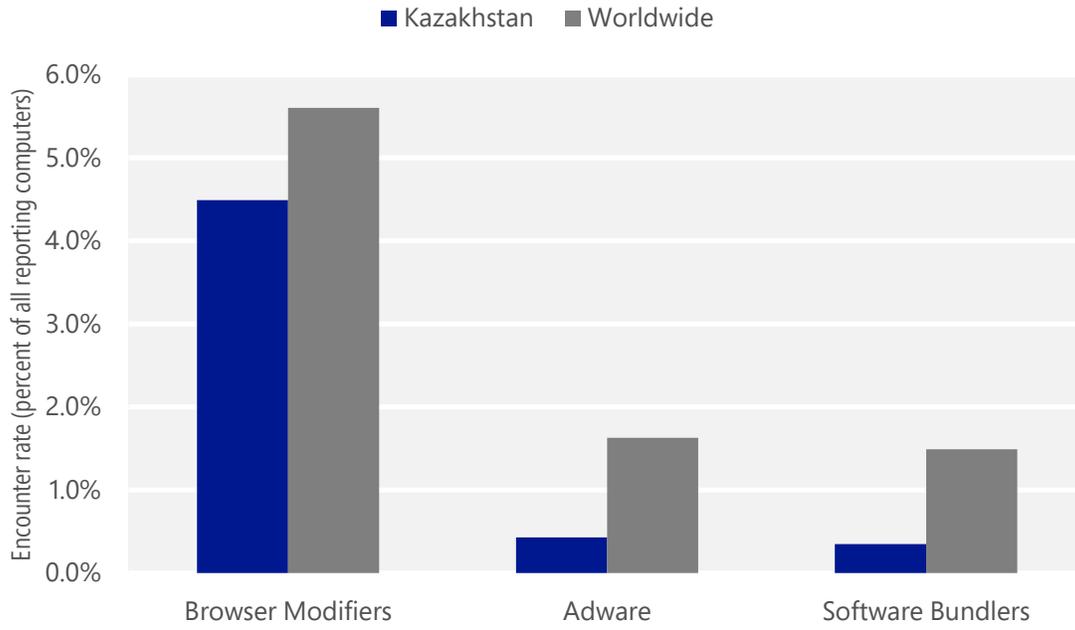
Malware encountered in Kazakhstan in 2Q15, by category



- The most common malware category in Kazakhstan in 2Q15 was Trojans. It was encountered by 12.3 percent of all computers there, down from 15.0 percent in 1Q15.
- The second most common malware category in Kazakhstan in 2Q15 was Worms. It was encountered by 8.2 percent of all computers there, down from 9.5 percent in 1Q15.
- The third most common malware category in Kazakhstan in 2Q15 was Obfuscators & Injectors, which was encountered by 3.5 percent of all computers there, down from 8.8 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Kazakhstan in 2Q15, by category



- The most common unwanted software category in Kazakhstan in 2Q15 was Browser Modifiers. It was encountered by 4.5 percent of all computers there, down from 6.6 percent in 1Q15.
- The second most common unwanted software category in Kazakhstan in 2Q15 was Adware. It was encountered by 0.4 percent of all computers there, down from 0.9 percent in 1Q15.
- The third most common unwanted software category in Kazakhstan in 2Q15 was Software Bundlers, which was encountered by 0.3 percent of all computers there, down from 0.6 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Kazakhstan in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Peals	Trojans	4.8%
2	Win32/Gamarue	Worms	3.2%
3	Win32/Obfuscator	Obfuscators & Injectors	2.8%
4	Win32/Skeeyah	Trojans	1.2%
5	Win32/Ogimant	Downloaders & Droppers	1.2%
6	Win32/Caphaw	Backdoors	1.2%
7	VBS/Jenxcus	Worms	1.1%
8	Win32/Dynamer	Trojans	0.9%
9	Win32/Radonskra	Trojans	0.9%
10	Win32/Vobfus	Worms	0.7%

- The most common malware family encountered in Kazakhstan in 2Q15 was [Win32/Peals](#), which was encountered by 4.8 percent of reporting computers there. [Win32/Peals](#) is a generic detection for various threats that display trojan characteristics.
- The second most common malware family encountered in Kazakhstan in 2Q15 was [Win32/Gamarue](#), which was encountered by 3.2 percent of reporting computers there. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The third most common malware family encountered in Kazakhstan in 2Q15 was [Win32/Obfuscator](#), which was encountered by 2.8 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The fourth most common malware family encountered in Kazakhstan in 2Q15 was [Win32/Skeeyah](#), which was encountered by 1.2 percent of reporting computers there. [Win32/Skeeyah](#) is a generic detection for various threats that display trojan characteristics.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Kazakhstan in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/KipodToolsCby	Browser Modifiers	2.8%
2	Win32/AlterbookSP	Browser Modifiers	0.8%
3	Win32/CouponRuc	Browser Modifiers	0.7%
4	Win32/InstalleRex	Software Bundlers	0.3%
5	Win32/SaverExtension	Adware	0.2%

- The most common unwanted software family encountered in Kazakhstan in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 2.8 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common unwanted software family encountered in Kazakhstan in 2Q15 was [Win32/AlterbookSP](#), which was encountered by 0.8 percent of reporting computers there. [Win32/AlterbookSP](#) is a browser add-on that formerly displayed behaviors of unwanted software. Recent versions of the add-on no longer meet Microsoft detection criteria, and are no longer considered unwanted software.
- The third most common unwanted software family encountered in Kazakhstan in 2Q15 was [Win32/CouponRuc](#), which was encountered by 0.7 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.

Top threat families by infection rate

The most common malware families by infection rate in Kazakhstan in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/Gamarue	Worms	6.6
2	Win32/leEnablerCby	Browser Modifiers	5.2
3	Win32/CompromisedCert	Other Malware	2.6
4	VBS/Jenxcus	Worms	1.9
5	Win32/Ramnit	Trojans	1.5
6	Win32/Vobfus	Worms	1.1
7	Win32/Dorkbot	Worms	0.9
8	Win32/Sality	Viruses	0.6
9	Win32/Lethic	Trojans	0.3
10	Win32/Kilim	Trojans	0.3

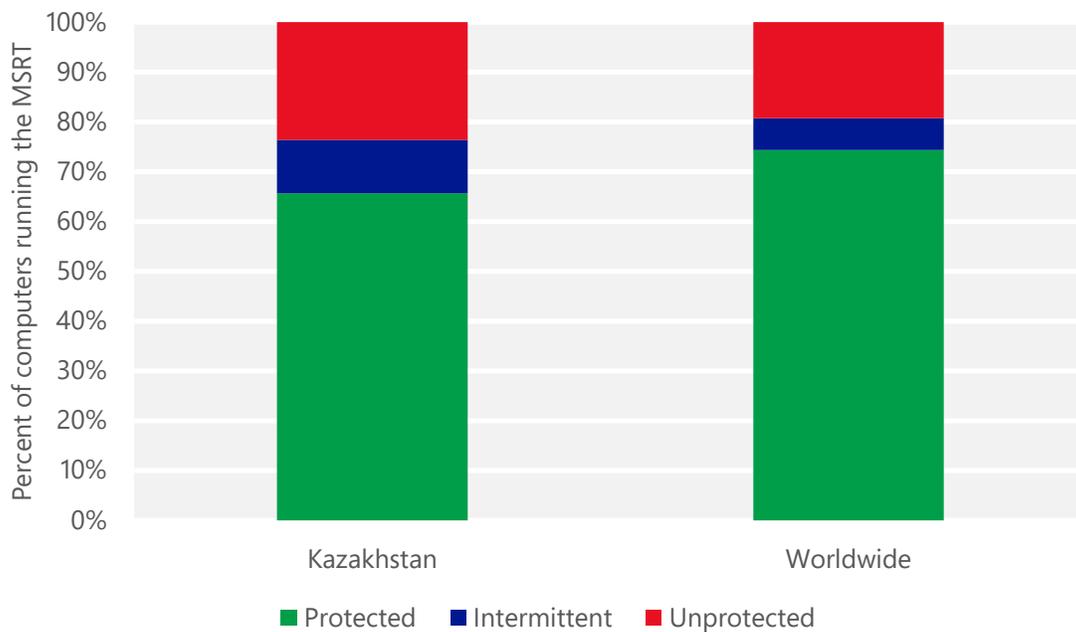
- The most common threat family infecting computers in Kazakhstan in 2Q15 was [Win32/Gamarue](#), which was detected and removed from 6.6 of every 1,000 unique computers scanned by the MSRT. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The second most common threat family infecting computers in Kazakhstan in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 5.2 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common threat family infecting computers in Kazakhstan in 2Q15 was [Win32/CompromisedCert](#), which was detected and removed from 2.6 of every 1,000 unique computers scanned by the MSRT. [Win32/CompromisedCert](#) is a detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.
- The fourth most common threat family infecting computers in Kazakhstan in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 1.9 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Kazakhstan and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Kazakhstan

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.76 (0.28)	0.39 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	11.44 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	19.24 (16.7)	

Kenya

The statistics presented here are generated by Microsoft security programs and services running on computers in Kenya in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Kenya

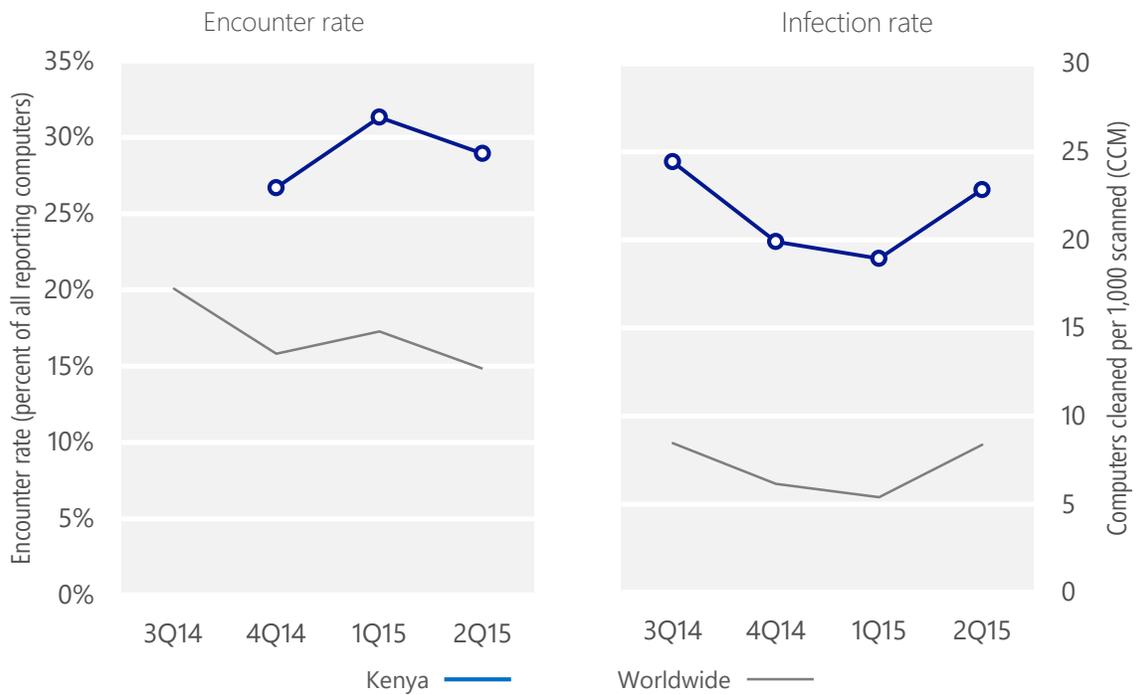
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Kenya	N/A	26.7%	31.3%	28.9%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Kenya	24.4	19.9	18.9	22.9
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcote, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 28.9% of computers in Kenya encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 22.9 of every 1,000 unique computers scanned in Kenya in 2Q15 (a CCM score of 22.9, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Kenya over the last four quarters, compared to the world as a whole.

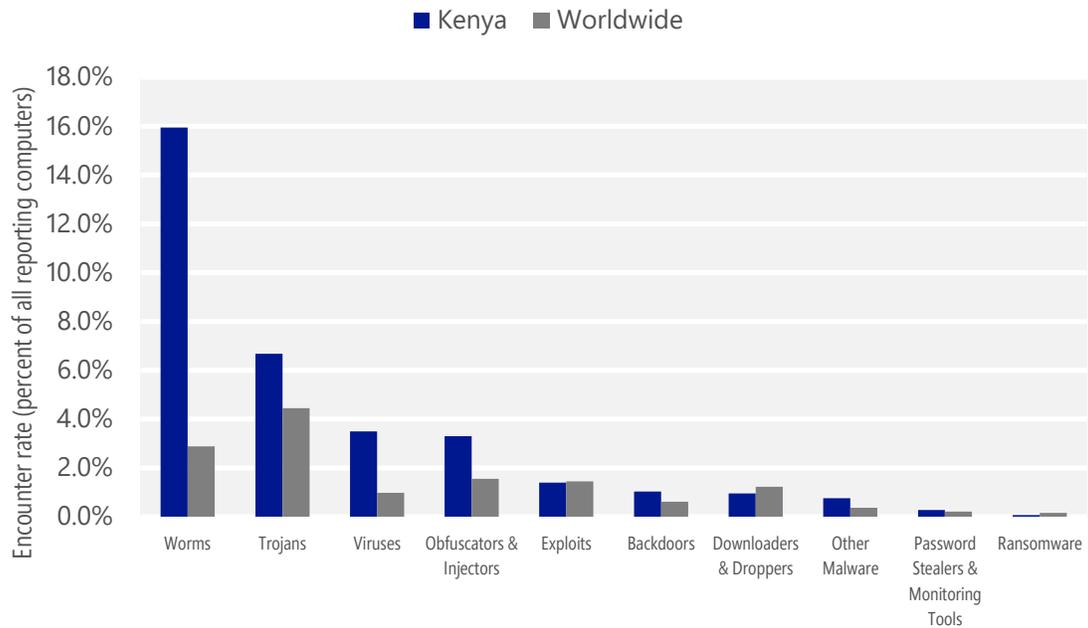
Malware encounter and infection rate trends in Kenya and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in Kenya and around the world, and for explanations of the methods and terms used here.

Malware categories

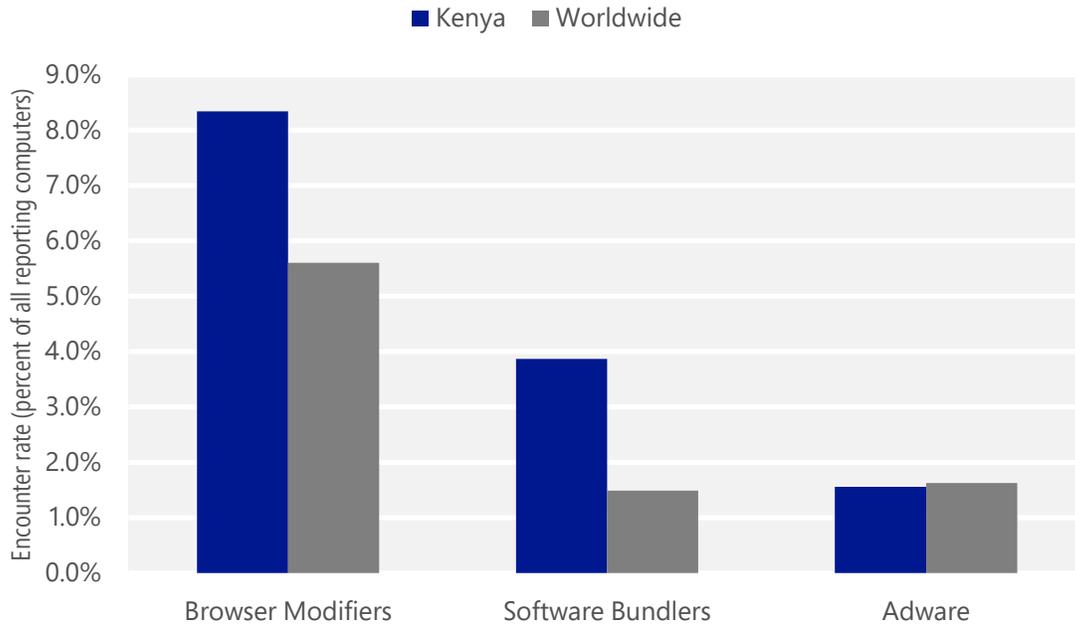
Malware encountered in Kenya in 2Q15, by category



- The most common malware category in Kenya in 2Q15 was Worms. It was encountered by 15.9 percent of all computers there, up from 14.9 percent in 1Q15.
- The second most common malware category in Kenya in 2Q15 was Trojans. It was encountered by 6.7 percent of all computers there, up from 5.5 percent in 1Q15.
- The third most common malware category in Kenya in 2Q15 was Viruses, which was encountered by 3.5 percent of all computers there, down from 4.1 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Kenya in 2Q15, by category



- The most common unwanted software category in Kenya in 2Q15 was Browser Modifiers. It was encountered by 8.3 percent of all computers there, down from 12.3 percent in 1Q15.
- The second most common unwanted software category in Kenya in 2Q15 was Software Bundlers. It was encountered by 3.9 percent of all computers there, up from 3.7 percent in 1Q15.
- The third most common unwanted software category in Kenya in 2Q15 was Adware, which was encountered by 1.6 percent of all computers there, up from 1.3 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Kenya in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Ippedo	Worms	8.6%
2	Win32/Gamarue	Worms	4.6%
3	INF/Autorun	Obfuscators & Injectors	4.4%
4	VBS/Jenxcus	Worms	3.8%
5	Win32/Copali	Worms	2.7%
6	Win32/Sality	Viruses	2.2%
7	Win32/Virut	Viruses	1.4%
8	Win32/Obfuscator	Obfuscators & Injectors	1.2%
9	Win32/Dynamer	Trojans	0.8%
10	Win32/CplLnk	Exploits	0.8%

- The most common malware family encountered in Kenya in 2Q15 was [Win32/Ippedo](#), which was encountered by 8.6 percent of reporting computers there. [Win32/Ippedo](#) is a worm that can send sensitive information to a malicious hacker. It spreads through removable drives, such as USB flash drives.
- The second most common malware family encountered in Kenya in 2Q15 was [Win32/Gamarue](#), which was encountered by 4.6 percent of reporting computers there. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The third most common malware family encountered in Kenya in 2Q15 was [INF/Autorun](#), which was encountered by 4.4 percent of reporting computers there. [INF/Autorun](#) is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The fourth most common malware family encountered in Kenya in 2Q15 was [VBS/Jenxcus](#), which was encountered by 3.8 percent of reporting computers there. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Kenya in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/KipodToolsCby	Browser Modifiers	4.5%
2	Win32/InstalleRex	Software Bundlers	3.7%
3	Win32/CouponRuc	Browser Modifiers	3.7%
4	Win32/SaverExtension	Adware	1.0%
5	Win32/AlterbookSP	Browser Modifiers	0.4%

- The most common unwanted software family encountered in Kenya in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 4.5 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common unwanted software family encountered in Kenya in 2Q15 was [Win32/InstalleRex](#), which was encountered by 3.7 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.
- The third most common unwanted software family encountered in Kenya in 2Q15 was [Win32/CouponRuc](#), which was encountered by 3.7 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.

Top threat families by infection rate

The most common malware families by infection rate in Kenya in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/Gamarue	Worms	6.4
2	VBS/Jenxcus	Worms	4.9
3	Win32/Sality	Viruses	4.7
4	Win32/leEnablerCby	Browser Modifiers	3.1
5	Win32/Virut	Viruses	1.5
6	Win32/CompromisedCert	Other Malware	0.9
7	Win32/Kilim	Trojans	0.8
8	Win32/Ramnit	Trojans	0.8
9	Win32/Pramro	Trojans	0.4
10	Win32/Parite	Viruses	0.3

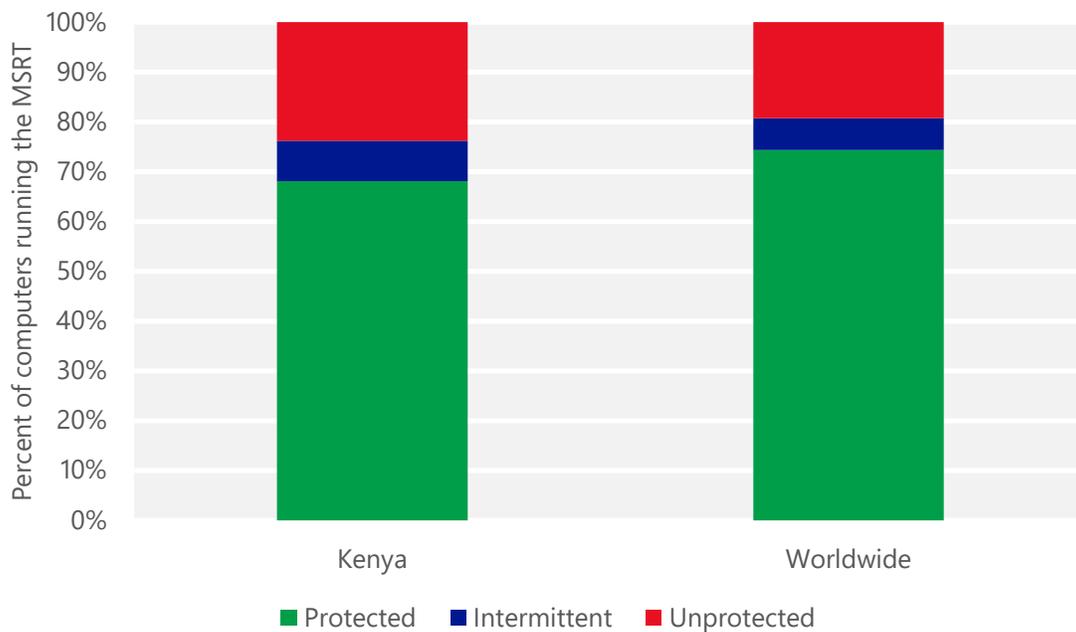
- The most common threat family infecting computers in Kenya in 2Q15 was [Win32/Gamarue](#), which was detected and removed from 6.4 of every 1,000 unique computers scanned by the MSRT. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The second most common threat family infecting computers in Kenya in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 4.9 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The third most common threat family infecting computers in Kenya in 2Q15 was [Win32/Sality](#), which was detected and removed from 4.7 of every 1,000 unique computers scanned by the MSRT. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The fourth most common threat family infecting computers in Kenya in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 3.1 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Kenya and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Kenya

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	2.17 (0.28)	1.60 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	5.92 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	7.64 (16.7)	

Korea

The statistics presented here are generated by Microsoft security programs and services running on computers in Korea in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Korea

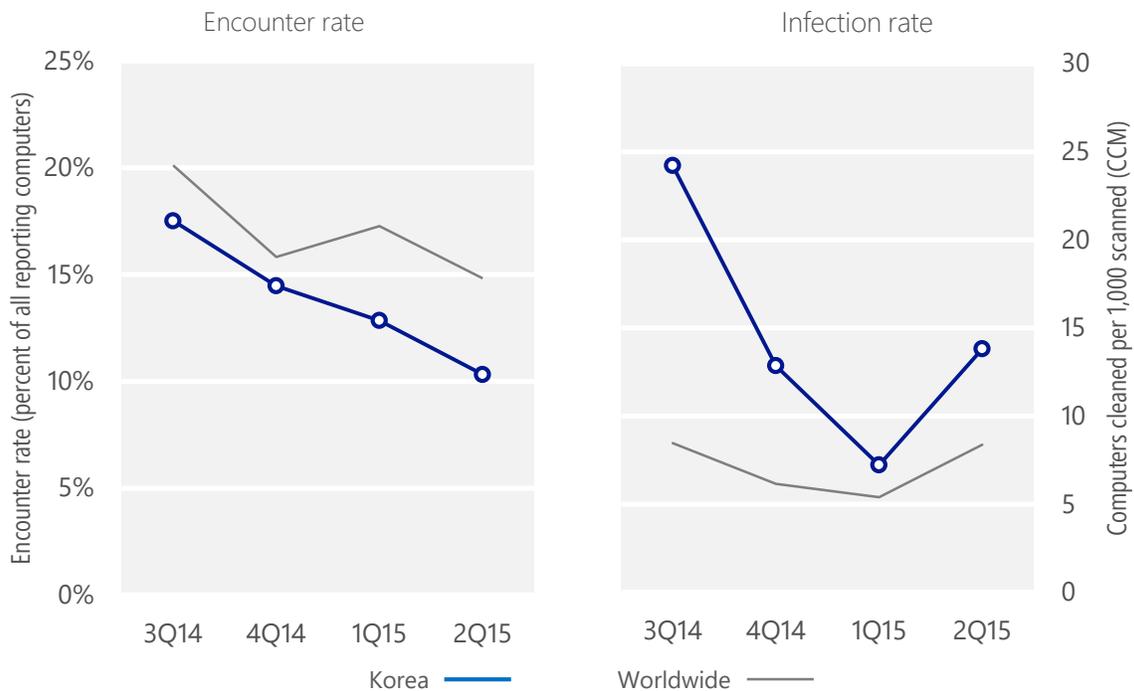
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Korea	17.5%	14.5%	12.8%	10.3%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Korea	24.2	12.9	7.2	13.8
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcote, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 10.3% of computers in Korea encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 13.8 of every 1,000 unique computers scanned in Korea in 2Q15 (a CCM score of 13.8, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Korea over the last four quarters, compared to the world as a whole.

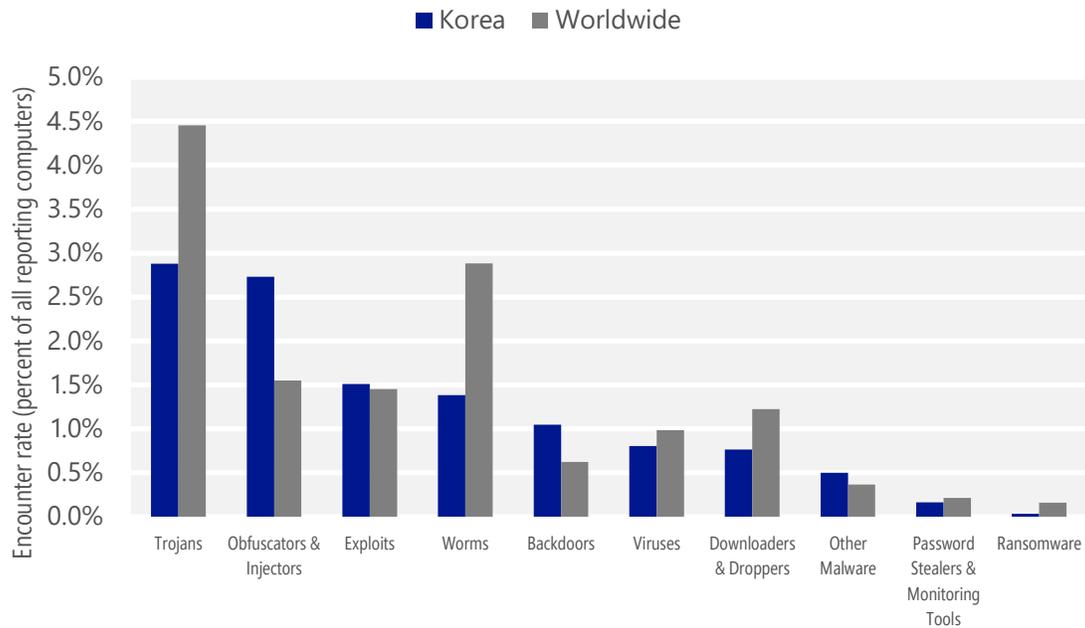
Malware encounter and infection rate trends in Korea and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in Korea and around the world, and for explanations of the methods and terms used here.

Malware categories

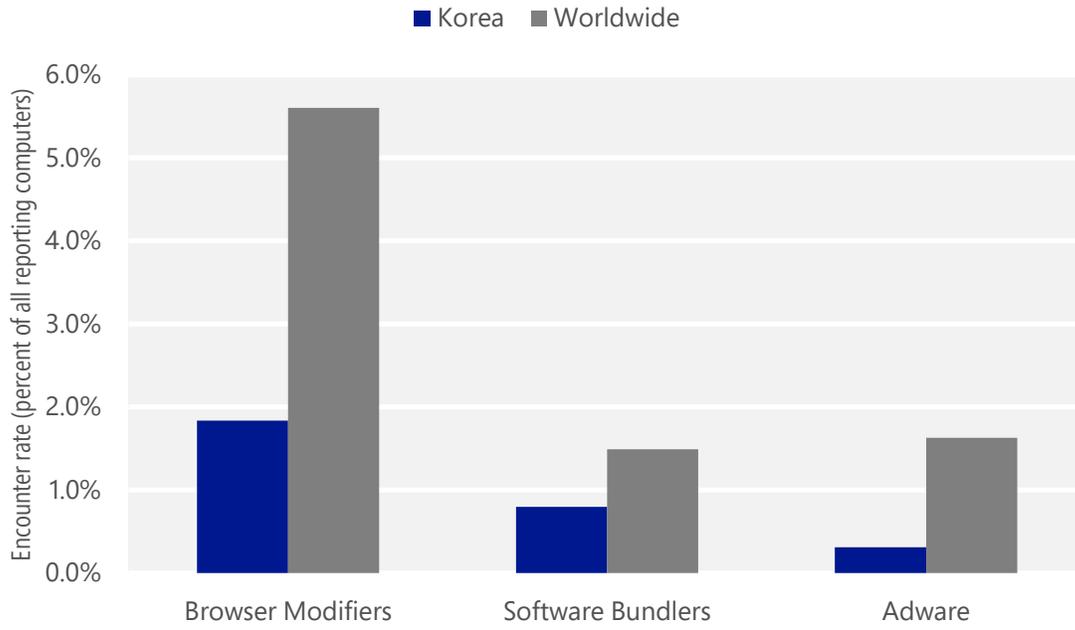
Malware encountered in Korea in 2Q15, by category



- The most common malware category in Korea in 2Q15 was Trojans. It was encountered by 2.9 percent of all computers there, down from 4.0 percent in 1Q15.
- The second most common malware category in Korea in 2Q15 was Obfuscators & Injectors. It was encountered by 2.7 percent of all computers there, down from 3.0 percent in 1Q15.
- The third most common malware category in Korea in 2Q15 was Exploits, which was encountered by 1.5 percent of all computers there, down from 2.6 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Korea in 2Q15, by category



- The most common unwanted software category in Korea in 2Q15 was Browser Modifiers. It was encountered by 1.8 percent of all computers there, down from 2.6 percent in 1Q15.
- The second most common unwanted software category in Korea in 2Q15 was Software Bundlers. It was encountered by 0.8 percent of all computers there, up from 0.7 percent in 1Q15.
- The third most common unwanted software category in Korea in 2Q15 was Adware, which was encountered by 0.3 percent of all computers there, up from 0.2 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Korea in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Obfuscator	Obfuscators & Injectors	2.4%
2	VBS/CVE-2014-6332	Exploits	0.7%
3	JS/DonxRef	Exploits	0.4%
4	VBS/Jenxcus	Worms	0.4%
5	Win32/Skeeyah	Trojans	0.4%
6	Win32/Nitol	Other Malware	0.4%
7	INF/Autorun	Obfuscators & Injectors	0.3%
8	Win32/Peals	Trojans	0.3%
9	Win32/Dynamer	Trojans	0.3%
10	HTML/Adodb	Downloaders & Droppers	0.2%

- The most common malware family encountered in Korea in 2Q15 was [Win32/Obfuscator](#), which was encountered by 2.4 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The second most common malware family encountered in Korea in 2Q15 was [VBS/CVE-2014-6332](#), which was encountered by 0.7 percent of reporting computers there. [VBS/CVE-2014-6332](#) is a detection for threats that use a vulnerability in Windows to download and run files on the computer, including other malware. Microsoft addressed the vulnerability with Security Bulletin MS14-064 in November 2014.
- The third most common malware family encountered in Korea in 2Q15 was [JS/DonxRef](#), which was encountered by 0.4 percent of reporting computers there. [JS/DonxRef](#) is a generic detection for malicious JavaScript objects that construct shellcode. The scripts may try to exploit vulnerabilities in Java, Adobe Flash Player, and Windows.
- The fourth most common malware family encountered in Korea in 2Q15 was [VBS/Jenxcus](#), which was encountered by 0.4 percent of reporting computers there. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Korea in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/InstalleRex	Software Bundlers	0.8%
2	Win32/KipodToolsCby	Browser Modifiers	0.7%
3	Win32/CouponRuc	Browser Modifiers	0.6%
4	Win32/AlterbookSP	Browser Modifiers	0.4%
5	Win32/SaverExtension	Adware	0.2%

- The most common unwanted software family encountered in Korea in 2Q15 was [Win32/InstalleRex](#), which was encountered by 0.8 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own “Installed On” date in Programs and Features to make it more difficult for a user to locate it and remove it.
- The second most common unwanted software family encountered in Korea in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 0.7 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user’s consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common unwanted software family encountered in Korea in 2Q15 was [Win32/CouponRuc](#), which was encountered by 0.6 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.

Top threat families by infection rate

The most common malware families by infection rate in Korea in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/OnLineGames	Password Stealers & Monitoring Tools	3.0
2	Win32/Nitol	Other Malware	2.7
3	Win32/Enterak	Password Stealers & Monitoring Tools	2.3
4	Win32/leEnablerCby	Browser Modifiers	2.1
5	Win32/Onescan	Other Malware	1.7
6	Win32/Banker	Trojans	0.9
7	VBS/Jenxcus	Worms	0.6
8	Win32/Kilim	Trojans	0.5
9	Win32/Virut	Viruses	0.4
10	MSIL/Bladabindi	Backdoors	0.3

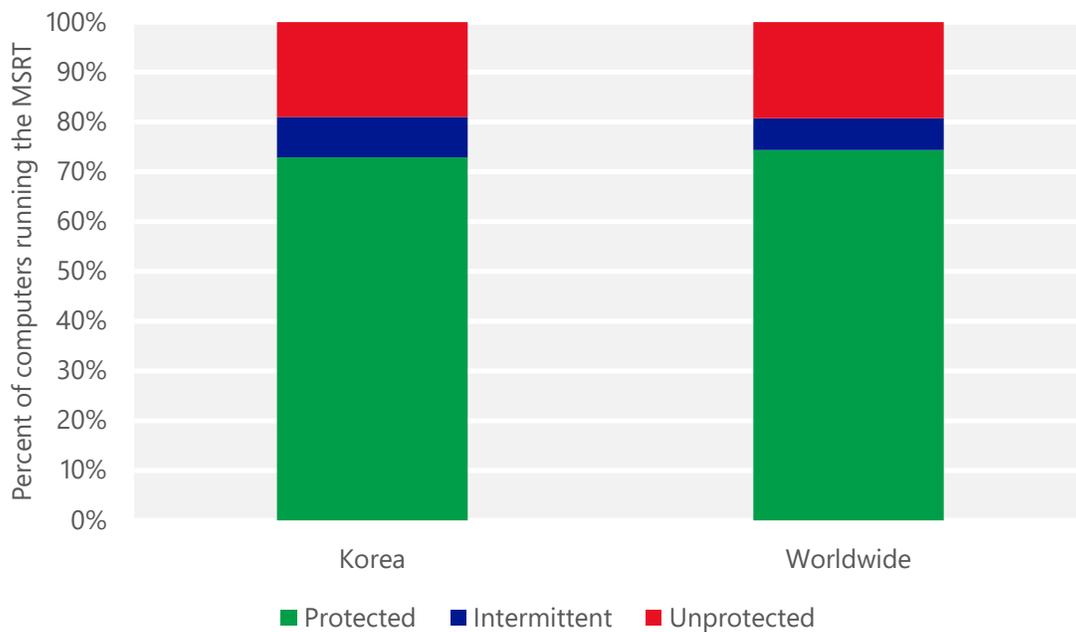
- The most common threat family infecting computers in Korea in 2Q15 was [Win32/OnLineGames](#), which was detected and removed from 3.0 of every 1,000 unique computers scanned by the MSRT.
- The second most common threat family infecting computers in Korea in 2Q15 was [Win32/Nitol](#), which was detected and removed from 2.7 of every 1,000 unique computers scanned by the MSRT. [Win32/Nitol](#) is a family of trojans that perform DDoS (distributed denial of service) attacks, allow backdoor access and control, download and run files, and perform a number of other malicious activities on the computer.
- The third most common threat family infecting computers in Korea in 2Q15 was [Win32/Enterak](#), which was detected and removed from 2.3 of every 1,000 unique computers scanned by the MSRT. [Win32/Enterak](#) is a threat that can steal online game and banking credentials when the user visits certain websites. It can be installed by TrojanDropper:WinNT/Enterok.
- The fourth most common threat family infecting computers in Korea in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 2.1 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Korea and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Korea

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	1.13 (0.28)	0.32 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	1.56 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	6.11 (16.7)	

Kuwait

The statistics presented here are generated by Microsoft security programs and services running on computers in Kuwait in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Kuwait

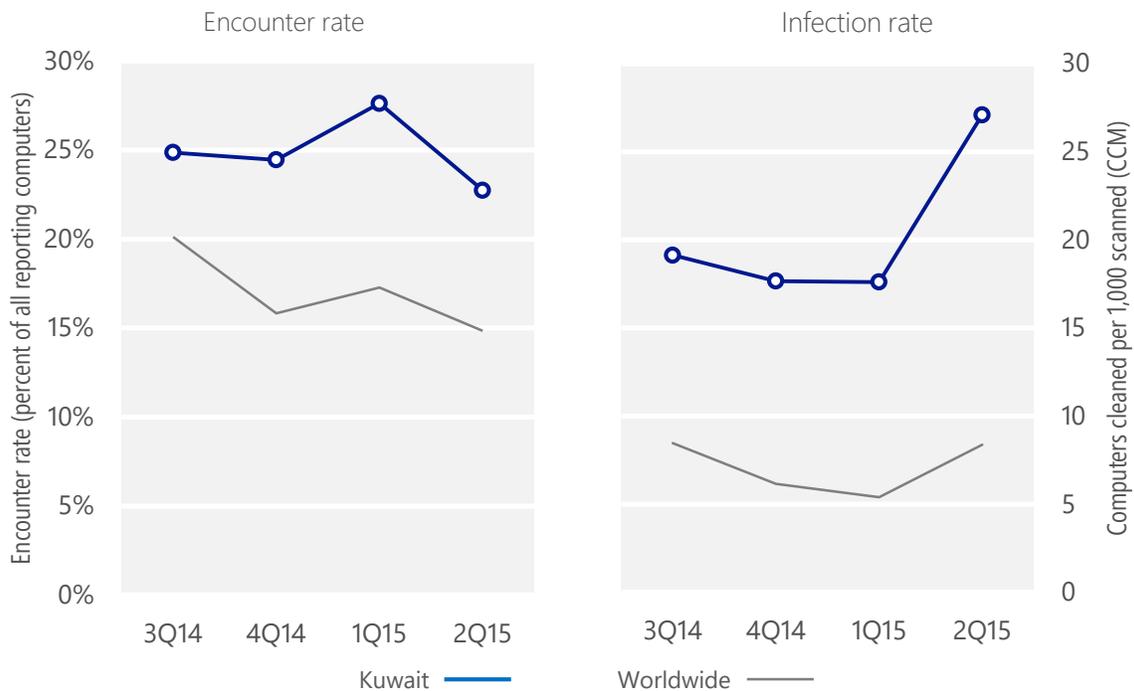
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Kuwait	24.9%	24.4%	27.6%	22.7%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Kuwait	19.1	17.7	17.6	27.1
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcout, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 22.7% of computers in Kuwait encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 27.1 of every 1,000 unique computers scanned in Kuwait in 2Q15 (a CCM score of 27.1, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Kuwait over the last four quarters, compared to the world as a whole.

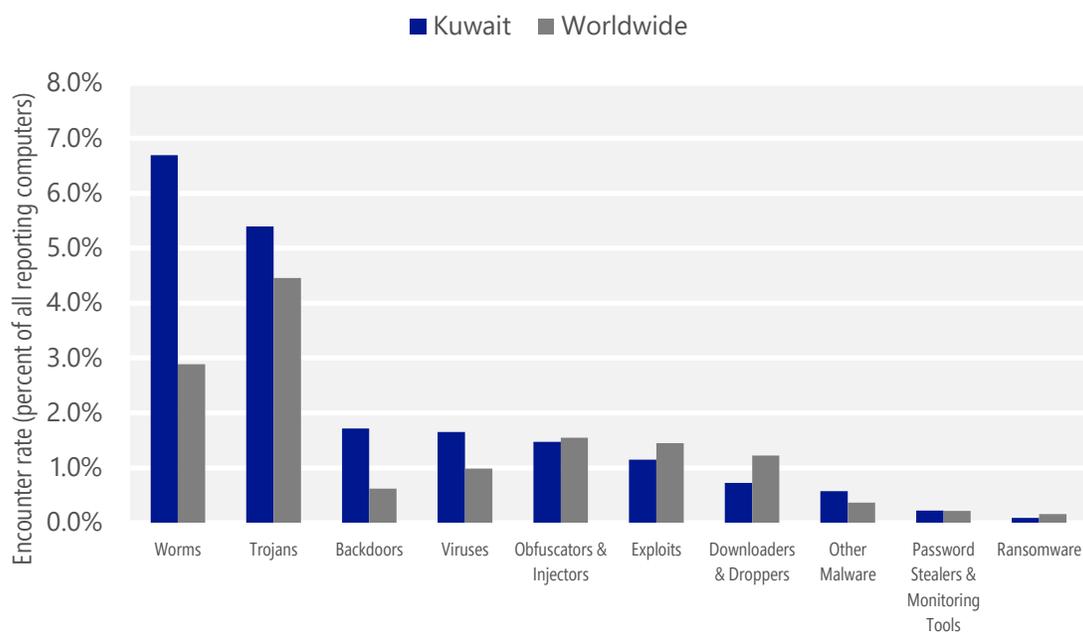
Malware encounter and infection rate trends in Kuwait and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in Kuwait and around the world, and for explanations of the methods and terms used here.

Malware categories

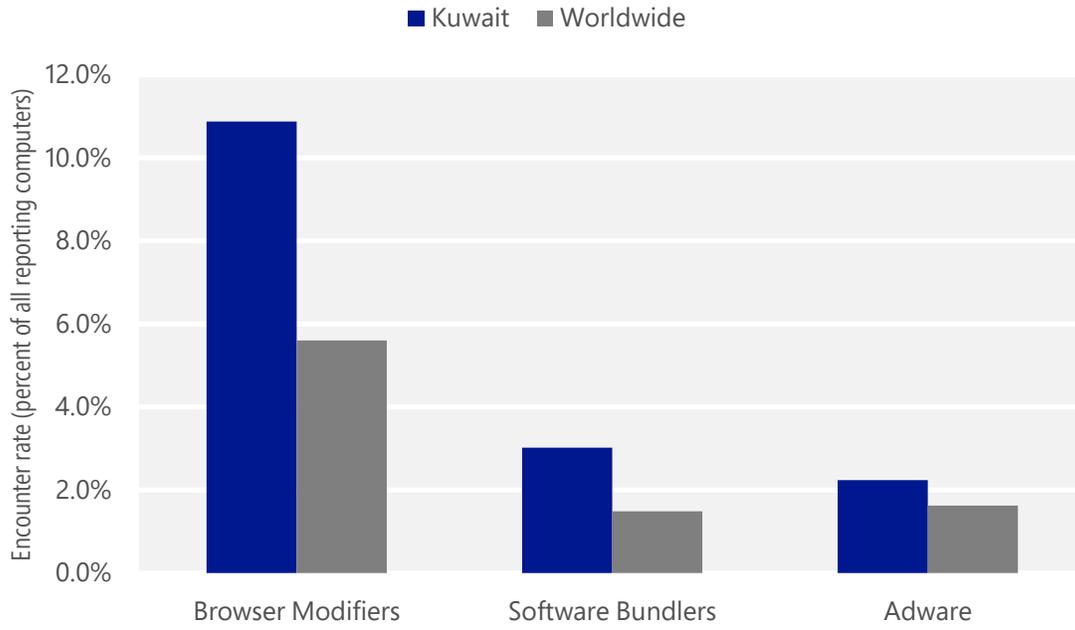
Malware encountered in Kuwait in 2Q15, by category



- The most common malware category in Kuwait in 2Q15 was Worms. It was encountered by 6.7 percent of all computers there, down from 7.4 percent in 1Q15.
- The second most common malware category in Kuwait in 2Q15 was Trojans. It was encountered by 5.4 percent of all computers there, up from 4.3 percent in 1Q15.
- The third most common malware category in Kuwait in 2Q15 was Backdoors, which was encountered by 1.7 percent of all computers there, down from 2.0 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Kuwait in 2Q15, by category



- The most common unwanted software category in Kuwait in 2Q15 was Browser Modifiers. It was encountered by 10.9 percent of all computers there, down from 15.5 percent in 1Q15.
- The second most common unwanted software category in Kuwait in 2Q15 was Software Bundlers. It was encountered by 3.0 percent of all computers there, down from 5.9 percent in 1Q15.
- The third most common unwanted software category in Kuwait in 2Q15 was Adware, which was encountered by 2.2 percent of all computers there, up from 1.1 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Kuwait in 2Q15

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	2.4%
2	Win32/Gamarue	Worms	1.4%
3	Win32/Skeeyah	Trojans	1.4%
4	INF/Autorun	Obfuscators & Injectors	0.9%
5	Win32/Kilim	Trojans	0.9%
6	Win32/Caphaw	Backdoors	0.8%
7	Win32/Obfuscator	Obfuscators & Injectors	0.7%
8	Win32/Vermis	Worms	0.6%
9	Win32/Peals	Trojans	0.6%
10	Win32/Sality	Viruses	0.6%

- The most common malware family encountered in Kuwait in 2Q15 was [VBS/Jenxcus](#), which was encountered by 2.4 percent of reporting computers there. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common malware family encountered in Kuwait in 2Q15 was [Win32/Gamarue](#), which was encountered by 1.4 percent of reporting computers there. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The third most common malware family encountered in Kuwait in 2Q15 was [Win32/Skeeyah](#), which was encountered by 1.4 percent of reporting computers there. [Win32/Skeeyah](#) is a generic detection for various threats that display trojan characteristics.
- The fourth most common malware family encountered in Kuwait in 2Q15 was [INF/Autorun](#), which was encountered by 0.9 percent of reporting computers there. [INF/Autorun](#) is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Kuwait in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/KipodToolsCby	Browser Modifiers	5.2%
2	Win32/CouponRuc	Browser Modifiers	4.6%
3	Win32/InstalleRex	Software Bundlers	2.8%
4	Win32/SaverExtension	Adware	1.4%
5	Win32/Vonteera	Browser Modifiers	1.1%

- The most common unwanted software family encountered in Kuwait in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 5.2 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common unwanted software family encountered in Kuwait in 2Q15 was [Win32/CouponRuc](#), which was encountered by 4.6 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The third most common unwanted software family encountered in Kuwait in 2Q15 was [Win32/InstalleRex](#), which was encountered by 2.8 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Kuwait in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	7.9
2	Win32/CompromisedCert	Other Malware	4.1
3	VBS/Jenxcus	Worms	4.1
4	Win32/Gamarue	Worms	2.8
5	Win32/Sality	Viruses	1.9
6	Win32/Kilim	Trojans	1.5
7	MSIL/Bladabindi	Backdoors	1.1
8	Win32/Dorkbot	Worms	0.8
9	Win32/Vobfus	Worms	0.6
10	Win32/Nuqel	Worms	0.5

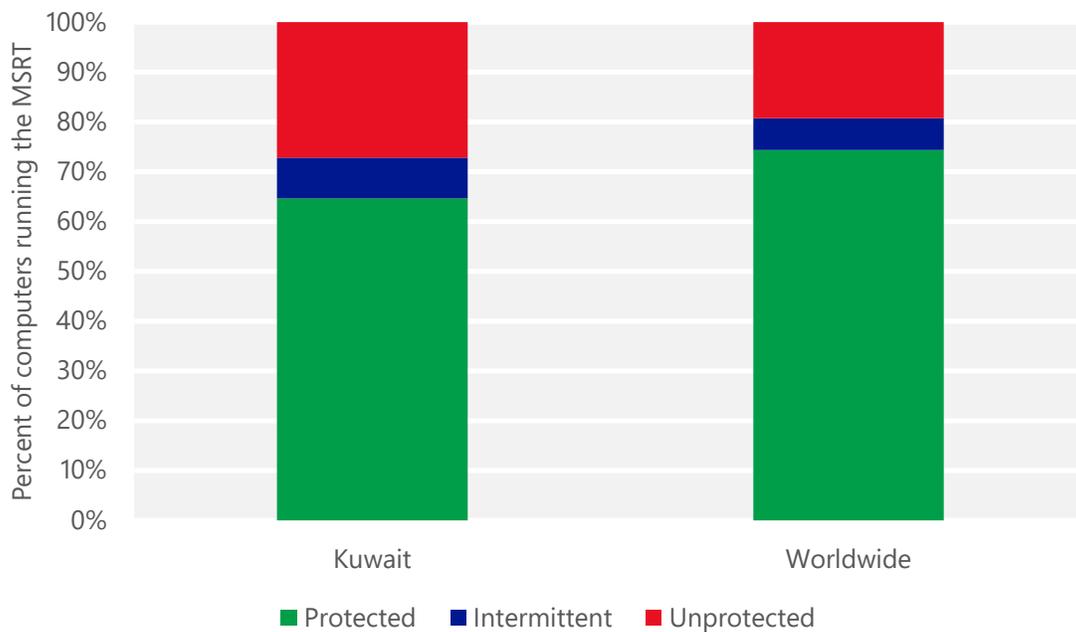
- The most common threat family infecting computers in Kuwait in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 7.9 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Kuwait in 2Q15 was [Win32/CompromisedCert](#), which was detected and removed from 4.1 of every 1,000 unique computers scanned by the MSRT. [Win32/CompromisedCert](#) is a detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.
- The third most common threat family infecting computers in Kuwait in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 4.1 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The fourth most common threat family infecting computers in Kuwait in 2Q15 was [Win32/Gamarue](#), which was detected and removed from 2.8 of every 1,000 unique computers scanned by the MSRT. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Kuwait and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Kuwait

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.01 (0.28)	0.02 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	2.24 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	11.56 (16.7)	

Latvia

The statistics presented here are generated by Microsoft security programs and services running on computers in Latvia in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Latvia

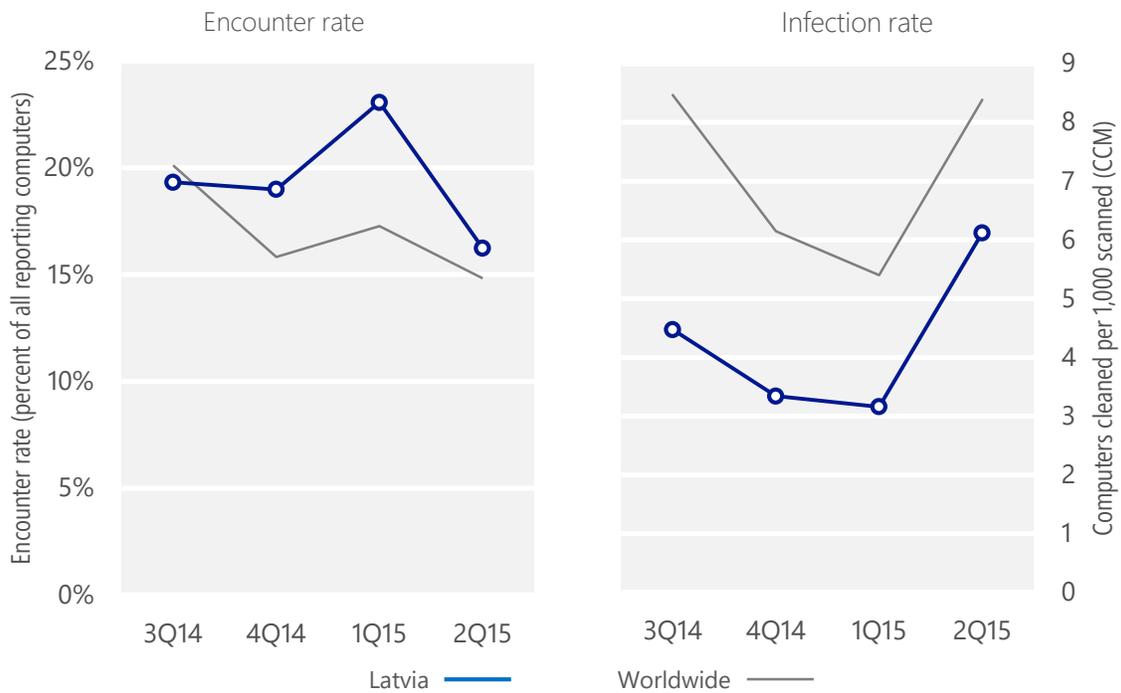
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Latvia	19.3%	19.0%	23.1%	16.2%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Latvia	4.5	3.3	3.2	6.1
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcout, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 16.2% of computers in Latvia encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 6.1 of every 1,000 unique computers scanned in Latvia in 2Q15 (a CCM score of 6.1, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Latvia over the last four quarters, compared to the world as a whole.

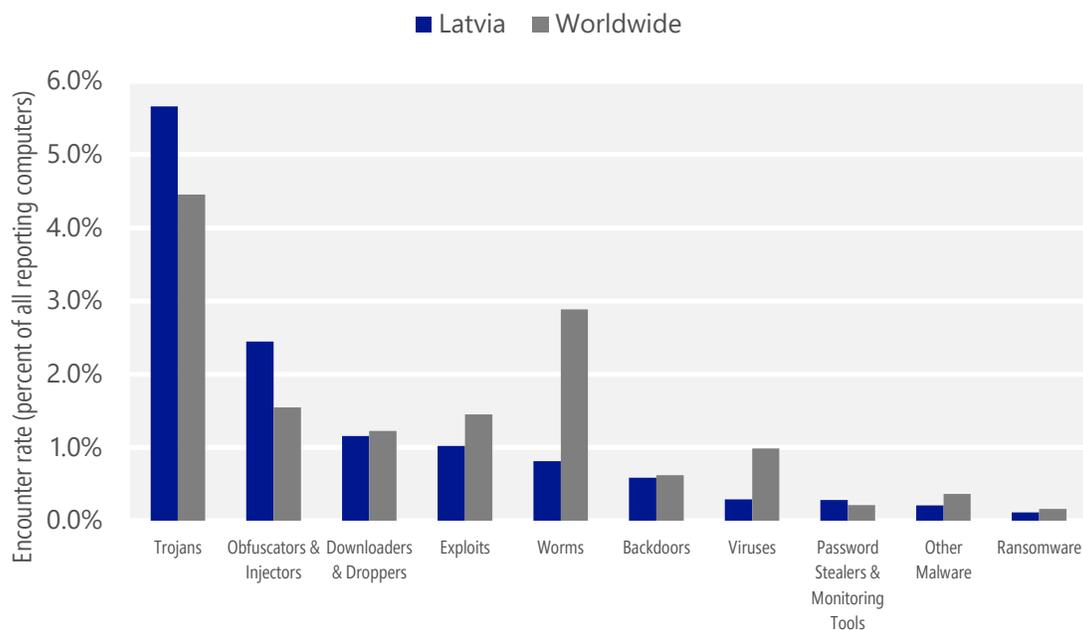
Malware encounter and infection rate trends in Latvia and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in Latvia and around the world, and for explanations of the methods and terms used here.

Malware categories

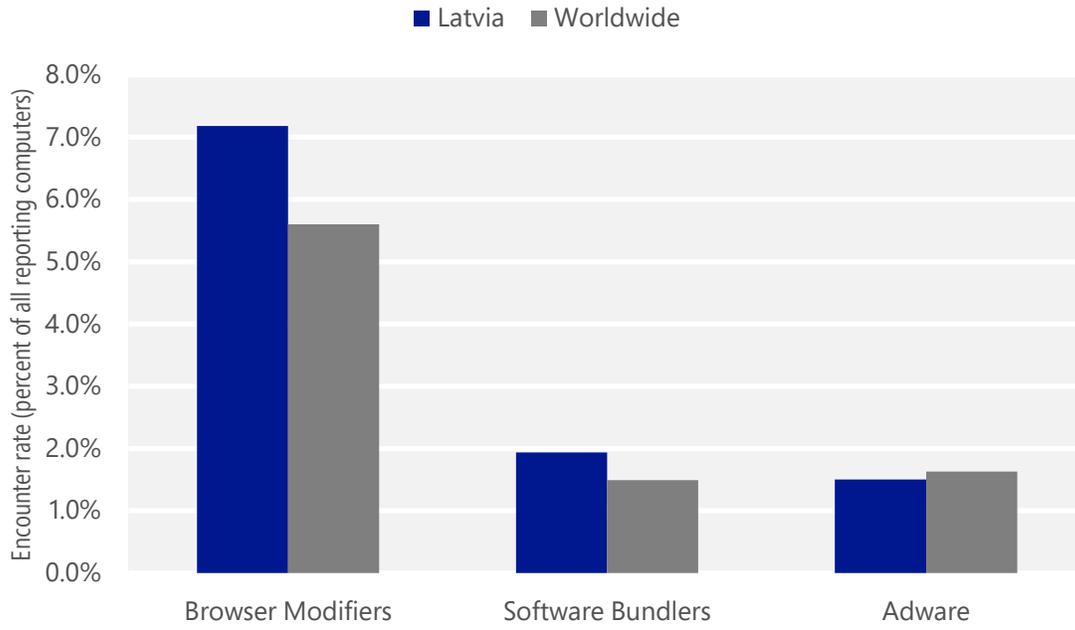
Malware encountered in Latvia in 2Q15, by category



- The most common malware category in Latvia in 2Q15 was Trojans. It was encountered by 5.7 percent of all computers there, down from 6.1 percent in 1Q15.
- The second most common malware category in Latvia in 2Q15 was Obfuscators & Injectors. It was encountered by 2.4 percent of all computers there, down from 2.5 percent in 1Q15.
- The third most common malware category in Latvia in 2Q15 was Downloaders & Droppers, which was encountered by 1.2 percent of all computers there, down from 2.5 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Latvia in 2Q15, by category



- The most common unwanted software category in Latvia in 2Q15 was Browser Modifiers. It was encountered by 7.2 percent of all computers there, down from 11.5 percent in 1Q15.
- The second most common unwanted software category in Latvia in 2Q15 was Software Bundlers. It was encountered by 1.9 percent of all computers there, down from 3.7 percent in 1Q15.
- The third most common unwanted software category in Latvia in 2Q15 was Adware, which was encountered by 1.5 percent of all computers there, up from 1.0 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Latvia in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Obfuscator	Obfuscators & Injectors	2.1%
2	Win32/Peals	Trojans	1.3%
3	Win32/Kilim	Trojans	1.0%
4	Win32/Skeeyah	Trojans	1.0%
5	JS/Axpergle	Exploits	0.6%
6	Win32/Dynamer	Trojans	0.4%
7	Win32/Ogimant	Downloaders & Droppers	0.3%
8	INF/Autorun	Obfuscators & Injectors	0.2%
9	Win32/Conficker	Worms	0.2%
10	Win32/Fynloski	Backdoors	0.2%

- The most common malware family encountered in Latvia in 2Q15 was [Win32/Obfuscator](#), which was encountered by 2.1 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The second most common malware family encountered in Latvia in 2Q15 was [Win32/Peals](#), which was encountered by 1.3 percent of reporting computers there. [Win32/Peals](#) is a generic detection for various threats that display trojan characteristics.
- The third most common malware family encountered in Latvia in 2Q15 was [Win32/Kilim](#), which was encountered by 1.0 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The fourth most common malware family encountered in Latvia in 2Q15 was [Win32/Skeeyah](#), which was encountered by 1.0 percent of reporting computers there. [Win32/Skeeyah](#) is a generic detection for various threats that display trojan characteristics.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Latvia in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	3.5%
2	Win32/KipodToolsCby	Browser Modifiers	3.4%
3	Win32/InstalleRex	Software Bundlers	1.8%
4	Win32/SaverExtension	Adware	1.1%
5	Win32/AlterbookSP	Browser Modifiers	0.4%

- The most common unwanted software family encountered in Latvia in 2Q15 was [Win32/CouponRuc](#), which was encountered by 3.5 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in Latvia in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 3.4 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common unwanted software family encountered in Latvia in 2Q15 was [Win32/InstalleRex](#), which was encountered by 1.8 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Latvia in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	2.5
2	Win32/Kilim	Trojans	1.2
3	Win32/CompromisedCert	Other Malware	0.4
4	Win32/Simda	Trojans	0.2
5	Win32/Ramnit	Trojans	0.2
6	MSIL/Bladabindi	Backdoors	0.2
7	Win32/Sality	Viruses	0.2
8	Win32/Brontok	Worms	0.1
9	Win32/Gamarue	Worms	0.1
10	Win32/Nitol	Other Malware	0.1

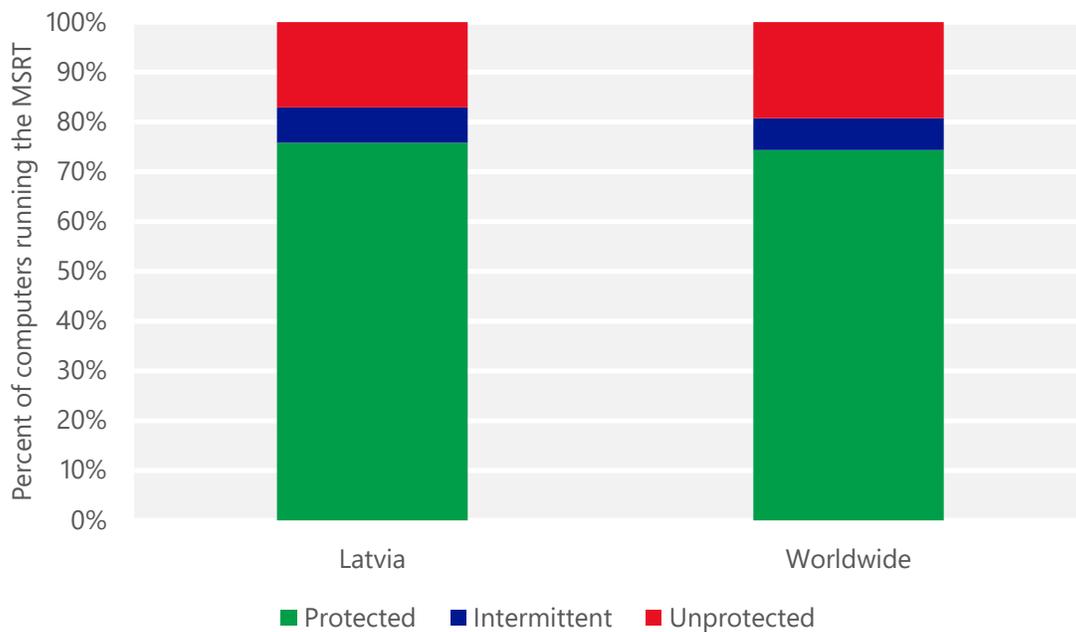
- The most common threat family infecting computers in Latvia in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 2.5 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Latvia in 2Q15 was [Win32/Kilim](#), which was detected and removed from 1.2 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The third most common threat family infecting computers in Latvia in 2Q15 was [Win32/CompromisedCert](#), which was detected and removed from 0.4 of every 1,000 unique computers scanned by the MSRT. [Win32/CompromisedCert](#) is a detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.
- The fourth most common threat family infecting computers in Latvia in 2Q15 was [Win32/Simda](#), which was detected and removed from 0.2 of every 1,000 unique computers scanned by the MSRT. [Win32/Simda](#) is a threat that can give an attacker backdoor access and control of an infected computer. It can then steal passwords and gather information about the computer to send to the attacker.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Latvia and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Latvia

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.15 (0.28)	0.71 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	5.35 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	12.20 (16.7)	

Lebanon

The statistics presented here are generated by Microsoft security programs and services running on computers in Lebanon in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Lebanon

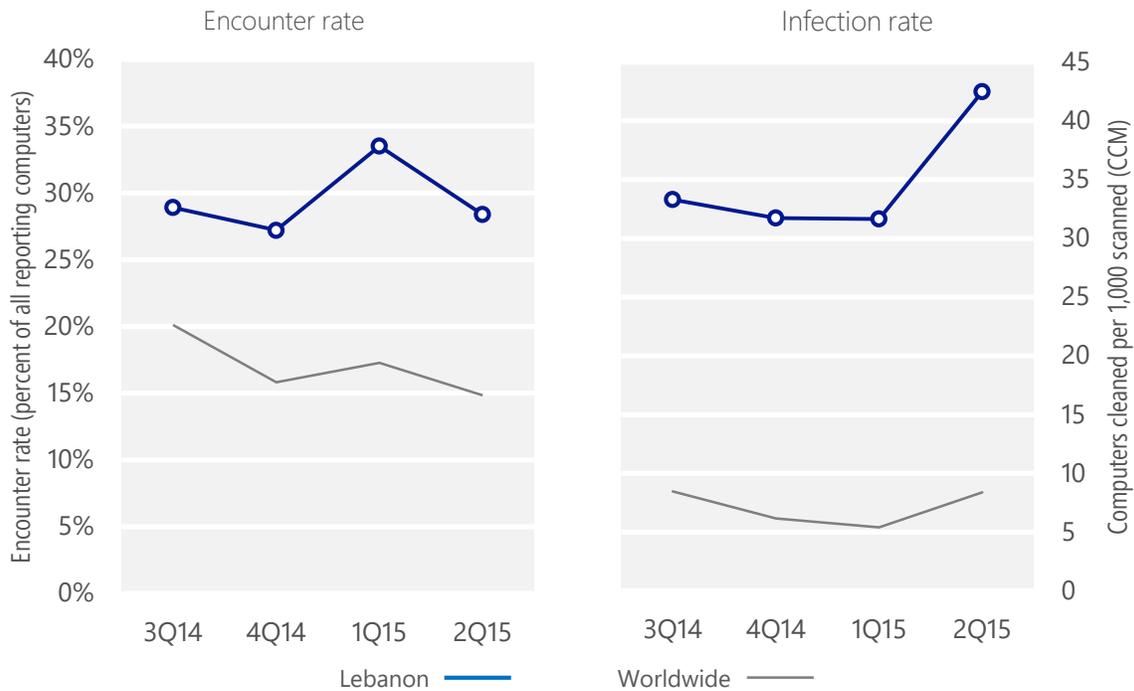
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Lebanon	28.9%	27.2%	33.5%	28.4%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Lebanon	33.3	31.7	31.7	42.5
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcoute, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 28.4% of computers in Lebanon encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 42.5 of every 1,000 unique computers scanned in Lebanon in 2Q15 (a CCM score of 42.5, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Lebanon over the last four quarters, compared to the world as a whole.

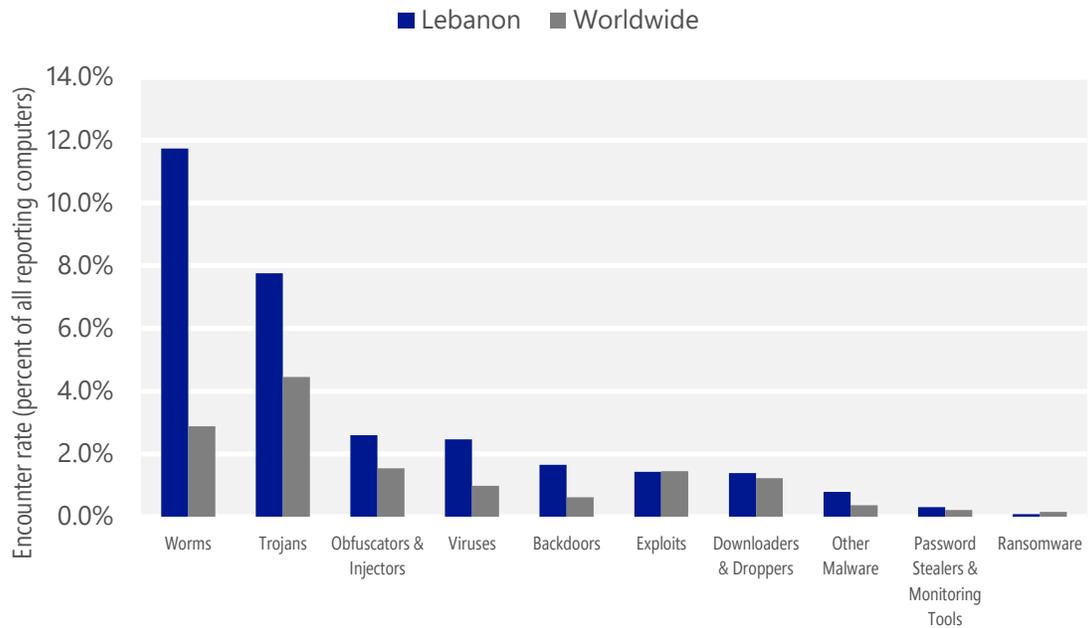
Malware encounter and infection rate trends in Lebanon and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in Lebanon and around the world, and for explanations of the methods and terms used here.

Malware categories

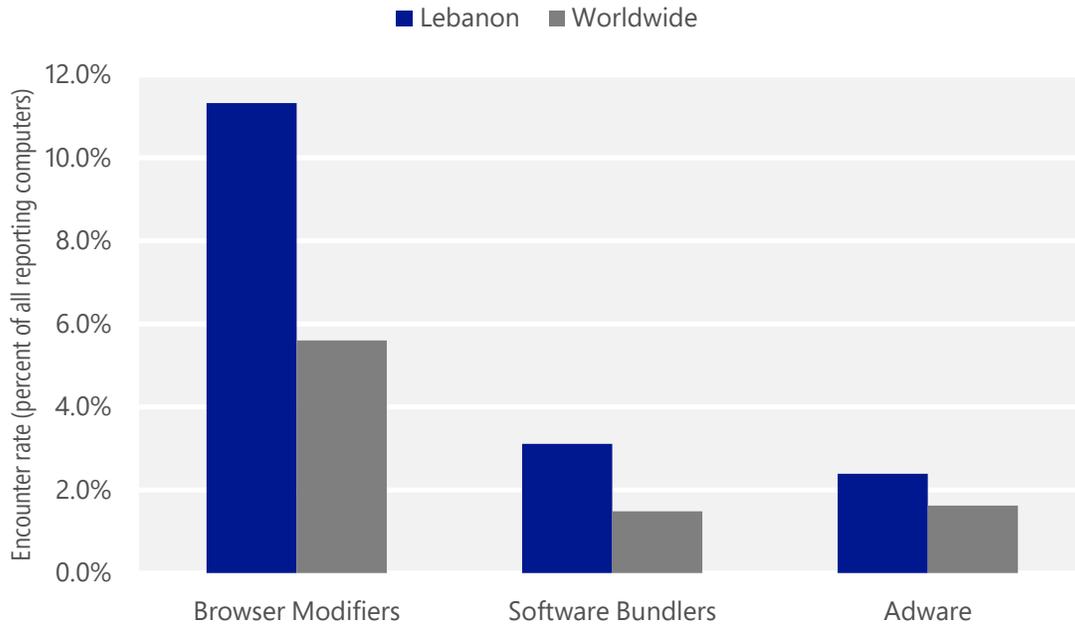
Malware encountered in Lebanon in 2Q15, by category



- The most common malware category in Lebanon in 2Q15 was Worms. It was encountered by 11.7 percent of all computers there, down from 13.5 percent in 1Q15.
- The second most common malware category in Lebanon in 2Q15 was Trojans. It was encountered by 7.8 percent of all computers there, up from 5.9 percent in 1Q15.
- The third most common malware category in Lebanon in 2Q15 was Obfuscators & Injectors, which was encountered by 2.6 percent of all computers there, down from 3.1 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Lebanon in 2Q15, by category



- The most common unwanted software category in Lebanon in 2Q15 was Browser Modifiers. It was encountered by 11.3 percent of all computers there, down from 16.6 percent in 1Q15.
- The second most common unwanted software category in Lebanon in 2Q15 was Software Bundlers. It was encountered by 3.1 percent of all computers there, down from 5.3 percent in 1Q15.
- The third most common unwanted software category in Lebanon in 2Q15 was Adware, which was encountered by 2.4 percent of all computers there, up from 1.4 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Lebanon in 2Q15

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	5.6%
2	Win32/Gamarue	Worms	4.6%
3	INF/Autorun	Obfuscators & Injectors	1.8%
4	Win32/Obfuscator	Obfuscators & Injectors	1.4%
5	Win32/Sality	Viruses	1.2%
6	Win32/Nuqel	Worms	1.1%
7	Win32/Kilim	Trojans	1.0%
8	Win32/Folstart	Worms	1.0%
9	Win32/Skeeyah	Trojans	1.0%
10	Win32/CplLnk	Exploits	0.9%

- The most common malware family encountered in Lebanon in 2Q15 was [VBS/Jenxcus](#), which was encountered by 5.6 percent of reporting computers there. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common malware family encountered in Lebanon in 2Q15 was [Win32/Gamarue](#), which was encountered by 4.6 percent of reporting computers there. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The third most common malware family encountered in Lebanon in 2Q15 was [INF/Autorun](#), which was encountered by 1.8 percent of reporting computers there. [INF/Autorun](#) is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The fourth most common malware family encountered in Lebanon in 2Q15 was [Win32/Obfuscator](#), which was encountered by 1.4 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Lebanon in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/KipodToolsCby	Browser Modifiers	6.0%
2	Win32/CouponRuc	Browser Modifiers	5.2%
3	Win32/InstalleRex	Software Bundlers	2.8%
4	Win32/SaverExtension	Adware	1.7%
5	Win32/AlterbookSP	Browser Modifiers	0.5%

- The most common unwanted software family encountered in Lebanon in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 6.0 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common unwanted software family encountered in Lebanon in 2Q15 was [Win32/CouponRuc](#), which was encountered by 5.2 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The third most common unwanted software family encountered in Lebanon in 2Q15 was [Win32/InstalleRex](#), which was encountered by 2.8 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Lebanon in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	13.1
2	Win32/Gamarue	Worms	9.2
3	Win32/leEnablerCby	Browser Modifiers	7.7
4	Win32/Sality	Viruses	4.0
5	Win32/Folstart	Worms	3.0
6	Win32/Nuqel	Worms	2.1
7	Win32/Kilim	Trojans	1.9
8	Win32/Brontok	Worms	1.4
9	MSIL/Bladabindi	Backdoors	1.3
10	Win32/Ramnit	Trojans	0.9

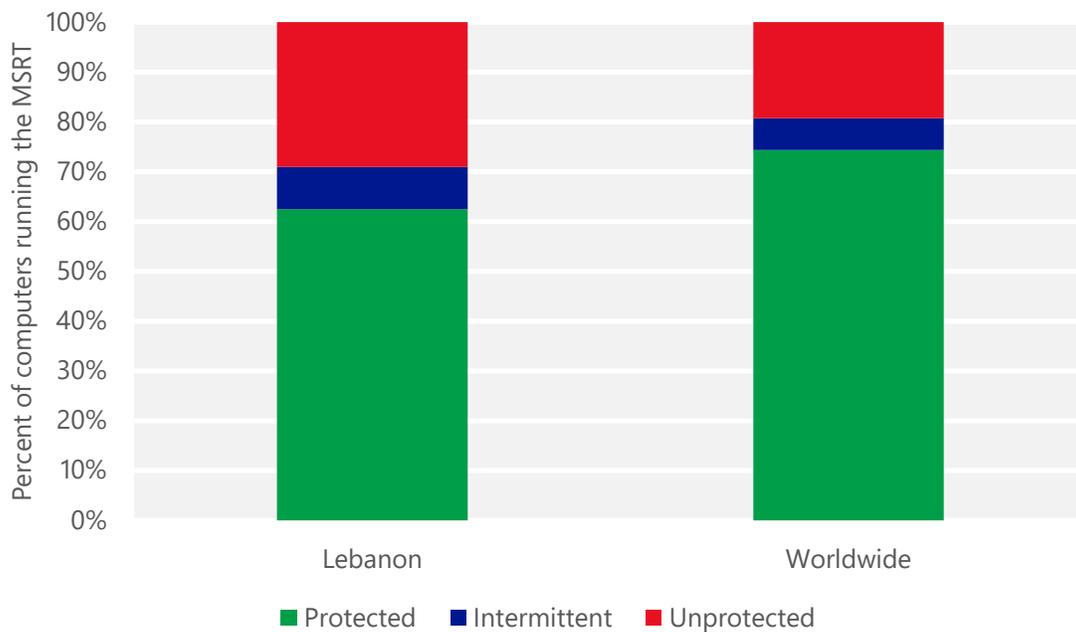
- The most common threat family infecting computers in Lebanon in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 13.1 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Lebanon in 2Q15 was [Win32/Gamarue](#), which was detected and removed from 9.2 of every 1,000 unique computers scanned by the MSRT. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The third most common threat family infecting computers in Lebanon in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 7.7 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The fourth most common threat family infecting computers in Lebanon in 2Q15 was [Win32/Sality](#), which was detected and removed from 4.0 of every 1,000 unique computers scanned by the MSRT. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Lebanon and worldwide protected by real-time security software in 2Q15



Lithuania

The statistics presented here are generated by Microsoft security programs and services running on computers in Lithuania in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Lithuania

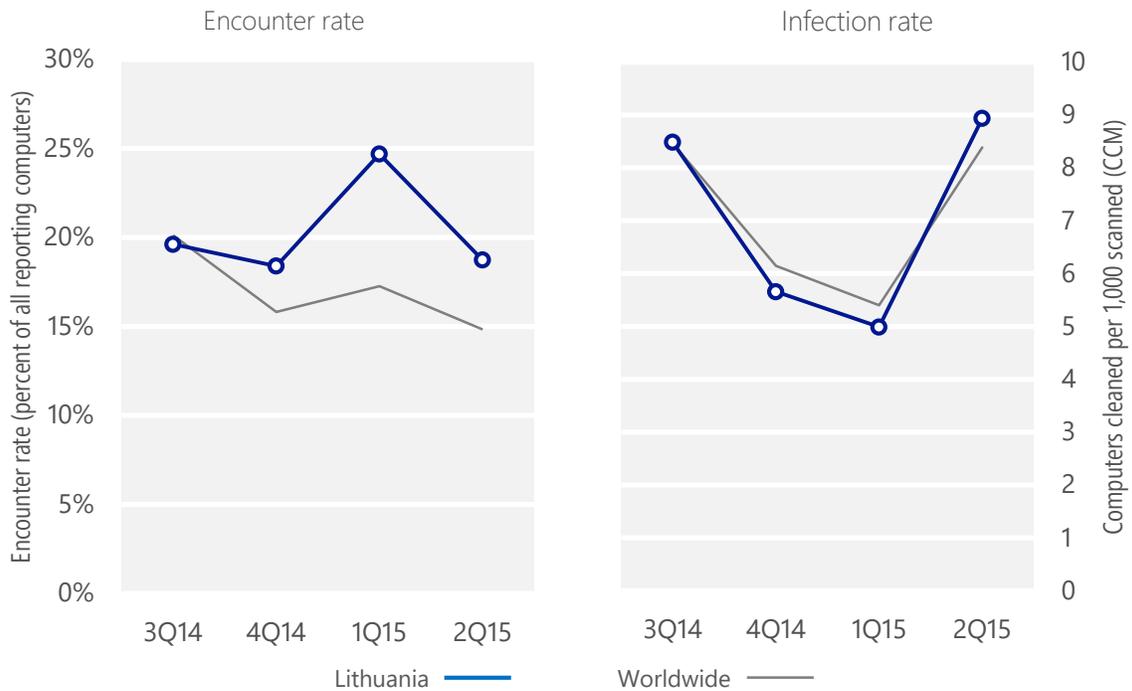
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Lithuania	19.6%	18.4%	24.7%	18.7%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Lithuania	8.5	5.7	5.0	8.9
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcoute, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 18.7% of computers in Lithuania encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 8.9 of every 1,000 unique computers scanned in Lithuania in 2Q15 (a CCM score of 8.9, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Lithuania over the last four quarters, compared to the world as a whole.

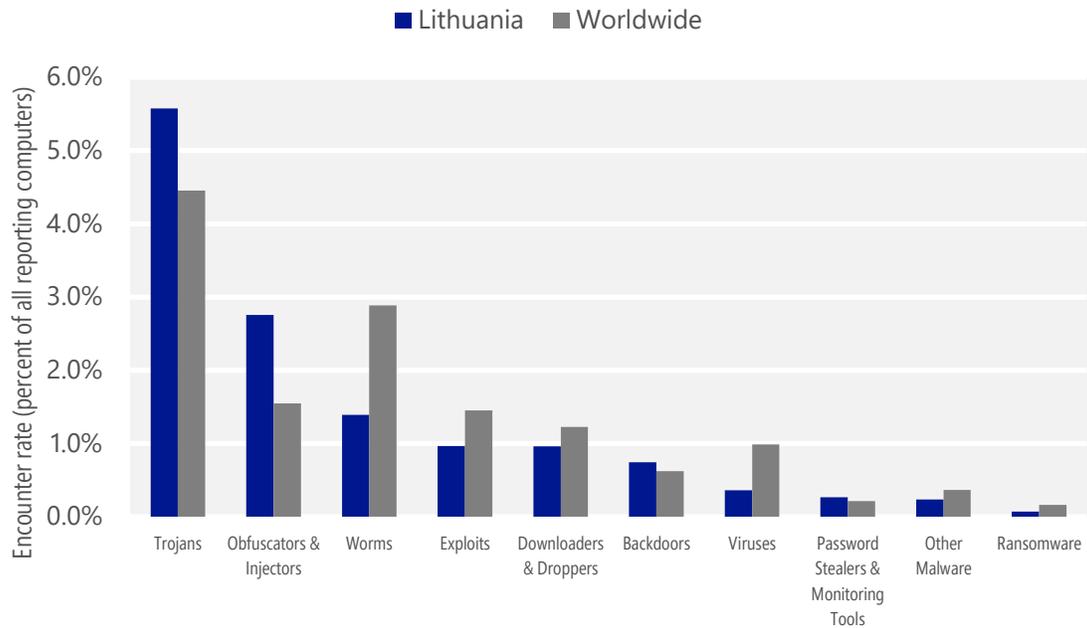
Malware encounter and infection rate trends in Lithuania and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in Lithuania and around the world, and for explanations of the methods and terms used here.

Malware categories

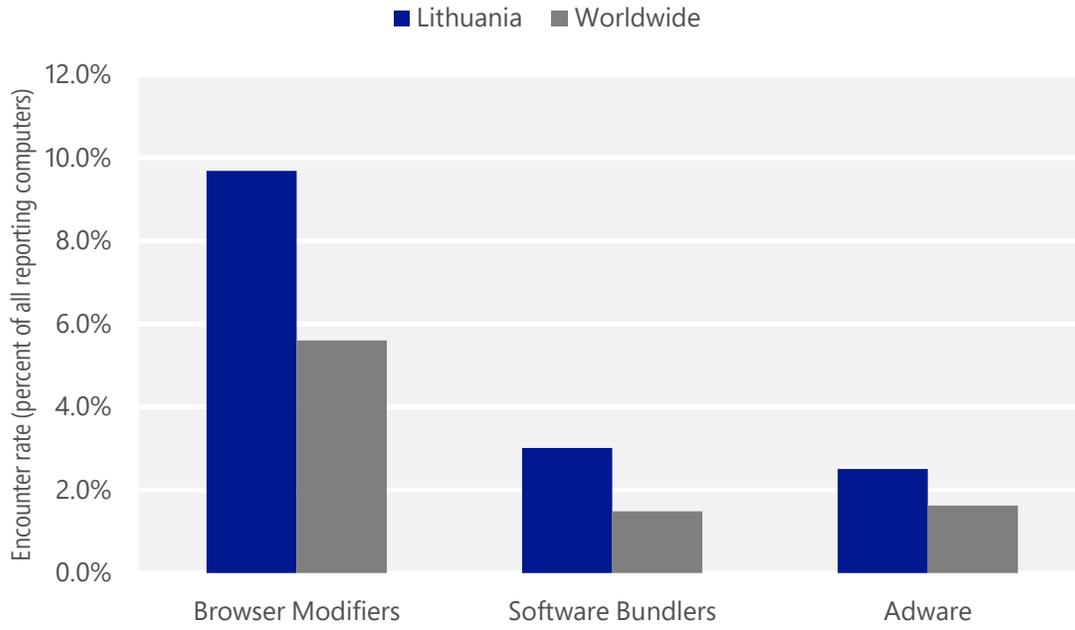
Malware encountered in Lithuania in 2Q15, by category



- The most common malware category in Lithuania in 2Q15 was Trojans. It was encountered by 5.6 percent of all computers there, up from 5.0 percent in 1Q15.
- The second most common malware category in Lithuania in 2Q15 was Obfuscators & Injectors. It was encountered by 2.8 percent of all computers there, up from 2.5 percent in 1Q15.
- The third most common malware category in Lithuania in 2Q15 was Worms, which was encountered by 1.4 percent of all computers there, down from 2.3 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Lithuania in 2Q15, by category



- The most common unwanted software category in Lithuania in 2Q15 was Browser Modifiers. It was encountered by 9.7 percent of all computers there, down from 14.8 percent in 1Q15.
- The second most common unwanted software category in Lithuania in 2Q15 was Software Bundlers. It was encountered by 3.0 percent of all computers there, down from 6.2 percent in 1Q15.
- The third most common unwanted software category in Lithuania in 2Q15 was Adware, which was encountered by 2.5 percent of all computers there, up from 1.4 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Lithuania in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Obfuscator	Obfuscators & Injectors	2.4%
2	Win32/Kilim	Trojans	1.6%
3	Win32/Skeeyah	Trojans	1.1%
4	Win32/Peals	Trojans	0.7%
5	JS/Axpergle	Exploits	0.5%
6	Win32/Dynamer	Trojans	0.4%
7	Win32/Killav	Trojans	0.3%
8	INF/Autorun	Obfuscators & Injectors	0.3%
9	Win32/Brontok	Worms	0.3%
10	Win32/Gamarue	Worms	0.2%

- The most common malware family encountered in Lithuania in 2Q15 was [Win32/Obfuscator](#), which was encountered by 2.4 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The second most common malware family encountered in Lithuania in 2Q15 was [Win32/Kilim](#), which was encountered by 1.6 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The third most common malware family encountered in Lithuania in 2Q15 was [Win32/Skeeyah](#), which was encountered by 1.1 percent of reporting computers there. [Win32/Skeeyah](#) is a generic detection for various threats that display trojan characteristics.
- The fourth most common malware family encountered in Lithuania in 2Q15 was [Win32/Peals](#), which was encountered by 0.7 percent of reporting computers there. [Win32/Peals](#) is a generic detection for various threats that display trojan characteristics.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Lithuania in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	5.6%
2	Win32/KipodToolsCby	Browser Modifiers	3.9%
3	Win32/InstalleRex	Software Bundlers	2.9%
4	Win32/SaverExtension	Adware	2.0%
5	Win32/AlterbookSP	Browser Modifiers	0.6%

- The most common unwanted software family encountered in Lithuania in 2Q15 was [Win32/CouponRuc](#), which was encountered by 5.6 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in Lithuania in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 3.9 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common unwanted software family encountered in Lithuania in 2Q15 was [Win32/InstalleRex](#), which was encountered by 2.9 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Lithuania in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	3.2
2	Win32/Kilim	Trojans	1.8
3	Win32/Brontok	Worms	0.6
4	Win32/Sality	Viruses	0.5
5	Win32/CompromisedCert	Other Malware	0.4
6	VBS/Jenxcus	Worms	0.3
7	MSIL/Bladabindi	Backdoors	0.3
8	Win32/Gamarue	Worms	0.3
9	Win32/Ramnit	Trojans	0.3
10	Win32/Jeefo	Viruses	0.2

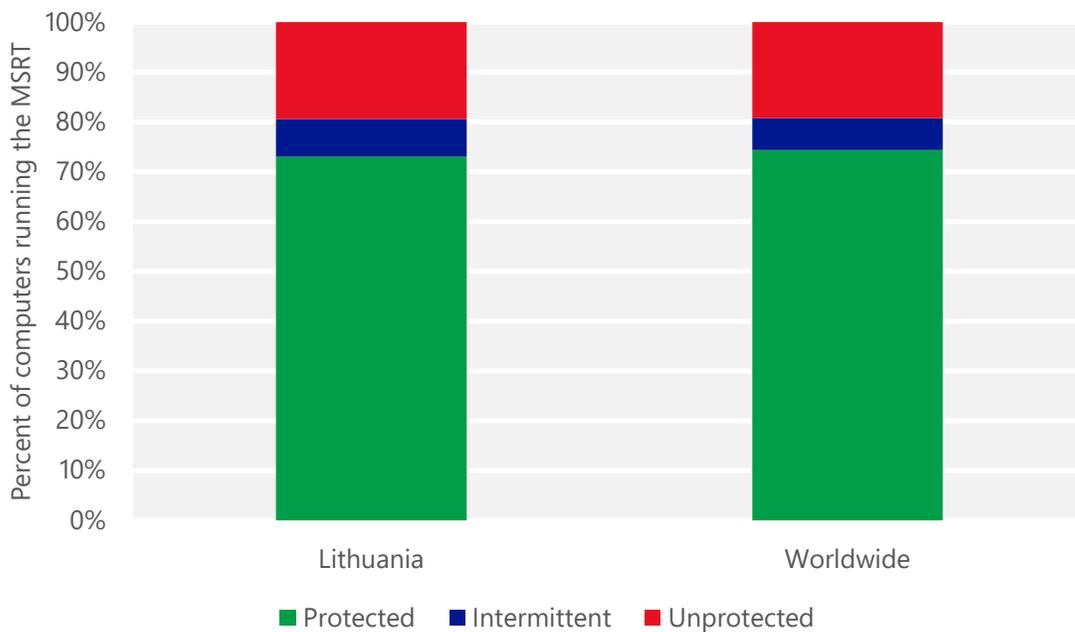
- The most common threat family infecting computers in Lithuania in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 3.2 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Lithuania in 2Q15 was [Win32/Kilim](#), which was detected and removed from 1.8 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The third most common threat family infecting computers in Lithuania in 2Q15 was [Win32/Brontok](#), which was detected and removed from 0.6 of every 1,000 unique computers scanned by the MSRT. [Win32/Brontok](#) is a mass-mailing email worm that spreads by sending copies of itself as email attachments to addresses gathered from files on the infected computer, and by copying itself to removable volumes. Brontok can disable security software, and may conduct DoS attacks against certain websites.
- The fourth most common threat family infecting computers in Lithuania in 2Q15 was [Win32/Sality](#), which was detected and removed from 0.5 of every 1,000 unique computers scanned by the MSRT. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Lithuania and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Lithuania

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.05 (0.28)	0.05 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	6.50 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	13.96 (16.7)	

Luxembourg

The statistics presented here are generated by Microsoft security programs and services running on computers in Luxembourg in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Luxembourg

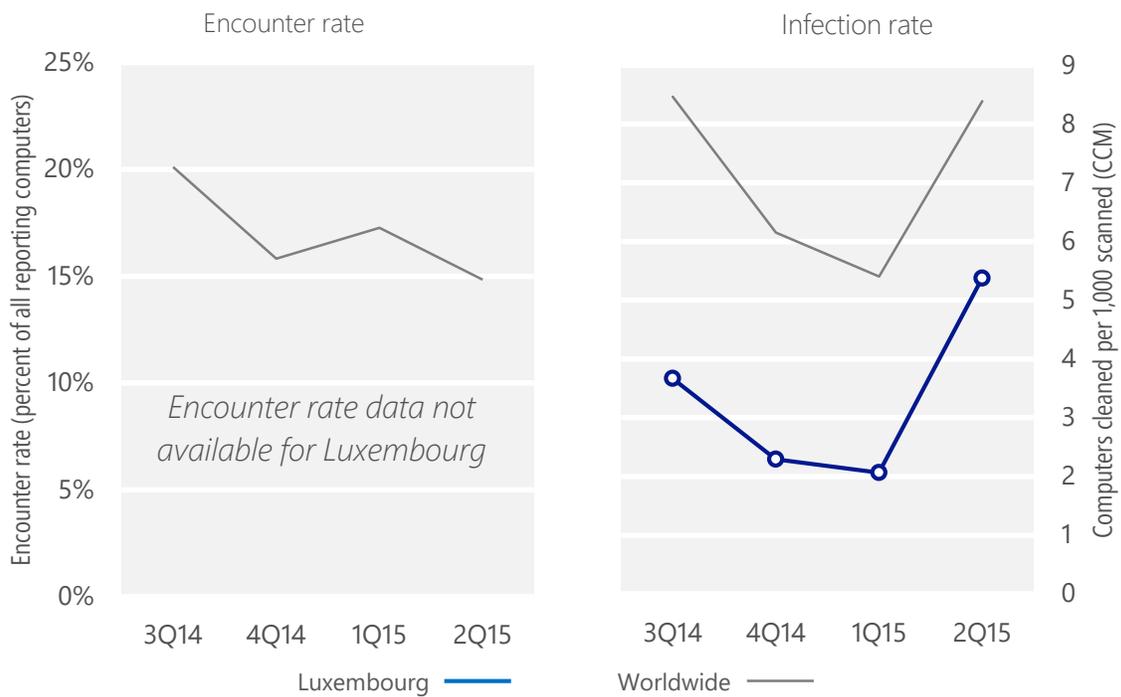
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Luxembourg	N/A	N/A	N/A	N/A
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Luxembourg	3.7	2.3	2.1	5.4
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcoute, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, the MSRT detected and removed malware from 5.4 of every 1,000 unique computers scanned in Luxembourg in 2Q15 (a CCM score of 5.4, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Luxembourg over the last four quarters, compared to the world as a whole.

Malware encounter and infection rate trends in Luxembourg and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in Luxembourg and around the world, and for explanations of the methods and terms used here.

Top threat families by infection rate

The most common malware families by infection rate in Luxembourg in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	3.0
2	Win32/Kilim	Trojans	0.5
3	Win32/CompromisedCert	Other Malware	0.5
4	VBS/Jenxcus	Worms	0.2
5	Win32/Emotet	Trojans	0.1
6	Win32/Gamarue	Worms	0.1
7	MSIL/Bladabindi	Backdoors	0.1
8	Win32/Dyzap	Password Stealers & Monitoring Tools	0.1
9	Win32/Ramnit	Trojans	0.1
10	Win32/Simda	Trojans	0.1

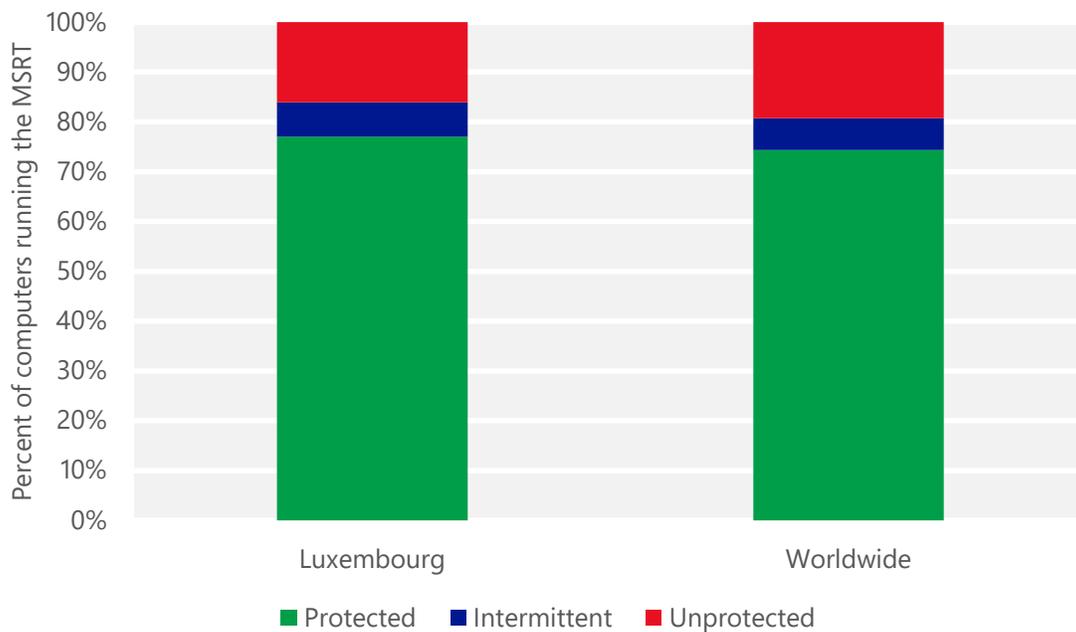
- The most common threat family infecting computers in Luxembourg in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 3.0 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Luxembourg in 2Q15 was [Win32/Kilim](#), which was detected and removed from 0.5 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The third most common threat family infecting computers in Luxembourg in 2Q15 was [Win32/CompromisedCert](#), which was detected and removed from 0.5 of every 1,000 unique computers scanned by the MSRT. [Win32/CompromisedCert](#) is a detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.
- The fourth most common threat family infecting computers in Luxembourg in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 0.2 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Luxembourg and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Luxembourg

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.03 (0.28)	0.08 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	5.72 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	21.72 (16.7)	

Macao S.A.R.

The statistics presented here are generated by Microsoft security programs and services running on computers in Macao S.A.R. in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Macao S.A.R.

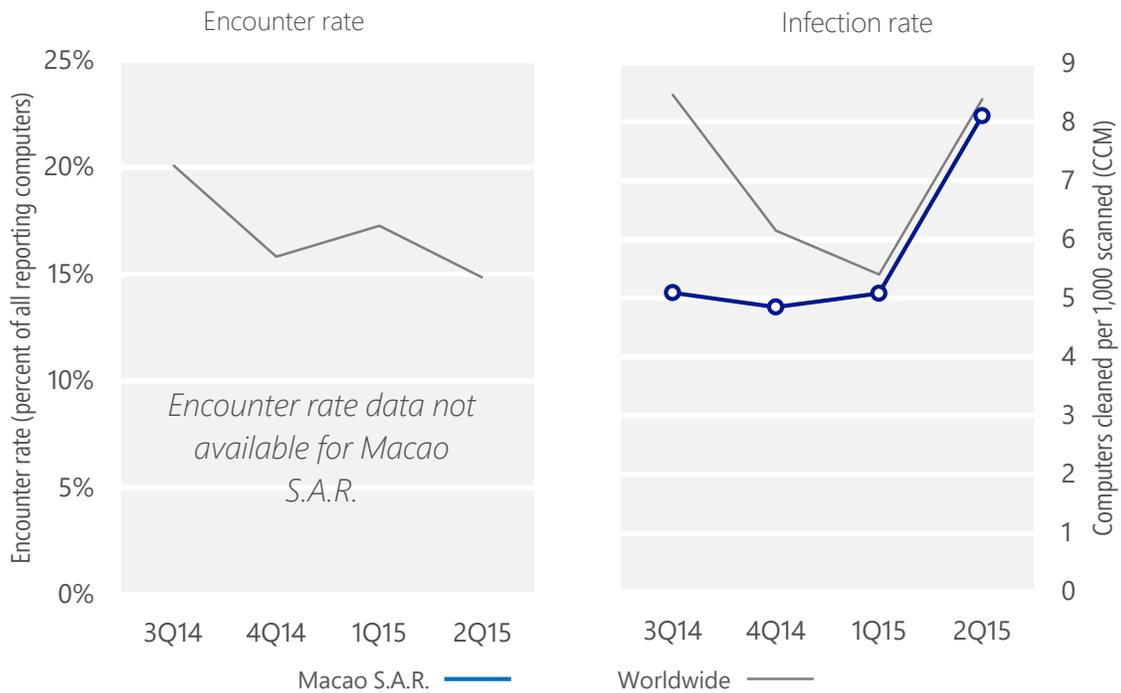
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Macao S.A.R.	N/A	N/A	N/A	N/A
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Macao S.A.R.	5.1	4.9	5.1	8.1
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcoute, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, the MSRT detected and removed malware from 8.1 of every 1,000 unique computers scanned in Macao S.A.R. in 2Q15 (a CCM score of 8.1, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Macao S.A.R. over the last four quarters, compared to the world as a whole.

Malware encounter and infection rate trends in Macao S.A.R. and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in Macao S.A.R. and around the world, and for explanations of the methods and terms used here.

Top threat families by infection rate

The most common malware families by infection rate in Macao S.A.R. in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/IeEnablerCby	Browser Modifiers	2.0
2	Win32/Kilim	Trojans	0.9
3	Win32/Ramnit	Trojans	0.9
4	Win32/CompromisedCert	Other Malware	0.8
5	VBS/Jenxcus	Worms	0.8
6	Win32/Winnti	Trojans	0.5
7	Win32/Gamarue	Worms	0.3
8	Win32/Nitol	Other Malware	0.3
9	Win32/Sality	Viruses	0.3
10	Win32/Conficker	Worms	0.2

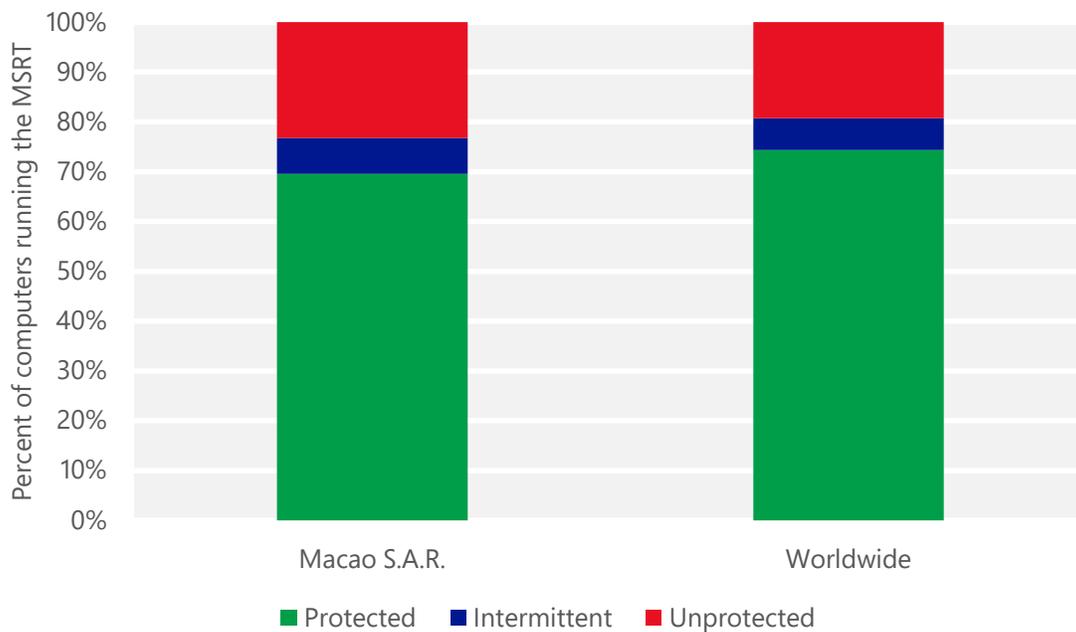
- The most common threat family infecting computers in Macao S.A.R. in 2Q15 was [Win32/IeEnablerCby](#), which was detected and removed from 2.0 of every 1,000 unique computers scanned by the MSRT. [Win32/IeEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Macao S.A.R. in 2Q15 was [Win32/Kilim](#), which was detected and removed from 0.9 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The third most common threat family infecting computers in Macao S.A.R. in 2Q15 was [Win32/Ramnit](#), which was detected and removed from 0.9 of every 1,000 unique computers scanned by the MSRT. [Win32/Ramnit](#) is a family of multi-component malware that infects executable files, Microsoft Office files, and HTML files. Win32/Ramnit spreads to removable drives and steals sensitive information such as saved FTP credentials and browser cookies. It may also open a backdoor to await instructions from a remote attacker.
- The fourth most common threat family infecting computers in Macao S.A.R. in 2Q15 was [Win32/CompromisedCert](#), which was detected and removed from 0.8 of every 1,000 unique computers scanned by the MSRT. [Win32/CompromisedCert](#) is a detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Macao S.A.R. and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Macao S.A.R.

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.06 (0.28)	0.08 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	1.90 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	6.45 (16.7)	

Malaysia

The statistics presented here are generated by Microsoft security programs and services running on computers in Malaysia in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Malaysia

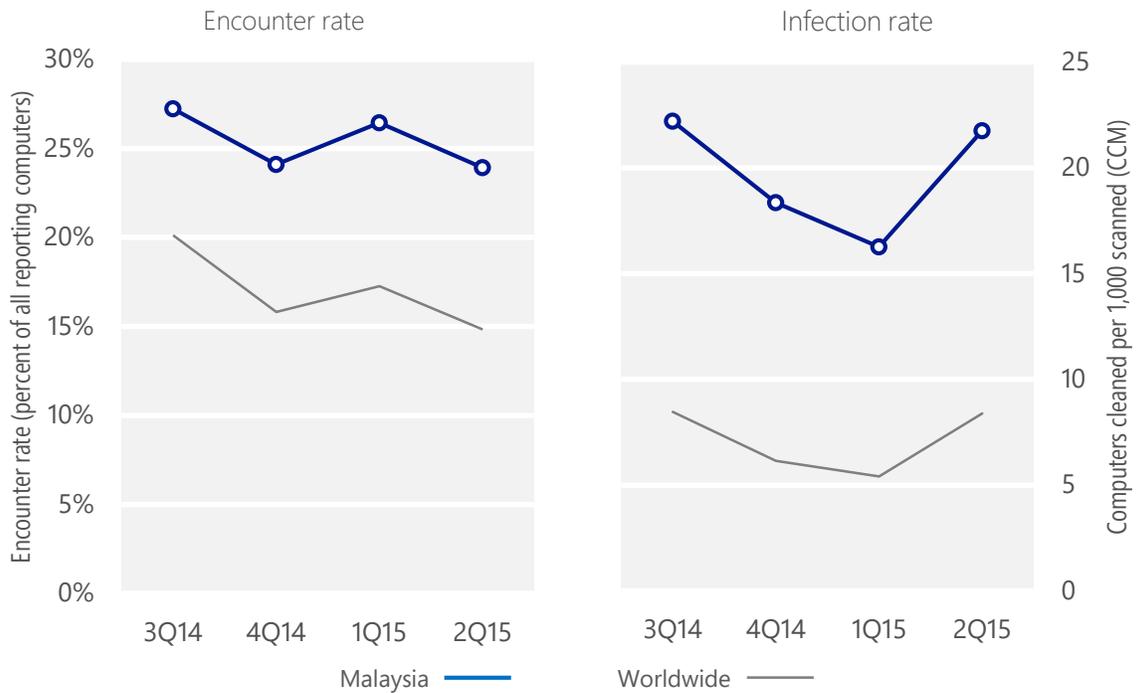
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Malaysia	27.2%	24.1%	26.4%	23.9%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Malaysia	22.2	18.4	16.3	21.8
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcote, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 23.9% of computers in Malaysia encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 21.8 of every 1,000 unique computers scanned in Malaysia in 2Q15 (a CCM score of 21.8, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Malaysia over the last four quarters, compared to the world as a whole.

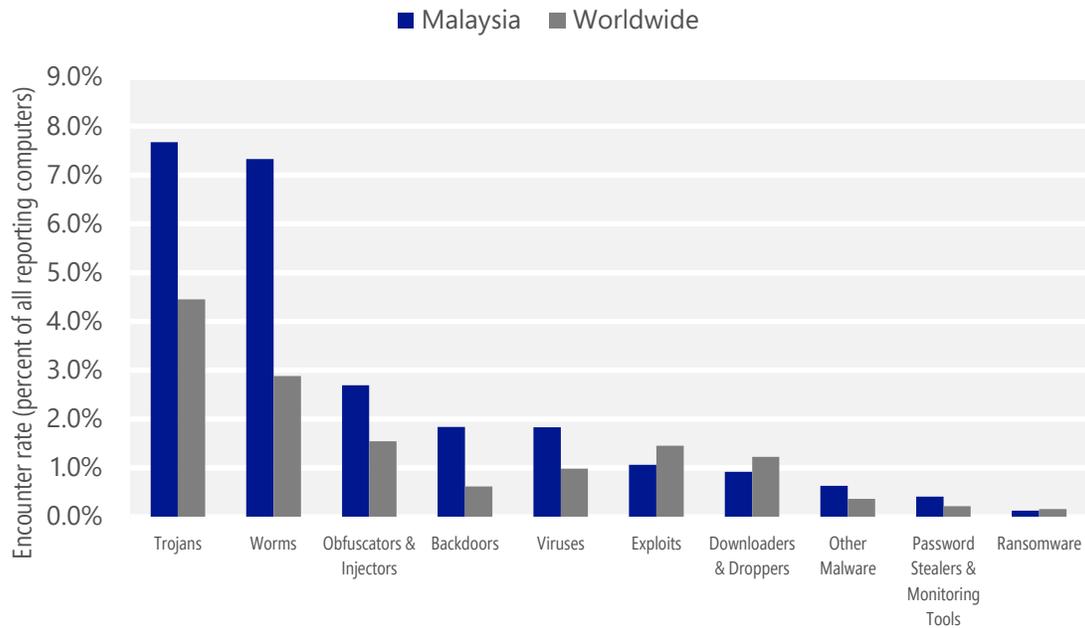
Malware encounter and infection rate trends in Malaysia and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in Malaysia and around the world, and for explanations of the methods and terms used here.

Malware categories

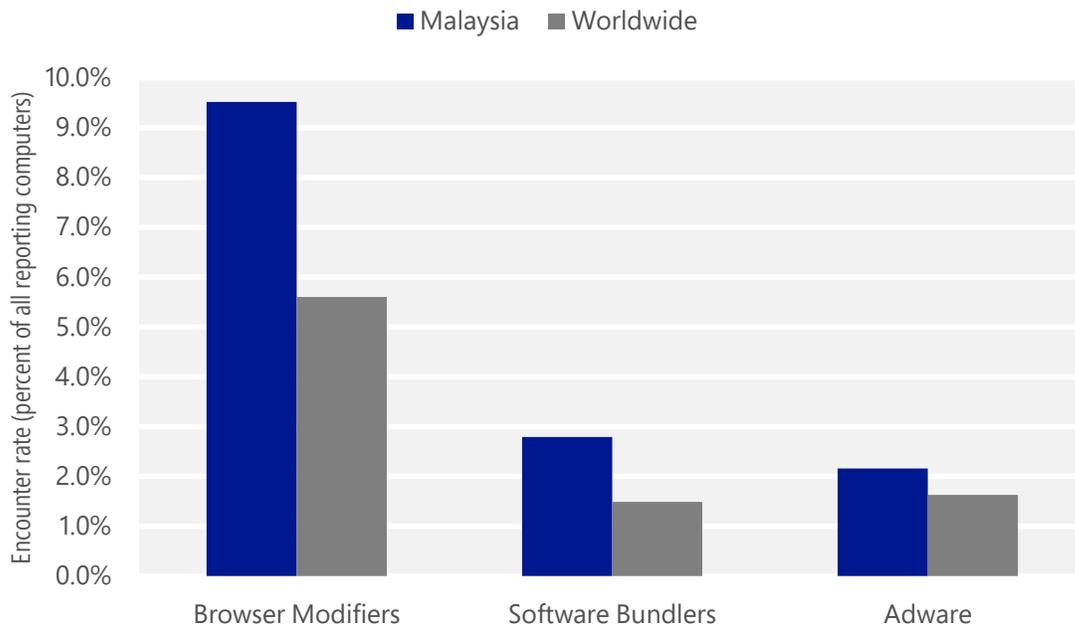
Malware encountered in Malaysia in 2Q15, by category



- The most common malware category in Malaysia in 2Q15 was Trojans. It was encountered by 7.7 percent of all computers there, down from 8.6 percent in 1Q15.
- The second most common malware category in Malaysia in 2Q15 was Worms. It was encountered by 7.3 percent of all computers there, up from 4.5 percent in 1Q15.
- The third most common malware category in Malaysia in 2Q15 was Obfuscators & Injectors, which was encountered by 2.7 percent of all computers there, down from 2.9 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Malaysia in 2Q15, by category



- The most common unwanted software category in Malaysia in 2Q15 was Browser Modifiers. It was encountered by 9.5 percent of all computers there, down from 12.8 percent in 1Q15.
- The second most common unwanted software category in Malaysia in 2Q15 was Software Bundlers. It was encountered by 2.8 percent of all computers there, down from 5.2 percent in 1Q15.
- The third most common unwanted software category in Malaysia in 2Q15 was Adware, which was encountered by 2.2 percent of all computers there, up from 1.1 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Malaysia in 2Q15

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	2.7%
2	Win32/Gamarue	Worms	2.1%
3	Win32/Obfuscator	Obfuscators & Injectors	1.6%
4	INF/Autorun	Obfuscators & Injectors	1.2%
5	Win32/Kilim	Trojans	1.1%
6	Win32/Caphaw	Backdoors	1.0%
7	Win32/Sality	Viruses	0.9%
8	Win32/Skeeyah	Trojans	0.8%
9	Win32/Ramnit	Trojans	0.8%
10	Win32/Conficker	Worms	0.8%

- The most common malware family encountered in Malaysia in 2Q15 was [VBS/Jenxcus](#), which was encountered by 2.7 percent of reporting computers there. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common malware family encountered in Malaysia in 2Q15 was [Win32/Gamarue](#), which was encountered by 2.1 percent of reporting computers there. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The third most common malware family encountered in Malaysia in 2Q15 was [Win32/Obfuscator](#), which was encountered by 1.6 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The fourth most common malware family encountered in Malaysia in 2Q15 was [INF/Autorun](#), which was encountered by 1.2 percent of reporting computers there. [INF/Autorun](#) is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Malaysia in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	5.2%
2	Win32/KipodToolsCby	Browser Modifiers	4.2%
3	Win32/InstalleRex	Software Bundlers	2.6%
4	Win32/SaverExtension	Adware	1.7%
5	Win32/AlterbookSP	Browser Modifiers	0.6%

- The most common unwanted software family encountered in Malaysia in 2Q15 was [Win32/CouponRuc](#), which was encountered by 5.2 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in Malaysia in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 4.2 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common unwanted software family encountered in Malaysia in 2Q15 was [Win32/InstalleRex](#), which was encountered by 2.6 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Malaysia in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	4.1
2	VBS/Jenxcus	Worms	4.0
3	Win32/Gamarue	Worms	2.7
4	Win32/Sality	Viruses	2.3
5	Win32/Kilim	Trojans	2.0
6	Win32/CompromisedCert	Other Malware	1.7
7	Win32/Ramnit	Trojans	1.4
8	Win32/Dorkbot	Worms	1.2
9	Win32/Lethic	Trojans	0.4
10	Win32/Dyzap	Password Stealers & Monitoring Tools	0.4

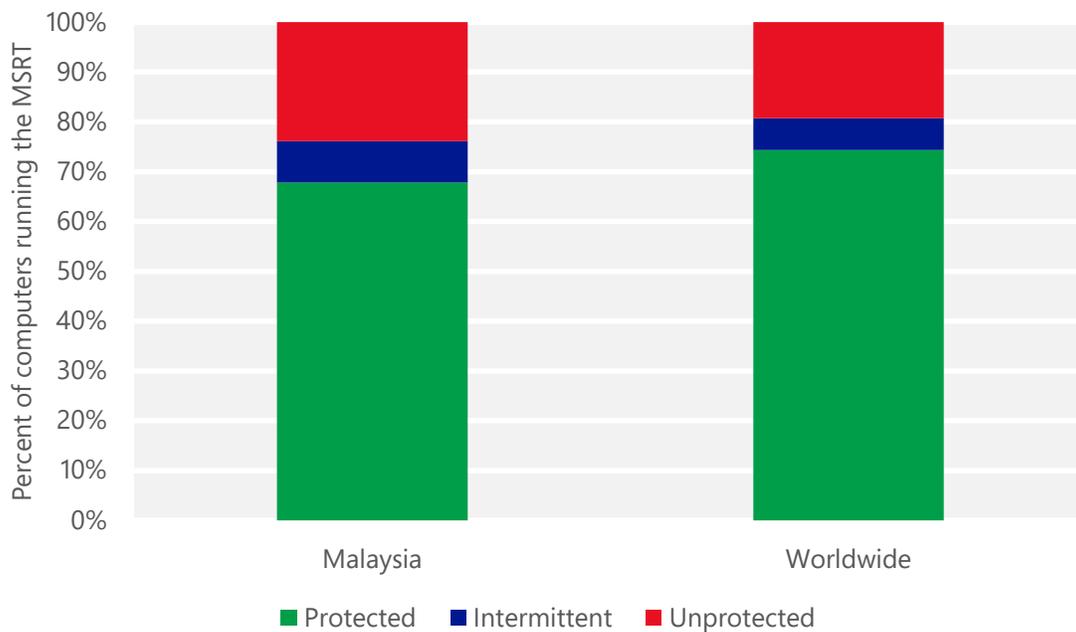
- The most common threat family infecting computers in Malaysia in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 4.1 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Malaysia in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 4.0 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The third most common threat family infecting computers in Malaysia in 2Q15 was [Win32/Gamarue](#), which was detected and removed from 2.7 of every 1,000 unique computers scanned by the MSRT. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The fourth most common threat family infecting computers in Malaysia in 2Q15 was [Win32/Sality](#), which was detected and removed from 2.3 of every 1,000 unique computers scanned by the MSRT. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Malaysia and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Malaysia

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.88 (0.28)	0.34 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	10.23 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	9.48 (16.7)	

Malta

The statistics presented here are generated by Microsoft security programs and services running on computers in Malta in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Malta

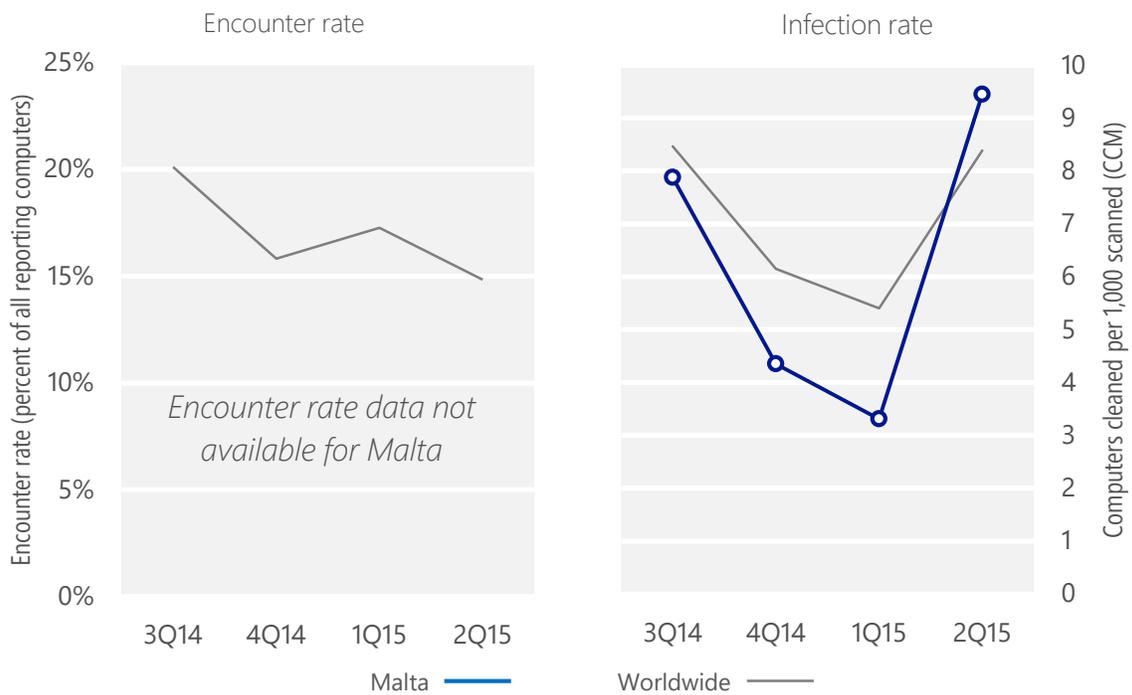
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Malta	N/A	N/A	N/A	N/A
<i>Worldwide encounter rate</i>	20.1%	15.8%	17.3%	14.8%
CCM, Malta	7.9	4.4	3.3	9.5
<i>Worldwide CCM</i>	8.5	6.1	5.4	8.4

Encounter and infection rates reported here do not include totals for the Brantall, Filcoute, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, the MSRT detected and removed malware from 9.5 of every 1,000 unique computers scanned in Malta in 2Q15 (a CCM score of 9.5, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Malta over the last four quarters, compared to the world as a whole.

Malware encounter and infection rate trends in Malta and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in Malta and around the world, and for explanations of the methods and terms used here.

Top threat families by infection rate

The most common malware families by infection rate in Malta in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/IeEnablerCby	Browser Modifiers	4.9
2	Win32/Kilim	Trojans	1.6
3	VBS/Jenxcus	Worms	0.8
4	Win32/CompromisedCert	Other Malware	0.5
5	Win32/Simda	Trojans	0.3
6	Win32/Gamarue	Worms	0.2
7	MSIL/Bladabindi	Backdoors	0.2
8	Win32/Sality	Viruses	0.1
9	Win32/Alureon	Trojans	0.1
10	Win32/Dyzap	Password Stealers & Monitoring Tools	0.1

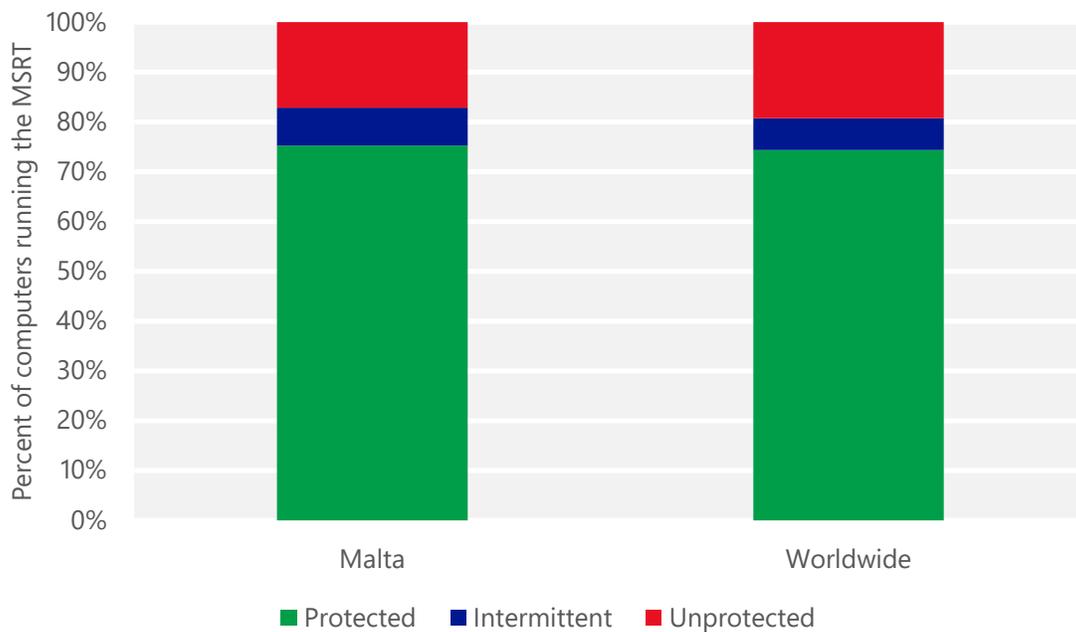
- The most common threat family infecting computers in Malta in 2Q15 was [Win32/IeEnablerCby](#), which was detected and removed from 4.9 of every 1,000 unique computers scanned by the MSRT. [Win32/IeEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Malta in 2Q15 was [Win32/Kilim](#), which was detected and removed from 1.6 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The third most common threat family infecting computers in Malta in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 0.8 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The fourth most common threat family infecting computers in Malta in 2Q15 was [Win32/CompromisedCert](#), which was detected and removed from 0.5 of every 1,000 unique computers scanned by the MSRT. [Win32/CompromisedCert](#) is a detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Malta and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Malta

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.00 (0.28)	0.00 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	1.71 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	12.80 (16.7)	

Mexico

The statistics presented here are generated by Microsoft security programs and services running on computers in Mexico in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Mexico

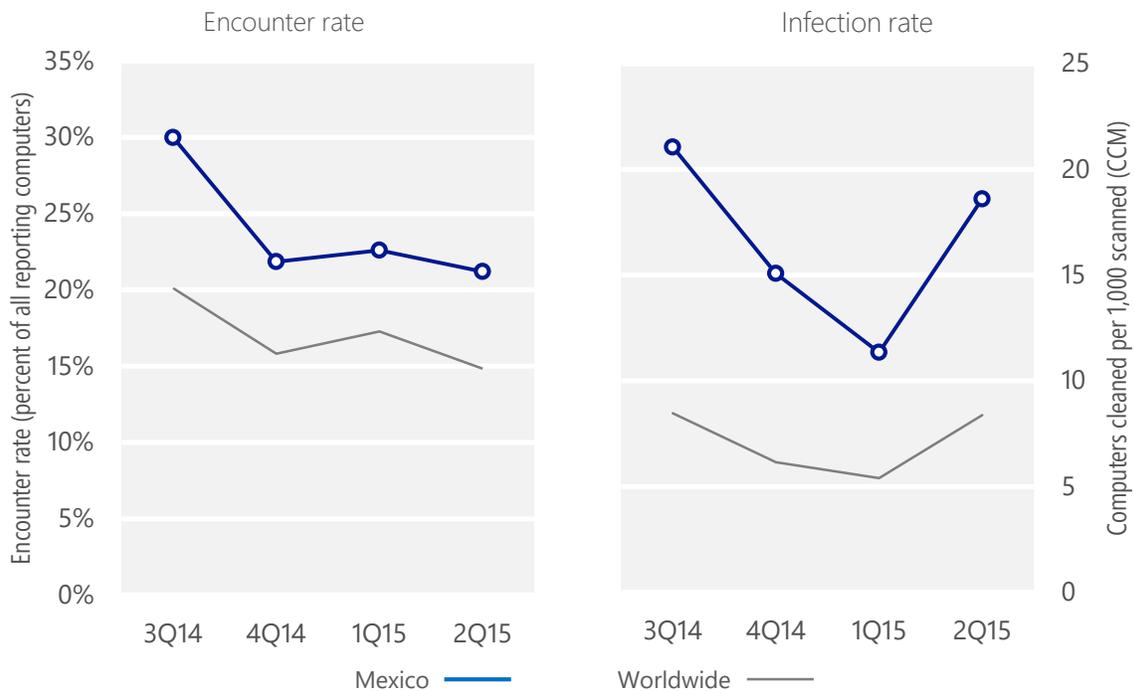
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Mexico	30.0%	21.9%	22.6%	21.2%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Mexico	21.1	15.1	11.4	18.6
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcoute, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 21.2% of computers in Mexico encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 18.6 of every 1,000 unique computers scanned in Mexico in 2Q15 (a CCM score of 18.6, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Mexico over the last four quarters, compared to the world as a whole.

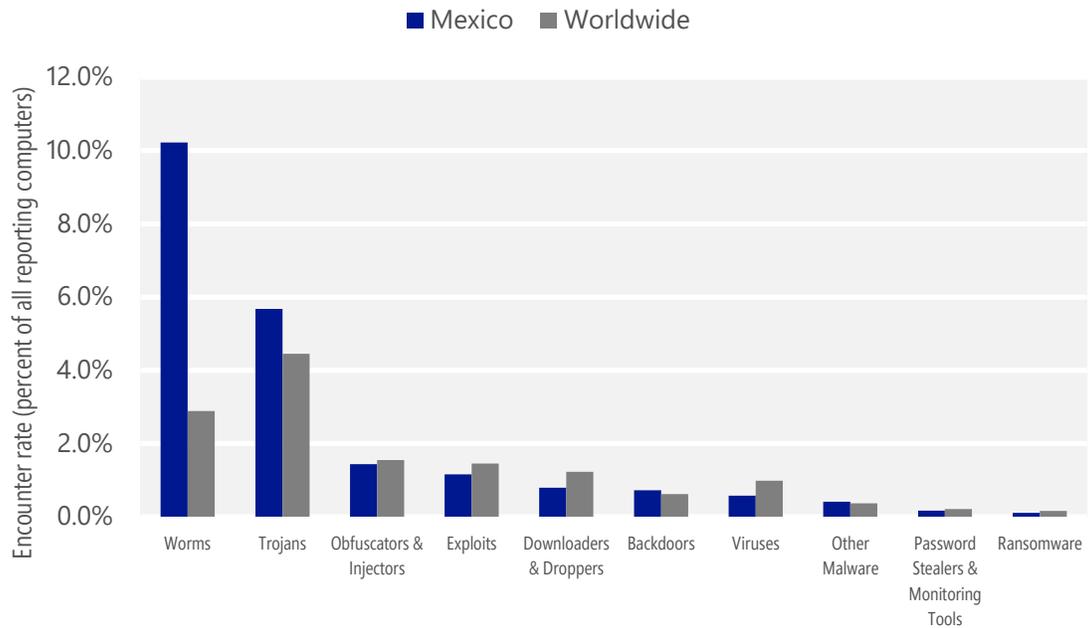
Malware encounter and infection rate trends in Mexico and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in Mexico and around the world, and for explanations of the methods and terms used here.

Malware categories

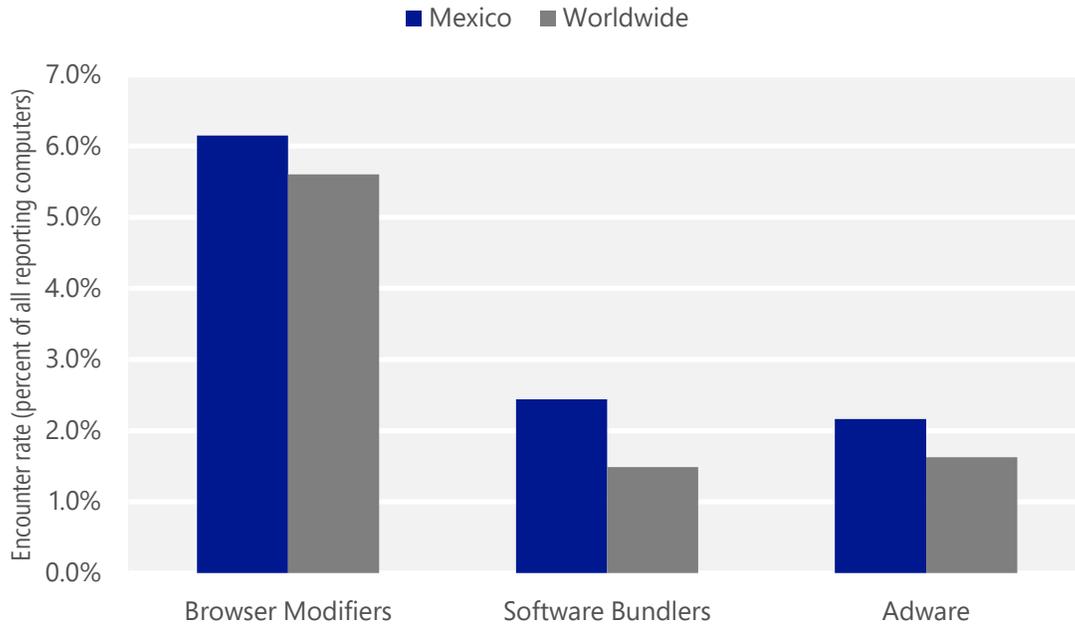
Malware encountered in Mexico in 2Q15, by category



- The most common malware category in Mexico in 2Q15 was Worms. It was encountered by 10.2 percent of all computers there, down from 10.6 percent in 1Q15.
- The second most common malware category in Mexico in 2Q15 was Trojans. It was encountered by 5.7 percent of all computers there, up from 3.3 percent in 1Q15.
- The third most common malware category in Mexico in 2Q15 was Obfuscators & Injectors, which was encountered by 1.4 percent of all computers there, down from 1.7 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Mexico in 2Q15, by category



- The most common unwanted software category in Mexico in 2Q15 was Browser Modifiers. It was encountered by 6.1 percent of all computers there, down from 7.8 percent in 1Q15.
- The second most common unwanted software category in Mexico in 2Q15 was Software Bundlers. It was encountered by 2.4 percent of all computers there, down from 4.1 percent in 1Q15.
- The third most common unwanted software category in Mexico in 2Q15 was Adware, which was encountered by 2.2 percent of all computers there, up from 0.5 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Mexico in 2Q15

	Family	Most significant category	% of reporting computers
1	JS/Bondat	Worms	4.2%
2	VBS/Jenxcus	Worms	3.4%
3	Win32/Gamarue	Worms	2.2%
4	Win32/Kilim	Trojans	1.0%
5	Win32/Skeeyah	Trojans	0.9%
6	INF/Autorun	Obfuscators & Injectors	0.8%
7	Win32/Obfuscator	Obfuscators & Injectors	0.7%
8	JS/Axpergle	Exploits	0.6%
9	Win32/Peals	Trojans	0.5%
10	Win32/Brontok	Worms	0.5%

- The most common malware family encountered in Mexico in 2Q15 was [JS/Bondat](#), which was encountered by 4.2 percent of reporting computers there. [JS/Bondat](#) is a family of threats that collects information about the computer, infects removable drives, and tries to stop the user from accessing files. It spreads by infecting removable drives, such as USB thumb drives and flash drives.
- The second most common malware family encountered in Mexico in 2Q15 was [VBS/Jenxcus](#), which was encountered by 3.4 percent of reporting computers there. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The third most common malware family encountered in Mexico in 2Q15 was [Win32/Gamarue](#), which was encountered by 2.2 percent of reporting computers there. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The fourth most common malware family encountered in Mexico in 2Q15 was [Win32/Kilim](#), which was encountered by 1.0 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Mexico in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	3.5%
2	Win32/InstalleRex	Software Bundlers	2.3%
3	Win32/KipodToolsCby	Browser Modifiers	1.6%
4	Win32/SaverExtension	Adware	1.1%
5	Win32/AlterbookSP	Browser Modifiers	0.8%

- The most common unwanted software family encountered in Mexico in 2Q15 was [Win32/CouponRuc](#), which was encountered by 3.5 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in Mexico in 2Q15 was [Win32/InstalleRex](#), which was encountered by 2.3 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own “Installed On” date in Programs and Features to make it more difficult for a user to locate it and remove it.
- The third most common unwanted software family encountered in Mexico in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 1.6 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user’s consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.

Top threat families by infection rate

The most common malware families by infection rate in Mexico in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	7.0
2	VBS/Jenxcus	Worms	4.5
3	Win32/Kilim	Trojans	1.4
4	Win32/Gamarue	Worms	1.3
5	Win32/Dorkbot	Worms	0.9
6	Win32/Brontok	Worms	0.7
7	Win32/CompromisedCert	Other Malware	0.5
8	Win32/Lefgroo	Worms	0.5
9	Win32/Sality	Viruses	0.4
10	Win32/Vobfus	Worms	0.3

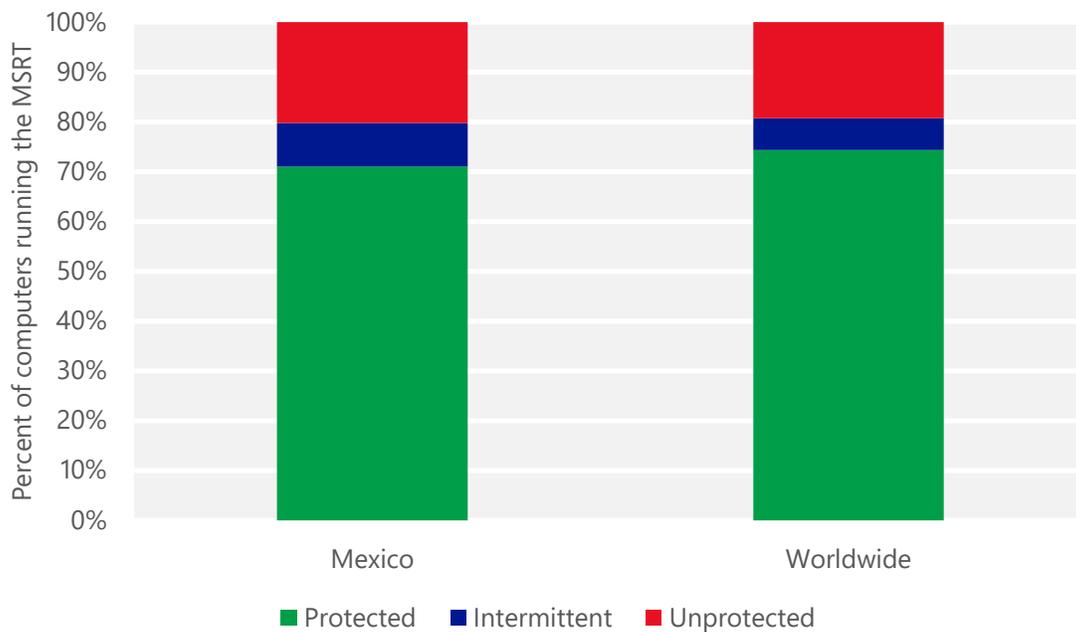
- The most common threat family infecting computers in Mexico in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 7.0 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Mexico in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 4.5 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The third most common threat family infecting computers in Mexico in 2Q15 was [Win32/Kilim](#), which was detected and removed from 1.4 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The fourth most common threat family infecting computers in Mexico in 2Q15 was [Win32/Gamarue](#), which was detected and removed from 1.3 of every 1,000 unique computers scanned by the MSRT. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Mexico and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Mexico

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.10 (0.28)	0.16 (0.24)
Phishing sites per 1,000 hosts (Worldwide)		2.30 (5.0)
Malware hosting sites per 1,000 hosts (Worldwide)		9.47 (16.7)

Moldova

The statistics presented here are generated by Microsoft security programs and services running on computers in Moldova in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Moldova

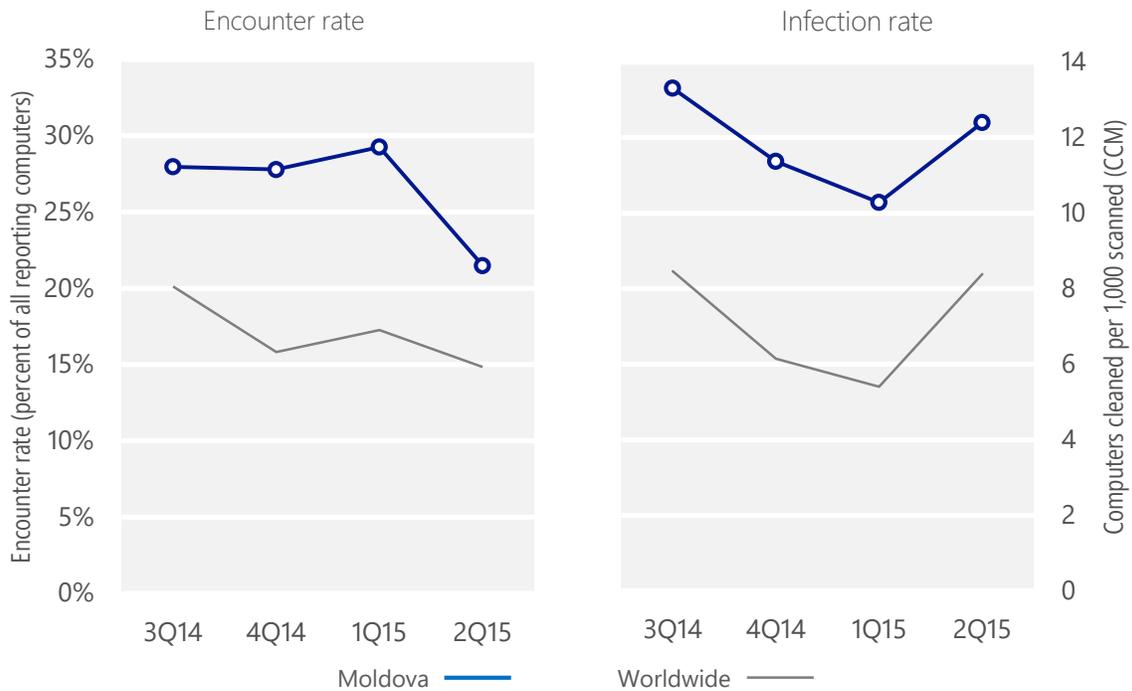
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Moldova	28.0%	27.8%	29.3%	21.5%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Moldova	13.3	11.4	10.3	12.4
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcout, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 21.5% of computers in Moldova encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 12.4 of every 1,000 unique computers scanned in Moldova in 2Q15 (a CCM score of 12.4, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Moldova over the last four quarters, compared to the world as a whole.

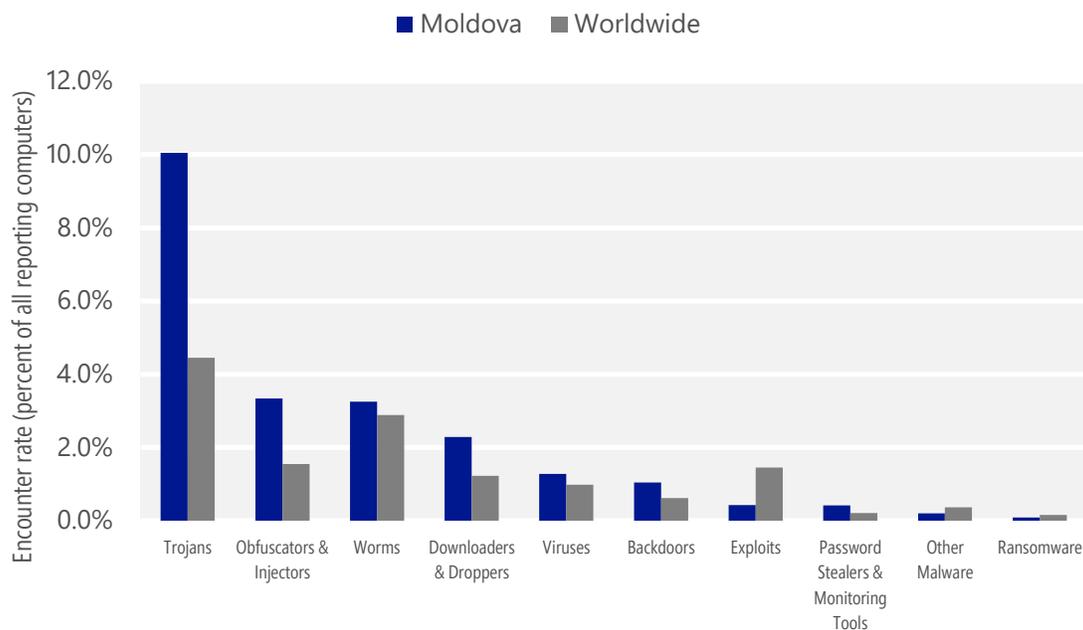
Malware encounter and infection rate trends in Moldova and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in Moldova and around the world, and for explanations of the methods and terms used here.

Malware categories

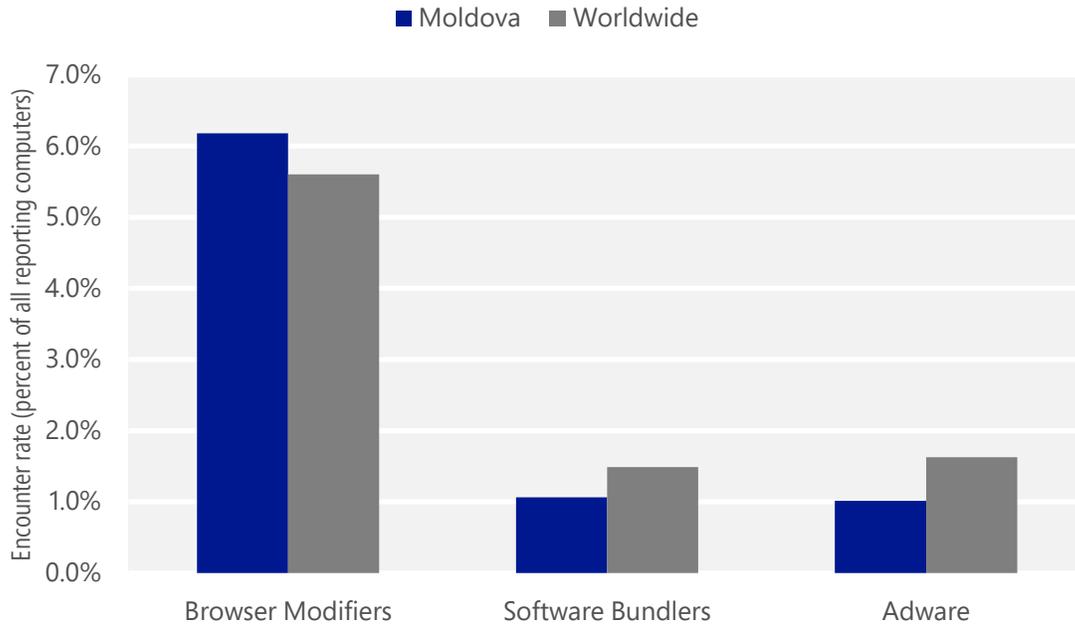
Malware encountered in Moldova in 2Q15, by category



- The most common malware category in Moldova in 2Q15 was Trojans. It was encountered by 10.0 percent of all computers there, down from 11.9 percent in 1Q15.
- The second most common malware category in Moldova in 2Q15 was Obfuscators & Injectors. It was encountered by 3.3 percent of all computers there, down from 6.9 percent in 1Q15.
- The third most common malware category in Moldova in 2Q15 was Worms, which was encountered by 3.3 percent of all computers there, down from 4.7 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Moldova in 2Q15, by category



- The most common unwanted software category in Moldova in 2Q15 was Browser Modifiers. It was encountered by 6.2 percent of all computers there, down from 9.7 percent in 1Q15.
- The second most common unwanted software category in Moldova in 2Q15 was Software Bundlers. It was encountered by 1.1 percent of all computers there, down from 2.3 percent in 1Q15.
- The third most common unwanted software category in Moldova in 2Q15 was Adware, which was encountered by 1.0 percent of all computers there, up from 0.7 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Moldova in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Peals	Trojans	3.2%
2	Win32/Obfuscator	Obfuscators & Injectors	2.8%
3	Win32/Skeeyah	Trojans	1.3%
4	Win32/Ogimant	Downloaders & Droppers	0.9%
5	Win32/Gamarue	Worms	0.8%
6	Win32/Dynamer	Trojans	0.8%
7	Win32/Brontok	Worms	0.7%
8	Win32/Sality	Viruses	0.6%
9	Win32/Kilim	Trojans	0.6%
10	VBS/Jenxcus	Worms	0.6%

- The most common malware family encountered in Moldova in 2Q15 was [Win32/Peals](#), which was encountered by 3.2 percent of reporting computers there. [Win32/Peals](#) is a generic detection for various threats that display trojan characteristics.
- The second most common malware family encountered in Moldova in 2Q15 was [Win32/Obfuscator](#), which was encountered by 2.8 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The third most common malware family encountered in Moldova in 2Q15 was [Win32/Skeeyah](#), which was encountered by 1.3 percent of reporting computers there. [Win32/Skeeyah](#) is a generic detection for various threats that display trojan characteristics.
- The fourth most common malware family encountered in Moldova in 2Q15 was [Win32/Ogimant](#), which was encountered by 0.9 percent of reporting computers there. [Win32/Ogimant](#) is a threat that claims to help download items from the Internet, but actually downloads and runs files that are specified by a remote attacker.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Moldova in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/KipodToolsCby	Browser Modifiers	3.5%
2	Win32/CouponRuc	Browser Modifiers	2.1%
3	Win32/InstalleRex	Software Bundlers	1.0%
4	Win32/SaverExtension	Adware	0.6%
5	Win32/AlterbookSP	Browser Modifiers	0.4%

- The most common unwanted software family encountered in Moldova in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 3.5 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common unwanted software family encountered in Moldova in 2Q15 was [Win32/CouponRuc](#), which was encountered by 2.1 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The third most common unwanted software family encountered in Moldova in 2Q15 was [Win32/InstalleRex](#), which was encountered by 1.0 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Moldova in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	3.0
2	Win32/Brontok	Worms	1.5
3	Win32/Gamarue	Worms	1.2
4	VBS/Jenxcus	Worms	1.0
5	Win32/Ramnit	Trojans	1.0
6	Win32/Kilim	Trojans	0.9
7	Win32/CompromisedCert	Other Malware	0.8
8	Win32/Sality	Viruses	0.6
9	Win32/Dorkbot	Worms	0.5
10	Win32/Helompy	Worms	0.4

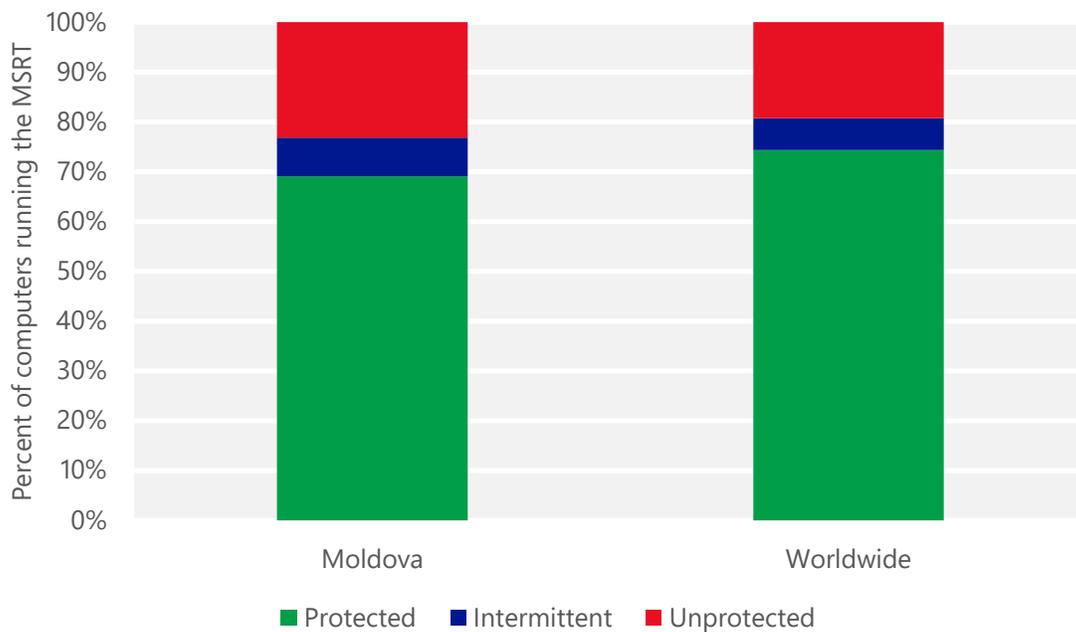
- The most common threat family infecting computers in Moldova in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 3.0 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Moldova in 2Q15 was [Win32/Brontok](#), which was detected and removed from 1.5 of every 1,000 unique computers scanned by the MSRT. [Win32/Brontok](#) is a mass-mailing email worm that spreads by sending copies of itself as email attachments to addresses gathered from files on the infected computer, and by copying itself to removable volumes. Brontok can disable security software, and may conduct DoS attacks against certain websites.
- The third most common threat family infecting computers in Moldova in 2Q15 was [Win32/Gamarue](#), which was detected and removed from 1.2 of every 1,000 unique computers scanned by the MSRT. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The fourth most common threat family infecting computers in Moldova in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 1.0 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Moldova and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Moldova

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	8.58 (0.28)	10.20 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	17.38 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	21.19 (16.7)	

Mongolia

The statistics presented here are generated by Microsoft security programs and services running on computers in Mongolia in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Mongolia

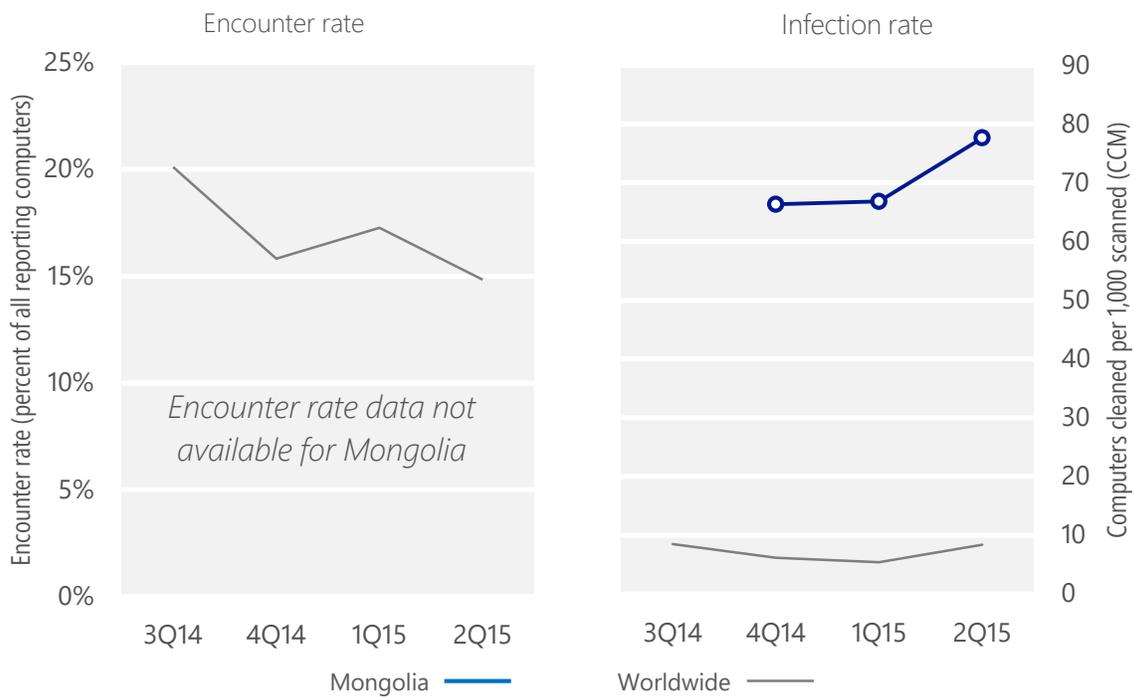
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Mongolia	N/A	N/A	N/A	N/A
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Mongolia	N/A	66.3	66.8	77.6
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcoute, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, the MSRT detected and removed malware from 77.6 of every 1,000 unique computers scanned in Mongolia in 2Q15 (a CCM score of 77.6, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Mongolia over the last four quarters, compared to the world as a whole.

Malware encounter and infection rate trends in Mongolia and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in Mongolia and around the world, and for explanations of the methods and terms used here.

Top threat families by infection rate

The most common malware families by infection rate in Mongolia in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/Gamarue	Worms	36.9
2	VBS/Jenxcus	Worms	12.8
3	Win32/Sality	Viruses	11.3
4	Win32/leEnablerCby	Browser Modifiers	10.4
5	Win32/Ramnit	Trojans	4.9
6	Win32/Kilim	Trojans	4.5
7	Win32/Vobfus	Worms	2.7
8	Win32/Dorkbot	Worms	2.4
9	Win32/Brontok	Worms	2.3
10	Win32/Virut	Viruses	2.3

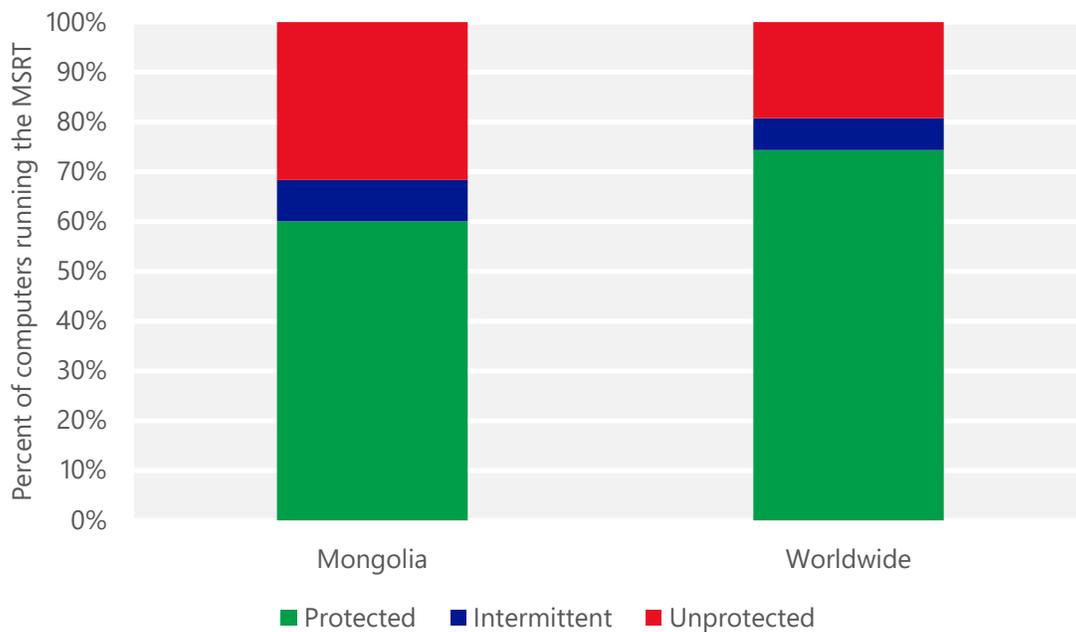
- The most common threat family infecting computers in Mongolia in 2Q15 was [Win32/Gamarue](#), which was detected and removed from 36.9 of every 1,000 unique computers scanned by the MSRT. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The second most common threat family infecting computers in Mongolia in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 12.8 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The third most common threat family infecting computers in Mongolia in 2Q15 was [Win32/Sality](#), which was detected and removed from 11.3 of every 1,000 unique computers scanned by the MSRT. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The fourth most common threat family infecting computers in Mongolia in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 10.4 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Mongolia and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Mongolia

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	4.11 (0.28)	1.91 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	7.99 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	11.67 (16.7)	

Morocco

The statistics presented here are generated by Microsoft security programs and services running on computers in Morocco in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Morocco

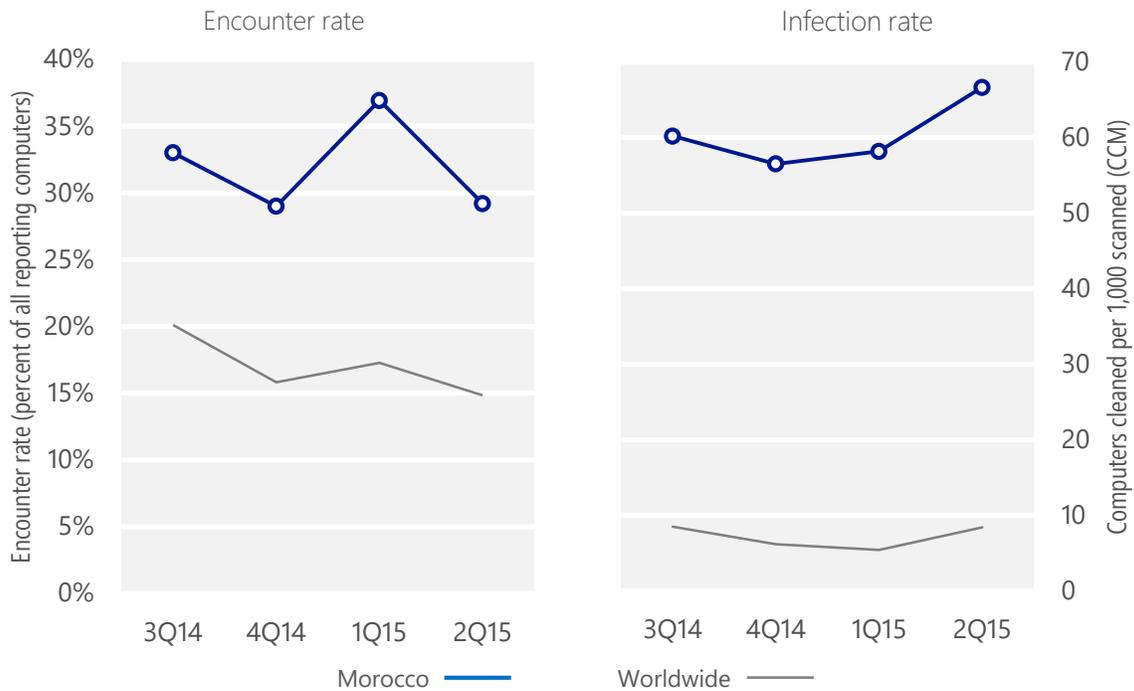
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Morocco	33.0%	29.0%	36.9%	29.2%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Morocco	60.2	56.5	58.2	66.6
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcout, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 29.2% of computers in Morocco encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 66.6 of every 1,000 unique computers scanned in Morocco in 2Q15 (a CCM score of 66.6, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Morocco over the last four quarters, compared to the world as a whole.

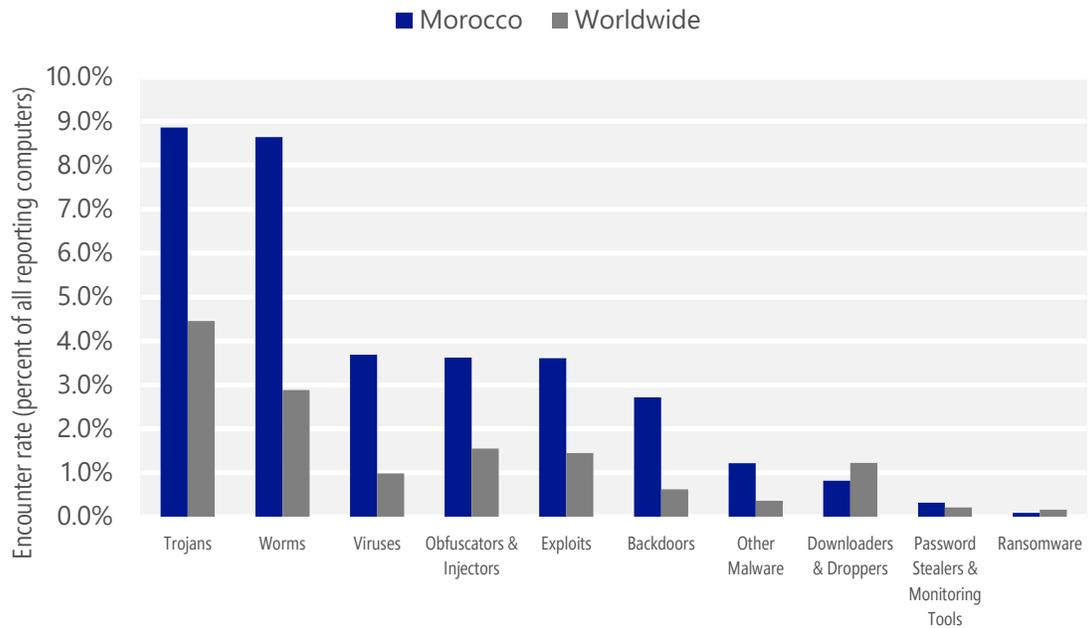
Malware encounter and infection rate trends in Morocco and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in Morocco and around the world, and for explanations of the methods and terms used here.

Malware categories

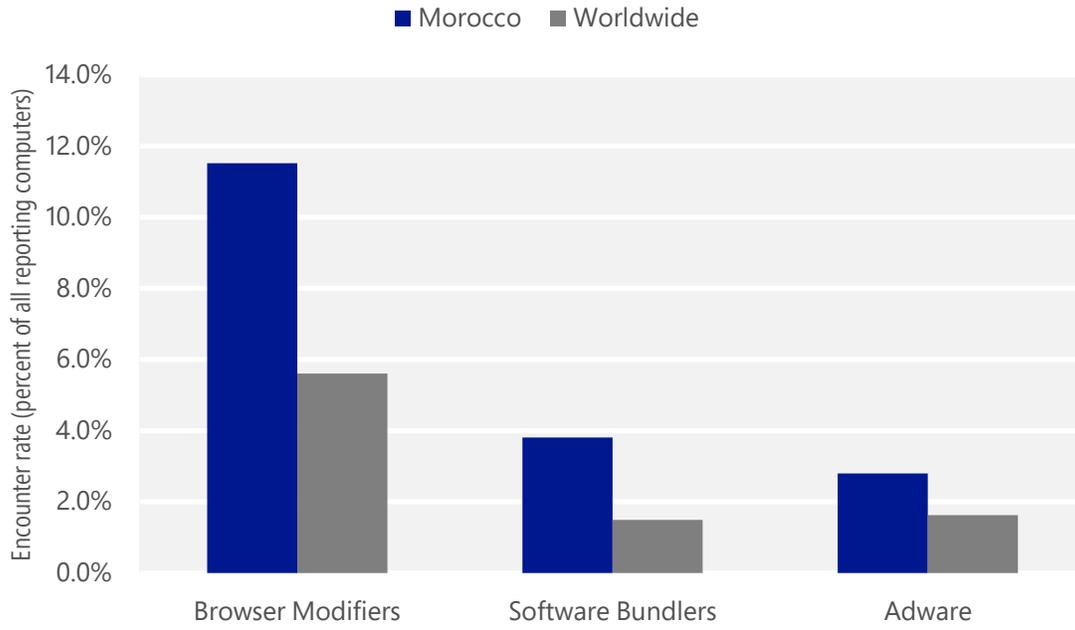
Malware encountered in Morocco in 2Q15, by category



- The most common malware category in Morocco in 2Q15 was Trojans. It was encountered by 8.9 percent of all computers there, down from 11.1 percent in 1Q15.
- The second most common malware category in Morocco in 2Q15 was Worms. It was encountered by 8.6 percent of all computers there, down from 9.6 percent in 1Q15.
- The third most common malware category in Morocco in 2Q15 was Viruses, which was encountered by 3.7 percent of all computers there, down from 4.2 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Morocco in 2Q15, by category



- The most common unwanted software category in Morocco in 2Q15 was Browser Modifiers. It was encountered by 11.5 percent of all computers there, down from 19.2 percent in 1Q15.
- The second most common unwanted software category in Morocco in 2Q15 was Software Bundlers. It was encountered by 3.8 percent of all computers there, down from 5.9 percent in 1Q15.
- The third most common unwanted software category in Morocco in 2Q15 was Adware, which was encountered by 2.8 percent of all computers there, up from 1.6 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Morocco in 2Q15

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	4.5%
2	Win32/Ramnit	Trojans	2.9%
3	Win32/CplLnk	Exploits	2.8%
4	INF/Autorun	Obfuscators & Injectors	2.0%
5	Win32/Obfuscator	Obfuscators & Injectors	1.8%
6	Win32/Sality	Viruses	1.7%
7	Win32/Kilim	Trojans	1.6%
8	MSIL/Bladabindi	Backdoors	1.2%
9	Win32/Skeeyah	Trojans	1.0%
10	Win32/Caphaw	Backdoors	0.8%

- The most common malware family encountered in Morocco in 2Q15 was [VBS/Jenxcus](#), which was encountered by 4.5 percent of reporting computers there. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common malware family encountered in Morocco in 2Q15 was [Win32/Ramnit](#), which was encountered by 2.9 percent of reporting computers there. [Win32/Ramnit](#) is a family of multi-component malware that infects executable files, Microsoft Office files, and HTML files. Win32/Ramnit spreads to removable drives and steals sensitive information such as saved FTP credentials and browser cookies. It may also open a backdoor to await instructions from a remote attacker.
- The third most common malware family encountered in Morocco in 2Q15 was [Win32/CplLnk](#), which was encountered by 2.8 percent of reporting computers there. [Win32/CplLnk](#) is a generic detection for specially-crafted malicious shortcut files that attempt to exploit the vulnerability addressed by Microsoft Security Bulletin MS10-046.
- The fourth most common malware family encountered in Morocco in 2Q15 was [INF/Autorun](#), which was encountered by 2.0 percent of reporting computers there. [INF/Autorun](#) is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Morocco in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/KipodToolsCby	Browser Modifiers	5.9%
2	Win32/CouponRuc	Browser Modifiers	5.6%
3	Win32/InstalleRex	Software Bundlers	3.7%
4	Win32/SaverExtension	Adware	1.8%
5	Win32/AlterbookSP	Browser Modifiers	0.4%

- The most common unwanted software family encountered in Morocco in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 5.9 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common unwanted software family encountered in Morocco in 2Q15 was [Win32/CouponRuc](#), which was encountered by 5.6 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The third most common unwanted software family encountered in Morocco in 2Q15 was [Win32/InstalleRex](#), which was encountered by 3.7 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Morocco in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/Yeltminky	Worms	23.8
2	VBS/Jenxcus	Worms	13.0
3	Win32/leEnablerCby	Browser Modifiers	8.8
4	Win32/Sality	Viruses	8.1
5	Win32/Nitol	Other Malware	7.8
6	Win32/Ramnit	Trojans	6.8
7	MSIL/Bladabindi	Backdoors	3.0
8	Win32/Kilim	Trojans	2.9
9	Win32/Dorkbot	Worms	1.3
10	Win32/Pramro	Trojans	1.0

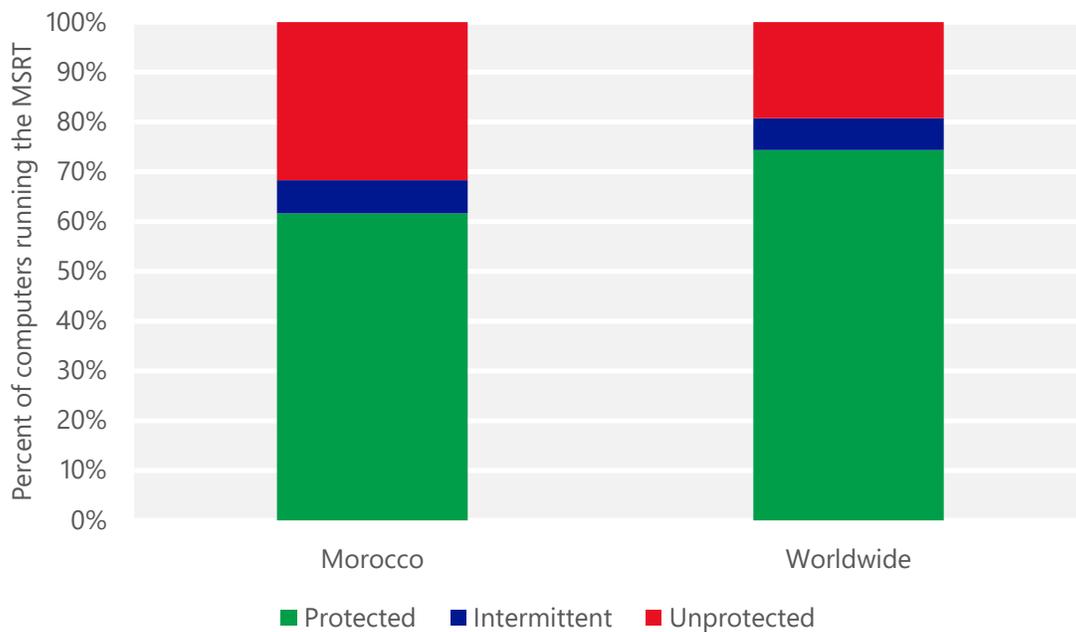
- The most common threat family infecting computers in Morocco in 2Q15 was [Win32/Yeltminky](#), which was detected and removed from 23.8 of every 1,000 unique computers scanned by the MSRT. [Win32/Yeltminky](#) is a family of worms that spreads by making copies of itself on all available drives and creating an autorun.inf file to execute that copy.
- The second most common threat family infecting computers in Morocco in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 13.0 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The third most common threat family infecting computers in Morocco in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 8.8 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The fourth most common threat family infecting computers in Morocco in 2Q15 was [Win32/Sality](#), which was detected and removed from 8.1 of every 1,000 unique computers scanned by the MSRT. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Morocco and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Morocco

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.01 (0.28)	0.03 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	4.89 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	7.17 (16.7)	

Nepal

The statistics presented here are generated by Microsoft security programs and services running on computers in Nepal in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Nepal

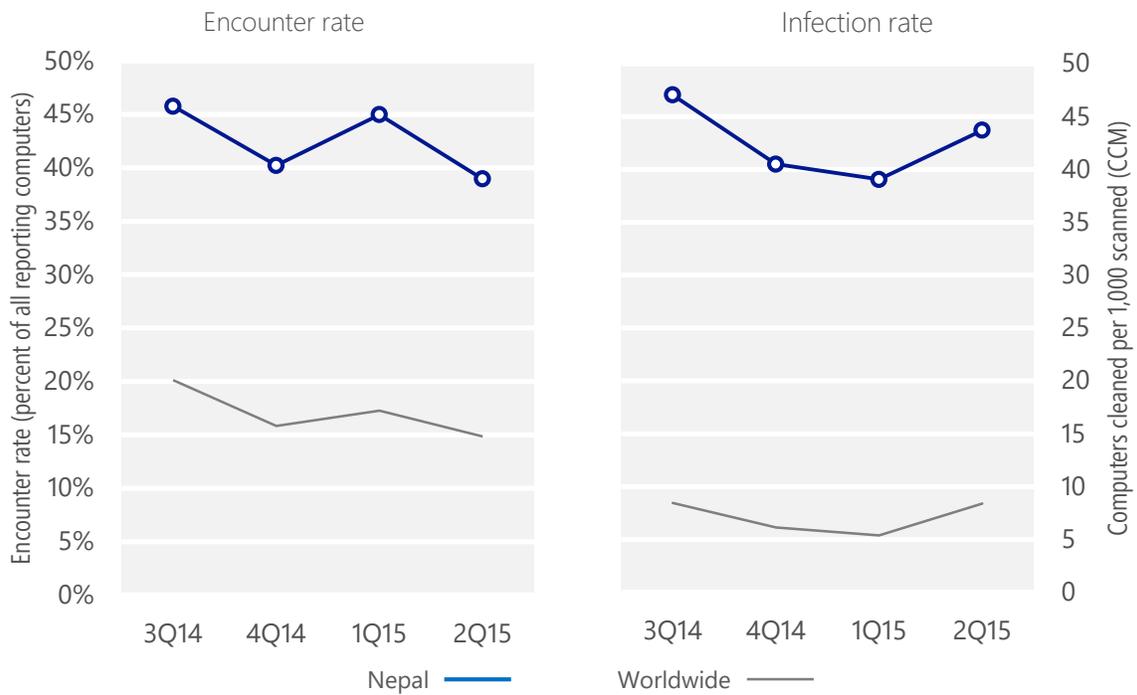
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Nepal	45.8%	40.2%	45.0%	39.0%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Nepal	47.1	40.5	39.1	43.7
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcoute, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 39.0% of computers in Nepal encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 43.7 of every 1,000 unique computers scanned in Nepal in 2Q15 (a CCM score of 43.7, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Nepal over the last four quarters, compared to the world as a whole.

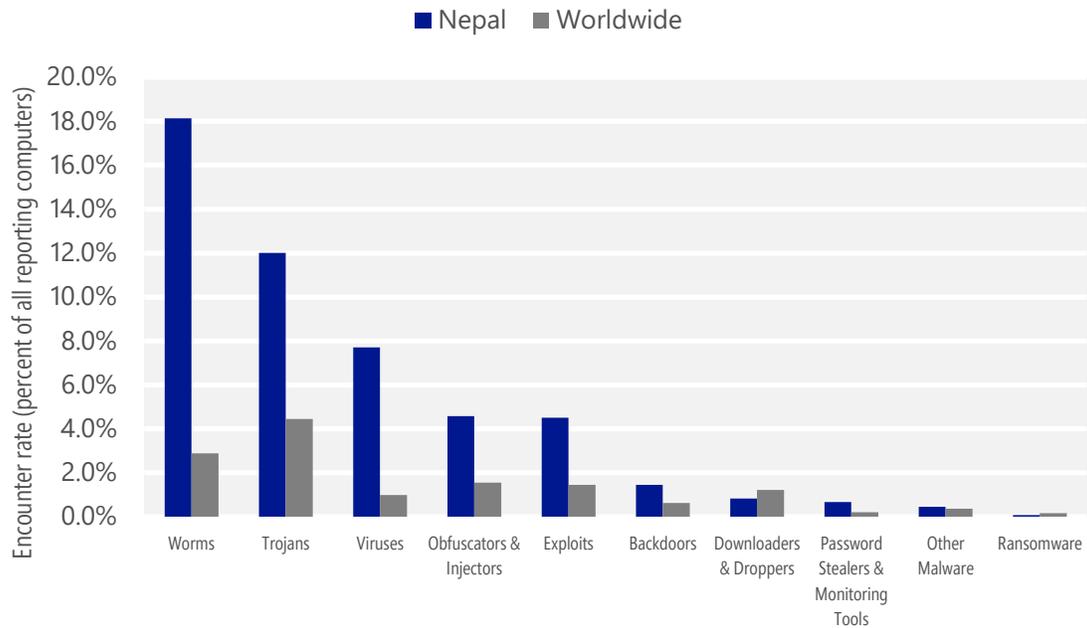
Malware encounter and infection rate trends in Nepal and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in Nepal and around the world, and for explanations of the methods and terms used here.

Malware categories

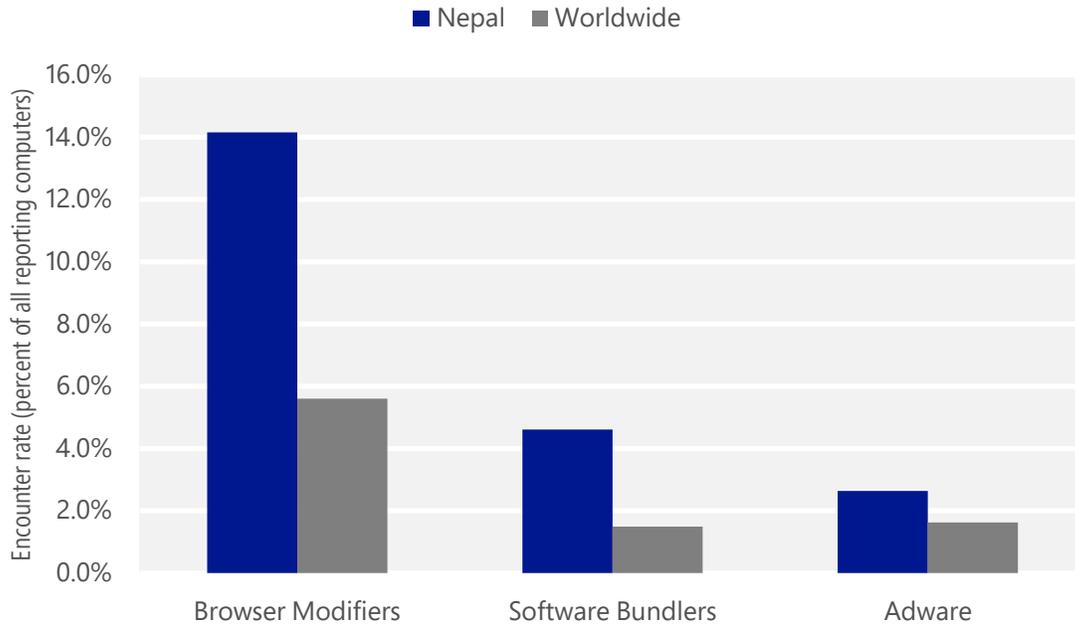
Malware encountered in Nepal in 2Q15, by category



- The most common malware category in Nepal in 2Q15 was Worms. It was encountered by 18.1 percent of all computers there, down from 22.2 percent in 1Q15.
- The second most common malware category in Nepal in 2Q15 was Trojans. It was encountered by 12.0 percent of all computers there, down from 12.4 percent in 1Q15.
- The third most common malware category in Nepal in 2Q15 was Viruses, which was encountered by 7.7 percent of all computers there, down from 9.2 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Nepal in 2Q15, by category



- The most common unwanted software category in Nepal in 2Q15 was Browser Modifiers. It was encountered by 14.2 percent of all computers there, down from 20.4 percent in 1Q15.
- The second most common unwanted software category in Nepal in 2Q15 was Software Bundlers. It was encountered by 4.6 percent of all computers there, down from 5.3 percent in 1Q15.
- The third most common unwanted software category in Nepal in 2Q15 was Adware, which was encountered by 2.6 percent of all computers there, up from 1.5 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Nepal in 2Q15

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	10.0%
2	INF/Autorun	Obfuscators & Injectors	4.1%
3	Win32/CplLnk	Exploits	3.8%
4	Win32/Ramnit	Trojans	3.8%
5	Win32/Virut	Viruses	2.8%
6	Win32/Sality	Viruses	2.5%
7	Win32/Finodes	Trojans	2.4%
8	Win32/Ippedo	Worms	2.3%
9	Win32/Jeefo	Viruses	2.3%
10	Win32/Obfuscator	Obfuscators & Injectors	2.2%

- The most common malware family encountered in Nepal in 2Q15 was [VBS/Jenxcus](#), which was encountered by 10.0 percent of reporting computers there. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common malware family encountered in Nepal in 2Q15 was [INF/Autorun](#), which was encountered by 4.1 percent of reporting computers there. [INF/Autorun](#) is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The third most common malware family encountered in Nepal in 2Q15 was [Win32/CplLnk](#), which was encountered by 3.8 percent of reporting computers there. [Win32/CplLnk](#) is a generic detection for specially-crafted malicious shortcut files that attempt to exploit the vulnerability addressed by Microsoft Security Bulletin MS10-046.
- The fourth most common malware family encountered in Nepal in 2Q15 was [Win32/Ramnit](#), which was encountered by 3.8 percent of reporting computers there. [Win32/Ramnit](#) is a family of multi-component malware that infects executable files, Microsoft Office files, and HTML files. [Win32/Ramnit](#) spreads to removable drives and steals sensitive information such as saved FTP credentials and browser cookies. It may also open a backdoor to await instructions from a remote attacker.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Nepal in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/KipodToolsCby	Browser Modifiers	8.4%
2	Win32/CouponRuc	Browser Modifiers	6.2%
3	Win32/InstalleRex	Software Bundlers	4.4%
4	Win32/SaverExtension	Adware	1.7%
5	Win32/AlterbookSP	Browser Modifiers	0.6%

- The most common unwanted software family encountered in Nepal in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 8.4 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common unwanted software family encountered in Nepal in 2Q15 was [Win32/CouponRuc](#), which was encountered by 6.2 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The third most common unwanted software family encountered in Nepal in 2Q15 was [Win32/InstalleRex](#), which was encountered by 4.4 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Nepal in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	15.7
2	Win32/Jeefo	Viruses	6.3
3	Win32/Sality	Viruses	5.9
4	Win32/Ramnit	Trojans	5.6
5	Win32/leEnablerCby	Browser Modifiers	5.3
6	Win32/Virut	Viruses	2.7
7	Win32/Nuqel	Worms	2.5
8	Win32/Gamarue	Worms	1.9
9	Win32/Kilim	Trojans	1.3
10	Win32/CompromisedCert	Other Malware	0.7

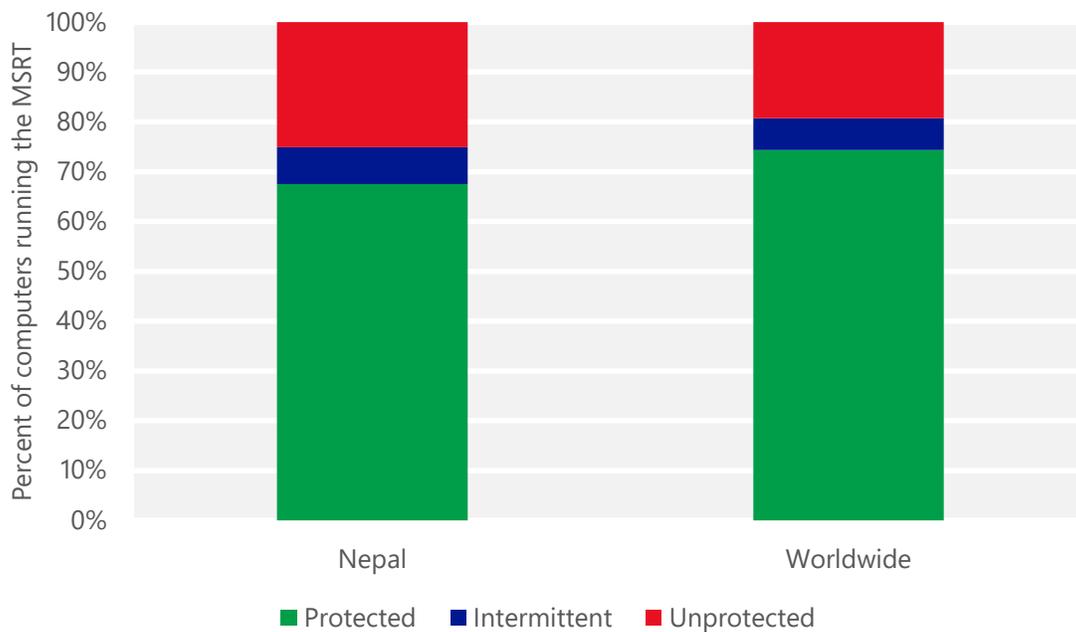
- The most common threat family infecting computers in Nepal in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 15.7 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Nepal in 2Q15 was [Win32/Jeefo](#), which was detected and removed from 6.3 of every 1,000 unique computers scanned by the MSRT. [Win32/Jeefo](#) is a parasitic file-infecting virus that infects Windows portable executable (PE) files that are greater than or equal to 102,400 bytes long. When an infected PE file runs, the virus tries to run the original content of the file.
- The third most common threat family infecting computers in Nepal in 2Q15 was [Win32/Sality](#), which was detected and removed from 5.9 of every 1,000 unique computers scanned by the MSRT. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The fourth most common threat family infecting computers in Nepal in 2Q15 was [Win32/Ramnit](#), which was detected and removed from 5.6 of every 1,000 unique computers scanned by the MSRT. [Win32/Ramnit](#) is a family of multi-component malware that infects executable files, Microsoft Office files, and HTML files. Win32/Ramnit spreads to removable drives and steals sensitive information such as saved FTP credentials and browser cookies. It may also open a backdoor to await instructions from a remote attacker.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Nepal and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Nepal

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.07 (0.28)	0.00 (0.24)
Phishing sites per 1,000 hosts (Worldwide)		3.58 (5.0)
Malware hosting sites per 1,000 hosts (Worldwide)		15.23 (16.7)

Netherlands

The statistics presented here are generated by Microsoft security programs and services running on computers in the Netherlands in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for the Netherlands

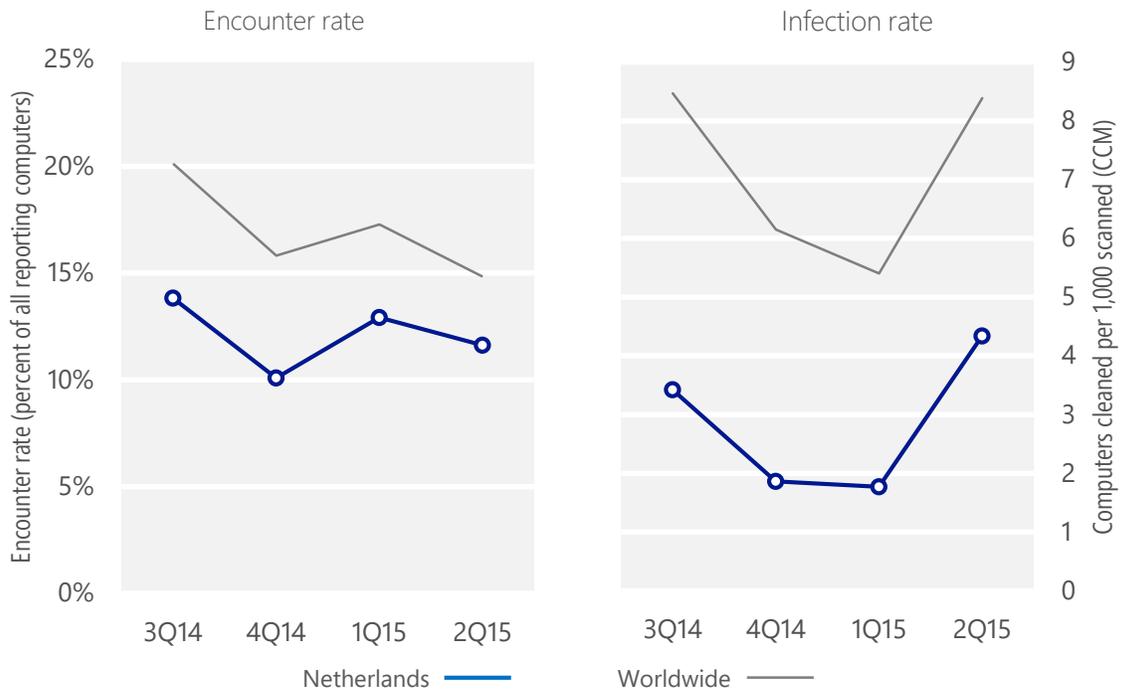
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Netherlands	13.8%	10.1%	12.9%	11.6%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Netherlands	3.4	1.9	1.8	4.3
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcout, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 11.6% of computers in the Netherlands encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 4.3 of every 1,000 unique computers scanned in the Netherlands in 2Q15 (a CCM score of 4.3, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for the Netherlands over the last four quarters, compared to the world as a whole.

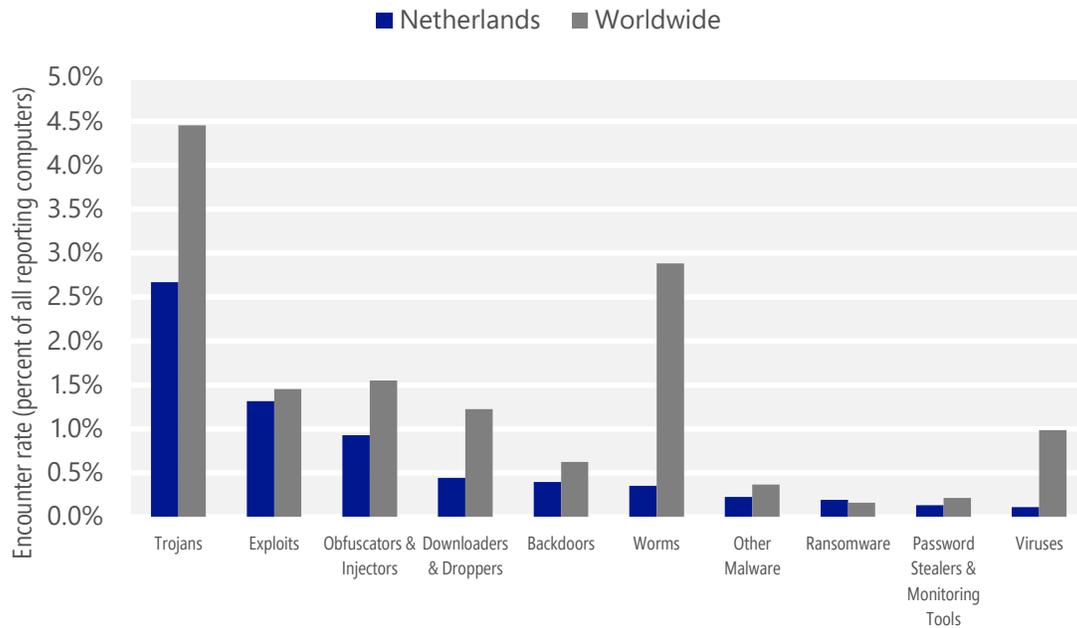
Malware encounter and infection rate trends in the Netherlands and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in the Netherlands and around the world, and for explanations of the methods and terms used here.

Malware categories

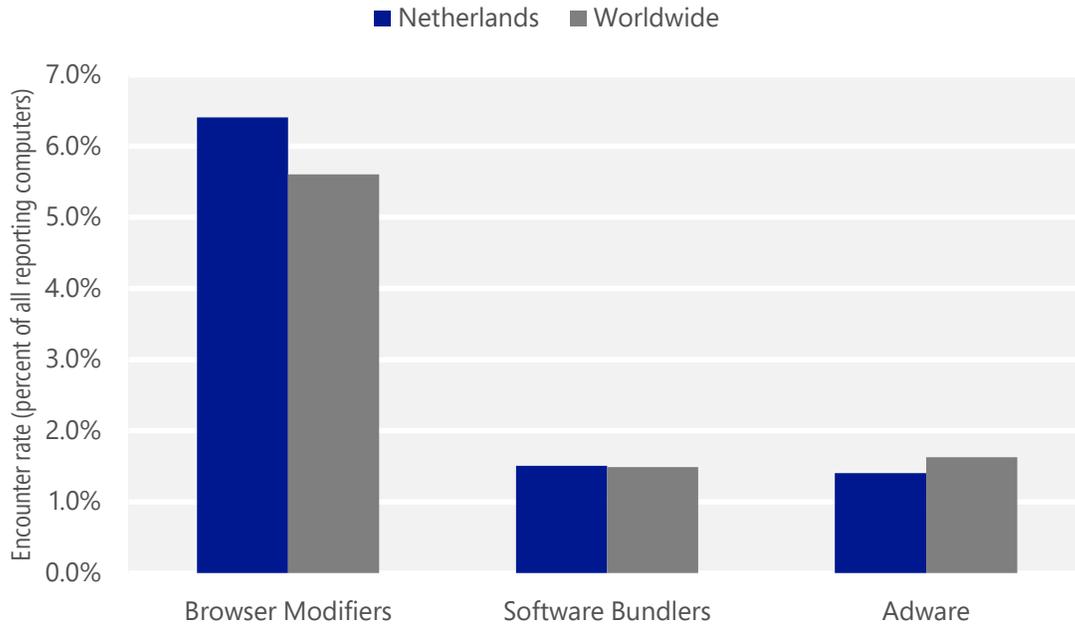
Malware encountered in the Netherlands in 2Q15, by category



- The most common malware category in the Netherlands in 2Q15 was Trojans. It was encountered by 2.7 percent of all computers there, up from 1.7 percent in 1Q15.
- The second most common malware category in the Netherlands in 2Q15 was Exploits. It was encountered by 1.3 percent of all computers there, down from 1.6 percent in 1Q15.
- The third most common malware category in the Netherlands in 2Q15 was Obfuscators & Injectors, which was encountered by 0.9 percent of all computers there, up from 0.9 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in the Netherlands in 2Q15, by category



- The most common unwanted software category in the Netherlands in 2Q15 was Browser Modifiers. It was encountered by 6.4 percent of all computers there, down from 6.8 percent in 1Q15.
- The second most common unwanted software category in the Netherlands in 2Q15 was Software Bundlers. It was encountered by 1.5 percent of all computers there, down from 3.8 percent in 1Q15.
- The third most common unwanted software category in the Netherlands in 2Q15 was Adware, which was encountered by 1.4 percent of all computers there, up from 0.4 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in the Netherlands in 2Q15

	Family	Most significant category	% of reporting computers
1	JS/Axpergle	Exploits	0.8%
2	Win32/Kilim	Trojans	0.8%
3	Win32/Obfuscator	Obfuscators & Injectors	0.8%
4	Win32/Skeeyah	Trojans	0.6%
5	Win32/Peals	Trojans	0.3%
6	Win32/Dynamer	Trojans	0.2%
7	Win32/Sdbby	Exploits	0.2%
8	Win32/Fynloski	Backdoors	0.1%
9	ASX/Wimad	Downloaders & Droppers	0.1%
10	JS/Neclu	Exploits	0.1%

- The most common malware family encountered in the Netherlands in 2Q15 was [JS/Axpergle](#), which was encountered by 0.8 percent of reporting computers there. [JS/Axpergle](#) is a detection for the Angler exploit kit, which exploits vulnerabilities in recent versions of Internet Explorer, Silverlight, Adobe Flash Player, and Java to install malware.
- The second most common malware family encountered in the Netherlands in 2Q15 was [Win32/Kilim](#), which was encountered by 0.8 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The third most common malware family encountered in the Netherlands in 2Q15 was [Win32/Obfuscator](#), which was encountered by 0.8 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The fourth most common malware family encountered in the Netherlands in 2Q15 was [Win32/Skeeyah](#), which was encountered by 0.6 percent of reporting computers there. [Win32/Skeeyah](#) is a generic detection for various threats that display trojan characteristics.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in the Netherlands in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/KipodToolsCby	Browser Modifiers	2.9%
2	Win32/CouponRuc	Browser Modifiers	2.5%
3	Win32/InstalleRex	Software Bundlers	1.5%
4	Win32/AlterbookSP	Browser Modifiers	0.9%
5	Win32/SaverExtension	Adware	0.9%

- The most common unwanted software family encountered in the Netherlands in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 2.9 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common unwanted software family encountered in the Netherlands in 2Q15 was [Win32/CouponRuc](#), which was encountered by 2.5 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The third most common unwanted software family encountered in the Netherlands in 2Q15 was [Win32/InstalleRex](#), which was encountered by 1.5 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in the Netherlands in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	1.2
2	Win32/Kilim	Trojans	1.0
3	Win32/CompromisedCert	Other Malware	1.0
4	Win32/Carberp	Trojans	0.1
5	Win32/Simda	Trojans	0.1
6	Win32/Alureon	Trojans	0.1
7	MSIL/Bladabindi	Backdoors	0.1
8	Win32/Nitol	Other Malware	0.1
9	Win32/Gamarue	Worms	0.1
10	Win32/Sinowal	Password Stealers & Monitoring Tools	0.1

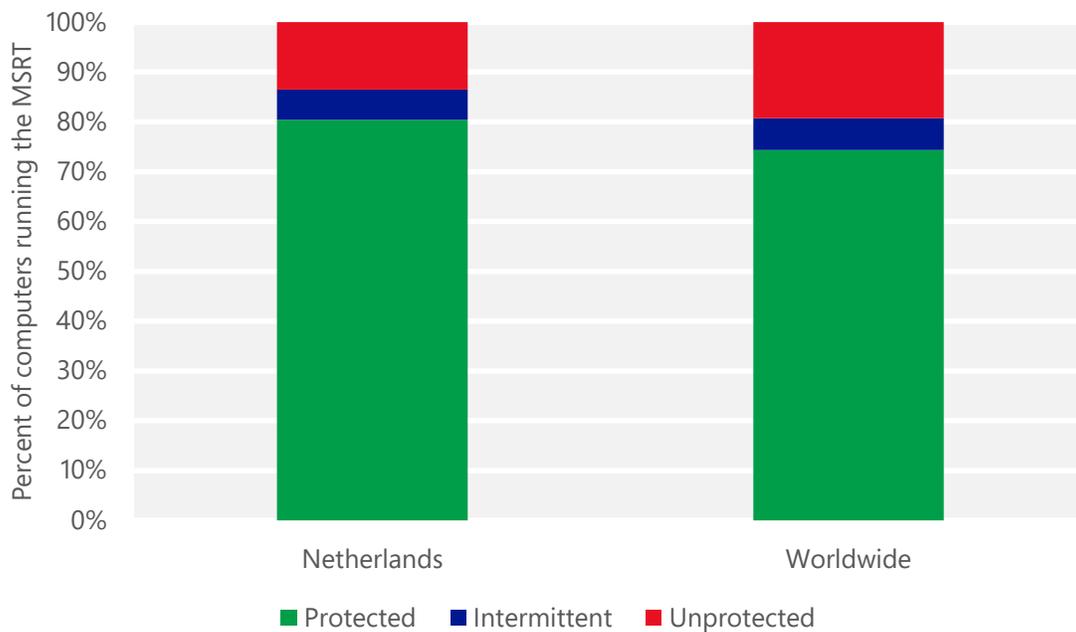
- The most common threat family infecting computers in the Netherlands in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 1.2 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in the Netherlands in 2Q15 was [Win32/Kilim](#), which was detected and removed from 1.0 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The third most common threat family infecting computers in the Netherlands in 2Q15 was [Win32/CompromisedCert](#), which was detected and removed from 1.0 of every 1,000 unique computers scanned by the MSRT. [Win32/CompromisedCert](#) is a detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.
- The fourth most common threat family infecting computers in the Netherlands in 2Q15 was [Win32/Carberp](#), which was detected and removed from 0.1 of every 1,000 unique computers scanned by the MSRT. [Win32/Carberp](#) is a family of trojans that can steal online banking credentials as well as user names and passwords from a number of applications. They can also download other malware and steal sensitive information by taking screenshots or recording which keys the user presses.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in the Netherlands and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for the Netherlands

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.16 (0.28)	0.19 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	5.12 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	17.33 (16.7)	

New Zealand

The statistics presented here are generated by Microsoft security programs and services running on computers in New Zealand in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for New Zealand

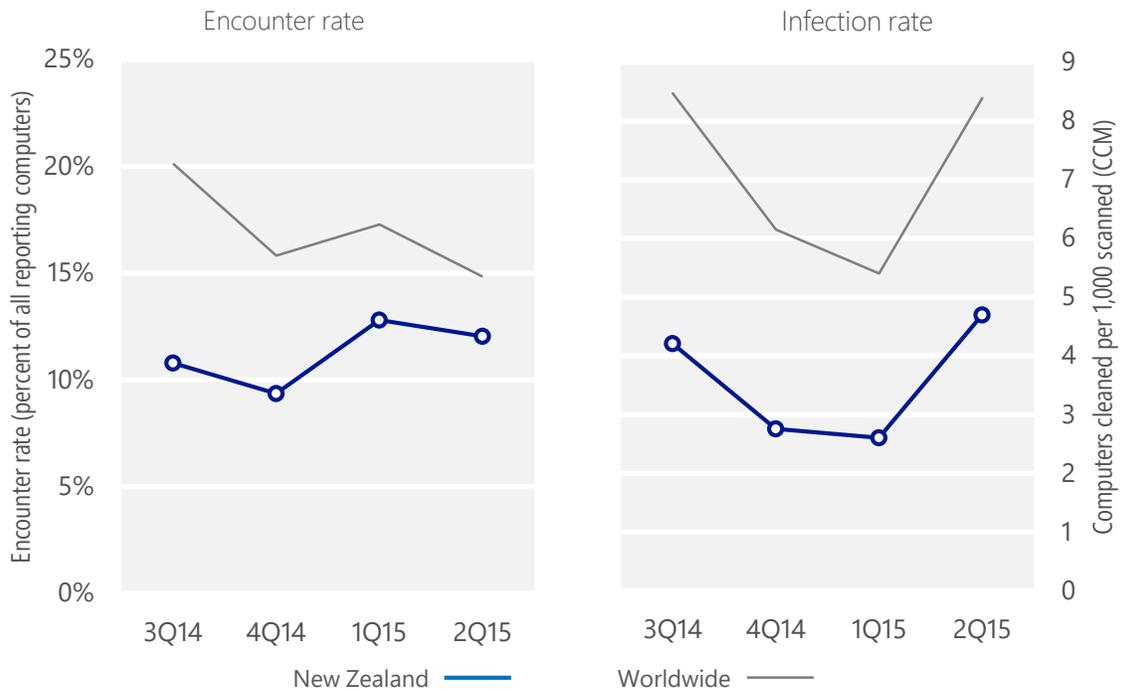
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, New Zealand	10.8%	9.4%	12.8%	12.0%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, New Zealand	4.2	2.8	2.6	4.7
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcoute, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 12.0% of computers in New Zealand encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 4.7 of every 1,000 unique computers scanned in New Zealand in 2Q15 (a CCM score of 4.7, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for New Zealand over the last four quarters, compared to the world as a whole.

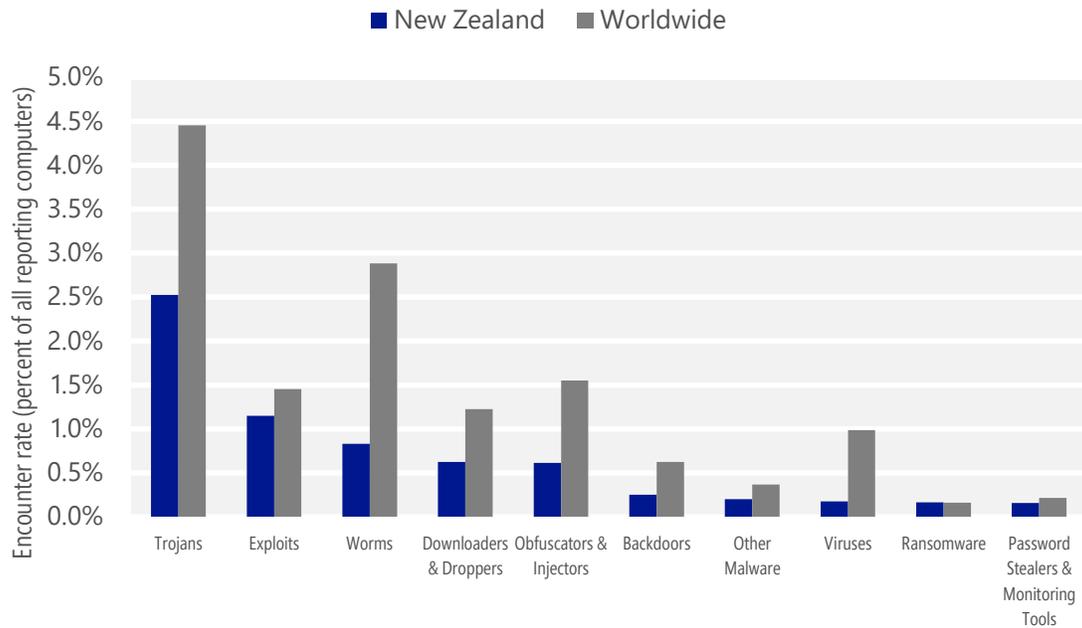
Malware encounter and infection rate trends in New Zealand and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in New Zealand and around the world, and for explanations of the methods and terms used here.

Malware categories

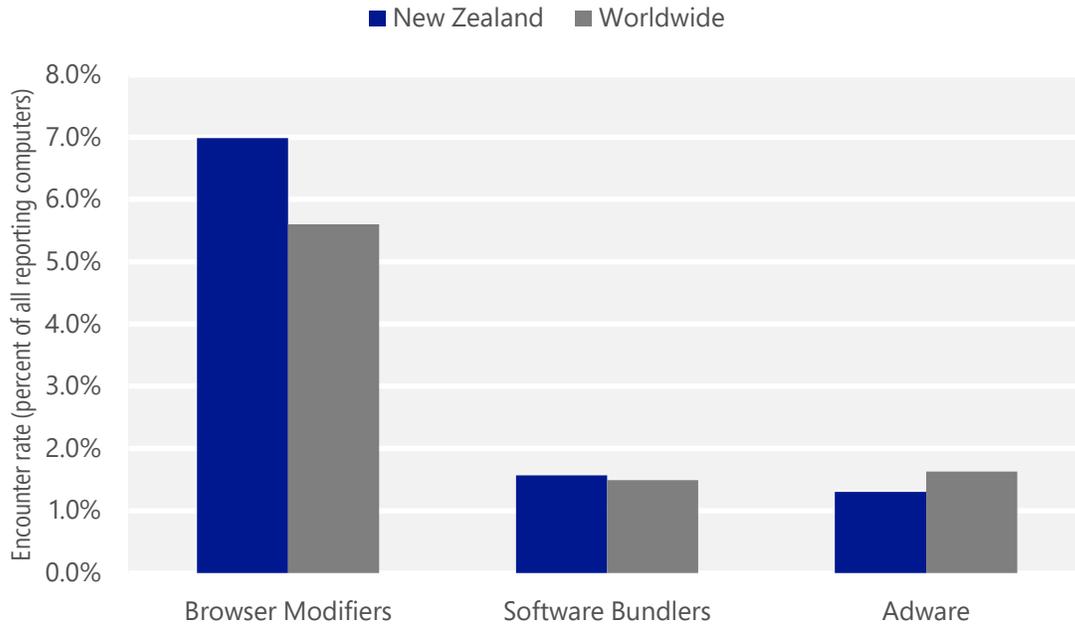
Malware encountered in New Zealand in 2Q15, by category



- The most common malware category in New Zealand in 2Q15 was Trojans. It was encountered by 2.5 percent of all computers there, up from 1.5 percent in 1Q15.
- The second most common malware category in New Zealand in 2Q15 was Exploits. It was encountered by 1.1 percent of all computers there, down from 1.3 percent in 1Q15.
- The third most common malware category in New Zealand in 2Q15 was Worms, which was encountered by 0.8 percent of all computers there, down from 1.1 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in New Zealand in 2Q15, by category



- The most common unwanted software category in New Zealand in 2Q15 was Browser Modifiers. It was encountered by 7.0 percent of all computers there, up from 6.9 percent in 1Q15.
- The second most common unwanted software category in New Zealand in 2Q15 was Software Bundlers. It was encountered by 1.6 percent of all computers there, down from 3.4 percent in 1Q15.
- The third most common unwanted software category in New Zealand in 2Q15 was Adware, which was encountered by 1.3 percent of all computers there, up from 0.5 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in New Zealand in 2Q15

	Family	Most significant category	% of reporting computers
1	JS/Axpergle	Exploits	0.7%
2	Win32/Kilim	Trojans	0.7%
3	Win32/Skeeyah	Trojans	0.6%
4	Win32/Obfuscator	Obfuscators & Injectors	0.5%
5	Win32/Peals	Trojans	0.4%
6	INF/Autorun	Obfuscators & Injectors	0.2%
7	Win32/Upatre	Downloaders & Droppers	0.2%
8	Win32/Nuqel	Worms	0.1%
9	Win32/Sdbby	Exploits	0.1%
10	Win32/Vobfus	Worms	0.1%

- The most common malware family encountered in New Zealand in 2Q15 was [JS/Axpergle](#), which was encountered by 0.7 percent of reporting computers there. [JS/Axpergle](#) is a detection for the Angler exploit kit, which exploits vulnerabilities in recent versions of Internet Explorer, Silverlight, Adobe Flash Player, and Java to install malware.
- The second most common malware family encountered in New Zealand in 2Q15 was [Win32/Kilim](#), which was encountered by 0.7 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The third most common malware family encountered in New Zealand in 2Q15 was [Win32/Skeeyah](#), which was encountered by 0.6 percent of reporting computers there. [Win32/Skeeyah](#) is a generic detection for various threats that display trojan characteristics.
- The fourth most common malware family encountered in New Zealand in 2Q15 was [Win32/Obfuscator](#), which was encountered by 0.5 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in New Zealand in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/KipodToolsCby	Browser Modifiers	3.1%
2	Win32/CouponRuc	Browser Modifiers	2.7%
3	Win32/InstalleRex	Software Bundlers	1.5%
4	Win32/AlterbookSP	Browser Modifiers	1.2%
5	Win32/SaverExtension	Adware	1.0%

- The most common unwanted software family encountered in New Zealand in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 3.1 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common unwanted software family encountered in New Zealand in 2Q15 was [Win32/CouponRuc](#), which was encountered by 2.7 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The third most common unwanted software family encountered in New Zealand in 2Q15 was [Win32/InstalleRex](#), which was encountered by 1.5 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in New Zealand in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	1.4
2	Win32/Kilim	Trojans	1.2
3	Win32/Nuqel	Worms	0.4
4	Win32/Vobfus	Worms	0.3
5	Win32/Brontok	Worms	0.2
6	Win32/Sality	Viruses	0.1
7	Win32/Dyzap	Password Stealers & Monitoring Tools	0.1
8	Win32/Simda	Trojans	0.1
9	VBS/Jenxcus	Worms	0.1
10	Win32/Alureon	Trojans	0.1

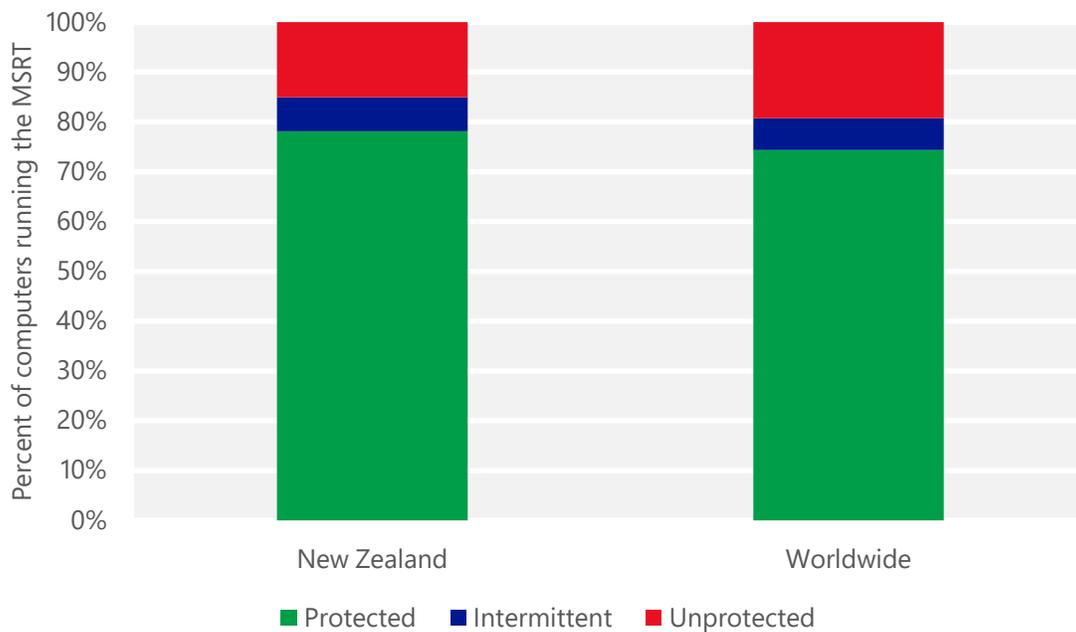
- The most common threat family infecting computers in New Zealand in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 1.4 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in New Zealand in 2Q15 was [Win32/Kilim](#), which was detected and removed from 1.2 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The third most common threat family infecting computers in New Zealand in 2Q15 was [Win32/Nuqel](#), which was detected and removed from 0.4 of every 1,000 unique computers scanned by the MSRT. [Win32/Nuqel](#) is a worm that spreads via mapped drives and certain instant messaging applications. It may modify system settings, connect to certain websites, download arbitrary files, or take other malicious actions.
- The fourth most common threat family infecting computers in New Zealand in 2Q15 was [Win32/Vobfus](#), which was detected and removed from 0.3 of every 1,000 unique computers scanned by the MSRT. [Win32/Vobfus](#) is a family of worms that spreads via network drives and removable drives and download/executes arbitrary files. Downloaded files may include additional malware.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in New Zealand and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for New Zealand

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.04 (0.28)	0.15 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	5.91 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	10.26 (16.7)	

Nicaragua

The statistics presented here are generated by Microsoft security programs and services running on computers in Nicaragua in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Nicaragua

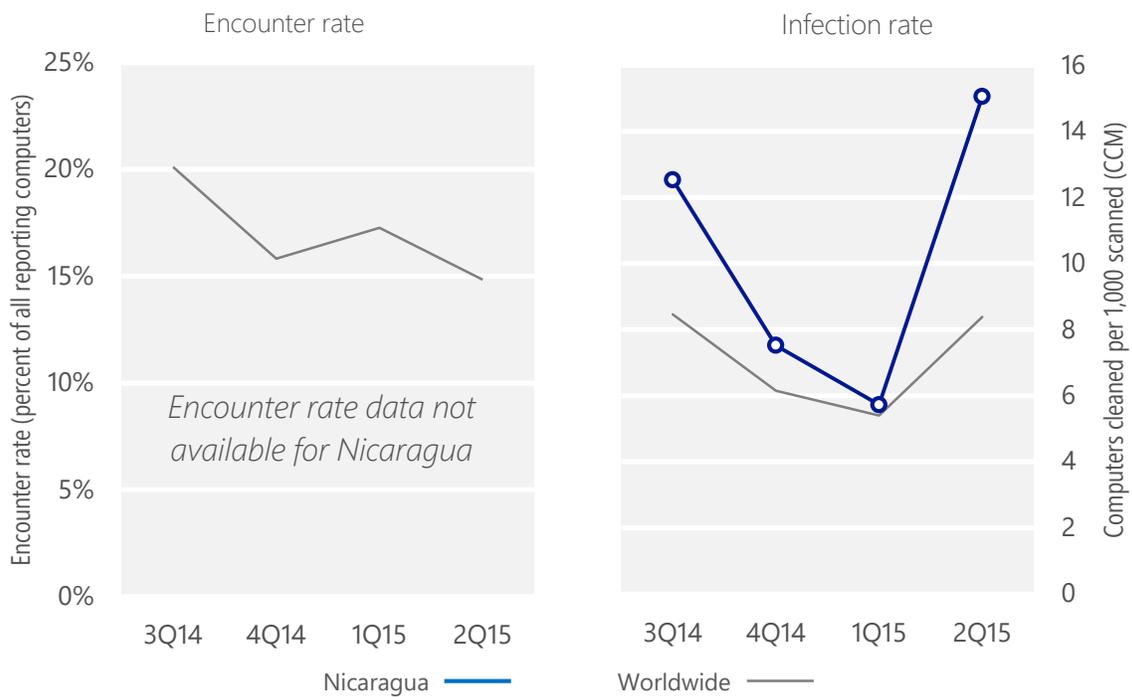
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Nicaragua	N/A	N/A	N/A	N/A
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Nicaragua	12.5	7.5	5.7	15.1
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcoute, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, the MSRT detected and removed malware from 15.1 of every 1,000 unique computers scanned in Nicaragua in 2Q15 (a CCM score of 15.1, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Nicaragua over the last four quarters, compared to the world as a whole.

Malware encounter and infection rate trends in Nicaragua and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in Nicaragua and around the world, and for explanations of the methods and terms used here.

Top threat families by infection rate

The most common malware families by infection rate in Nicaragua in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	8.8
2	Win32/Kilim	Trojans	1.7
3	VBS/Jenxcus	Worms	1.3
4	Win32/Sality	Viruses	0.6
5	Win32/Brontok	Worms	0.5
6	Win32/Yeltminky	Worms	0.3
7	Win32/CompromisedCert	Other Malware	0.2
8	MSIL/Spacekito	Trojans	0.2
9	MSIL/Bladabindi	Backdoors	0.2
10	Win32/Alureon	Trojans	0.2

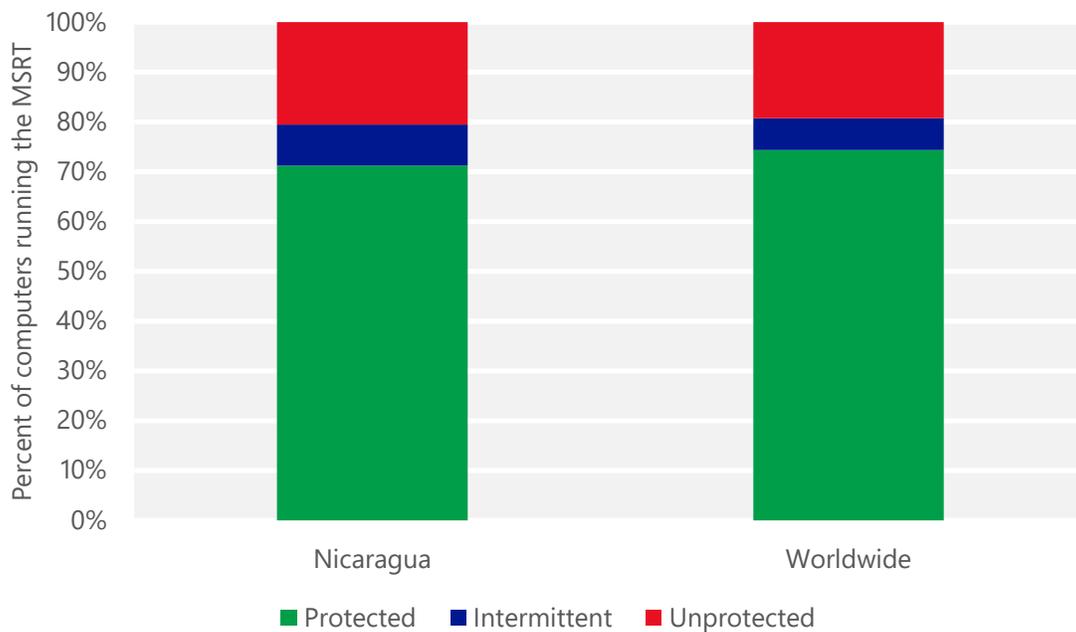
- The most common threat family infecting computers in Nicaragua in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 8.8 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Nicaragua in 2Q15 was [Win32/Kilim](#), which was detected and removed from 1.7 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The third most common threat family infecting computers in Nicaragua in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 1.3 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The fourth most common threat family infecting computers in Nicaragua in 2Q15 was [Win32/Sality](#), which was detected and removed from 0.6 of every 1,000 unique computers scanned by the MSRT. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Nicaragua and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Nicaragua

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.20 (0.28)	0.09 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	4.54 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	9.08 (16.7)	

Nigeria

The statistics presented here are generated by Microsoft security programs and services running on computers in Nigeria in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Nigeria

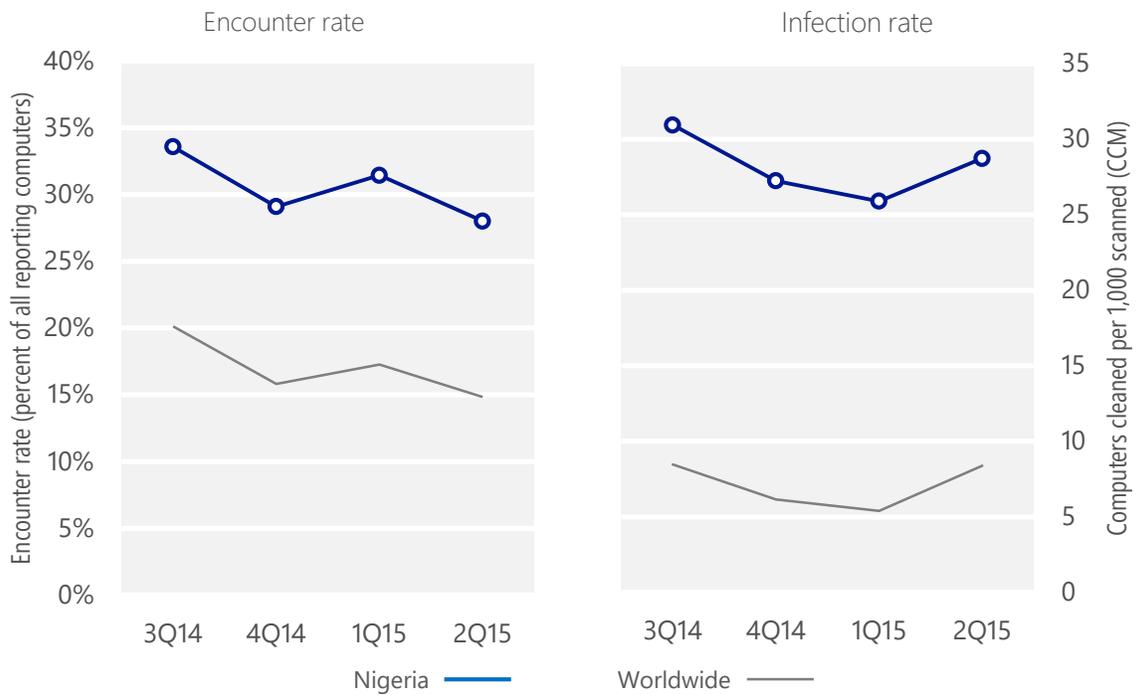
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Nigeria	33.6%	29.1%	31.4%	28.0%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Nigeria	30.9	27.2	25.9	28.7
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcote, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 28.0% of computers in Nigeria encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 28.7 of every 1,000 unique computers scanned in Nigeria in 2Q15 (a CCM score of 28.7, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Nigeria over the last four quarters, compared to the world as a whole.

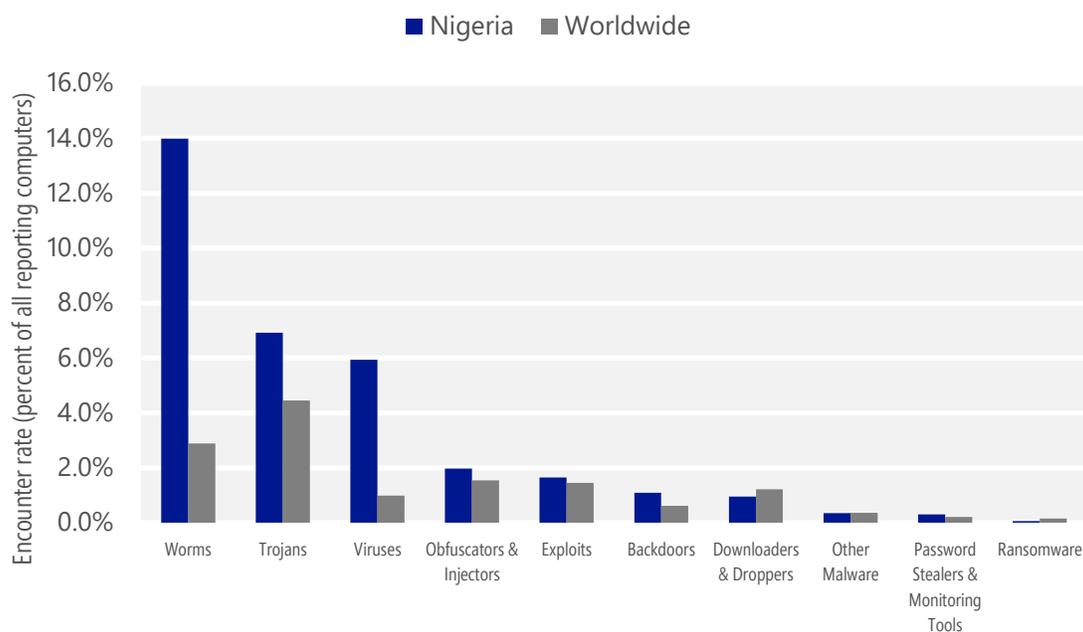
Malware encounter and infection rate trends in Nigeria and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in Nigeria and around the world, and for explanations of the methods and terms used here.

Malware categories

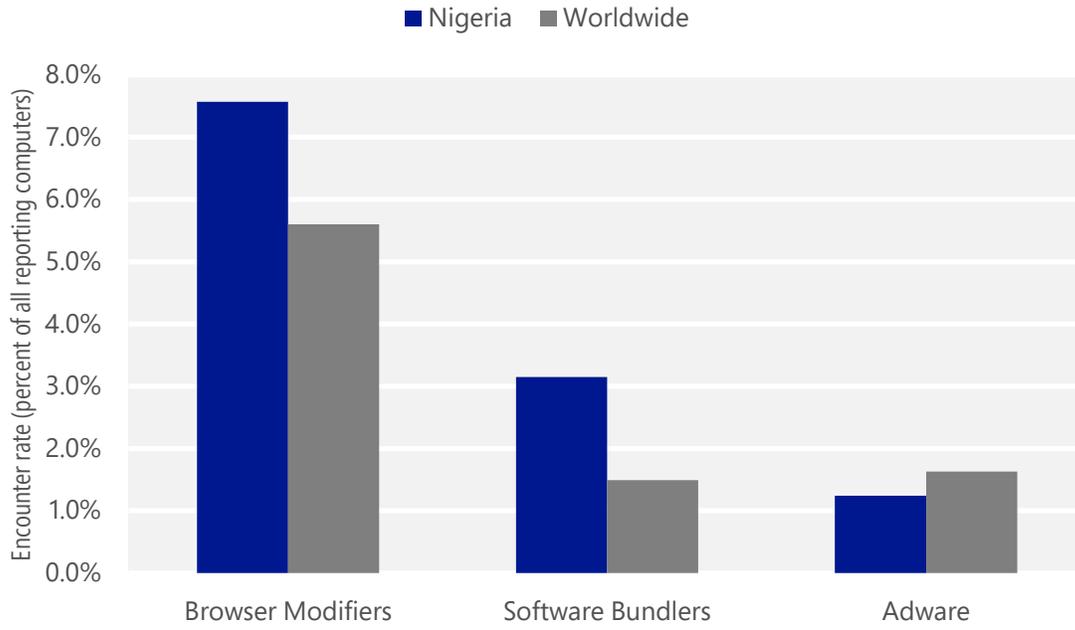
Malware encountered in Nigeria in 2Q15, by category



- The most common malware category in Nigeria in 2Q15 was Worms. It was encountered by 14.0 percent of all computers there, down from 15.3 percent in 1Q15.
- The second most common malware category in Nigeria in 2Q15 was Trojans. It was encountered by 6.9 percent of all computers there, up from 6.9 percent in 1Q15.
- The third most common malware category in Nigeria in 2Q15 was Viruses, which was encountered by 5.9 percent of all computers there, up from 5.1 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Nigeria in 2Q15, by category



- The most common unwanted software category in Nigeria in 2Q15 was Browser Modifiers. It was encountered by 7.6 percent of all computers there, down from 11.1 percent in 1Q15.
- The second most common unwanted software category in Nigeria in 2Q15 was Software Bundlers. It was encountered by 3.1 percent of all computers there, down from 3.6 percent in 1Q15.
- The third most common unwanted software category in Nigeria in 2Q15 was Adware, which was encountered by 1.2 percent of all computers there, up from 1.0 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Nigeria in 2Q15

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	4.6%
2	Win32/Gamarue	Worms	4.6%
3	Win32/Grenam	Viruses	4.3%
4	Win32/Ippedo	Worms	3.9%
5	Win32/Copali	Worms	2.7%
6	INF/Autorun	Obfuscators & Injectors	2.0%
7	Win32/Virut	Viruses	1.4%
8	MSIL/Mofin	Worms	1.1%
9	Win32/Ramnit	Trojans	1.1%
10	Win32/Sality	Viruses	1.0%

- The most common malware family encountered in Nigeria in 2Q15 was [VBS/Jenxcus](#), which was encountered by 4.6 percent of reporting computers there. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common malware family encountered in Nigeria in 2Q15 was [Win32/Gamarue](#), which was encountered by 4.6 percent of reporting computers there. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The third most common malware family encountered in Nigeria in 2Q15 was [Win32/Grenam](#), which was encountered by 4.3 percent of reporting computers there. [Win32/Grenam](#) is a multi-component family that includes a trojan component that runs at startup, a worm component that spreads via removable drives, and a virus component that renames executables.
- The fourth most common malware family encountered in Nigeria in 2Q15 was [Win32/Ippedo](#), which was encountered by 3.9 percent of reporting computers there. [Win32/Ippedo](#) is a worm that can send sensitive information to a malicious hacker. It spreads through removable drives, such as USB flash drives.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Nigeria in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/KipodToolsCby	Browser Modifiers	4.5%
2	Win32/CouponRuc	Browser Modifiers	3.0%
3	Win32/InstalleRex	Software Bundlers	3.0%
4	Win32/SaverExtension	Adware	0.9%
5	Win32/AlterbookSP	Browser Modifiers	0.3%

- The most common unwanted software family encountered in Nigeria in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 4.5 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common unwanted software family encountered in Nigeria in 2Q15 was [Win32/CouponRuc](#), which was encountered by 3.0 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The third most common unwanted software family encountered in Nigeria in 2Q15 was [Win32/InstalleRex](#), which was encountered by 3.0 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Nigeria in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	9.6
2	Win32/Gamarue	Worms	9.3
3	Win32/leEnablerCby	Browser Modifiers	2.7
4	Win32/Virut	Viruses	1.7
5	Win32/Sality	Viruses	1.6
6	Win32/Ramnit	Trojans	1.6
7	Win32/Chir	Viruses	1.0
8	Win32/Kilim	Trojans	0.9
9	Win32/CompromisedCert	Other Malware	0.7
10	Win32/Vobfus	Worms	0.6

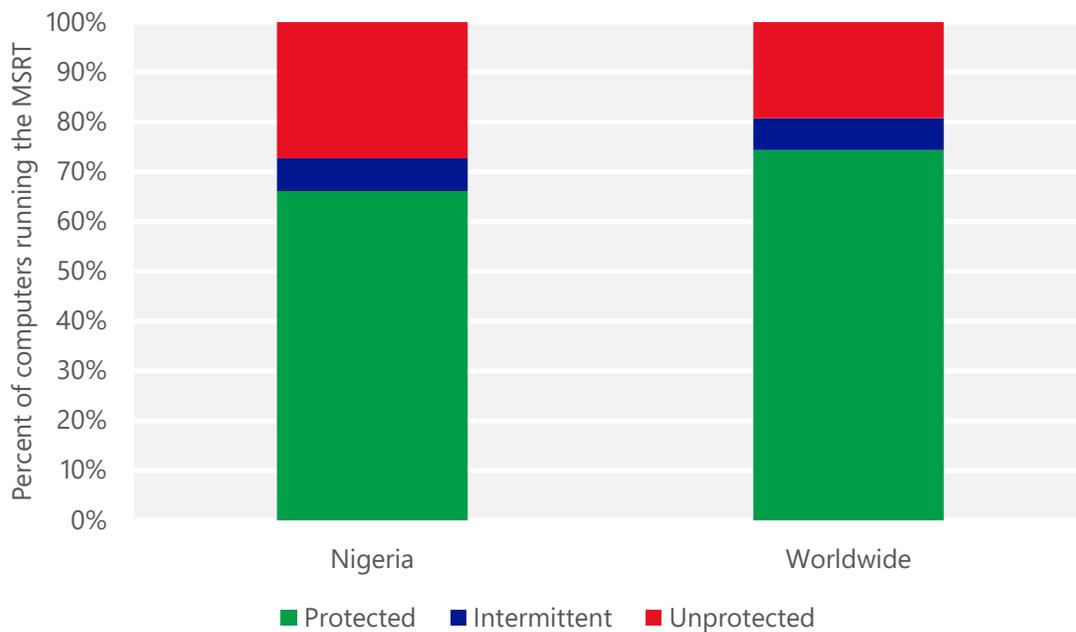
- The most common threat family infecting computers in Nigeria in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 9.6 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Nigeria in 2Q15 was [Win32/Gamarue](#), which was detected and removed from 9.3 of every 1,000 unique computers scanned by the MSRT. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The third most common threat family infecting computers in Nigeria in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 2.7 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The fourth most common threat family infecting computers in Nigeria in 2Q15 was [Win32/Virut](#), which was detected and removed from 1.7 of every 1,000 unique computers scanned by the MSRT. [Win32/Virut](#) is a family of file-infecting viruses that target and infect .exe and .scr files accessed on infected systems. Win32/Virut also opens a backdoor by connecting to an IRC server.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Nigeria and worldwide protected by real-time security software in 2Q15



Norway

The statistics presented here are generated by Microsoft security programs and services running on computers in Norway in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille, or CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Norway

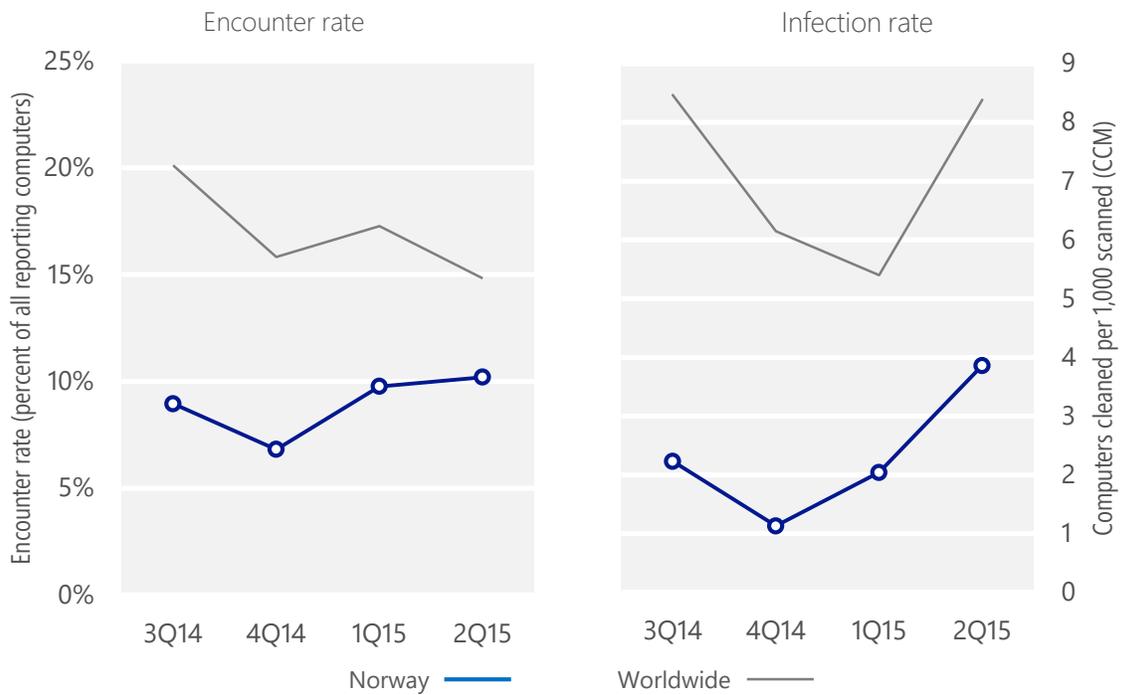
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Norway	9.0%	6.8%	9.8%	10.2%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Norway	2.2	1.1	2.0	3.9
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcoute, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 10.2% of computers in Norway encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 3.9 of every 1,000 unique computers scanned in Norway in 2Q15 (a CCM score of 3.9, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Norway over the last four quarters, compared to the world as a whole.

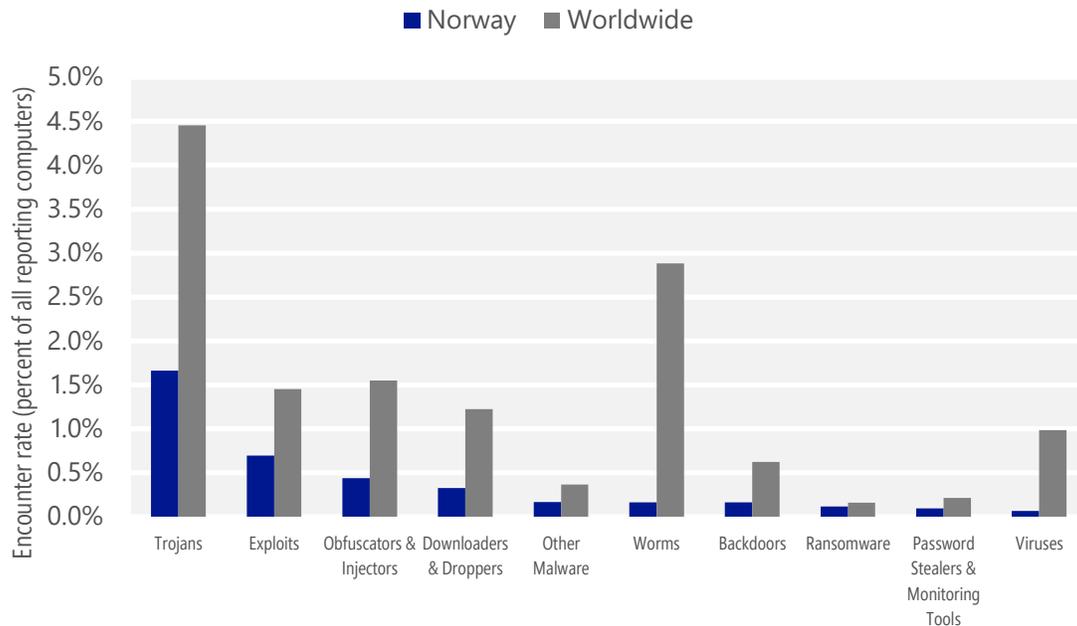
Malware encounter and infection rate trends in Norway and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in Norway and around the world, and for explanations of the methods and terms used here.

Malware categories

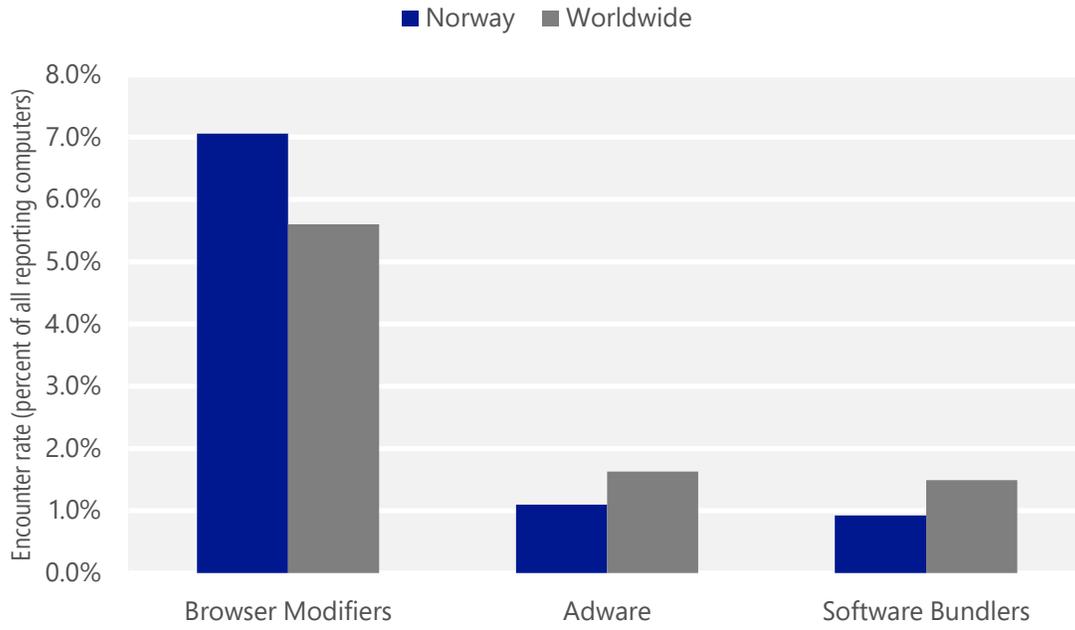
Malware encountered in Norway in 2Q15, by category



- The most common malware category in Norway in 2Q15 was Trojans. It was encountered by 1.7 percent of all computers there, up from 1.2 percent in 1Q15.
- The second most common malware category in Norway in 2Q15 was Exploits. It was encountered by 0.7 percent of all computers there, down from 1.1 percent in 1Q15.
- The third most common malware category in Norway in 2Q15 was Obfuscators & Injectors, which was encountered by 0.4 percent of all computers there, down from 0.6 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Norway in 2Q15, by category



- The most common unwanted software category in Norway in 2Q15 was Browser Modifiers. It was encountered by 7.1 percent of all computers there, up from 4.9 percent in 1Q15.
- The second most common unwanted software category in Norway in 2Q15 was Adware. It was encountered by 1.1 percent of all computers there, down from 3.3 percent in 1Q15.
- The third most common unwanted software category in Norway in 2Q15 was Software Bundlers, which was encountered by 0.9 percent of all computers there, up from 0.3 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Norway in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Kilim	Trojans	0.5%
2	Win32/Skeeyah	Trojans	0.4%
3	Win32/Obfuscator	Obfuscators & Injectors	0.4%
4	JS/Axpergle	Exploits	0.4%
5	Win32/Peals	Trojans	0.2%
6	Win32/Sdbby	Exploits	0.1%
7	Win32/Crowti	Ransomware	0.1%
8	Win32/Dynamer	Trojans	0.1%
9	ASX/Wimad	Downloaders & Droppers	0.1%
10	Win32/Dalexis	Downloaders & Droppers	0.1%

- The most common malware family encountered in Norway in 2Q15 was [Win32/Kilim](#), which was encountered by 0.5 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The second most common malware family encountered in Norway in 2Q15 was [Win32/Skeeyah](#), which was encountered by 0.4 percent of reporting computers there. [Win32/Skeeyah](#) is a generic detection for various threats that display trojan characteristics.
- The third most common malware family encountered in Norway in 2Q15 was [Win32/Obfuscator](#), which was encountered by 0.4 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The fourth most common malware family encountered in Norway in 2Q15 was [JS/Axpergle](#), which was encountered by 0.4 percent of reporting computers there. [JS/Axpergle](#) is a detection for the Angler exploit kit, which exploits vulnerabilities in recent versions of Internet Explorer, Silverlight, Adobe Flash Player, and Java to install malware.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Norway in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/AlterbookSP	Browser Modifiers	3.1%
2	Win32/CouponRuc	Browser Modifiers	2.2%
3	Win32/KipodToolsCby	Browser Modifiers	1.7%
4	Win32/InstalleRex	Software Bundlers	0.9%
5	Win32/SaverExtension	Adware	0.8%

- The most common unwanted software family encountered in Norway in 2Q15 was [Win32/AlterbookSP](#), which was encountered by 3.1 percent of reporting computers there. [Win32/AlterbookSP](#) is a browser add-on that formerly displayed behaviors of unwanted software. Recent versions of the add-on no longer meet Microsoft detection criteria, and are no longer considered unwanted software.
- The second most common unwanted software family encountered in Norway in 2Q15 was [Win32/CouponRuc](#), which was encountered by 2.2 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The third most common unwanted software family encountered in Norway in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 1.7 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.

Top threat families by infection rate

The most common malware families by infection rate in Norway in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/CompromisedCert	Other Malware	1.6
2	Win32/Kilim	Trojans	0.8
3	Win32/leEnablerCby	Browser Modifiers	0.8
4	MSIL/Bladabindi	Backdoors	0.1
5	Win32/Alureon	Trojans	0.1
6	Win32/Simda	Trojans	0.1
7	Win32/Ramnit	Trojans	<0.1
8	Win32/Sality	Viruses	<0.1
9	VBS/Jenxcus	Worms	<0.1
10	Win32/Nitol	Other Malware	<0.1

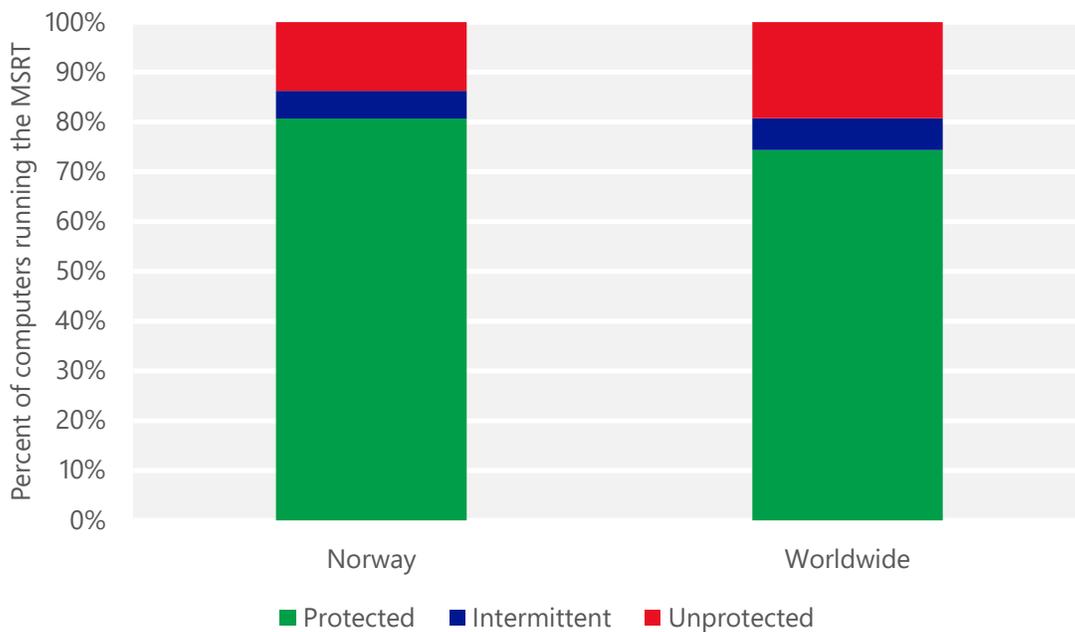
- The most common threat family infecting computers in Norway in 2Q15 was [Win32/CompromisedCert](#), which was detected and removed from 1.6 of every 1,000 unique computers scanned by the MSRT. [Win32/CompromisedCert](#) is a detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.
- The second most common threat family infecting computers in Norway in 2Q15 was [Win32/Kilim](#), which was detected and removed from 0.8 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The third most common threat family infecting computers in Norway in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 0.8 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The fourth most common threat family infecting computers in Norway in 2Q15 was [MSIL/Bladabindi](#), which was detected and removed from 0.1 of every 1,000 unique computers scanned by the MSRT. [MSIL/Bladabindi](#) is a family of backdoors created by a malicious hacker tool called NJ Rat. The can steal sensitive information, download other malware, and allow backdoor access to an infected computer.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Norway and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Norway

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.03 (0.28)	0.02 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	4.36 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	6.38 (16.7)	

Oman

The statistics presented here are generated by Microsoft security programs and services running on computers in Oman in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Oman

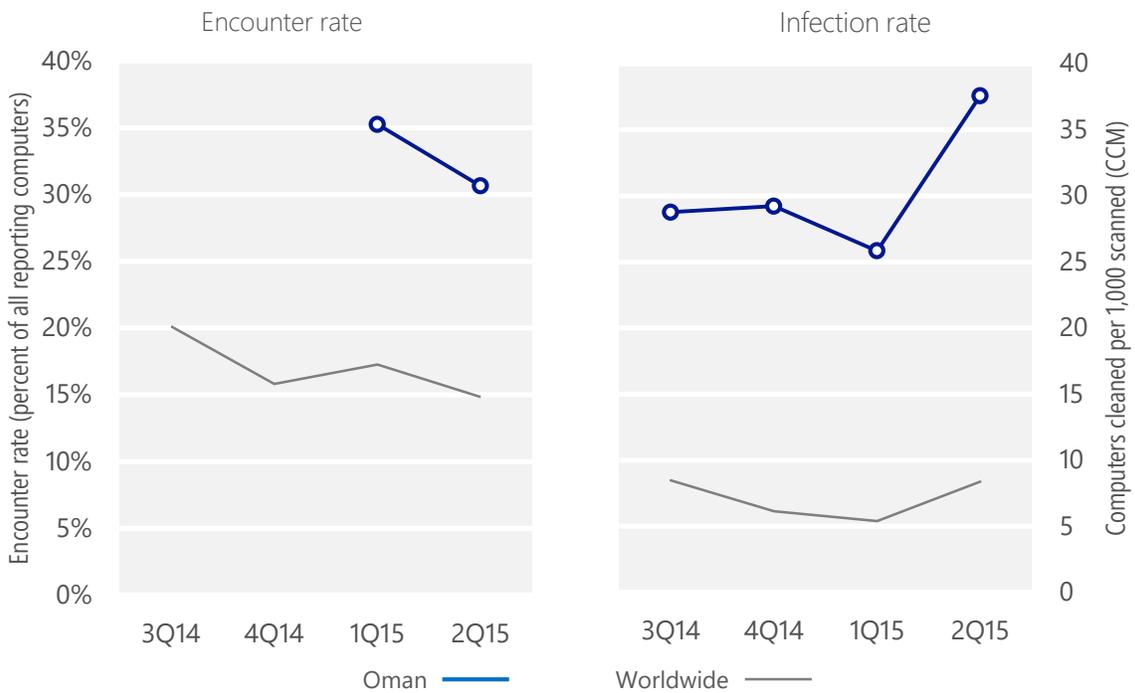
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Oman	N/A	N/A	35.3%	30.6%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Oman	28.8	29.2	25.8	37.6
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcote, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 30.6% of computers in Oman encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 37.6 of every 1,000 unique computers scanned in Oman in 2Q15 (a CCM score of 37.6, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Oman over the last four quarters, compared to the world as a whole.

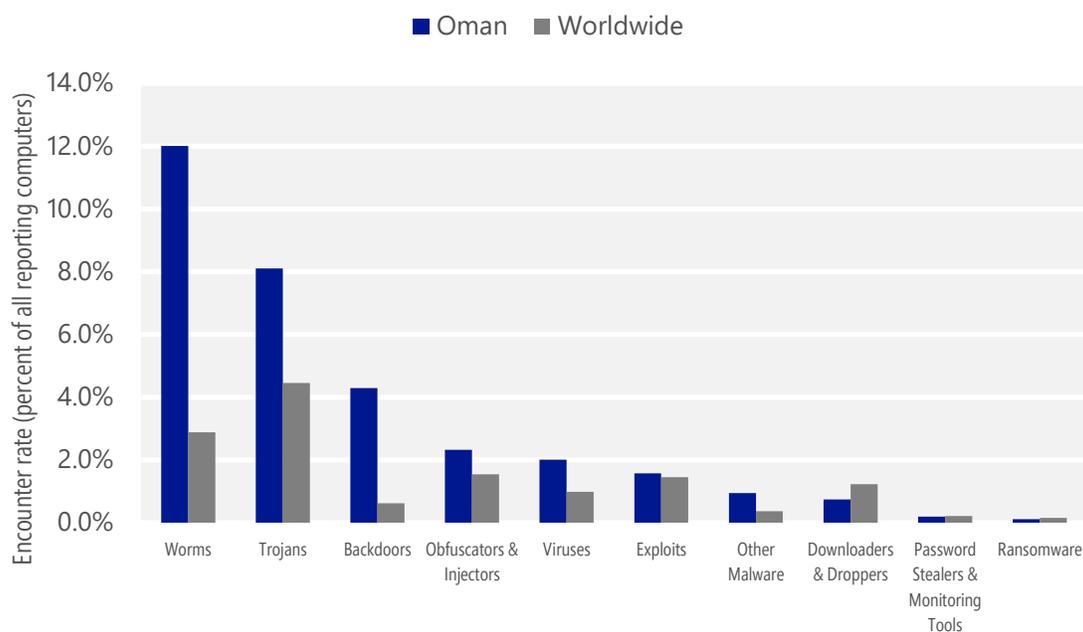
Malware encounter and infection rate trends in Oman and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in Oman and around the world, and for explanations of the methods and terms used here.

Malware categories

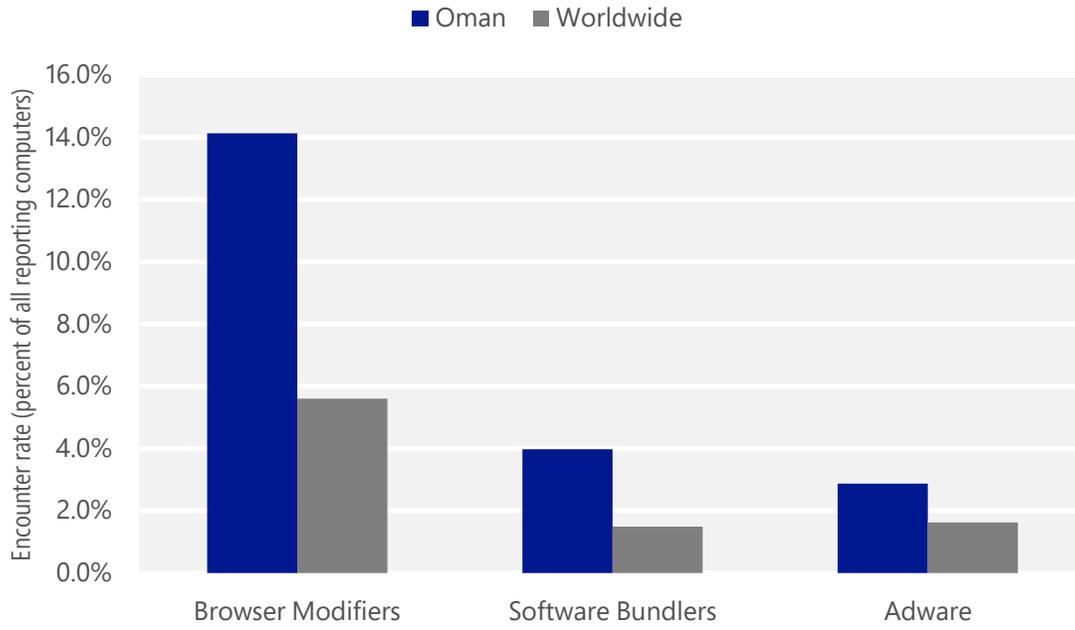
Malware encountered in Oman in 2Q15, by category



- The most common malware category in Oman in 2Q15 was Worms. It was encountered by 12.0 percent of all computers there, down from 12.7 percent in 1Q15.
- The second most common malware category in Oman in 2Q15 was Trojans. It was encountered by 8.1 percent of all computers there, up from 5.7 percent in 1Q15.
- The third most common malware category in Oman in 2Q15 was Backdoors, which was encountered by 4.3 percent of all computers there, up from 3.8 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Oman in 2Q15, by category



- The most common unwanted software category in Oman in 2Q15 was Browser Modifiers. It was encountered by 14.1 percent of all computers there, down from 19.8 percent in 1Q15.
- The second most common unwanted software category in Oman in 2Q15 was Software Bundlers. It was encountered by 4.0 percent of all computers there, down from 6.9 percent in 1Q15.
- The third most common unwanted software category in Oman in 2Q15 was Adware, which was encountered by 2.9 percent of all computers there, up from 1.8 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Oman in 2Q15

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	0.1%
2	Win32/Caphaw	Backdoors	<0.1%
3	Win32/Gamarue	Worms	<0.1%
4	INF/Autorun	Obfuscators & Injectors	<0.1%
5	Win32/Dorkbot	Worms	<0.1%
6	Win32/Kilim	Trojans	<0.1%
7	Win32/Skeeyah	Trojans	<0.1%
8	Win32/Vobfus	Worms	<0.1%
9	Win32/Peals	Trojans	<0.1%
10	Win32/Obfuscator	Obfuscators & Injectors	<0.1%

- The most common malware family encountered in Oman in 2Q15 was [VBS/Jenxcus](#), which was encountered by 0.1 percent of reporting computers there. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common malware family encountered in Oman in 2Q15 was [Win32/Caphaw](#), which was encountered by <0.1 percent of reporting computers there. [Win32/Caphaw](#) is a family of backdoors that spread via Facebook, YouTube, Skype, removable drives, and drive-by download. It can make Facebook posts via the user's account, and may steal online banking details.
- The third most common malware family encountered in Oman in 2Q15 was [Win32/Gamarue](#), which was encountered by <0.1 percent of reporting computers there. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The fourth most common malware family encountered in Oman in 2Q15 was [INF/Autorun](#), which was encountered by <0.1 percent of reporting computers there. [INF/Autorun](#) is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Oman in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/KipodToolsCby	Browser Modifiers	0.1%
2	Win32/CouponRuc	Browser Modifiers	0.1%
3	Win32/InstalleRex	Software Bundlers	<0.1%
4	Win32/SaverExtension	Adware	<0.1%
5	Win32/Vonteera	Browser Modifiers	<0.1%

- The most common unwanted software family encountered in Oman in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 0.1 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common unwanted software family encountered in Oman in 2Q15 was [Win32/CouponRuc](#), which was encountered by 0.1 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The third most common unwanted software family encountered in Oman in 2Q15 was [Win32/InstalleRex](#), which was encountered by <0.1 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Oman in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	10.7
2	Win32/leEnablerCby	Browser Modifiers	9.7
3	Win32/Gamarue	Worms	3.4
4	Win32/Dorkbot	Worms	3.1
5	Win32/CompromisedCert	Other Malware	2.7
6	Win32/Sality	Viruses	2.1
7	Win32/Kilim	Trojans	1.9
8	Win32/Vobfus	Worms	1.6
9	MSIL/Bladabindi	Backdoors	1.4
10	Win32/Ramnit	Trojans	1.2

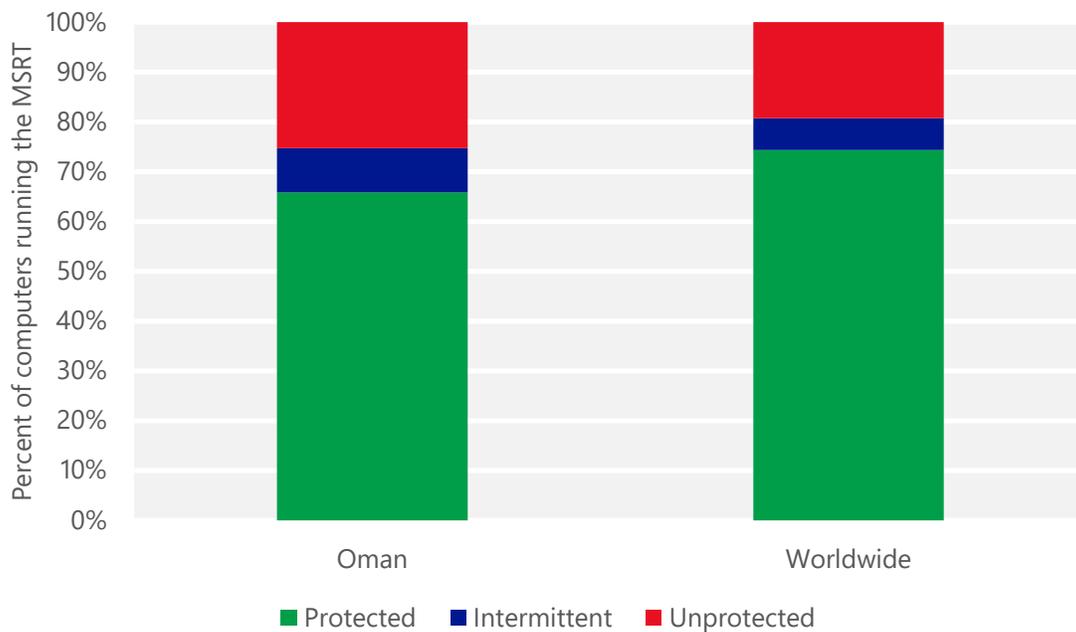
- The most common threat family infecting computers in Oman in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 10.7 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Oman in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 9.7 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common threat family infecting computers in Oman in 2Q15 was [Win32/Gamarue](#), which was detected and removed from 3.4 of every 1,000 unique computers scanned by the MSRT. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The fourth most common threat family infecting computers in Oman in 2Q15 was [Win32/Dorkbot](#), which was detected and removed from 3.1 of every 1,000 unique computers scanned by the MSRT. [Win32/Dorkbot](#) is a worm that spreads via instant messaging and removable drives. It also contains backdoor functionality that allows unauthorized access and control of the affected computer. Win32/Dorkbot may be distributed from compromised or malicious websites using PDF or browser exploits.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Oman and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Oman

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.01 (0.28)	0.00 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	1.88 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	9.80 (16.7)	

Pakistan

The statistics presented here are generated by Microsoft security programs and services running on computers in Pakistan in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Pakistan

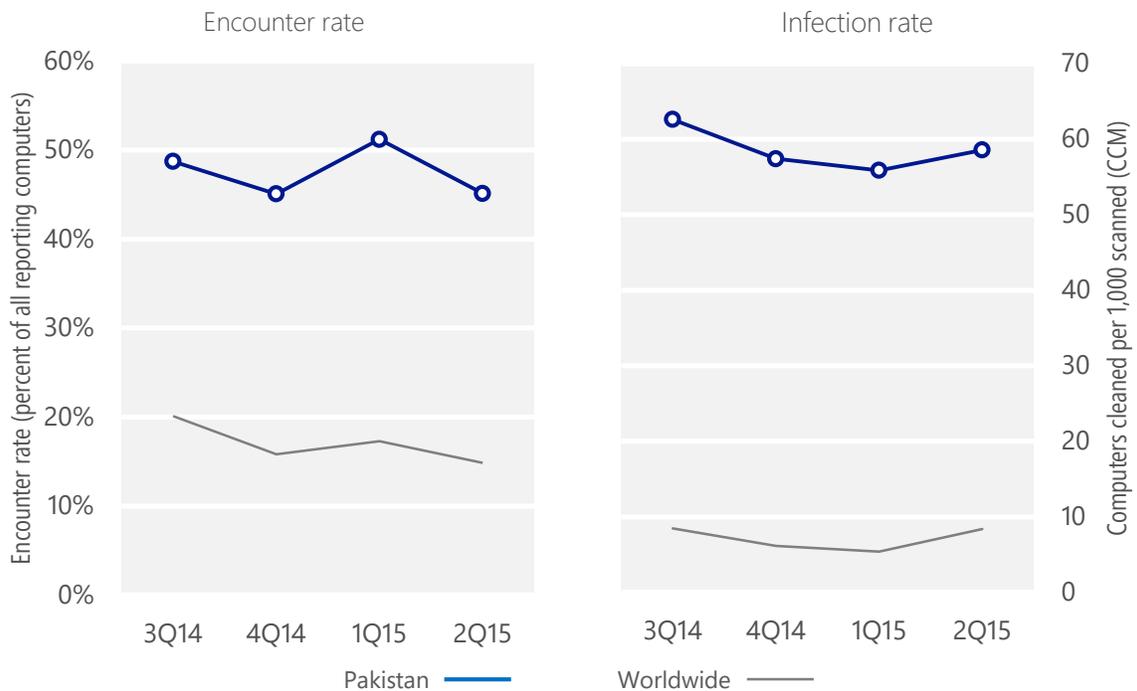
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Pakistan	48.7%	45.1%	51.2%	45.1%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Pakistan	62.6	57.4	55.9	58.6
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcote, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 45.1% of computers in Pakistan encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 58.6 of every 1,000 unique computers scanned in Pakistan in 2Q15 (a CCM score of 58.6, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Pakistan over the last four quarters, compared to the world as a whole.

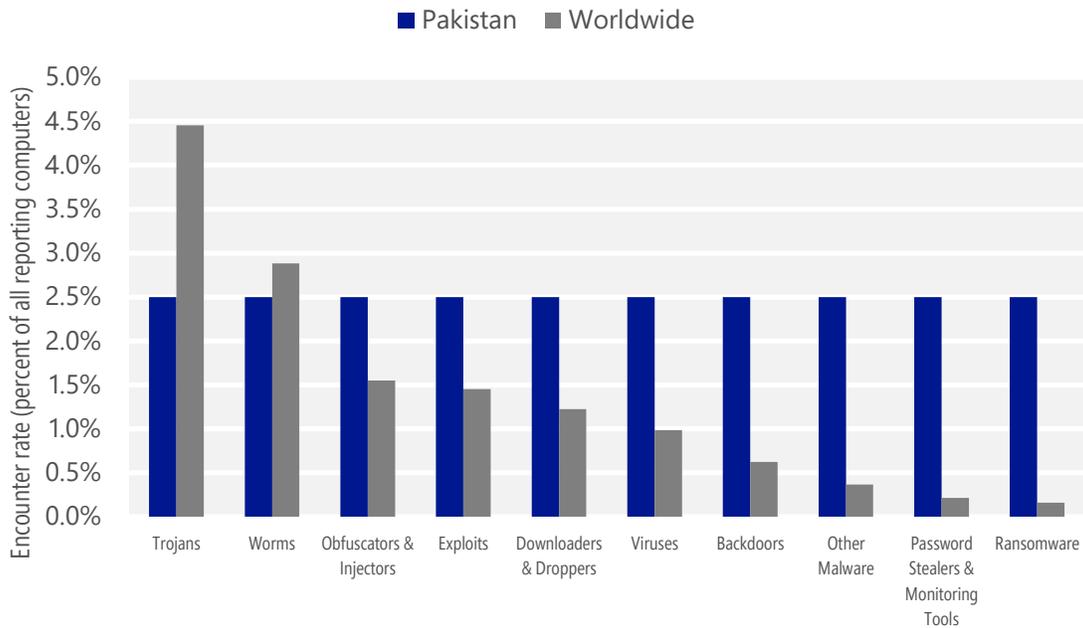
Malware encounter and infection rate trends in Pakistan and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in Pakistan and around the world, and for explanations of the methods and terms used here.

Malware categories

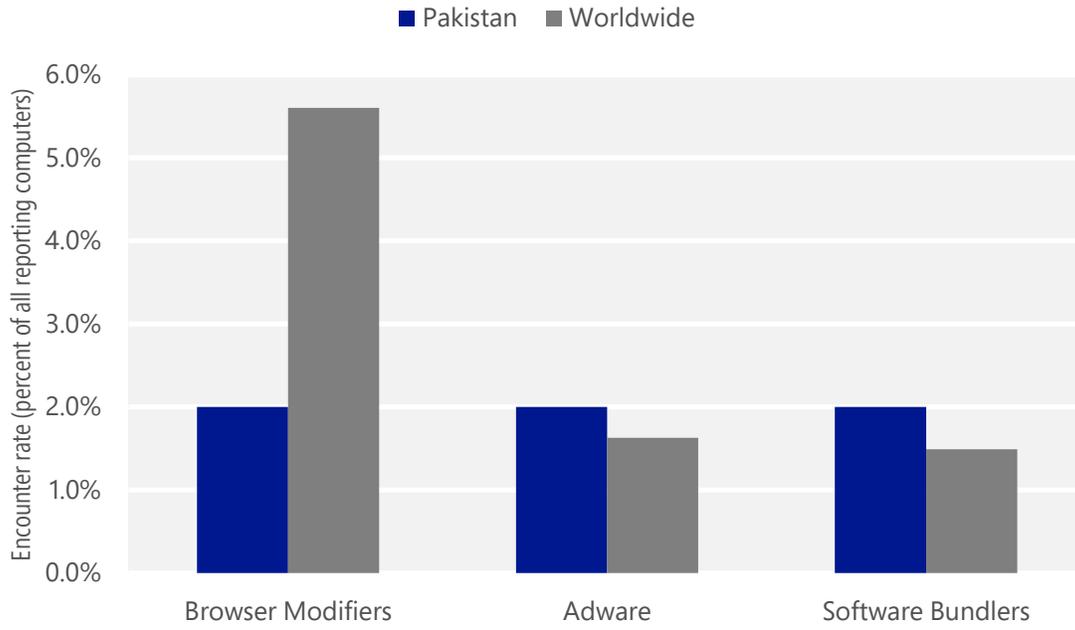
Malware encountered in Pakistan in 2Q15, by category



- The most common malware category in Pakistan in 2Q15 was . It was encountered by N/A percent of all computers there, down from 26.9 percent in 1Q15.
- The second most common malware category in Pakistan in 2Q15 was . It was encountered by N/A percent of all computers there, down from 14.3 percent in 1Q15.
- The third most common malware category in Pakistan in 2Q15 was , which was encountered by N/A percent of all computers there, down from 12.6 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Pakistan in 2Q15, by category



- The most common unwanted software category in Pakistan in 2Q15 was . It was encountered by N/A percent of all computers there, down from 20.8 percent in 1Q15.
- The second most common unwanted software category in Pakistan in 2Q15 was . It was encountered by N/A percent of all computers there, down from 10.3 percent in 1Q15.
- The third most common unwanted software category in Pakistan in 2Q15 was , which was encountered by N/A percent of all computers there, down from 2.2 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Pakistan in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Gamarue	Worms	9.9%
2	VBS/Jenxcus	Worms	7.9%
3	INF/Autorun	Obfuscators & Injectors	7.6%
4	Win32/Ippedo	Worms	6.0%
5	Win32/Sality	Viruses	5.4%
6	Win32/Virut	Viruses	4.4%
7	Win32/Nuqel	Worms	4.1%
8	Win32/Ramnit	Trojans	3.9%
9	Win32/CplLnk	Exploits	3.6%
10	Win32/Chir	Viruses	3.3%

- The most common malware family encountered in Pakistan in 2Q15 was [Win32/Gamarue](#), which was encountered by 9.9 percent of reporting computers there. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The second most common malware family encountered in Pakistan in 2Q15 was [VBS/Jenxcus](#), which was encountered by 7.9 percent of reporting computers there. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The third most common malware family encountered in Pakistan in 2Q15 was [INF/Autorun](#), which was encountered by 7.6 percent of reporting computers there. [INF/Autorun](#) is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The fourth most common malware family encountered in Pakistan in 2Q15 was [Win32/Ippedo](#), which was encountered by 6.0 percent of reporting computers there. [Win32/Ippedo](#) is a worm that can send sensitive information to a malicious hacker. It spreads through removable drives, such as USB flash drives.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Pakistan in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	10.0%
2	Win32/InstalleRex	Software Bundlers	6.1%
3	Win32/KipodToolsCby	Browser Modifiers	5.0%
4	Win32/SaverExtension	Adware	3.3%
5	Win32/AlterbookSP	Browser Modifiers	0.3%

- The most common unwanted software family encountered in Pakistan in 2Q15 was [Win32/CouponRuc](#), which was encountered by 10.0 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in Pakistan in 2Q15 was [Win32/InstalleRex](#), which was encountered by 6.1 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own “Installed On” date in Programs and Features to make it more difficult for a user to locate it and remove it.
- The third most common unwanted software family encountered in Pakistan in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 5.0 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user’s consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.

Top threat families by infection rate

The most common malware families by infection rate in Pakistan in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/Sality	Viruses	14.5
2	VBS/Jenxcus	Worms	12.5
3	Win32/Gamarue	Worms	10.4
4	Win32/Nuqel	Worms	7.1
5	Win32/Chir	Viruses	7.0
6	Win32/IeEnablerCby	Browser Modifiers	5.9
7	Win32/Ramnit	Trojans	4.1
8	Win32/Virut	Viruses	3.4
9	Win32/Kilim	Trojans	2.7
10	Win32/Tupym	Worms	2.0

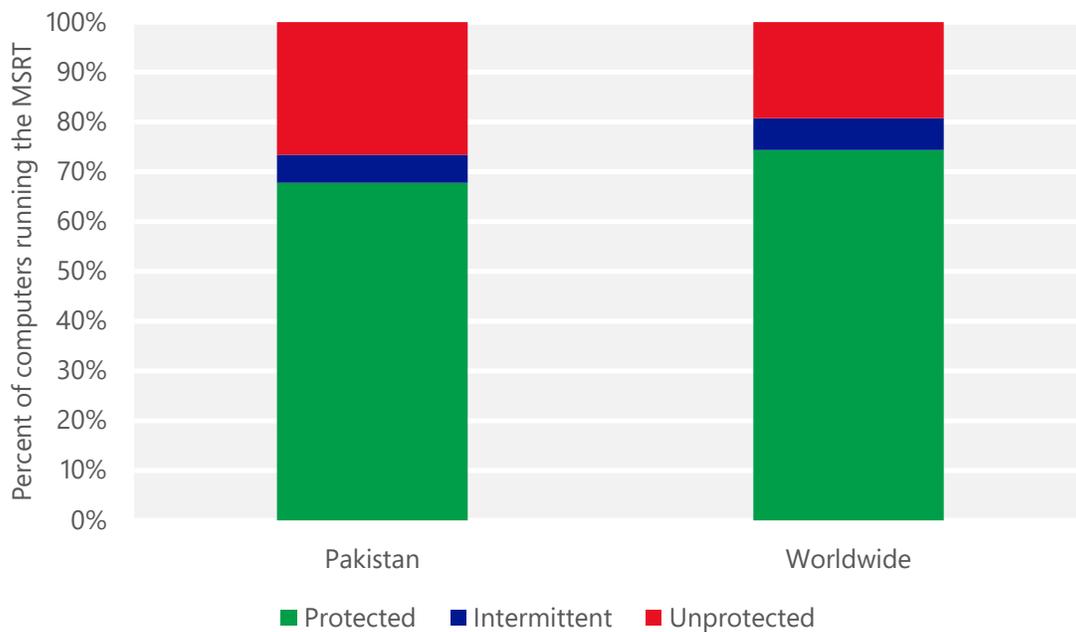
- The most common threat family infecting computers in Pakistan in 2Q15 was [Win32/Sality](#), which was detected and removed from 14.5 of every 1,000 unique computers scanned by the MSRT. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The second most common threat family infecting computers in Pakistan in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 12.5 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The third most common threat family infecting computers in Pakistan in 2Q15 was [Win32/Gamarue](#), which was detected and removed from 10.4 of every 1,000 unique computers scanned by the MSRT. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The fourth most common threat family infecting computers in Pakistan in 2Q15 was [Win32/Nuqel](#), which was detected and removed from 7.1 of every 1,000 unique computers scanned by the MSRT. [Win32/Nuqel](#) is a worm that spreads via mapped drives and certain instant messaging applications. It may modify system settings, connect to certain websites, download arbitrary files, or take other malicious actions.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Pakistan and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Pakistan

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.15 (0.28)	0.14 (0.24)
Phishing sites per 1,000 hosts (Worldwide)		2.53 (5.0)
Malware hosting sites per 1,000 hosts (Worldwide)		6.27 (16.7)

Palestinian Authority

The statistics presented here are generated by Microsoft security programs and services running on computers in the Palestinian territories (West Bank and Gaza Strip) in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for the Palestinian territories

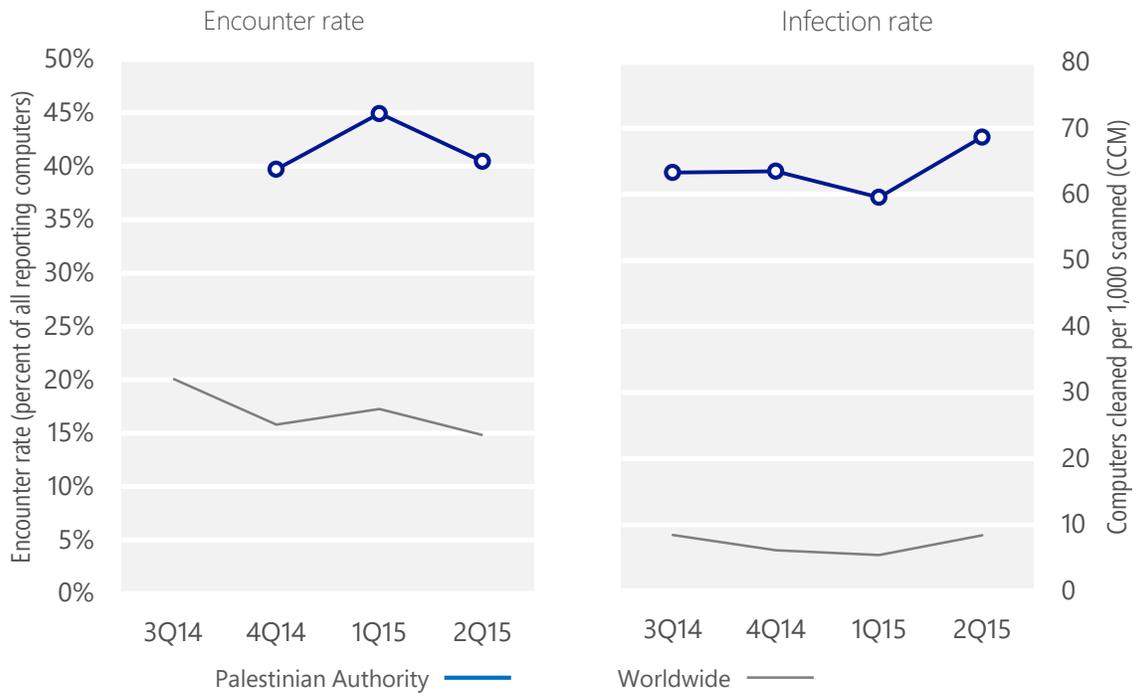
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Palestinian Authority	N/A	39.7%	44.9%	40.5%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Palestinian Authority	63.3	63.5	59.5	68.7
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcote, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 40.5% of computers in the Palestinian territories encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 68.7 of every 1,000 unique computers scanned in the Palestinian territories in 2Q15 (a CCM score of 68.7, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for the Palestinian territories over the last four quarters, compared to the world as a whole.

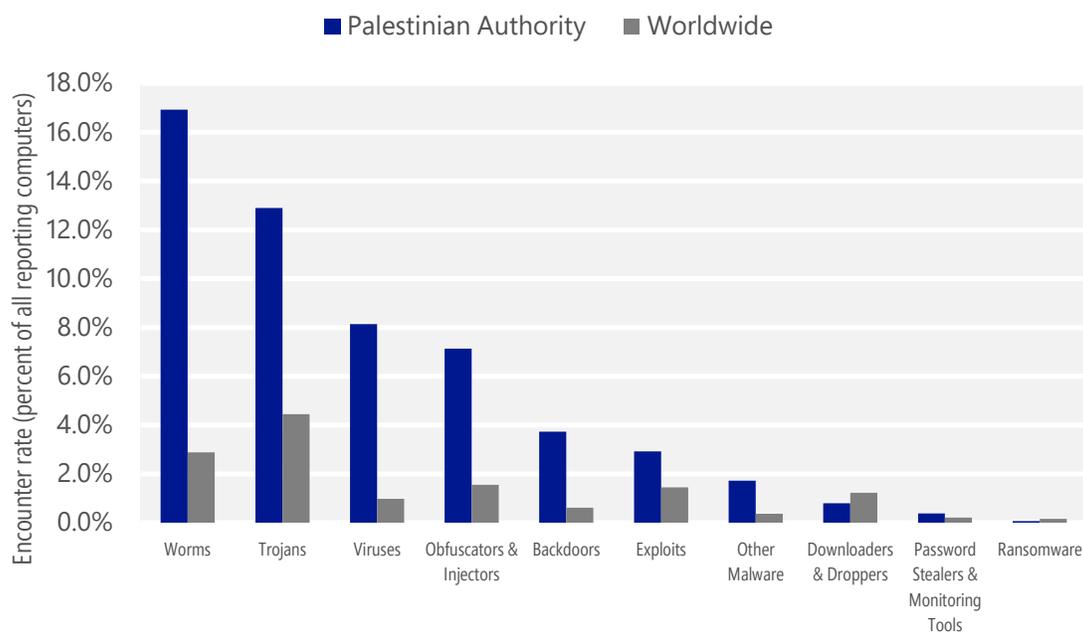
Malware encounter and infection rate trends in the Palestinian territories and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in the Palestinian territories and around the world, and for explanations of the methods and terms used here.

Malware categories

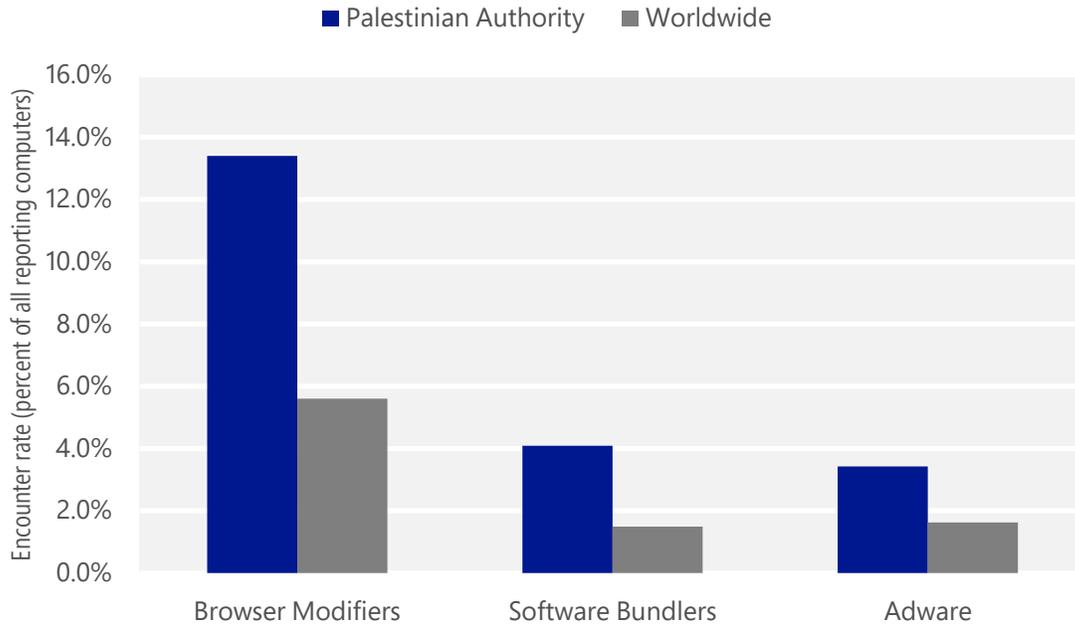
Malware encountered in the Palestinian territories in 2Q15, by category



- The most common malware category in the Palestinian territories in 2Q15 was Worms. It was encountered by 16.9 percent of all computers there, down from 17.7 percent in 1Q15.
- The second most common malware category in the Palestinian territories in 2Q15 was Trojans. It was encountered by 12.9 percent of all computers there, up from 11.8 percent in 1Q15.
- The third most common malware category in the Palestinian territories in 2Q15 was Viruses, which was encountered by 8.1 percent of all computers there, down from 8.9 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in the Palestinian territories in 2Q15, by category



- The most common unwanted software category in the Palestinian territories in 2Q15 was Browser Modifiers. It was encountered by 13.4 percent of all computers there, down from 19.1 percent in 1Q15.
- The second most common unwanted software category in the Palestinian territories in 2Q15 was Software Bundlers. It was encountered by 4.1 percent of all computers there, down from 7.2 percent in 1Q15.
- The third most common unwanted software category in the Palestinian territories in 2Q15 was Adware, which was encountered by 3.4 percent of all computers there, up from 2.1 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in the Palestinian territories in 2Q15

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	9.0%
2	Win32/Gamarue	Worms	5.0%
3	Win32/Sality	Viruses	4.8%
4	INF/Autorun	Obfuscators & Injectors	4.8%
5	Win32/Obfuscator	Obfuscators & Injectors	3.6%
6	Win32/Virut	Viruses	2.8%
7	Win32/Sulunch	Trojans	2.5%
8	MSIL/Bladabindi	Backdoors	2.5%
9	Win32/CplLnk	Exploits	2.0%
10	Win32/Ramnit	Trojans	1.9%

- The most common malware family encountered in the Palestinian territories in 2Q15 was [VBS/Jenxcus](#), which was encountered by 9.0 percent of reporting computers there. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common malware family encountered in the Palestinian territories in 2Q15 was [Win32/Gamarue](#), which was encountered by 5.0 percent of reporting computers there. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The third most common malware family encountered in the Palestinian territories in 2Q15 was [Win32/Sality](#), which was encountered by 4.8 percent of reporting computers there. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The fourth most common malware family encountered in the Palestinian territories in 2Q15 was [INF/Autorun](#), which was encountered by 4.8 percent of reporting computers there. [INF/Autorun](#) is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in the Palestinian territories in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/KipodToolsCby	Browser Modifiers	7.4%
2	Win32/CouponRuc	Browser Modifiers	6.6%
3	Win32/InstalleRex	Software Bundlers	3.9%
4	Win32/SaverExtension	Adware	2.5%
5	Win32/AlterbookSP	Browser Modifiers	0.5%

- The most common unwanted software family encountered in the Palestinian territories in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 7.4 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common unwanted software family encountered in the Palestinian territories in 2Q15 was [Win32/CouponRuc](#), which was encountered by 6.6 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The third most common unwanted software family encountered in the Palestinian territories in 2Q15 was [Win32/InstalleRex](#), which was encountered by 3.9 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in the Palestinian territories in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/Sality	Viruses	19.4
2	VBS/Jenxcus	Worms	18.5
3	Win32/Gamarue	Worms	8.6
4	Win32/leEnablerCby	Browser Modifiers	7.2
5	MSIL/Bladabindi	Backdoors	5.3
6	Win32/Virut	Viruses	4.9
7	Win32/Ramnit	Trojans	3.8
8	Win32/Nuqel	Worms	3.2
9	Win32/Nitol	Other Malware	3.0
10	Win32/Kilim	Trojans	3.0

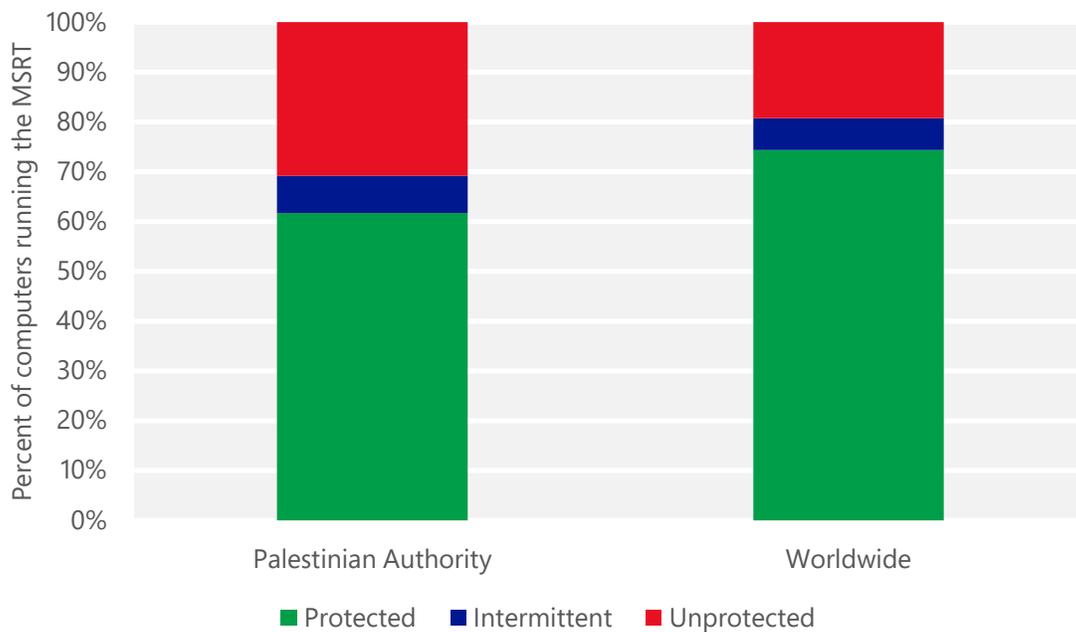
- The most common threat family infecting computers in the Palestinian territories in 2Q15 was [Win32/Sality](#), which was detected and removed from 19.4 of every 1,000 unique computers scanned by the MSRT. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The second most common threat family infecting computers in the Palestinian territories in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 18.5 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The third most common threat family infecting computers in the Palestinian territories in 2Q15 was [Win32/Gamarue](#), which was detected and removed from 8.6 of every 1,000 unique computers scanned by the MSRT. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The fourth most common threat family infecting computers in the Palestinian territories in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 7.2 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in the Palestinian territories and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for the Palestinian territories

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.10 (0.28)	0.11 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	5.38 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	4.30 (16.7)	

Panama

The statistics presented here are generated by Microsoft security programs and services running on computers in Panama in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Panama

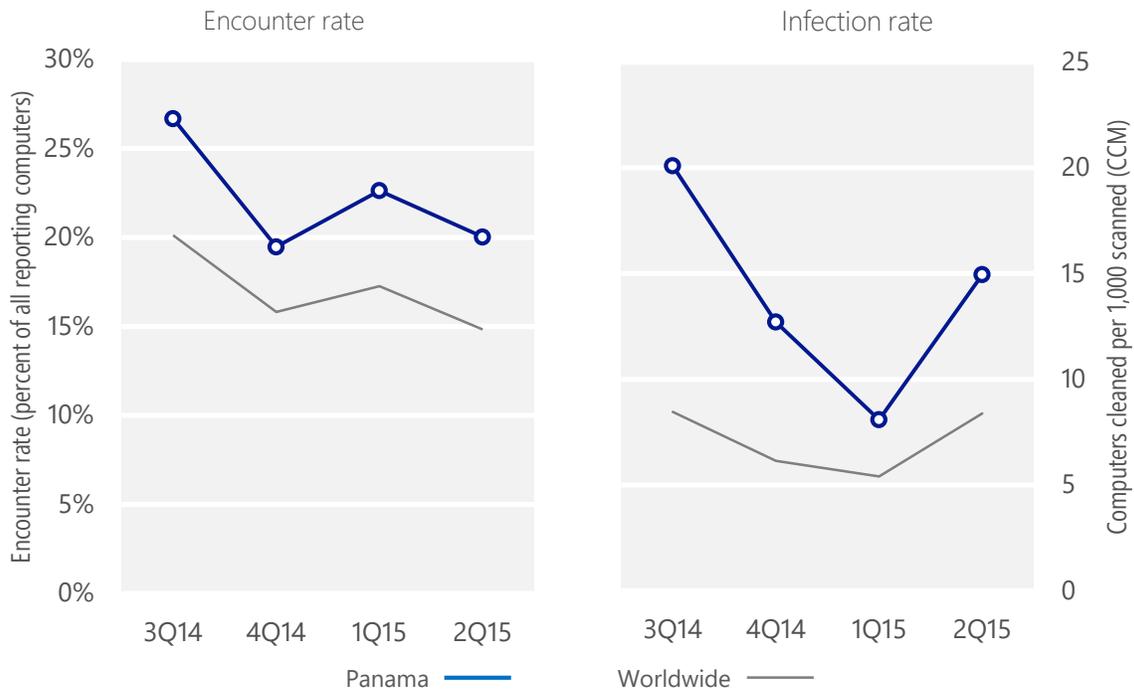
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Panama	26.7%	19.5%	22.6%	20.0%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Panama	20.1	12.7	8.1	15.0
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcoute, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 20.0% of computers in Panama encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 15.0 of every 1,000 unique computers scanned in Panama in 2Q15 (a CCM score of 15.0, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Panama over the last four quarters, compared to the world as a whole.

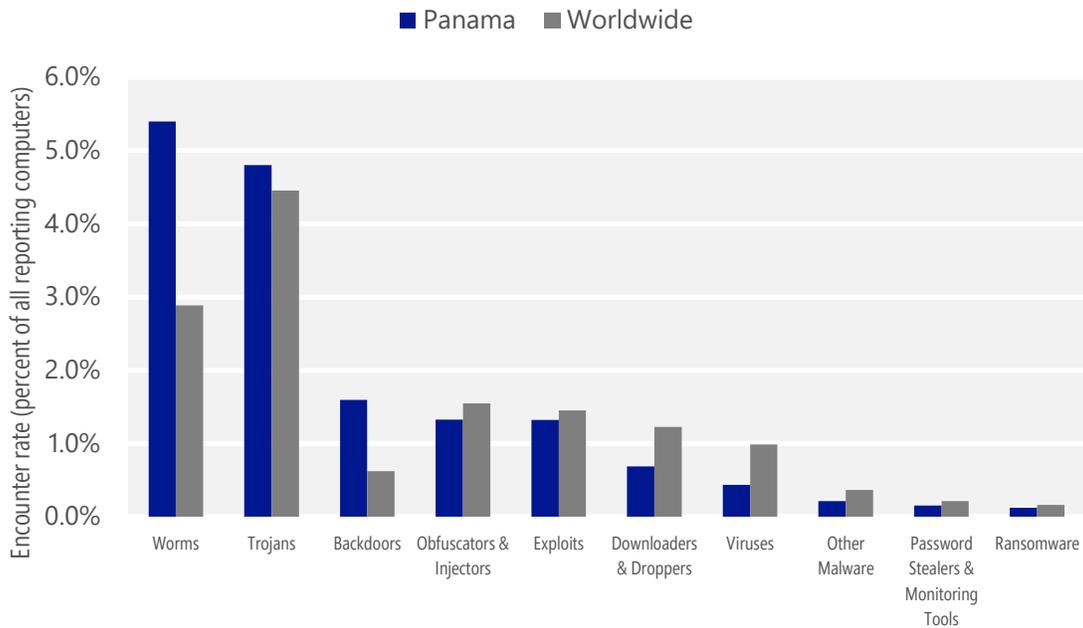
Malware encounter and infection rate trends in Panama and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in Panama and around the world, and for explanations of the methods and terms used here.

Malware categories

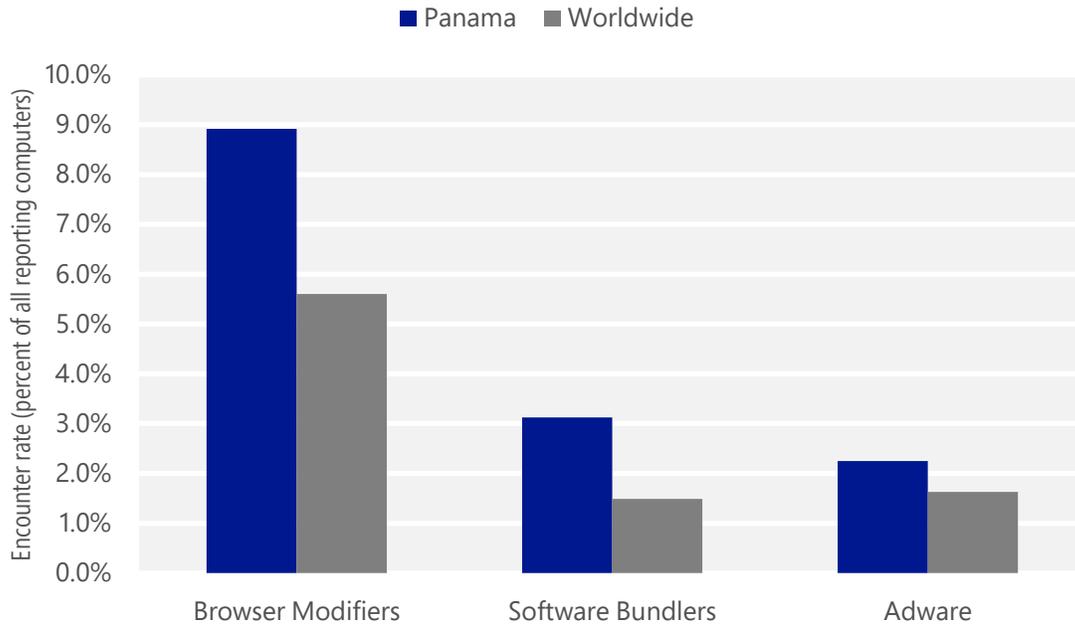
Malware encountered in Panama in 2Q15, by category



- The most common malware category in Panama in 2Q15 was Worms. It was encountered by 5.4 percent of all computers there, up from 5.2 percent in 1Q15.
- The second most common malware category in Panama in 2Q15 was Trojans. It was encountered by 4.8 percent of all computers there, up from 3.1 percent in 1Q15.
- The third most common malware category in Panama in 2Q15 was Backdoors, which was encountered by 1.6 percent of all computers there, up from 1.5 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Panama in 2Q15, by category



- The most common unwanted software category in Panama in 2Q15 was Browser Modifiers. It was encountered by 8.9 percent of all computers there, down from 13.0 percent in 1Q15.
- The second most common unwanted software category in Panama in 2Q15 was Software Bundlers. It was encountered by 3.1 percent of all computers there, down from 5.4 percent in 1Q15.
- The third most common unwanted software category in Panama in 2Q15 was Adware, which was encountered by 2.2 percent of all computers there, up from 0.7 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Panama in 2Q15

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	3.0%
2	Win32/Caphaw	Backdoors	1.2%
3	JS/Bondat	Worms	1.0%
4	Win32/Kilim	Trojans	1.0%
5	JS/Axpergle	Exploits	0.8%
6	Win32/Obfuscator	Obfuscators & Injectors	0.7%
7	Win32/Dorkbot	Worms	0.7%
8	Win32/Skeeyah	Trojans	0.6%
9	Win32/Dynamer	Trojans	0.5%
10	INF/Autorun	Obfuscators & Injectors	0.4%

- The most common malware family encountered in Panama in 2Q15 was [VBS/Jenxcus](#), which was encountered by 3.0 percent of reporting computers there. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common malware family encountered in Panama in 2Q15 was [Win32/Caphaw](#), which was encountered by 1.2 percent of reporting computers there. [Win32/Caphaw](#) is a family of backdoors that spread via Facebook, YouTube, Skype, removable drives, and drive-by download. It can make Facebook posts via the user's account, and may steal online banking details.
- The third most common malware family encountered in Panama in 2Q15 was [JS/Bondat](#), which was encountered by 1.0 percent of reporting computers there. [JS/Bondat](#) is a family of threats that collects information about the computer, infects removable drives, and tries to stop the user from accessing files. It spreads by infecting removable drives, such as USB thumb drives and flash drives.
- The fourth most common malware family encountered in Panama in 2Q15 was [Win32/Kilim](#), which was encountered by 1.0 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Panama in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	4.9%
2	Win32/KipodToolsCby	Browser Modifiers	3.4%
3	Win32/InstalleRex	Software Bundlers	3.0%
4	Win32/SaverExtension	Adware	1.7%
5	Win32/AlterbookSP	Browser Modifiers	0.4%

- The most common unwanted software family encountered in Panama in 2Q15 was [Win32/CouponRuc](#), which was encountered by 4.9 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in Panama in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 3.4 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common unwanted software family encountered in Panama in 2Q15 was [Win32/InstalleRex](#), which was encountered by 3.0 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Panama in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	5.7
2	VBS/Jenxcus	Worms	4.5
3	Win32/Kilim	Trojans	1.5
4	Win32/Dorkbot	Worms	0.8
5	Win32/Sality	Viruses	0.4
6	Win32/Lethic	Trojans	0.3
7	Win32/Dyzap	Password Stealers & Monitoring Tools	0.2
8	Win32/CompromisedCert	Other Malware	0.2
9	Win32/Vobfus	Worms	0.2
10	Win32/Brontok	Worms	0.2

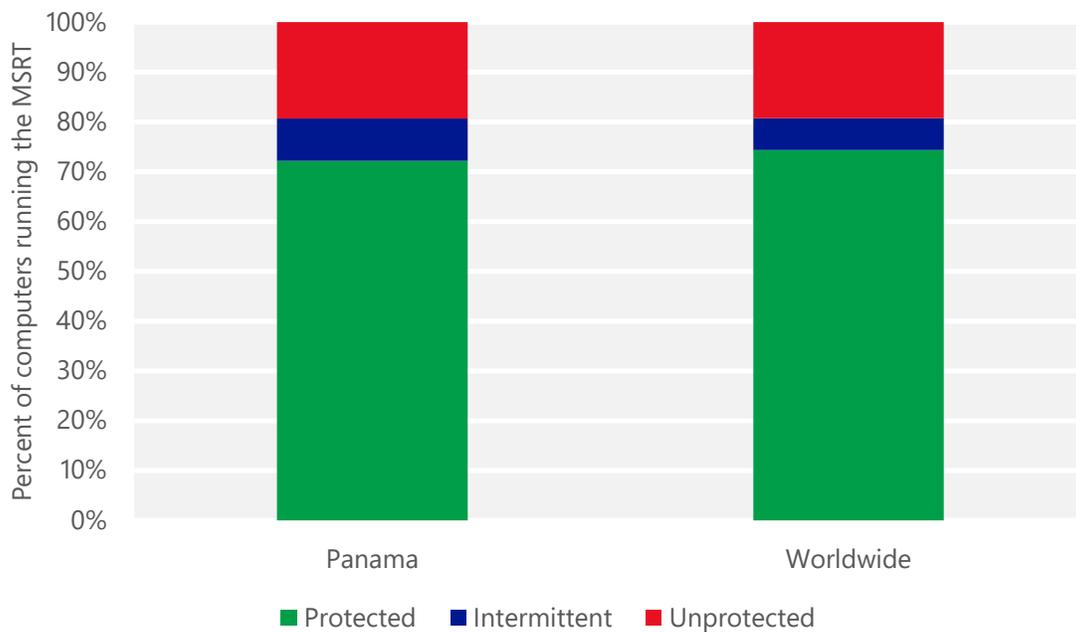
- The most common threat family infecting computers in Panama in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 5.7 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Panama in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 4.5 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The third most common threat family infecting computers in Panama in 2Q15 was [Win32/Kilim](#), which was detected and removed from 1.5 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The fourth most common threat family infecting computers in Panama in 2Q15 was [Win32/Dorkbot](#), which was detected and removed from 0.8 of every 1,000 unique computers scanned by the MSRT. [Win32/Dorkbot](#) is a worm that spreads via instant messaging and removable drives. It also contains backdoor functionality that allows unauthorized access and control of the affected computer. [Win32/Dorkbot](#) may be distributed from compromised or malicious websites using PDF or browser exploits.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Panama and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Panama

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	19.05 (0.28)	8.67 (0.24)
Phishing sites per 1,000 hosts (Worldwide)		8.65 (5.0)
Malware hosting sites per 1,000 hosts (Worldwide)		9.19 (16.7)

Paraguay

The statistics presented here are generated by Microsoft security programs and services running on computers in Paraguay in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Paraguay

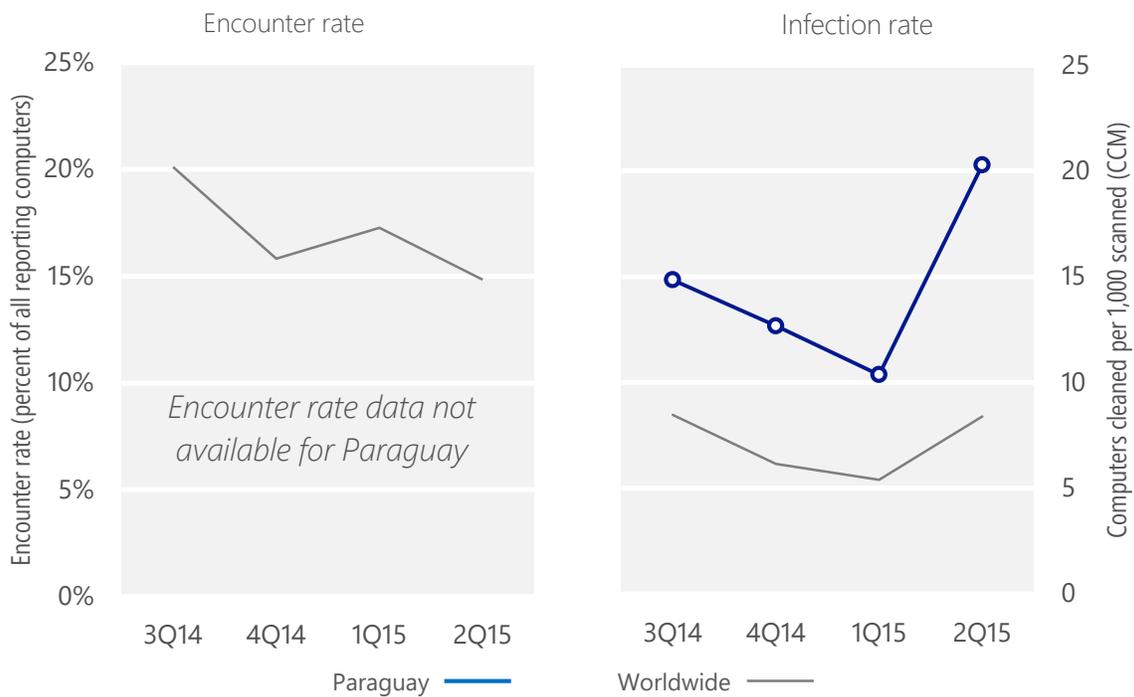
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Paraguay	N/A	N/A	N/A	N/A
<i>Worldwide encounter rate</i>	20.1%	15.8%	17.3%	14.8%
CCM, Paraguay	14.9	12.7	10.4	20.3
<i>Worldwide CCM</i>	8.5	6.1	5.4	8.4

Encounter and infection rates reported here do not include totals for the Brantall, Filcoute, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, the MSRT detected and removed malware from 20.3 of every 1,000 unique computers scanned in Paraguay in 2Q15 (a CCM score of 20.3, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Paraguay over the last four quarters, compared to the world as a whole.

Malware encounter and infection rate trends in Paraguay and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in Paraguay and around the world, and for explanations of the methods and terms used here.

Top threat families by infection rate

The most common malware families by infection rate in Paraguay in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	6.7
2	VBS/Jenxcus	Worms	6.3
3	Win32/Dorkbot	Worms	2.0
4	Win32/Kilim	Trojans	1.4
5	Win32/Sality	Viruses	1.0
6	Win32/Lethic	Trojans	0.7
7	Win32/Brontok	Worms	0.6
8	Win32/CompromisedCert	Other Malware	0.5
9	MSIL/Spacekito	Trojans	0.2
10	MSIL/Bladabindi	Backdoors	0.2

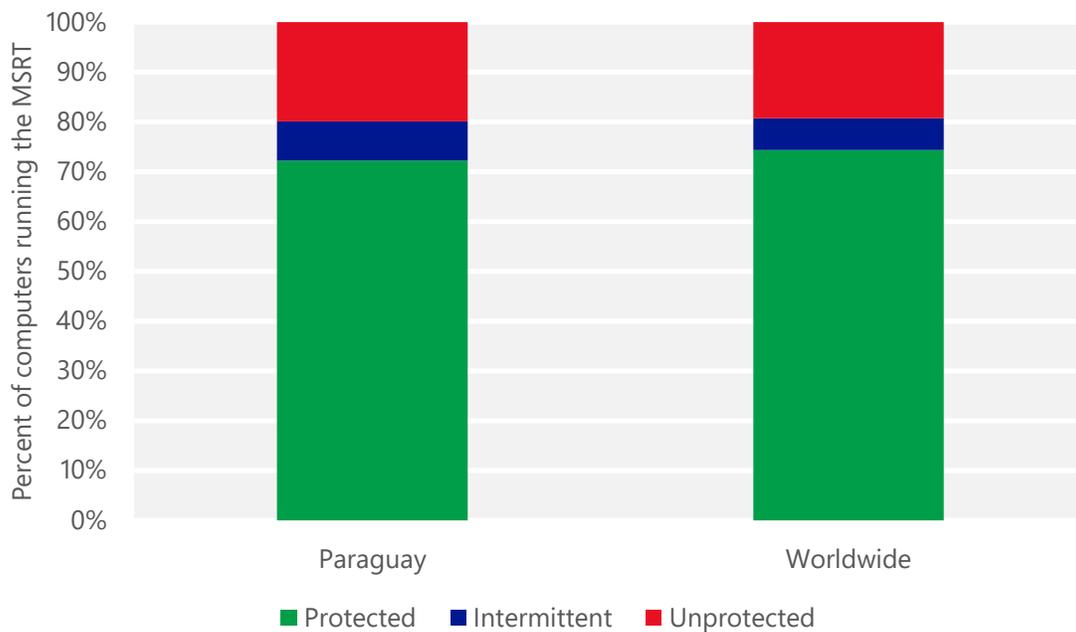
- The most common threat family infecting computers in Paraguay in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 6.7 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Paraguay in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 6.3 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The third most common threat family infecting computers in Paraguay in 2Q15 was [Win32/Dorkbot](#), which was detected and removed from 2.0 of every 1,000 unique computers scanned by the MSRT. [Win32/Dorkbot](#) is a worm that spreads via instant messaging and removable drives. It also contains backdoor functionality that allows unauthorized access and control of the affected computer. Win32/Dorkbot may be distributed from compromised or malicious websites using PDF or browser exploits.
- The fourth most common threat family infecting computers in Paraguay in 2Q15 was [Win32/Kilim](#), which was detected and removed from 1.4 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Paraguay and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Paraguay

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.00 (0.28)	0.00 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	4.90 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	6.54 (16.7)	

Peru

The statistics presented here are generated by Microsoft security programs and services running on computers in Peru in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Peru

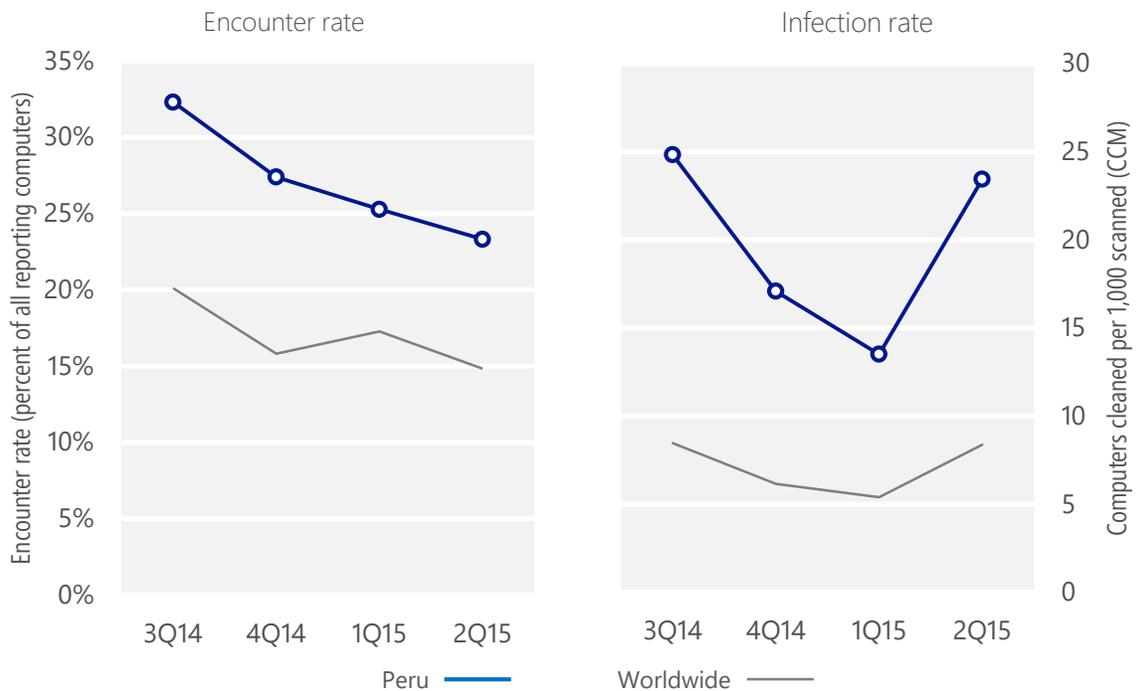
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Peru	32.3%	27.4%	25.3%	23.3%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Peru	24.8	17.1	13.5	23.4
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcout, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 23.3% of computers in Peru encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 23.4 of every 1,000 unique computers scanned in Peru in 2Q15 (a CCM score of 23.4, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Peru over the last four quarters, compared to the world as a whole.

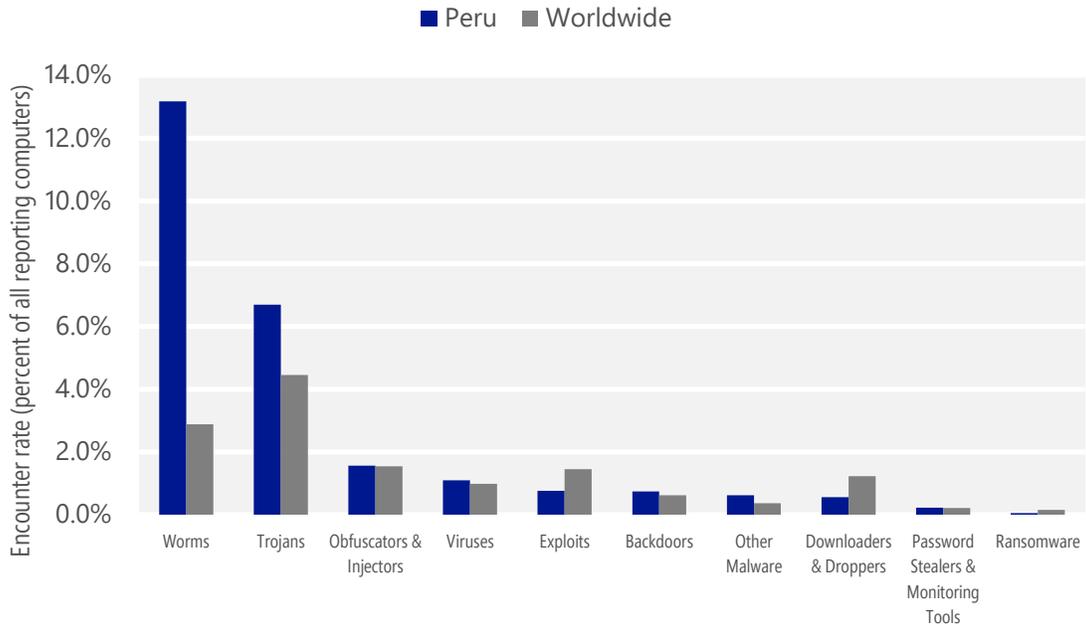
Malware encounter and infection rate trends in Peru and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in Peru and around the world, and for explanations of the methods and terms used here.

Malware categories

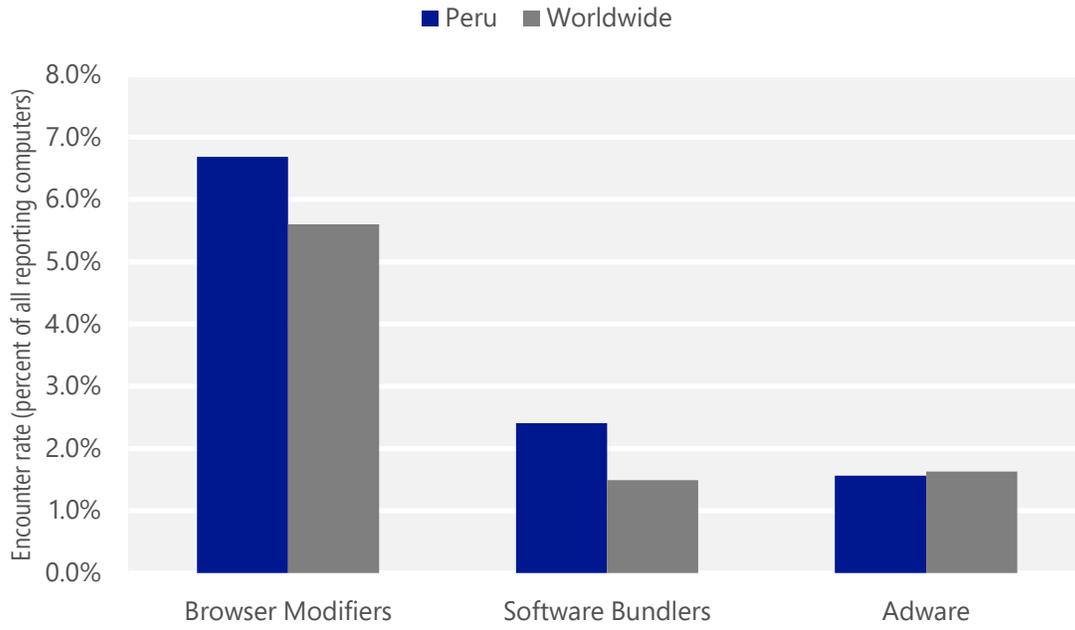
Malware encountered in Peru in 2Q15, by category



- The most common malware category in Peru in 2Q15 was Worms. It was encountered by 13.2 percent of all computers there, up from 12.5 percent in 1Q15.
- The second most common malware category in Peru in 2Q15 was Trojans. It was encountered by 6.7 percent of all computers there, up from 4.4 percent in 1Q15.
- The third most common malware category in Peru in 2Q15 was Obfuscators & Injectors, which was encountered by 1.6 percent of all computers there, down from 1.9 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Peru in 2Q15, by category



- The most common unwanted software category in Peru in 2Q15 was Browser Modifiers. It was encountered by 6.7 percent of all computers there, down from 9.8 percent in 1Q15.
- The second most common unwanted software category in Peru in 2Q15 was Software Bundlers. It was encountered by 2.4 percent of all computers there, down from 4.1 percent in 1Q15.
- The third most common unwanted software category in Peru in 2Q15 was Adware, which was encountered by 1.6 percent of all computers there, up from 0.5 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Peru in 2Q15

	Family	Most significant category	% of reporting computers
1	JS/Bondat	Worms	7.2%
2	Win32/Gamarue	Worms	4.2%
3	VBS/Jenxcus	Worms	2.5%
4	Win32/Nohad	Worms	1.4%
5	Win32/Kilim	Trojans	1.0%
6	Win32/Vobfus	Worms	0.9%
7	Win32/Obfuscator	Obfuscators & Injectors	0.9%
8	Win32/Skeeyah	Trojans	0.8%
9	Win32/Yeltminky	Worms	0.6%
10	Win32/Peals	Trojans	0.6%

- The most common malware family encountered in Peru in 2Q15 was [JS/Bondat](#), which was encountered by 7.2 percent of reporting computers there. [JS/Bondat](#) is a family of threats that collects information about the computer, infects removable drives, and tries to stop the user from accessing files. It spreads by infecting removable drives, such as USB thumb drives and flash drives.
- The second most common malware family encountered in Peru in 2Q15 was [Win32/Gamarue](#), which was encountered by 4.2 percent of reporting computers there. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The third most common malware family encountered in Peru in 2Q15 was [VBS/Jenxcus](#), which was encountered by 2.5 percent of reporting computers there. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The fourth most common malware family encountered in Peru in 2Q15 was [Win32/Nohad](#), which was encountered by 1.4 percent of reporting computers there. [Win32/Nohad](#) is a worm that spreads via removable drives, such as USB flash drives.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Peru in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	3.7%
2	Win32/KipodToolsCby	Browser Modifiers	2.4%
3	Win32/InstalleRex	Software Bundlers	2.3%
4	Win32/SaverExtension	Adware	1.2%
5	Win32/AlterbookSP	Browser Modifiers	0.5%

- The most common unwanted software family encountered in Peru in 2Q15 was [Win32/CouponRuc](#), which was encountered by 3.7 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in Peru in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 2.4 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common unwanted software family encountered in Peru in 2Q15 was [Win32/InstalleRex](#), which was encountered by 2.3 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Peru in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/IeEnablerCby	Browser Modifiers	7.9
2	Win32/Gamarue	Worms	3.9
3	VBS/Jenxcus	Worms	3.7
4	Win32/CompromisedCert	Other Malware	2.3
5	Win32/Kilim	Trojans	1.7
6	Win32/Vobfus	Worms	1.1
7	Win32/Ramnit	Trojans	0.7
8	Win32/Sality	Viruses	0.7
9	Win32/Yeltminky	Worms	0.6
10	Win32/Dorkbot	Worms	0.3

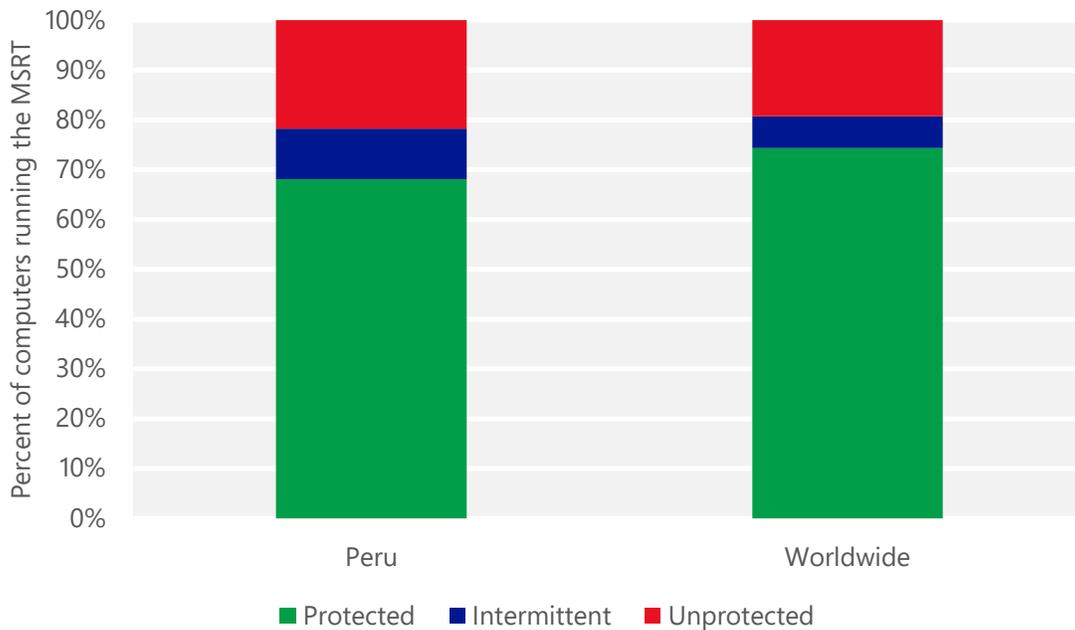
- The most common threat family infecting computers in Peru in 2Q15 was [Win32/IeEnablerCby](#), which was detected and removed from 7.9 of every 1,000 unique computers scanned by the MSRT. [Win32/IeEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Peru in 2Q15 was [Win32/Gamarue](#), which was detected and removed from 3.9 of every 1,000 unique computers scanned by the MSRT. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The third most common threat family infecting computers in Peru in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 3.7 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The fourth most common threat family infecting computers in Peru in 2Q15 was [Win32/CompromisedCert](#), which was detected and removed from 2.3 of every 1,000 unique computers scanned by the MSRT. [Win32/CompromisedCert](#) is a detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Peru and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Peru

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.02 (0.28)	0.05 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	2.60 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	5.94 (16.7)	

Philippines

The statistics presented here are generated by Microsoft security programs and services running on computers in Philippines in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Philippines

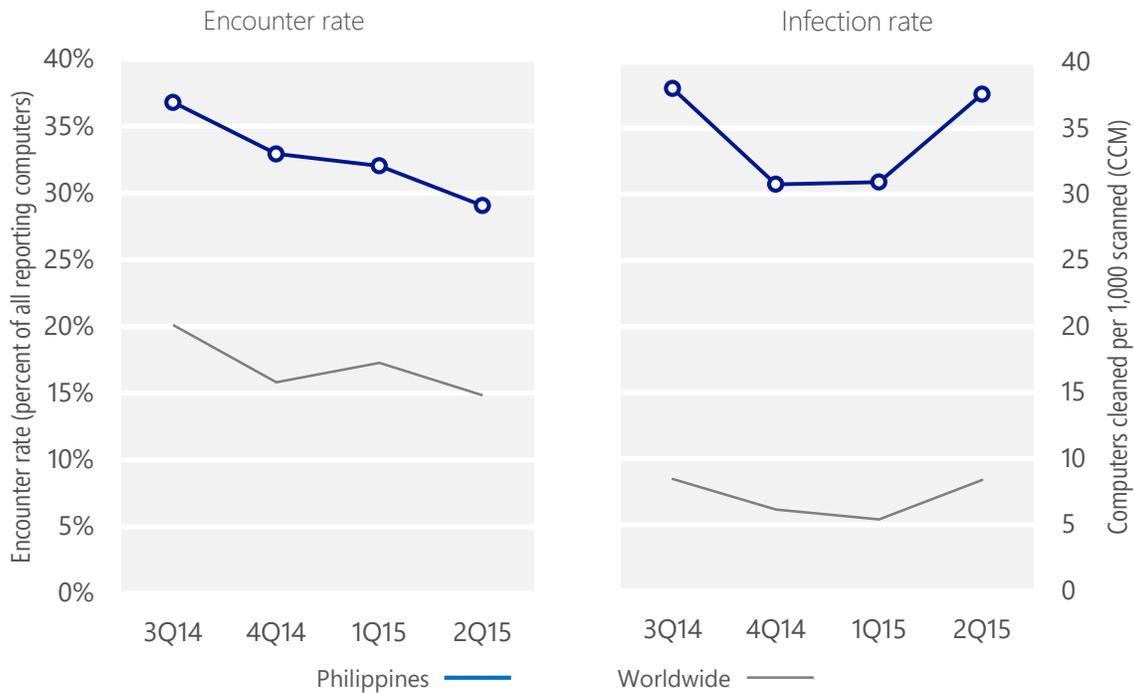
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Philippines	36.8%	32.9%	32.0%	29.1%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Philippines	38.0	30.8	30.9	37.6
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcoute, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 29.1% of computers in Philippines encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 37.6 of every 1,000 unique computers scanned in Philippines in 2Q15 (a CCM score of 37.6, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Philippines over the last four quarters, compared to the world as a whole.

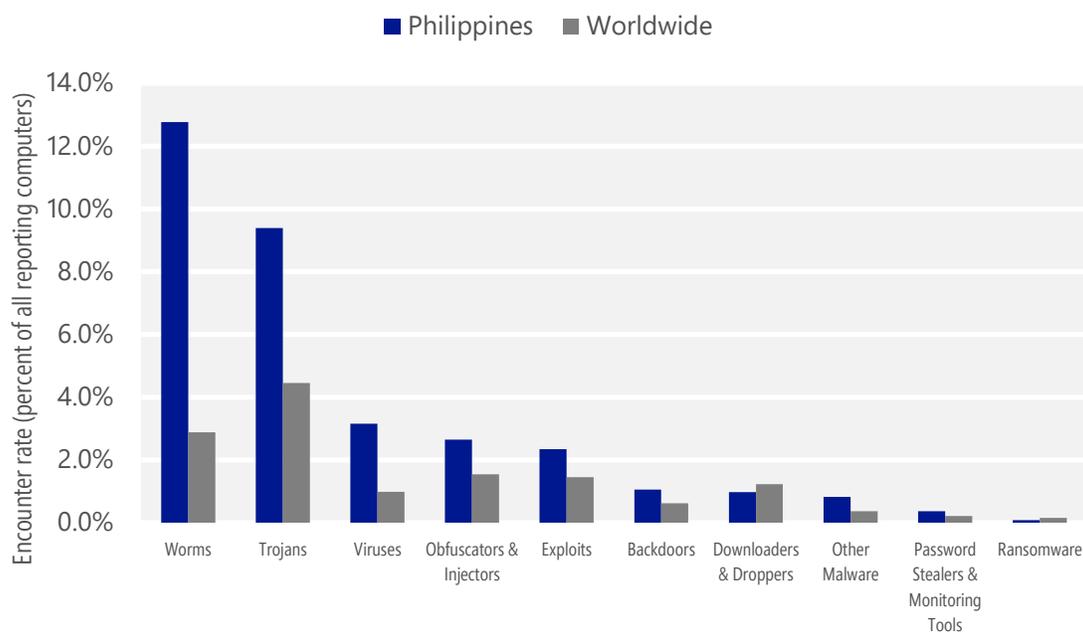
Malware encounter and infection rate trends in Philippines and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in Philippines and around the world, and for explanations of the methods and terms used here.

Malware categories

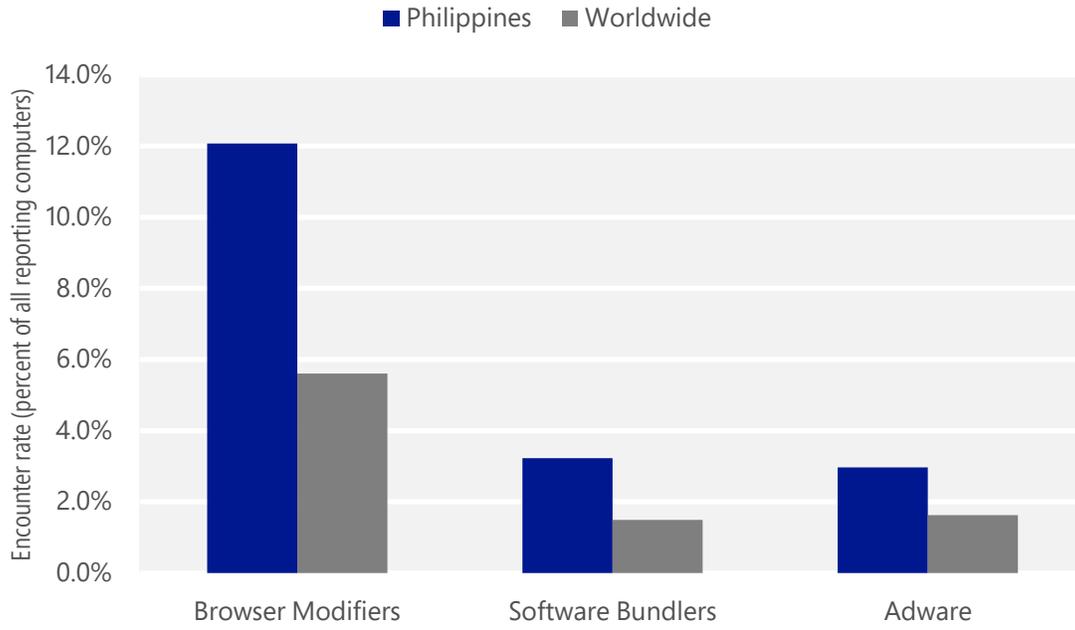
Malware encountered in Philippines in 2Q15, by category



- The most common malware category in Philippines in 2Q15 was Worms. It was encountered by 12.8 percent of all computers there, down from 14.6 percent in 1Q15.
- The second most common malware category in Philippines in 2Q15 was Trojans. It was encountered by 9.4 percent of all computers there, up from 6.4 percent in 1Q15.
- The third most common malware category in Philippines in 2Q15 was Viruses, which was encountered by 3.2 percent of all computers there, down from 3.8 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Philippines in 2Q15, by category



- The most common unwanted software category in Philippines in 2Q15 was Browser Modifiers. It was encountered by 12.1 percent of all computers there, down from 16.3 percent in 1Q15.
- The second most common unwanted software category in Philippines in 2Q15 was Software Bundlers. It was encountered by 3.2 percent of all computers there, down from 6.4 percent in 1Q15.
- The third most common unwanted software category in Philippines in 2Q15 was Adware, which was encountered by 3.0 percent of all computers there, up from 1.3 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Philippines in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Gamarue	Worms	5.3%
2	VBS/Jenxcus	Worms	3.5%
3	Win32/Ippedo	Worms	3.1%
4	INF/Autorun	Obfuscators & Injectors	2.2%
5	Win32/Ramnit	Trojans	2.1%
6	VBS/Cantix	Worms	2.0%
7	Win32/CplLnk	Exploits	1.8%
8	Win32/Sality	Viruses	1.8%
9	Win32/Kilim	Trojans	1.6%
10	Win32/Skeeyah	Trojans	1.4%

- The most common malware family encountered in Philippines in 2Q15 was [Win32/Gamarue](#), which was encountered by 5.3 percent of reporting computers there. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The second most common malware family encountered in Philippines in 2Q15 was [VBS/Jenxcus](#), which was encountered by 3.5 percent of reporting computers there. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The third most common malware family encountered in Philippines in 2Q15 was [Win32/Ippedo](#), which was encountered by 3.1 percent of reporting computers there. [Win32/Ippedo](#) is a worm that can send sensitive information to a malicious hacker. It spreads through removable drives, such as USB flash drives.
- The fourth most common malware family encountered in Philippines in 2Q15 was [INF/Autorun](#), which was encountered by 2.2 percent of reporting computers there. [INF/Autorun](#) is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Philippines in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/KipodToolsCby	Browser Modifiers	6.2%
2	Win32/CouponRuc	Browser Modifiers	6.2%
3	Win32/InstalleRex	Software Bundlers	2.9%
4	Win32/SaverExtension	Adware	2.0%
5	Win32/AlterbookSP	Browser Modifiers	0.5%

- The most common unwanted software family encountered in Philippines in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 6.2 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common unwanted software family encountered in Philippines in 2Q15 was [Win32/CouponRuc](#), which was encountered by 6.2 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The third most common unwanted software family encountered in Philippines in 2Q15 was [Win32/InstalleRex](#), which was encountered by 2.9 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Philippines in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/Gamarue	Worms	8.5
2	VBS/Jenxcus	Worms	7.2
3	Win32/leEnablerCby	Browser Modifiers	6.4
4	Win32/Sality	Viruses	6.4
5	Win32/Ramnit	Trojans	4.5
6	Win32/Kilim	Trojans	2.1
7	Win32/CompromisedCert	Other Malware	1.4
8	Win32/Pramro	Trojans	1.0
9	Win32/Yeltminky	Worms	0.8
10	Win32/Brontok	Worms	0.8

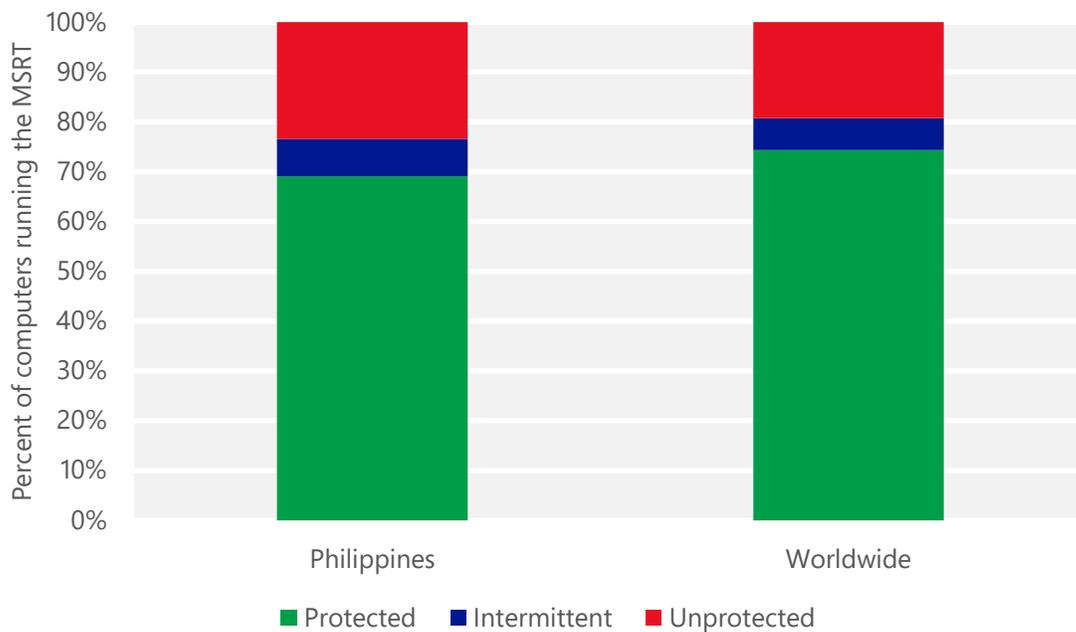
- The most common threat family infecting computers in Philippines in 2Q15 was [Win32/Gamarue](#), which was detected and removed from 8.5 of every 1,000 unique computers scanned by the MSRT. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The second most common threat family infecting computers in Philippines in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 7.2 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The third most common threat family infecting computers in Philippines in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 6.4 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The fourth most common threat family infecting computers in Philippines in 2Q15 was [Win32/Sality](#), which was detected and removed from 6.4 of every 1,000 unique computers scanned by the MSRT. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Philippines and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Philippines

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.33 (0.28)	0.16 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	1.89 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	11.66 (16.7)	

Poland

The statistics presented here are generated by Microsoft security programs and services running on computers in Poland in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Poland

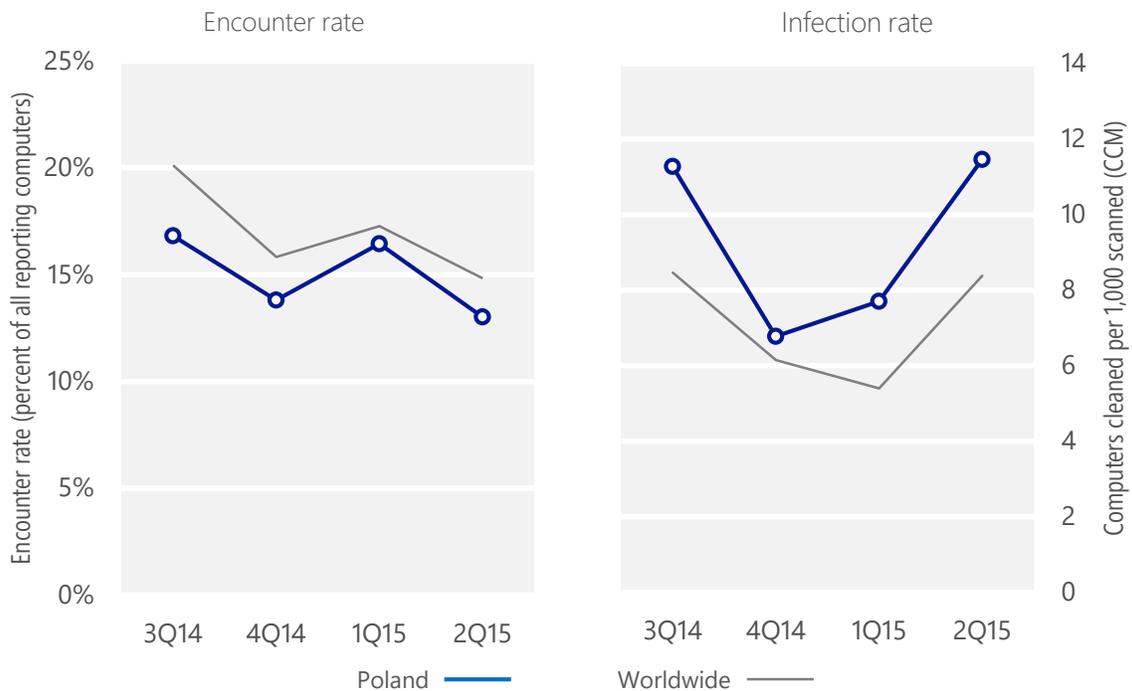
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Poland	16.8%	13.8%	16.4%	13.0%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Poland	11.3	6.8	7.7	11.5
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcout, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 13.0% of computers in Poland encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 11.5 of every 1,000 unique computers scanned in Poland in 2Q15 (a CCM score of 11.5, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Poland over the last four quarters, compared to the world as a whole.

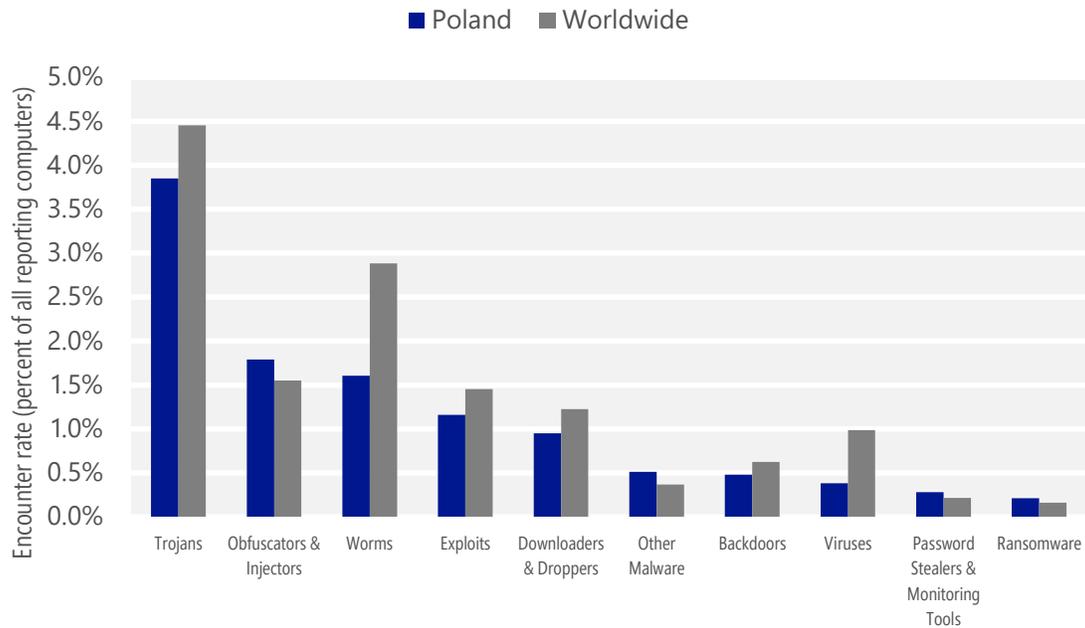
Malware encounter and infection rate trends in Poland and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in Poland and around the world, and for explanations of the methods and terms used here.

Malware categories

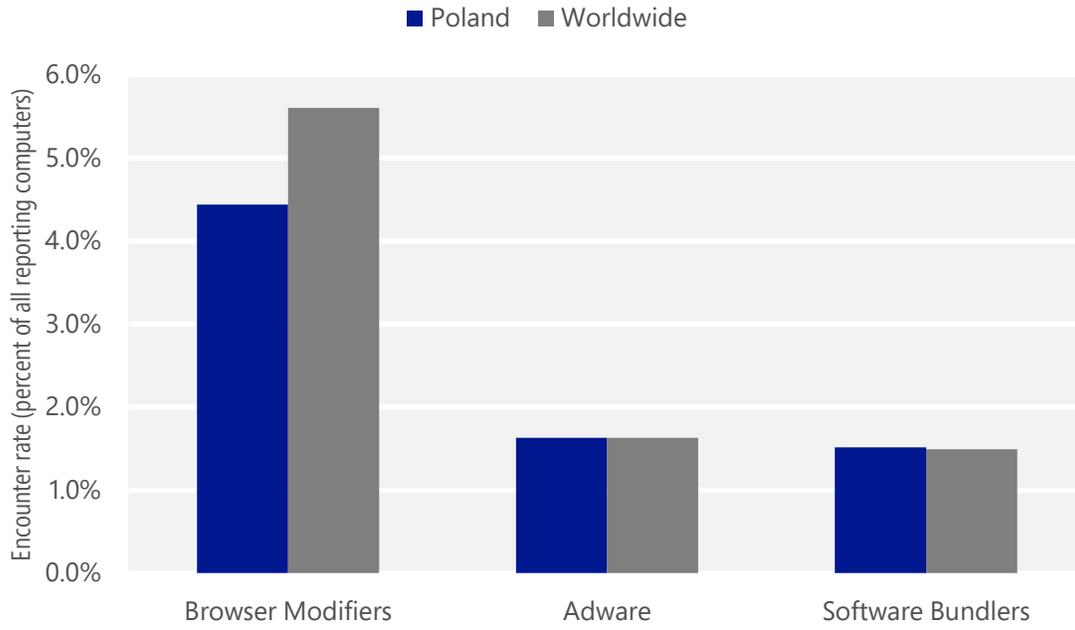
Malware encountered in Poland in 2Q15, by category



- The most common malware category in Poland in 2Q15 was Trojans. It was encountered by 3.8 percent of all computers there, up from 3.6 percent in 1Q15.
- The second most common malware category in Poland in 2Q15 was Obfuscators & Injectors. It was encountered by 1.8 percent of all computers there, down from 2.3 percent in 1Q15.
- The third most common malware category in Poland in 2Q15 was Worms, which was encountered by 1.6 percent of all computers there, down from 2.2 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Poland in 2Q15, by category



- The most common unwanted software category in Poland in 2Q15 was Browser Modifiers. It was encountered by 4.4 percent of all computers there, down from 6.2 percent in 1Q15.
- The second most common unwanted software category in Poland in 2Q15 was Adware. It was encountered by 1.6 percent of all computers there, down from 3.9 percent in 1Q15.
- The third most common unwanted software category in Poland in 2Q15 was Software Bundlers, which was encountered by 1.5 percent of all computers there, up from 0.5 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Poland in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Obfuscator	Obfuscators & Injectors	1.3%
2	Win32/Peals	Trojans	0.6%
3	Win32/Skeeyah	Trojans	0.6%
4	Win32/Kilim	Trojans	0.6%
5	JS/Axpergle	Exploits	0.6%
6	Win32/Gamarue	Worms	0.5%
7	INF/Autorun	Obfuscators & Injectors	0.4%
8	Win32/Dynamer	Trojans	0.3%
9	Win32/Brontok	Worms	0.3%
10	JS/Neclu	Exploits	0.3%

- The most common malware family encountered in Poland in 2Q15 was [Win32/Obfuscator](#), which was encountered by 1.3 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The second most common malware family encountered in Poland in 2Q15 was [Win32/Peals](#), which was encountered by 0.6 percent of reporting computers there. [Win32/Peals](#) is a generic detection for various threats that display trojan characteristics.
- The third most common malware family encountered in Poland in 2Q15 was [Win32/Skeeyah](#), which was encountered by 0.6 percent of reporting computers there. [Win32/Skeeyah](#) is a generic detection for various threats that display trojan characteristics.
- The fourth most common malware family encountered in Poland in 2Q15 was [Win32/Kilim](#), which was encountered by 0.6 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Poland in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	2.5%
2	Win32/InstalleRex	Software Bundlers	1.5%
3	Win32/KipodToolsCby	Browser Modifiers	1.3%
4	Win32/SaverExtension	Adware	0.8%
5	Win32/AlterbookSP	Browser Modifiers	0.6%

- The most common unwanted software family encountered in Poland in 2Q15 was [Win32/CouponRuc](#), which was encountered by 2.5 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in Poland in 2Q15 was [Win32/InstalleRex](#), which was encountered by 1.5 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own “Installed On” date in Programs and Features to make it more difficult for a user to locate it and remove it.
- The third most common unwanted software family encountered in Poland in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 1.3 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user’s consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.

Top threat families by infection rate

The most common malware families by infection rate in Poland in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/CompromisedCert	Other Malware	4.4
2	Win32/leEnablerCby	Browser Modifiers	2.3
3	Win32/Kilim	Trojans	1.0
4	Win32/Brontok	Worms	0.7
5	Win32/Sality	Viruses	0.6
6	Win32/Vobfus	Worms	0.4
7	Win32/Wysotot	Trojans	0.2
8	Win32/Gamarue	Worms	0.2
9	MSIL/Bladabindi	Backdoors	0.2
10	Win32/Simda	Trojans	0.2

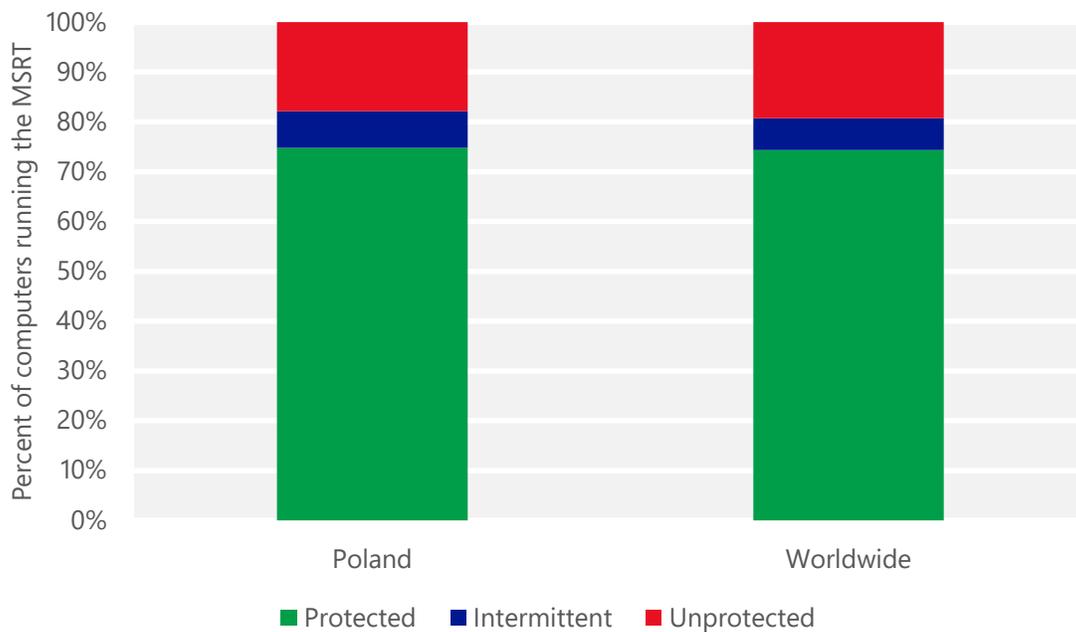
- The most common threat family infecting computers in Poland in 2Q15 was [Win32/CompromisedCert](#), which was detected and removed from 4.4 of every 1,000 unique computers scanned by the MSRT. [Win32/CompromisedCert](#) is a detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.
- The second most common threat family infecting computers in Poland in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 2.3 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common threat family infecting computers in Poland in 2Q15 was [Win32/Kilim](#), which was detected and removed from 1.0 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The fourth most common threat family infecting computers in Poland in 2Q15 was [Win32/Brontok](#), which was detected and removed from 0.7 of every 1,000 unique computers scanned by the MSRT. [Win32/Brontok](#) is a mass-mailing email worm that spreads by sending copies of itself as email attachments to addresses gathered from files on the infected computer, and by copying itself to removable volumes. Brontok can disable security software, and may conduct DoS attacks against certain websites.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Poland and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Poland

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.21 (0.28)	0.20 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	4.42 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	5.72 (16.7)	

Portugal

The statistics presented here are generated by Microsoft security programs and services running on computers in Portugal in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Portugal

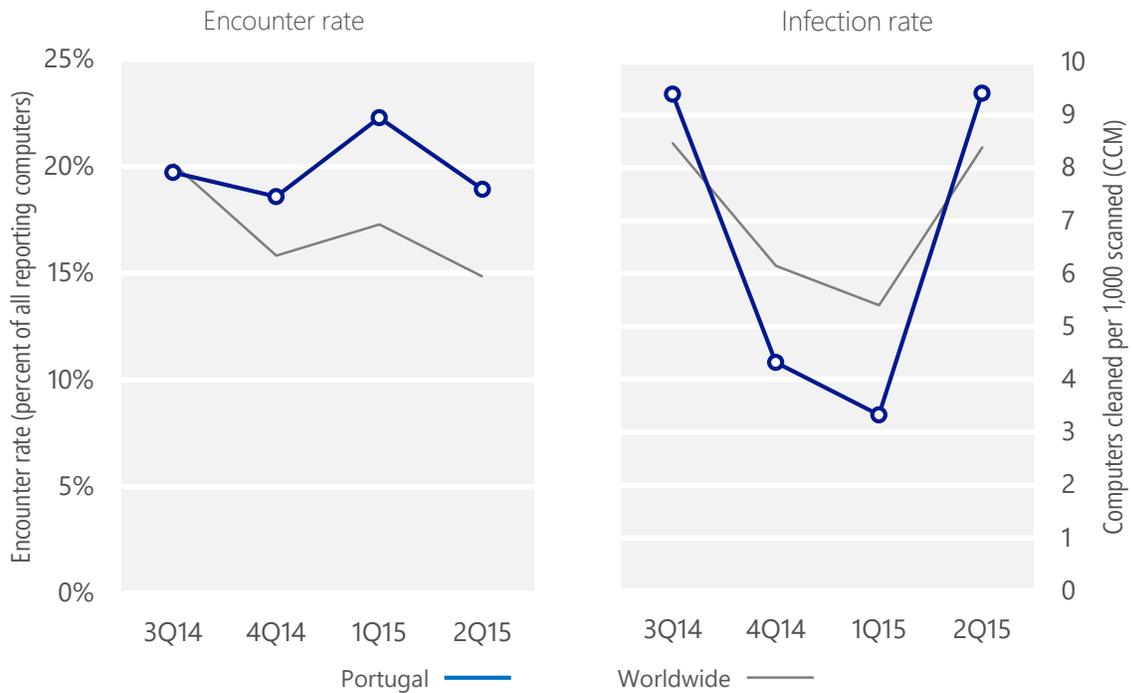
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Portugal	19.7%	18.6%	22.3%	18.9%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Portugal	9.4	4.3	3.3	9.4
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcout, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 18.9% of computers in Portugal encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 9.4 of every 1,000 unique computers scanned in Portugal in 2Q15 (a CCM score of 9.4, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Portugal over the last four quarters, compared to the world as a whole.

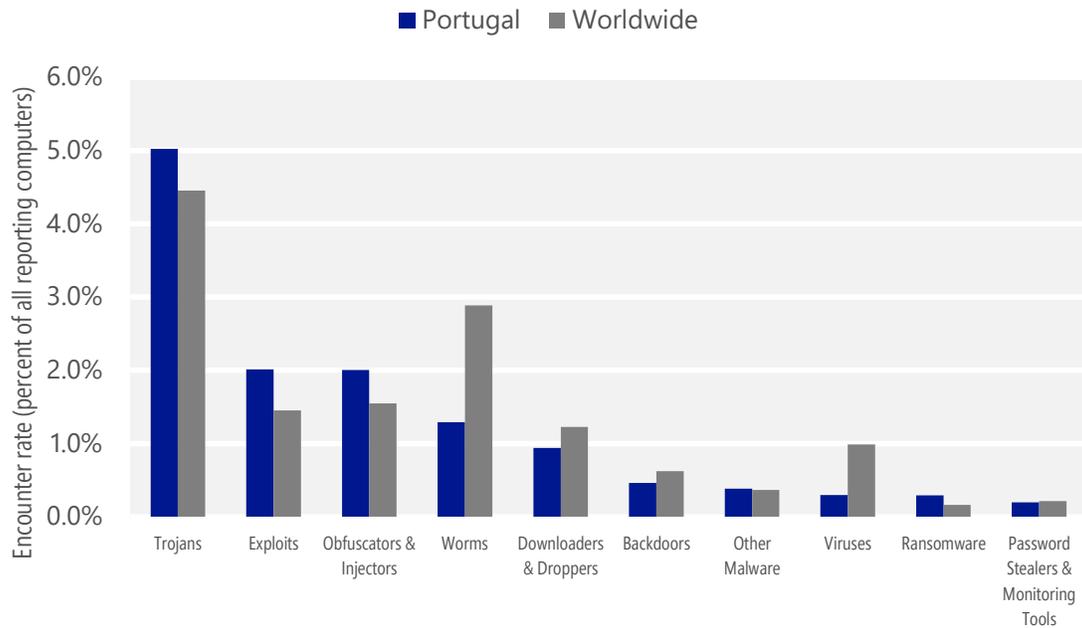
Malware encounter and infection rate trends in Portugal and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in Portugal and around the world, and for explanations of the methods and terms used here.

Malware categories

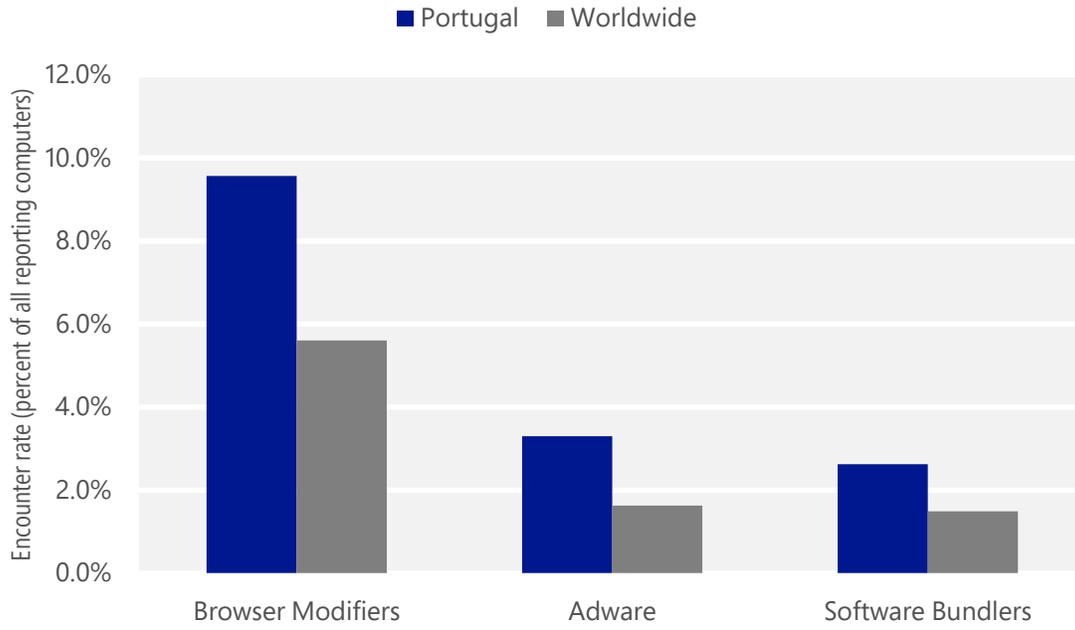
Malware encountered in Portugal in 2Q15, by category



- The most common malware category in Portugal in 2Q15 was Trojans. It was encountered by 5.0 percent of all computers there, up from 3.3 percent in 1Q15.
- The second most common malware category in Portugal in 2Q15 was Exploits. It was encountered by 2.0 percent of all computers there, down from 2.5 percent in 1Q15.
- The third most common malware category in Portugal in 2Q15 was Obfuscators & Injectors, which was encountered by 2.0 percent of all computers there, down from 2.4 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Portugal in 2Q15, by category



- The most common unwanted software category in Portugal in 2Q15 was Browser Modifiers. It was encountered by 9.6 percent of all computers there, down from 12.6 percent in 1Q15.
- The second most common unwanted software category in Portugal in 2Q15 was Adware. It was encountered by 3.3 percent of all computers there, down from 6.0 percent in 1Q15.
- The third most common unwanted software category in Portugal in 2Q15 was Software Bundlers, which was encountered by 2.6 percent of all computers there, up from 0.6 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Portugal in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Obfuscator	Obfuscators & Injectors	1.6%
2	Win32/Kilim	Trojans	1.4%
3	JS/Axpergle	Exploits	1.3%
4	Win32/Skeeyah	Trojans	1.1%
5	Win32/Peals	Trojans	0.5%
6	INF/Autorun	Obfuscators & Injectors	0.4%
7	Win32/Dynamer	Trojans	0.3%
8	VBS/Jenxcus	Worms	0.3%
9	Win32/Gamarue	Worms	0.3%
10	Win32/Brontok	Worms	0.2%

- The most common malware family encountered in Portugal in 2Q15 was [Win32/Obfuscator](#), which was encountered by 1.6 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The second most common malware family encountered in Portugal in 2Q15 was [Win32/Kilim](#), which was encountered by 1.4 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The third most common malware family encountered in Portugal in 2Q15 was [JS/Axpergle](#), which was encountered by 1.3 percent of reporting computers there. [JS/Axpergle](#) is a detection for the Angler exploit kit, which exploits vulnerabilities in recent versions of Internet Explorer, Silverlight, Adobe Flash Player, and Java to install malware.
- The fourth most common malware family encountered in Portugal in 2Q15 was [Win32/Skeeyah](#), which was encountered by 1.1 percent of reporting computers there. [Win32/Skeeyah](#) is a generic detection for various threats that display trojan characteristics.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Portugal in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	5.2%
2	Win32/KipodToolsCby	Browser Modifiers	4.0%
3	Win32/InstalleRex	Software Bundlers	2.5%
4	Win32/SaverExtension	Adware	1.8%
5	Win32/EoRezo	Adware	1.3%

- The most common unwanted software family encountered in Portugal in 2Q15 was [Win32/CouponRuc](#), which was encountered by 5.2 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in Portugal in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 4.0 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common unwanted software family encountered in Portugal in 2Q15 was [Win32/InstalleRex](#), which was encountered by 2.5 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Portugal in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/IeEnablerCby	Browser Modifiers	4.2
2	Win32/Kilim	Trojans	1.4
3	Win32/CompromisedCert	Other Malware	0.7
4	Win32/BrobanDel	Trojans	0.6
5	VBS/Jenxcus	Worms	0.4
6	Win32/Brontok	Worms	0.3
7	MSIL/Bladabindi	Backdoors	0.2
8	Win32/Ramnit	Trojans	0.2
9	Win32/Simda	Trojans	0.2
10	Win32/Wysotot	Trojans	0.2

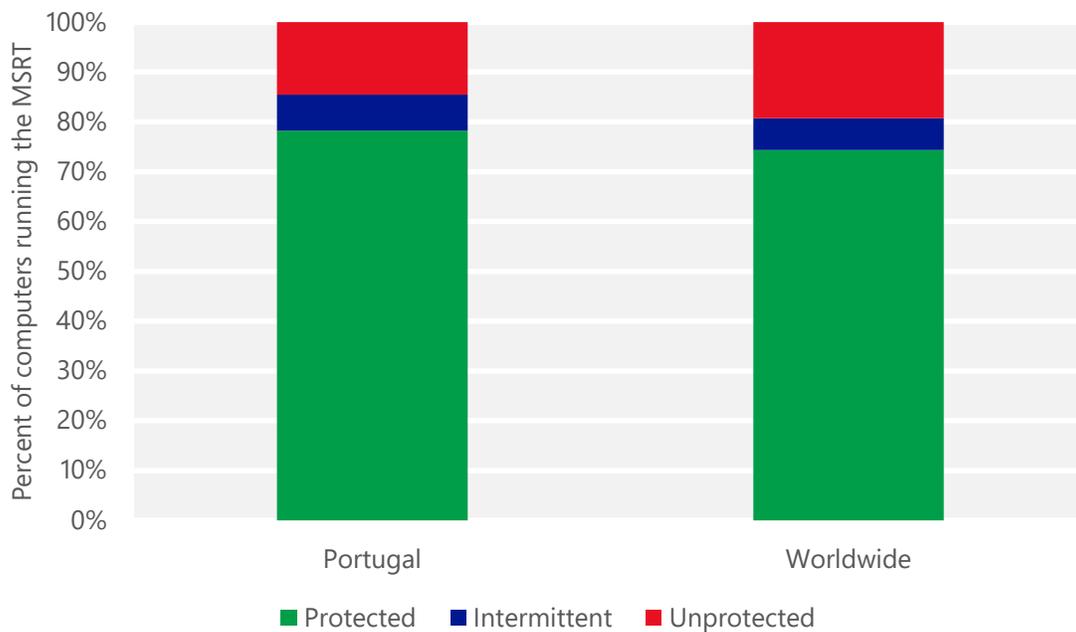
- The most common threat family infecting computers in Portugal in 2Q15 was [Win32/IeEnablerCby](#), which was detected and removed from 4.2 of every 1,000 unique computers scanned by the MSRT. [Win32/IeEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Portugal in 2Q15 was [Win32/Kilim](#), which was detected and removed from 1.4 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The third most common threat family infecting computers in Portugal in 2Q15 was [Win32/CompromisedCert](#), which was detected and removed from 0.7 of every 1,000 unique computers scanned by the MSRT. [Win32/CompromisedCert](#) is a detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.
- The fourth most common threat family infecting computers in Portugal in 2Q15 was [Win32/BrobanDel](#), which was detected and removed from 0.6 of every 1,000 unique computers scanned by the MSRT. [Win32/BrobanDel](#) is a family of trojans that can modify Boleto Bancário, a common payment method in Brazil. They can be installed on the computer when a user opens a malicious spam email attachment.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Portugal and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Portugal

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.16 (0.28)	0.19 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	8.42 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	14.47 (16.7)	

Puerto Rico

The statistics presented here are generated by Microsoft security programs and services running on computers in Puerto Rico in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Puerto Rico

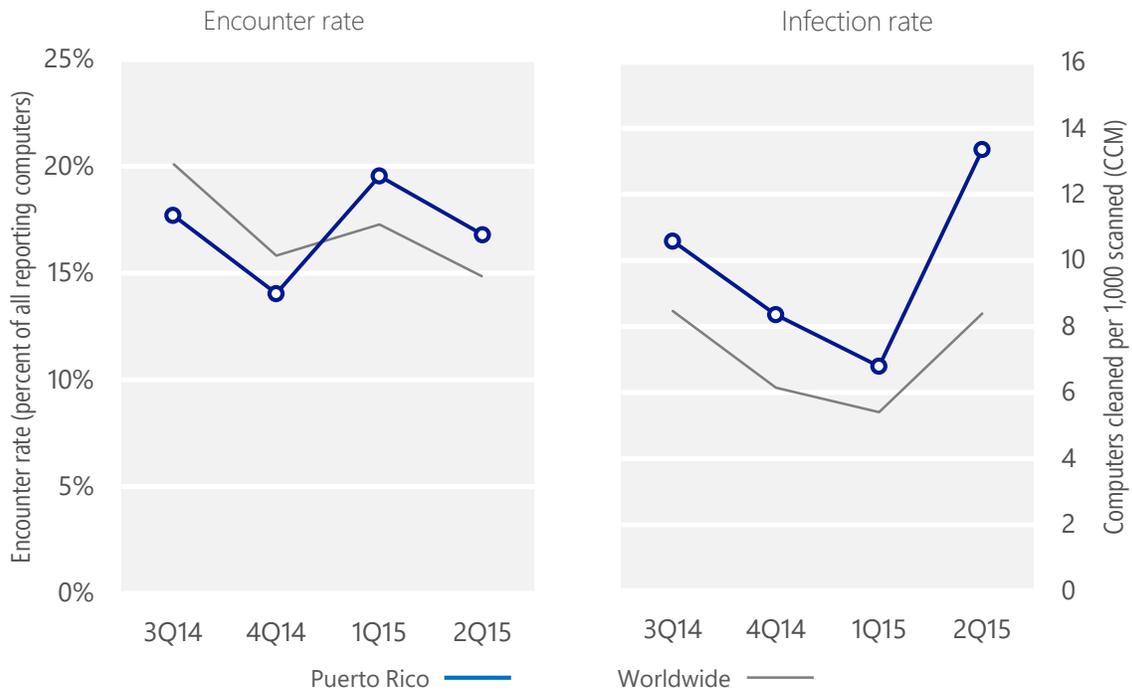
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Puerto Rico	17.7%	14.0%	19.5%	16.8%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Puerto Rico	10.6	8.4	6.8	13.4
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcout, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 16.8% of computers in Puerto Rico encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 13.4 of every 1,000 unique computers scanned in Puerto Rico in 2Q15 (a CCM score of 13.4, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Puerto Rico over the last four quarters, compared to the world as a whole.

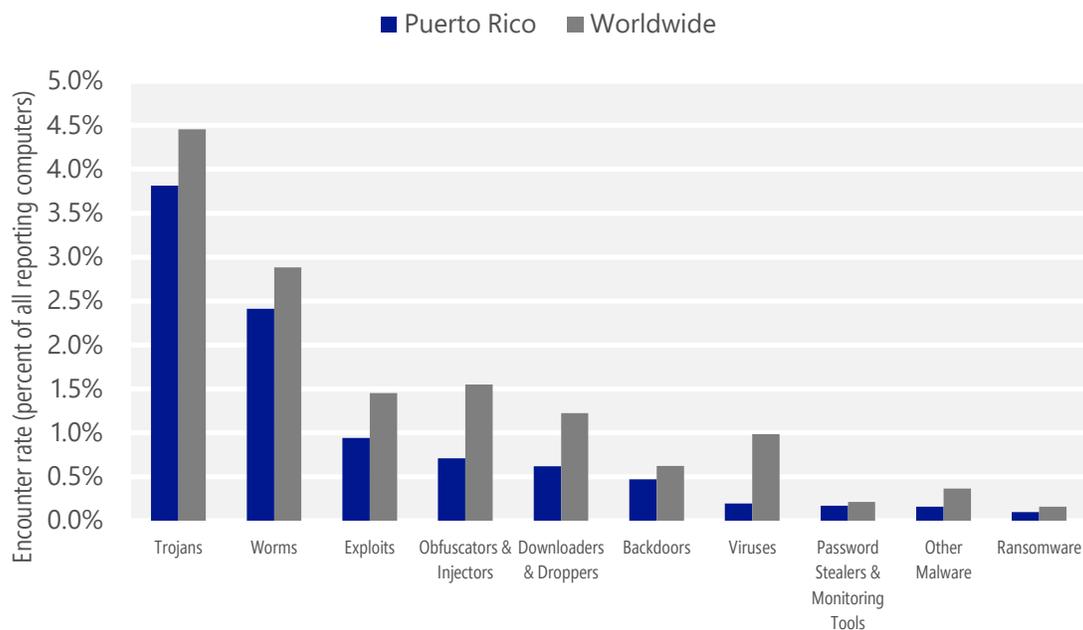
Malware encounter and infection rate trends in Puerto Rico and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in Puerto Rico and around the world, and for explanations of the methods and terms used here.

Malware categories

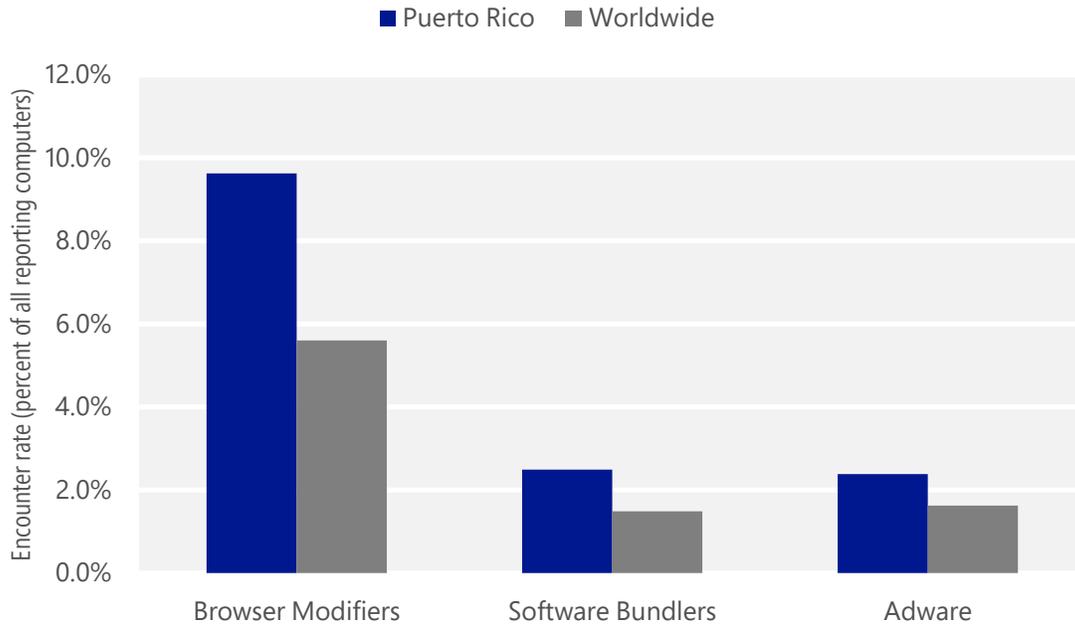
Malware encountered in Puerto Rico in 2Q15, by category



- The most common malware category in Puerto Rico in 2Q15 was Trojans. It was encountered by 3.8 percent of all computers there, up from 3.3 percent in 1Q15.
- The second most common malware category in Puerto Rico in 2Q15 was Worms. It was encountered by 2.4 percent of all computers there, up from 1.7 percent in 1Q15.
- The third most common malware category in Puerto Rico in 2Q15 was Exploits, which was encountered by 0.9 percent of all computers there, down from 1.5 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Puerto Rico in 2Q15, by category



- The most common unwanted software category in Puerto Rico in 2Q15 was Browser Modifiers. It was encountered by 9.6 percent of all computers there, down from 12.4 percent in 1Q15.
- The second most common unwanted software category in Puerto Rico in 2Q15 was Software Bundlers. It was encountered by 2.5 percent of all computers there, down from 5.4 percent in 1Q15.
- The third most common unwanted software category in Puerto Rico in 2Q15 was Adware, which was encountered by 2.4 percent of all computers there, up from 0.8 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Puerto Rico in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Kilim	Trojans	1.0%
2	VBS/Jenxcus	Worms	0.9%
3	Win32/Skeeyah	Trojans	0.6%
4	JS/Axpergle	Exploits	0.6%
5	INF/Autorun	Obfuscators & Injectors	0.5%
6	Win32/Obfuscator	Obfuscators & Injectors	0.4%
7	Win32/Vobfus	Worms	0.4%
8	Win32/Brontok	Worms	0.4%
9	Win32/Caphaw	Backdoors	0.2%
10	MSIL/Shaskooth	Worms	0.2%

- The most common malware family encountered in Puerto Rico in 2Q15 was [Win32/Kilim](#), which was encountered by 1.0 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The second most common malware family encountered in Puerto Rico in 2Q15 was [VBS/Jenxcus](#), which was encountered by 0.9 percent of reporting computers there. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The third most common malware family encountered in Puerto Rico in 2Q15 was [Win32/Skeeyah](#), which was encountered by 0.6 percent of reporting computers there. [Win32/Skeeyah](#) is a generic detection for various threats that display trojan characteristics.
- The fourth most common malware family encountered in Puerto Rico in 2Q15 was [JS/Axpergle](#), which was encountered by 0.6 percent of reporting computers there. [JS/Axpergle](#) is a detection for the Angler exploit kit, which exploits vulnerabilities in recent versions of Internet Explorer, Silverlight, Adobe Flash Player, and Java to install malware.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Puerto Rico in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	4.5%
2	Win32/KipodToolsCby	Browser Modifiers	4.4%
3	Win32/InstalleRex	Software Bundlers	2.3%
4	Win32/SaverExtension	Adware	1.7%
5	Win32/AlterbookSP	Browser Modifiers	0.8%

- The most common unwanted software family encountered in Puerto Rico in 2Q15 was [Win32/CouponRuc](#), which was encountered by 4.5 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in Puerto Rico in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 4.4 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common unwanted software family encountered in Puerto Rico in 2Q15 was [Win32/InstalleRex](#), which was encountered by 2.3 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Puerto Rico in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/IeEnablerCby	Browser Modifiers	5.9
2	VBS/Jenxcus	Worms	2.2
3	Win32/Kilim	Trojans	1.6
4	Win32/Vobfus	Worms	0.8
5	Win32/Brontok	Worms	0.8
6	Win32/CompromisedCert	Other Malware	0.5
7	Win32/Dorkbot	Worms	0.3
8	Win32/Alureon	Trojans	0.2
9	Win32/Dyzap	Password Stealers & Monitoring Tools	0.2
10	Win32/Simda	Trojans	0.2

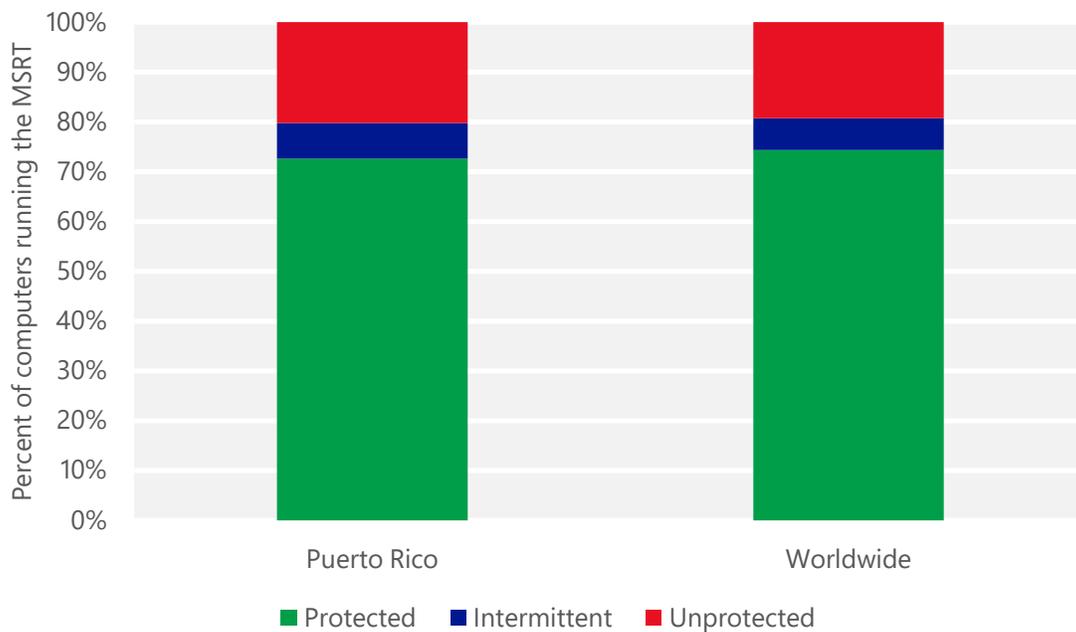
- The most common threat family infecting computers in Puerto Rico in 2Q15 was [Win32/IeEnablerCby](#), which was detected and removed from 5.9 of every 1,000 unique computers scanned by the MSRT. [Win32/IeEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Puerto Rico in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 2.2 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The third most common threat family infecting computers in Puerto Rico in 2Q15 was [Win32/Kilim](#), which was detected and removed from 1.6 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The fourth most common threat family infecting computers in Puerto Rico in 2Q15 was [Win32/Vobfus](#), which was detected and removed from 0.8 of every 1,000 unique computers scanned by the MSRT. [Win32/Vobfus](#) is a family of worms that spreads via network drives and removable drives and download/executes arbitrary files. Downloaded files may include additional malware.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Puerto Rico and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Puerto Rico

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.02 (0.28)	0.03 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	1.11 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	17.84 (16.7)	

Qatar

The statistics presented here are generated by Microsoft security programs and services running on computers in Qatar in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Qatar

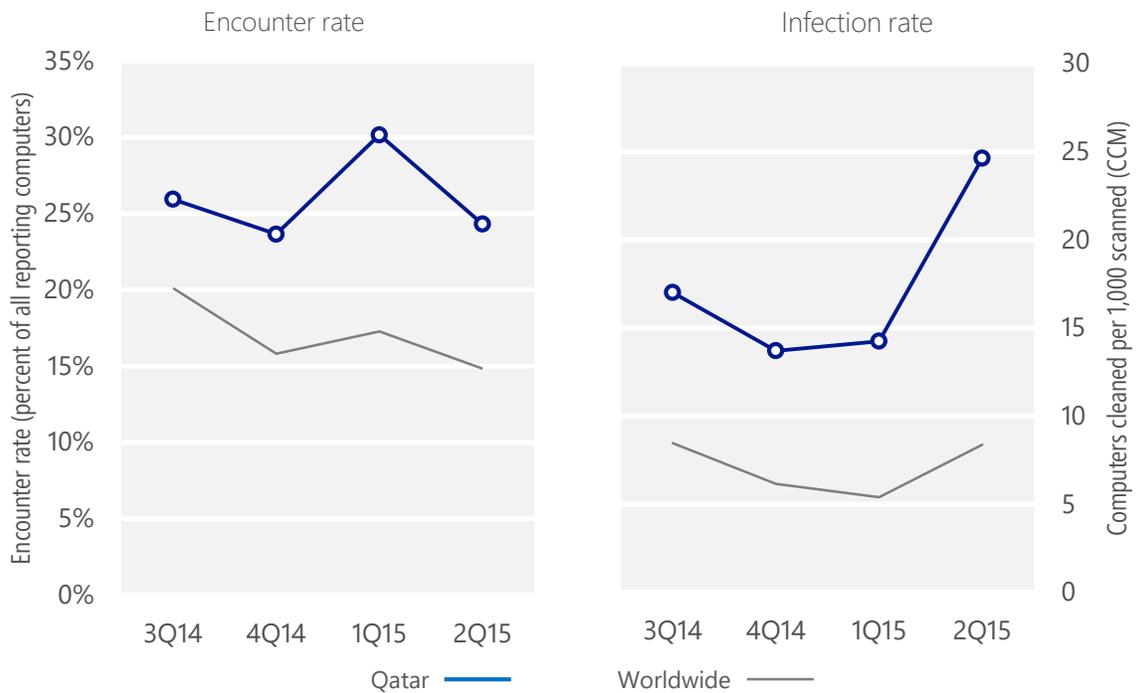
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Qatar	25.9%	23.7%	30.2%	24.3%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Qatar	17.0	13.7	14.3	24.6
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcote, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 24.3% of computers in Qatar encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 24.6 of every 1,000 unique computers scanned in Qatar in 2Q15 (a CCM score of 24.6, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Qatar over the last four quarters, compared to the world as a whole.

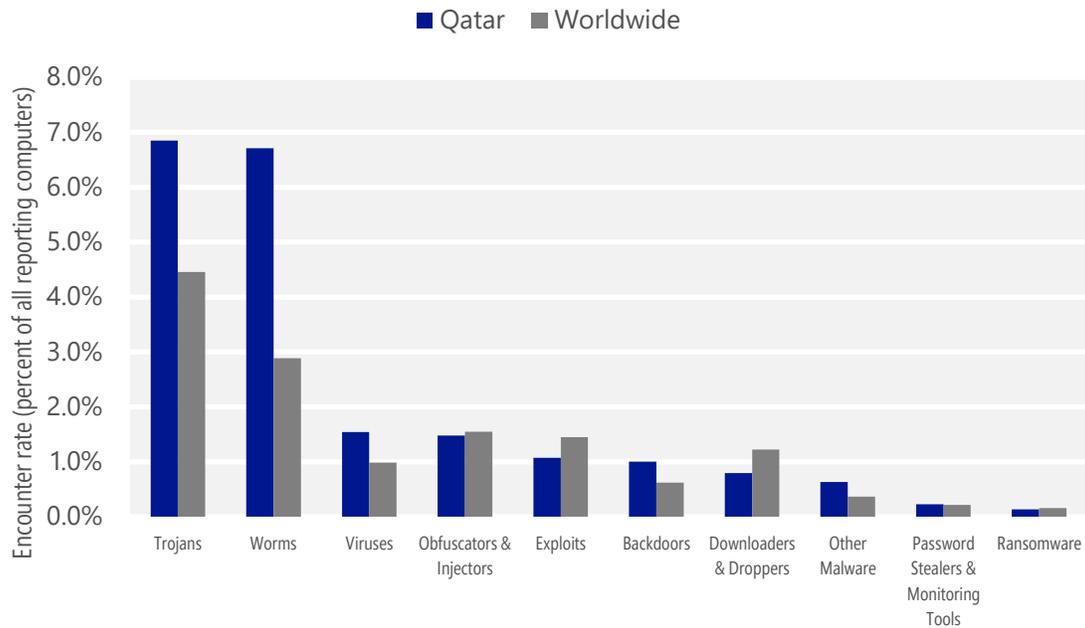
Malware encounter and infection rate trends in Qatar and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in Qatar and around the world, and for explanations of the methods and terms used here.

Malware categories

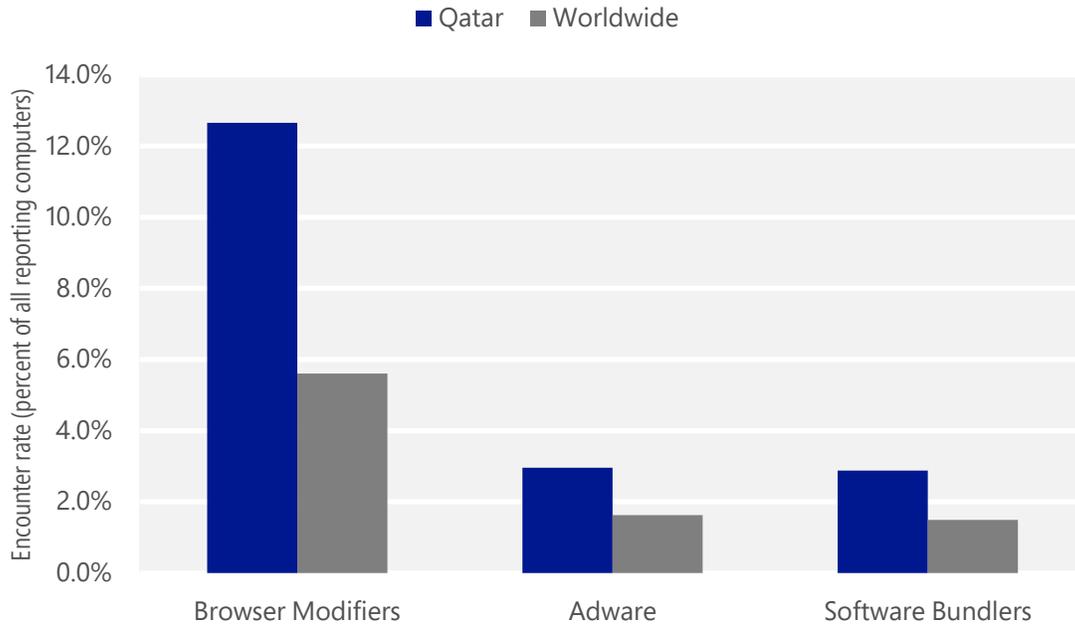
Malware encountered in Qatar in 2Q15, by category



- The most common malware category in Qatar in 2Q15 was Trojans. It was encountered by 6.8 percent of all computers there, down from 7.0 percent in 1Q15.
- The second most common malware category in Qatar in 2Q15 was Worms. It was encountered by 6.7 percent of all computers there, up from 6.0 percent in 1Q15.
- The third most common malware category in Qatar in 2Q15 was Viruses, which was encountered by 1.5 percent of all computers there, down from 2.0 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Qatar in 2Q15, by category



- The most common unwanted software category in Qatar in 2Q15 was Browser Modifiers. It was encountered by 12.7 percent of all computers there, down from 17.3 percent in 1Q15.
- The second most common unwanted software category in Qatar in 2Q15 was Adware. It was encountered by 3.0 percent of all computers there, down from 8.0 percent in 1Q15.
- The third most common unwanted software category in Qatar in 2Q15 was Software Bundlers, which was encountered by 2.9 percent of all computers there, up from 1.4 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Qatar in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Skeeyah	Trojans	1.7%
2	VBS/Jenxcus	Worms	1.6%
3	Win32/Kilim	Trojans	1.6%
4	Win32/Gamarue	Worms	1.1%
5	INF/Autorun	Obfuscators & Injectors	0.9%
6	Win32/Obfuscator	Obfuscators & Injectors	0.9%
7	Win32/Peals	Trojans	0.7%
8	Win32/Nuqel	Worms	0.6%
9	ALisp/Bursted	Viruses	0.5%
10	MSIL/Bladabindi	Backdoors	0.5%

- The most common malware family encountered in Qatar in 2Q15 was [Win32/Skeeyah](#), which was encountered by 1.7 percent of reporting computers there. [Win32/Skeeyah](#) is a generic detection for various threats that display trojan characteristics.
- The second most common malware family encountered in Qatar in 2Q15 was [VBS/Jenxcus](#), which was encountered by 1.6 percent of reporting computers there. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The third most common malware family encountered in Qatar in 2Q15 was [Win32/Kilim](#), which was encountered by 1.6 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The fourth most common malware family encountered in Qatar in 2Q15 was [Win32/Gamarue](#), which was encountered by 1.1 percent of reporting computers there. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Qatar in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	6.0%
2	Win32/KipodToolsCby	Browser Modifiers	5.5%
3	Win32/InstalleRex	Software Bundlers	2.7%
4	Win32/SaverExtension	Adware	2.2%
5	Win32/Vonteera	Browser Modifiers	1.3%

- The most common unwanted software family encountered in Qatar in 2Q15 was [Win32/CouponRuc](#), which was encountered by 6.0 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in Qatar in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 5.5 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common unwanted software family encountered in Qatar in 2Q15 was [Win32/InstalleRex](#), which was encountered by 2.7 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Qatar in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	7.7
2	Win32/CompromisedCert	Other Malware	4.5
3	VBS/Jenxcus	Worms	3.0
4	Win32/Kilim	Trojans	2.6
5	Win32/Gamarue	Worms	1.6
6	Win32/Sality	Viruses	1.3
7	Win32/Nuqel	Worms	1.1
8	MSIL/Bladabindi	Backdoors	0.8
9	Win32/Ramnit	Trojans	0.4
10	Win32/Brontok	Worms	0.4

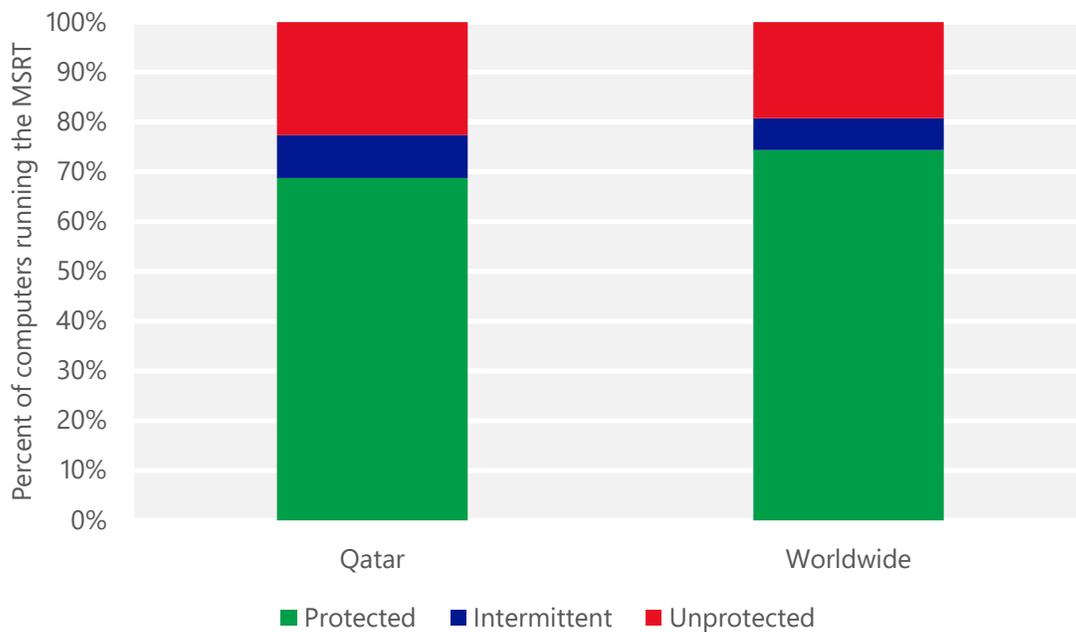
- The most common threat family infecting computers in Qatar in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 7.7 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Qatar in 2Q15 was [Win32/CompromisedCert](#), which was detected and removed from 4.5 of every 1,000 unique computers scanned by the MSRT. [Win32/CompromisedCert](#) is a detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.
- The third most common threat family infecting computers in Qatar in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 3.0 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The fourth most common threat family infecting computers in Qatar in 2Q15 was [Win32/Kilim](#), which was detected and removed from 2.6 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Qatar and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Qatar

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.01 (0.28)	0.02 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	6.94 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	31.40 (16.7)	

Romania

The statistics presented here are generated by Microsoft security programs and services running on computers in Romania in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Romania

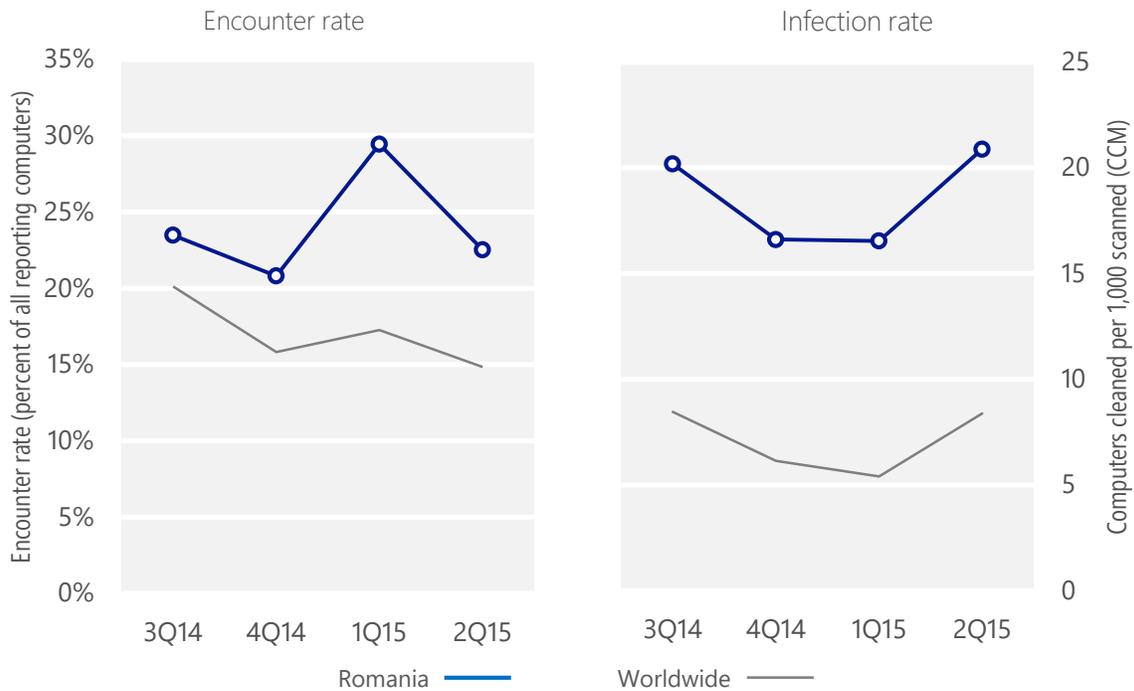
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Romania	23.5%	20.8%	29.4%	22.5%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Romania	20.2	16.6	16.5	20.9
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcout, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 22.5% of computers in Romania encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 20.9 of every 1,000 unique computers scanned in Romania in 2Q15 (a CCM score of 20.9, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Romania over the last four quarters, compared to the world as a whole.

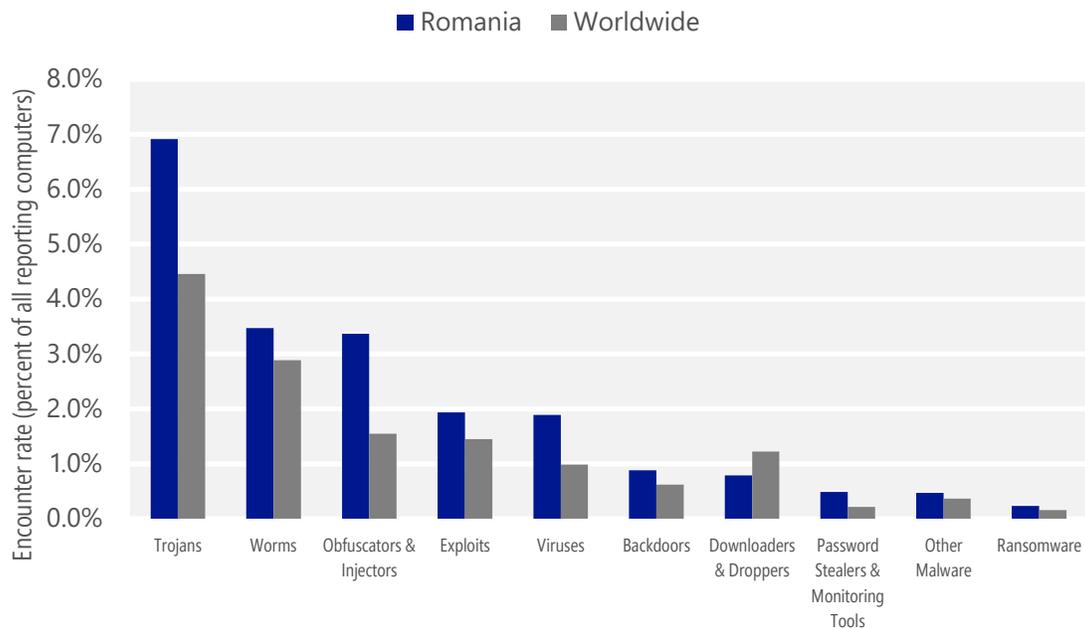
Malware encounter and infection rate trends in Romania and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in Romania and around the world, and for explanations of the methods and terms used here.

Malware categories

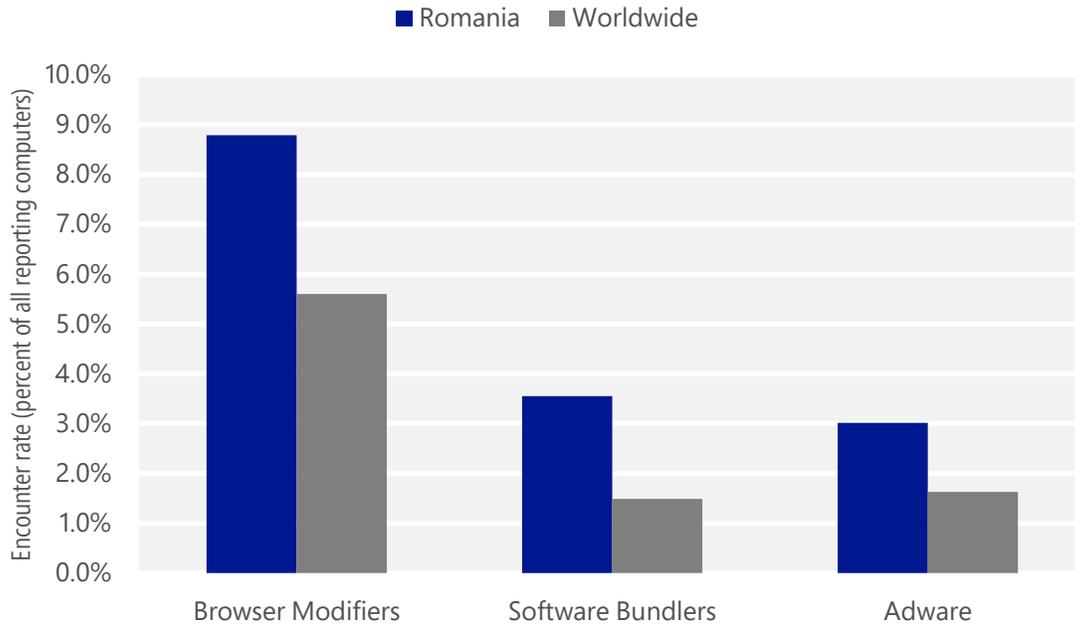
Malware encountered in Romania in 2Q15, by category



- The most common malware category in Romania in 2Q15 was Trojans. It was encountered by 6.9 percent of all computers there, down from 6.9 percent in 1Q15.
- The second most common malware category in Romania in 2Q15 was Worms. It was encountered by 3.5 percent of all computers there, down from 5.1 percent in 1Q15.
- The third most common malware category in Romania in 2Q15 was Obfuscators & Injectors, which was encountered by 3.4 percent of all computers there, down from 4.2 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Romania in 2Q15, by category



- The most common unwanted software category in Romania in 2Q15 was Browser Modifiers. It was encountered by 8.8 percent of all computers there, down from 13.4 percent in 1Q15.
- The second most common unwanted software category in Romania in 2Q15 was Software Bundlers. It was encountered by 3.6 percent of all computers there, down from 6.6 percent in 1Q15.
- The third most common unwanted software category in Romania in 2Q15 was Adware, which was encountered by 3.0 percent of all computers there, up from 1.6 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Romania in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Obfuscator	Obfuscators & Injectors	2.1%
2	Win32/Kilim	Trojans	1.6%
3	Win32/Skeeyah	Trojans	1.3%
4	INF/Autorun	Obfuscators & Injectors	1.2%
5	Win32/Sality	Viruses	0.9%
6	Win32/Gamarue	Worms	0.9%
7	Win32/Peals	Trojans	0.9%
8	JS/Neclu	Exploits	0.8%
9	JS/Axpergle	Exploits	0.8%
10	VBS/Jenxcus	Worms	0.7%

- The most common malware family encountered in Romania in 2Q15 was [Win32/Obfuscator](#), which was encountered by 2.1 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The second most common malware family encountered in Romania in 2Q15 was [Win32/Kilim](#), which was encountered by 1.6 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The third most common malware family encountered in Romania in 2Q15 was [Win32/Skeeyah](#), which was encountered by 1.3 percent of reporting computers there. [Win32/Skeeyah](#) is a generic detection for various threats that display trojan characteristics.
- The fourth most common malware family encountered in Romania in 2Q15 was [INF/Autorun](#), which was encountered by 1.2 percent of reporting computers there. [INF/Autorun](#) is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Romania in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	5.5%
2	Win32/InstalleRex	Software Bundlers	3.4%
3	Win32/KipodToolsCby	Browser Modifiers	2.8%
4	Win32/SaverExtension	Adware	2.0%
5	Win32/AlterbookSP	Browser Modifiers	0.6%

- The most common unwanted software family encountered in Romania in 2Q15 was [Win32/CouponRuc](#), which was encountered by 5.5 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in Romania in 2Q15 was [Win32/InstalleRex](#), which was encountered by 3.4 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own “Installed On” date in Programs and Features to make it more difficult for a user to locate it and remove it.
- The third most common unwanted software family encountered in Romania in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 2.8 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user’s consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.

Top threat families by infection rate

The most common malware families by infection rate in Romania in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	4.9
2	Win32/Sality	Viruses	4.7
3	Win32/Kilim	Trojans	2.1
4	Win32/Ramnit	Trojans	2.0
5	Win32/Brontok	Worms	1.6
6	VBS/Jenxcus	Worms	1.5
7	Win32/CompromisedCert	Other Malware	1.1
8	Win32/Gamarue	Worms	0.9
9	Win32/Pramro	Trojans	0.8
10	Win32/Helompy	Worms	0.5

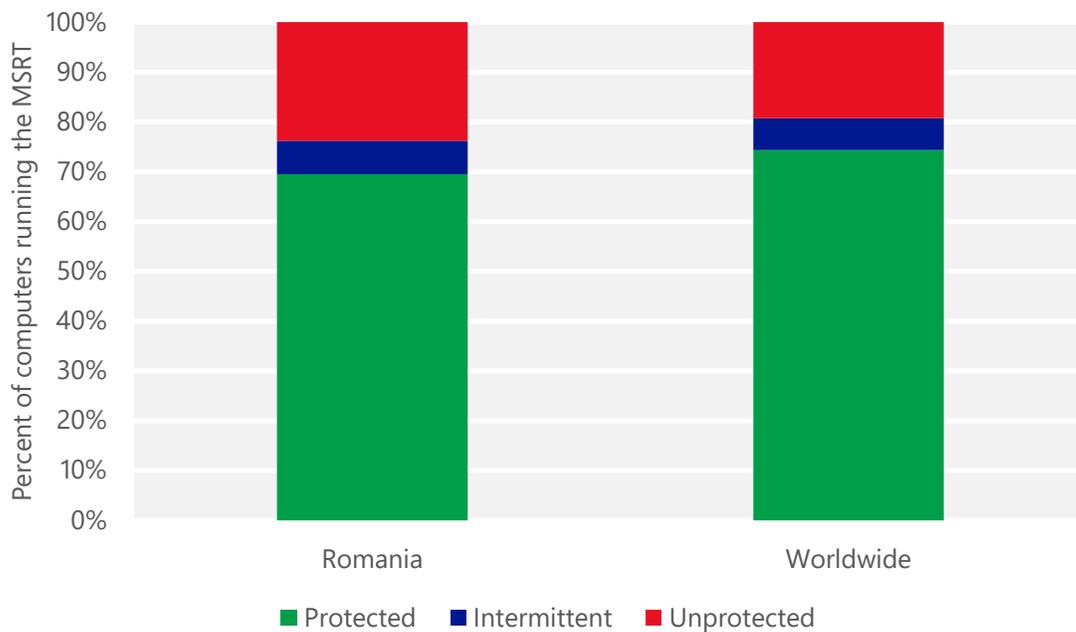
- The most common threat family infecting computers in Romania in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 4.9 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Romania in 2Q15 was [Win32/Sality](#), which was detected and removed from 4.7 of every 1,000 unique computers scanned by the MSRT. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The third most common threat family infecting computers in Romania in 2Q15 was [Win32/Kilim](#), which was detected and removed from 2.1 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The fourth most common threat family infecting computers in Romania in 2Q15 was [Win32/Ramnit](#), which was detected and removed from 2.0 of every 1,000 unique computers scanned by the MSRT. [Win32/Ramnit](#) is a family of multi-component malware that infects executable files, Microsoft Office files, and HTML files. Win32/Ramnit spreads to removable drives and steals sensitive information such as saved FTP credentials and browser cookies. It may also open a backdoor to await instructions from a remote attacker.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Romania and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Romania

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.20 (0.28)	0.17 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	6.46 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	10.80 (16.7)	

Russia

The statistics presented here are generated by Microsoft security programs and services running on computers in Russia in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Russia

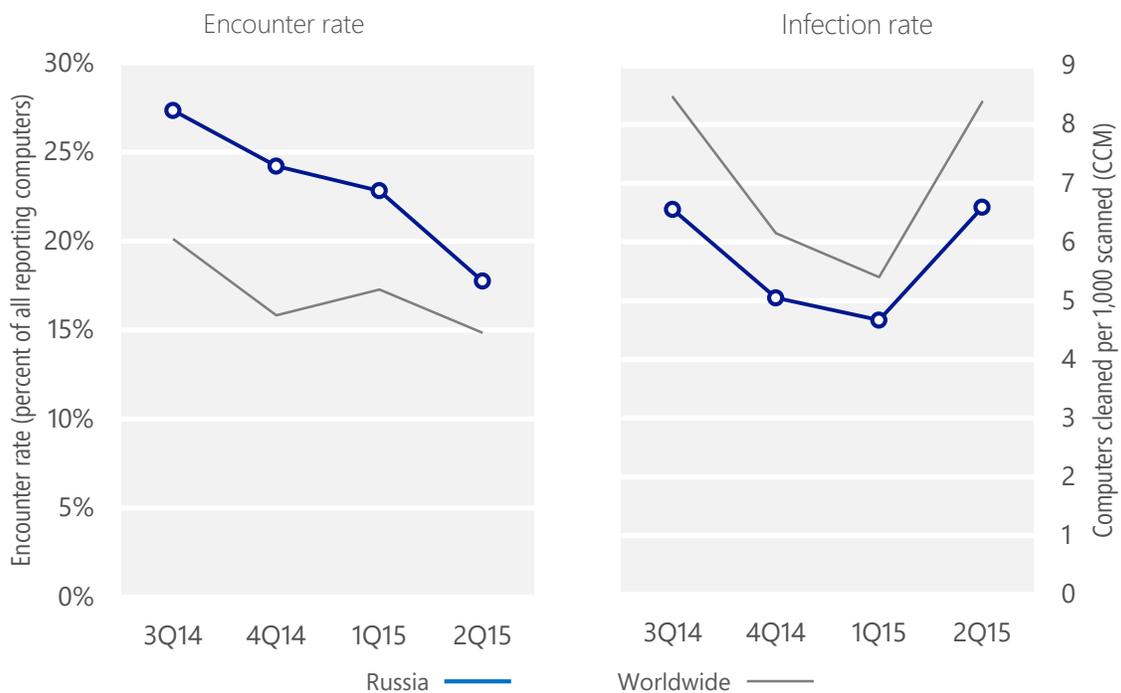
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Russia	27.3%	24.2%	22.8%	17.7%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Russia	6.6	5.0	4.7	6.6
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcote, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 17.7% of computers in Russia encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 6.6 of every 1,000 unique computers scanned in Russia in 2Q15 (a CCM score of 6.6, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Russia over the last four quarters, compared to the world as a whole.

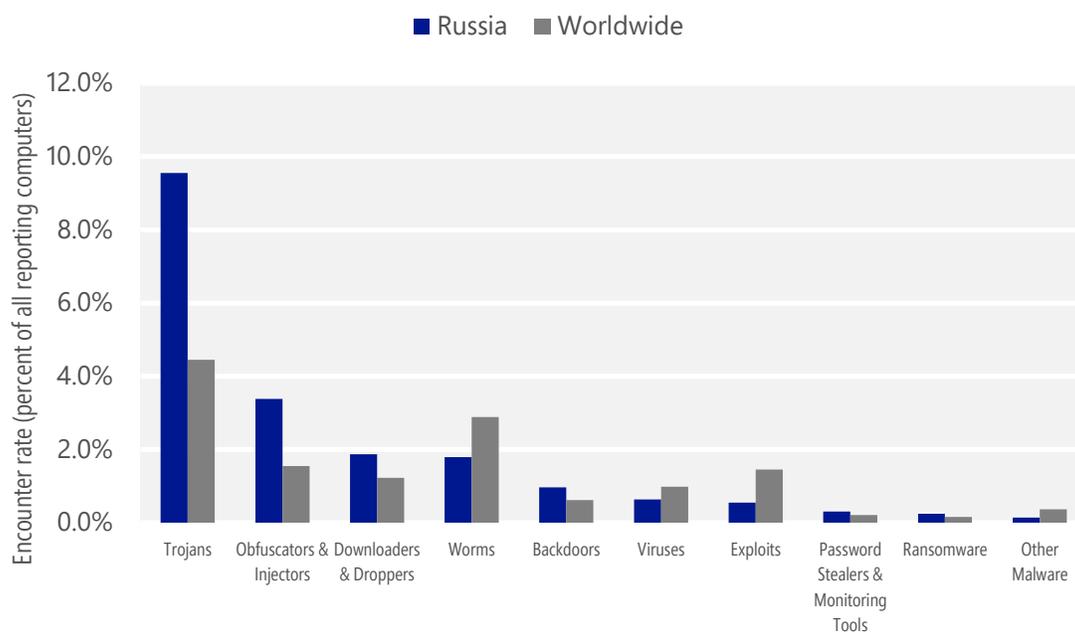
Malware encounter and infection rate trends in Russia and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in Russia and around the world, and for explanations of the methods and terms used here.

Malware categories

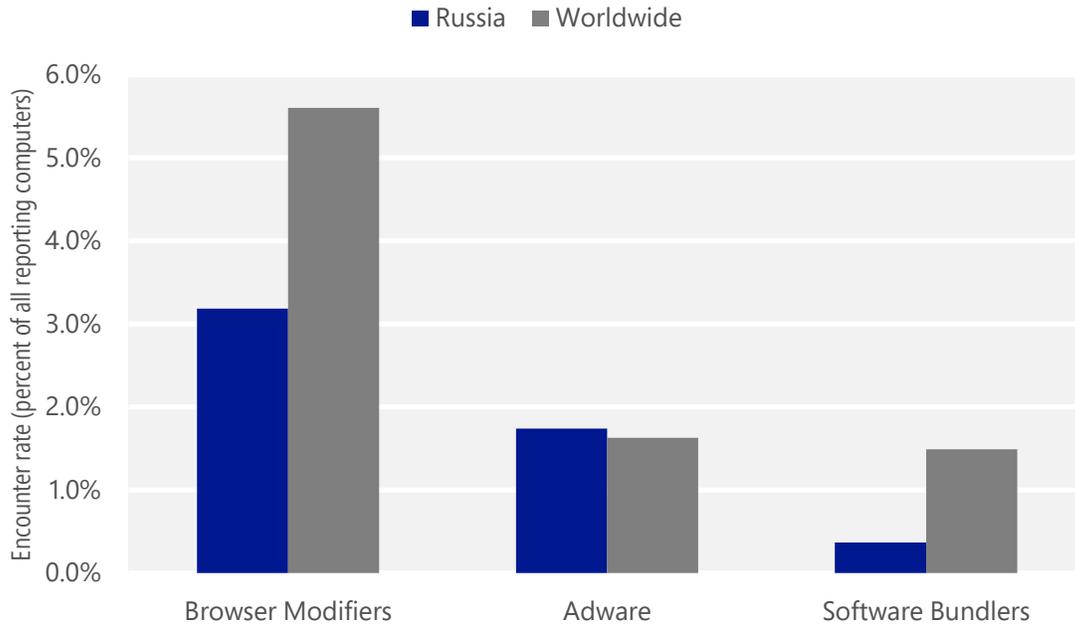
Malware encountered in Russia in 2Q15, by category



- The most common malware category in Russia in 2Q15 was Trojans. It was encountered by 9.5 percent of all computers there, down from 11.1 percent in 1Q15.
- The second most common malware category in Russia in 2Q15 was Obfuscators & Injectors. It was encountered by 3.4 percent of all computers there, down from 4.7 percent in 1Q15.
- The third most common malware category in Russia in 2Q15 was Downloaders & Droppers, which was encountered by 1.9 percent of all computers there, down from 3.9 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Russia in 2Q15, by category



- The most common unwanted software category in Russia in 2Q15 was Browser Modifiers. It was encountered by 3.2 percent of all computers there, down from 3.8 percent in 1Q15.
- The second most common unwanted software category in Russia in 2Q15 was Adware. It was encountered by 1.7 percent of all computers there, down from 3.4 percent in 1Q15.
- The third most common unwanted software category in Russia in 2Q15 was Software Bundlers, which was encountered by 0.4 percent of all computers there, up from 0.2 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Russia in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Peals	Trojans	3.1%
2	Win32/Obfuscator	Obfuscators & Injectors	3.0%
3	Win32/Skeeyah	Trojans	1.3%
4	Win32/Dynamer	Trojans	0.8%
5	Win32/Ogimant	Downloaders & Droppers	0.7%
6	Win32/Caphaw	Backdoors	0.4%
7	Win32/Radonskra	Trojans	0.4%
8	INF/Autorun	Obfuscators & Injectors	0.4%
9	Win32/Kilim	Trojans	0.3%
10	Win32/Anaki	Trojans	0.3%

- The most common malware family encountered in Russia in 2Q15 was [Win32/Peals](#), which was encountered by 3.1 percent of reporting computers there. [Win32/Peals](#) is a generic detection for various threats that display trojan characteristics.
- The second most common malware family encountered in Russia in 2Q15 was [Win32/Obfuscator](#), which was encountered by 3.0 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The third most common malware family encountered in Russia in 2Q15 was [Win32/Skeeyah](#), which was encountered by 1.3 percent of reporting computers there. [Win32/Skeeyah](#) is a generic detection for various threats that display trojan characteristics.
- The fourth most common malware family encountered in Russia in 2Q15 was [Win32/Dynamer](#), which was encountered by 0.8 percent of reporting computers there. [Win32/Dynamer](#) is a generic detection for a variety of threats.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Russia in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	1.6%
2	Win32/KipodToolsCby	Browser Modifiers	0.9%
3	Win32/EoRezo	Adware	0.7%
4	Win32/SaverExtension	Adware	0.6%
5	Win32/AlterbookSP	Browser Modifiers	0.6%

- The most common unwanted software family encountered in Russia in 2Q15 was [Win32/CouponRuc](#), which was encountered by 1.6 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in Russia in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 0.9 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common unwanted software family encountered in Russia in 2Q15 was [Win32/EoRezo](#), which was encountered by 0.7 percent of reporting computers there. [Win32/EoRezo](#) is adware that displays targeted advertising to affected users while browsing the Internet, based on downloaded pre-configured information.

Top threat families by infection rate

The most common malware families by infection rate in Russia in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	1.5
2	Win32/Kilim	Trojans	1.0
3	Win32/CompromisedCert	Other Malware	0.8
4	Win32/Dorkbot	Worms	0.5
5	Win32/Gamarue	Worms	0.5
6	Win32/Ramnit	Trojans	0.5
7	Win32/Brontok	Worms	0.4
8	Win32/Sality	Viruses	0.2
9	VBS/Jenxcus	Worms	0.2
10	Win32/Lethic	Trojans	0.2

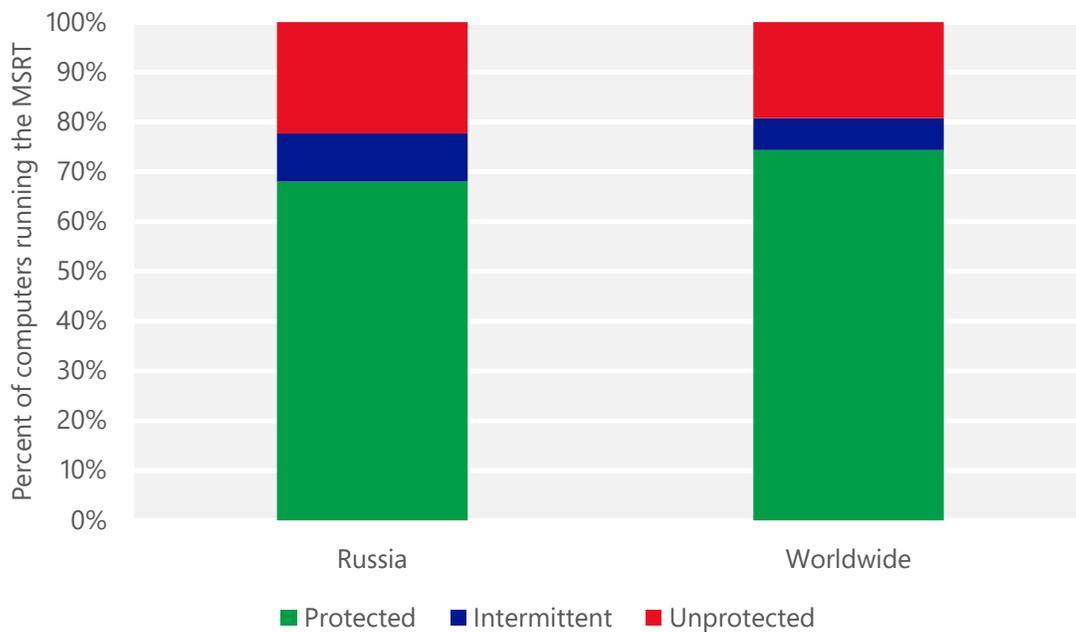
- The most common threat family infecting computers in Russia in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 1.5 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Russia in 2Q15 was [Win32/Kilim](#), which was detected and removed from 1.0 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The third most common threat family infecting computers in Russia in 2Q15 was [Win32/CompromisedCert](#), which was detected and removed from 0.8 of every 1,000 unique computers scanned by the MSRT. [Win32/CompromisedCert](#) is a detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.
- The fourth most common threat family infecting computers in Russia in 2Q15 was [Win32/Dorkbot](#), which was detected and removed from 0.5 of every 1,000 unique computers scanned by the MSRT. [Win32/Dorkbot](#) is a worm that spreads via instant messaging and removable drives. It also contains backdoor functionality that allows unauthorized access and control of the affected computer. Win32/Dorkbot may be distributed from compromised or malicious websites using PDF or browser exploits.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Russia and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Russia

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	1.97 (0.28)	1.72 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	7.50 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	23.92 (16.7)	

Saudi Arabia

The statistics presented here are generated by Microsoft security programs and services running on computers in Saudi Arabia in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Saudi Arabia

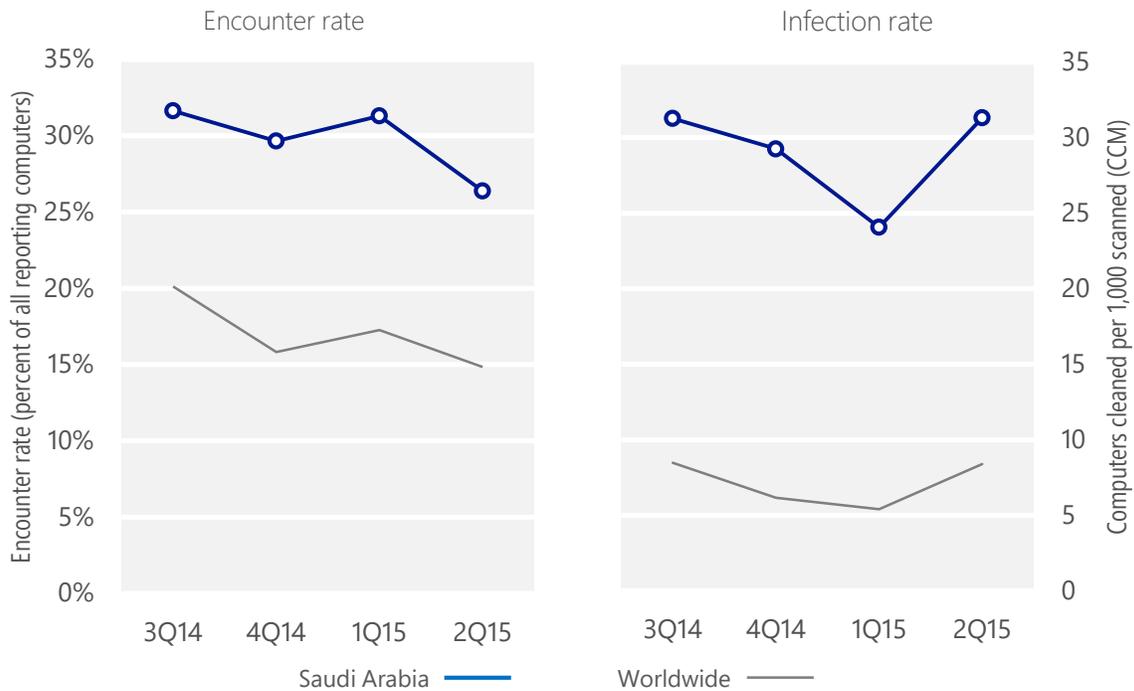
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Saudi Arabia	31.6%	29.7%	31.3%	26.4%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Saudi Arabia	31.3	29.3	24.1	31.3
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcoute, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 26.4% of computers in Saudi Arabia encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 31.3 of every 1,000 unique computers scanned in Saudi Arabia in 2Q15 (a CCM score of 31.3, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Saudi Arabia over the last four quarters, compared to the world as a whole.

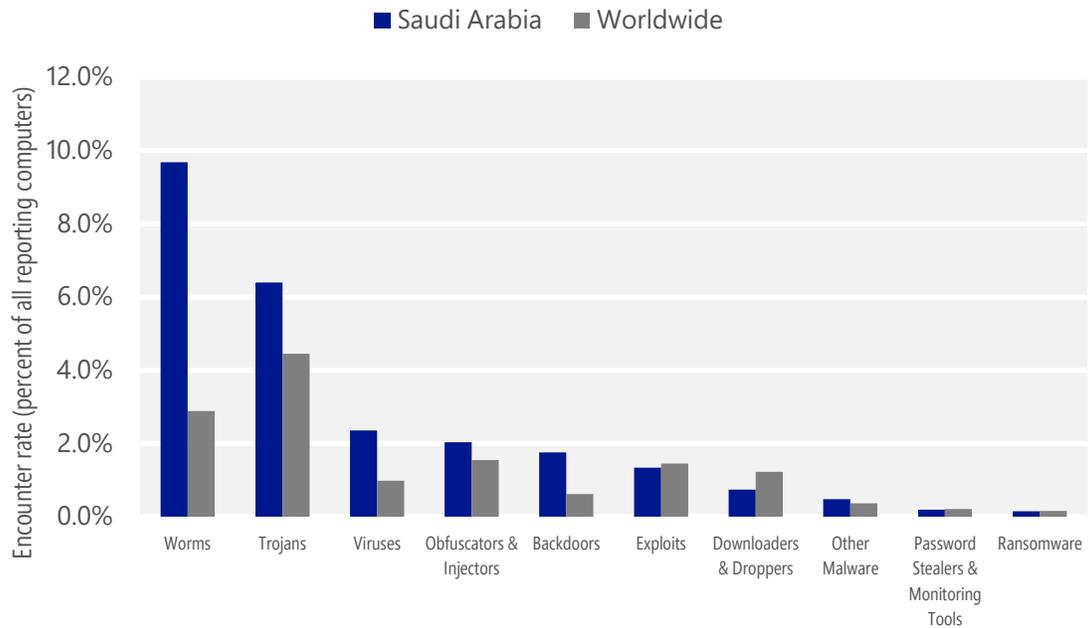
Malware encounter and infection rate trends in Saudi Arabia and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in Saudi Arabia and around the world, and for explanations of the methods and terms used here.

Malware categories

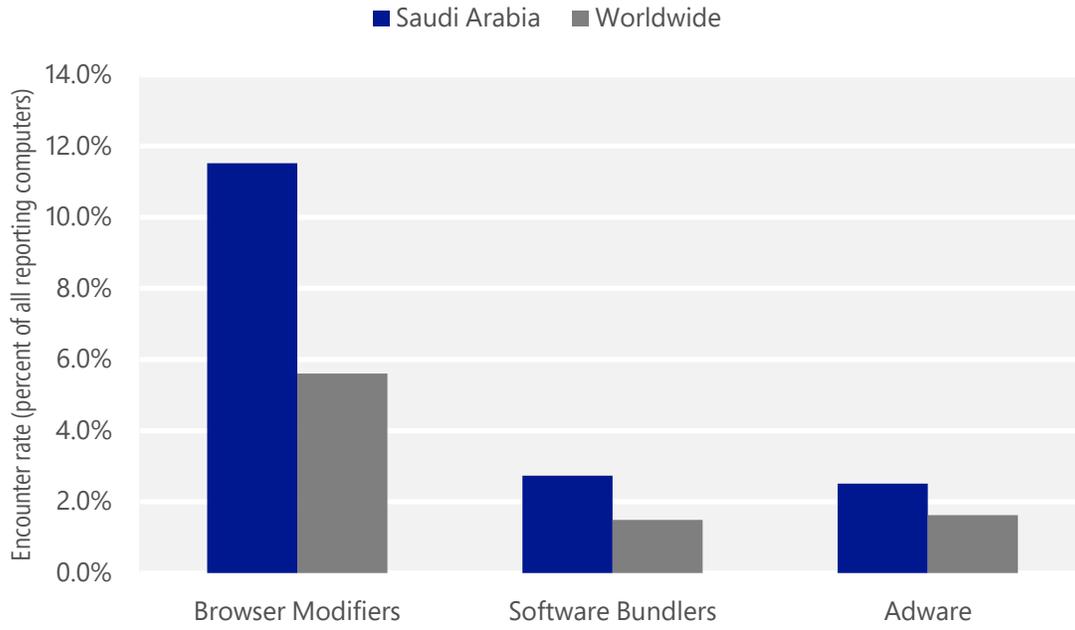
Malware encountered in Saudi Arabia in 2Q15, by category



- The most common malware category in Saudi Arabia in 2Q15 was Worms. It was encountered by 9.7 percent of all computers there, down from 10.0 percent in 1Q15.
- The second most common malware category in Saudi Arabia in 2Q15 was Trojans. It was encountered by 6.4 percent of all computers there, up from 5.6 percent in 1Q15.
- The third most common malware category in Saudi Arabia in 2Q15 was Viruses, which was encountered by 2.4 percent of all computers there, down from 2.8 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Saudi Arabia in 2Q15, by category



- The most common unwanted software category in Saudi Arabia in 2Q15 was Browser Modifiers. It was encountered by 11.5 percent of all computers there, down from 15.6 percent in 1Q15.
- The second most common unwanted software category in Saudi Arabia in 2Q15 was Software Bundlers. It was encountered by 2.7 percent of all computers there, down from 6.2 percent in 1Q15.
- The third most common unwanted software category in Saudi Arabia in 2Q15 was Adware, which was encountered by 2.5 percent of all computers there, up from 1.3 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Saudi Arabia in 2Q15

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	4.4%
2	JS/Bondat	Worms	2.5%
3	Win32/Skeeyah	Trojans	1.5%
4	INF/Autorun	Obfuscators & Injectors	1.3%
5	Win32/Kilim	Trojans	1.0%
6	Win32/Obfuscator	Obfuscators & Injectors	1.0%
7	Win32/Sality	Viruses	0.8%
8	MSIL/Bladabindi	Backdoors	0.8%
9	Win32/Peals	Trojans	0.8%
10	Win32/CplLnk	Exploits	0.6%

- The most common malware family encountered in Saudi Arabia in 2Q15 was [VBS/Jenxcus](#), which was encountered by 4.4 percent of reporting computers there. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common malware family encountered in Saudi Arabia in 2Q15 was [JS/Bondat](#), which was encountered by 2.5 percent of reporting computers there. [JS/Bondat](#) is a family of threats that collects information about the computer, infects removable drives, and tries to stop the user from accessing files. It spreads by infecting removable drives, such as USB thumb drives and flash drives.
- The third most common malware family encountered in Saudi Arabia in 2Q15 was [Win32/Skeeyah](#), which was encountered by 1.5 percent of reporting computers there. [Win32/Skeeyah](#) is a generic detection for various threats that display trojan characteristics.
- The fourth most common malware family encountered in Saudi Arabia in 2Q15 was [INF/Autorun](#), which was encountered by 1.3 percent of reporting computers there. [INF/Autorun](#) is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Saudi Arabia in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/KipodToolsCby	Browser Modifiers	5.6%
2	Win32/CouponRuc	Browser Modifiers	4.8%
3	Win32/InstalleRex	Software Bundlers	2.6%
4	Win32/SaverExtension	Adware	1.6%
5	Win32/Vonteera	Browser Modifiers	1.2%

- The most common unwanted software family encountered in Saudi Arabia in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 5.6 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common unwanted software family encountered in Saudi Arabia in 2Q15 was [Win32/CouponRuc](#), which was encountered by 4.8 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The third most common unwanted software family encountered in Saudi Arabia in 2Q15 was [Win32/InstalleRex](#), which was encountered by 2.6 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Saudi Arabia in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	10.6
2	Win32/leEnablerCby	Browser Modifiers	8.9
3	Win32/Sality	Viruses	3.1
4	Win32/Kilim	Trojans	1.9
5	MSIL/Bladabindi	Backdoors	1.8
6	Win32/Ramnit	Trojans	1.1
7	Win32/CompromisedCert	Other Malware	1.0
8	Win32/Gamarue	Worms	1.0
9	Win32/Nuqel	Worms	0.6
10	Win32/Dorkbot	Worms	0.5

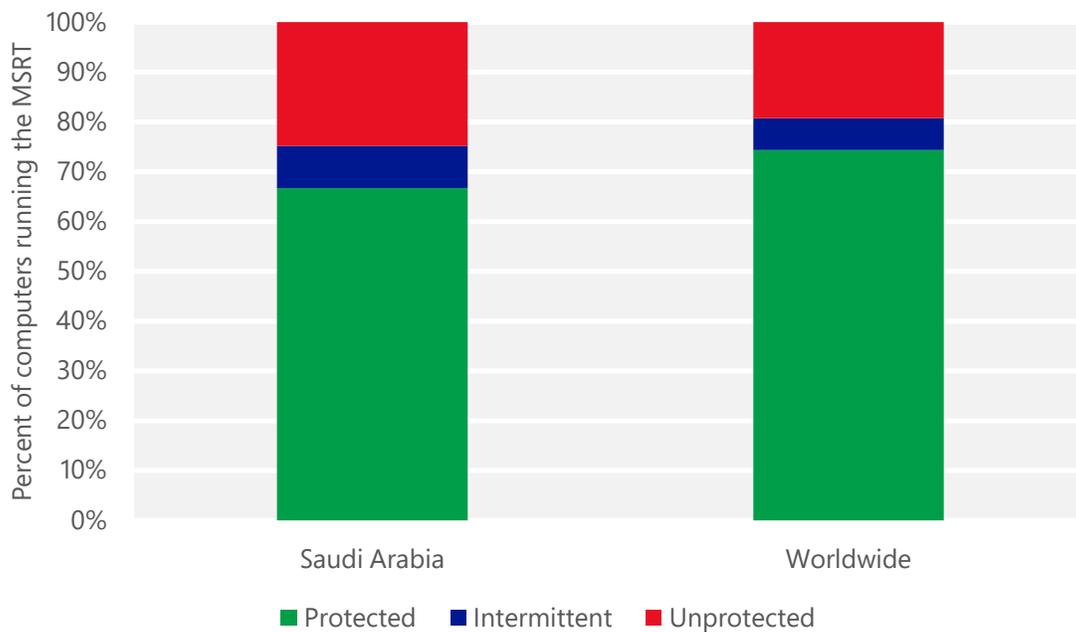
- The most common threat family infecting computers in Saudi Arabia in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 10.6 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Saudi Arabia in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 8.9 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common threat family infecting computers in Saudi Arabia in 2Q15 was [Win32/Sality](#), which was detected and removed from 3.1 of every 1,000 unique computers scanned by the MSRT. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The fourth most common threat family infecting computers in Saudi Arabia in 2Q15 was [Win32/Kilim](#), which was detected and removed from 1.9 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Saudi Arabia and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Saudi Arabia

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.16 (0.28)	0.07 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	2.18 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	4.29 (16.7)	

Senegal

The statistics presented here are generated by Microsoft security programs and services running on computers in Senegal in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Senegal

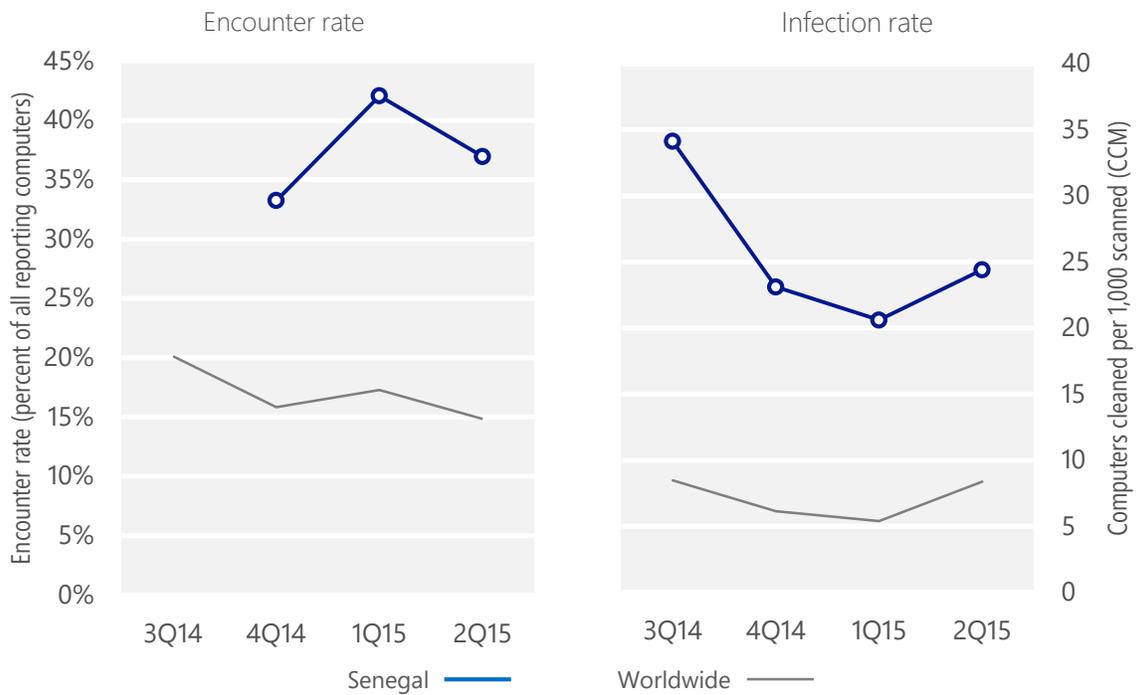
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Senegal	N/A	33.2%	42.1%	37.0%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Senegal	34.1	23.1	20.6	24.4
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcoute, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 37.0% of computers in Senegal encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 24.4 of every 1,000 unique computers scanned in Senegal in 2Q15 (a CCM score of 24.4, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Senegal over the last four quarters, compared to the world as a whole.

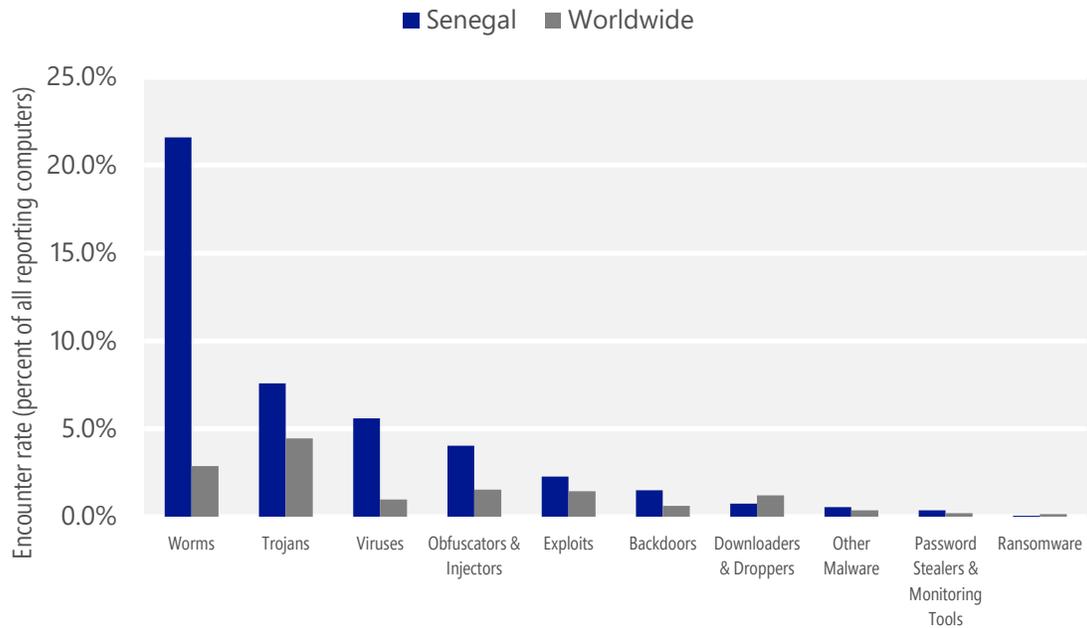
Malware encounter and infection rate trends in Senegal and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in Senegal and around the world, and for explanations of the methods and terms used here.

Malware categories

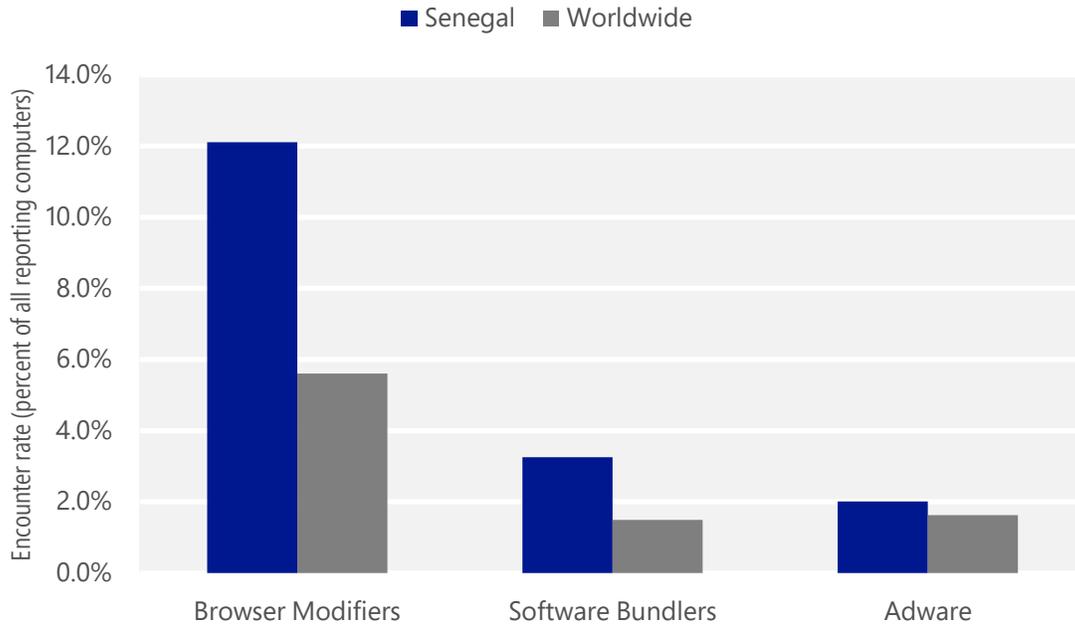
Malware encountered in Senegal in 2Q15, by category



- The most common malware category in Senegal in 2Q15 was Worms. It was encountered by 21.6 percent of all computers there, down from 21.7 percent in 1Q15.
- The second most common malware category in Senegal in 2Q15 was Trojans. It was encountered by 7.6 percent of all computers there, up from 7.1 percent in 1Q15.
- The third most common malware category in Senegal in 2Q15 was Viruses, which was encountered by 5.6 percent of all computers there, down from 6.1 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Senegal in 2Q15, by category



- The most common unwanted software category in Senegal in 2Q15 was Browser Modifiers. It was encountered by 12.1 percent of all computers there, down from 19.6 percent in 1Q15.
- The second most common unwanted software category in Senegal in 2Q15 was Software Bundlers. It was encountered by 3.3 percent of all computers there, down from 4.3 percent in 1Q15.
- The third most common unwanted software category in Senegal in 2Q15 was Adware, which was encountered by 2.0 percent of all computers there, up from 1.3 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Senegal in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Ippedo	Worms	7.6%
2	VBS/Jenxcus	Worms	6.9%
3	Win32/Macoute	Worms	6.5%
4	INF/Autorun	Obfuscators & Injectors	4.5%
5	VBS/Cantix	Worms	4.0%
6	Win32/Sality	Viruses	2.8%
7	Win32/Virut	Viruses	2.3%
8	Win32/Ramnit	Trojans	2.0%
9	VBS/Rtbot	Worms	1.9%
10	Win32/Gamarue	Worms	1.8%

- The most common malware family encountered in Senegal in 2Q15 was [Win32/Ippedo](#), which was encountered by 7.6 percent of reporting computers there. [Win32/Ippedo](#) is a worm that can send sensitive information to a malicious hacker. It spreads through removable drives, such as USB flash drives.
- The second most common malware family encountered in Senegal in 2Q15 was [VBS/Jenxcus](#), which was encountered by 6.9 percent of reporting computers there. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The third most common malware family encountered in Senegal in 2Q15 was [Win32/Macoute](#), which was encountered by 6.5 percent of reporting computers there. [Win32/Macoute](#) is a worm that can spread itself to removable USB drives, and may communicate with a remote host.
- The fourth most common malware family encountered in Senegal in 2Q15 was [INF/Autorun](#), which was encountered by 4.5 percent of reporting computers there. [INF/Autorun](#) is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Senegal in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/KipodToolsCby	Browser Modifiers	8.3%
2	Win32/CouponRuc	Browser Modifiers	3.9%
3	Win32/InstalleRex	Software Bundlers	3.1%
4	Win32/SaverExtension	Adware	1.3%
5	Win32/AlterbookSP	Browser Modifiers	0.5%

- The most common unwanted software family encountered in Senegal in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 8.3 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common unwanted software family encountered in Senegal in 2Q15 was [Win32/CouponRuc](#), which was encountered by 3.9 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The third most common unwanted software family encountered in Senegal in 2Q15 was [Win32/InstalleRex](#), which was encountered by 3.1 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Senegal in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	6.6
2	Win32/Sality	Viruses	5.4
3	Win32/leEnablerCby	Browser Modifiers	5.2
4	Win32/Gamarue	Worms	1.9
5	Win32/Ramnit	Trojans	1.7
6	Win32/Virut	Viruses	1.4
7	Win32/Kilim	Trojans	1.2
8	Win32/Chir	Viruses	0.8
9	MSIL/Bladabindi	Backdoors	0.7
10	Win32/Pramro	Trojans	0.4

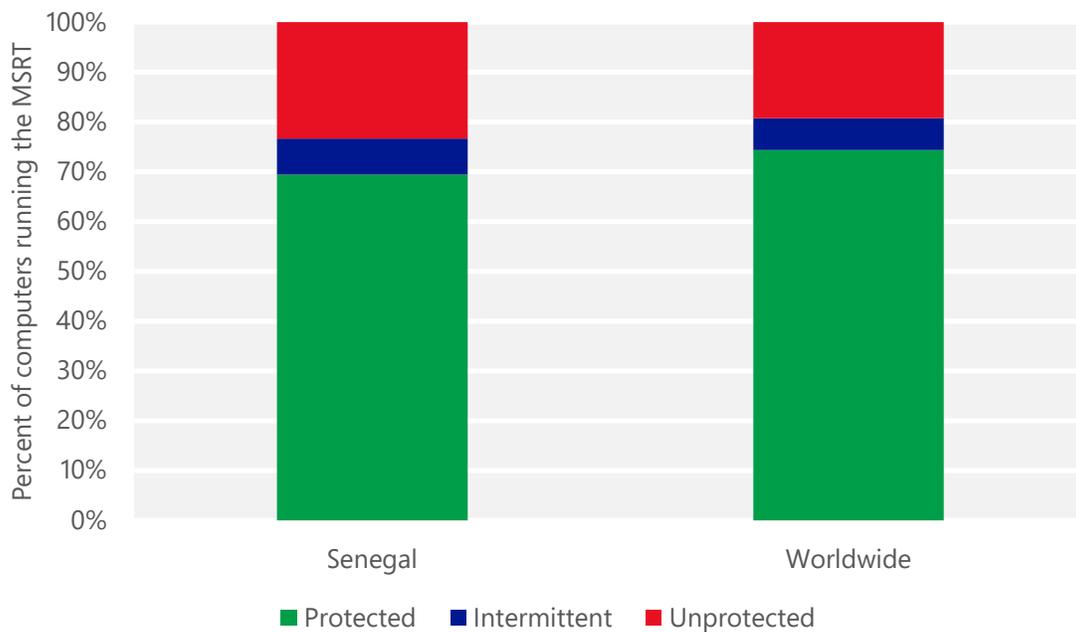
- The most common threat family infecting computers in Senegal in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 6.6 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Senegal in 2Q15 was [Win32/Sality](#), which was detected and removed from 5.4 of every 1,000 unique computers scanned by the MSRT. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The third most common threat family infecting computers in Senegal in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 5.2 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The fourth most common threat family infecting computers in Senegal in 2Q15 was [Win32/Gamarue](#), which was detected and removed from 1.9 of every 1,000 unique computers scanned by the MSRT. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Senegal and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Senegal

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.09 (0.28)	0.09 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	2.81 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	18.28 (16.7)	

Serbia

The statistics presented here are generated by Microsoft security programs and services running on computers in Serbia in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Serbia

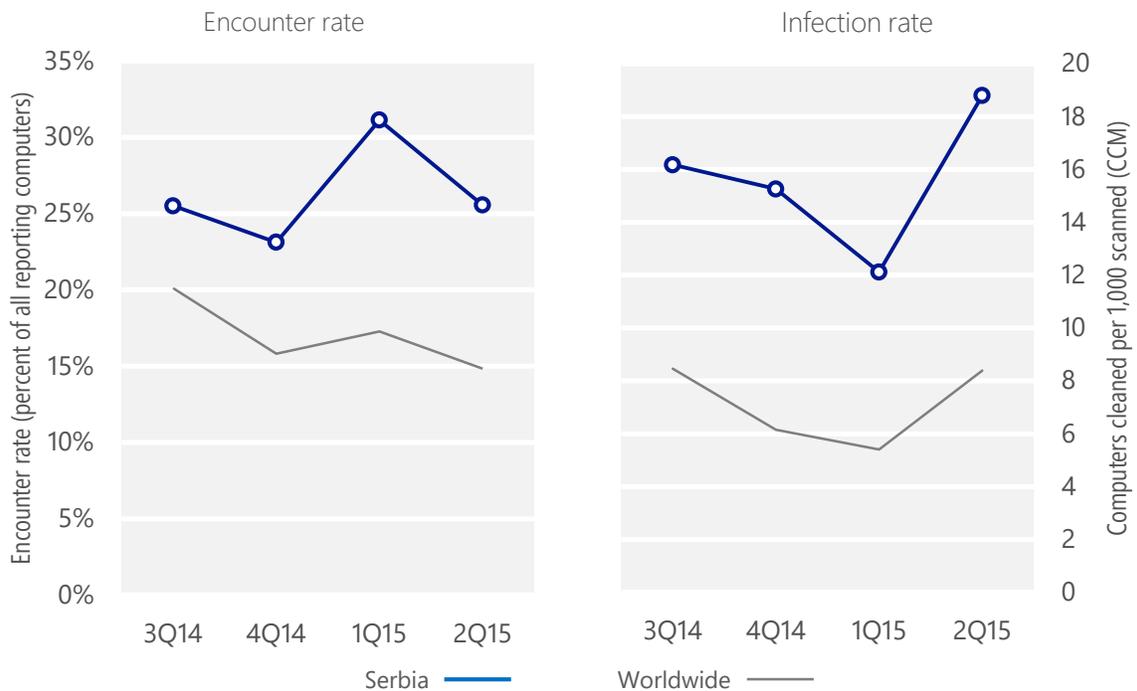
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Serbia	25.5%	23.1%	31.1%	25.6%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Serbia	16.2	15.3	12.1	18.8
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcote, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 25.6% of computers in Serbia encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 18.8 of every 1,000 unique computers scanned in Serbia in 2Q15 (a CCM score of 18.8, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Serbia over the last four quarters, compared to the world as a whole.

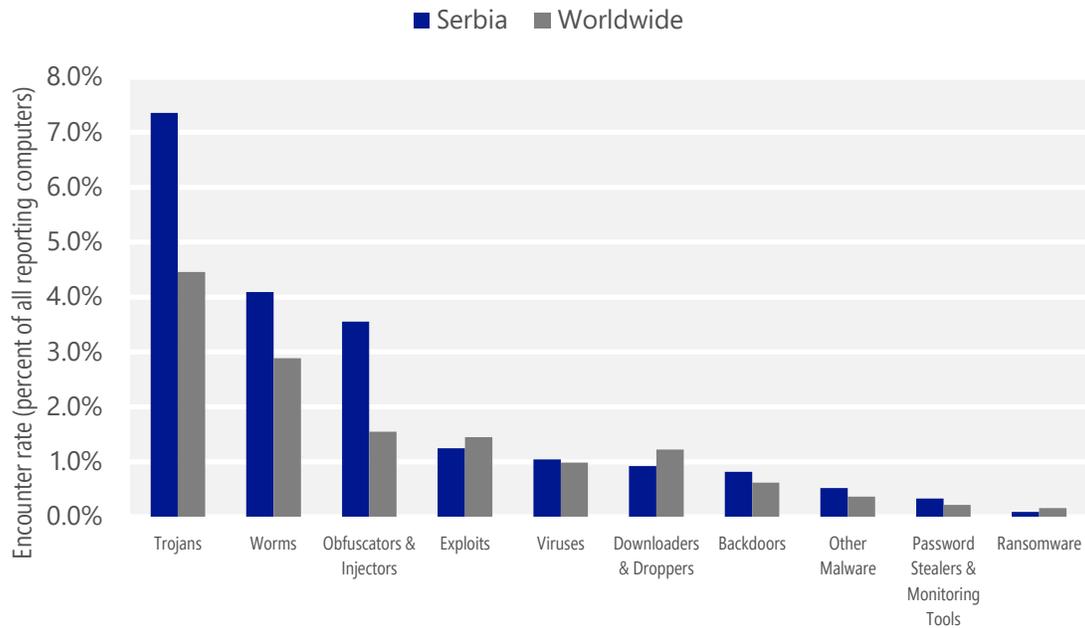
Malware encounter and infection rate trends in Serbia and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in Serbia and around the world, and for explanations of the methods and terms used here.

Malware categories

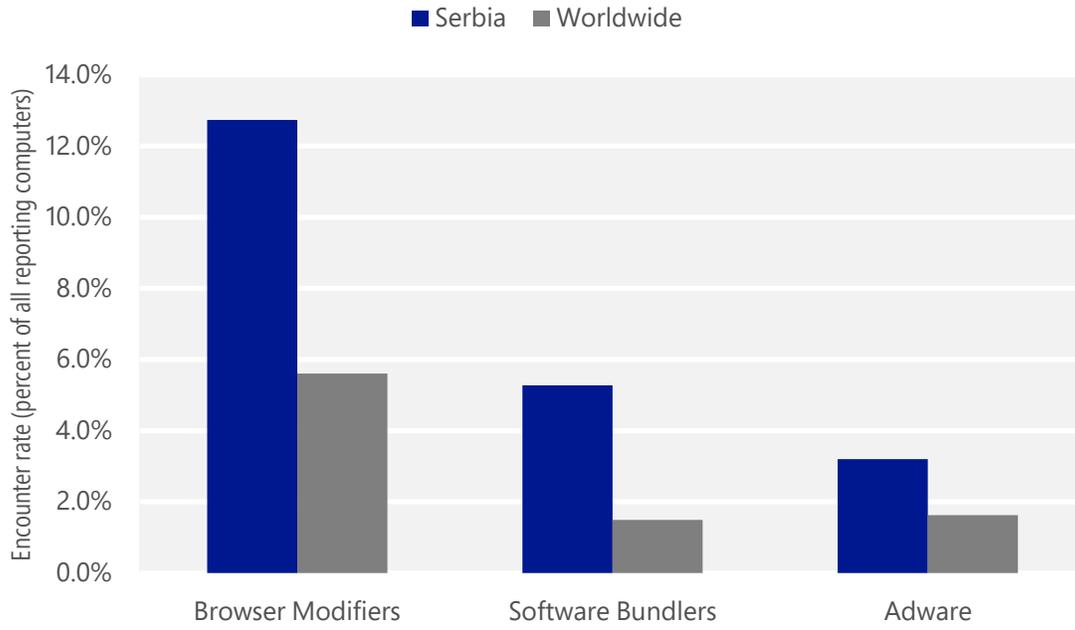
Malware encountered in Serbia in 2Q15, by category



- The most common malware category in Serbia in 2Q15 was Trojans. It was encountered by 7.4 percent of all computers there, up from 5.8 percent in 1Q15.
- The second most common malware category in Serbia in 2Q15 was Worms. It was encountered by 4.1 percent of all computers there, down from 5.4 percent in 1Q15.
- The third most common malware category in Serbia in 2Q15 was Obfuscators & Injectors, which was encountered by 3.6 percent of all computers there, down from 4.1 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Serbia in 2Q15, by category



- The most common unwanted software category in Serbia in 2Q15 was Browser Modifiers. It was encountered by 12.7 percent of all computers there, down from 18.3 percent in 1Q15.
- The second most common unwanted software category in Serbia in 2Q15 was Software Bundlers. It was encountered by 5.3 percent of all computers there, down from 7.8 percent in 1Q15.
- The third most common unwanted software category in Serbia in 2Q15 was Adware, which was encountered by 3.2 percent of all computers there, up from 1.7 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Serbia in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Obfuscator	Obfuscators & Injectors	2.4%
2	Win32/Kilim	Trojans	2.3%
3	Win32/Skeeyah	Trojans	1.4%
4	Win32/Gamarue	Worms	1.2%
5	INF/Autorun	Obfuscators & Injectors	1.1%
6	VBS/Jenxcus	Worms	1.0%
7	Win32/Sality	Viruses	0.7%
8	Win32/Peals	Trojans	0.6%
9	Win32/Helompy	Worms	0.6%
10	Win32/Sdbby	Exploits	0.5%

- The most common malware family encountered in Serbia in 2Q15 was [Win32/Obfuscator](#), which was encountered by 2.4 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The second most common malware family encountered in Serbia in 2Q15 was [Win32/Kilim](#), which was encountered by 2.3 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The third most common malware family encountered in Serbia in 2Q15 was [Win32/Skeeyah](#), which was encountered by 1.4 percent of reporting computers there. [Win32/Skeeyah](#) is a generic detection for various threats that display trojan characteristics.
- The fourth most common malware family encountered in Serbia in 2Q15 was [Win32/Gamarue](#), which was encountered by 1.2 percent of reporting computers there. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Serbia in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	7.7%
2	Win32/InstalleRex	Software Bundlers	5.1%
3	Win32/KipodToolsCby	Browser Modifiers	4.8%
4	Win32/SaverExtension	Adware	2.4%
5	Win32/AlterbookSP	Browser Modifiers	0.9%

- The most common unwanted software family encountered in Serbia in 2Q15 was [Win32/CouponRuc](#), which was encountered by 7.7 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in Serbia in 2Q15 was [Win32/InstalleRex](#), which was encountered by 5.1 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.
- The third most common unwanted software family encountered in Serbia in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 4.8 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.

Top threat families by infection rate

The most common malware families by infection rate in Serbia in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	6.1
2	Win32/Sality	Viruses	3.5
3	Win32/Kilim	Trojans	2.7
4	VBS/Jenxcus	Worms	1.4
5	Win32/Helompy	Worms	1.4
6	Win32/Gamarue	Worms	0.9
7	Win32/CompromisedCert	Other Malware	0.6
8	Win32/Pramro	Trojans	0.5
9	MSIL/Bladabindi	Backdoors	0.5
10	Win32/Simda	Trojans	0.4

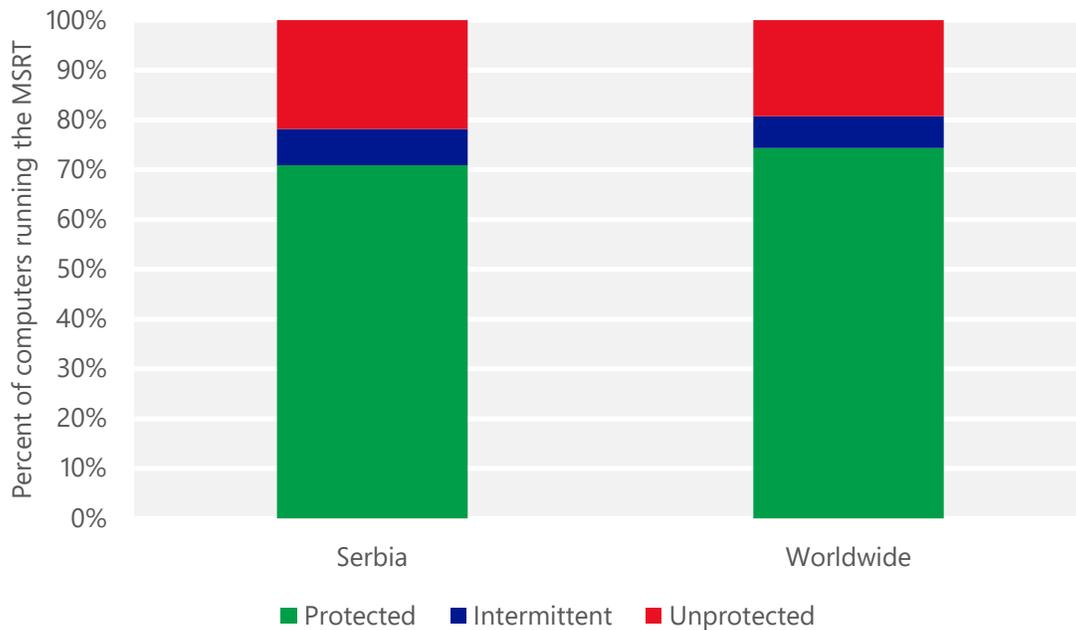
- The most common threat family infecting computers in Serbia in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 6.1 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Serbia in 2Q15 was [Win32/Sality](#), which was detected and removed from 3.5 of every 1,000 unique computers scanned by the MSRT. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The third most common threat family infecting computers in Serbia in 2Q15 was [Win32/Kilim](#), which was detected and removed from 2.7 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The fourth most common threat family infecting computers in Serbia in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 1.4 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Serbia and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Serbia

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.03 (0.28)	0.05 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	6.64 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	21.30 (16.7)	

Singapore

The statistics presented here are generated by Microsoft security programs and services running on computers in Singapore in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Singapore

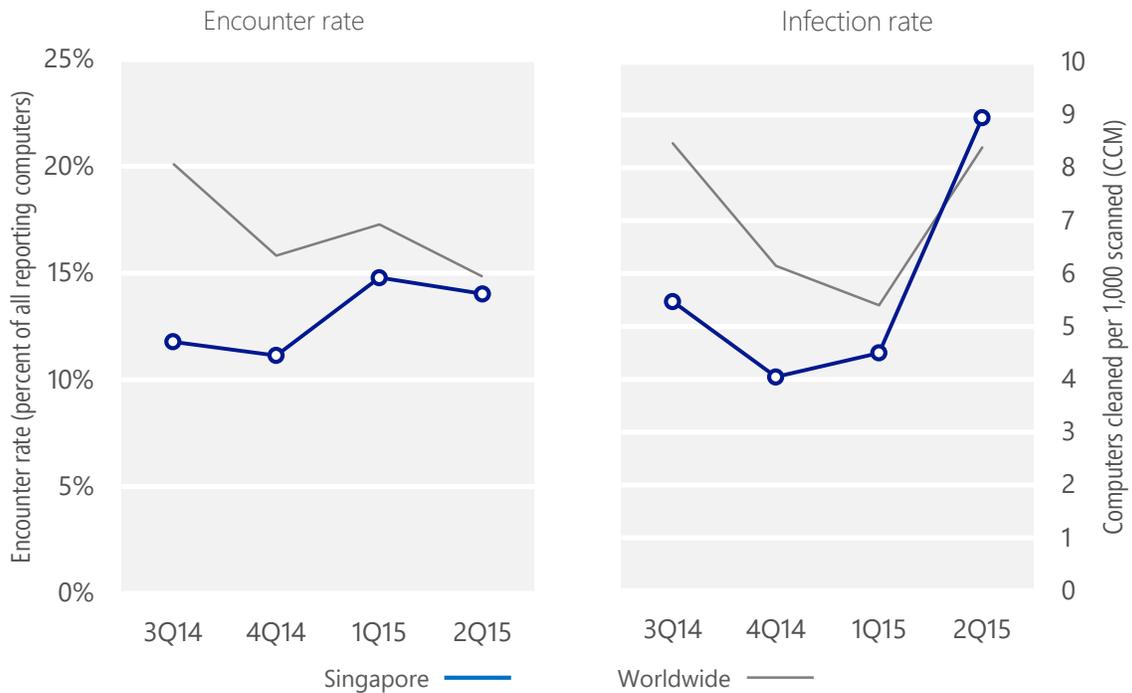
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Singapore	11.8%	11.1%	14.8%	14.0%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Singapore	5.5	4.0	4.5	8.9
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcote, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 14.0% of computers in Singapore encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 8.9 of every 1,000 unique computers scanned in Singapore in 2Q15 (a CCM score of 8.9, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Singapore over the last four quarters, compared to the world as a whole.

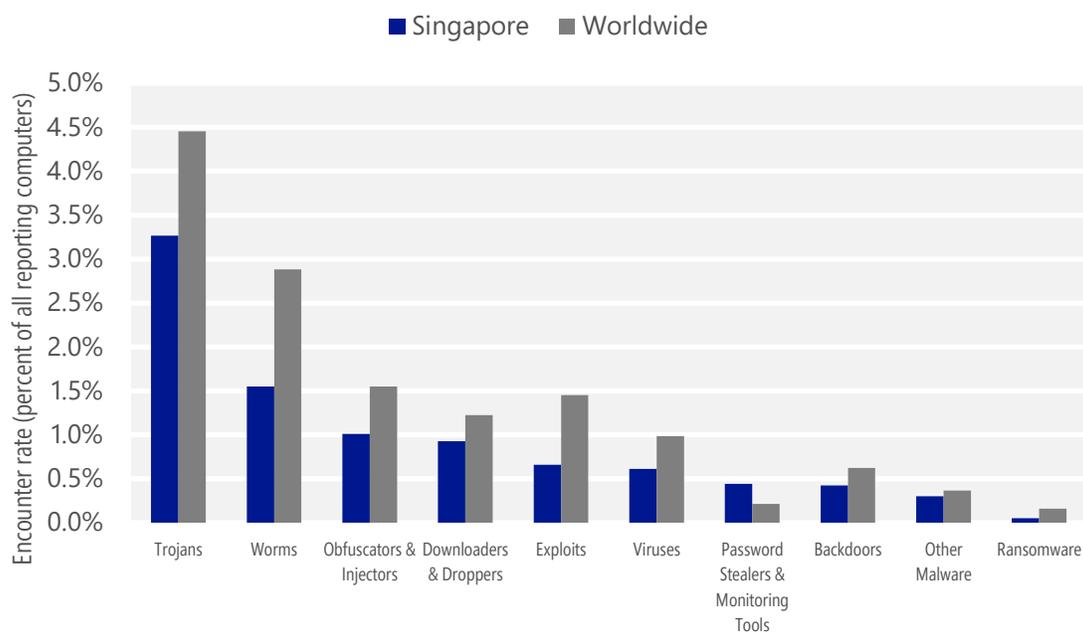
Malware encounter and infection rate trends in Singapore and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in Singapore and around the world, and for explanations of the methods and terms used here.

Malware categories

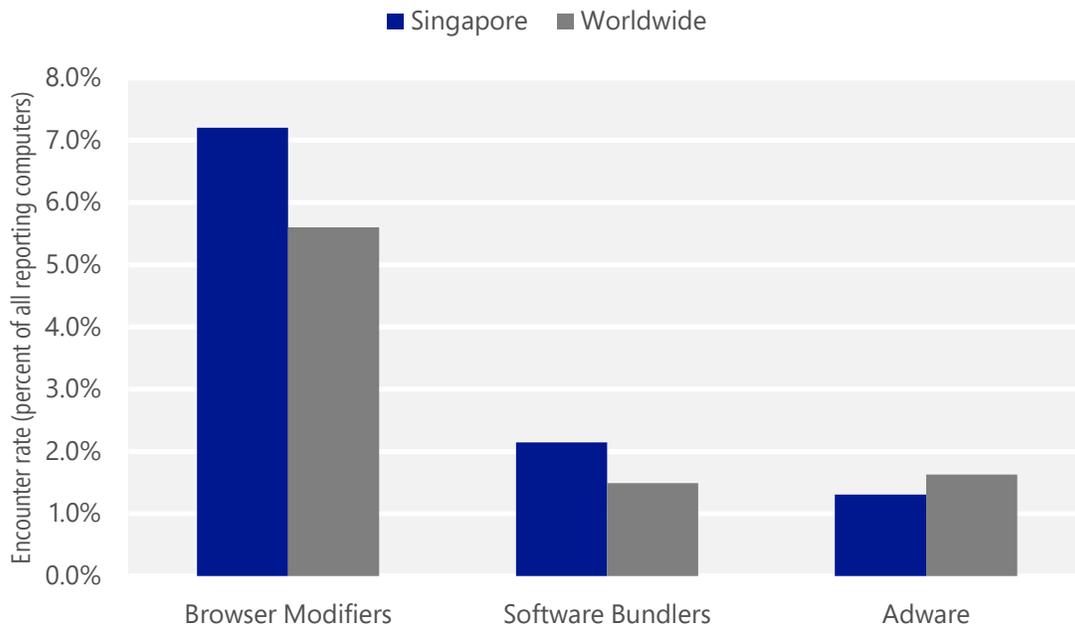
Malware encountered in Singapore in 2Q15, by category



- The most common malware category in Singapore in 2Q15 was Trojans. It was encountered by 3.3 percent of all computers there, up from 2.1 percent in 1Q15.
- The second most common malware category in Singapore in 2Q15 was Worms. It was encountered by 1.5 percent of all computers there, down from 2.1 percent in 1Q15.
- The third most common malware category in Singapore in 2Q15 was Obfuscators & Injectors, which was encountered by 1.0 percent of all computers there, down from 1.2 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Singapore in 2Q15, by category



- The most common unwanted software category in Singapore in 2Q15 was Browser Modifiers. It was encountered by 7.2 percent of all computers there, down from 8.1 percent in 1Q15.
- The second most common unwanted software category in Singapore in 2Q15 was Software Bundlers. It was encountered by 2.1 percent of all computers there, down from 3.3 percent in 1Q15.
- The third most common unwanted software category in Singapore in 2Q15 was Adware, which was encountered by 1.3 percent of all computers there, up from 0.6 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Singapore in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Obfuscator	Obfuscators & Injectors	0.7%
2	Win32/Kilim	Trojans	0.7%
3	Win32/Skeeyah	Trojans	0.5%
4	Win32/Peals	Trojans	0.5%
5	INF/Autorun	Obfuscators & Injectors	0.4%
6	Win32/Upatre	Downloaders & Droppers	0.4%
7	VBS/Jenxcus	Worms	0.2%
8	Win32/Gamarue	Worms	0.2%
9	JS/Axpergle	Exploits	0.2%
10	Win32/Dynamer	Trojans	0.2%

- The most common malware family encountered in Singapore in 2Q15 was [Win32/Obfuscator](#), which was encountered by 0.7 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The second most common malware family encountered in Singapore in 2Q15 was [Win32/Kilim](#), which was encountered by 0.7 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The third most common malware family encountered in Singapore in 2Q15 was [Win32/Skeeyah](#), which was encountered by 0.5 percent of reporting computers there. [Win32/Skeeyah](#) is a generic detection for various threats that display trojan characteristics.
- The fourth most common malware family encountered in Singapore in 2Q15 was [Win32/Peals](#), which was encountered by 0.5 percent of reporting computers there. [Win32/Peals](#) is a generic detection for various threats that display trojan characteristics.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Singapore in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	3.1%
2	Win32/KipodToolsCby	Browser Modifiers	2.9%
3	Win32/InstalleRex	Software Bundlers	2.0%
4	Win32/AlterbookSP	Browser Modifiers	1.1%
5	Win32/SaverExtension	Adware	1.0%

- The most common unwanted software family encountered in Singapore in 2Q15 was [Win32/CouponRuc](#), which was encountered by 3.1 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in Singapore in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 2.9 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common unwanted software family encountered in Singapore in 2Q15 was [Win32/InstalleRex](#), which was encountered by 2.0 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Singapore in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	2.8
2	Win32/CompromisedCert	Other Malware	1.3
3	Win32/Kilim	Trojans	1.3
4	Win32/Dyzap	Password Stealers & Monitoring Tools	0.6
5	VBS/Jenxcus	Worms	0.4
6	Win32/Gamarue	Worms	0.3
7	Win32/Sality	Viruses	0.2
8	Win32/Ramnit	Trojans	0.2
9	Win32/Brontok	Worms	0.2
10	Win32/Simda	Trojans	0.2

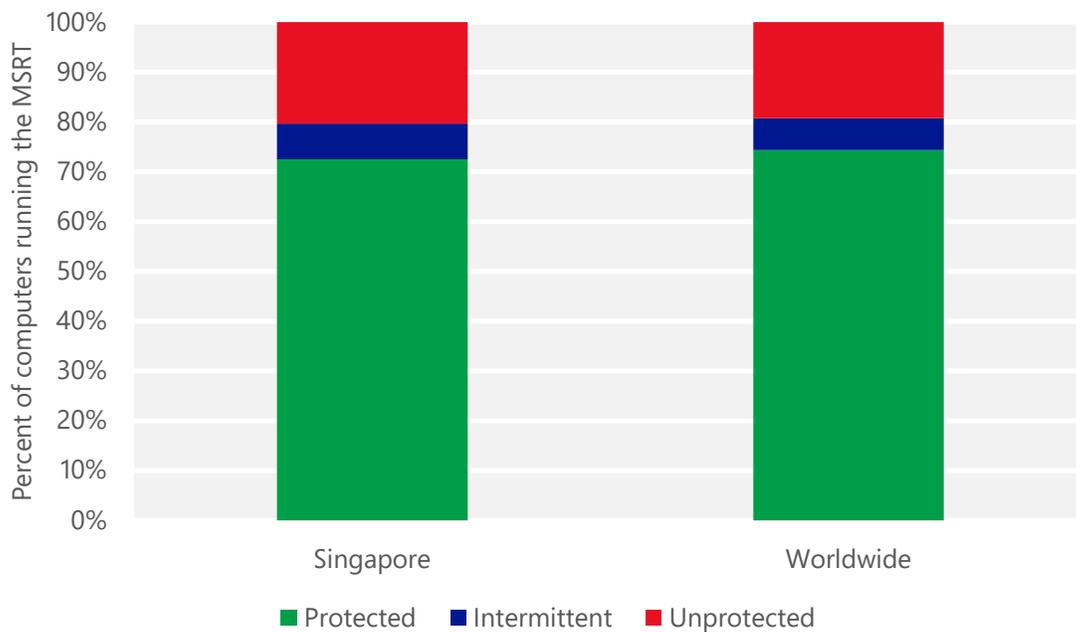
- The most common threat family infecting computers in Singapore in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 2.8 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Singapore in 2Q15 was [Win32/CompromisedCert](#), which was detected and removed from 1.3 of every 1,000 unique computers scanned by the MSRT. [Win32/CompromisedCert](#) is a detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.
- The third most common threat family infecting computers in Singapore in 2Q15 was [Win32/Kilim](#), which was detected and removed from 1.3 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The fourth most common threat family infecting computers in Singapore in 2Q15 was [Win32/Dyzap](#), which was detected and removed from 0.6 of every 1,000 unique computers scanned by the MSRT. [Win32/Dyzap](#) is a threat that steals login credentials for a long list of banking websites using man-in-the-browser (MITB) attacks. It is usually installed on the infected computer by TrojanDownloader:Win32/Upatre.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Singapore and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Singapore

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.50 (0.28)	0.65 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	6.25 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	19.24 (16.7)	

Slovakia

The statistics presented here are generated by Microsoft security programs and services running on computers in Slovakia in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Slovakia

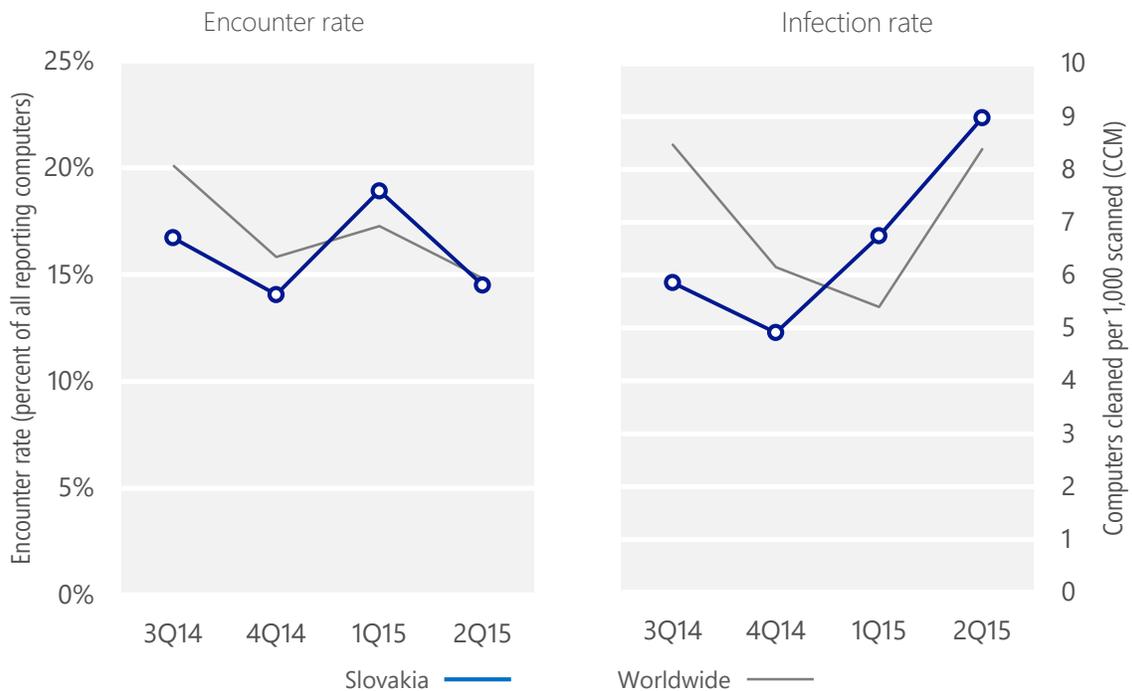
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Slovakia	16.7%	14.1%	18.9%	14.5%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Slovakia	5.9	4.9	6.7	9.0
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcote, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 14.5% of computers in Slovakia encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 9.0 of every 1,000 unique computers scanned in Slovakia in 2Q15 (a CCM score of 9.0, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Slovakia over the last four quarters, compared to the world as a whole.

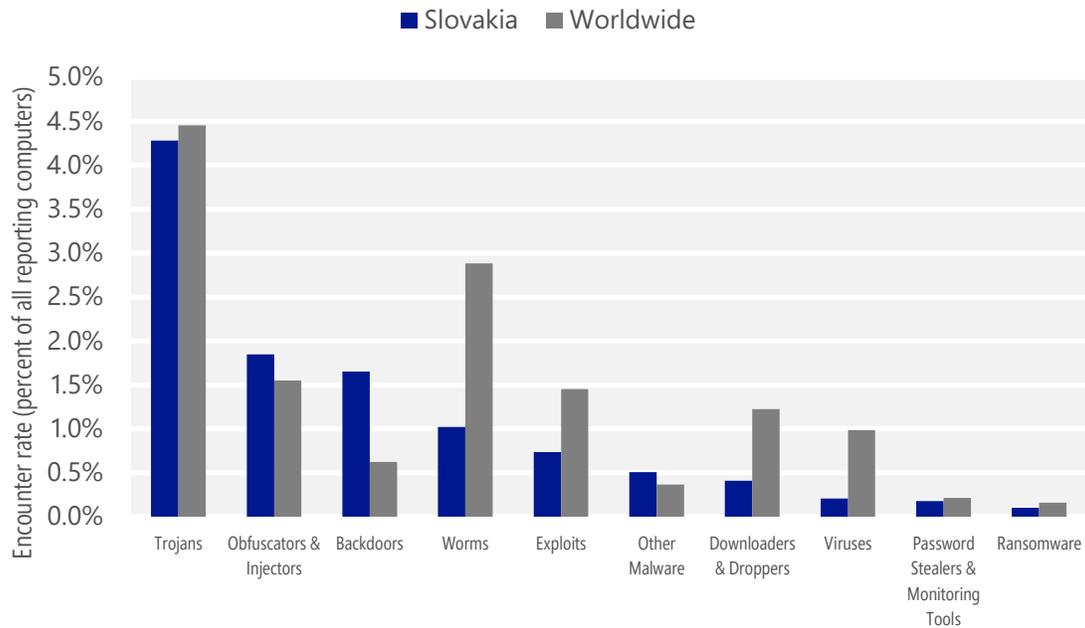
Malware encounter and infection rate trends in Slovakia and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in Slovakia and around the world, and for explanations of the methods and terms used here.

Malware categories

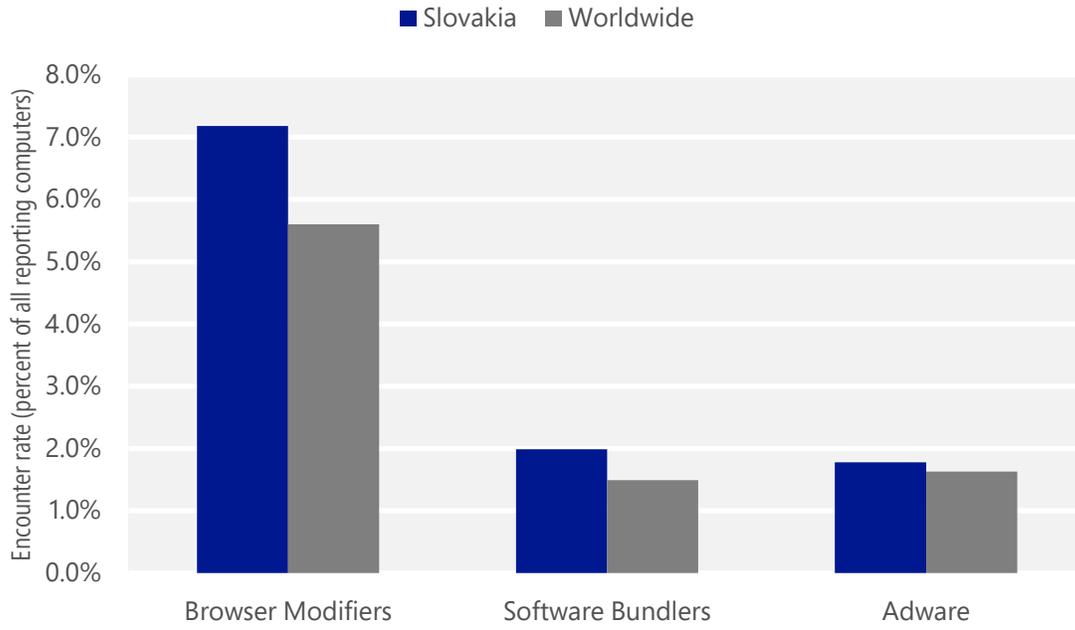
Malware encountered in Slovakia in 2Q15, by category



- The most common malware category in Slovakia in 2Q15 was Trojans. It was encountered by 4.3 percent of all computers there, up from 4.1 percent in 1Q15.
- The second most common malware category in Slovakia in 2Q15 was Obfuscators & Injectors. It was encountered by 1.8 percent of all computers there, down from 1.9 percent in 1Q15.
- The third most common malware category in Slovakia in 2Q15 was Backdoors, which was encountered by 1.7 percent of all computers there, down from 1.8 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Slovakia in 2Q15, by category



- The most common unwanted software category in Slovakia in 2Q15 was Browser Modifiers. It was encountered by 7.2 percent of all computers there, down from 9.8 percent in 1Q15.
- The second most common unwanted software category in Slovakia in 2Q15 was Software Bundlers. It was encountered by 2.0 percent of all computers there, down from 4.5 percent in 1Q15.
- The third most common unwanted software category in Slovakia in 2Q15 was Adware, which was encountered by 1.8 percent of all computers there, up from 0.7 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Slovakia in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Obfuscator	Obfuscators & Injectors	1.5%
2	MSIL/Bladabindi	Backdoors	1.5%
3	Win32/Kilim	Trojans	1.1%
4	Win32/Skeeyah	Trojans	0.8%
5	Win32/Peals	Trojans	0.6%
6	JS/Axpergle	Exploits	0.4%
7	VBS/Jenxcus	Worms	0.4%
8	Win32/Dynamer	Trojans	0.3%
9	Win32/Anaki	Trojans	0.3%
10	INF/Autorun	Obfuscators & Injectors	0.3%

- The most common malware family encountered in Slovakia in 2Q15 was [Win32/Obfuscator](#), which was encountered by 1.5 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The second most common malware family encountered in Slovakia in 2Q15 was [MSIL/Bladabindi](#), which was encountered by 1.5 percent of reporting computers there. [MSIL/Bladabindi](#) is a family of backdoors created by a malicious hacker tool called NJ Rat. The can steal sensitive information, download other malware, and allow backdoor access to an infected computer.
- The third most common malware family encountered in Slovakia in 2Q15 was [Win32/Kilim](#), which was encountered by 1.1 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The fourth most common malware family encountered in Slovakia in 2Q15 was [Win32/Skeeyah](#), which was encountered by 0.8 percent of reporting computers there. [Win32/Skeeyah](#) is a generic detection for various threats that display trojan characteristics.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Slovakia in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	4.0%
2	Win32/KipodToolsCby	Browser Modifiers	3.0%
3	Win32/InstalleRex	Software Bundlers	1.9%
4	Win32/SaverExtension	Adware	1.4%
5	Win32/AlterbookSP	Browser Modifiers	0.4%

- The most common unwanted software family encountered in Slovakia in 2Q15 was [Win32/CouponRuc](#), which was encountered by 4.0 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in Slovakia in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 3.0 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common unwanted software family encountered in Slovakia in 2Q15 was [Win32/InstalleRex](#), which was encountered by 1.9 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Slovakia in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/IeEnablerCby	Browser Modifiers	2.2
2	Win32/CompromisedCert	Other Malware	2.0
3	MSIL/Bladabindi	Backdoors	1.6
4	Win32/Kilim	Trojans	1.1
5	VBS/Jenxcus	Worms	0.9
6	Win32/Sality	Viruses	0.3
7	Win32/Brontok	Worms	0.3
8	Win32/Simda	Trojans	0.2
9	Win32/Zbot	Password Stealers & Monitoring Tools	0.1
10	Win32/Ramnit	Trojans	0.1

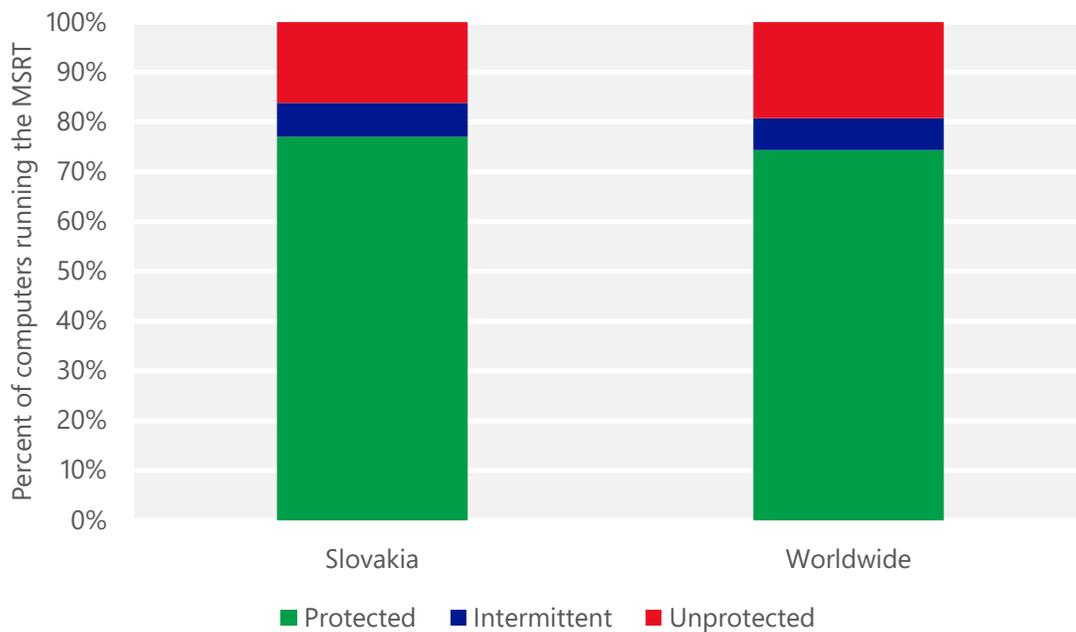
- The most common threat family infecting computers in Slovakia in 2Q15 was [Win32/IeEnablerCby](#), which was detected and removed from 2.2 of every 1,000 unique computers scanned by the MSRT. [Win32/IeEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Slovakia in 2Q15 was [Win32/CompromisedCert](#), which was detected and removed from 2.0 of every 1,000 unique computers scanned by the MSRT. [Win32/CompromisedCert](#) is a detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.
- The third most common threat family infecting computers in Slovakia in 2Q15 was [MSIL/Bladabindi](#), which was detected and removed from 1.6 of every 1,000 unique computers scanned by the MSRT. [MSIL/Bladabindi](#) is a family of backdoors created by a malicious hacker tool called NJ Rat. The can steal sensitive information, download other malware, and allow backdoor access to an infected computer.
- The fourth most common threat family infecting computers in Slovakia in 2Q15 was [Win32/Kilim](#), which was detected and removed from 1.1 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Slovakia and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Slovakia

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.20 (0.28)	0.19 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	4.77 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	7.71 (16.7)	

Slovenia

The statistics presented here are generated by Microsoft security programs and services running on computers in Slovenia in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Slovenia

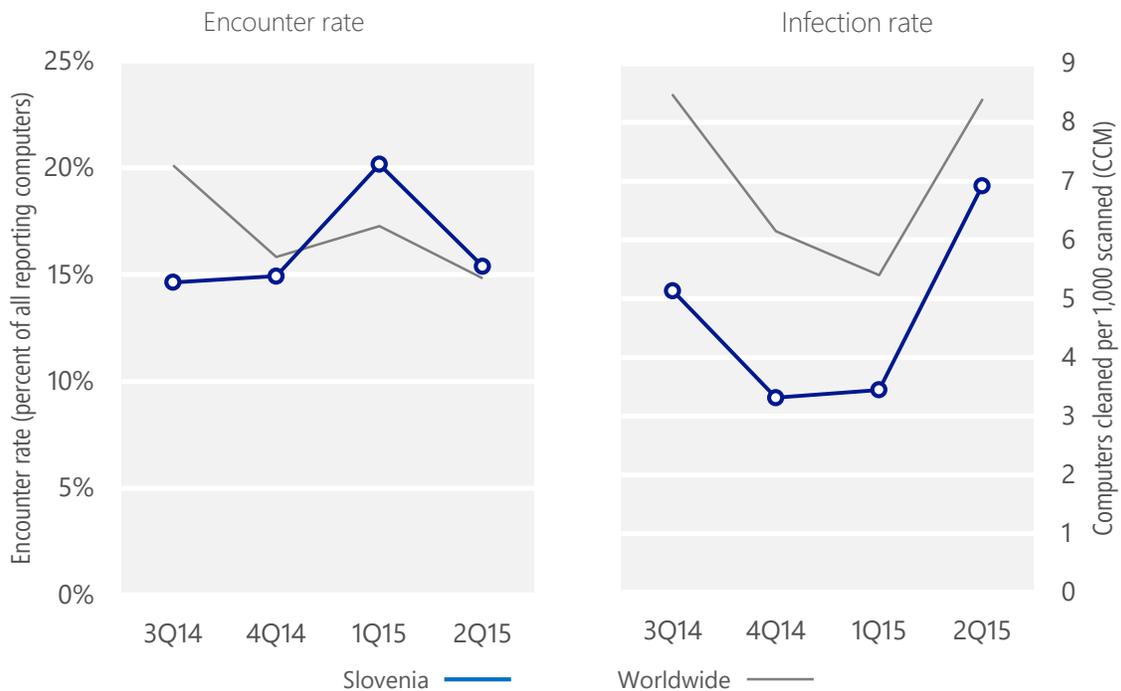
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Slovenia	14.6%	14.9%	20.2%	15.4%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Slovenia	5.1	3.3	3.4	6.9
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcout, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 15.4% of computers in Slovenia encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 6.9 of every 1,000 unique computers scanned in Slovenia in 2Q15 (a CCM score of 6.9, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Slovenia over the last four quarters, compared to the world as a whole.

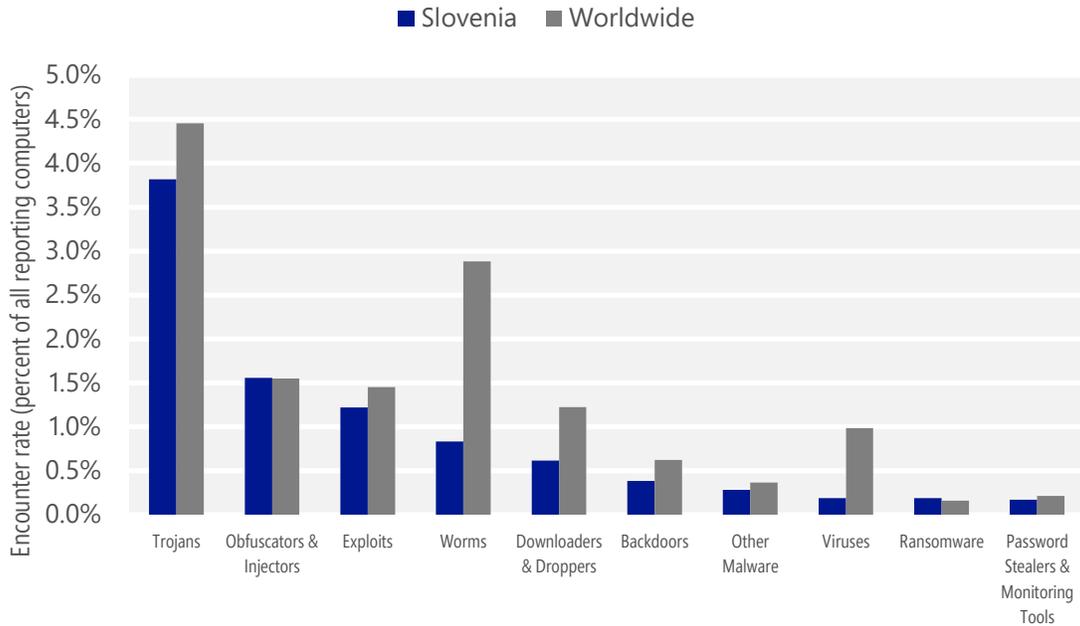
Malware encounter and infection rate trends in Slovenia and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in Slovenia and around the world, and for explanations of the methods and terms used here.

Malware categories

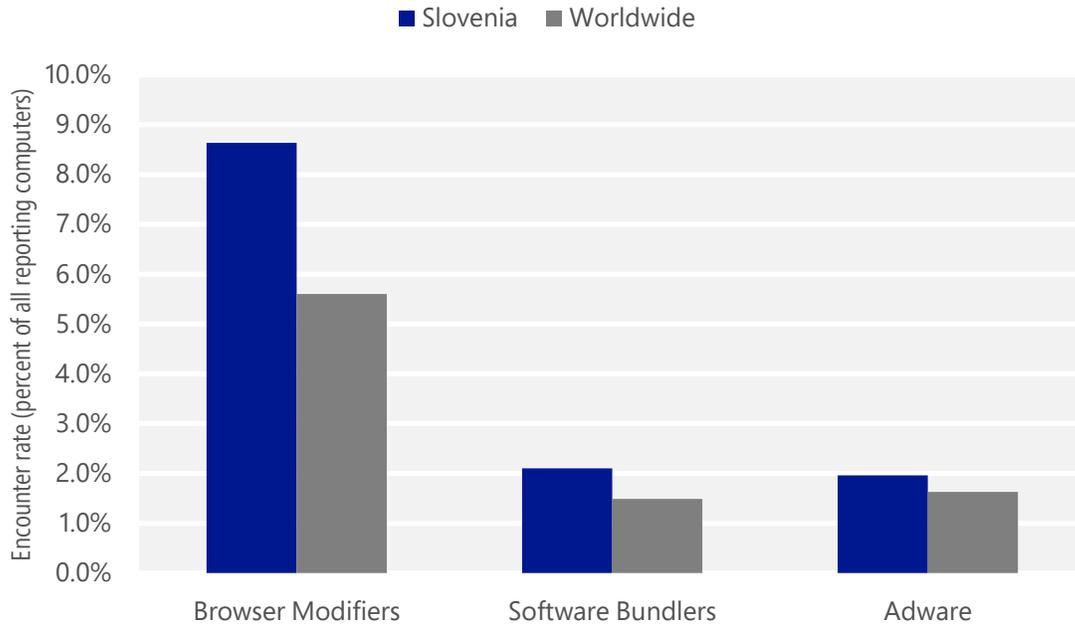
Malware encountered in Slovenia in 2Q15, by category



- The most common malware category in Slovenia in 2Q15 was Trojans. It was encountered by 3.8 percent of all computers there, up from 3.6 percent in 1Q15.
- The second most common malware category in Slovenia in 2Q15 was Obfuscators & Injectors. It was encountered by 1.6 percent of all computers there, down from 1.9 percent in 1Q15.
- The third most common malware category in Slovenia in 2Q15 was Exploits, which was encountered by 1.2 percent of all computers there, down from 1.7 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Slovenia in 2Q15, by category



- The most common unwanted software category in Slovenia in 2Q15 was Browser Modifiers. It was encountered by 8.6 percent of all computers there, down from 11.5 percent in 1Q15.
- The second most common unwanted software category in Slovenia in 2Q15 was Software Bundlers. It was encountered by 2.1 percent of all computers there, down from 5.4 percent in 1Q15.
- The third most common unwanted software category in Slovenia in 2Q15 was Adware, which was encountered by 2.0 percent of all computers there, up from 1.0 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Slovenia in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Obfuscator	Obfuscators & Injectors	1.3%
2	Win32/Kilim	Trojans	1.2%
3	Win32/Skeeyah	Trojans	0.7%
4	JS/Axpergle	Exploits	0.7%
5	Win32/Peals	Trojans	0.6%
6	INF/Autorun	Obfuscators & Injectors	0.2%
7	Win32/Dynamer	Trojans	0.2%
8	Win32/Gamarue	Worms	0.2%
9	Win32/Sdbby	Exploits	0.2%
10	Win32/Conficker	Worms	0.1%

- The most common malware family encountered in Slovenia in 2Q15 was [Win32/Obfuscator](#), which was encountered by 1.3 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The second most common malware family encountered in Slovenia in 2Q15 was [Win32/Kilim](#), which was encountered by 1.2 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The third most common malware family encountered in Slovenia in 2Q15 was [Win32/Skeeyah](#), which was encountered by 0.7 percent of reporting computers there. [Win32/Skeeyah](#) is a generic detection for various threats that display trojan characteristics.
- The fourth most common malware family encountered in Slovenia in 2Q15 was [JS/Axpergle](#), which was encountered by 0.7 percent of reporting computers there. [JS/Axpergle](#) is a detection for the Angler exploit kit, which exploits vulnerabilities in recent versions of Internet Explorer, Silverlight, Adobe Flash Player, and Java to install malware.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Slovenia in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	4.4%
2	Win32/KipodToolsCby	Browser Modifiers	3.0%
3	Win32/InstalleRex	Software Bundlers	2.0%
4	Win32/SaverExtension	Adware	1.6%
5	Win32/AlterbookSP	Browser Modifiers	1.5%

- The most common unwanted software family encountered in Slovenia in 2Q15 was [Win32/CouponRuc](#), which was encountered by 4.4 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in Slovenia in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 3.0 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common unwanted software family encountered in Slovenia in 2Q15 was [Win32/InstalleRex](#), which was encountered by 2.0 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Slovenia in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	2.3
2	Win32/Kilim	Trojans	1.4
3	Win32/CompromisedCert	Other Malware	1.2
4	Win32/Simda	Trojans	0.3
5	Win32/Sality	Viruses	0.2
6	Win32/Ramnit	Trojans	0.2
7	MSIL/Bladabindi	Backdoors	0.1
8	Win32/Alureon	Trojans	0.1
9	Win32/Brontok	Worms	0.1
10	Win32/Helompy	Worms	0.1

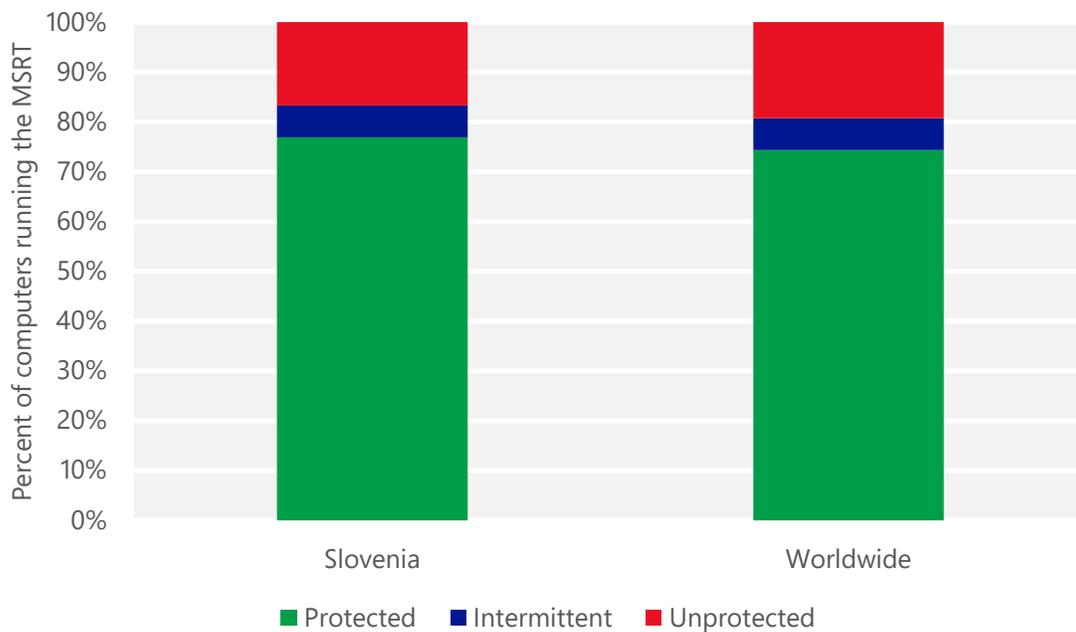
- The most common threat family infecting computers in Slovenia in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 2.3 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Slovenia in 2Q15 was [Win32/Kilim](#), which was detected and removed from 1.4 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The third most common threat family infecting computers in Slovenia in 2Q15 was [Win32/CompromisedCert](#), which was detected and removed from 1.2 of every 1,000 unique computers scanned by the MSRT. [Win32/CompromisedCert](#) is a detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.
- The fourth most common threat family infecting computers in Slovenia in 2Q15 was [Win32/Simda](#), which was detected and removed from 0.3 of every 1,000 unique computers scanned by the MSRT. [Win32/Simda](#) is a threat that can give an attacker backdoor access and control of an infected computer. It can then steal passwords and gather information about the computer to send to the attacker.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Slovenia and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Slovenia

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.25 (0.28)	0.21 (0.24)
Phishing sites per 1,000 hosts (Worldwide)		3.99 (5.0)
Malware hosting sites per 1,000 hosts (Worldwide)		7.14 (16.7)

South Africa

The statistics presented here are generated by Microsoft security programs and services running on computers in South Africa in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for South Africa

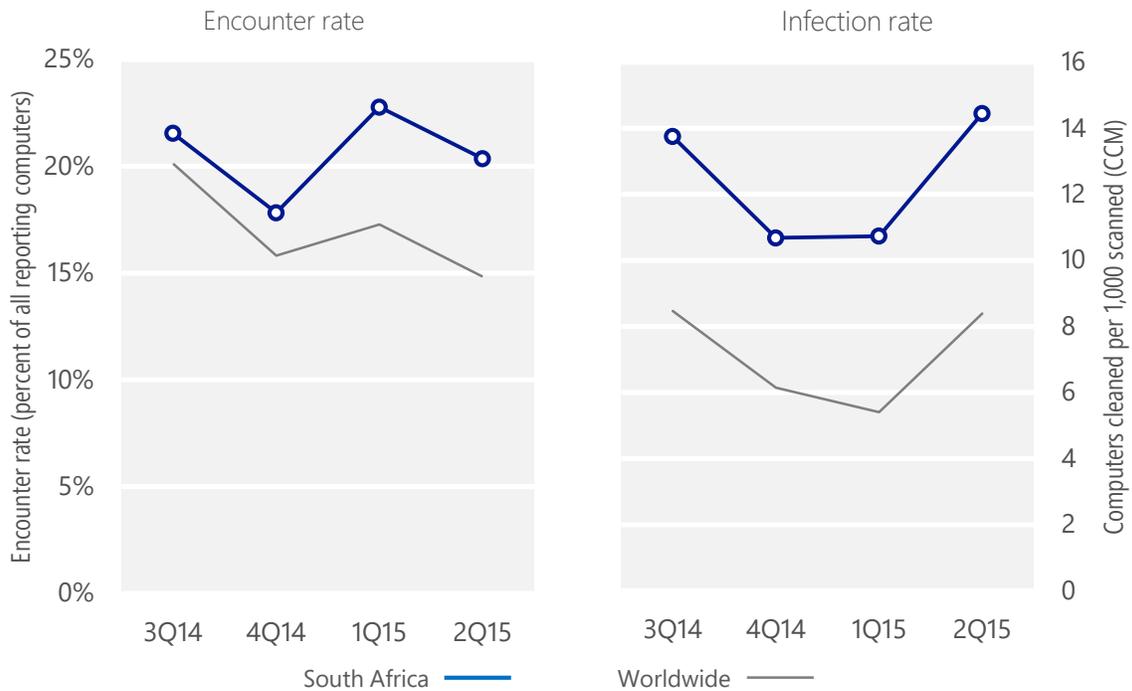
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, South Africa	21.5%	17.8%	22.8%	20.4%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, South Africa	13.7	10.7	10.7	14.4
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcoute, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 20.4% of computers in South Africa encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 14.4 of every 1,000 unique computers scanned in South Africa in 2Q15 (a CCM score of 14.4, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for South Africa over the last four quarters, compared to the world as a whole.

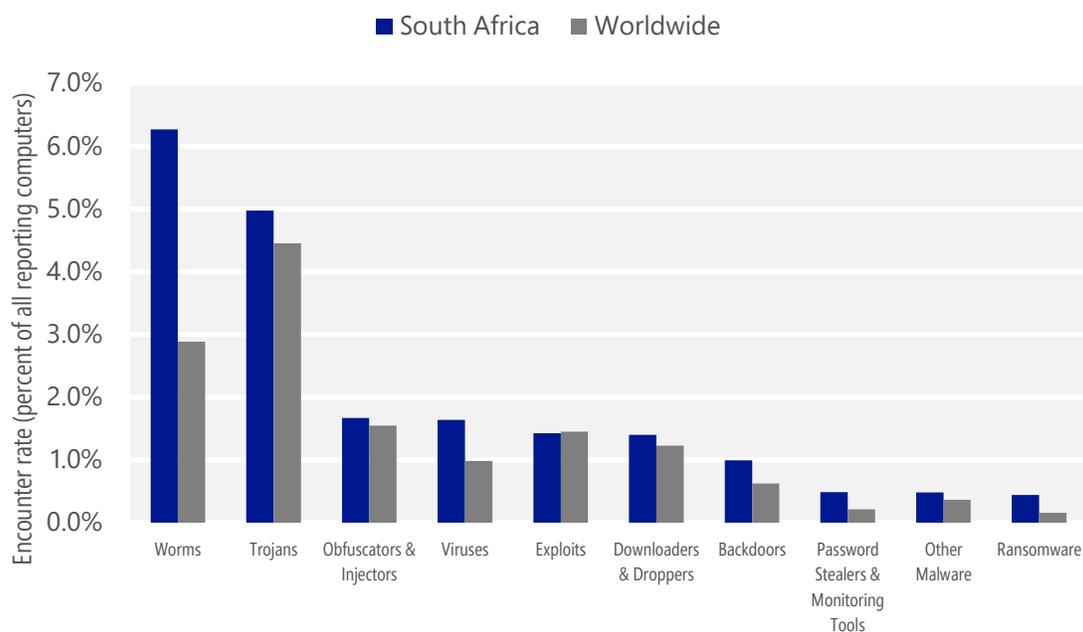
Malware encounter and infection rate trends in South Africa and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in South Africa and around the world, and for explanations of the methods and terms used here.

Malware categories

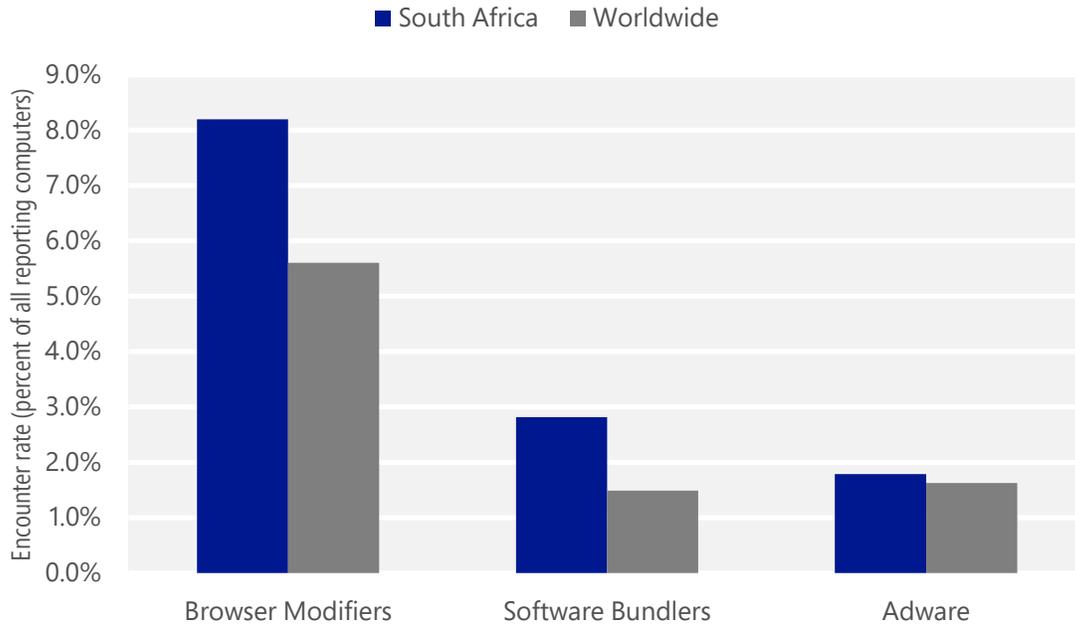
Malware encountered in South Africa in 2Q15, by category



- The most common malware category in South Africa in 2Q15 was Worms. It was encountered by 6.3 percent of all computers there, down from 7.2 percent in 1Q15.
- The second most common malware category in South Africa in 2Q15 was Trojans. It was encountered by 5.0 percent of all computers there, up from 3.0 percent in 1Q15.
- The third most common malware category in South Africa in 2Q15 was Obfuscators & Injectors, which was encountered by 1.7 percent of all computers there, down from 2.0 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in South Africa in 2Q15, by category



- The most common unwanted software category in South Africa in 2Q15 was Browser Modifiers. It was encountered by 8.2 percent of all computers there, down from 10.4 percent in 1Q15.
- The second most common unwanted software category in South Africa in 2Q15 was Software Bundlers. It was encountered by 2.8 percent of all computers there, down from 5.0 percent in 1Q15.
- The third most common unwanted software category in South Africa in 2Q15 was Adware, which was encountered by 1.8 percent of all computers there, up from 0.9 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in South Africa in 2Q15

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	2.7%
2	INF/Autorun	Obfuscators & Injectors	1.3%
3	Win32/Enosch	Worms	1.3%
4	Win32/Peals	Trojans	1.0%
5	Win32/Skeeyah	Trojans	1.0%
6	Win32/Kilim	Trojans	0.9%
7	Win32/Obfuscator	Obfuscators & Injectors	0.7%
8	Win32/Ippedo	Worms	0.7%
9	Win32/Virut	Viruses	0.6%
10	Win32/Copali	Worms	0.6%

- The most common malware family encountered in South Africa in 2Q15 was [VBS/Jenxcus](#), which was encountered by 2.7 percent of reporting computers there. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common malware family encountered in South Africa in 2Q15 was [INF/Autorun](#), which was encountered by 1.3 percent of reporting computers there. [INF/Autorun](#) is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The third most common malware family encountered in South Africa in 2Q15 was [Win32/Enosch](#), which was encountered by 1.3 percent of reporting computers there. [Win32/Enosch](#) is a worm that steals Microsoft Word documents (which may include sensitive information) from the computer and emails them to a remote attacker.
- The fourth most common malware family encountered in South Africa in 2Q15 was [Win32/Peals](#), which was encountered by 1.0 percent of reporting computers there. [Win32/Peals](#) is a generic detection for various threats that display trojan characteristics.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in South Africa in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	4.0%
2	Win32/KipodToolsCby	Browser Modifiers	3.3%
3	Win32/InstalleRex	Software Bundlers	2.7%
4	Win32/SaverExtension	Adware	1.4%
5	Win32/AlterbookSP	Browser Modifiers	1.2%

- The most common unwanted software family encountered in South Africa in 2Q15 was [Win32/CouponRuc](#), which was encountered by 4.0 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in South Africa in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 3.3 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common unwanted software family encountered in South Africa in 2Q15 was [Win32/InstalleRex](#), which was encountered by 2.7 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in South Africa in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	3.6
2	Win32/leEnablerCby	Browser Modifiers	2.2
3	Win32/CompromisedCert	Other Malware	2.0
4	Win32/Kilim	Trojans	1.2
5	Win32/Sality	Viruses	1.0
6	Win32/Vobfus	Worms	0.7
7	Win32/Virut	Viruses	0.6
8	Win32/Chir	Viruses	0.5
9	MSIL/Bladabindi	Backdoors	0.4
10	Win32/Nuqel	Worms	0.4

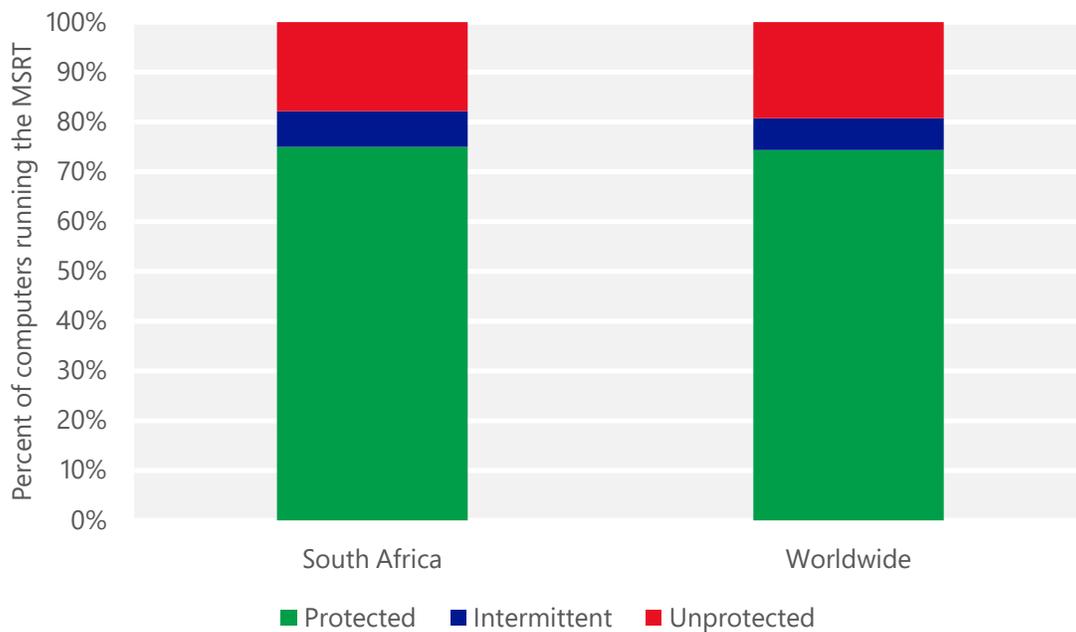
- The most common threat family infecting computers in South Africa in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 3.6 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in South Africa in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 2.2 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common threat family infecting computers in South Africa in 2Q15 was [Win32/CompromisedCert](#), which was detected and removed from 2.0 of every 1,000 unique computers scanned by the MSRT. [Win32/CompromisedCert](#) is a detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.
- The fourth most common threat family infecting computers in South Africa in 2Q15 was [Win32/Kilim](#), which was detected and removed from 1.2 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in South Africa and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for South Africa

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.07 (0.28)	0.08 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	8.37 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	8.69 (16.7)	

Spain

The statistics presented here are generated by Microsoft security programs and services running on computers in Spain in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Spain

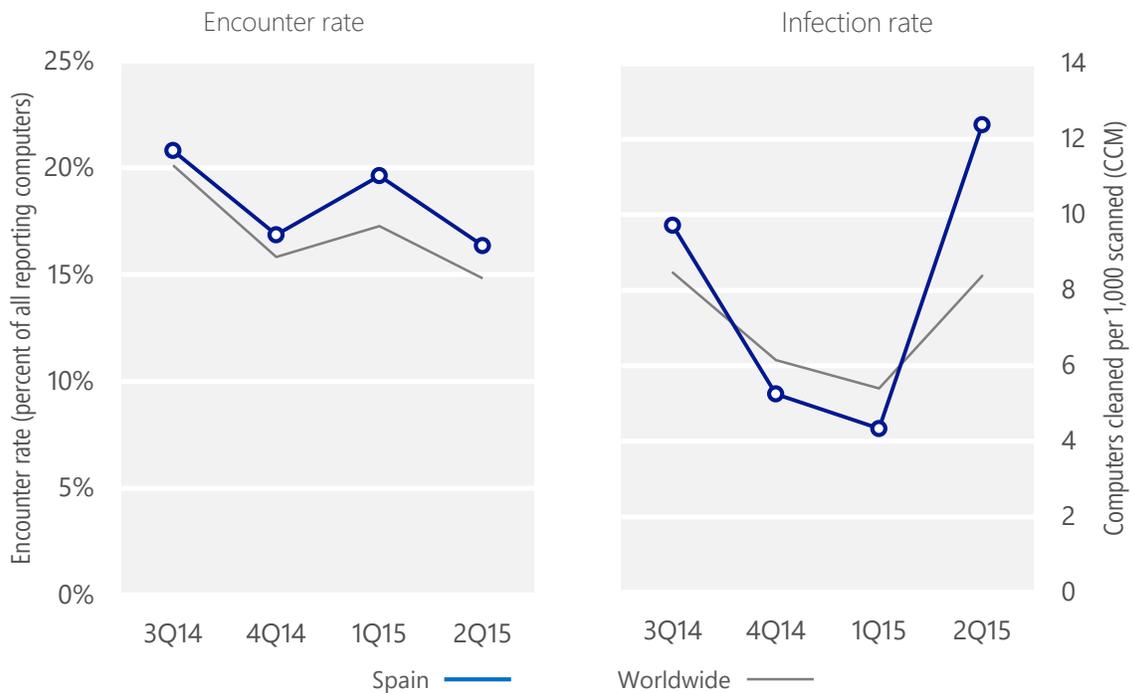
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Spain	20.8%	16.9%	19.6%	16.4%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Spain	9.7	5.3	4.3	12.4
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcote, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 16.4% of computers in Spain encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 12.4 of every 1,000 unique computers scanned in Spain in 2Q15 (a CCM score of 12.4, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Spain over the last four quarters, compared to the world as a whole.

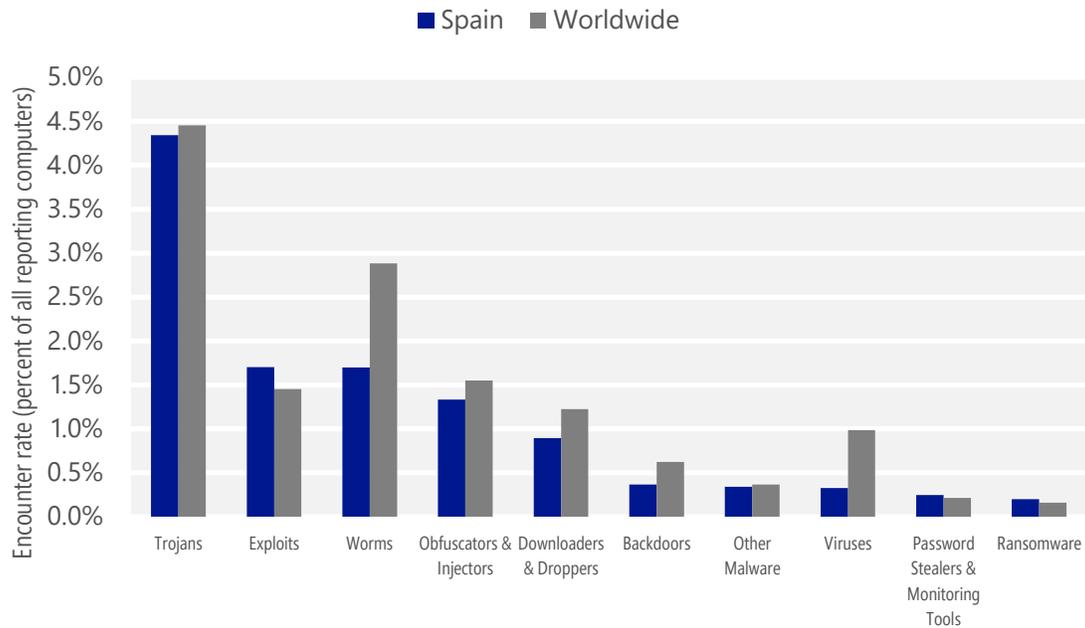
Malware encounter and infection rate trends in Spain and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in Spain and around the world, and for explanations of the methods and terms used here.

Malware categories

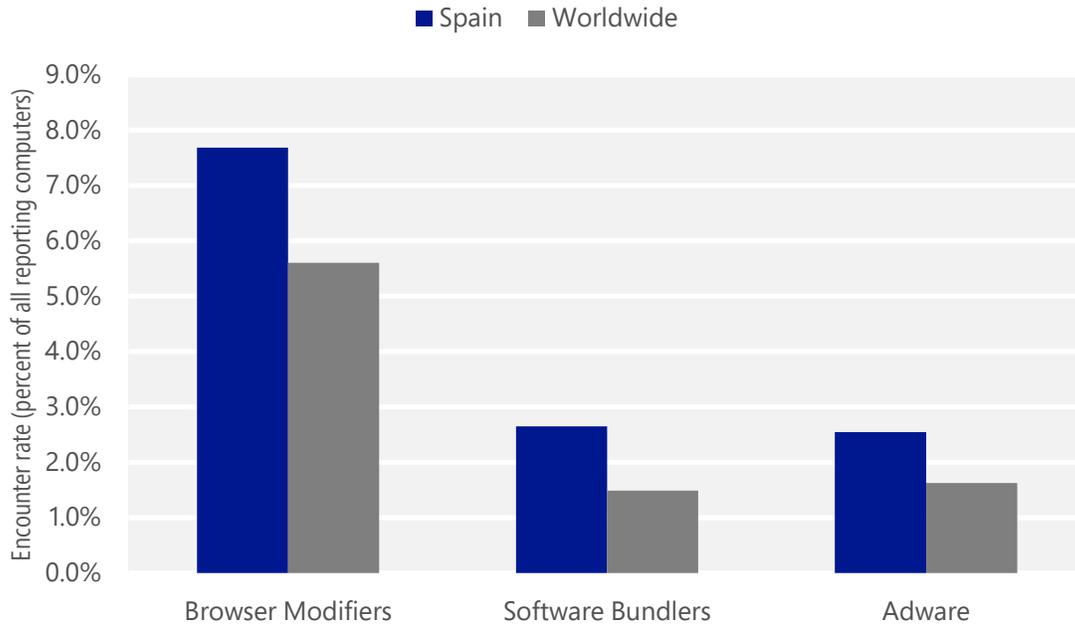
Malware encountered in Spain in 2Q15, by category



- The most common malware category in Spain in 2Q15 was Trojans. It was encountered by 4.3 percent of all computers there, up from 3.1 percent in 1Q15.
- The second most common malware category in Spain in 2Q15 was Exploits. It was encountered by 1.7 percent of all computers there, down from 2.7 percent in 1Q15.
- The third most common malware category in Spain in 2Q15 was Worms, which was encountered by 1.7 percent of all computers there, down from 2.4 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Spain in 2Q15, by category



- The most common unwanted software category in Spain in 2Q15 was Browser Modifiers. It was encountered by 7.7 percent of all computers there, down from 9.0 percent in 1Q15.
- The second most common unwanted software category in Spain in 2Q15 was Software Bundlers. It was encountered by 2.6 percent of all computers there, down from 6.3 percent in 1Q15.
- The third most common unwanted software category in Spain in 2Q15 was Adware, which was encountered by 2.5 percent of all computers there, up from 0.6 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Spain in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Kilim	Trojans	1.5%
2	JS/Axpergle	Exploits	0.9%
3	Win32/Obfuscator	Obfuscators & Injectors	0.9%
4	Win32/Skeeyah	Trojans	0.8%
5	INF/Autorun	Obfuscators & Injectors	0.5%
6	Win32/Peals	Trojans	0.4%
7	Win32/Conficker	Worms	0.4%
8	VBS/Jenxcus	Worms	0.3%
9	Win32/Sdbby	Exploits	0.3%
10	Win32/Dynamer	Trojans	0.2%

- The most common malware family encountered in Spain in 2Q15 was [Win32/Kilim](#), which was encountered by 1.5 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The second most common malware family encountered in Spain in 2Q15 was [JS/Axpergle](#), which was encountered by 0.9 percent of reporting computers there. [JS/Axpergle](#) is a detection for the Angler exploit kit, which exploits vulnerabilities in recent versions of Internet Explorer, Silverlight, Adobe Flash Player, and Java to install malware.
- The third most common malware family encountered in Spain in 2Q15 was [Win32/Obfuscator](#), which was encountered by 0.9 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The fourth most common malware family encountered in Spain in 2Q15 was [Win32/Skeeyah](#), which was encountered by 0.8 percent of reporting computers there. [Win32/Skeeyah](#) is a generic detection for various threats that display trojan characteristics.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Spain in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	4.5%
2	Win32/InstalleRex	Software Bundlers	2.5%
3	Win32/KipodToolsCby	Browser Modifiers	2.3%
4	Win32/SaverExtension	Adware	1.6%
5	Win32/AlterbookSP	Browser Modifiers	0.7%

- The most common unwanted software family encountered in Spain in 2Q15 was [Win32/CouponRuc](#), which was encountered by 4.5 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in Spain in 2Q15 was [Win32/InstalleRex](#), which was encountered by 2.5 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.
- The third most common unwanted software family encountered in Spain in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 2.3 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.

Top threat families by infection rate

The most common malware families by infection rate in Spain in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	5.8
2	Win32/Kilim	Trojans	2.1
3	Win32/CompromisedCert	Other Malware	1.1
4	VBS/Jenxcus	Worms	0.5
5	Win32/Zbot	Password Stealers & Monitoring Tools	0.3
6	Win32/Brontok	Worms	0.3
7	Win32/Ramnit	Trojans	0.2
8	Win32/Sality	Viruses	0.2
9	Win32/Alureon	Trojans	0.2
10	Win32/Simda	Trojans	0.2

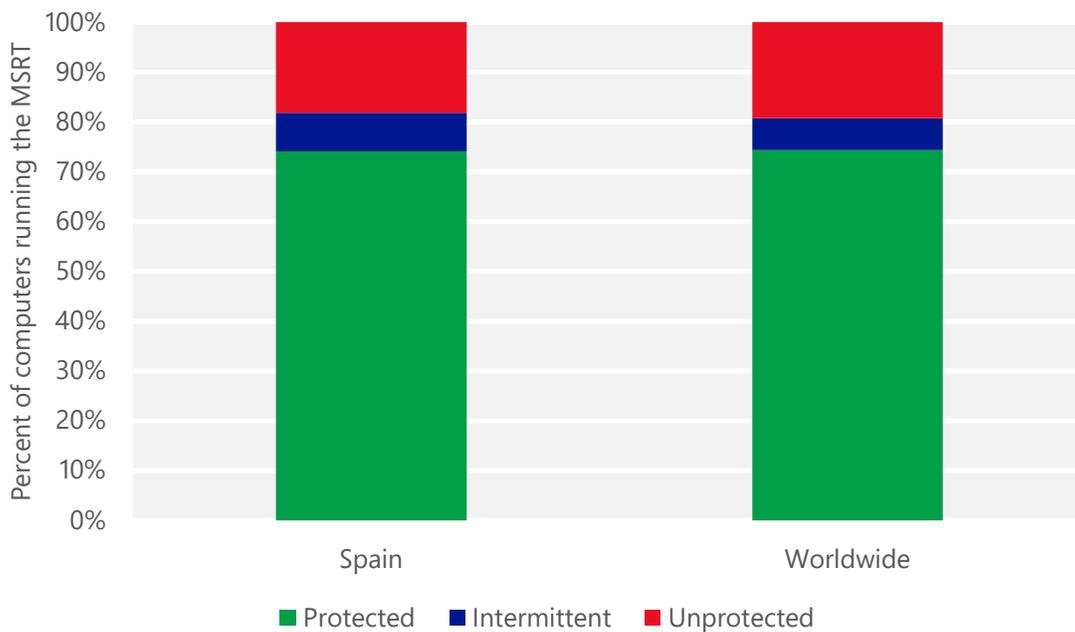
- The most common threat family infecting computers in Spain in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 5.8 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Spain in 2Q15 was [Win32/Kilim](#), which was detected and removed from 2.1 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The third most common threat family infecting computers in Spain in 2Q15 was [Win32/CompromisedCert](#), which was detected and removed from 1.1 of every 1,000 unique computers scanned by the MSRT. [Win32/CompromisedCert](#) is a detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.
- The fourth most common threat family infecting computers in Spain in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 0.5 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Spain and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Spain

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.14 (0.28)	0.13 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	4.70 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	13.22 (16.7)	

Sri Lanka

The statistics presented here are generated by Microsoft security programs and services running on computers in Sri Lanka in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Sri Lanka

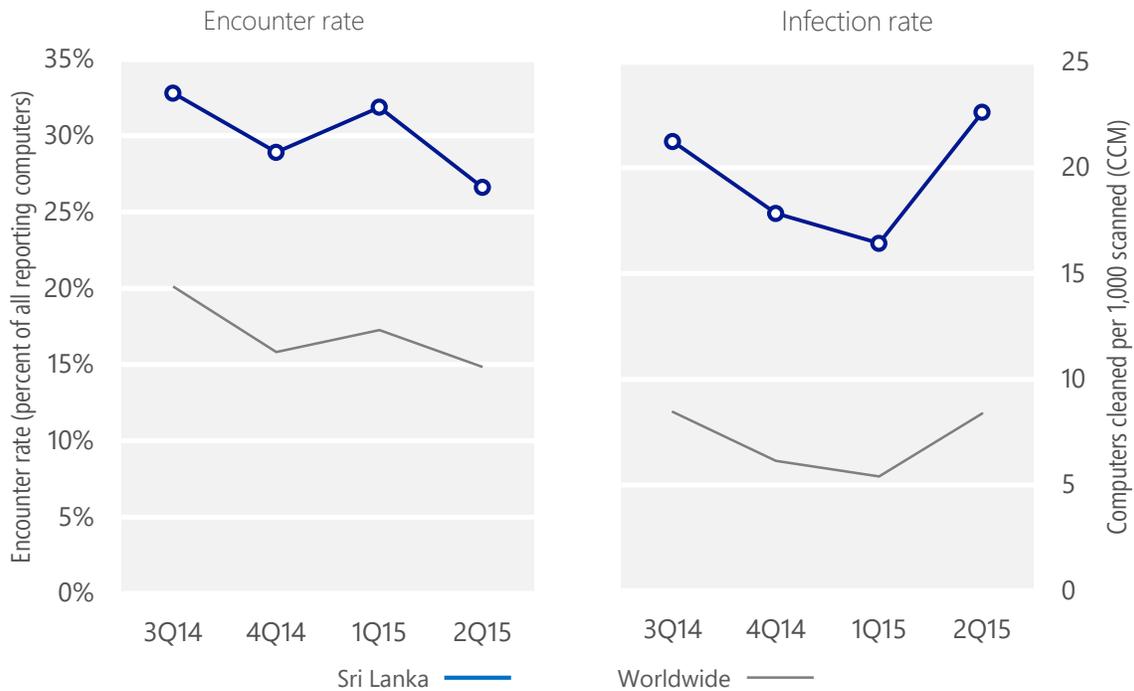
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Sri Lanka	32.8%	28.9%	31.9%	26.6%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Sri Lanka	21.2	17.8	16.4	22.6
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcoute, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 26.6% of computers in Sri Lanka encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 22.6 of every 1,000 unique computers scanned in Sri Lanka in 2Q15 (a CCM score of 22.6, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Sri Lanka over the last four quarters, compared to the world as a whole.

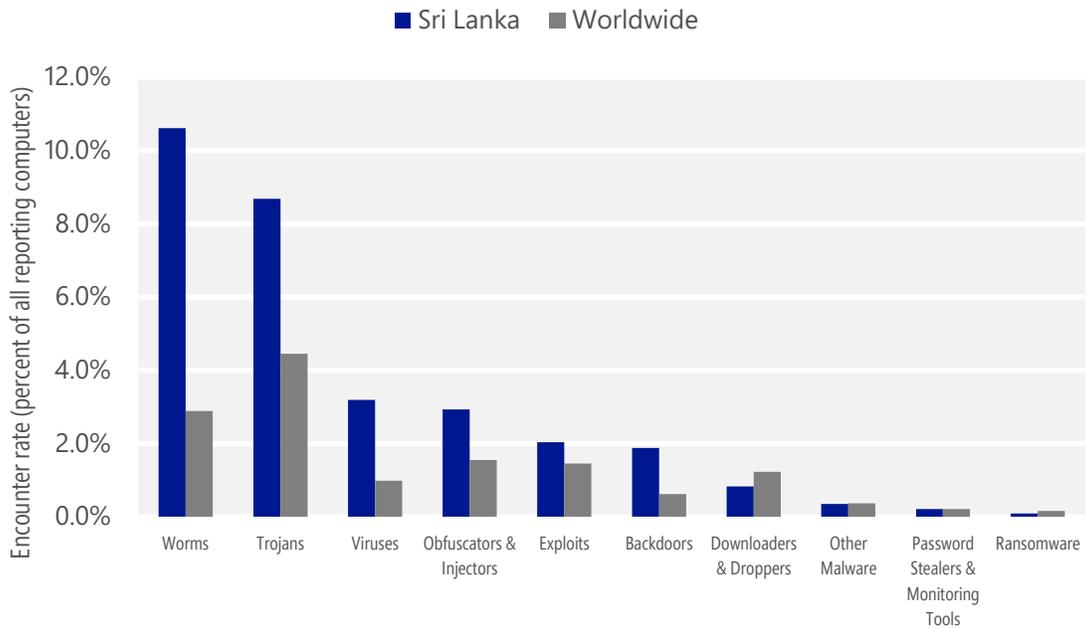
Malware encounter and infection rate trends in Sri Lanka and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in Sri Lanka and around the world, and for explanations of the methods and terms used here.

Malware categories

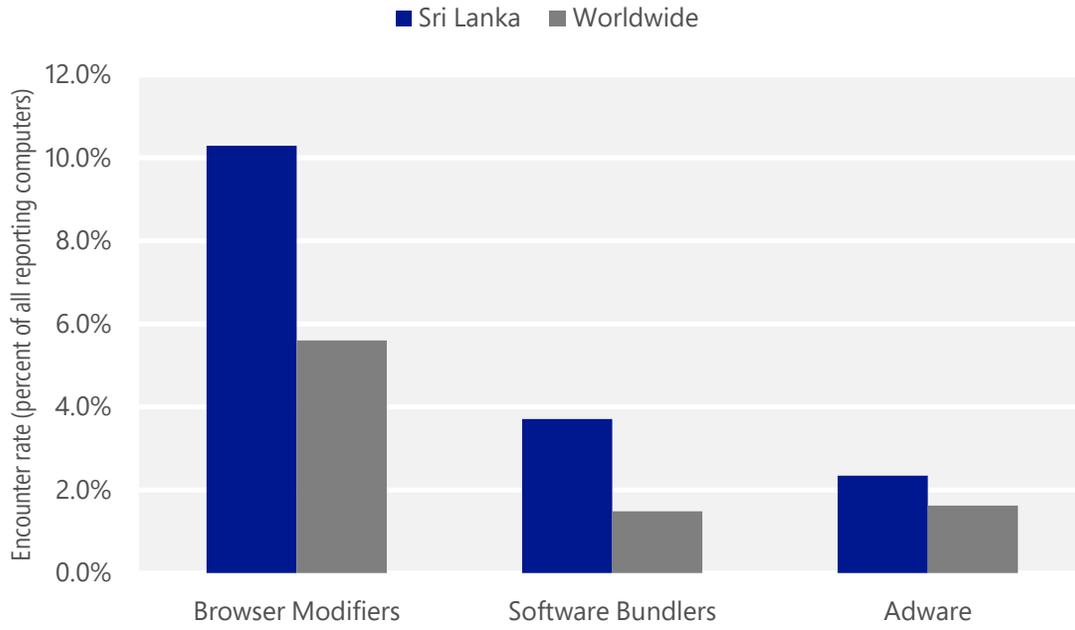
Malware encountered in Sri Lanka in 2Q15, by category



- The most common malware category in Sri Lanka in 2Q15 was Worms. It was encountered by 10.6 percent of all computers there, down from 11.5 percent in 1Q15.
- The second most common malware category in Sri Lanka in 2Q15 was Trojans. It was encountered by 8.7 percent of all computers there, up from 8.3 percent in 1Q15.
- The third most common malware category in Sri Lanka in 2Q15 was Viruses, which was encountered by 3.2 percent of all computers there, down from 4.1 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Sri Lanka in 2Q15, by category



- The most common unwanted software category in Sri Lanka in 2Q15 was Browser Modifiers. It was encountered by 10.3 percent of all computers there, down from 15.5 percent in 1Q15.
- The second most common unwanted software category in Sri Lanka in 2Q15 was Software Bundlers. It was encountered by 3.7 percent of all computers there, down from 5.7 percent in 1Q15.
- The third most common unwanted software category in Sri Lanka in 2Q15 was Adware, which was encountered by 2.3 percent of all computers there, up from 1.5 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Sri Lanka in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Ippedo	Worms	5.2%
2	INF/Autorun	Obfuscators & Injectors	3.3%
3	VBS/Jenxcus	Worms	2.5%
4	Win32/Sality	Viruses	1.7%
5	Win32/CplLnk	Exploits	1.4%
6	Win32/Obfuscator	Obfuscators & Injectors	1.3%
7	Win32/Caphaw	Backdoors	1.3%
8	Win32/Ramnit	Trojans	1.2%
9	Win32/Peals	Trojans	1.2%
10	Win32/Kilim	Trojans	1.2%

- The most common malware family encountered in Sri Lanka in 2Q15 was [Win32/Ippedo](#), which was encountered by 5.2 percent of reporting computers there. [Win32/Ippedo](#) is a worm that can send sensitive information to a malicious hacker. It spreads through removable drives, such as USB flash drives.
- The second most common malware family encountered in Sri Lanka in 2Q15 was [INF/Autorun](#), which was encountered by 3.3 percent of reporting computers there. [INF/Autorun](#) is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The third most common malware family encountered in Sri Lanka in 2Q15 was [VBS/Jenxcus](#), which was encountered by 2.5 percent of reporting computers there. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The fourth most common malware family encountered in Sri Lanka in 2Q15 was [Win32/Sality](#), which was encountered by 1.7 percent of reporting computers there. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Sri Lanka in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	5.4%
2	Win32/KipodToolsCby	Browser Modifiers	5.1%
3	Win32/InstalleRex	Software Bundlers	3.5%
4	Win32/SaverExtension	Adware	1.7%
5	Win32/AlterbookSP	Browser Modifiers	0.3%

- The most common unwanted software family encountered in Sri Lanka in 2Q15 was [Win32/CouponRuc](#), which was encountered by 5.4 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in Sri Lanka in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 5.1 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common unwanted software family encountered in Sri Lanka in 2Q15 was [Win32/InstalleRex](#), which was encountered by 3.5 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Sri Lanka in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/Sality	Viruses	5.9
2	Win32/leEnablerCby	Browser Modifiers	5.0
3	VBS/Jenxcus	Worms	3.3
4	Win32/Dorkbot	Worms	1.7
5	Win32/Nuqel	Worms	1.5
6	Win32/Kilim	Trojans	1.1
7	Win32/Ramnit	Trojans	1.0
8	Win32/Chir	Viruses	0.6
9	Win32/Gamarue	Worms	0.6
10	Win32/Virut	Viruses	0.6

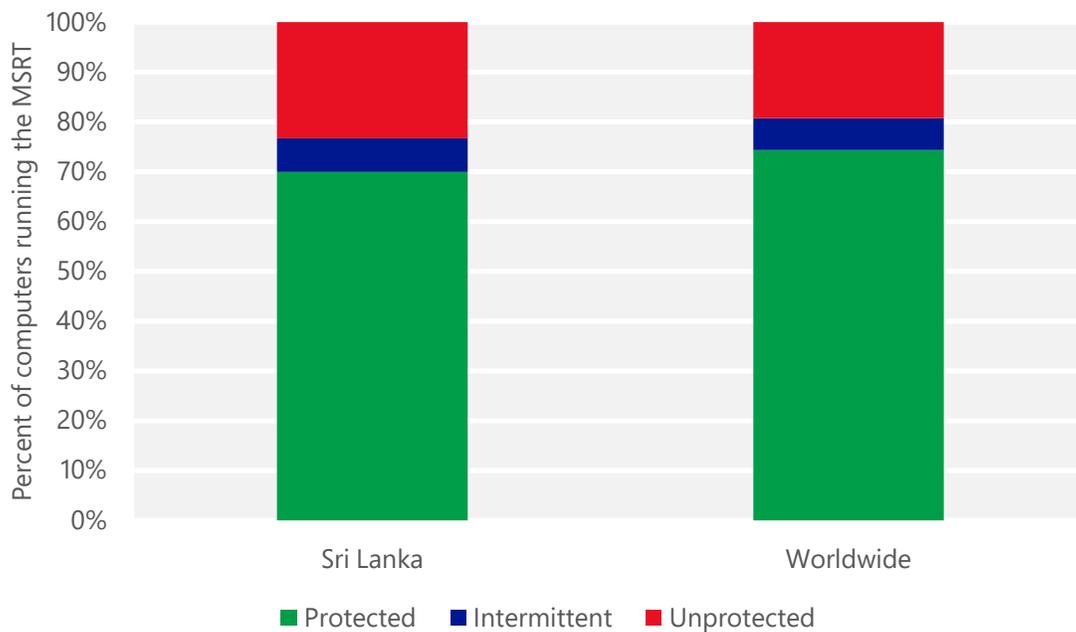
- The most common threat family infecting computers in Sri Lanka in 2Q15 was [Win32/Sality](#), which was detected and removed from 5.9 of every 1,000 unique computers scanned by the MSRT. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The second most common threat family infecting computers in Sri Lanka in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 5.0 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common threat family infecting computers in Sri Lanka in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 3.3 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The fourth most common threat family infecting computers in Sri Lanka in 2Q15 was [Win32/Dorkbot](#), which was detected and removed from 1.7 of every 1,000 unique computers scanned by the MSRT. [Win32/Dorkbot](#) is a worm that spreads via instant messaging and removable drives. It also contains backdoor functionality that allows unauthorized access and control of the affected computer. Win32/Dorkbot may be distributed from compromised or malicious websites using PDF or browser exploits.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Sri Lanka and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Sri Lanka

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.20 (0.28)	0.28 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	2.54 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	12.39 (16.7)	

Sweden

The statistics presented here are generated by Microsoft security programs and services running on computers in Sweden in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Sweden

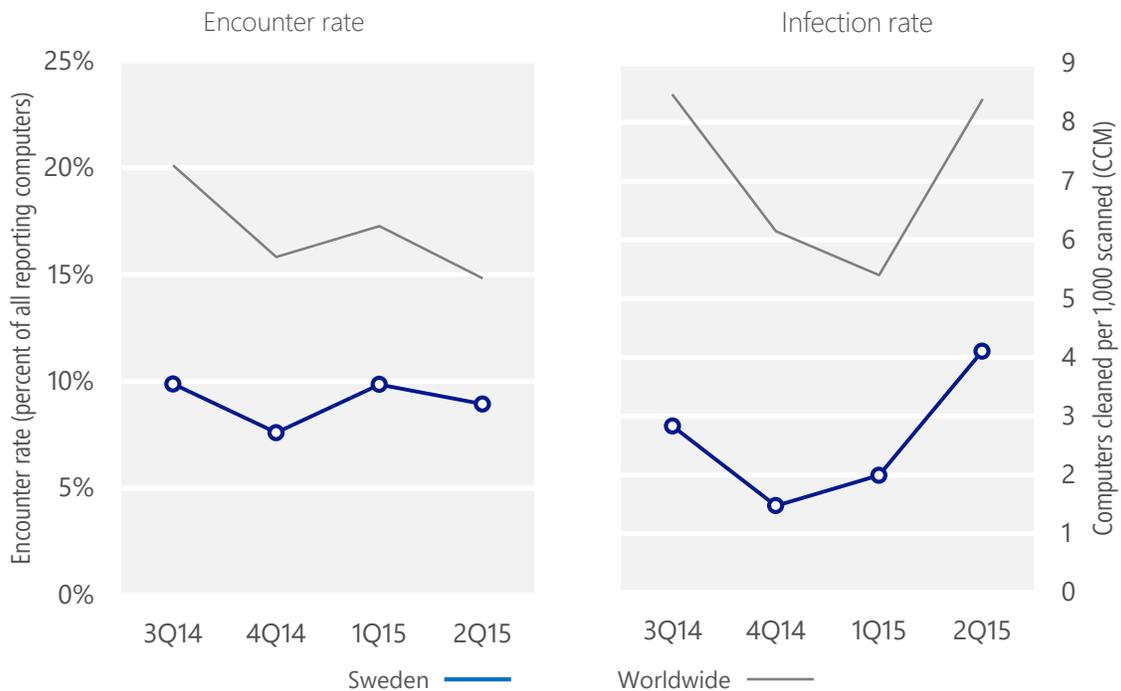
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Sweden	9.9%	7.6%	9.9%	8.9%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Sweden	2.8	1.5	2.0	4.1
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcout, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 8.9% of computers in Sweden encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 4.1 of every 1,000 unique computers scanned in Sweden in 2Q15 (a CCM score of 4.1, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Sweden over the last four quarters, compared to the world as a whole.

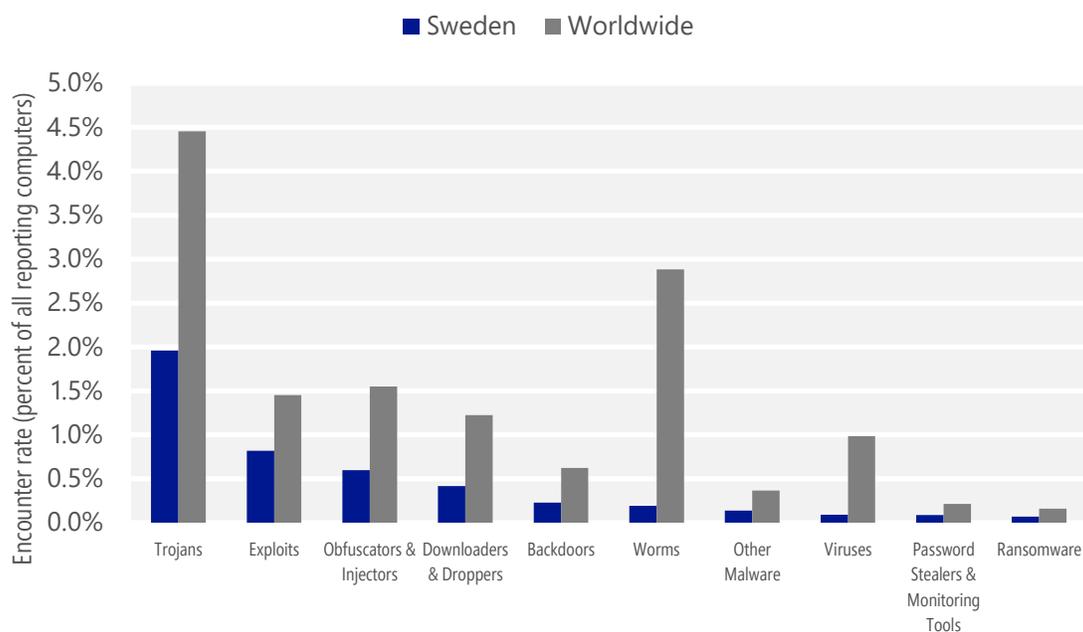
Malware encounter and infection rate trends in Sweden and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in Sweden and around the world, and for explanations of the methods and terms used here.

Malware categories

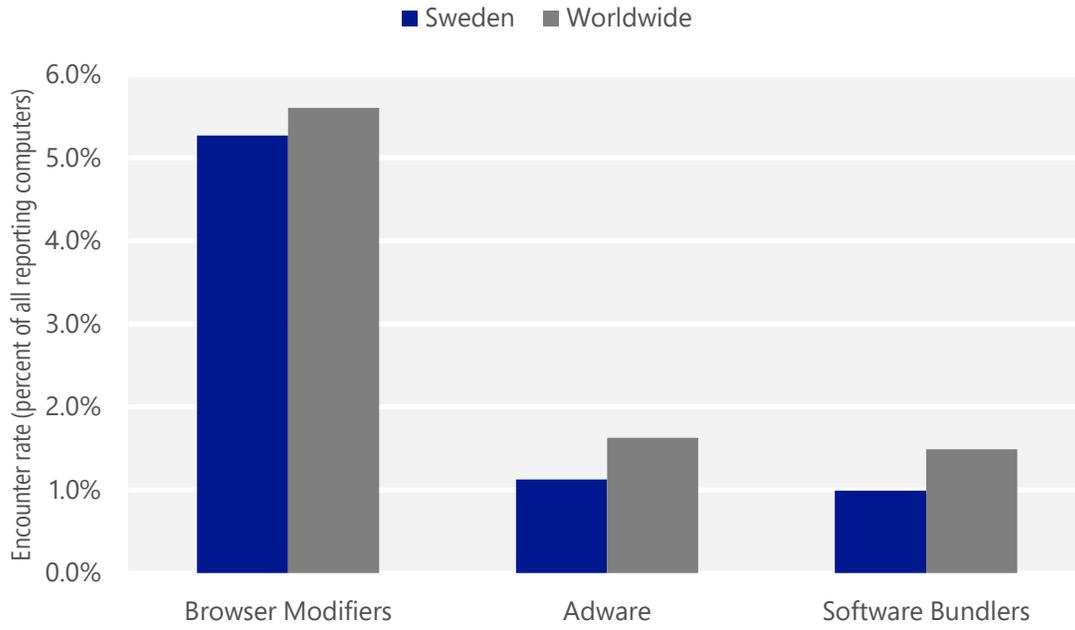
Malware encountered in Sweden in 2Q15, by category



- The most common malware category in Sweden in 2Q15 was Trojans. It was encountered by 2.0 percent of all computers there, up from 1.2 percent in 1Q15.
- The second most common malware category in Sweden in 2Q15 was Exploits. It was encountered by 0.8 percent of all computers there, down from 1.2 percent in 1Q15.
- The third most common malware category in Sweden in 2Q15 was Obfuscators & Injectors, which was encountered by 0.6 percent of all computers there, down from 0.7 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Sweden in 2Q15, by category



- The most common unwanted software category in Sweden in 2Q15 was Browser Modifiers. It was encountered by 5.3 percent of all computers there, up from 4.9 percent in 1Q15.
- The second most common unwanted software category in Sweden in 2Q15 was Adware. It was encountered by 1.1 percent of all computers there, down from 3.5 percent in 1Q15.
- The third most common unwanted software category in Sweden in 2Q15 was Software Bundlers, which was encountered by 1.0 percent of all computers there, up from 0.3 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Sweden in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Kilim	Trojans	0.6%
2	Win32/Obfuscator	Obfuscators & Injectors	0.5%
3	JS/Axpergle	Exploits	0.4%
4	Win32/Skeeyah	Trojans	0.4%
5	Win32/Peals	Trojans	0.2%
6	Win32/Sdbby	Exploits	0.1%
7	Win32/Dynamer	Trojans	0.1%
8	JS/Neclu	Exploits	0.1%
9	MSIL/Bladabindi	Backdoors	0.1%
10	JS/Faceliker	Trojans	<0.1%

- The most common malware family encountered in Sweden in 2Q15 was [Win32/Kilim](#), which was encountered by 0.6 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The second most common malware family encountered in Sweden in 2Q15 was [Win32/Obfuscator](#), which was encountered by 0.5 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The third most common malware family encountered in Sweden in 2Q15 was [JS/Axpergle](#), which was encountered by 0.4 percent of reporting computers there. [JS/Axpergle](#) is a detection for the Angler exploit kit, which exploits vulnerabilities in recent versions of Internet Explorer, Silverlight, Adobe Flash Player, and Java to install malware.
- The fourth most common malware family encountered in Sweden in 2Q15 was [Win32/Skeeyah](#), which was encountered by 0.4 percent of reporting computers there. [Win32/Skeeyah](#) is a generic detection for various threats that display trojan characteristics.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Sweden in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	2.2%
2	Win32/KipodToolsCby	Browser Modifiers	1.7%
3	Win32/AlterbookSP	Browser Modifiers	1.0%
4	Win32/InstalleRex	Software Bundlers	1.0%
5	Win32/SaverExtension	Adware	0.8%

- The most common unwanted software family encountered in Sweden in 2Q15 was [Win32/CouponRuc](#), which was encountered by 2.2 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in Sweden in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 1.7 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common unwanted software family encountered in Sweden in 2Q15 was [Win32/AlterbookSP](#), which was encountered by 1.0 percent of reporting computers there. [Win32/AlterbookSP](#) is a browser add-on that formerly displayed behaviors of unwanted software. Recent versions of the add-on no longer meet Microsoft detection criteria, and are no longer considered unwanted software.

Top threat families by infection rate

The most common malware families by infection rate in Sweden in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/CompromisedCert	Other Malware	1.3
2	Win32/Kilim	Trojans	1.0
3	Win32/leEnablerCby	Browser Modifiers	0.9
4	Win32/Simda	Trojans	0.2
5	MSIL/Bladabindi	Backdoors	0.1
6	Win32/Nitol	Other Malware	0.1
7	Win32/Alureon	Trojans	0.1
8	Win32/Sality	Viruses	0.1
9	VBS/Jenxcus	Worms	0.1
10	Win32/Brontok	Worms	<0.1

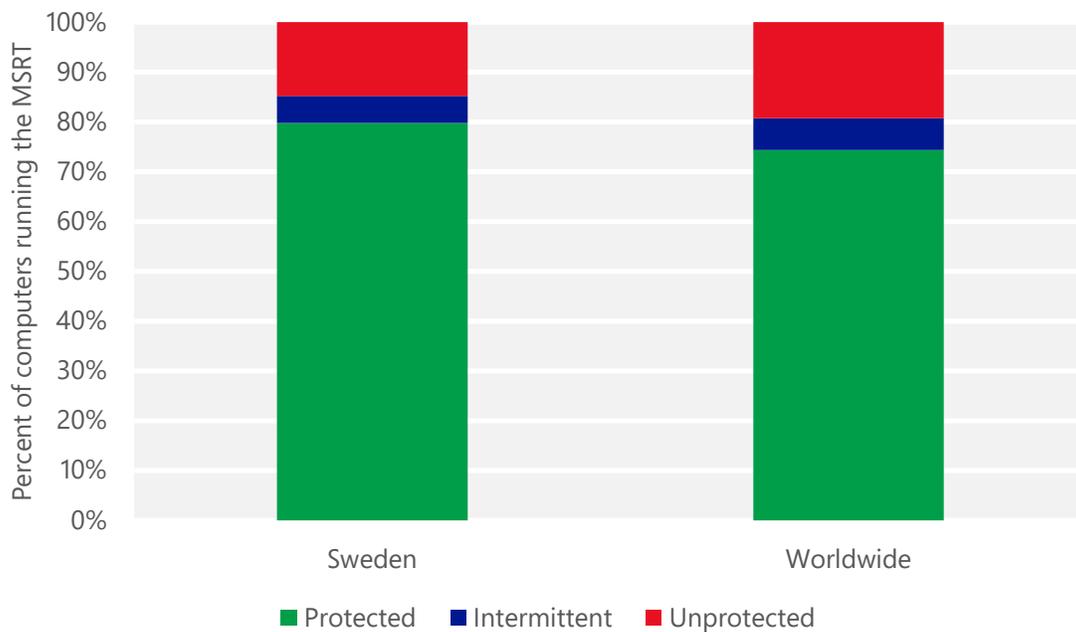
- The most common threat family infecting computers in Sweden in 2Q15 was [Win32/CompromisedCert](#), which was detected and removed from 1.3 of every 1,000 unique computers scanned by the MSRT. [Win32/CompromisedCert](#) is a detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.
- The second most common threat family infecting computers in Sweden in 2Q15 was [Win32/Kilim](#), which was detected and removed from 1.0 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The third most common threat family infecting computers in Sweden in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 0.9 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The fourth most common threat family infecting computers in Sweden in 2Q15 was [Win32/Simda](#), which was detected and removed from 0.2 of every 1,000 unique computers scanned by the MSRT. [Win32/Simda](#) is a threat that can give an attacker backdoor access and control of an infected computer. It can then steal passwords and gather information about the computer to send to the attacker.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Sweden and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Sweden

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.09 (0.28)	0.01 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	3.76 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	9.61 (16.7)	

Switzerland

The statistics presented here are generated by Microsoft security programs and services running on computers in Switzerland in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Switzerland

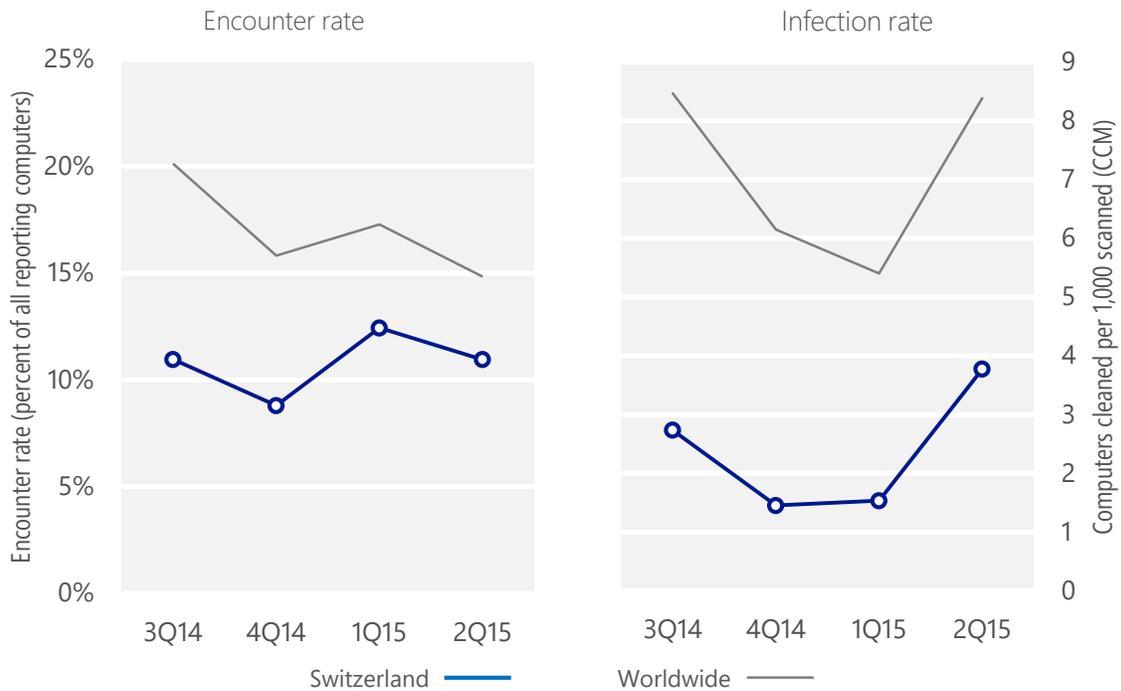
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Switzerland	11.0%	8.8%	12.4%	11.0%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Switzerland	2.7	1.5	1.5	3.8
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcout, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 11.0% of computers in Switzerland encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 3.8 of every 1,000 unique computers scanned in Switzerland in 2Q15 (a CCM score of 3.8, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Switzerland over the last four quarters, compared to the world as a whole.

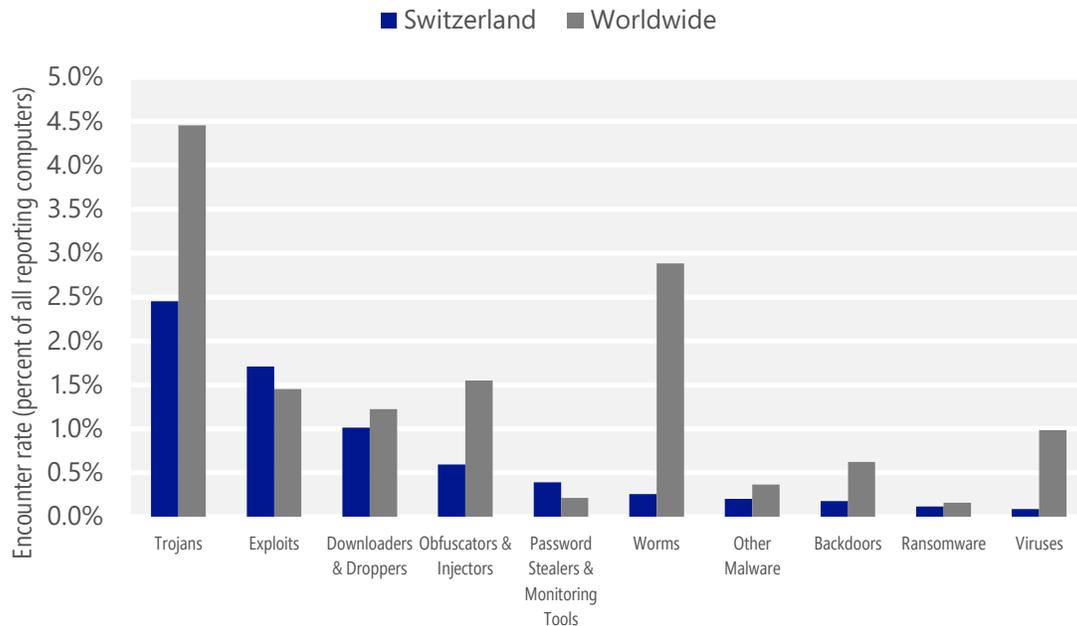
Malware encounter and infection rate trends in Switzerland and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in Switzerland and around the world, and for explanations of the methods and terms used here.

Malware categories

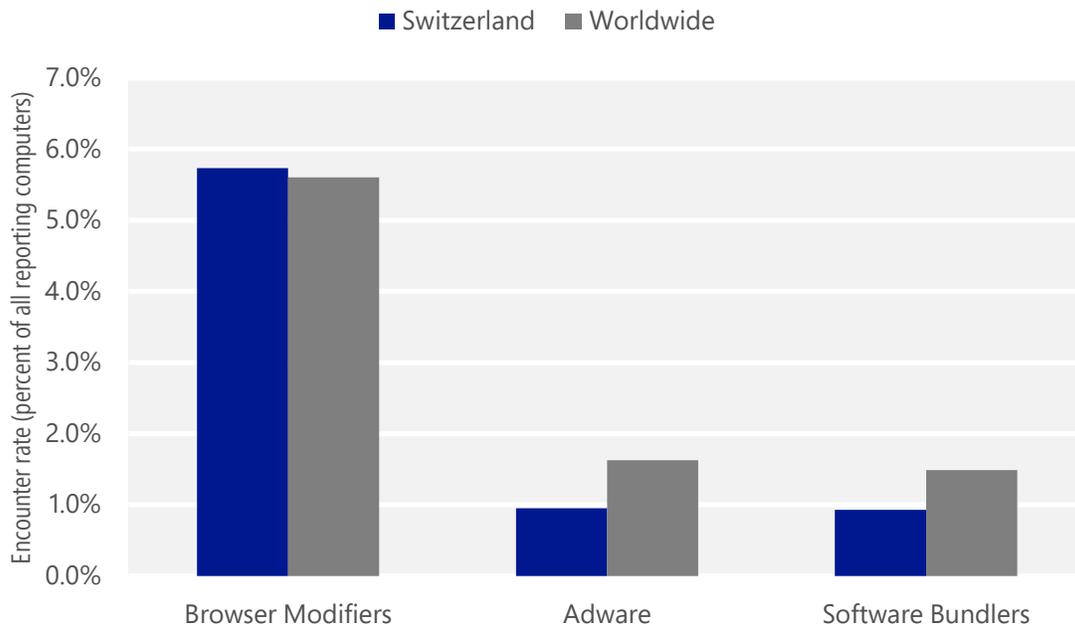
Malware encountered in Switzerland in 2Q15, by category



- The most common malware category in Switzerland in 2Q15 was Trojans. It was encountered by 2.5 percent of all computers there, down from 2.5 percent in 1Q15.
- The second most common malware category in Switzerland in 2Q15 was Exploits. It was encountered by 1.7 percent of all computers there, up from 1.6 percent in 1Q15.
- The third most common malware category in Switzerland in 2Q15 was Downloaders & Droppers, which was encountered by 1.0 percent of all computers there, up from 0.9 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Switzerland in 2Q15, by category



- The most common unwanted software category in Switzerland in 2Q15 was Browser Modifiers. It was encountered by 5.7 percent of all computers there, down from 6.1 percent in 1Q15.
- The second most common unwanted software category in Switzerland in 2Q15 was Adware. It was encountered by 1.0 percent of all computers there, down from 3.0 percent in 1Q15.
- The third most common unwanted software category in Switzerland in 2Q15 was Software Bundlers, which was encountered by 0.9 percent of all computers there, up from 0.3 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Switzerland in 2Q15

	Family	Most significant category	% of reporting computers
1	JS/Axpergle	Exploits	0.9%
2	HTML/Costacas	Exploits	0.6%
3	Win32/Upatre	Downloaders & Droppers	0.6%
4	Win32/Peals	Trojans	0.5%
5	Win32/Skeeyah	Trojans	0.5%
6	Win32/Obfuscator	Obfuscators & Injectors	0.4%
7	Win32/Kilim	Trojans	0.4%
8	Win32/Dyzap	Password Stealers & Monitoring Tools	0.3%
9	Win32/Emotet	Trojans	0.1%
10	Win32/Dynamer	Trojans	0.1%

- The most common malware family encountered in Switzerland in 2Q15 was [JS/Axpergle](#), which was encountered by 0.9 percent of reporting computers there. [JS/Axpergle](#) is a detection for the Angler exploit kit, which exploits vulnerabilities in recent versions of Internet Explorer, Silverlight, Adobe Flash Player, and Java to install malware.
- The second most common malware family encountered in Switzerland in 2Q15 was [HTML/Costacas](#), which was encountered by 0.6 percent of reporting computers there. [HTML/Costacas](#) is a threat that uses vulnerabilities in Adobe Flash Player and Oracle Java to install malware on the computer.
- The third most common malware family encountered in Switzerland in 2Q15 was [Win32/Upatre](#), which was encountered by 0.6 percent of reporting computers there. [Win32/Upatre](#) is a downloader that installs malware and unwanted software on the affected computer without the user's consent. It is frequently distributed as an attachment to spam email messages.
- The fourth most common malware family encountered in Switzerland in 2Q15 was [Win32/Peals](#), which was encountered by 0.5 percent of reporting computers there. [Win32/Peals](#) is a generic detection for various threats that display trojan characteristics.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Switzerland in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/KipodToolsCby	Browser Modifiers	2.4%
2	Win32/CouponRuc	Browser Modifiers	2.2%
3	Win32/AlterbookSP	Browser Modifiers	1.0%
4	Win32/InstalleRex	Software Bundlers	0.9%
5	Win32/SaverExtension	Adware	0.7%

- The most common unwanted software family encountered in Switzerland in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 2.4 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common unwanted software family encountered in Switzerland in 2Q15 was [Win32/CouponRuc](#), which was encountered by 2.2 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The third most common unwanted software family encountered in Switzerland in 2Q15 was [Win32/AlterbookSP](#), which was encountered by 1.0 percent of reporting computers there. [Win32/AlterbookSP](#) is a browser add-on that formerly displayed behaviors of unwanted software. Recent versions of the add-on no longer meet Microsoft detection criteria, and are no longer considered unwanted software.

Top threat families by infection rate

The most common malware families by infection rate in Switzerland in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	1.4
2	Win32/Kilim	Trojans	0.7
3	Win32/CompromisedCert	Other Malware	0.4
4	Win32/Dyzap	Password Stealers & Monitoring Tools	0.3
5	Win32/Carberp	Trojans	0.2
6	Win32/Emotet	Trojans	0.1
7	Win32/Zbot	Password Stealers & Monitoring Tools	0.1
8	Win32/Simda	Trojans	0.1
9	Win32/Nitol	Other Malware	0.1
10	Win32/Alureon	Trojans	<0.1

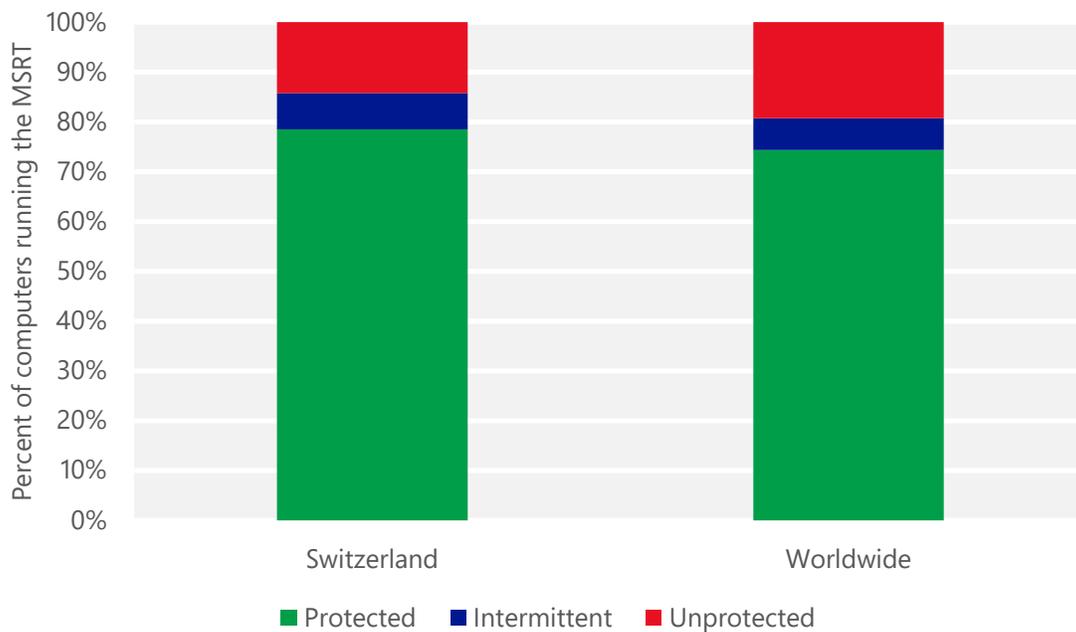
- The most common threat family infecting computers in Switzerland in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 1.4 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Switzerland in 2Q15 was [Win32/Kilim](#), which was detected and removed from 0.7 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The third most common threat family infecting computers in Switzerland in 2Q15 was [Win32/CompromisedCert](#), which was detected and removed from 0.4 of every 1,000 unique computers scanned by the MSRT. [Win32/CompromisedCert](#) is a detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.
- The fourth most common threat family infecting computers in Switzerland in 2Q15 was [Win32/Dyzap](#), which was detected and removed from 0.3 of every 1,000 unique computers scanned by the MSRT. [Win32/Dyzap](#) is a threat that steals login credentials for a long list of banking websites using man-in-the-browser (MITB) attacks. It is usually installed on the infected computer by TrojanDownloader:Win32/Upatre.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Switzerland and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Switzerland

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.09 (0.28)	0.11 (0.24)
Phishing sites per 1,000 hosts (Worldwide)		3.94 (5.0)
Malware hosting sites per 1,000 hosts (Worldwide)		8.22 (16.7)

Taiwan

The statistics presented here are generated by Microsoft security programs and services running on computers in Taiwan in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Taiwan

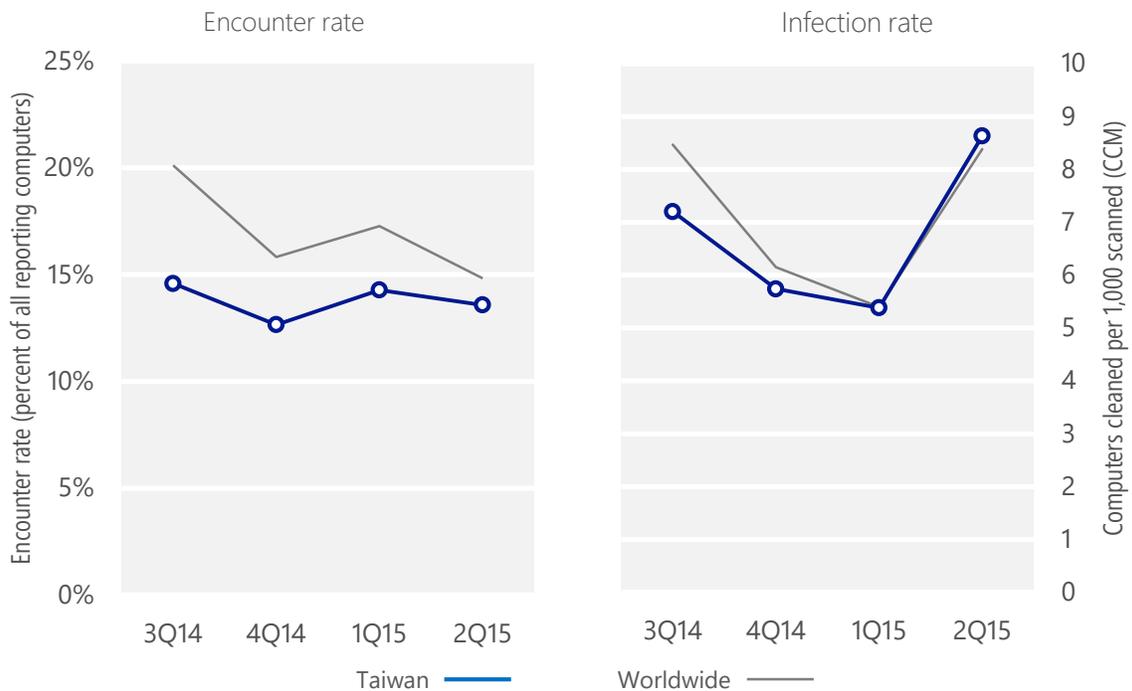
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Taiwan	14.6%	12.7%	14.3%	13.6%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Taiwan	7.2	5.7	5.4	8.6
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcote, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 13.6% of computers in Taiwan encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 8.6 of every 1,000 unique computers scanned in Taiwan in 2Q15 (a CCM score of 8.6, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Taiwan over the last four quarters, compared to the world as a whole.

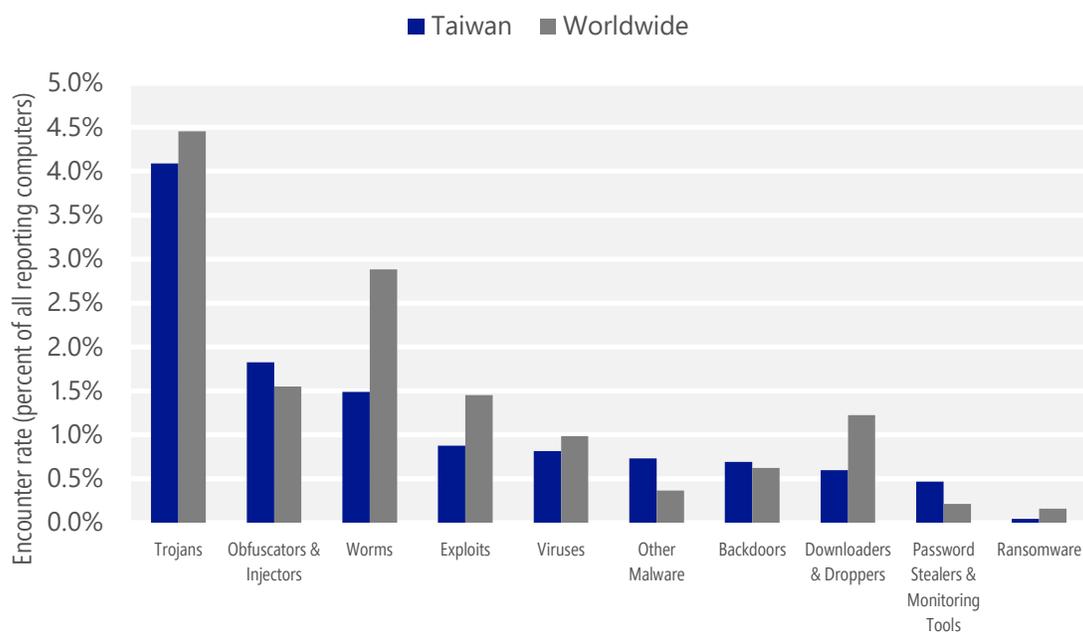
Malware encounter and infection rate trends in Taiwan and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in Taiwan and around the world, and for explanations of the methods and terms used here.

Malware categories

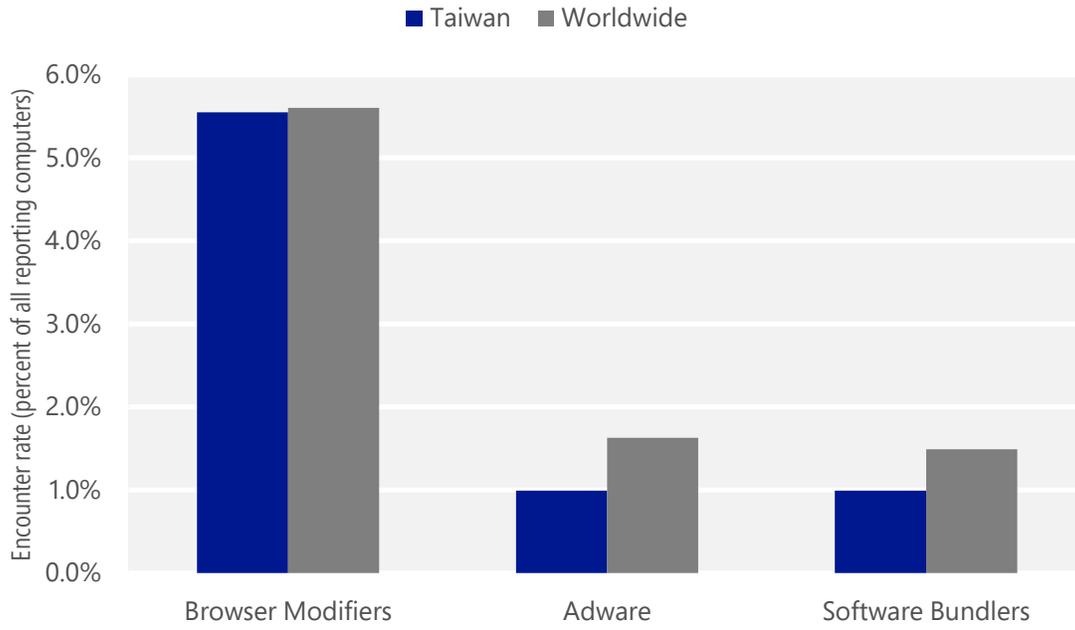
Malware encountered in Taiwan in 2Q15, by category



- The most common malware category in Taiwan in 2Q15 was Trojans. It was encountered by 4.1 percent of all computers there, up from 3.4 percent in 1Q15.
- The second most common malware category in Taiwan in 2Q15 was Obfuscators & Injectors. It was encountered by 1.8 percent of all computers there, down from 2.1 percent in 1Q15.
- The third most common malware category in Taiwan in 2Q15 was Worms, which was encountered by 1.5 percent of all computers there, down from 1.8 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Taiwan in 2Q15, by category



- The most common unwanted software category in Taiwan in 2Q15 was Browser Modifiers. It was encountered by 5.6 percent of all computers there, down from 5.9 percent in 1Q15.
- The second most common unwanted software category in Taiwan in 2Q15 was Adware. It was encountered by 1.0 percent of all computers there, down from 2.5 percent in 1Q15.
- The third most common unwanted software category in Taiwan in 2Q15 was Software Bundlers, which was encountered by 1.0 percent of all computers there, up from 0.3 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Taiwan in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Obfuscator	Obfuscators & Injectors	1.3%
2	INF/Autorun	Obfuscators & Injectors	0.7%
3	Win32/Nitol	Other Malware	0.6%
4	MSIL/Hakey	Trojans	0.6%
5	Win32/Kilim	Trojans	0.5%
6	Win32/Skeeyah	Trojans	0.5%
7	JS/Axpergle	Exploits	0.4%
8	Win32/Conficker	Worms	0.3%
9	VBS/Jenxcus	Worms	0.3%
10	Win32/Dynamer	Trojans	0.3%

- The most common malware family encountered in Taiwan in 2Q15 was [Win32/Obfuscator](#), which was encountered by 1.3 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The second most common malware family encountered in Taiwan in 2Q15 was [INF/Autorun](#), which was encountered by 0.7 percent of reporting computers there. [INF/Autorun](#) is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The third most common malware family encountered in Taiwan in 2Q15 was [Win32/Nitol](#), which was encountered by 0.6 percent of reporting computers there. [Win32/Nitol](#) is a family of trojans that perform DDoS (distributed denial of service) attacks, allow backdoor access and control, download and run files, and perform a number of other malicious activities on the computer.
- The fourth most common malware family encountered in Taiwan in 2Q15 was [MSIL/Hakey](#), which was encountered by 0.6 percent of reporting computers there. [MSIL/Hakey](#) is a threat that can watch and record what the user does on the computer and send this information to an attacker.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Taiwan in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	2.2%
2	Win32/KipodToolsCby	Browser Modifiers	2.0%
3	Win32/AlterbookSP	Browser Modifiers	1.4%
4	Win32/InstalleRex	Software Bundlers	1.0%
5	Win32/SaverExtension	Adware	0.8%

- The most common unwanted software family encountered in Taiwan in 2Q15 was [Win32/CouponRuc](#), which was encountered by 2.2 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in Taiwan in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 2.0 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common unwanted software family encountered in Taiwan in 2Q15 was [Win32/AlterbookSP](#), which was encountered by 1.4 percent of reporting computers there. [Win32/AlterbookSP](#) is a browser add-on that formerly displayed behaviors of unwanted software. Recent versions of the add-on no longer meet Microsoft detection criteria, and are no longer considered unwanted software.

Top threat families by infection rate

The most common malware families by infection rate in Taiwan in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/Nitol	Other Malware	2.2
2	Win32/Kilim	Trojans	1.2
3	Win32/leEnablerCby	Browser Modifiers	1.1
4	Win32/Winnti	Trojans	0.8
5	Win32/Sality	Viruses	0.5
6	Win32/Ramnit	Trojans	0.4
7	VBS/Jenxcus	Worms	0.4
8	Win32/Hupigon	Backdoors	0.3
9	Win32/Frethog	Password Stealers & Monitoring Tools	0.2
10	Win32/Taterf	Worms	0.2

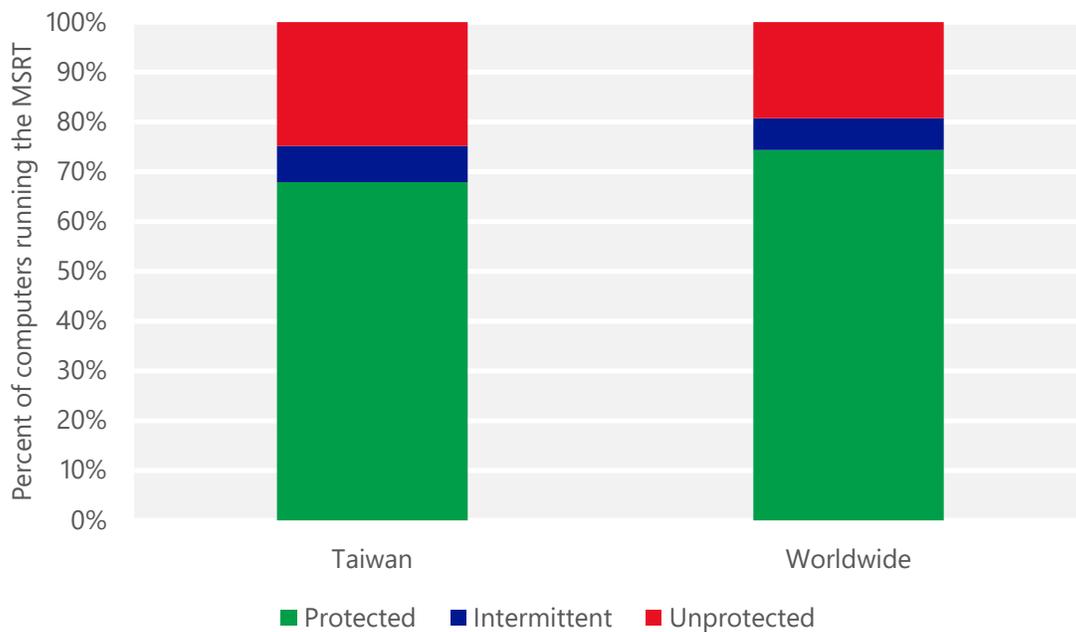
- The most common threat family infecting computers in Taiwan in 2Q15 was [Win32/Nitol](#), which was detected and removed from 2.2 of every 1,000 unique computers scanned by the MSRT. [Win32/Nitol](#) is a family of trojans that perform DDoS (distributed denial of service) attacks, allow backdoor access and control, download and run files, and perform a number of other malicious activities on the computer.
- The second most common threat family infecting computers in Taiwan in 2Q15 was [Win32/Kilim](#), which was detected and removed from 1.2 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The third most common threat family infecting computers in Taiwan in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 1.1 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The fourth most common threat family infecting computers in Taiwan in 2Q15 was [Win32/Winnti](#), which was detected and removed from 0.8 of every 1,000 unique computers scanned by the MSRT. [Win32/Winnti](#) is a trojan that opens a remote connection to an attacker, who can execute remote commands on the computer, download and run other malware, delete files, and perform other malicious activities.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Taiwan and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Taiwan

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.10 (0.28)	0.09 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	1.21 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	2.82 (16.7)	

Tanzania

The statistics presented here are generated by Microsoft security programs and services running on computers in Tanzania in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Tanzania

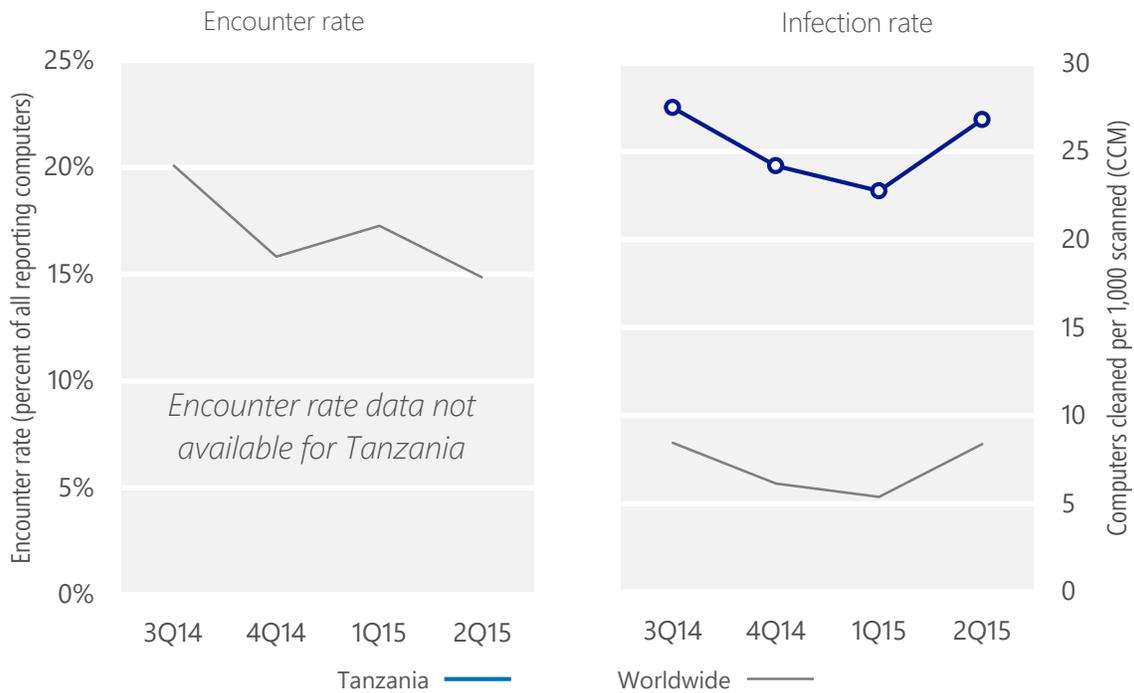
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Tanzania	N/A	N/A	N/A	N/A
<i>Worldwide encounter rate</i>	20.1%	15.8%	17.3%	14.8%
CCM, Tanzania	27.5	24.2	22.7	26.8
<i>Worldwide CCM</i>	8.5	6.1	5.4	8.4

Encounter and infection rates reported here do not include totals for the Brantall, Filcote, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, the MSRT detected and removed malware from 26.8 of every 1,000 unique computers scanned in Tanzania in 2Q15 (a CCM score of 26.8, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Tanzania over the last four quarters, compared to the world as a whole.

Malware encounter and infection rate trends in Tanzania and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in Tanzania and around the world, and for explanations of the methods and terms used here.

Top threat families by infection rate

The most common malware families by infection rate in Tanzania in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/Gamarue	Worms	8.6
2	VBS/Jenxcus	Worms	5.9
3	Win32/Sality	Viruses	4.8
4	Win32/leEnablerCby	Browser Modifiers	2.8
5	Win32/Ramnit	Trojans	1.6
6	Win32/Chir	Viruses	1.4
7	Win32/Virut	Viruses	1.1
8	Win32/Dorkbot	Worms	0.6
9	Win32/Nuqel	Worms	0.5
10	Win32/Kilim	Trojans	0.4

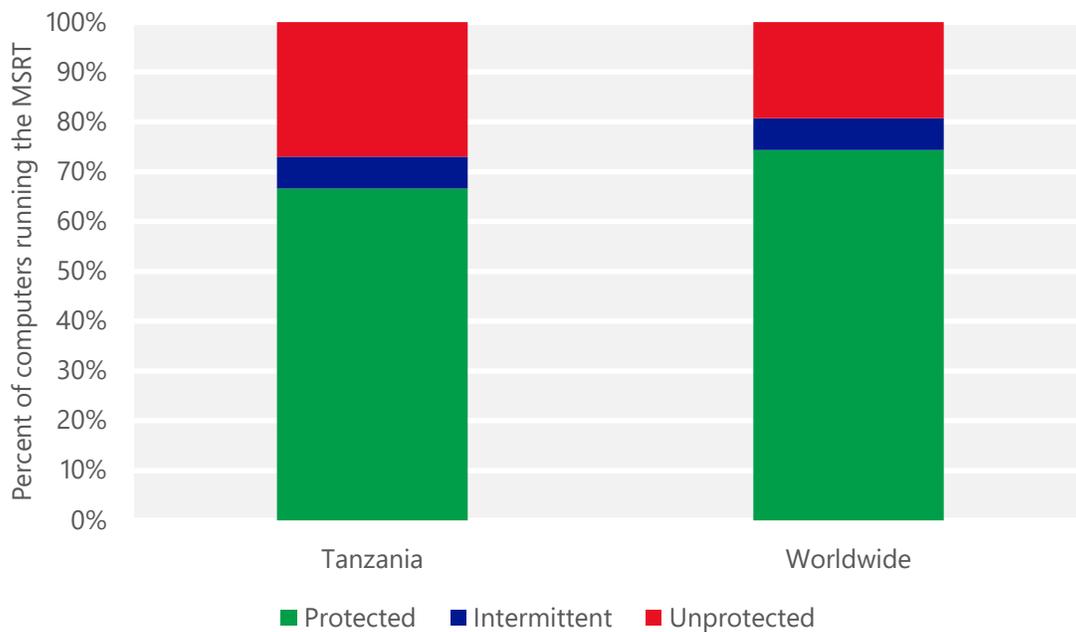
- The most common threat family infecting computers in Tanzania in 2Q15 was [Win32/Gamarue](#), which was detected and removed from 8.6 of every 1,000 unique computers scanned by the MSRT. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The second most common threat family infecting computers in Tanzania in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 5.9 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The third most common threat family infecting computers in Tanzania in 2Q15 was [Win32/Sality](#), which was detected and removed from 4.8 of every 1,000 unique computers scanned by the MSRT. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The fourth most common threat family infecting computers in Tanzania in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 2.8 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Tanzania and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Tanzania

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	3.27 (0.28)	3.71 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	3.17 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	10.78 (16.7)	

Thailand

The statistics presented here are generated by Microsoft security programs and services running on computers in Thailand in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Thailand

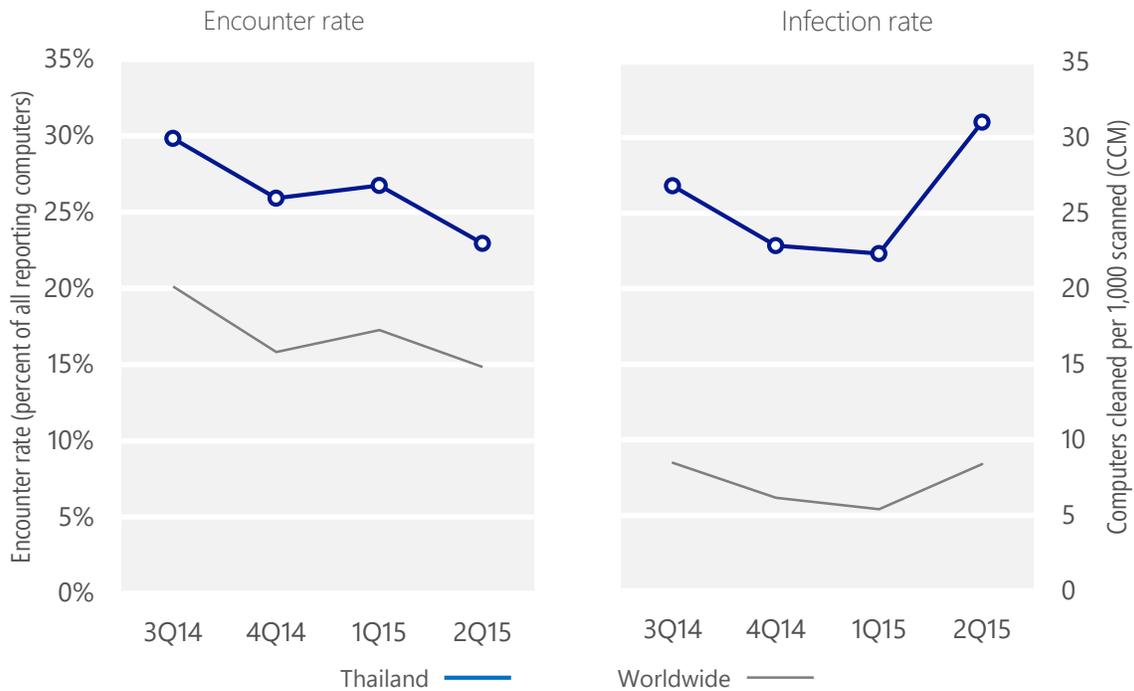
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Thailand	29.8%	25.9%	26.8%	22.9%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Thailand	26.8	22.9	22.3	31.0
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcote, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 22.9% of computers in Thailand encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 31.0 of every 1,000 unique computers scanned in Thailand in 2Q15 (a CCM score of 31.0, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Thailand over the last four quarters, compared to the world as a whole.

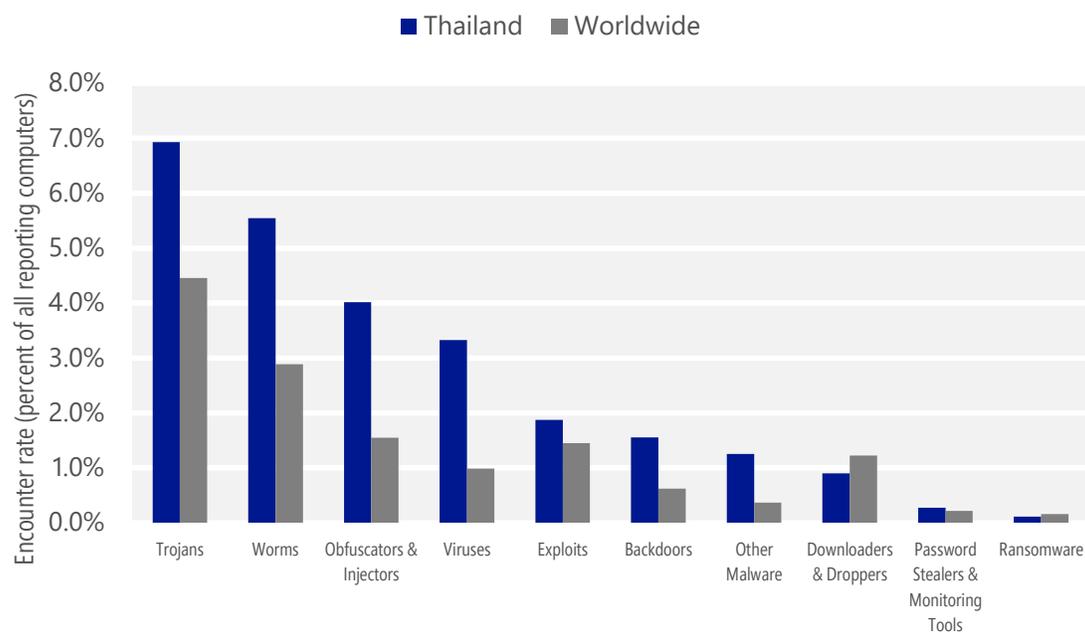
Malware encounter and infection rate trends in Thailand and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in Thailand and around the world, and for explanations of the methods and terms used here.

Malware categories

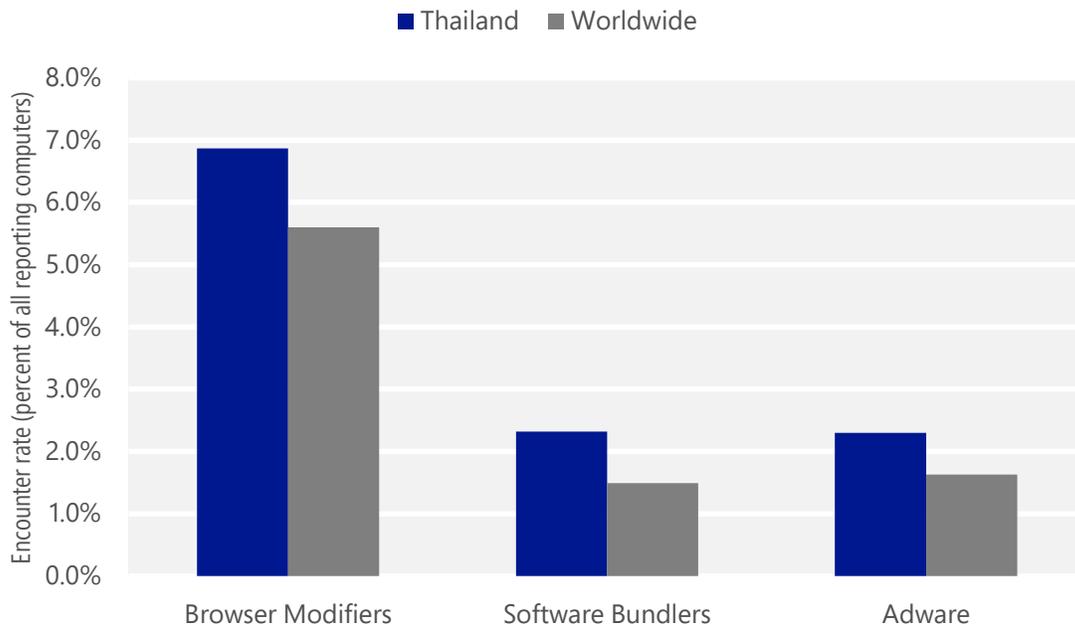
Malware encountered in Thailand in 2Q15, by category



- The most common malware category in Thailand in 2Q15 was Trojans. It was encountered by 6.9 percent of all computers there, down from 7.7 percent in 1Q15.
- The second most common malware category in Thailand in 2Q15 was Worms. It was encountered by 5.5 percent of all computers there, up from 5.3 percent in 1Q15.
- The third most common malware category in Thailand in 2Q15 was Obfuscators & Injectors, which was encountered by 4.0 percent of all computers there, down from 4.9 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Thailand in 2Q15, by category



- The most common unwanted software category in Thailand in 2Q15 was Browser Modifiers. It was encountered by 6.9 percent of all computers there, down from 9.7 percent in 1Q15.
- The second most common unwanted software category in Thailand in 2Q15 was Software Bundlers. It was encountered by 2.3 percent of all computers there, down from 5.1 percent in 1Q15.
- The third most common unwanted software category in Thailand in 2Q15 was Adware, which was encountered by 2.3 percent of all computers there, up from 0.7 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Thailand in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Gamarue	Worms	2.7%
2	Win32/Obfuscator	Obfuscators & Injectors	2.7%
3	Win32/Sality	Viruses	1.4%
4	Win32/Ramnit	Trojans	1.2%
5	Win32/Kilim	Trojans	1.2%
6	INF/Autorun	Obfuscators & Injectors	1.2%
7	Win32/Skeeyah	Trojans	0.8%
8	VBS/Jenxcus	Worms	0.7%
9	Win32/Xorer	Viruses	0.7%
10	Win32/Nitol	Other Malware	0.7%

- The most common malware family encountered in Thailand in 2Q15 was [Win32/Gamarue](#), which was encountered by 2.7 percent of reporting computers there. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The second most common malware family encountered in Thailand in 2Q15 was [Win32/Obfuscator](#), which was encountered by 2.7 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The third most common malware family encountered in Thailand in 2Q15 was [Win32/Sality](#), which was encountered by 1.4 percent of reporting computers there. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The fourth most common malware family encountered in Thailand in 2Q15 was [Win32/Ramnit](#), which was encountered by 1.2 percent of reporting computers there. [Win32/Ramnit](#) is a family of multi-component malware that infects executable files, Microsoft Office files, and HTML files. Win32/Ramnit spreads to removable drives and steals sensitive information such as saved FTP credentials and browser cookies. It may also open a backdoor to await instructions from a remote attacker.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Thailand in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	4.0%
2	Win32/KipodToolsCby	Browser Modifiers	2.6%
3	Win32/InstalleRex	Software Bundlers	2.2%
4	Win32/SaverExtension	Adware	1.6%
5	Win32/AlterbookSP	Browser Modifiers	0.4%

- The most common unwanted software family encountered in Thailand in 2Q15 was [Win32/CouponRuc](#), which was encountered by 4.0 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in Thailand in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 2.6 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common unwanted software family encountered in Thailand in 2Q15 was [Win32/InstalleRex](#), which was encountered by 2.2 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Thailand in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	7.7
2	Win32/Sality	Viruses	5.4
3	Win32/Gamarue	Worms	3.7
4	Win32/Ramnit	Trojans	3.2
5	Win32/Kilim	Trojans	2.4
6	MSIL/Bladabindi	Backdoors	2.2
7	Win32/Nitol	Other Malware	1.8
8	VBS/Jenxcus	Worms	1.5
9	Win32/CompromisedCert	Other Malware	1.2
10	Win32/Carberp	Trojans	0.7

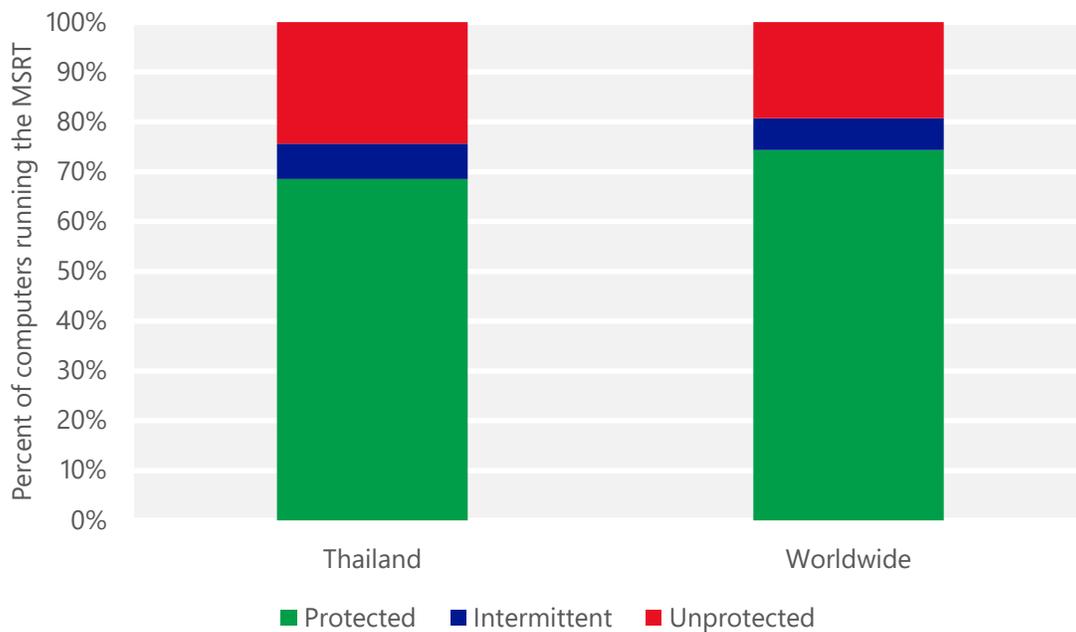
- The most common threat family infecting computers in Thailand in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 7.7 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Thailand in 2Q15 was [Win32/Sality](#), which was detected and removed from 5.4 of every 1,000 unique computers scanned by the MSRT. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The third most common threat family infecting computers in Thailand in 2Q15 was [Win32/Gamarue](#), which was detected and removed from 3.7 of every 1,000 unique computers scanned by the MSRT. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The fourth most common threat family infecting computers in Thailand in 2Q15 was [Win32/Ramnit](#), which was detected and removed from 3.2 of every 1,000 unique computers scanned by the MSRT. [Win32/Ramnit](#) is a family of multi-component malware that infects executable files, Microsoft Office files, and HTML files. Win32/Ramnit spreads to removable drives and steals sensitive information such as saved FTP credentials and browser cookies. It may also open a backdoor to await instructions from a remote attacker.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Thailand and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Thailand

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.91 (0.28)	0.19 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	5.77 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	14.30 (16.7)	

Trinidad and Tobago

The statistics presented here are generated by Microsoft security programs and services running on computers in Trinidad and Tobago in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Trinidad and Tobago

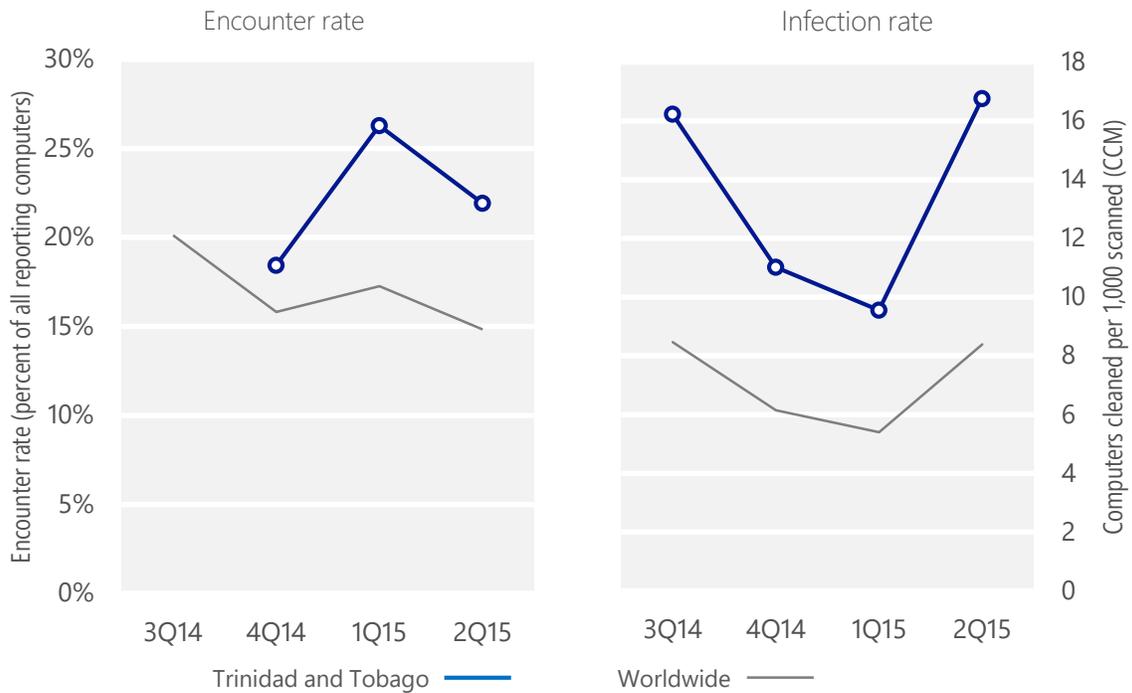
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Trinidad and Tobago	N/A	18.4%	26.3%	21.9%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Trinidad and Tobago	16.2	11.0	9.6	16.8
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcote, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 21.9% of computers in Trinidad and Tobago encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 16.8 of every 1,000 unique computers scanned in Trinidad and Tobago in 2Q15 (a CCM score of 16.8, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Trinidad and Tobago over the last four quarters, compared to the world as a whole.

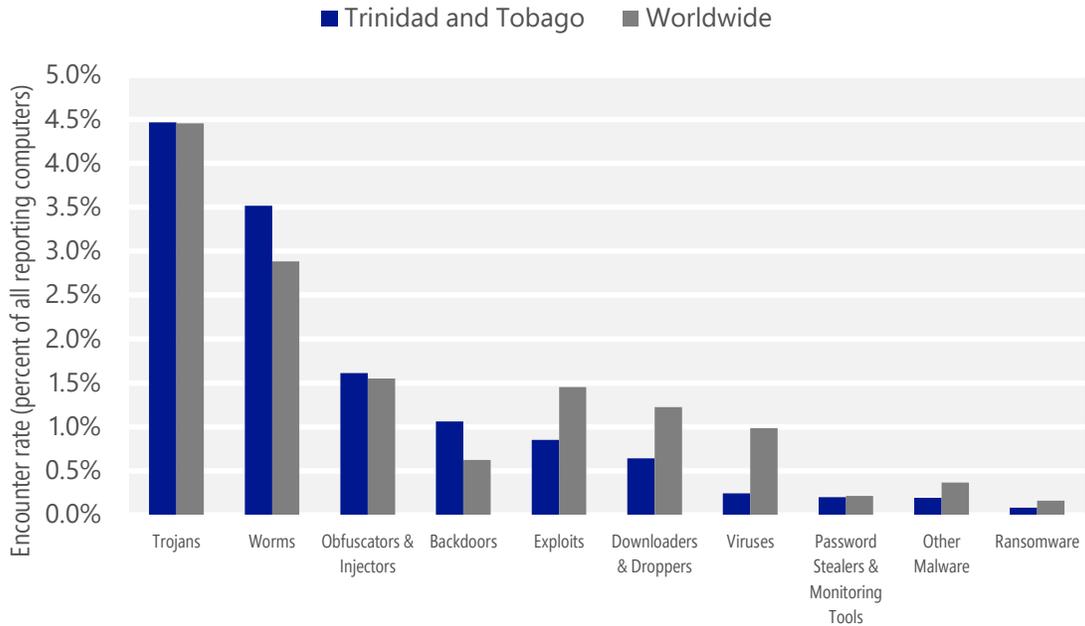
Malware encounter and infection rate trends in Trinidad and Tobago and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in Trinidad and Tobago and around the world, and for explanations of the methods and terms used here.

Malware categories

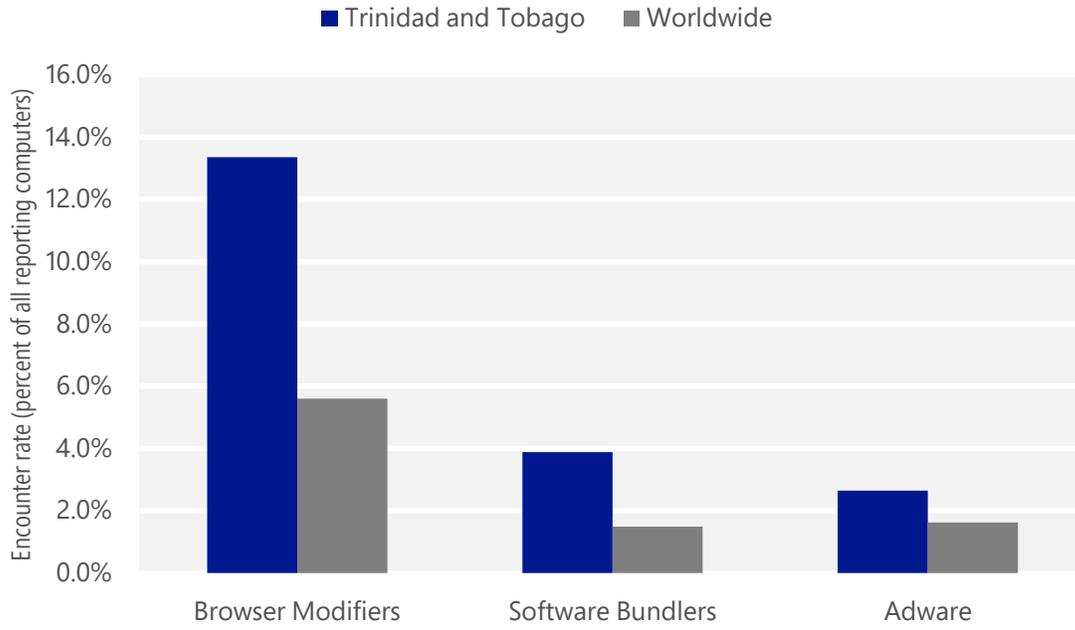
Malware encountered in Trinidad and Tobago in 2Q15, by category



- The most common malware category in Trinidad and Tobago in 2Q15 was Trojans. It was encountered by 4.5 percent of all computers there, down from 4.9 percent in 1Q15.
- The second most common malware category in Trinidad and Tobago in 2Q15 was Worms. It was encountered by 3.5 percent of all computers there, up from 2.9 percent in 1Q15.
- The third most common malware category in Trinidad and Tobago in 2Q15 was Obfuscators & Injectors, which was encountered by 1.6 percent of all computers there, down from 1.9 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Trinidad and Tobago in 2Q15, by category



- The most common unwanted software category in Trinidad and Tobago in 2Q15 was Browser Modifiers. It was encountered by 13.4 percent of all computers there, down from 17.7 percent in 1Q15.
- The second most common unwanted software category in Trinidad and Tobago in 2Q15 was Software Bundlers. It was encountered by 3.9 percent of all computers there, down from 5.9 percent in 1Q15.
- The third most common unwanted software category in Trinidad and Tobago in 2Q15 was Adware, which was encountered by 2.6 percent of all computers there, up from 1.3 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Trinidad and Tobago in 2Q15

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	2.1%
2	Win32/Kilim	Trojans	1.5%
3	Win32/Skeeyah	Trojans	1.0%
4	Win32/Obfuscator	Obfuscators & Injectors	1.0%
5	INF/Autorun	Obfuscators & Injectors	0.6%
6	MSIL/Bladabindi	Backdoors	0.4%
7	Win32/Peals	Trojans	0.4%
8	Win32/Caphaw	Backdoors	0.4%
9	Win32/Vobfus	Worms	0.3%
10	Win32/Sdbby	Exploits	0.3%

- The most common malware family encountered in Trinidad and Tobago in 2Q15 was [VBS/Jenxcus](#), which was encountered by 2.1 percent of reporting computers there. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common malware family encountered in Trinidad and Tobago in 2Q15 was [Win32/Kilim](#), which was encountered by 1.5 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The third most common malware family encountered in Trinidad and Tobago in 2Q15 was [Win32/Skeeyah](#), which was encountered by 1.0 percent of reporting computers there. [Win32/Skeeyah](#) is a generic detection for various threats that display trojan characteristics.
- The fourth most common malware family encountered in Trinidad and Tobago in 2Q15 was [Win32/Obfuscator](#), which was encountered by 1.0 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Trinidad and Tobago in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/KipodToolsCby	Browser Modifiers	7.5%
2	Win32/CouponRuc	Browser Modifiers	5.9%
3	Win32/InstalleRex	Software Bundlers	3.7%
4	Win32/SaverExtension	Adware	2.0%
5	Win32/AlterbookSP	Browser Modifiers	0.8%

- The most common unwanted software family encountered in Trinidad and Tobago in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 7.5 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common unwanted software family encountered in Trinidad and Tobago in 2Q15 was [Win32/CouponRuc](#), which was encountered by 5.9 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The third most common unwanted software family encountered in Trinidad and Tobago in 2Q15 was [Win32/InstalleRex](#), which was encountered by 3.7 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Trinidad and Tobago in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	6.9
2	VBS/Jenxcus	Worms	3.8
3	Win32/Kilim	Trojans	2.0
4	MSIL/Bladabindi	Backdoors	0.7
5	Win32/Brontok	Worms	0.6
6	Win32/Dorkbot	Worms	0.5
7	Win32/IRCbot	Backdoors	0.5
8	Win32/Vobfus	Worms	0.4
9	Win32/CompromisedCert	Other Malware	0.4
10	Win32/Lethic	Trojans	0.3

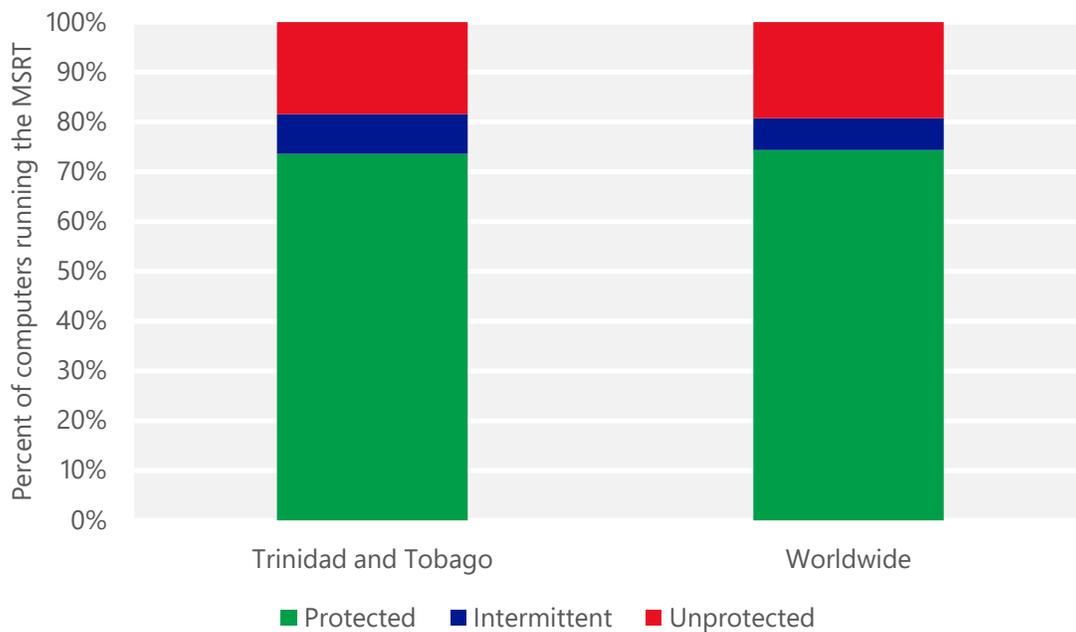
- The most common threat family infecting computers in Trinidad and Tobago in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 6.9 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Trinidad and Tobago in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 3.8 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The third most common threat family infecting computers in Trinidad and Tobago in 2Q15 was [Win32/Kilim](#), which was detected and removed from 2.0 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The fourth most common threat family infecting computers in Trinidad and Tobago in 2Q15 was [MSIL/Bladabindi](#), which was detected and removed from 0.7 of every 1,000 unique computers scanned by the MSRT. [MSIL/Bladabindi](#) is a family of backdoors created by a malicious hacker tool called NJ Rat. The can steal sensitive information, download other malware, and allow backdoor access to an infected computer.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Trinidad and Tobago and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Trinidad and Tobago

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.00 (0.28)	0.00 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	19.01 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	32.05 (16.7)	

Tunisia

The statistics presented here are generated by Microsoft security programs and services running on computers in Tunisia in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Tunisia

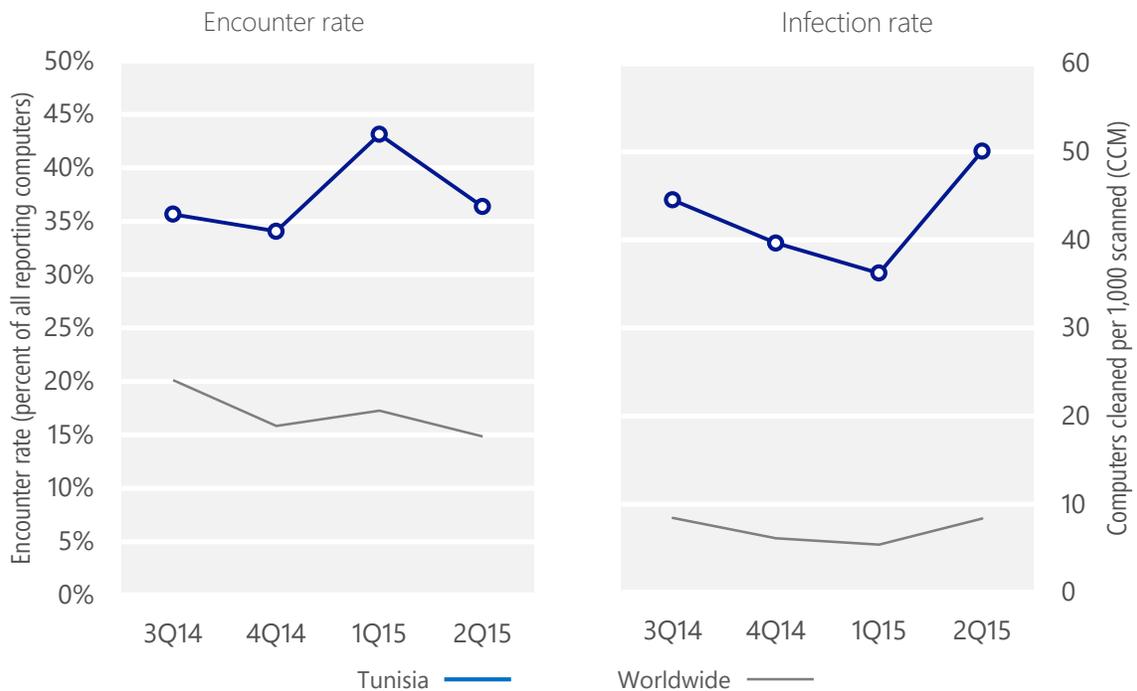
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Tunisia	35.7%	34.1%	43.1%	36.4%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Tunisia	44.5	39.7	36.2	50.1
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcote, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 36.4% of computers in Tunisia encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 50.1 of every 1,000 unique computers scanned in Tunisia in 2Q15 (a CCM score of 50.1, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Tunisia over the last four quarters, compared to the world as a whole.

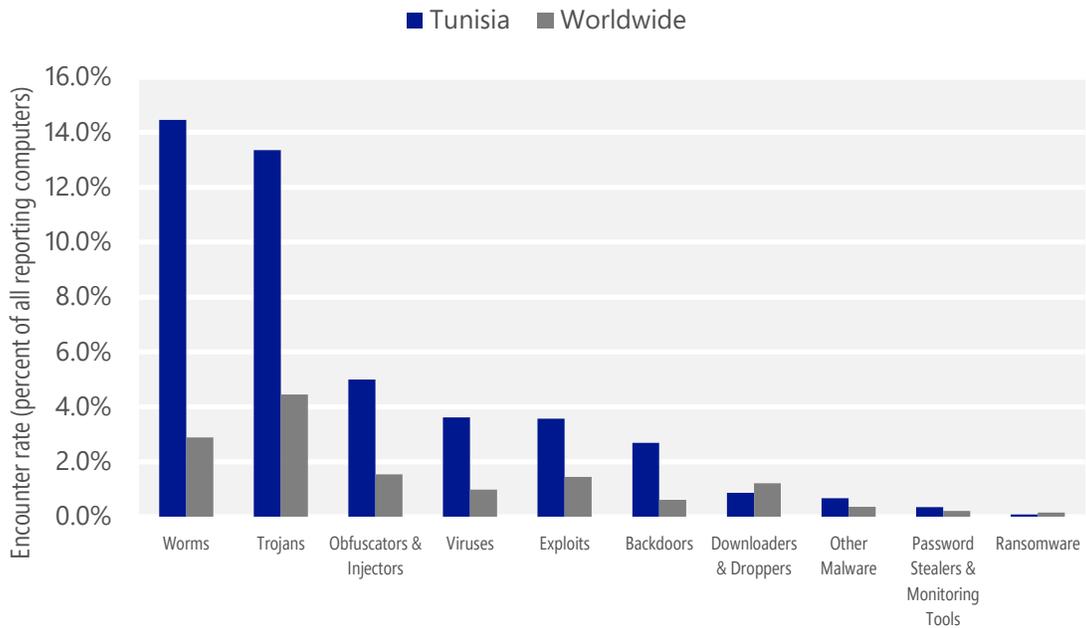
Malware encounter and infection rate trends in Tunisia and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in Tunisia and around the world, and for explanations of the methods and terms used here.

Malware categories

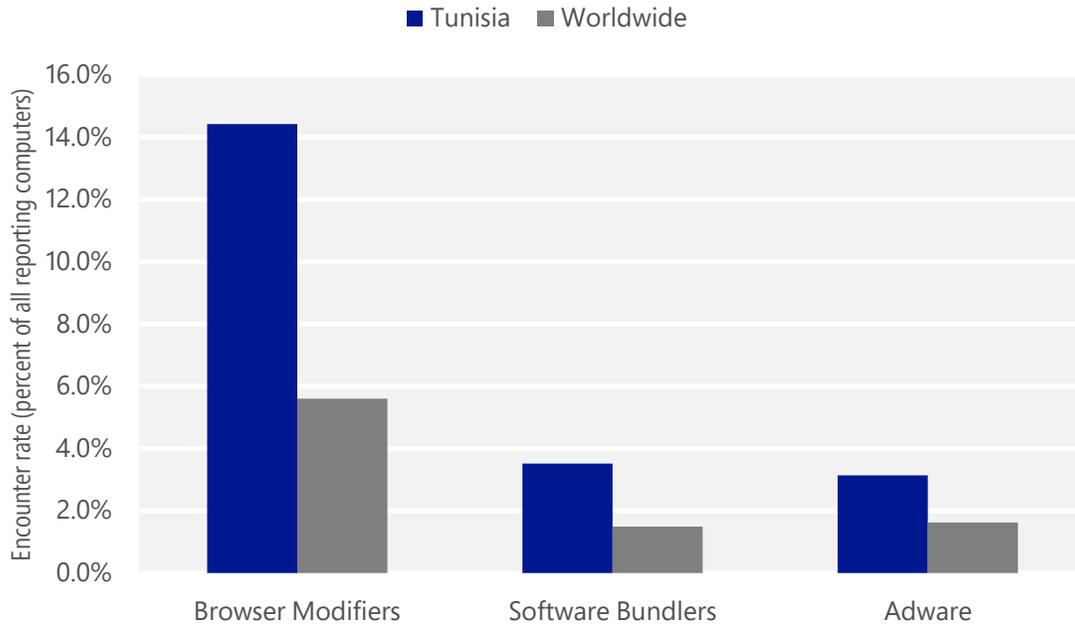
Malware encountered in Tunisia in 2Q15, by category



- The most common malware category in Tunisia in 2Q15 was Worms. It was encountered by 14.5 percent of all computers there, up from 14.3 percent in 1Q15.
- The second most common malware category in Tunisia in 2Q15 was Trojans. It was encountered by 13.4 percent of all computers there, down from 14.1 percent in 1Q15.
- The third most common malware category in Tunisia in 2Q15 was Obfuscators & Injectors, which was encountered by 5.0 percent of all computers there, down from 5.8 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Tunisia in 2Q15, by category



- The most common unwanted software category in Tunisia in 2Q15 was Browser Modifiers. It was encountered by 14.4 percent of all computers there, down from 22.2 percent in 1Q15.
- The second most common unwanted software category in Tunisia in 2Q15 was Software Bundlers. It was encountered by 3.5 percent of all computers there, down from 7.0 percent in 1Q15.
- The third most common unwanted software category in Tunisia in 2Q15 was Adware, which was encountered by 3.1 percent of all computers there, up from 2.2 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Tunisia in 2Q15

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	8.8%
2	JS/Faceliker	Trojans	3.6%
3	INF/Autorun	Obfuscators & Injectors	3.4%
4	Win32/Ippedo	Worms	3.2%
5	Win32/CplLnk	Exploits	3.0%
6	Win32/Ramnit	Trojans	2.8%
7	Win32/Kilim	Trojans	2.7%
8	Win32/Obfuscator	Obfuscators & Injectors	2.4%
9	Win32/Sality	Viruses	1.9%
10	MSIL/Bladabindi	Backdoors	1.5%

- The most common malware family encountered in Tunisia in 2Q15 was [VBS/Jenxcus](#), which was encountered by 8.8 percent of reporting computers there. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common malware family encountered in Tunisia in 2Q15 was [JS/Faceliker](#), which was encountered by 3.6 percent of reporting computers there. [JS/Faceliker](#) is a malicious script that “likes” content on Facebook without the user’s knowledge or consent.
- The third most common malware family encountered in Tunisia in 2Q15 was [INF/Autorun](#), which was encountered by 3.4 percent of reporting computers there. [INF/Autorun](#) is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The fourth most common malware family encountered in Tunisia in 2Q15 was [Win32/Ippedo](#), which was encountered by 3.2 percent of reporting computers there. [Win32/Ippedo](#) is a worm that can send sensitive information to a malicious hacker. It spreads through removable drives, such as USB flash drives.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Tunisia in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/KipodToolsCby	Browser Modifiers	7.9%
2	Win32/CouponRuc	Browser Modifiers	6.8%
3	Win32/InstalleRex	Software Bundlers	3.3%
4	Win32/SaverExtension	Adware	2.1%
5	Win32/AlterbookSP	Browser Modifiers	0.5%

- The most common unwanted software family encountered in Tunisia in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 7.9 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common unwanted software family encountered in Tunisia in 2Q15 was [Win32/CouponRuc](#), which was encountered by 6.8 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The third most common unwanted software family encountered in Tunisia in 2Q15 was [Win32/InstalleRex](#), which was encountered by 3.3 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Tunisia in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	19.9
2	Win32/leEnablerCby	Browser Modifiers	9.0
3	Win32/Sality	Viruses	6.8
4	Win32/Ramnit	Trojans	6.2
5	Win32/Kilim	Trojans	3.9
6	MSIL/Bladabindi	Backdoors	3.0
7	Win32/Gamarue	Worms	1.6
8	Win32/Vobfus	Worms	1.5
9	Win32/Dorkbot	Worms	1.4
10	Win32/Pramro	Trojans	0.7

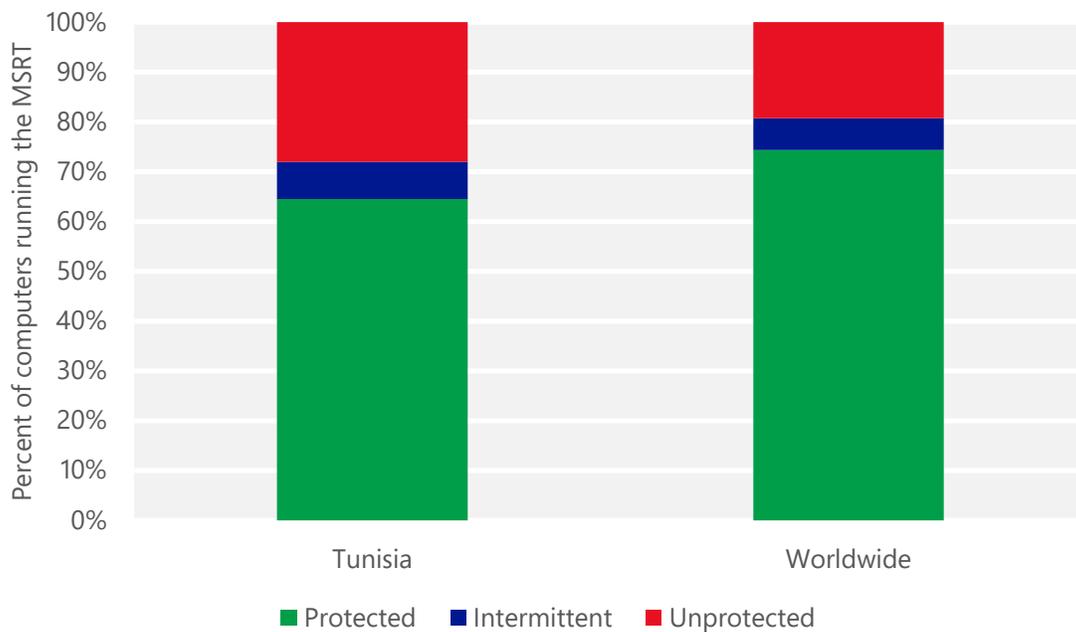
- The most common threat family infecting computers in Tunisia in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 19.9 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Tunisia in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 9.0 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common threat family infecting computers in Tunisia in 2Q15 was [Win32/Sality](#), which was detected and removed from 6.8 of every 1,000 unique computers scanned by the MSRT. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The fourth most common threat family infecting computers in Tunisia in 2Q15 was [Win32/Ramnit](#), which was detected and removed from 6.2 of every 1,000 unique computers scanned by the MSRT. [Win32/Ramnit](#) is a family of multi-component malware that infects executable files, Microsoft Office files, and HTML files. Win32/Ramnit spreads to removable drives and steals sensitive information such as saved FTP credentials and browser cookies. It may also open a backdoor to await instructions from a remote attacker.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Tunisia and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Tunisia

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	6.46 (0.28)	2.18 (0.24)
Phishing sites per 1,000 hosts (Worldwide)		3.81 (5.0)
Malware hosting sites per 1,000 hosts (Worldwide)		8.76 (16.7)

Turkey

The statistics presented here are generated by Microsoft security programs and services running on computers in Turkey in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Turkey

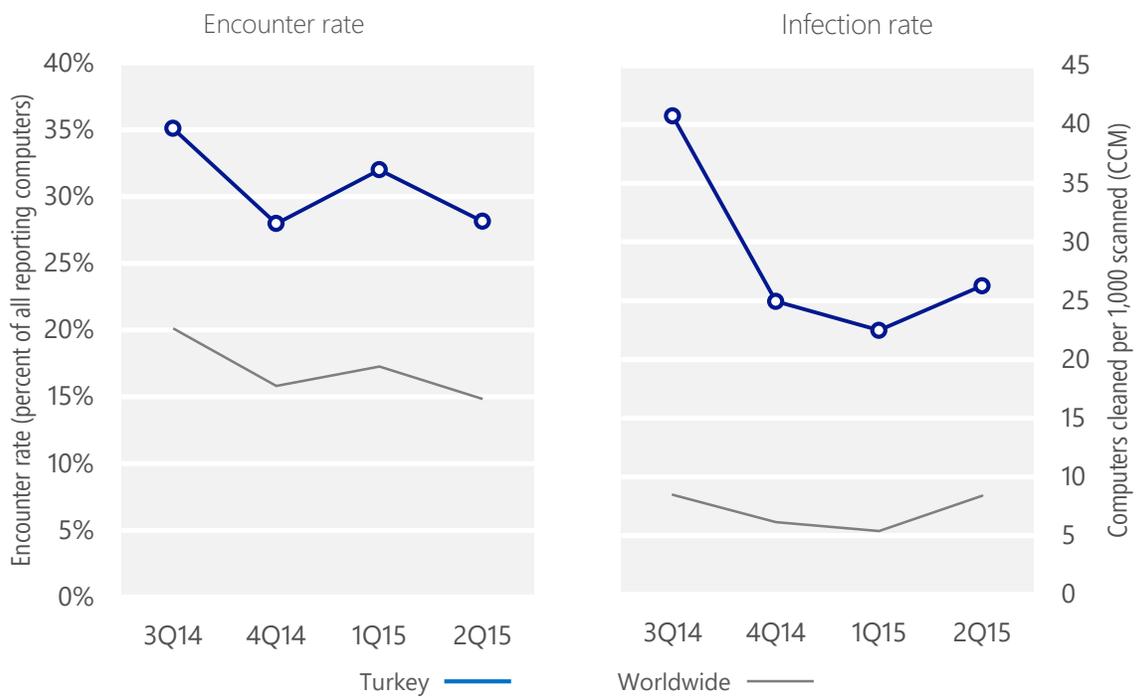
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Turkey	35.1%	28.0%	32.0%	28.1%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Turkey	40.7	24.9	22.5	26.3
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcote, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 28.1% of computers in Turkey encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 26.3 of every 1,000 unique computers scanned in Turkey in 2Q15 (a CCM score of 26.3, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Turkey over the last four quarters, compared to the world as a whole.

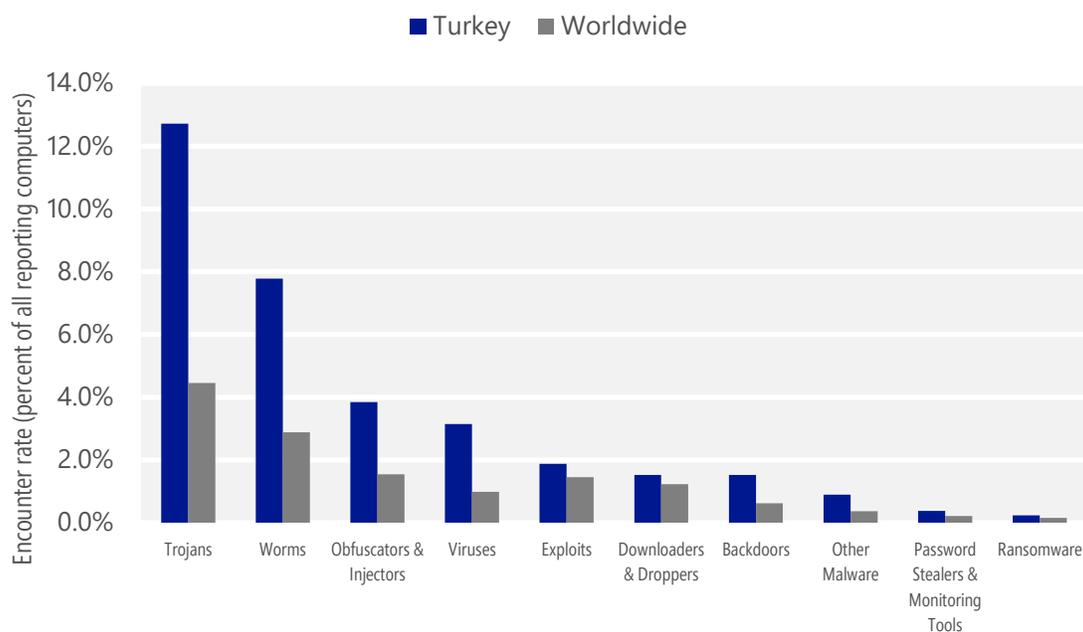
Malware encounter and infection rate trends in Turkey and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in Turkey and around the world, and for explanations of the methods and terms used here.

Malware categories

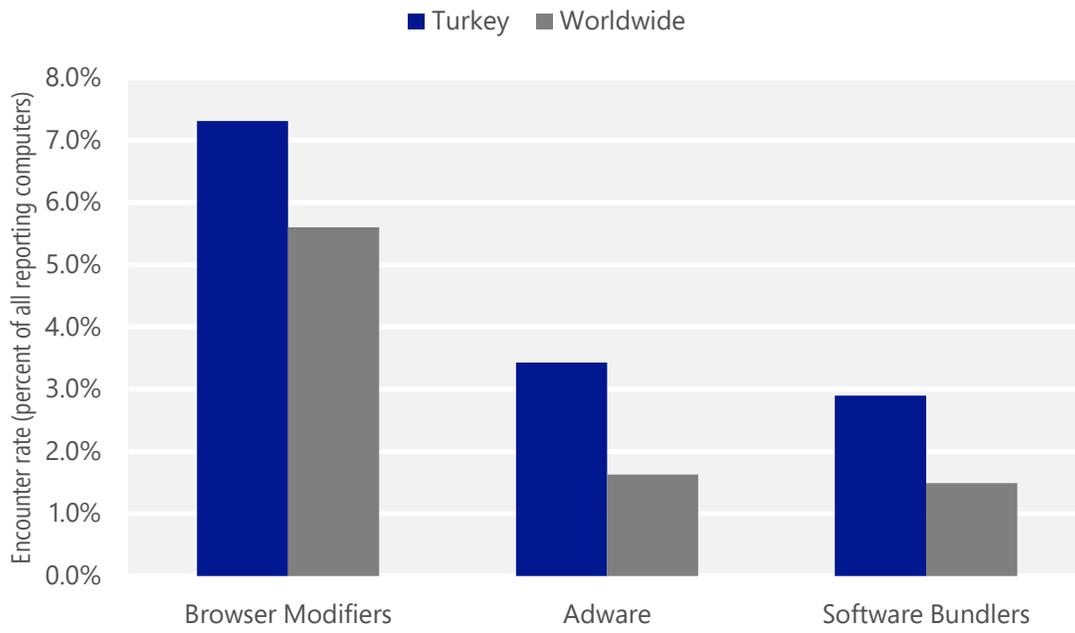
Malware encountered in Turkey in 2Q15, by category



- The most common malware category in Turkey in 2Q15 was Trojans. It was encountered by 12.7 percent of all computers there, down from 13.2 percent in 1Q15.
- The second most common malware category in Turkey in 2Q15 was Worms. It was encountered by 7.8 percent of all computers there, down from 9.4 percent in 1Q15.
- The third most common malware category in Turkey in 2Q15 was Obfuscators & Injectors, which was encountered by 3.8 percent of all computers there, up from 3.8 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Turkey in 2Q15, by category



- The most common unwanted software category in Turkey in 2Q15 was Browser Modifiers. It was encountered by 7.3 percent of all computers there, down from 9.2 percent in 1Q15.
- The second most common unwanted software category in Turkey in 2Q15 was Adware. It was encountered by 3.4 percent of all computers there, down from 6.1 percent in 1Q15.
- The third most common unwanted software category in Turkey in 2Q15 was Software Bundlers, which was encountered by 2.9 percent of all computers there, up from 0.6 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Turkey in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Peals	Trojans	3.8%
2	Win32/Gamarue	Worms	3.8%
3	Win32/Obfuscator	Obfuscators & Injectors	2.9%
4	Win32/Kilim	Trojans	1.8%
5	Win32/Sality	Viruses	1.6%
6	Win32/BeeVry	Trojans	1.4%
7	Win32/Ramnit	Trojans	1.4%
8	INF/Autorun	Obfuscators & Injectors	1.3%
9	Win32/Skeeyah	Trojans	1.3%
10	MSIL/Wooniky	Worms	0.8%

- The most common malware family encountered in Turkey in 2Q15 was [Win32/Peals](#), which was encountered by 3.8 percent of reporting computers there. [Win32/Peals](#) is a generic detection for various threats that display trojan characteristics.
- The second most common malware family encountered in Turkey in 2Q15 was [Win32/Gamarue](#), which was encountered by 3.8 percent of reporting computers there. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The third most common malware family encountered in Turkey in 2Q15 was [Win32/Obfuscator](#), which was encountered by 2.9 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The fourth most common malware family encountered in Turkey in 2Q15 was [Win32/Kilim](#), which was encountered by 1.8 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Turkey in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	4.2%
2	Win32/InstalleRex	Software Bundlers	2.8%
3	Win32/KipodToolsCby	Browser Modifiers	2.5%
4	Win32/SaverExtension	Adware	1.5%
5	Win32/EoRezo	Adware	1.4%

- The most common unwanted software family encountered in Turkey in 2Q15 was [Win32/CouponRuc](#), which was encountered by 4.2 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in Turkey in 2Q15 was [Win32/InstalleRex](#), which was encountered by 2.8 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own “Installed On” date in Programs and Features to make it more difficult for a user to locate it and remove it.
- The third most common unwanted software family encountered in Turkey in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 2.5 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user’s consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.

Top threat families by infection rate

The most common malware families by infection rate in Turkey in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/Gamarue	Worms	4.5
2	Win32/leEnablerCby	Browser Modifiers	3.9
3	Win32/Sality	Viruses	3.7
4	Win32/Kilim	Trojans	3.2
5	Win32/Ramnit	Trojans	2.9
6	Win32/CompromisedCert	Other Malware	1.5
7	Win32/Brontok	Worms	1.3
8	VBS/Jenxcus	Worms	1.2
9	Win32/Helompy	Worms	1.0
10	Win32/Nuqel	Worms	0.9

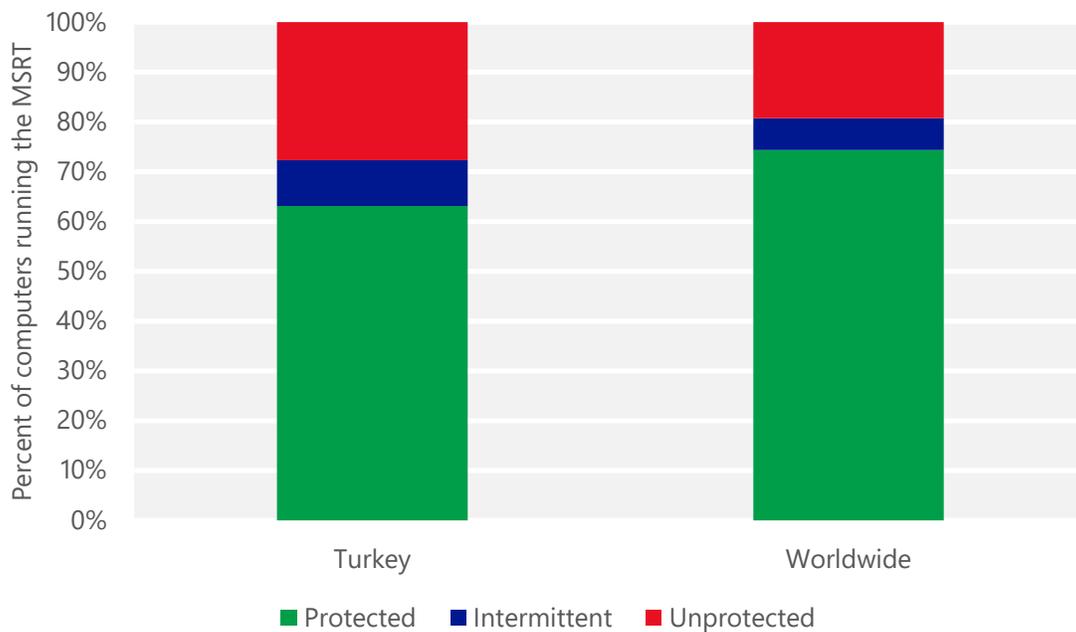
- The most common threat family infecting computers in Turkey in 2Q15 was [Win32/Gamarue](#), which was detected and removed from 4.5 of every 1,000 unique computers scanned by the MSRT. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The second most common threat family infecting computers in Turkey in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 3.9 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common threat family infecting computers in Turkey in 2Q15 was [Win32/Sality](#), which was detected and removed from 3.7 of every 1,000 unique computers scanned by the MSRT. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The fourth most common threat family infecting computers in Turkey in 2Q15 was [Win32/Kilim](#), which was detected and removed from 3.2 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Turkey and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Turkey

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.27 (0.28)	0.16 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	7.54 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	23.77 (16.7)	

Ukraine

The statistics presented here are generated by Microsoft security programs and services running on computers in Ukraine in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Ukraine

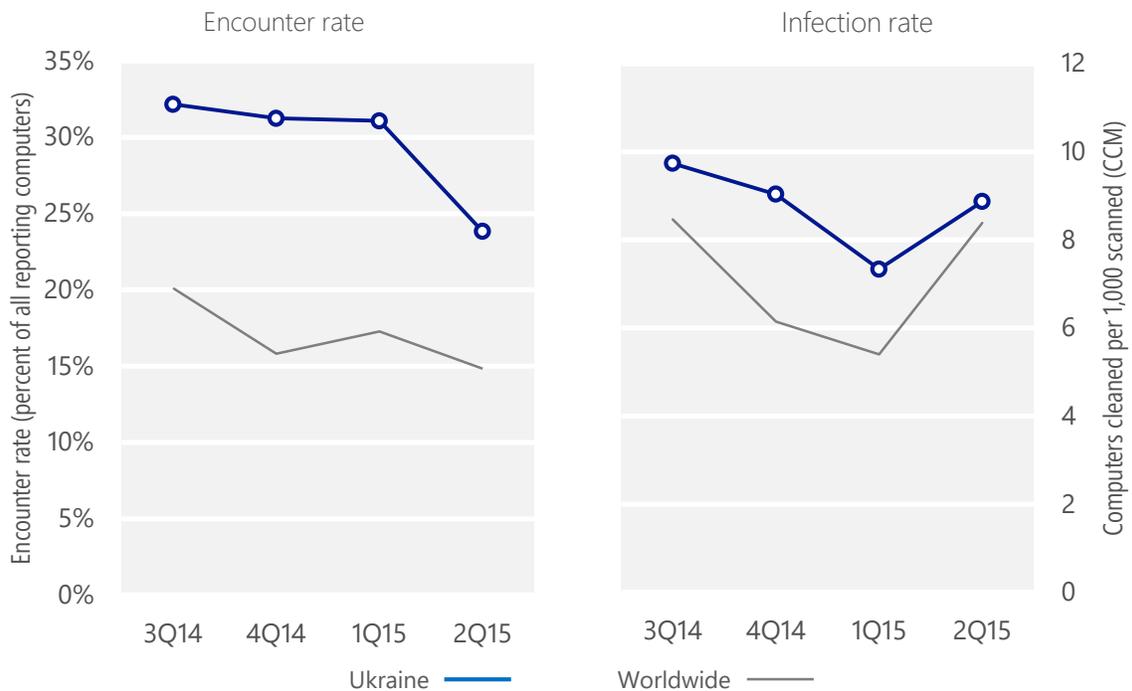
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Ukraine	32.2%	31.2%	31.1%	23.8%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Ukraine	9.7	9.0	7.3	8.9
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcote, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 23.8% of computers in Ukraine encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 8.9 of every 1,000 unique computers scanned in Ukraine in 2Q15 (a CCM score of 8.9, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Ukraine over the last four quarters, compared to the world as a whole.

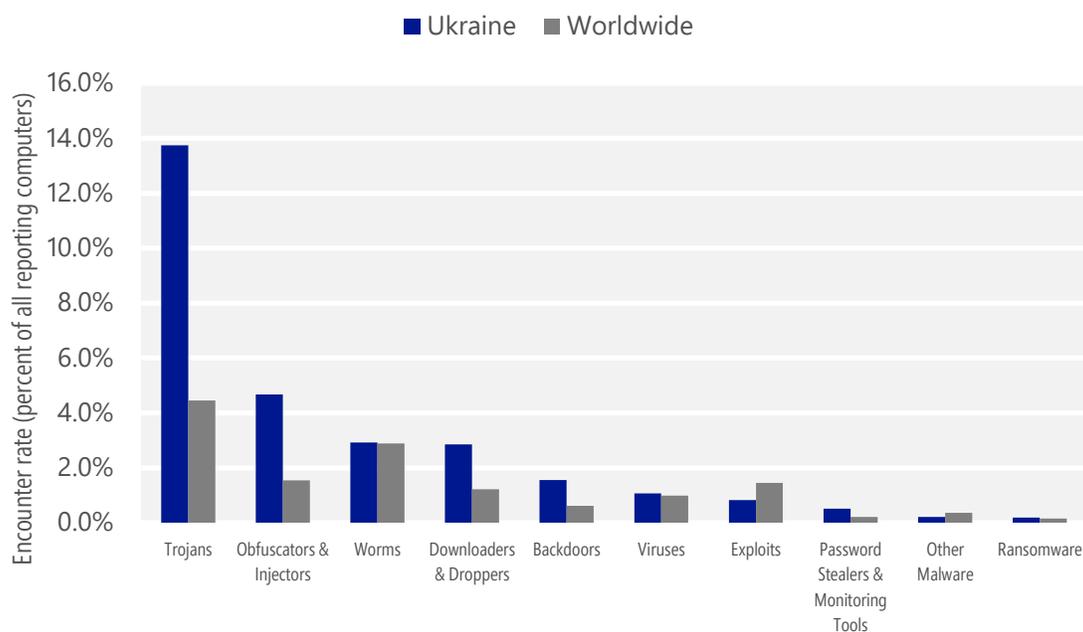
Malware encounter and infection rate trends in Ukraine and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in Ukraine and around the world, and for explanations of the methods and terms used here.

Malware categories

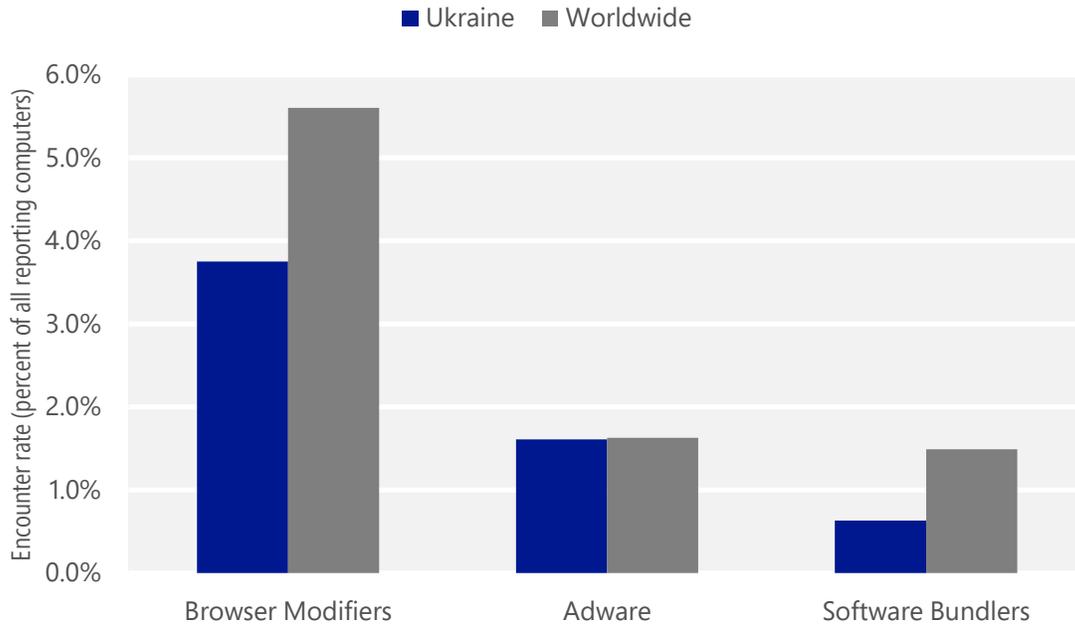
Malware encountered in Ukraine in 2Q15, by category



- The most common malware category in Ukraine in 2Q15 was Trojans. It was encountered by 13.7 percent of all computers there, down from 16.2 percent in 1Q15.
- The second most common malware category in Ukraine in 2Q15 was Obfuscators & Injectors. It was encountered by 4.7 percent of all computers there, down from 7.3 percent in 1Q15.
- The third most common malware category in Ukraine in 2Q15 was Worms, which was encountered by 2.9 percent of all computers there, down from 5.3 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Ukraine in 2Q15, by category



- The most common unwanted software category in Ukraine in 2Q15 was Browser Modifiers. It was encountered by 3.8 percent of all computers there, down from 7.2 percent in 1Q15.
- The second most common unwanted software category in Ukraine in 2Q15 was Adware. It was encountered by 1.6 percent of all computers there, up from 1.6 percent in 1Q15.
- The third most common unwanted software category in Ukraine in 2Q15 was Software Bundlers, which was encountered by 0.6 percent of all computers there, up from 0.3 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Ukraine in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Peals	Trojans	5.2%
2	Win32/Obfuscator	Obfuscators & Injectors	4.1%
3	Win32/Skeeyah	Trojans	1.6%
4	Win32/Gamarue	Worms	1.1%
5	Win32/Ogimant	Downloaders & Droppers	1.1%
6	Win32/Dynamer	Trojans	1.0%
7	Win32/Radonskra	Trojans	0.7%
8	Win32/Anaki	Trojans	0.6%
9	INF/Autorun	Obfuscators & Injectors	0.5%
10	Win32/Ramnit	Trojans	0.5%

- The most common malware family encountered in Ukraine in 2Q15 was [Win32/Peals](#), which was encountered by 5.2 percent of reporting computers there. [Win32/Peals](#) is a generic detection for various threats that display trojan characteristics.
- The second most common malware family encountered in Ukraine in 2Q15 was [Win32/Obfuscator](#), which was encountered by 4.1 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The third most common malware family encountered in Ukraine in 2Q15 was [Win32/Skeeyah](#), which was encountered by 1.6 percent of reporting computers there. [Win32/Skeeyah](#) is a generic detection for various threats that display trojan characteristics.
- The fourth most common malware family encountered in Ukraine in 2Q15 was [Win32/Gamarue](#), which was encountered by 1.1 percent of reporting computers there. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Ukraine in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/KipodToolsCby	Browser Modifiers	2.1%
2	Win32/CouponRuc	Browser Modifiers	0.9%
3	Win32/EoRezo	Adware	0.7%
4	Win32/AlterbookSP	Browser Modifiers	0.7%
5	Win32/InstalleRex	Software Bundlers	0.5%

- The most common unwanted software family encountered in Ukraine in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 2.1 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common unwanted software family encountered in Ukraine in 2Q15 was [Win32/CouponRuc](#), which was encountered by 0.9 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The third most common unwanted software family encountered in Ukraine in 2Q15 was [Win32/EoRezo](#), which was encountered by 0.7 percent of reporting computers there. [Win32/EoRezo](#) is adware that displays targeted advertising to affected users while browsing the Internet, based on downloaded pre-configured information.

Top threat families by infection rate

The most common malware families by infection rate in Ukraine in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	2.6
2	Win32/Gamarue	Worms	1.1
3	Win32/Ramnit	Trojans	0.8
4	Win32/Sality	Viruses	0.6
5	VBS/Jenxcus	Worms	0.6
6	Win32/Helompy	Worms	0.4
7	Win32/Kilim	Trojans	0.4
8	Win32/Dorkbot	Worms	0.4
9	Win32/CompromisedCert	Other Malware	0.3
10	Win32/Brontok	Worms	0.2

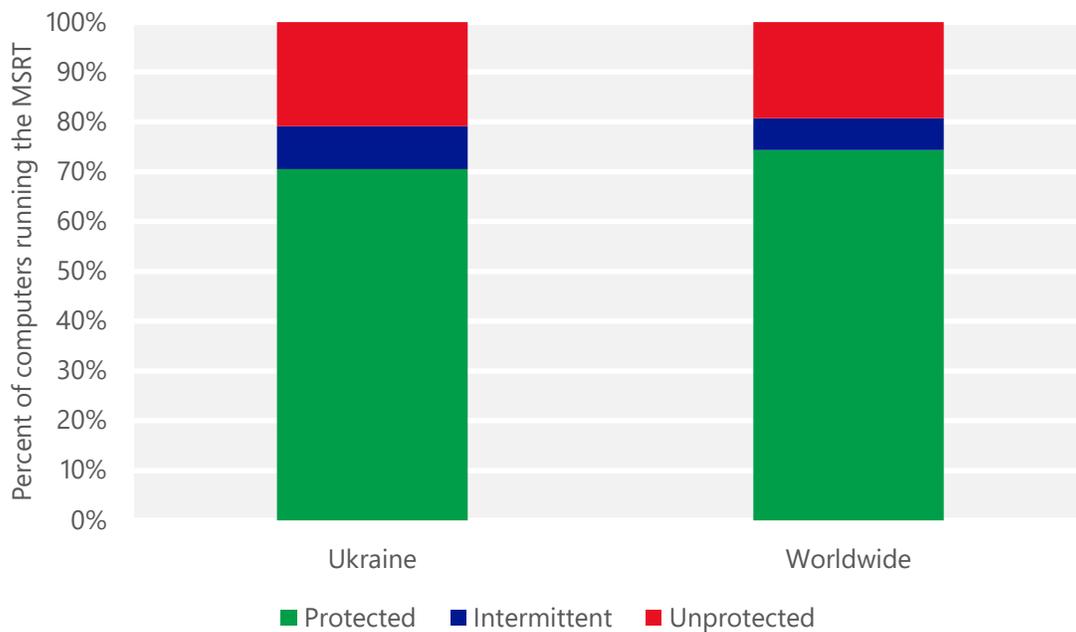
- The most common threat family infecting computers in Ukraine in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 2.6 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Ukraine in 2Q15 was [Win32/Gamarue](#), which was detected and removed from 1.1 of every 1,000 unique computers scanned by the MSRT. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The third most common threat family infecting computers in Ukraine in 2Q15 was [Win32/Ramnit](#), which was detected and removed from 0.8 of every 1,000 unique computers scanned by the MSRT. [Win32/Ramnit](#) is a family of multi-component malware that infects executable files, Microsoft Office files, and HTML files. Win32/Ramnit spreads to removable drives and steals sensitive information such as saved FTP credentials and browser cookies. It may also open a backdoor to await instructions from a remote attacker.
- The fourth most common threat family infecting computers in Ukraine in 2Q15 was [Win32/Sality](#), which was detected and removed from 0.6 of every 1,000 unique computers scanned by the MSRT. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Ukraine and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Ukraine

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.39 (0.28)	0.56 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	10.89 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	22.92 (16.7)	

United Arab Emirates

The statistics presented here are generated by Microsoft security programs and services running on computers in the United Arab Emirates in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for the United Arab Emirates

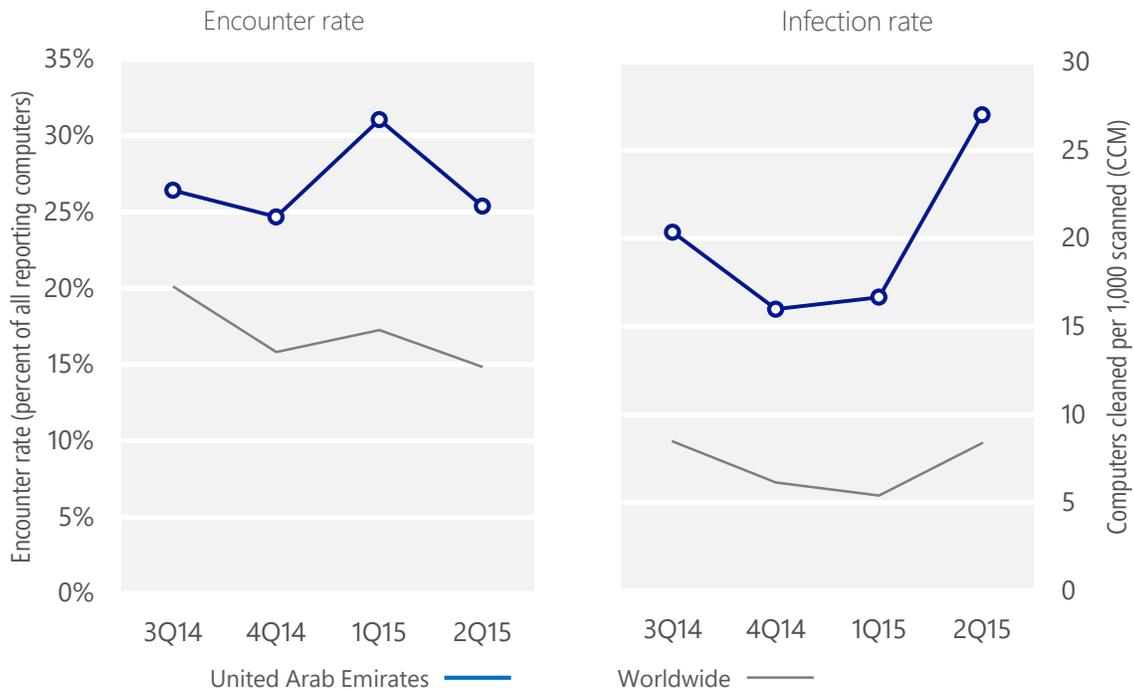
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, United Arab Emirates	26.4%	24.7%	31.1%	25.4%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, United Arab Emirates	20.4	16.0	16.7	27.0
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcote, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 25.4% of computers in the United Arab Emirates encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 27.0 of every 1,000 unique computers scanned in the United Arab Emirates in 2Q15 (a CCM score of 27.0, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for the United Arab Emirates over the last four quarters, compared to the world as a whole.

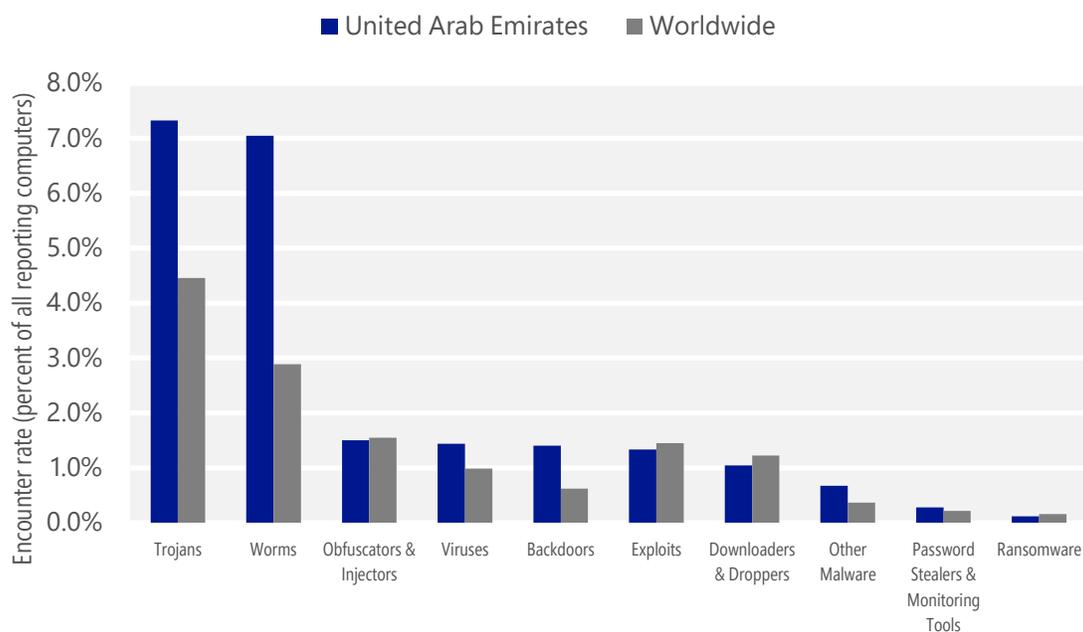
Malware encounter and infection rate trends in the United Arab Emirates and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in the United Arab Emirates and around the world, and for explanations of the methods and terms used here.

Malware categories

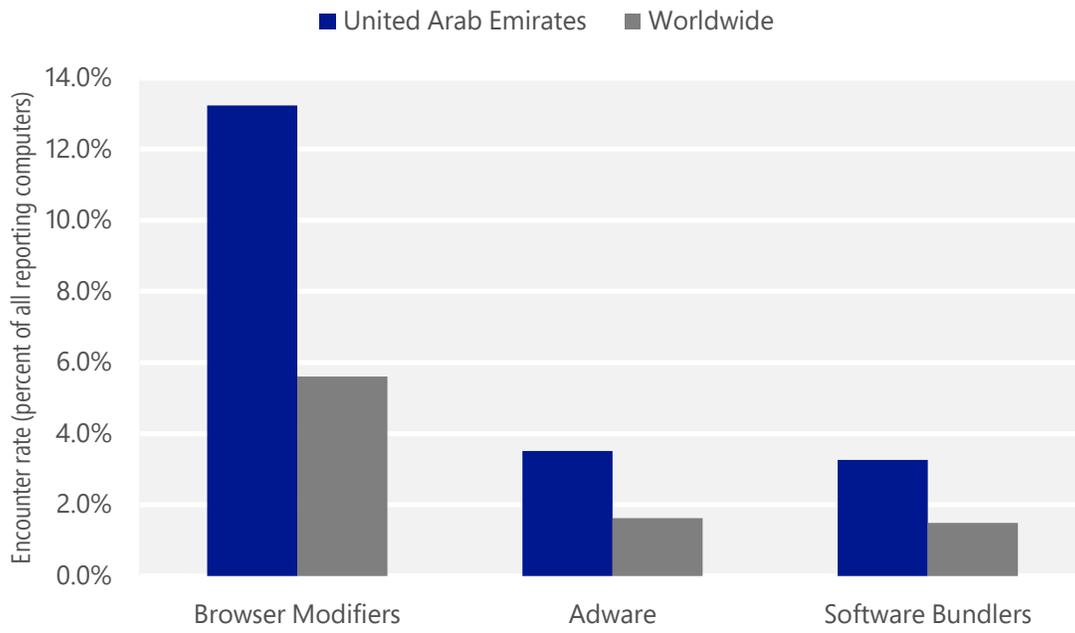
Malware encountered in the United Arab Emirates in 2Q15, by category



- The most common malware category in the United Arab Emirates in 2Q15 was Trojans. It was encountered by 7.3 percent of all computers there, up from 6.9 percent in 1Q15.
- The second most common malware category in the United Arab Emirates in 2Q15 was Worms. It was encountered by 7.0 percent of all computers there, up from 5.8 percent in 1Q15.
- The third most common malware category in the United Arab Emirates in 2Q15 was Obfuscators & Injectors, which was encountered by 1.5 percent of all computers there, down from 2.9 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in the United Arab Emirates in 2Q15, by category



- The most common unwanted software category in the United Arab Emirates in 2Q15 was Browser Modifiers. It was encountered by 13.2 percent of all computers there, down from 17.5 percent in 1Q15.
- The second most common unwanted software category in the United Arab Emirates in 2Q15 was Adware. It was encountered by 3.5 percent of all computers there, down from 9.4 percent in 1Q15.
- The third most common unwanted software category in the United Arab Emirates in 2Q15 was Software Bundlers, which was encountered by 3.3 percent of all computers there, up from 1.3 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in the United Arab Emirates in 2Q15

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	1.8%
2	Win32/Kilim	Trojans	1.7%
3	Win32/Skeeyah	Trojans	1.6%
4	Win32/Gamarue	Worms	1.3%
5	INF/Autorun	Obfuscators & Injectors	1.0%
6	Win32/Peals	Trojans	0.8%
7	Win32/Obfuscator	Obfuscators & Injectors	0.8%
8	Win32/Sality	Viruses	0.6%
9	ALisp/Copicad	Worms	0.6%
10	Win32/Ramnit	Trojans	0.5%

- The most common malware family encountered in the United Arab Emirates in 2Q15 was [VBS/Jenxcus](#), which was encountered by 1.8 percent of reporting computers there. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common malware family encountered in the United Arab Emirates in 2Q15 was [Win32/Kilim](#), which was encountered by 1.7 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The third most common malware family encountered in the United Arab Emirates in 2Q15 was [Win32/Skeeyah](#), which was encountered by 1.6 percent of reporting computers there. [Win32/Skeeyah](#) is a generic detection for various threats that display trojan characteristics.
- The fourth most common malware family encountered in the United Arab Emirates in 2Q15 was [Win32/Gamarue](#), which was encountered by 1.3 percent of reporting computers there. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in the United Arab Emirates in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	7.4%
2	Win32/KipodToolsCby	Browser Modifiers	5.0%
3	Win32/InstalleRex	Software Bundlers	3.1%
4	Win32/SaverExtension	Adware	2.7%
5	Win32/Vonteera	Browser Modifiers	1.4%

- The most common unwanted software family encountered in the United Arab Emirates in 2Q15 was [Win32/CouponRuc](#), which was encountered by 7.4 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in the United Arab Emirates in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 5.0 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common unwanted software family encountered in the United Arab Emirates in 2Q15 was [Win32/InstalleRex](#), which was encountered by 3.1 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in the United Arab Emirates in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	7.1
2	Win32/CompromisedCert	Other Malware	5.4
3	VBS/Jenxcus	Worms	3.3
4	Win32/Kilim	Trojans	2.8
5	Win32/Gamarue	Worms	2.6
6	Win32/Sality	Viruses	1.7
7	Win32/Nuqel	Worms	0.9
8	Win32/Ramnit	Trojans	0.9
9	MSIL/Bladabindi	Backdoors	0.6
10	Win32/Dorkbot	Worms	0.4

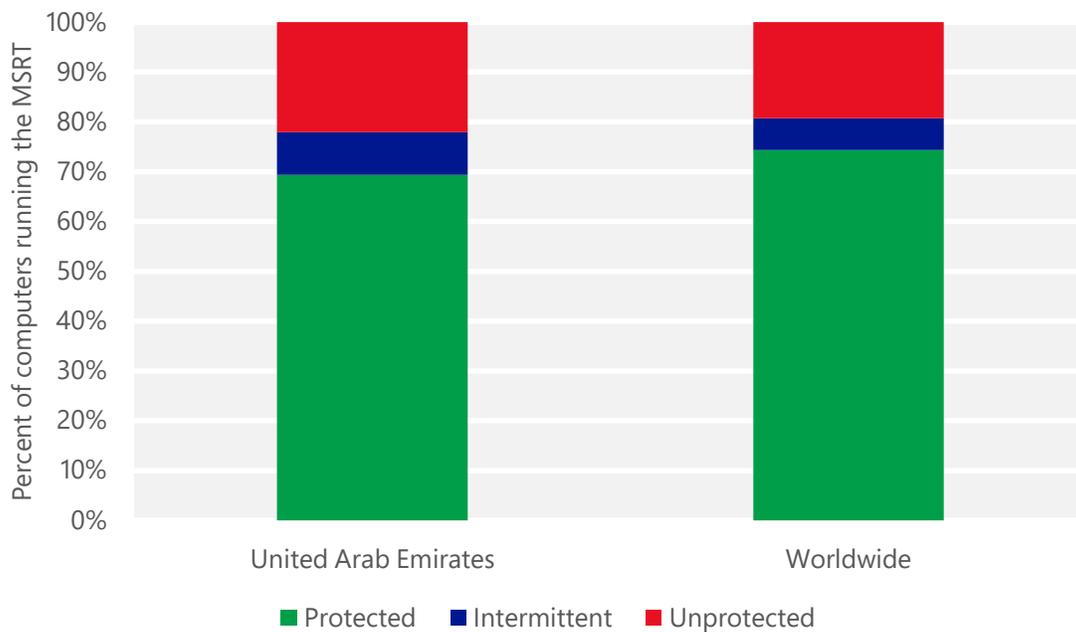
- The most common threat family infecting computers in the United Arab Emirates in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 7.1 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in the United Arab Emirates in 2Q15 was [Win32/CompromisedCert](#), which was detected and removed from 5.4 of every 1,000 unique computers scanned by the MSRT. [Win32/CompromisedCert](#) is a detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.
- The third most common threat family infecting computers in the United Arab Emirates in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 3.3 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The fourth most common threat family infecting computers in the United Arab Emirates in 2Q15 was [Win32/Kilim](#), which was detected and removed from 2.8 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in the United Arab Emirates and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for the United Arab Emirates

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.02 (0.28)	0.02 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	1.42 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	5.36 (16.7)	

United Kingdom

The statistics presented here are generated by Microsoft security programs and services running on computers in the United Kingdom in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for the United Kingdom

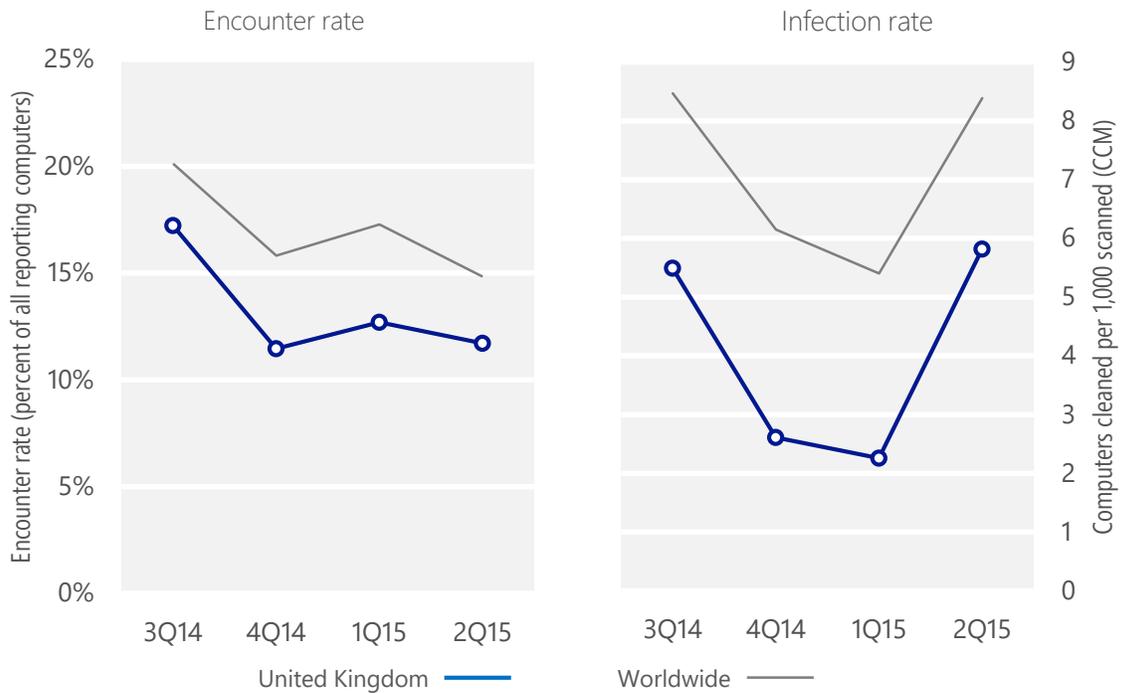
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, United Kingdom	17.2%	11.5%	12.7%	11.7%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, United Kingdom	5.5	2.6	2.3	5.8
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcout, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 11.7% of computers in the United Kingdom encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 5.8 of every 1,000 unique computers scanned in the United Kingdom in 2Q15 (a CCM score of 5.8, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for the United Kingdom over the last four quarters, compared to the world as a whole.

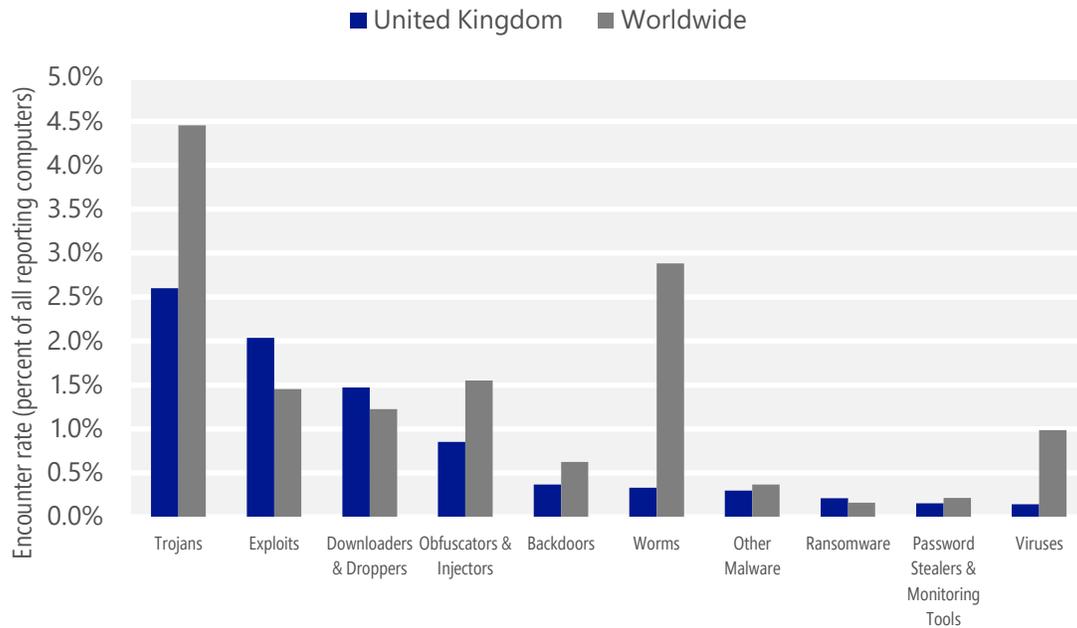
Malware encounter and infection rate trends in the United Kingdom and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in the United Kingdom and around the world, and for explanations of the methods and terms used here.

Malware categories

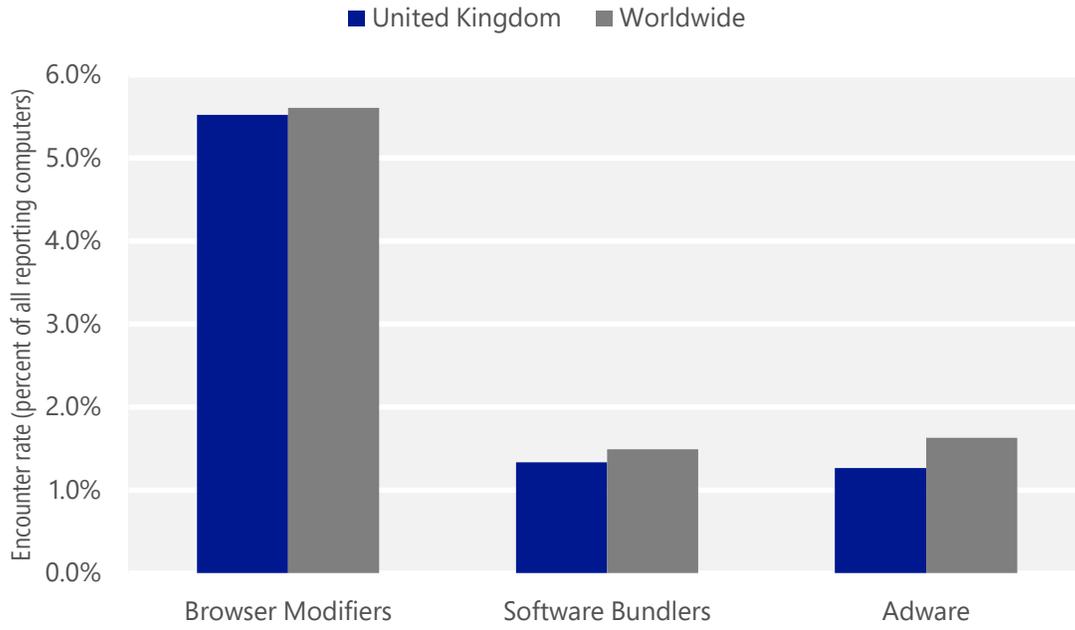
Malware encountered in the United Kingdom in 2Q15, by category



- The most common malware category in the United Kingdom in 2Q15 was Trojans. It was encountered by 2.6 percent of all computers there, up from 2.3 percent in 1Q15.
- The second most common malware category in the United Kingdom in 2Q15 was Exploits. It was encountered by 2.0 percent of all computers there, up from 1.8 percent in 1Q15.
- The third most common malware category in the United Kingdom in 2Q15 was Downloaders & Droppers, which was encountered by 1.5 percent of all computers there, down from 1.7 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in the United Kingdom in 2Q15, by category



- The most common unwanted software category in the United Kingdom in 2Q15 was Browser Modifiers. It was encountered by 5.5 percent of all computers there, up from 5.3 percent in 1Q15.
- The second most common unwanted software category in the United Kingdom in 2Q15 was Software Bundlers. It was encountered by 1.3 percent of all computers there, down from 3.4 percent in 1Q15.
- The third most common unwanted software category in the United Kingdom in 2Q15 was Adware, which was encountered by 1.3 percent of all computers there, up from 1.0 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in the United Kingdom in 2Q15

	Family	Most significant category	% of reporting computers
1	JS/Axpergle	Exploits	1.5%
2	Win32/Obfuscator	Obfuscators & Injectors	0.8%
3	Win32/Kilim	Trojans	0.6%
4	Win32/Skeeyah	Trojans	0.5%
5	Win32/Peals	Trojans	0.4%
6	W97M/Adnel	Downloaders & Droppers	0.2%
7	Win32/Dynamer	Trojans	0.2%
8	Win32/Crowti	Ransomware	0.2%
9	JS/Neclu	Exploits	0.1%
10	Win32/Tugspay	Downloaders & Droppers	0.1%

- The most common malware family encountered in the United Kingdom in 2Q15 was [JS/Axpergle](#), which was encountered by 1.5 percent of reporting computers there. [JS/Axpergle](#) is a detection for the Angler exploit kit, which exploits vulnerabilities in recent versions of Internet Explorer, Silverlight, Adobe Flash Player, and Java to install malware.
- The second most common malware family encountered in the United Kingdom in 2Q15 was [Win32/Obfuscator](#), which was encountered by 0.8 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The third most common malware family encountered in the United Kingdom in 2Q15 was [Win32/Kilim](#), which was encountered by 0.6 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The fourth most common malware family encountered in the United Kingdom in 2Q15 was [Win32/Skeeyah](#), which was encountered by 0.5 percent of reporting computers there. [Win32/Skeeyah](#) is a generic detection for various threats that display trojan characteristics.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in the United Kingdom in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/KipodToolsCby	Browser Modifiers	2.3%
2	Win32/CouponRuc	Browser Modifiers	2.1%
3	Win32/InstalleRex	Software Bundlers	1.0%
4	Win32/SaverExtension	Adware	0.7%
5	Win32/AlterbookSP	Browser Modifiers	0.7%

- The most common unwanted software family encountered in the United Kingdom in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 2.3 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common unwanted software family encountered in the United Kingdom in 2Q15 was [Win32/CouponRuc](#), which was encountered by 2.1 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The third most common unwanted software family encountered in the United Kingdom in 2Q15 was [Win32/InstalleRex](#), which was encountered by 1.0 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in the United Kingdom in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	2.2
2	Win32/CompromisedCert	Other Malware	1.3
3	Win32/Kilim	Trojans	0.9
4	Win32/Simda	Trojans	0.2
5	Win32/Nitol	Other Malware	0.1
6	Win32/Ramnit	Trojans	0.1
7	Win32/Alureon	Trojans	0.1
8	MSIL/Bladabindi	Backdoors	0.1
9	VBS/Jenxcus	Worms	0.1
10	Win32/Zbot	Password Stealers & Monitoring Tools	0.1

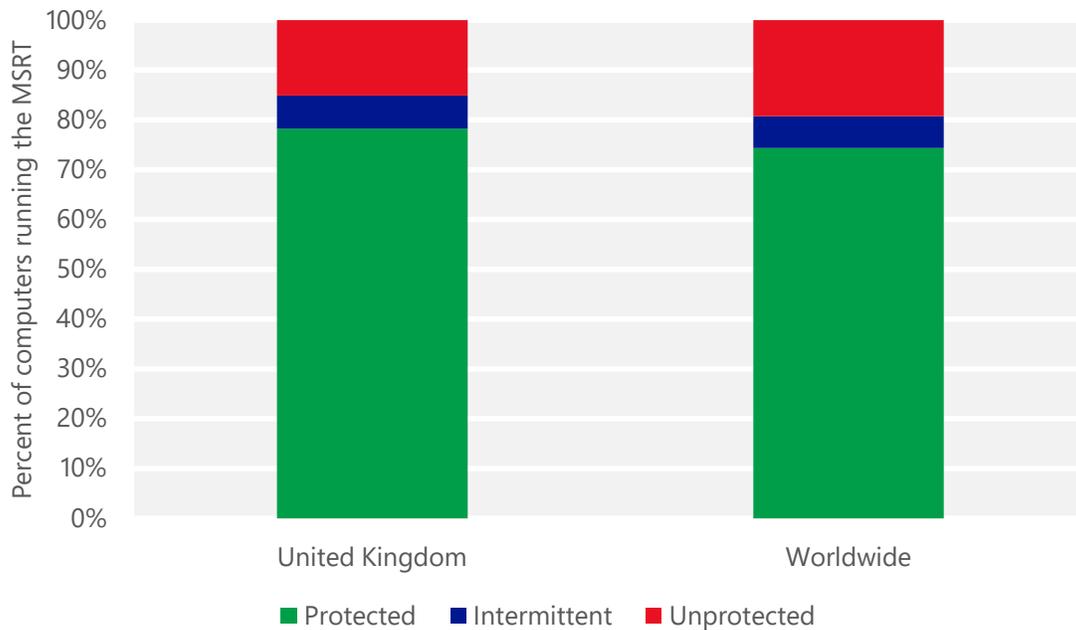
- The most common threat family infecting computers in the United Kingdom in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 2.2 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in the United Kingdom in 2Q15 was [Win32/CompromisedCert](#), which was detected and removed from 1.3 of every 1,000 unique computers scanned by the MSRT. [Win32/CompromisedCert](#) is a detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.
- The third most common threat family infecting computers in the United Kingdom in 2Q15 was [Win32/Kilim](#), which was detected and removed from 0.9 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The fourth most common threat family infecting computers in the United Kingdom in 2Q15 was [Win32/Simda](#), which was detected and removed from 0.2 of every 1,000 unique computers scanned by the MSRT. [Win32/Simda](#) is a threat that can give an attacker backdoor access and control of an infected computer. It can then steal passwords and gather information about the computer to send to the attacker.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in the United Kingdom and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for the United Kingdom

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.11 (0.28)	0.12 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	5.96 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	13.46 (16.7)	

United States

The statistics presented here are generated by Microsoft security programs and services running on computers in the United States in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for the United States

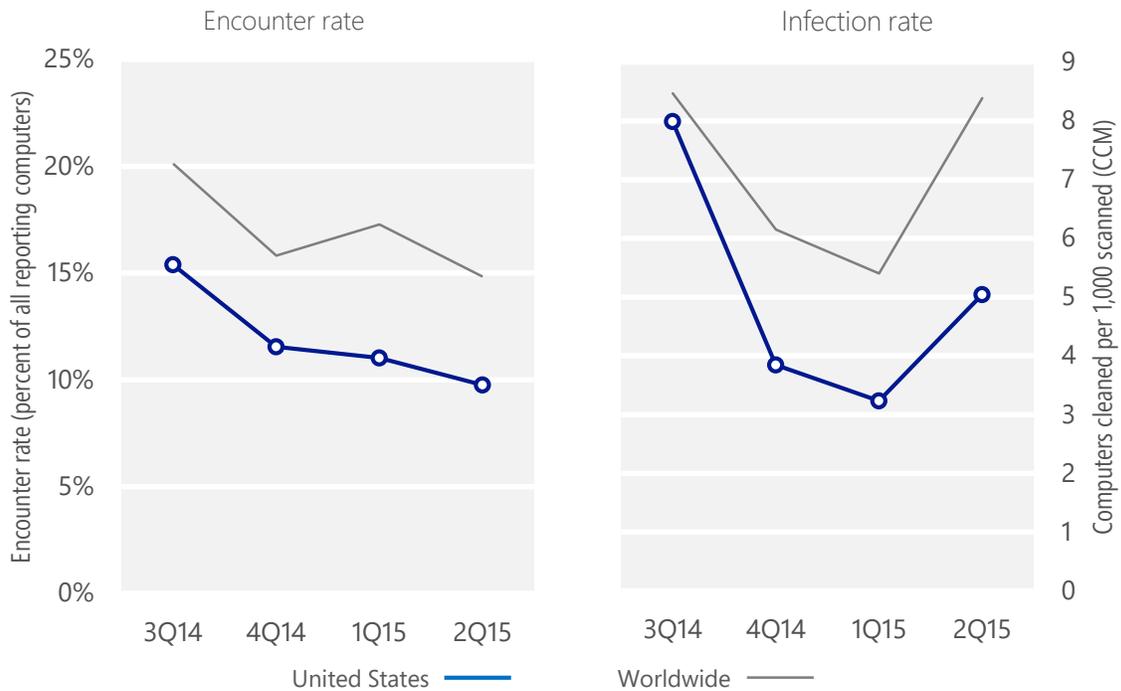
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, United States	15.4%	11.5%	11.0%	9.8%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, United States	8.0	3.8	3.2	5.0
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcoute, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 9.8% of computers in the United States encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 5.0 of every 1,000 unique computers scanned in the United States in 2Q15 (a CCM score of 5.0, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for the United States over the last four quarters, compared to the world as a whole.

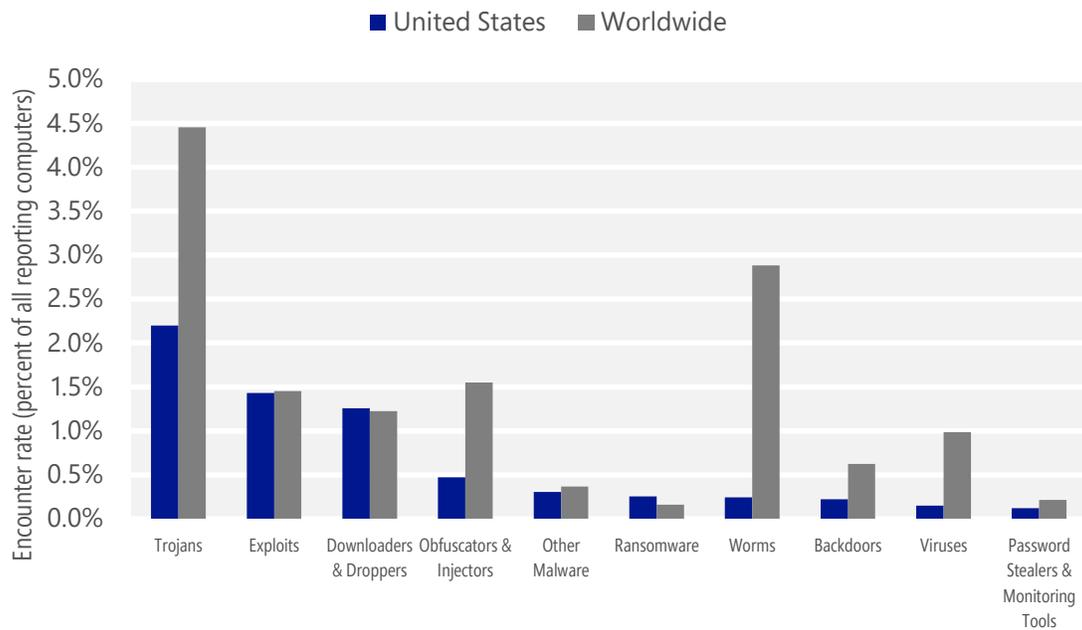
Malware encounter and infection rate trends in the United States and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in the United States and around the world, and for explanations of the methods and terms used here.

Malware categories

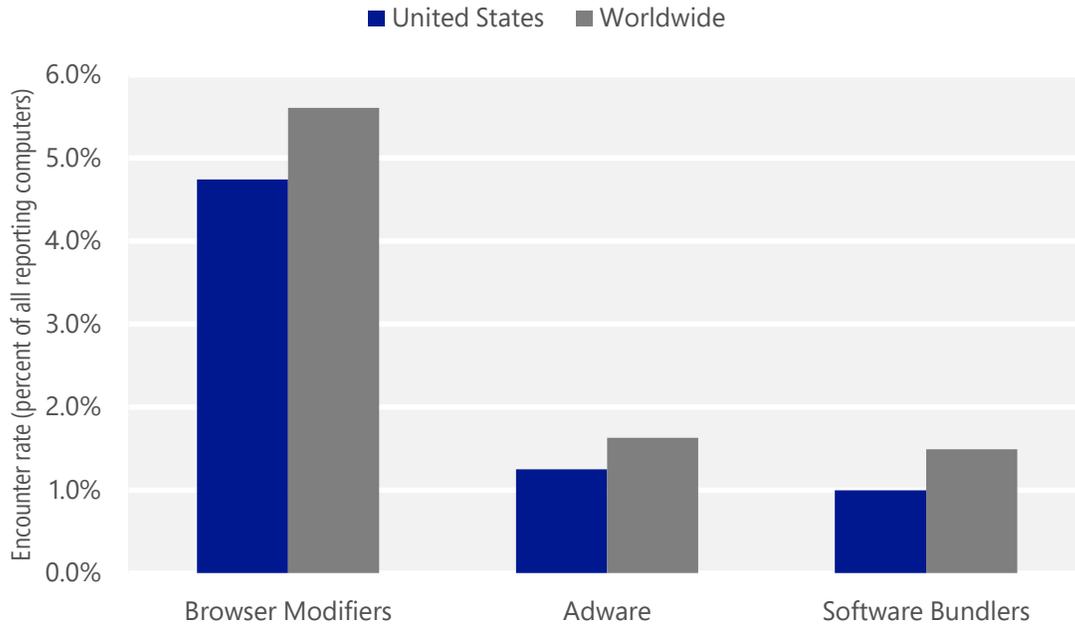
Malware encountered in the United States in 2Q15, by category



- The most common malware category in the United States in 2Q15 was Trojans. It was encountered by 2.2 percent of all computers there, up from 2.0 percent in 1Q15.
- The second most common malware category in the United States in 2Q15 was Exploits. It was encountered by 1.4 percent of all computers there, down from 1.9 percent in 1Q15.
- The third most common malware category in the United States in 2Q15 was Downloaders & Droppers, which was encountered by 1.3 percent of all computers there, up from 1.0 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in the United States in 2Q15, by category



- The most common unwanted software category in the United States in 2Q15 was Browser Modifiers. It was encountered by 4.7 percent of all computers there, up from 4.3 percent in 1Q15.
- The second most common unwanted software category in the United States in 2Q15 was Adware. It was encountered by 1.2 percent of all computers there, down from 3.3 percent in 1Q15.
- The third most common unwanted software category in the United States in 2Q15 was Software Bundlers, which was encountered by 1.0 percent of all computers there, up from 0.7 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in the United States in 2Q15

	Family	Most significant category	% of reporting computers
1	JS/Axpergle	Exploits	0.8%
2	Win32/Kilim	Trojans	0.5%
3	Win32/Obfuscator	Obfuscators & Injectors	0.4%
4	Win32/Skeeyah	Trojans	0.4%
5	Win32/Peals	Trojans	0.3%
6	Win32/Crowti	Ransomware	0.2%
7	JS/Fiexp	Exploits	0.1%
8	Win32/Upatre	Downloaders & Droppers	0.1%
9	Win32/Clukug	Trojans	0.1%
10	JS/Neclu	Exploits	0.1%

- The most common malware family encountered in the United States in 2Q15 was [JS/Axpergle](#), which was encountered by 0.8 percent of reporting computers there. [JS/Axpergle](#) is a detection for the Angler exploit kit, which exploits vulnerabilities in recent versions of Internet Explorer, Silverlight, Adobe Flash Player, and Java to install malware.
- The second most common malware family encountered in the United States in 2Q15 was [Win32/Kilim](#), which was encountered by 0.5 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The third most common malware family encountered in the United States in 2Q15 was [Win32/Obfuscator](#), which was encountered by 0.4 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The fourth most common malware family encountered in the United States in 2Q15 was [Win32/Skeeyah](#), which was encountered by 0.4 percent of reporting computers there. [Win32/Skeeyah](#) is a generic detection for various threats that display trojan characteristics.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in the United States in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	1.6%
2	Win32/KipodToolsCby	Browser Modifiers	1.2%
3	Win32/AlterbookSP	Browser Modifiers	1.2%
4	Win32/InstalleRex	Software Bundlers	0.7%
5	Win32/SaverExtension	Adware	0.6%

- The most common unwanted software family encountered in the United States in 2Q15 was [Win32/CouponRuc](#), which was encountered by 1.6 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in the United States in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 1.2 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common unwanted software family encountered in the United States in 2Q15 was [Win32/AlterbookSP](#), which was encountered by 1.2 percent of reporting computers there. [Win32/AlterbookSP](#) is a browser add-on that formerly displayed behaviors of unwanted software. Recent versions of the add-on no longer meet Microsoft detection criteria, and are no longer considered unwanted software.

Top threat families by infection rate

The most common malware families by infection rate in the United States in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	1.3
2	Win32/Kilim	Trojans	0.9
3	Win32/Alureon	Trojans	0.8
4	Win32/CompromisedCert	Other Malware	0.7
5	Win32/Simda	Trojans	0.3
6	Win32/Nitol	Other Malware	0.1
7	Win32/Tracur	Trojans	0.1
8	Win32/Dyzap	Password Stealers & Monitoring Tools	0.1
9	JS/Miuref	Trojans	0.1
10	Win32/Sirefef	Trojans	0.1

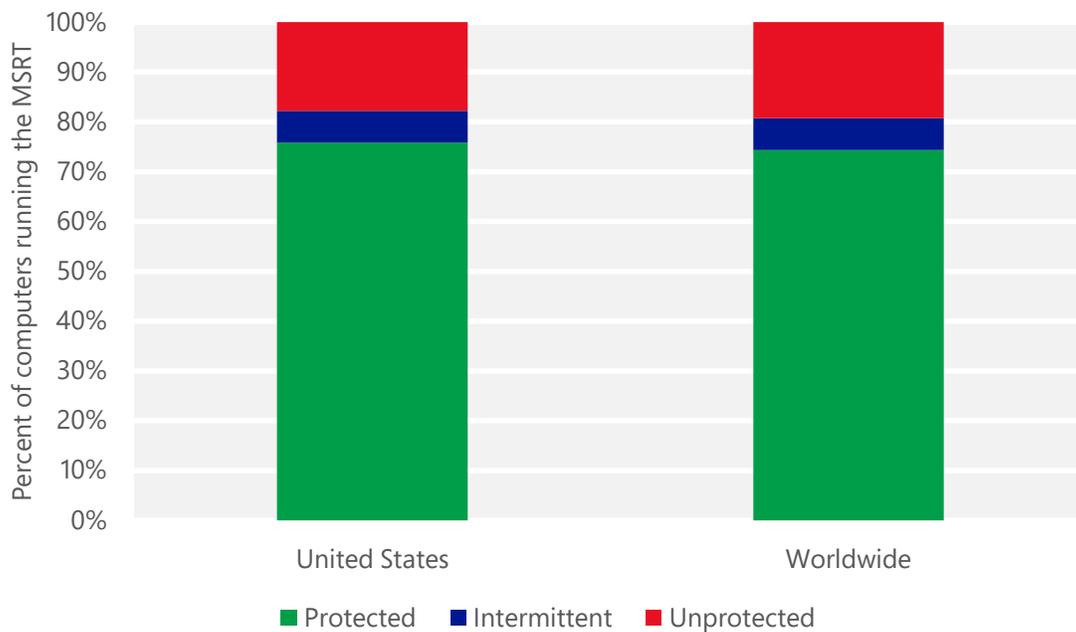
- The most common threat family infecting computers in the United States in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 1.3 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in the United States in 2Q15 was [Win32/Kilim](#), which was detected and removed from 0.9 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The third most common threat family infecting computers in the United States in 2Q15 was [Win32/Alureon](#), which was detected and removed from 0.8 of every 1,000 unique computers scanned by the MSRT. [Win32/Alureon](#) is a data-stealing trojan that gathers confidential information such as user names, passwords, and credit card data from incoming and outgoing Internet traffic. It may also download malicious data and modify DNS settings.
- The fourth most common threat family infecting computers in the United States in 2Q15 was [Win32/CompromisedCert](#), which was detected and removed from 0.7 of every 1,000 unique computers scanned by the MSRT. [Win32/CompromisedCert](#) is a detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in the United States and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for the United States

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.27 (0.28)	0.22 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	6.58 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	16.26 (16.7)	

Uruguay

The statistics presented here are generated by Microsoft security programs and services running on computers in Uruguay in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Uruguay

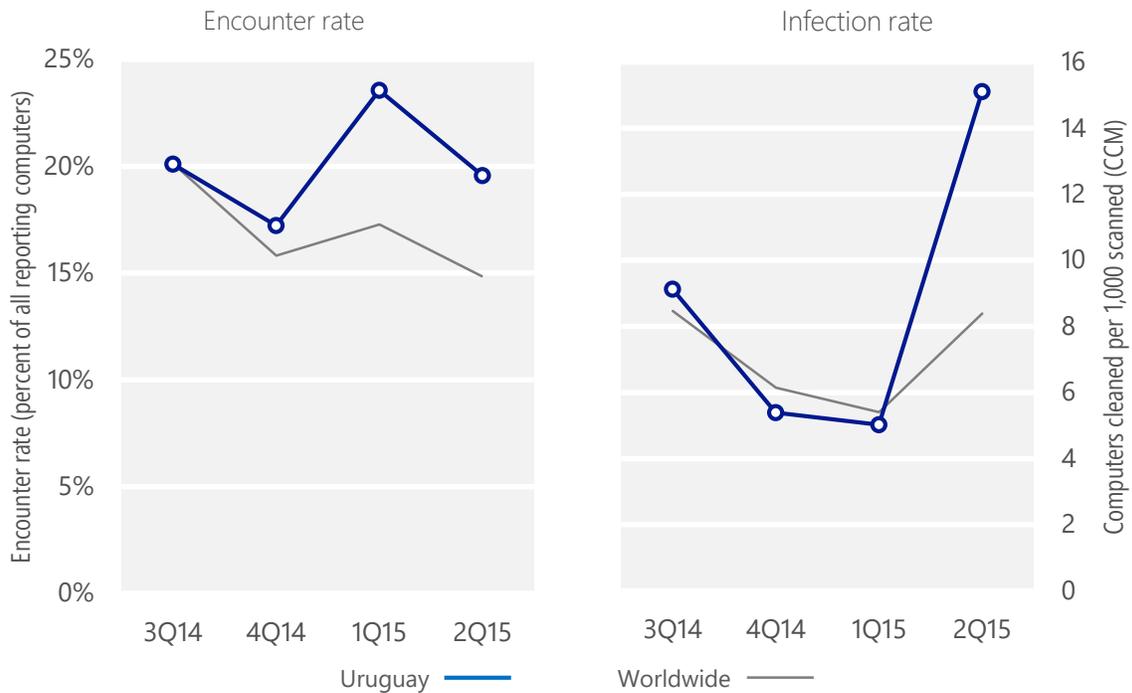
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Uruguay	20.1%	17.2%	23.6%	19.6%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Uruguay	9.1	5.4	5.0	15.1
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcoute, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 19.6% of computers in Uruguay encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 15.1 of every 1,000 unique computers scanned in Uruguay in 2Q15 (a CCM score of 15.1, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Uruguay over the last four quarters, compared to the world as a whole.

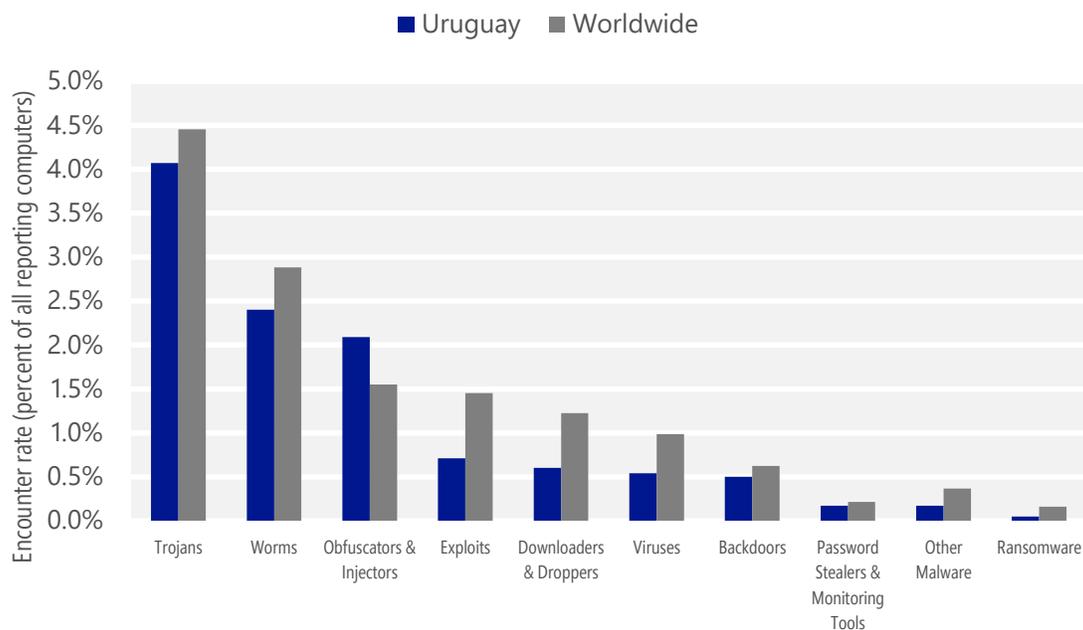
Malware encounter and infection rate trends in Uruguay and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in Uruguay and around the world, and for explanations of the methods and terms used here.

Malware categories

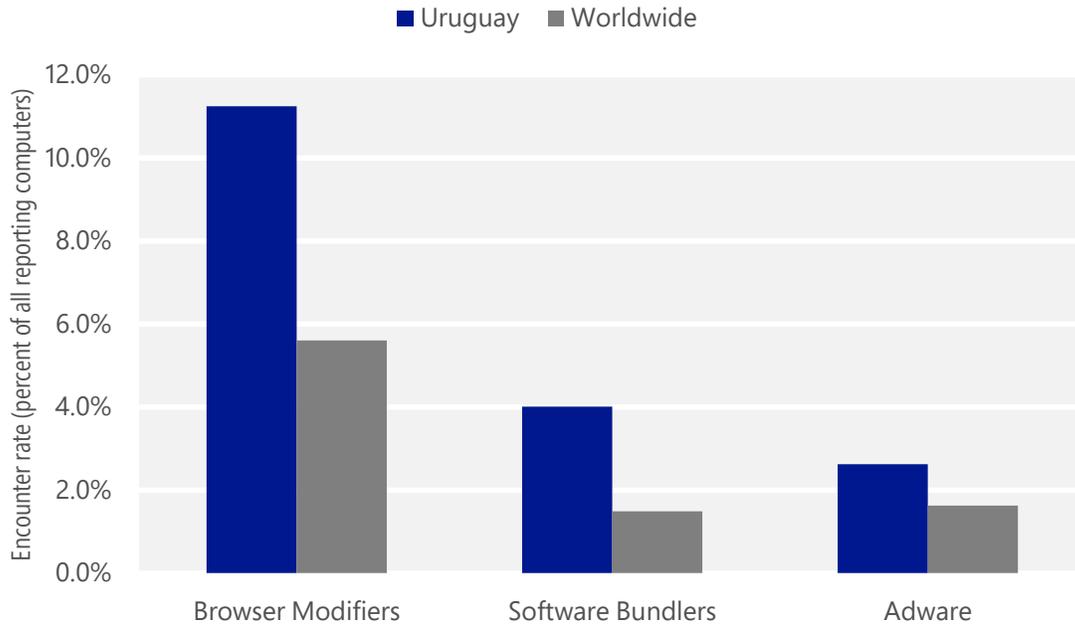
Malware encountered in Uruguay in 2Q15, by category



- The most common malware category in Uruguay in 2Q15 was Trojans. It was encountered by 4.1 percent of all computers there, up from 2.5 percent in 1Q15.
- The second most common malware category in Uruguay in 2Q15 was Worms. It was encountered by 2.4 percent of all computers there, down from 2.5 percent in 1Q15.
- The third most common malware category in Uruguay in 2Q15 was Obfuscators & Injectors, which was encountered by 2.1 percent of all computers there, down from 2.3 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Uruguay in 2Q15, by category



- The most common unwanted software category in Uruguay in 2Q15 was Browser Modifiers. It was encountered by 11.2 percent of all computers there, down from 15.8 percent in 1Q15.
- The second most common unwanted software category in Uruguay in 2Q15 was Software Bundlers. It was encountered by 4.0 percent of all computers there, down from 6.7 percent in 1Q15.
- The third most common unwanted software category in Uruguay in 2Q15 was Adware, which was encountered by 2.6 percent of all computers there, up from 0.7 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Uruguay in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Obfuscator	Obfuscators & Injectors	1.6%
2	Win32/Kilim	Trojans	1.5%
3	Win32/Skeeyah	Trojans	0.7%
4	JS/Bondat	Worms	0.7%
5	INF/Autorun	Obfuscators & Injectors	0.4%
6	VBS/Jenxcus	Worms	0.3%
7	Win32/Conficker	Worms	0.3%
8	JS/Axpergle	Exploits	0.3%
9	Win32/Gamarue	Worms	0.3%
10	Win32/Peals	Trojans	0.2%

- The most common malware family encountered in Uruguay in 2Q15 was [Win32/Obfuscator](#), which was encountered by 1.6 percent of reporting computers there. [Win32/Obfuscator](#) is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The second most common malware family encountered in Uruguay in 2Q15 was [Win32/Kilim](#), which was encountered by 1.5 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The third most common malware family encountered in Uruguay in 2Q15 was [Win32/Skeeyah](#), which was encountered by 0.7 percent of reporting computers there. [Win32/Skeeyah](#) is a generic detection for various threats that display trojan characteristics.
- The fourth most common malware family encountered in Uruguay in 2Q15 was [JS/Bondat](#), which was encountered by 0.7 percent of reporting computers there. [JS/Bondat](#) is a family of threats that collects information about the computer, infects removable drives, and tries to stop the user from accessing files. It spreads by infecting removable drives, such as USB thumb drives and flash drives.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Uruguay in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	5.9%
2	Win32/KipodToolsCby	Browser Modifiers	4.7%
3	Win32/InstalleRex	Software Bundlers	3.9%
4	Win32/SaverExtension	Adware	2.0%
5	Win32/AlterbookSP	Browser Modifiers	0.9%

- The most common unwanted software family encountered in Uruguay in 2Q15 was [Win32/CouponRuc](#), which was encountered by 5.9 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in Uruguay in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 4.7 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common unwanted software family encountered in Uruguay in 2Q15 was [Win32/InstalleRex](#), which was encountered by 3.9 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Uruguay in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	8.8
2	Win32/Kilim	Trojans	1.8
3	Win32/CompromisedCert	Other Malware	1.0
4	VBS/Jenxcus	Worms	0.6
5	Win32/Sality	Viruses	0.5
6	Win32/Ramnit	Trojans	0.5
7	MSIL/Spacekito	Trojans	0.3
8	Win32/Dorkbot	Worms	0.2
9	Win32/Conficker	Worms	0.2
10	MSIL/Bladabindi	Backdoors	0.2

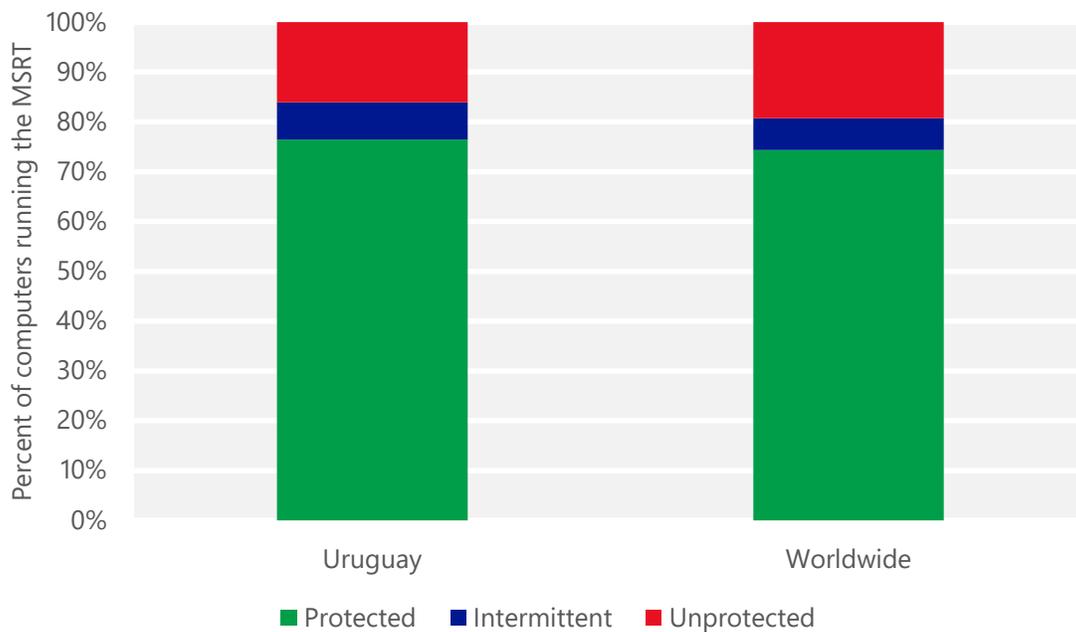
- The most common threat family infecting computers in Uruguay in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 8.8 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Uruguay in 2Q15 was [Win32/Kilim](#), which was detected and removed from 1.8 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The third most common threat family infecting computers in Uruguay in 2Q15 was [Win32/CompromisedCert](#), which was detected and removed from 1.0 of every 1,000 unique computers scanned by the MSRT. [Win32/CompromisedCert](#) is a detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.
- The fourth most common threat family infecting computers in Uruguay in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 0.6 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Uruguay and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Uruguay

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.03 (0.28)	0.01 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	1.42 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	10.76 (16.7)	

Venezuela

The statistics presented here are generated by Microsoft security programs and services running on computers in Venezuela in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Venezuela

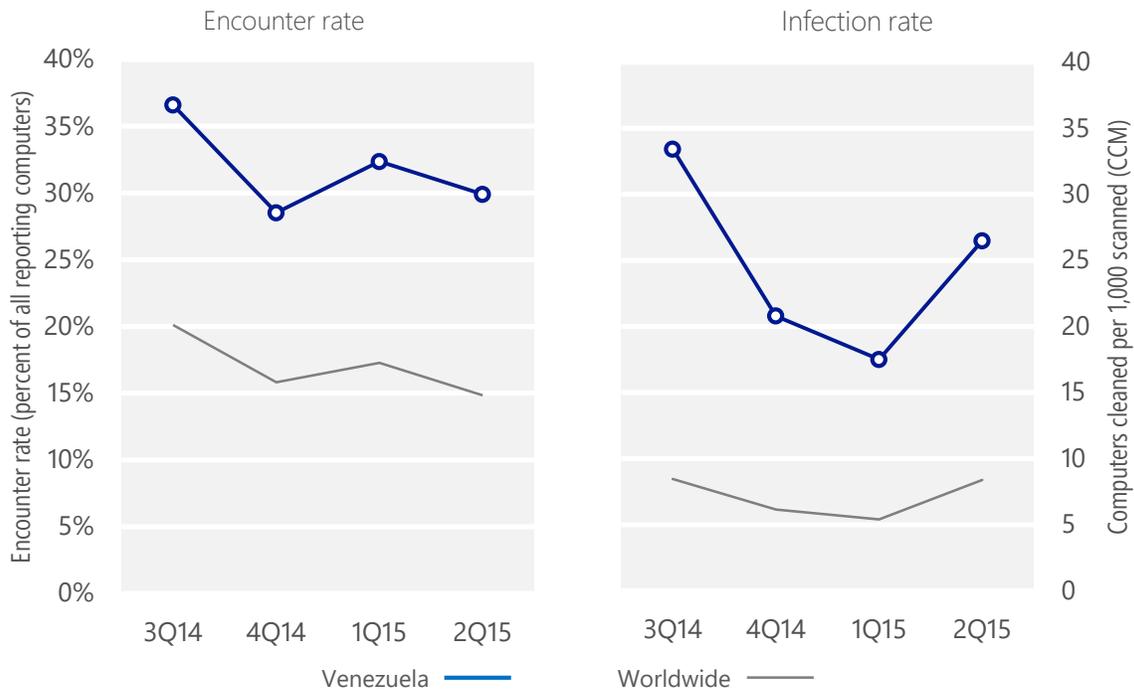
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Venezuela	36.6%	28.5%	32.4%	29.9%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Venezuela	33.4	20.8	17.5	26.5
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcoute, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 29.9% of computers in Venezuela encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 26.5 of every 1,000 unique computers scanned in Venezuela in 2Q15 (a CCM score of 26.5, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Venezuela over the last four quarters, compared to the world as a whole.

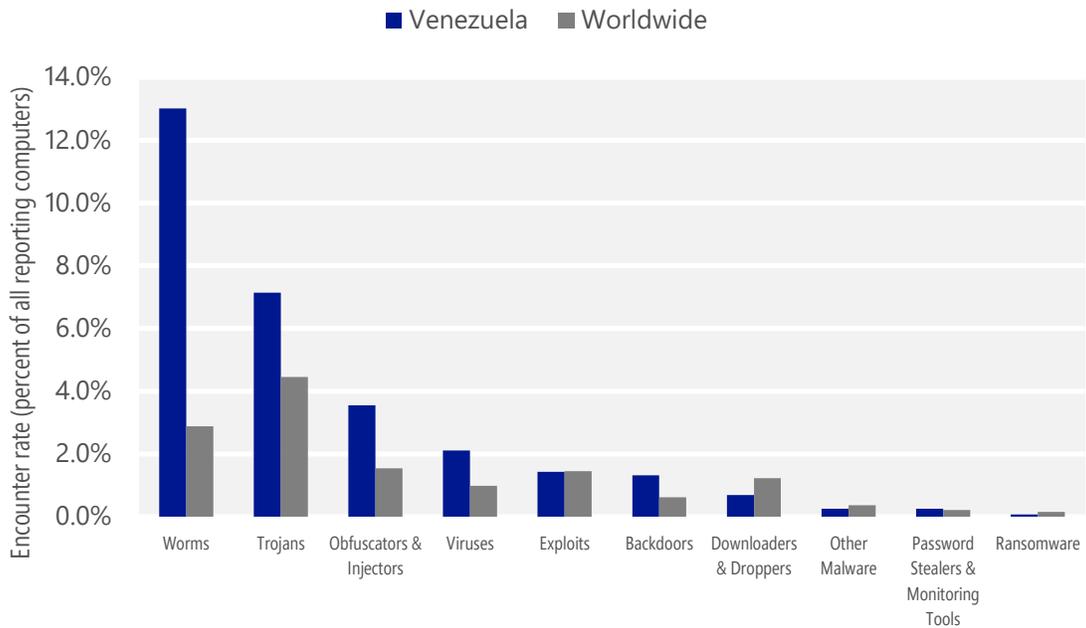
Malware encounter and infection rate trends in Venezuela and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in Venezuela and around the world, and for explanations of the methods and terms used here.

Malware categories

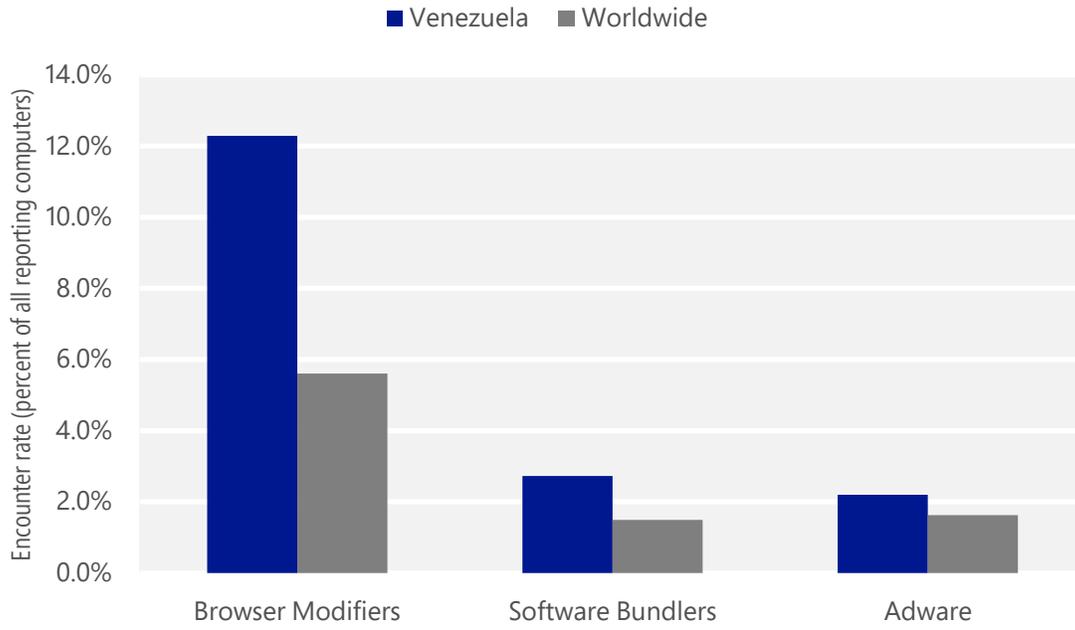
Malware encountered in Venezuela in 2Q15, by category



- The most common malware category in Venezuela in 2Q15 was Worms. It was encountered by 13.0 percent of all computers there, down from 14.3 percent in 1Q15.
- The second most common malware category in Venezuela in 2Q15 was Trojans. It was encountered by 7.1 percent of all computers there, up from 5.3 percent in 1Q15.
- The third most common malware category in Venezuela in 2Q15 was Obfuscators & Injectors, which was encountered by 3.6 percent of all computers there, up from 3.2 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Venezuela in 2Q15, by category



- The most common unwanted software category in Venezuela in 2Q15 was Browser Modifiers. It was encountered by 12.3 percent of all computers there, down from 15.3 percent in 1Q15.
- The second most common unwanted software category in Venezuela in 2Q15 was Software Bundlers. It was encountered by 2.7 percent of all computers there, down from 5.1 percent in 1Q15.
- The third most common unwanted software category in Venezuela in 2Q15 was Adware, which was encountered by 2.2 percent of all computers there, up from 0.7 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Venezuela in 2Q15

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	7.6%
2	JS/Bondat	Worms	2.9%
3	INF/Autorun	Obfuscators & Injectors	1.8%
4	Win32/Kilim	Trojans	1.5%
5	Win32/Conficker	Worms	1.2%
6	Win32/Obfuscator	Obfuscators & Injectors	1.2%
7	Win32/Sality	Viruses	1.1%
8	Win32/Skeeyah	Trojans	1.0%
9	Win32/DelfInject	Obfuscators & Injectors	0.9%
10	Win32/Nuqel	Worms	0.7%

- The most common malware family encountered in Venezuela in 2Q15 was [VBS/Jenxcus](#), which was encountered by 7.6 percent of reporting computers there. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common malware family encountered in Venezuela in 2Q15 was [JS/Bondat](#), which was encountered by 2.9 percent of reporting computers there. [JS/Bondat](#) is a family of threats that collects information about the computer, infects removable drives, and tries to stop the user from accessing files. It spreads by infecting removable drives, such as USB thumb drives and flash drives.
- The third most common malware family encountered in Venezuela in 2Q15 was [INF/Autorun](#), which was encountered by 1.8 percent of reporting computers there. [INF/Autorun](#) is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The fourth most common malware family encountered in Venezuela in 2Q15 was [Win32/Kilim](#), which was encountered by 1.5 percent of reporting computers there. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Venezuela in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/KipodToolsCby	Browser Modifiers	7.0%
2	Win32/CouponRuc	Browser Modifiers	4.7%
3	Win32/InstalleRex	Software Bundlers	2.6%
4	Win32/SaverExtension	Adware	1.6%
5	Win32/AlterbookSP	Browser Modifiers	0.9%

- The most common unwanted software family encountered in Venezuela in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 7.0 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common unwanted software family encountered in Venezuela in 2Q15 was [Win32/CouponRuc](#), which was encountered by 4.7 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The third most common unwanted software family encountered in Venezuela in 2Q15 was [Win32/InstalleRex](#), which was encountered by 2.6 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Venezuela in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	11.7
2	Win32/leEnablerCby	Browser Modifiers	6.4
3	Win32/Sality	Viruses	2.0
4	Win32/Kilim	Trojans	1.8
5	Win32/Ramnit	Trojans	1.2
6	Win32/Dorkbot	Worms	0.7
7	MSIL/Bladabindi	Backdoors	0.4
8	Win32/Nuqel	Worms	0.4
9	Win32/Gamarue	Worms	0.4
10	Win32/Vobfus	Worms	0.3

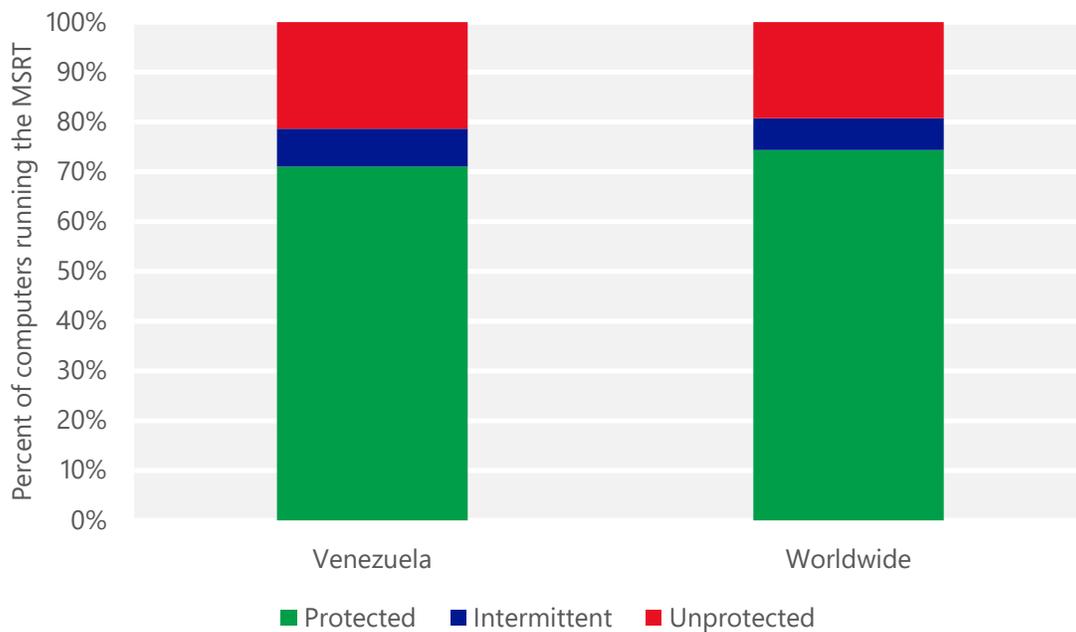
- The most common threat family infecting computers in Venezuela in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 11.7 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Venezuela in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 6.4 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common threat family infecting computers in Venezuela in 2Q15 was [Win32/Sality](#), which was detected and removed from 2.0 of every 1,000 unique computers scanned by the MSRT. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The fourth most common threat family infecting computers in Venezuela in 2Q15 was [Win32/Kilim](#), which was detected and removed from 1.8 of every 1,000 unique computers scanned by the MSRT. [Win32/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Venezuela and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Venezuela

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.29 (0.28)	0.30 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	4.33 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	5.77 (16.7)	

Vietnam

The statistics presented here are generated by Microsoft security programs and services running on computers in Vietnam in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Vietnam

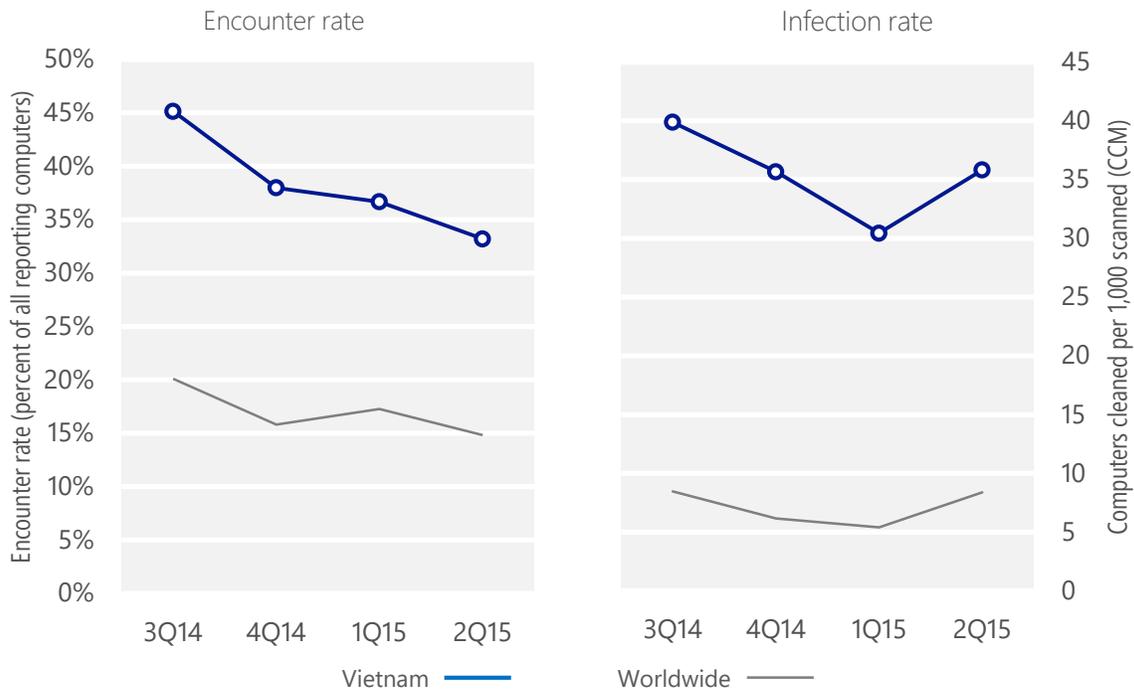
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Vietnam	45.1%	38.0%	36.7%	33.2%
<i>Worldwide encounter rate</i>	<i>20.1%</i>	<i>15.8%</i>	<i>17.3%</i>	<i>14.8%</i>
CCM, Vietnam	39.9	35.7	30.4	35.8
<i>Worldwide CCM</i>	<i>8.5</i>	<i>6.1</i>	<i>5.4</i>	<i>8.4</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcote, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, 33.2% of computers in Vietnam encountered malware, compared to the 2Q15 worldwide encounter rate of 14.8 percent. In addition, the MSRT detected and removed malware from 35.8 of every 1,000 unique computers scanned in Vietnam in 2Q15 (a CCM score of 35.8, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Vietnam over the last four quarters, compared to the world as a whole.

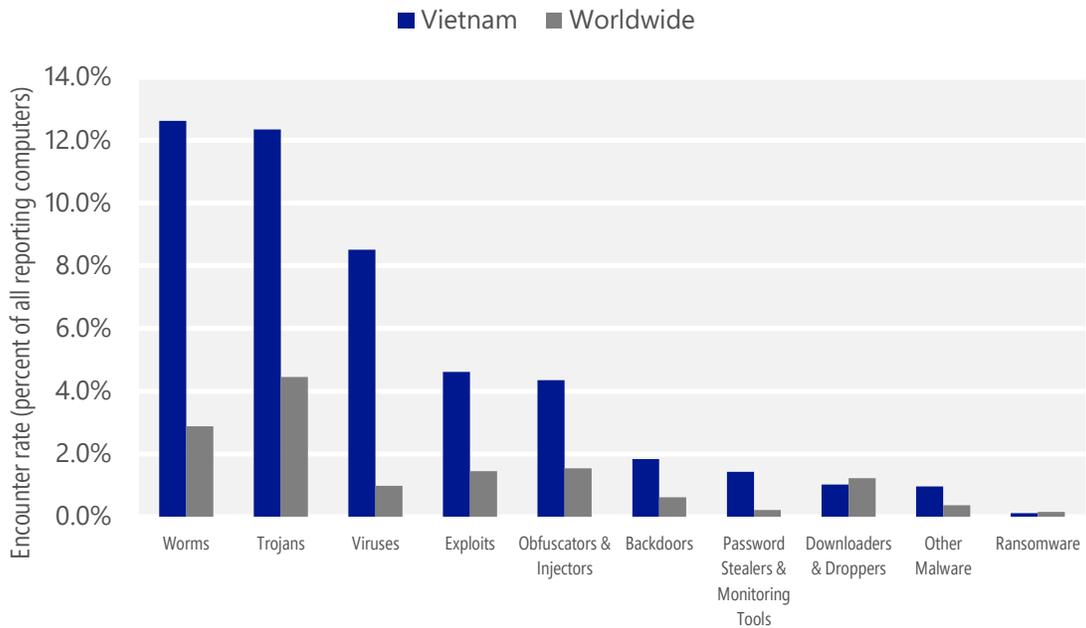
Malware encounter and infection rate trends in Vietnam and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](http://www.microsoft.com/sir) at www.microsoft.com/sir for more information about threats in Vietnam and around the world, and for explanations of the methods and terms used here.

Malware categories

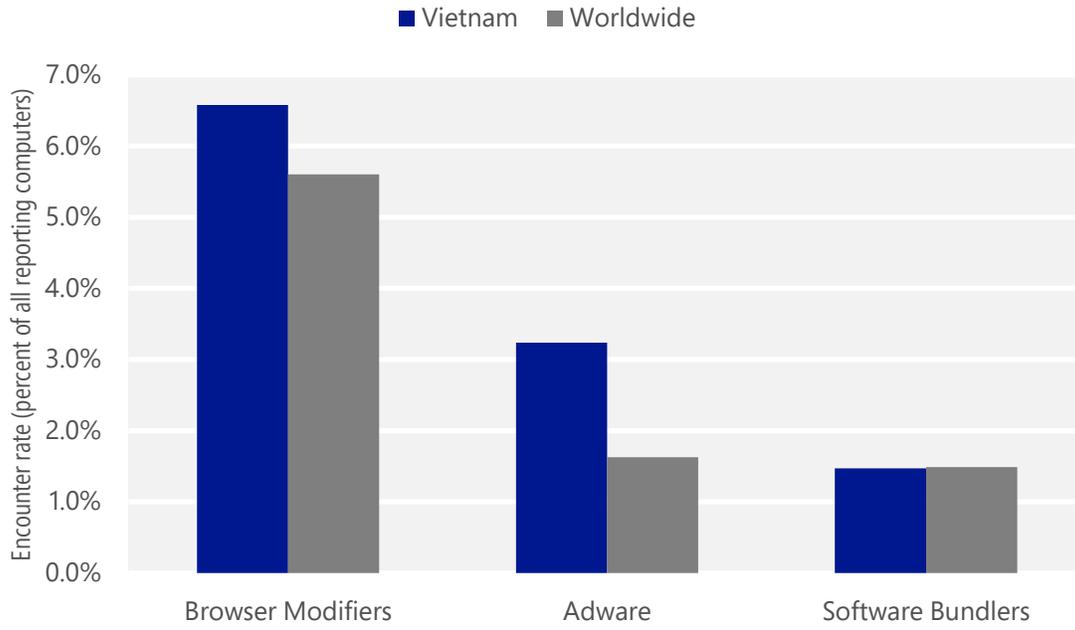
Malware encountered in Vietnam in 2Q15, by category



- The most common malware category in Vietnam in 2Q15 was Worms. It was encountered by 12.6 percent of all computers there, down from 14.0 percent in 1Q15.
- The second most common malware category in Vietnam in 2Q15 was Trojans. It was encountered by 12.3 percent of all computers there, up from 11.4 percent in 1Q15.
- The third most common malware category in Vietnam in 2Q15 was Viruses, which was encountered by 8.5 percent of all computers there, down from 10.5 percent in 1Q15.

Unwanted software categories

Unwanted software encountered in Vietnam in 2Q15, by category



- The most common unwanted software category in Vietnam in 2Q15 was Browser Modifiers. It was encountered by 6.6 percent of all computers there, down from 9.5 percent in 1Q15.
- The second most common unwanted software category in Vietnam in 2Q15 was Adware. It was encountered by 3.2 percent of all computers there, down from 4.3 percent in 1Q15.
- The third most common unwanted software category in Vietnam in 2Q15 was Software Bundlers, which was encountered by 1.5 percent of all computers there, up from 0.7 percent in 1Q15.

Top malware families by encounter rate

The most common malware families encountered in Vietnam in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/Gamarue	Worms	6.3%
2	INF/Autorun	Obfuscators & Injectors	4.0%
3	Win32/CplLnk	Exploits	4.0%
4	Win32/Ramnit	Trojans	3.9%
5	Win32/Sality	Viruses	3.2%
6	DOS/Sigru	Viruses	2.4%
7	VBS/Jenxcus	Worms	2.0%
8	Win32/Obfuscator	Obfuscators & Injectors	1.6%
9	Win32/VB	Worms	1.5%
10	JS/Faceliker	Trojans	1.4%

- The most common malware family encountered in Vietnam in 2Q15 was [Win32/Gamarue](#), which was encountered by 6.3 percent of reporting computers there. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The second most common malware family encountered in Vietnam in 2Q15 was [INF/Autorun](#), which was encountered by 4.0 percent of reporting computers there. [INF/Autorun](#) is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The third most common malware family encountered in Vietnam in 2Q15 was [Win32/CplLnk](#), which was encountered by 4.0 percent of reporting computers there. [Win32/CplLnk](#) is a generic detection for specially-crafted malicious shortcut files that attempt to exploit the vulnerability addressed by Microsoft Security Bulletin MS10-046.
- The fourth most common malware family encountered in Vietnam in 2Q15 was [Win32/Ramnit](#), which was encountered by 3.9 percent of reporting computers there. [Win32/Ramnit](#) is a family of multi-component malware that infects executable files, Microsoft Office files, and HTML files. [Win32/Ramnit](#) spreads to removable drives and steals sensitive information such as saved FTP credentials and browser cookies. It may also open a backdoor to await instructions from a remote attacker.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Vietnam in 2Q15

	Family	Most significant category	% of reporting computers
1	Win32/CouponRuc	Browser Modifiers	3.1%
2	Win32/KipodToolsCby	Browser Modifiers	2.9%
3	Win32/InstalleRex	Software Bundlers	1.4%
4	Win32/SaverExtension	Adware	0.9%
5	Win32/EoRezo	Adware	0.8%

- The most common unwanted software family encountered in Vietnam in 2Q15 was [Win32/CouponRuc](#), which was encountered by 3.1 percent of reporting computers there. [Win32/CouponRuc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in Vietnam in 2Q15 was [Win32/KipodToolsCby](#), which was encountered by 2.9 percent of reporting computers there. [Win32/KipodToolsCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The third most common unwanted software family encountered in Vietnam in 2Q15 was [Win32/InstalleRex](#), which was encountered by 1.4 percent of reporting computers there. [Win32/InstalleRex](#) is a software bundler that installs unwanted software, including [Win32/CouponRuc](#) and [Win32/SaverExtension](#). It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

Top threat families by infection rate

The most common malware families by infection rate in Vietnam in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/leEnablerCby	Browser Modifiers	7.3
2	Win32/Gamarue	Worms	6.8
3	Win32/Ramnit	Trojans	6.5
4	Win32/Sality	Viruses	6.3
5	VBS/Jenxcus	Worms	2.7
6	Win32/Kilim	Trojans	1.5
7	Win32/Brontok	Worms	1.3
8	Win32/Folstart	Worms	1.0
9	Win32/Virut	Viruses	1.0
10	Win32/Pramro	Trojans	0.9

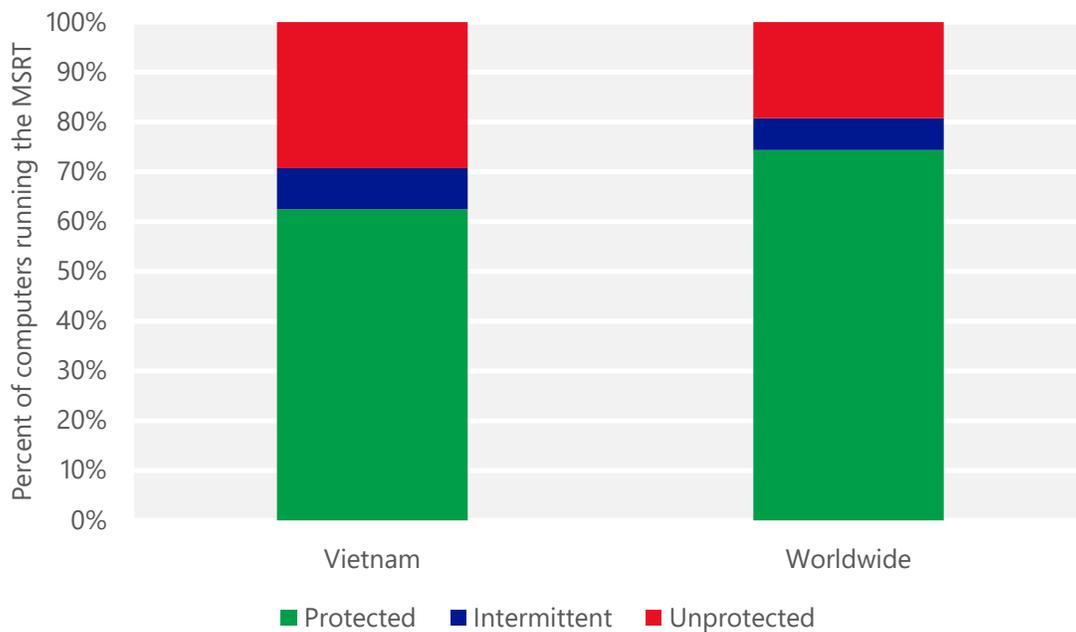
- The most common threat family infecting computers in Vietnam in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 7.3 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The second most common threat family infecting computers in Vietnam in 2Q15 was [Win32/Gamarue](#), which was detected and removed from 6.8 of every 1,000 unique computers scanned by the MSRT. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The third most common threat family infecting computers in Vietnam in 2Q15 was [Win32/Ramnit](#), which was detected and removed from 6.5 of every 1,000 unique computers scanned by the MSRT. [Win32/Ramnit](#) is a family of multi-component malware that infects executable files, Microsoft Office files, and HTML files. Win32/Ramnit spreads to removable drives and steals sensitive information such as saved FTP credentials and browser cookies. It may also open a backdoor to await instructions from a remote attacker.
- The fourth most common threat family infecting computers in Vietnam in 2Q15 was [Win32/Sality](#), which was detected and removed from 6.3 of every 1,000 unique computers scanned by the MSRT. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Vietnam and worldwide protected by real-time security software in 2Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Vietnam

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	3.96 (0.28)	3.03 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	8.13 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	16.71 (16.7)	

Zimbabwe

The statistics presented here are generated by Microsoft security programs and services running on computers in Zimbabwe in 2Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Zimbabwe

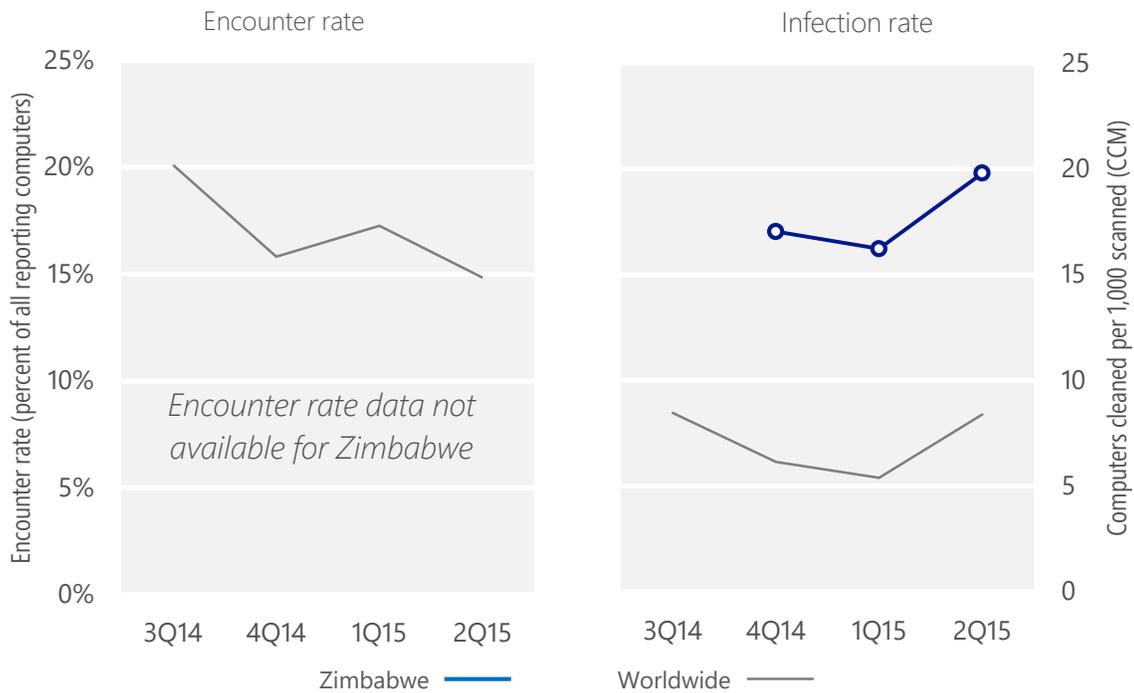
Metric	3Q14	4Q14	1Q15	2Q15
Encounter rate, Zimbabwe	N/A	N/A	N/A	N/A
<i>Worldwide encounter rate</i>	20.1%	15.8%	17.3%	14.8%
CCM, Zimbabwe	N/A	17.0	16.2	19.8
<i>Worldwide CCM</i>	8.5	6.1	5.4	8.4

Encounter and infection rates reported here do not include totals for the Brantall, Filcote, and Rotbrow malware families. See pages 57–64 of [Microsoft Security Intelligence Report, Volume 17](#) for an explanation of this decision.

Encounter and infection rate trends

In 2Q15, the MSRT detected and removed malware from 19.8 of every 1,000 unique computers scanned in Zimbabwe in 2Q15 (a CCM score of 19.8, compared to the 2Q15 worldwide CCM of 8.4). The following figure shows the encounter and infection rate trends for Zimbabwe over the last four quarters, compared to the world as a whole.

Malware encounter and infection rate trends in Zimbabwe and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) at www.microsoft.com/sir for more information about threats in Zimbabwe and around the world, and for explanations of the methods and terms used here.

Top threat families by infection rate

The most common malware families by infection rate in Zimbabwe in 2Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/Chir	Viruses	4.2
2	VBS/Jenxcus	Worms	4.1
3	Win32/leEnablerCby	Browser Modifiers	4.0
4	Win32/Sality	Viruses	2.1
5	Win32/Virut	Viruses	2.0
6	Win32/Kilim	Trojans	1.0
7	Win32/CompromisedCert	Other Malware	1.0
8	Win32/Ramnit	Trojans	0.7
9	MSIL/Bladabindi	Backdoors	0.4
10	Win32/Vobfus	Worms	0.4

- The most common threat family infecting computers in Zimbabwe in 2Q15 was [Win32/Chir](#), which was detected and removed from 4.2 of every 1,000 unique computers scanned by the MSRT. [Win32/Chir](#) is a family with a worm component and a virus component. The worm component spreads by email and by exploiting a vulnerability addressed by Microsoft Security Bulletin MS01-020. The virus component may infect .exe, .scr, and HTML files.
- The second most common threat family infecting computers in Zimbabwe in 2Q15 was [VBS/Jenxcus](#), which was detected and removed from 4.1 of every 1,000 unique computers scanned by the MSRT. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The third most common threat family infecting computers in Zimbabwe in 2Q15 was [Win32/leEnablerCby](#), which was detected and removed from 4.0 of every 1,000 unique computers scanned by the MSRT. [Win32/leEnablerCby](#) is a browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
- The fourth most common threat family infecting computers in Zimbabwe in 2Q15 was [Win32/Sality](#), which was detected and removed from 2.1 of every 1,000 unique computers scanned by the MSRT. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.

Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Internet Explorer. See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 19](#) for more information about these protections and how the data is collected.

Malicious website statistics for Zimbabwe

Metric	1Q15	2Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.75 (0.28)	0.91 (0.24)
Phishing sites per 1,000 hosts (Worldwide)	6.88 (5.0)	
Malware hosting sites per 1,000 hosts (Worldwide)	23.38 (16.7)	



One Microsoft Way
Redmond, WA 98052-6399
microsoft.com/security