Microsoft Security Intelligence Report

Volume 18 | July through December, 2014

REGIONAL THREAT ASSESSMENT

Microsoft

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.

Contents

Albania

The statistics presented here are generated by Microsoft security programs and services running on computers in Albania in 4Q14 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 succeds 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

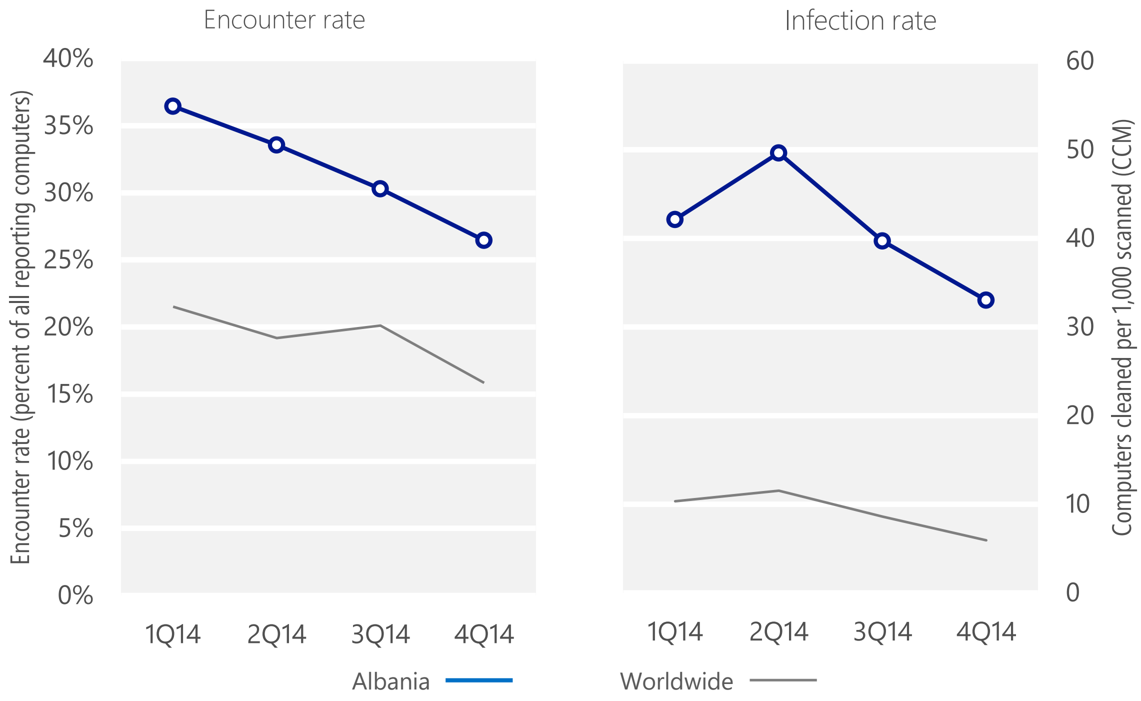
Metric	**1Q14**	**2Q14**	**3Q14**	**4Q14**
Encounter rate, Albania	36.5%	33.6%	30.3%	26.5%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Albania	42.1	49.6	39.7	33.0
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 26.5% percent of computers in Albania encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 33.0 of every 1,000 unique computers scanned in Albania in 4Q14 (a CCM score of 33.0, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Albania over the last four quarters, compared to the world as a whole.

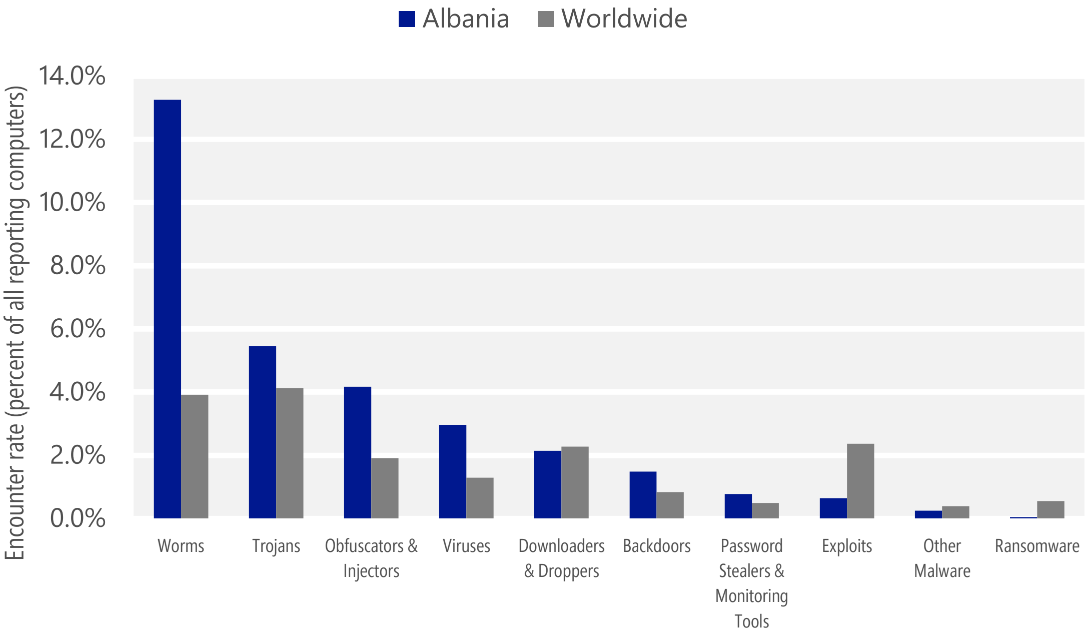
Malware encounter and infection rate trends in Albania and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

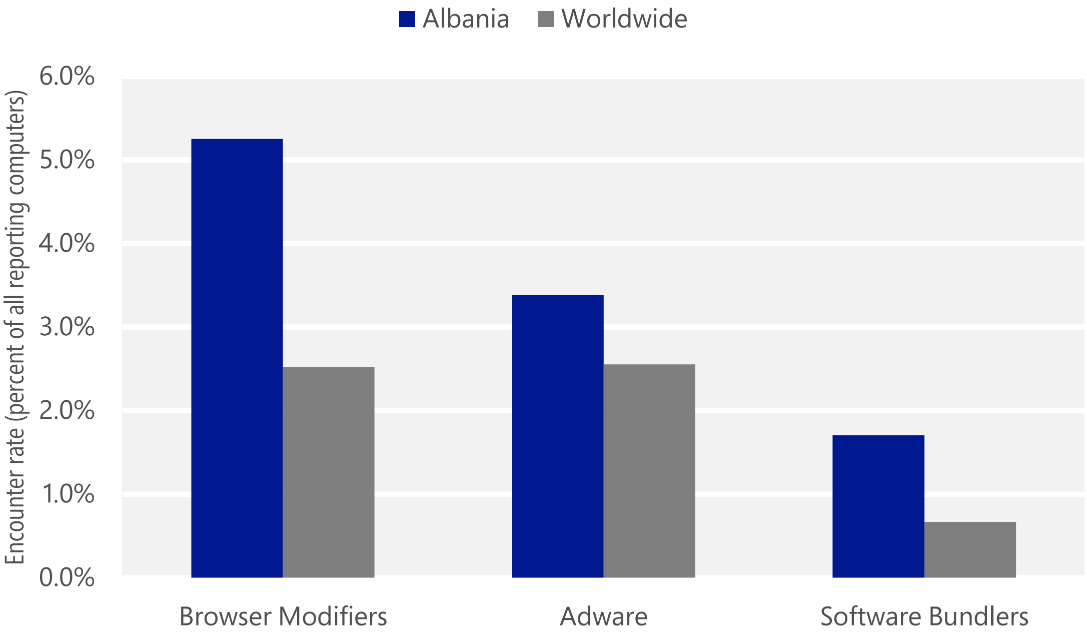
Malware encountered in Albania in 4Q14, by category



- The most common malware category in Albania in 4Q14 was Worms. It was encountered by 13.3 percent of all computers there, up from 12.3 percent in 3Q14.
- The second most common malware category in Albania in 4Q14 was Trojans. It was encountered by 5.5 percent of all computers there, down from 11.4 percent in 3Q14.
- The third most common malware category in Albania in 4Q14 was Obfuscators & Injectors, which was encountered by 4.2 percent of all computers there, down from 4.4 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Albania in 4Q14, by category



- The most common unwanted software category in Albania in 4Q14 was Browser Modifiers. It was encountered by 5.2 percent of all computers there, down from 7.8 percent in 3Q14.
- The second most common unwanted software category in Albania in 4Q14 was Adware. It was encountered by 3.4 percent of all computers there, up from 0.9 percent in 3Q14.
- The third most common unwanted software category in Albania in 4Q14 was Software Bundlers, which was encountered by 1.7 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Albania in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Gamarue	Worms	5.5%
2	VBS/Jenxcus	Worms	4.2%
3	INF/Autorun	Obfuscators & Injectors	3.7%
4	Win32/Sality	Viruses	2.3%
5	Win32/Helompy	Worms	2.3%
6	Win32/Conficker	Worms	1.6%
7	Win32/Brontok	Worms	1.1%
8	Win32/Yeltminky	Worms	1.1%
9	Win32/Vobfus	Worms	0.9%
10	Win32/Obfuscator	Obfuscators & Injectors	0.8%

- The most common malware family encountered in Albania in 4Q14 was Win32/Gamarue, which was encountered by 5.5 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 4Q14 was VBS/Jenxcus, which was encountered by 4.2 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 4Q14 was INF/Autorun, which was encountered by 3.7 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 fourth most common malware family encountered in Albania in 4Q14 was Win32/Sality, which was encountered by 2.3 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 Albania in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	3.1%
2	Win32/Defaulttab	Browser Modifiers	2.4%
3	Win32/BetterSurf	Adware	1.9%
4	Win32/Costmin	Adware	1.3%
5	Win32/Gofileexpress	Software Bundlers	1.2%

- The most common unwanted software family encountered in Albania in 4Q14 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 Albania in 4Q14 was Win32/Defaulttab, which was encountered by 2.4 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.
- The third most common unwanted software family encountered in Albania in 4Q14 was Win32/BetterSurf, which was encountered by 1.9 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.

Top threat families by infection rate

The most common malware families by infection rate in Albania in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Sality	Viruses	10.7
2	Win32/Gamarue	Worms	6.7
3	VBS/Jenxcus	Worms	5.3
4	Win32/Helompy	Worms	3.5
5	JS/Kilim	Trojans	2.6
6	Win32/Pramro	Trojans	2.3
7	Win32/Brontok	Worms	2.1
8	Win32/Yeltminky	Worms	1.7
9	Win32/Sefnit	Trojans	0.9
10	Win32/Vobfus	Worms	0.9

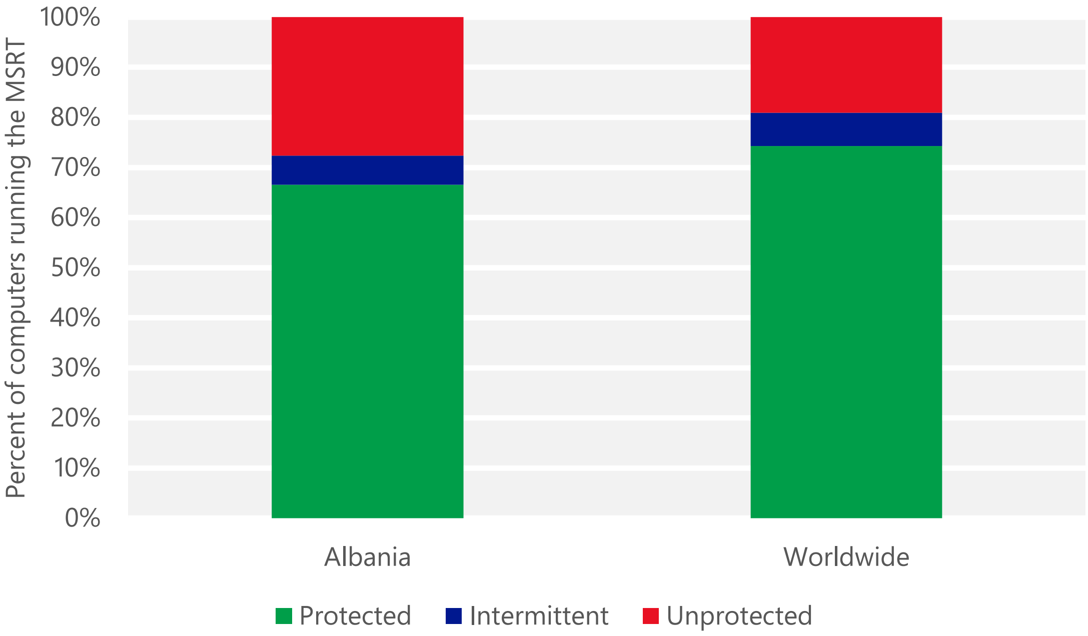
- The most common threat family infecting computers in Albania in 4Q14 was Win32/Sality, which was detected and removed from 10.7 of every 1,000 unique computers scanned by the MSRT. Win32/Sality is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The second most common threat family infecting computers in Albania in 4Q14 was Win32/Gamarue, which was detected and removed from 6.7 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 third most common threat family infecting computers in Albania in 4Q14 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.
- The fourth most common threat family infecting computers in Albania in 4Q14 was Win32/Helompy, which was detected and removed from 3.5 of every 1,000 unique computers scanned by the MSRT. Win32/Helompy is a worm that spreads via removable drives and attempts to capture and steal authentication details for a number of different websites or online 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 Albania and worldwide protected by real-time security software in 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 2.39 drive-by download URLs for every 1,000 URLs hosted in Albania, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.83 drive-by download URLs for every 1,000 URLs hosted in Albania, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Albania and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Albania	2.39	0.83
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Algeria

The statistics presented here are generated by Microsoft security programs and services running on computers in Algeria in 4Q14 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 succeds 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

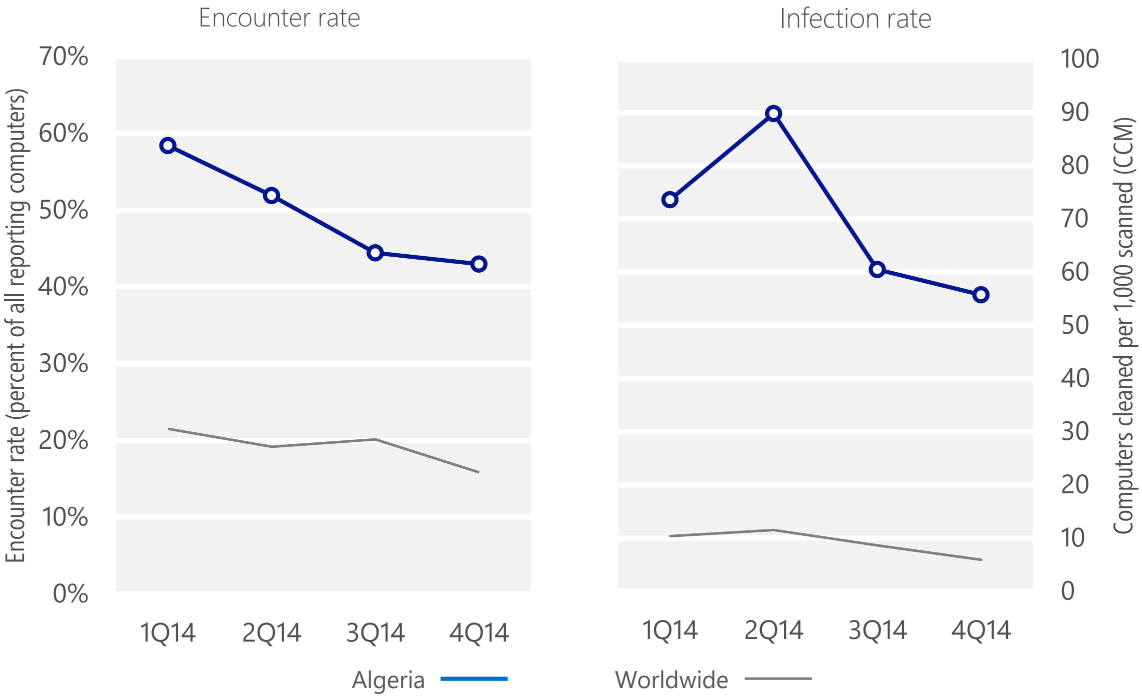
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Algeria	58.4%	51.9%	44.4%	43.0%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Algeria	73.6	89.8	60.5	55.7
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 43.0% percent of computers in Algeria encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 55.7 of every 1,000 unique computers scanned in Algeria in 4Q14 (a CCM score of 55.7, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Algeria over the last four quarters, compared to the world as a whole.

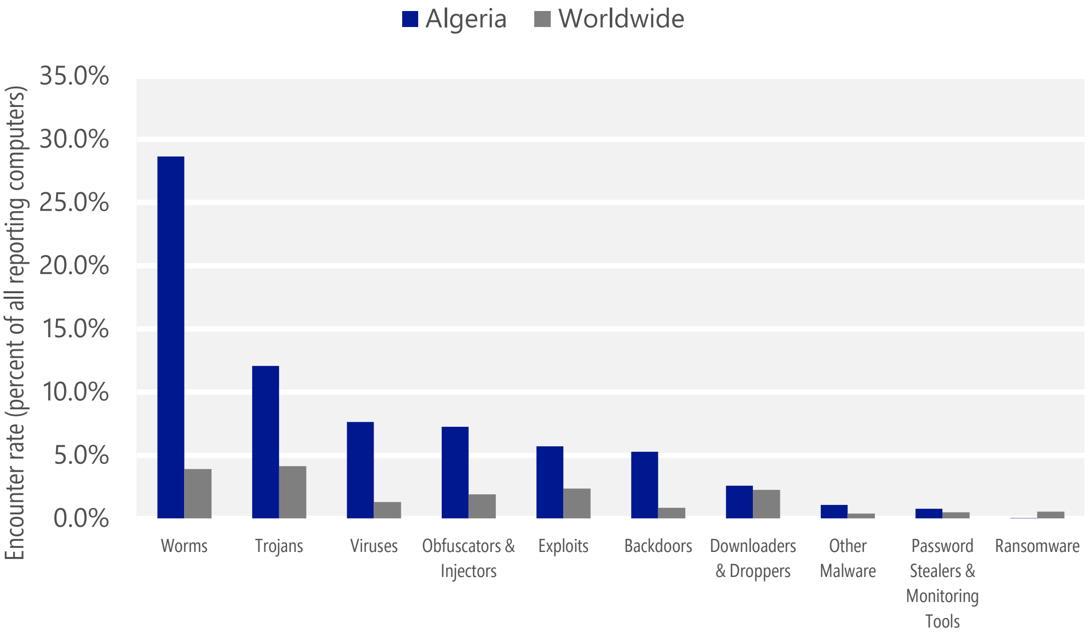
Malware encounter and infection rate trends in Algeria and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

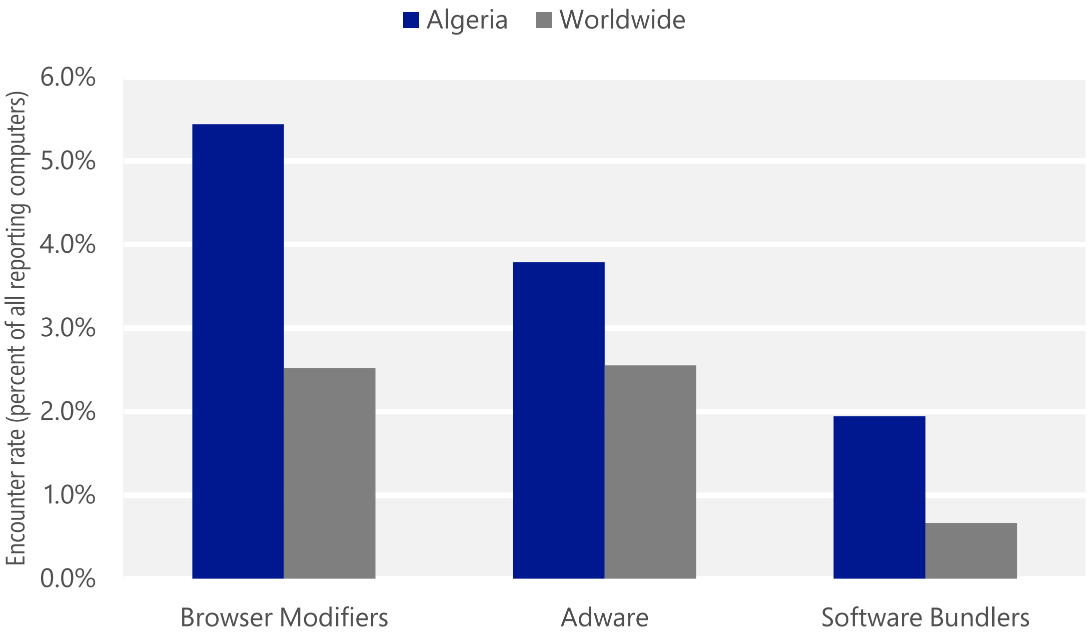
Malware encountered in Algeria in 4Q14, by category



- The most common malware category in Algeria in 4Q14 was Worms. It was encountered by 28.7 percent of all computers there, up from 26.2 percent in 3Q14.
- The second most common malware category in Algeria in 4Q14 was Trojans. It was encountered by 12.1 percent of all computers there, down from 15.5 percent in 3Q14.
- The third most common malware category in Algeria in 4Q14 was Viruses, which was encountered by 7.6 percent of all computers there, up from 7.2 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Algeria in 4Q14, by category



- The most common unwanted software category in Algeria in 4Q14 was Browser Modifiers. It was encountered by 5.4 percent of all computers there, down from 7.4 percent in 3Q14.
- The second most common unwanted software category in Algeria in 4Q14 was Adware. It was encountered by 3.8 percent of all computers there, up from 3.2 percent in 3Q14.
- The third most common unwanted software category in Algeria in 4Q14 was Software Bundlers, which was encountered by 1.9 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Algeria in 4Q14

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	17.2%
2	INF/Autorun	Obfuscators & Injectors	12.0%
3	Win32/Ippedo	Worms	7.8%
4	Win32/Ramnit	Trojans	5.4%
5	Win32/Gamarue	Worms	5.4%
6	Win32/CplLnk	Exploits	5.0%
7	Win32/Sality	Viruses	4.2%
8	MSIL/Bladabindi	Backdoors	3.5%
9	Win32/Virut	Viruses	2.7%
10	Win32/Yeltminky	Worms	1.8%

- The most common malware family encountered in Algeria in 4Q14 was VBS/Jenxcus, which was encountered by 17.2 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 Algeria in 4Q14 was INF/Autorun, which was encountered by 12.0 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 Algeria in 4Q14 was Win32/Ippedo, which was encountered by 7.8 percent of reporting computers there. Win32/Ippedo is a worm that can send sensitive information to a malicious hacker. It spreads through infected removable drives, such as USB flash drives.
- The fourth most common malware family encountered in Algeria in 4Q14 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 Algeria in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	3.9%
2	Win32/Defaulttab	Browser Modifiers	1.7%
3	Win32/Gofileexpress	Software Bundlers	1.6%
4	Win32/BetterSurf	Adware	1.5%
5	Win32/Costmin	Adware	1.2%

- The most common unwanted software family encountered in Algeria in 4Q14 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 second most common unwanted software family encountered in Algeria in 4Q14 was Win32/Defaulttab, which was encountered by 1.7 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.
- The third most common unwanted software family encountered in Algeria in 4Q14 was Win32/Gofileexpress, which was encountered by 1.6 percent of reporting computers there. Win32/Gofileexpress is a software bundler that installs other unwanted software, including Adware:Win32/Lollipop and Adware:Win32/CostMin.

Top threat families by infection rate

The most common malware families by infection rate in Algeria in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	27.5
2	Win32/Sality	Viruses	9.9
3	Win32/Ramnit	Trojans	5.7
4	Win32/Gamarue	Worms	5.1
5	MSIL/Bladabindi	Backdoors	4.6
6	Win32/Yeltminky	Worms	3.4
7	Win32/Vobfus	Worms	1.4
8	JS/Kilim	Trojans	1.4
9	Win32/Dorkbot	Worms	1.1
10	Win32/Pramro	Trojans	1.1

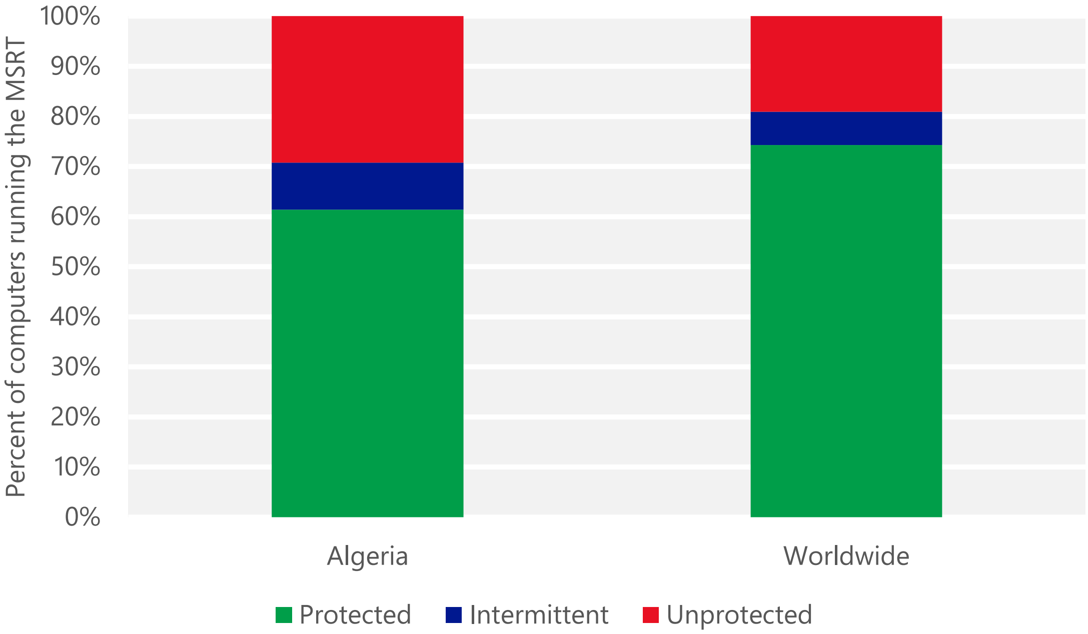
- The most common threat family infecting computers in Algeria in 4Q14 was VBS/Jenxcus, which was detected and removed from 27.5 of every 1,000 unique computers scanned by the MSRT. VBS/Jenxcus is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Algeria in 4Q14 was Win32/Sality, which was detected and removed from 9.9 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 third most common threat family infecting computers in Algeria in 4Q14 was Win32/Ramnit, which was detected and removed from 5.7 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 Algeria in 4Q14 was Win32/Gamarue, which was detected and removed from 5.1 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.

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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.15 drive-by download URLs for every 1,000 URLs hosted in Algeria, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.10 drive-by download URLs for every 1,000 URLs hosted in Algeria, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Algeria and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Algeria	0.15	0.10
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Angola

The statistics presented here are generated by Microsoft security programs and services running on computers in Angola in 4Q14 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 succeds 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

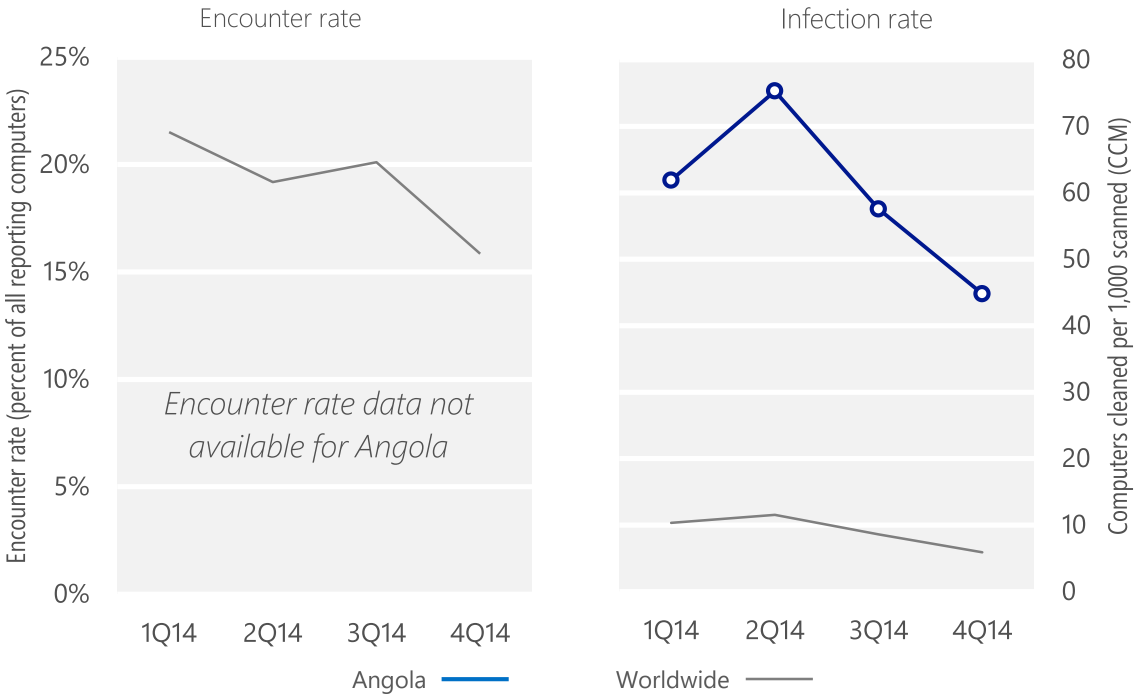
Metric	**1Q14**	**2Q14**	**3Q14**	**4Q14**
Encounter rate, Angola	N/A	N/A	N/A	N/A
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Angola	61.9	75.3	57.6	44.8
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, the MSRT detected and removed malware from 44.8 of every 1,000 unique computers scanned in Angola in 4Q14 (a CCM score of 44.8, compared to the 4Q14 worldwide CCM of 5.9). 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 18* 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 4Q14

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	26.4
2	Win32/Gamarue	Worms	9.1
3	Win32/Tupym	Worms	5.4
4	Win32/Chir	Viruses	2.5
5	Win32/Ramnit	Trojans	2.3
6	Win32/Vobfus	Worms	2.1
7	Win32/Sality	Viruses	1.0
8	MSIL/Bladabindi	Backdoors	0.7
9	Win32/Folstart	Worms	0.5
10	Win32/Wysotot	Trojans	0.4

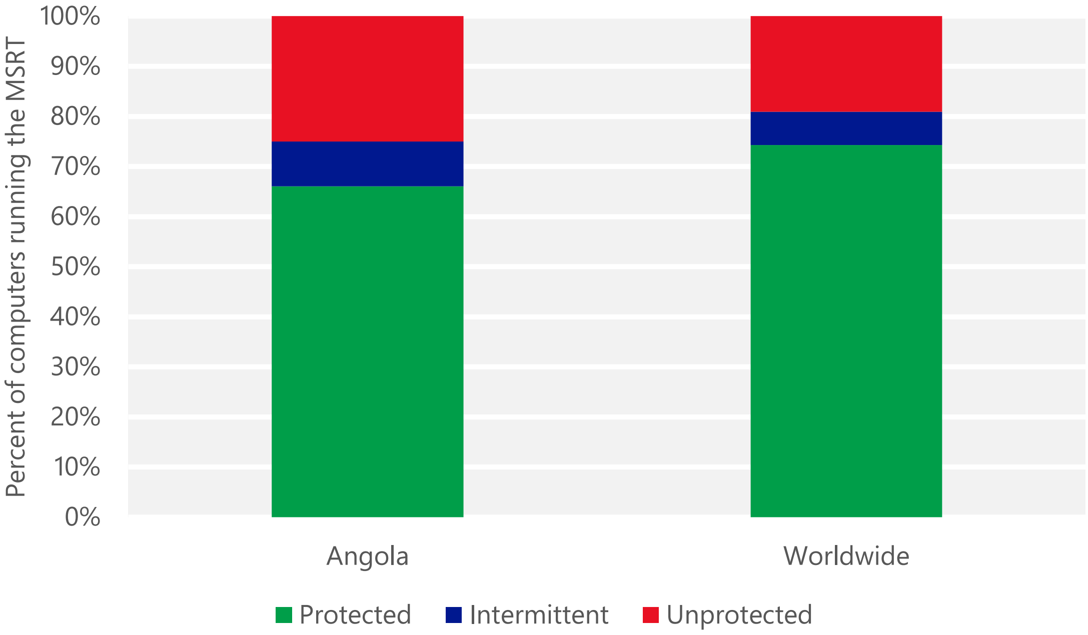
- The most common threat family infecting computers in Angola in 4Q14 was VBS/Jenxcus, which was detected and removed from 26.4 of every 1,000 unique computers scanned by the MSRT. VBS/Jenxcus is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Angola in 4Q14 was Win32/Gamarue, which was detected and removed from 9.1 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 Angola in 4Q14 was Win32/Tupym, which was detected and removed from 5.4 of every 1,000 unique computers scanned by the MSRT. Win32/Tupym is a worm that copies itself to the system folder of the affected computer, and attempts to contact remote hosts.
- The fourth most common threat family infecting computers in Angola in 4Q14 was Win32/Chir, which was detected and removed from 2.5 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.

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 4Q14



Argentina

The statistics presented here are generated by Microsoft security programs and services running on computers in Argentina in 4Q14 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 succeds 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

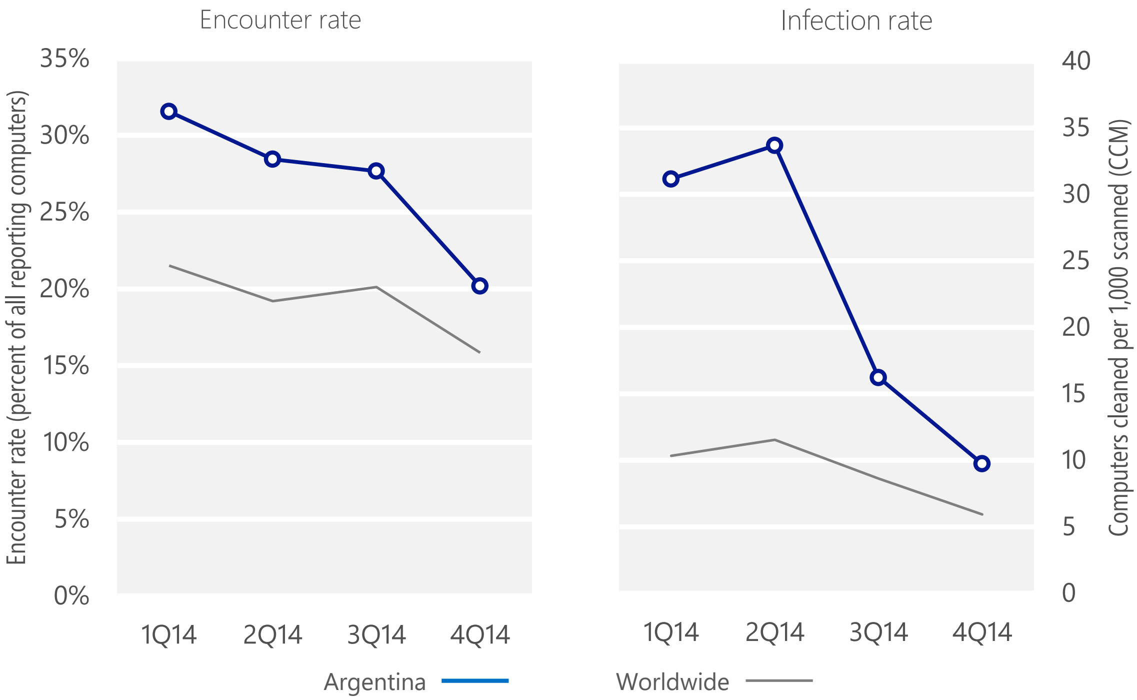
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Argentina	31.6%	28.4%	27.7%	20.2%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Argentina	31.2	33.7	16.2	9.7
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 20.2% percent of computers in Argentina encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 9.7 of every 1,000 unique computers scanned in Argentina in 4Q14 (a CCM score of 9.7, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Argentina over the last four quarters, compared to the world as a whole.

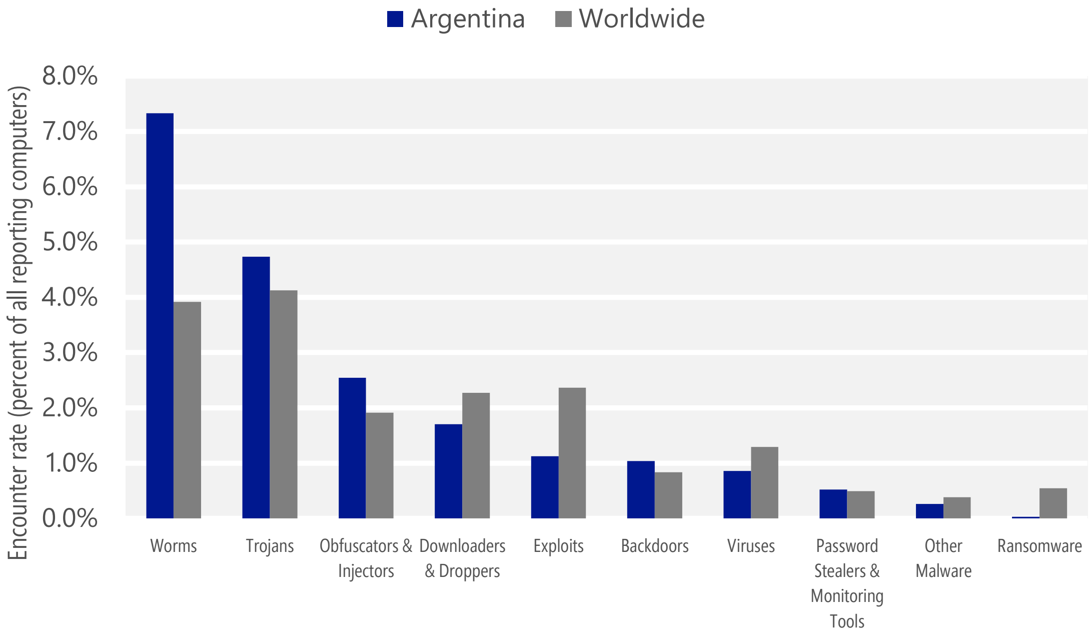
Malware encounter and infection rate trends in Argentina and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

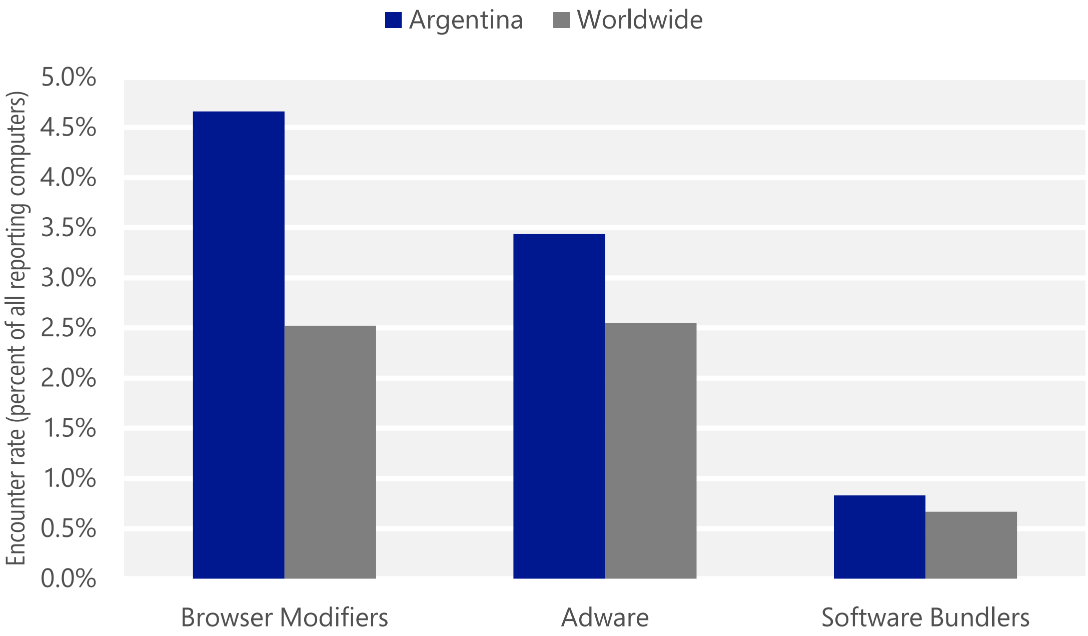
Malware encountered in Argentina in 4Q14, by category



- The most common malware category in Argentina in 4Q14 was Worms. It was encountered by 7.3 percent of all computers there, down from 8.2 percent in 3Q14.
- The second most common malware category in Argentina in 4Q14 was Trojans. It was encountered by 4.7 percent of all computers there, down from 8.1 percent in 3Q14.
- The third most common malware category in Argentina in 4Q14 was Obfuscators & Injectors, which was encountered by 2.5 percent of all computers there, down from 4.9 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Argentina in 4Q14, by category



- The most common unwanted software category in Argentina in 4Q14 was Browser Modifiers. It was encountered by 4.7 percent of all computers there, down from 8.4 percent in 3Q14.
- The second most common unwanted software category in Argentina in 4Q14 was Adware. It was encountered by 3.4 percent of all computers there, down from 4.1 percent in 3Q14.
- The third most common unwanted software category in Argentina in 4Q14 was Software Bundlers, which was encountered by 0.8 percent of all computers there, up from 0.3 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Argentina in 4Q14

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	2.4%
2	Win32/Dorkbot	Worms	1.4%
3	Win32/Obfuscator	Obfuscators & Injectors	1.2%
4	INF/Autorun	Obfuscators & Injectors	1.0%
5	Win32/Vermis	Worms	1.0%
6	Win32/Conficker	Worms	0.9%
7	JS/Bondat	Worms	0.8%
8	JS/Redirector	Trojans	0.6%
9	Win32/Wysotot	Trojans	0.5%
10	Win32/Anaki	Trojans	0.5%

- The most common malware family encountered in Argentina in 4Q14 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 Argentina in 4Q14 was Win32/Dorkbot, which was encountered by 1.4 percent of reporting computers there. 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 third most common malware family encountered in Argentina in 4Q14 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 Argentina in 4Q14 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.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Argentina in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	4.1%
2	Win32/Costmin	Adware	1.1%
3	Win32/BetterSurf	Adware	0.9%
4	Win32/Defaulttab	Browser Modifiers	0.6%
5	Win32/Pennybee	Adware	0.5%

- The most common unwanted software family encountered in Argentina in 4Q14 was Win32/Couponruc, which was encountered by 4.1 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 Argentina in 4Q14 was Win32/Costmin, which was encountered by 1.1 percent of reporting computers there. Win32/Costmin is an adware family that installs itself as a browser extension for Internet Explorer, Mozilla Firefox, and Google Chrome, and displays advertisements as the user browses the Internet.

- The third most common unwanted software family encountered in Argentina in 4Q14 was Win32/BetterSurf, which was encountered by 0.9 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.

Top threat families by infection rate

The most common malware families by infection rate in Argentina in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	3.3
2	Win32/Wysotot	Trojans	1.2
3	Win32/Sality	Viruses	0.9
4	Win32/Dorkbot	Worms	0.8
5	Win32/Sefnit	Trojans	0.7
6	Win32/Brontok	Worms	0.5
7	Win32/Lethic	Trojans	0.4
8	MSIL/Spacekito	Trojans	0.4
9	Win32/Ramnit	Trojans	0.3
10	Win32/Necurs	Trojans	0.3

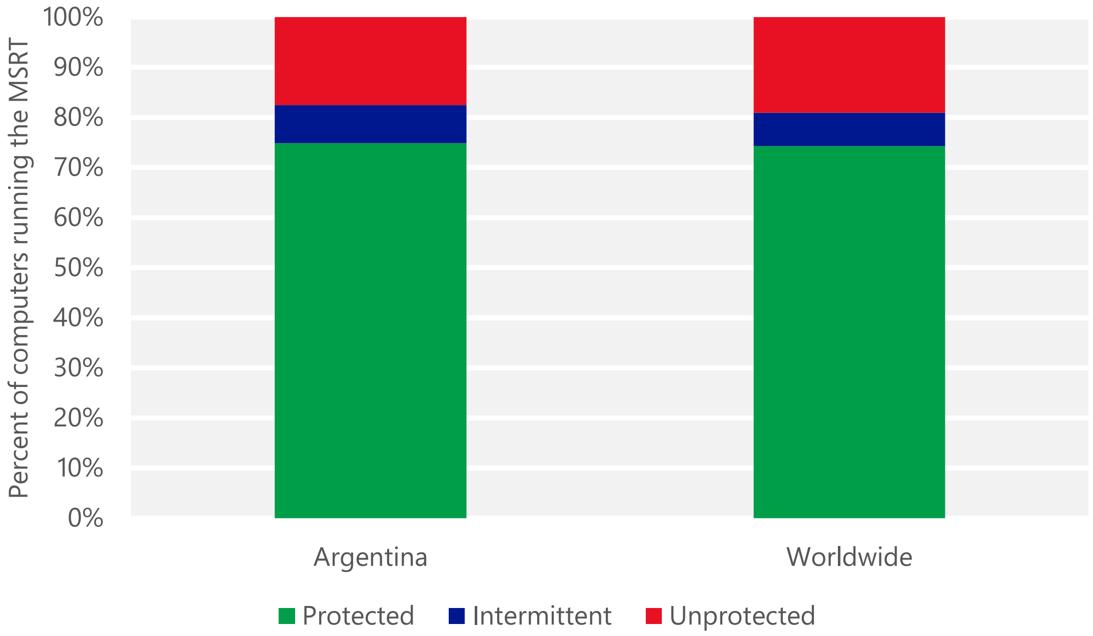
- The most common threat family infecting computers in Argentina in 4Q14 was VBS/Jenxcus, which was detected and removed from 3.3 of every 1,000 unique computers scanned by the MSRT. VBS/Jenxcus is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Argentina in 4Q14 was Win32/Wysotot, which was detected and removed from 1.2 of every 1,000 unique computers scanned by the MSRT. Win32/Wysotot is a threat that can change the start page of the user's web browser, and may download and install other files to the computer. It is installed by software bundlers that advertise free software or games.
- The third most common threat family infecting computers in Argentina in 4Q14 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 Argentina in 4Q14 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 Argentina and worldwide protected by real-time security software in 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.23 drive-by download URLs for every 1,000 URLs hosted in Argentina, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.14 drive-by download URLs for every 1,000 URLs hosted in Argentina, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Argentina and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Argentina	0.23	0.14
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Australia

The statistics presented here are generated by Microsoft security programs and services running on computers in Australia in 4Q14 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 succeds 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

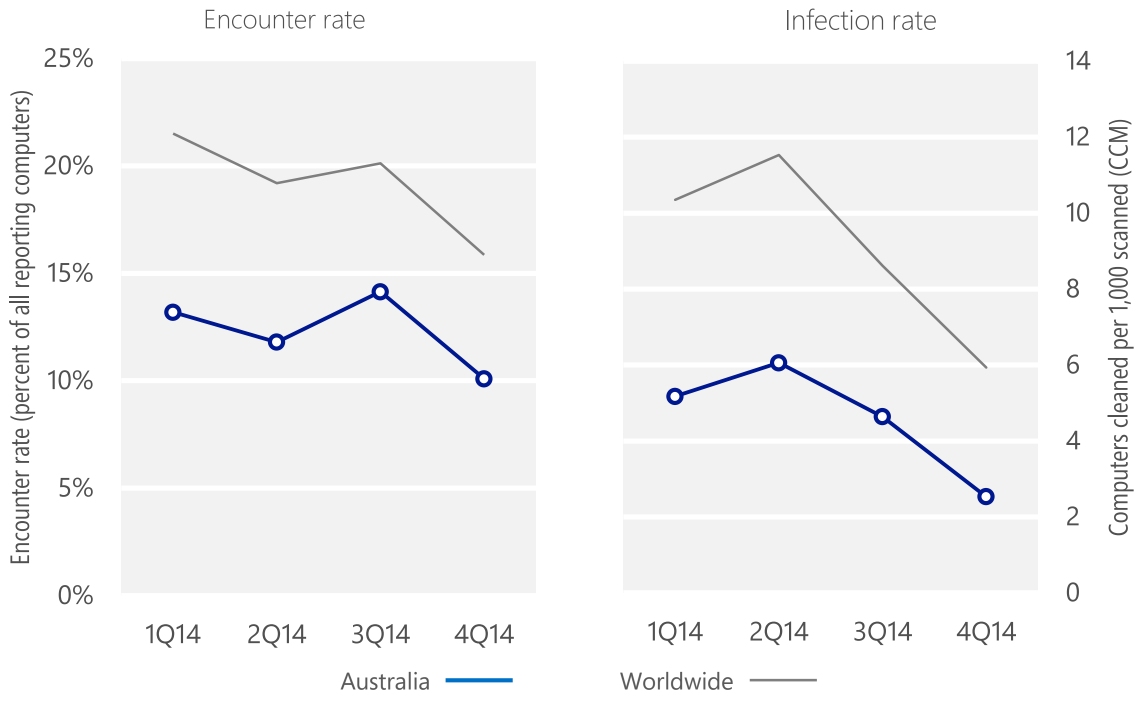
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Australia	13.2%	11.8%	14.1%	10.1%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Australia	5.2	6.1	4.6	2.5
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 10.1% percent of computers in Australia encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 2.5 of every 1,000 unique computers scanned in Australia in 4Q14 (a CCM score of 2.5, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Australia over the last four quarters, compared to the world as a whole.

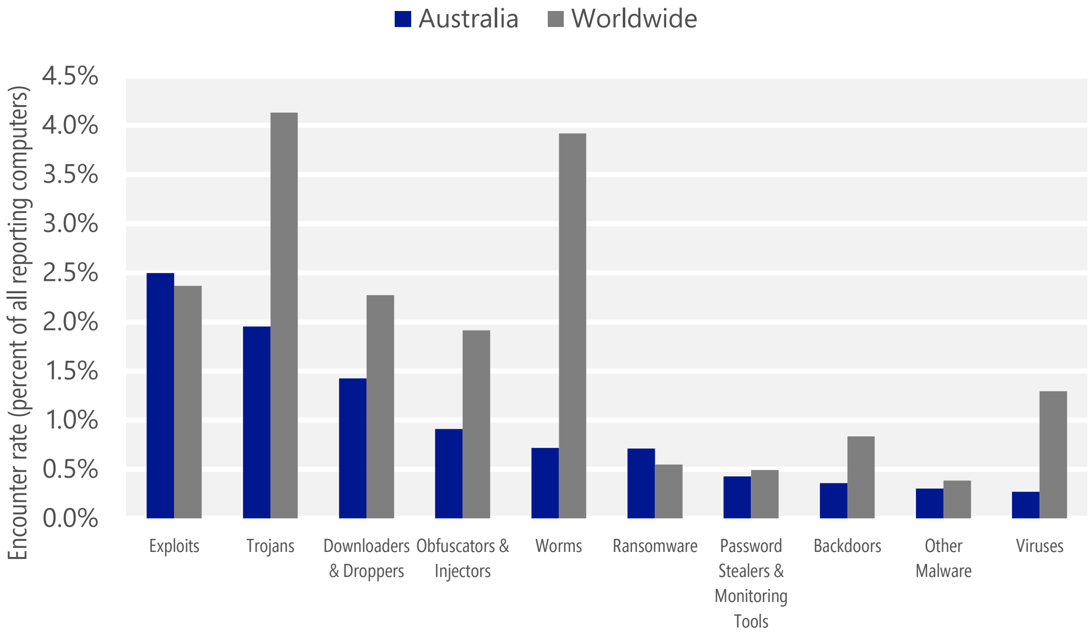
Malware encounter and infection rate trends in Australia and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

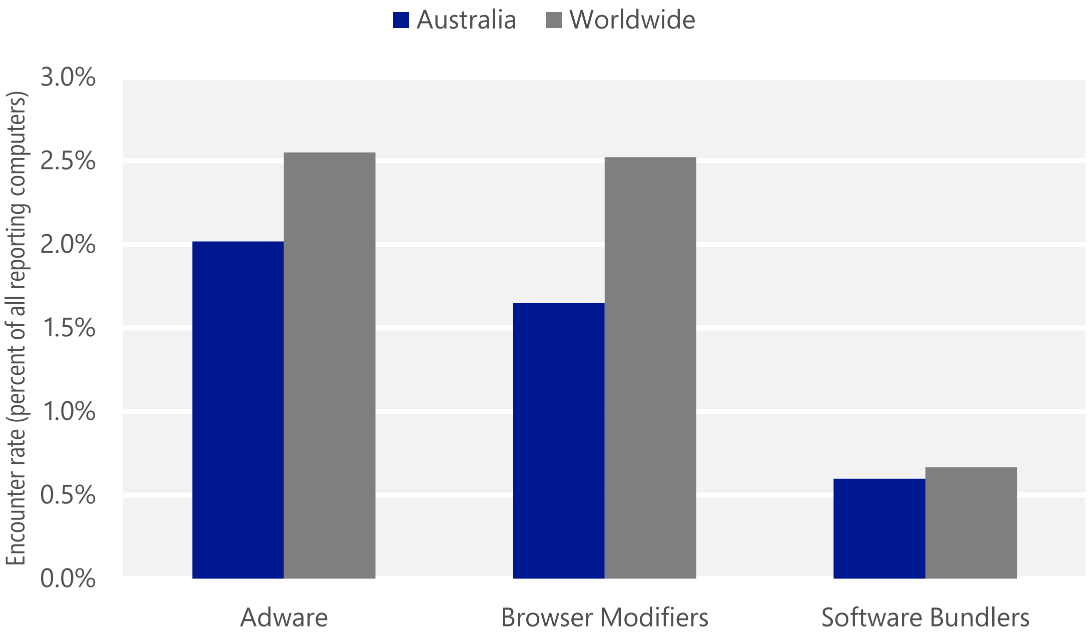
Malware encountered in Australia in 4Q14, by category



- The most common malware category in Australia in 4Q14 was Exploits. It was encountered by 2.5 percent of all computers there, down from 3.7 percent in 3Q14.
- The second most common malware category in Australia in 4Q14 was Trojans. It was encountered by 2.0 percent of all computers there, down from 3.6 percent in 3Q14.
- The third most common malware category in Australia in 4Q14 was Downloaders & Droppers, which was encountered by 1.4 percent of all computers there, down from 2.8 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Australia in 4Q14, by category



- The most common unwanted software category in Australia in 4Q14 was Adware. It was encountered by 2.0 percent of all computers there, down from 5.1 percent in 3Q14.
- The second most common unwanted software category in Australia in 4Q14 was Browser Modifiers. It was encountered by 1.6 percent of all computers there, up from 1.4 percent in 3Q14.
- The third most common unwanted software category in Australia in 4Q14 was Software Bundlers, which was encountered by 0.6 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Australia in 4Q14

	Family	Most significant category	% of reporting computers
1	JS/Axpergle	Exploits	1.3%
2	Win32/Obfuscator	Obfuscators & Injectors	0.7%
3	JS/Fiexp	Exploits	0.7%
4	JS/Krypterade	Ransomware	0.4%
5	Win32/Tugspay	Downloaders & Droppers	0.3%
6	INF/Autorun	Obfuscators & Injectors	0.3%
7	ASX/Wimad	Downloaders & Droppers	0.3%
8	Win32/Zbot	Password Stealers & Monitoring Tools	0.2%
9	Win32/Dynamer	Trojans	0.2%
10	Win32/Clikug	Trojans	0.2%

- The most common malware family encountered in Australia in 4Q14 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 second most common malware family encountered in Australia in 4Q14 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 third most common malware family encountered in Australia in 4Q14 was JS/Fiexp, which was encountered by 0.7 percent of reporting computers there. JS/Fiexp is a detection for the Fiesta exploit kit, which attempts to exploit Java, Adobe Flash Player, Adobe Reader, Silverlight, and Internet Explorer to install malware.
- The fourth most common malware family encountered in Australia in 4Q14 was JS/Krypterade, which was encountered by 0.4 percent of reporting computers there. JS/Krypterade is ransomware that fraudulently claims the computer has been used for unlawful activity, locks it, and demands that the user pay to unlock it.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Australia in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	1.4%
2	Win32/Costmin	Adware	0.8%
3	Win32/BetterSurf	Adware	0.3%
4	Win32/Gofileexpress	Software Bundlers	0.3%
5	Win32/Defaulttab	Browser Modifiers	0.3%

- The most common unwanted software family encountered in Australia in 4Q14 was Win32/Couponruc, which was encountered by 1.4 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 Australia in 4Q14 was Win32/Costmin, which was encountered by 0.8 percent of reporting computers there. Win32/Costmin is an adware family that installs itself as a browser extension for Internet Explorer, Mozilla Firefox, and Google Chrome, and displays advertisements as the user browses the Internet.
- The third most common unwanted software family encountered in Australia in 4Q14 was Win32/BetterSurf, which was encountered by 0.3 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.

Top threat families by infection rate

The most common malware families by infection rate in Australia in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Zbot	Password Stealers & Monitoring Tools	0.3
2	JS/Medfos	Trojans	0.3
3	Win32/Wysotot	Trojans	0.2
4	Win32/Alureon	Trojans	0.2
5	JS/Miuref	Trojans	0.2
6	Win32/Sirefef	Trojans	0.1
7	VBS/Jenxcus	Worms	0.1
8	Win32/Sefnit	Trojans	0.1
9	Win32/Sinowal	Password Stealers & Monitoring Tools	0.1
10	Win32/Brontok	Worms	0.1

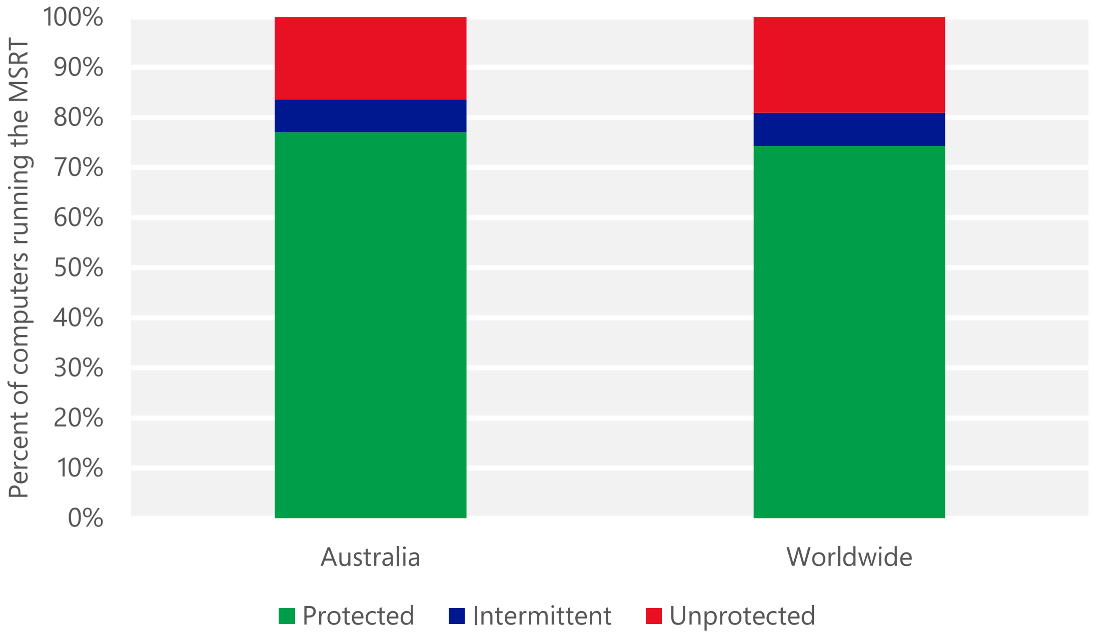
- The most common threat family infecting computers in Australia in 4Q14 was Win32/Zbot, which was detected and removed from 0.3 of every 1,000 unique computers scanned by the MSRT. Win32/Zbot is a family of password stealing trojans that also contains backdoor functionality allowing unauthorized access and control of an affected computer.
- The second most common threat family infecting computers in Australia in 4Q14 was JS/Medfos, which was detected and removed from 0.3 of every 1,000 unique computers scanned by the MSRT. JS/Medfos is ?A trojan that installs malicious Internet browser extensions and redirects search results from popular search engines.
- The third most common threat family infecting computers in Australia in 4Q14 was Win32/Wysotot, which was detected and removed from 0.2 of every 1,000 unique computers scanned by the MSRT. Win32/Wysotot is a threat that can change the start page of the user's web browser, and may download and install other files to the computer. It is installed by software bundlers that advertise free software or games.
- The fourth most common threat family infecting computers in Australia in 4Q14 was Win32/Alureon, which was detected and removed from 0.2 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.

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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.11 drive-by download URLs for every 1,000 URLs hosted in Australia, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.15 drive-by download URLs for every 1,000 URLs hosted in Australia, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Australia and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Australia	0.11	0.15
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Austria

The statistics presented here are generated by Microsoft security programs and services running on computers in Austria in 4Q14 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 succeds 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

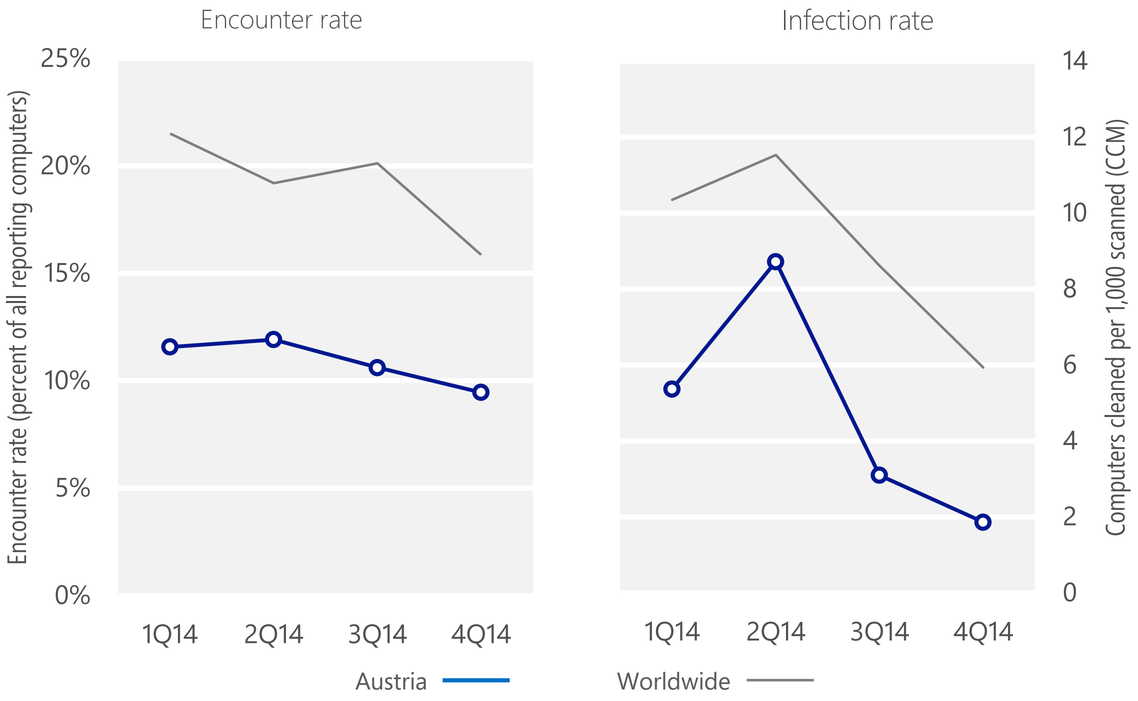
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Austria	11.6%	11.9%	10.6%	9.5%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Austria	5.4	8.7	3.1	1.9
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 9.5% percent of computers in Austria encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 1.9 of every 1,000 unique computers scanned in Austria in 4Q14 (a CCM score of 1.9, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Austria over the last four quarters, compared to the world as a whole.

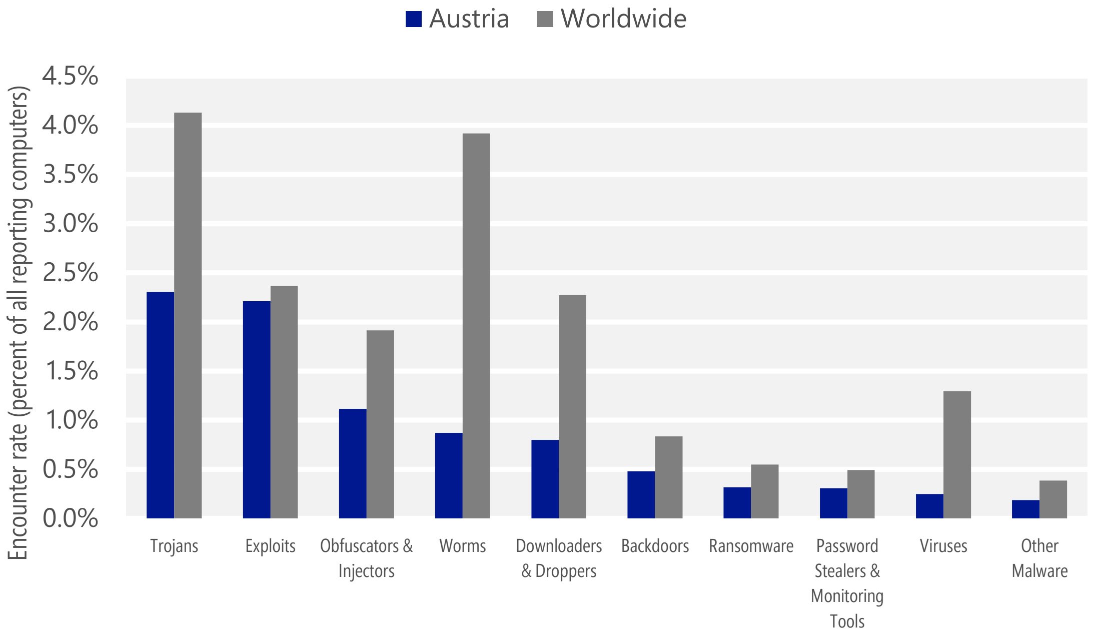
Malware encounter and infection rate trends in Austria and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

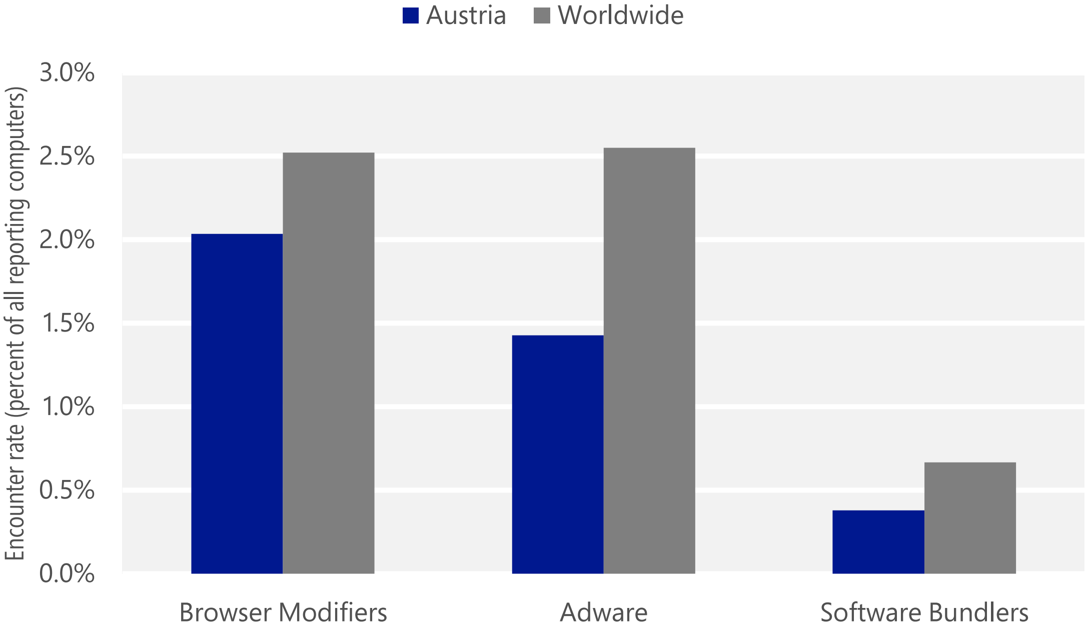
Malware encountered in Austria in 4Q14, by category



- The most common malware category in Austria in 4Q14 was Trojans. It was encountered by 2.3 percent of all computers there, down from 2.8 percent in 3Q14.
- The second most common malware category in Austria in 4Q14 was Exploits. It was encountered by 2.2 percent of all computers there, up from 2.1 percent in 3Q14.
- The third most common malware category in Austria in 4Q14 was Obfuscators & Injectors, which was encountered by 1.1 percent of all computers there, down from 1.8 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Austria in 4Q14, by category



- The most common unwanted software category in Austria in 4Q14 was Browser Modifiers. It was encountered by 2.0 percent of all computers there, down from 3.0 percent in 3Q14.
- The second most common unwanted software category in Austria in 4Q14 was Adware. It was encountered by 1.4 percent of all computers there, up from 0.5 percent in 3Q14.
- The third most common unwanted software category in Austria in 4Q14 was Software Bundlers, which was encountered by 0.4 percent of all computers there, up from 0.0 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Austria in 4Q14

	Family	Most significant category	% of reporting computers
1	JS/Axpergle	Exploits	1.5%
2	Win32/Obfuscator	Obfuscators & Injectors	0.7%
3	Win32/Emotet	Trojans	0.6%
4	Win32/CeeInject	Obfuscators & Injectors	0.3%
5	Win32/Gamarue	Worms	0.3%
6	Win32/Cetsiol	Backdoors	0.2%
7	Win32/Dynamer	Trojans	0.2%
8	INF/Autorun	Obfuscators & Injectors	0.2%
9	Win32/Anaki	Trojans	0.2%
10	Win32/Conficker	Worms	0.2%

- The most common malware family encountered in Austria in 4Q14 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 Austria in 4Q14 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 third most common malware family encountered in Austria in 4Q14 was Win32/Emotet, which was encountered by 0.6 percent of reporting computers there. 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.
- The fourth most common malware family encountered in Austria in 4Q14 was Win32/CeeInject, which was encountered by 0.3 percent of reporting computers there. Win32/CeeInject is a generic detection for malicious files that are obfuscated using particular techniques to protect them from detection or analysis.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Austria in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	1.8%
2	Win32/Costmin	Adware	0.5%
3	Win32/BetterSurf	Adware	0.4%
4	Win32/Pennybee	Adware	0.3%
5	Win32/Gofileexpress	Software Bundlers	0.2%

- The most common unwanted software family encountered in Austria in 4Q14 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 Austria in 4Q14 was Win32/Costmin, which was encountered by 0.5 percent of reporting computers there. Win32/Costmin is an adware family that installs itself as a browser extension for Internet Explorer, Mozilla Firefox, and Google Chrome, and displays advertisements as the user browses the Internet.
- The third most common unwanted software family encountered in Austria in 4Q14 was Win32/BetterSurf, which was encountered by 0.4 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.

Top threat families by infection rate

The most common malware families by infection rate in Austria in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Sefnit	Trojans	0.3
2	Win32/Wysotot	Trojans	0.1
3	Win32/Zbot	Password Stealers & Monitoring Tools	0.1
4	Win32/Alureon	Trojans	0.1
5	Win32/Sality	Viruses	0.1
6	Win32/Brontok	Worms	0.1
7	JS/Kilim	Trojans	0.1
8	VBS/Jenxcus	Worms	0.1
9	Win32/Ramnit	Trojans	0.1
10	Win32/Matsnu	Trojans	0.1

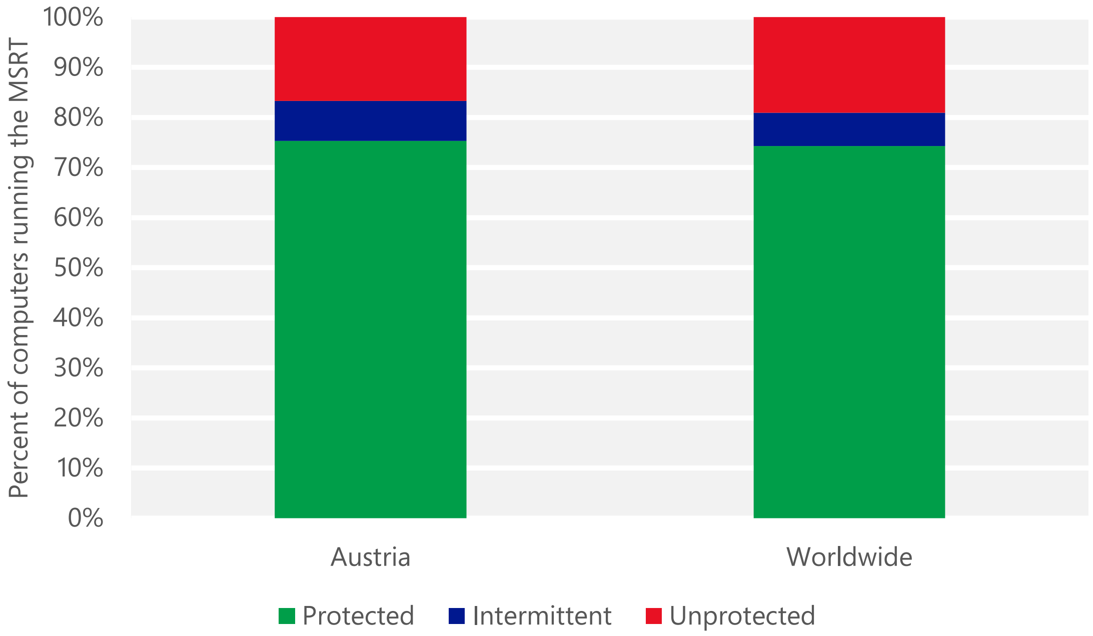
- The most common threat family infecting computers in Austria in 4Q14 was Win32/Sefnit, which was detected and removed from 0.3 of every 1,000 unique computers scanned by the MSRT. Win32/Sefnit is a family of trojans that can allow backdoor access, download files, and use the computer and Internet connection for click fraud. Some variants can monitor web browsers and hijack search results.
- The second most common threat family infecting computers in Austria in 4Q14 was Win32/Wysotot, which was detected and removed from 0.1 of every 1,000 unique computers scanned by the MSRT. Win32/Wysotot is a threat that can change the start page of the user's web browser, and may download and install other files to the computer. It is installed by software bundlers that advertise free software or games.
- The third most common threat family infecting computers in Austria in 4Q14 was Win32/Zbot, which was detected and removed from 0.1 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 fourth most common threat family infecting computers in Austria in 4Q14 was Win32/Alureon, which was detected and removed from 0.1 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.

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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.10 drive-by download URLs for every 1,000 URLs hosted in Austria, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.07 drive-by download URLs for every 1,000 URLs hosted in Austria, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Austria and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Austria	0.10	0.07
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Bahamas, The

The statistics presented here are generated by Microsoft security programs and services running on computers in the Bahamas in 4Q14 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 succeds 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

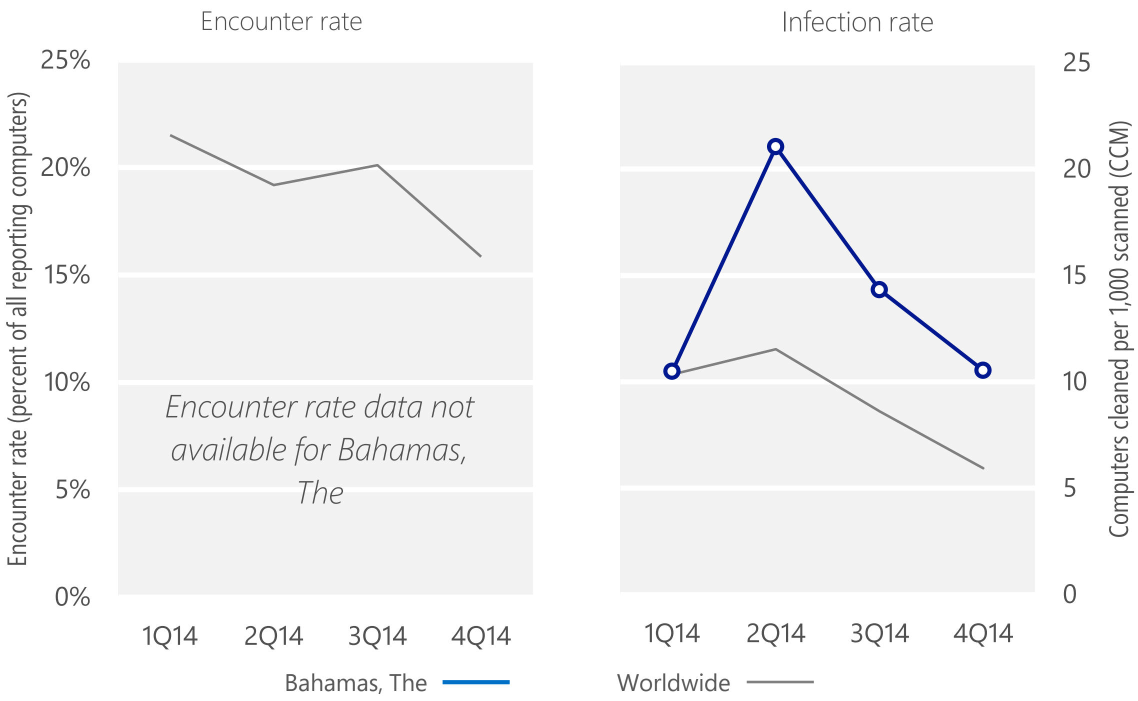
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Bahamas, The	N/A	N/A	N/A	N/A
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Bahamas, The	10.5	21.1	14.3	10.5
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, the MSRT detected and removed malware from 10.5 of every 1,000 unique computers scanned in the Bahamas in 4Q14 (a CCM score of 10.5, compared to the 4Q14 worldwide CCM of 5.9). 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 18* 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 4Q14

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	3.6
2	Win32/Brontok	Worms	1.7
3	Win32/Vobfus	Worms	1.5
4	Win32/Sality	Viruses	0.6
5	Win32/Zbot	Password Stealers & Monitoring Tools	0.4
6	Win32/Alureon	Trojans	0.3
7	Win32/Dorkbot	Worms	0.3
8	Win32/Sefnit	Trojans	0.3
9	Win32/Gamarue	Worms	0.2
10	Win32/IRCbot	Backdoors	0.2

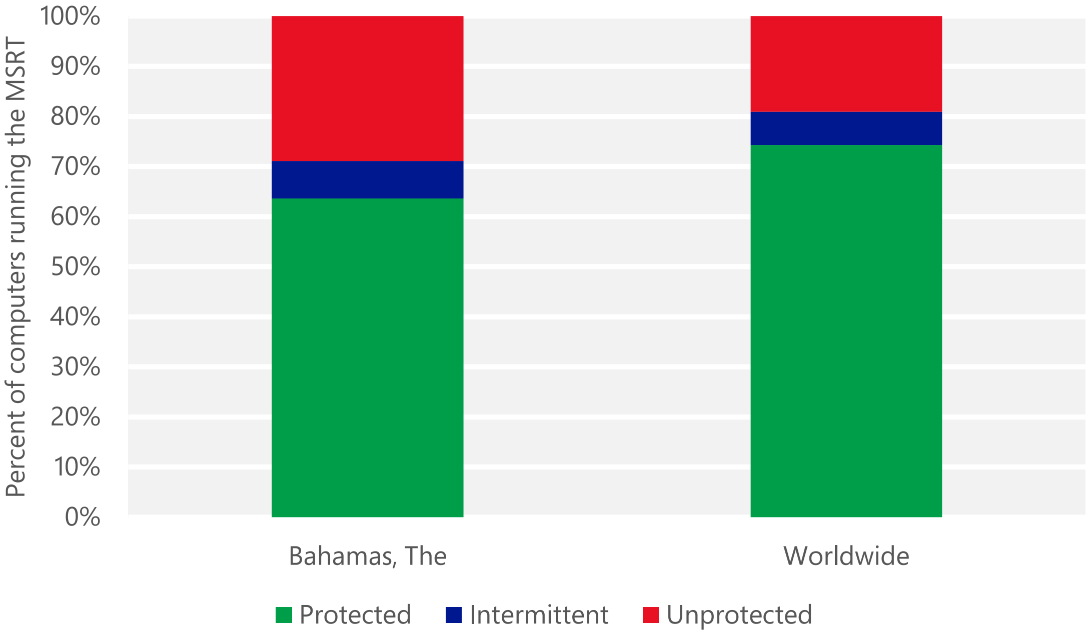
- The most common threat family infecting computers in the Bahamas in 4Q14 was VBS/Jenxcus, which was detected and removed from 3.6 of every 1,000 unique computers scanned by the MSRT. VBS/Jenxcus is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in the Bahamas in 4Q14 was Win32/Brontok, which was detected and removed from 1.7 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.
- The third most common threat family infecting computers in the Bahamas in 4Q14 was Win32/Vobfus, which was detected and removed from 1.5 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.
- The fourth most common threat family infecting computers in the Bahamas in 4Q14 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 the Bahamas and worldwide protected by real-time security software in 4Q14



Bahrain

The statistics presented here are generated by Microsoft security programs and services running on computers in Bahrain in 4Q14 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 succeds 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

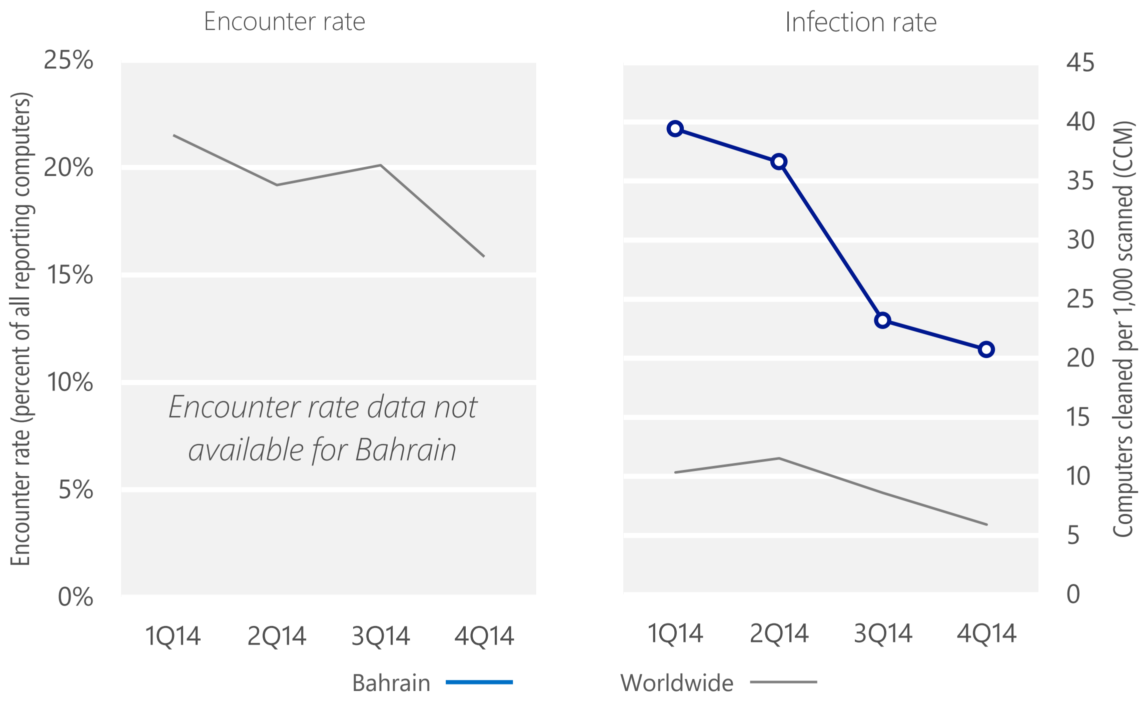
Metric	**1Q14**	**2Q14**	**3Q14**	**4Q14**
Encounter rate, Bahrain	N/A	N/A	N/A	N/A
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Bahrain	39.4	36.6	23.2	20.7
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, the MSRT detected and removed malware from 20.7 of every 1,000 unique computers scanned in Bahrain in 4Q14 (a CCM score of 20.7, compared to the 4Q14 worldwide CCM of 5.9). 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 18* 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.

Top threat families by infection rate

The most common malware families by infection rate in Bahrain in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	8.6
2	Win32/Sality	Viruses	2.4
3	Win32/Nuqel	Worms	2.4
4	MSIL/Bladabindi	Backdoors	1.6
5	Win32/Dorkbot	Worms	1.2
6	Win32/Gamarue	Worms	1.2
7	Win32/Ramnit	Trojans	1.0
8	Win32/Vobfus	Worms	0.4
9	Win32/Brontok	Worms	0.4
10	Win32/Zbot	Password Stealers & Monitoring Tools	0.4

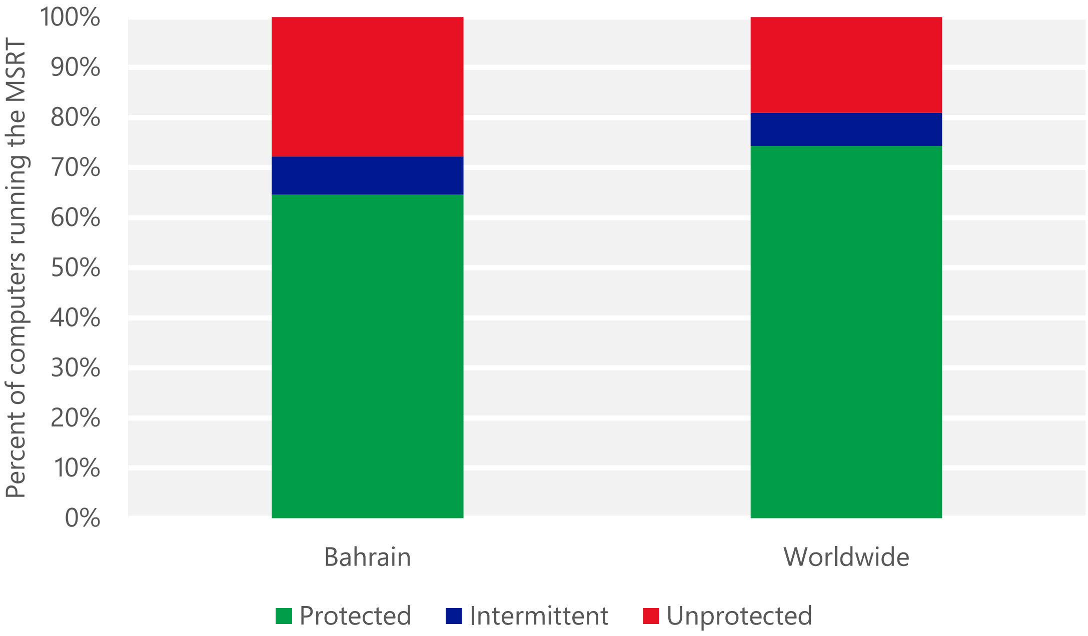
- The most common threat family infecting computers in Bahrain in 4Q14 was VBS/Jenxcus, which was detected and removed from 8.6 of every 1,000 unique computers scanned by the MSRT. VBS/Jenxcus is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Bahrain in 4Q14 was Win32/Sality, which was detected and removed from 2.4 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 Bahrain in 4Q14 was Win32/Nuqel, which was detected and removed from 2.4 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 Bahrain in 4Q14 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.

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 4Q14



Bangladesh

The statistics presented here are generated by Microsoft security programs and services running on computers in Bangladesh in 4Q14 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 succeds 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

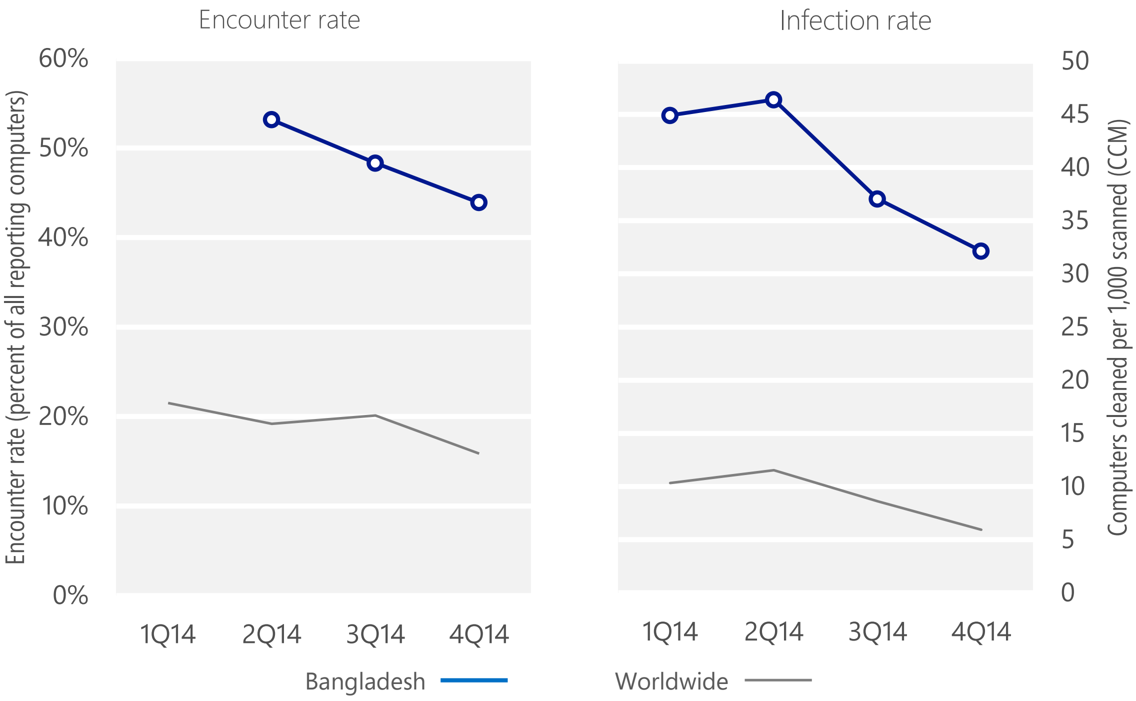
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Bangladesh	N/A	53.2%	48.3%	43.9%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Bangladesh	44.9	46.4	37.1	32.1
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 43.9% percent of computers in Bangladesh encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 32.1 of every 1,000 unique computers scanned in Bangladesh in 4Q14 (a CCM score of 32.1, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Bangladesh over the last four quarters, compared to the world as a whole.

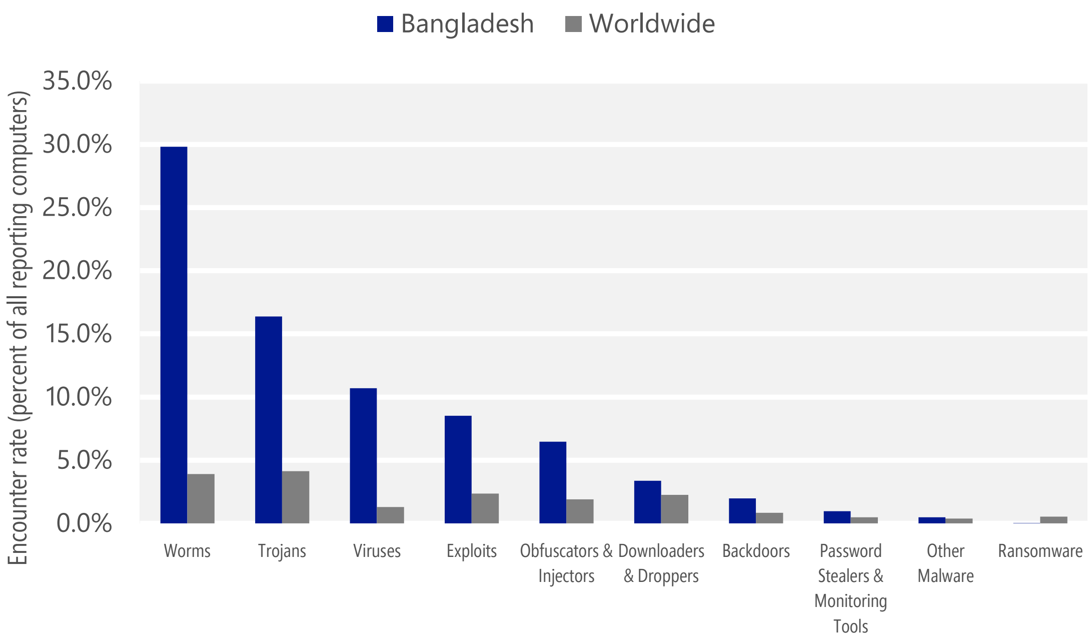
Malware encounter and infection rate trends in Bangladesh and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

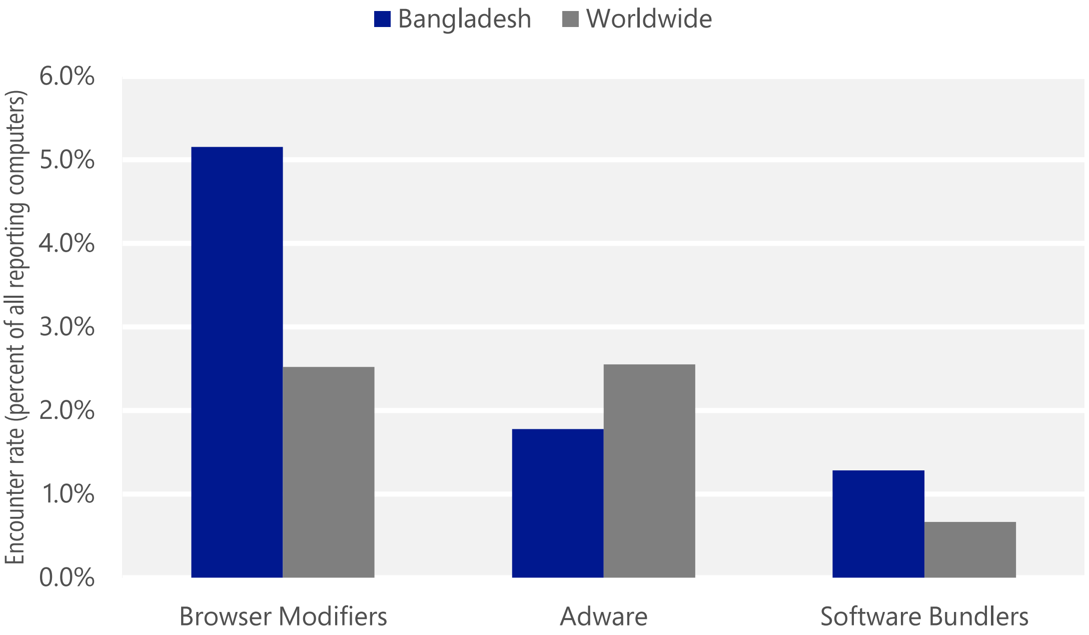
Malware encountered in Bangladesh in 4Q14, by category



- The most common malware category in Bangladesh in 4Q14 was Worms. It was encountered by 29.8 percent of all computers there, down from 33.5 percent in 3Q14.
- The second most common malware category in Bangladesh in 4Q14 was Trojans. It was encountered by 16.4 percent of all computers there, down from 18.8 percent in 3Q14.
- The third most common malware category in Bangladesh in 4Q14 was Viruses, which was encountered by 10.7 percent of all computers there, down from 11.5 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Bangladesh in 4Q14, by category



- The most common unwanted software category in Bangladesh in 4Q14 was Browser Modifiers. It was encountered by 5.2 percent of all computers there, up from 4.1 percent in 3Q14.
- The second most common unwanted software category in Bangladesh in 4Q14 was Adware. It was encountered by 1.8 percent of all computers there, up from 0.8 percent in 3Q14.
- The third most common unwanted software category in Bangladesh in 4Q14 was Software Bundlers, which was encountered by 1.3 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Bangladesh in 4Q14

	Family	Most significant category	% of reporting computers
1	INF/Autorun	Obfuscators & Injectors	17.4%
2	Win32/Ippedo	Worms	13.9%
3	VBS/Jenxcus	Worms	10.9%
4	Win32/Ramnit	Trojans	9.5%
5	Win32/Gamarue	Worms	8.7%
6	Win32/CplLnk	Exploits	7.9%
7	Win32/Sality	Viruses	5.0%
8	Win32/Virut	Viruses	3.1%
9	Win32/Vercuser	Worms	3.1%
10	Win32/Obfuscator	Obfuscators & Injectors	1.9%

- The most common malware family encountered in Bangladesh in 4Q14 was INF/Autorun, which was encountered by 17.4 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 second most common malware family encountered in Bangladesh in 4Q14 was Win32/Ippedo, which was encountered by 13.9 percent of reporting computers there. Win32/Ippedo is a worm that can send sensitive information to a malicious hacker. It spreads through infected removable drives, such as USB flash drives.
- The third most common malware family encountered in Bangladesh in 4Q14 was VBS/Jenxcus, which was encountered by 10.9 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 fourth most common malware family encountered in Bangladesh in 4Q14 was Win32/Ramnit, which was encountered by 9.5 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.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Bangladesh in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	4.3%
2	Win32/Gofileexpress	Software Bundlers	1.0%
3	Win32/Defaulttab	Browser Modifiers	0.9%
4	Win32/Costmin	Adware	0.8%
5	Win32/BetterSurf	Adware	0.7%

- The most common unwanted software family encountered in Bangladesh in 4Q14 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 second most common unwanted software family encountered in Bangladesh in 4Q14 was Win32/Gofileexpress, which was encountered by 1.0 percent of reporting computers there. Win32/Gofileexpress is a software bundler that installs other unwanted software, including Adware:Win32/Lollipop and Adware:Win32/CostMin.
- The third most common unwanted software family encountered in Bangladesh in 4Q14 was Win32/Defaulttab, which was encountered by 0.9 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.

Top threat families by infection rate

The most common malware families by infection rate in Bangladesh in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	10.5
2	Win32/Ramnit	Trojans	8.4
3	Win32/Sality	Viruses	7.7
4	Win32/Gamarue	Worms	5.8
5	Win32/Pramro	Trojans	0.7
6	Win32/Chir	Viruses	0.7
7	MSIL/Bladabindi	Backdoors	0.5
8	Win32/Parite	Viruses	0.4
9	Win32/Brontok	Worms	0.4
10	Win32/Nuqel	Worms	0.3

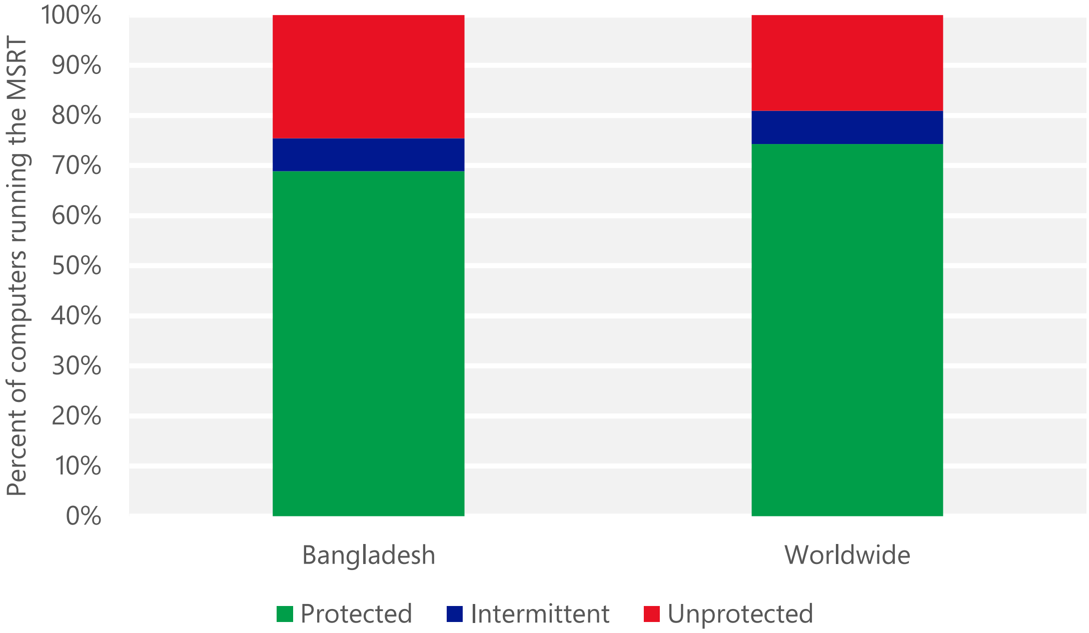
- The most common threat family infecting computers in Bangladesh in 4Q14 was VBS/Jenxcus, which was detected and removed from 10.5 of every 1,000 unique computers scanned by the MSRT. VBS/Jenxcus is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Bangladesh in 4Q14 was Win32/Ramnit, which was detected and removed from 8.4 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 Bangladesh in 4Q14 was Win32/Sality, which was detected and removed from 7.7 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 Bangladesh in 4Q14 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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.51 drive-by download URLs for every 1,000 URLs hosted in Bangladesh, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 3.93 drive-by download URLs for every 1,000 URLs hosted in Bangladesh, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Bangladesh and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Bangladesh	0.51	3.93
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Belarus

The statistics presented here are generated by Microsoft security programs and services running on computers in Belarus in 4Q14 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 succeds 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

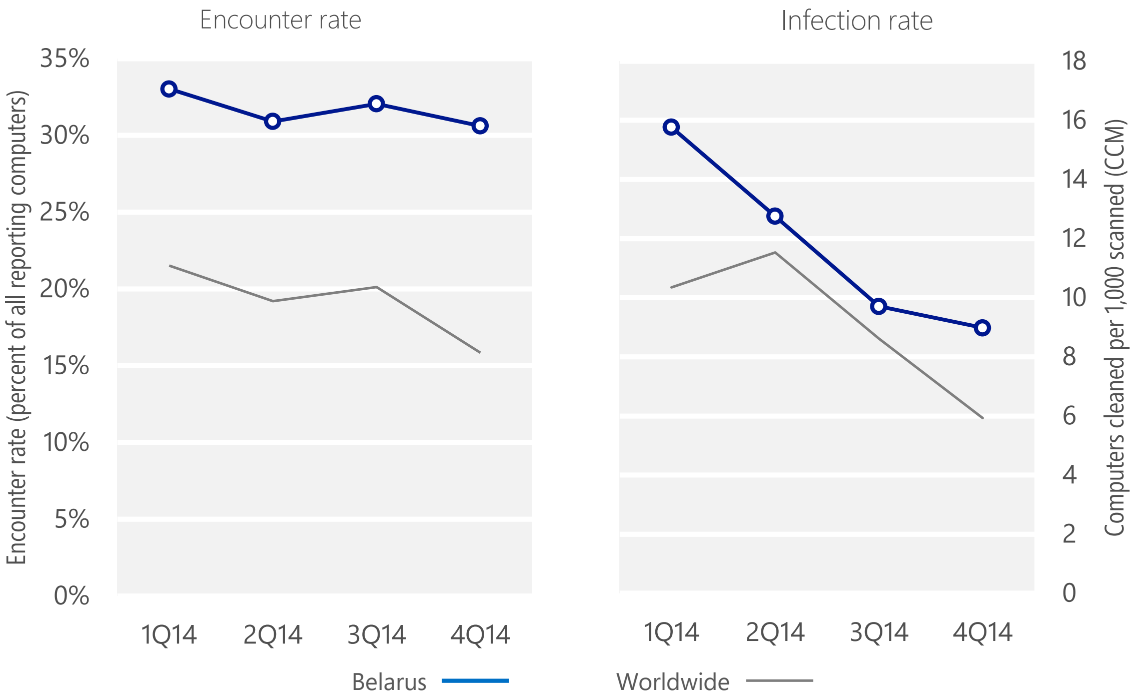
Metric	**1Q14**	**2Q14**	**3Q14**	**4Q14**
Encounter rate, Belarus	33.0%	30.9%	32.1%	30.6%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Belarus	15.8	12.8	9.7	9.0
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 30.6% percent of computers in Belarus encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 9.0 of every 1,000 unique computers scanned in Belarus in 4Q14 (a CCM score of 9.0, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Belarus over the last four quarters, compared to the world as a whole.

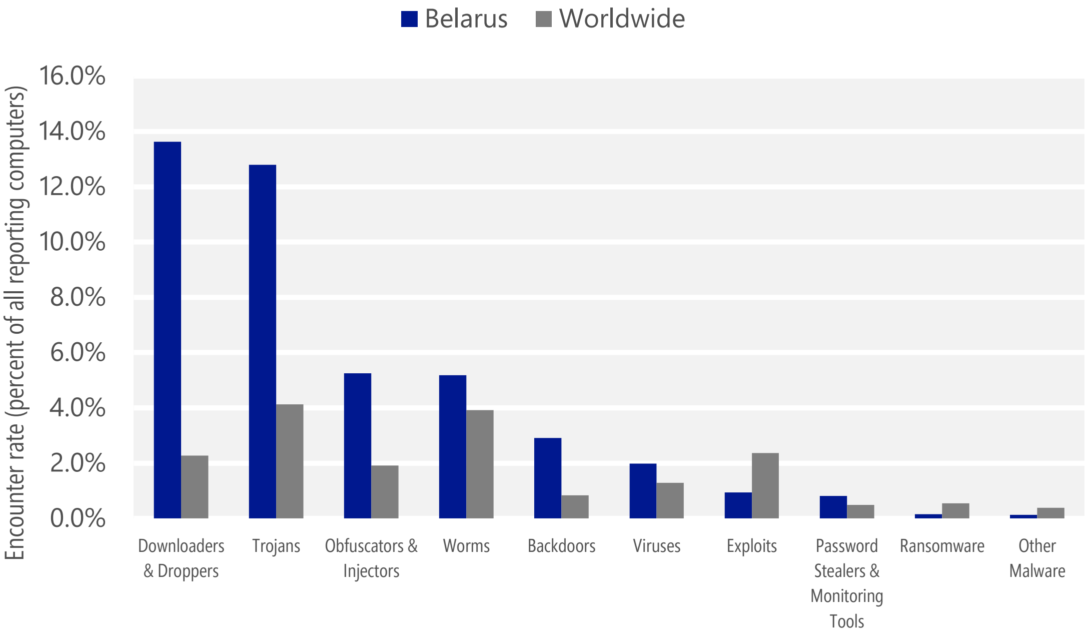
Malware encounter and infection rate trends in Belarus and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

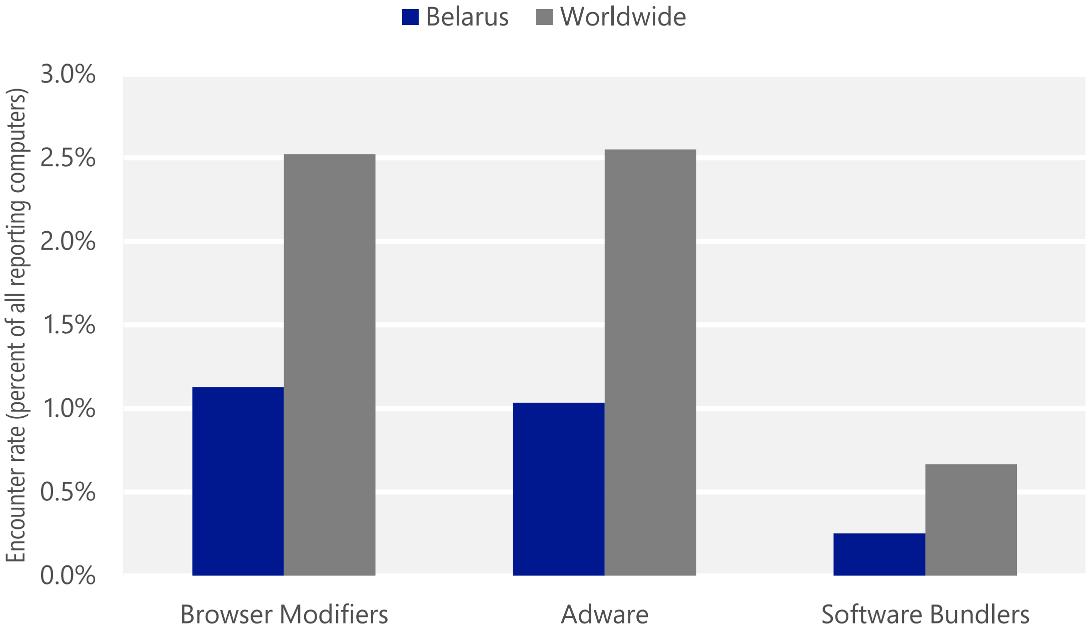
Malware encountered in Belarus in 4Q14, by category



- The most common malware category in Belarus in 4Q14 was Downloaders & Droppers. It was encountered by 13.6 percent of all computers there, down from 17.2 percent in 3Q14.
- The second most common malware category in Belarus in 4Q14 was Trojans. It was encountered by 12.8 percent of all computers there, up from 11.3 percent in 3Q14.
- The third most common malware category in Belarus in 4Q14 was Obfuscators & Injectors, which was encountered by 5.3 percent of all computers there, down from 5.3 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Belarus in 4Q14, by category



- The most common unwanted software category in Belarus in 4Q14 was Browser Modifiers. It was encountered by 1.1 percent of all computers there, down from 2.1 percent in 3Q14.
- The second most common unwanted software category in Belarus in 4Q14 was Adware. It was encountered by 1.0 percent of all computers there, up from 0.1 percent in 3Q14.
- The third most common unwanted software category in Belarus in 4Q14 was Software Bundlers, which was encountered by 0.3 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Belarus in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Ogimant	Downloaders & Droppers	12.1%
2	Win32/Peaac	Trojans	4.5%
3	Win32/Obfuscator	Obfuscators & Injectors	4.5%
4	Win32/Gamarue	Worms	2.2%
5	Win32/Peals	Trojans	1.5%
6	Win32/Dynamer	Trojans	1.3%
7	Win32/Morix	Backdoors	0.9%
8	INF/Autorun	Obfuscators & Injectors	0.9%
9	Win32/Tofsee	Backdoors	0.8%
10	Win32/Dorkbot	Worms	0.7%

- The most common malware family encountered in Belarus in 4Q14 was Win32/Ogimant, which was encountered by 12.1 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 second most common malware family encountered in Belarus in 4Q14 was Win32/Peaac, which was encountered by 4.5 percent of reporting computers there. Win32/Peaac is a generic detection for various threats that display trojan characteristics.
- The third most common malware family encountered in Belarus in 4Q14 was Win32/Obfuscator, which was encountered by 4.5 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 fourth most common malware family encountered in Belarus in 4Q14 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.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Belarus in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	0.7%
2	Win32/BetterSurf	Adware	0.7%
3	Win32/Defaulttab	Browser Modifiers	0.4%

- The most common unwanted software family encountered in Belarus in 4Q14 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.
- The second most common unwanted software family encountered in Belarus in 4Q14 was Win32/BetterSurf, which was encountered by 0.7 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.
- The third most common unwanted software family encountered in Belarus in 4Q14 was Win32/Defaulttab, which was encountered by 0.4 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.

Top threat families by infection rate

The most common malware families by infection rate in Belarus in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Gamarue	Worms	2.4
2	Win32/Tofsee	Backdoors	1.5
3	Win32/Ramnit	Trojans	1.0
4	Win32/Deminnix	Trojans	0.8
5	Win32/Dorkbot	Worms	0.7
6	Win32/Sality	Viruses	0.6
7	Win32/Lethic	Trojans	0.3
8	VBS/Jenxcus	Worms	0.3
9	Win32/Sefnit	Trojans	0.3
10	Win32/Nuqel	Worms	0.2

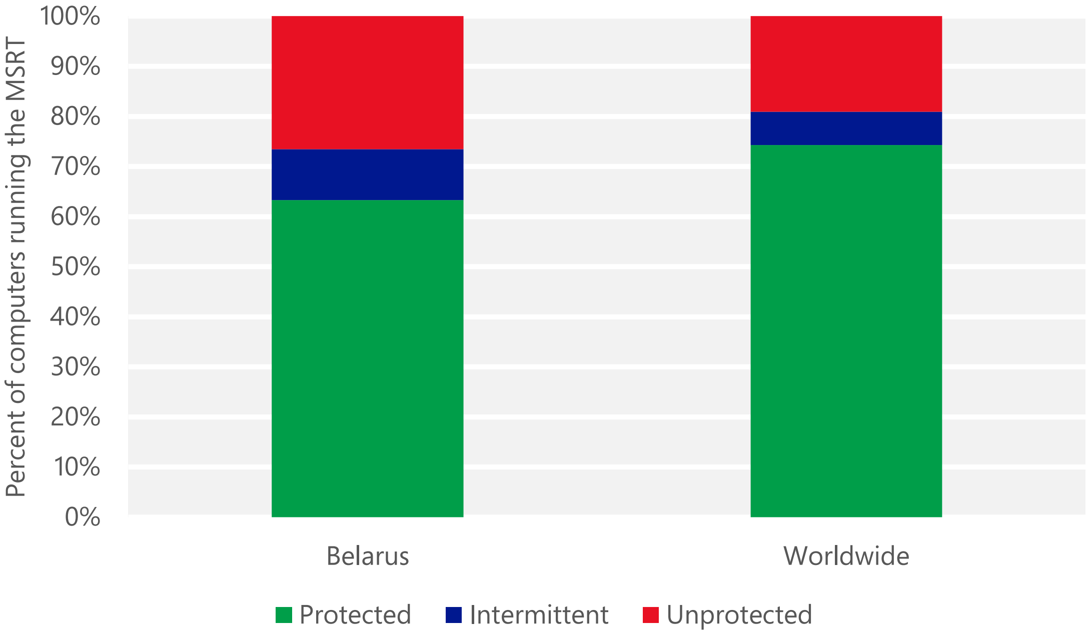
- The most common threat family infecting computers in Belarus in 4Q14 was Win32/Gamarue, which was detected and removed from 2.4 of every 1,000 unique computers scanned by the MSRT. Win32/Gamarue is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed 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 Belarus in 4Q14 was Win32/Tofsee, which was detected and removed from 1.5 of every 1,000 unique computers scanned by the MSRT. Win32/Tofsee is a multi-component family of backdoor trojans that act as a spam and traffic relay.
- The third most common threat family infecting computers in Belarus in 4Q14 was Win32/Ramnit, which was detected and removed from 1.0 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.
- The fourth most common threat family infecting computers in Belarus in 4Q14 was Win32/Deminnix, which was detected and removed from 0.8 of every 1,000 unique computers scanned by the MSRT. Win32/Deminnix is a trojan that uses the computer for bitcoin mining and changes the home page of the web browser. It can accidentally be downloaded along with other files from torrent sites.

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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.54 drive-by download URLs for every 1,000 URLs hosted in Belarus, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 1.38 drive-by download URLs for every 1,000 URLs hosted in Belarus, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Belarus and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Belarus	0.54	1.38
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Belgium

The statistics presented here are generated by Microsoft security programs and services running on computers in Belgium in 4Q14 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 succeds 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

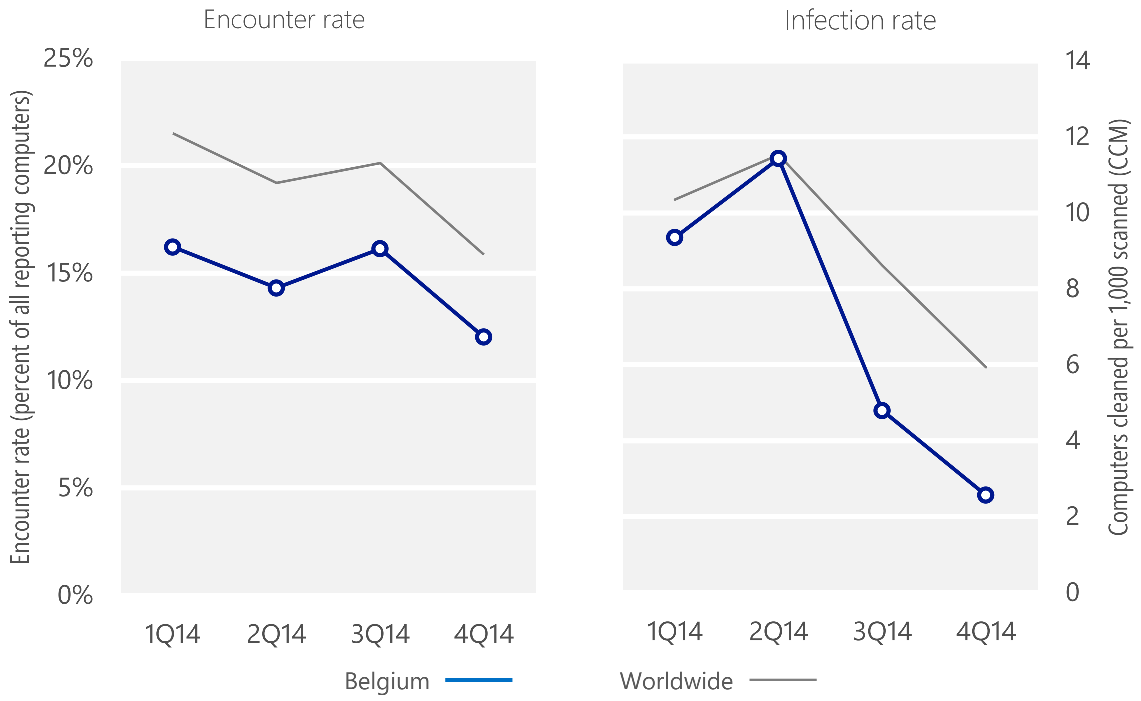
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Belgium	16.2%	14.3%	16.1%	12.0%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Belgium	9.3	11.4	4.8	2.6
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 12.0% percent of computers in Belgium encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 2.6 of every 1,000 unique computers scanned in Belgium in 4Q14 (a CCM score of 2.6, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Belgium over the last four quarters, compared to the world as a whole.

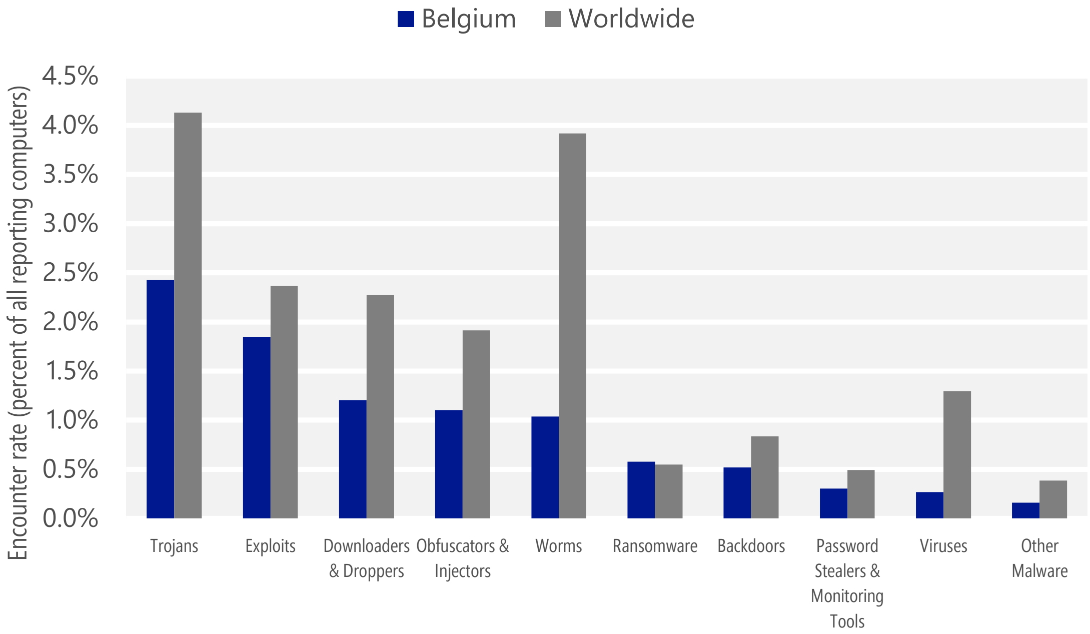
Malware encounter and infection rate trends in Belgium and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

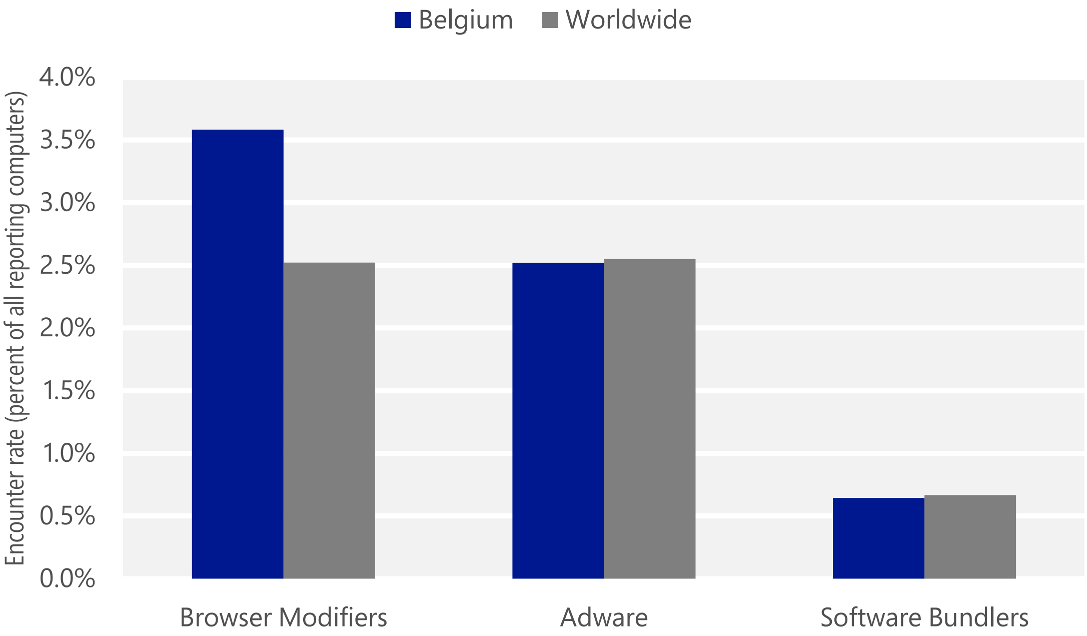
Malware encountered in Belgium in 4Q14, by category



- The most common malware category in Belgium in 4Q14 was Trojans. It was encountered by 2.4 percent of all computers there, down from 4.1 percent in 3Q14.
- The second most common malware category in Belgium in 4Q14 was Exploits. It was encountered by 1.8 percent of all computers there, down from 2.9 percent in 3Q14.
- The third most common malware category in Belgium in 4Q14 was Downloaders & Droppers, which was encountered by 1.2 percent of all computers there, down from 2.6 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Belgium in 4Q14, by category



- The most common unwanted software category in Belgium in 4Q14 was Browser Modifiers. It was encountered by 3.6 percent of all computers there, down from 6.2 percent in 3Q14.
- The second most common unwanted software category in Belgium in 4Q14 was Adware. It was encountered by 2.5 percent of all computers there, down from 2.9 percent in 3Q14.
- The third most common unwanted software category in Belgium in 4Q14 was Software Bundlers, which was encountered by 0.6 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Belgium in 4Q14

	Family	Most significant category	% of reporting computers
1	JS/Axpergle	Exploits	1.0%
2	Win32/Obfuscator	Obfuscators & Injectors	0.8%
3	ASX/Wimad	Downloaders & Droppers	0.3%
4	JS/Krypterade	Ransomware	0.3%
5	INF/Autorun	Obfuscators & Injectors	0.3%
6	JS/Redirector	Trojans	0.3%
7	VBS/Jenxcus	Worms	0.3%
8	Win32/Wysotot	Trojans	0.2%
9	JS/Faceliker	Trojans	0.2%
10	Win32/Anogre	Exploits	0.2%

- The most common malware family encountered in Belgium in 4Q14 was JS/Axpergle, which was encountered by 1.0 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 Belgium in 4Q14 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 Belgium in 4Q14 was ASX/Wimad, which was encountered by 0.3 percent of reporting computers there. ASX/Wimad is a detection for malicious Windows Media files that can be used to encourage users to download and execute arbitrary files on an affected machine.
- The fourth most common malware family encountered in Belgium in 4Q14 was JS/Krypterade, which was encountered by 0.3 percent of reporting computers there. JS/Krypterade is ransomware that fraudulently claims the computer has been used for unlawful activity, locks it, and demands that the user pay to unlock it.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Belgium in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	2.8%
2	Win32/Costmin	Adware	1.0%
3	Win32/Defaulttab	Browser Modifiers	0.9%
4	Win32/BetterSurf	Adware	0.5%
5	Win32/Gofileexpress	Software Bundlers	0.4%

- The most common unwanted software family encountered in Belgium in 4Q14 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 second most common unwanted software family encountered in Belgium in 4Q14 was Win32/Costmin, which was encountered by 1.0 percent of reporting computers there. Win32/Costmin is an adware family that installs itself as a browser extension for Internet Explorer, Mozilla Firefox, and Google Chrome, and displays advertisements as the user browses the Internet.

- The third most common unwanted software family encountered in Belgium in 4Q14 was Win32/Defaulttab, which was encountered by 0.9 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.

Top threat families by infection rate

The most common malware families by infection rate in Belgium in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	0.4
2	Win32/Wysotot	Trojans	0.3
3	Win32/Sefnit	Trojans	0.3
4	Win32/Alureon	Trojans	0.2
5	Win32/Brontok	Worms	0.1
6	Win32/Sality	Viruses	0.1
7	JS/Miuref	Trojans	0.1
8	MSIL/Bladabindi	Backdoors	0.1
9	Win32/Zbot	Password Stealers & Monitoring Tools	0.1
10	JS/Kilim	Trojans	0.1

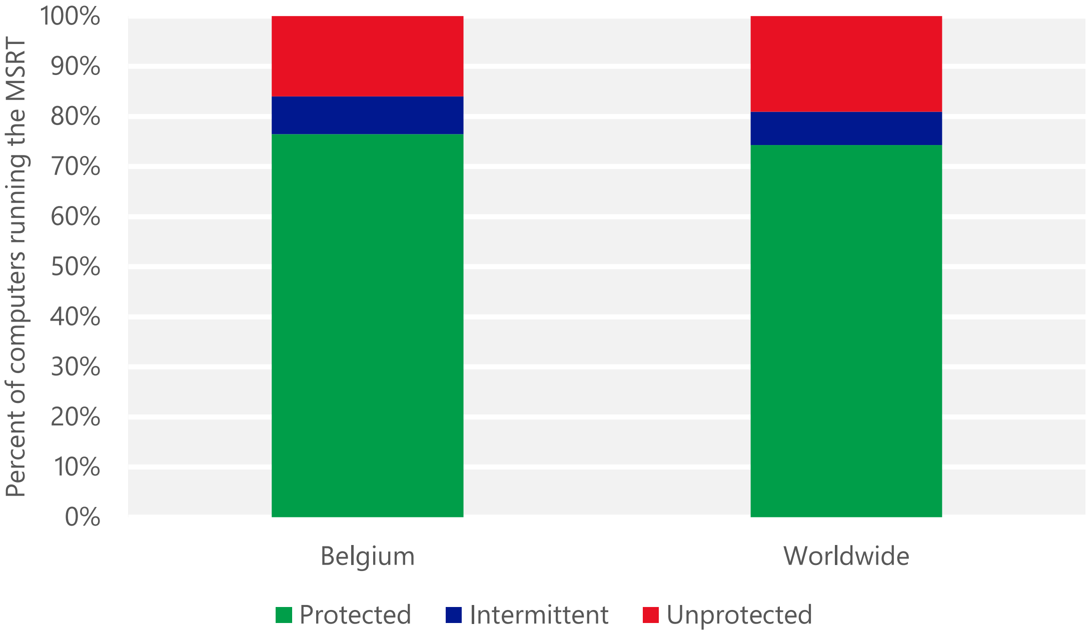
- The most common threat family infecting computers in Belgium in 4Q14 was VBS/Jenxcus, which was detected and removed from 0.4 of every 1,000 unique computers scanned by the MSRT. VBS/Jenxcus is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Belgium in 4Q14 was Win32/Wysotot, which was detected and removed from 0.3 of every 1,000 unique computers scanned by the MSRT. Win32/Wysotot is a threat that can change the start page of the user's web browser, and may download and install other files to the computer. It is installed by software bundlers that advertise free software or games.
- The third most common threat family infecting computers in Belgium in 4Q14 was Win32/Sefnit, which was detected and removed from 0.3 of every 1,000 unique computers scanned by the MSRT. Win32/Sefnit is a family of trojans that can allow backdoor access, download files, and use the computer and Internet connection for click fraud. Some variants can monitor web browsers and hijack search results.
- The fourth most common threat family infecting computers in Belgium in 4Q14 was Win32/Alureon, which was detected and removed from 0.2 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.

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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.06 drive-by download URLs for every 1,000 URLs hosted in Belgium, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.13 drive-by download URLs for every 1,000 URLs hosted in Belgium, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Belgium and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Belgium	0.06	0.13
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Bolivia

The statistics presented here are generated by Microsoft security programs and services running on computers in Bolivia in 4Q14 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 succeds 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

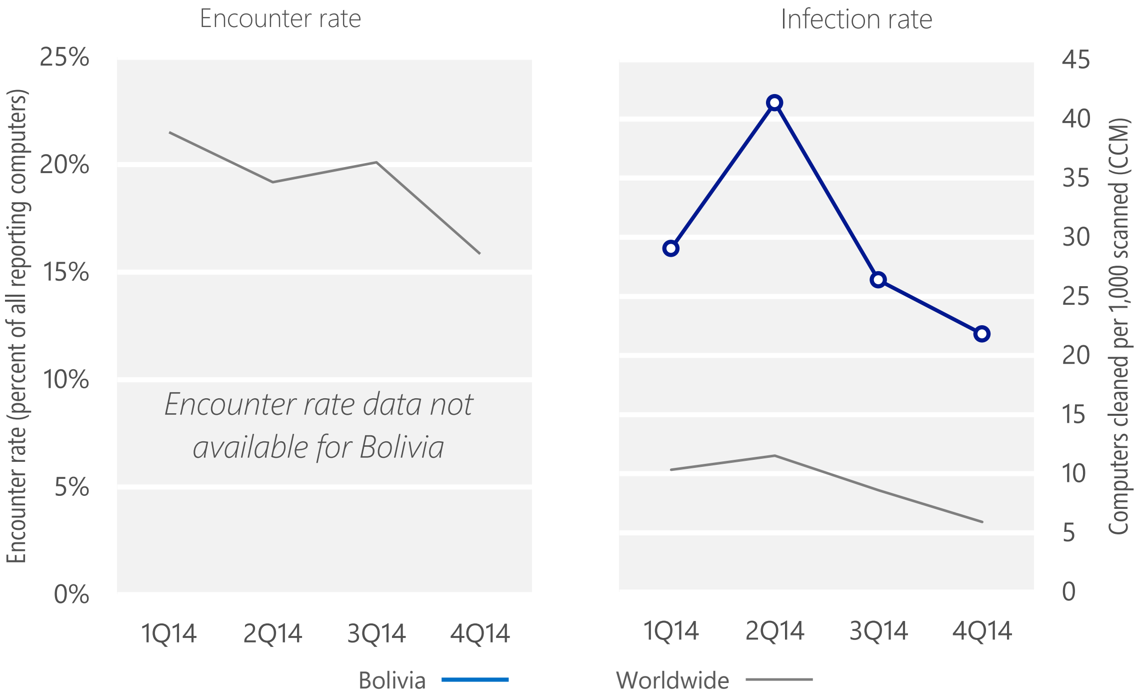
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Bolivia	N/A	N/A	N/A	N/A
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Bolivia	29.0	41.4	26.4	21.8
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, the MSRT detected and removed malware from 21.8 of every 1,000 unique computers scanned in Bolivia in 4Q14 (a CCM score of 21.8, compared to the 4Q14 worldwide CCM of 5.9). 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 18* 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.

Top threat families by infection rate

The most common malware families by infection rate in Bolivia in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	9.6
2	Win32/Gamarue	Worms	7.6
3	Win32/Sality	Viruses	2.0
4	Win32/Ramnit	Trojans	0.7
5	Win32/Vobfus	Worms	0.6
6	Win32/Dorkbot	Worms	0.4
7	MSIL/Spacekito	Trojans	0.3
8	Win32/Conficker	Worms	0.3
9	Win32/Wysotot	Trojans	0.2
10	Win32/Sefnit	Trojans	0.2

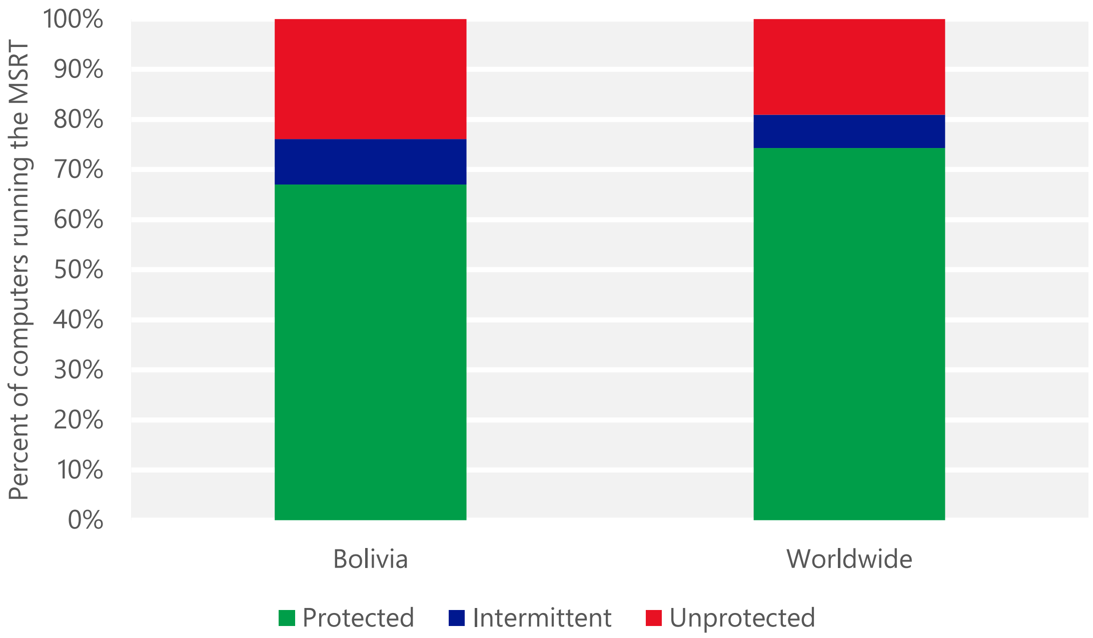
- The most common threat family infecting computers in Bolivia in 4Q14 was VBS/Jenxcus, which was detected and removed from 9.6 of every 1,000 unique computers scanned by the MSRT. VBS/Jenxcus is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Bolivia in 4Q14 was Win32/Gamarue, which was detected and removed from 7.6 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 third most common threat family infecting computers in Bolivia in 4Q14 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 Bolivia in 4Q14 was Win32/Ramnit, which was detected and removed from 0.7 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 Bolivia and worldwide protected by real-time security software in 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.00 drive-by download URLs for every 1,000 URLs hosted in Bolivia, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.57 drive-by download URLs for every 1,000 URLs hosted in Bolivia, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Bolivia and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Bolivia	0.00	0.57
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Brazil

The statistics presented here are generated by Microsoft security programs and services running on computers in Brazil in 4Q14 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 succeds 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

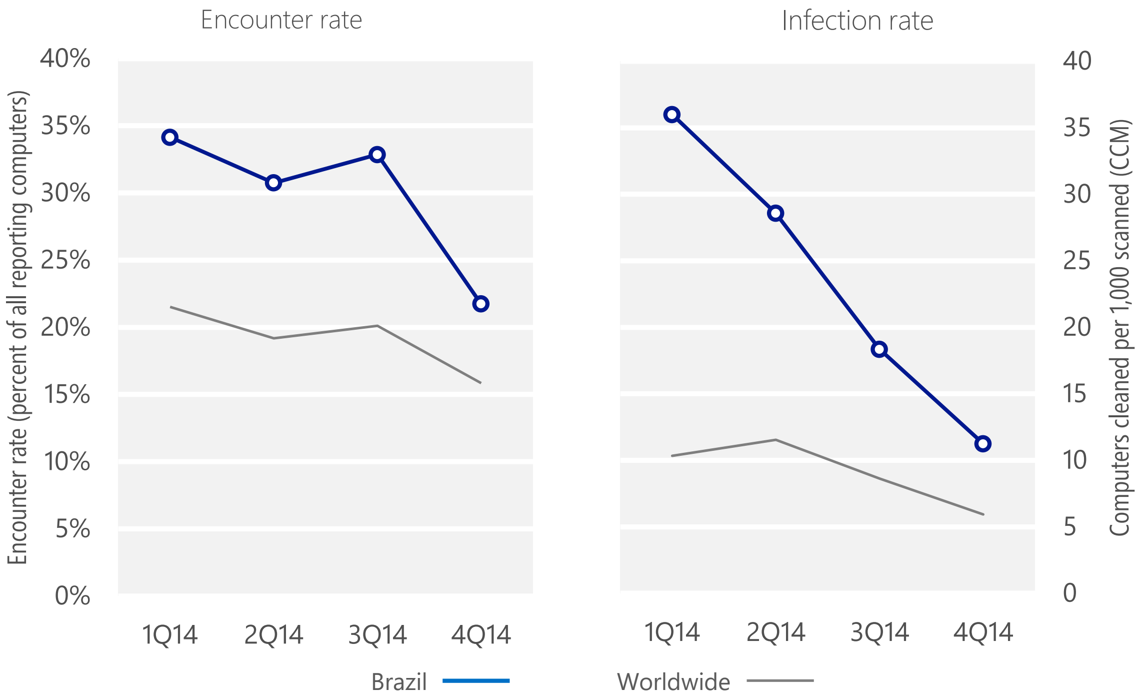
Metric	**1Q14**	**2Q14**	**3Q14**	**4Q14**
Encounter rate, Brazil	34.1%	30.8%	32.9%	21.7%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Brazil	36.0	28.6	18.4	11.2
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 21.7% percent of computers in Brazil encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 11.2 of every 1,000 unique computers scanned in Brazil in 4Q14 (a CCM score of 11.2, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Brazil over the last four quarters, compared to the world as a whole.

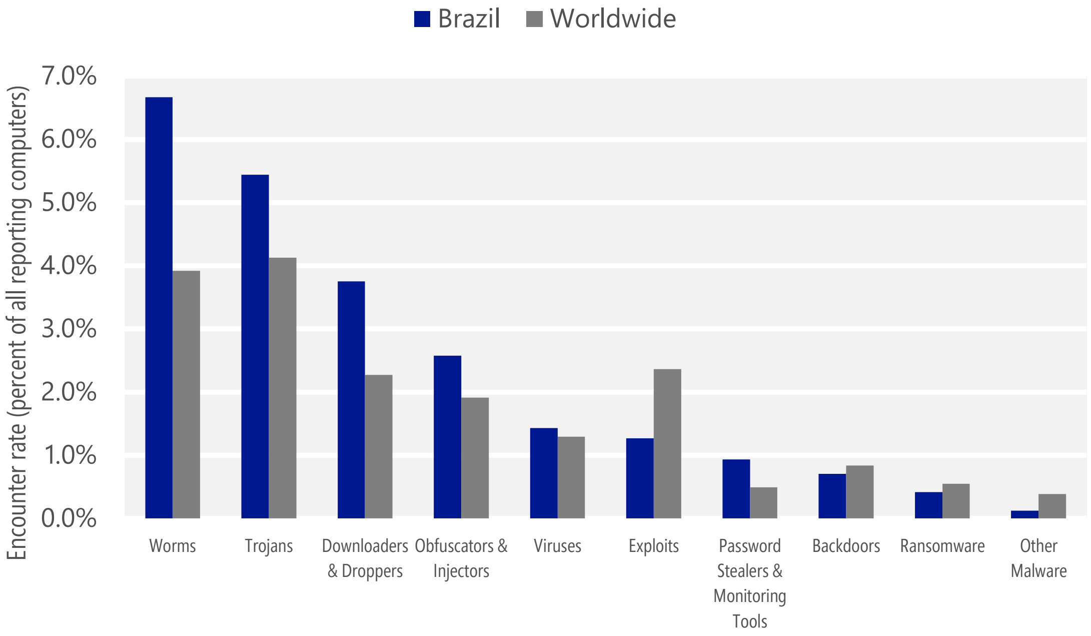
Malware encounter and infection rate trends in Brazil and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

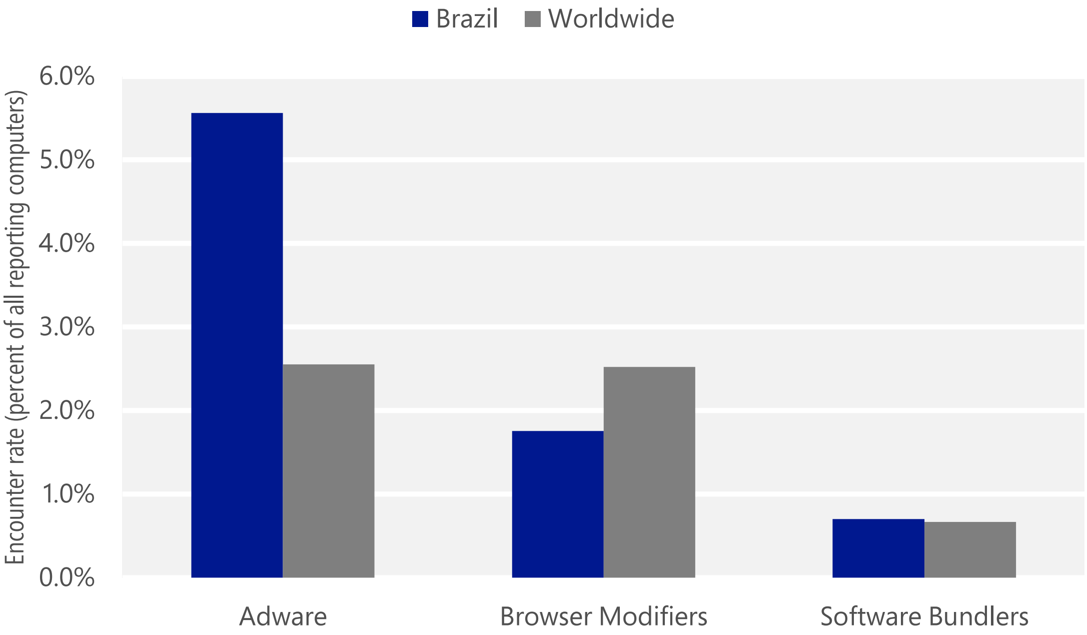
Malware encountered in Brazil in 4Q14, by category



- The most common malware category in Brazil in 4Q14 was Worms. It was encountered by 6.7 percent of all computers there, down from 9.9 percent in 3Q14.
- The second most common malware category in Brazil in 4Q14 was Trojans. It was encountered by 5.4 percent of all computers there, down from 9.6 percent in 3Q14.
- The third most common malware category in Brazil in 4Q14 was Downloaders & Droppers, which was encountered by 3.8 percent of all computers there, down from 9.0 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Brazil in 4Q14, by category



- The most common unwanted software category in Brazil in 4Q14 was Adware. It was encountered by 5.6 percent of all computers there, down from 9.3 percent in 3Q14.
- The second most common unwanted software category in Brazil in 4Q14 was Browser Modifiers. It was encountered by 1.8 percent of all computers there, down from 6.2 percent in 3Q14.
- The third most common unwanted software category in Brazil in 4Q14 was Software Bundlers, which was encountered by 0.7 percent of all computers there, up from 0.2 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Brazil in 4Q14

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	3.4%
2	JS/Proslikefan	Worms	1.4%
3	Win32/Banload	Downloaders & Droppers	1.3%
4	INF/Autorun	Obfuscators & Injectors	1.1%
5	Win32/Obfuscator	Obfuscators & Injectors	1.0%
6	Win32/Tugspay	Downloaders & Droppers	0.9%
7	Win32/Dynamer	Trojans	0.8%
8	Win32/Conficker	Worms	0.7%
9	Win32/Wysotot	Trojans	0.6%
10	Win32/Mujormel	Password Stealers & Monitoring Tools	0.6%

- The most common malware family encountered in Brazil in 4Q14 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 second most common malware family encountered in Brazil in 4Q14 was JS/Proslikefan, which was encountered by 1.4 percent of reporting computers there. JS/Proslikefan is a worm that spreads through removable drives, network shares, and P2P programs. It can lower the computer's security settings and disable antivirus products.
- The third most common malware family encountered in Brazil in 4Q14 was Win32/Banload, which was encountered by 1.3 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 fourth most common malware family encountered in Brazil in 4Q14 was INF/Autorun, which was encountered by 1.1 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 Brazil in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Pennybee	Adware	3.1%
2	Win32/Couponruc	Browser Modifiers	1.6%
3	Win32/Costmin	Adware	0.9%
4	Win32/Adpeak	Adware	0.4%
5	Win32/Softpulse	Software Bundlers	0.3%

- The most common unwanted software family encountered in Brazil in 4Q14 was Win32/Pennybee, which was encountered by 3.1 percent of reporting computers there. Win32/Pennybee is adware that shows ads as the user browses the web. It can be installed from the program's website or bundled with some third-party software installation programs.
- The second most common unwanted software family encountered in Brazil in 4Q14 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 third most common unwanted software family encountered in Brazil in 4Q14 was Win32/Costmin, which was encountered by 0.9 percent of reporting computers there. Win32/Costmin is an adware family that installs itself as a browser extension for Internet Explorer, Mozilla Firefox, and Google Chrome, and displays advertisements as the user browses the Internet.

Top threat families by infection rate

The most common malware families by infection rate in Brazil in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	4.7
2	Win32/Wysotot	Trojans	1.5
3	Win32/Sality	Viruses	1.1
4	Win32/Banload	Downloaders & Droppers	0.6
5	Win32/Ramnit	Trojans	0.5
6	Win32/Brontok	Worms	0.4
7	Win32/Sefnit	Trojans	0.4
8	Win32/Bancos	Trojans	0.3
9	MSIL/Bladabindi	Backdoors	0.3
10	Win32/Banker	Trojans	0.3

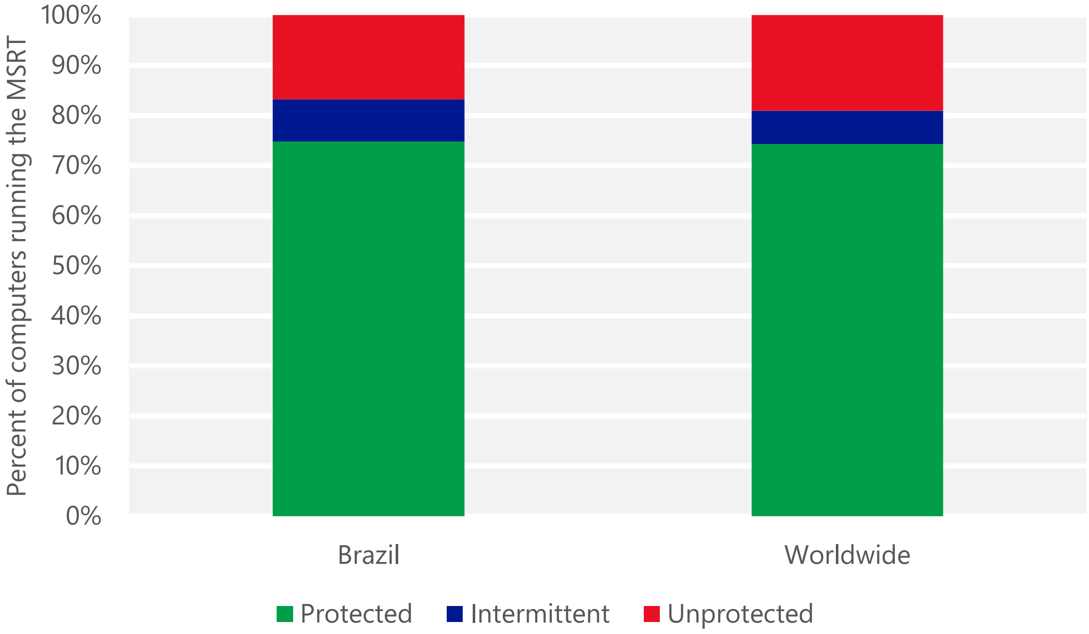
- The most common threat family infecting computers in Brazil in 4Q14 was VBS/Jenxcus, which was detected and removed from 4.7 of every 1,000 unique computers scanned by the MSRT. VBS/Jenxcus is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Brazil in 4Q14 was Win32/Wysotot, which was detected and removed from 1.5 of every 1,000 unique computers scanned by the MSRT. Win32/Wysotot is a threat that can change the start page of the user's web browser, and may download and install other files to the computer. It is installed by software bundlers that advertise free software or games.
- The third most common threat family infecting computers in Brazil in 4Q14 was Win32/Sality, which was detected and removed from 1.1 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 Brazil in 4Q14 was Win32/Banload, which was detected and removed from 0.6 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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.32 drive-by download URLs for every 1,000 URLs hosted in Brazil, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.27 drive-by download URLs for every 1,000 URLs hosted in Brazil, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Brazil and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Brazil	0.32	0.27
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Bulgaria

The statistics presented here are generated by Microsoft security programs and services running on computers in Bulgaria in 4Q14 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 succeds 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

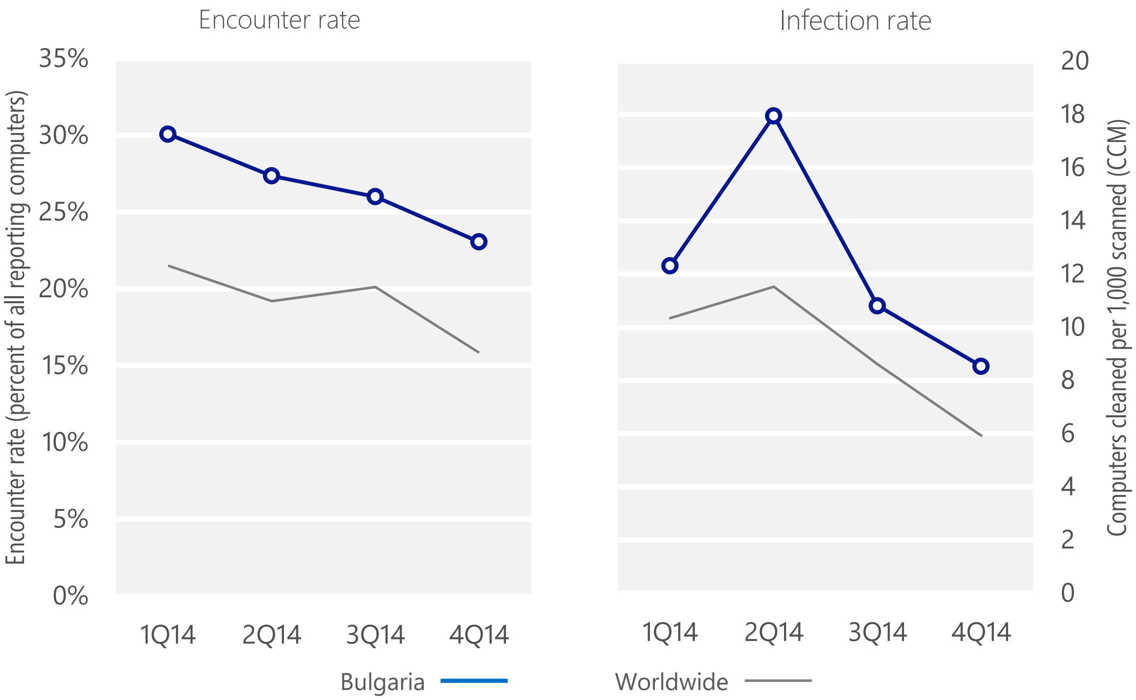
Metric	**1Q14**	**2Q14**	**3Q14**	**4Q14**
Encounter rate, Bulgaria	30.1%	27.4%	26.0%	23.1%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Bulgaria	12.3	18.0	10.8	8.5
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 23.1% percent of computers in Bulgaria encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 8.5 of every 1,000 unique computers scanned in Bulgaria in 4Q14 (a CCM score of 8.5, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Bulgaria over the last four quarters, compared to the world as a whole.

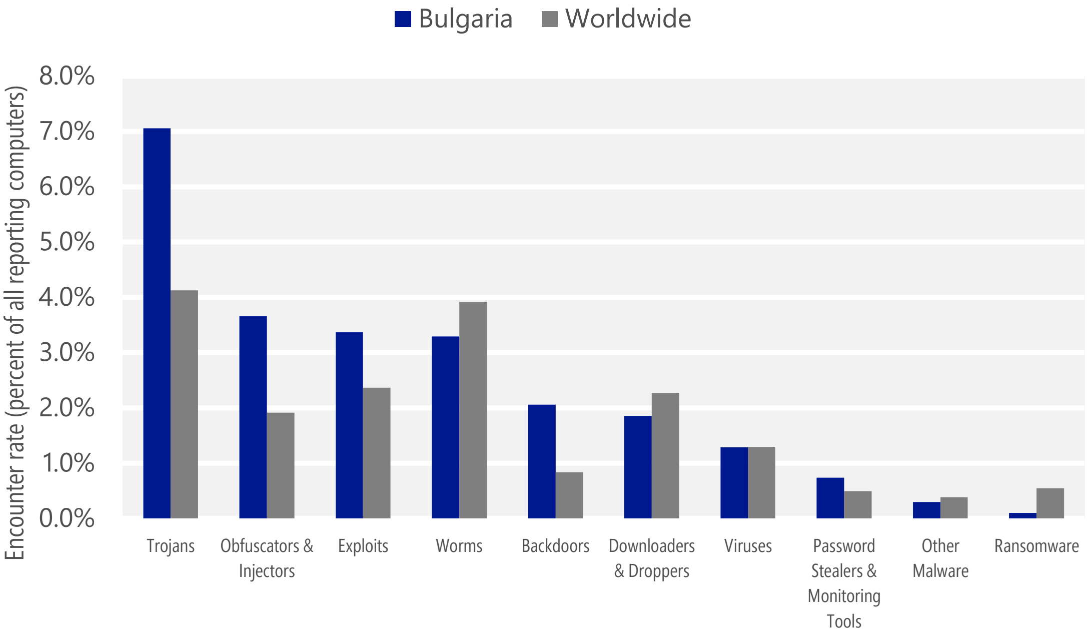
Malware encounter and infection rate trends in Bulgaria and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

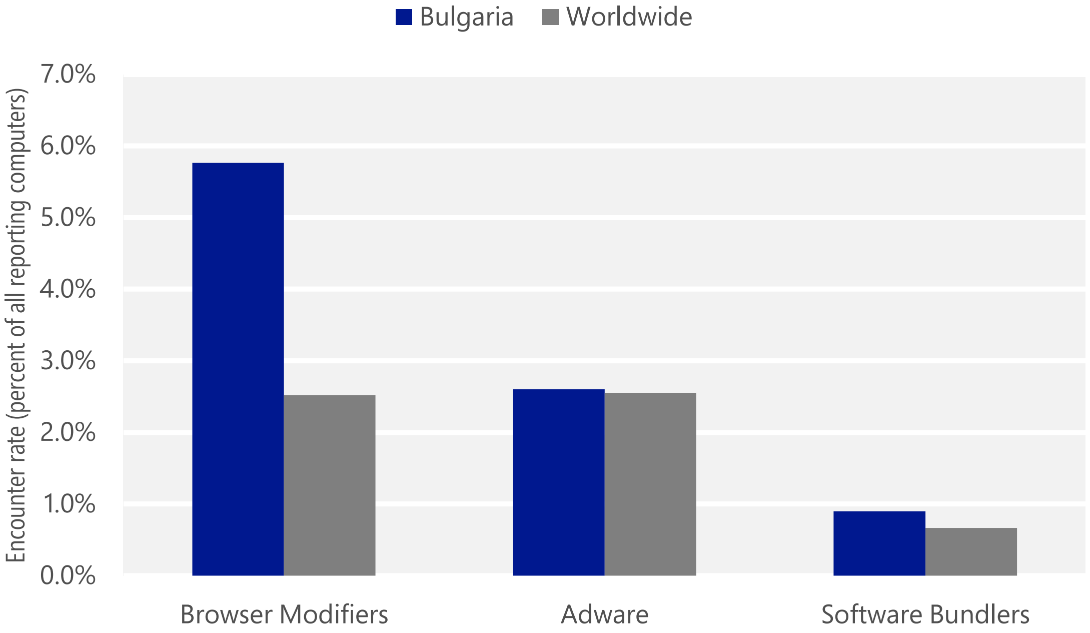
Malware encountered in Bulgaria in 4Q14, by category



- The most common malware category in Bulgaria in 4Q14 was Trojans. It was encountered by 7.1 percent of all computers there, down from 9.7 percent in 3Q14.
- The second most common malware category in Bulgaria in 4Q14 was Obfuscators & Injectors. It was encountered by 3.7 percent of all computers there, down from 5.7 percent in 3Q14.
- The third most common malware category in Bulgaria in 4Q14 was Exploits, which was encountered by 3.4 percent of all computers there, down from 4.0 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Bulgaria in 4Q14, by category



- The most common unwanted software category in Bulgaria in 4Q14 was Browser Modifiers. It was encountered by 5.8 percent of all computers there, down from 6.0 percent in 3Q14.
- The second most common unwanted software category in Bulgaria in 4Q14 was Adware. It was encountered by 2.6 percent of all computers there, up from 0.5 percent in 3Q14.
- The third most common unwanted software category in Bulgaria in 4Q14 was Software Bundlers, which was encountered by 0.9 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Bulgaria in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Obfuscator	Obfuscators & Injectors	2.1%
2	JS/Axpergle	Exploits	1.8%
3	INF/Autorun	Obfuscators & Injectors	1.3%
4	Win32/Anogre	Exploits	1.2%
5	Win32/Conficker	Worms	0.9%
6	Win32/Fynloski	Backdoors	0.8%
7	Win32/Tarcloin	Trojans	0.7%
8	Win32/Sality	Viruses	0.7%
9	Win32/Killav	Trojans	0.6%
10	Win32/Gamarue	Worms	0.6%

- The most common malware family encountered in Bulgaria in 4Q14 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 Bulgaria in 4Q14 was JS/Axpergle, which was encountered by 1.8 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 third most common malware family encountered in Bulgaria in 4Q14 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 fourth most common malware family encountered in Bulgaria in 4Q14 was Win32/Anogre, which was encountered by 1.2 percent of reporting computers there. Win32/Anogre is a threat that exploits a vulnerability addressed by Microsoft Security Bulletin MS11-087. This vulnerability can allow a hacker to install programs, view, change, or delete data or create new accounts with full administrative privileges.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Bulgaria in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	4.0%
2	Win32/Defaulttab	Browser Modifiers	2.0%
3	Win32/Costmin	Adware	1.3%
4	Win32/BetterSurf	Adware	1.1%
5	Win32/Gofileexpress	Software Bundlers	0.7%

- The most common unwanted software family encountered in Bulgaria in 4Q14 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 Bulgaria in 4Q14 was Win32/Defaulttab, which was encountered by 2.0 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.
- The third most common unwanted software family encountered in Bulgaria in 4Q14 was Win32/Costmin, which was encountered by 1.3 percent of reporting computers there. Win32/Costmin is an adware family that installs itself as a browser extension for Internet Explorer, Mozilla Firefox, and Google Chrome, and displays advertisements as the user browses the Internet.

Top threat families by infection rate

The most common malware families by infection rate in Bulgaria in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Sality	Viruses	2.3
2	Win32/Brontok	Worms	0.6
3	JS/Kilim	Trojans	0.5
4	MSIL/Bladabindi	Backdoors	0.5
5	VBS/Jenxcus	Worms	0.5
6	Win32/Pramro	Trojans	0.4
7	Win32/Helompy	Worms	0.4
8	Win32/Gamarue	Worms	0.4
9	Win32/Carberp	Trojans	0.4
10	Win32/Sefnit	Trojans	0.3

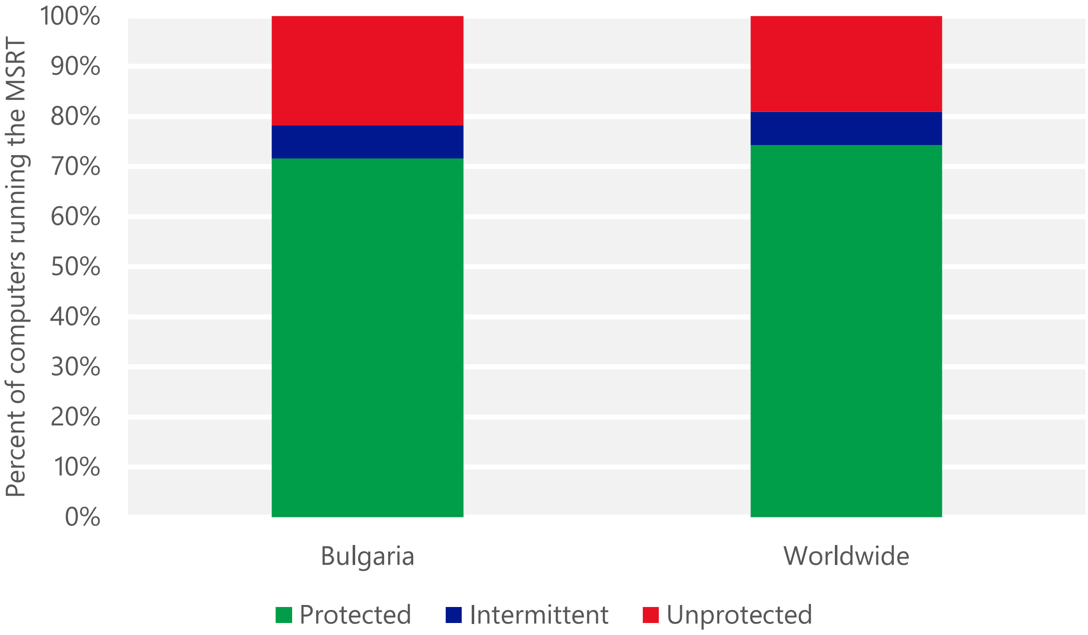
- The most common threat family infecting computers in Bulgaria in 4Q14 was Win32/Sality, which was detected and removed from 2.3 of every 1,000 unique computers scanned by the MSRT. Win32/Sality is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The second most common threat family infecting computers in Bulgaria in 4Q14 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 third most common threat family infecting computers in Bulgaria in 4Q14 was JS/Kilim, which was detected and removed from 0.5 of every 1,000 unique computers scanned by the MSRT. JS/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 Bulgaria in 4Q14 was MSIL/Bladabindi, which was detected and removed from 0.5 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.

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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.51 drive-by download URLs for every 1,000 URLs hosted in Bulgaria, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.51 drive-by download URLs for every 1,000 URLs hosted in Bulgaria, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Bulgaria and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Bulgaria	0.51	0.51
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Canada

The statistics presented here are generated by Microsoft security programs and services running on computers in Canada in 4Q14 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 succeds 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

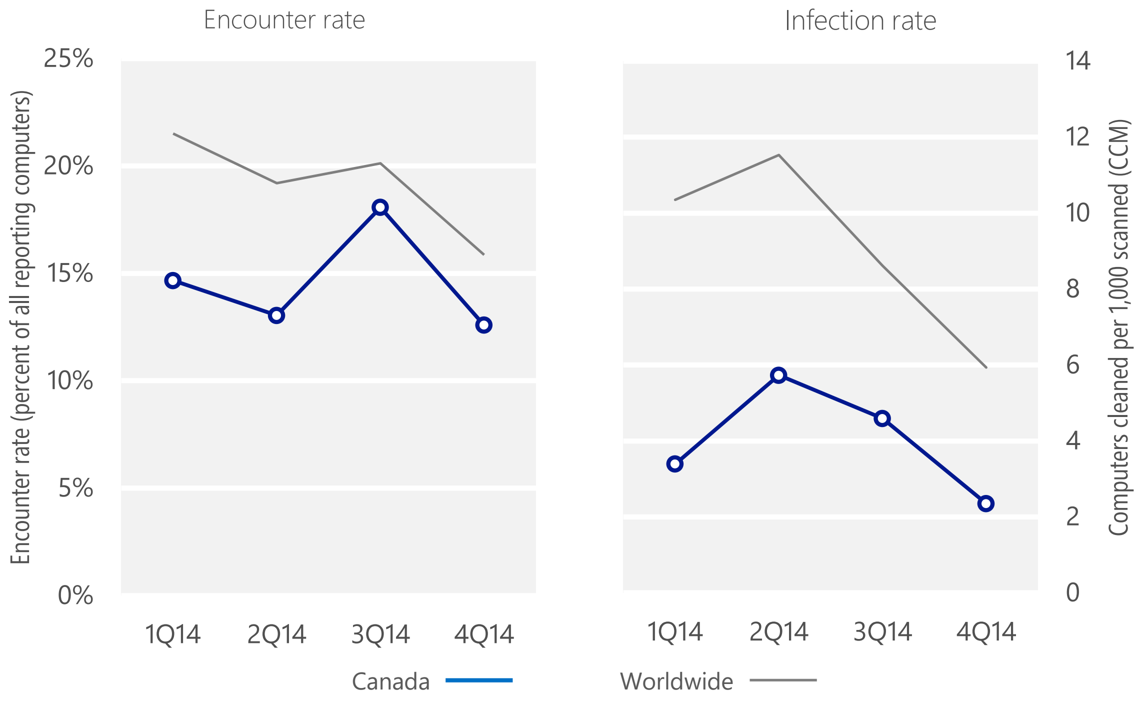
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Canada	14.7%	13.0%	18.1%	12.6%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Canada	3.4	5.7	4.6	2.4
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 12.6% percent of computers in Canada encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 2.4 of every 1,000 unique computers scanned in Canada in 4Q14 (a CCM score of 2.4, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Canada over the last four quarters, compared to the world as a whole.

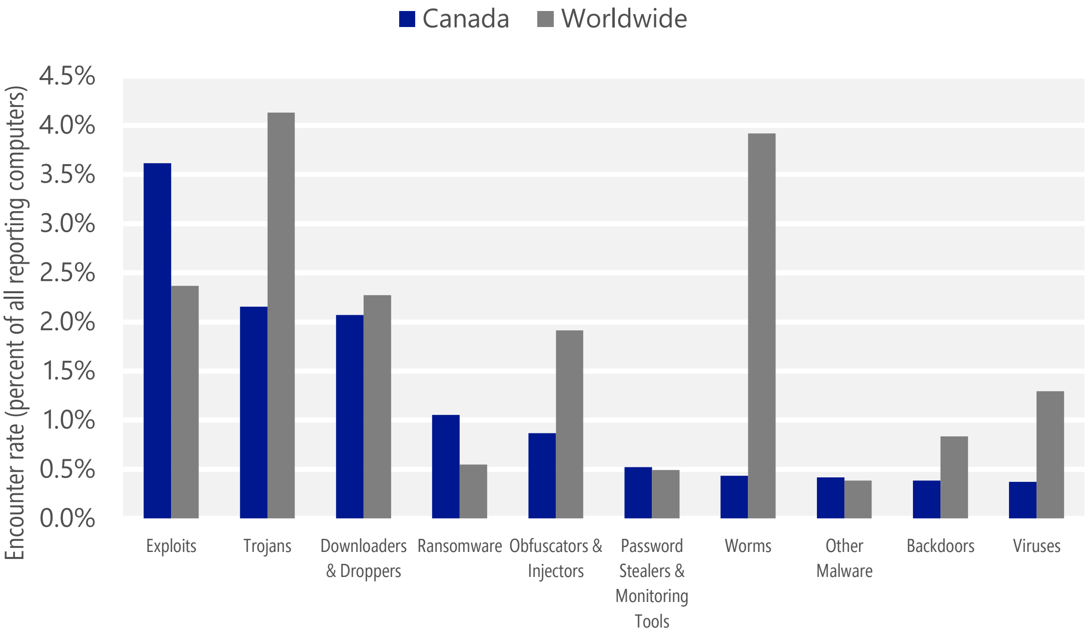
Malware encounter and infection rate trends in Canada and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

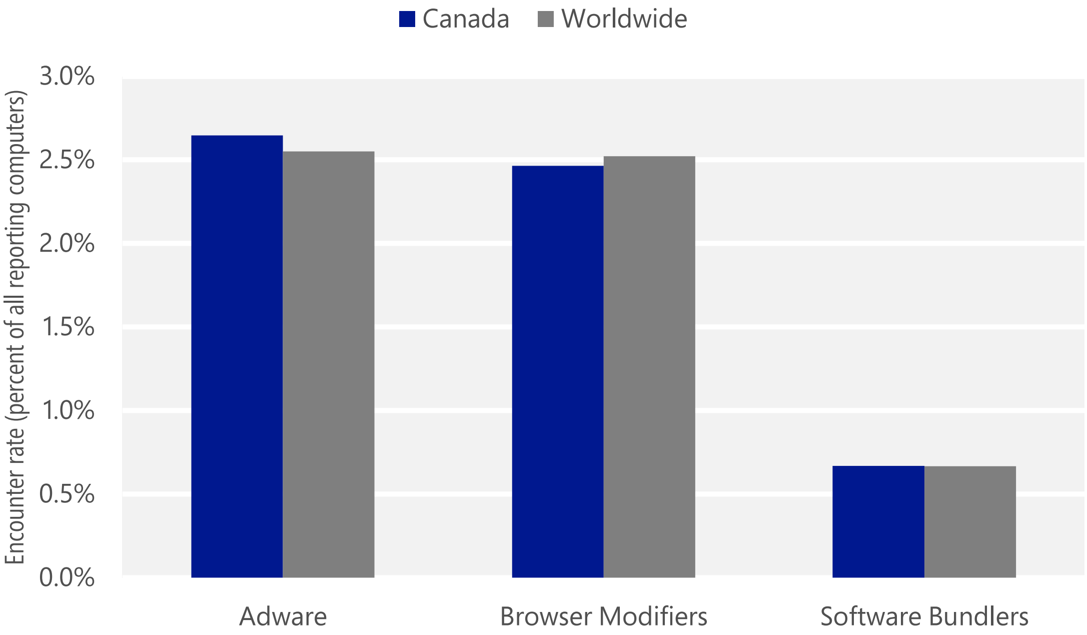
Malware encountered in Canada in 4Q14, by category



- The most common malware category in Canada in 4Q14 was Exploits. It was encountered by 3.6 percent of all computers there, down from 6.4 percent in 3Q14.
- The second most common malware category in Canada in 4Q14 was Trojans. It was encountered by 2.2 percent of all computers there, down from 4.0 percent in 3Q14.
- The third most common malware category in Canada in 4Q14 was Downloaders & Droppers, which was encountered by 2.1 percent of all computers there, down from 3.6 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Canada in 4Q14, by category



- The most common unwanted software category in Canada in 4Q14 was Adware. It was encountered by 2.6 percent of all computers there, down from 6.7 percent in 3Q14.
- The second most common unwanted software category in Canada in 4Q14 was Browser Modifiers. It was encountered by 2.5 percent of all computers there, up from 2.5 percent in 3Q14.
- The third most common unwanted software category in Canada in 4Q14 was Software Bundlers, which was encountered by 0.7 percent of all computers there, up from 0.3 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Canada in 4Q14

	Family	Most significant category	% of reporting computers
1	JS/Axpergle	Exploits	1.7%
2	JS/Fiexp	Exploits	1.0%
3	Win32/Tugspay	Downloaders & Droppers	0.7%
4	Win32/Obfuscator	Obfuscators & Injectors	0.7%
5	JS/Krypterade	Ransomware	0.7%
6	Win32/Anogre	Exploits	0.6%
7	Win32/Upatre	Downloaders & Droppers	0.3%
8	Win32/Zbot	Password Stealers & Monitoring Tools	0.2%
9	Win32/Clikug	Trojans	0.2%
10	ASX/Wimad	Downloaders & Droppers	0.2%

- The most common malware family encountered in Canada in 4Q14 was JS/Axpergle, which was encountered by 1.7 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 Canada in 4Q14 was JS/Fiexp, which was encountered by 1.0 percent of reporting computers there. JS/Fiexp is a detection for the Fiesta exploit kit, which attempts to exploit Java, Adobe Flash Player, Adobe Reader, Silverlight, and Internet Explorer to install malware.
- The third most common malware family encountered in Canada in 4Q14 was Win32/Tugspay, which was encountered by 0.7 percent of reporting computers there. Win32/Tugspay is a downloader that spreads by posing as an installer for legitimate software, such as a Java update, or through other malware. When installed, it downloads unwanted software to the computer.
- The fourth most common malware family encountered in Canada in 4Q14 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.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Canada in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	1.7%
2	Win32/Costmin	Adware	1.0%
3	Win32/Defaulttab	Browser Modifiers	0.7%
4	Win32/BetterSurf	Adware	0.5%
5	Win32/Couponarific	Adware	0.4%

- The most common unwanted software family encountered in Canada in 4Q14 was Win32/Couponruc, which was encountered by 1.7 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 Canada in 4Q14 was Win32/Costmin, which was encountered by 1.0 percent of reporting computers there. Win32/Costmin is an adware family that installs itself as a browser extension for Internet Explorer, Mozilla Firefox, and Google Chrome, and displays advertisements as the user browses the Internet.
- The third most common unwanted software family encountered in Canada in 4Q14 was Win32/Defaulttab, which was encountered by 0.7 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.

Top threat families by infection rate

The most common malware families by infection rate in Canada in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Zbot	Password Stealers & Monitoring Tools	0.3
2	Win32/Alureon	Trojans	0.3
3	JS/Medfos	Trojans	0.3
4	JS/Miuref	Trojans	0.2
5	Win32/Wysotot	Trojans	0.2
6	Win32/Sirefef	Trojans	0.2
7	Win32/Ramnit	Trojans	0.1
8	Win32/Sefnit	Trojans	0.1
9	VBS/Jenxcus	Worms	0.1
10	Win32/Cutwail	Downloaders & Droppers	0.1

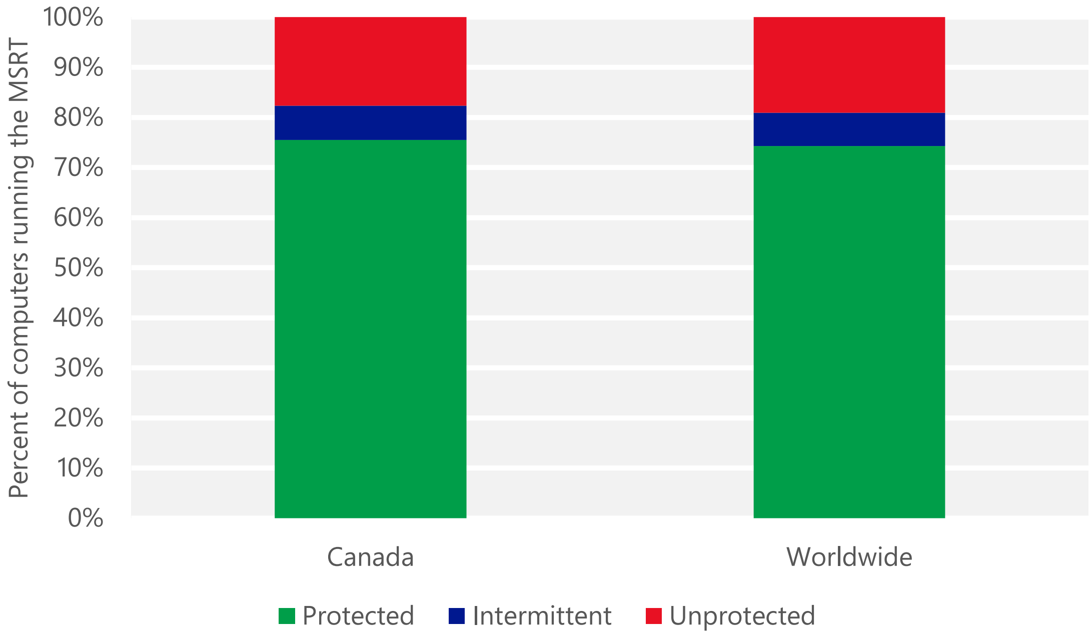
- The most common threat family infecting computers in Canada in 4Q14 was Win32/Zbot, which was detected and removed from 0.3 of every 1,000 unique computers scanned by the MSRT. Win32/Zbot is a family of password stealing trojans that also contains backdoor functionality allowing unauthorized access and control of an affected computer.
- The second most common threat family infecting computers in Canada in 4Q14 was Win32/Alureon, which was detected and removed from 0.3 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 third most common threat family infecting computers in Canada in 4Q14 was JS/Medfos, which was detected and removed from 0.3 of every 1,000 unique computers scanned by the MSRT. JS/Medfos is ?A trojan that installs malicious Internet browser extensions and redirects search results from popular search engines.
- The fourth most common threat family infecting computers in Canada in 4Q14 was JS/Miuref, which was detected and removed from 0.2 of every 1,000 unique computers scanned by the MSRT. JS/Miuref is a family of malicious JavaScript files that redirect the web browser to show ads or download malware. They can be installed by other malware, including Win32/Fareit, or installed through spam email attachments.

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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.27 drive-by download URLs for every 1,000 URLs hosted in Canada, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.23 drive-by download URLs for every 1,000 URLs hosted in Canada, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Canada and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Canada	0.27	0.23
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Chile

The statistics presented here are generated by Microsoft security programs and services running on computers in Chile in 4Q14 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 succeds 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

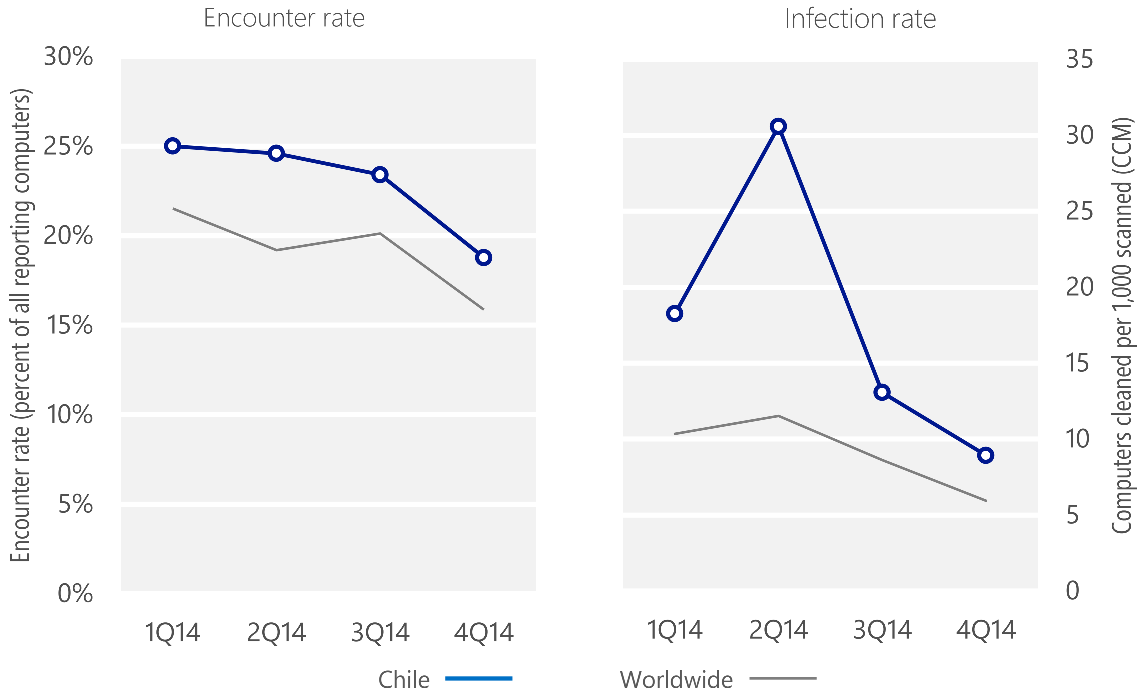
Metric	**1Q14**	**2Q14**	**3Q14**	**4Q14**
Encounter rate, Chile	25.0%	24.6%	23.4%	18.8%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Chile	18.3	30.6	13.1	8.9
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 18.8% percent of computers in Chile encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 8.9 of every 1,000 unique computers scanned in Chile in 4Q14 (a CCM score of 8.9, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Chile over the last four quarters, compared to the world as a whole.

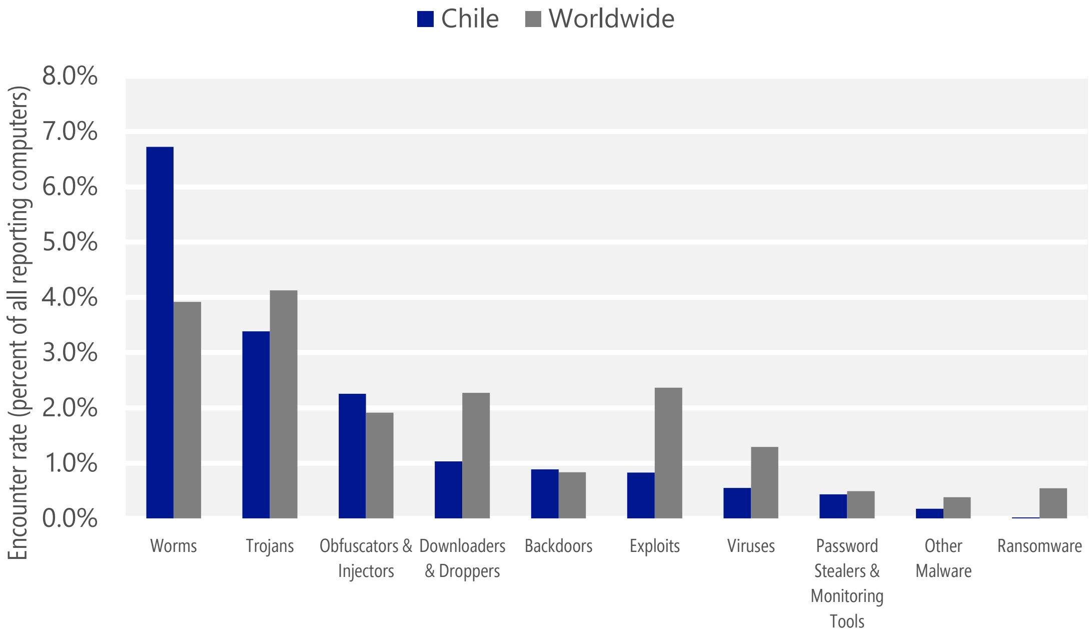
Malware encounter and infection rate trends in Chile and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

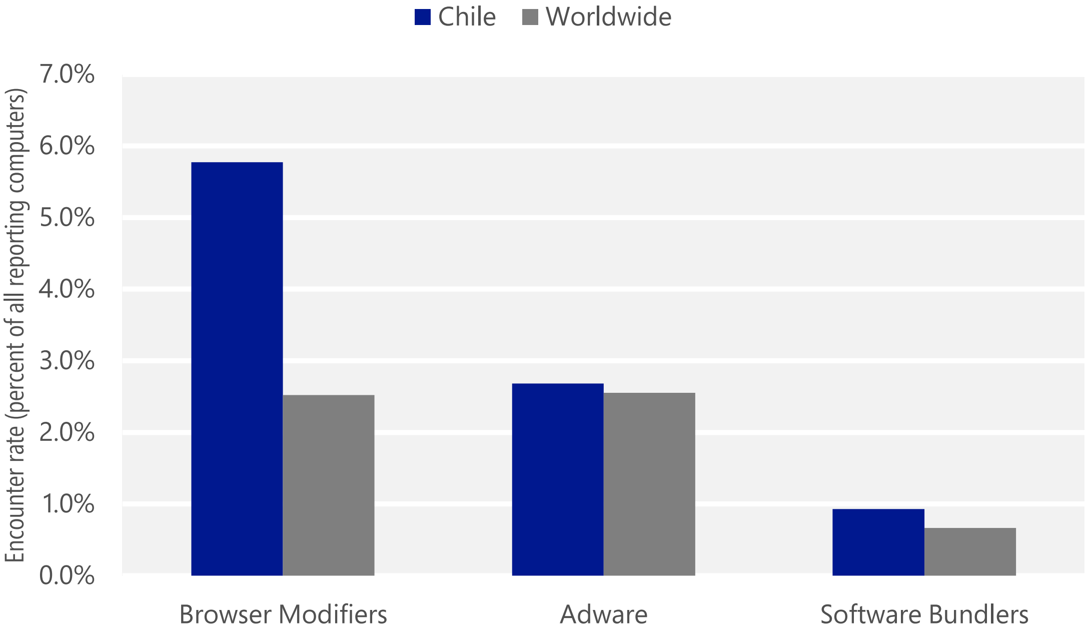
Malware encountered in Chile in 4Q14, by category



- The most common malware category in Chile in 4Q14 was Worms. It was encountered by 6.7 percent of all computers there, down from 7.6 percent in 3Q14.
- The second most common malware category in Chile in 4Q14 was Trojans. It was encountered by 3.4 percent of all computers there, down from 5.9 percent in 3Q14.
- The third most common malware category in Chile in 4Q14 was Obfuscators & Injectors, which was encountered by 2.3 percent of all computers there, down from 3.1 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Chile in 4Q14, by category



- The most common unwanted software category in Chile in 4Q14 was Browser Modifiers. It was encountered by 5.8 percent of all computers there, down from 7.4 percent in 3Q14.
- The second most common unwanted software category in Chile in 4Q14 was Adware. It was encountered by 2.7 percent of all computers there, up from 1.9 percent in 3Q14.
- The third most common unwanted software category in Chile in 4Q14 was Software Bundlers, which was encountered by 0.9 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Chile in 4Q14

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	2.6%
2	Win32/Vermis	Worms	1.1%
3	Win32/Obfuscator	Obfuscators & Injectors	1.1%
4	JS/Bondat	Worms	1.0%
5	INF/Autorun	Obfuscators & Injectors	1.0%
6	Win32/Dorkbot	Worms	0.9%
7	Win32/Conficker	Worms	0.6%
8	Win32/Brontok	Worms	0.4%
9	Win32/Dynamer	Trojans	0.4%
10	Win32/VBInject	Obfuscators & Injectors	0.3%

- The most common malware family encountered in Chile in 4Q14 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 Chile in 4Q14 was Win32/Vermis, which was encountered by 1.1 percent of reporting computers there. Win32/Vermis is a generic detection for malicious .inf and .lnk files dropped by different worms, including IRCBot, Phorpiex, Dorkbot, and Caphaw.
- The third most common malware family encountered in Chile in 4Q14 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 fourth most common malware family encountered in Chile in 4Q14 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.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Chile in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	5.0%
2	Win32/Costmin	Adware	1.1%
3	Win32/BetterSurf	Adware	0.9%
4	Win32/Defaulttab	Browser Modifiers	0.9%
5	Win32/Gofileexpress	Software Bundlers	0.4%

- The most common unwanted software family encountered in Chile in 4Q14 was Win32/Couponruc, which was encountered by 5.0 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 Chile in 4Q14 was Win32/Costmin, which was encountered by 1.1 percent of reporting computers there. Win32/Costmin is an adware family that installs itself as a browser extension for Internet Explorer, Mozilla Firefox, and Google Chrome, and displays advertisements as the user browses the Internet.
- The third most common unwanted software family encountered in Chile in 4Q14 was Win32/BetterSurf, which was encountered by 0.9 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.

Top threat families by infection rate

The most common malware families by infection rate in Chile in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	3.3
2	Win32/Dorkbot	Worms	1.1
3	Win32/Brontok	Worms	0.7
4	Win32/Sefnit	Trojans	0.7
5	Win32/Lethic	Trojans	0.5
6	MSIL/Spacekito	Trojans	0.5
7	Win32/Sality	Viruses	0.4
8	Win32/Ramnit	Trojans	0.3
9	Win32/Vobfus	Worms	0.2
10	Win32/Wysotot	Trojans	0.2

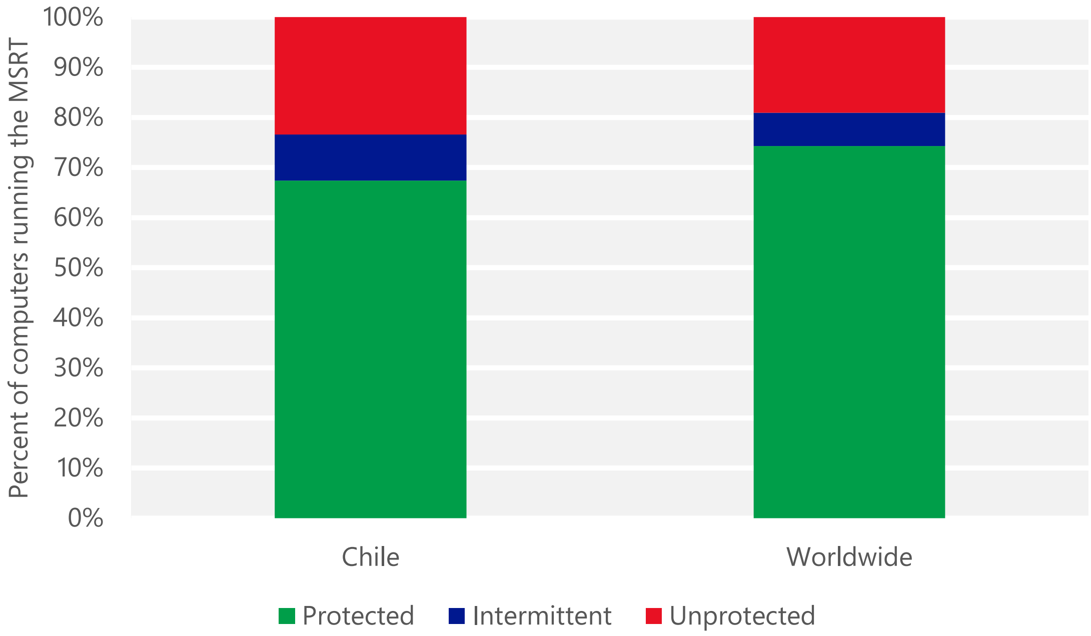
- The most common threat family infecting computers in Chile in 4Q14 was VBS/Jenxcus, which was detected and removed from 3.3 of every 1,000 unique computers scanned by the MSRT. VBS/Jenxcus is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Chile in 4Q14 was Win32/Dorkbot, which was detected and removed from 1.1 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.
- The third most common threat family infecting computers in Chile in 4Q14 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.
- The fourth most common threat family infecting computers in Chile in 4Q14 was Win32/Sefnit, which was detected and removed from 0.7 of every 1,000 unique computers scanned by the MSRT. Win32/Sefnit is a family of trojans that can allow backdoor access, download files, and use the computer and Internet connection for click fraud. Some variants can monitor web browsers and hijack search results.

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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.29 drive-by download URLs for every 1,000 URLs hosted in Chile, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.25 drive-by download URLs for every 1,000 URLs hosted in Chile, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Chile and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Chile	0.29	0.25
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

China

The statistics presented here are generated by Microsoft security programs and services running on computers in China in 4Q14 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 succeds 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

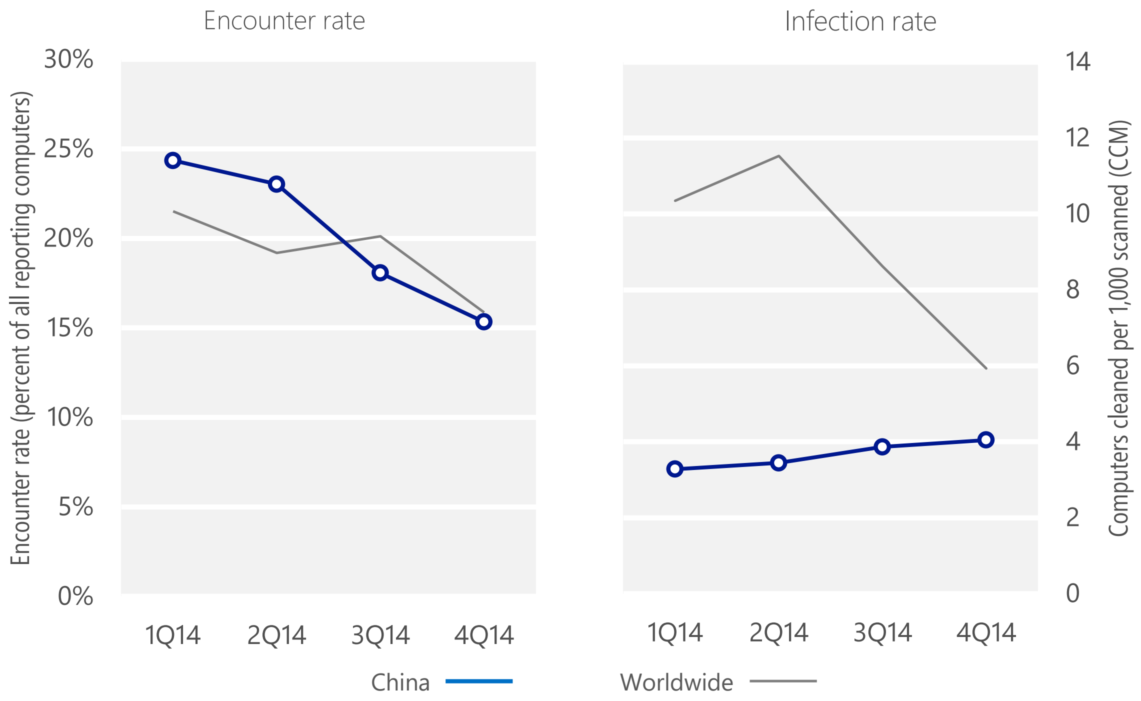
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, China	24.4%	23.0%	18.1%	15.3%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, China	3.3	3.4	3.9	4.0
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 15.3% percent of computers in China encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 4.0 of every 1,000 unique computers scanned in China in 4Q14 (a CCM score of 4.0, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for China over the last four quarters, compared to the world as a whole.

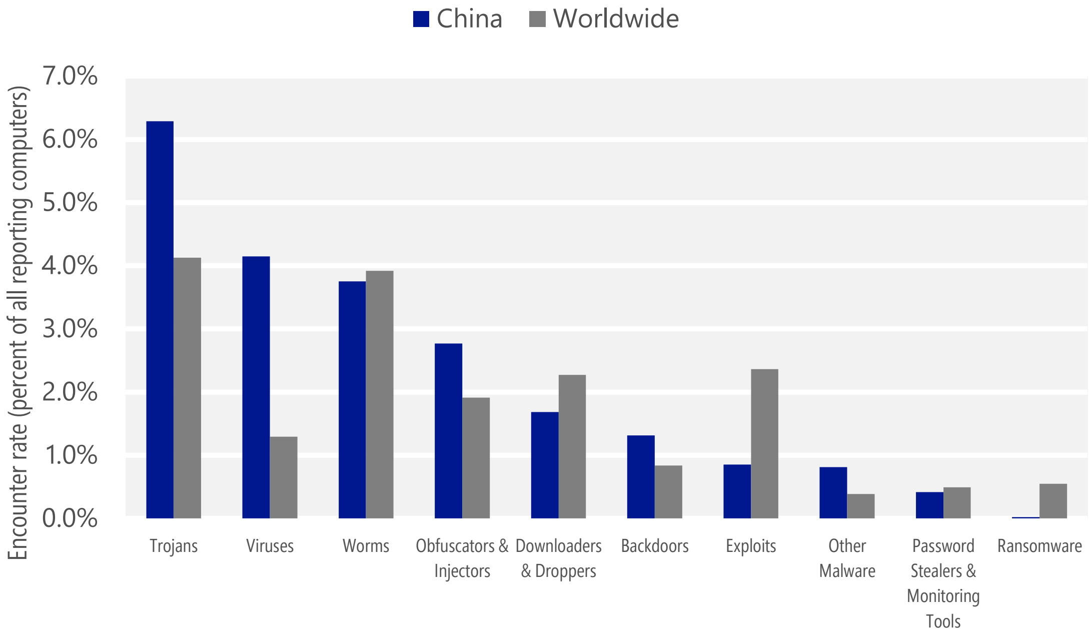
Malware encounter and infection rate trends in China and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

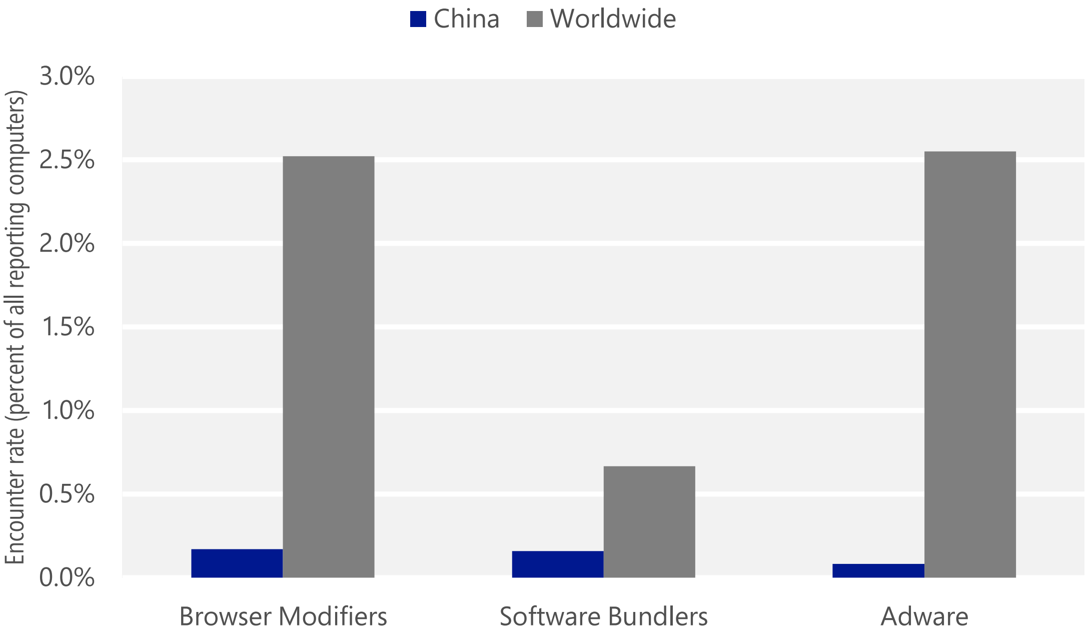
Malware encountered in China in 4Q14, by category



- The most common malware category in China in 4Q14 was Trojans. It was encountered by 6.3 percent of all computers there, down from 7.9 percent in 3Q14.
- The second most common malware category in China in 4Q14 was Viruses. It was encountered by 4.1 percent of all computers there, down from 4.8 percent in 3Q14.
- The third most common malware category in China in 4Q14 was Worms, which was encountered by 3.8 percent of all computers there, up from 3.6 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in China in 4Q14, by category



- The most common unwanted software category in China in 4Q14 was Browser Modifiers. It was encountered by 0.2 percent of all computers there, down from 0.2 percent in 3Q14.
- The second most common unwanted software category in China in 4Q14 was Software Bundlers. It was encountered by 0.2 percent of all computers there, down from 0.2 percent in 3Q14.
- The third most common unwanted software category in China in 4Q14 was Adware, which was encountered by 0.1 percent of all computers there, down from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in China in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Obfuscator	Obfuscators & Injectors	2.2%
2	INF/Autorun	Obfuscators & Injectors	1.1%
3	Win32/Dynamer	Trojans	0.9%
4	DOS/JackTheRipper	Viruses	0.9%
5	ALisp/Bursted	Viruses	0.8%
6	Win32/Nitol	Other Malware	0.7%
7	Win32/Conficker	Worms	0.7%
8	ALisp/Kenilfe	Worms	0.6%
9	Win32/Bumat	Trojans	0.6%
10	Win32/FlyAgent	Backdoors	0.5%

- The most common malware family encountered in China in 4Q14 was Win32/Obfuscator, which was encountered by 2.2 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 second most common malware family encountered in China in 4Q14 was INF/Autorun, which was encountered by 1.1 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 China in 4Q14 was Win32/Dynamer, which was encountered by 0.9 percent of reporting computers there. Win32/Dynamer is a generic detection for a variety of threats.
- The fourth most common malware family encountered in China in 4Q14 was DOS/JackTheRipper, which was encountered by 0.9 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.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in China in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Chindo	Software Bundlers	0.1%
2	Win32/Couponruc	Browser Modifiers	0.1%
3	Win32/Defaulttab	Browser Modifiers	<0.1%
4	Win32/CNNIC	Browser Modifiers	<0.1%
5	Win32/Gofileexpress	Software Bundlers	<0.1%

- The most common unwanted software family encountered in China in 4Q14 was Win32/Chindo, which was encountered by 0.1 percent of reporting computers there.
- The second most common unwanted software family encountered in China in 4Q14 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 China in 4Q14 was Win32/Defaulttab, which was encountered by <0.1 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.

Top threat families by infection rate

The most common malware families by infection rate in China in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Nitol	Other Malware	1.3
2	Win32/Frethog	Password Stealers & Monitoring Tools	0.8
3	Win32/Ramnit	Trojans	0.7
4	Win32/Sality	Viruses	0.3
5	Win32/Conficker	Worms	0.2
6	Win32/Parite	Viruses	0.2
7	Win32/Hupigon	Backdoors	0.1
8	VBS/Jenxcus	Worms	0.1
9	Win32/Yeltminky	Worms	0.1
10	Win32/Virut	Viruses	0.1

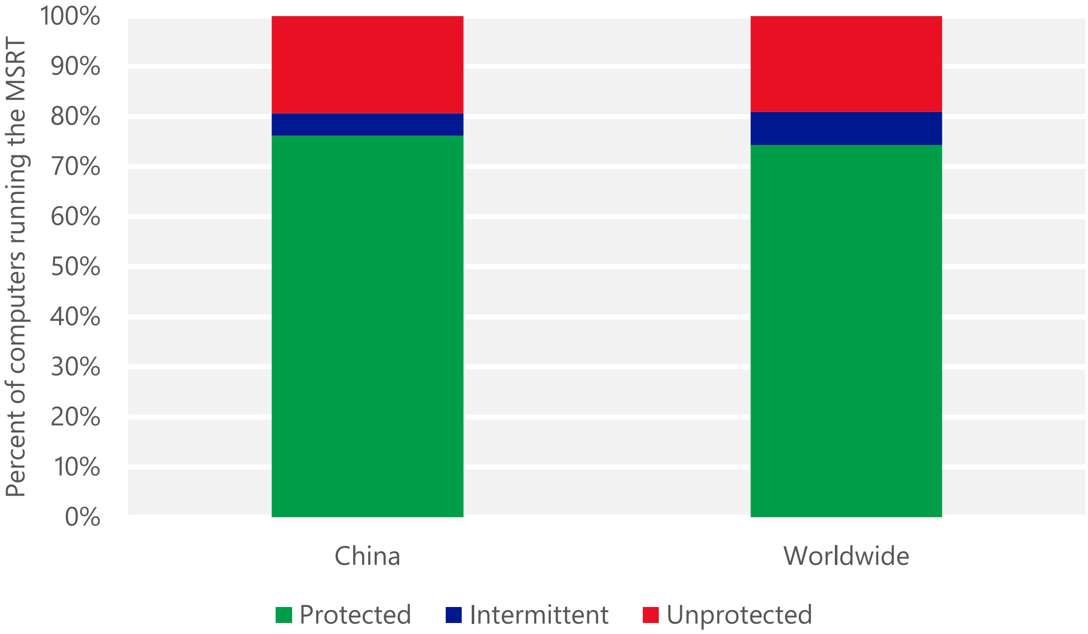
- The most common threat family infecting computers in China in 4Q14 was Win32/Nitol, which was detected and removed from 1.3 of every 1,000 unique computers scanned by the MSRT. Win32/Nitol is a family of trojans that perform DDoS (distributed denial of service) attacks, allow backdoor access and control, 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 4Q14 was Win32/Frethog, which was detected and removed from 0.8 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 third most common threat family infecting computers in China in 4Q14 was Win32/Ramnit, which was detected and removed from 0.7 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 China in 4Q14 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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.24 drive-by download URLs for every 1,000 URLs hosted in China, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.20 drive-by download URLs for every 1,000 URLs hosted in China, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in China and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, China	0.24	0.20
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Colombia

The statistics presented here are generated by Microsoft security programs and services running on computers in Colombia in 4Q14 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 succeds 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

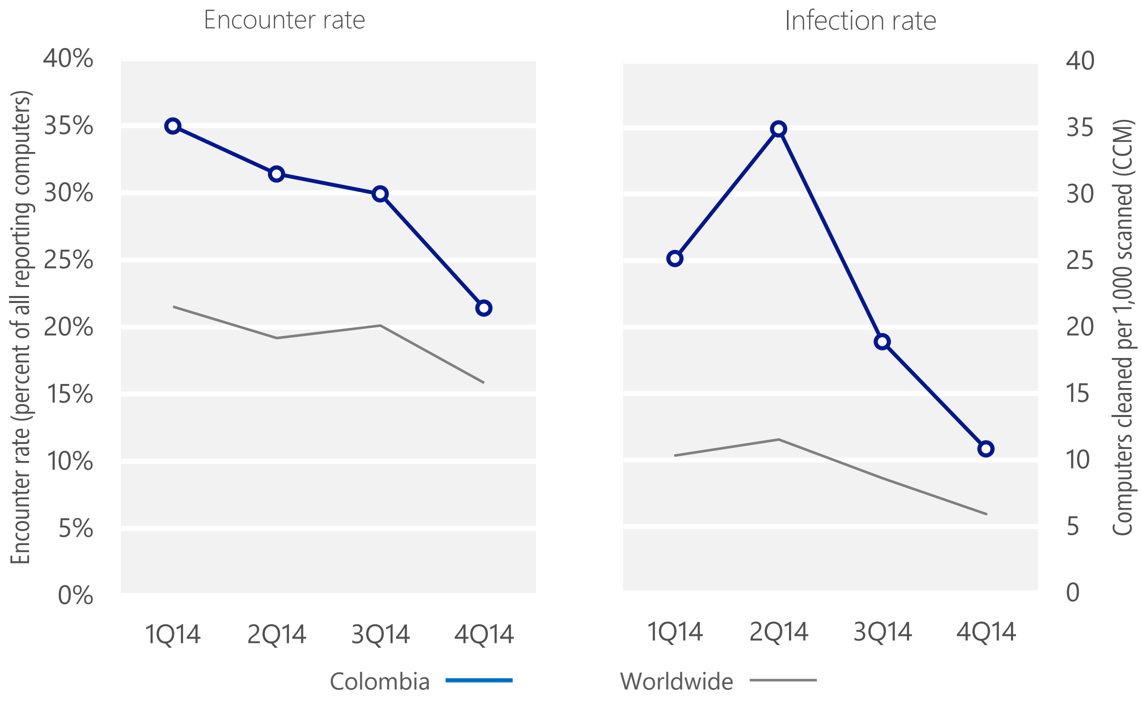
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Colombia	35.0%	31.4%	29.9%	21.4%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Colombia	25.2	34.9	18.9	10.8
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 21.4% percent of computers in Colombia encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 10.8 of every 1,000 unique computers scanned in Colombia in 4Q14 (a CCM score of 10.8, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Colombia over the last four quarters, compared to the world as a whole.

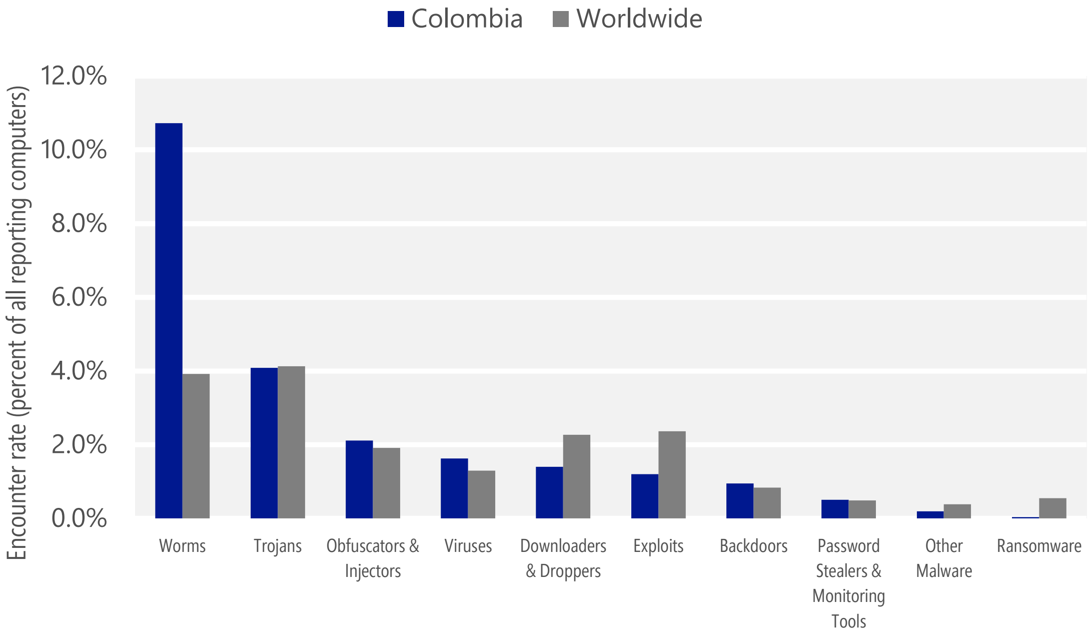
Malware encounter and infection rate trends in Colombia and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

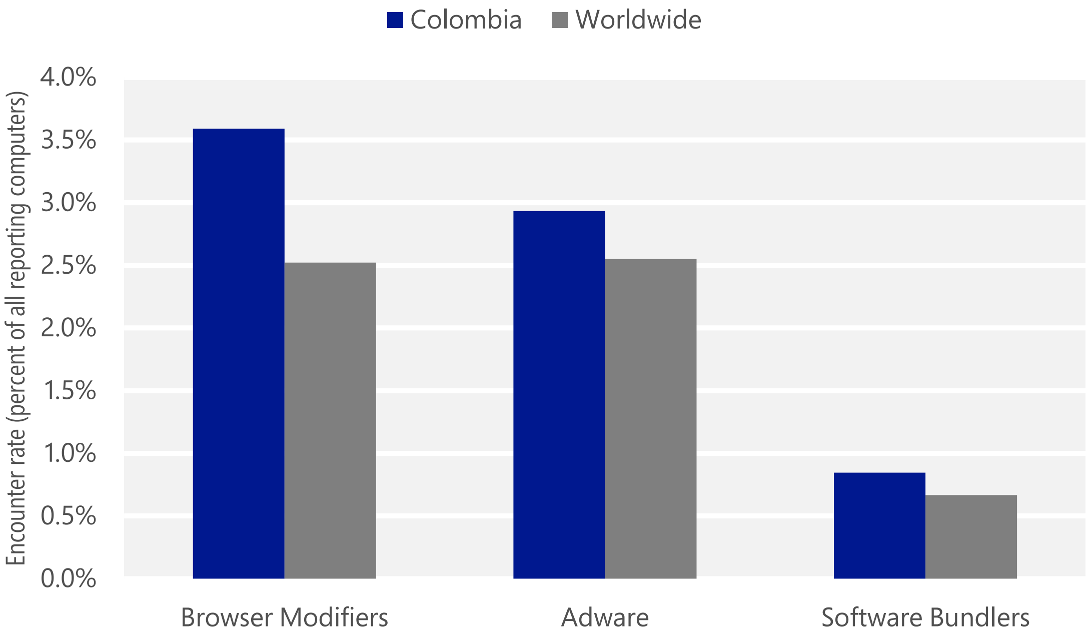
Malware encountered in Colombia in 4Q14, by category



- The most common malware category in Colombia in 4Q14 was Worms. It was encountered by 10.7 percent of all computers there, down from 12.5 percent in 3Q14.
- The second most common malware category in Colombia in 4Q14 was Trojans. It was encountered by 4.1 percent of all computers there, down from 8.2 percent in 3Q14.
- The third most common malware category in Colombia in 4Q14 was Obfuscators & Injectors, which was encountered by 2.1 percent of all computers there, down from 4.1 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Colombia in 4Q14, by category



- The most common unwanted software category in Colombia in 4Q14 was Browser Modifiers. It was encountered by 3.6 percent of all computers there, down from 6.8 percent in 3Q14.
- The second most common unwanted software category in Colombia in 4Q14 was Adware. It was encountered by 2.9 percent of all computers there, down from 5.5 percent in 3Q14.
- The third most common unwanted software category in Colombia in 4Q14 was Software Bundlers, which was encountered by 0.8 percent of all computers there, up from 0.2 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Colombia in 4Q14

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	5.4%
2	JS/Bondat	Worms	3.2%
3	INF/Autorun	Obfuscators & Injectors	1.5%
4	Win32/Gamarue	Worms	1.3%
5	Win32/Obfuscator	Obfuscators & Injectors	0.8%
6	Win32/Conficker	Worms	0.7%
7	Win32/Ramnit	Trojans	0.7%
8	Win32/Sality	Viruses	0.7%
9	Win32/Vermis	Worms	0.7%
10	Win32/CplLnk	Exploits	0.6%

- The most common malware family encountered in Colombia in 4Q14 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 Colombia in 4Q14 was JS/Bondat, which was encountered by 3.2 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 third most common malware family encountered in Colombia in 4Q14 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 Colombia in 4Q14 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 Colombia in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	2.8%
2	Win32/Defaulttab	Browser Modifiers	0.9%
3	Win32/BetterSurf	Adware	0.8%
4	Win32/Costmin	Adware	0.7%
5	Win32/Pennybee	Adware	0.7%

- The most common unwanted software family encountered in Colombia in 4Q14 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 second most common unwanted software family encountered in Colombia in 4Q14 was Win32/Defaulttab, which was encountered by 0.9 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.
- The third most common unwanted software family encountered in Colombia in 4Q14 was Win32/BetterSurf, which was encountered by 0.8 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.

Top threat families by infection rate

The most common malware families by infection rate in Colombia in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	5.6
2	Win32/Sality	Viruses	1.1
3	Win32/Ramnit	Trojans	0.7
4	Win32/Gamarue	Worms	0.6
5	Win32/Sefnit	Trojans	0.4
6	MSIL/Spacekito	Trojans	0.4
7	Win32/Wysotot	Trojans	0.3
8	Win32/Dorkbot	Worms	0.3
9	Win32/Brontok	Worms	0.2
10	MSIL/Bladabindi	Backdoors	0.2

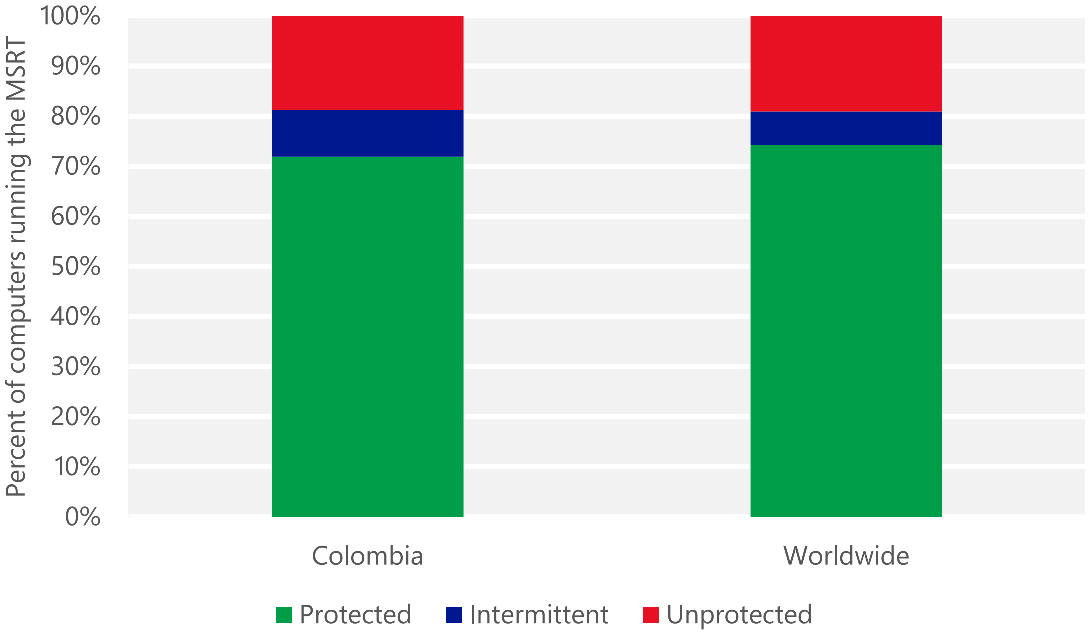
- The most common threat family infecting computers in Colombia in 4Q14 was VBS/Jenxcus, which was detected and removed from 5.6 of every 1,000 unique computers scanned by the MSRT. VBS/Jenxcus is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Colombia in 4Q14 was Win32/Sality, which was detected and removed from 1.1 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 Colombia in 4Q14 was Win32/Ramnit, which was detected and removed from 0.7 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 Colombia in 4Q14 was Win32/Gamarue, which was detected and removed from 0.6 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.

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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.11 drive-by download URLs for every 1,000 URLs hosted in Colombia, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.09 drive-by download URLs for every 1,000 URLs hosted in Colombia, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Colombia and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Colombia	0.11	0.09
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Costa Rica

The statistics presented here are generated by Microsoft security programs and services running on computers in Costa Rica in 4Q14 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 succeds 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

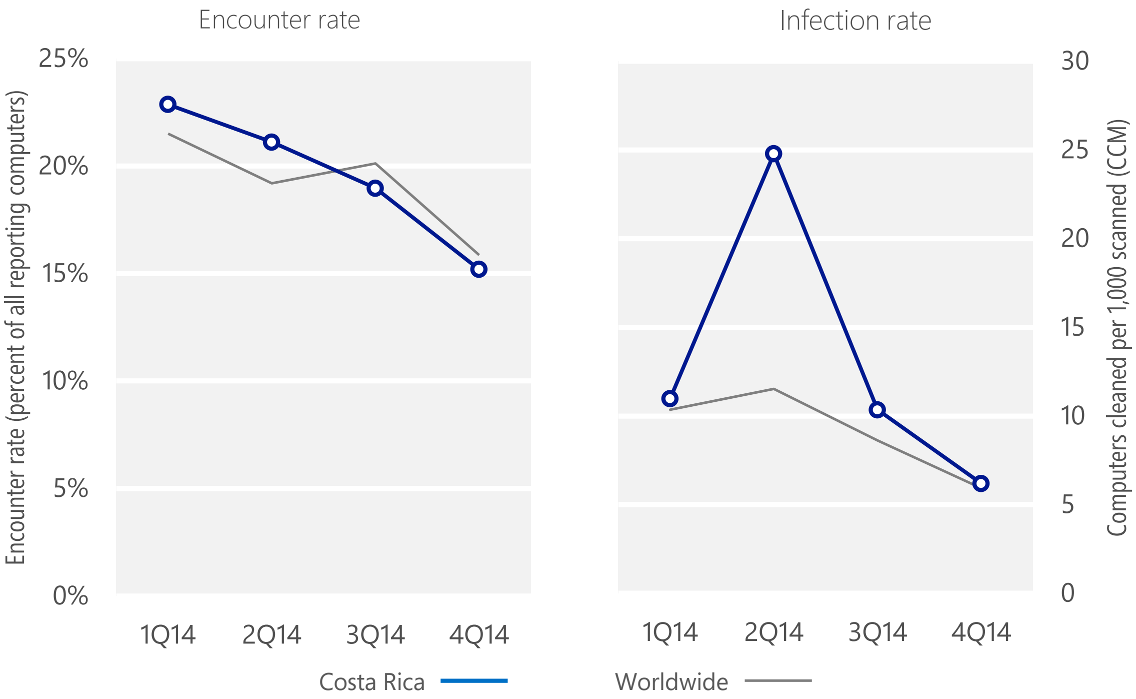
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Costa Rica	22.9%	21.1%	19.0%	15.2%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Costa Rica	11.0	24.8	10.3	6.2
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 15.2% percent of computers in Costa Rica encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 6.2 of every 1,000 unique computers scanned in Costa Rica in 4Q14 (a CCM score of 6.2, compared to the 4Q14 worldwide CCM of 5.9). 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.

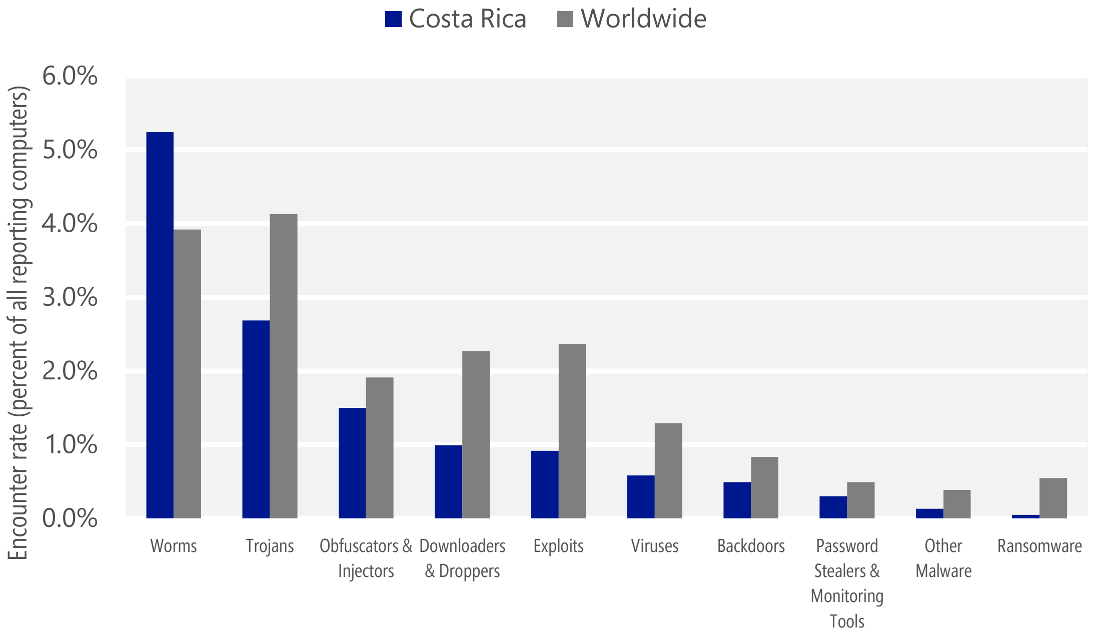
Malware encounter and infection rate trends in Costa Rica and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

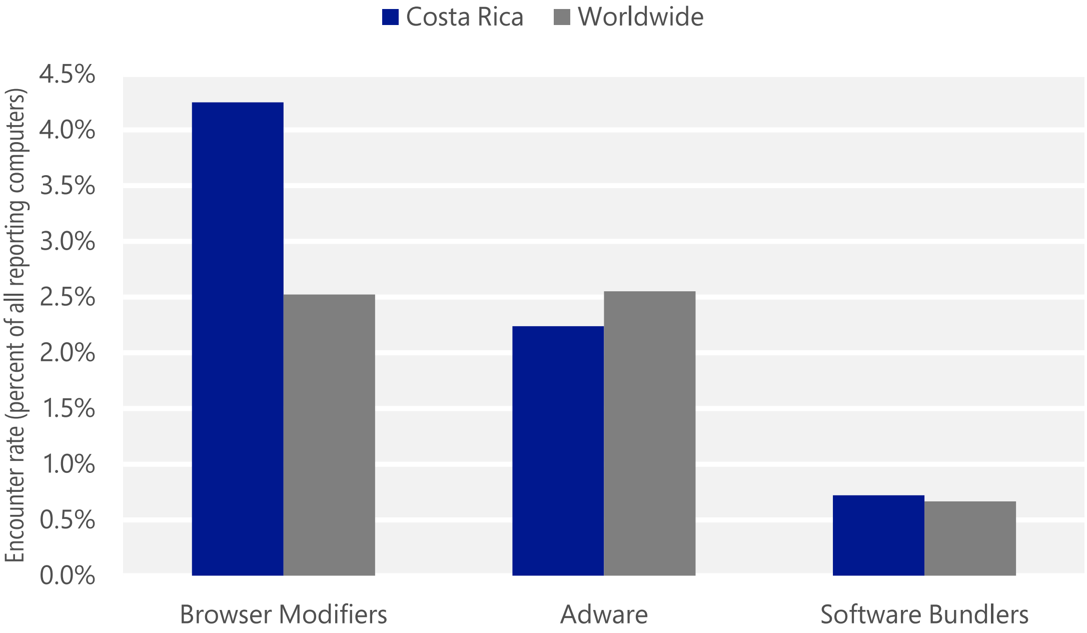
Malware encountered in Costa Rica in 4Q14, by category



- The most common malware category in Costa Rica in 4Q14 was Worms. It was encountered by 5.2 percent of all computers there, down from 7.2 percent in 3Q14.
- The second most common malware category in Costa Rica in 4Q14 was Trojans. It was encountered by 2.7 percent of all computers there, down from 5.1 percent in 3Q14.
- The third most common malware category in Costa Rica in 4Q14 was Obfuscators & Injectors, which was encountered by 1.5 percent of all computers there, down from 2.2 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Costa Rica in 4Q14, by category



- The most common unwanted software category in Costa Rica in 4Q14 was Browser Modifiers. It was encountered by 4.2 percent of all computers there, down from 5.1 percent in 3Q14.

- The second most common unwanted software category in Costa Rica in 4Q14 was Adware. It was encountered by 2.2 percent of all computers there, up from 0.7 percent in 3Q14.

- The third most common unwanted software category in Costa Rica in 4Q14 was Software Bundlers, which was encountered by 0.7 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Costa Rica in 4Q14

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	3.2%
2	INF/Autorun	Obfuscators & Injectors	0.7%
3	Win32/Obfuscator	Obfuscators & Injectors	0.7%
4	JS/Proslikefan	Worms	0.6%

- The most common malware family encountered in Costa Rica in 4Q14 was VBS/Jenxcus, which was encountered by 3.2 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 4Q14 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 Costa Rica in 4Q14 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 Costa Rica in 4Q14 was JS/Proslikefan, which was encountered by 0.6 percent of reporting computers there. JS/Proslikefan is a worm that spreads through removable drives, network shares, and P2P programs. It can lower the computer's security settings and disable antivirus products.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Costa Rica in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	3.3%
2	Win32/BetterSurf	Adware	1.1%
3	Win32/Defaulttab	Browser Modifiers	1.1%
4	Win32/Costmin	Adware	0.8%

- The most common unwanted software family encountered in Costa Rica in 4Q14 was Win32/Couponruc, which was encountered by 3.3 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 Costa Rica in 4Q14 was Win32/BetterSurf, which was encountered by 1.1 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.
- The third most common unwanted software family encountered in Costa Rica in 4Q14 was Win32/Defaulttab, which was encountered by 1.1 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.

Top threat families by infection rate

The most common malware families by infection rate in Costa Rica in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	3.3
2	Win32/Sefnit	Trojans	0.4
3	MSIL/Spacekito	Trojans	0.4
4	Win32/Sality	Viruses	0.3
5	Win32/Conficker	Worms	0.2
6	Win32/Brontok	Worms	0.2
7	Win32/Dorkbot	Worms	0.2
8	Win32/Vobfus	Worms	0.1
9	MSIL/Bladabindi	Backdoors	0.1
10	Win32/Ramnit	Trojans	0.1

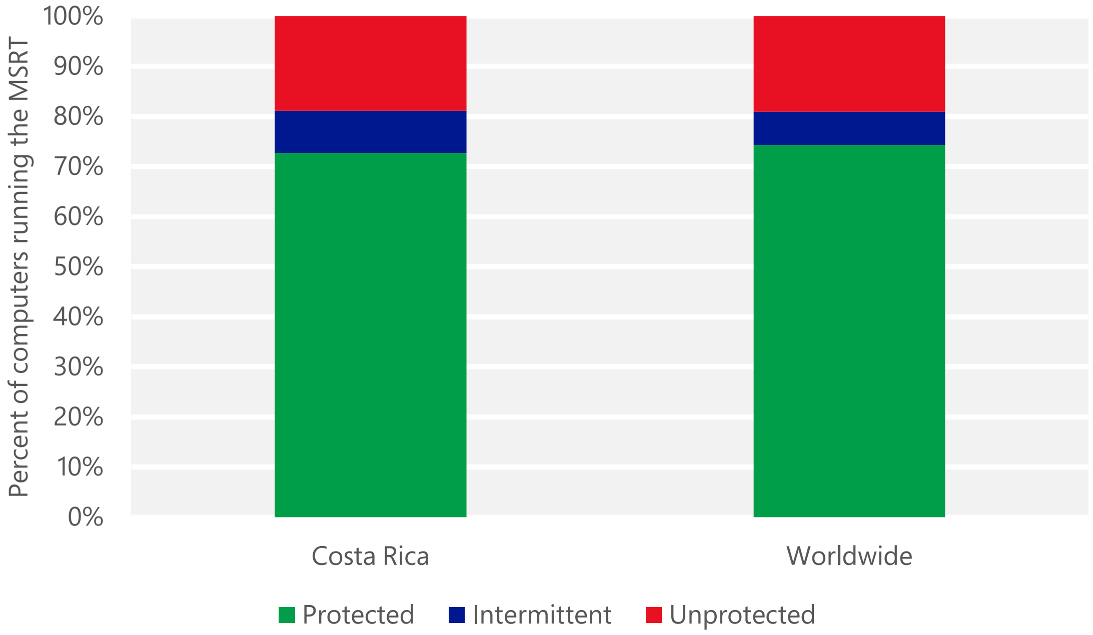
- The most common threat family infecting computers in Costa Rica in 4Q14 was VBS/Jenxcus, which was detected and removed from 3.3 of every 1,000 unique computers scanned by the MSRT. VBS/Jenxcus is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Costa Rica in 4Q14 was Win32/Sefnit, which was detected and removed from 0.4 of every 1,000 unique computers scanned by the MSRT. Win32/Sefnit is a family of trojans that can allow backdoor access, download files, and use the computer and Internet connection for click fraud. Some variants can monitor web browsers and hijack search results.
- The third most common threat family infecting computers in Costa Rica in 4Q14 was MSIL/Spacekito, which was detected and removed from 0.4 of every 1,000 unique computers scanned by the MSRT. MSIL/Spacekito is a threat that steals information about the computer and installs browser add-ons that display ads.
- The fourth most common threat family infecting computers in Costa Rica in 4Q14 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 Costa Rica and worldwide protected by real-time security software in 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.09 drive-by download URLs for every 1,000 URLs hosted in Costa Rica, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.05 drive-by download URLs for every 1,000 URLs hosted in Costa Rica, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Costa Rica and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Costa Rica	0.09	0.05
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Croatia

The statistics presented here are generated by Microsoft security programs and services running on computers in Croatia in 4Q14 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 succeds 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

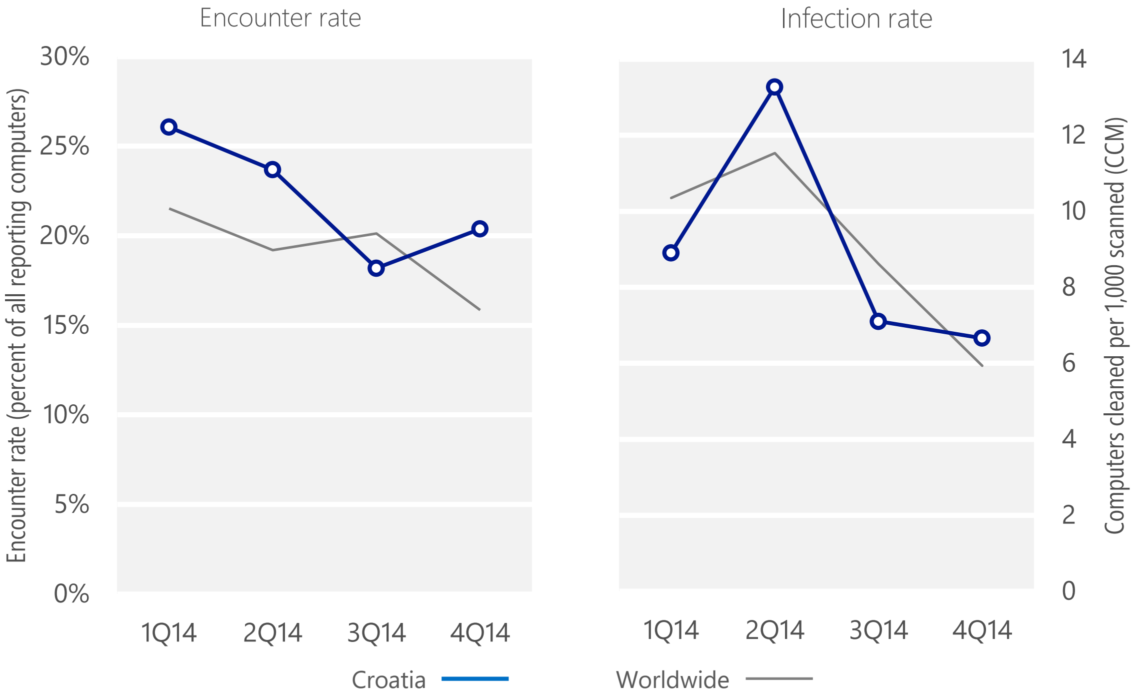
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Croatia	26.1%	23.7%	18.2%	20.4%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Croatia	8.9	13.3	7.1	6.7
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 20.4% percent of computers in Croatia encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 6.7 of every 1,000 unique computers scanned in Croatia in 4Q14 (a CCM score of 6.7, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Croatia over the last four quarters, compared to the world as a whole.

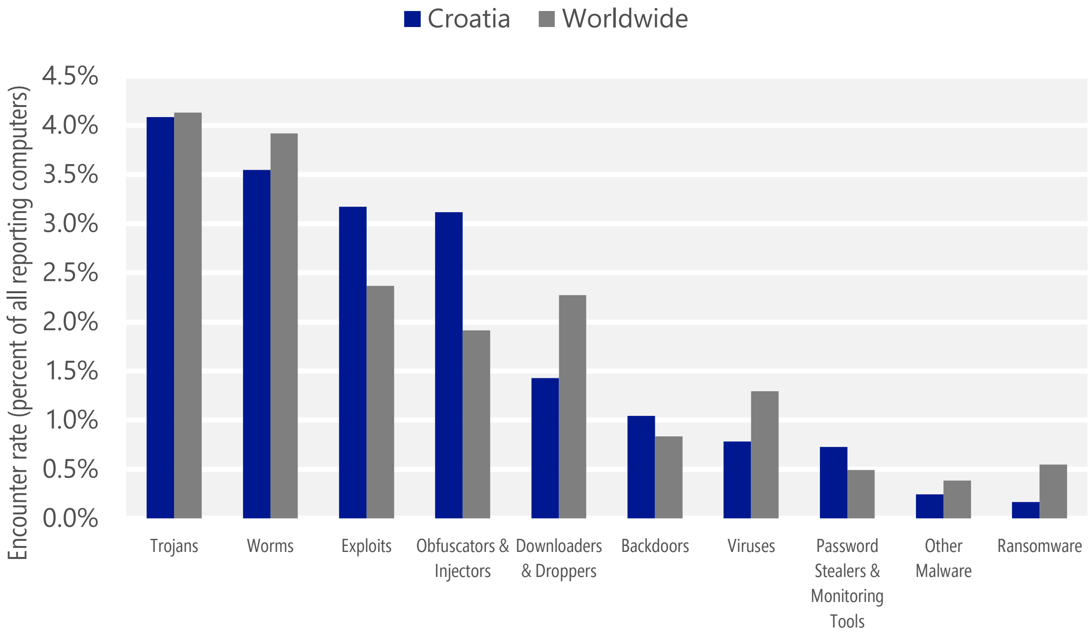
Malware encounter and infection rate trends in Croatia and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

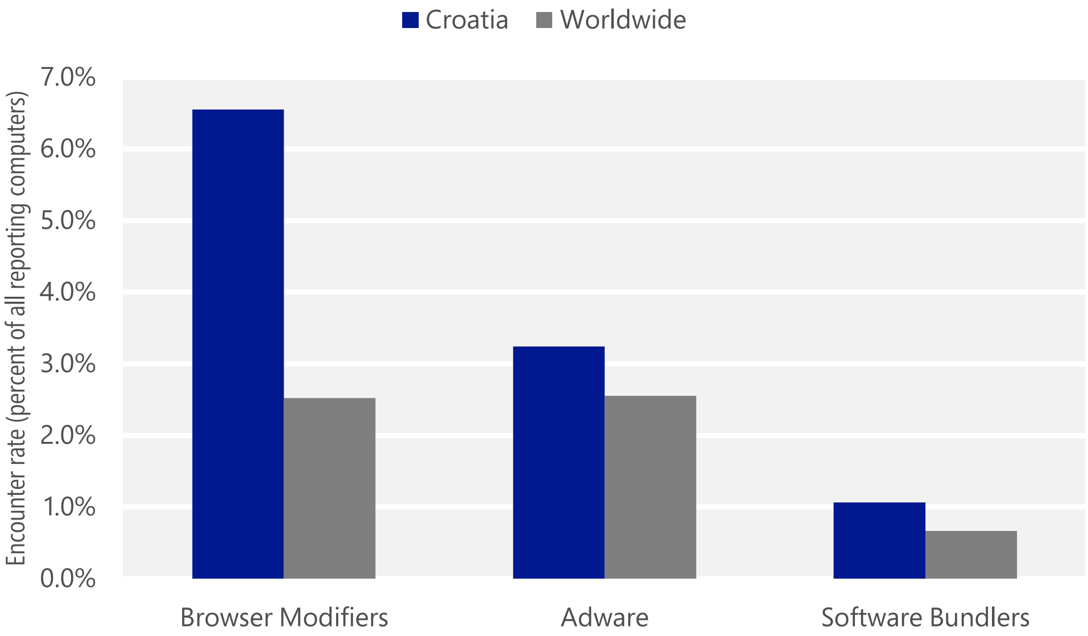
Malware encountered in Croatia in 4Q14, by category



- The most common malware category in Croatia in 4Q14 was Trojans. It was encountered by 4.1 percent of all computers there, down from 5.5 percent in 3Q14.
- The second most common malware category in Croatia in 4Q14 was Worms. It was encountered by 3.5 percent of all computers there, up from 3.1 percent in 3Q14.
- The third most common malware category in Croatia in 4Q14 was Exploits, which was encountered by 3.2 percent of all computers there, up from 2.9 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Croatia in 4Q14, by category



- The most common unwanted software category in Croatia in 4Q14 was Browser Modifiers. It was encountered by 6.5 percent of all computers there, up from 6.5 percent in 3Q14.
- The second most common unwanted software category in Croatia in 4Q14 was Adware. It was encountered by 3.2 percent of all computers there, up from 0.5 percent in 3Q14.
- The third most common unwanted software category in Croatia in 4Q14 was Software Bundlers, which was encountered by 1.1 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Croatia in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Obfuscator	Obfuscators & Injectors	2.1%
2	Win32/Anogre	Exploits	1.8%
3	JS/Axpergle	Exploits	1.0%
4	INF/Autorun	Obfuscators & Injectors	0.9%
5	Win32/Gamarue	Worms	0.8%
6	Win32/Conficker	Worms	0.6%
7	VBS/Jenxcus	Worms	0.5%
8	Win32/Dynamer	Trojans	0.4%
9	Win32/Helompy	Worms	0.4%
10	Win32/Brontok	Worms	0.4%

- The most common malware family encountered in Croatia in 4Q14 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 Croatia in 4Q14 was Win32/Anogre, which was encountered by 1.8 percent of reporting computers there. Win32/Anogre is a threat that exploits a vulnerability addressed by Microsoft Security Bulletin MS11-087. This vulnerability can allow a hacker to install programs, view, change, or delete data or create new accounts with full administrative privileges.
- The third most common malware family encountered in Croatia in 4Q14 was JS/Axpergle, which was encountered by 1.0 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 Croatia in 4Q14 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 Croatia in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	4.6%
2	Win32/Defaulttab	Browser Modifiers	2.3%
3	Win32/Costmin	Adware	1.7%
4	Win32/BetterSurf	Adware	1.3%
5	Win32/Gofileexpress	Software Bundlers	0.8%

- The most common unwanted software family encountered in Croatia in 4Q14 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 second most common unwanted software family encountered in Croatia in 4Q14 was Win32/Defaulttab, which was encountered by 2.3 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.

- The third most common unwanted software family encountered in Croatia in 4Q14 was Win32/Costmin, which was encountered by 1.7 percent of reporting computers there. Win32/Costmin is an adware family that installs itself as a browser extension for Internet Explorer, Mozilla Firefox, and Google Chrome, and displays advertisements as the user browses the Internet.

Top threat families by infection rate

The most common malware families by infection rate in Croatia in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	JS/Kilim	Trojans	1.3
2	Win32/Sality	Viruses	0.8
3	Win32/Helompy	Worms	0.6
4	VBS/Jenxcus	Worms	0.6
5	Win32/Brontok	Worms	0.6
6	Win32/Gamarue	Worms	0.4
7	Win32/Zbot	Password Stealers & Monitoring Tools	0.3
8	Win32/Sefnit	Trojans	0.3
9	MSIL/Bladabindi	Backdoors	0.2
10	JS/Miuref	Trojans	0.2

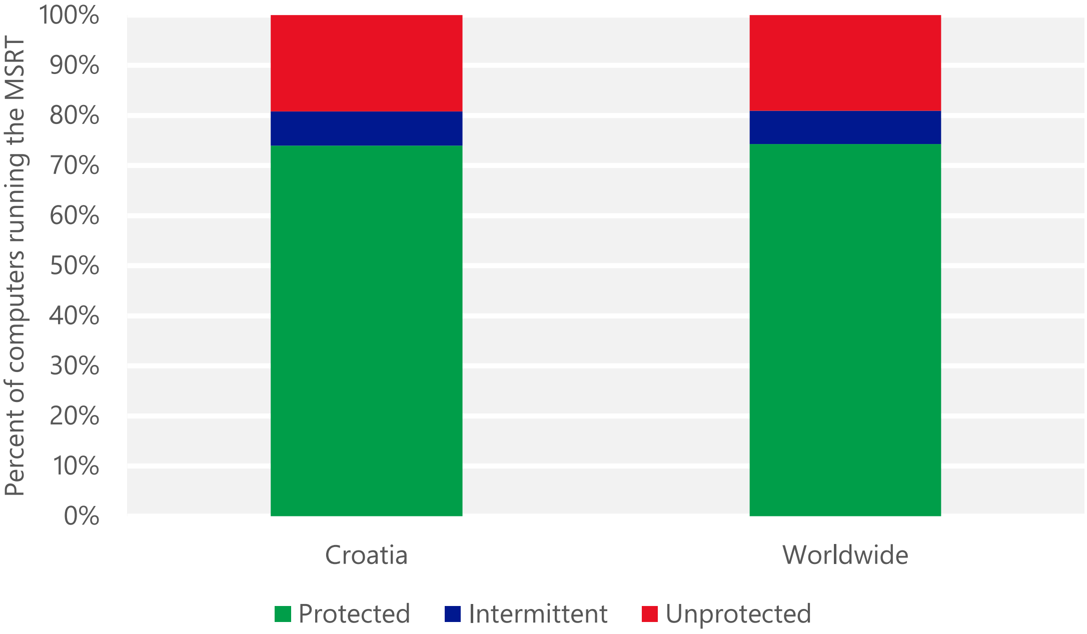
- The most common threat family infecting computers in Croatia in 4Q14 was JS/Kilim, which was detected and removed from 1.3 of every 1,000 unique computers scanned by the MSRT. JS/Kilim is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks 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 threat family infecting computers in Croatia in 4Q14 was Win32/Sality, which was detected and removed from 0.8 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 third most common threat family infecting computers in Croatia in 4Q14 was Win32/Helompy, which was detected and removed from 0.6 of every 1,000 unique computers scanned by the MSRT. Win32/Helompy is a worm that spreads via removable drives and attempts to capture and steal authentication details for a number of different websites or online services.
- The fourth most common threat family infecting computers in Croatia in 4Q14 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 Croatia and worldwide protected by real-time security software in 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.21 drive-by download URLs for every 1,000 URLs hosted in Croatia, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.14 drive-by download URLs for every 1,000 URLs hosted in Croatia, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Croatia and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Croatia	0.21	0.14
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Cyprus

The statistics presented here are generated by Microsoft security programs and services running on computers in Cyprus in 4Q14 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 succeds 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

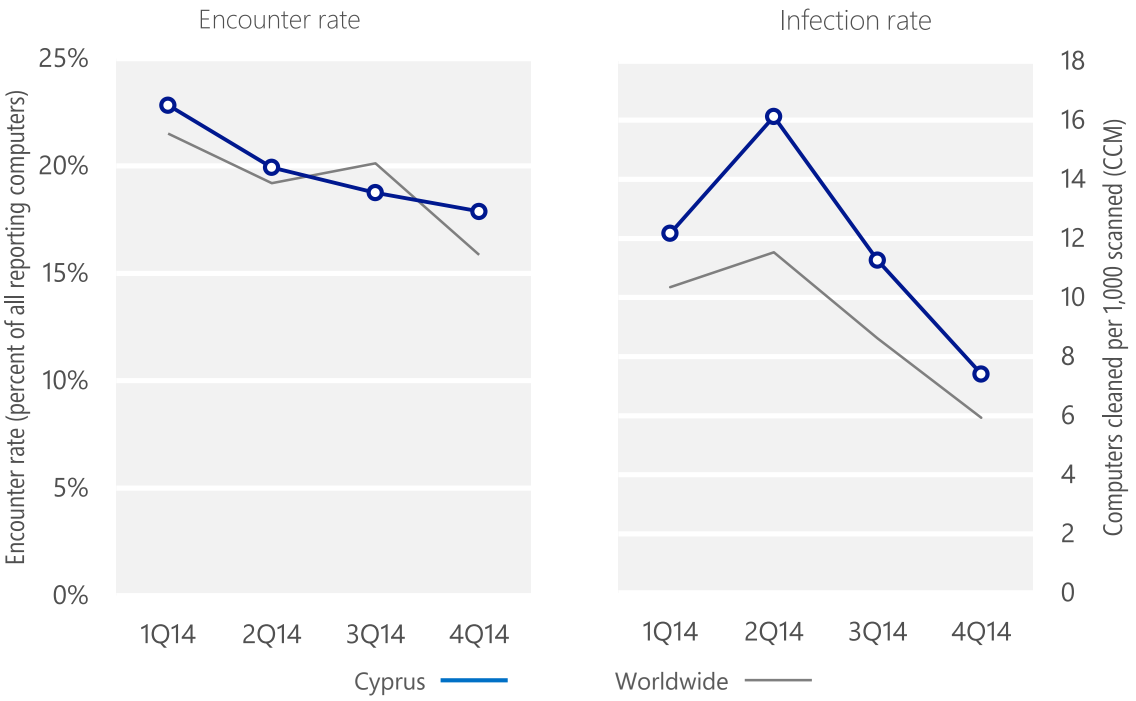
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Cyprus	22.8%	19.9%	18.8%	17.9%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Cyprus	12.2	16.1	11.3	7.4
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 17.9% percent of computers in Cyprus encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 7.4 of every 1,000 unique computers scanned in Cyprus in 4Q14 (a CCM score of 7.4, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Cyprus over the last four quarters, compared to the world as a whole.

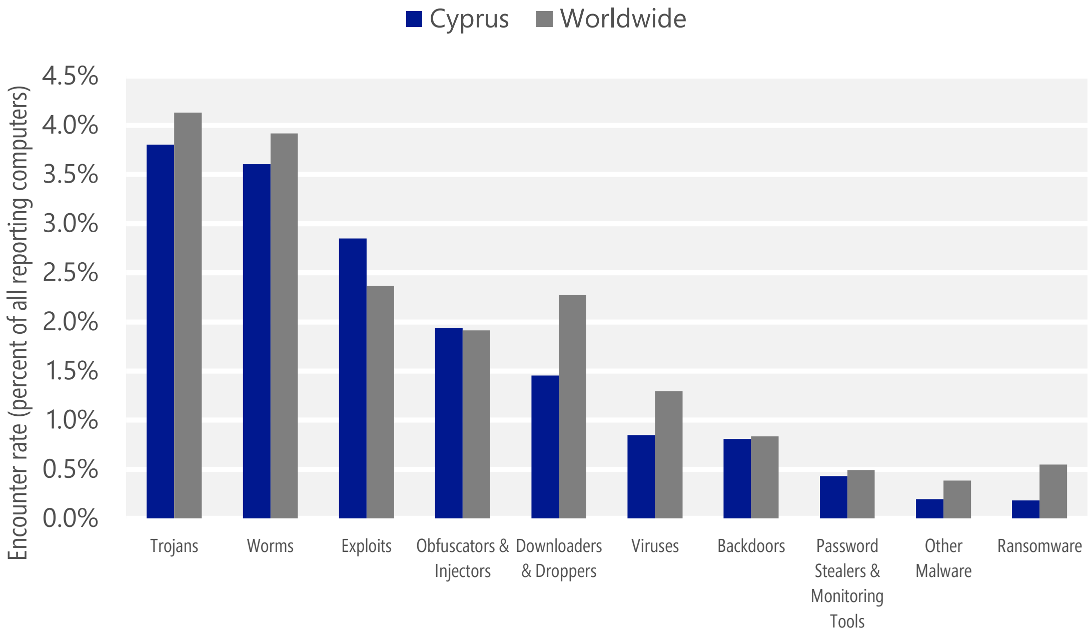
Malware encounter and infection rate trends in Cyprus and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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 4Q14, by category



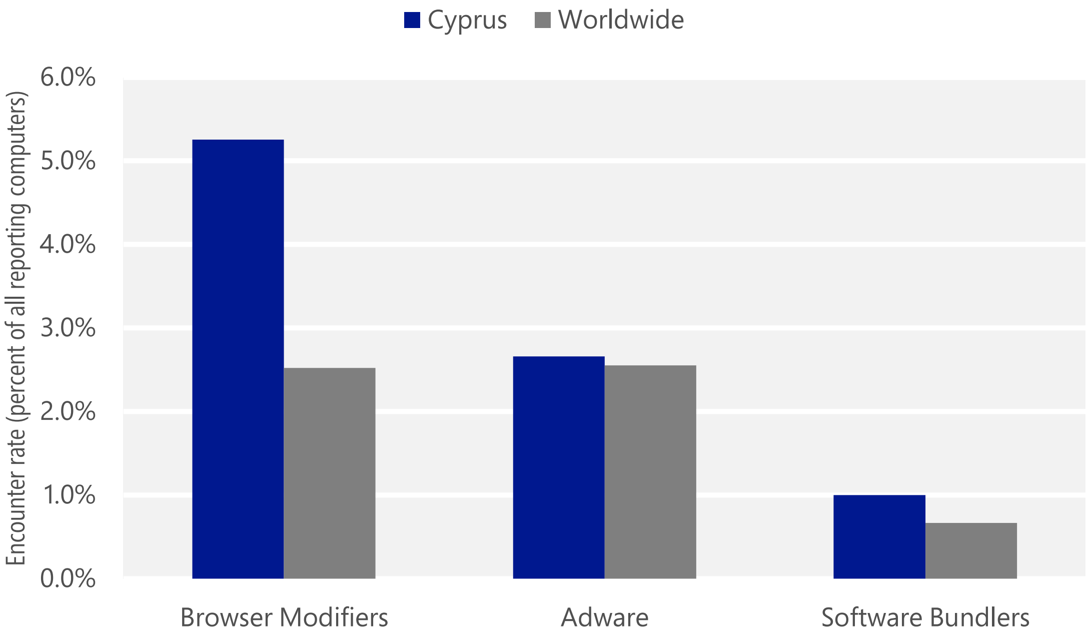
- The most common malware category in Cyprus in 4Q14 was Trojans. It was encountered by 3.8 percent of all computers there, down from 5.7 percent in 3Q14.

- The second most common malware category in Cyprus in 4Q14 was Worms. It was encountered by 3.6 percent of all computers there, up from 3.6 percent in 3Q14.

- The third most common malware category in Cyprus in 4Q14 was Exploits, which was encountered by 2.8 percent of all computers there, down from 2.9 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Cyprus in 4Q14, by category



- The most common unwanted software category in Cyprus in 4Q14 was Browser Modifiers. It was encountered by 5.3 percent of all computers there, down from 5.8 percent in 3Q14.
- The second most common unwanted software category in Cyprus in 4Q14 was Adware. It was encountered by 2.7 percent of all computers there, up from 1.1 percent in 3Q14.
- The third most common unwanted software category in Cyprus in 4Q14 was Software Bundlers, which was encountered by 1.0 percent of all computers there, up from 0.2 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Cyprus in 4Q14

	Family	Most significant category	% of reporting computers
1	JS/Axpergle	Exploits	2.0%
2	INF/Autorun	Obfuscators & Injectors	1.3%
3	Win32/Obfuscator	Obfuscators & Injectors	1.0%
4	Win32/Gamarue	Worms	0.9%

- The most common malware family encountered in Cyprus in 4Q14 was JS/Axpergle, which was encountered by 2.0 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 Cyprus in 4Q14 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 Cyprus in 4Q14 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.
- The fourth most common malware family encountered in Cyprus in 4Q14 was Win32/Gamarue, which was encountered by 0.9 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.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Cyprus in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	3.8%
2	Win32/Defaulttab	Browser Modifiers	1.7%
3	Win32/Costmin	Adware	1.1%
4	Win32/BetterSurf	Adware	1.1%
5	Win32/Gofileexpress	Software Bundlers	0.7%

- The most common unwanted software family encountered in Cyprus in 4Q14 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 Cyprus in 4Q14 was Win32/Defaulttab, which was encountered by 1.7 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.
- The third most common unwanted software family encountered in Cyprus in 4Q14 was Win32/Costmin, which was encountered by 1.1 percent of reporting computers there. Win32/Costmin is an adware family that installs itself as a browser extension for Internet Explorer, Mozilla Firefox, and Google Chrome, and displays advertisements as the user browses the Internet.

Top threat families by infection rate

The most common malware families by infection rate in Cyprus in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Gamarue	Worms	1.1
2	Win32/Sality	Viruses	0.8
3	VBS/Jenxcus	Worms	0.7
4	JS/Kilim	Trojans	0.6
5	Win32/Brontok	Worms	0.5
6	Win32/Sefnit	Trojans	0.4
7	Win32/Ramnit	Trojans	0.4
8	Win32/Wysotot	Trojans	0.3
9	MSIL/Bladabindi	Backdoors	0.3
10	Win32/Zbot	Password Stealers & Monitoring Tools	0.2

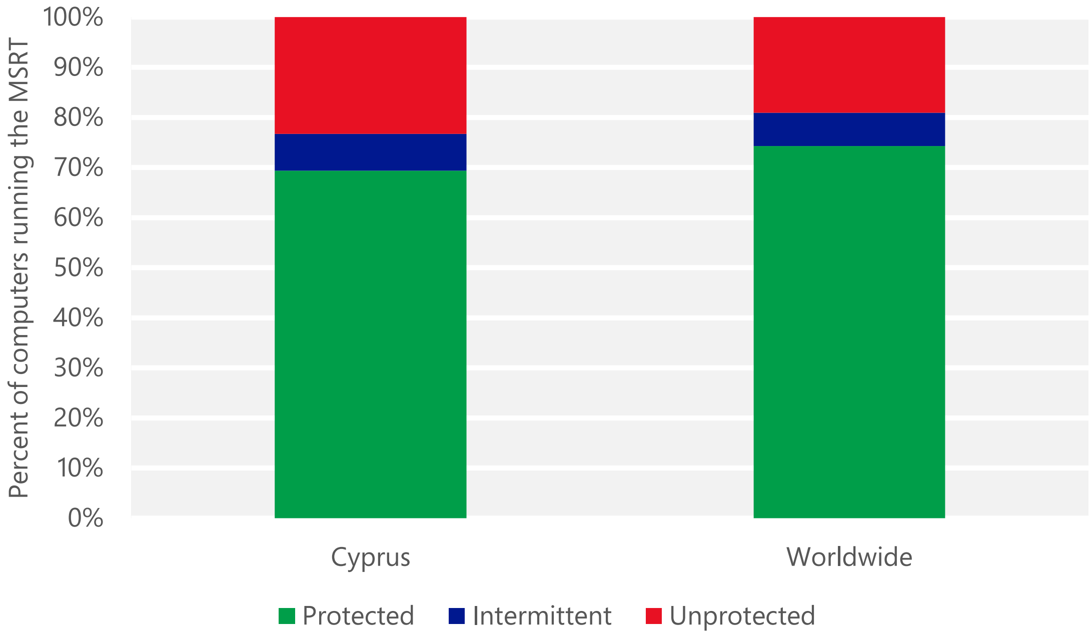
- The most common threat family infecting computers in Cyprus in 4Q14 was Win32/Gamarue, which was detected and removed from 1.1 of every 1,000 unique computers scanned by the MSRT. Win32/Gamarue is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The second most common threat family infecting computers in Cyprus in 4Q14 was Win32/Sality, which was detected and removed from 0.8 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 third most common threat family infecting computers in Cyprus in 4Q14 was VBS/Jenxcus, which was detected and removed from 0.7 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 Cyprus in 4Q14 was JS/Kilim, which was detected and removed from 0.6 of every 1,000 unique computers scanned by the MSRT. JS/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 Cyprus and worldwide protected by real-time security software in 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 1.45 drive-by download URLs for every 1,000 URLs hosted in Cyprus, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 1.29 drive-by download URLs for every 1,000 URLs hosted in Cyprus, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Cyprus and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Cyprus	1.45	1.29
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Czech Republic

The statistics presented here are generated by Microsoft security programs and services running on computers in the Czech Republic in 4Q14 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 succeds 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

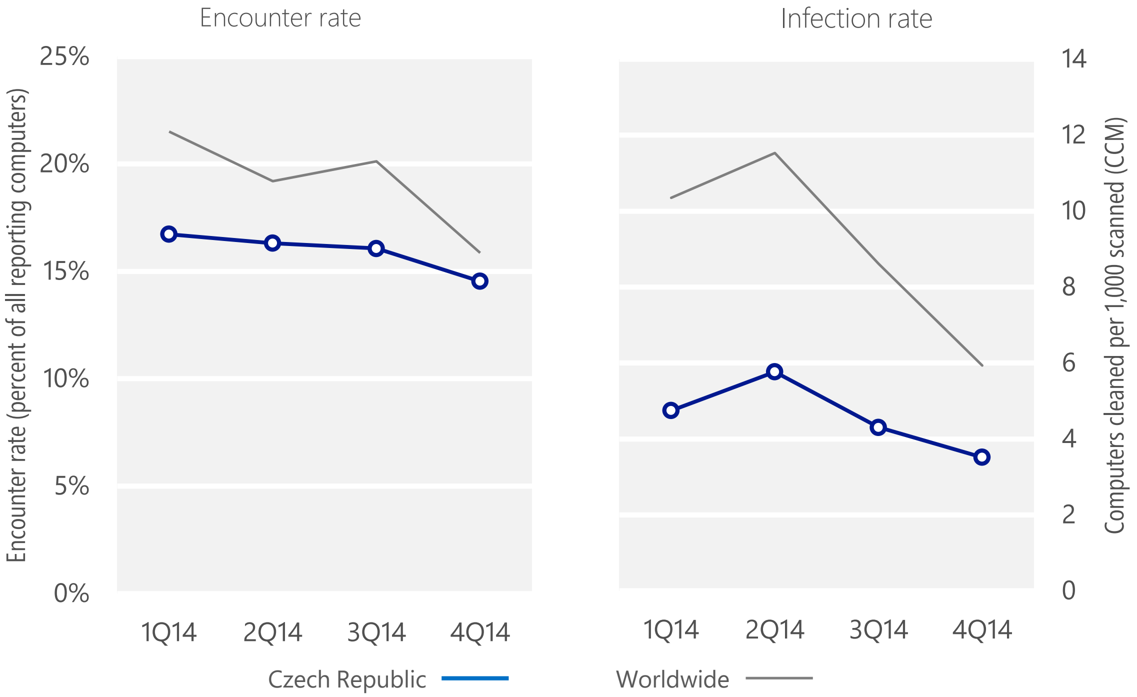
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Czech Republic	16.7%	16.3%	16.1%	14.5%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Czech Republic	4.7	5.8	4.3	3.5
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 14.5% percent of computers in the Czech Republic encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 3.5 of every 1,000 unique computers scanned in the Czech Republic in 4Q14 (a CCM score of 3.5, compared to the 4Q14 worldwide CCM of 5.9). 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.

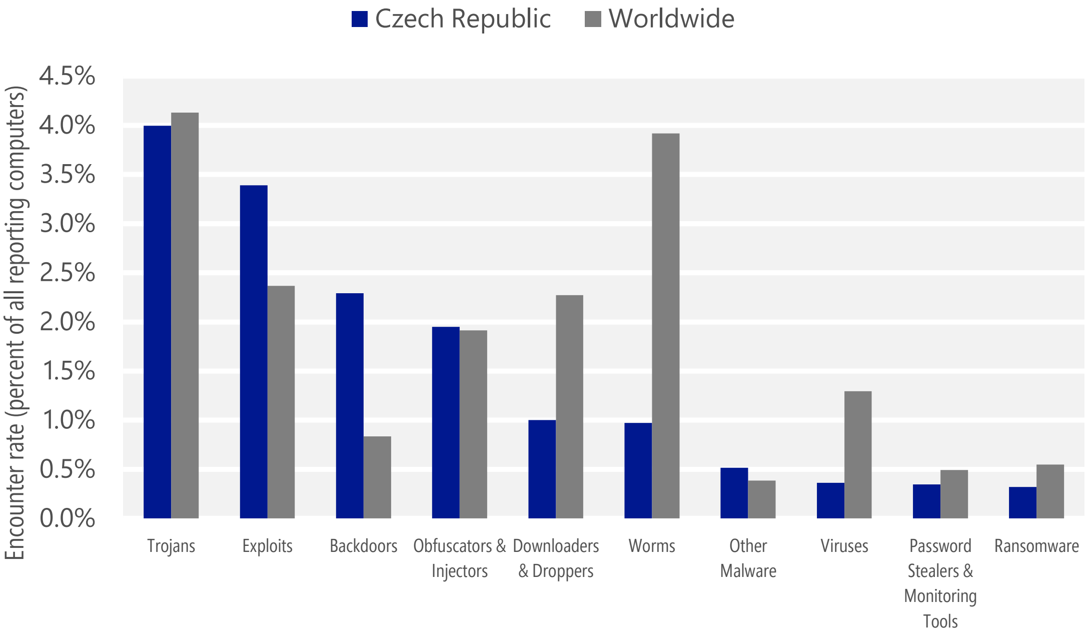
Malware encounter and infection rate trends in the Czech Republic and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

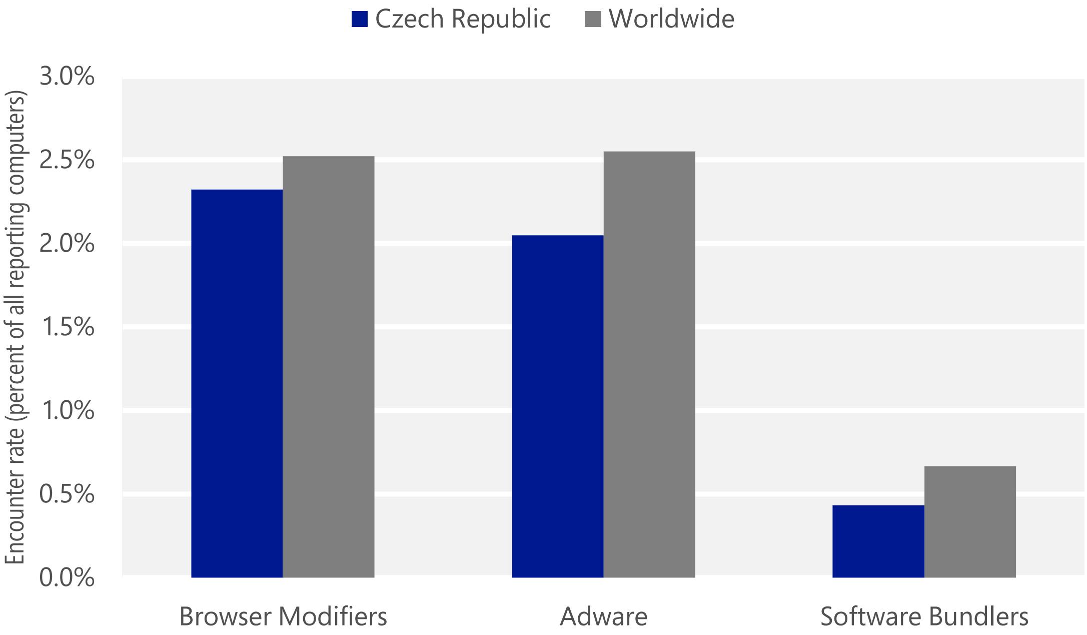
Malware encountered in the Czech Republic in 4Q14, by category



- The most common malware category in the Czech Republic in 4Q14 was Trojans. It was encountered by 4.0 percent of all computers there, down from 5.4 percent in 3Q14.
- The second most common malware category in the Czech Republic in 4Q14 was Exploits. It was encountered by 3.4 percent of all computers there, up from 3.2 percent in 3Q14.
- The third most common malware category in the Czech Republic in 4Q14 was Backdoors, which was encountered by 2.3 percent of all computers there, down from 2.7 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in the Czech Republic in 4Q14, by category



- The most common unwanted software category in the Czech Republic in 4Q14 was Browser Modifiers. It was encountered by 2.3 percent of all computers there, down from 4.0 percent in 3Q14.
- The second most common unwanted software category in the Czech Republic in 4Q14 was Adware. It was encountered by 2.0 percent of all computers there, up from 0.3 percent in 3Q14.
- The third most common unwanted software category in the Czech Republic in 4Q14 was Software Bundlers, which was encountered by 0.4 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in the Czech Republic in 4Q14

	Family	Most significant category	% of reporting computers
1	MSIL/Bladabindi	Backdoors	1.8%
2	Win32/Anogre	Exploits	1.7%
3	Win32/Obfuscator	Obfuscators & Injectors	1.6%
4	JS/Axpergle	Exploits	1.4%
5	JS/Faceliker	Trojans	0.6%
6	Win32/Dynamer	Trojans	0.5%
7	JS/Iframe	Trojans	0.4%
8	Win32/Anaki	Trojans	0.3%
9	VBS/Jenxcus	Worms	0.3%
10	Win32/Dalexis	Downloaders & Droppers	0.3%

- The most common malware family encountered in the Czech Republic in 4Q14 was MSIL/Bladabindi, which was encountered by 1.8 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 second most common malware family encountered in the Czech Republic in 4Q14 was Win32/Anogre, which was encountered by 1.7 percent of reporting computers there. Win32/Anogre is a threat that exploits a vulnerability addressed by Microsoft Security Bulletin MS11-087. This vulnerability can allow a hacker to install programs, view, change, or delete data or create new accounts with full administrative privileges.
- The third most common malware family encountered in the Czech Republic in 4Q14 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 4Q14 was JS/Axpergle, which was encountered by 1.4 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 the Czech Republic in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	1.8%
2	Win32/BetterSurf	Adware	1.2%
3	Win32/Costmin	Adware	0.6%
4	Win32/Defaulttab	Browser Modifiers	0.6%
5	Win32/Gofileexpress	Software Bundlers	0.3%

- The most common unwanted software family encountered in the Czech Republic in 4Q14 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 the Czech Republic in 4Q14 was Win32/BetterSurf, which was encountered by 1.2 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.
- The third most common unwanted software family encountered in the Czech Republic in 4Q14 was Win32/Costmin, which was encountered by 0.6 percent of reporting computers there. Win32/Costmin is an adware family that installs itself as a browser extension for Internet Explorer, Mozilla Firefox, and Google Chrome, and displays advertisements as the user browses the Internet.

Top threat families by infection rate

The most common malware families by infection rate in the Czech Republic in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	MSIL/Bladabindi	Backdoors	1.3
2	JS/Kilim	Trojans	0.7
3	VBS/Jenxcus	Worms	0.3
4	Win32/Sality	Viruses	0.2
5	Win32/Brontok	Worms	0.1
6	Win32/Sefnit	Trojans	0.1
7	Win32/Ramnit	Trojans	0.1
8	Win32/Gamarue	Worms	0.1
9	Win32/Wysotot	Trojans	0.1
10	Win32/Zbot	Password Stealers & Monitoring Tools	0.1

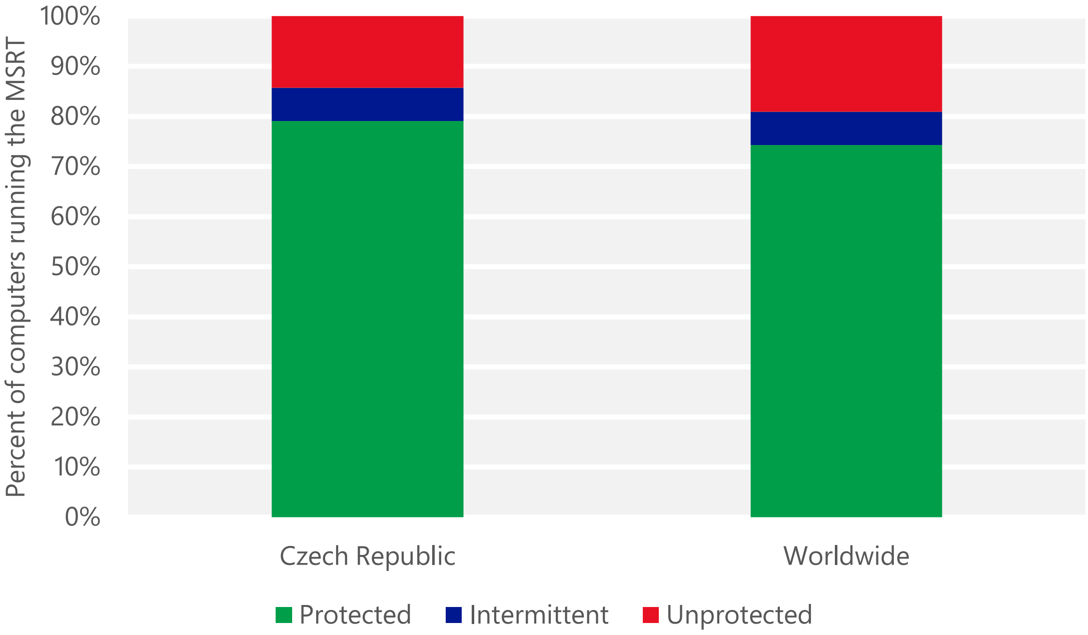
- The most common threat family infecting computers in the Czech Republic in 4Q14 was MSIL/Bladabindi, which was detected and removed from 1.3 of every 1,000 unique computers scanned by the MSRT. MSIL/Bladabindi is a family of backdoors created by a malicious hacker tool called NJ Rat. The can steal sensitive information, download other malware, and allow backdoor access to an infected computer.
- The second most common threat family infecting computers in the Czech Republic in 4Q14 was JS/Kilim, which was detected and removed from 0.7 of every 1,000 unique computers scanned by the MSRT. JS/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 Czech Republic in 4Q14 was VBS/Jenxcus, which was detected and removed from 0.3 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 Czech Republic in 4Q14 was Win32/Sality, which was detected and removed from 0.2 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 the Czech Republic and worldwide protected by real-time security software in 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.24 drive-by download URLs for every 1,000 URLs hosted in the Czech Republic, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.40 drive-by download URLs for every 1,000 URLs hosted in the Czech Republic, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in the Czech Republic and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Czech Republic	0.24	0.40
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Denmark

The statistics presented here are generated by Microsoft security programs and services running on computers in Denmark in 4Q14 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 succeds 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

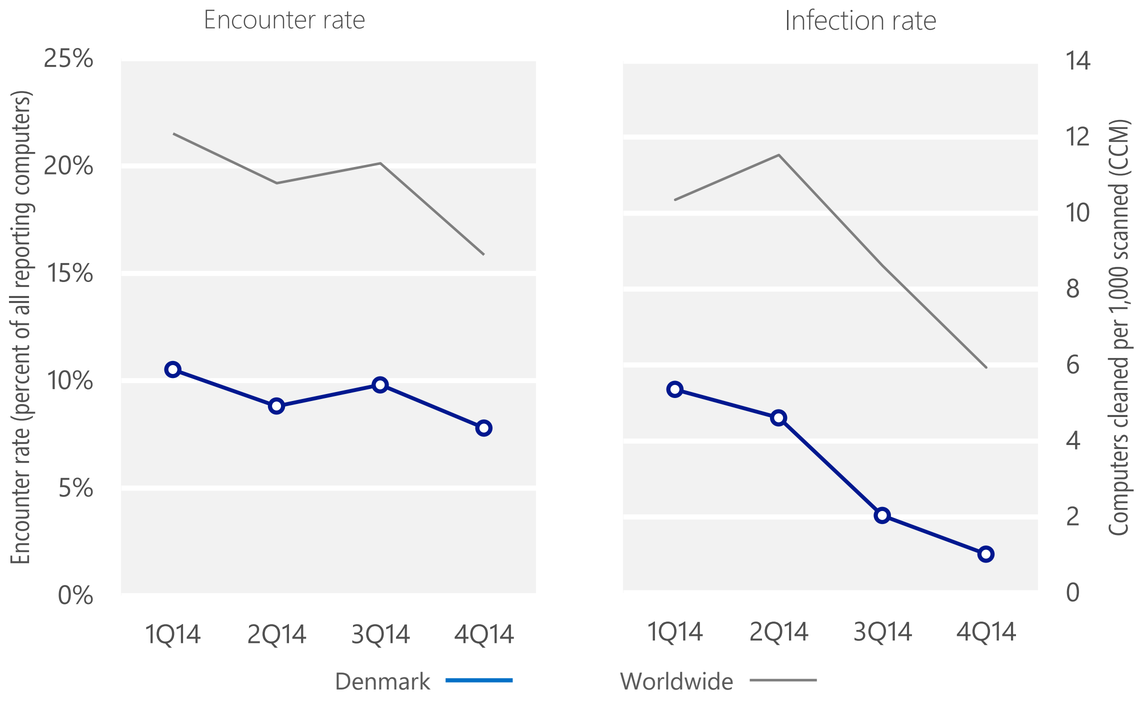
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Denmark	10.5%	8.8%	9.8%	7.8%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Denmark	5.4	4.6	2.0	1.0
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 7.8% percent of computers in Denmark encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 1.0 of every 1,000 unique computers scanned in Denmark in 4Q14 (a CCM score of 1.0, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Denmark over the last four quarters, compared to the world as a whole.

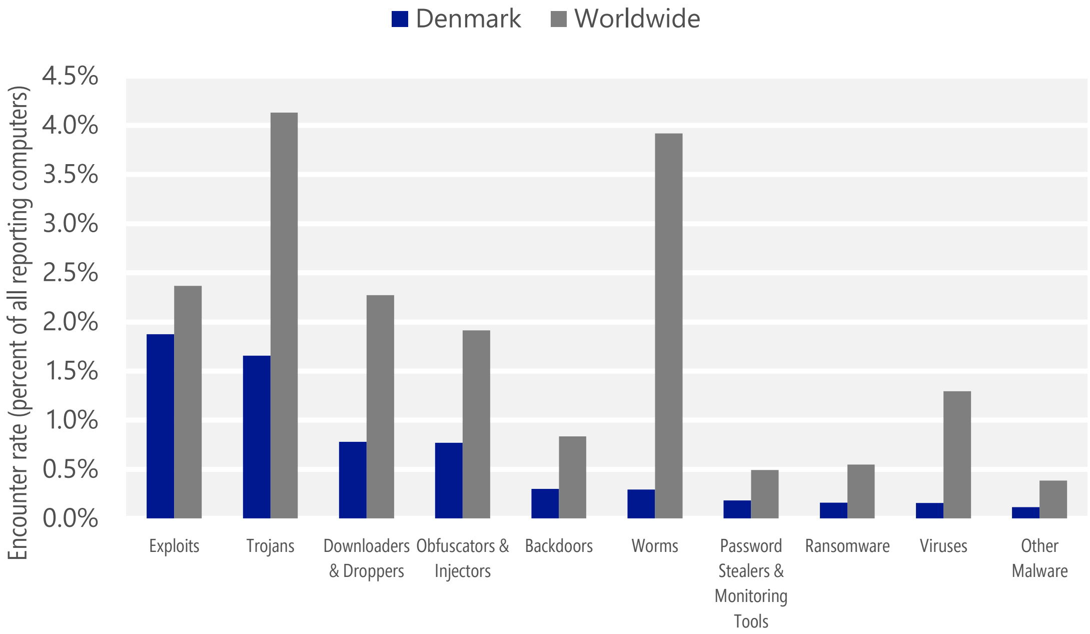
Malware encounter and infection rate trends in Denmark and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

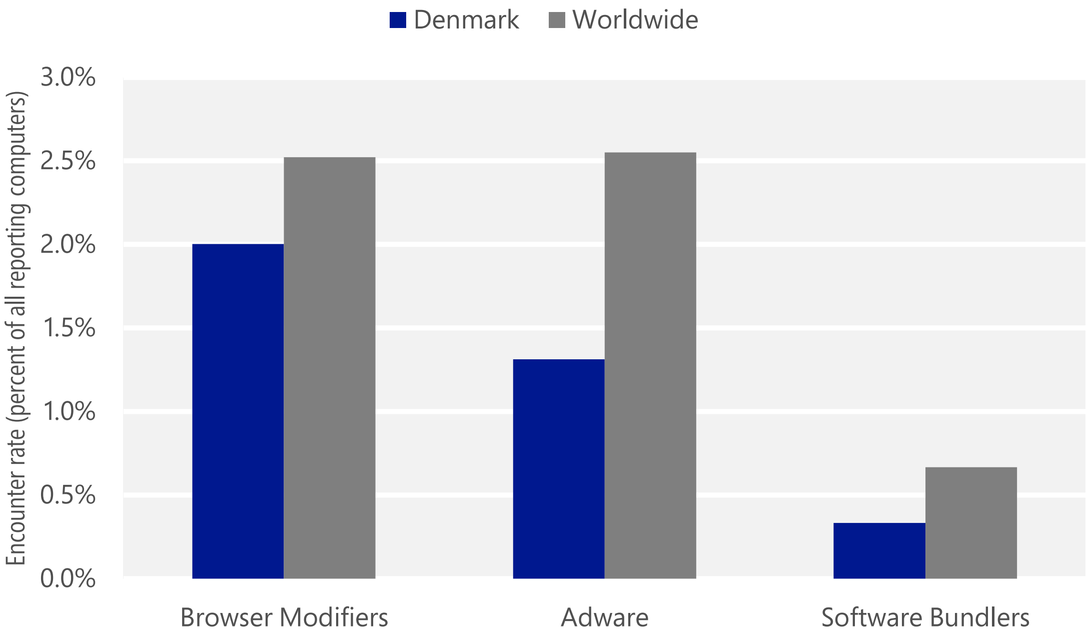
Malware encountered in Denmark in 4Q14, by category



- The most common malware category in Denmark in 4Q14 was Exploits. It was encountered by 1.9 percent of all computers there, down from 2.3 percent in 3Q14.
- The second most common malware category in Denmark in 4Q14 was Trojans. It was encountered by 1.7 percent of all computers there, down from 2.1 percent in 3Q14.
- The third most common malware category in Denmark in 4Q14 was Downloaders & Droppers, which was encountered by 0.8 percent of all computers there, down from 2.0 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Denmark in 4Q14, by category



- The most common unwanted software category in Denmark in 4Q14 was Browser Modifiers. It was encountered by 2.0 percent of all computers there, down from 3.4 percent in 3Q14.
- The second most common unwanted software category in Denmark in 4Q14 was Adware. It was encountered by 1.3 percent of all computers there, up from 0.9 percent in 3Q14.
- The third most common unwanted software category in Denmark in 4Q14 was Software Bundlers, which was encountered by 0.3 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Denmark in 4Q14

	Family	Most significant category	% of reporting computers
1	JS/Axpergle	Exploits	1.0%
2	Win32/Obfuscator	Obfuscators & Injectors	0.7%
3	Win32/Anogre	Exploits	0.3%
4	Win32/Tugspay	Downloaders & Droppers	0.2%
5	Win32/Sanusra	Trojans	0.2%
6	JS/Faceliker	Trojans	0.2%
7	JS/Astsan	Exploits	0.1%
8	JS/Fiexp	Exploits	0.1%
9	Win32/Reveton	Ransomware	0.1%
10	Java/CVE-2013-1488	Exploits	0.1%

- The most common malware family encountered in Denmark in 4Q14 was JS/Axpergle, which was encountered by 1.0 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 Denmark in 4Q14 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 third most common malware family encountered in Denmark in 4Q14 was Win32/Anogre, which was encountered by 0.3 percent of reporting computers there. Win32/Anogre is a threat that exploits a vulnerability addressed by Microsoft Security Bulletin MS11-087. This vulnerability can allow a hacker to install programs, view, change, or delete data or create new accounts with full administrative privileges.
- The fourth most common malware family encountered in Denmark in 4Q14 was Win32/Tugspay, which was encountered by 0.2 percent of reporting computers there. Win32/Tugspay is a downloader that spreads by posing as an installer for legitimate software, such as a Java update, or through other malware. When installed, it downloads unwanted software to the computer.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Denmark in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	1.8%
2	Win32/Costmin	Adware	0.6%
3	Win32/BetterSurf	Adware	0.3%
4	Win32/Defaulttab	Browser Modifiers	0.2%
5	Win32/Gofileexpress	Software Bundlers	0.2%

- The most common unwanted software family encountered in Denmark in 4Q14 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 Denmark in 4Q14 was Win32/Costmin, which was encountered by 0.6 percent of reporting computers there. Win32/Costmin is an adware family that installs itself as a browser extension for Internet Explorer, Mozilla Firefox, and Google Chrome, and displays advertisements as the user browses the Internet.
- The third most common unwanted software family encountered in Denmark in 4Q14 was Win32/BetterSurf, which was encountered by 0.3 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.

Top threat families by infection rate

The most common malware families by infection rate in Denmark in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Wysotot	Trojans	0.2
2	Win32/Sefnit	Trojans	0.1
3	Win32/Alureon	Trojans	0.1
4	Win32/Zbot	Password Stealers & Monitoring Tools	0.1
5	MSIL/Bladabindi	Backdoors	0.1
6	Win32/Sirefef	Trojans	<0.1
7	JS/Miuref	Trojans	<0.1
8	VBS/Jenxcus	Worms	<0.1
9	Win32/Sality	Viruses	<0.1
10	Win32/Brontok	Worms	<0.1

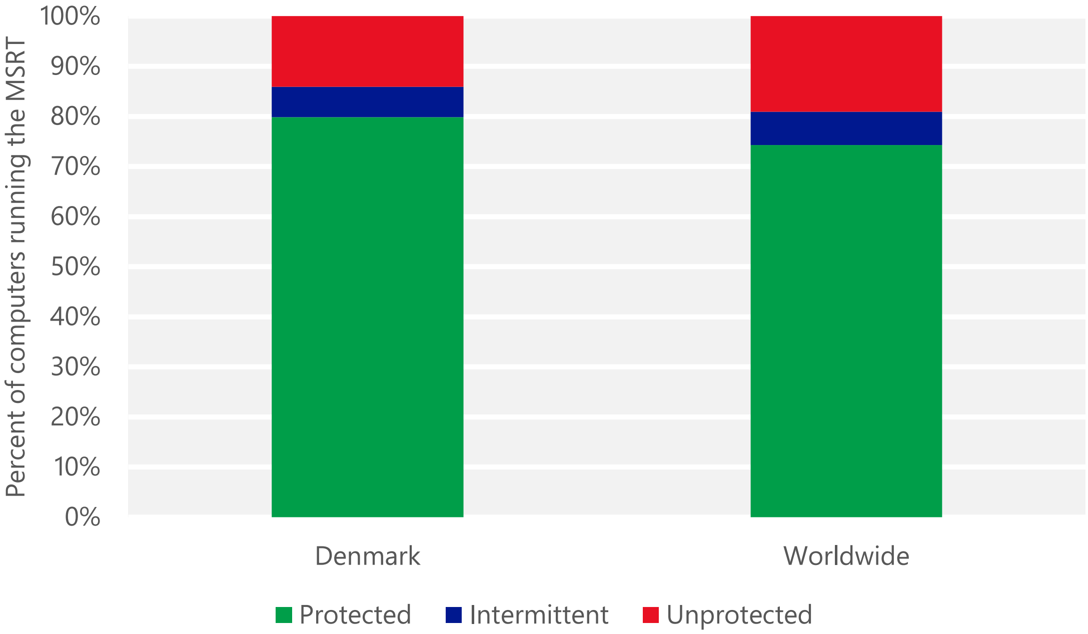
- The most common threat family infecting computers in Denmark in 4Q14 was Win32/Wysotot, which was detected and removed from 0.2 of every 1,000 unique computers scanned by the MSRT. Win32/Wysotot is a threat that can change the start page of the user's web browser, and may download and install other files to the computer. It is installed by software bundlers that advertise free software or games.
- The second most common threat family infecting computers in Denmark in 4Q14 was Win32/Sefnit, which was detected and removed from 0.1 of every 1,000 unique computers scanned by the MSRT. Win32/Sefnit is a family of trojans that can allow backdoor access, download files, and use the computer and Internet connection for click fraud. Some variants can monitor web browsers and hijack search results.
- The third most common threat family infecting computers in Denmark in 4Q14 was Win32/Alureon, which was detected and removed from 0.1 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 Denmark in 4Q14 was Win32/Zbot, which was detected and removed from 0.1 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.

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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.25 drive-by download URLs for every 1,000 URLs hosted in Denmark, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.21 drive-by download URLs for every 1,000 URLs hosted in Denmark, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Denmark and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Denmark	0.25	0.21
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Dominican Republic

The statistics presented here are generated by Microsoft security programs and services running on computers in the Dominican Republic in 4Q14 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 succeds 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

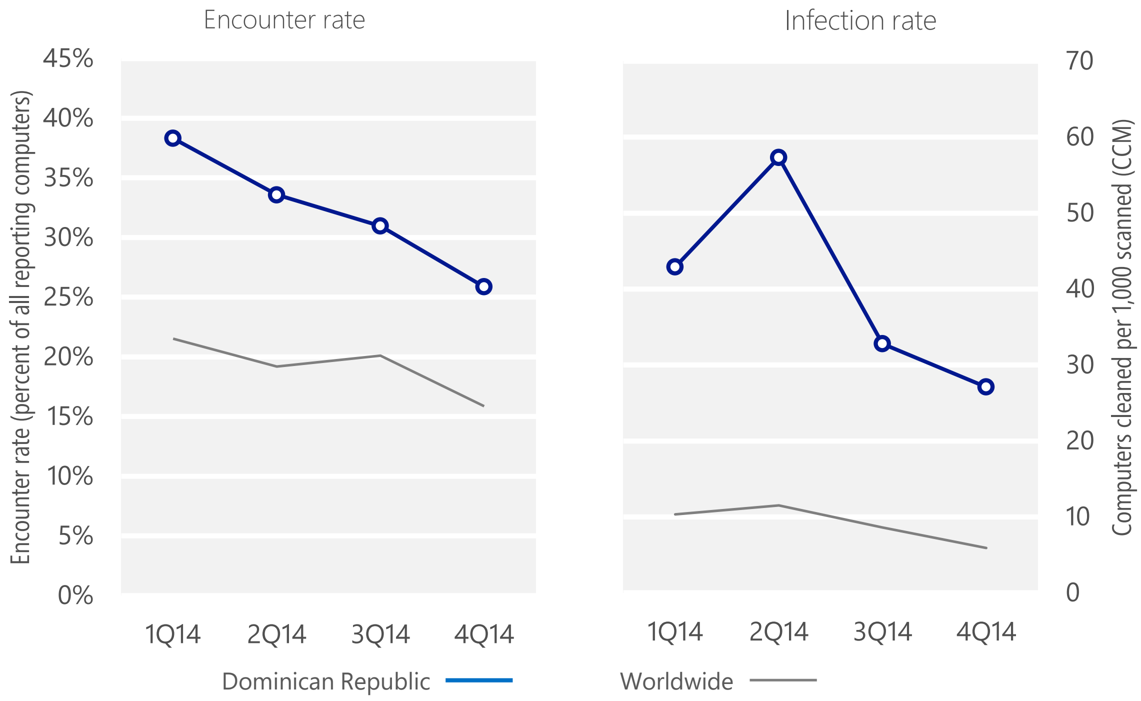
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Dominican Republic	38.3%	33.6%	31.0%	25.9%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Dominican Republic	42.9	57.3	32.8	27.1
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 25.9% percent of computers in the Dominican Republic encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 27.1 of every 1,000 unique computers scanned in the Dominican Republic in 4Q14 (a CCM score of 27.1, compared to the 4Q14 worldwide CCM of 5.9). 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.

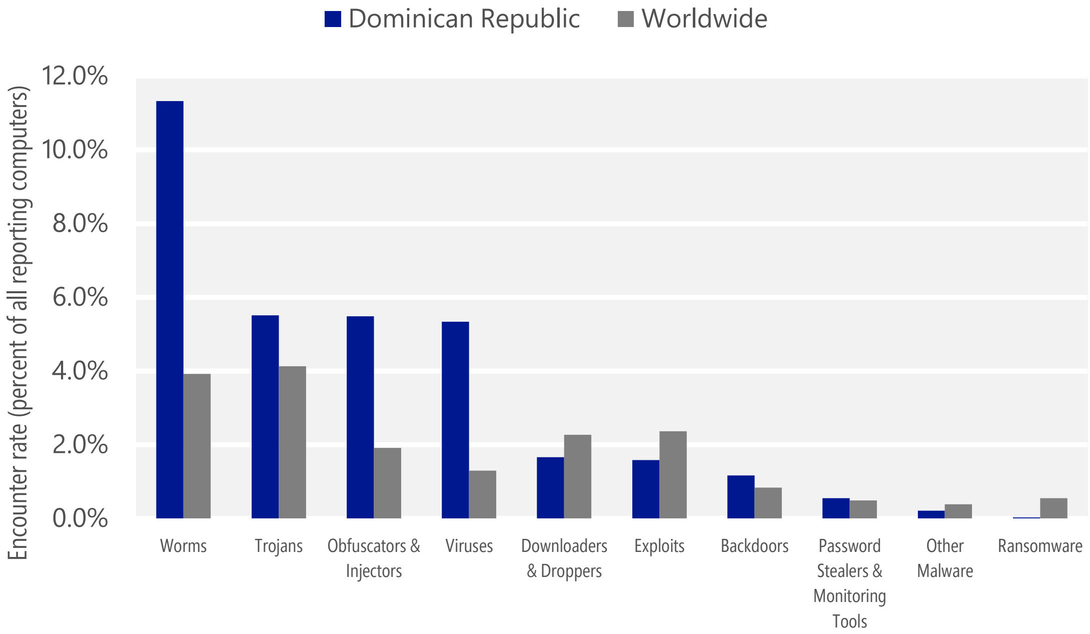
Malware encounter and infection rate trends in the Dominican Republic and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

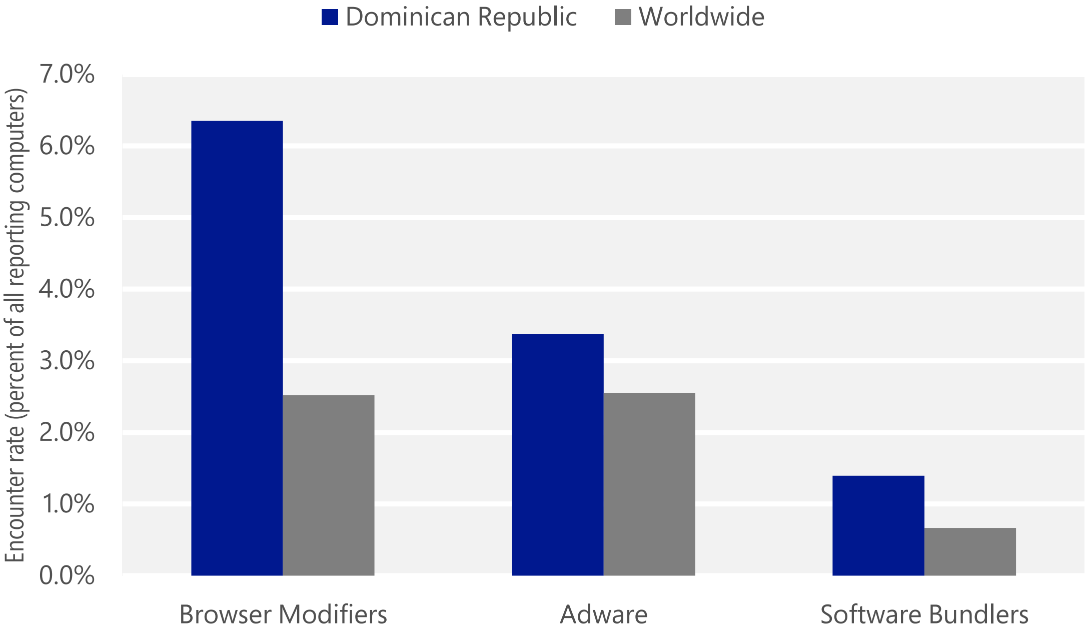
Malware encountered in the Dominican Republic in 4Q14, by category



- The most common malware category in the Dominican Republic in 4Q14 was Worms. It was encountered by 11.3 percent of all computers there, down from 13.1 percent in 3Q14.
- The second most common malware category in the Dominican Republic in 4Q14 was Trojans. It was encountered by 5.5 percent of all computers there, down from 8.9 percent in 3Q14.
- The third most common malware category in the Dominican Republic in 4Q14 was Obfuscators & Injectors, which was encountered by 5.5 percent of all computers there, down from 5.8 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in the Dominican Republic in 4Q14, by category



- The most common unwanted software category in the Dominican Republic in 4Q14 was Browser Modifiers. It was encountered by 6.3 percent of all computers there, down from 8.1 percent in 3Q14.
- The second most common unwanted software category in the Dominican Republic in 4Q14 was Adware. It was encountered by 3.4 percent of all computers there, up from 2.1 percent in 3Q14.
- The third most common unwanted software category in the Dominican Republic in 4Q14 was Software Bundlers, which was encountered by 1.4 percent of all computers there, up from 0.2 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in the Dominican Republic in 4Q14

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	6.0%
2	INF/Autorun	Obfuscators & Injectors	4.8%
3	Win32/Sality	Viruses	4.3%
4	Win32/Gamarue	Worms	2.3%
5	Win32/Brontok	Worms	1.5%
6	Win32/Nuqel	Worms	1.0%
7	Win32/Dynamer	Trojans	1.0%
8	Win32/Conficker	Worms	0.9%
9	Win32/CplLnk	Exploits	0.9%
10	Win32/Obfuscator	Obfuscators & Injectors	0.9%

- The most common malware family encountered in the Dominican Republic in 4Q14 was VBS/Jenxcus, which was encountered by 6.0 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 Dominican Republic in 4Q14 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 the Dominican Republic in 4Q14 was Win32/Sality, which was encountered by 4.3 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 Dominican Republic in 4Q14 was Win32/Gamarue, which was encountered by 2.3 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 Dominican Republic in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	5.2%
2	Win32/BetterSurf	Adware	1.7%
3	Win32/Defaulttab	Browser Modifiers	1.2%
4	Win32/Costmin	Adware	1.2%
5	Win32/Gofileexpress	Software Bundlers	0.6%

- The most common unwanted software family encountered in the Dominican Republic in 4Q14 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 the Dominican Republic in 4Q14 was Win32/BetterSurf, which was encountered by 1.7 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.
- The third most common unwanted software family encountered in the Dominican Republic in 4Q14 was Win32/Defaulttab, which was encountered by 1.2 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.

Top threat families by infection rate

The most common malware families by infection rate in the Dominican Republic in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Sality	Viruses	11.1
2	VBS/Jenxcus	Worms	8.1
3	Win32/Gamarue	Worms	2.1
4	Win32/Brontok	Worms	2.0
5	Win32/Helompy	Worms	1.1
6	Win32/Pramro	Trojans	1.0
7	MSIL/Spacekito	Trojans	0.7
8	Win32/Vobfus	Worms	0.6
9	Win32/Sefnit	Trojans	0.6
10	Win32/Ramnit	Trojans	0.6

- The most common threat family infecting computers in the Dominican Republic in 4Q14 was Win32/Sality, which was detected and removed from 11.1 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 second most common threat family infecting computers in the Dominican Republic in 4Q14 was VBS/Jenxcus, which was detected and removed from 8.1 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 the Dominican Republic in 4Q14 was Win32/Gamarue, which was detected and removed from 2.1 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 fourth most common threat family infecting computers in the Dominican Republic in 4Q14 was Win32/Brontok, which was detected and removed from 2.0 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

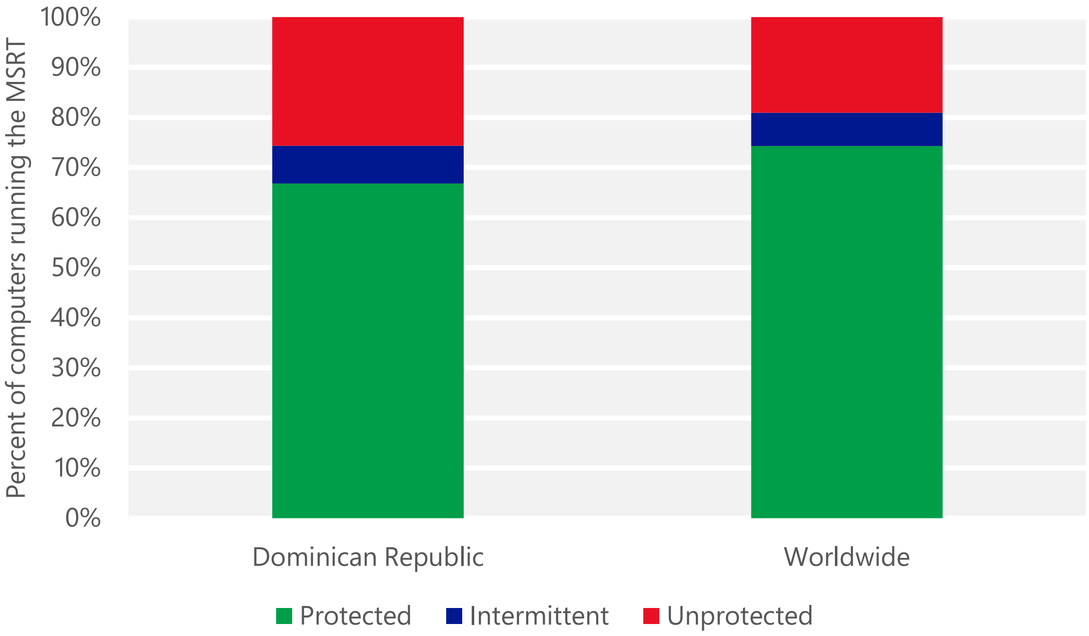
copying itself to removable volumes. Brontok can disable security software, and may conduct DoS attacks against certain websites.

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 the Dominican Republic and worldwide protected by real-time security software in 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.45 drive-by download URLs for every 1,000 URLs hosted in the Dominican Republic, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.39 drive-by download URLs for every 1,000 URLs hosted in the Dominican Republic, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in the Dominican Republic and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Dominican Republic	0.45	0.39
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Ecuador

The statistics presented here are generated by Microsoft security programs and services running on computers in Ecuador in 4Q14 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 succeds 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

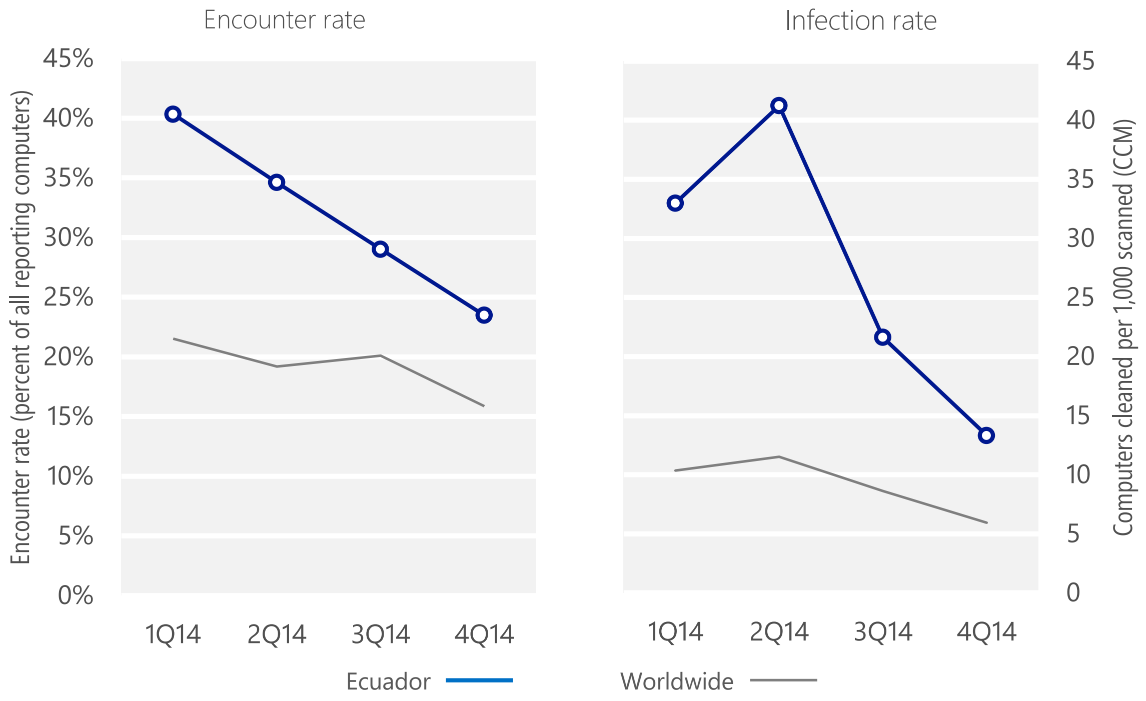
Metric	**1Q14**	**2Q14**	**3Q14**	**4Q14**
Encounter rate, Ecuador	40.3%	34.6%	29.0%	23.5%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Ecuador	33.0	41.2	21.6	13.3
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 23.5% percent of computers in Ecuador encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 13.3 of every 1,000 unique computers scanned in Ecuador in 4Q14 (a CCM score of 13.3, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Ecuador over the last four quarters, compared to the world as a whole.

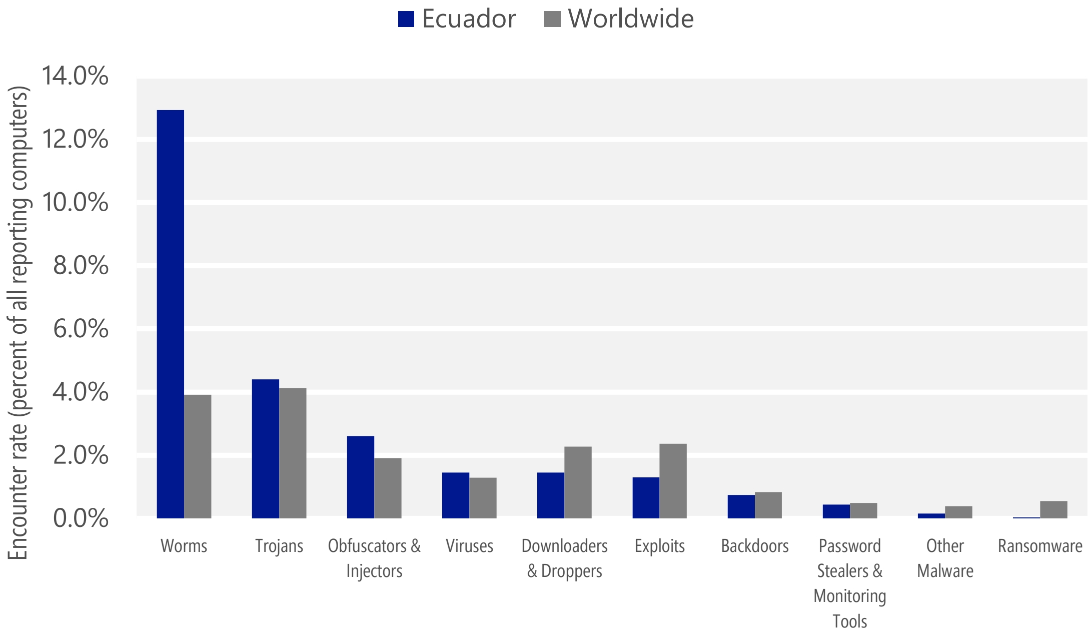
Malware encounter and infection rate trends in Ecuador and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

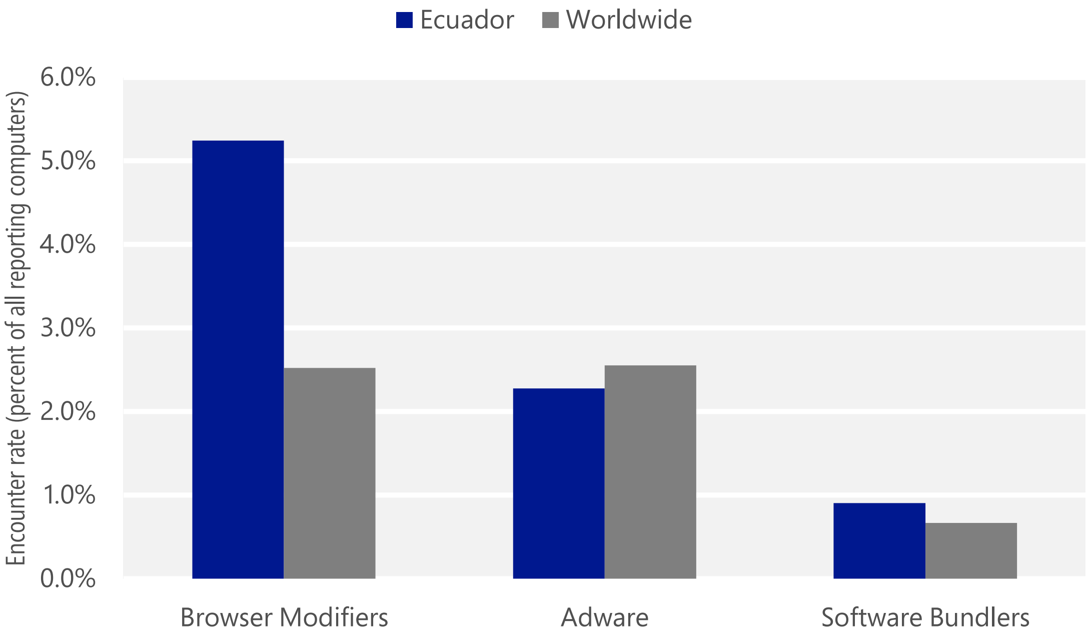
Malware encountered in Ecuador in 4Q14, by category



- The most common malware category in Ecuador in 4Q14 was Worms. It was encountered by 12.9 percent of all computers there, down from 15.6 percent in 3Q14.
- The second most common malware category in Ecuador in 4Q14 was Trojans. It was encountered by 4.4 percent of all computers there, down from 9.0 percent in 3Q14.
- The third most common malware category in Ecuador in 4Q14 was Obfuscators & Injectors, which was encountered by 2.6 percent of all computers there, down from 3.4 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Ecuador in 4Q14, by category



- The most common unwanted software category in Ecuador in 4Q14 was Browser Modifiers. It was encountered by 5.2 percent of all computers there, down from 5.7 percent in 3Q14.
- The second most common unwanted software category in Ecuador in 4Q14 was Adware. It was encountered by 2.3 percent of all computers there, up from 0.9 percent in 3Q14.
- The third most common unwanted software category in Ecuador in 4Q14 was Software Bundlers, which was encountered by 0.9 percent of all computers there, up from 0.3 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Ecuador in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Gamarue	Worms	6.2%
2	VBS/Jenxcus	Worms	5.7%
3	INF/Autorun	Obfuscators & Injectors	1.2%
4	JS/Bondat	Worms	1.0%
5	Win32/Vermis	Worms	0.9%
6	Win32/Obfuscator	Obfuscators & Injectors	0.9%
7	Win32/CplLnk	Exploits	0.8%
8	Win32/Yeltminky	Worms	0.8%
9	Win32/Ramnit	Trojans	0.8%
10	Win32/Vobfus	Worms	0.7%

- The most common malware family encountered in Ecuador in 4Q14 was Win32/Gamarue, which was encountered by 6.2 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 second most common malware family encountered in Ecuador in 4Q14 was VBS/Jenxcus, which was encountered by 5.7 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 third most common malware family encountered in Ecuador in 4Q14 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.
- The fourth most common malware family encountered in Ecuador in 4Q14 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.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Ecuador in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	4.0%
2	Win32/Defaulttab	Browser Modifiers	1.3%
3	Win32/BetterSurf	Adware	1.0%
4	Win32/Costmin	Adware	0.9%
5	Win32/Gofileexpress	Software Bundlers	0.4%

- The most common unwanted software family encountered in Ecuador in 4Q14 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 4Q14 was Win32/Defaulttab, which was encountered by 1.3 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.

- The third most common unwanted software family encountered in Ecuador in 4Q14 was Win32/BetterSurf, which was encountered by 1.0 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.

Top threat families by infection rate

The most common malware families by infection rate in Ecuador in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	5.2
2	Win32/Gamarue	Worms	3.3
3	Win32/Sality	Viruses	0.9
4	Win32/Ramnit	Trojans	0.6
5	MSIL/Spacekito	Trojans	0.6
6	Win32/Vobfus	Worms	0.5
7	Win32/Yeltminky	Worms	0.5
8	Win32/Sefnit	Trojans	0.4
9	Win32/Brontok	Worms	0.4
10	Win32/Dorkbot	Worms	0.3

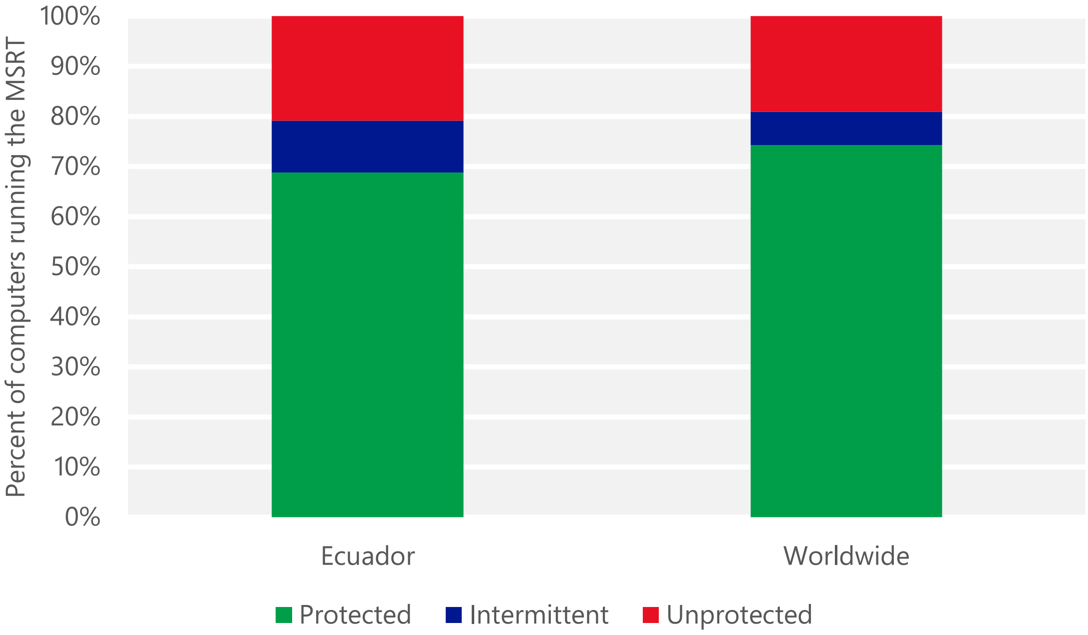
- The most common threat family infecting computers in Ecuador in 4Q14 was VBS/Jenxcus, which was detected and removed from 5.2 of every 1,000 unique computers scanned by the MSRT. VBS/Jenxcus is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Ecuador in 4Q14 was Win32/Gamarue, which was detected and removed from 3.3 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 Ecuador in 4Q14 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 Ecuador in 4Q14 was Win32/Ramnit, which was detected and removed from 0.6 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 Ecuador and worldwide protected by real-time security software in 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.27 drive-by download URLs for every 1,000 URLs hosted in Ecuador, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.09 drive-by download URLs for every 1,000 URLs hosted in Ecuador, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Ecuador and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Ecuador	0.27	0.09
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Egypt

The statistics presented here are generated by Microsoft security programs and services running on computers in Egypt in 4Q14 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 succeds 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

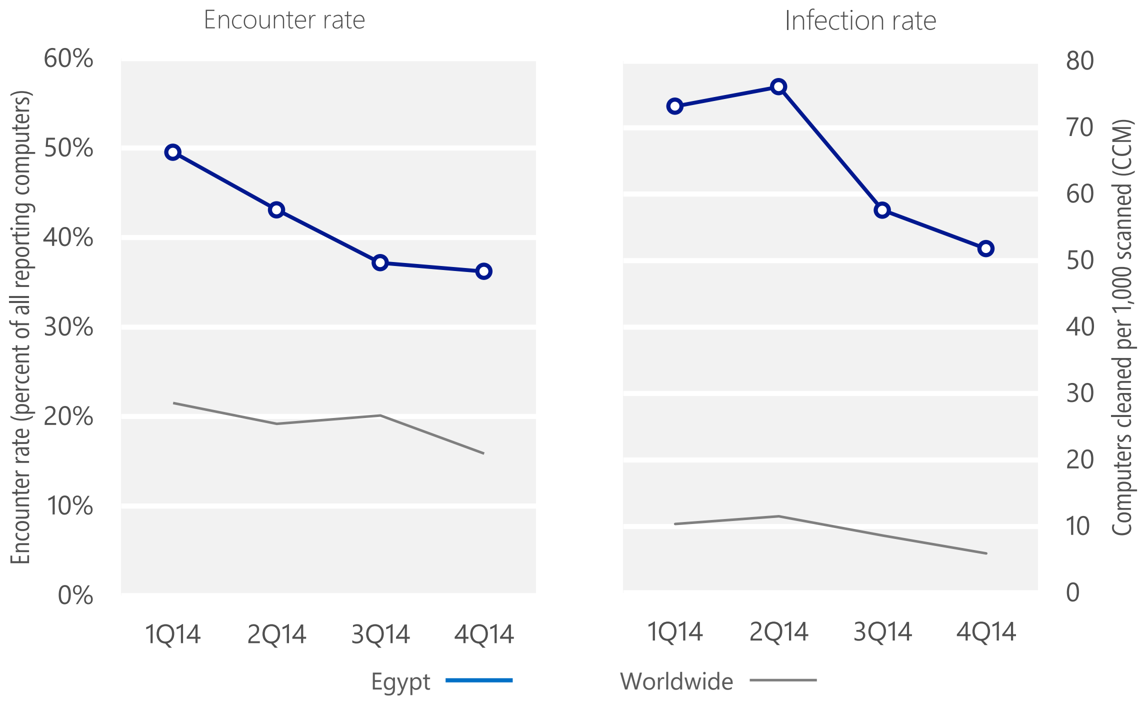
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Egypt	49.5%	43.1%	37.2%	36.2%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Egypt	73.2	76.1	57.6	51.8
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 36.2% percent of computers in Egypt encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 51.8 of every 1,000 unique computers scanned in Egypt in 4Q14 (a CCM score of 51.8, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Egypt over the last four quarters, compared to the world as a whole.

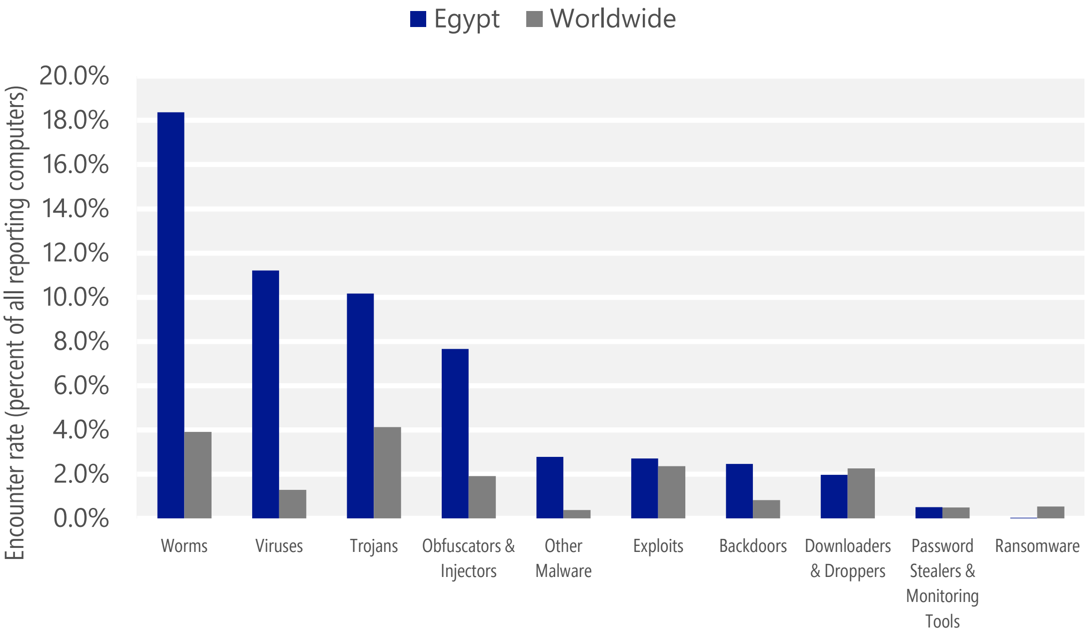
Malware encounter and infection rate trends in Egypt and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

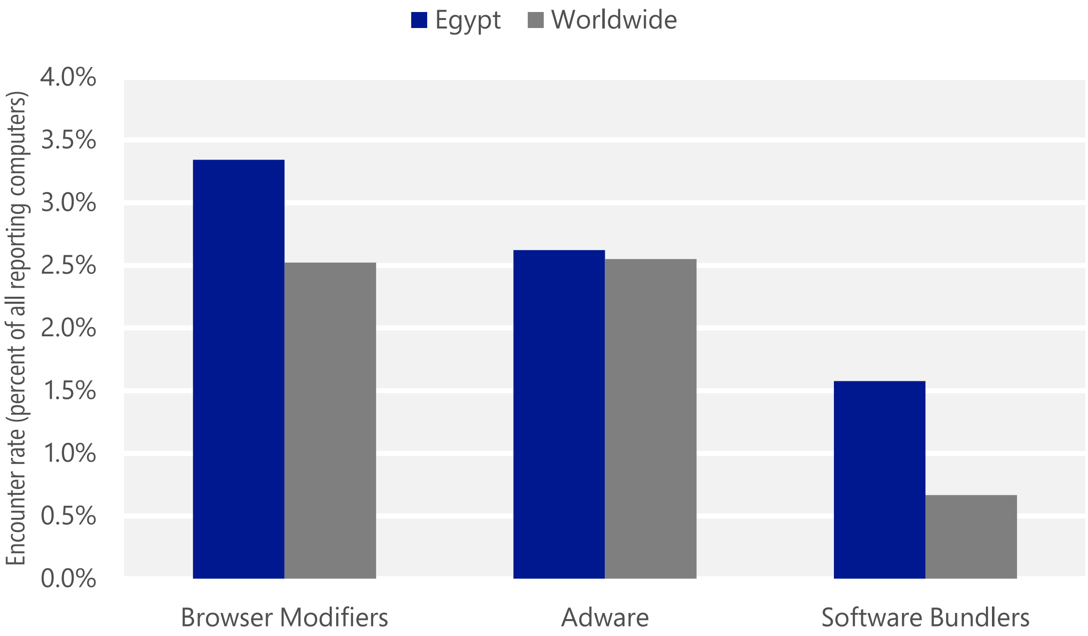
Malware encountered in Egypt in 4Q14, by category



- The most common malware category in Egypt in 4Q14 was Worms. It was encountered by 18.4 percent of all computers there, up from 17.1 percent in 3Q14.
- The second most common malware category in Egypt in 4Q14 was Viruses. It was encountered by 11.2 percent of all computers there, down from 12.1 percent in 3Q14.
- The third most common malware category in Egypt in 4Q14 was Trojans, which was encountered by 10.2 percent of all computers there, down from 10.9 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Egypt in 4Q14, by category



- The most common unwanted software category in Egypt in 4Q14 was Browser Modifiers. It was encountered by 3.3 percent of all computers there, down from 5.0 percent in 3Q14.
- The second most common unwanted software category in Egypt in 4Q14 was Adware. It was encountered by 2.6 percent of all computers there, up from 0.9 percent in 3Q14.
- The third most common unwanted software category in Egypt in 4Q14 was Software Bundlers, which was encountered by 1.6 percent of all computers there, up from 0.0 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Egypt in 4Q14

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	10.6%
2	INF/Autorun	Obfuscators & Injectors	6.7%
3	Win32/Sality	Viruses	6.2%
4	Win32/Virut	Viruses	4.3%
5	Win32/Ramnit	Trojans	2.9%
6	Win32/Gamarue	Worms	2.7%
7	Win32/Nitol	Other Malware	2.5%
8	Win32/Obfuscator	Obfuscators & Injectors	2.3%
9	Win32/Nuqel	Worms	2.3%
10	JS/Bondat	Worms	2.0%

- The most common malware family encountered in Egypt in 4Q14 was VBS/Jenxcus, which was encountered by 10.6 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 Egypt in 4Q14 was INF/Autorun, which was encountered by 6.7 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 Egypt in 4Q14 was Win32/Sality, which was encountered by 6.2 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 Egypt in 4Q14 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 Egypt in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	2.7%
2	Win32/Gofileexpress	Software Bundlers	1.3%
3	Win32/BetterSurf	Adware	0.9%
4	Win32/Costmin	Adware	0.9%
5	Win32/Defaulttab	Browser Modifiers	0.6%

- The most common unwanted software family encountered in Egypt in 4Q14 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 second most common unwanted software family encountered in Egypt in 4Q14 was Win32/Gofileexpress, which was encountered by 1.3 percent of reporting computers there. Win32/Gofileexpress is a software bundler that installs other unwanted software, including Adware:Win32/Lollipop and Adware:Win32/CostMin.
- The third most common unwanted software family encountered in Egypt in 4Q14 was Win32/BetterSurf, which was encountered by 0.9 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.

Top threat families by infection rate

The most common malware families by infection rate in Egypt in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	19.8
2	Win32/Sality	Viruses	18.5
3	Win32/Nitol	Other Malware	5.3
4	Win32/Ramnit	Trojans	4.1
5	Win32/Nuqel	Worms	2.7
6	MSIL/Bladabindi	Backdoors	2.1
7	Win32/Gamarue	Worms	1.9
8	Win32/Pramro	Trojans	1.6
9	Win32/Folstart	Worms	1.4
10	Win32/Wysotot	Trojans	0.6

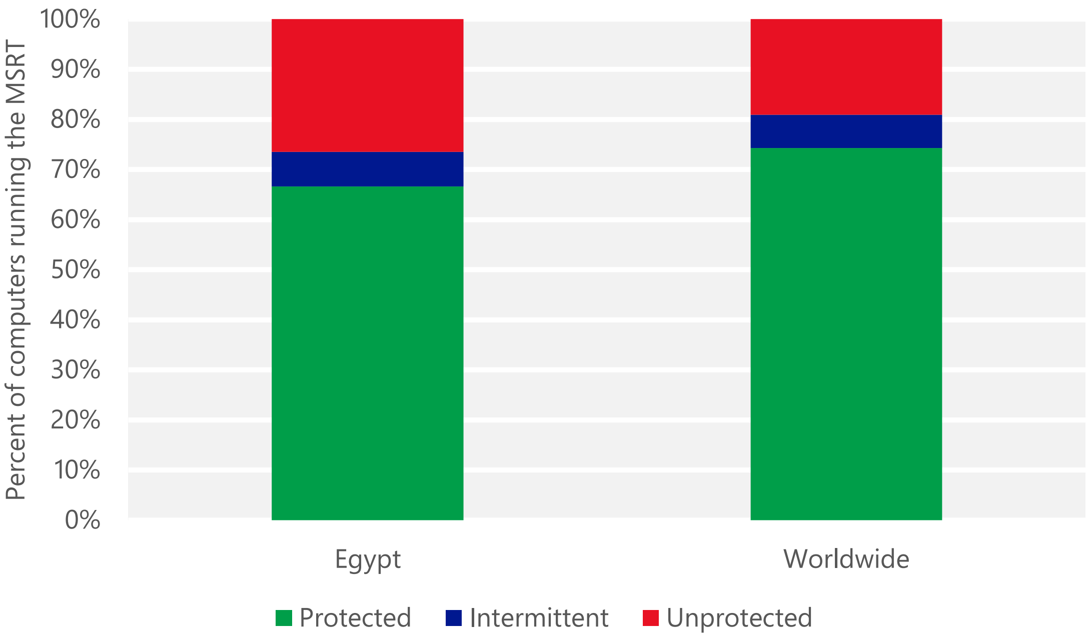
- The most common threat family infecting computers in Egypt in 4Q14 was VBS/Jenxcus, which was detected and removed from 19.8 of every 1,000 unique computers scanned by the MSRT. VBS/Jenxcus is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Egypt in 4Q14 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 third most common threat family infecting computers in Egypt in 4Q14 was Win32/Nitol, which was detected and removed from 5.3 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 fourth most common threat family infecting computers in Egypt in 4Q14 was Win32/Ramnit, which was detected and removed from 4.1 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.

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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 2.25 drive-by download URLs for every 1,000 URLs hosted in Egypt, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.78 drive-by download URLs for every 1,000 URLs hosted in Egypt, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Egypt and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Egypt	2.25	0.78
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

El Salvador

The statistics presented here are generated by Microsoft security programs and services running on computers in El Salvador in 4Q14 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 succeds 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

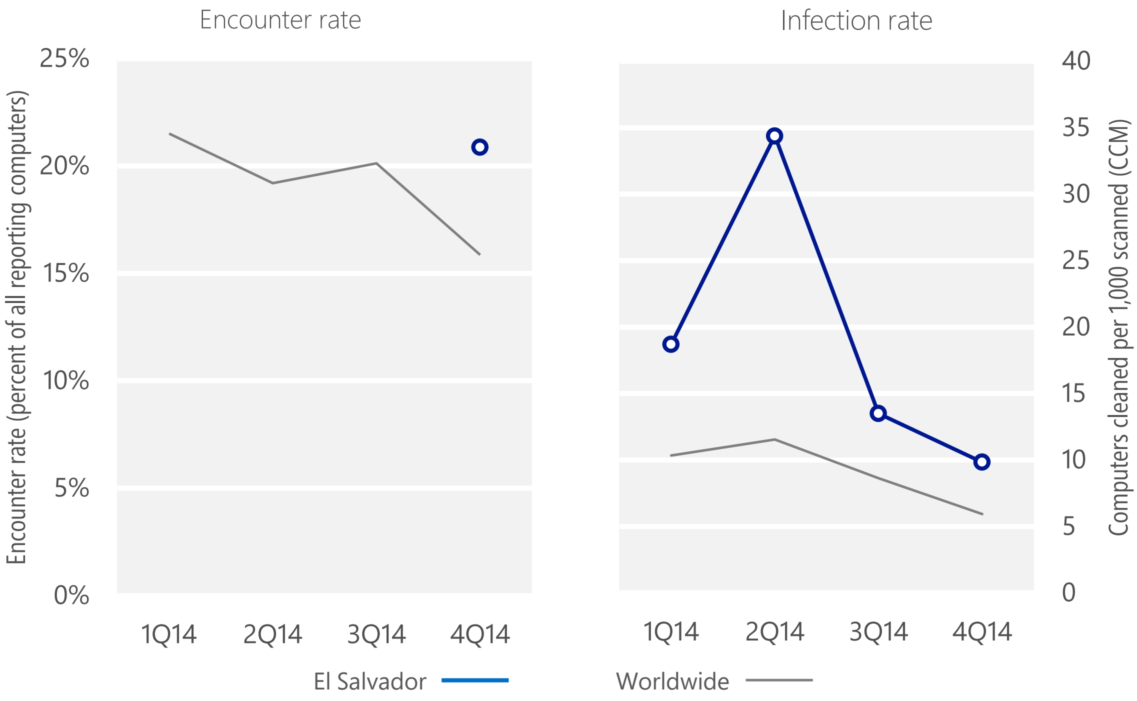
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, El Salvador	N/A	N/A	N/A	20.9%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, El Salvador	18.7	34.4	13.5	9.8
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 20.9% percent of computers in El Salvador encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 9.8 of every 1,000 unique computers scanned in El Salvador in 4Q14 (a CCM score of 9.8, compared to the 4Q14 worldwide CCM of 5.9). 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.

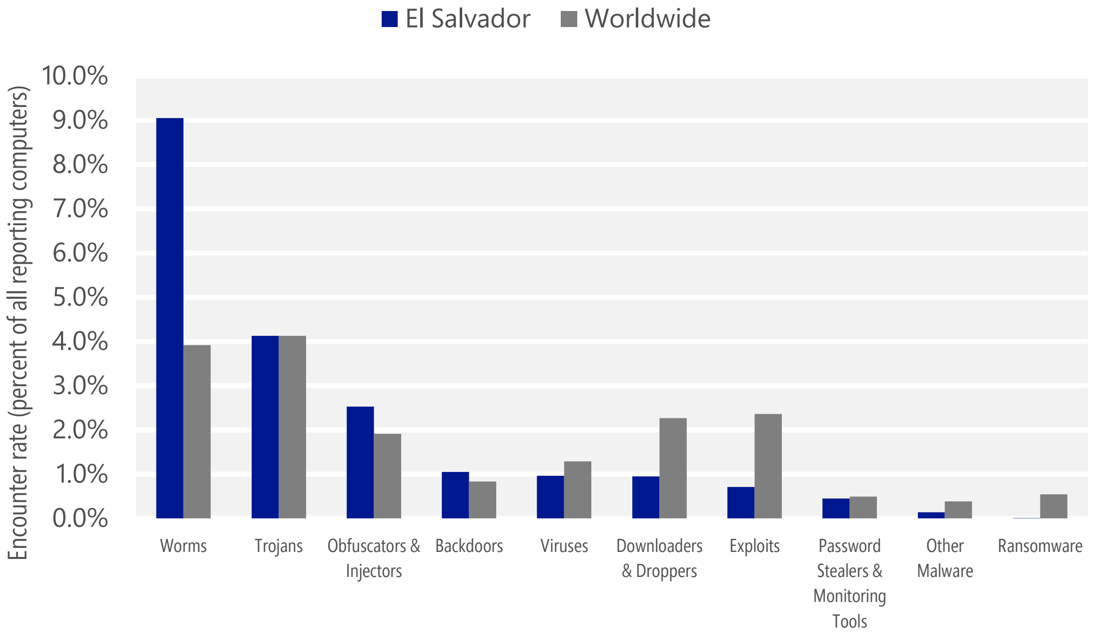
Malware encounter and infection rate trends in El Salvador and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

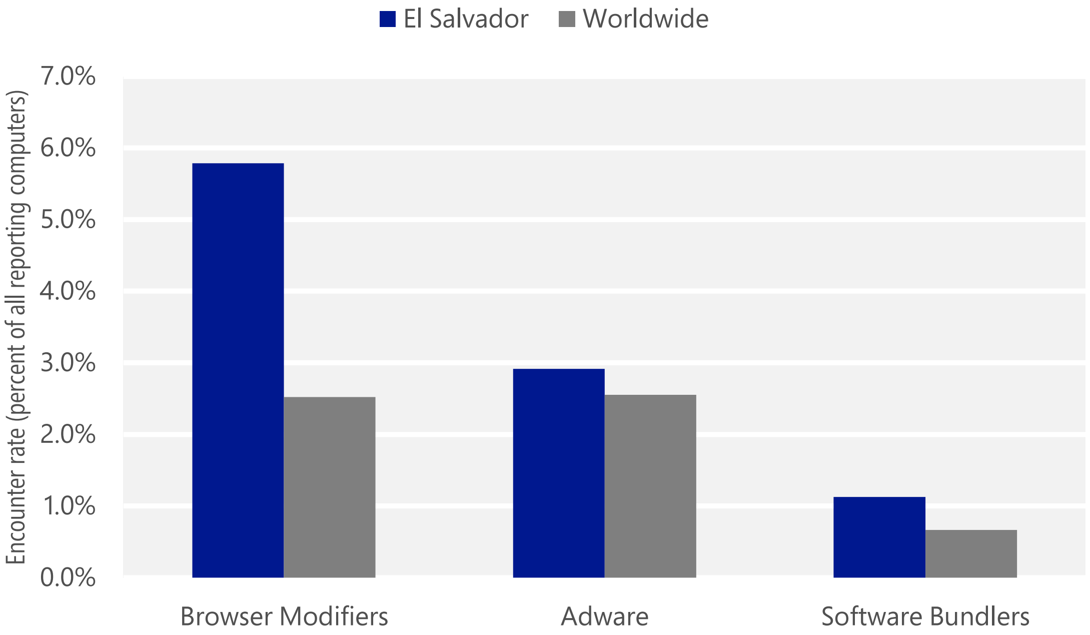
Malware encountered in El Salvador in 4Q14, by category



- The most common malware category in El Salvador in 4Q14 was Worms. It was encountered by 9.1 percent of all computers there, up from N/A percent in 3Q14.
- The second most common malware category in El Salvador in 4Q14 was Trojans. It was encountered by 4.1 percent of all computers there, up from N/A percent in 3Q14.
- The third most common malware category in El Salvador in 4Q14 was Obfuscators & Injectors, which was encountered by 2.5 percent of all computers there, up from N/A percent in 3Q14.

Unwanted software categories

Unwanted software encountered in El Salvador in 4Q14, by category



- The most common unwanted software category in El Salvador in 4Q14 was Browser Modifiers. It was encountered by 5.8 percent of all computers there, up from N/A percent in 3Q14.
- The second most common unwanted software category in El Salvador in 4Q14 was Adware. It was encountered by 2.9 percent of all computers there, up from N/A percent in 3Q14.
- The third most common unwanted software category in El Salvador in 4Q14 was Software Bundlers, which was encountered by 1.1 percent of all computers there, up from N/A percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in El Salvador in 4Q14

	Family	Most significant category	% of reporting computers
1	INF/Autorun	Obfuscators & Injectors	3.1%
2	VBS/Jenxcus	Worms	3.0%
3	Win32/Brontok	Worms	1.2%
4	Win32/Vermis	Worms	1.1%
5	Win32/Conficker	Worms	1.0%
6	Win32/Ippedo	Worms	0.9%

- The most common malware family encountered in El Salvador in 4Q14 was INF/Autorun, which was encountered by 3.1 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 second most common malware family encountered in El Salvador in 4Q14 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 third most common malware family encountered in El Salvador in 4Q14 was Win32/Brontok, which was encountered by 1.2 percent of reporting computers there. 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 malware family encountered in El Salvador in 4Q14 was Win32/Vermis, which was encountered by 1.1 percent of reporting computers there. Win32/Vermis is a generic detection for malicious .inf and .lnk files dropped by different worms, including IRCBot, Phorpiex, Dorkbot, and Caphaw.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in El Salvador in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	4.5%
2	Win32/BetterSurf	Adware	1.6%
3	Win32/Defaulttab	Browser Modifiers	1.4%
4	Win32/Costmin	Adware	0.9%

- The most common unwanted software family encountered in El Salvador in 4Q14 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 El Salvador in 4Q14 was Win32/BetterSurf, which was encountered by 1.6 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.
- The third most common unwanted software family encountered in El Salvador in 4Q14 was Win32/Defaulttab, which was encountered by 1.4 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.

Top threat families by infection rate

The most common malware families by infection rate in El Salvador in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	3.9
2	Win32/Brontok	Worms	1.2
3	Win32/Sality	Viruses	0.9
4	MSIL/Spacekito	Trojans	0.6
5	Win32/Dorkbot	Worms	0.6
6	Win32/Sefnit	Trojans	0.5
7	Win32/Gamarue	Worms	0.3
8	Win32/Vobfus	Worms	0.3
9	Win32/Lethic	Trojans	0.3
10	MSIL/Bladabindi	Backdoors	0.2

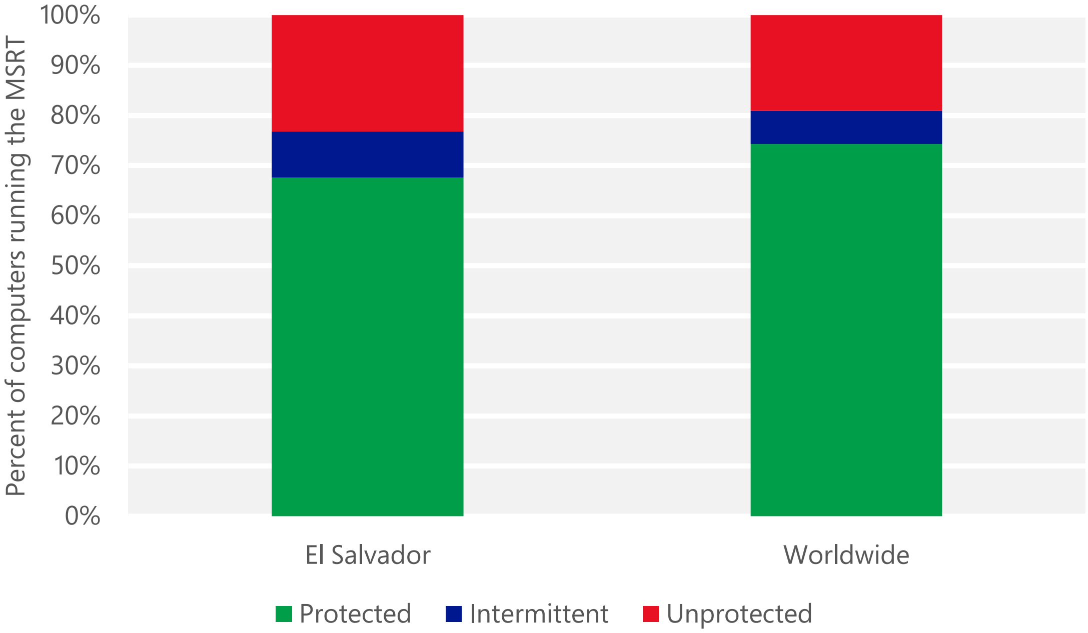
- The most common threat family infecting computers in El Salvador in 4Q14 was VBS/Jenxcus, which was detected and removed from 3.9 of every 1,000 unique computers scanned by the MSRT. VBS/Jenxcus is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in El Salvador in 4Q14 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.
- The third most common threat family infecting computers in El Salvador in 4Q14 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 El Salvador in 4Q14 was MSIL/Spacekito, which was detected and removed from 0.6 of every 1,000 unique computers scanned by the MSRT. MSIL/Spacekito is a threat that steals information about the computer and installs browser add-ons that display ads.

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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.39 drive-by download URLs for every 1,000 URLs hosted in El Salvador, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.14 drive-by download URLs for every 1,000 URLs hosted in El Salvador, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in El Salvador and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, El Salvador	0.39	0.14
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Estonia

The statistics presented here are generated by Microsoft security programs and services running on computers in Estonia in 4Q14 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 succeds 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

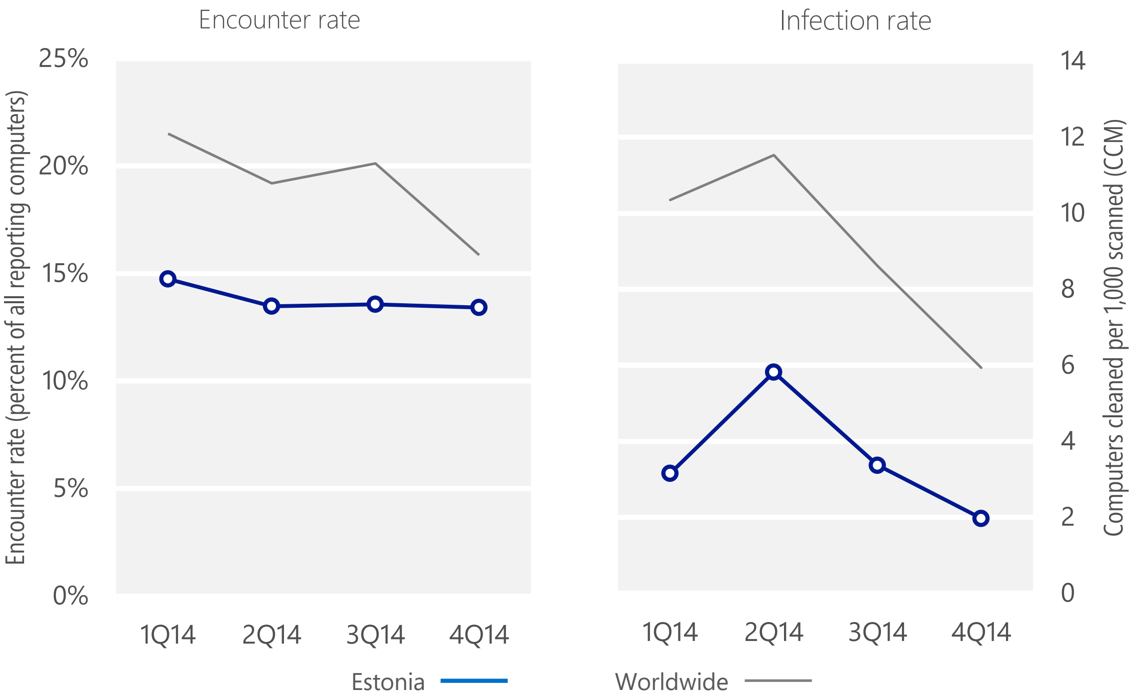
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Estonia	14.7%	13.5%	13.6%	13.4%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Estonia	3.2	5.8	3.4	2.0
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 13.4% percent of computers in Estonia encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 2.0 of every 1,000 unique computers scanned in Estonia in 4Q14 (a CCM score of 2.0, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Estonia over the last four quarters, compared to the world as a whole.

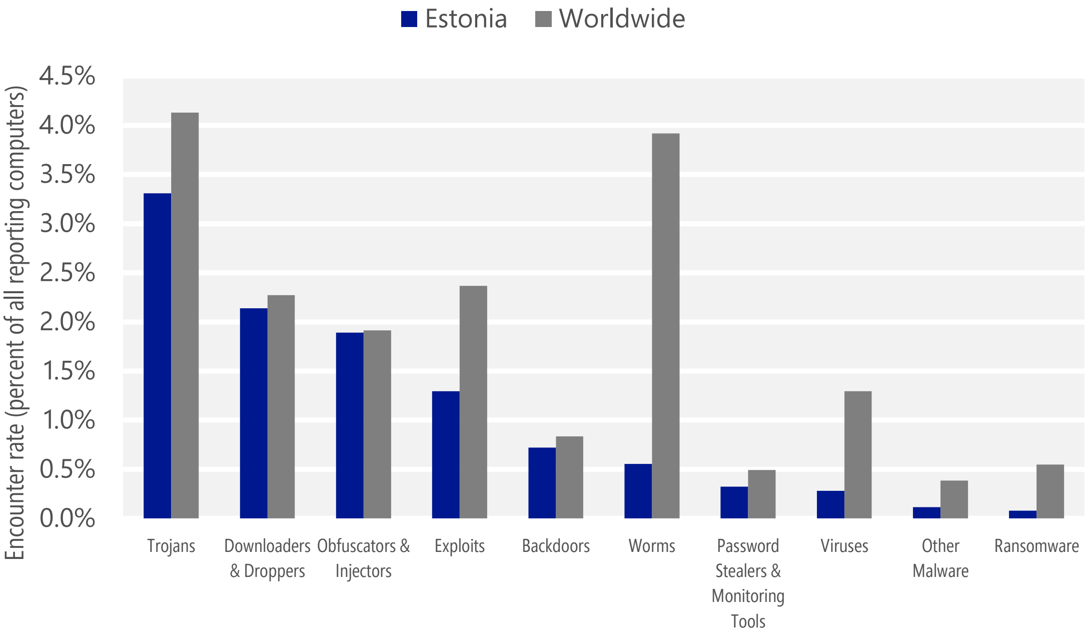
Malware encounter and infection rate trends in Estonia and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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 4Q14, by category



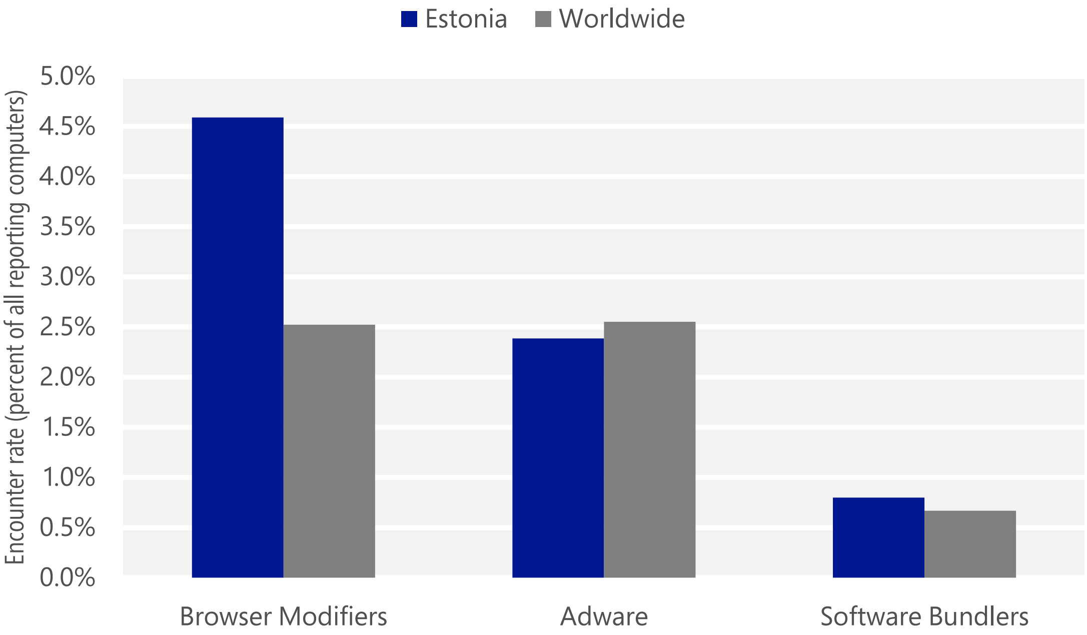
- The most common malware category in Estonia in 4Q14 was Trojans. It was encountered by 3.3 percent of all computers there, down from 4.3 percent in 3Q14.

- The second most common malware category in Estonia in 4Q14 was Downloaders & Droppers. It was encountered by 2.1 percent of all computers there, down from 3.6 percent in 3Q14.

- The third most common malware category in Estonia in 4Q14 was Obfuscators & Injectors, which was encountered by 1.9 percent of all computers there, up from 1.8 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Estonia in 4Q14, by category



- The most common unwanted software category in Estonia in 4Q14 was Browser Modifiers. It was encountered by 4.6 percent of all computers there, down from 4.8 percent in 3Q14.

- The second most common unwanted software category in Estonia in 4Q14 was Adware. It was encountered by 2.4 percent of all computers there, up from 0.4 percent in 3Q14.

- The third most common unwanted software category in Estonia in 4Q14 was Software Bundlers, which was encountered by 0.8 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Estonia in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Obfuscator	Obfuscators & Injectors	1.6%
2	Win32/Ogimant	Downloaders & Droppers	1.3%
3	JS/Axpergle	Exploits	0.7%
4	Win32/Peaac	Trojans	0.5%

- The most common malware family encountered in Estonia in 4Q14 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 Estonia in 4Q14 was Win32/Ogimant, which was encountered by 1.3 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 third most common malware family encountered in Estonia in 4Q14 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 fourth most common malware family encountered in Estonia in 4Q14 was Win32/Peaac, which was encountered by 0.5 percent of reporting computers there. Win32/Peaac 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 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	3.2%
2	Win32/Defaulttab	Browser Modifiers	1.6%
3	Win32/BetterSurf	Adware	1.3%
4	Win32/Costmin	Adware	1.0%
5	Win32/Gofileexpress	Software Bundlers	0.6%

- The most common unwanted software family encountered in Estonia in 4Q14 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 Estonia in 4Q14 was Win32/Defaulttab, which was encountered by 1.6 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.
- The third most common unwanted software family encountered in Estonia in 4Q14 was Win32/BetterSurf, which was encountered by 1.3 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.

Top threat families by infection rate

The most common malware families by infection rate in Estonia in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Tofsee	Backdoors	0.3
2	MSIL/Bladabindi	Backdoors	0.1
3	Win32/Ramnit	Trojans	0.1
4	JS/Kilim	Trojans	0.1
5	Win32/Sefnit	Trojans	0.1
6	Win32/Sality	Viruses	0.1
7	Win32/Jeefo	Viruses	0.1
8	Win32/Zbot	Password Stealers & Monitoring Tools	0.1
9	Win32/Gamarue	Worms	0.1
10	JS/Miuref	Trojans	0.1

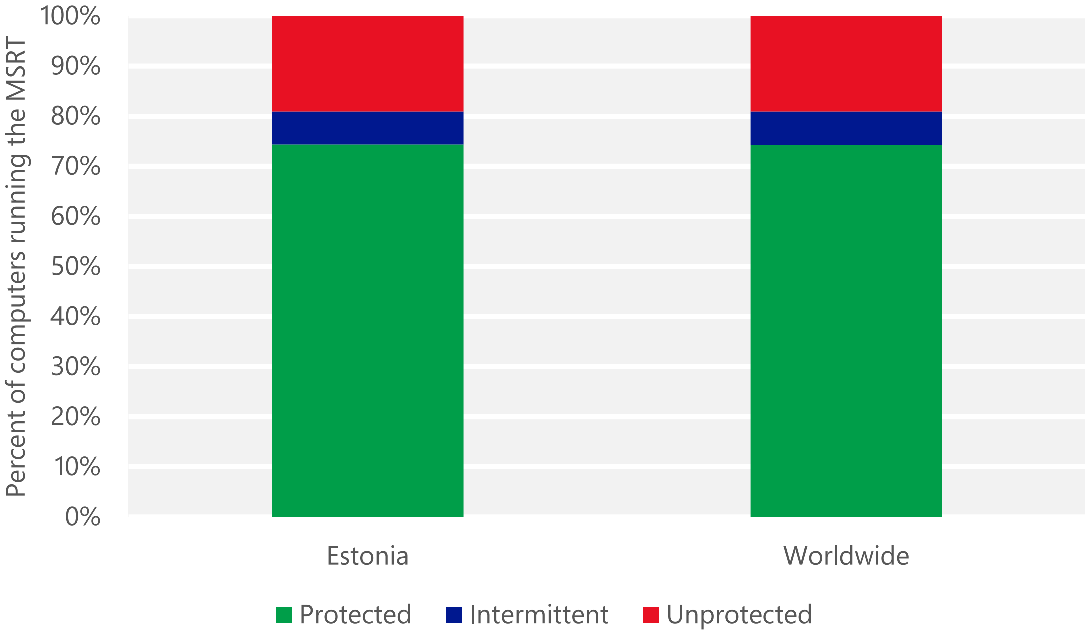
- The most common threat family infecting computers in Estonia in 4Q14 was Win32/Tofsee, which was detected and removed from 0.3 of every 1,000 unique computers scanned by the MSRT. Win32/Tofsee is a multi-component family of backdoor trojans that act as a spam and traffic relay.
- The second most common threat family infecting computers in Estonia in 4Q14 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.
- The third most common threat family infecting computers in Estonia in 4Q14 was Win32/Ramnit, which was detected and removed from 0.1 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 fourth most common threat family infecting computers in Estonia in 4Q14 was JS/Kilim, which was detected and removed from 0.1 of every 1,000 unique computers scanned by the MSRT. JS/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 Estonia and worldwide protected by real-time security software in 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.25 drive-by download URLs for every 1,000 URLs hosted in Estonia, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.22 drive-by download URLs for every 1,000 URLs hosted in Estonia, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Estonia and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Estonia	0.25	0.22
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Finland

The statistics presented here are generated by Microsoft security programs and services running on computers in Finland in 4Q14 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 succeds 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

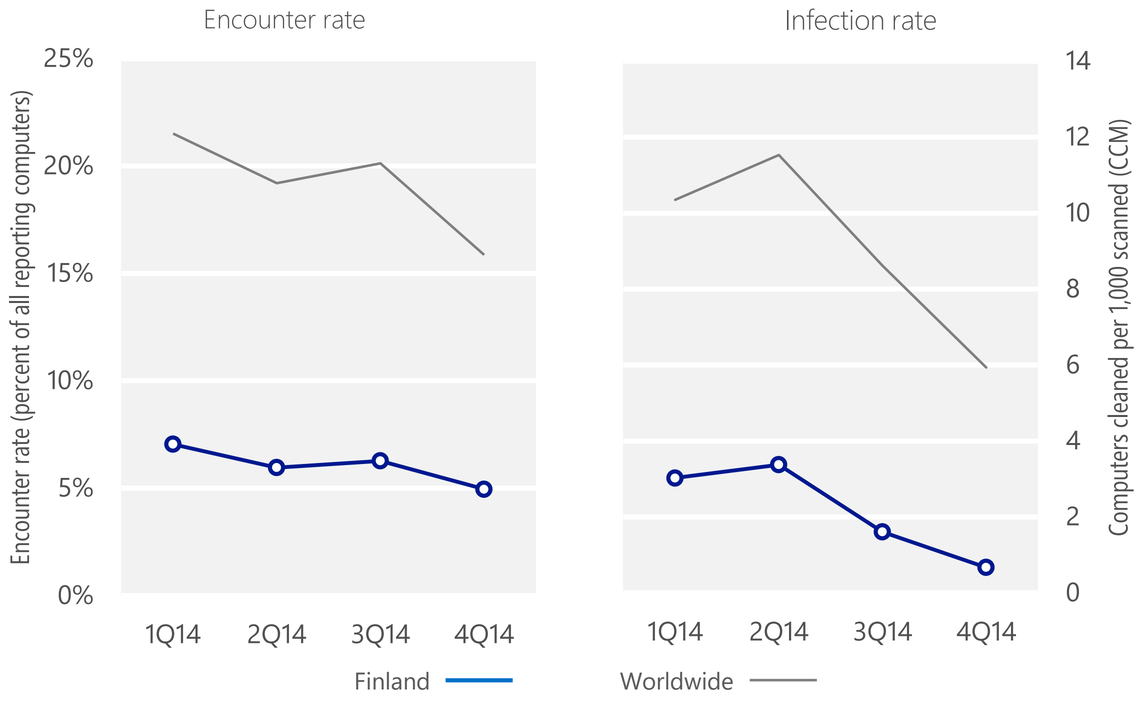
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Finland	7.0%	6.0%	6.3%	5.0%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Finland	3.0	3.4	1.6	0.7
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 5.0% percent of computers in Finland encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 0.7 of every 1,000 unique computers scanned in Finland in 4Q14 (a CCM score of 0.7, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Finland over the last four quarters, compared to the world as a whole.

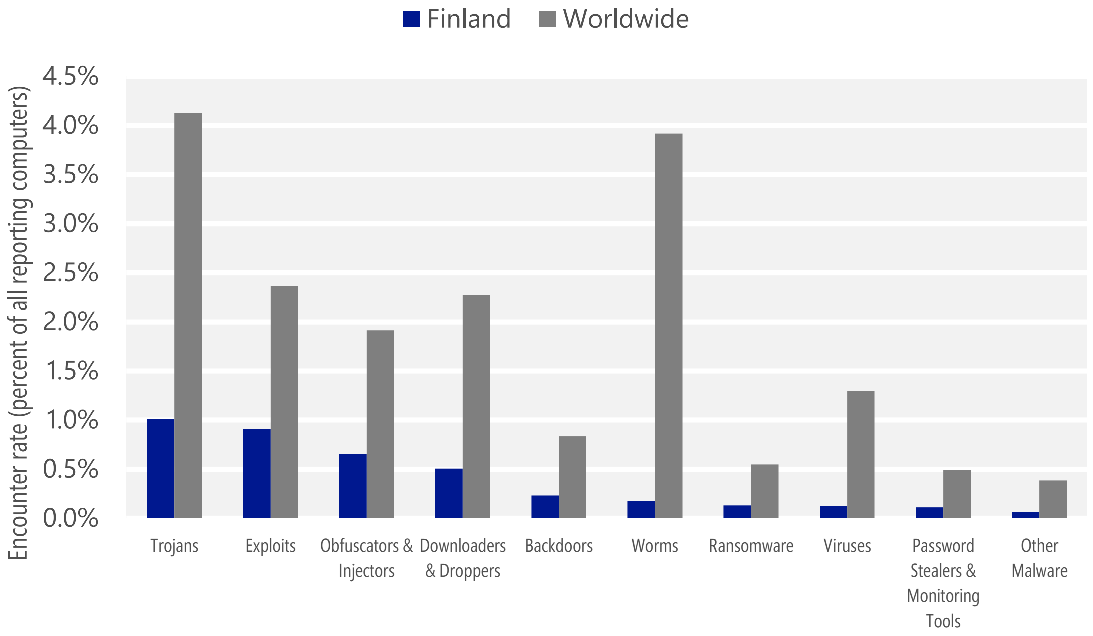
Malware encounter and infection rate trends in Finland and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

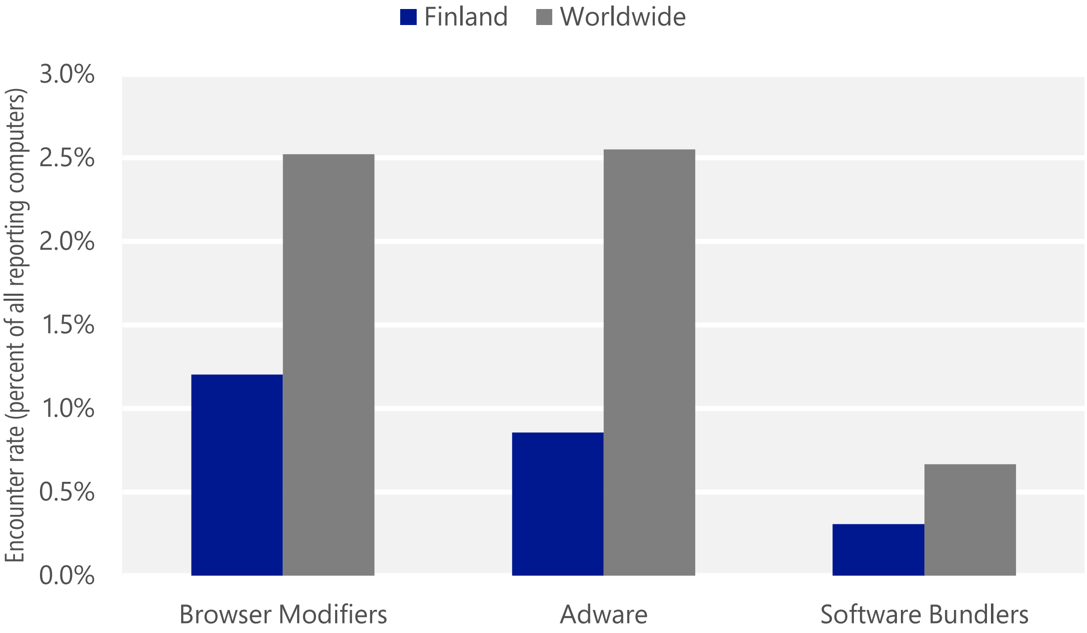
Malware encountered in Finland in 4Q14, by category



- The most common malware category in Finland in 4Q14 was Trojans. It was encountered by 1.0 percent of all computers there, down from 1.6 percent in 3Q14.
- The second most common malware category in Finland in 4Q14 was Exploits. It was encountered by 0.9 percent of all computers there, down from 1.3 percent in 3Q14.
- The third most common malware category in Finland in 4Q14 was Obfuscators & Injectors, which was encountered by 0.7 percent of all computers there, down from 1.1 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Finland in 4Q14, by category



- The most common unwanted software category in Finland in 4Q14 was Browser Modifiers. It was encountered by 1.2 percent of all computers there, down from 2.0 percent in 3Q14.
- The second most common unwanted software category in Finland in 4Q14 was Adware. It was encountered by 0.9 percent of all computers there, up from 0.4 percent in 3Q14.
- The third most common unwanted software category in Finland in 4Q14 was Software Bundlers, which was encountered by 0.3 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Finland in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Obfuscator	Obfuscators & Injectors	0.6%
2	JS/Axpergle	Exploits	0.5%
3	Win32/Wysotot	Trojans	0.1%

- The most common malware family encountered in Finland in 4Q14 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 second most common malware family encountered in Finland in 4Q14 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 third most common malware family encountered in Finland in 4Q14 was Win32/Wysotot, which was encountered by 0.1 percent of reporting computers there. Win32/Wysotot is a threat that can change the start page of the user's web browser, and may download and install other files to the computer. It is installed by software bundlers that advertise free software or games.
- The fourth most common malware family encountered in Finland in 4Q14 was N/A, which was encountered by percent of reporting computers there.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Finland in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	1.0%
2	Win32/Costmin	Adware	0.4%
3	Win32/BetterSurf	Adware	0.3%
4	Win32/Defaulttab	Browser Modifiers	0.2%
5	Win32/Gofileexpress	Software Bundlers	0.2%

- The most common unwanted software family encountered in Finland in 4Q14 was Win32/Couponruc, which was encountered by 1.0 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 Finland in 4Q14 was Win32/Costmin, which was encountered by 0.4 percent of reporting computers there. Win32/Costmin is an adware family that installs itself as a browser extension for Internet Explorer, Mozilla Firefox, and Google Chrome, and displays advertisements as the user browses the Internet.
- The third most common unwanted software family encountered in Finland in 4Q14 was Win32/BetterSurf, which was encountered by 0.3 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.

Top threat families by infection rate

The most common malware families by infection rate in Finland in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Wysotot	Trojans	0.1
2	Win32/Sefnit	Trojans	0.1
3	Win32/Alureon	Trojans	0.1
4	MSIL/Bladabindi	Backdoors	<0.1
5	JS/Miuref	Trojans	<0.1
6	Win32/Zbot	Password Stealers & Monitoring Tools	<0.1
7	VBS/Jenxcus	Worms	<0.1
8	Win32/Gamarue	Worms	<0.1
9	Win32/Sality	Viruses	<0.1
10	JS/Kilim	Trojans	<0.1

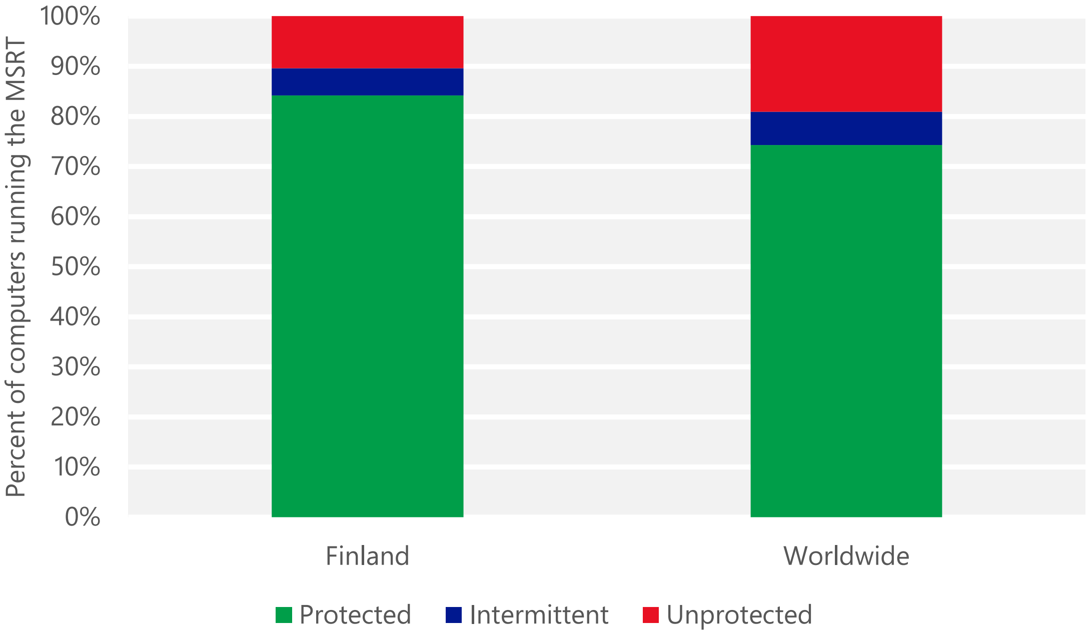
- The most common threat family infecting computers in Finland in 4Q14 was Win32/Wysotot, which was detected and removed from 0.1 of every 1,000 unique computers scanned by the MSRT. Win32/Wysotot is a threat that can change the start page of the user's web browser, and may download and install other files to the computer. It is installed by software bundlers that advertise free software or games.
- The second most common threat family infecting computers in Finland in 4Q14 was Win32/Sefnit, which was detected and removed from 0.1 of every 1,000 unique computers scanned by the MSRT. Win32/Sefnit is a family of trojans that can allow backdoor access, download files, and use the computer and Internet connection for click fraud. Some variants can monitor web browsers and hijack search results.
- The third most common threat family infecting computers in Finland in 4Q14 was Win32/Alureon, which was detected and removed from 0.1 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 Finland in 4Q14 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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.03 drive-by download URLs for every 1,000 URLs hosted in Finland, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.10 drive-by download URLs for every 1,000 URLs hosted in Finland, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Finland and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Finland	0.03	0.10
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

France

The statistics presented here are generated by Microsoft security programs and services running on computers in France in 4Q14 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 succeds 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

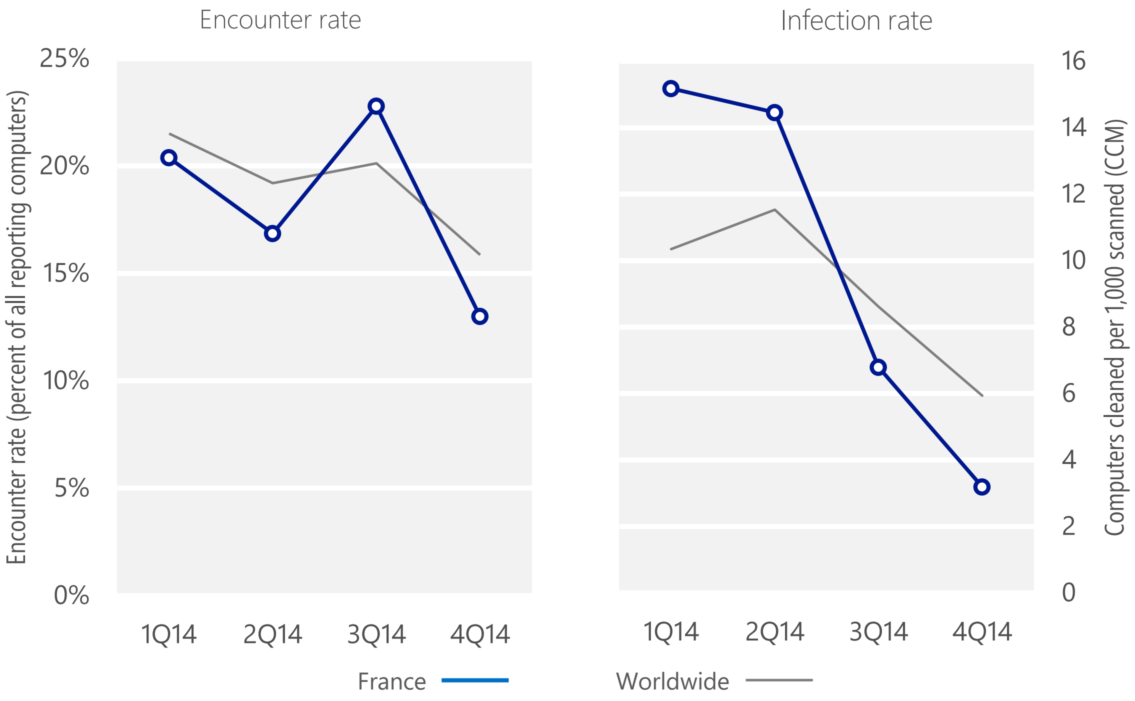
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, France	20.4%	16.9%	22.8%	13.0%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, France	15.2	14.5	6.8	3.2
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 13.0% percent of computers in France encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 3.2 of every 1,000 unique computers scanned in France in 4Q14 (a CCM score of 3.2, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for France over the last four quarters, compared to the world as a whole.

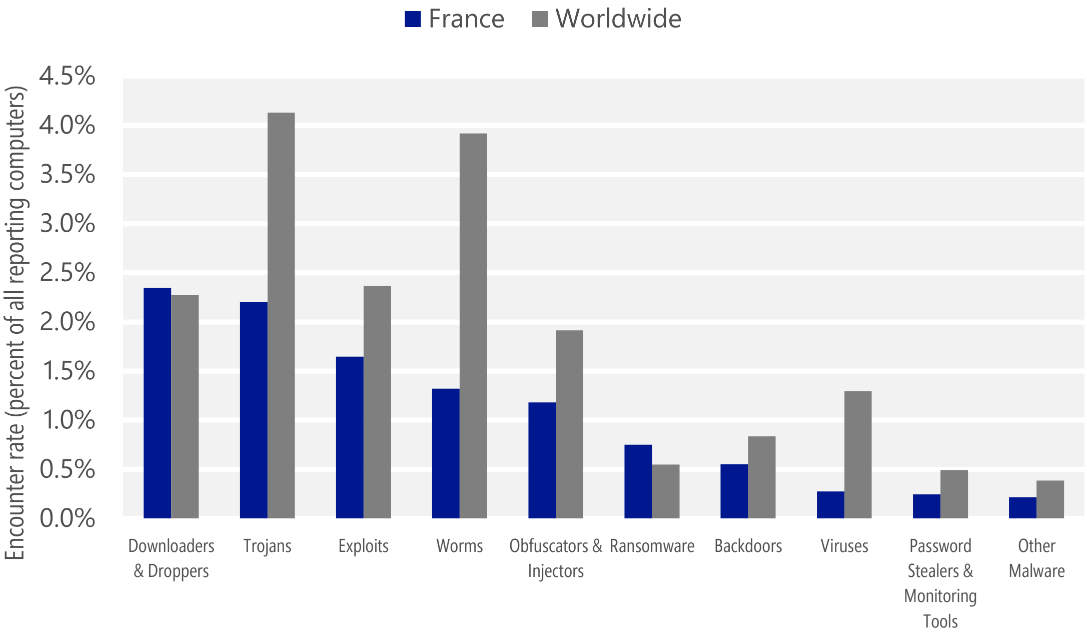
Malware encounter and infection rate trends in France and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

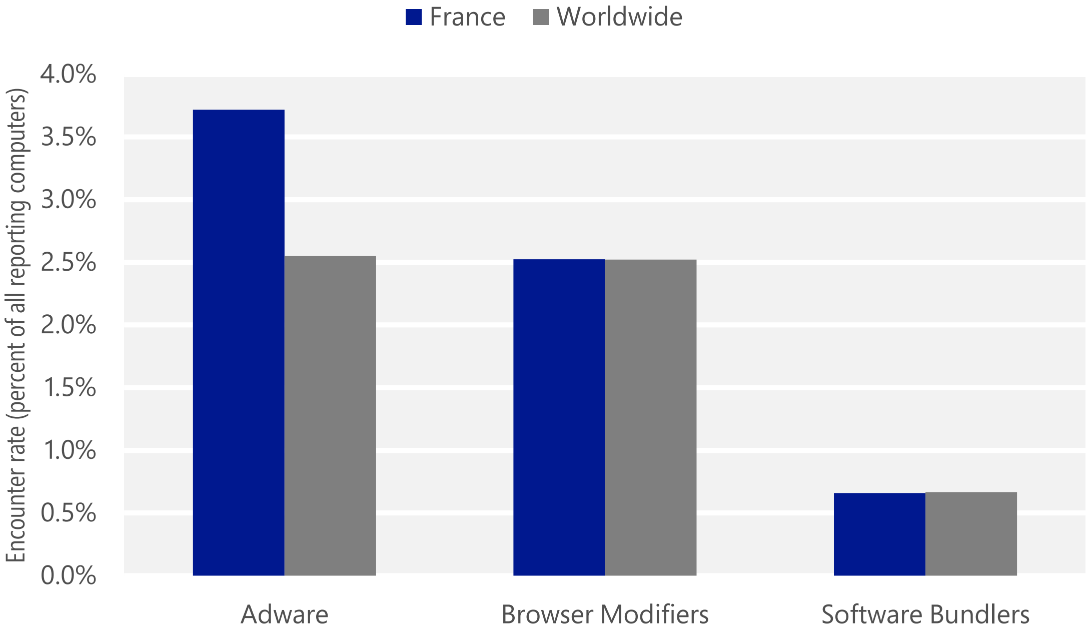
Malware encountered in France in 4Q14, by category



- The most common malware category in France in 4Q14 was Downloaders & Droppers. It was encountered by 2.3 percent of all computers there, down from 10.3 percent in 3Q14.
- The second most common malware category in France in 4Q14 was Trojans. It was encountered by 2.2 percent of all computers there, down from 4.1 percent in 3Q14.
- The third most common malware category in France in 4Q14 was Exploits, which was encountered by 1.6 percent of all computers there, down from 2.3 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in France in 4Q14, by category



- The most common unwanted software category in France in 4Q14 was Adware. It was encountered by 3.7 percent of all computers there, down from 7.8 percent in 3Q14.
- The second most common unwanted software category in France in 4Q14 was Browser Modifiers. It was encountered by 2.5 percent of all computers there, down from 5.1 percent in 3Q14.
- The third most common unwanted software category in France in 4Q14 was Software Bundlers, which was encountered by 0.7 percent of all computers there, up from 0.3 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in France in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Tugspay	Downloaders & Droppers	1.4%
2	Win32/Obfuscator	Obfuscators & Injectors	0.8%
3	JS/Axpergle	Exploits	0.6%
4	JS/Krypterade	Ransomware	0.6%
5	INF/Autorun	Obfuscators & Injectors	0.5%
6	JS/Fiexp	Exploits	0.4%
7	JS/Faceliker	Trojans	0.4%
8	Win32/Wysotot	Trojans	0.3%
9	VBS/Jenxcus	Worms	0.3%
10	ASX/Wimad	Downloaders & Droppers	0.3%

- The most common malware family encountered in France in 4Q14 was Win32/Tugspay, which was encountered by 1.4 percent of reporting computers there. Win32/Tugspay is a downloader that spreads by posing as an installer for legitimate software, such as a Java update, or through other malware. When installed, it downloads unwanted software to the computer.
- The second most common malware family encountered in France in 4Q14 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 France in 4Q14 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 4Q14 was JS/Krypterade, which was encountered by 0.6 percent of reporting computers there. JS/Krypterade is ransomware that fraudulently claims the computer has been used for unlawful activity, locks it, and demands that the user pay to unlock it.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in France in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	2.3%
2	Win32/Costmin	Adware	1.2%
3	Win32/BetterSurf	Adware	0.5%
4	Win32/Pennybee	Adware	0.5%
5	Win32/Couponarific	Adware	0.4%

- The most common unwanted software family encountered in France in 4Q14 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 France in 4Q14 was Win32/Costmin, which was encountered by 1.2 percent of reporting computers there. Win32/Costmin is an adware family that installs itself as a browser extension for Internet Explorer, Mozilla Firefox, and Google Chrome, and displays advertisements as the user browses the Internet.
- The third most common unwanted software family encountered in France in 4Q14 was Win32/BetterSurf, which was encountered by 0.5 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.

Top threat families by infection rate

The most common malware families by infection rate in France in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Wysotot	Trojans	0.8
2	VBS/Jenxcus	Worms	0.5
3	Win32/Sefnit	Trojans	0.4
4	JS/Miuref	Trojans	0.2
5	Win32/Brontok	Worms	0.2
6	Win32/Alureon	Trojans	0.1
7	Win32/Zbot	Password Stealers & Monitoring Tools	0.1
8	MSIL/Bladabindi	Backdoors	0.1
9	Win32/Vobfus	Worms	0.1
10	Win32/Sality	Viruses	0.1

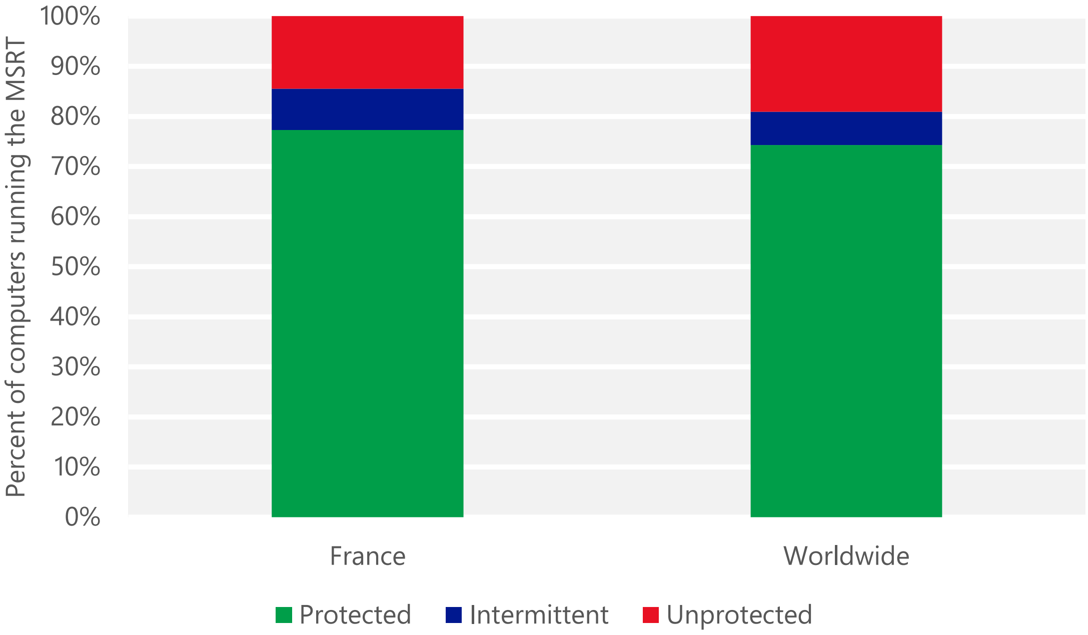
- The most common threat family infecting computers in France in 4Q14 was Win32/Wysotot, which was detected and removed from 0.8 of every 1,000 unique computers scanned by the MSRT. Win32/Wysotot is a threat that can change the start page of the user's web browser, and may download and install other files to the computer. It is installed by software bundlers that advertise free software or games.
- The second most common threat family infecting computers in France in 4Q14 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.
- The third most common threat family infecting computers in France in 4Q14 was Win32/Sefnit, which was detected and removed from 0.4 of every 1,000 unique computers scanned by the MSRT. Win32/Sefnit is a family of trojans that can allow backdoor access, download files, and use the computer and Internet connection for click fraud. Some variants can monitor web browsers and hijack search results.
- The fourth most common threat family infecting computers in France in 4Q14 was JS/Miuref, which was detected and removed from 0.2 of every 1,000 unique computers scanned by the MSRT. JS/Miuref is a family of malicious JavaScript files that redirect the web browser to show ads or download malware. They can be installed by other malware, including Win32/Fareit, or installed through spam email attachments.

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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.34 drive-by download URLs for every 1,000 URLs hosted in France, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.16 drive-by download URLs for every 1,000 URLs hosted in France, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in France and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, France	0.34	0.16
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Georgia

The statistics presented here are generated by Microsoft security programs and services running on computers in Georgia in 4Q14 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 succeds 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

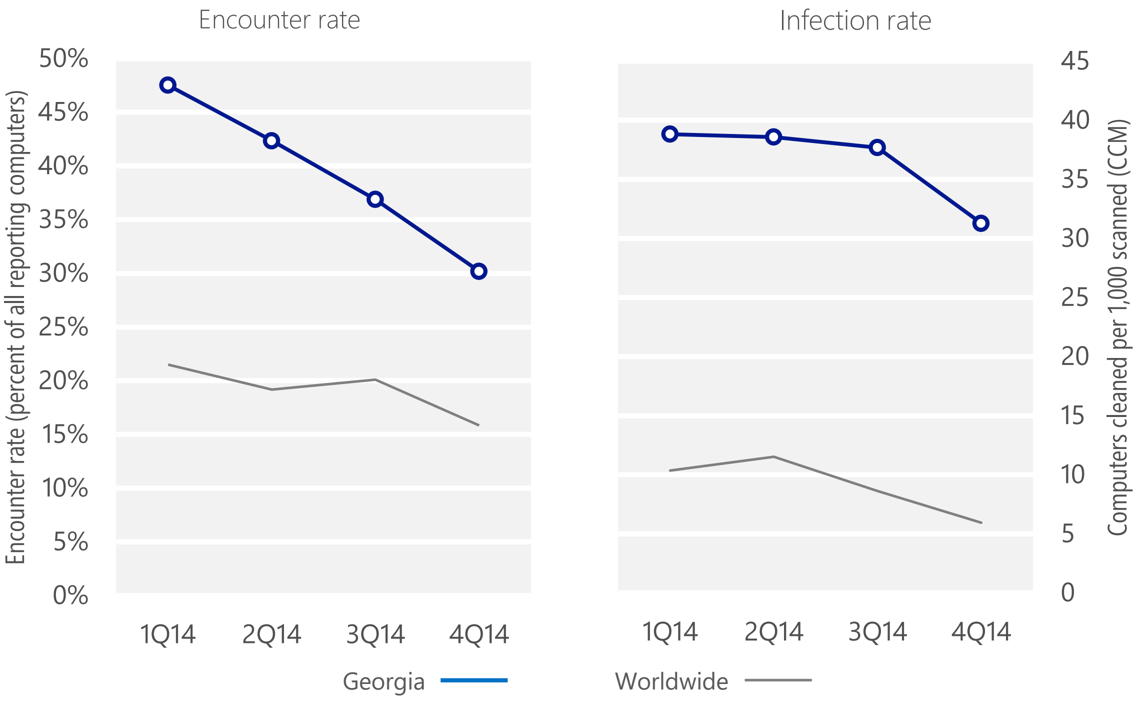
Metric	**1Q14**	**2Q14**	**3Q14**	**4Q14**
Encounter rate, Georgia	47.5%	42.3%	36.9%	30.2%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Georgia	38.8	38.6	37.7	31.3
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 30.2% percent of computers in Georgia encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 31.3 of every 1,000 unique computers scanned in Georgia in 4Q14 (a CCM score of 31.3, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Georgia over the last four quarters, compared to the world as a whole.

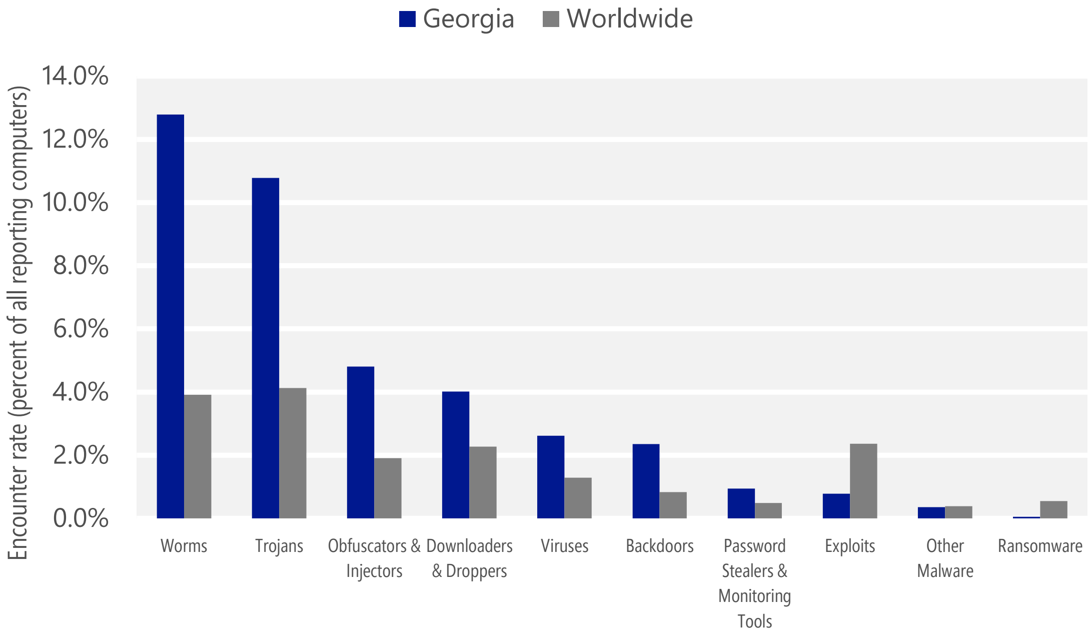
Malware encounter and infection rate trends in Georgia and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

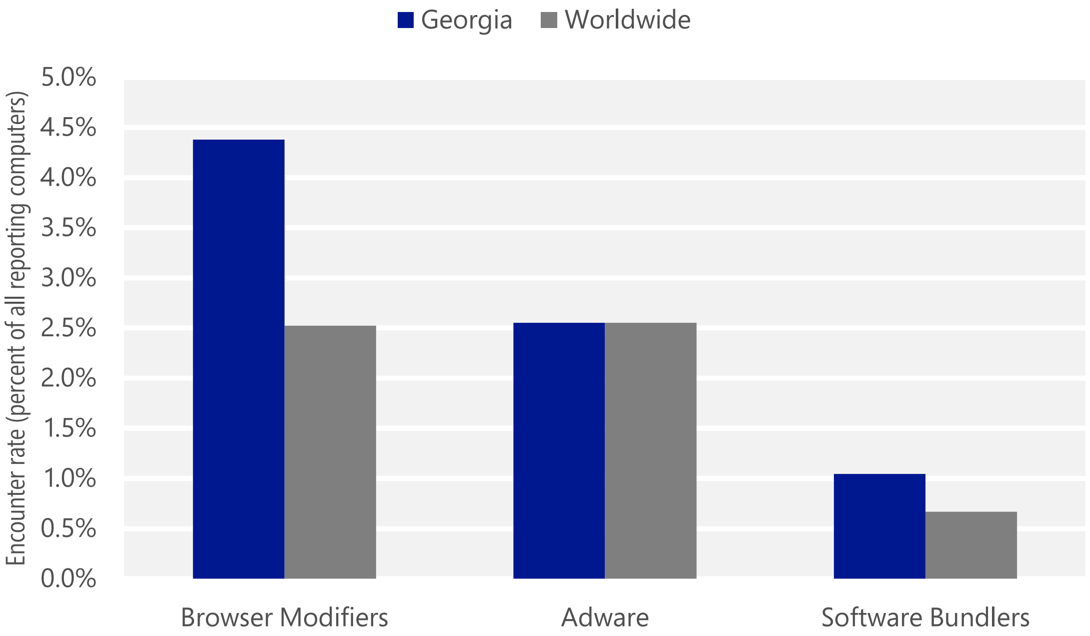
Malware encountered in Georgia in 4Q14, by category



- The most common malware category in Georgia in 4Q14 was Worms. It was encountered by 12.8 percent of all computers there, down from 18.5 percent in 3Q14.
- The second most common malware category in Georgia in 4Q14 was Trojans. It was encountered by 10.8 percent of all computers there, down from 13.5 percent in 3Q14.
- The third most common malware category in Georgia in 4Q14 was Obfuscators & Injectors, which was encountered by 4.8 percent of all computers there, down from 7.0 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Georgia in 4Q14, by category



- The most common unwanted software category in Georgia in 4Q14 was Browser Modifiers. It was encountered by 4.4 percent of all computers there, down from 5.8 percent in 3Q14.
- The second most common unwanted software category in Georgia in 4Q14 was Adware. It was encountered by 2.6 percent of all computers there, up from 0.5 percent in 3Q14.
- The third most common unwanted software category in Georgia in 4Q14 was Software Bundlers, which was encountered by 1.0 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Georgia in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Gamarue	Worms	4.6%
2	JS/Kilim	Trojans	3.7%
3	Win32/Tophos	Worms	3.1%
4	Win32/Obfuscator	Obfuscators & Injectors	2.7%
5	Win32/Ogimant	Downloaders & Droppers	2.3%
6	INF/Autorun	Obfuscators & Injectors	2.2%
7	Win32/Brontok	Worms	2.1%
8	Win32/Sality	Viruses	1.3%
9	Win32/Peaac	Trojans	1.2%
10	Win32/Vermis	Worms	1.2%

- The most common malware family encountered in Georgia in 4Q14 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 second most common malware family encountered in Georgia in 4Q14 was JS/Kilim, which was encountered by 3.7 percent of reporting computers there. JS/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 4Q14 was Win32/Tophos, which was encountered by 3.1 percent of reporting computers there. Win32/Tophos is a worm that copies itself to network shares and removable drives, displays an adult-oriented image, and may download additional malware.
- The fourth most common malware family encountered in Georgia in 4Q14 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.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Georgia in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	3.6%
2	Win32/BetterSurf	Adware	1.5%
3	Win32/Costmin	Adware	1.0%
4	Win32/Defaulttab	Browser Modifiers	0.9%
5	Win32/Gofileexpress	Software Bundlers	0.8%

- The most common unwanted software family encountered in Georgia in 4Q14 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 Georgia in 4Q14 was Win32/BetterSurf, which was encountered by 1.5 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.
- The third most common unwanted software family encountered in Georgia in 4Q14 was Win32/Costmin, which was encountered by 1.0 percent of reporting computers there. Win32/Costmin is an adware family that installs itself as a browser extension for Internet Explorer, Mozilla Firefox, and Google Chrome, and displays advertisements as the user browses the Internet.

Top threat families by infection rate

The most common malware families by infection rate in Georgia in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	JS/Kilim	Trojans	7.0
2	Win32/Gamarue	Worms	6.0
3	Win32/Sality	Viruses	4.3
4	Win32/Brontok	Worms	3.8
5	Win32/Ramnit	Trojans	2.3
6	Win32/Jeefo	Viruses	2.0
7	Win32/Dorkbot	Worms	1.4
8	Win32/Helompy	Worms	1.4
9	Win32/Nuqel	Worms	1.4
10	Win32/Lethic	Trojans	0.8

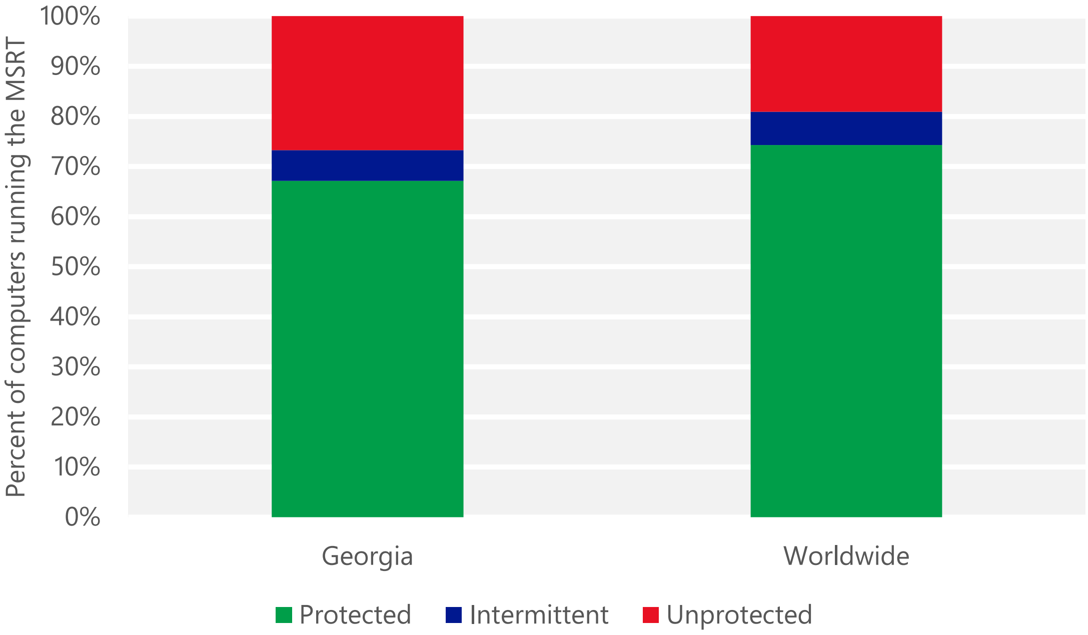
- The most common threat family infecting computers in Georgia in 4Q14 was JS/Kilim, which was detected and removed from 7.0 of every 1,000 unique computers scanned by the MSRT. JS/Kilim is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks 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 threat family infecting computers in Georgia in 4Q14 was Win32/Gamarue, which was detected and removed from 6.0 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 third most common threat family infecting computers in Georgia in 4Q14 was Win32/Sality, which was detected and removed from 4.3 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 Georgia in 4Q14 was Win32/Brontok, which was detected and removed from 3.8 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 Georgia and worldwide protected by real-time security software in 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.16 drive-by download URLs for every 1,000 URLs hosted in Georgia, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.19 drive-by download URLs for every 1,000 URLs hosted in Georgia, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Georgia and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Georgia	0.16	0.19
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Germany

The statistics presented here are generated by Microsoft security programs and services running on computers in Germany in 4Q14 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 succeds 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

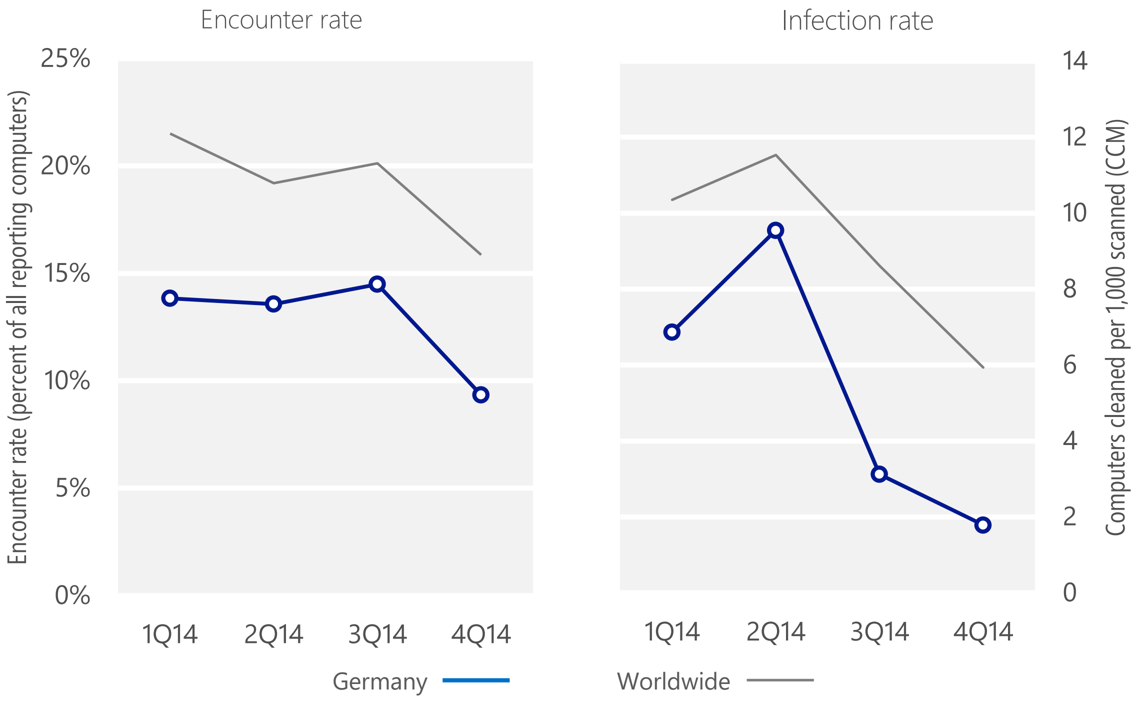
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Germany	13.8%	13.6%	14.5%	9.3%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Germany	6.9	9.5	3.1	1.8
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 9.3% percent of computers in Germany encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 1.8 of every 1,000 unique computers scanned in Germany in 4Q14 (a CCM score of 1.8, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Germany over the last four quarters, compared to the world as a whole.

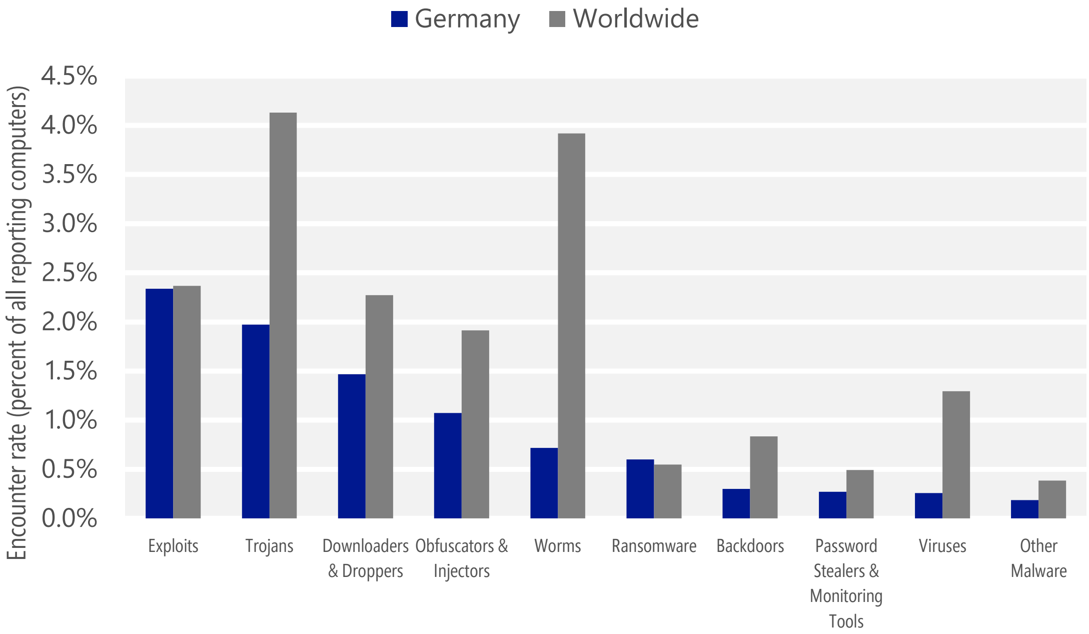
Malware encounter and infection rate trends in Germany and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

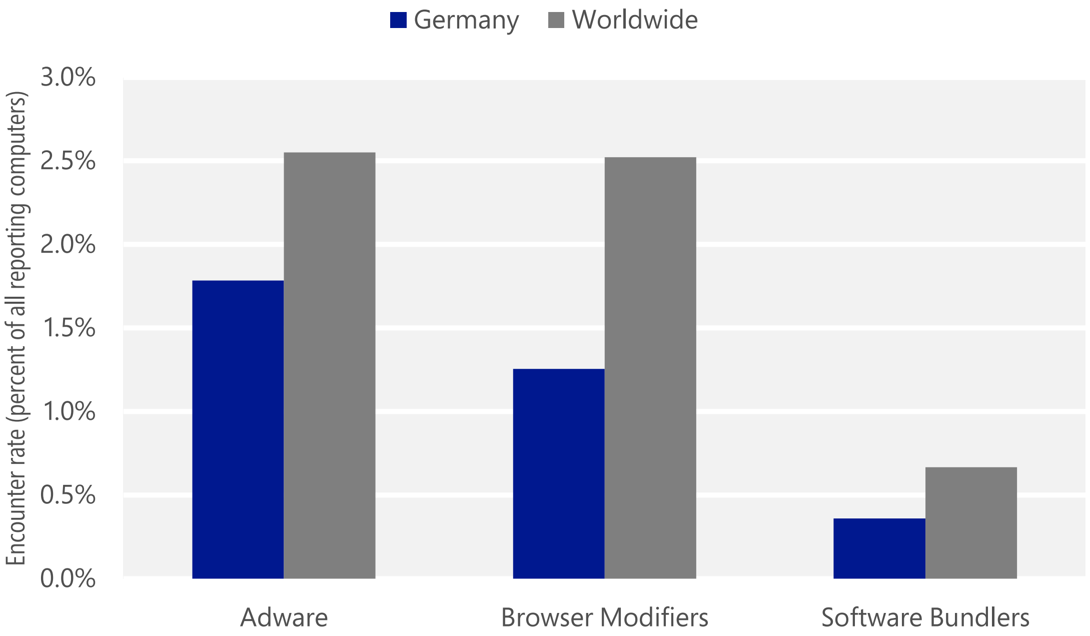
Malware encountered in Germany in 4Q14, by category



- The most common malware category in Germany in 4Q14 was Exploits. It was encountered by 2.3 percent of all computers there, down from 5.7 percent in 3Q14.
- The second most common malware category in Germany in 4Q14 was Trojans. It was encountered by 2.0 percent of all computers there, down from 2.7 percent in 3Q14.
- The third most common malware category in Germany in 4Q14 was Downloaders & Droppers, which was encountered by 1.5 percent of all computers there, down from 2.7 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Germany in 4Q14, by category



- The most common unwanted software category in Germany in 4Q14 was Adware. It was encountered by 1.8 percent of all computers there, down from 4.1 percent in 3Q14.
- The second most common unwanted software category in Germany in 4Q14 was Browser Modifiers. It was encountered by 1.3 percent of all computers there, down from 1.7 percent in 3Q14.
- The third most common unwanted software category in Germany in 4Q14 was Software Bundlers, which was encountered by 0.4 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Germany in 4Q14

	Family	Most significant category	% of reporting computers
1	JS/Axpergle	Exploits	1.6%
2	Win32/Obfuscator	Obfuscators & Injectors	0.8%
3	Win32/Tugspay	Downloaders & Droppers	0.8%
4	JS/Krypterade	Ransomware	0.3%
5	Win32/Emotet	Trojans	0.3%
6	Win32/Anogre	Exploits	0.2%
7	Win32/Dynamer	Trojans	0.2%
8	INF/Autorun	Obfuscators & Injectors	0.2%
9	Win32/Gamarue	Worms	0.2%
10	Win32/CeeInject	Obfuscators & Injectors	0.2%

- The most common malware family encountered in Germany in 4Q14 was JS/Axpergle, which was encountered by 1.6 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 second most common malware family encountered in Germany in 4Q14 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 Germany in 4Q14 was Win32/Tugspay, which was encountered by 0.8 percent of reporting computers there. Win32/Tugspay is a downloader that spreads by posing as an installer for legitimate software, such as a Java update, or through other malware. When installed, it downloads unwanted software to the computer.
- The fourth most common malware family encountered in Germany in 4Q14 was JS/Krypterade, which was encountered by 0.3 percent of reporting computers there. JS/Krypterade is ransomware that fraudulently claims the computer has been used for unlawful activity, locks it, and demands that the user pay to unlock it.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Germany in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	1.1%
2	Win32/Costmin	Adware	0.5%
3	Win32/BetterSurf	Adware	0.3%
4	Win32/Pennybee	Adware	0.3%
5	Win32/Couponarific	Adware	0.2%

- The most common unwanted software family encountered in Germany in 4Q14 was Win32/Couponruc, which was encountered by 1.1 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 Germany in 4Q14 was Win32/Costmin, which was encountered by 0.5 percent of reporting computers there. Win32/Costmin is an adware family that installs itself as a browser extension for Internet Explorer, Mozilla Firefox, and Google Chrome, and displays advertisements as the user browses the Internet.
- The third most common unwanted software family encountered in Germany in 4Q14 was Win32/BetterSurf, which was encountered by 0.3 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.

Top threat families by infection rate

The most common malware families by infection rate in Germany in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Wysotot	Trojans	0.2
2	Win32/Sefnit	Trojans	0.2
3	Win32/Matsnu	Trojans	0.2
4	Win32/Zbot	Password Stealers & Monitoring Tools	0.1
5	Win32/Ramnit	Trojans	0.1
6	Win32/Alureon	Trojans	0.1
7	VBS/Jenxcus	Worms	0.1
8	Win32/Gamarue	Worms	0.1
9	Win32/Sality	Viruses	0.1
10	Win32/Conficker	Worms	0.1

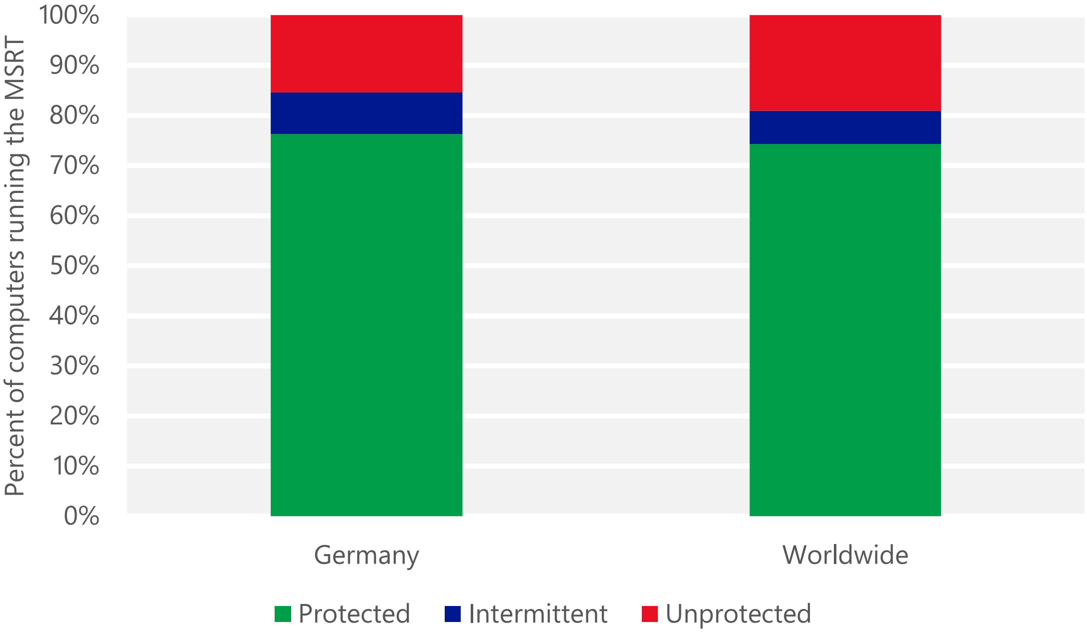
- The most common threat family infecting computers in Germany in 4Q14 was Win32/Wysotot, which was detected and removed from 0.2 of every 1,000 unique computers scanned by the MSRT. Win32/Wysotot is a threat that can change the start page of the user's web browser, and may download and install other files to the computer. It is installed by software bundlers that advertise free software or games.
- The second most common threat family infecting computers in Germany in 4Q14 was Win32/Sefnit, which was detected and removed from 0.2 of every 1,000 unique computers scanned by the MSRT. Win32/Sefnit is a family of trojans that can allow backdoor access, download files, and use the computer and Internet connection for click fraud. Some variants can monitor web browsers and hijack search results.
- The third most common threat family infecting computers in Germany in 4Q14 was Win32/Matsnu, which was detected and removed from 0.2 of every 1,000 unique computers scanned by the MSRT. Win32/Matsnu is a malware family that can perform certain actions based on instructions from a remote server. It also changes certain computer settings.
- The fourth most common threat family infecting computers in Germany in 4Q14 was Win32/Zbot, which was detected and removed from 0.1 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.

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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.25 drive-by download URLs for every 1,000 URLs hosted in Germany, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.22 drive-by download URLs for every 1,000 URLs hosted in Germany, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Germany and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Germany	0.25	0.22
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Greece

The statistics presented here are generated by Microsoft security programs and services running on computers in Greece in 4Q14 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 succeds 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

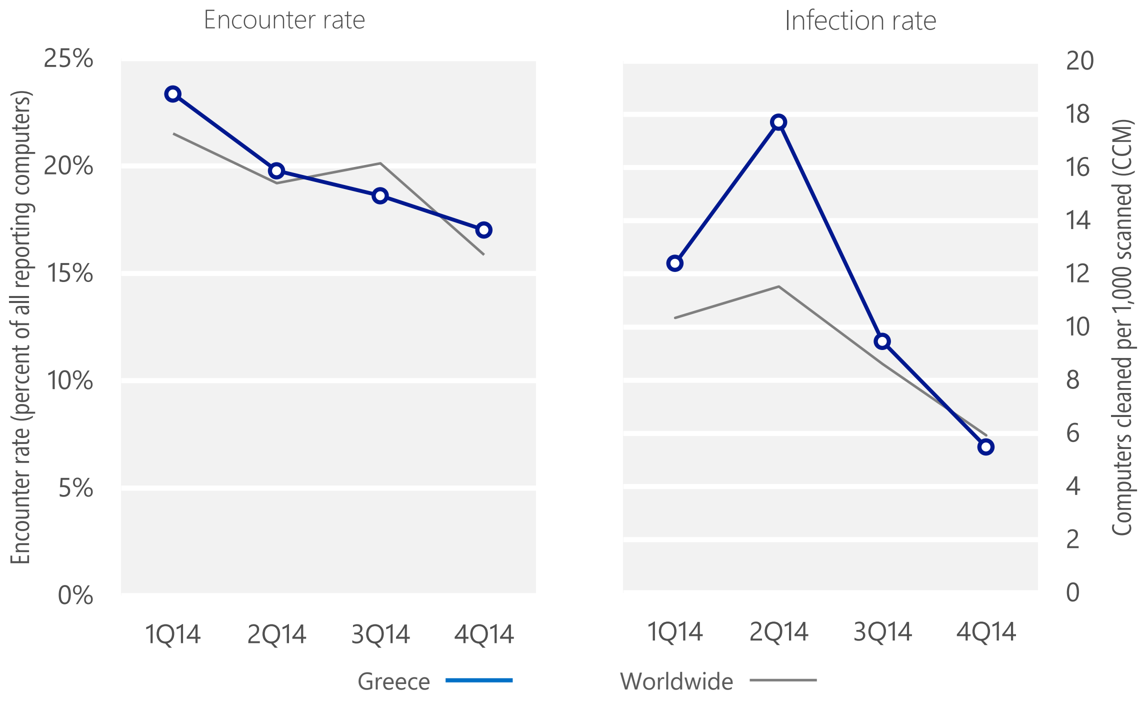
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Greece	23.4%	19.8%	18.6%	17.0%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Greece	12.4	17.7	9.5	5.5
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 17.0% percent of computers in Greece encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 5.5 of every 1,000 unique computers scanned in Greece in 4Q14 (a CCM score of 5.5, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Greece over the last four quarters, compared to the world as a whole.

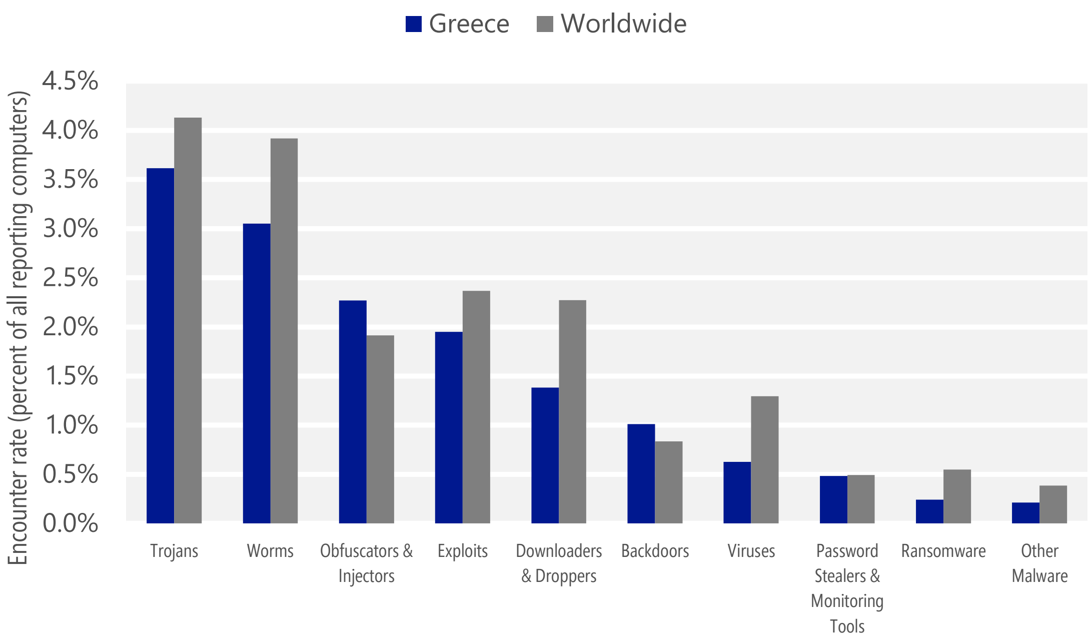
Malware encounter and infection rate trends in Greece and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

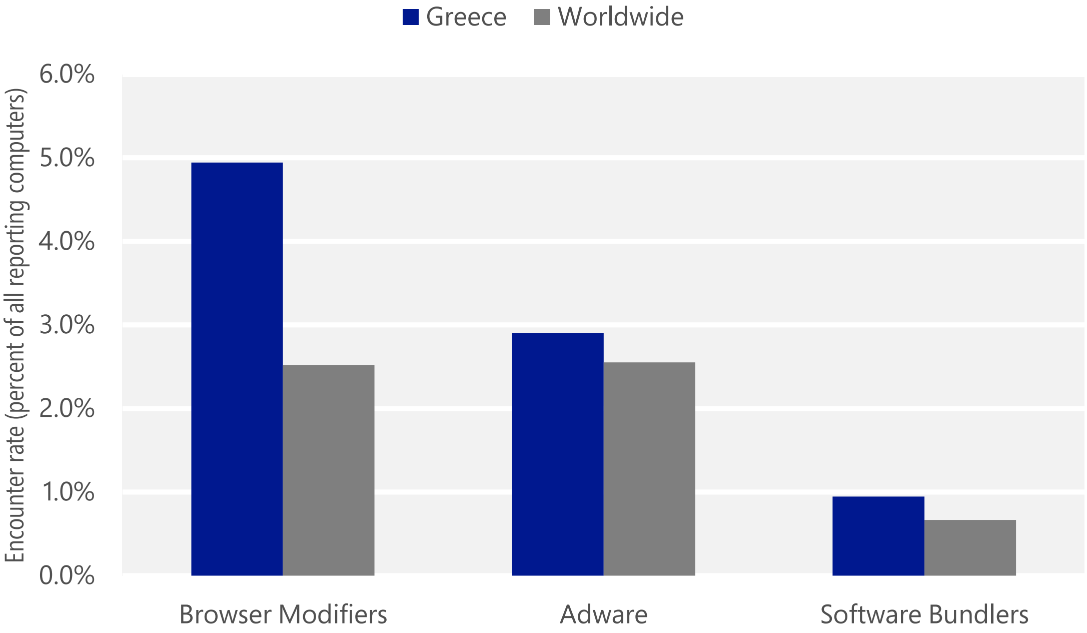
Malware encountered in Greece in 4Q14, by category



- The most common malware category in Greece in 4Q14 was Trojans. It was encountered by 3.6 percent of all computers there, down from 5.5 percent in 3Q14.
- The second most common malware category in Greece in 4Q14 was Worms. It was encountered by 3.1 percent of all computers there, down from 3.9 percent in 3Q14.
- The third most common malware category in Greece in 4Q14 was Obfuscators & Injectors, which was encountered by 2.3 percent of all computers there, down from 2.8 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Greece in 4Q14, by category



- The most common unwanted software category in Greece in 4Q14 was Browser Modifiers. It was encountered by 4.9 percent of all computers there, down from 6.1 percent in 3Q14.
- The second most common unwanted software category in Greece in 4Q14 was Adware. It was encountered by 2.9 percent of all computers there, up from 0.6 percent in 3Q14.
- The third most common unwanted software category in Greece in 4Q14 was Software Bundlers, which was encountered by 0.9 percent of all computers there, up from 0.2 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Greece in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Obfuscator	Obfuscators & Injectors	1.4%
2	INF/Autorun	Obfuscators & Injectors	1.3%
3	JS/Axpergle	Exploits	0.8%
4	Win32/Gamarue	Worms	0.6%
5	Win32/Conficker	Worms	0.5%
6	Win32/Anogre	Exploits	0.5%
7	Win32/Dynamer	Trojans	0.3%
8	VBS/Jenxcus	Worms	0.3%
9	Win32/Vobfus	Worms	0.3%
10	JS/Faceliker	Trojans	0.3%

- The most common malware family encountered in Greece in 4Q14 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 second most common malware family encountered in Greece in 4Q14 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 Greece in 4Q14 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 fourth most common malware family encountered in Greece in 4Q14 was Win32/Gamarue, which was encountered by 0.6 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 Greece in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	3.5%
2	Win32/Defaulttab	Browser Modifiers	1.6%
3	Win32/Costmin	Adware	1.4%
4	Win32/BetterSurf	Adware	1.0%
5	Win32/Gofileexpress	Software Bundlers	0.7%

- The most common unwanted software family encountered in Greece in 4Q14 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 Greece in 4Q14 was Win32/Defaulttab, which was encountered by 1.6 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.

- The third most common unwanted software family encountered in Greece in 4Q14 was Win32/Costmin, which was encountered by 1.4 percent of reporting computers there. Win32/Costmin is an adware family that installs itself as a browser extension for Internet Explorer, Mozilla Firefox, and Google Chrome, and displays advertisements as the user browses the Internet.

Top threat families by infection rate

The most common malware families by infection rate in Greece in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Sality	Viruses	0.6
2	Win32/Sefnit	Trojans	0.5
3	VBS/Jenxcus	Worms	0.4
4	Win32/Brontok	Worms	0.4
5	Win32/Wysotot	Trojans	0.4
6	JS/Kilim	Trojans	0.4
7	Win32/Vobfus	Worms	0.3
8	Win32/Gamarue	Worms	0.3
9	Win32/Alureon	Trojans	0.2
10	Win32/Helompy	Worms	0.2

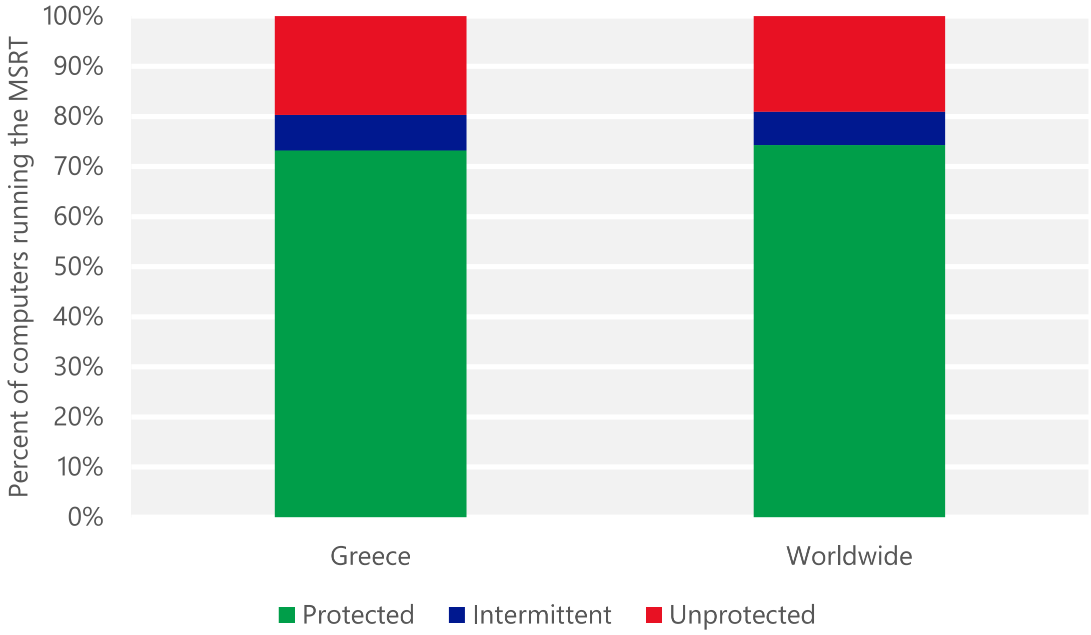
- The most common threat family infecting computers in Greece in 4Q14 was Win32/Sality, which was detected and removed from 0.6 of every 1,000 unique computers scanned by the MSRT. Win32/Sality is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The second most common threat family infecting computers in Greece in 4Q14 was Win32/Sefnit, which was detected and removed from 0.5 of every 1,000 unique computers scanned by the MSRT. Win32/Sefnit is a family of trojans that can allow backdoor access, download files, and use the computer and Internet connection for click fraud. Some variants can monitor web browsers and hijack search results.
- The third most common threat family infecting computers in Greece in 4Q14 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.
- The fourth most common threat family infecting computers in Greece in 4Q14 was Win32/Brontok, which was detected and removed from 0.4 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 Greece and worldwide protected by real-time security software in 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.25 drive-by download URLs for every 1,000 URLs hosted in Greece, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.21 drive-by download URLs for every 1,000 URLs hosted in Greece, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Greece and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Greece	0.25	0.21
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Guatemala

The statistics presented here are generated by Microsoft security programs and services running on computers in Guatemala in 4Q14 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 succeds 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

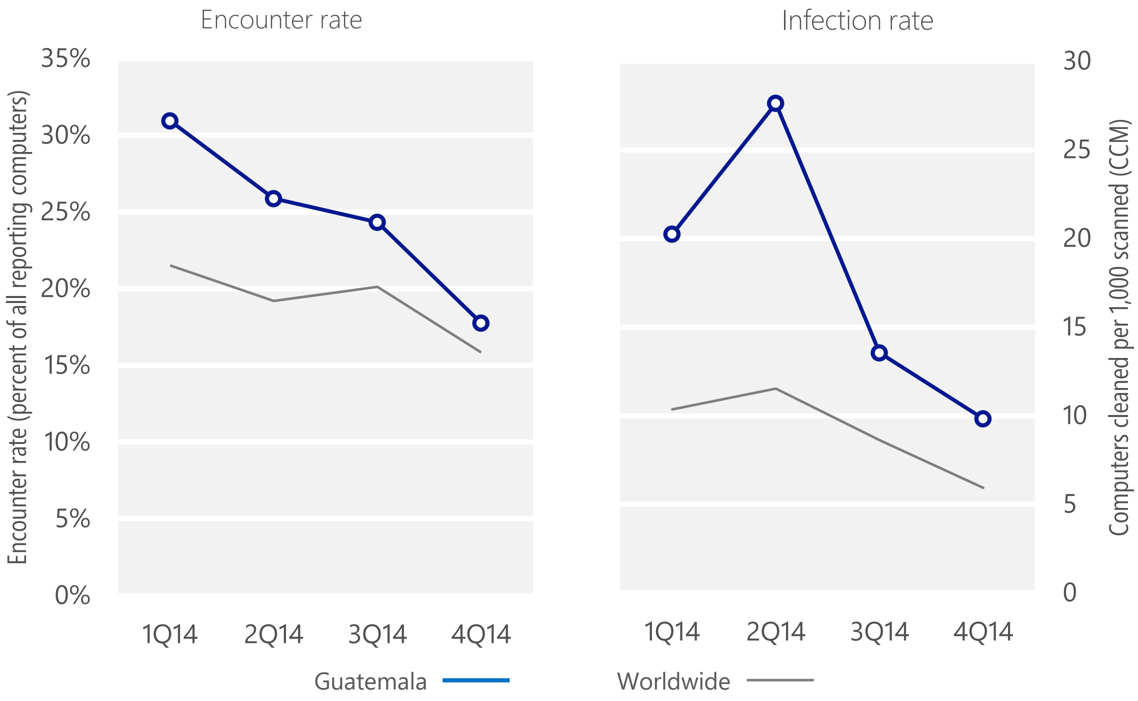
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Guatemala	30.9%	25.9%	24.3%	17.8%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Guatemala	20.2	27.6	13.5	9.8
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 17.8% percent of computers in Guatemala encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 9.8 of every 1,000 unique computers scanned in Guatemala in 4Q14 (a CCM score of 9.8, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Guatemala over the last four quarters, compared to the world as a whole.

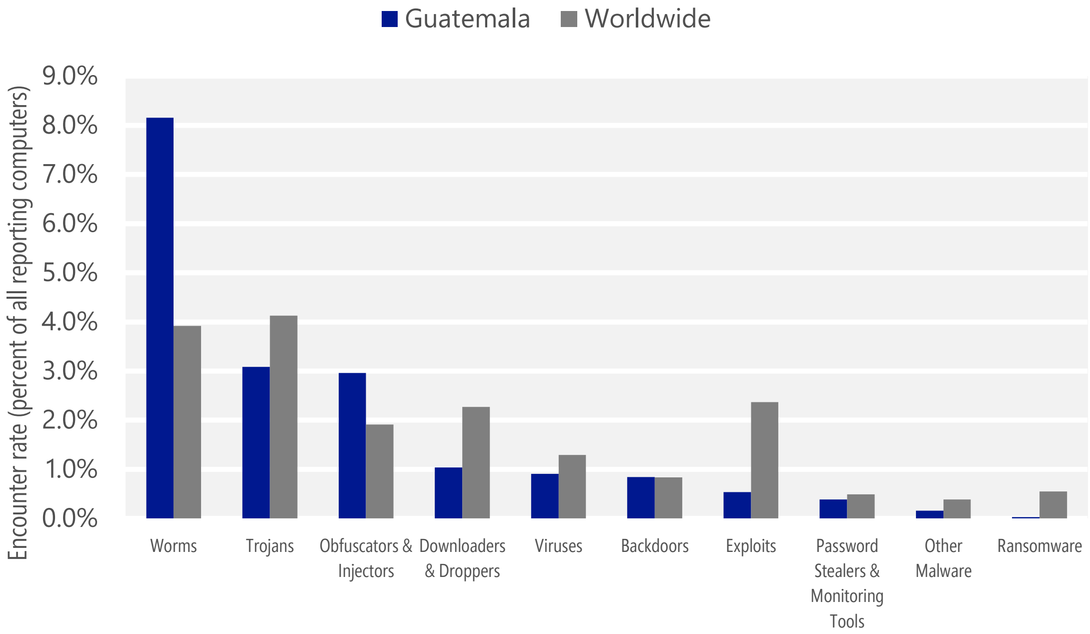
Malware encounter and infection rate trends in Guatemala and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

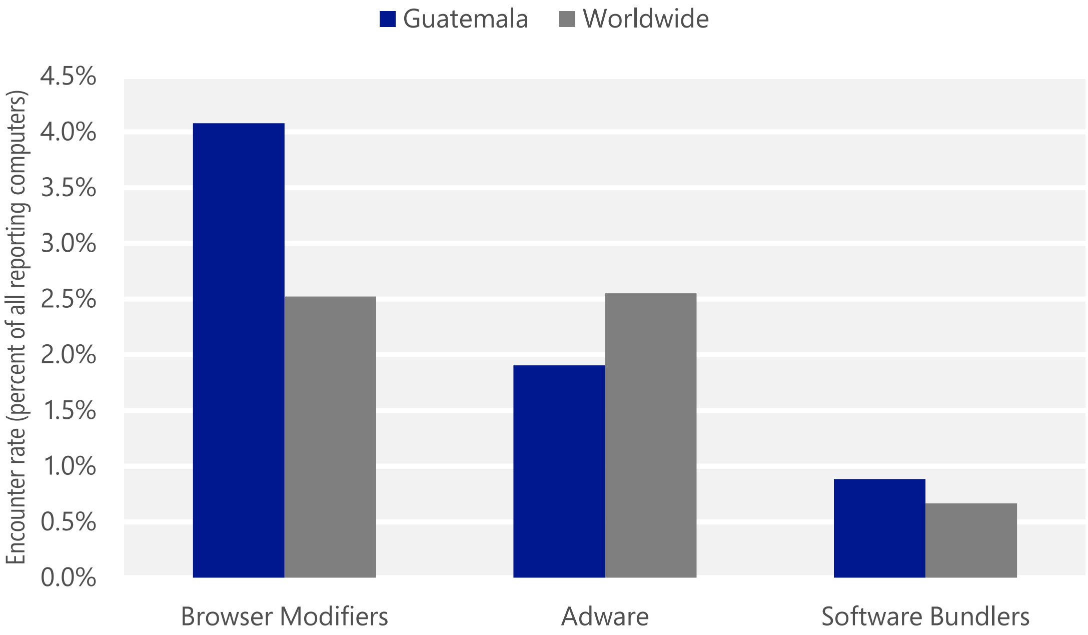
Malware encountered in Guatemala in 4Q14, by category



- The most common malware category in Guatemala in 4Q14 was Worms. It was encountered by 8.2 percent of all computers there, down from 12.5 percent in 3Q14.
- The second most common malware category in Guatemala in 4Q14 was Trojans. It was encountered by 3.1 percent of all computers there, down from 5.5 percent in 3Q14.
- The third most common malware category in Guatemala in 4Q14 was Obfuscators & Injectors, which was encountered by 3.0 percent of all computers there, down from 3.7 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Guatemala in 4Q14, by category



- The most common unwanted software category in Guatemala in 4Q14 was Browser Modifiers. It was encountered by 4.1 percent of all computers there, down from 5.2 percent in 3Q14.
- The second most common unwanted software category in Guatemala in 4Q14 was Adware. It was encountered by 1.9 percent of all computers there, up from 0.9 percent in 3Q14.
- The third most common unwanted software category in Guatemala in 4Q14 was Software Bundlers, which was encountered by 0.9 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Guatemala in 4Q14

	Family	Most significant category	% of reporting computers
1	JS/Proslikefan	Worms	2.4%
2	VBS/Jenxcus	Worms	1.9%
3	INF/Autorun	Obfuscators & Injectors	1.8%
4	Win32/Gamarue	Worms	1.3%
5	Win32/Vobfus	Worms	1.1%
6	Win32/Dorkbot	Worms	0.9%
7	Win32/Vermis	Worms	0.9%
8	Win32/CeeInject	Obfuscators & Injectors	0.7%
9	Win32/Conficker	Worms	0.7%

- The most common malware family encountered in Guatemala in 4Q14 was JS/Proslikefan, which was encountered by 2.4 percent of reporting computers there. JS/Proslikefan is a worm that spreads through removable drives, network shares, and P2P programs. It can lower the computer's security settings and disable antivirus products.
- The second most common malware family encountered in Guatemala in 4Q14 was VBS/Jenxcus, which was encountered by 1.9 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 Guatemala in 4Q14 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 Guatemala in 4Q14 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 Guatemala in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	3.1%
2	Win32/Defaulttab	Browser Modifiers	1.0%
3	Win32/Costmin	Adware	0.9%
4	Win32/BetterSurf	Adware	0.6%

- The most common unwanted software family encountered in Guatemala in 4Q14 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 Guatemala in 4Q14 was Win32/Defaulttab, which was encountered by 1.0 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.
- The third most common unwanted software family encountered in Guatemala in 4Q14 was Win32/Costmin, which was encountered by 0.9 percent of reporting computers there. Win32/Costmin is an adware family that installs itself as a browser extension for Internet Explorer, Mozilla Firefox, and Google Chrome, and displays advertisements as the user browses the Internet.

Top threat families by infection rate

The most common malware families by infection rate in Guatemala in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	2.6
2	Win32/Vobfus	Worms	1.4
3	Win32/Gamarue	Worms	1.1
4	Win32/Dorkbot	Worms	0.9
5	Win32/Sality	Viruses	0.9
6	Win32/Brontok	Worms	0.7
7	MSIL/Spacekito	Trojans	0.4
8	Win32/Lethic	Trojans	0.3
9	Win32/Sefnit	Trojans	0.2
10	Win32/Alureon	Trojans	0.2

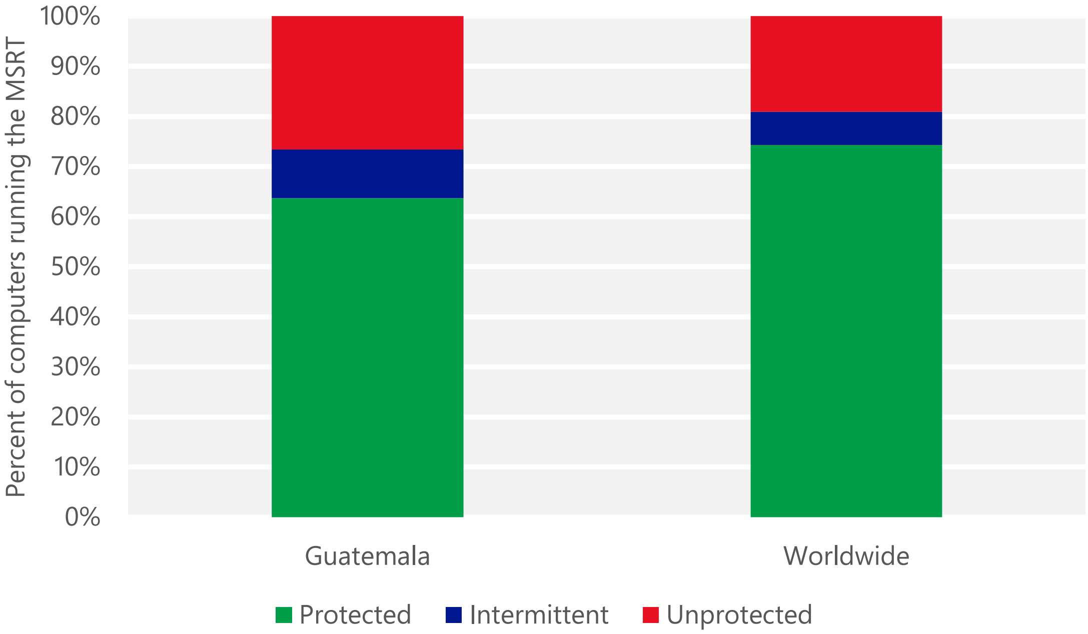
- The most common threat family infecting computers in Guatemala in 4Q14 was VBS/Jenxcus, which was detected and removed from 2.6 of every 1,000 unique computers scanned by the MSRT. VBS/Jenxcus is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Guatemala in 4Q14 was Win32/Vobfus, which was detected and removed from 1.4 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.
- The third most common threat family infecting computers in Guatemala in 4Q14 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 fourth most common threat family infecting computers in Guatemala in 4Q14 was Win32/Dorkbot, which was detected and removed from 0.9 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 Guatemala and worldwide protected by real-time security software in 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.00 drive-by download URLs for every 1,000 URLs hosted in Guatemala, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.03 drive-by download URLs for every 1,000 URLs hosted in Guatemala, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Guatemala and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Guatemala	0.00	0.03
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Honduras

The statistics presented here are generated by Microsoft security programs and services running on computers in Honduras in 4Q14 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 succeds 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

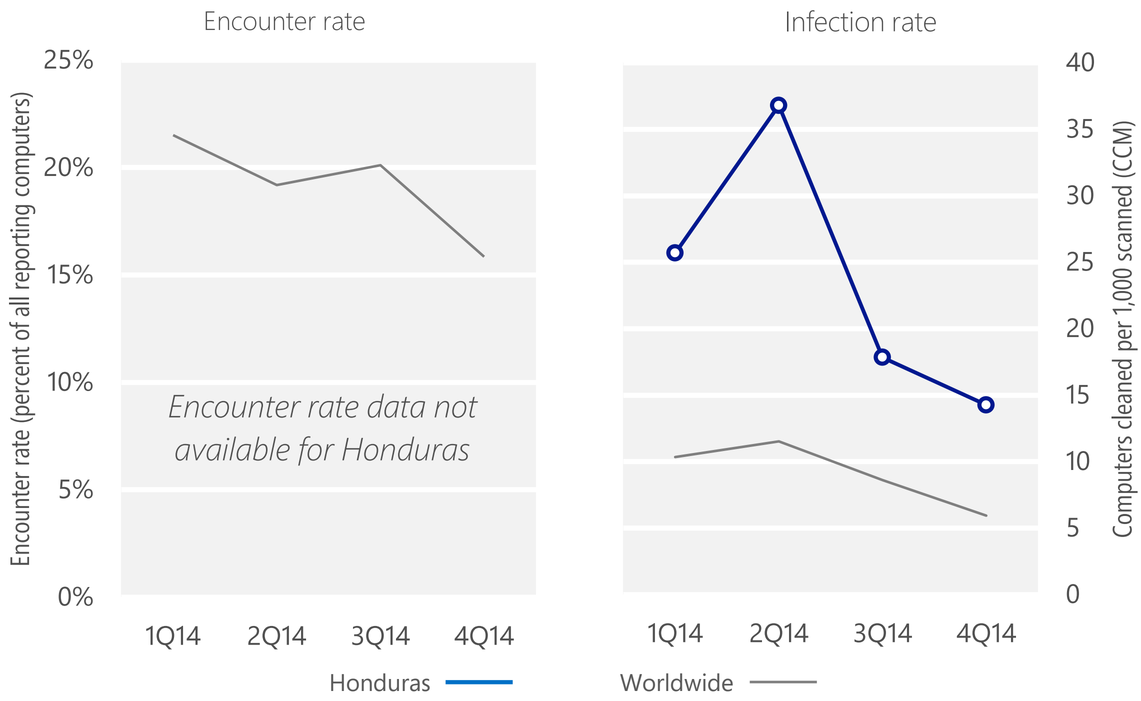
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Honduras	N/A	N/A	N/A	N/A
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Honduras	25.7	36.8	17.8	14.3
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, the MSRT detected and removed malware from 14.3 of every 1,000 unique computers scanned in Honduras in 4Q14 (a CCM score of 14.3, compared to the 4Q14 worldwide CCM of 5.9). 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 18* 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.

Top threat families by infection rate

The most common malware families by infection rate in Honduras in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	5.6
2	Win32/Sality	Viruses	1.9
3	Win32/Gamarue	Worms	1.2
4	Win32/Nuqel	Worms	0.9
5	Win32/Dorkbot	Worms	0.9
6	Win32/Brontok	Worms	0.7
7	Win32/Vobfus	Worms	0.6
8	MSIL/Spacekito	Trojans	0.6
9	Win32/Lethic	Trojans	0.4
10	Win32/Conficker	Worms	0.3

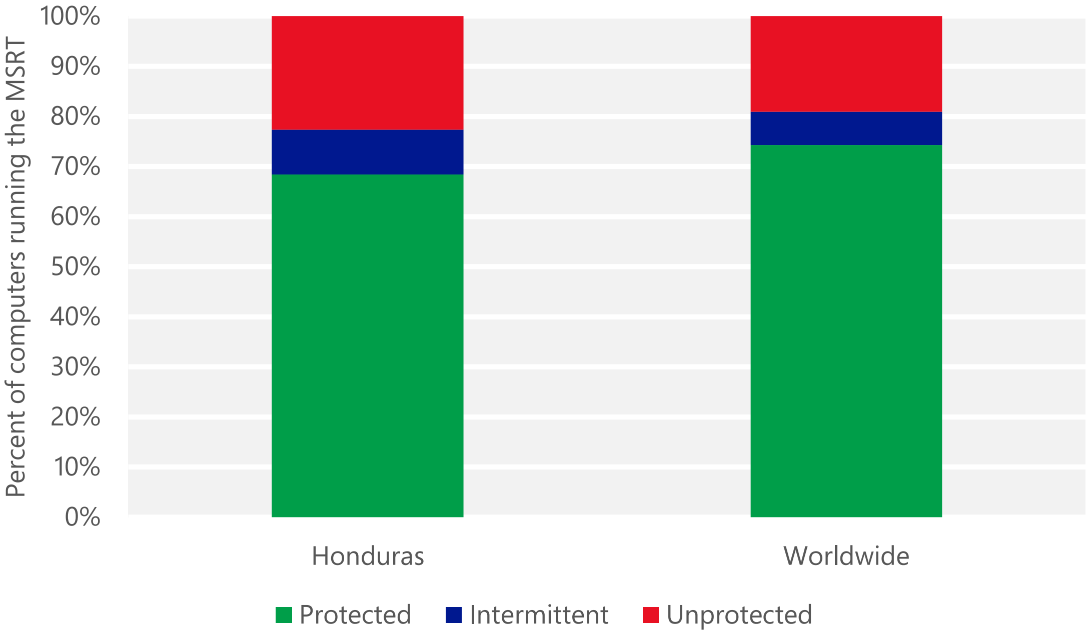
- The most common threat family infecting computers in Honduras in 4Q14 was VBS/Jenxcus, which was detected and removed from 5.6 of every 1,000 unique computers scanned by the MSRT. VBS/Jenxcus is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Honduras in 4Q14 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 third most common threat family infecting computers in Honduras in 4Q14 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 Honduras in 4Q14 was Win32/Nuqel, which was detected and removed from 0.9 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 Honduras and worldwide protected by real-time security software in 4Q14



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 4Q14 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 succeds 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.

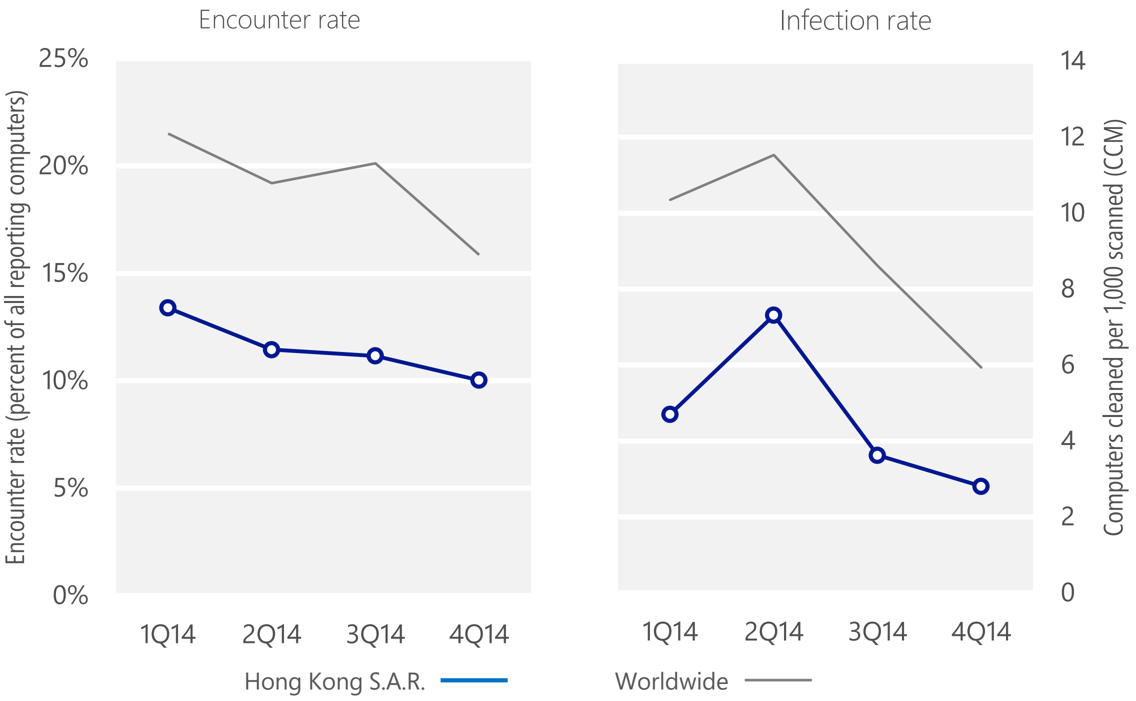
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Hong Kong S.A.R.	13.4%	11.4%	11.2%	10.0%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Hong Kong S.A.R.	4.7	7.3	3.6	2.8
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 10.0% percent of computers in Hong Kong S.A.R. encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 2.8 of every 1,000 unique computers scanned in Hong Kong S.A.R. in 4Q14 (a CCM score of 2.8, compared to the 4Q14 worldwide CCM of 5.9). 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.

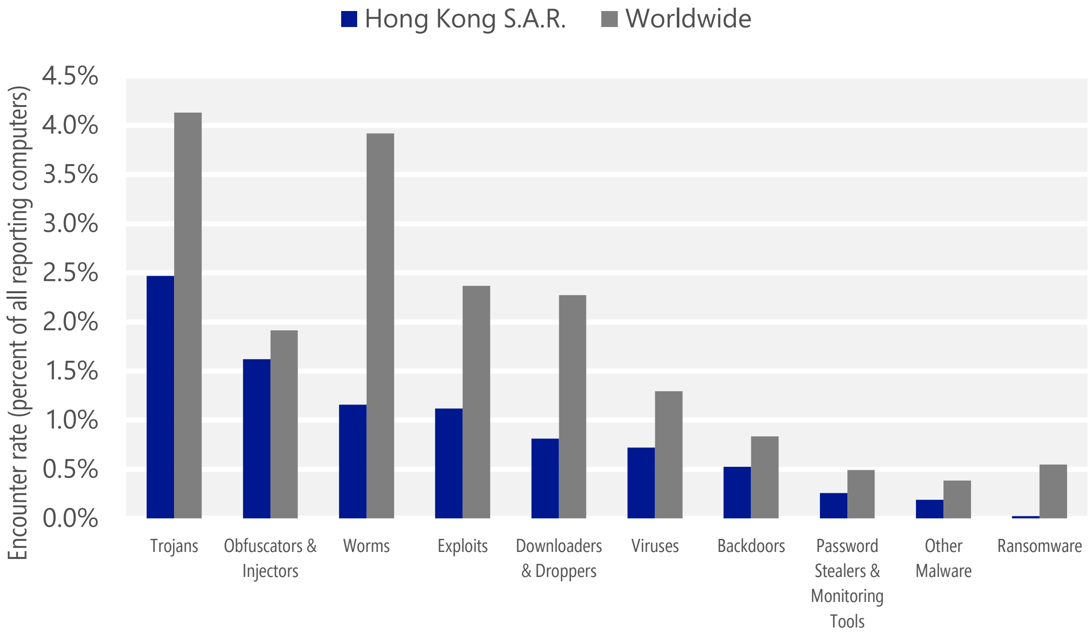
Malware encounter and infection rate trends in Hong Kong S.A.R. and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

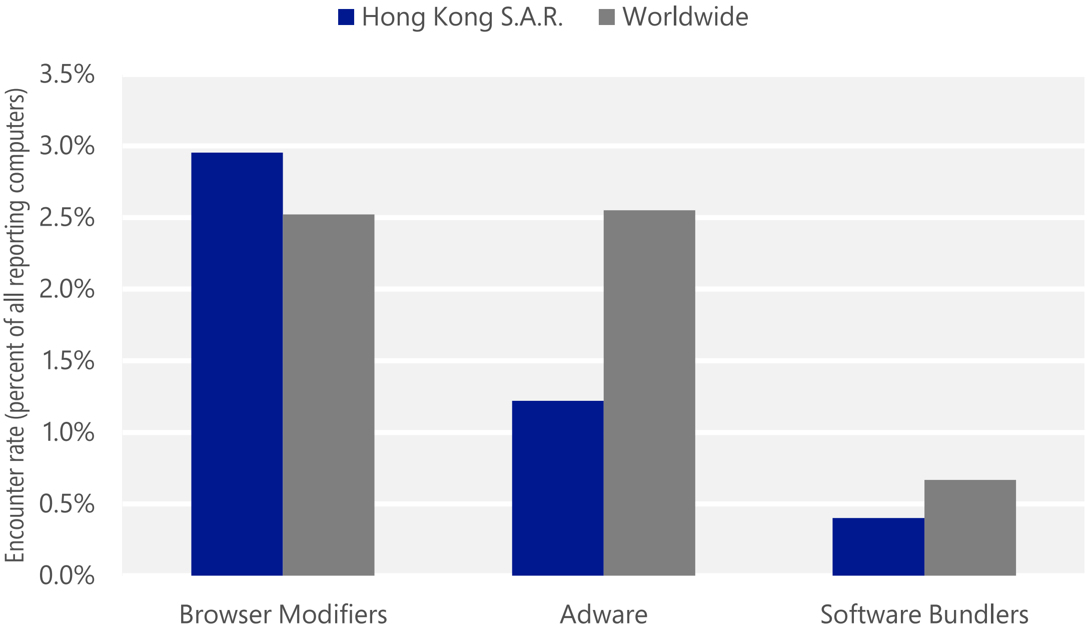
Malware encountered in Hong Kong S.A.R. in 4Q14, by category



- The most common malware category in Hong Kong S.A.R. in 4Q14 was Trojans. It was encountered by 2.5 percent of all computers there, down from 3.3 percent in 3Q14.
- The second most common malware category in Hong Kong S.A.R. in 4Q14 was Obfuscators & Injectors. It was encountered by 1.6 percent of all computers there, down from 1.8 percent in 3Q14.
- The third most common malware category in Hong Kong S.A.R. in 4Q14 was Worms, which was encountered by 1.2 percent of all computers there, down from 1.5 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Hong Kong S.A.R. in 4Q14, by category



- The most common unwanted software category in Hong Kong S.A.R. in 4Q14 was Browser Modifiers. It was encountered by 3.0 percent of all computers there, down from 3.3 percent in 3Q14.
- The second most common unwanted software category in Hong Kong S.A.R. in 4Q14 was Adware. It was encountered by 1.2 percent of all computers there, up from 0.2 percent in 3Q14.
- The third most common unwanted software category in Hong Kong S.A.R. in 4Q14 was Software Bundlers, which was encountered by 0.4 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Hong Kong S.A.R. in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Obfuscator	Obfuscators & Injectors	1.0%
2	INF/Autorun	Obfuscators & Injectors	0.7%
3	Win32/Anogre	Exploits	0.4%
4	Win32/Dynamer	Trojans	0.3%
5	Win32/Bumat	Trojans	0.2%
6	Win32/Conficker	Worms	0.2%
7	JS/Axpergle	Exploits	0.2%
8	Win32/Gamarue	Worms	0.2%
9	JS/Fiexp	Exploits	0.2%
10	JS/Redirector	Trojans	0.2%

- The most common malware family encountered in Hong Kong S.A.R. in 4Q14 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.
- The second most common malware family encountered in Hong Kong S.A.R. in 4Q14 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 Hong Kong S.A.R. in 4Q14 was Win32/Anogre, which was encountered by 0.4 percent of reporting computers there. Win32/Anogre is a threat that exploits a vulnerability addressed by Microsoft Security Bulletin MS11-087. This vulnerability can allow a hacker to install programs, view, change, or delete data or create new accounts with full administrative privileges.
- The fourth most common malware family encountered in Hong Kong S.A.R. in 4Q14 was Win32/Dynamer, which was encountered by 0.3 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 Hong Kong S.A.R. in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	2.3%
2	Win32/Defaulttab	Browser Modifiers	0.7%
3	Win32/Costmin	Adware	0.7%
4	Win32/BetterSurf	Adware	0.4%
5	Win32/Gofileexpress	Software Bundlers	0.3%

- The most common unwanted software family encountered in Hong Kong S.A.R. in 4Q14 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 4Q14 was Win32/Defaulttab, which was encountered by 0.7 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.

- The third most common unwanted software family encountered in Hong Kong S.A.R. in 4Q14 was Win32/Costmin, which was encountered by 0.7 percent of reporting computers there. Win32/Costmin is an adware family that installs itself as a browser extension for Internet Explorer, Mozilla Firefox, and Google Chrome, and displays advertisements as the user browses the Internet.

Top threat families by infection rate

The most common malware families by infection rate in Hong Kong S.A.R. in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Nitol	Other Malware	0.3
2	Win32/Ramnit	Trojans	0.3
3	Win32/Zbot	Password Stealers & Monitoring Tools	0.2
4	Win32/Necurs	Trojans	0.2
5	Win32/Alureon	Trojans	0.2
6	Win32/Sefnit	Trojans	0.2
7	Win32/Sality	Viruses	0.1
8	JS/Miuref	Trojans	0.1
9	Win32/Taterf	Worms	0.1
10	Win32/Brontok	Worms	0.1

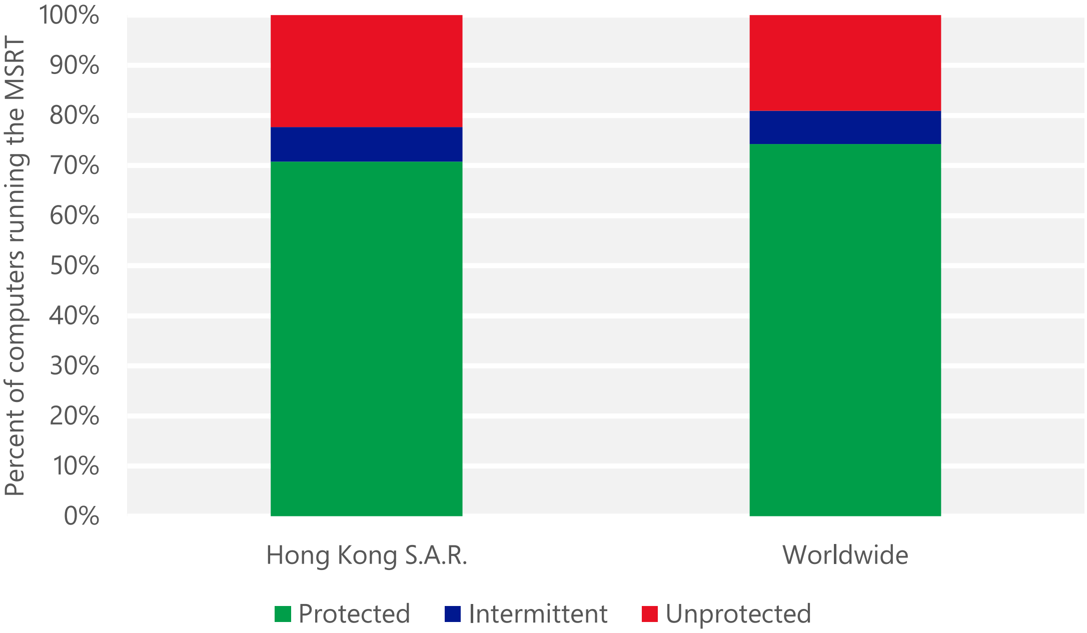
- The most common threat family infecting computers in Hong Kong S.A.R. in 4Q14 was Win32/Nitol, which was detected and removed from 0.3 of every 1,000 unique computers scanned by the MSRT. Win32/Nitol is a family of trojans that perform DDoS (distributed denial of service) attacks, allow backdoor access 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 Hong Kong S.A.R. in 4Q14 was Win32/Ramnit, which was detected and removed from 0.3 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 Hong Kong S.A.R. in 4Q14 was Win32/Zbot, which was detected and removed from 0.2 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 fourth most common threat family infecting computers in Hong Kong S.A.R. in 4Q14 was Win32/Necurs, which was detected and removed from 0.2 of every 1,000 unique computers scanned by the MSRT. Win32/Necurs is a family of malware that downloads additional malware,?including variants from the Win32/Sirefef and Win32/Medfos families,?and?enables backdoor access and control of 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 Hong Kong S.A.R. and worldwide protected by real-time security software in 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.79 drive-by download URLs for every 1,000 URLs hosted in Hong Kong S.A.R., compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.61 drive-by download URLs for every 1,000 URLs hosted in Hong Kong S.A.R., compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Hong Kong S.A.R. and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Hong Kong S.A.R.	0.79	0.61
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Hungary

The statistics presented here are generated by Microsoft security programs and services running on computers in Hungary in 4Q14 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 succeds 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

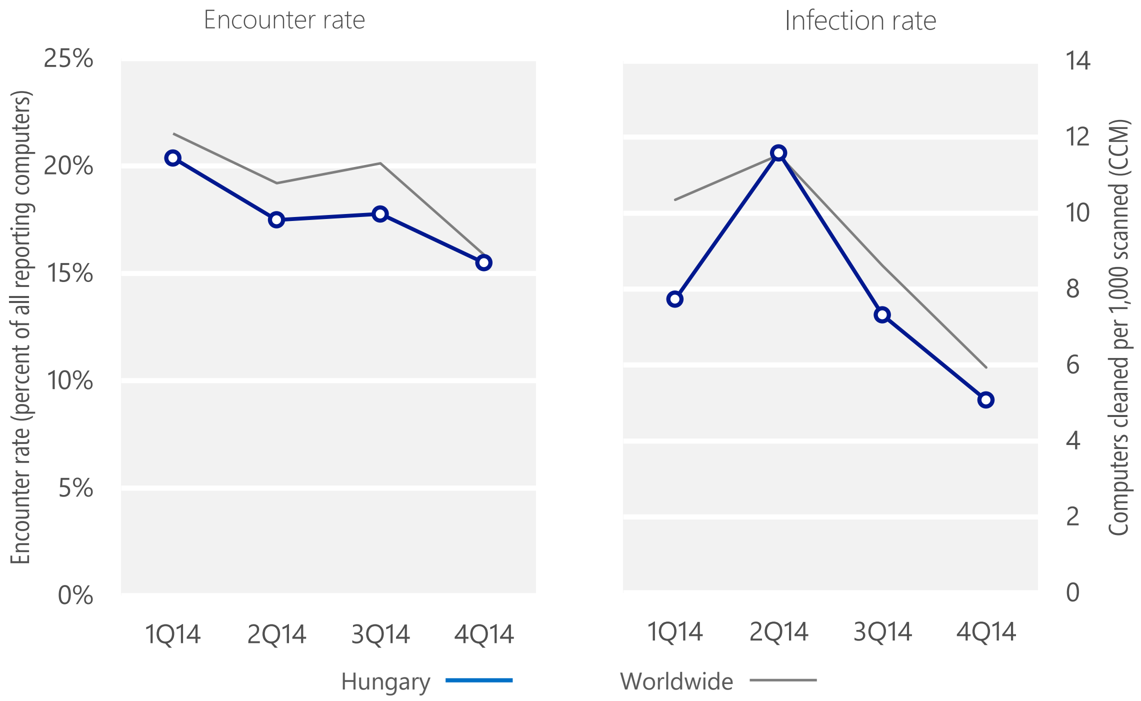
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Hungary	20.4%	17.5%	17.8%	15.5%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Hungary	7.7	11.6	7.3	5.1
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 15.5% percent of computers in Hungary encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 5.1 of every 1,000 unique computers scanned in Hungary in 4Q14 (a CCM score of 5.1, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Hungary over the last four quarters, compared to the world as a whole.

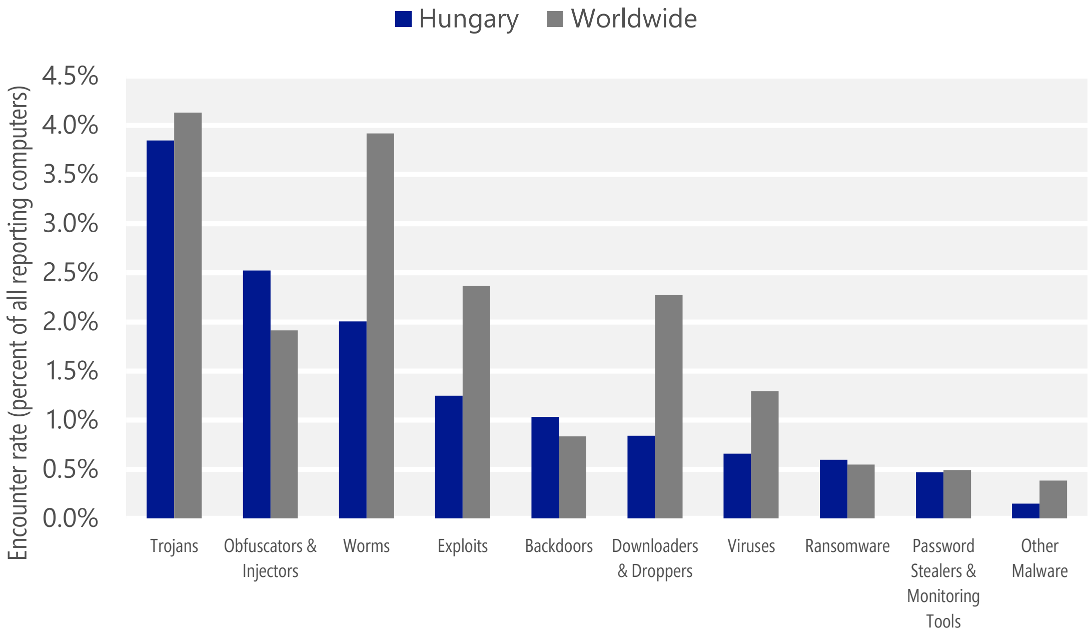
Malware encounter and infection rate trends in Hungary and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

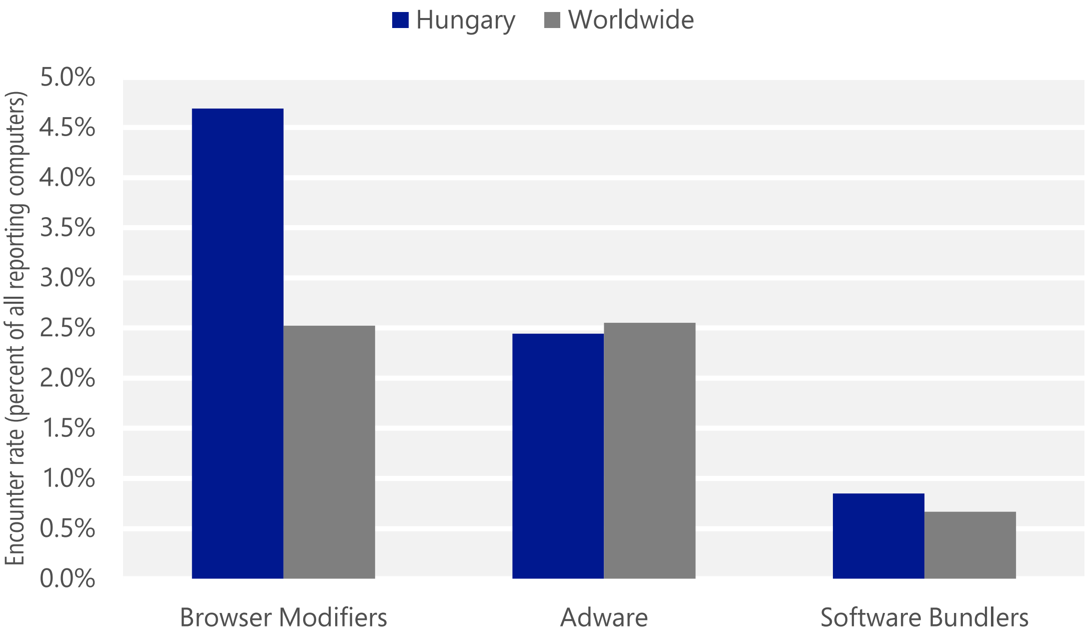
Malware encountered in Hungary in 4Q14, by category



- The most common malware category in Hungary in 4Q14 was Trojans. It was encountered by 3.8 percent of all computers there, down from 6.7 percent in 3Q14.
- The second most common malware category in Hungary in 4Q14 was Obfuscators & Injectors. It was encountered by 2.5 percent of all computers there, up from 2.4 percent in 3Q14.
- The third most common malware category in Hungary in 4Q14 was Worms, which was encountered by 2.0 percent of all computers there, down from 2.3 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Hungary in 4Q14, by category



- The most common unwanted software category in Hungary in 4Q14 was Browser Modifiers. It was encountered by 4.7 percent of all computers there, down from 6.1 percent in 3Q14.
- The second most common unwanted software category in Hungary in 4Q14 was Adware. It was encountered by 2.4 percent of all computers there, up from 0.5 percent in 3Q14.
- The third most common unwanted software category in Hungary in 4Q14 was Software Bundlers, which was encountered by 0.8 percent of all computers there, up from 0.2 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Hungary in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Obfuscator	Obfuscators & Injectors	1.7%
2	INF/Autorun	Obfuscators & Injectors	0.8%
3	Win32/Conficker	Worms	0.5%
4	JS/Axpergle	Exploits	0.5%
5	JS/Krypterade	Ransomware	0.4%
6	Win32/Orsam	Trojans	0.4%
7	Win32/Dynamer	Trojans	0.4%
8	Win32/Brontok	Worms	0.4%
9	Win32/Fynloski	Backdoors	0.3%
10	Win32/Sality	Viruses	0.3%

- The most common malware family encountered in Hungary in 4Q14 was Win32/Obfuscator, which was encountered by 1.7 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 Hungary in 4Q14 was INF/Autorun, which was encountered by 0.8 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 Hungary in 4Q14 was Win32/Conficker, which was encountered by 0.5 percent of reporting computers there. Win32/Conficker is a worm that spreads by exploiting a vulnerability addressed by Security Bulletin MS08-067. Some variants also spread via removable drives and by exploiting weak passwords. It disables several important system services and security products, and downloads arbitrary files.
- The fourth most common malware family encountered in Hungary in 4Q14 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 Hungary in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	4.0%
2	Win32/Costmin	Adware	1.2%
3	Win32/BetterSurf	Adware	1.0%
4	Win32/Defaulttab	Browser Modifiers	0.7%
5	Win32/Gofileexpress	Software Bundlers	0.7%

- The most common unwanted software family encountered in Hungary in 4Q14 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 Hungary in 4Q14 was Win32/Costmin, which was encountered by 1.2 percent of reporting computers there. Win32/Costmin is an adware family that installs itself as a browser extension for Internet Explorer, Mozilla Firefox, and Google Chrome, and displays advertisements as the user browses the Internet.
- The third most common unwanted software family encountered in Hungary in 4Q14 was Win32/BetterSurf, which was encountered by 1.0 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.

Top threat families by infection rate

The most common malware families by infection rate in Hungary in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Sality	Viruses	1.1
2	JS/Kilim	Trojans	0.8
3	Win32/Brontok	Worms	0.8
4	MSIL/Bladabindi	Backdoors	0.3
5	Win32/Sefnit	Trojans	0.3
6	Win32/Ramnit	Trojans	0.3
7	Win32/Jeefo	Viruses	0.2
8	Win32/Pramro	Trojans	0.2
9	VBS/Jenxcus	Worms	0.1
10	Win32/Wysotot	Trojans	0.1

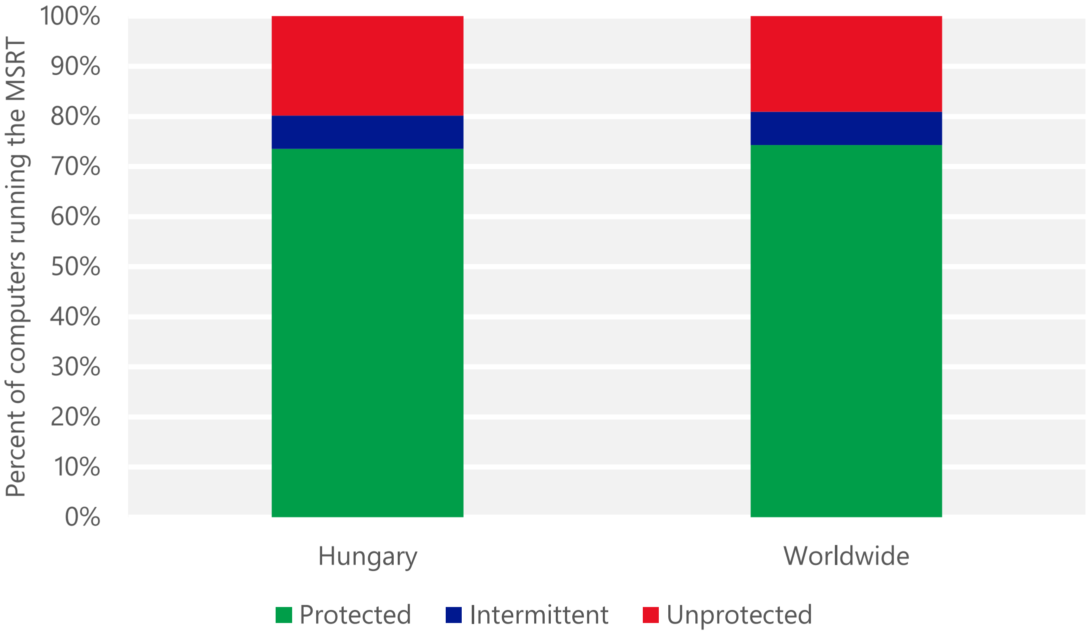
- The most common threat family infecting computers in Hungary in 4Q14 was Win32/Sality, which was detected and removed from 1.1 of every 1,000 unique computers scanned by the MSRT. Win32/Sality is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The second most common threat family infecting computers in Hungary in 4Q14 was JS/Kilim, which was detected and removed from 0.8 of every 1,000 unique computers scanned by the MSRT. JS/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 4Q14 was Win32/Brontok, which was detected and removed from 0.8 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 Hungary in 4Q14 was MSIL/Bladabindi, which was detected and removed from 0.3 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 Hungary and worldwide protected by real-time security software in 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.33 drive-by download URLs for every 1,000 URLs hosted in Hungary, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.39 drive-by download URLs for every 1,000 URLs hosted in Hungary, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Hungary and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Hungary	0.33	0.39
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Iceland

The statistics presented here are generated by Microsoft security programs and services running on computers in Iceland in 4Q14 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 succeds 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

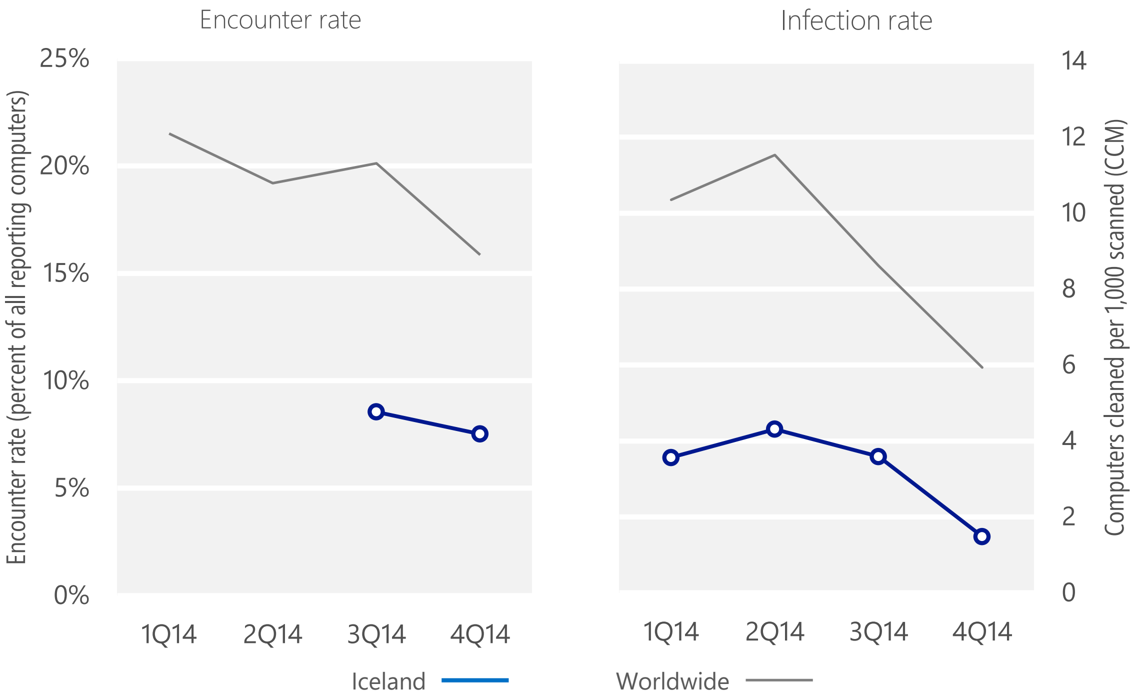
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Iceland	N/A	N/A	8.5%	7.5%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Iceland	3.6	4.3	3.6	1.5
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 7.5% percent of computers in Iceland encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 1.5 of every 1,000 unique computers scanned in Iceland in 4Q14 (a CCM score of 1.5, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Iceland over the last four quarters, compared to the world as a whole.

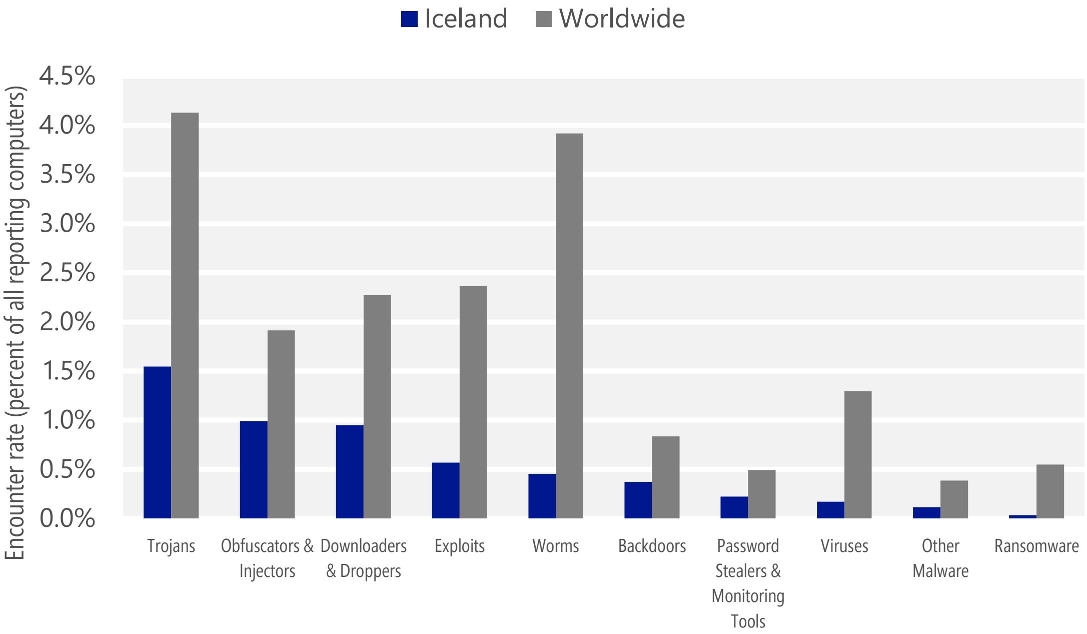
Malware encounter and infection rate trends in Iceland and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

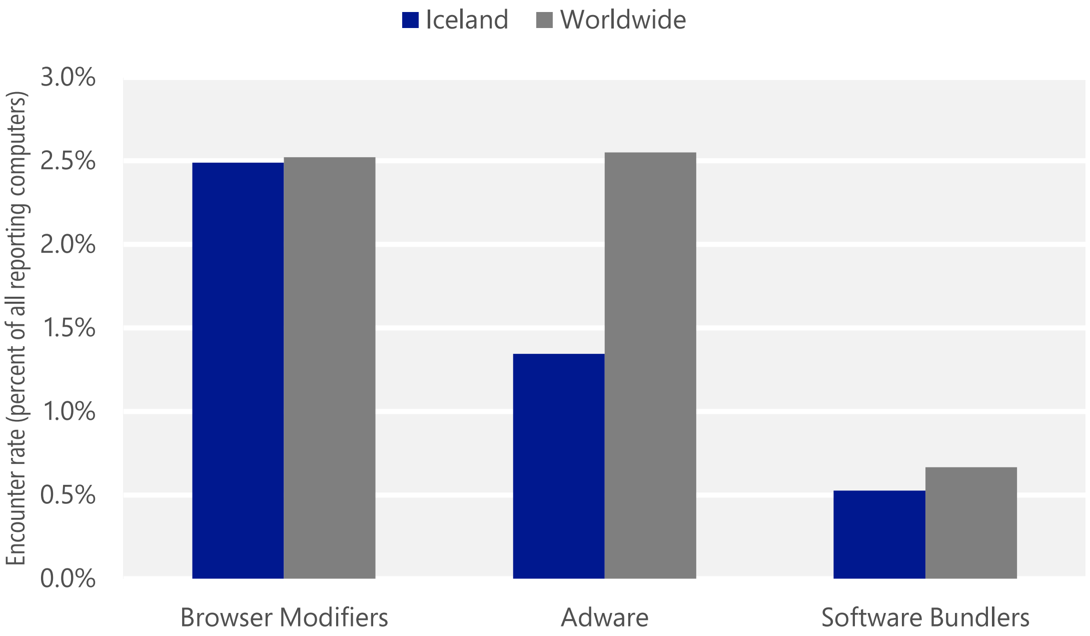
Malware encountered in Iceland in 4Q14, by category



- The most common malware category in Iceland in 4Q14 was Trojans. It was encountered by 1.5 percent of all computers there, down from 2.3 percent in 3Q14.
- The second most common malware category in Iceland in 4Q14 was Obfuscators & Injectors. It was encountered by 1.0 percent of all computers there, down from 2.3 percent in 3Q14.
- The third most common malware category in Iceland in 4Q14 was Downloaders & Droppers, which was encountered by 0.9 percent of all computers there, up from 0.9 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Iceland in 4Q14, by category



- The most common unwanted software category in Iceland in 4Q14 was Browser Modifiers. It was encountered by 2.5 percent of all computers there, down from 3.2 percent in 3Q14.
- The second most common unwanted software category in Iceland in 4Q14 was Adware. It was encountered by 1.3 percent of all computers there, up from 0.4 percent in 3Q14.
- The third most common unwanted software category in Iceland in 4Q14 was Software Bundlers, which was encountered by 0.5 percent of all computers there, up from 0.1 percent in 3Q14.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Iceland in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Defaulttab	Browser Modifiers	1.5%
2	Win32/Couponruc	Browser Modifiers	1.1%

- The most common unwanted software family encountered in Iceland in 4Q14 was Win32/Defaulttab, which was encountered by 1.5 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.
- The second most common unwanted software family encountered in Iceland in 4Q14 was Win32/Couponruc, which was encountered by 1.1 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 Iceland in 4Q14 was N/A, which was encountered by percent of reporting computers there.

Top threat families by infection rate

The most common malware families by infection rate in Iceland in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	JS/Kilim	Trojans	0.1
2	MSIL/Bladabindi	Backdoors	0.1
3	Win32/Alureon	Trojans	0.1
4	Win32/Wysotot	Trojans	0.1
5	Win32/Cutwail	Downloaders & Droppers	0.1
6	Win32/Sefnit	Trojans	0.1
7	Win32/Conficker	Worms	0.1
8	Win32/Zbot	Password Stealers & Monitoring Tools	0.1
9	Win32/Sality	Viruses	0.1
10	Win32/Tofsee	Backdoors	0.1

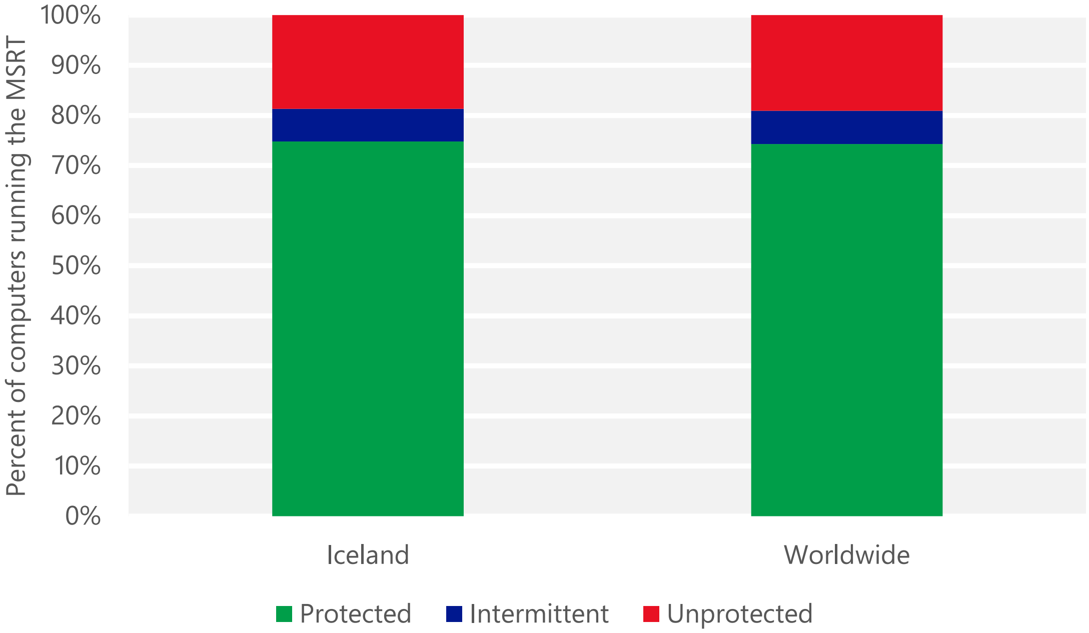
- The most common threat family infecting computers in Iceland in 4Q14 was JS/Kilim, which was detected and removed from 0.1 of every 1,000 unique computers scanned by the MSRT. JS/Kilim is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks 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 threat family infecting computers in Iceland in 4Q14 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.
- The third most common threat family infecting computers in Iceland in 4Q14 was Win32/Alureon, which was detected and removed from 0.1 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 Iceland in 4Q14 was Win32/Wysotot, which was detected and removed from 0.1 of every 1,000 unique computers scanned by the MSRT. Win32/Wysotot is a threat that can change the start page of the user's web browser, and may download and install other files to the computer. It is installed by software bundlers that advertise free software or games.

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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.51 drive-by download URLs for every 1,000 URLs hosted in Iceland, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 1.18 drive-by download URLs for every 1,000 URLs hosted in Iceland, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Iceland and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Iceland	0.51	1.18
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

India

The statistics presented here are generated by Microsoft security programs and services running on computers in India in 4Q14 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 succeds 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

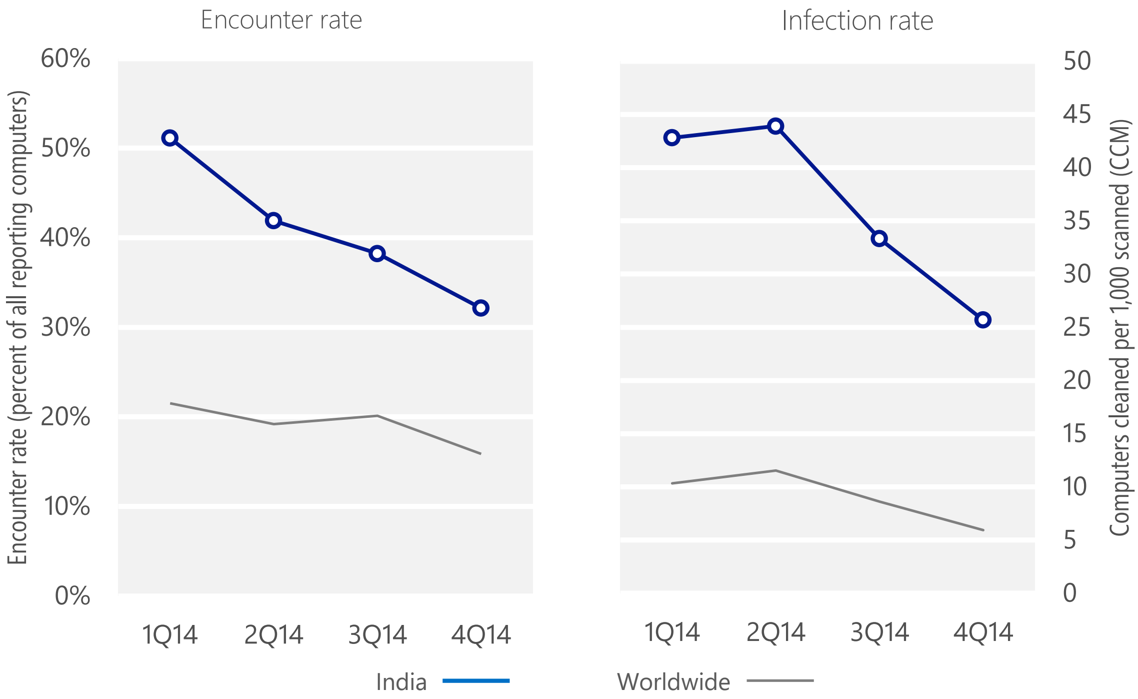
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, India	51.1%	41.9%	38.2%	32.1%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, India	42.8	43.9	33.3	25.7
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 32.1% percent of computers in India encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 25.7 of every 1,000 unique computers scanned in India in 4Q14 (a CCM score of 25.7, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for India over the last four quarters, compared to the world as a whole.

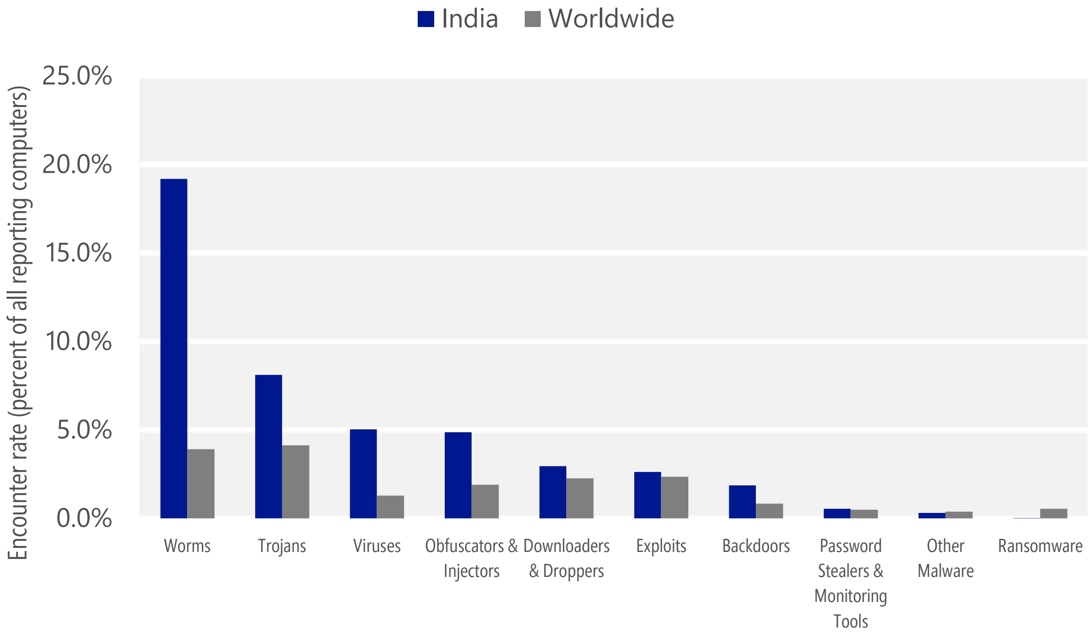
Malware encounter and infection rate trends in India and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

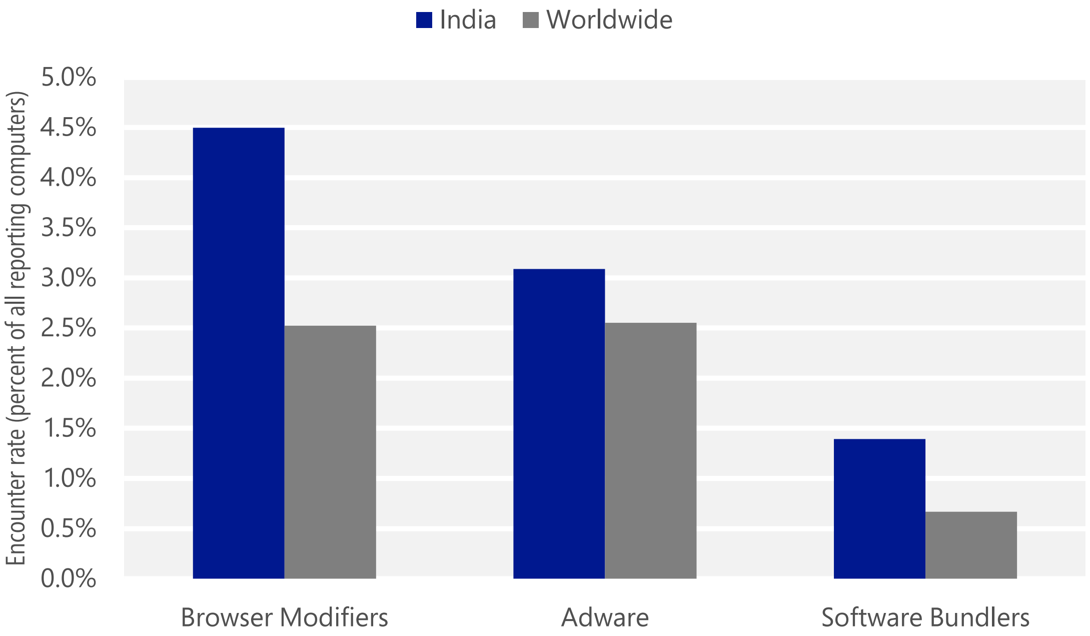
Malware encountered in India in 4Q14, by category



- The most common malware category in India in 4Q14 was Worms. It was encountered by 19.2 percent of all computers there, down from 22.7 percent in 3Q14.
- The second most common malware category in India in 4Q14 was Trojans. It was encountered by 8.1 percent of all computers there, down from 11.7 percent in 3Q14.
- The third most common malware category in India in 4Q14 was Viruses, which was encountered by 5.0 percent of all computers there, down from 6.0 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in India in 4Q14, by category



- The most common unwanted software category in India in 4Q14 was Browser Modifiers. It was encountered by 4.5 percent of all computers there, down from 6.3 percent in 3Q14.
- The second most common unwanted software category in India in 4Q14 was Adware. It was encountered by 3.1 percent of all computers there, up from 1.7 percent in 3Q14.
- The third most common unwanted software category in India in 4Q14 was Software Bundlers, which was encountered by 1.4 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in India in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Gamarue	Worms	7.9%
2	VBS/Jenxcus	Worms	6.0%
3	INF/Autorun	Obfuscators & Injectors	4.8%
4	Win32/Sality	Viruses	3.0%
5	Win32/CplLnk	Exploits	2.1%
6	Win32/Ramnit	Trojans	1.9%
7	MSIL/Mofin	Worms	1.6%
8	Win32/Vercuser	Worms	1.6%
9	Win32/Nuqel	Worms	1.5%
10	Win32/Obfuscator	Obfuscators & Injectors	1.4%

- The most common malware family encountered in India in 4Q14 was Win32/Gamarue, which was encountered by 7.9 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 India in 4Q14 was VBS/Jenxcus, which was encountered by 6.0 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 India in 4Q14 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 fourth most common malware family encountered in India in 4Q14 was Win32/Sality, which was encountered by 3.0 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 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	2.9%
2	Win32/Defaulttab	Browser Modifiers	1.7%
3	Win32/Gofileexpress	Software Bundlers	1.1%
4	Win32/Costmin	Adware	1.0%
5	Win32/Pennybee	Adware	0.8%

- The most common unwanted software family encountered in India in 4Q14 was Win32/Couponruc, which was encountered by 2.9 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 India in 4Q14 was Win32/Defaulttab, which was encountered by 1.7 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.
- The third most common unwanted software family encountered in India in 4Q14 was Win32/Gofileexpress, which was encountered by 1.1 percent of reporting computers there. Win32/Gofileexpress is a software bundler that installs other unwanted software, including Adware:Win32/Lollipop and Adware:Win32/CostMin.

Top threat families by infection rate

The most common malware families by infection rate in India in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Gamarue	Worms	8.2
2	VBS/Jenxcus	Worms	5.8
3	Win32/Sality	Viruses	4.6
4	Win32/Ramnit	Trojans	1.3
5	Win32/Nuqel	Worms	1.2
6	Win32/Tupym	Worms	0.9
7	Win32/Wysotot	Trojans	0.8
8	MSIL/Bladabindi	Backdoors	0.8
9	Win32/Vesenlosow	Worms	0.7
10	Win32/Babonock	Worms	0.5

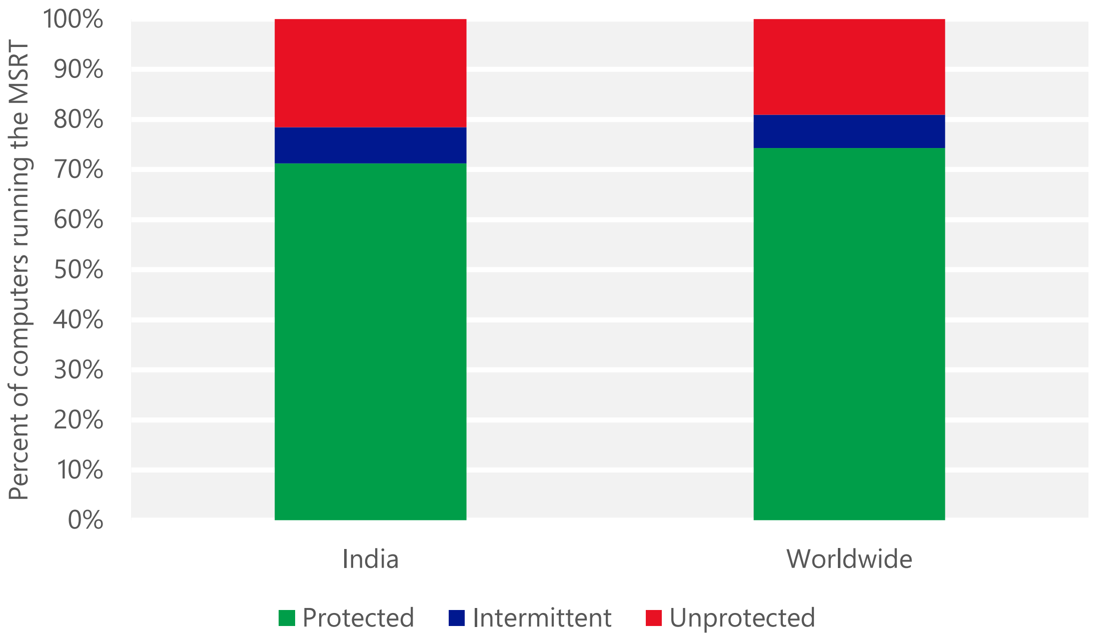
- The most common threat family infecting computers in India in 4Q14 was Win32/Gamarue, which was detected and removed from 8.2 of every 1,000 unique computers scanned by the MSRT. Win32/Gamarue is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The second most common threat family infecting computers in India in 4Q14 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 India in 4Q14 was Win32/Sality, which was detected and removed from 4.6 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.
- The fourth most common threat family infecting computers in India in 4Q14 was Win32/Ramnit, which was detected and removed from 1.3 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 India and worldwide protected by real-time security software in 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.17 drive-by download URLs for every 1,000 URLs hosted in India, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.17 drive-by download URLs for every 1,000 URLs hosted in India, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in India and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, India	0.17	0.17
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Indonesia

The statistics presented here are generated by Microsoft security programs and services running on computers in Indonesia in 4Q14 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 succeds 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

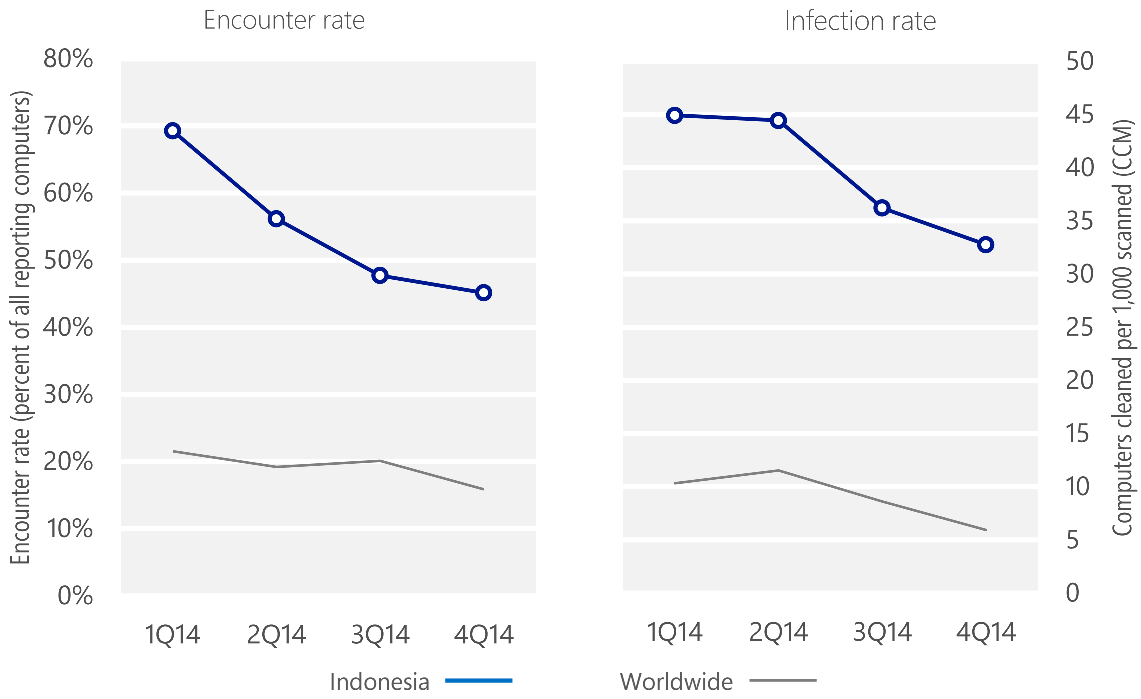
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Indonesia	69.3%	56.2%	47.7%	45.1%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Indonesia	44.9	44.4	36.2	32.8
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 45.1% percent of computers in Indonesia encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 32.8 of every 1,000 unique computers scanned in Indonesia in 4Q14 (a CCM score of 32.8, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Indonesia over the last four quarters, compared to the world as a whole.

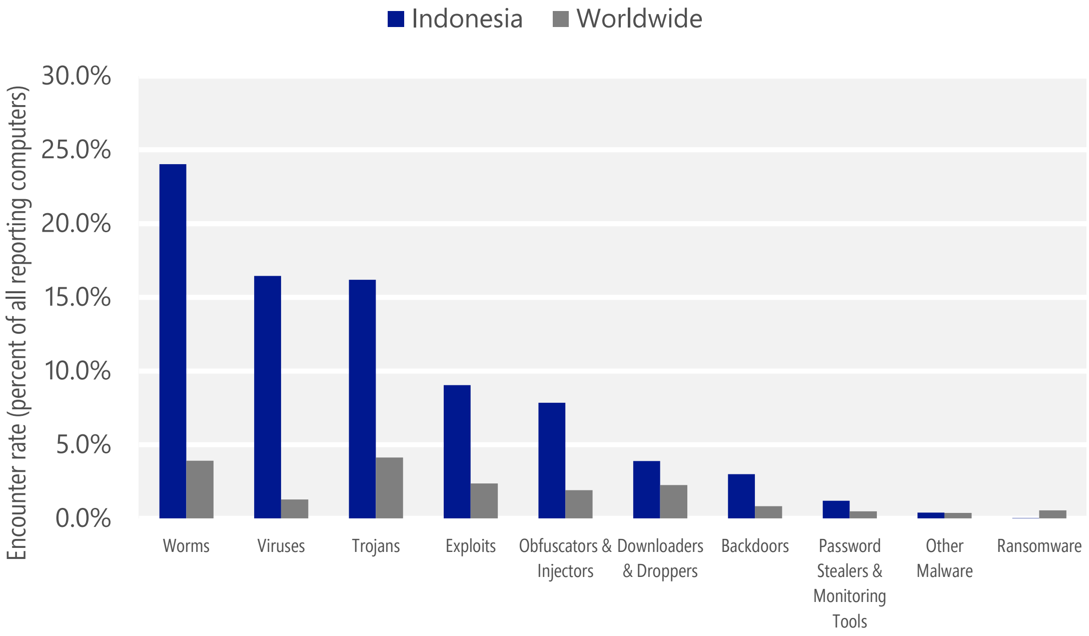
Malware encounter and infection rate trends in Indonesia and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

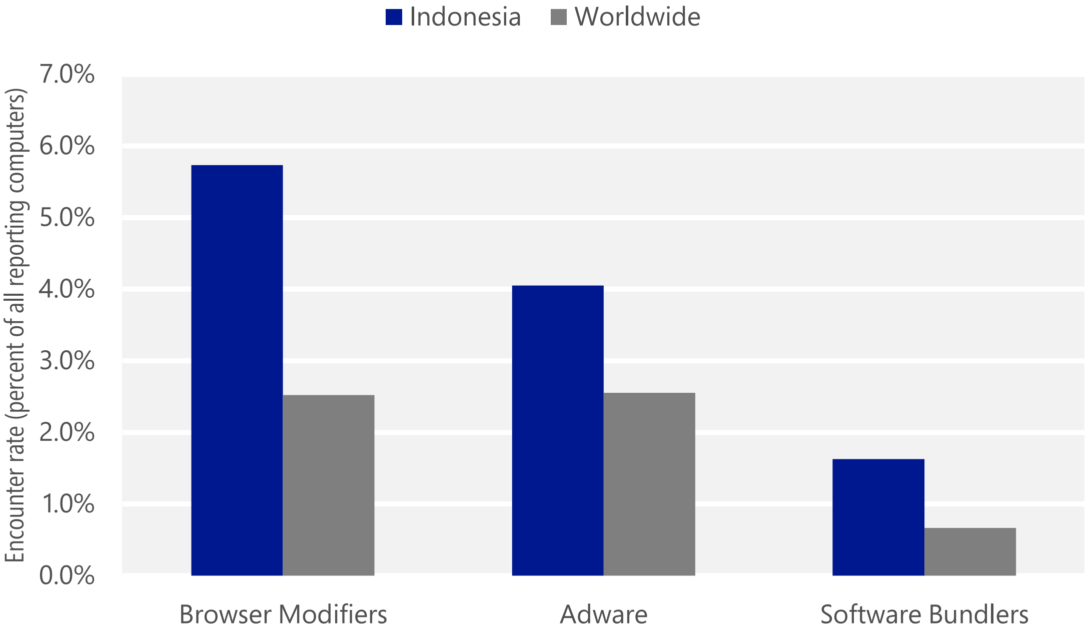
Malware encountered in Indonesia in 4Q14, by category



- The most common malware category in Indonesia in 4Q14 was Worms. It was encountered by 24.0 percent of all computers there, up from 23.6 percent in 3Q14.
- The second most common malware category in Indonesia in 4Q14 was Viruses. It was encountered by 16.5 percent of all computers there, down from 18.8 percent in 3Q14.
- The third most common malware category in Indonesia in 4Q14 was Trojans, which was encountered by 16.2 percent of all computers there, down from 17.5 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Indonesia in 4Q14, by category



- The most common unwanted software category in Indonesia in 4Q14 was Browser Modifiers. It was encountered by 5.7 percent of all computers there, down from 8.3 percent in 3Q14.
- The second most common unwanted software category in Indonesia in 4Q14 was Adware. It was encountered by 4.1 percent of all computers there, up from 1.4 percent in 3Q14.
- The third most common unwanted software category in Indonesia in 4Q14 was Software Bundlers, which was encountered by 1.6 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Indonesia in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Gamarue	Worms	11.5%
2	Win32/Ramnit	Trojans	10.7%
3	Win32/CplLnk	Exploits	8.1%
4	VBS/Jenxcus	Worms	7.4%
5	INF/Autorun	Obfuscators & Injectors	6.5%
6	Win32/Virut	Viruses	6.4%
7	Win32/Sality	Viruses	5.4%
8	Win32/Dorkbot	Worms	3.0%
9	Win32/Slugin	Viruses	2.9%
10	JS/Faceliker	Trojans	2.9%

- The most common malware family encountered in Indonesia in 4Q14 was Win32/Gamarue, which was encountered by 11.5 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 4Q14 was Win32/Ramnit, which was encountered by 10.7 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 4Q14 was Win32/CplLnk, which was encountered by 8.1 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 4Q14 was VBS/Jenxcus, which was encountered by 7.4 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 Indonesia in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	5.0%
2	Win32/Costmin	Adware	2.2%
3	Win32/BetterSurf	Adware	1.3%
4	Win32/Gofileexpress	Software Bundlers	1.3%
5	Win32/Defaulttab	Browser Modifiers	0.9%

- The most common unwanted software family encountered in Indonesia in 4Q14 was Win32/Couponruc, which was encountered by 5.0 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 Indonesia in 4Q14 was Win32/Costmin, which was encountered by 2.2 percent of reporting computers there. Win32/Costmin is an adware family that installs itself as a browser extension for Internet Explorer, Mozilla Firefox, and Google Chrome, and displays advertisements as the user browses the Internet.
- The third most common unwanted software family encountered in Indonesia in 4Q14 was Win32/BetterSurf, which was encountered by 1.3 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.

Top threat families by infection rate

The most common malware families by infection rate in Indonesia in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Ramnit	Trojans	8.5
2	Win32/Sality	Viruses	7.1
3	Win32/Gamarue	Worms	6.5
4	VBS/Jenxcus	Worms	5.9
5	Win32/Pramro	Trojans	0.9
6	Win32/Chir	Viruses	0.9
7	MSIL/Bladabindi	Backdoors	0.8
8	Win32/Dorkbot	Worms	0.8
9	Win32/Yeltminky	Worms	0.7
10	Win32/Wysotot	Trojans	0.7

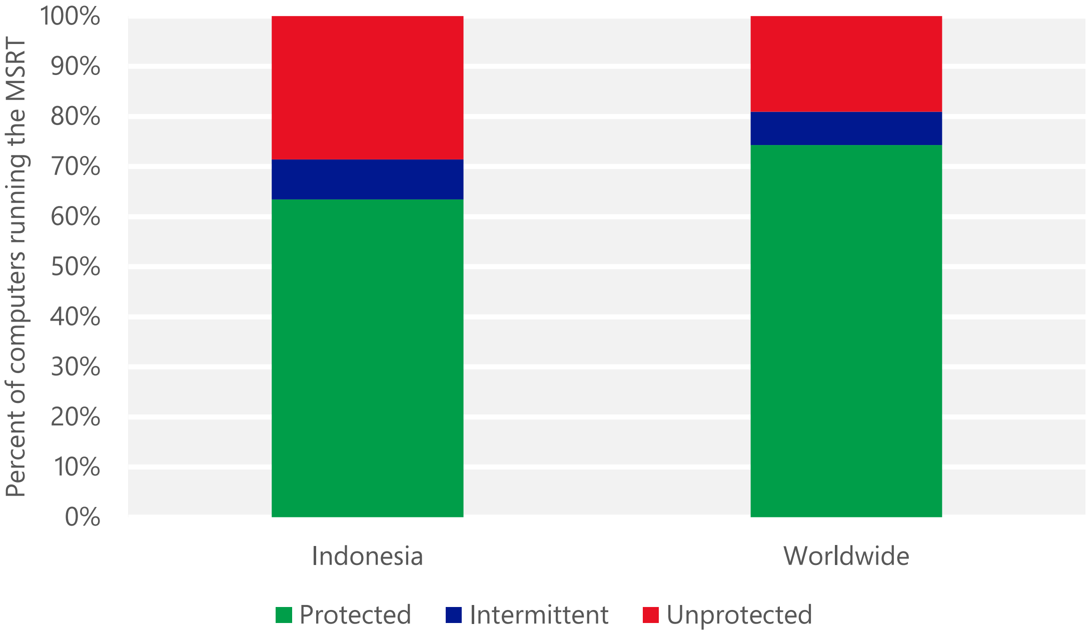
- The most common threat family infecting computers in Indonesia in 4Q14 was Win32/Ramnit, which was detected and removed from 8.5 of every 1,000 unique computers scanned by the MSRT. Win32/Ramnit is a family of multi-component malware that infects executable files, Microsoft Office files, and HTML files. 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 second most common threat family infecting computers in Indonesia in 4Q14 was Win32/Sality, which was detected and removed from 7.1 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 Indonesia in 4Q14 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 4Q14 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.

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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.58 drive-by download URLs for every 1,000 URLs hosted in Indonesia, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.68 drive-by download URLs for every 1,000 URLs hosted in Indonesia, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Indonesia and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Indonesia	0.58	0.68
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Iraq

The statistics presented here are generated by Microsoft security programs and services running on computers in Iraq in 4Q14 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 succeds 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

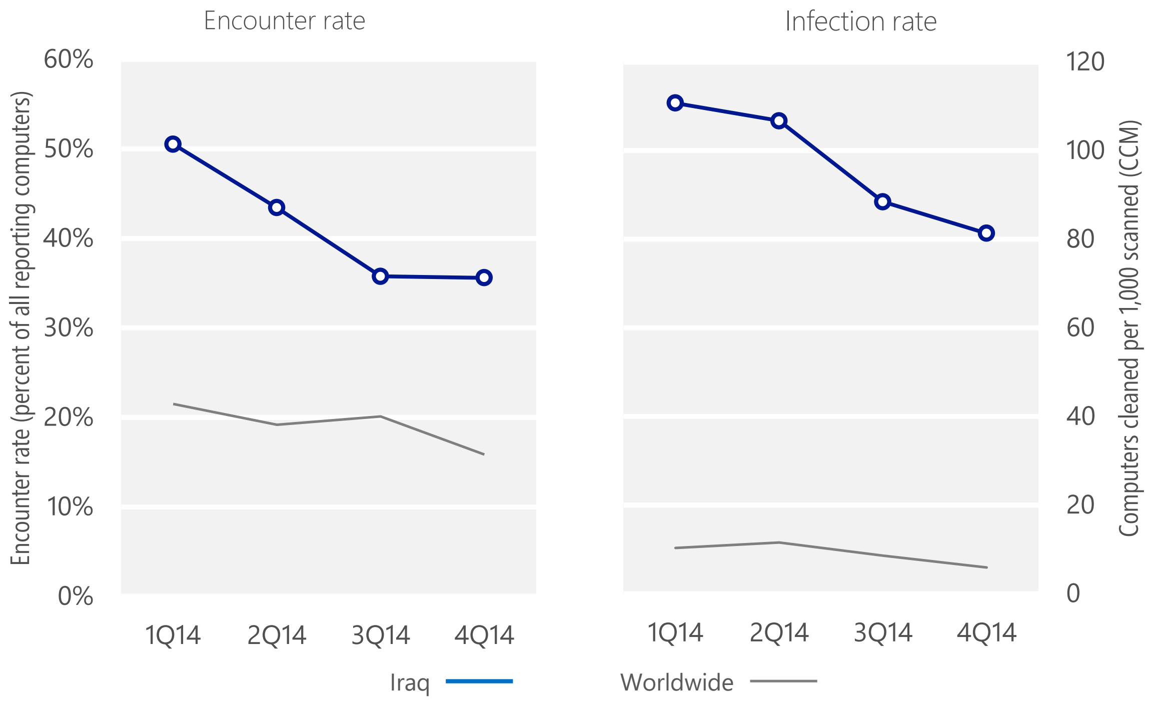
Metric	**1Q14**	**2Q14**	**3Q14**	**4Q14**
Encounter rate, Iraq	50.5%	43.4%	35.7%	35.6%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Iraq	110.7	106.7	88.5	81.3
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 35.6% percent of computers in Iraq encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 81.3 of every 1,000 unique computers scanned in Iraq in 4Q14 (a CCM score of 81.3, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Iraq over the last four quarters, compared to the world as a whole.

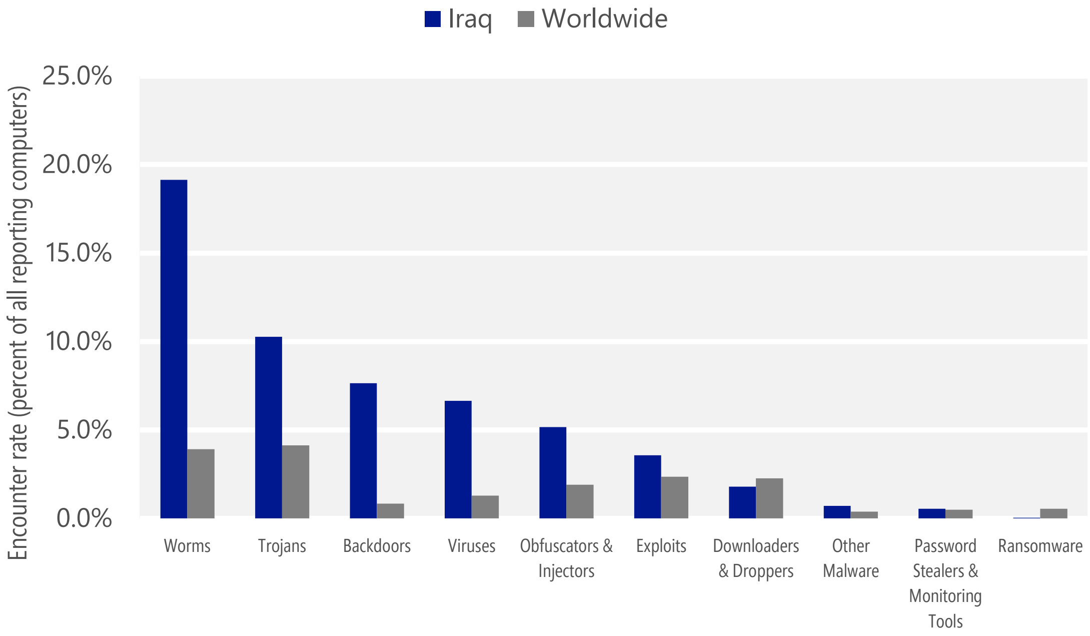
Malware encounter and infection rate trends in Iraq and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

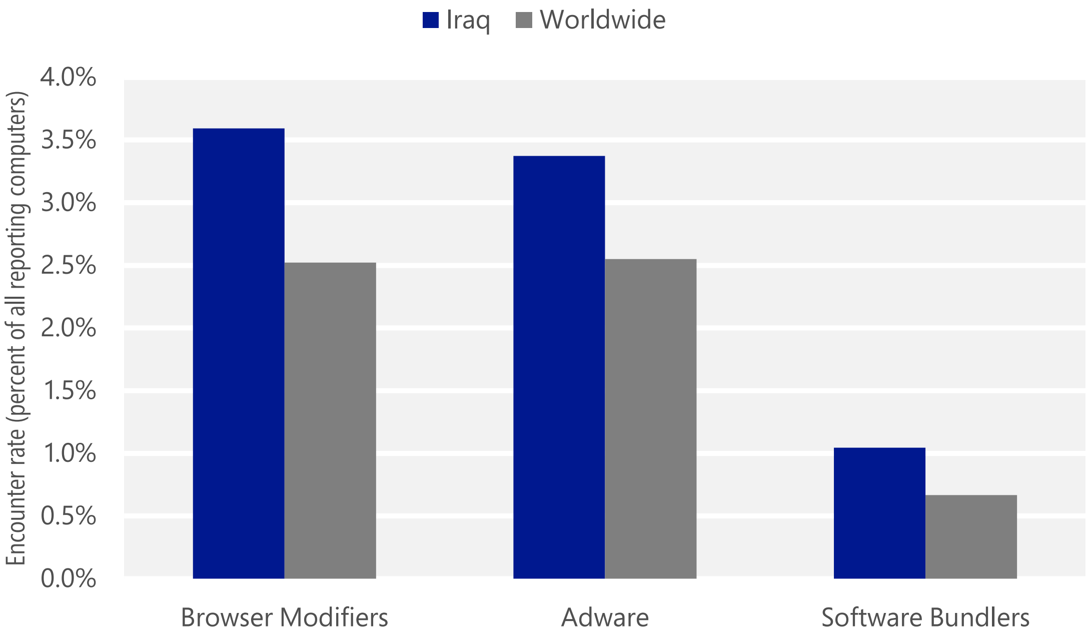
Malware encountered in Iraq in 4Q14, by category



- The most common malware category in Iraq in 4Q14 was Worms. It was encountered by 19.1 percent of all computers there, up from 17.6 percent in 3Q14.
- The second most common malware category in Iraq in 4Q14 was Trojans. It was encountered by 10.3 percent of all computers there, down from 11.6 percent in 3Q14.
- The third most common malware category in Iraq in 4Q14 was Backdoors, which was encountered by 7.6 percent of all computers there, down from 8.3 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Iraq in 4Q14, by category



- The most common unwanted software category in Iraq in 4Q14 was Browser Modifiers. It was encountered by 3.6 percent of all computers there, down from 4.8 percent in 3Q14.
- The second most common unwanted software category in Iraq in 4Q14 was Adware. It was encountered by 3.4 percent of all computers there, up from 1.0 percent in 3Q14.
- The third most common unwanted software category in Iraq in 4Q14 was Software Bundlers, which was encountered by 1.0 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Iraq in 4Q14

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	10.6%
2	INF/Autorun	Obfuscators & Injectors	7.4%
3	MSIL/Bladabindi	Backdoors	6.1%
4	Win32/Wecykler	Worms	4.5%
5	Win32/Sality	Viruses	3.5%
6	Win32/Ramnit	Trojans	3.0%
7	Win32/CplLnk	Exploits	3.0%
8	Win32/Gamarue	Worms	2.4%
9	Win32/Vermis	Worms	1.8%
10	Win32/Sulunch	Trojans	1.5%

- The most common malware family encountered in Iraq in 4Q14 was VBS/Jenxcus, which was encountered by 10.6 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 Iraq in 4Q14 was INF/Autorun, which was encountered by 7.4 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 third most common malware family encountered in Iraq in 4Q14 was MSIL/Bladabindi, which was encountered by 6.1 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 4Q14 was Win32/Wecykler, which was encountered by 4.5 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 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	2.5%
2	Win32/Brya	Adware	1.4%
3	Win32/Defaulttab	Browser Modifiers	1.1%
4	Win32/BetterSurf	Adware	1.0%
5	Win32/Gofileexpress	Software Bundlers	0.8%

- The most common unwanted software family encountered in Iraq in 4Q14 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 Iraq in 4Q14 was Win32/Brya, which was encountered by 1.4 percent of reporting computers there. Win32/Brya is a program that shows ads that the user cannot control as they browse the web. It does not have a working uninstaller.
- The third most common unwanted software family encountered in Iraq in 4Q14 was Win32/Defaulttab, which was encountered by 1.1 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.

Top threat families by infection rate

The most common malware families by infection rate in Iraq in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	25.1
2	Win32/Sality	Viruses	16.4
3	MSIL/Bladabindi	Backdoors	14.9
4	Win32/Wecykler	Worms	10.9
5	Win32/Ramnit	Trojans	7.8
6	Win32/Gamarue	Worms	4.1
7	Win32/Brontok	Worms	3.9
8	Win32/Dorkbot	Worms	2.8
9	Win32/Folstart	Worms	2.6
10	Win32/Nuqel	Worms	2.4

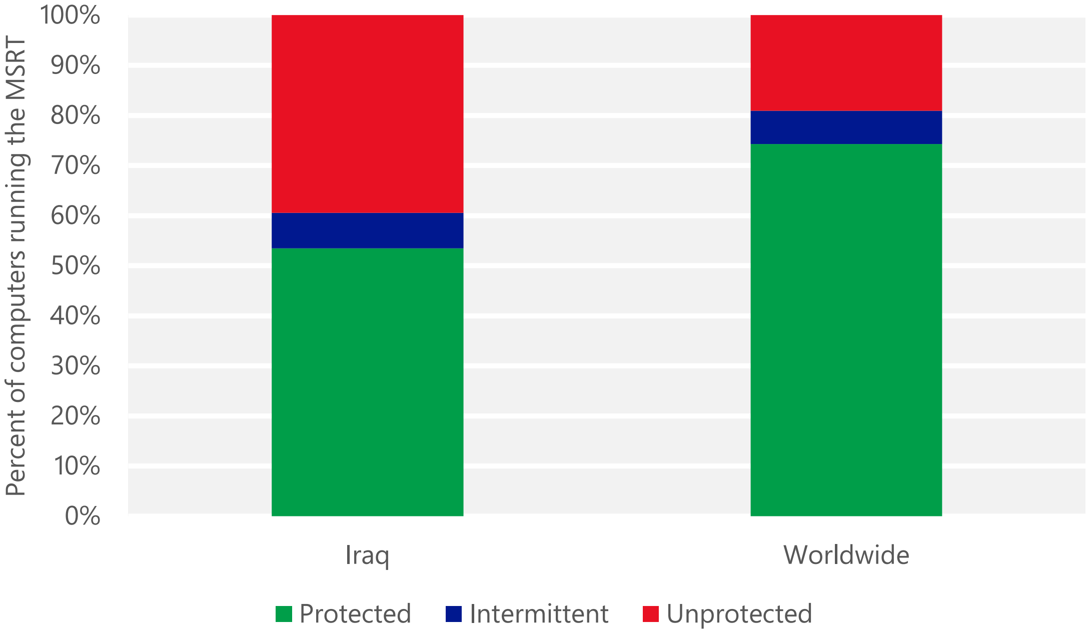
- The most common threat family infecting computers in Iraq in 4Q14 was VBS/Jenxcus, which was detected and removed from 25.1 of every 1,000 unique computers scanned by the MSRT. VBS/Jenxcus is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Iraq in 4Q14 was Win32/Sality, which was detected and removed from 16.4 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 4Q14 was MSIL/Bladabindi, which was detected and removed from 14.9 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 4Q14 was Win32/Wecykler, which was detected and removed from 10.9 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 4Q14



Ireland

The statistics presented here are generated by Microsoft security programs and services running on computers in Ireland in 4Q14 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 succeds 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

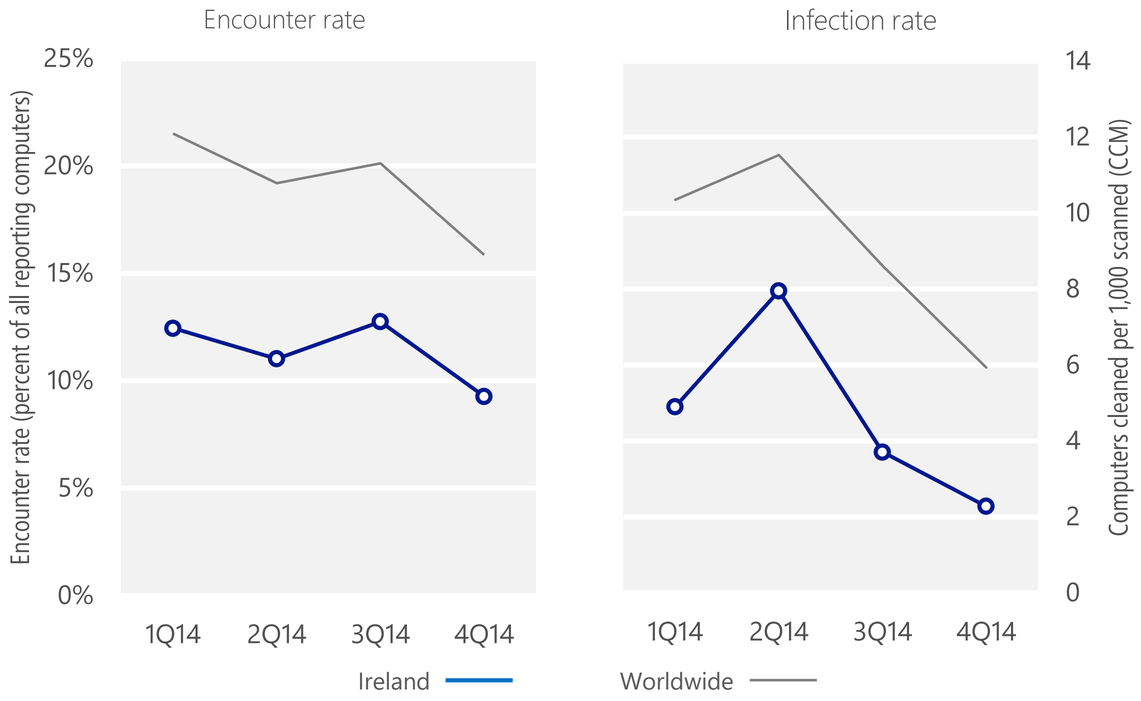
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Ireland	12.4%	11.0%	12.8%	9.3%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Ireland	4.9	8.0	3.7	2.3
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 9.3% percent of computers in Ireland encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 2.3 of every 1,000 unique computers scanned in Ireland in 4Q14 (a CCM score of 2.3, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Ireland over the last four quarters, compared to the world as a whole.

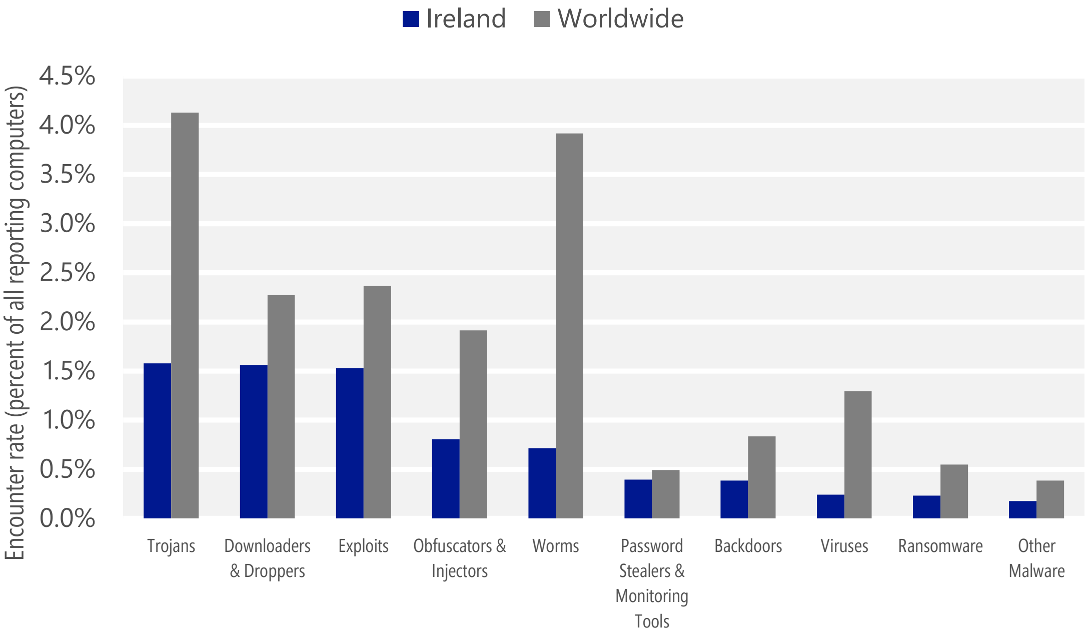
Malware encounter and infection rate trends in Ireland and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

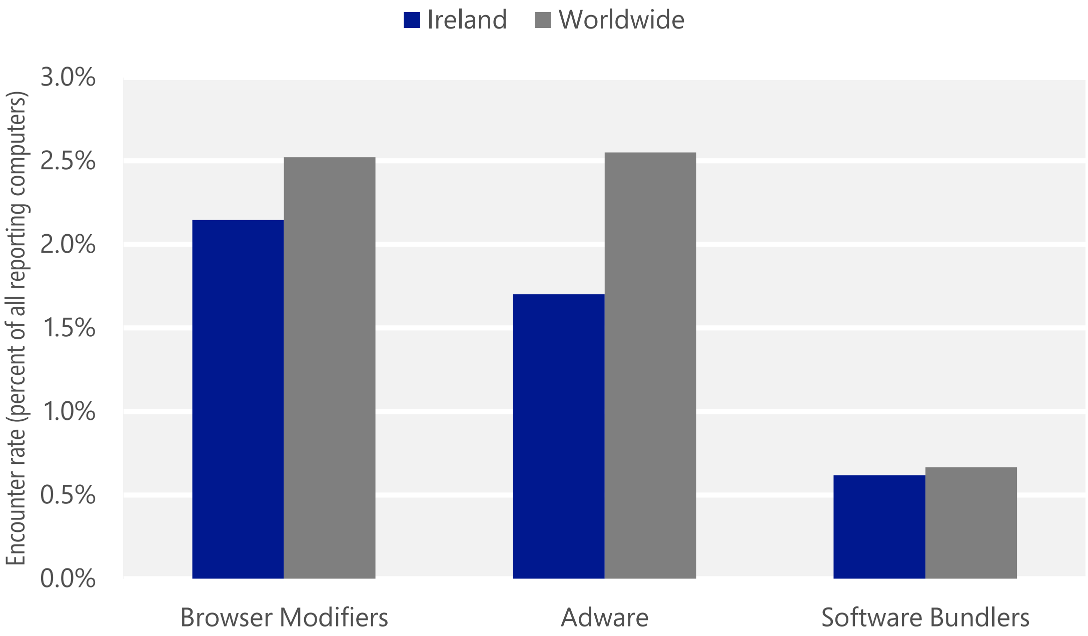
Malware encountered in Ireland in 4Q14, by category



- The most common malware category in Ireland in 4Q14 was Trojans. It was encountered by 1.6 percent of all computers there, down from 4.7 percent in 3Q14.
- The second most common malware category in Ireland in 4Q14 was Downloaders & Droppers. It was encountered by 1.6 percent of all computers there, down from 2.4 percent in 3Q14.
- The third most common malware category in Ireland in 4Q14 was Exploits, which was encountered by 1.5 percent of all computers there, down from 1.6 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Ireland in 4Q14, by category



- The most common unwanted software category in Ireland in 4Q14 was Browser Modifiers. It was encountered by 2.1 percent of all computers there, down from 4.4 percent in 3Q14.
- The second most common unwanted software category in Ireland in 4Q14 was Adware. It was encountered by 1.7 percent of all computers there, up from 0.8 percent in 3Q14.
- The third most common unwanted software category in Ireland in 4Q14 was Software Bundlers, which was encountered by 0.6 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Ireland in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Obfuscator	Obfuscators & Injectors	0.6%
2	JS/Axpergle	Exploits	0.5%
3	Win32/Tugspay	Downloaders & Droppers	0.4%
4	JS/Fiexp	Exploits	0.3%
5	INF/Autorun	Obfuscators & Injectors	0.3%
6	Win32/Upatre	Downloaders & Droppers	0.3%

- The most common malware family encountered in Ireland in 4Q14 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 second most common malware family encountered in Ireland in 4Q14 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 third most common malware family encountered in Ireland in 4Q14 was Win32/Tugspay, which was encountered by 0.4 percent of reporting computers there. Win32/Tugspay is a downloader that spreads by posing as an installer for legitimate software, such as a Java update, or through other malware. When installed, it downloads unwanted software to the computer.
- The fourth most common malware family encountered in Ireland in 4Q14 was JS/Fiexp, which was encountered by 0.3 percent of reporting computers there. JS/Fiexp is a detection for the Fiesta exploit kit, which attempts to exploit Java, Adobe Flash Player, Adobe Reader, Silverlight, and Internet Explorer to install malware.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Ireland in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	1.6%
2	Win32/Costmin	Adware	0.9%
3	Win32/BetterSurf	Adware	0.6%
4	Win32/Defaulttab	Browser Modifiers	0.5%
5	Win32/Gofileexpress	Software Bundlers	0.4%

- The most common unwanted software family encountered in Ireland in 4Q14 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 Ireland in 4Q14 was Win32/Costmin, which was encountered by 0.9 percent of reporting computers there. Win32/Costmin is an adware family that installs itself as a browser extension for Internet Explorer, Mozilla Firefox, and Google Chrome, and displays advertisements as the user browses the Internet.

- The third most common unwanted software family encountered in Ireland in 4Q14 was Win32/BetterSurf, which was encountered by 0.6 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.

Top threat families by infection rate

The most common malware families by infection rate in Ireland in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Sefnit	Trojans	0.2
2	Win32/Alureon	Trojans	0.2
3	Win32/Wysotot	Trojans	0.2
4	Win32/Zbot	Password Stealers & Monitoring Tools	0.2
5	JS/Miuref	Trojans	0.1
6	Win32/Cutwail	Downloaders & Droppers	0.1
7	VBS/Jenxcus	Worms	0.1
8	Win32/Conficker	Worms	0.1
9	Win32/Sality	Viruses	0.1
10	JS/Kilim	Trojans	0.1

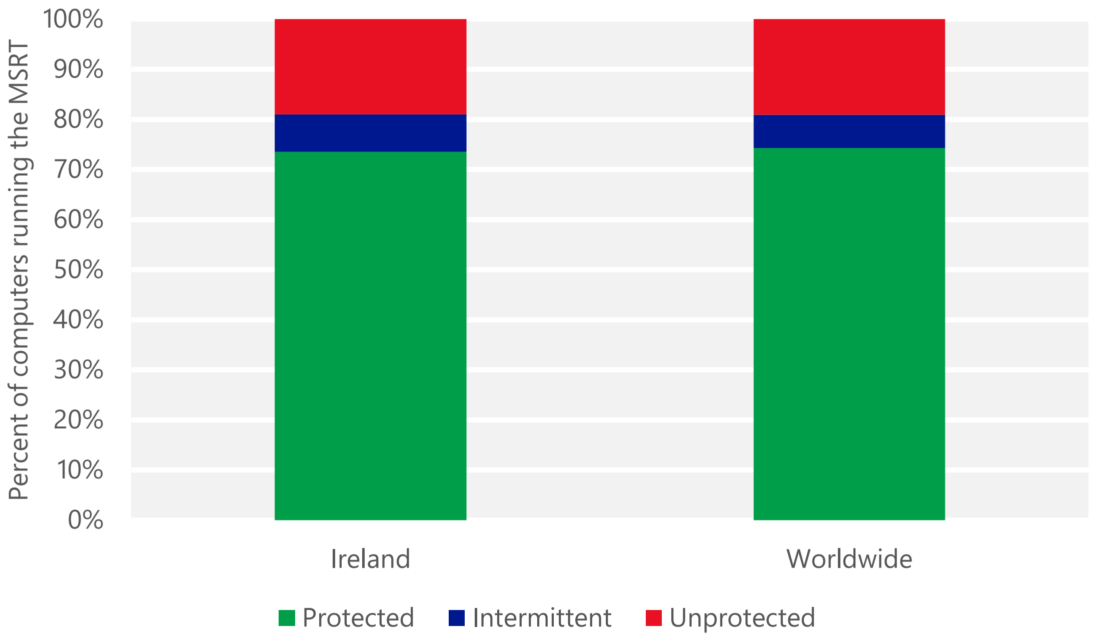
- The most common threat family infecting computers in Ireland in 4Q14 was Win32/Sefnit, which was detected and removed from 0.2 of every 1,000 unique computers scanned by the MSRT. Win32/Sefnit is a family of trojans that can allow backdoor access, download files, and use the computer and Internet connection for click fraud. Some variants can monitor web browsers and hijack search results.
- The second most common threat family infecting computers in Ireland in 4Q14 was Win32/Alureon, which was detected and removed from 0.2 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 third most common threat family infecting computers in Ireland in 4Q14 was Win32/Wysotot, which was detected and removed from 0.2 of every 1,000 unique computers scanned by the MSRT. Win32/Wysotot is a threat that can change the start page of the user's web browser, and may download and install other files to the computer. It is installed by software bundlers that advertise free software or games.
- The fourth most common threat family infecting computers in Ireland in 4Q14 was Win32/Zbot, which was detected and removed from 0.2 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.

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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.16 drive-by download URLs for every 1,000 URLs hosted in Ireland, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.07 drive-by download URLs for every 1,000 URLs hosted in Ireland, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Ireland and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Ireland	0.16	0.07
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Israel

The statistics presented here are generated by Microsoft security programs and services running on computers in Israel in 4Q14 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 succeds 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

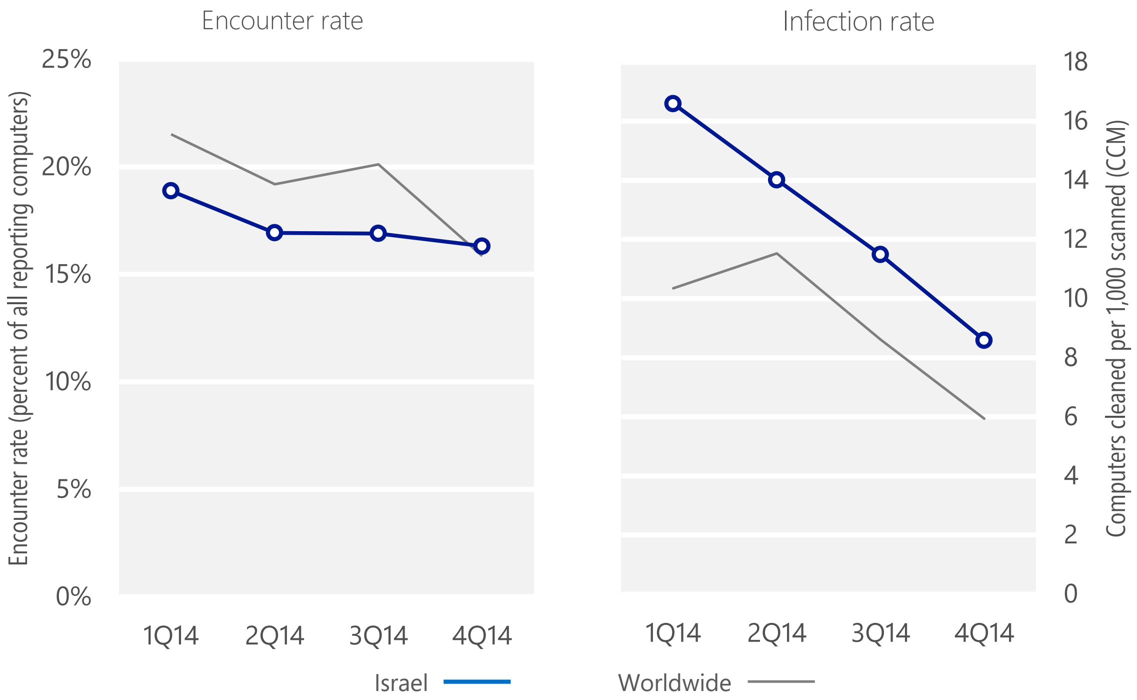
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Israel	18.9%	16.9%	16.9%	16.3%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Israel	16.6	14.0	11.5	8.6
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 16.3% percent of computers in Israel encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 8.6 of every 1,000 unique computers scanned in Israel in 4Q14 (a CCM score of 8.6, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Israel over the last four quarters, compared to the world as a whole.

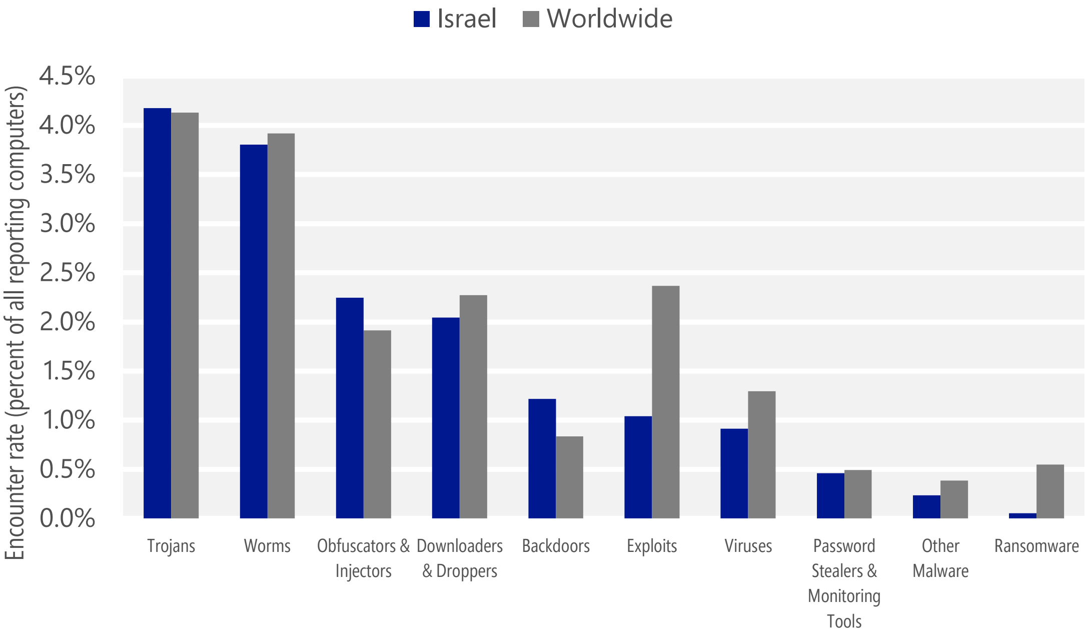
Malware encounter and infection rate trends in Israel and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

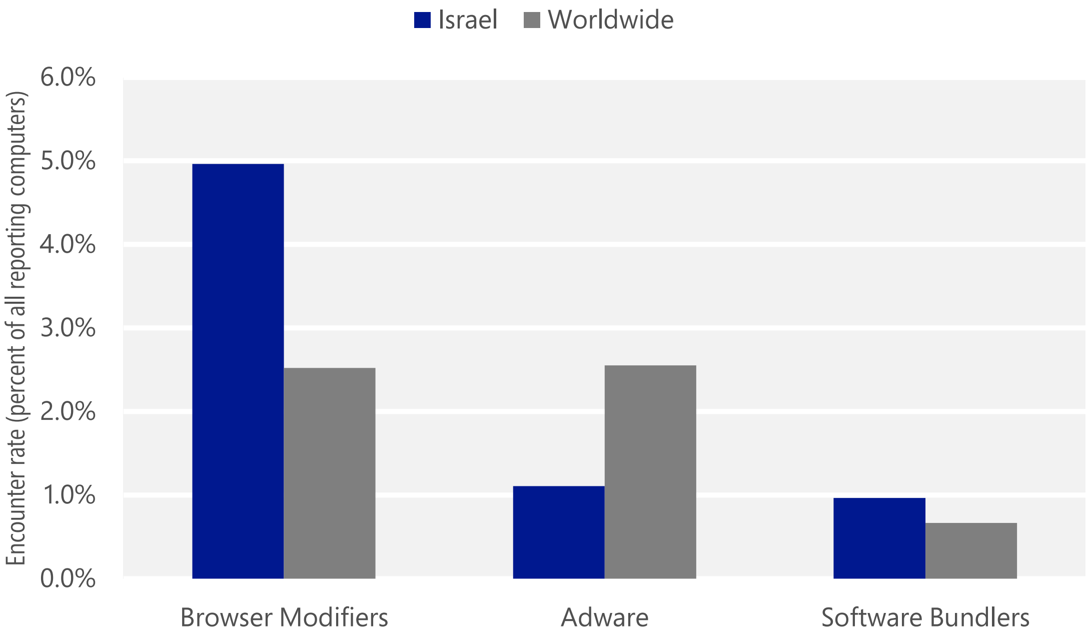
Malware encountered in Israel in 4Q14, by category



- The most common malware category in Israel in 4Q14 was Trojans. It was encountered by 4.2 percent of all computers there, down from 5.3 percent in 3Q14.
- The second most common malware category in Israel in 4Q14 was Worms. It was encountered by 3.8 percent of all computers there, down from 5.0 percent in 3Q14.
- The third most common malware category in Israel in 4Q14 was Obfuscators & Injectors, which was encountered by 2.2 percent of all computers there, down from 3.7 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Israel in 4Q14, by category



- The most common unwanted software category in Israel in 4Q14 was Browser Modifiers. It was encountered by 5.0 percent of all computers there, up from 1.8 percent in 3Q14.
- The second most common unwanted software category in Israel in 4Q14 was Adware. It was encountered by 1.1 percent of all computers there, down from 1.4 percent in 3Q14.
- The third most common unwanted software category in Israel in 4Q14 was Software Bundlers, which was encountered by 1.0 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Israel in 4Q14

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	1.6%
2	Win32/Obfuscator	Obfuscators & Injectors	1.3%
3	INF/Autorun	Obfuscators & Injectors	1.2%
4	Win32/Datper	Trojans	0.6%
5	Win32/Brontok	Worms	0.5%
6	Win32/Ogimant	Downloaders & Droppers	0.5%
7	MSIL/Bladabindi	Backdoors	0.5%
8	Win32/Sanusra	Trojans	0.4%
9	Win32/Dynamer	Trojans	0.4%
10	Win32/Sality	Viruses	0.4%

- The most common malware family encountered in Israel in 4Q14 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 second most common malware family encountered in Israel in 4Q14 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 third most common malware family encountered in Israel in 4Q14 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.
- The fourth most common malware family encountered in Israel in 4Q14 was Win32/Datper, which was encountered by 0.6 percent of reporting computers there.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Israel in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	2.9%
2	Win32/Defaulttab	Browser Modifiers	2.3%
3	Win32/Costmin	Adware	0.7%
4	Win32/Gofileexpress	Software Bundlers	0.6%
5	Win32/OneClickDownloader	Software Bundlers	0.1%

- The most common unwanted software family encountered in Israel in 4Q14 was Win32/Couponruc, which was encountered by 2.9 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 Israel in 4Q14 was Win32/Defaulttab, which was encountered by 2.3 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.
- The third most common unwanted software family encountered in Israel in 4Q14 was Win32/Costmin, which was encountered by 0.7 percent of reporting computers there. Win32/Costmin is an adware family that installs itself as a browser extension for Internet Explorer, Mozilla Firefox, and Google Chrome, and displays advertisements as the user browses the Internet.

Top threat families by infection rate

The most common malware families by infection rate in Israel in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	2.3
2	Win32/Sality	Viruses	1.2
3	Win32/Brontok	Worms	1.0
4	Win32/Ramnit	Trojans	0.6
5	MSIL/Bladabindi	Backdoors	0.5
6	Win32/Wysotot	Trojans	0.5
7	Win32/Pramro	Trojans	0.3
8	Win32/Vobfus	Worms	0.3
9	Win32/Dorkbot	Worms	0.2
10	Win32/Gamarue	Worms	0.2

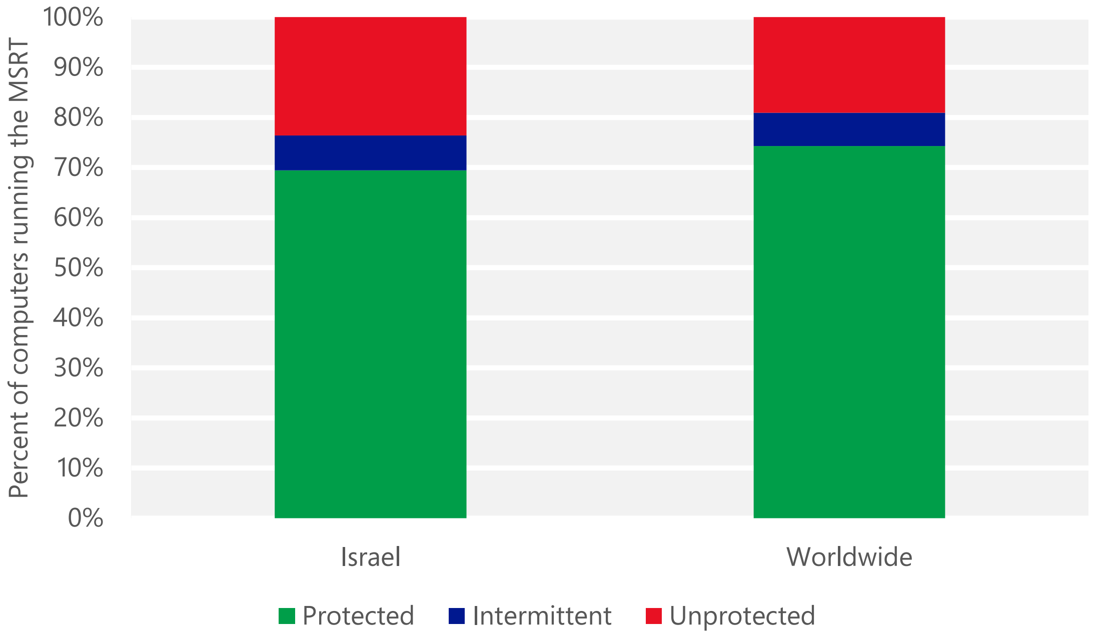
- The most common threat family infecting computers in Israel in 4Q14 was VBS/Jenxcus, which was detected and removed from 2.3 of every 1,000 unique computers scanned by the MSRT. VBS/Jenxcus is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Israel in 4Q14 was Win32/Sality, which was detected and removed from 1.2 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.
- The third most common threat family infecting computers in Israel in 4Q14 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.
- The fourth most common threat family infecting computers in Israel in 4Q14 was Win32/Ramnit, which was detected and removed from 0.6 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 Israel and worldwide protected by real-time security software in 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.13 drive-by download URLs for every 1,000 URLs hosted in Israel, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.11 drive-by download URLs for every 1,000 URLs hosted in Israel, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Israel and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Israel	0.13	0.11
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Italy

The statistics presented here are generated by Microsoft security programs and services running on computers in Italy in 4Q14 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 succeds 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

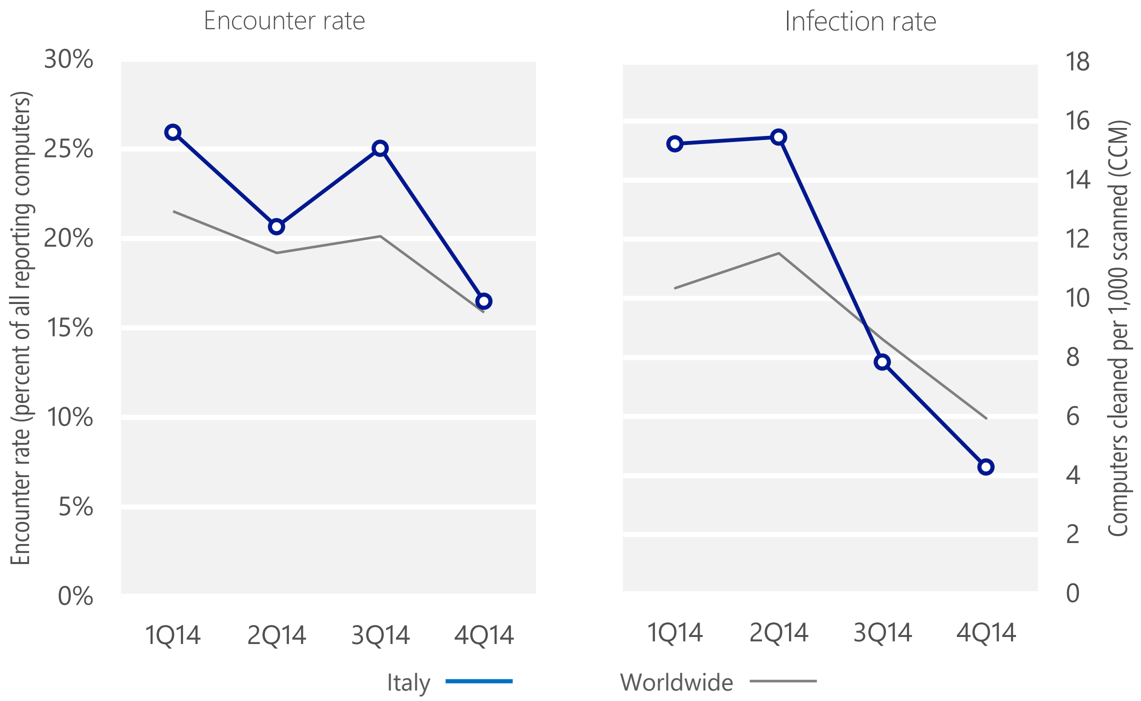
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Italy	25.9%	20.7%	25.0%	16.5%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Italy	15.2	15.5	7.8	4.3
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 16.5% percent of computers in Italy encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 4.3 of every 1,000 unique computers scanned in Italy in 4Q14 (a CCM score of 4.3, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Italy over the last four quarters, compared to the world as a whole.

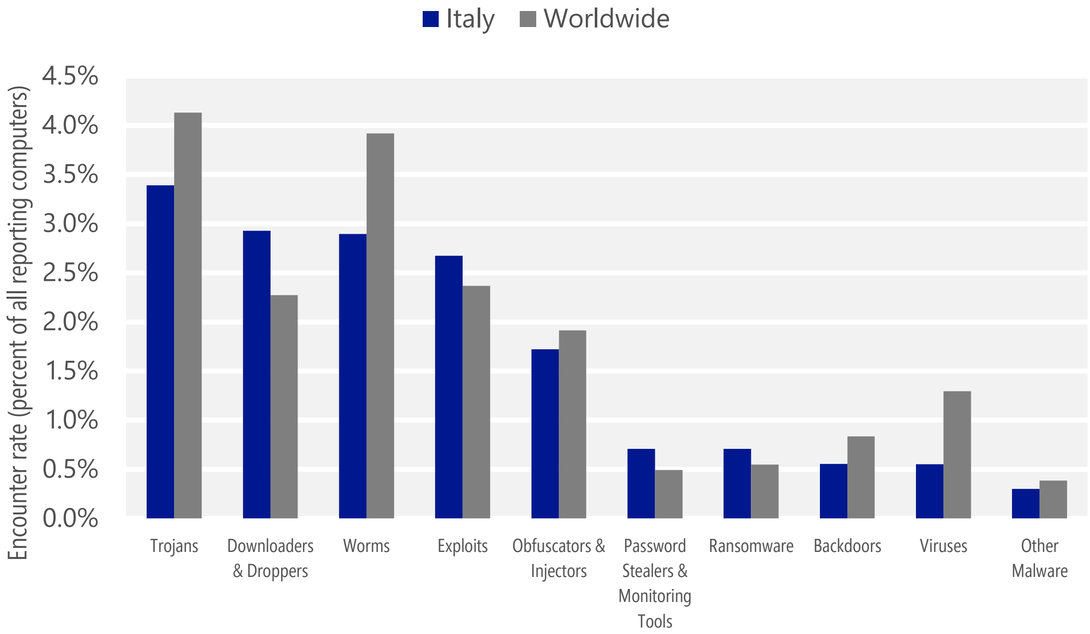
Malware encounter and infection rate trends in Italy and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

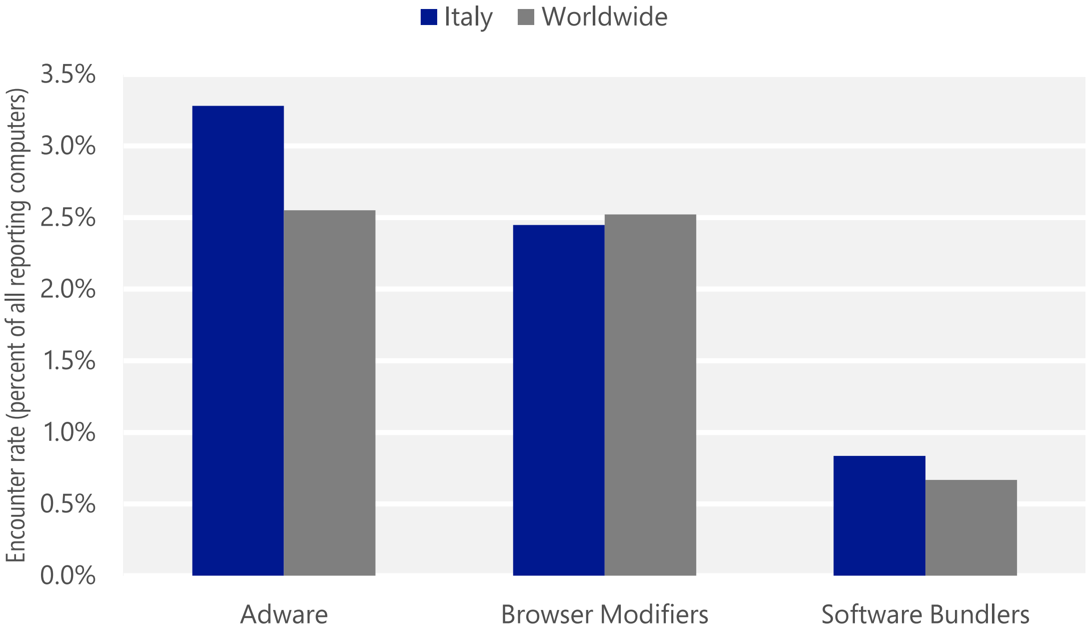
Malware encountered in Italy in 4Q14, by category



- The most common malware category in Italy in 4Q14 was Trojans. It was encountered by 3.4 percent of all computers there, down from 11.3 percent in 3Q14.
- The second most common malware category in Italy in 4Q14 was Downloaders & Droppers. It was encountered by 2.9 percent of all computers there, down from 5.1 percent in 3Q14.
- The third most common malware category in Italy in 4Q14 was Worms, which was encountered by 2.9 percent of all computers there, up from 2.8 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Italy in 4Q14, by category



- The most common unwanted software category in Italy in 4Q14 was Adware. It was encountered by 3.3 percent of all computers there, down from 6.7 percent in 3Q14.
- The second most common unwanted software category in Italy in 4Q14 was Browser Modifiers. It was encountered by 2.4 percent of all computers there, down from 3.7 percent in 3Q14.
- The third most common unwanted software category in Italy in 4Q14 was Software Bundlers, which was encountered by 0.8 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Italy in 4Q14

	Family	Most significant category	% of reporting computers
1	JS/Axpergle	Exploits	1.6%
2	Win32/Tugspay	Downloaders & Droppers	1.5%
3	Win32/Obfuscator	Obfuscators & Injectors	1.0%
4	INF/Autorun	Obfuscators & Injectors	0.8%
5	Win32/Conficker	Worms	0.8%
6	ASX/Wimad	Downloaders & Droppers	0.7%
7	Win32/Gamarue	Worms	0.7%
8	Win32/Dynamer	Trojans	0.5%
9	Win32/Zbot	Password Stealers & Monitoring Tools	0.5%
10	VBS/Jenxcus	Worms	0.5%

- The most common malware family encountered in Italy in 4Q14 was JS/Axpergle, which was encountered by 1.6 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 second most common malware family encountered in Italy in 4Q14 was Win32/Tugspay, which was encountered by 1.5 percent of reporting computers there. Win32/Tugspay is a downloader that spreads by posing as an installer for legitimate software, such as a Java update, or through other malware. When installed, it downloads unwanted software to the computer.
- The third most common malware family encountered in Italy in 4Q14 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.
- The fourth most common malware family encountered in Italy in 4Q14 was INF/Autorun, which was encountered by 0.8 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 Italy in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	2.2%
2	Win32/Costmin	Adware	1.1%
3	Win32/BetterSurf	Adware	0.7%
4	Win32/Pennybee	Adware	0.6%
5	Win32/Gofileexpress	Software Bundlers	0.4%

- The most common unwanted software family encountered in Italy in 4Q14 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 Italy in 4Q14 was Win32/Costmin, which was encountered by 1.1 percent of reporting computers there. Win32/Costmin is an adware family that installs itself as a browser extension for Internet Explorer, Mozilla Firefox, and Google Chrome, and displays advertisements as the user browses the Internet.

- The third most common unwanted software family encountered in Italy in 4Q14 was Win32/BetterSurf, which was encountered by 0.7 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.

Top threat families by infection rate

The most common malware families by infection rate in Italy in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Wysotot	Trojans	0.7
2	VBS/Jenxcus	Worms	0.6
3	Win32/Sefnit	Trojans	0.4
4	Win32/Zbot	Password Stealers & Monitoring Tools	0.4
5	Win32/Conficker	Worms	0.2
6	Win32/Alureon	Trojans	0.2
7	Win32/Ramnit	Trojans	0.2
8	Win32/Sality	Viruses	0.2
9	Win32/Brontok	Worms	0.1
10	Win32/Sirefef	Trojans	0.1

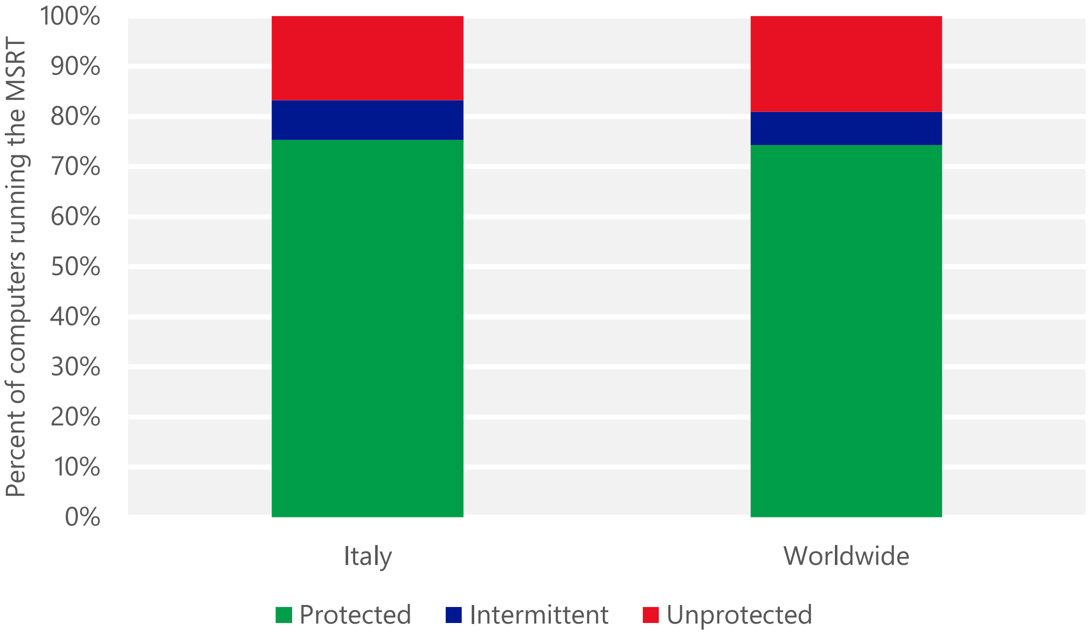
- The most common threat family infecting computers in Italy in 4Q14 was Win32/Wysotot, which was detected and removed from 0.7 of every 1,000 unique computers scanned by the MSRT. Win32/Wysotot is a threat that can change the start page of the user's web browser, and may download and install other files to the computer. It is installed by software bundlers that advertise free software or games.
- The second most common threat family infecting computers in Italy in 4Q14 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.
- The third most common threat family infecting computers in Italy in 4Q14 was Win32/Sefnit, which was detected and removed from 0.4 of every 1,000 unique computers scanned by the MSRT. Win32/Sefnit is a family of trojans that can allow backdoor access, download files, and use the computer and Internet connection for click fraud. Some variants can monitor web browsers and hijack search results.
- The fourth most common threat family infecting computers in Italy in 4Q14 was Win32/Zbot, which was detected and removed from 0.4 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.

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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.31 drive-by download URLs for every 1,000 URLs hosted in Italy, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.27 drive-by download URLs for every 1,000 URLs hosted in Italy, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Italy and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Italy	0.31	0.27
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Jamaica

The statistics presented here are generated by Microsoft security programs and services running on computers in Jamaica in 4Q14 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 succeds 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

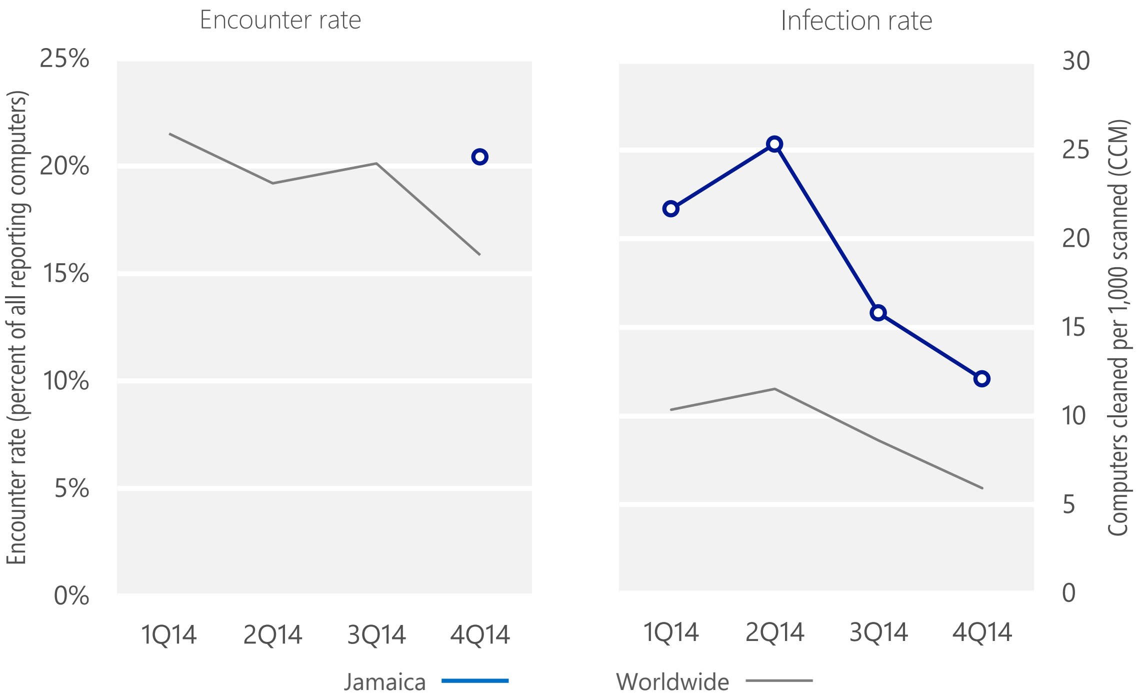
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Jamaica	N/A	N/A	N/A	20.4%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Jamaica	21.7	25.3	15.8	12.1
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 20.4% percent of computers in Jamaica encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 12.1 of every 1,000 unique computers scanned in Jamaica in 4Q14 (a CCM score of 12.1, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Jamaica over the last four quarters, compared to the world as a whole.

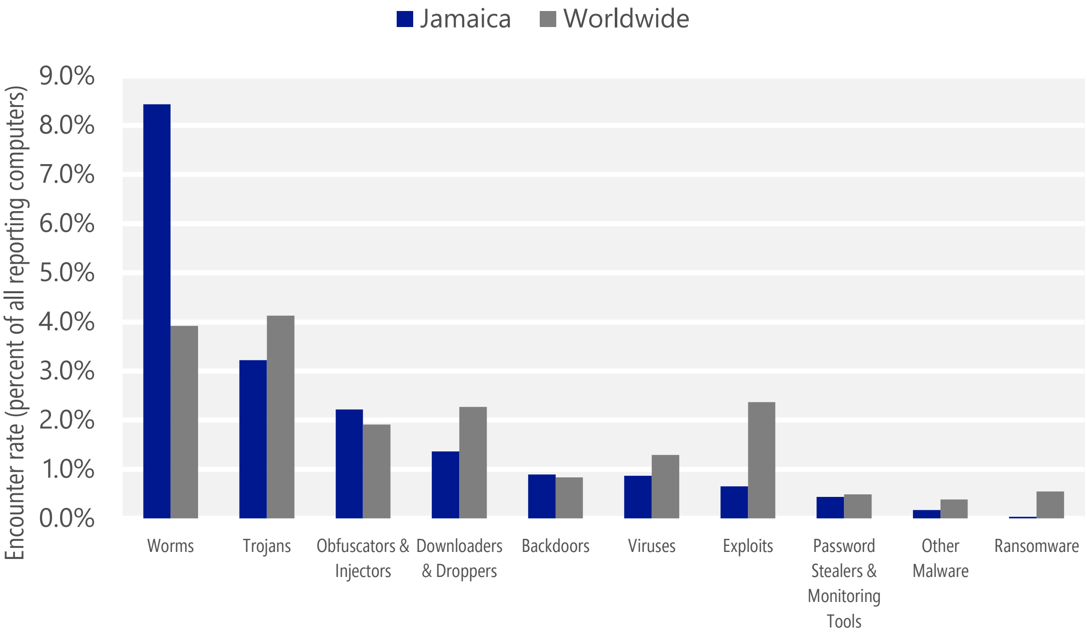
Malware encounter and infection rate trends in Jamaica and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

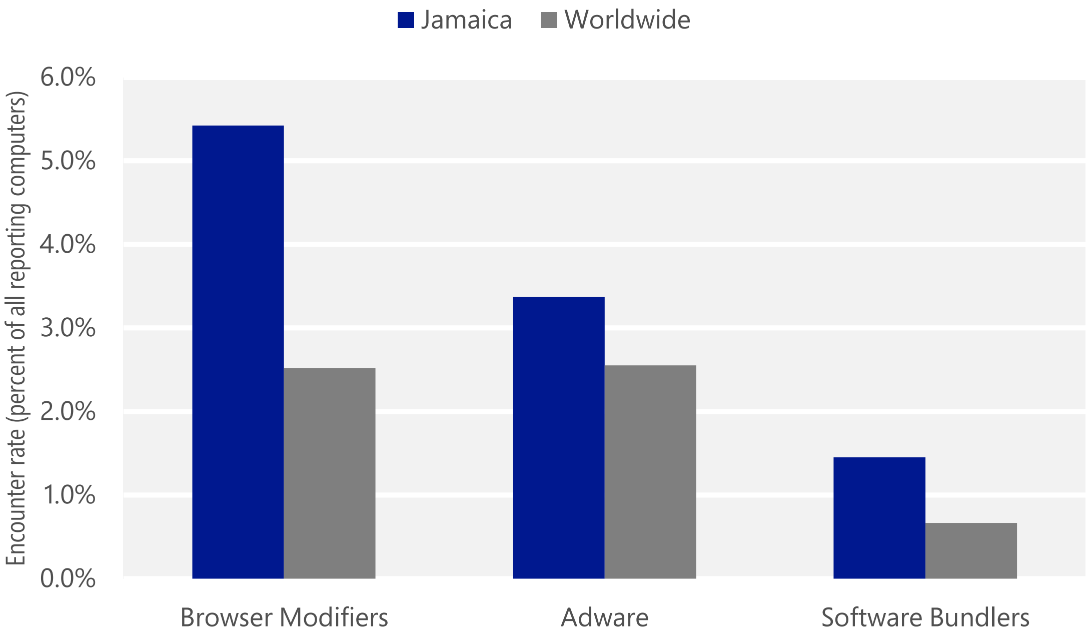
Malware encountered in Jamaica in 4Q14, by category



- The most common malware category in Jamaica in 4Q14 was Worms. It was encountered by 8.4 percent of all computers there, up from N/A percent in 3Q14.
- The second most common malware category in Jamaica in 4Q14 was Trojans. It was encountered by 3.2 percent of all computers there, up from N/A percent in 3Q14.
- The third most common malware category in Jamaica in 4Q14 was Obfuscators & Injectors, which was encountered by 2.2 percent of all computers there, up from N/A percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Jamaica in 4Q14, by category



- The most common unwanted software category in Jamaica in 4Q14 was Browser Modifiers. It was encountered by 5.4 percent of all computers there, up from N/A percent in 3Q14.
- The second most common unwanted software category in Jamaica in 4Q14 was Adware. It was encountered by 3.4 percent of all computers there, up from N/A percent in 3Q14.
- The third most common unwanted software category in Jamaica in 4Q14 was Software Bundlers, which was encountered by 1.5 percent of all computers there, up from N/A percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Jamaica in 4Q14

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	4.5%
2	INF/Autorun	Obfuscators & Injectors	1.4%
3	Win32/Gamarue	Worms	1.4%
4	Win32/Obfuscator	Obfuscators & Injectors	1.1%
5	JS/Proslikefan	Worms	1.1%
6	Win32/Brontok	Worms	1.0%

- The most common malware family encountered in Jamaica in 4Q14 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 Jamaica in 4Q14 was INF/Autorun, which was encountered by 1.4 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 third most common malware family encountered in Jamaica in 4Q14 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 fourth most common malware family encountered in Jamaica in 4Q14 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.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Jamaica in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	3.4%
2	Win32/Defaulttab	Browser Modifiers	2.2%
3	Win32/BetterSurf	Adware	1.6%
4	Win32/Costmin	Adware	1.4%
5	Win32/Gofileexpress	Software Bundlers	1.0%

- The most common unwanted software family encountered in Jamaica in 4Q14 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 Jamaica in 4Q14 was Win32/Defaulttab, which was encountered by 2.2 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.
- The third most common unwanted software family encountered in Jamaica in 4Q14 was Win32/BetterSurf, which was encountered by 1.6 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.

Top threat families by infection rate

The most common malware families by infection rate in Jamaica in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	5.8
2	Win32/Brontok	Worms	1.2
3	Win32/Gamarue	Worms	1.1
4	Win32/Vobfus	Worms	0.8
5	Win32/Sality	Viruses	0.5
6	Win32/Alureon	Trojans	0.4
7	Win32/Sefnit	Trojans	0.4
8	MSIL/Bladabindi	Backdoors	0.4
9	Win32/Zbot	Password Stealers & Monitoring Tools	0.2
10	Win32/Virut	Viruses	0.2

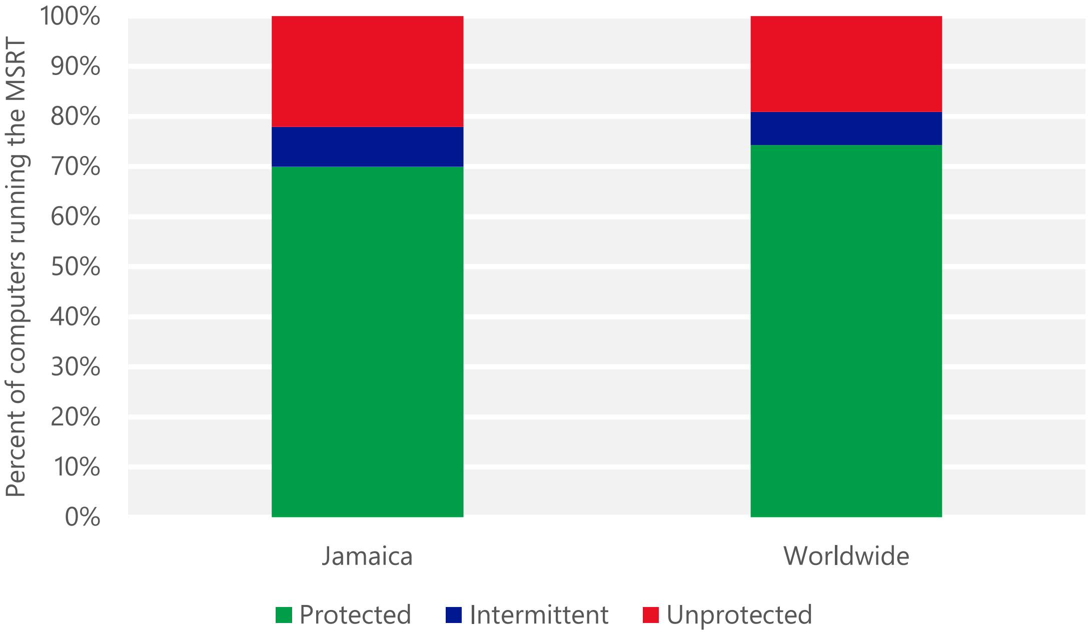
- The most common threat family infecting computers in Jamaica in 4Q14 was VBS/Jenxcus, which was detected and removed from 5.8 of every 1,000 unique computers scanned by the MSRT. VBS/Jenxcus is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Jamaica in 4Q14 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.
- The third most common threat family infecting computers in Jamaica in 4Q14 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 fourth most common threat family infecting computers in Jamaica in 4Q14 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 Jamaica and worldwide protected by real-time security software in 4Q14



Japan

The statistics presented here are generated by Microsoft security programs and services running on computers in Japan in 4Q14 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 succeds 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

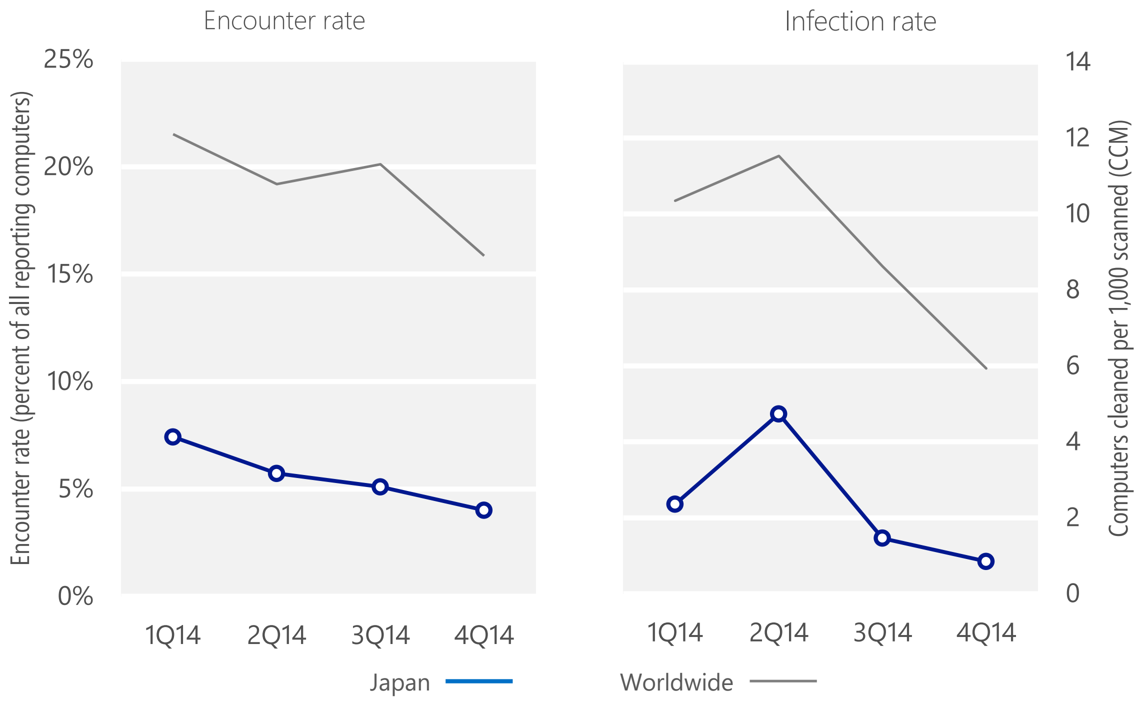
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Japan	7.4%	5.7%	5.1%	4.0%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Japan	2.4	4.7	1.5	0.8
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 4.0% percent of computers in Japan encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 0.8 of every 1,000 unique computers scanned in Japan in 4Q14 (a CCM score of 0.8, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Japan over the last four quarters, compared to the world as a whole.

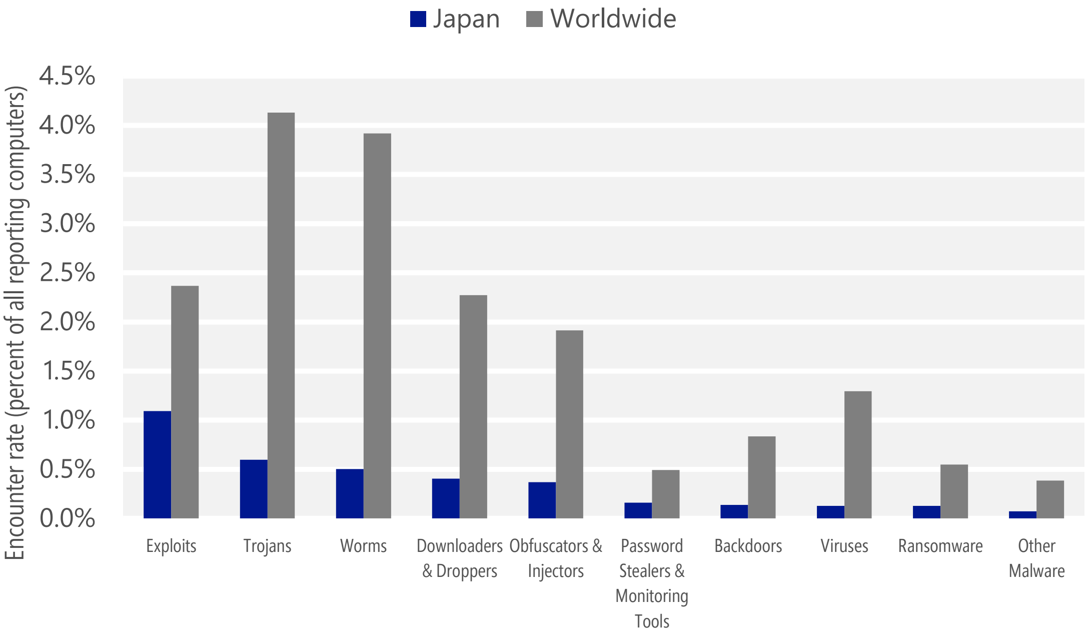
Malware encounter and infection rate trends in Japan and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

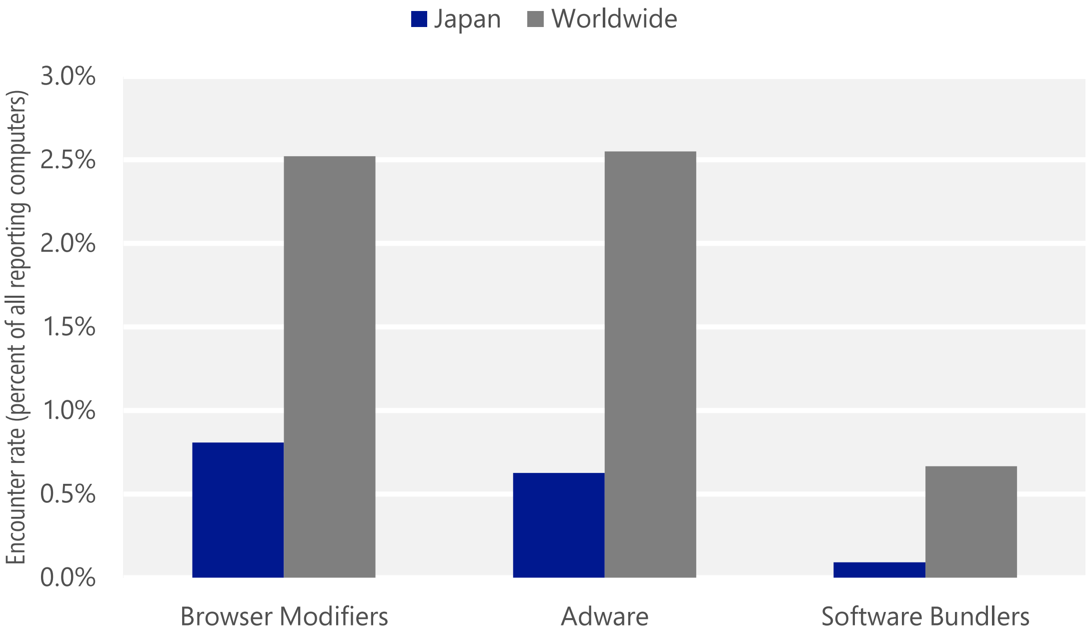
Malware encountered in Japan in 4Q14, by category



- The most common malware category in Japan in 4Q14 was Exploits. It was encountered by 1.1 percent of all computers there, down from 1.5 percent in 3Q14.
- The second most common malware category in Japan in 4Q14 was Trojans. It was encountered by 0.6 percent of all computers there, down from 1.0 percent in 3Q14.
- The third most common malware category in Japan in 4Q14 was Worms, which was encountered by 0.5 percent of all computers there, down from 0.5 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Japan in 4Q14, by category



- The most common unwanted software category in Japan in 4Q14 was Browser Modifiers. It was encountered by 0.8 percent of all computers there, down from 1.6 percent in 3Q14.
- The second most common unwanted software category in Japan in 4Q14 was Adware. It was encountered by 0.6 percent of all computers there, up from 0.3 percent in 3Q14.
- The third most common unwanted software category in Japan in 4Q14 was Software Bundlers, which was encountered by 0.1 percent of all computers there, up from 0.0 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Japan in 4Q14

	Family	Most significant category	% of reporting computers
1	JS/Axpergle	Exploits	0.6%
2	INF/Autorun	Obfuscators & Injectors	0.3%
3	Win32/Obfuscator	Obfuscators & Injectors	0.2%
4	Win32/Garveep	Downloaders & Droppers	0.2%
5	Win32/Conficker	Worms	0.1%
6	JS/Neclu	Exploits	0.1%
7	JS/Krypterade	Ransomware	0.1%
8	HTML/Meadgive	Exploits	0.1%
9	Win32/Zbot	Password Stealers & Monitoring Tools	0.1%
10	Win32/Anogre	Exploits	0.1%

- The most common malware family encountered in Japan in 4Q14 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 second most common malware family encountered in Japan in 4Q14 was INF/Autorun, which was encountered by 0.3 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 Japan in 4Q14 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.
- The fourth most common malware family encountered in Japan in 4Q14 was Win32/Garveep, which was encountered by 0.2 percent of reporting computers there. Win32/Garveep is a threat that downloads and installs other programs without the user’s consent, including other malware.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Japan in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	0.7%
2	Win32/Costmin	Adware	0.2%
3	Win32/Pennybee	Adware	0.1%
4	Win32/BetterSurf	Adware	0.1%
5	Win32/Defaulttab	Browser Modifiers	0.1%

- The most common unwanted software family encountered in Japan in 4Q14 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.
- The second most common unwanted software family encountered in Japan in 4Q14 was Win32/Costmin, which was encountered by 0.2 percent of reporting computers there. Win32/Costmin is an adware family that installs itself as a browser extension for Internet Explorer, Mozilla Firefox, and Google Chrome, and displays advertisements as the user browses the Internet.
- The third most common unwanted software family encountered in Japan in 4Q14 was Win32/Pennybee, which was encountered by 0.1 percent of reporting computers there. Win32/Pennybee is adware that shows ads as the user browses the web. It can be installed from the program's website or bundled with some third-party software installation programs.

Top threat families by infection rate

The most common malware families by infection rate in Japan in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Zbot	Password Stealers & Monitoring Tools	0.3
2	Win32/Alureon	Trojans	0.1
3	Win32/Sefnit	Trojans	0.1
4	Win32/Sirefef	Trojans	<0.1
5	Win32/Taterf	Worms	<0.1
6	JS/Miuref	Trojans	<0.1
7	Win32/Cutwail	Downloaders & Droppers	<0.1
8	Win32/Conficker	Worms	<0.1
9	Win32/Sality	Viruses	<0.1
10	MSIL/Spacekito	Trojans	<0.1

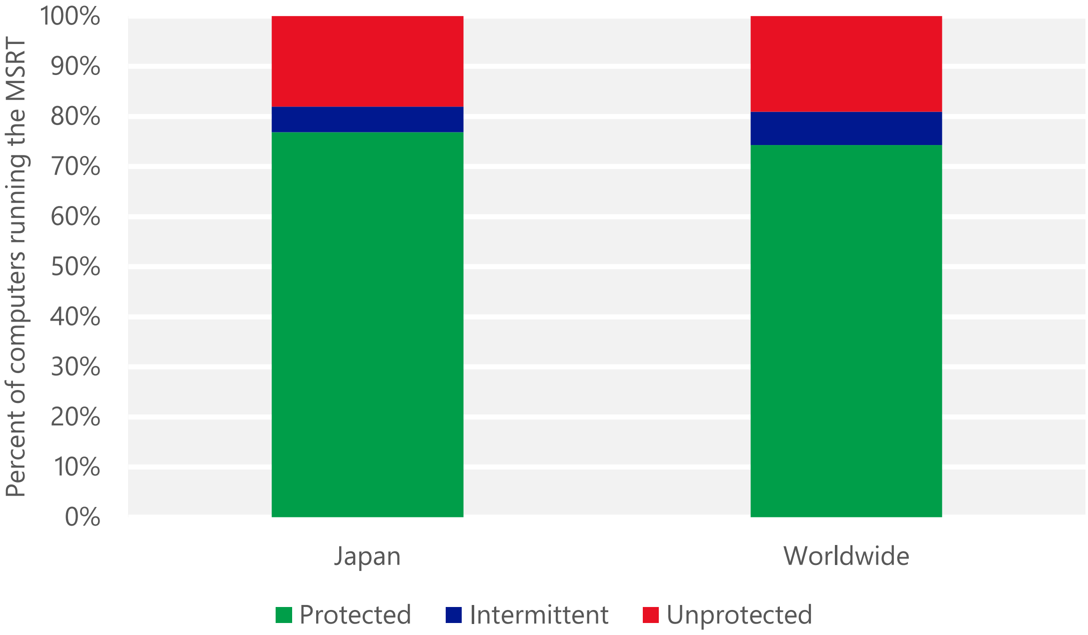
- The most common threat family infecting computers in Japan in 4Q14 was Win32/Zbot, which was detected and removed from 0.3 of every 1,000 unique computers scanned by the MSRT. Win32/Zbot is a family of password stealing trojans that also contains backdoor functionality allowing unauthorized access and control of an affected computer.
- The second most common threat family infecting computers in Japan in 4Q14 was Win32/Alureon, which was detected and removed from 0.1 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 third most common threat family infecting computers in Japan in 4Q14 was Win32/Sefnit, which was detected and removed from 0.1 of every 1,000 unique computers scanned by the MSRT. Win32/Sefnit is a family of trojans that can allow backdoor access, download files, and use the computer and Internet connection for click fraud. Some variants can monitor web browsers and hijack search results.
- The fourth most common threat family infecting computers in Japan in 4Q14 was Win32/Sirefef, which was detected and removed from <0.1 of every 1,000 unique computers scanned by the MSRT. Win32/Sirefef is a malware platform that receives and runs modules that perform different 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 Japan and worldwide protected by real-time security software in 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.13 drive-by download URLs for every 1,000 URLs hosted in Japan, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.09 drive-by download URLs for every 1,000 URLs hosted in Japan, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Japan and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Japan	0.13	0.09
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Jordan

The statistics presented here are generated by Microsoft security programs and services running on computers in Jordan in 4Q14 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 succeds 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

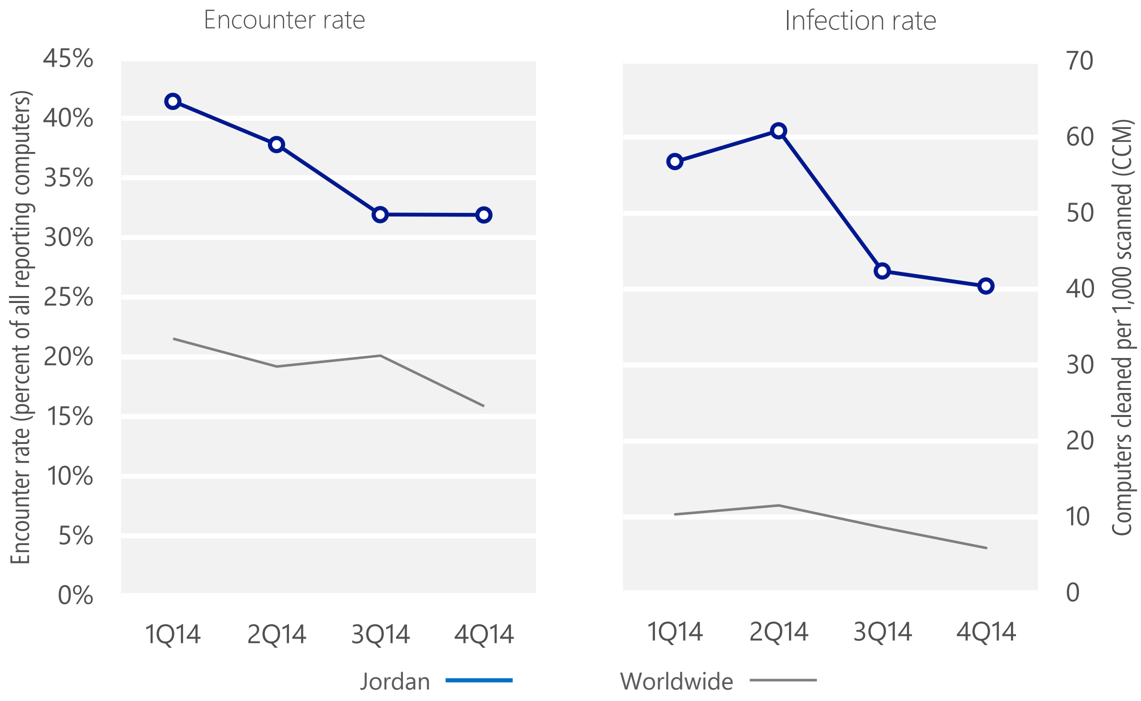
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Jordan	41.4%	37.8%	31.9%	31.9%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Jordan	56.8	60.8	42.4	40.4
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 31.9% percent of computers in Jordan encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 40.4 of every 1,000 unique computers scanned in Jordan in 4Q14 (a CCM score of 40.4, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Jordan over the last four quarters, compared to the world as a whole.

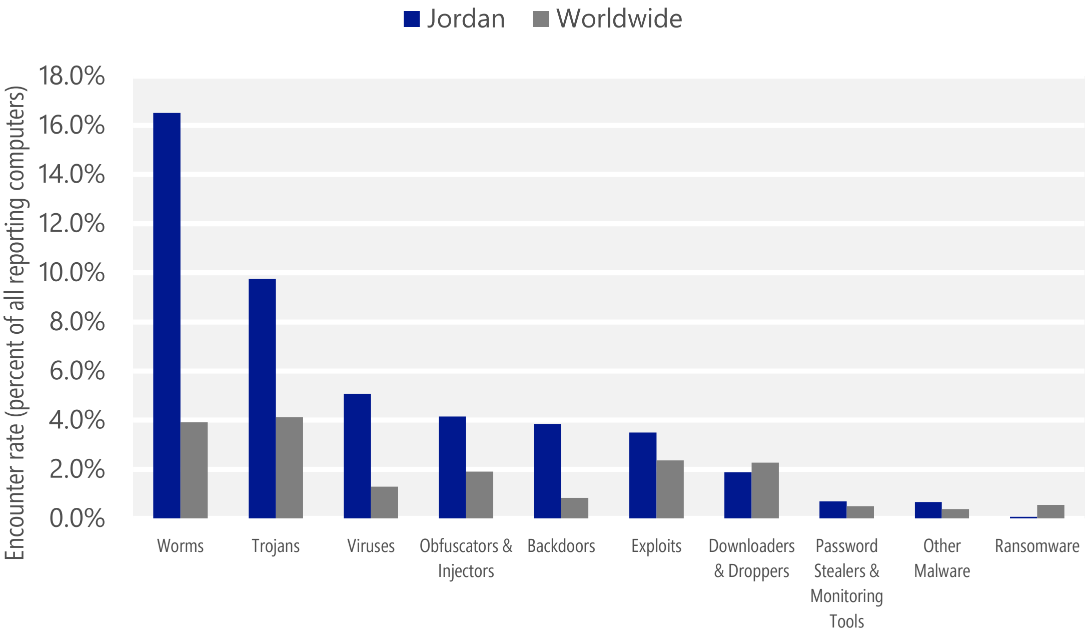
Malware encounter and infection rate trends in Jordan and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

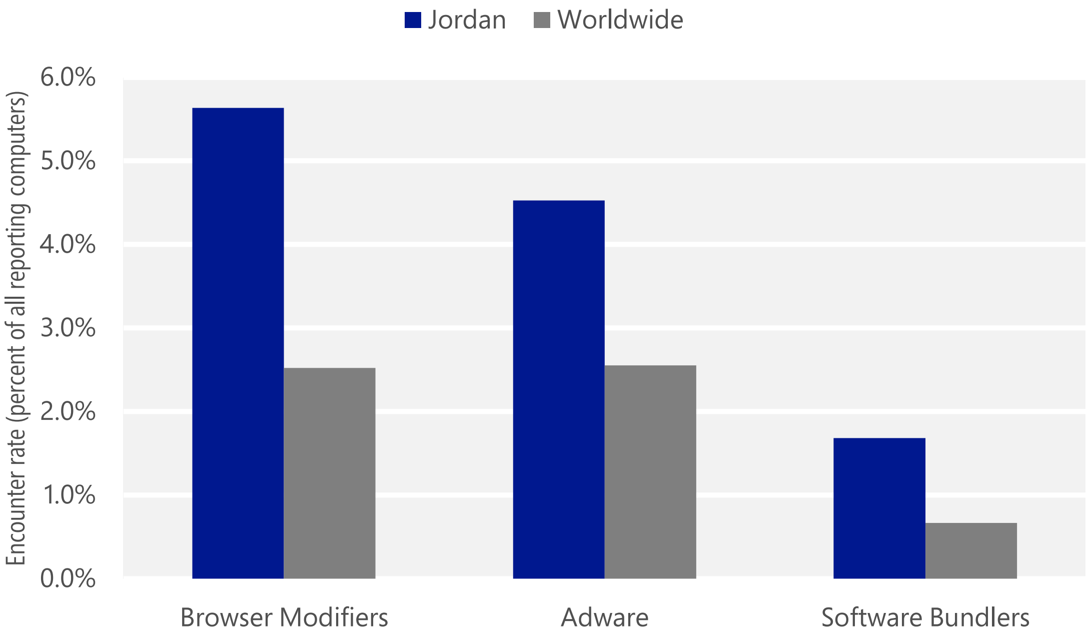
Malware encountered in Jordan in 4Q14, by category



- The most common malware category in Jordan in 4Q14 was Worms. It was encountered by 16.5 percent of all computers there, up from 14.5 percent in 3Q14.
- The second most common malware category in Jordan in 4Q14 was Trojans. It was encountered by 9.8 percent of all computers there, down from 11.5 percent in 3Q14.
- The third most common malware category in Jordan in 4Q14 was Viruses, which was encountered by 5.1 percent of all computers there, up from 4.4 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Jordan in 4Q14, by category



- The most common unwanted software category in Jordan in 4Q14 was Browser Modifiers. It was encountered by 5.6 percent of all computers there, down from 7.6 percent in 3Q14.
- The second most common unwanted software category in Jordan in 4Q14 was Adware. It was encountered by 4.5 percent of all computers there, up from 0.7 percent in 3Q14.
- The third most common unwanted software category in Jordan in 4Q14 was Software Bundlers, which was encountered by 1.7 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Jordan in 4Q14

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	10.5%
2	Win32/Gamarue	Worms	4.2%
3	INF/Autorun	Obfuscators & Injectors	3.7%
4	Win32/Sality	Viruses	2.9%
5	Win32/Ramnit	Trojans	2.7%
6	Win32/CplLnk	Exploits	2.7%
7	Win32/Sulunch	Trojans	2.0%
8	Win32/Dorkbot	Worms	2.0%
9	Win32/Vermis	Worms	2.0%
10	Win32/Caphaw	Backdoors	1.7%

- The most common malware family encountered in Jordan in 4Q14 was VBS/Jenxcus, which was encountered by 10.5 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 Jordan in 4Q14 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 Jordan in 4Q14 was INF/Autorun, which was encountered by 3.7 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 fourth most common malware family encountered in Jordan in 4Q14 was Win32/Sality, which was encountered by 2.9 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 Jordan in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	3.9%
2	Win32/Defaulttab	Browser Modifiers	1.9%
3	Win32/BetterSurf	Adware	1.6%
4	Win32/Brya	Adware	1.4%
5	Win32/Costmin	Adware	1.4%

- The most common unwanted software family encountered in Jordan in 4Q14 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 second most common unwanted software family encountered in Jordan in 4Q14 was Win32/Defaulttab, which was encountered by 1.9 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.
- The third most common unwanted software family encountered in Jordan in 4Q14 was Win32/BetterSurf, which was encountered by 1.6 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.

Top threat families by infection rate

The most common malware families by infection rate in Jordan in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	17.8
2	Win32/Sality	Viruses	7.7
3	Win32/Gamarue	Worms	5.4
4	Win32/Ramnit	Trojans	3.8
5	MSIL/Bladabindi	Backdoors	2.2
6	Win32/Dorkbot	Worms	2.1
7	Win32/Pramro	Trojans	1.0
8	Win32/Vobfus	Worms	0.8
9	Win32/Lethic	Trojans	0.8
10	Win32/Nuqel	Worms	0.8

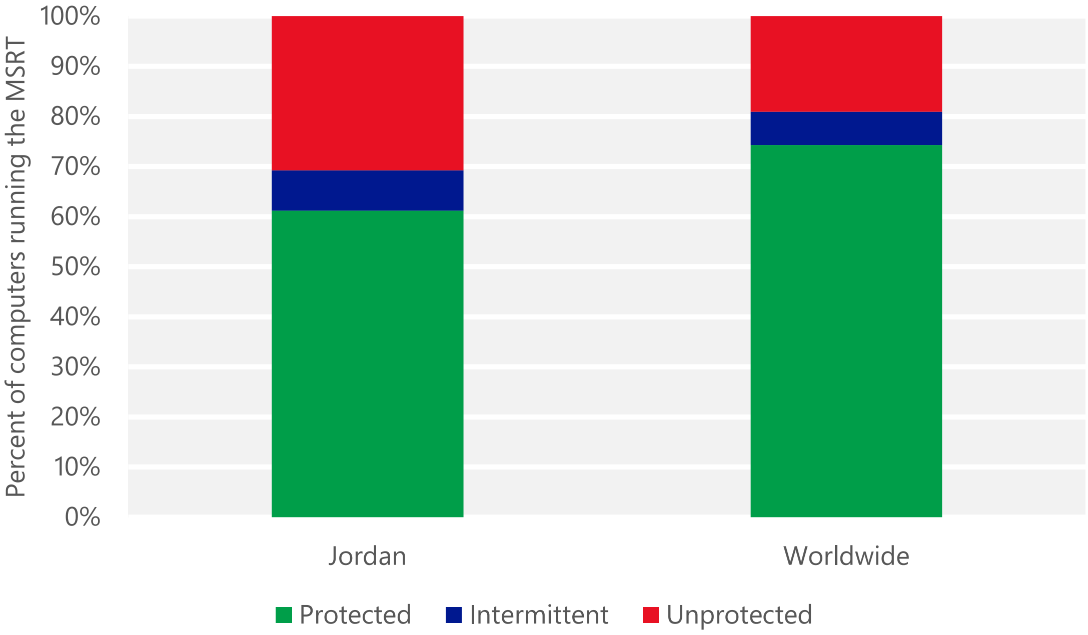
- The most common threat family infecting computers in Jordan in 4Q14 was VBS/Jenxcus, which was detected and removed from 17.8 of every 1,000 unique computers scanned by the MSRT. VBS/Jenxcus is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Jordan in 4Q14 was Win32/Sality, which was detected and removed from 7.7 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 Jordan in 4Q14 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.
- The fourth most common threat family infecting computers in Jordan in 4Q14 was Win32/Ramnit, which was detected and removed from 3.8 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.

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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.78 drive-by download URLs for every 1,000 URLs hosted in Jordan, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.36 drive-by download URLs for every 1,000 URLs hosted in Jordan, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Jordan and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Jordan	0.78	0.36
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Kazakhstan

The statistics presented here are generated by Microsoft security programs and services running on computers in Kazakhstan in 4Q14 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 succeds 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

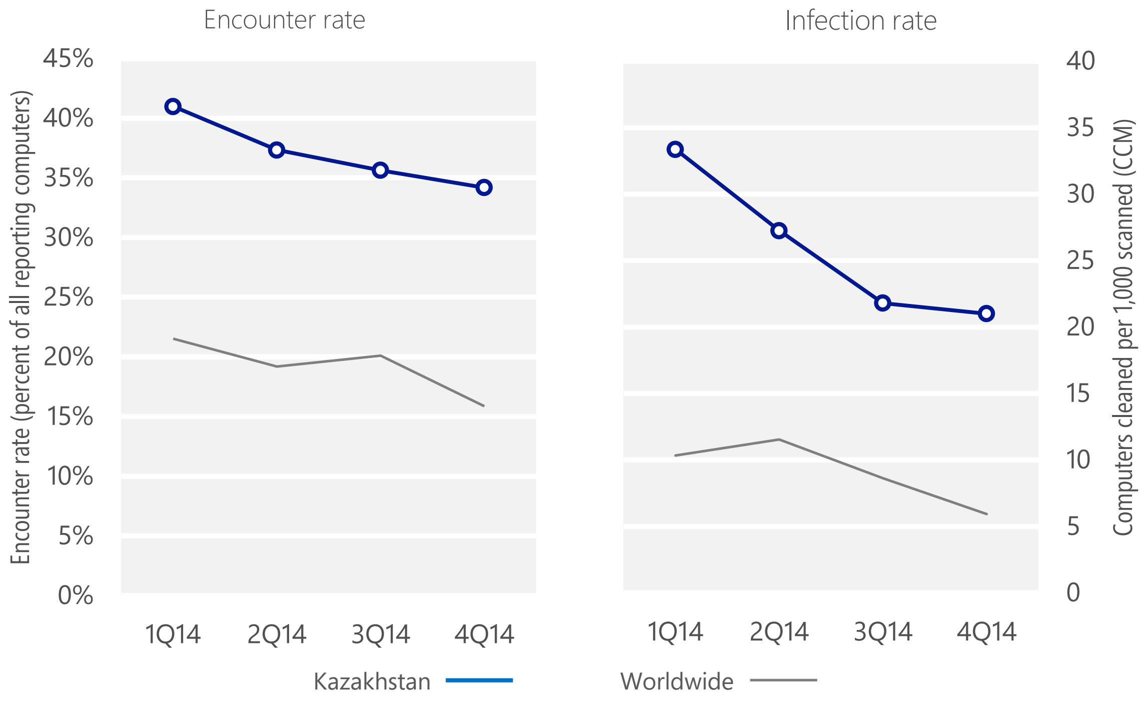
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Kazakhstan	41.0%	37.3%	35.6%	34.2%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Kazakhstan	33.4	27.3	21.8	21.0
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 34.2% percent of computers in Kazakhstan encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 21.0 of every 1,000 unique computers scanned in Kazakhstan in 4Q14 (a CCM score of 21.0, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Kazakhstan over the last four quarters, compared to the world as a whole.

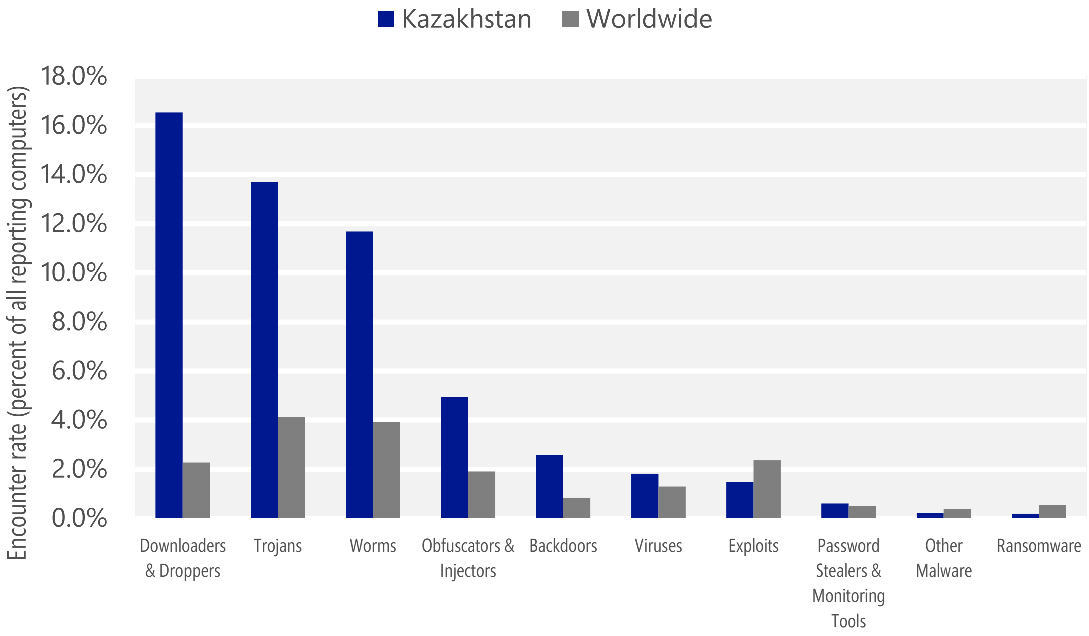
Malware encounter and infection rate trends in Kazakhstan and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

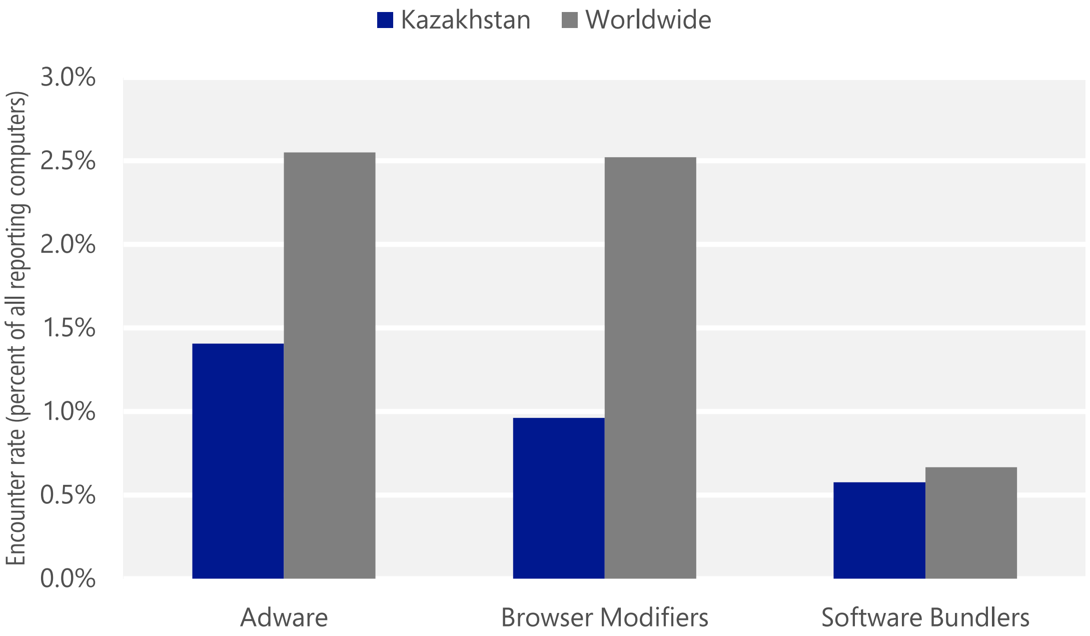
Malware encountered in Kazakhstan in 4Q14, by category



- The most common malware category in Kazakhstan in 4Q14 was Downloaders & Droppers. It was encountered by 16.5 percent of all computers there, down from 18.6 percent in 3Q14.
- The second most common malware category in Kazakhstan in 4Q14 was Trojans. It was encountered by 13.7 percent of all computers there, up from 12.5 percent in 3Q14.
- The third most common malware category in Kazakhstan in 4Q14 was Worms, which was encountered by 11.7 percent of all computers there, up from 10.8 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Kazakhstan in 4Q14, by category



- The most common unwanted software category in Kazakhstan in 4Q14 was Adware. It was encountered by 1.4 percent of all computers there, down from 2.7 percent in 3Q14.
- The second most common unwanted software category in Kazakhstan in 4Q14 was Browser Modifiers. It was encountered by 1.0 percent of all computers there, up from 0.2 percent in 3Q14.
- The third most common unwanted software category in Kazakhstan in 4Q14 was Software Bundlers, which was encountered by 0.6 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Kazakhstan in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Ogimant	Downloaders & Droppers	14.2%
2	Win32/Gamarue	Worms	8.2%
3	Win32/Peaac	Trojans	5.1%
4	Win32/Obfuscator	Obfuscators & Injectors	3.0%
5	VBS/Jenxcus	Worms	1.7%
6	Win32/Peals	Trojans	1.5%
7	Win32/Esaprof	Downloaders & Droppers	1.3%
8	Win32/Morix	Backdoors	1.2%
9	INF/Autorun	Obfuscators & Injectors	1.2%
10	BAT/Puccmine	Worms	1.2%

- The most common malware family encountered in Kazakhstan in 4Q14 was Win32/Ogimant, which was encountered by 14.2 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 second most common malware family encountered in Kazakhstan in 4Q14 was Win32/Gamarue, which was encountered by 8.2 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 4Q14 was Win32/Peaac, which was encountered by 5.1 percent of reporting computers there. Win32/Peaac is a generic detection for various threats that display trojan characteristics.
- The fourth most common malware family encountered in Kazakhstan in 4Q14 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.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Kazakhstan in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/BetterSurf	Adware	1.1%
2	Win32/Gofileexpress	Software Bundlers	0.5%
3	Win32/Defaulttab	Browser Modifiers	0.5%
4	Win32/Couponruc	Browser Modifiers	0.4%

- The most common unwanted software family encountered in Kazakhstan in 4Q14 was Win32/BetterSurf, which was encountered by 1.1 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.
- The second most common unwanted software family encountered in Kazakhstan in 4Q14 was Win32/Gofileexpress, which was encountered by 0.5 percent of reporting computers there. Win32/Gofileexpress is a software bundler that installs other unwanted software, including Adware:Win32/Lollipop and Adware:Win32/CostMin.
- The third most common unwanted software family encountered in Kazakhstan in 4Q14 was Win32/Defaulttab, which was encountered by 0.5 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.

Top threat families by infection rate

The most common malware families by infection rate in Kazakhstan in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Gamarue	Worms	11.8
2	VBS/Jenxcus	Worms	2.3
3	Win32/Ramnit	Trojans	1.9
4	Win32/Vobfus	Worms	1.5
5	Win32/Tofsee	Backdoors	0.9
6	Win32/Deminnix	Trojans	0.9
7	Win32/Sality	Viruses	0.7
8	Win32/Dorkbot	Worms	0.6
9	Win32/Lethic	Trojans	0.3
10	Win32/Nuqel	Worms	0.2

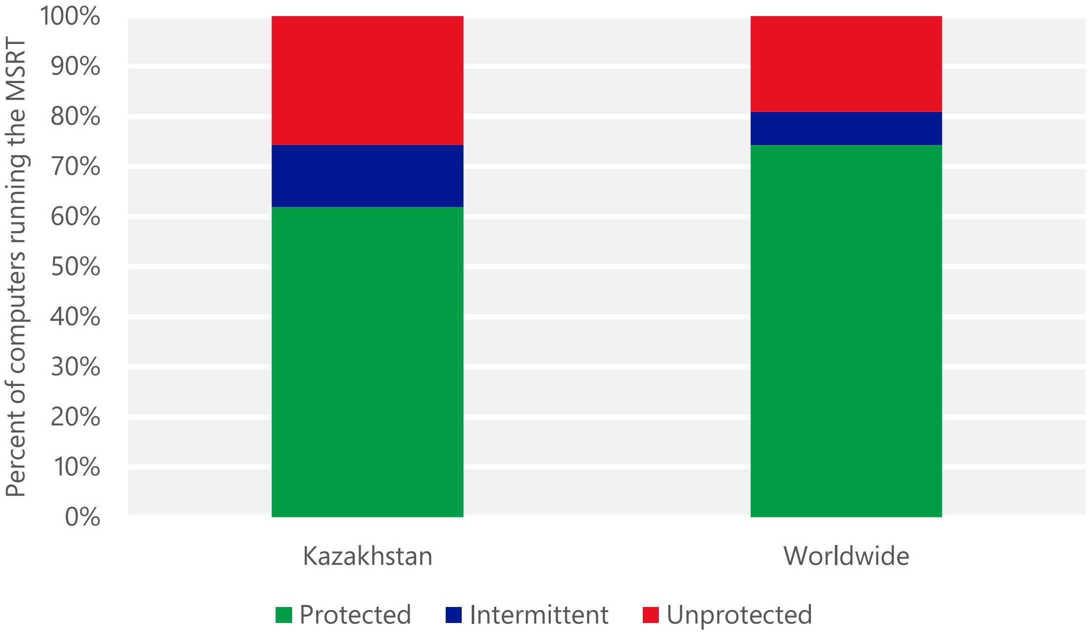
- The most common threat family infecting computers in Kazakhstan in 4Q14 was Win32/Gamarue, which was detected and removed from 11.8 of every 1,000 unique computers scanned by the MSRT. Win32/Gamarue is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The second most common threat family infecting computers in Kazakhstan in 4Q14 was VBS/Jenxcus, which was detected and removed from 2.3 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 Kazakhstan in 4Q14 was Win32/Ramnit, which was detected and removed from 1.9 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 Kazakhstan in 4Q14 was Win32/Vobfus, which was detected and removed from 1.5 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 Kazakhstan and worldwide protected by real-time security software in 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.35 drive-by download URLs for every 1,000 URLs hosted in Kazakhstan, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.86 drive-by download URLs for every 1,000 URLs hosted in Kazakhstan, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Kazakhstan and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Kazakhstan	0.35	0.86
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Kenya

The statistics presented here are generated by Microsoft security programs and services running on computers in Kenya in 4Q14 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 succeds 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

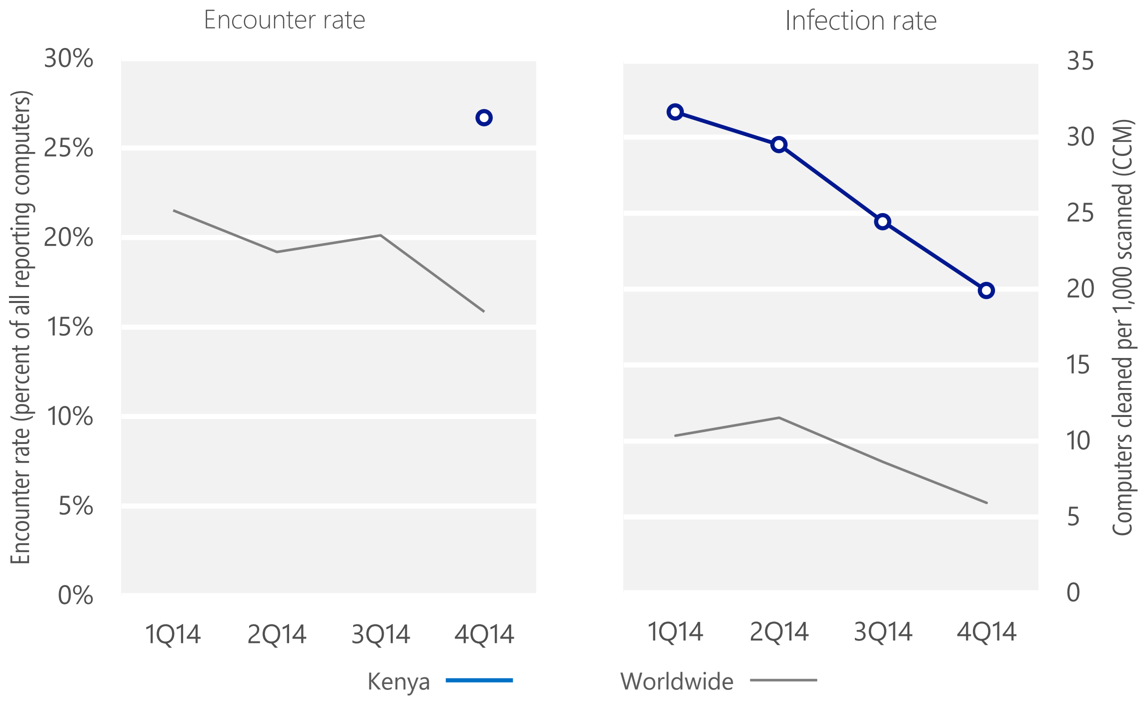
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Kenya	N/A	N/A	N/A	26.7%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Kenya	31.6	29.5	24.4	19.9
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 26.7% percent of computers in Kenya encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 19.9 of every 1,000 unique computers scanned in Kenya in 4Q14 (a CCM score of 19.9, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Kenya over the last four quarters, compared to the world as a whole.

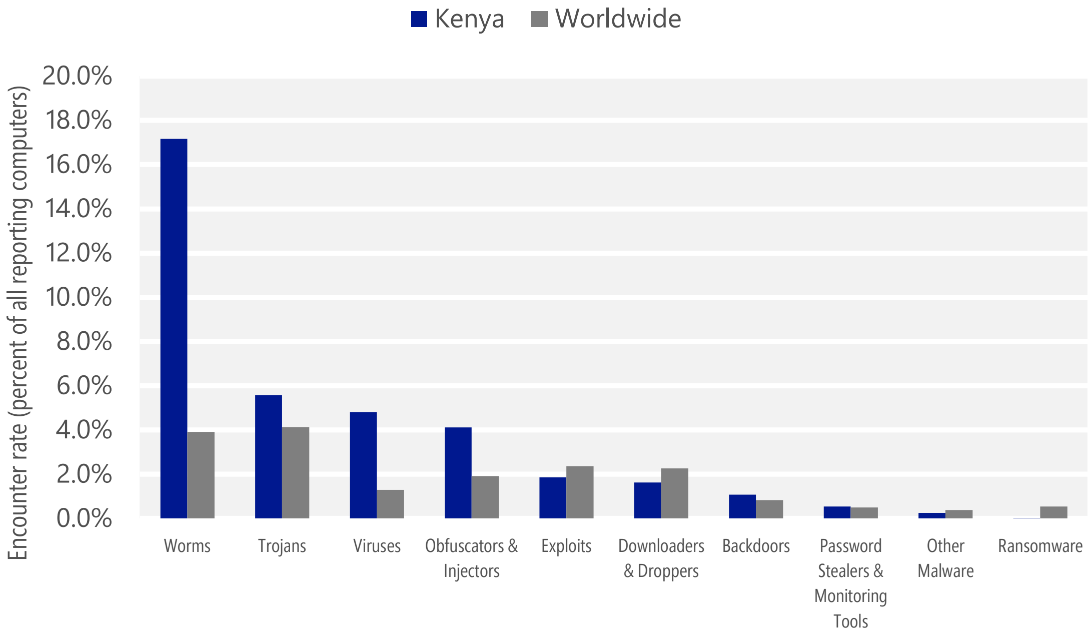
Malware encounter and infection rate trends in Kenya and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

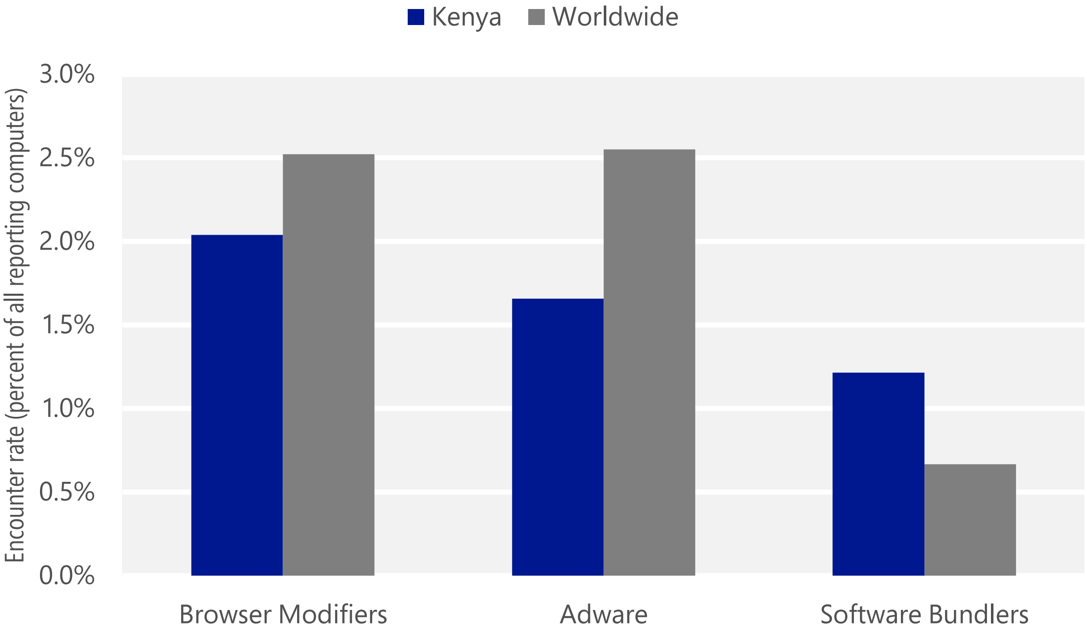
Malware encountered in Kenya in 4Q14, by category



- The most common malware category in Kenya in 4Q14 was Worms. It was encountered by 17.2 percent of all computers there, up from N/A percent in 3Q14.
- The second most common malware category in Kenya in 4Q14 was Trojans. It was encountered by 5.6 percent of all computers there, up from N/A percent in 3Q14.
- The third most common malware category in Kenya in 4Q14 was Viruses, which was encountered by 4.8 percent of all computers there, up from N/A percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Kenya in 4Q14, by category



- The most common unwanted software category in Kenya in 4Q14 was Browser Modifiers. It was encountered by 2.0 percent of all computers there, up from N/A percent in 3Q14.
- The second most common unwanted software category in Kenya in 4Q14 was Adware. It was encountered by 1.7 percent of all computers there, up from N/A percent in 3Q14.
- The third most common unwanted software category in Kenya in 4Q14 was Software Bundlers, which was encountered by 1.2 percent of all computers there, up from N/A percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Kenya in 4Q14

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	7.1%
2	INF/Autorun	Obfuscators & Injectors	6.7%
3	Win32/Gamarue	Worms	6.3%
4	Win32/Copali	Worms	3.4%
5	Win32/Sality	Viruses	3.0%
6	Win32/Ippedo	Worms	2.0%
7	Win32/Virut	Viruses	2.0%
8	Win32/Comame	Trojans	2.0%
9	Win32/CplLnk	Exploits	1.4%
10	Win32/Ramnit	Trojans	1.1%

- The most common malware family encountered in Kenya in 4Q14 was VBS/Jenxcus, which was encountered by 7.1 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 Kenya in 4Q14 was INF/Autorun, which was encountered by 6.7 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 Kenya in 4Q14 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 Kenya in 4Q14 was Win32/Copali, which was encountered by 3.4 percent of reporting computers there. Win32/Copali is a family of worms that can download other malware, including PWS:Win32/Zbot. They spread through infected network and removable drives.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Kenya in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	1.2%
2	Win32/Gofileexpress	Software Bundlers	1.0%

- The most common unwanted software family encountered in Kenya in 4Q14 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 Kenya in 4Q14 was Win32/Gofileexpress, which was encountered by 1.0 percent of reporting computers there. Win32/Gofileexpress is a software bundler that installs other unwanted software, including Adware:Win32/Lollipop and Adware:Win32/CostMin.
- The third most common unwanted software family encountered in Kenya in 4Q14 was N/A, which was encountered by percent of reporting computers there.

Top threat families by infection rate

The most common malware families by infection rate in Kenya in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	6.9
2	Win32/Gamarue	Worms	6.2
3	Win32/Sality	Viruses	4.9
4	Win32/Zbot	Password Stealers & Monitoring Tools	0.8
5	Win32/Ramnit	Trojans	0.7
6	Win32/Pramro	Trojans	0.5
7	Win32/Parite	Viruses	0.3
8	MSIL/Bladabindi	Backdoors	0.3
9	Win32/Dorkbot	Worms	0.2
10	Win32/Chir	Viruses	0.2

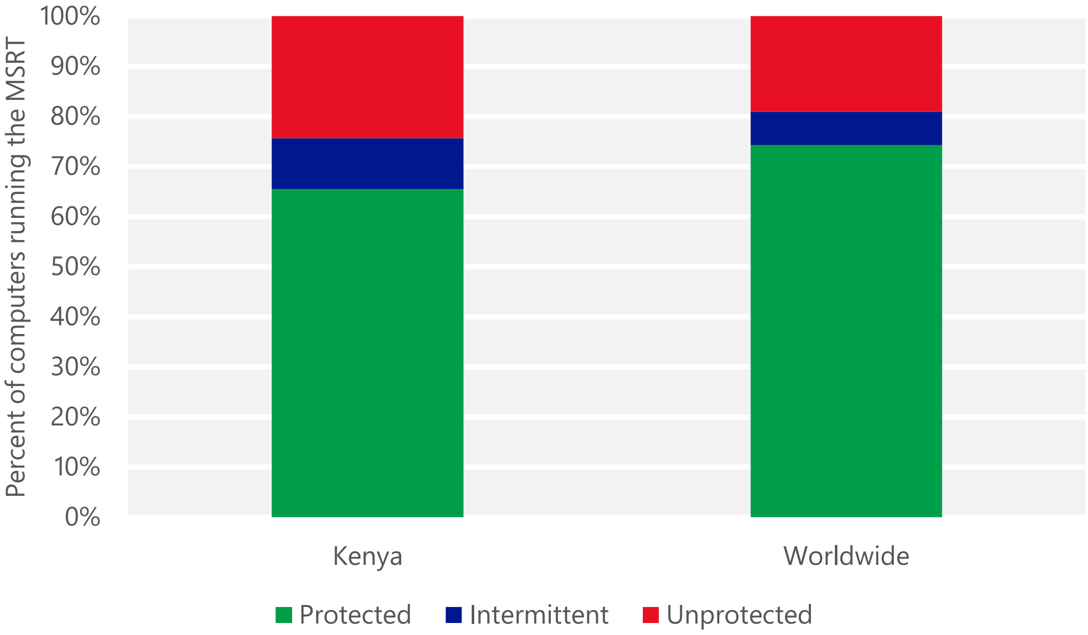
- The most common threat family infecting computers in Kenya in 4Q14 was VBS/Jenxcus, which was detected and removed from 6.9 of every 1,000 unique computers scanned by the MSRT. VBS/Jenxcus is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Kenya in 4Q14 was Win32/Gamarue, which was detected and removed from 6.2 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 Kenya in 4Q14 was Win32/Sality, which was detected and removed from 4.9 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 Kenya in 4Q14 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.

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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 3.67 drive-by download URLs for every 1,000 URLs hosted in Kenya, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 1.83 drive-by download URLs for every 1,000 URLs hosted in Kenya, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Kenya and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Kenya	3.67	1.83
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Korea

The statistics presented here are generated by Microsoft security programs and services running on computers in Korea in 4Q14 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 succeds 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

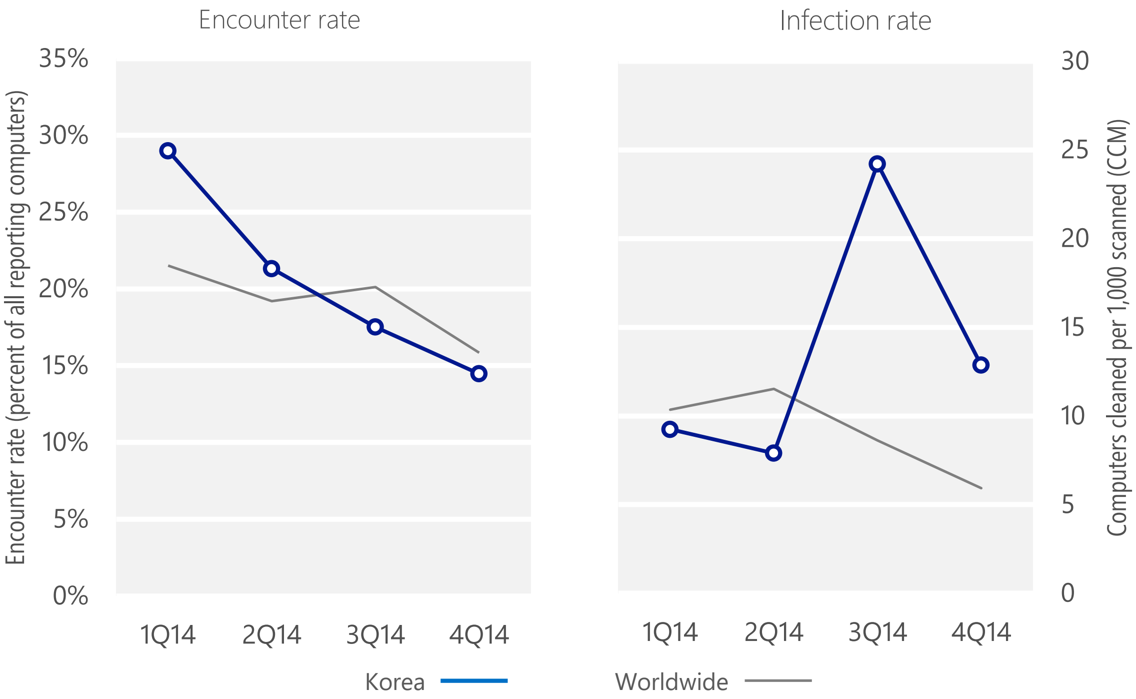
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Korea	29.0%	21.3%	17.5%	14.5%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Korea	9.2	7.9	24.2	12.9
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 14.5% percent of computers in Korea encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 12.9 of every 1,000 unique computers scanned in Korea in 4Q14 (a CCM score of 12.9, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Korea over the last four quarters, compared to the world as a whole.

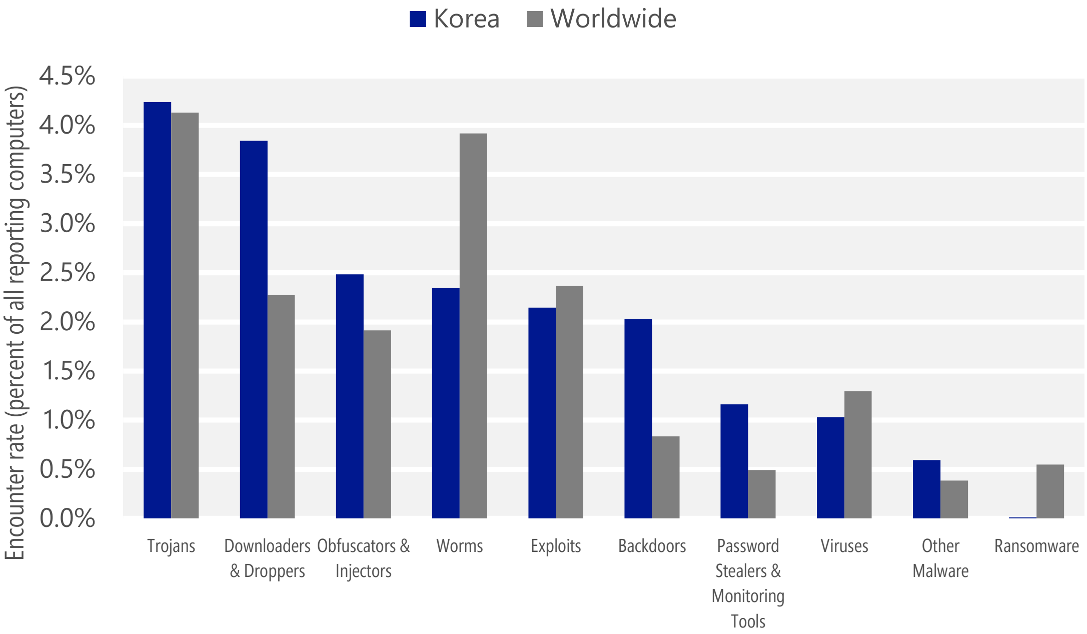
Malware encounter and infection rate trends in Korea and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

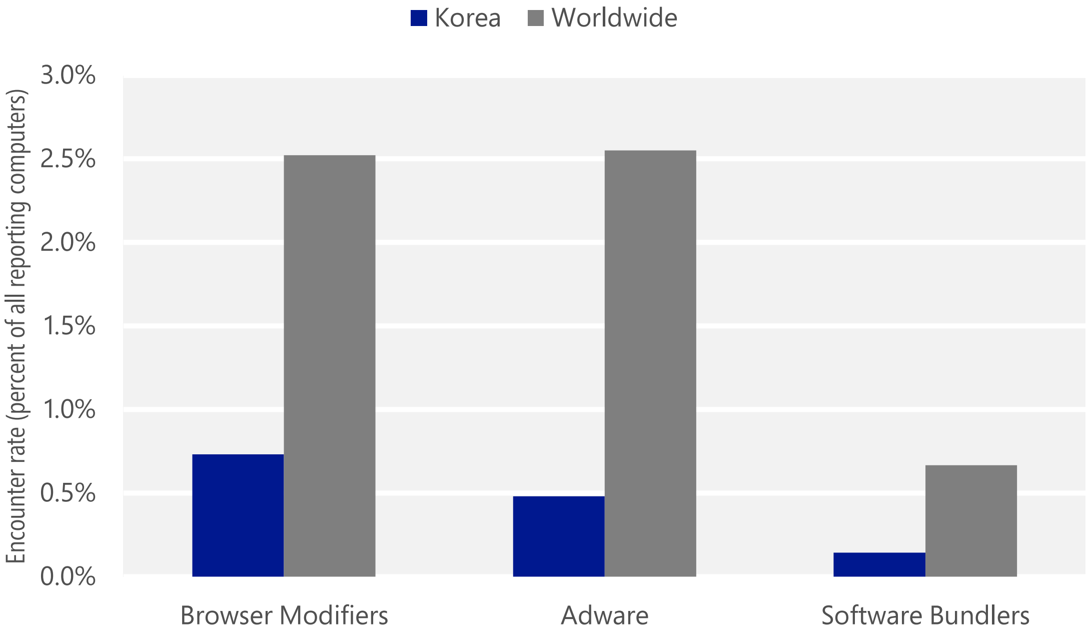
Malware encountered in Korea in 4Q14, by category



- The most common malware category in Korea in 4Q14 was Trojans. It was encountered by 4.2 percent of all computers there, down from 5.9 percent in 3Q14.
- The second most common malware category in Korea in 4Q14 was Downloaders & Droppers. It was encountered by 3.8 percent of all computers there, down from 5.6 percent in 3Q14.
- The third most common malware category in Korea in 4Q14 was Obfuscators & Injectors, which was encountered by 2.5 percent of all computers there, down from 3.0 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Korea in 4Q14, by category



- The most common unwanted software category in Korea in 4Q14 was Browser Modifiers. It was encountered by 0.7 percent of all computers there, down from 2.1 percent in 3Q14.
- The second most common unwanted software category in Korea in 4Q14 was Adware. It was encountered by 0.5 percent of all computers there, up from 0.1 percent in 3Q14.
- The third most common unwanted software category in Korea in 4Q14 was Software Bundlers, which was encountered by 0.1 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Korea in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Obfuscator	Obfuscators & Injectors	2.0%
2	Win32/Enterok	Downloaders & Droppers	2.0%
3	VBS/CVE-2014-6332	Exploits	1.1%
4	Win32/Xtrat	Backdoors	0.9%
5	Win32/OnLineGames	Password Stealers & Monitoring Tools	0.9%
6	Win32/Small	Backdoors	0.7%
7	INF/Autorun	Obfuscators & Injectors	0.6%
8	Win32/Estiwir	Trojans	0.6%
9	Win32/Msidebar	Trojans	0.6%
10	Win32/Dynamer	Trojans	0.6%

- The most common malware family encountered in Korea in 4Q14 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 Korea in 4Q14 was Win32/Enterok, which was encountered by 2.0 percent of reporting computers there.
- The third most common malware family encountered in Korea in 4Q14 was VBS/CVE-2014-6332, which was encountered by 1.1 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 fourth most common malware family encountered in Korea in 4Q14 was Win32/Xtrat, which was encountered by 0.9 percent of reporting computers there. Win32/Xtrat is a threat can install other malware on the computer, including malware that can record passwords, take pictures with a webcam, and steal personal information. It spreads by copying itself to removable drives, and might be downloaded from file sharing websites.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Korea in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	0.4%
2	Win32/Defaulttab	Browser Modifiers	0.2%
3	Win32/Hebogo	Adware	0.2%
4	Win32/Costmin	Adware	0.1%
5	Win32/BetterSurf	Adware	0.1%

- The most common unwanted software family encountered in Korea in 4Q14 was Win32/Couponruc, which was encountered by 0.4 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 Korea in 4Q14 was Win32/Defaulttab, which was encountered by 0.2 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.
- The third most common unwanted software family encountered in Korea in 4Q14 was Win32/Hebogo, which was encountered by 0.2 percent of reporting computers there. Win32/Hebogo is a program that offers language conversion features within Windows Internet Explorer. It may open pop-up advertisements based on web browsing habits.

Top threat families by infection rate

The most common malware families by infection rate in Korea in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Onescan	Other Malware	7.1
2	Win32/Nitol	Other Malware	2.7
3	VBS/Jenxcus	Worms	0.6
4	Win32/Sensode	Backdoors	0.5
5	Win32/Pluzoks	Downloaders & Droppers	0.3
6	MSIL/Bladabindi	Backdoors	0.2
7	Win32/Parite	Viruses	0.2
8	Win32/Taterf	Worms	0.2
9	Win32/Banker	Trojans	0.2
10	Win32/Frethog	Password Stealers & Monitoring Tools	0.2

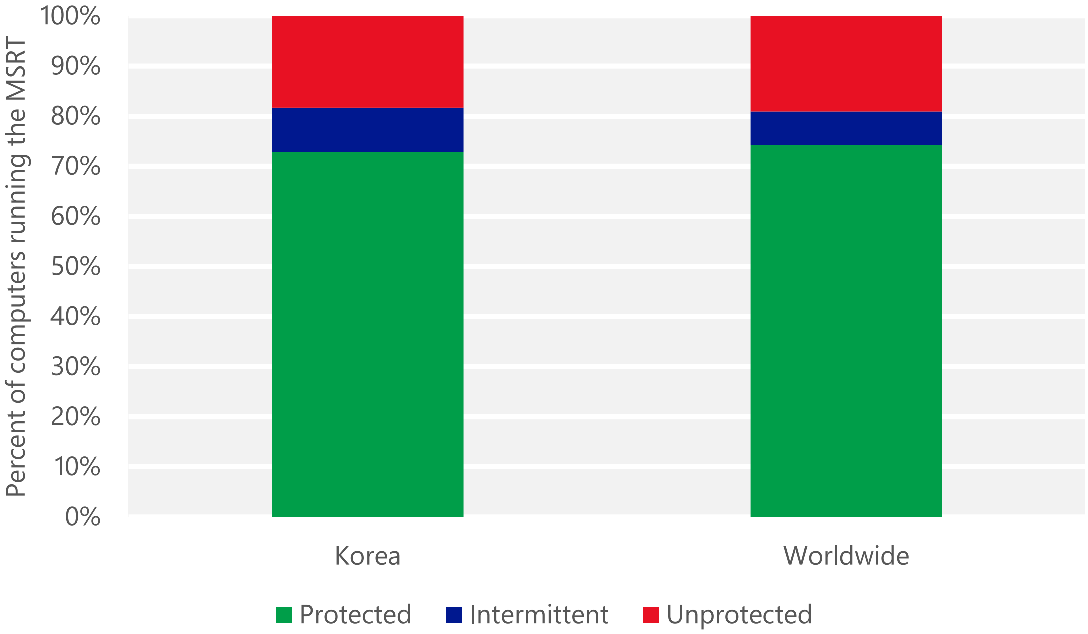
- The most common threat family infecting computers in Korea in 4Q14 was Win32/Onescan, which was detected and removed from 7.1 of every 1,000 unique computers scanned by the MSRT. Win32/Onescan is a Korean-language rogue security software family distributed under the names One Scan, Siren114, EnPrivacy, PC Trouble, Smart Vaccine, and many others.
- The second most common threat family infecting computers in Korea in 4Q14 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 4Q14 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.
- The fourth most common threat family infecting computers in Korea in 4Q14 was Win32/Sensode, which was detected and removed from 0.5 of every 1,000 unique computers scanned by the MSRT.

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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.36 drive-by download URLs for every 1,000 URLs hosted in Korea, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.45 drive-by download URLs for every 1,000 URLs hosted in Korea, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Korea and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Korea	0.36	0.45
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Kuwait

The statistics presented here are generated by Microsoft security programs and services running on computers in Kuwait in 4Q14 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 succeds 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

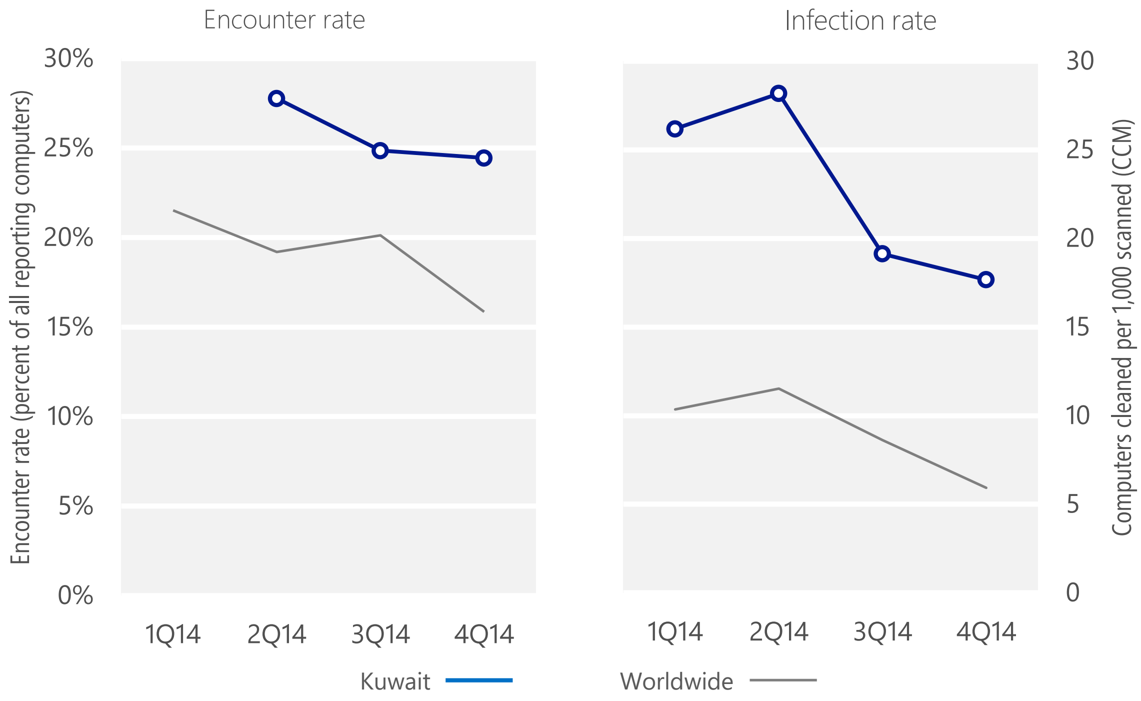
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Kuwait	N/A	27.8%	24.9%	24.4%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Kuwait	26.2	28.2	19.1	17.7
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 24.4% percent of computers in Kuwait encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 17.7 of every 1,000 unique computers scanned in Kuwait in 4Q14 (a CCM score of 17.7, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Kuwait over the last four quarters, compared to the world as a whole.

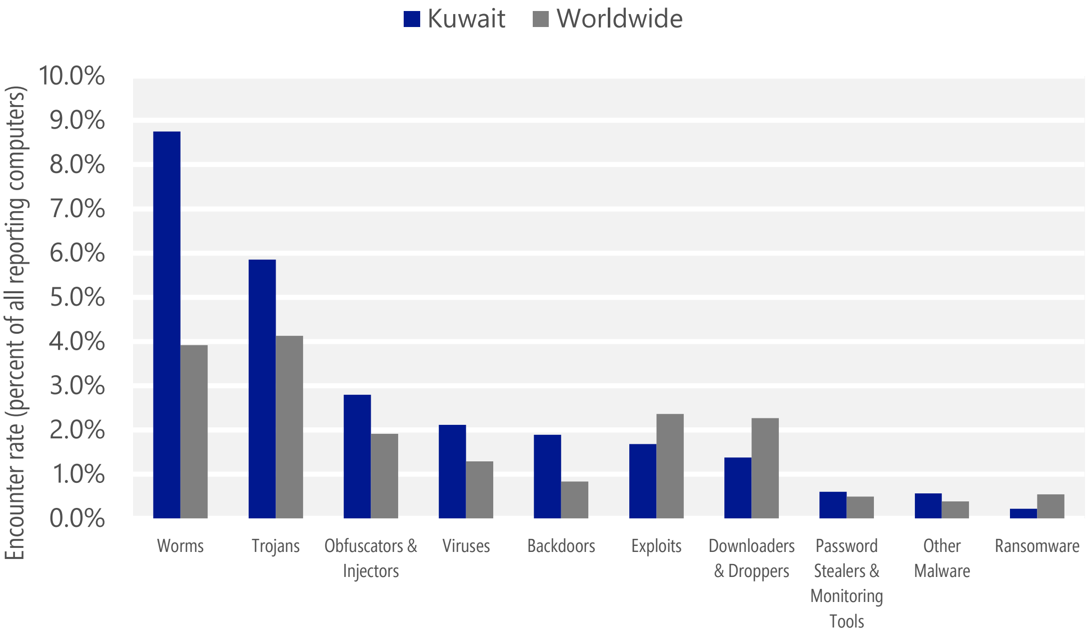
Malware encounter and infection rate trends in Kuwait and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

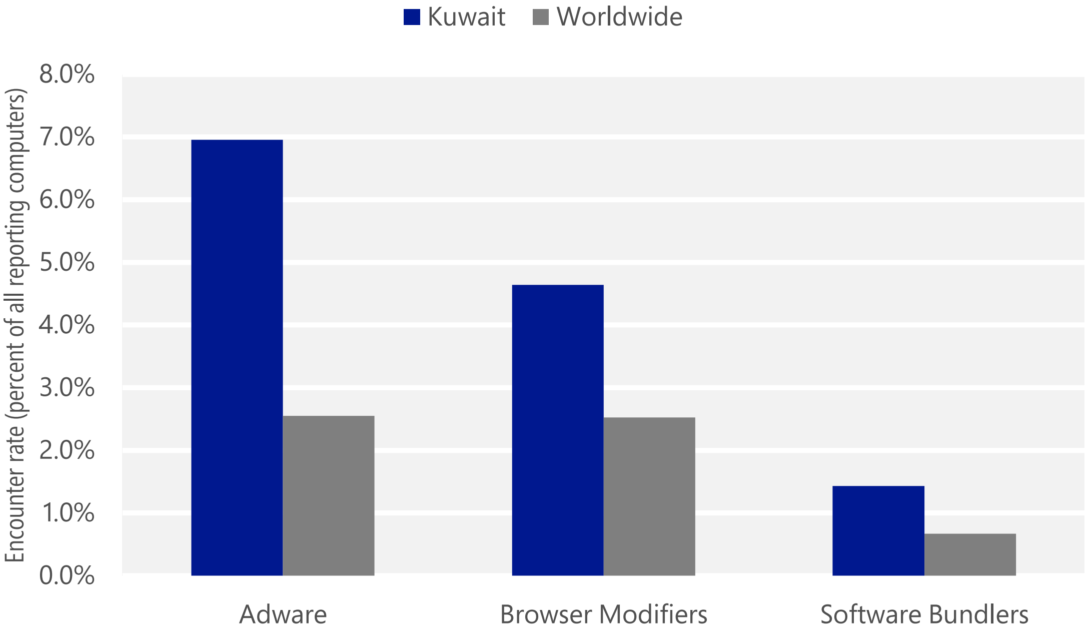
Malware encountered in Kuwait in 4Q14, by category



- The most common malware category in Kuwait in 4Q14 was Worms. It was encountered by 8.7 percent of all computers there, up from 8.0 percent in 3Q14.
- The second most common malware category in Kuwait in 4Q14 was Trojans. It was encountered by 5.9 percent of all computers there, down from 7.6 percent in 3Q14.
- The third most common malware category in Kuwait in 4Q14 was Obfuscators & Injectors, which was encountered by 2.8 percent of all computers there, down from 2.9 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Kuwait in 4Q14, by category



- The most common unwanted software category in Kuwait in 4Q14 was Adware. It was encountered by 7.0 percent of all computers there, down from 8.0 percent in 3Q14.
- The second most common unwanted software category in Kuwait in 4Q14 was Browser Modifiers. It was encountered by 4.6 percent of all computers there, up from 1.2 percent in 3Q14.
- The third most common unwanted software category in Kuwait in 4Q14 was Software Bundlers, which was encountered by 1.4 percent of all computers there, up from 0.2 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Kuwait in 4Q14

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	3.2%
2	Win32/Gamarue	Worms	2.4%
3	INF/Autorun	Obfuscators & Injectors	2.2%
4	Win32/Sality	Viruses	1.0%
5	Win32/Vermis	Worms	1.0%
6	Win32/Startpage	Trojans	1.0%
7	Win32/Obfuscator	Obfuscators & Injectors	0.9%
8	MSIL/Bladabindi	Backdoors	0.8%

- The most common malware family encountered in Kuwait in 4Q14 was VBS/Jenxcus, which was encountered by 3.2 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 4Q14 was Win32/Gamarue, which was encountered by 2.4 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 4Q14 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.
- The fourth most common malware family encountered in Kuwait in 4Q14 was Win32/Sality, which was encountered by 1.0 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 Kuwait in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Brya	Adware	4.1%
2	Win32/Couponruc	Browser Modifiers	3.0%
3	Win32/BetterSurf	Adware	1.5%
4	Win32/Defaulttab	Browser Modifiers	1.5%
5	Win32/Costmin	Adware	1.2%

- The most common unwanted software family encountered in Kuwait in 4Q14 was Win32/Brya, which was encountered by 4.1 percent of reporting computers there. Win32/Brya is a program that shows ads that the user cannot control as they browse the web. It does not have a working uninstaller.

- The second most common unwanted software family encountered in Kuwait in 4Q14 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 Kuwait in 4Q14 was Win32/BetterSurf, which was encountered by 1.5 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.

Top threat families by infection rate

The most common malware families by infection rate in Kuwait in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	5.0
2	Win32/Gamarue	Worms	3.2
3	Win32/Sality	Viruses	2.5
4	MSIL/Bladabindi	Backdoors	1.3
5	Win32/Vobfus	Worms	0.9
6	Win32/Dorkbot	Worms	0.9
7	Win32/Brontok	Worms	0.7
8	Win32/Ramnit	Trojans	0.6
9	Win32/Nuqel	Worms	0.5
10	Win32/Pramro	Trojans	0.4

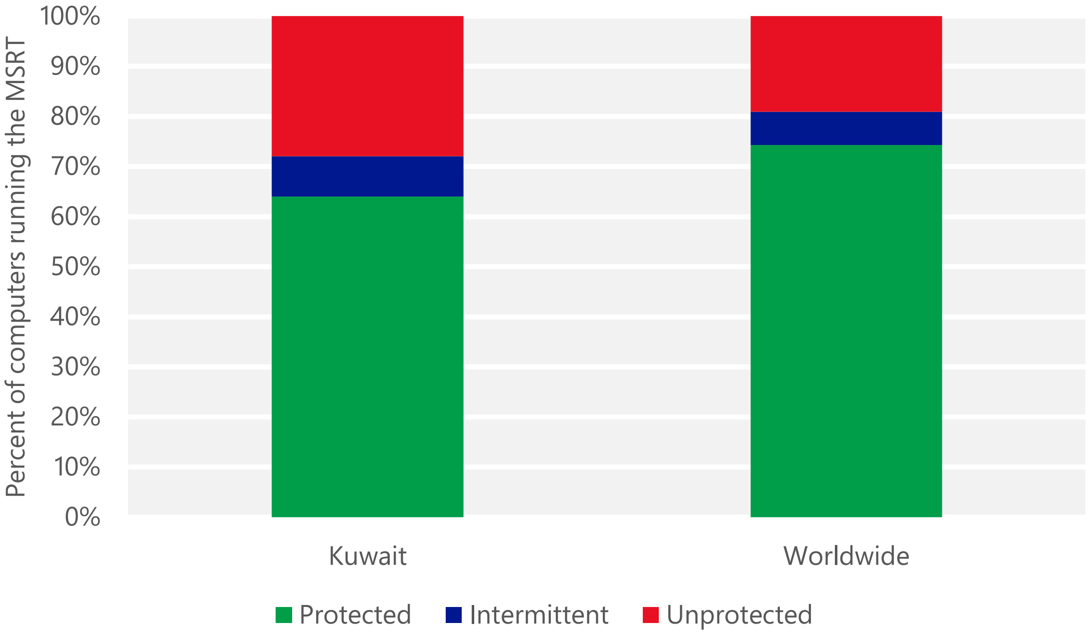
- The most common threat family infecting computers in Kuwait in 4Q14 was VBS/Jenxcus, which was detected and removed from 5.0 of every 1,000 unique computers scanned by the MSRT. VBS/Jenxcus is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Kuwait in 4Q14 was Win32/Gamarue, which was detected and removed from 3.2 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 Kuwait in 4Q14 was Win32/Sality, which was detected and removed from 2.5 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 fourth most common threat family infecting computers in Kuwait in 4Q14 was MSIL/Bladabindi, which was detected and removed from 1.3 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 Kuwait and worldwide protected by real-time security software in 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.00 drive-by download URLs for every 1,000 URLs hosted in Kuwait, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.01 drive-by download URLs for every 1,000 URLs hosted in Kuwait, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Kuwait and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Kuwait	0.00	0.01
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Latvia

The statistics presented here are generated by Microsoft security programs and services running on computers in Latvia in 4Q14 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 succeds 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

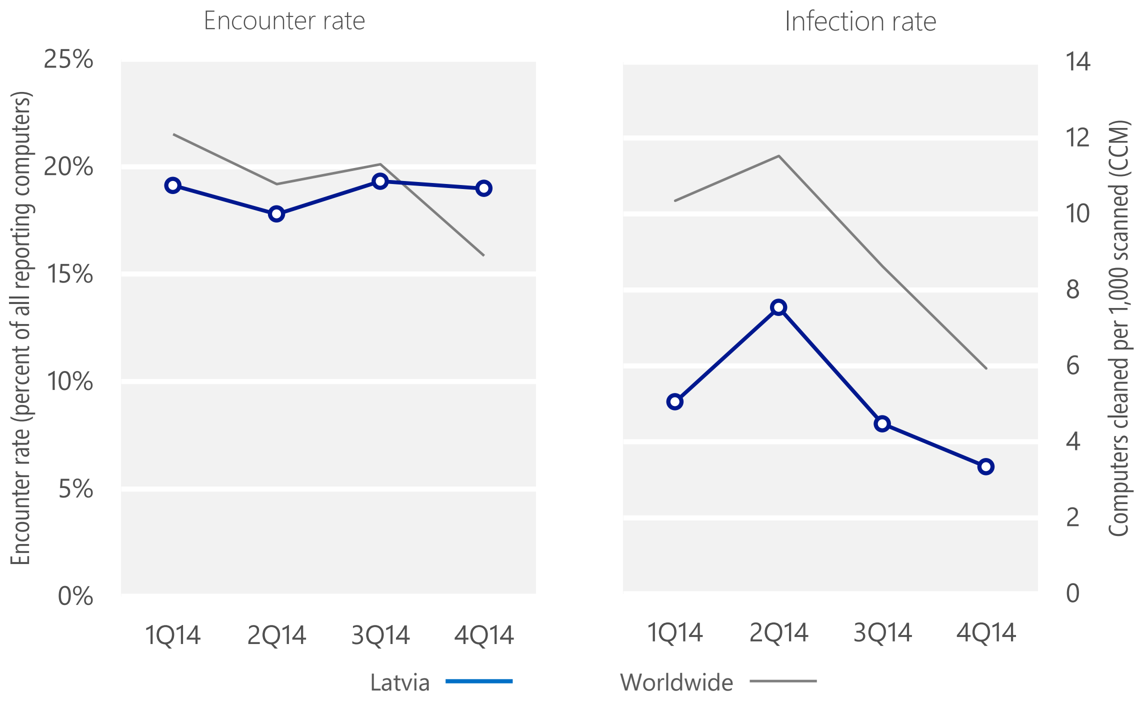
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Latvia	19.1%	17.8%	19.3%	19.0%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Latvia	5.1	7.5	4.5	3.3
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 19.0% percent of computers in Latvia encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 3.3 of every 1,000 unique computers scanned in Latvia in 4Q14 (a CCM score of 3.3, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Latvia over the last four quarters, compared to the world as a whole.

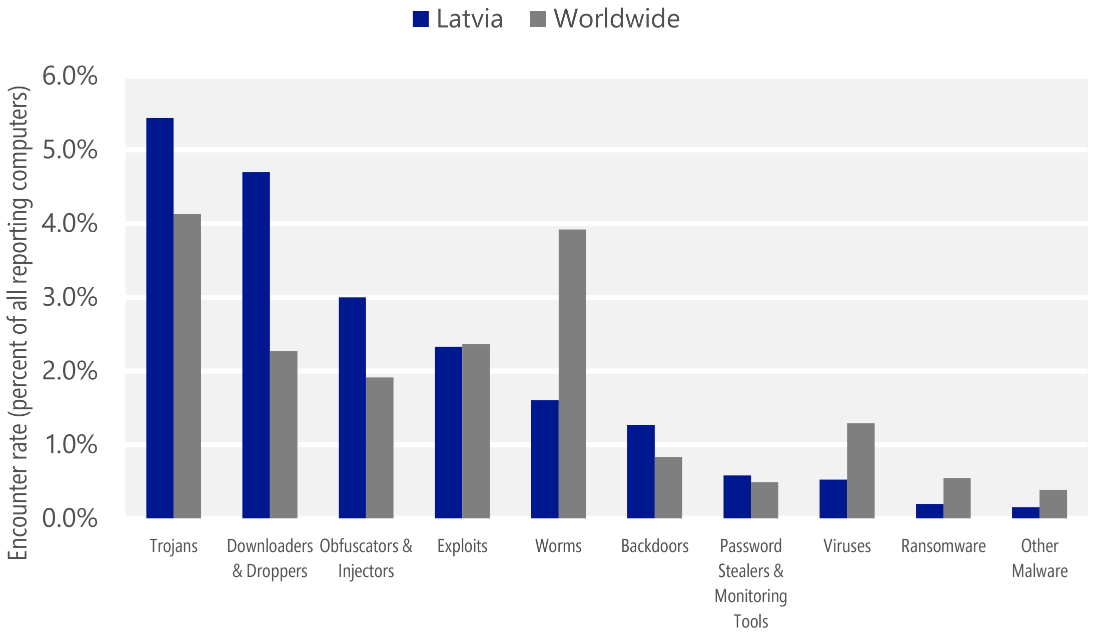
Malware encounter and infection rate trends in Latvia and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

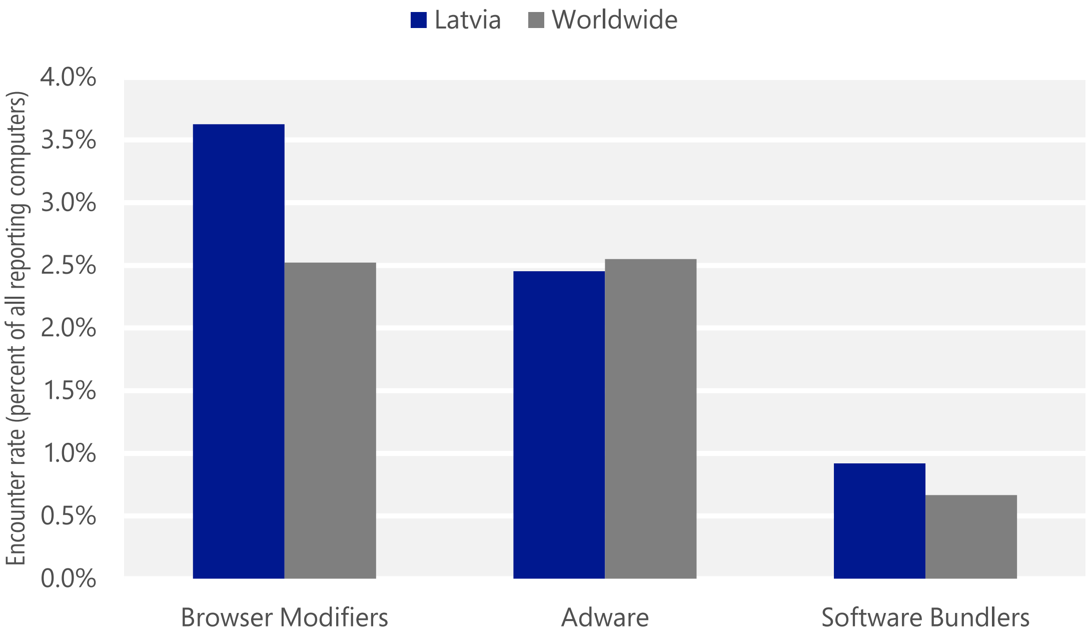
Malware encountered in Latvia in 4Q14, by category



- The most common malware category in Latvia in 4Q14 was Trojans. It was encountered by 5.4 percent of all computers there, down from 6.9 percent in 3Q14.
- The second most common malware category in Latvia in 4Q14 was Downloaders & Droppers. It was encountered by 4.7 percent of all computers there, down from 5.9 percent in 3Q14.
- The third most common malware category in Latvia in 4Q14 was Obfuscators & Injectors, which was encountered by 3.0 percent of all computers there, up from 2.6 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Latvia in 4Q14, by category



- The most common unwanted software category in Latvia in 4Q14 was Browser Modifiers. It was encountered by 3.6 percent of all computers there, down from 5.3 percent in 3Q14.
- The second most common unwanted software category in Latvia in 4Q14 was Adware. It was encountered by 2.5 percent of all computers there, up from 0.4 percent in 3Q14.
- The third most common unwanted software category in Latvia in 4Q14 was Software Bundlers, which was encountered by 0.9 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Latvia in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Ogimant	Downloaders & Droppers	3.8%
2	Win32/Obfuscator	Obfuscators & Injectors	2.2%
3	Win32/Anogre	Exploits	1.4%
4	Win32/Peaac	Trojans	1.0%
5	JS/Axpergle	Exploits	0.6%
6	Win32/Dynamer	Trojans	0.6%
7	INF/Autorun	Obfuscators & Injectors	0.5%
8	Win32/Conficker	Worms	0.4%

- The most common malware family encountered in Latvia in 4Q14 was Win32/Ogimant, which was encountered by 3.8 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 second most common malware family encountered in Latvia in 4Q14 was Win32/Obfuscator, which was encountered by 2.2 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 Latvia in 4Q14 was Win32/Anogre, which was encountered by 1.4 percent of reporting computers there. Win32/Anogre is a threat that exploits a vulnerability addressed by Microsoft Security Bulletin MS11-087. This vulnerability can allow a hacker to install programs, view, change, or delete data or create new accounts with full administrative privileges.
- The fourth most common malware family encountered in Latvia in 4Q14 was Win32/Peaac, which was encountered by 1.0 percent of reporting computers there. Win32/Peaac 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 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	2.1%
2	Win32/Defaulttab	Browser Modifiers	1.7%
3	Win32/BetterSurf	Adware	1.3%
4	Win32/Costmin	Adware	1.0%
5	Win32/Gofileexpress	Software Bundlers	0.7%

- The most common unwanted software family encountered in Latvia in 4Q14 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 second most common unwanted software family encountered in Latvia in 4Q14 was Win32/Defaulttab, which was encountered by 1.7 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.
- The third most common unwanted software family encountered in Latvia in 4Q14 was Win32/BetterSurf, which was encountered by 1.3 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.

Top threat families by infection rate

The most common malware families by infection rate in Latvia in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Gamarue	Worms	0.3
2	Win32/Brontok	Worms	0.3
3	Win32/Tofsee	Backdoors	0.2
4	Win32/Ramnit	Trojans	0.2
5	Win32/Sality	Viruses	0.2
6	MSIL/Bladabindi	Backdoors	0.2
7	Win32/Sefnit	Trojans	0.2
8	JS/Kilim	Trojans	0.2
9	Win32/Alureon	Trojans	0.1
10	Win32/Zbot	Password Stealers & Monitoring Tools	0.1

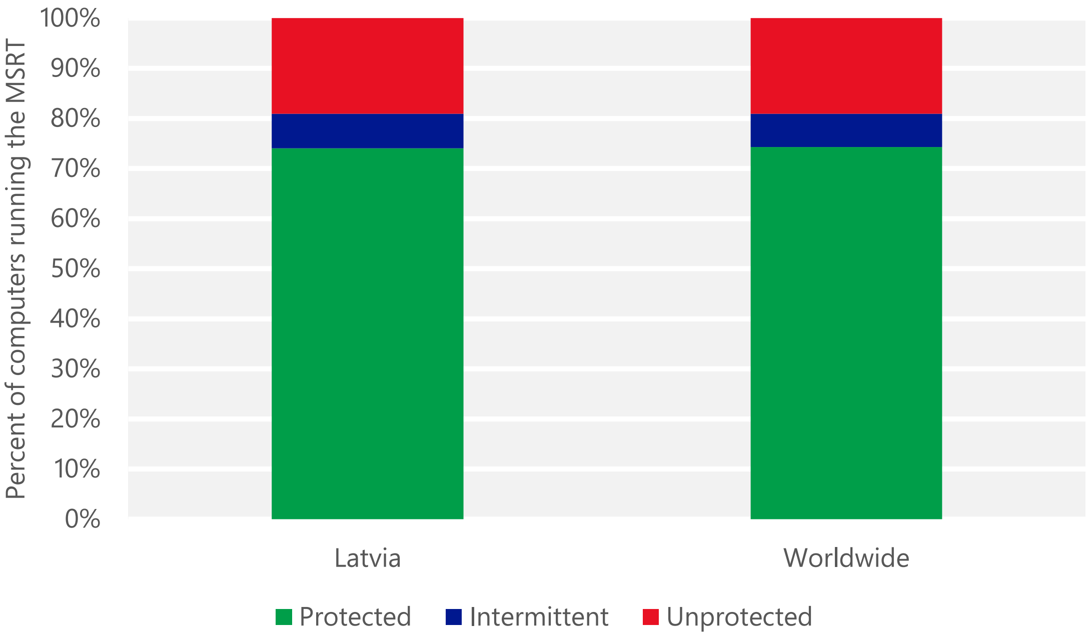
- The most common threat family infecting computers in Latvia in 4Q14 was Win32/Gamarue, which was detected and removed from 0.3 of every 1,000 unique computers scanned by the MSRT. Win32/Gamarue is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The second most common threat family infecting computers in Latvia in 4Q14 was Win32/Brontok, which was detected and removed from 0.3 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 Latvia in 4Q14 was Win32/Tofsee, which was detected and removed from 0.2 of every 1,000 unique computers scanned by the MSRT. Win32/Tofsee is a multi-component family of backdoor trojans that act as a spam and traffic relay.
- The fourth most common threat family infecting computers in Latvia in 4Q14 was Win32/Ramnit, which was detected and removed from 0.2 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 Latvia and worldwide protected by real-time security software in 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.34 drive-by download URLs for every 1,000 URLs hosted in Latvia, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.25 drive-by download URLs for every 1,000 URLs hosted in Latvia, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Latvia and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Latvia	0.34	0.25
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Lebanon

The statistics presented here are generated by Microsoft security programs and services running on computers in Lebanon in 4Q14 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 succeds 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

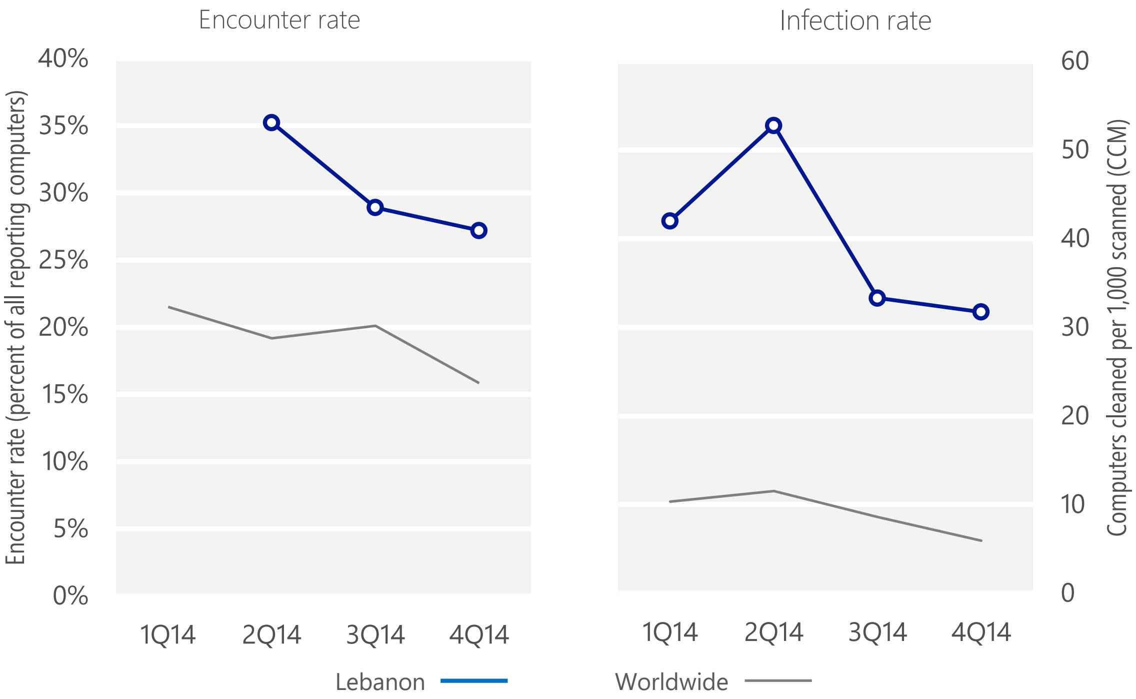
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Lebanon	N/A	35.2%	28.9%	27.2%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Lebanon	42.0	52.8	33.3	31.7
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 27.2% percent of computers in Lebanon encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 31.7 of every 1,000 unique computers scanned in Lebanon in 4Q14 (a CCM score of 31.7, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Lebanon over the last four quarters, compared to the world as a whole.

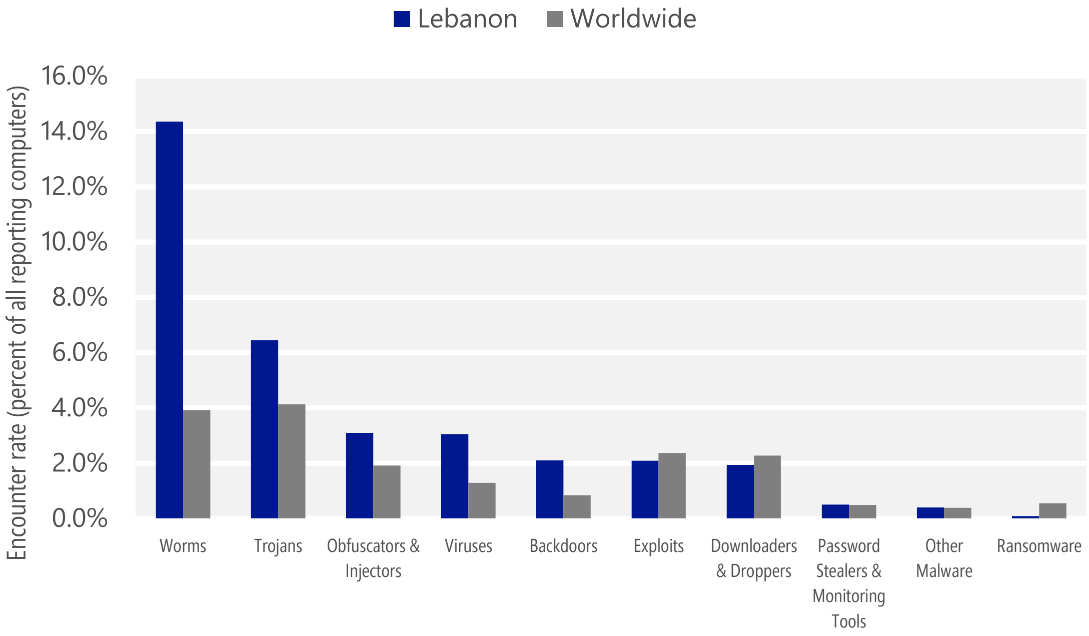
Malware encounter and infection rate trends in Lebanon and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

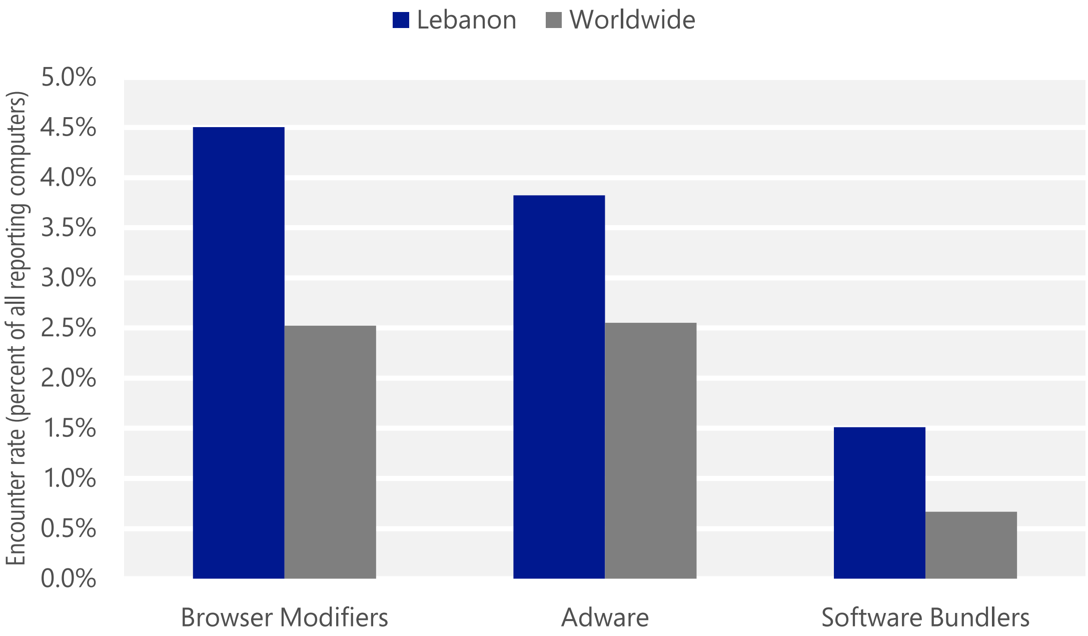
Malware encountered in Lebanon in 4Q14, by category



- The most common malware category in Lebanon in 4Q14 was Worms. It was encountered by 14.4 percent of all computers there, up from 12.3 percent in 3Q14.
- The second most common malware category in Lebanon in 4Q14 was Trojans. It was encountered by 6.4 percent of all computers there, down from 12.1 percent in 3Q14.
- The third most common malware category in Lebanon in 4Q14 was Obfuscators & Injectors, which was encountered by 3.1 percent of all computers there, up from 3.0 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Lebanon in 4Q14, by category



- The most common unwanted software category in Lebanon in 4Q14 was Browser Modifiers. It was encountered by 4.5 percent of all computers there, down from 6.1 percent in 3Q14.
- The second most common unwanted software category in Lebanon in 4Q14 was Adware. It was encountered by 3.8 percent of all computers there, up from 0.7 percent in 3Q14.
- The third most common unwanted software category in Lebanon in 4Q14 was Software Bundlers, which was encountered by 1.5 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Lebanon in 4Q14

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	6.7%
2	Win32/Gamarue	Worms	5.4%
3	INF/Autorun	Obfuscators & Injectors	3.0%
4	Win32/Sality	Viruses	1.7%
5	Win32/Nuqel	Worms	1.6%
6	Win32/Folstart	Worms	1.5%
7	Win32/CplLnk	Exploits	1.4%
8	Win32/Ramnit	Trojans	1.3%
9	Win32/Obfuscator	Obfuscators & Injectors	1.0%

- The most common malware family encountered in Lebanon in 4Q14 was VBS/Jenxcus, which was encountered by 6.7 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 Lebanon in 4Q14 was Win32/Gamarue, which was encountered by 5.4 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 Lebanon in 4Q14 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 Lebanon in 4Q14 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 Lebanon in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	3.0%
2	Win32/Defaulttab	Browser Modifiers	1.6%
3	Win32/BetterSurf	Adware	1.4%
4	Win32/Gofileexpress	Software Bundlers	1.2%
5	Win32/Brya	Adware	1.1%

- The most common unwanted software family encountered in Lebanon in 4Q14 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 second most common unwanted software family encountered in Lebanon in 4Q14 was Win32/Defaulttab, which was encountered by 1.6 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.

- The third most common unwanted software family encountered in Lebanon in 4Q14 was Win32/BetterSurf, which was encountered by 1.4 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.

Top threat families by infection rate

The most common malware families by infection rate in Lebanon in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	10.2
2	Win32/Gamarue	Worms	8.2
3	Win32/Sality	Viruses	3.9
4	Win32/Folstart	Worms	3.7
5	Win32/Nuqel	Worms	2.3
6	Win32/Brontok	Worms	1.6
7	Win32/Ramnit	Trojans	1.2
8	MSIL/Bladabindi	Backdoors	1.1
9	Win32/Dorkbot	Worms	0.8
10	Win32/Vobfus	Worms	0.6

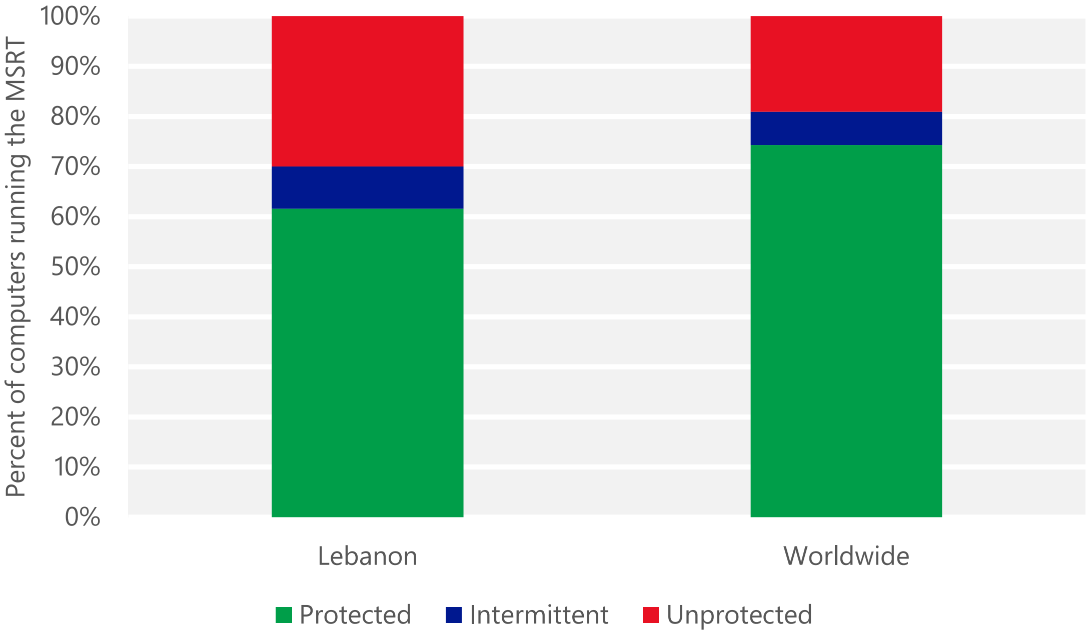
- The most common threat family infecting computers in Lebanon in 4Q14 was VBS/Jenxcus, which was detected and removed from 10.2 of every 1,000 unique computers scanned by the MSRT. VBS/Jenxcus is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Lebanon in 4Q14 was Win32/Gamarue, which was detected and removed from 8.2 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 4Q14 was Win32/Sality, which was detected and removed from 3.9 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 Lebanon in 4Q14 was Win32/Folstart, which was detected and removed from 3.7 of every 1,000 unique computers scanned by the MSRT. Win32/Folstart is a worm that spreads through removable drives and modifies some system settings.

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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.01 drive-by download URLs for every 1,000 URLs hosted in Lebanon, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.00 drive-by download URLs for every 1,000 URLs hosted in Lebanon, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Lebanon and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Lebanon	0.01	0.00
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Lithuania

The statistics presented here are generated by Microsoft security programs and services running on computers in Lithuania in 4Q14 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 succeds 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

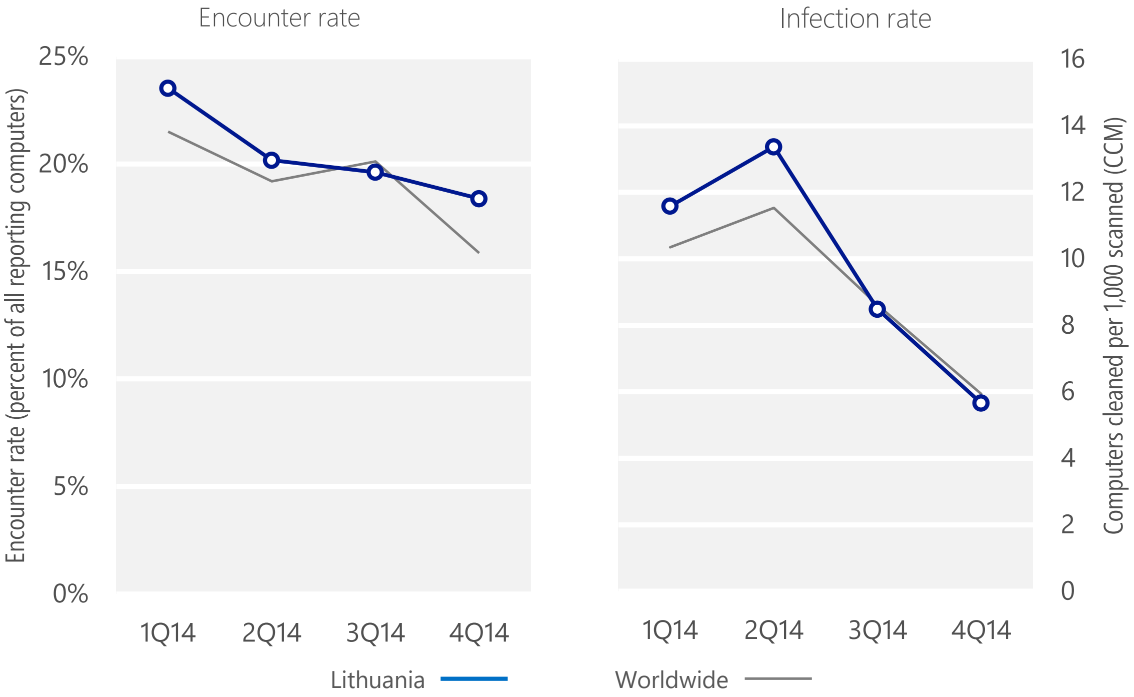
Metric	**1Q14**	**2Q14**	**3Q14**	**4Q14**
Encounter rate, Lithuania	23.5%	20.2%	19.6%	18.4%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Lithuania	11.6	13.4	8.5	5.7
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 18.4% percent of computers in Lithuania encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 5.7 of every 1,000 unique computers scanned in Lithuania in 4Q14 (a CCM score of 5.7, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Lithuania over the last four quarters, compared to the world as a whole.

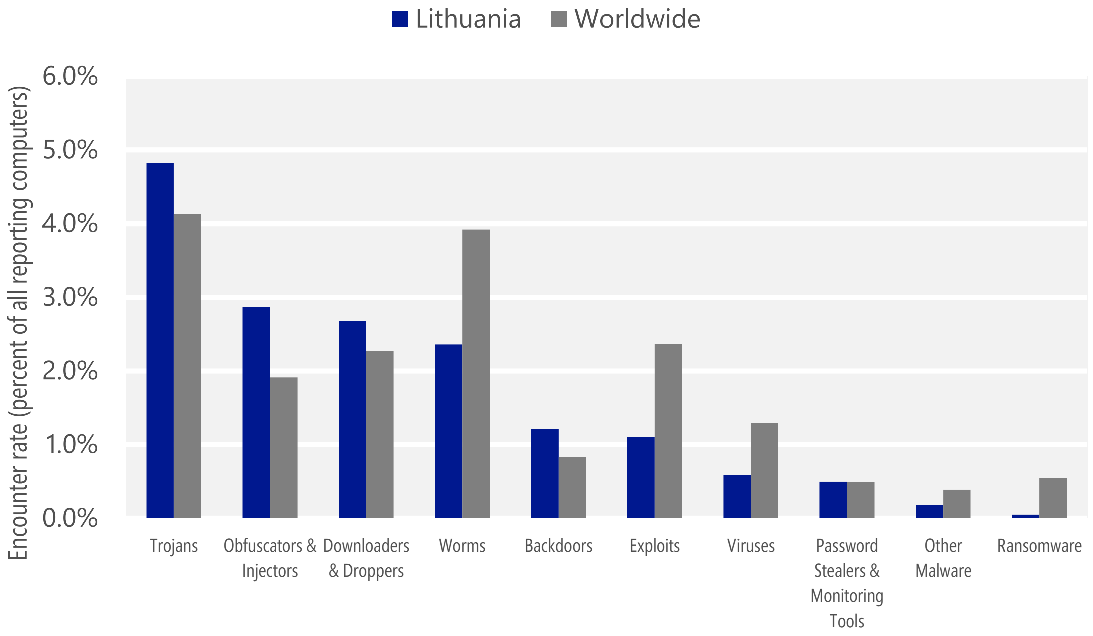
Malware encounter and infection rate trends in Lithuania and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

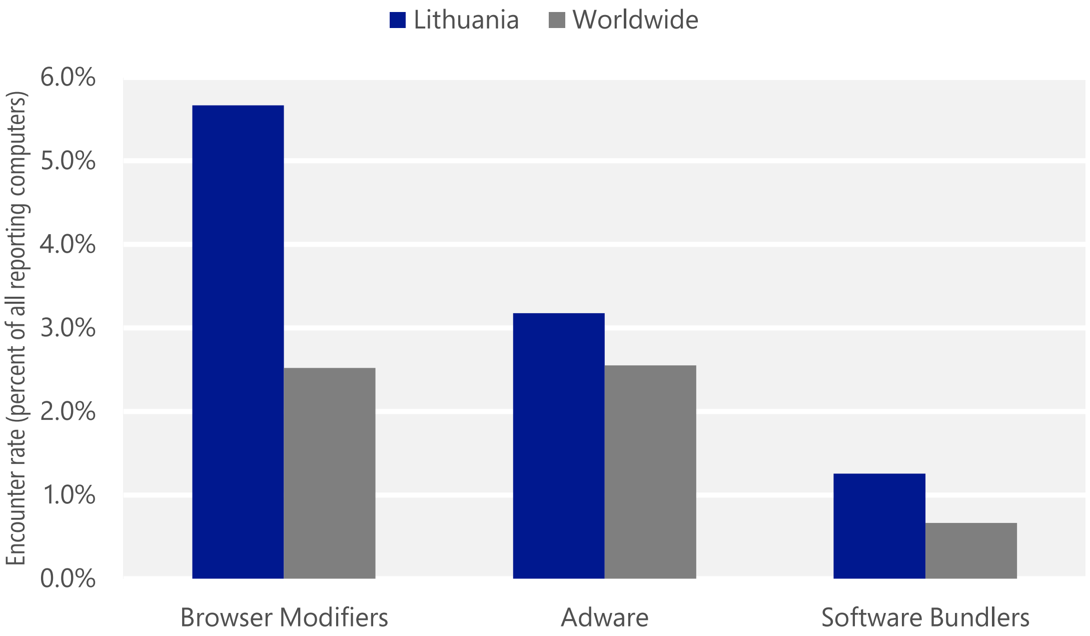
Malware encountered in Lithuania in 4Q14, by category



- The most common malware category in Lithuania in 4Q14 was Trojans. It was encountered by 4.8 percent of all computers there, down from 6.9 percent in 3Q14.
- The second most common malware category in Lithuania in 4Q14 was Obfuscators & Injectors. It was encountered by 2.9 percent of all computers there, down from 4.7 percent in 3Q14.
- The third most common malware category in Lithuania in 4Q14 was Downloaders & Droppers, which was encountered by 2.7 percent of all computers there, down from 2.8 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Lithuania in 4Q14, by category



- The most common unwanted software category in Lithuania in 4Q14 was Browser Modifiers. It was encountered by 5.7 percent of all computers there, down from 6.7 percent in 3Q14.
- The second most common unwanted software category in Lithuania in 4Q14 was Adware. It was encountered by 3.2 percent of all computers there, up from 0.7 percent in 3Q14.
- The third most common unwanted software category in Lithuania in 4Q14 was Software Bundlers, which was encountered by 1.3 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Lithuania in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Obfuscator	Obfuscators & Injectors	2.1%
2	Win32/Ogimant	Downloaders & Droppers	1.6%
3	INF/Autorun	Obfuscators & Injectors	0.6%
4	Win32/Dynamer	Trojans	0.5%
5	Win32/Brontok	Worms	0.5%
6	JS/Axpergle	Exploits	0.5%
7	Win32/Peaac	Trojans	0.5%
8	Win32/Gamarue	Worms	0.4%
9	Win32/Killav	Trojans	0.4%
10	Win32/Conficker	Worms	0.4%

- The most common malware family encountered in Lithuania in 4Q14 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 Lithuania in 4Q14 was Win32/Ogimant, which was encountered by 1.6 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 third most common malware family encountered in Lithuania in 4Q14 was INF/Autorun, which was encountered by 0.6 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 Lithuania in 4Q14 was Win32/Dynamer, which was encountered by 0.5 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 Lithuania in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	4.1%
2	Win32/Defaulttab	Browser Modifiers	1.8%
3	Win32/BetterSurf	Adware	1.7%
4	Win32/Costmin	Adware	1.3%
5	Win32/Gofileexpress	Software Bundlers	1.0%

- The most common unwanted software family encountered in Lithuania in 4Q14 was Win32/Couponruc, which was encountered by 4.1 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 Lithuania in 4Q14 was Win32/Defaulttab, which was encountered by 1.8 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.
- The third most common unwanted software family encountered in Lithuania in 4Q14 was Win32/BetterSurf, which was encountered by 1.7 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.

Top threat families by infection rate

The most common malware families by infection rate in Lithuania in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Brontok	Worms	0.8
2	JS/Kilim	Trojans	0.7
3	Win32/Sality	Viruses	0.7
4	VBS/Jenxcus	Worms	0.5
5	Win32/Gamarue	Worms	0.4
6	Win32/Sefnit	Trojans	0.3
7	MSIL/Bladabindi	Backdoors	0.3
8	Win32/Jeefo	Viruses	0.2
9	Win32/Alureon	Trojans	0.2
10	Win32/Ramnit	Trojans	0.2

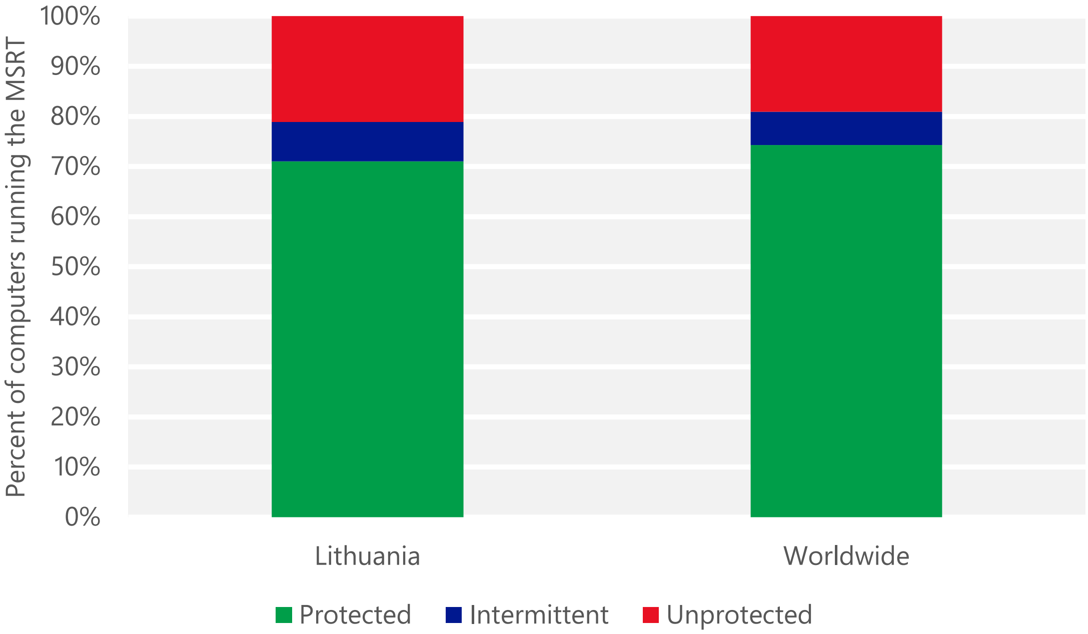
- The most common threat family infecting computers in Lithuania in 4Q14 was Win32/Brontok, which was detected and removed from 0.8 of every 1,000 unique computers scanned by the MSRT. Win32/Brontok is a mass-mailing email worm that spreads by sending copies of itself as email attachments to addresses 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 second most common threat family infecting computers in Lithuania in 4Q14 was JS/Kilim, which was detected and removed from 0.7 of every 1,000 unique computers scanned by the MSRT. JS/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 4Q14 was Win32/Sality, which was detected and removed from 0.7 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 Lithuania in 4Q14 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 Lithuania and worldwide protected by real-time security software in 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.16 drive-by download URLs for every 1,000 URLs hosted in Lithuania, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.13 drive-by download URLs for every 1,000 URLs hosted in Lithuania, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Lithuania and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Lithuania	0.16	0.13
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Luxembourg

The statistics presented here are generated by Microsoft security programs and services running on computers in Luxembourg in 4Q14 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 succeds 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

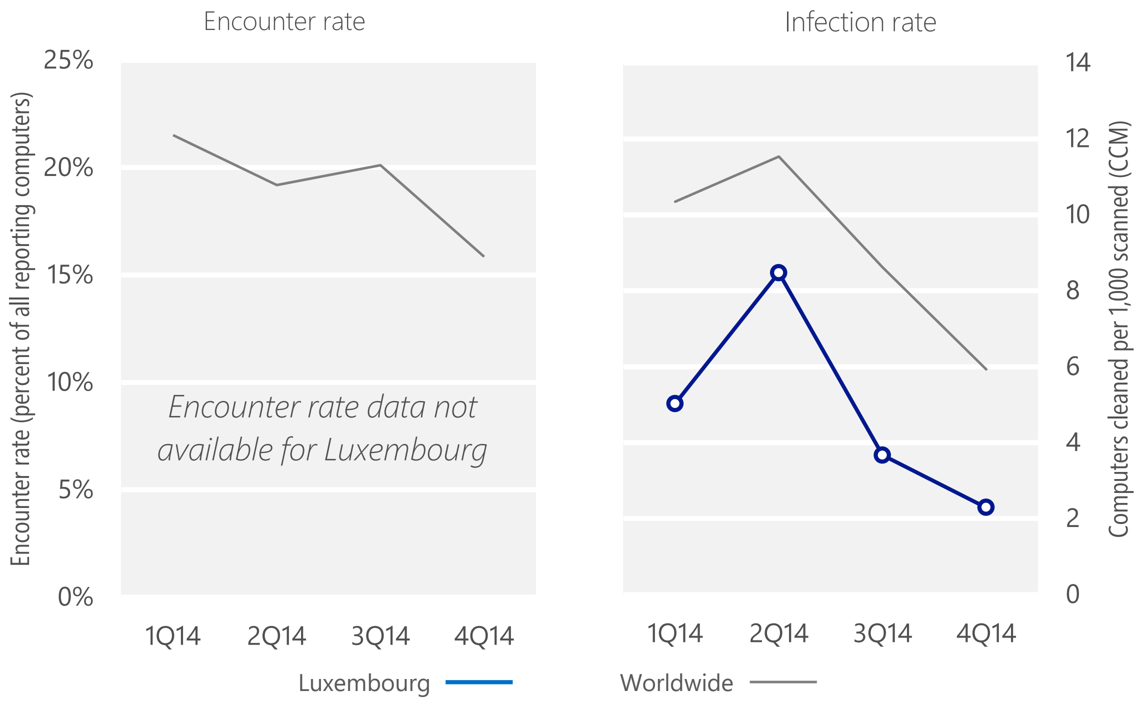
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Luxembourg	N/A	N/A	N/A	N/A
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Luxembourg	5.0	8.5	3.7	2.3
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, the MSRT detected and removed malware from 2.3 of every 1,000 unique computers scanned in Luxembourg in 4Q14 (a CCM score of 2.3, compared to the 4Q14 worldwide CCM of 5.9). 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 18* 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 4Q14

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	0.4
2	Win32/Sefnit	Trojans	0.3
3	Win32/Gamarue	Worms	0.2
4	MSIL/Bladabindi	Backdoors	0.1
5	Win32/Zbot	Password Stealers & Monitoring Tools	0.1
6	Win32/Ramnit	Trojans	0.1
7	Win32/Brontok	Worms	0.1
8	Win32/Sality	Viruses	0.1
9	Win32/Alureon	Trojans	0.1
10	Win32/Conficker	Worms	0.1

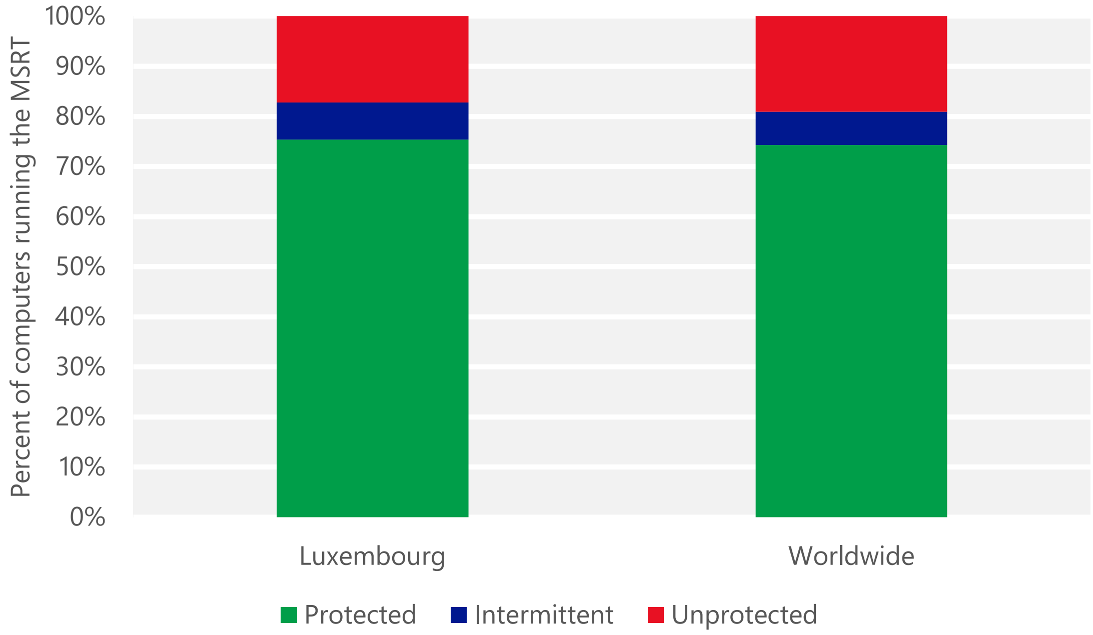
- The most common threat family infecting computers in Luxembourg in 4Q14 was VBS/Jenxcus, which was detected and removed from 0.4 of every 1,000 unique computers scanned by the MSRT. VBS/Jenxcus is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Luxembourg in 4Q14 was Win32/Sefnit, which was detected and removed from 0.3 of every 1,000 unique computers scanned by the MSRT. Win32/Sefnit is a family of trojans that can allow backdoor access, download files, and use the computer and Internet connection for click fraud. Some variants can monitor web browsers and hijack search results.
- The third most common threat family infecting computers in Luxembourg in 4Q14 was Win32/Gamarue, which was detected and removed from 0.2 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 Luxembourg in 4Q14 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 Luxembourg and worldwide protected by real-time security software in 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.47 drive-by download URLs for every 1,000 URLs hosted in Luxembourg, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.44 drive-by download URLs for every 1,000 URLs hosted in Luxembourg, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Luxembourg and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Luxembourg	0.47	0.44
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

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 4Q14 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 succeds 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.

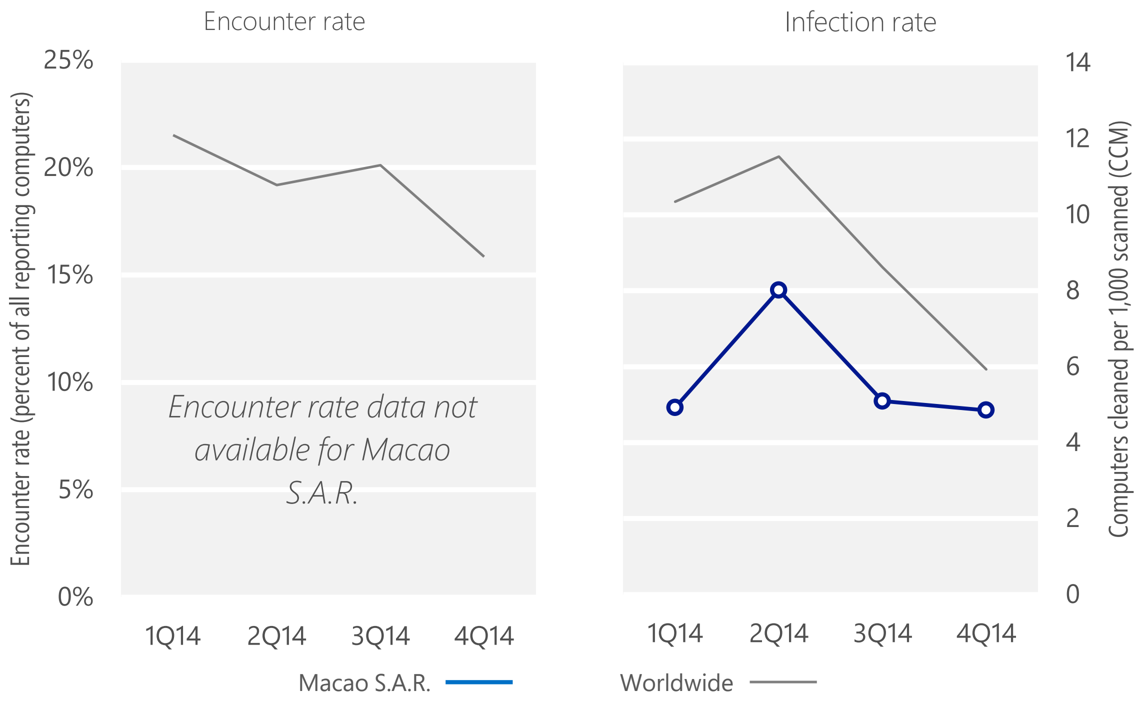
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Macao S.A.R.	N/A	N/A	N/A	N/A
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Macao S.A.R.	4.9	8.0	5.1	4.9
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, the MSRT detected and removed malware from 4.9 of every 1,000 unique computers scanned in Macao S.A.R. in 4Q14 (a CCM score of 4.9, compared to the 4Q14 worldwide CCM of 5.9). 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 18* 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 4Q14

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	1.0
2	Win32/Ramnit	Trojans	0.9
3	Win32/Gamarue	Worms	0.8
4	Win32/Necurs	Trojans	0.3
5	Win32/Sality	Viruses	0.3
6	Win32/Nitol	Other Malware	0.2
7	Win32/Conficker	Worms	0.2
8	Win32/Brontok	Worms	0.2
9	Win32/Sefnit	Trojans	0.1
10	Win32/Zbot	Password Stealers & Monitoring Tools	0.1

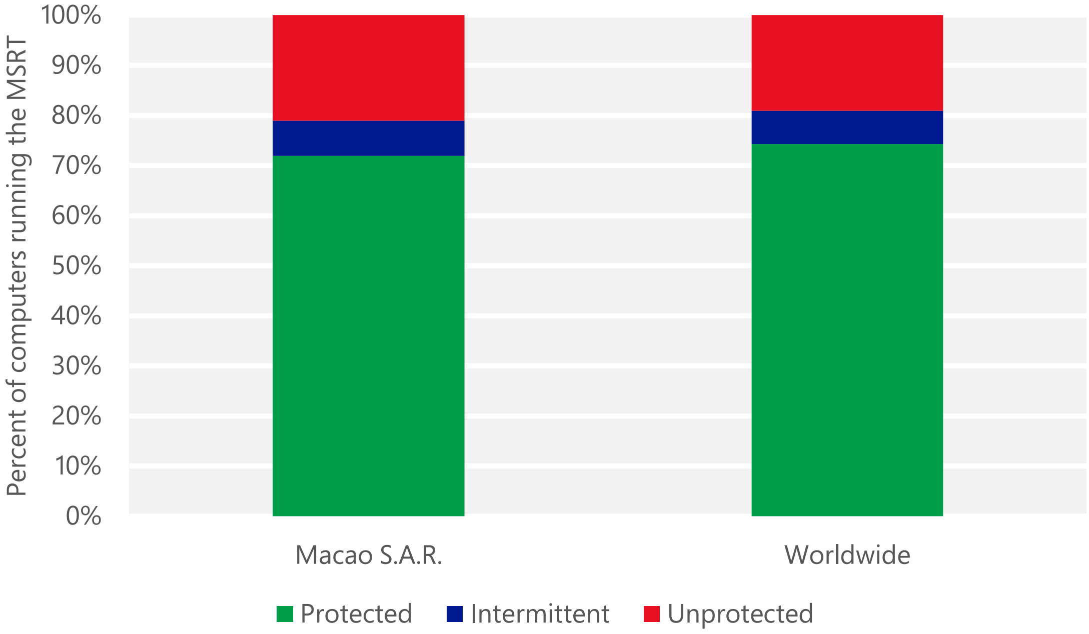
- The most common threat family infecting computers in Macao S.A.R. in 4Q14 was VBS/Jenxcus, which was detected and removed from 1.0 of every 1,000 unique computers scanned by the MSRT. VBS/Jenxcus is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Macao S.A.R. in 4Q14 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 third most common threat family infecting computers in Macao S.A.R. in 4Q14 was Win32/Gamarue, which was detected and removed from 0.8 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 Macao S.A.R. in 4Q14 was Win32/Necurs, which was detected and removed from 0.3 of every 1,000 unique computers scanned by the MSRT. Win32/Necurs is a family of malware that downloads additional malware,?including variants from the Win32/Sirefef and Win32/Medfos families,?and?enables backdoor access and control of 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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.04 drive-by download URLs for every 1,000 URLs hosted in Macao S.A.R., compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.10 drive-by download URLs for every 1,000 URLs hosted in Macao S.A.R., compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Macao S.A.R. and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Macao S.A.R.	0.04	0.10
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Malaysia

The statistics presented here are generated by Microsoft security programs and services running on computers in Malaysia in 4Q14 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 succeds 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

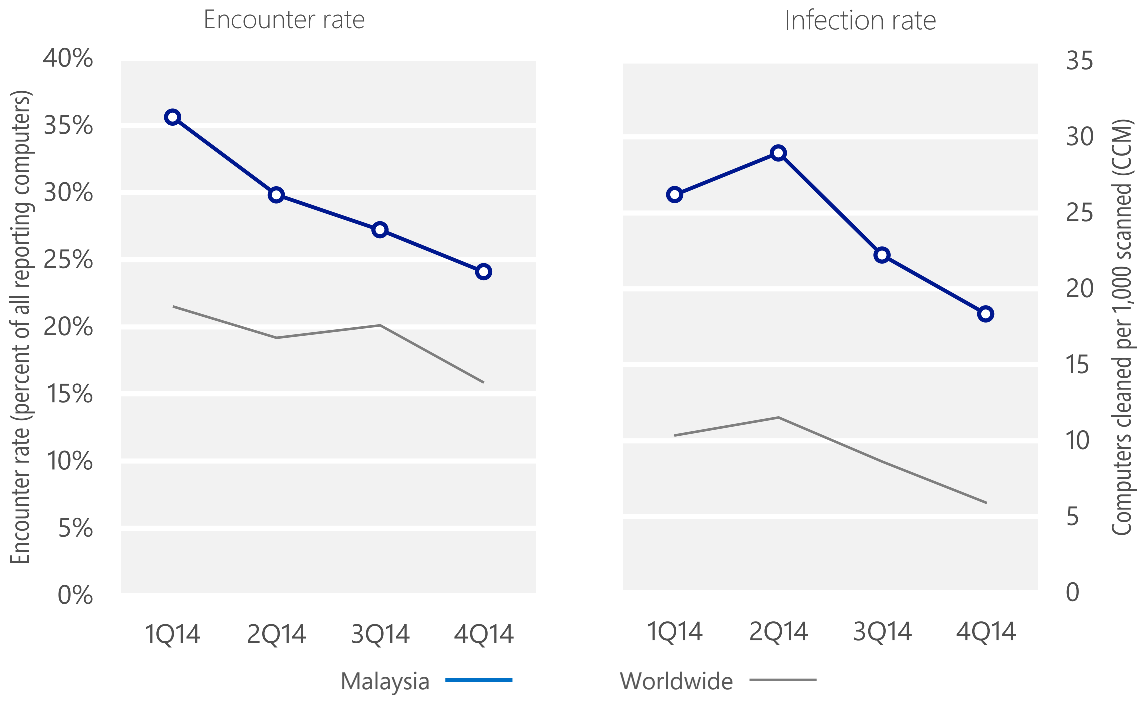
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Malaysia	35.6%	29.8%	27.2%	24.1%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Malaysia	26.2	29.0	22.2	18.4
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 24.1% percent of computers in Malaysia encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 18.4 of every 1,000 unique computers scanned in Malaysia in 4Q14 (a CCM score of 18.4, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Malaysia over the last four quarters, compared to the world as a whole.

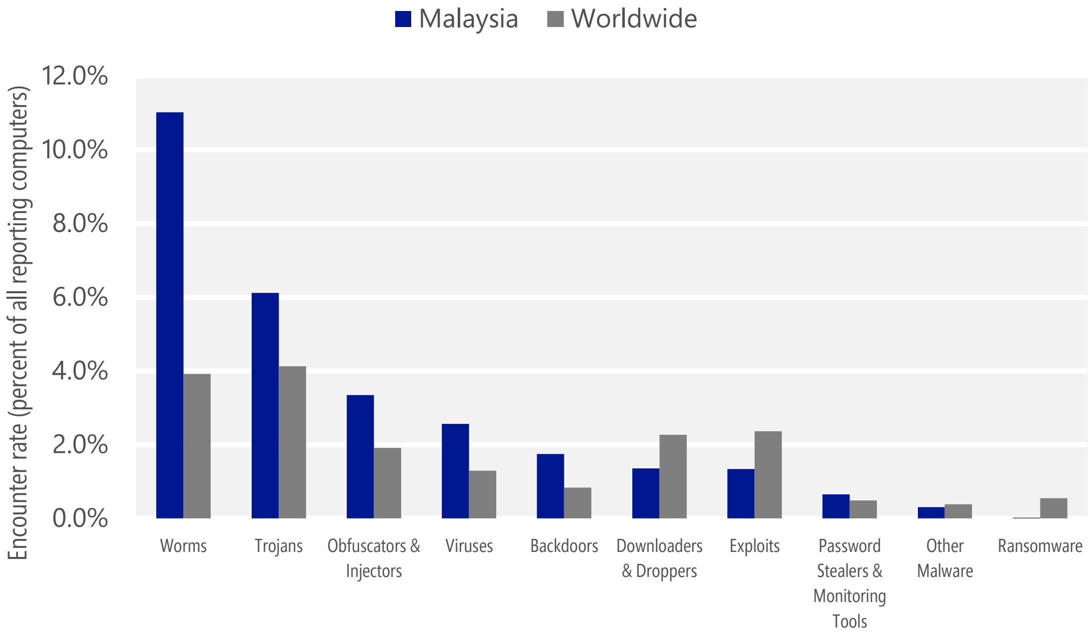
Malware encounter and infection rate trends in Malaysia and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

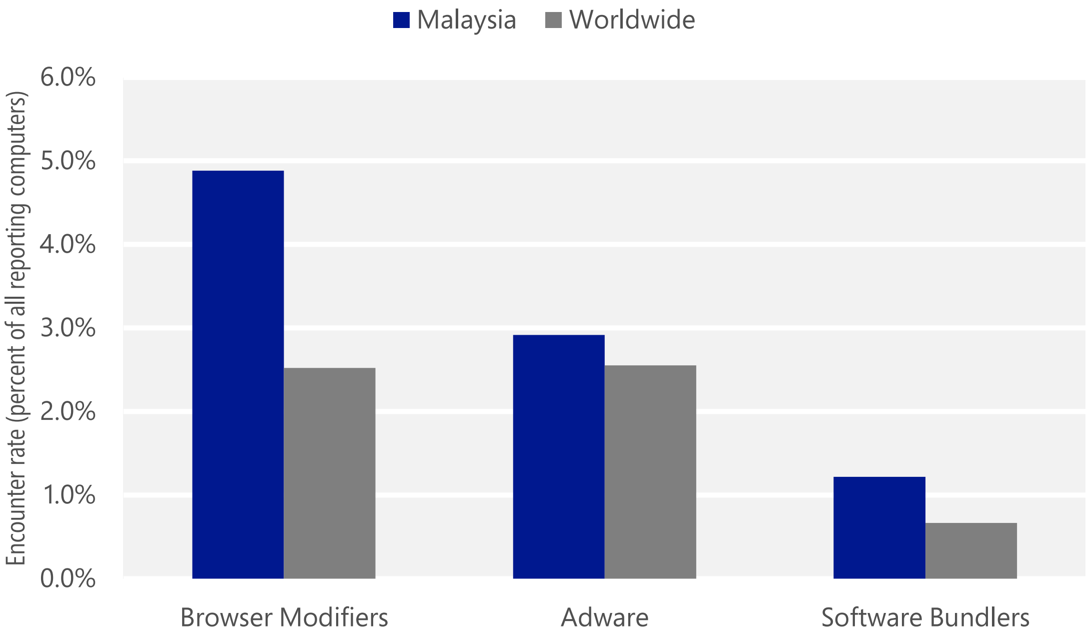
Malware encountered in Malaysia in 4Q14, by category



- The most common malware category in Malaysia in 4Q14 was Worms. It was encountered by 11.0 percent of all computers there, down from 13.1 percent in 3Q14.
- The second most common malware category in Malaysia in 4Q14 was Trojans. It was encountered by 6.1 percent of all computers there, down from 8.4 percent in 3Q14.
- The third most common malware category in Malaysia in 4Q14 was Obfuscators & Injectors, which was encountered by 3.3 percent of all computers there, down from 3.5 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Malaysia in 4Q14, by category



- The most common unwanted software category in Malaysia in 4Q14 was Browser Modifiers. It was encountered by 4.9 percent of all computers there, down from 6.4 percent in 3Q14.
- The second most common unwanted software category in Malaysia in 4Q14 was Adware. It was encountered by 2.9 percent of all computers there, up from 0.8 percent in 3Q14.
- The third most common unwanted software category in Malaysia in 4Q14 was Software Bundlers, which was encountered by 1.2 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Malaysia in 4Q14

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	5.0%
2	Win32/Gamarue	Worms	2.9%
3	INF/Autorun	Obfuscators & Injectors	2.2%
4	JS/Faceliker	Trojans	1.9%
5	Win32/Obfuscator	Obfuscators & Injectors	1.4%
6	Win32/Sality	Viruses	1.3%
7	Win32/Dorkbot	Worms	1.3%
8	Win32/Ramnit	Trojans	1.1%
9	Win32/Vermis	Worms	1.0%
10	Win32/Conficker	Worms	0.9%

- The most common malware family encountered in Malaysia in 4Q14 was VBS/Jenxcus, which was encountered by 5.0 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 Malaysia in 4Q14 was Win32/Gamarue, which was encountered by 2.9 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 Malaysia in 4Q14 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.
- The fourth most common malware family encountered in Malaysia in 4Q14 was JS/Faceliker, which was encountered by 1.9 percent of reporting computers there. JS/Faceliker is a malicious script that ?likes? content on Facebook without the user’s knowledge or consent.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Malaysia in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	3.4%
2	Win32/Defaulttab	Browser Modifiers	1.6%
3	Win32/Costmin	Adware	1.4%
4	Win32/BetterSurf	Adware	1.1%
5	Win32/Gofileexpress	Software Bundlers	0.9%

- The most common unwanted software family encountered in Malaysia in 4Q14 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 Malaysia in 4Q14 was Win32/Defaulttab, which was encountered by 1.6 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.

- The third most common unwanted software family encountered in Malaysia in 4Q14 was Win32/Costmin, which was encountered by 1.4 percent of reporting computers there. Win32/Costmin is an adware family that installs itself as a browser extension for Internet Explorer, Mozilla Firefox, and Google Chrome, and displays advertisements as the user browses the Internet.

Top threat families by infection rate

The most common malware families by infection rate in Malaysia in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	6.5
2	Win32/Gamarue	Worms	2.9
3	Win32/Sality	Viruses	2.8
4	Win32/Ramnit	Trojans	1.6
5	Win32/Dorkbot	Worms	1.0
6	Win32/Sefnit	Trojans	0.5
7	Win32/Lethic	Trojans	0.5
8	Win32/Pramro	Trojans	0.4
9	Win32/Brontok	Worms	0.4
10	Win32/Conficker	Worms	0.3

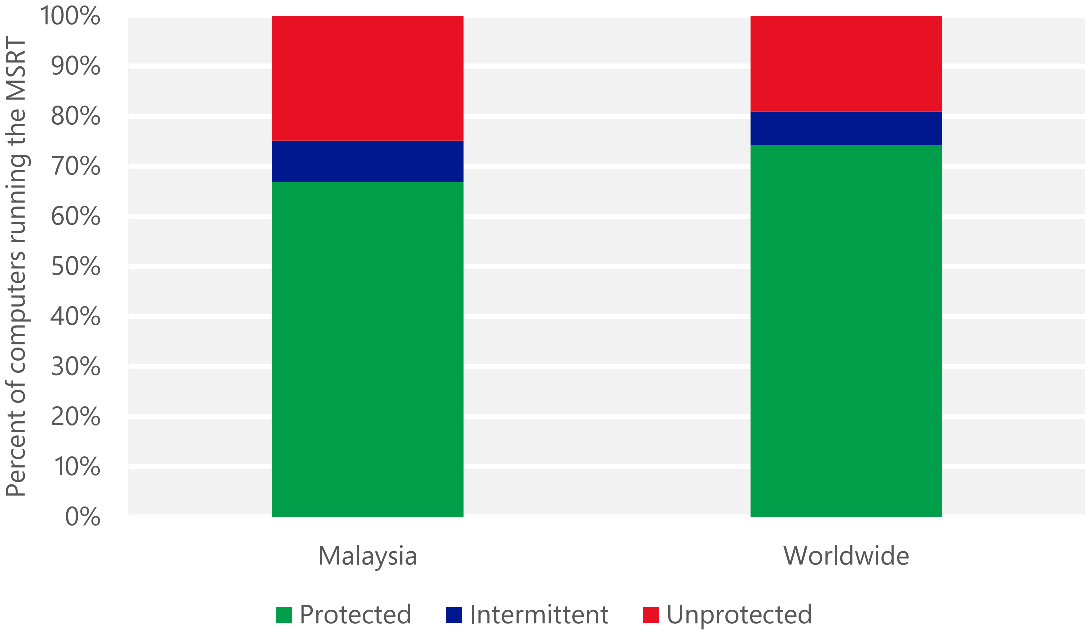
- The most common threat family infecting computers in Malaysia in 4Q14 was VBS/Jenxcus, which was detected and removed from 6.5 of every 1,000 unique computers scanned by the MSRT. VBS/Jenxcus is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Malaysia in 4Q14 was Win32/Gamarue, which was detected and removed from 2.9 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 Malaysia in 4Q14 was Win32/Sality, which was detected and removed from 2.8 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 Malaysia in 4Q14 was Win32/Ramnit, which was detected and removed from 1.6 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 Malaysia and worldwide protected by real-time security software in 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.63 drive-by download URLs for every 1,000 URLs hosted in Malaysia, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.37 drive-by download URLs for every 1,000 URLs hosted in Malaysia, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Malaysia and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Malaysia	0.63	0.37
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Malta

The statistics presented here are generated by Microsoft security programs and services running on computers in Malta in 4Q14 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 succeds 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

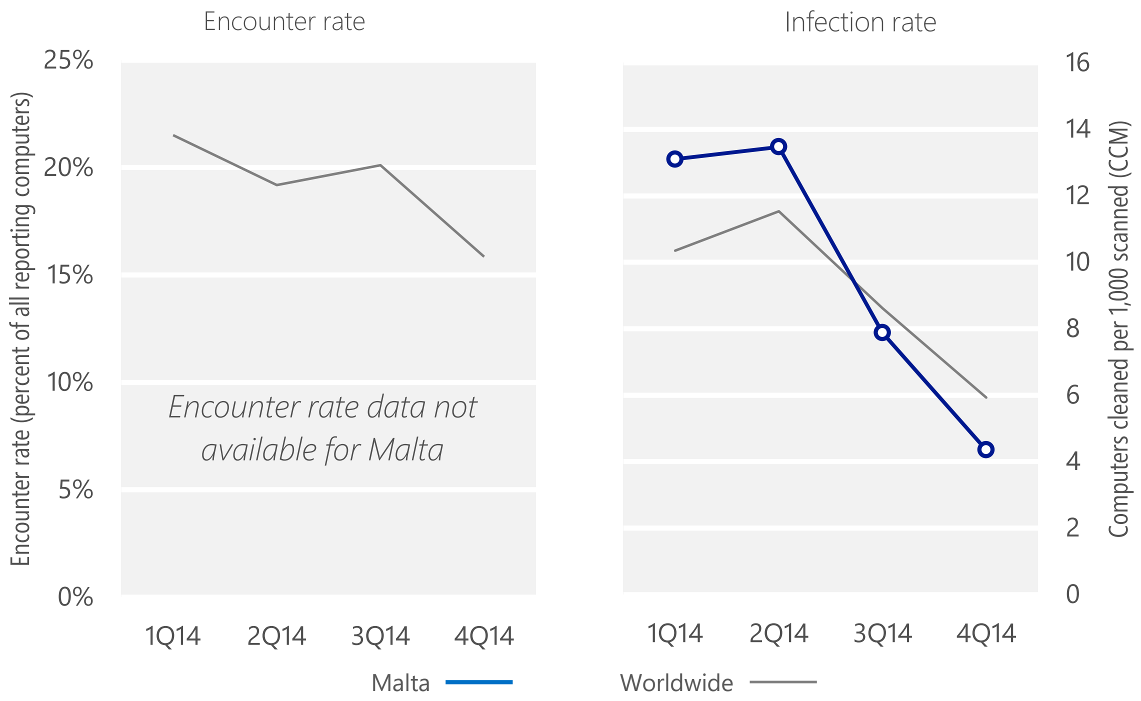
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Malta	N/A	N/A	N/A	N/A
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Malta	13.1	13.5	7.9	4.4
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, the MSRT detected and removed malware from 4.4 of every 1,000 unique computers scanned in Malta in 4Q14 (a CCM score of 4.4, compared to the 4Q14 worldwide CCM of 5.9). 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 18* 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 4Q14

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	1.7
2	Win32/Sefnit	Trojans	0.3
3	MSIL/Bladabindi	Backdoors	0.2
4	Win32/Zbot	Password Stealers & Monitoring Tools	0.2
5	Win32/Sality	Viruses	0.2
6	Win32/Alureon	Trojans	0.2
7	JS/Miuref	Trojans	0.1
8	JS/Kilim	Trojans	0.1
9	Win32/Wysotot	Trojans	0.1
10	Win32/Lecpetex	Downloaders & Droppers	0.1

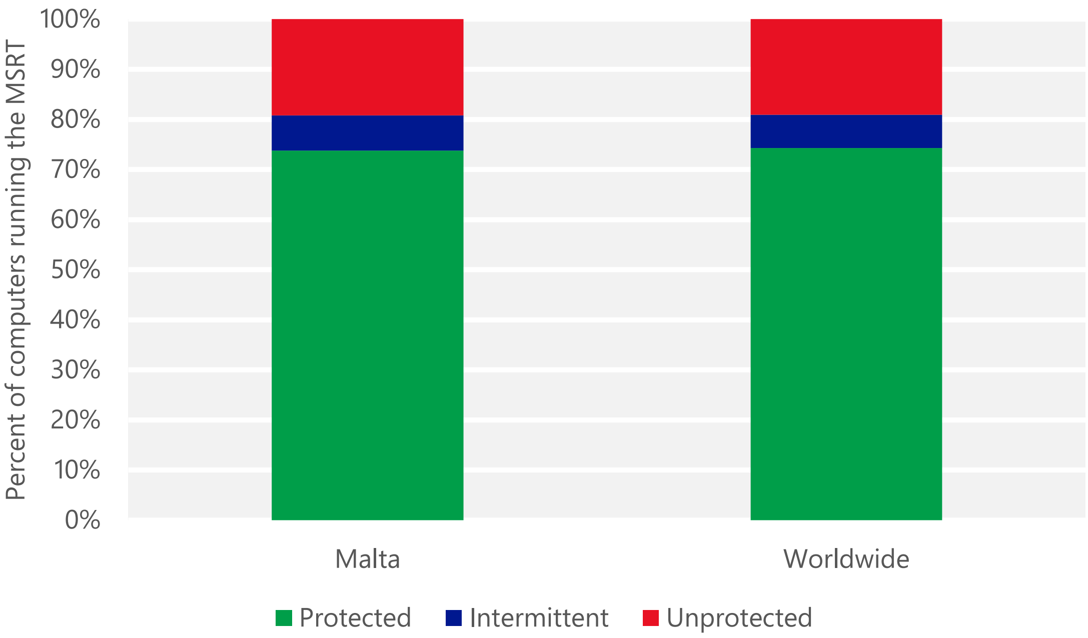
- The most common threat family infecting computers in Malta in 4Q14 was VBS/Jenxcus, which was detected and removed from 1.7 of every 1,000 unique computers scanned by the MSRT. VBS/Jenxcus is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Malta in 4Q14 was Win32/Sefnit, which was detected and removed from 0.3 of every 1,000 unique computers scanned by the MSRT. Win32/Sefnit is a family of trojans that can allow backdoor access, download files, and use the computer and Internet connection for click fraud. Some variants can monitor web browsers and hijack search results.
- The third most common threat family infecting computers in Malta in 4Q14 was MSIL/Bladabindi, which was detected and removed from 0.2 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 Malta in 4Q14 was Win32/Zbot, which was detected and removed from 0.2 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.

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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.12 drive-by download URLs for every 1,000 URLs hosted in Malta, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.03 drive-by download URLs for every 1,000 URLs hosted in Malta, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Malta and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Malta	0.12	0.03
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Mexico

The statistics presented here are generated by Microsoft security programs and services running on computers in Mexico in 4Q14 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 succeds 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

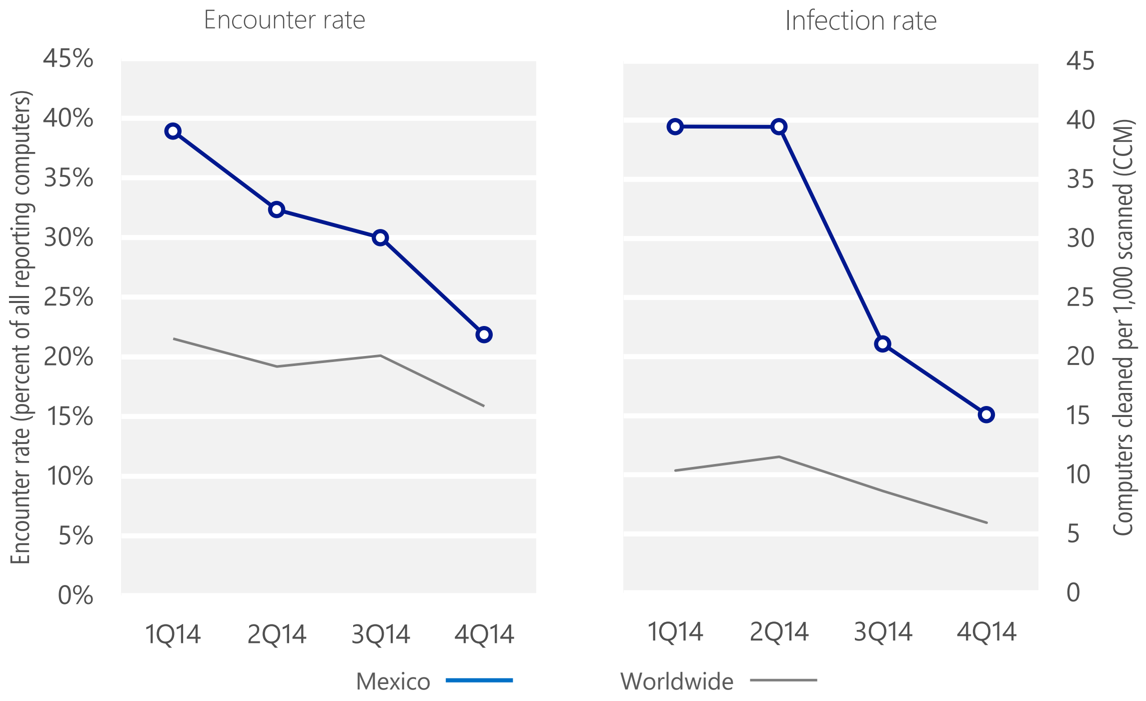
Metric	**1Q14**	**2Q14**	**3Q14**	**4Q14**
Encounter rate, Mexico	38.9%	32.3%	30.0%	21.9%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Mexico	39.5	39.5	21.1	15.1
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 21.9% percent of computers in Mexico encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 15.1 of every 1,000 unique computers scanned in Mexico in 4Q14 (a CCM score of 15.1, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Mexico over the last four quarters, compared to the world as a whole.

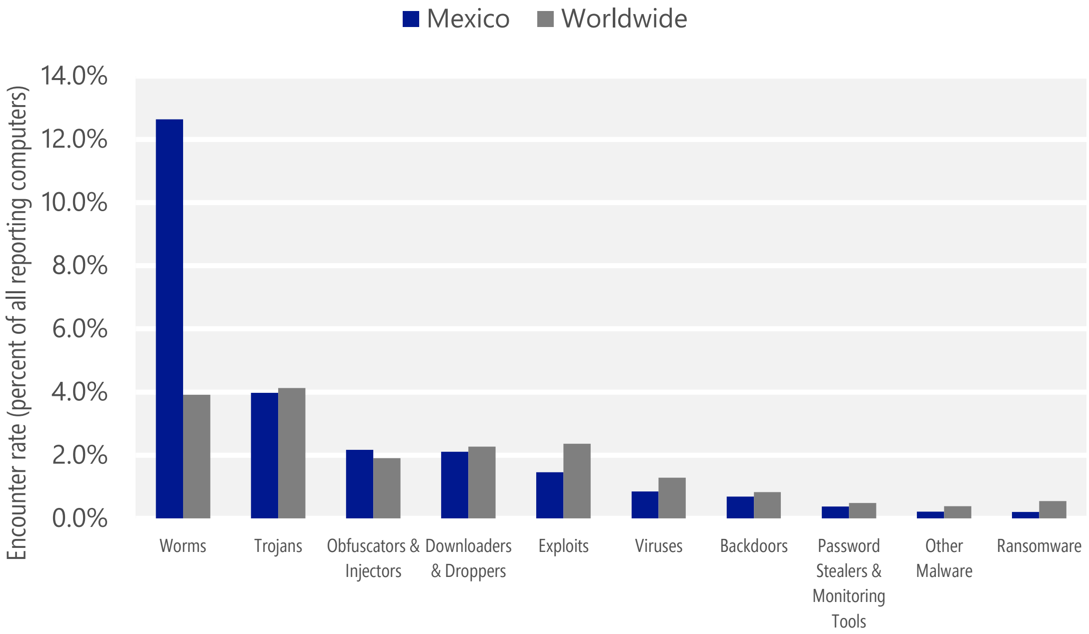
Malware encounter and infection rate trends in Mexico and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

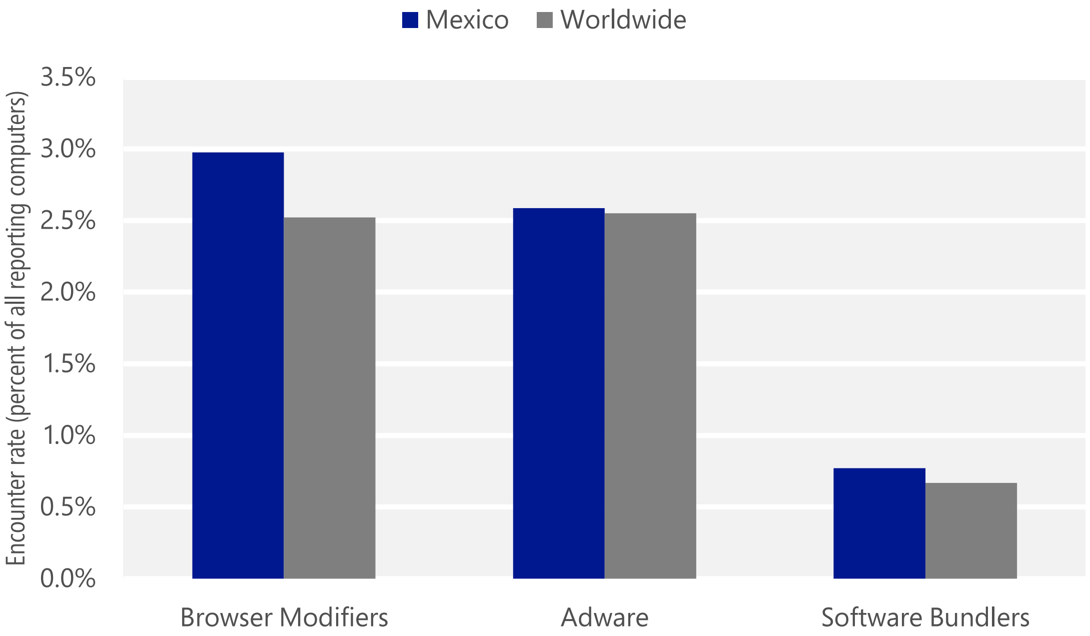
Malware encountered in Mexico in 4Q14, by category



- The most common malware category in Mexico in 4Q14 was Worms. It was encountered by 12.6 percent of all computers there, down from 14.2 percent in 3Q14.
- The second most common malware category in Mexico in 4Q14 was Trojans. It was encountered by 4.0 percent of all computers there, down from 6.8 percent in 3Q14.
- The third most common malware category in Mexico in 4Q14 was Obfuscators & Injectors, which was encountered by 2.2 percent of all computers there, down from 6.5 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Mexico in 4Q14, by category



- The most common unwanted software category in Mexico in 4Q14 was Browser Modifiers. It was encountered by 3.0 percent of all computers there, down from 6.7 percent in 3Q14.
- The second most common unwanted software category in Mexico in 4Q14 was Adware. It was encountered by 2.6 percent of all computers there, down from 4.1 percent in 3Q14.
- The third most common unwanted software category in Mexico in 4Q14 was Software Bundlers, which was encountered by 0.8 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Mexico in 4Q14

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	6.5%
2	Win32/Gamarue	Worms	2.3%
3	JS/Bondat	Worms	2.0%
4	INF/Autorun	Obfuscators & Injectors	1.6%
5	Win32/Dorkbot	Worms	1.0%
6	Win32/Vermis	Worms	0.9%
7	Win32/Crastic	Worms	0.9%
8	Win32/Conficker	Worms	0.9%
9	Win32/Brontok	Worms	0.8%
10	Win32/Tugspay	Downloaders & Droppers	0.7%

- The most common malware family encountered in Mexico in 4Q14 was VBS/Jenxcus, which was encountered by 6.5 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 Mexico in 4Q14 was Win32/Gamarue, which was encountered by 2.3 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 third most common malware family encountered in Mexico in 4Q14 was JS/Bondat, which was encountered by 2.0 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 Mexico in 4Q14 was INF/Autorun, which was encountered by 1.6 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.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Mexico in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	2.4%
2	Win32/Costmin	Adware	0.9%
3	Win32/BetterSurf	Adware	0.6%
4	Win32/Defaulttab	Browser Modifiers	0.6%
5	Win32/AddLyrics	Adware	0.3%

- The most common unwanted software family encountered in Mexico in 4Q14 was Win32/Couponruc, which was encountered by 2.4 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 Mexico in 4Q14 was Win32/Costmin, which was encountered by 0.9 percent of reporting computers there. Win32/Costmin is an adware family that installs itself as a browser extension for Internet Explorer, Mozilla Firefox, and Google Chrome, and displays advertisements as the user browses the Internet.
- The third most common unwanted software family encountered in Mexico in 4Q14 was Win32/BetterSurf, which was encountered by 0.6 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.

Top threat families by infection rate

The most common malware families by infection rate in Mexico in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	7.8
2	Win32/Gamarue	Worms	1.3
3	Win32/Wysotot	Trojans	1.0
4	Win32/Brontok	Worms	0.9
5	Win32/Dorkbot	Worms	0.8
6	Win32/Lefgroo	Worms	0.7
7	Win32/Sefnit	Trojans	0.6
8	Win32/Sality	Viruses	0.5
9	Win32/Vobfus	Worms	0.4
10	MSIL/Spacekito	Trojans	0.3

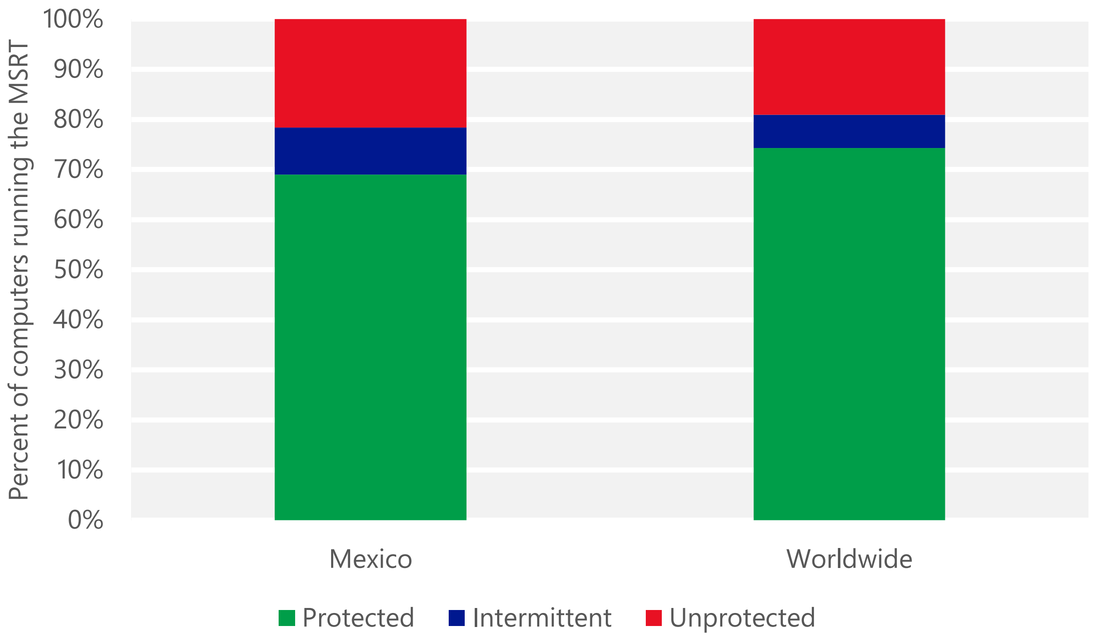
- The most common threat family infecting computers in Mexico in 4Q14 was VBS/Jenxcus, which was detected and removed from 7.8 of every 1,000 unique computers scanned by the MSRT. VBS/Jenxcus is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Mexico in 4Q14 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.
- The third most common threat family infecting computers in Mexico in 4Q14 was Win32/Wysotot, which was detected and removed from 1.0 of every 1,000 unique computers scanned by the MSRT. Win32/Wysotot is a threat that can change the start page of the user's web browser, and may download and install other files to the computer. It is installed by software bundlers that advertise free software or games.
- The fourth most common threat family infecting computers in Mexico in 4Q14 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 Mexico and worldwide protected by real-time security software in 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.24 drive-by download URLs for every 1,000 URLs hosted in Mexico, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.10 drive-by download URLs for every 1,000 URLs hosted in Mexico, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Mexico and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Mexico	0.24	0.10
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Moldova

The statistics presented here are generated by Microsoft security programs and services running on computers in Moldova in 4Q14 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 succeds 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

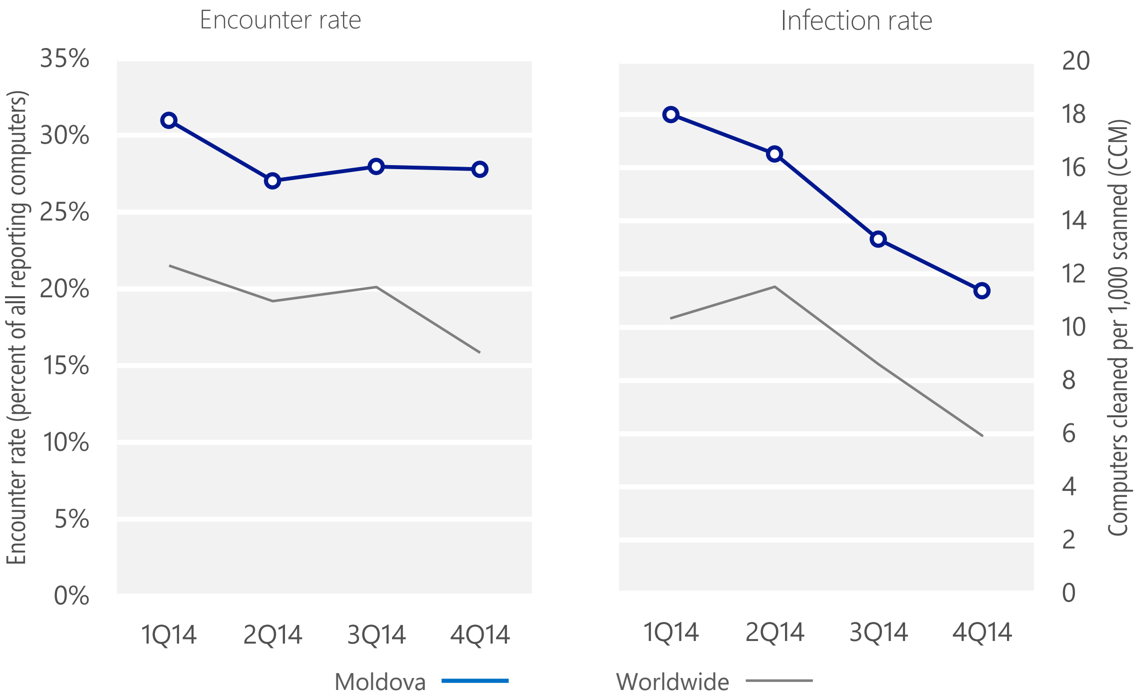
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Moldova	31.0%	27.0%	28.0%	27.8%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Moldova	18.0	16.5	13.3	11.4
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 27.8% percent of computers in Moldova encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 11.4 of every 1,000 unique computers scanned in Moldova in 4Q14 (a CCM score of 11.4, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Moldova over the last four quarters, compared to the world as a whole.

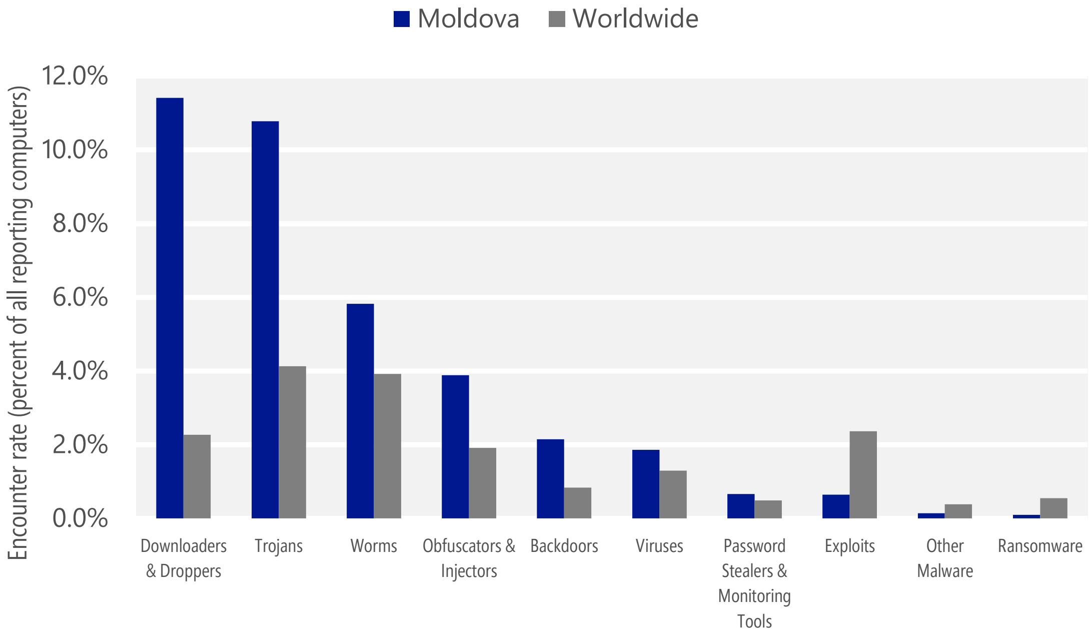
Malware encounter and infection rate trends in Moldova and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

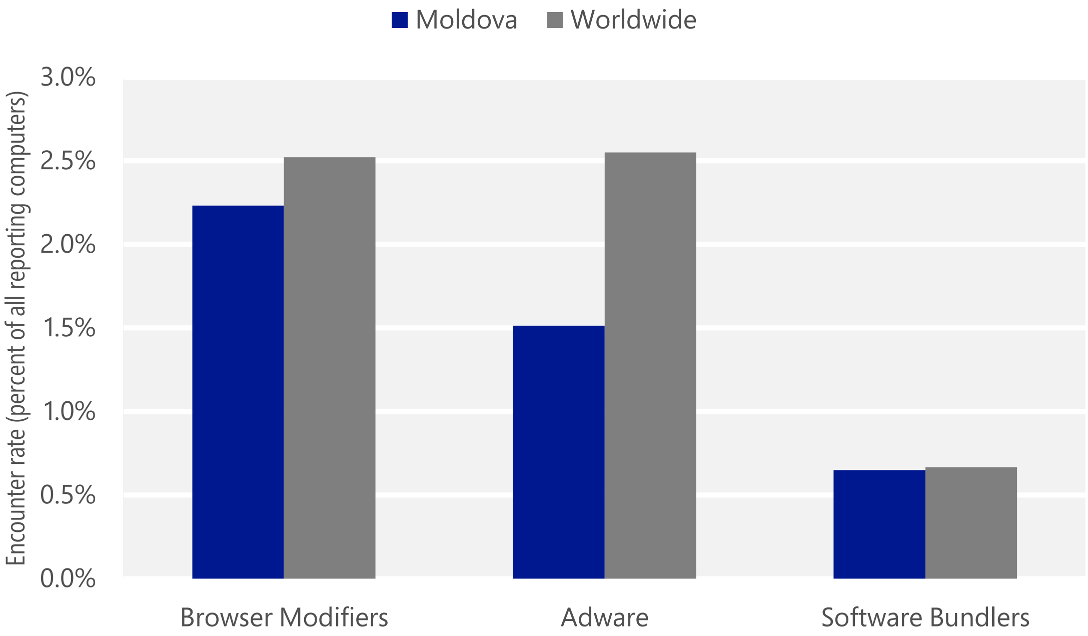
Malware encountered in Moldova in 4Q14, by category



- The most common malware category in Moldova in 4Q14 was Downloaders & Droppers. It was encountered by 11.4 percent of all computers there, down from 12.3 percent in 3Q14.
- The second most common malware category in Moldova in 4Q14 was Trojans. It was encountered by 10.8 percent of all computers there, down from 10.8 percent in 3Q14.
- The third most common malware category in Moldova in 4Q14 was Worms, which was encountered by 5.8 percent of all computers there, up from 5.5 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Moldova in 4Q14, by category



- The most common unwanted software category in Moldova in 4Q14 was Browser Modifiers. It was encountered by 2.2 percent of all computers there, down from 3.4 percent in 3Q14.
- The second most common unwanted software category in Moldova in 4Q14 was Adware. It was encountered by 1.5 percent of all computers there, up from 0.3 percent in 3Q14.
- The third most common unwanted software category in Moldova in 4Q14 was Software Bundlers, which was encountered by 0.6 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Moldova in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Ogimant	Downloaders & Droppers	10.1%
2	Win32/Peaac	Trojans	3.4%
3	Win32/Obfuscator	Obfuscators & Injectors	2.6%
4	Win32/Gamarue	Worms	1.6%
5	VBS/Jenxcus	Worms	1.4%
6	Win32/Peals	Trojans	1.2%
7	Win32/Brontok	Worms	1.1%
8	Win32/Dynamer	Trojans	0.9%
9	Win32/Sality	Viruses	0.9%
10	Win32/Morix	Backdoors	0.7%

- The most common malware family encountered in Moldova in 4Q14 was Win32/Ogimant, which was encountered by 10.1 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 second most common malware family encountered in Moldova in 4Q14 was Win32/Peaac, which was encountered by 3.4 percent of reporting computers there. Win32/Peaac is a generic detection for various threats that display trojan characteristics.
- The third most common malware family encountered in Moldova in 4Q14 was Win32/Obfuscator, which was encountered by 2.6 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 Moldova in 4Q14 was Win32/Gamarue, which was encountered by 1.6 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 Moldova in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	1.3%
2	Win32/Defaulttab	Browser Modifiers	1.0%
3	Win32/BetterSurf	Adware	0.8%
4	Win32/Costmin	Adware	0.6%
5	Win32/Gofileexpress	Software Bundlers	0.5%

- The most common unwanted software family encountered in Moldova in 4Q14 was Win32/Couponruc, which was encountered by 1.3 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 Moldova in 4Q14 was Win32/Defaulttab, which was encountered by 1.0 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.
- The third most common unwanted software family encountered in Moldova in 4Q14 was Win32/BetterSurf, which was encountered by 0.8 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.

Top threat families by infection rate

The most common malware families by infection rate in Moldova in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Brontok	Worms	1.9
2	Win32/Gamarue	Worms	1.7
3	VBS/Jenxcus	Worms	1.6
4	Win32/Ramnit	Trojans	1.1
5	Win32/Sality	Viruses	0.7
6	JS/Kilim	Trojans	0.7
7	Win32/Helompy	Worms	0.5
8	Win32/Dorkbot	Worms	0.5
9	Win32/Tofsee	Backdoors	0.4
10	Win32/Deminnix	Trojans	0.4

- The most common threat family infecting computers in Moldova in 4Q14 was Win32/Brontok, which was detected and removed from 1.9 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.
- The second most common threat family infecting computers in Moldova in 4Q14 was Win32/Gamarue, which was detected and removed from 1.7 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 third most common threat family infecting computers in Moldova in 4Q14 was VBS/Jenxcus, which was detected and removed from 1.6 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 fourth most common threat family infecting computers in Moldova in 4Q14 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

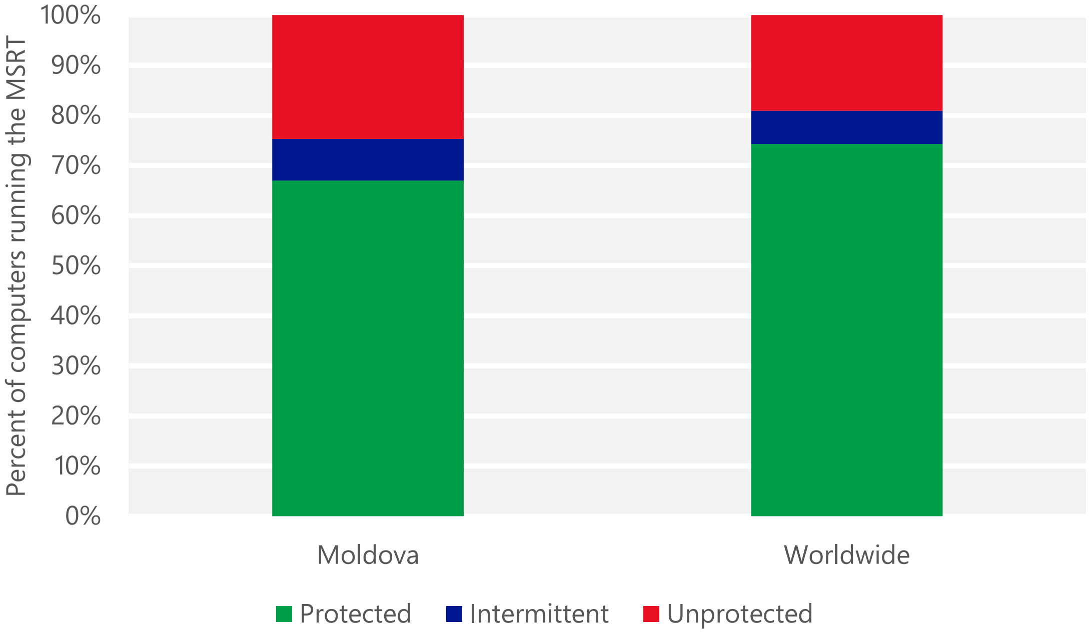
information such as saved FTP credentials and browser cookies. It may also open a backdoor to await instructions from a remote attacker.

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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 4.23 drive-by download URLs for every 1,000 URLs hosted in Moldova, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 10.45 drive-by download URLs for every 1,000 URLs hosted in Moldova, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Moldova and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Moldova	4.23	10.45
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Mongolia

The statistics presented here are generated by Microsoft security programs and services running on computers in Mongolia in 4Q14 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 succeds 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

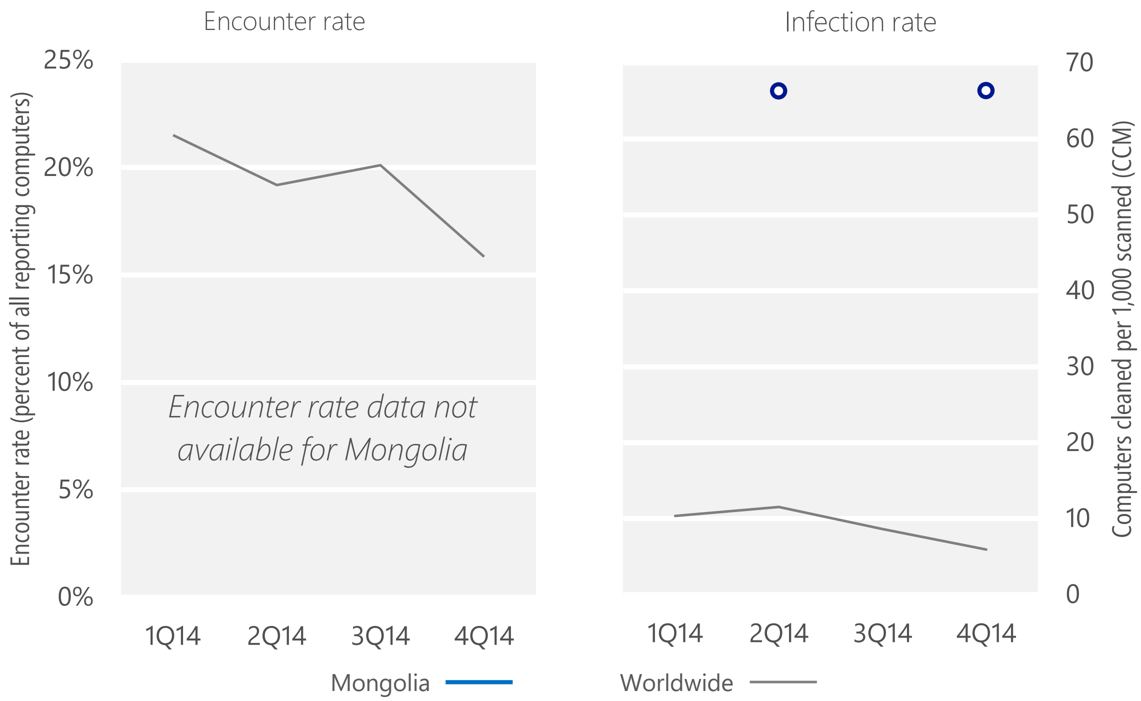
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Mongolia	N/A	N/A	N/A	N/A
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Mongolia	N/A	66.3	N/A	66.3
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, the MSRT detected and removed malware from 66.3 of every 1,000 unique computers scanned in Mongolia in 4Q14 (a CCM score of 66.3, compared to the 4Q14 worldwide CCM of 5.9). 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 18* 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 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Gamarue	Worms	33.5
2	Win32/Sality	Viruses	12.4
3	VBS/Jenxcus	Worms	12.4
4	Win32/Ramnit	Trojans	4.7
5	Win32/Vobfus	Worms	4.0
6	JS/Kilim	Trojans	2.3
7	Win32/Brontok	Worms	1.8
8	Win32/Dorkbot	Worms	1.7
9	MSIL/Bladabindi	Backdoors	1.4
10	Win32/Lethic	Trojans	0.9

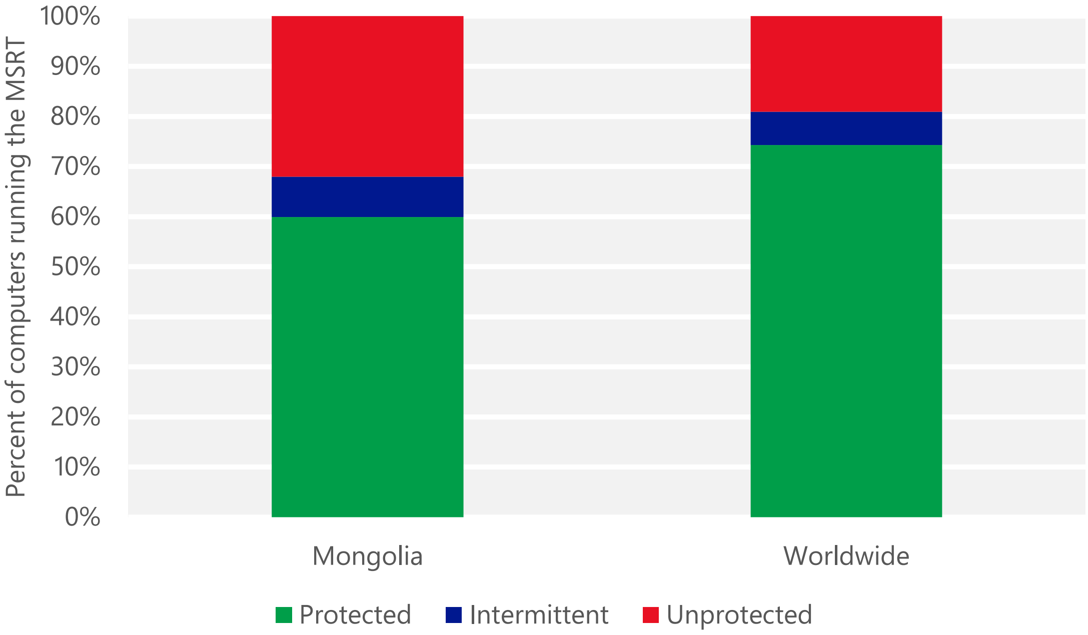
- The most common threat family infecting computers in Mongolia in 4Q14 was Win32/Gamarue, which was detected and removed from 33.5 of every 1,000 unique computers scanned by the MSRT. Win32/Gamarue is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed 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 Mongolia in 4Q14 was Win32/Sality, which was detected and removed from 12.4 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 Mongolia in 4Q14 was VBS/Jenxcus, which was detected and removed from 12.4 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 fourth most common threat family infecting computers in Mongolia in 4Q14 was Win32/Ramnit, which was detected and removed from 4.7 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 Mongolia and worldwide protected by real-time security software in 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 4.32 drive-by download URLs for every 1,000 URLs hosted in Mongolia, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 4.98 drive-by download URLs for every 1,000 URLs hosted in Mongolia, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Mongolia and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Mongolia	4.32	4.98
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Morocco

The statistics presented here are generated by Microsoft security programs and services running on computers in Morocco in 4Q14 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 succeds 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

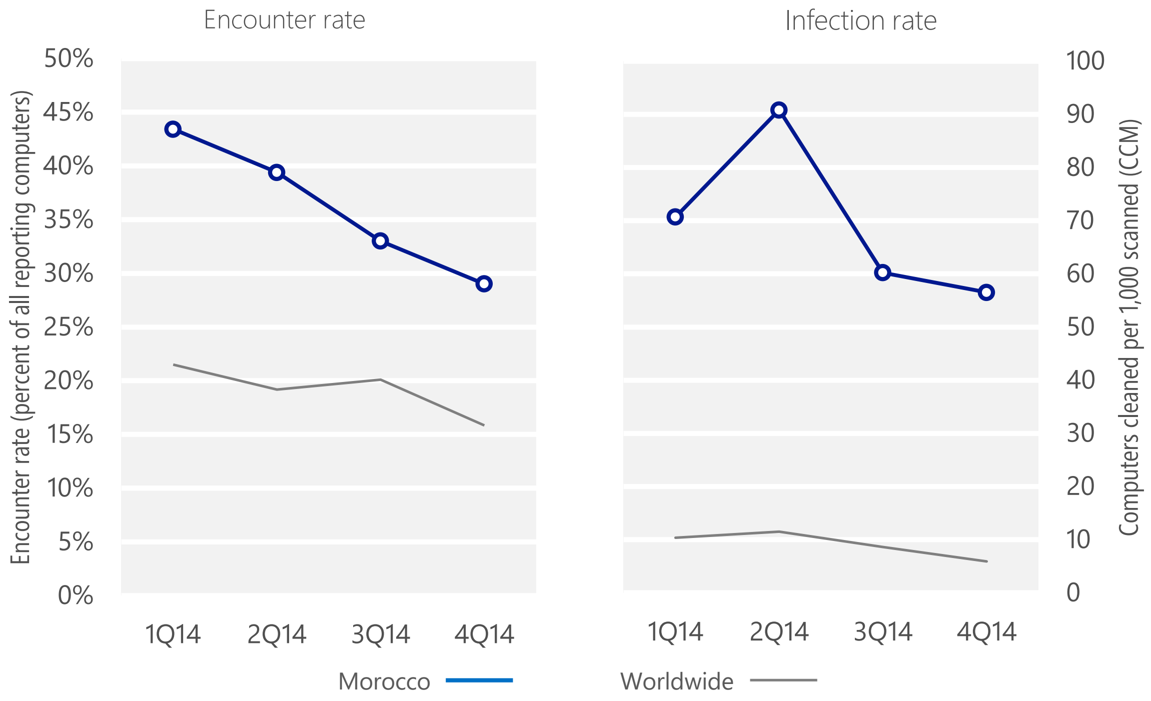
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Morocco	43.4%	39.4%	33.0%	29.0%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Morocco	70.7	90.8	60.2	56.5
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 29.0% percent of computers in Morocco encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 56.5 of every 1,000 unique computers scanned in Morocco in 4Q14 (a CCM score of 56.5, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Morocco over the last four quarters, compared to the world as a whole.

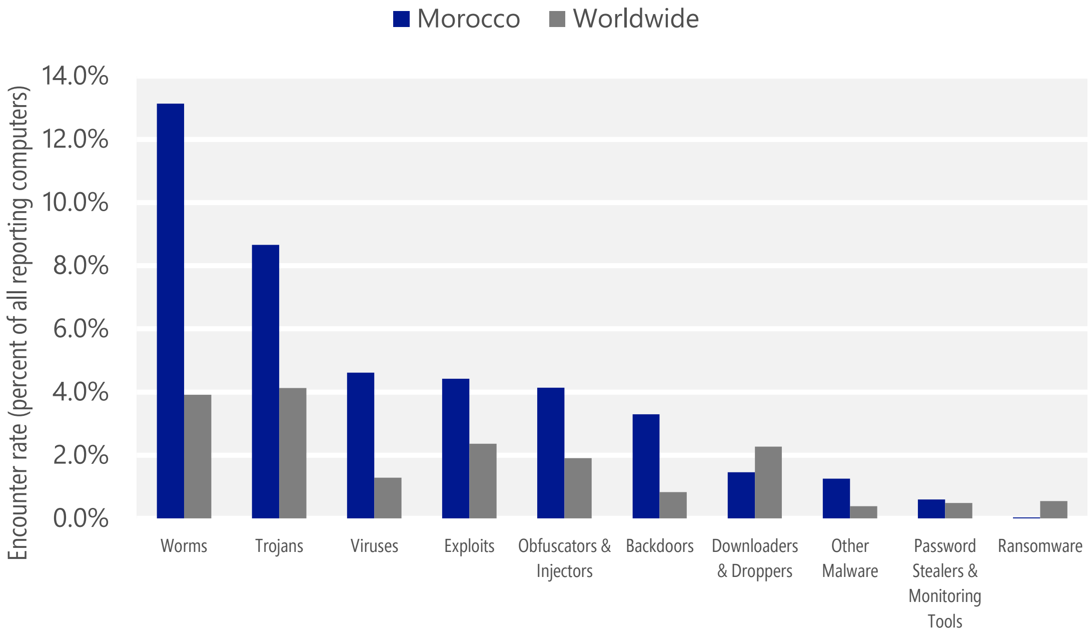
Malware encounter and infection rate trends in Morocco and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

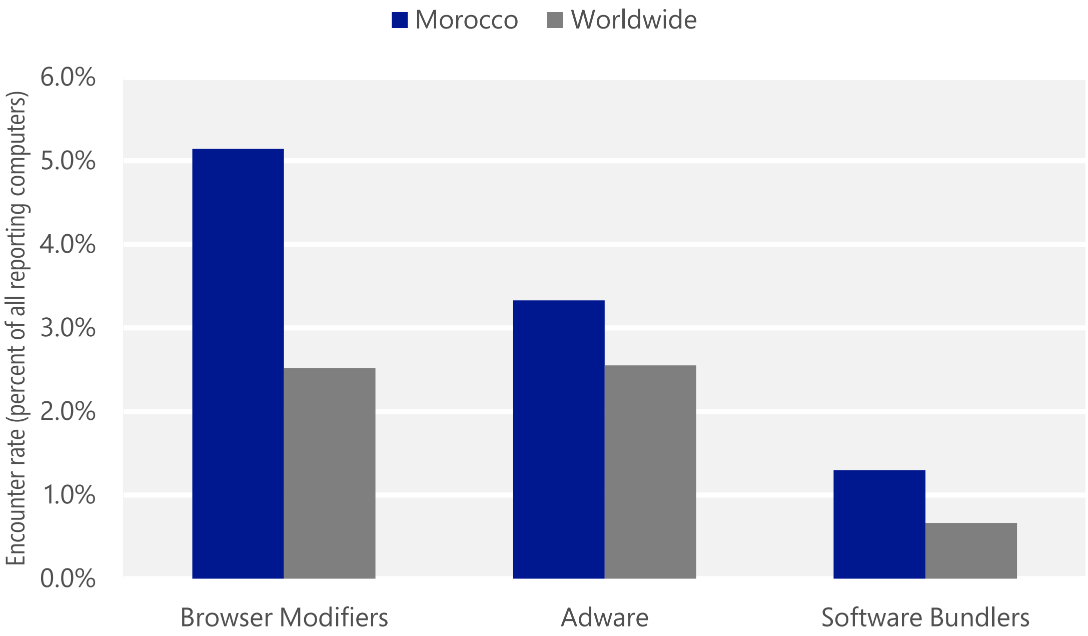
Malware encountered in Morocco in 4Q14, by category



- The most common malware category in Morocco in 4Q14 was Worms. It was encountered by 13.1 percent of all computers there, down from 14.0 percent in 3Q14.
- The second most common malware category in Morocco in 4Q14 was Trojans. It was encountered by 8.7 percent of all computers there, down from 11.6 percent in 3Q14.
- The third most common malware category in Morocco in 4Q14 was Viruses, which was encountered by 4.6 percent of all computers there, up from 4.5 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Morocco in 4Q14, by category



- The most common unwanted software category in Morocco in 4Q14 was Browser Modifiers. It was encountered by 5.1 percent of all computers there, down from 6.8 percent in 3Q14.
- The second most common unwanted software category in Morocco in 4Q14 was Adware. It was encountered by 3.3 percent of all computers there, up from 2.8 percent in 3Q14.
- The third most common unwanted software category in Morocco in 4Q14 was Software Bundlers, which was encountered by 1.3 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Morocco in 4Q14

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	7.2%
2	Win32/CplLnk	Exploits	3.8%
3	Win32/Ramnit	Trojans	3.8%
4	INF/Autorun	Obfuscators & Injectors	3.5%
5	Win32/Sality	Viruses	2.4%
6	Win32/Vermis	Worms	1.4%
7	Win32/Yeltminky	Worms	1.4%
8	MSIL/Bladabindi	Backdoors	1.4%
9	Win32/Mabezat	Viruses	1.2%
10	Win32/Caphaw	Backdoors	1.1%

- The most common malware family encountered in Morocco in 4Q14 was VBS/Jenxcus, which was encountered by 7.2 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 4Q14 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 third most common malware family encountered in Morocco in 4Q14 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.
- The fourth most common malware family encountered in Morocco in 4Q14 was INF/Autorun, which was encountered by 3.5 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 Morocco in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	3.6%
2	Win32/Defaulttab	Browser Modifiers	1.7%
3	Win32/BetterSurf	Adware	1.4%
4	Win32/Costmin	Adware	1.1%
5	Win32/Gofileexpress	Software Bundlers	1.0%

- The most common unwanted software family encountered in Morocco in 4Q14 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 Morocco in 4Q14 was Win32/Defaulttab, which was encountered by 1.7 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.

- The third most common unwanted software family encountered in Morocco in 4Q14 was Win32/BetterSurf, which was encountered by 1.4 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.

Top threat families by infection rate

The most common malware families by infection rate in Morocco in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Yeltminky	Worms	21.2
2	VBS/Jenxcus	Worms	13.7
3	Win32/Sality	Viruses	8.3
4	Win32/Ramnit	Trojans	8.0
5	Win32/Nitol	Other Malware	6.1
6	MSIL/Bladabindi	Backdoors	2.7
7	Win32/Pramro	Trojans	1.4
8	Win32/Dorkbot	Worms	1.3
9	JS/Kilim	Trojans	0.7
10	Win32/Brontok	Worms	0.6

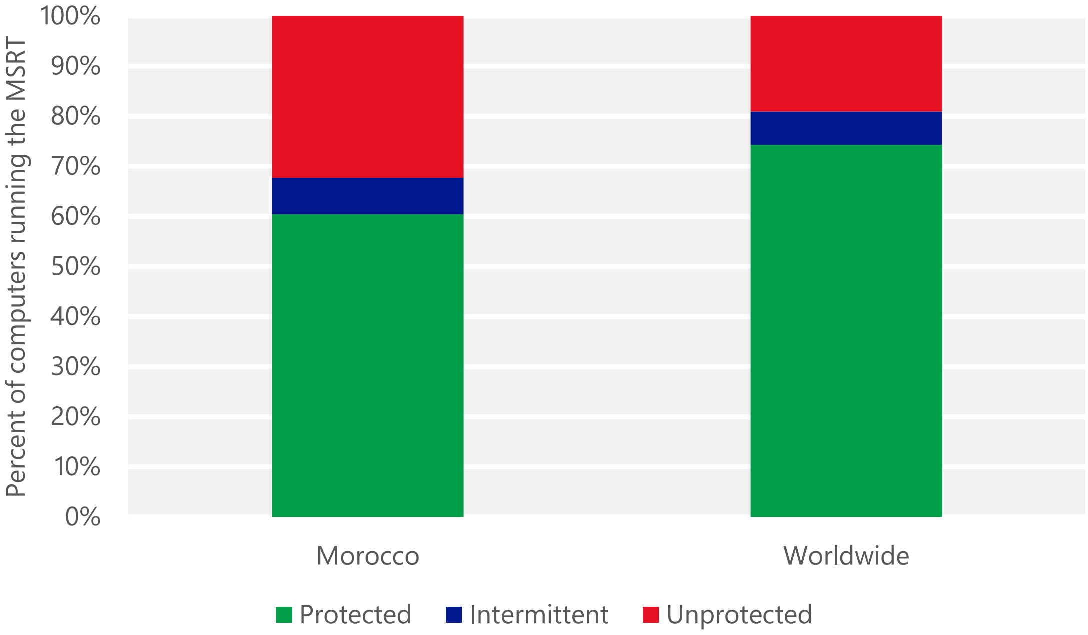
- The most common threat family infecting computers in Morocco in 4Q14 was Win32/Yeltminky, which was detected and removed from 21.2 of every 1,000 unique computers scanned by the MSRT. Win32/Yeltminky is a family of worms that spreads by making copies of itself on all available drives and creating an autorun.inf file to execute that copy.
- The second most common threat family infecting computers in Morocco in 4Q14 was VBS/Jenxcus, which was detected and removed from 13.7 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 Morocco in 4Q14 was Win32/Sality, which was detected and removed from 8.3 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 Morocco in 4Q14 was Win32/Ramnit, which was detected and removed from 8.0 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 Morocco and worldwide protected by real-time security software in 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 2.03 drive-by download URLs for every 1,000 URLs hosted in Morocco, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 2.64 drive-by download URLs for every 1,000 URLs hosted in Morocco, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Morocco and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Morocco	2.03	2.64
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Nepal

The statistics presented here are generated by Microsoft security programs and services running on computers in Nepal in 4Q14 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 succeds 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

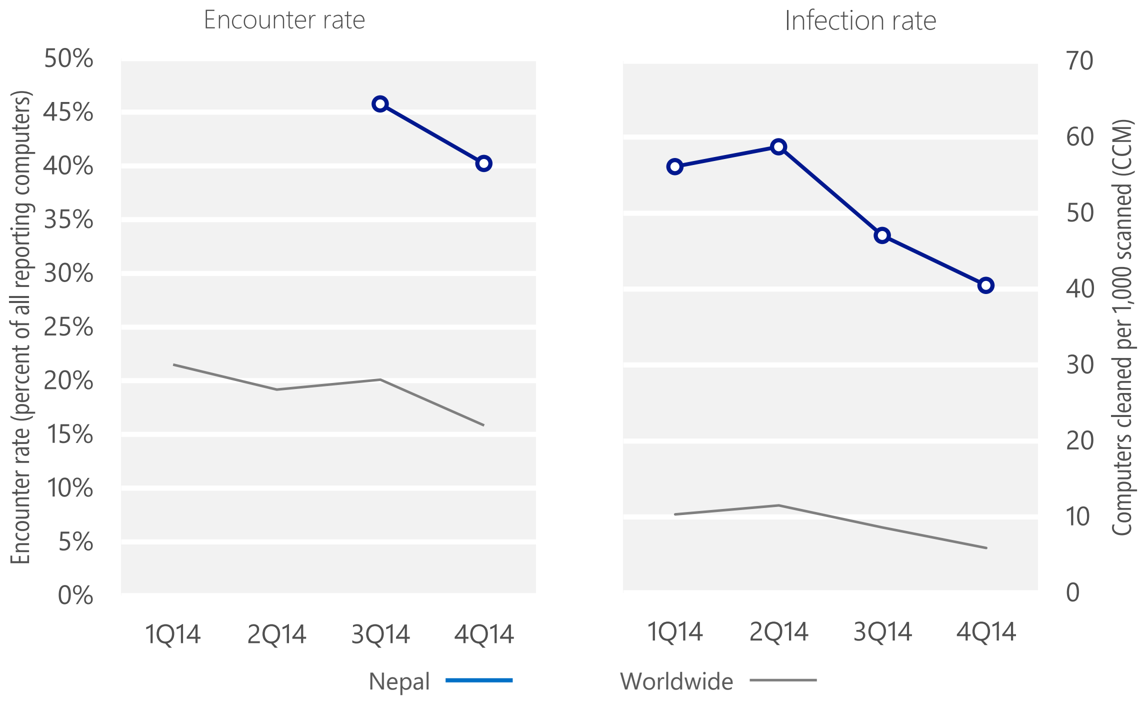
Metric	**1Q14**	**2Q14**	**3Q14**	**4Q14**
Encounter rate, Nepal	N/A	N/A	45.8%	40.2%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Nepal	56.1	58.7	47.1	40.5
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 40.2% percent of computers in Nepal encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 40.5 of every 1,000 unique computers scanned in Nepal in 4Q14 (a CCM score of 40.5, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Nepal over the last four quarters, compared to the world as a whole.

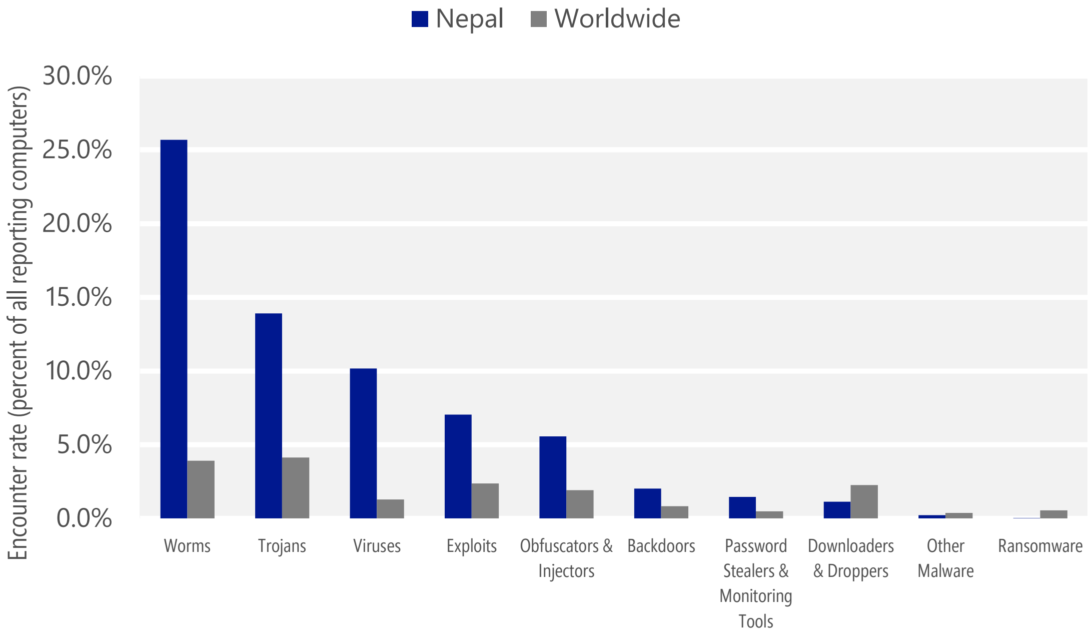
Malware encounter and infection rate trends in Nepal and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

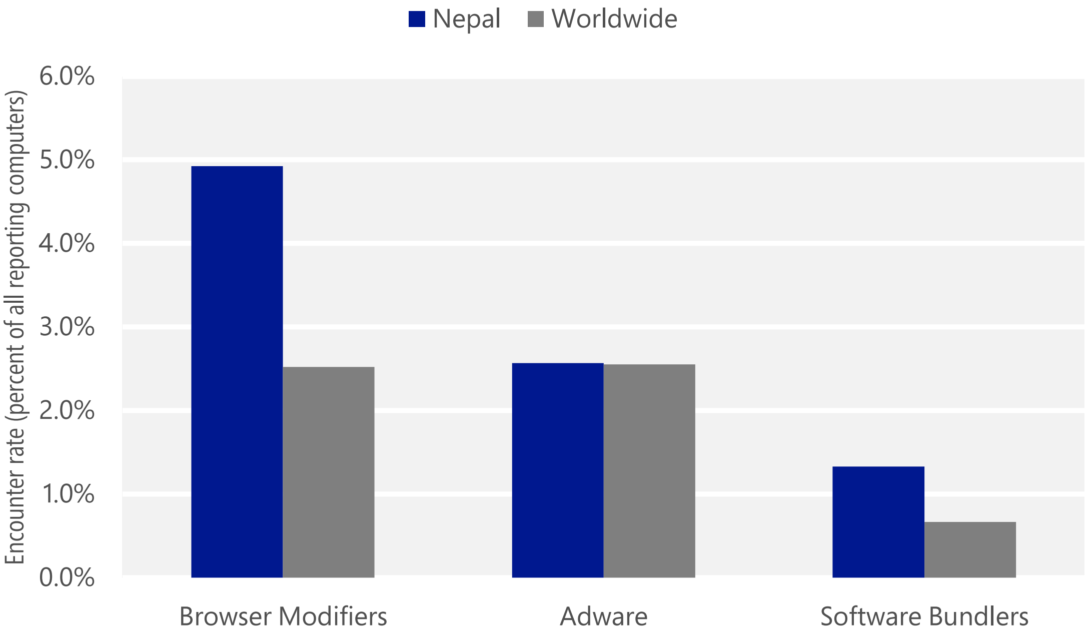
Malware encountered in Nepal in 4Q14, by category



- The most common malware category in Nepal in 4Q14 was Worms. It was encountered by 25.7 percent of all computers there, down from 30.4 percent in 3Q14.
- The second most common malware category in Nepal in 4Q14 was Trojans. It was encountered by 13.9 percent of all computers there, down from 17.6 percent in 3Q14.
- The third most common malware category in Nepal in 4Q14 was Viruses, which was encountered by 10.2 percent of all computers there, down from 12.1 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Nepal in 4Q14, by category



- The most common unwanted software category in Nepal in 4Q14 was Browser Modifiers. It was encountered by 4.9 percent of all computers there, down from 5.0 percent in 3Q14.
- The second most common unwanted software category in Nepal in 4Q14 was Adware. It was encountered by 2.6 percent of all computers there, up from 0.7 percent in 3Q14.
- The third most common unwanted software category in Nepal in 4Q14 was Software Bundlers, which was encountered by 1.3 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Nepal in 4Q14

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	16.0%
2	INF/Autorun	Obfuscators & Injectors	7.2%
3	Win32/CplLnk	Exploits	6.6%
4	Win32/Ramnit	Trojans	6.6%
5	Win32/Virut	Viruses	4.5%
6	Win32/Finodes	Trojans	4.1%
7	Win32/Sality	Viruses	4.1%
8	Win32/Vercuser	Worms	2.7%
9	Win32/Yeltminky	Worms	2.4%
10	Win32/Nuqel	Worms	2.2%

- The most common malware family encountered in Nepal in 4Q14 was VBS/Jenxcus, which was encountered by 16.0 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 4Q14 was INF/Autorun, which was encountered by 7.2 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.
- The third most common malware family encountered in Nepal in 4Q14 was Win32/CplLnk, which was encountered by 6.6 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 4Q14 was Win32/Ramnit, which was encountered by 6.6 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 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	3.4%
2	Win32/Defaulttab	Browser Modifiers	1.6%
3	Win32/BetterSurf	Adware	1.3%
4	Win32/Costmin	Adware	0.9%
5	Win32/Gofileexpress	Software Bundlers	0.9%

- The most common unwanted software family encountered in Nepal in 4Q14 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 Nepal in 4Q14 was Win32/Defaulttab, which was encountered by 1.6 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.

- The third most common unwanted software family encountered in Nepal in 4Q14 was Win32/BetterSurf, which was encountered by 1.3 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.

Top threat families by infection rate

The most common malware families by infection rate in Nepal in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	19.3
2	Win32/Sality	Viruses	7.2
3	Win32/Ramnit	Trojans	6.4
4	Win32/Jeefo	Viruses	4.1
5	Win32/Tupym	Worms	1.7
6	Win32/Gamarue	Worms	1.5
7	Win32/Nuqel	Worms	1.3
8	Win32/Wecykler	Worms	0.8
9	Win32/Vesenlosow	Worms	0.7
10	MSIL/Bladabindi	Backdoors	0.7

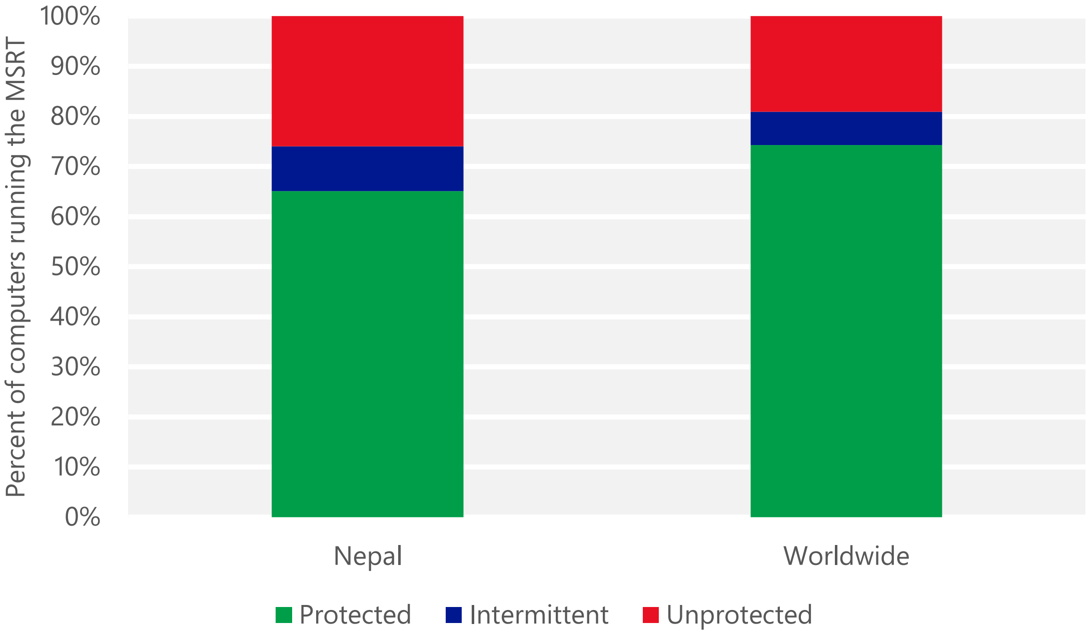
- The most common threat family infecting computers in Nepal in 4Q14 was VBS/Jenxcus, which was detected and removed from 19.3 of every 1,000 unique computers scanned by the MSRT. VBS/Jenxcus is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Nepal in 4Q14 was Win32/Sality, which was detected and removed from 7.2 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.
- The third most common threat family infecting computers in Nepal in 4Q14 was Win32/Ramnit, which was detected and removed from 6.4 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 Nepal in 4Q14 was Win32/Jeefo, which was detected and removed from 4.1 of every 1,000 unique computers scanned by the MSRT. Win32/Jeefo is a parasitic file-infector 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.

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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.19 drive-by download URLs for every 1,000 URLs hosted in Nepal, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.01 drive-by download URLs for every 1,000 URLs hosted in Nepal, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Nepal and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Nepal	0.19	0.01
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Netherlands

The statistics presented here are generated by Microsoft security programs and services running on computers in the Netherlands in 4Q14 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 succeds 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

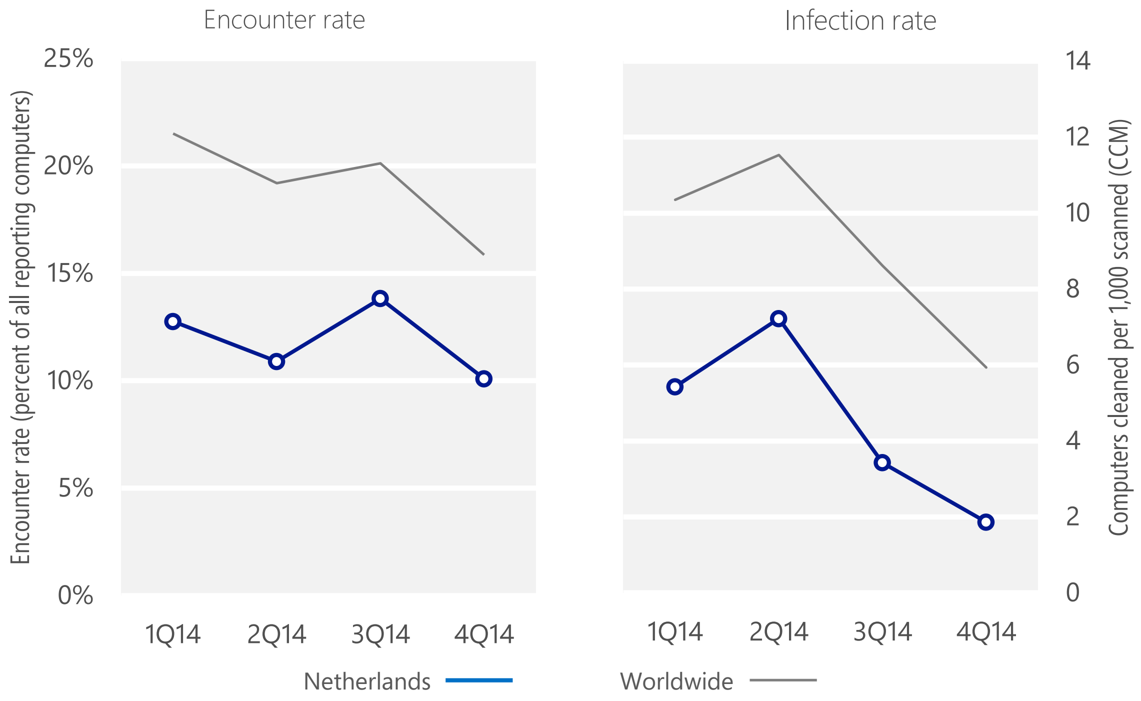
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Netherlands	12.8%	10.9%	13.8%	10.1%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Netherlands	5.4	7.2	3.4	1.9
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 10.1% percent of computers in the Netherlands encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 1.9 of every 1,000 unique computers scanned in the Netherlands in 4Q14 (a CCM score of 1.9, compared to the 4Q14 worldwide CCM of 5.9). 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.

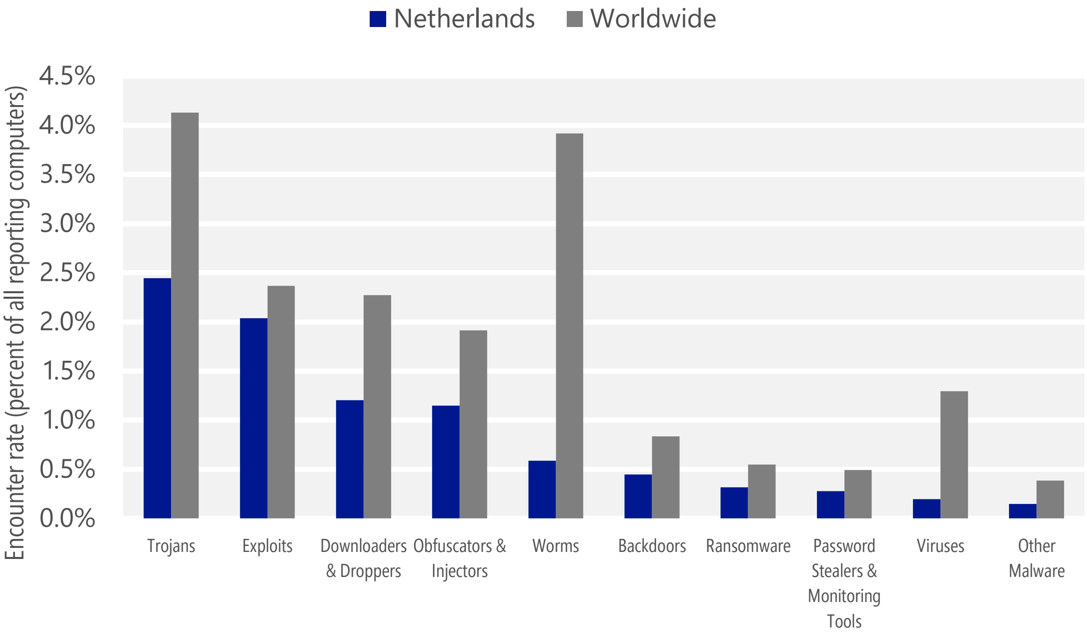
Malware encounter and infection rate trends in the Netherlands and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

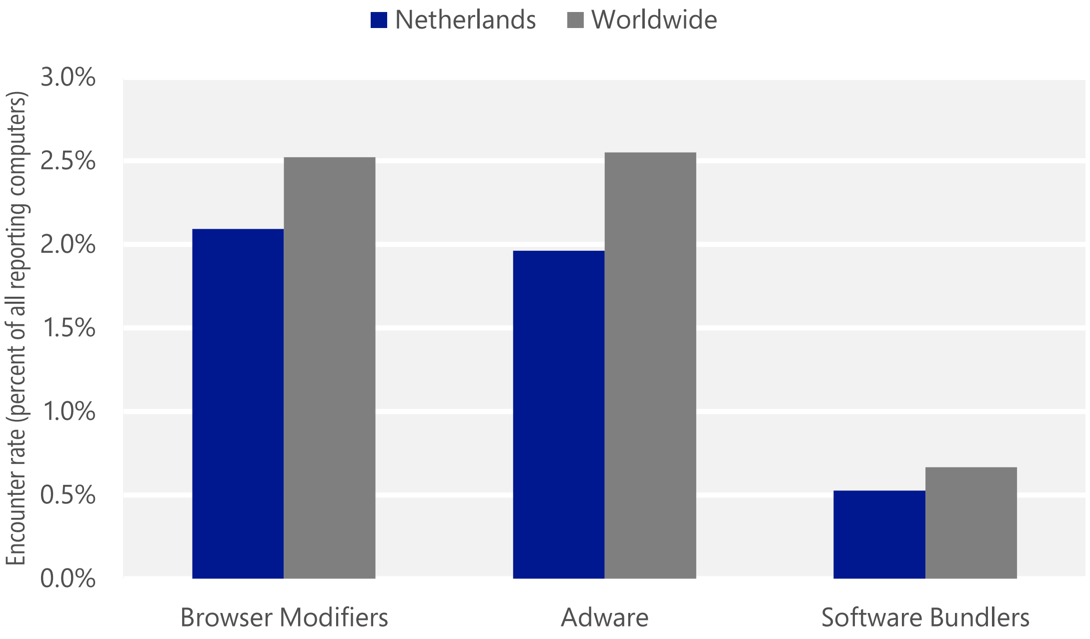
Malware encountered in the Netherlands in 4Q14, by category



- The most common malware category in the Netherlands in 4Q14 was Trojans. It was encountered by 2.4 percent of all computers there, down from 3.8 percent in 3Q14.
- The second most common malware category in the Netherlands in 4Q14 was Exploits. It was encountered by 2.0 percent of all computers there, down from 3.4 percent in 3Q14.
- The third most common malware category in the Netherlands in 4Q14 was Downloaders & Droppers, which was encountered by 1.2 percent of all computers there, down from 3.2 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in the Netherlands in 4Q14, by category



- The most common unwanted software category in the Netherlands in 4Q14 was Browser Modifiers. It was encountered by 2.1 percent of all computers there, down from 3.5 percent in 3Q14.
- The second most common unwanted software category in the Netherlands in 4Q14 was Adware. It was encountered by 2.0 percent of all computers there, up from 1.6 percent in 3Q14.
- The third most common unwanted software category in the Netherlands in 4Q14 was Software Bundlers, which was encountered by 0.5 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in the Netherlands in 4Q14

	Family	Most significant category	% of reporting computers
1	JS/Axpergle	Exploits	1.0%
2	Win32/Obfuscator	Obfuscators & Injectors	1.0%
3	Win32/Sanusra	Trojans	0.3%
4	Win32/Tugspay	Downloaders & Droppers	0.3%
5	JS/Redirector	Trojans	0.3%
6	JS/Fiexp	Exploits	0.3%
7	Win32/Dynamer	Trojans	0.2%
8	ASX/Wimad	Downloaders & Droppers	0.2%
9	Win32/Gamarue	Worms	0.2%
10	Win32/Anogre	Exploits	0.2%

- The most common malware family encountered in the Netherlands in 4Q14 was JS/Axpergle, which was encountered by 1.0 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 4Q14 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.
- The third most common malware family encountered in the Netherlands in 4Q14 was Win32/Sanusra, which was encountered by 0.3 percent of reporting computers there. Win32/Sanusra is a threat that connects to a remote attacker to send encrypted information about the computer.
- The fourth most common malware family encountered in the Netherlands in 4Q14 was Win32/Tugspay, which was encountered by 0.3 percent of reporting computers there. Win32/Tugspay is a downloader that spreads by posing as an installer for legitimate software, such as a Java update, or through other malware. When installed, it downloads unwanted software to the computer.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in the Netherlands in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	1.8%
2	Win32/Costmin	Adware	0.6%
3	Win32/Pirrit	Adware	0.4%
4	Win32/BetterSurf	Adware	0.4%
5	Win32/Gofileexpress	Software Bundlers	0.3%

- The most common unwanted software family encountered in the Netherlands in 4Q14 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 the Netherlands in 4Q14 was Win32/Costmin, which was encountered by 0.6 percent of reporting computers there. Win32/Costmin is an adware family that installs itself as a browser extension for Internet Explorer, Mozilla Firefox, and Google Chrome, and displays advertisements as the user browses the Internet.
- The third most common unwanted software family encountered in the Netherlands in 4Q14 was Win32/Pirrit, which was encountered by 0.4 percent of reporting computers there. Win32/Pirrit is a program that shows ads as the user browses the web. It can be downloaded from the program's website or bundled with some third-party software installation programs.

Top threat families by infection rate

The most common malware families by infection rate in the Netherlands in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Sinowal	Password Stealers & Monitoring Tools	0.2
2	Win32/Sefnit	Trojans	0.2
3	Win32/Wysotot	Trojans	0.2
4	Win32/Alureon	Trojans	0.2
5	Win32/Zbot	Password Stealers & Monitoring Tools	0.1
6	Win32/Gamarue	Worms	0.1
7	JS/Miuref	Trojans	0.1
8	MSIL/Bladabindi	Backdoors	0.1
9	Win32/Brontok	Worms	0.1
10	VBS/Jenxcus	Worms	0.1

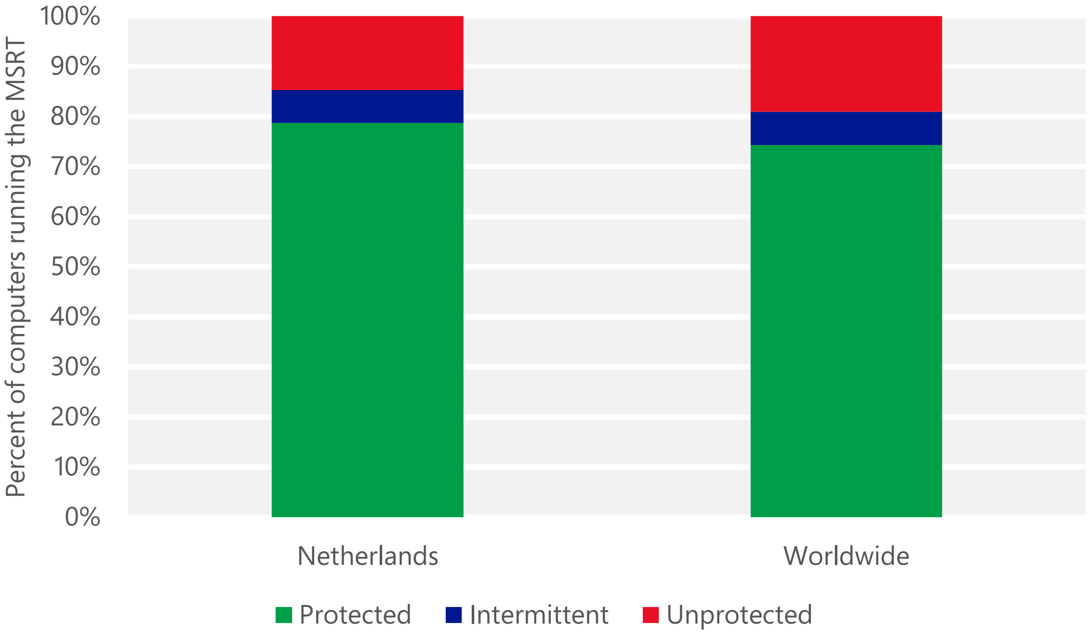
- The most common threat family infecting computers in the Netherlands in 4Q14 was Win32/Sinowal, which was detected and removed from 0.2 of every 1,000 unique computers scanned by the MSRT. Win32/Sinowal is a family of password-stealing and backdoor trojans. It may try to install a fraudulent SSL certificate on the computer. Sinowal may also capture user data such as banking credentials from various user accounts and send the data to Web sites specified by the attacker.
- The second most common threat family infecting computers in the Netherlands in 4Q14 was Win32/Sefnit, which was detected and removed from 0.2 of every 1,000 unique computers scanned by the MSRT. Win32/Sefnit is a family of trojans that can allow backdoor access, download files, and use the computer and Internet connection for click fraud. Some variants can monitor web browsers and hijack search results.
- The third most common threat family infecting computers in the Netherlands in 4Q14 was Win32/Wysotot, which was detected and removed from 0.2 of every 1,000 unique computers scanned by the MSRT. Win32/Wysotot is a threat that can change the start page of the user's web browser, and may download and install other files to the computer. It is installed by software bundlers that advertise free software or games.
- The fourth most common threat family infecting computers in the Netherlands in 4Q14 was Win32/Alureon, which was detected and removed from 0.2 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.

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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.27 drive-by download URLs for every 1,000 URLs hosted in the Netherlands, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.31 drive-by download URLs for every 1,000 URLs hosted in the Netherlands, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in the Netherlands and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Netherlands	0.27	0.31
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

New Zealand

The statistics presented here are generated by Microsoft security programs and services running on computers in New Zealand in 4Q14 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 succeds 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

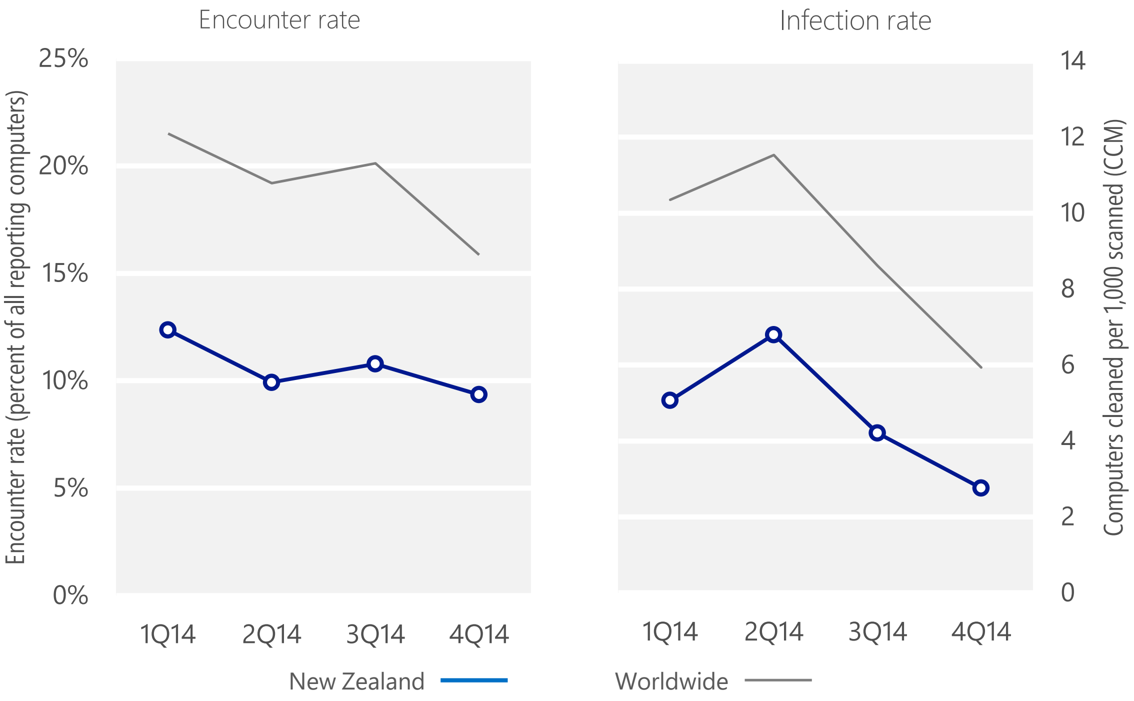
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, New Zealand	12.4%	9.9%	10.8%	9.4%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, New Zealand	5.1	6.8	4.2	2.8
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 9.4% percent of computers in New Zealand encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 2.8 of every 1,000 unique computers scanned in New Zealand in 4Q14 (a CCM score of 2.8, compared to the 4Q14 worldwide CCM of 5.9). 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.

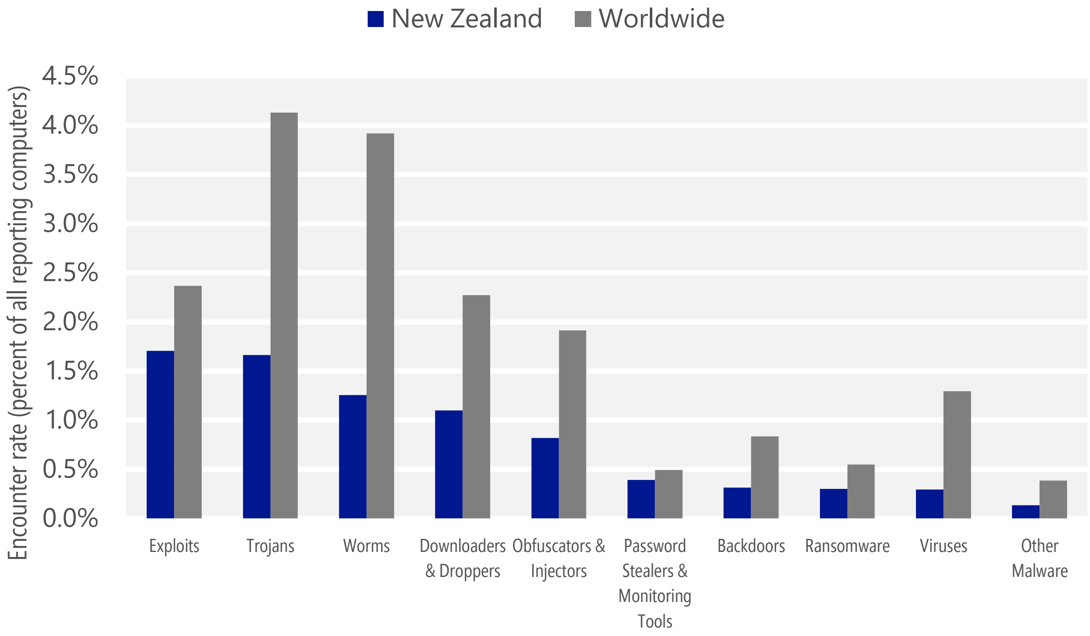
Malware encounter and infection rate trends in New Zealand and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

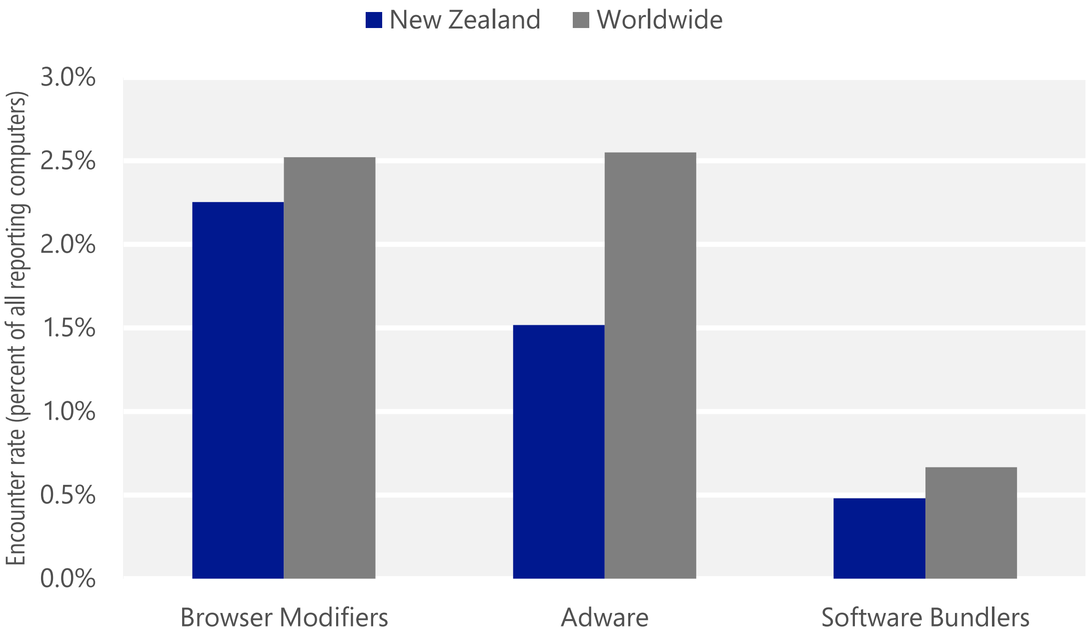
Malware encountered in New Zealand in 4Q14, by category



- The most common malware category in New Zealand in 4Q14 was Exploits. It was encountered by 1.7 percent of all computers there, down from 2.5 percent in 3Q14.
- The second most common malware category in New Zealand in 4Q14 was Trojans. It was encountered by 1.7 percent of all computers there, down from 2.0 percent in 3Q14.
- The third most common malware category in New Zealand in 4Q14 was Worms, which was encountered by 1.3 percent of all computers there, down from 1.5 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in New Zealand in 4Q14, by category



- The most common unwanted software category in New Zealand in 4Q14 was Browser Modifiers. It was encountered by 2.3 percent of all computers there, down from 3.8 percent in 3Q14.
- The second most common unwanted software category in New Zealand in 4Q14 was Adware. It was encountered by 1.5 percent of all computers there, up from 0.6 percent in 3Q14.
- The third most common unwanted software category in New Zealand in 4Q14 was Software Bundlers, which was encountered by 0.5 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in New Zealand in 4Q14

	Family	Most significant category	% of reporting computers
1	JS/Axpergle	Exploits	0.8%
2	Win32/Obfuscator	Obfuscators & Injectors	0.6%
3	JS/Fiexp	Exploits	0.5%
4	INF/Autorun	Obfuscators & Injectors	0.5%
5	Win32/Upatre	Downloaders & Droppers	0.2%
6	Win32/Tupym	Worms	0.2%
7	Win32/Vobfus	Worms	0.2%
8	HTML/Phish	Trojans	0.2%
9	ASX/Wimad	Downloaders & Droppers	0.2%
10	Win32/Lightmoon	Worms	0.2%

- The most common malware family encountered in New Zealand in 4Q14 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 New Zealand in 4Q14 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 New Zealand in 4Q14 was JS/Fiexp, which was encountered by 0.5 percent of reporting computers there. JS/Fiexp is a detection for the Fiesta exploit kit, which attempts to exploit Java, Adobe Flash Player, Adobe Reader, Silverlight, and Internet Explorer to install malware.
- The fourth most common malware family encountered in New Zealand in 4Q14 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 New Zealand in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	1.7%
2	Win32/Costmin	Adware	0.8%
3	Win32/Defaulttab	Browser Modifiers	0.6%
4	Win32/BetterSurf	Adware	0.5%
5	Win32/Gofileexpress	Software Bundlers	0.3%

- The most common unwanted software family encountered in New Zealand in 4Q14 was Win32/Couponruc, which was encountered by 1.7 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 New Zealand in 4Q14 was Win32/Costmin, which was encountered by 0.8 percent of reporting computers there. Win32/Costmin is an adware family that installs itself as a browser extension for Internet Explorer, Mozilla Firefox, and Google Chrome, and displays advertisements as the user browses the Internet.
- The third most common unwanted software family encountered in New Zealand in 4Q14 was Win32/Defaulttab, which was encountered by 0.6 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.

Top threat families by infection rate

The most common malware families by infection rate in New Zealand in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Tupym	Worms	0.5
2	Win32/Vobfus	Worms	0.5
3	Win32/Brontok	Worms	0.3
4	Win32/Zbot	Password Stealers & Monitoring Tools	0.2
5	Win32/Sality	Viruses	0.2
6	Win32/Sefnit	Trojans	0.1
7	JS/Miuref	Trojans	0.1
8	VBS/Jenxcus	Worms	0.1
9	Win32/Alureon	Trojans	0.1
10	Win32/Wysotot	Trojans	0.1

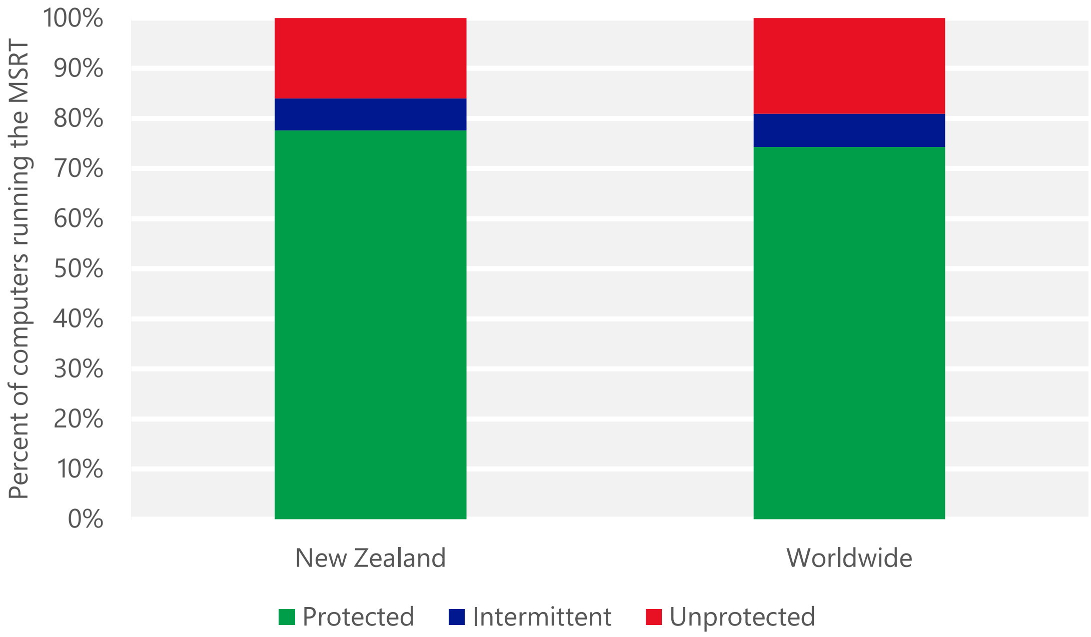
- The most common threat family infecting computers in New Zealand in 4Q14 was Win32/Tupym, which was detected and removed from 0.5 of every 1,000 unique computers scanned by the MSRT. Win32/Tupym is a worm that copies itself to the system folder of the affected computer, and attempts to contact remote hosts.
- The second most common threat family infecting computers in New Zealand in 4Q14 was Win32/Vobfus, which was detected and removed from 0.5 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.
- The third most common threat family infecting computers in New Zealand in 4Q14 was Win32/Brontok, which was detected and removed from 0.3 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 New Zealand in 4Q14 was Win32/Zbot, which was detected and removed from 0.2 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.

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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.07 drive-by download URLs for every 1,000 URLs hosted in New Zealand, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.07 drive-by download URLs for every 1,000 URLs hosted in New Zealand, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in New Zealand and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, New Zealand	0.07	0.07
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Nicaragua

The statistics presented here are generated by Microsoft security programs and services running on computers in Nicaragua in 4Q14 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 succeds 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

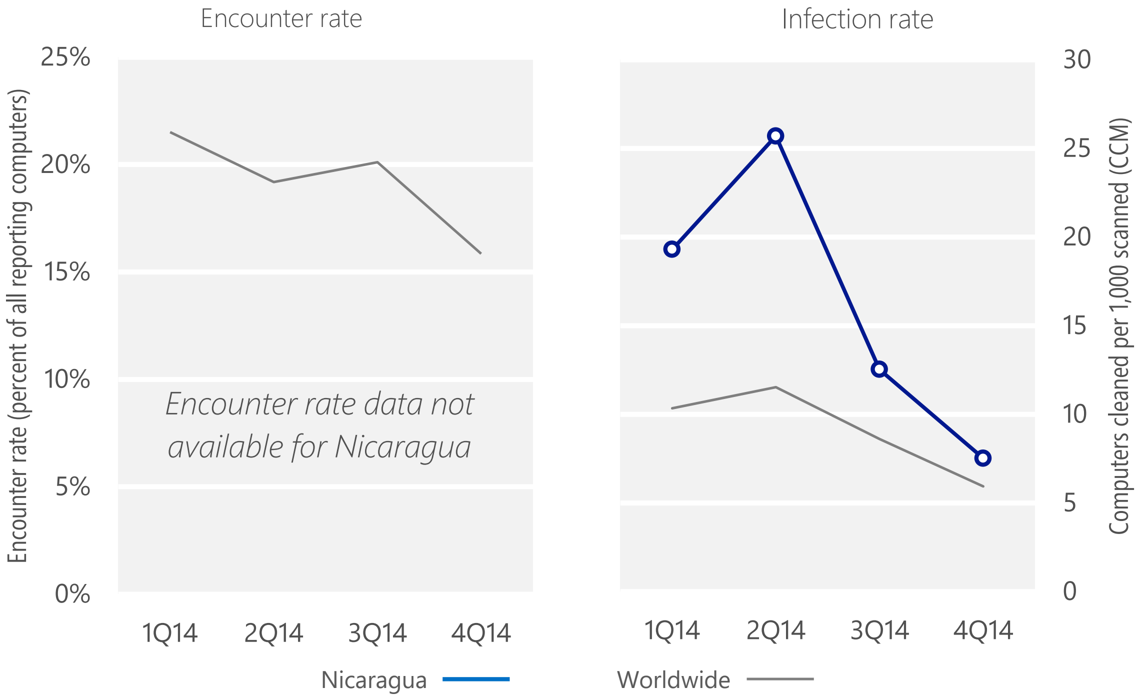
Metric	**1Q14**	**2Q14**	**3Q14**	**4Q14**
Encounter rate, Nicaragua	N/A	N/A	N/A	N/A
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Nicaragua	19.3	25.7	12.5	7.5
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, the MSRT detected and removed malware from 7.5 of every 1,000 unique computers scanned in Nicaragua in 4Q14 (a CCM score of 7.5, compared to the 4Q14 worldwide CCM of 5.9). 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 18* 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 4Q14

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	2.4
2	Win32/Yeltminky	Worms	1.4
3	Win32/Sality	Viruses	0.7
4	Win32/Brontok	Worms	0.6
5	MSIL/Spacekito	Trojans	0.4
6	Win32/Sefnit	Trojans	0.4
7	Win32/Nuqel	Worms	0.2
8	MSIL/Bladabindi	Backdoors	0.2
9	Win32/Alureon	Trojans	0.2
10	Win32/Dorkbot	Worms	0.2

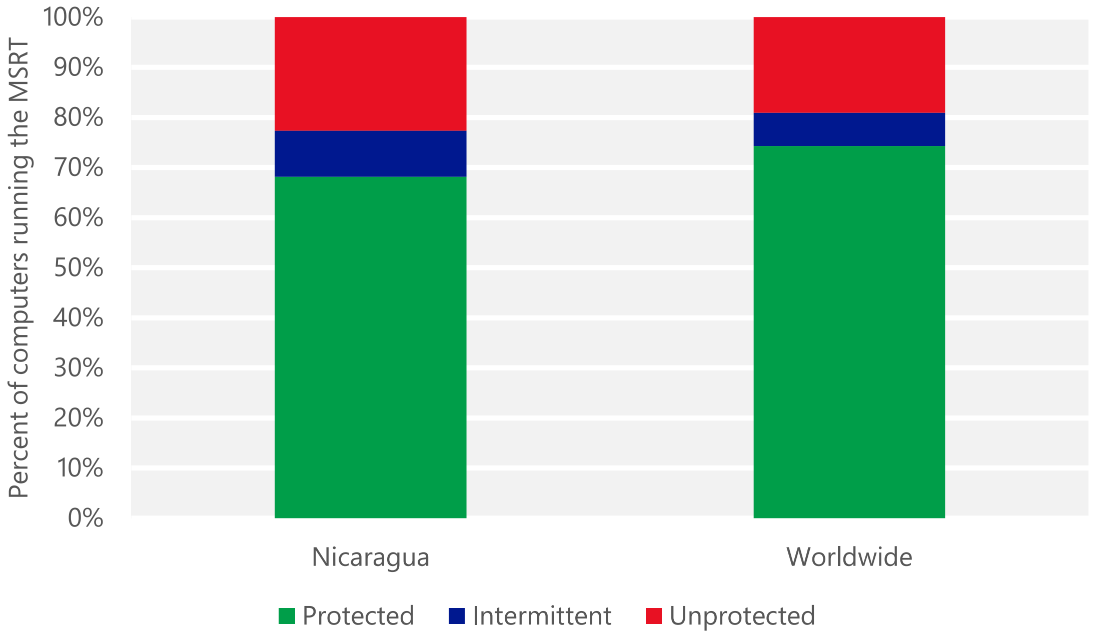
- The most common threat family infecting computers in Nicaragua in 4Q14 was VBS/Jenxcus, which was detected and removed from 2.4 of every 1,000 unique computers scanned by the MSRT. VBS/Jenxcus is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Nicaragua in 4Q14 was Win32/Yeltminky, which was detected and removed from 1.4 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 third most common threat family infecting computers in Nicaragua in 4Q14 was Win32/Sality, which was detected and removed from 0.7 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 Nicaragua in 4Q14 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.

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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.01 drive-by download URLs for every 1,000 URLs hosted in Nicaragua, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.34 drive-by download URLs for every 1,000 URLs hosted in Nicaragua, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Nicaragua and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Nicaragua	0.01	0.34
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Nigeria

The statistics presented here are generated by Microsoft security programs and services running on computers in Nigeria in 4Q14 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 succeds 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

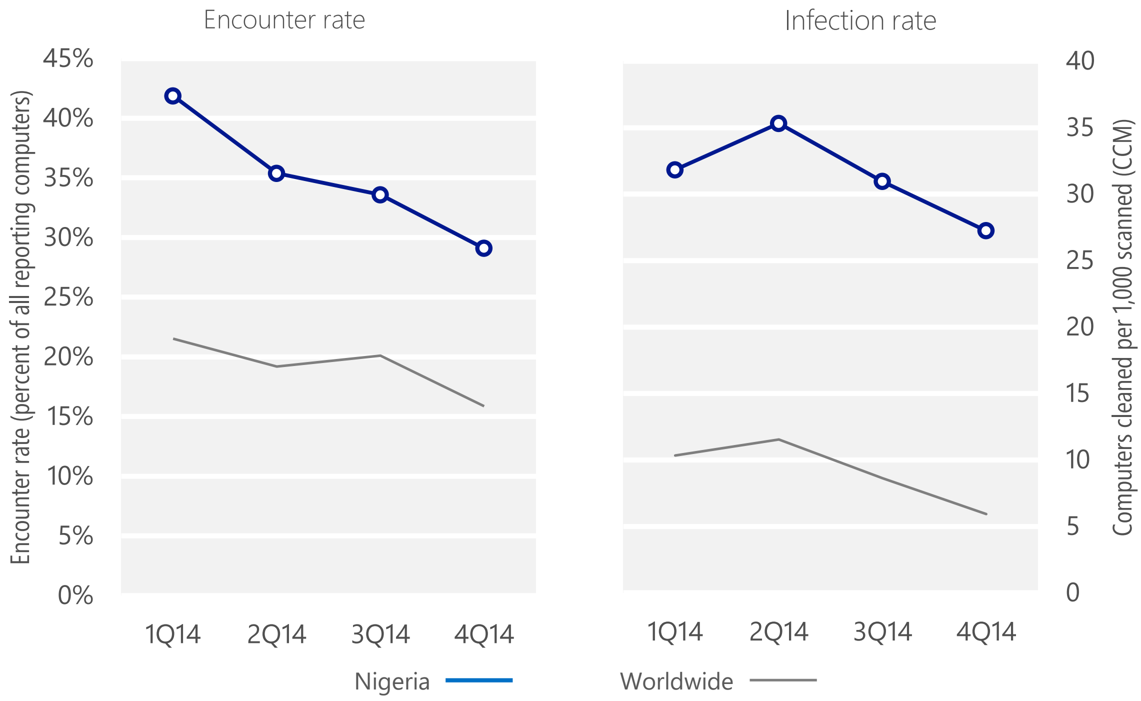
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Nigeria	41.9%	35.4%	33.6%	29.1%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Nigeria	31.8	35.3	30.9	27.2
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 29.1% percent of computers in Nigeria encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 27.2 of every 1,000 unique computers scanned in Nigeria in 4Q14 (a CCM score of 27.2, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Nigeria over the last four quarters, compared to the world as a whole.

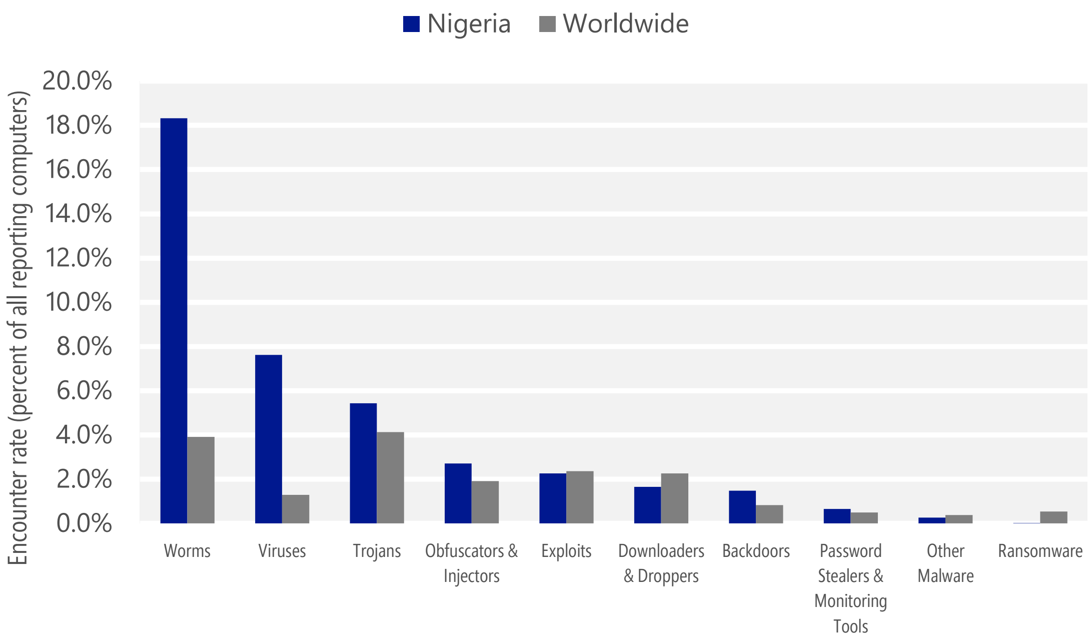
Malware encounter and infection rate trends in Nigeria and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

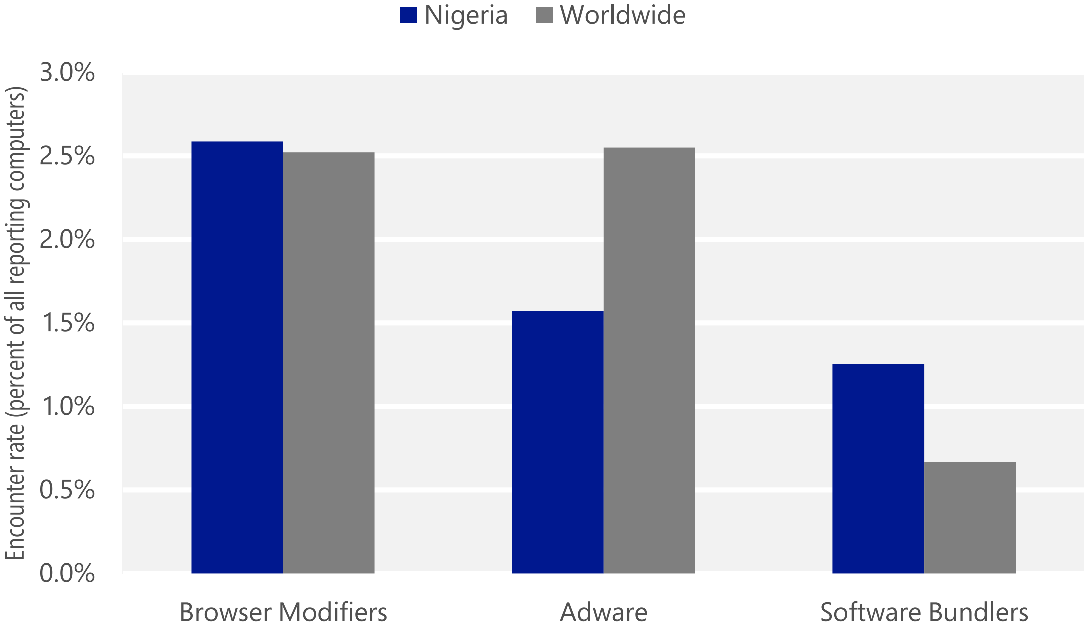
Malware encountered in Nigeria in 4Q14, by category



- The most common malware category in Nigeria in 4Q14 was Worms. It was encountered by 18.3 percent of all computers there, down from 20.7 percent in 3Q14.
- The second most common malware category in Nigeria in 4Q14 was Viruses. It was encountered by 7.6 percent of all computers there, down from 9.2 percent in 3Q14.
- The third most common malware category in Nigeria in 4Q14 was Trojans, which was encountered by 5.4 percent of all computers there, down from 7.2 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Nigeria in 4Q14, by category



- The most common unwanted software category in Nigeria in 4Q14 was Browser Modifiers. It was encountered by 2.6 percent of all computers there, down from 3.6 percent in 3Q14.
- The second most common unwanted software category in Nigeria in 4Q14 was Adware. It was encountered by 1.6 percent of all computers there, up from 0.9 percent in 3Q14.
- The third most common unwanted software category in Nigeria in 4Q14 was Software Bundlers, which was encountered by 1.3 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Nigeria in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Gamarue	Worms	7.8%
2	VBS/Jenxcus	Worms	7.1%
3	Win32/Grenam	Viruses	4.7%
4	Win32/Copali	Worms	3.3%
5	INF/Autorun	Obfuscators & Injectors	3.2%
6	Win32/Virut	Viruses	1.9%
7	Win32/Ramnit	Trojans	1.7%
8	Win32/CplLnk	Exploits	1.7%
9	Win32/Sality	Viruses	1.4%
10	Win32/Ippedo	Worms	1.2%

- The most common malware family encountered in Nigeria in 4Q14 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 Nigeria in 4Q14 was VBS/Jenxcus, which was encountered by 7.1 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 Nigeria in 4Q14 was Win32/Grenam, which was encountered by 4.7 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 4Q14 was Win32/Copali, which was encountered by 3.3 percent of reporting computers there. Win32/Copali is a family of worms that can download other malware, including PWS:Win32/Zbot. They spread through infected network and removable drives.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Nigeria in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	1.8%
2	Win32/Gofileexpress	Software Bundlers	1.0%
3	Win32/Defaulttab	Browser Modifiers	0.9%
4	Win32/Costmin	Adware	0.7%

- The most common unwanted software family encountered in Nigeria in 4Q14 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 Nigeria in 4Q14 was Win32/Gofileexpress, which was encountered by 1.0 percent of reporting computers there. Win32/Gofileexpress is a software bundler that installs other unwanted software, including Adware:Win32/Lollipop and Adware:Win32/CostMin.
- The third most common unwanted software family encountered in Nigeria in 4Q14 was Win32/Defaulttab, which was encountered by 0.9 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.

Top threat families by infection rate

The most common malware families by infection rate in Nigeria in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Gamarue	Worms	10.7
2	VBS/Jenxcus	Worms	10.1
3	Win32/Ramnit	Trojans	2.0
4	Win32/Sality	Viruses	1.8
5	Win32/Vobfus	Worms	1.0
6	Win32/Chir	Viruses	0.9
7	Win32/Dorkbot	Worms	0.6
8	Win32/Zbot	Password Stealers & Monitoring Tools	0.5
9	MSIL/Bladabindi	Backdoors	0.4
10	Win32/Tupym	Worms	0.4

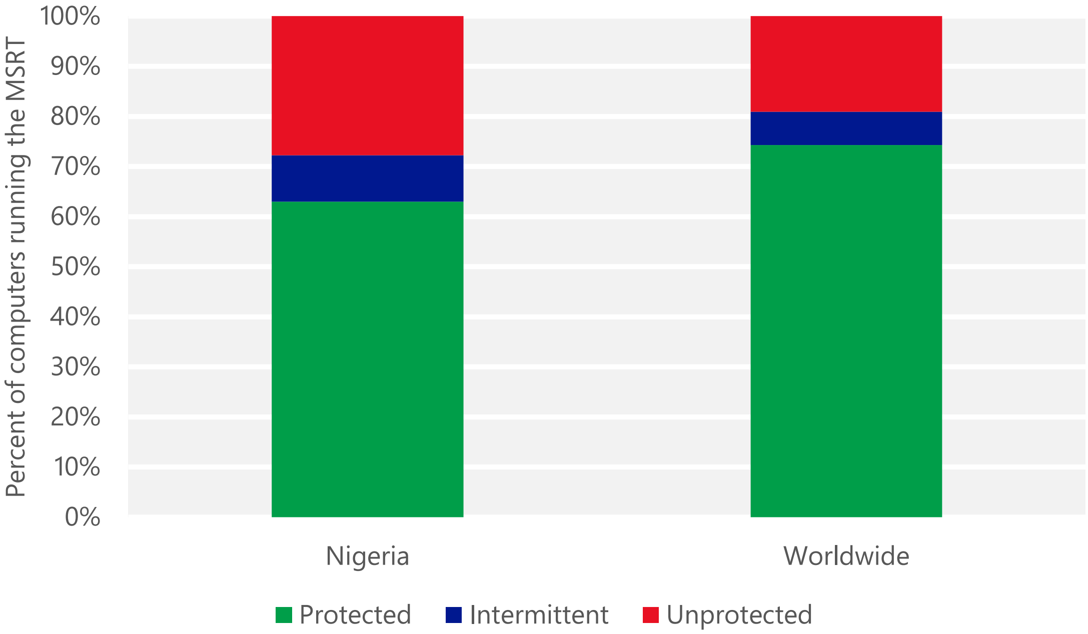
- The most common threat family infecting computers in Nigeria in 4Q14 was Win32/Gamarue, which was detected and removed from 10.7 of every 1,000 unique computers scanned by the MSRT. Win32/Gamarue is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The second most common threat family infecting computers in Nigeria in 4Q14 was VBS/Jenxcus, which was detected and removed from 10.1 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 Nigeria in 4Q14 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.
- The fourth most common threat family infecting computers in Nigeria in 4Q14 was Win32/Sality, which was detected and removed from 1.8 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.

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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.31 drive-by download URLs for every 1,000 URLs hosted in Nigeria, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.25 drive-by download URLs for every 1,000 URLs hosted in Nigeria, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Nigeria and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Nigeria	0.31	0.25
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Norway

The statistics presented here are generated by Microsoft security programs and services running on computers in Norway in 4Q14 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 succeds 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

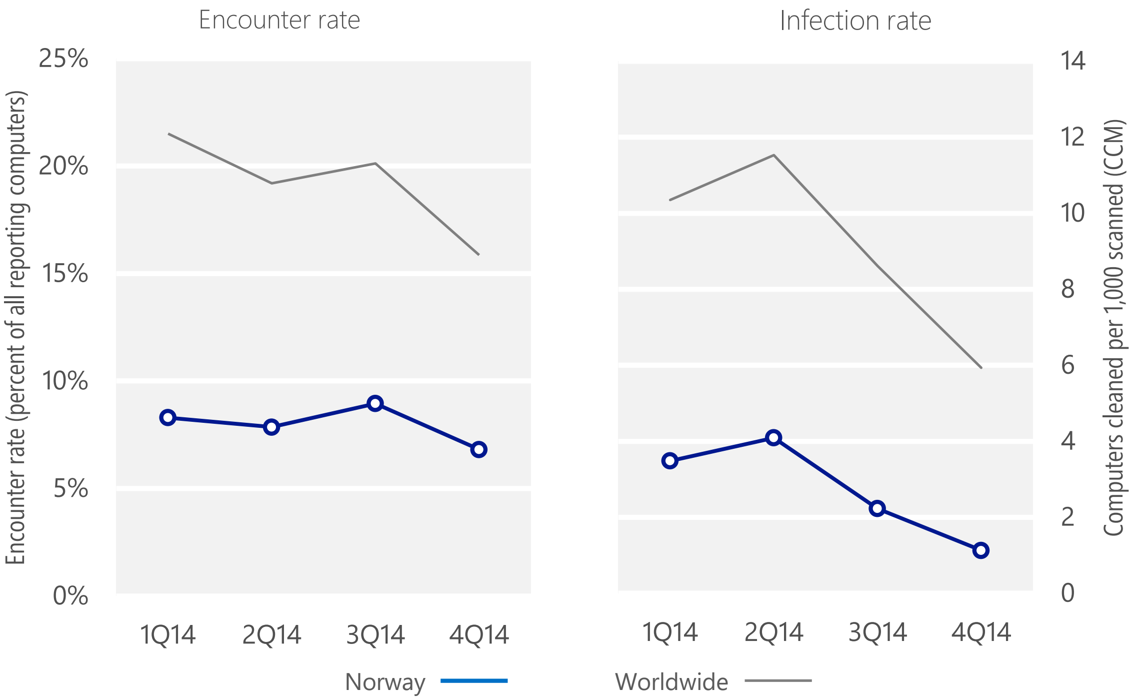
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Norway	8.3%	7.9%	9.0%	6.8%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Norway	3.5	4.1	2.2	1.1
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 6.8% percent of computers in Norway encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 1.1 of every 1,000 unique computers scanned in Norway in 4Q14 (a CCM score of 1.1, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Norway over the last four quarters, compared to the world as a whole.

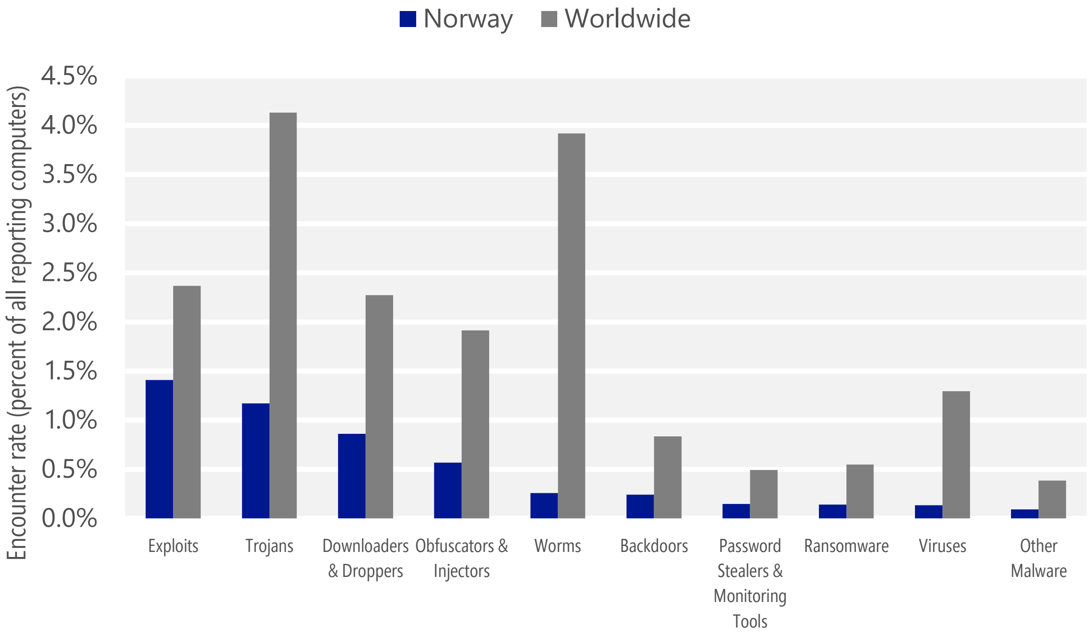
Malware encounter and infection rate trends in Norway and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

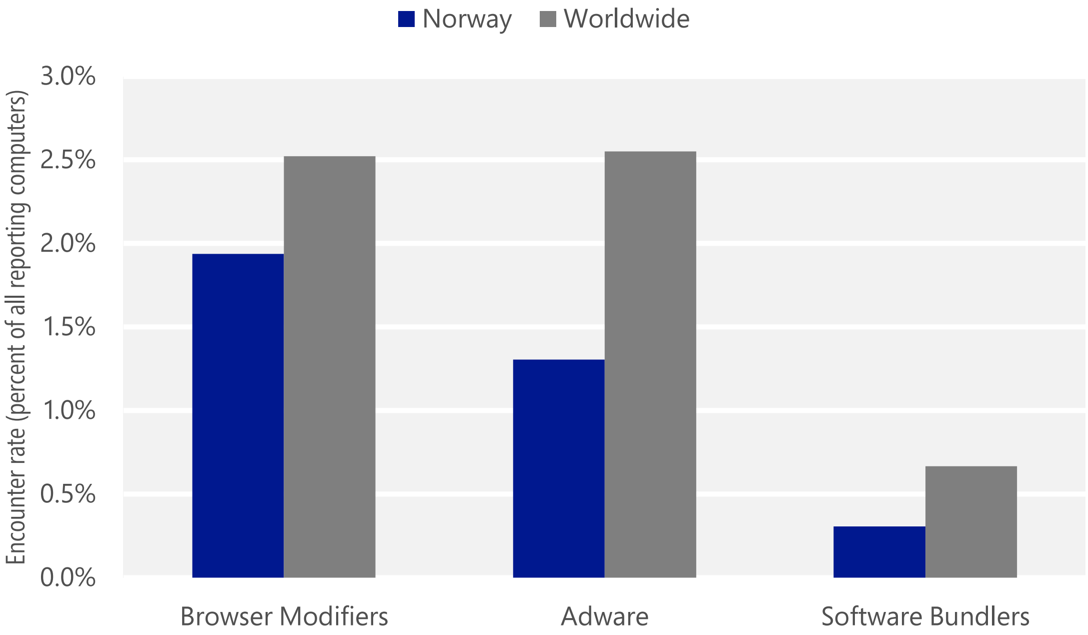
Malware encountered in Norway in 4Q14, by category



- The most common malware category in Norway in 4Q14 was Exploits. It was encountered by 1.4 percent of all computers there, down from 2.6 percent in 3Q14.
- The second most common malware category in Norway in 4Q14 was Trojans. It was encountered by 1.2 percent of all computers there, down from 1.6 percent in 3Q14.
- The third most common malware category in Norway in 4Q14 was Downloaders & Droppers, which was encountered by 0.9 percent of all computers there, down from 1.6 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Norway in 4Q14, by category



- The most common unwanted software category in Norway in 4Q14 was Browser Modifiers. It was encountered by 1.9 percent of all computers there, down from 3.2 percent in 3Q14.
- The second most common unwanted software category in Norway in 4Q14 was Adware. It was encountered by 1.3 percent of all computers there, up from 0.8 percent in 3Q14.
- The third most common unwanted software category in Norway in 4Q14 was Software Bundlers, which was encountered by 0.3 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Norway in 4Q14

	Family	Most significant category	% of reporting computers
1	JS/Axpergle	Exploits	0.7%
2	Win32/Obfuscator	Obfuscators & Injectors	0.5%
3	Win32/Anogre	Exploits	0.2%
4	Win32/Tugspay	Downloaders & Droppers	0.2%
5	Win32/Sanusra	Trojans	0.1%
6	ASX/Wimad	Downloaders & Droppers	0.1%
7	Java/CVE-2013-1488	Exploits	0.1%
8	Win32/Vatsics	Downloaders & Droppers	0.1%
9	JS/Faceliker	Trojans	0.1%
10	Java/Cve-2013-1489	Exploits	0.1%

- The most common malware family encountered in Norway in 4Q14 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 Norway in 4Q14 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 Norway in 4Q14 was Win32/Anogre, which was encountered by 0.2 percent of reporting computers there. Win32/Anogre is a threat that exploits a vulnerability addressed by Microsoft Security Bulletin MS11-087. This vulnerability can allow a hacker to install programs, view, change, or delete data or create new accounts with full administrative privileges.
- The fourth most common malware family encountered in Norway in 4Q14 was Win32/Tugspay, which was encountered by 0.2 percent of reporting computers there. Win32/Tugspay is a downloader that spreads by posing as an installer for legitimate software, such as a Java update, or through other malware. When installed, it downloads unwanted software to the computer.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Norway in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	1.7%
2	Win32/Costmin	Adware	0.6%
3	Win32/Defaulttab	Browser Modifiers	0.3%
4	Win32/BetterSurf	Adware	0.3%
5	Win32/Pennybee	Adware	0.2%

- The most common unwanted software family encountered in Norway in 4Q14 was Win32/Couponruc, which was encountered by 1.7 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 Norway in 4Q14 was Win32/Costmin, which was encountered by 0.6 percent of reporting computers there. Win32/Costmin is an adware family that installs itself as a browser extension for Internet Explorer, Mozilla Firefox, and Google Chrome, and displays advertisements as the user browses the Internet.
- The third most common unwanted software family encountered in Norway in 4Q14 was Win32/Defaulttab, which was encountered by 0.3 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.

Top threat families by infection rate

The most common malware families by infection rate in Norway in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Sefnit	Trojans	0.1
2	Win32/Alureon	Trojans	0.1
3	Win32/Wysotot	Trojans	0.1
4	Win32/Zbot	Password Stealers & Monitoring Tools	0.1
5	Win32/Sinowal	Password Stealers & Monitoring Tools	0.1
6	MSIL/Bladabindi	Backdoors	0.1
7	JS/Kilim	Trojans	<0.1
8	Win32/Carberp	Trojans	<0.1
9	VBS/Jenxcus	Worms	<0.1
10	Win32/Pushbot	Worms	<0.1

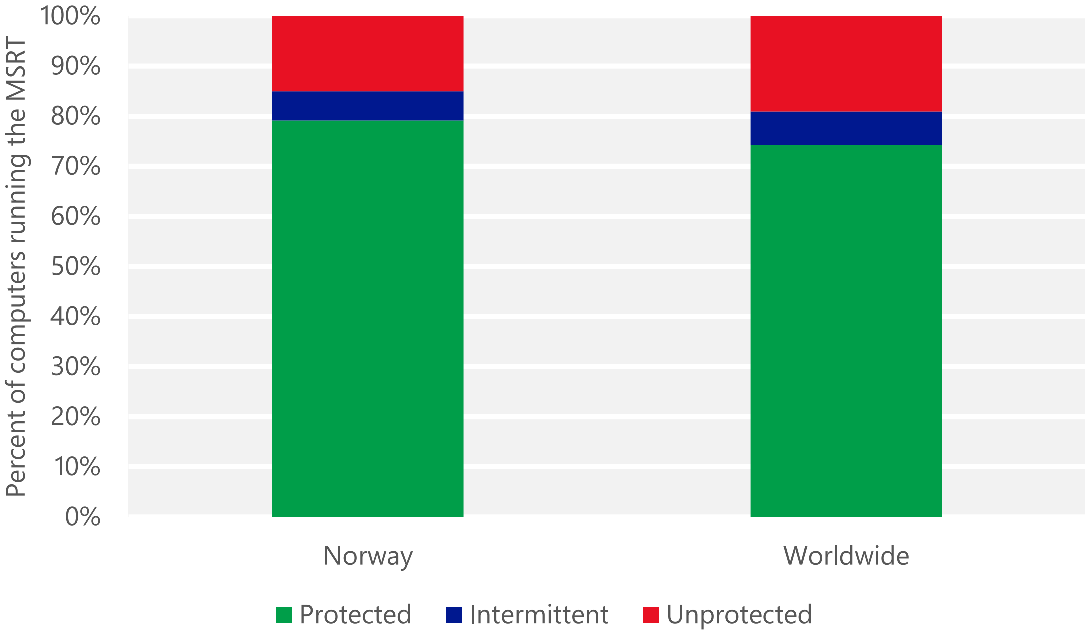
- The most common threat family infecting computers in Norway in 4Q14 was Win32/Sefnit, which was detected and removed from 0.1 of every 1,000 unique computers scanned by the MSRT. Win32/Sefnit is a family of trojans that can allow backdoor access, download files, and use the computer and Internet connection for click fraud. Some variants can monitor web browsers and hijack search results.
- The second most common threat family infecting computers in Norway in 4Q14 was Win32/Alureon, which was detected and removed from 0.1 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 third most common threat family infecting computers in Norway in 4Q14 was Win32/Wysotot, which was detected and removed from 0.1 of every 1,000 unique computers scanned by the MSRT. Win32/Wysotot is a threat that can change the start page of the user's web browser, and may download and install other files to the computer. It is installed by software bundlers that advertise free software or games.
- The fourth most common threat family infecting computers in Norway in 4Q14 was Win32/Zbot, which was detected and removed from 0.1 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.

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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.07 drive-by download URLs for every 1,000 URLs hosted in Norway, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.05 drive-by download URLs for every 1,000 URLs hosted in Norway, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Norway and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Norway	0.07	0.05
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Oman

The statistics presented here are generated by Microsoft security programs and services running on computers in Oman in 4Q14 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 succeds 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

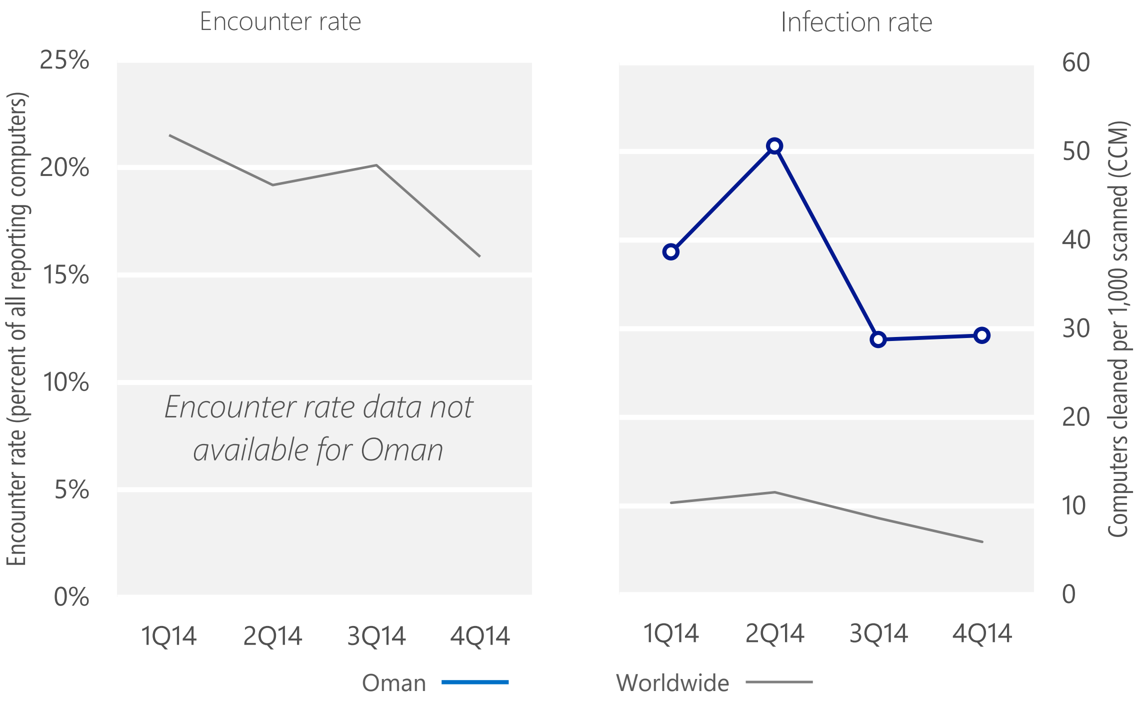
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Oman	N/A	N/A	N/A	N/A
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Oman	38.6	50.6	28.8	29.2
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, the MSRT detected and removed malware from 29.2 of every 1,000 unique computers scanned in Oman in 4Q14 (a CCM score of 29.2, compared to the 4Q14 worldwide CCM of 5.9). 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 18* 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.

Top threat families by infection rate

The most common malware families by infection rate in Oman in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	14.7
2	Win32/Gamarue	Worms	3.1
3	Win32/Sality	Viruses	2.3
4	Win32/Vobfus	Worms	2.3
5	Win32/Dorkbot	Worms	2.0
6	MSIL/Bladabindi	Backdoors	1.5
7	Win32/Ramnit	Trojans	1.4
8	Win32/Nuqel	Worms	1.1
9	Win32/Lethic	Trojans	0.8
10	Win32/Folstart	Worms	0.8

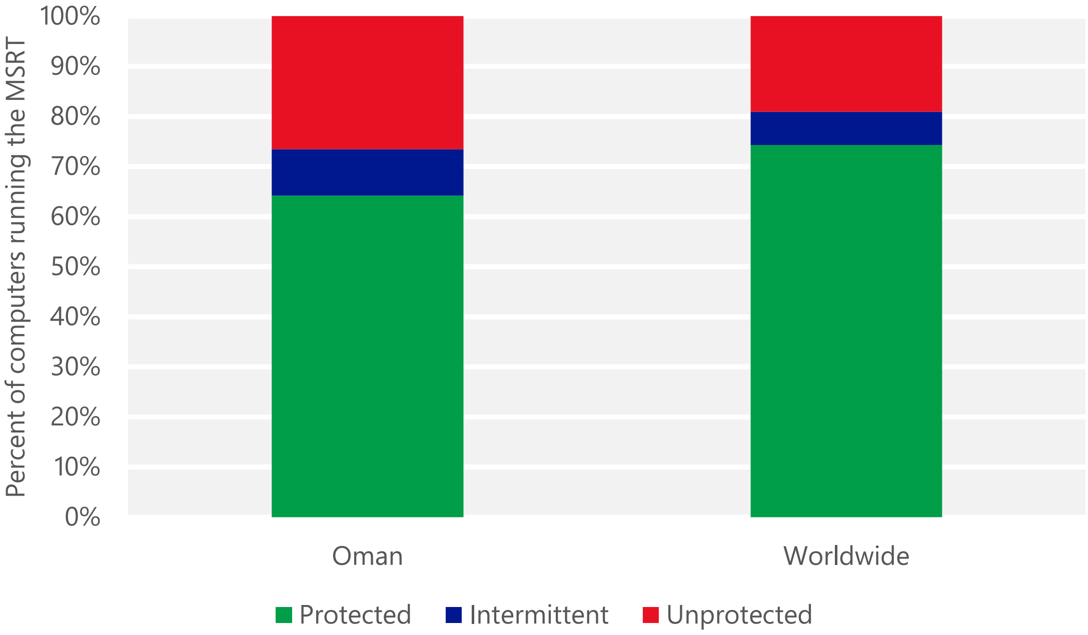
- The most common threat family infecting computers in Oman in 4Q14 was VBS/Jenxcus, which was detected and removed from 14.7 of every 1,000 unique computers scanned by the MSRT. VBS/Jenxcus is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Oman in 4Q14 was Win32/Gamarue, which was detected and removed from 3.1 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 Oman in 4Q14 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.
- The fourth most common threat family infecting computers in Oman in 4Q14 was Win32/Vobfus, which was detected and removed from 2.3 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 Oman and worldwide protected by real-time security software in 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.00 drive-by download URLs for every 1,000 URLs hosted in Oman, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.00 drive-by download URLs for every 1,000 URLs hosted in Oman, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Oman and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Oman	0.00	0.00
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Pakistan

The statistics presented here are generated by Microsoft security programs and services running on computers in Pakistan in 4Q14 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 succeds 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

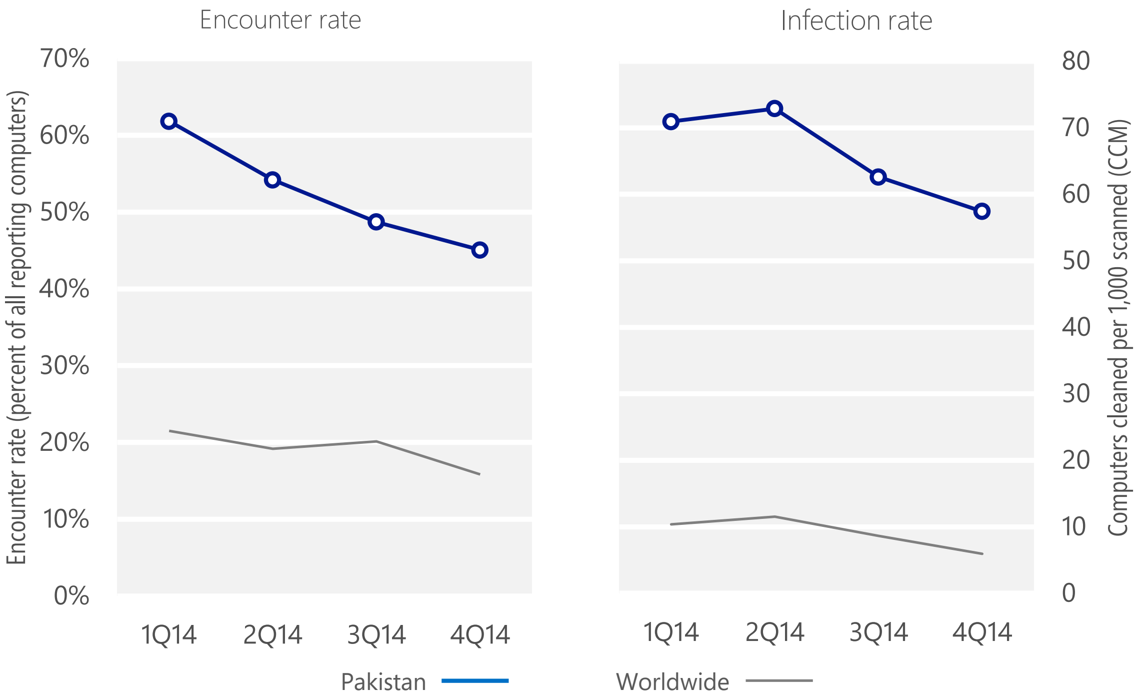
Metric	**1Q14**	**2Q14**	**3Q14**	**4Q14**
Encounter rate, Pakistan	61.8%	54.2%	48.7%	45.1%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Pakistan	70.9	72.9	62.6	57.4
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 45.1% percent of computers in Pakistan encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 57.4 of every 1,000 unique computers scanned in Pakistan in 4Q14 (a CCM score of 57.4, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Pakistan over the last four quarters, compared to the world as a whole.

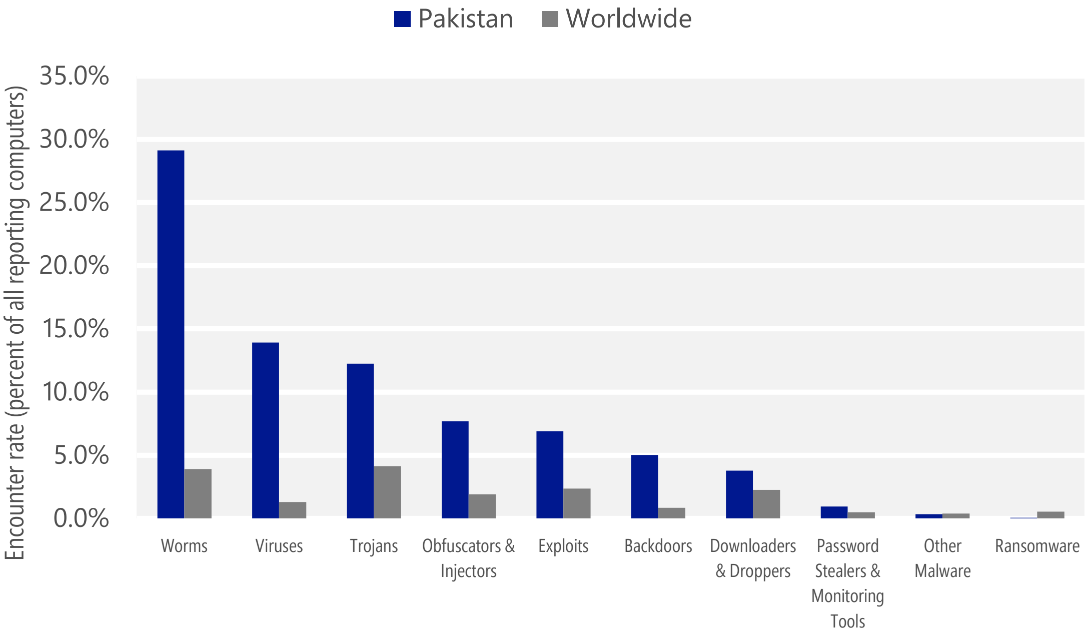
Malware encounter and infection rate trends in Pakistan and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

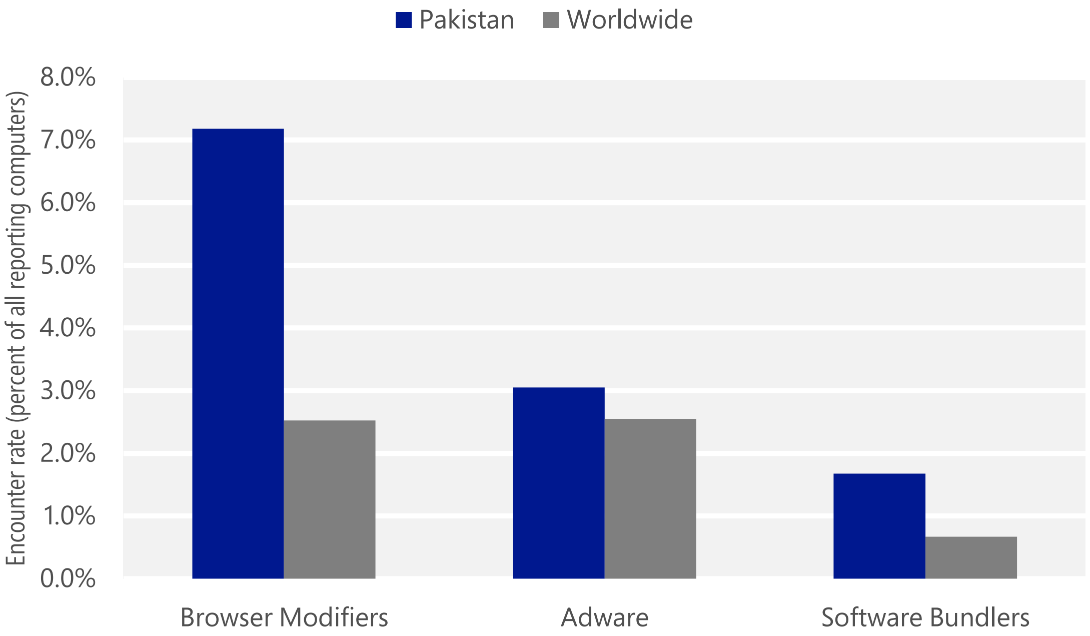
Malware encountered in Pakistan in 4Q14, by category



- The most common malware category in Pakistan in 4Q14 was Worms. It was encountered by 29.1 percent of all computers there, down from 30.2 percent in 3Q14.
- The second most common malware category in Pakistan in 4Q14 was Viruses. It was encountered by 13.9 percent of all computers there, down from 15.7 percent in 3Q14.
- The third most common malware category in Pakistan in 4Q14 was Trojans, which was encountered by 12.3 percent of all computers there, down from 15.0 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Pakistan in 4Q14, by category



- The most common unwanted software category in Pakistan in 4Q14 was Browser Modifiers. It was encountered by 7.2 percent of all computers there, down from 7.6 percent in 3Q14.
- The second most common unwanted software category in Pakistan in 4Q14 was Adware. It was encountered by 3.1 percent of all computers there, up from 1.7 percent in 3Q14.
- The third most common unwanted software category in Pakistan in 4Q14 was Software Bundlers, which was encountered by 1.7 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Pakistan in 4Q14

	Family	Most significant category	% of reporting computers
1	INF/Autorun	Obfuscators & Injectors	12.7%
2	VBS/Jenxcus	Worms	12.3%
3	Win32/Gamarue	Worms	11.0%
4	Win32/Sality	Viruses	7.9%
5	Win32/Virut	Viruses	6.3%
6	Win32/Ramnit	Trojans	6.0%
7	Win32/CplLnk	Exploits	5.5%
8	Win32/Chir	Viruses	4.3%
9	Win32/Tupym	Worms	3.5%
10	Win32/Bifrose	Backdoors	3.5%

- The most common malware family encountered in Pakistan in 4Q14 was INF/Autorun, which was encountered by 12.7 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 second most common malware family encountered in Pakistan in 4Q14 was VBS/Jenxcus, which was encountered by 12.3 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 Pakistan in 4Q14 was Win32/Gamarue, which was encountered by 11.0 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 fourth most common malware family encountered in Pakistan in 4Q14 was Win32/Sality, which was encountered by 7.9 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 Pakistan in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	5.9%
2	Win32/Defaulttab	Browser Modifiers	1.5%
3	Win32/BetterSurf	Adware	1.5%
4	Win32/Gofileexpress	Software Bundlers	1.3%
5	Win32/Costmin	Adware	1.2%

- The most common unwanted software family encountered in Pakistan in 4Q14 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 Pakistan in 4Q14 was Win32/Defaulttab, which was encountered by 1.5 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.
- The third most common unwanted software family encountered in Pakistan in 4Q14 was Win32/BetterSurf, which was encountered by 1.5 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.

Top threat families by infection rate

The most common malware families by infection rate in Pakistan in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Sality	Viruses	17.7
2	VBS/Jenxcus	Worms	15.1
3	Win32/Gamarue	Worms	11.1
4	Win32/Chir	Viruses	8.3
5	Win32/Tupym	Worms	5.2
6	Win32/Ramnit	Trojans	4.8
7	Win32/Nuqel	Worms	2.4
8	Win32/Virut	Viruses	1.6
9	Win32/Pramro	Trojans	1.2
10	Win32/Parite	Viruses	1.0

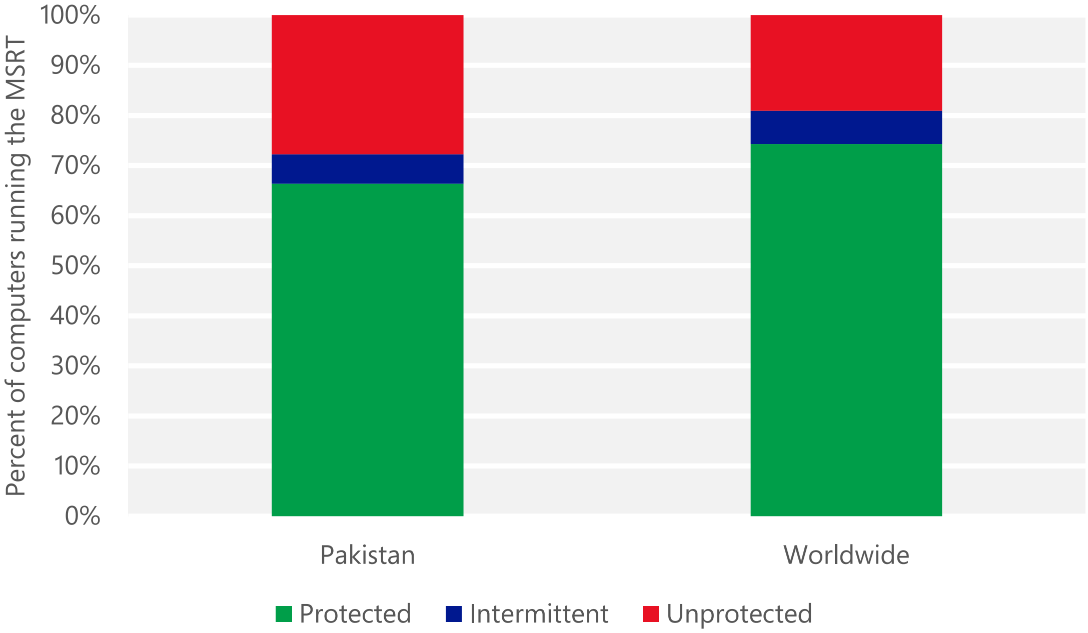
- The most common threat family infecting computers in Pakistan in 4Q14 was Win32/Sality, which was detected and removed from 17.7 of every 1,000 unique computers scanned by the MSRT. Win32/Sality is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The second most common threat family infecting computers in Pakistan in 4Q14 was VBS/Jenxcus, which was detected and removed from 15.1 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 Pakistan in 4Q14 was Win32/Gamarue, which was detected and removed from 11.1 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 fourth most common threat family infecting computers in Pakistan in 4Q14 was Win32/Chir, which was detected and removed from 8.3 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.

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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.16 drive-by download URLs for every 1,000 URLs hosted in Pakistan, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.06 drive-by download URLs for every 1,000 URLs hosted in Pakistan, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Pakistan and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Pakistan	0.16	0.06
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

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 4Q14 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 succeds 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

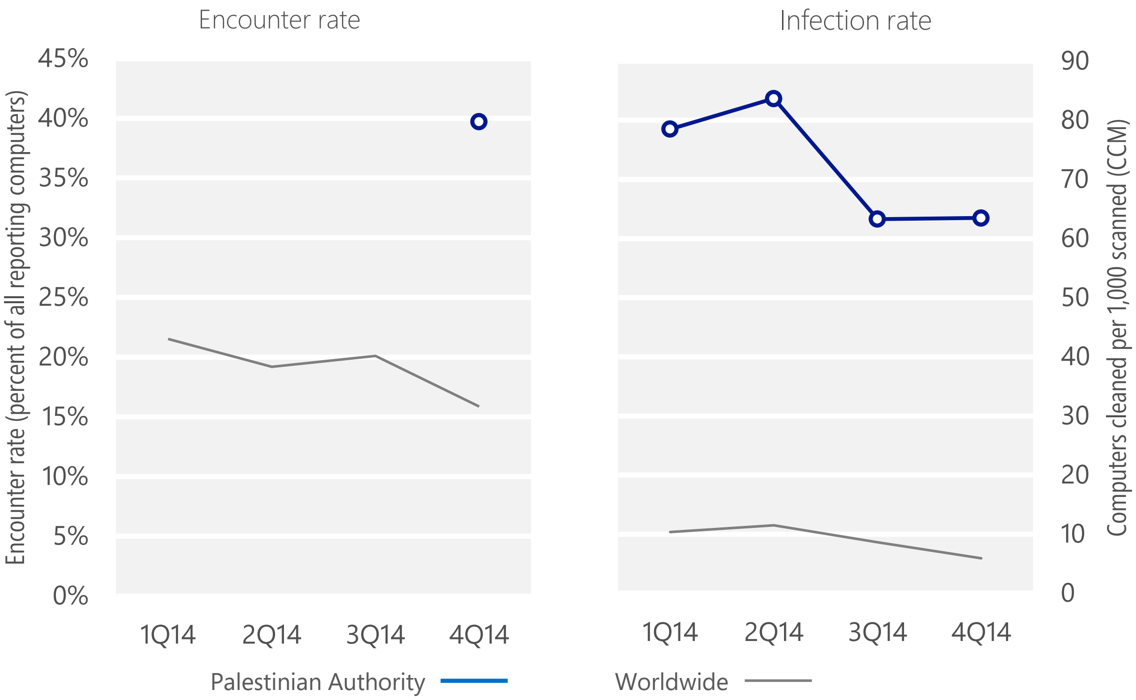
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Palestinian Authority	N/A	N/A	N/A	39.7%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Palestinian Authority	78.5	83.7	63.3	63.5
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 39.7% percent of computers in the Palestinian territories encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 63.5 of every 1,000 unique computers scanned in the Palestinian territories in 4Q14 (a CCM score of 63.5, compared to the 4Q14 worldwide CCM of 5.9). 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.

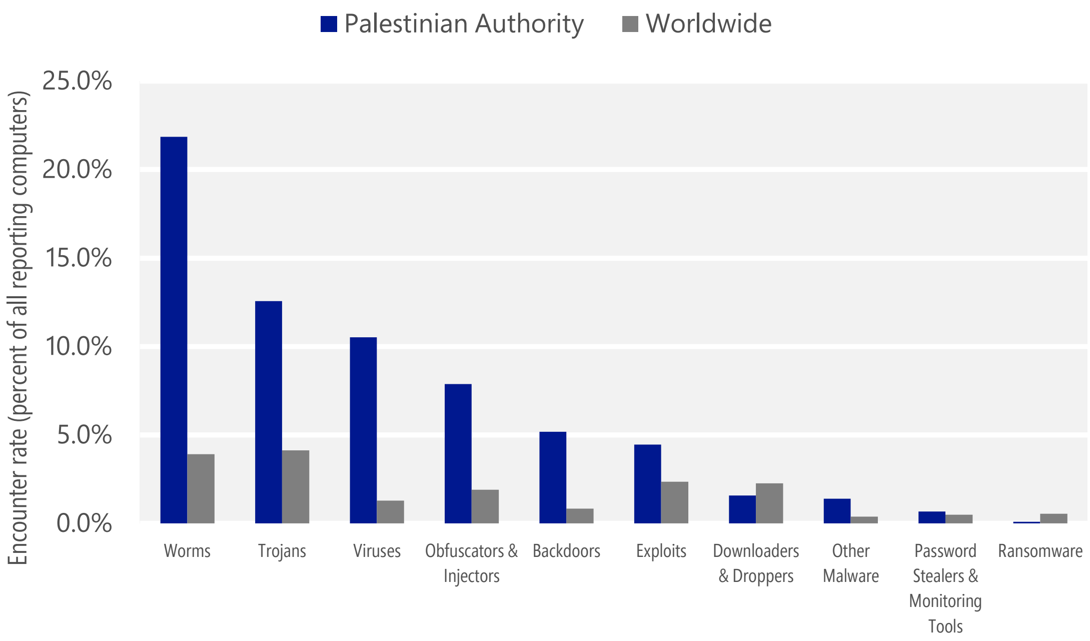
Malware encounter and infection rate trends in the Palestinian territories and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

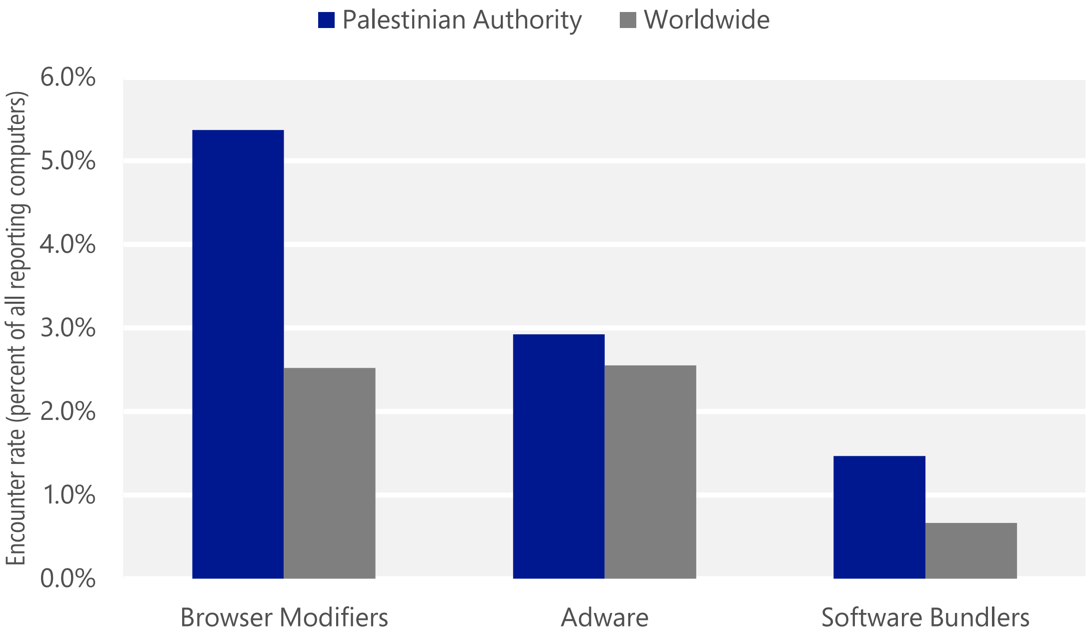
Malware encountered in the Palestinian territories in 4Q14, by category



- The most common malware category in the Palestinian territories in 4Q14 was Worms. It was encountered by 21.9 percent of all computers there, up from N/A percent in 3Q14.
- The second most common malware category in the Palestinian territories in 4Q14 was Trojans. It was encountered by 12.6 percent of all computers there, up from N/A percent in 3Q14.
- The third most common malware category in the Palestinian territories in 4Q14 was Viruses, which was encountered by 10.5 percent of all computers there, up from N/A percent in 3Q14.

Unwanted software categories

Unwanted software encountered in the Palestinian territories in 4Q14, by category



- The most common unwanted software category in the Palestinian territories in 4Q14 was Browser Modifiers. It was encountered by 5.4 percent of all computers there, up from N/A percent in 3Q14.
- The second most common unwanted software category in the Palestinian territories in 4Q14 was Adware. It was encountered by 2.9 percent of all computers there, up from N/A percent in 3Q14.
- The third most common unwanted software category in the Palestinian territories in 4Q14 was Software Bundlers, which was encountered by 1.5 percent of all computers there, up from N/A percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in the Palestinian territories in 4Q14

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	13.8%
2	INF/Autorun	Obfuscators & Injectors	8.0%
3	Win32/Sality	Viruses	6.6%
4	Win32/Gamarue	Worms	4.4%
5	Win32/Virut	Viruses	4.1%
6	Win32/CplLnk	Exploits	3.7%
7	Win32/Sulunch	Trojans	3.6%
8	MSIL/Bladabindi	Backdoors	3.4%
9	Win32/Ramnit	Trojans	3.2%
10	Win32/Nuqel	Worms	2.3%

- The most common malware family encountered in the Palestinian territories in 4Q14 was VBS/Jenxcus, which was encountered by 13.8 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 Palestinian territories in 4Q14 was INF/Autorun, which was encountered by 8.0 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 the Palestinian territories in 4Q14 was Win32/Sality, which was encountered by 6.6 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.
- The fourth most common malware family encountered in the Palestinian territories in 4Q14 was Win32/Gamarue, which was encountered by 4.4 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.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in the Palestinian territories in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	4.4%
2	Win32/BetterSurf	Adware	1.6%
3	Win32/Costmin	Adware	1.1%
4	Win32/Gofileexpress	Software Bundlers	1.1%
5	Win32/Defaulttab	Browser Modifiers	1.1%

- The most common unwanted software family encountered in the Palestinian territories in 4Q14 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 the Palestinian territories in 4Q14 was Win32/BetterSurf, which was encountered by 1.6 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.
- The third most common unwanted software family encountered in the Palestinian territories in 4Q14 was Win32/Costmin, which was encountered by 1.1 percent of reporting computers there. Win32/Costmin is an adware family that installs itself as a browser extension for Internet Explorer, Mozilla Firefox, and Google Chrome, and displays advertisements as the user browses the Internet.

Top threat families by infection rate

The most common malware families by infection rate in the Palestinian territories in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	22.8
2	Win32/Sality	Viruses	21.2
3	Win32/Gamarue	Worms	5.2
4	MSIL/Bladabindi	Backdoors	5.2
5	Win32/Ramnit	Trojans	4.4
6	Win32/Nuqel	Worms	3.5
7	Win32/Pramro	Trojans	3.0
8	Win32/Nitol	Other Malware	2.5
9	Win32/Folstart	Worms	2.3
10	Win32/Vobfus	Worms	1.9

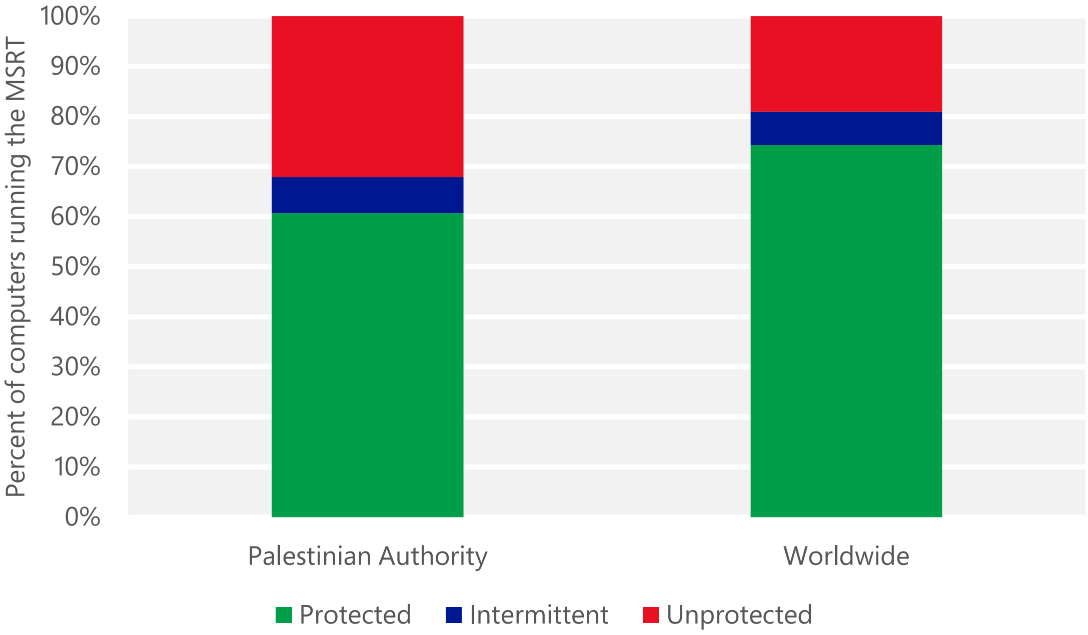
- The most common threat family infecting computers in the Palestinian territories in 4Q14 was VBS/Jenxcus, which was detected and removed from 22.8 of every 1,000 unique computers scanned by the MSRT. VBS/Jenxcus is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in the Palestinian territories in 4Q14 was Win32/Sality, which was detected and removed from 21.2 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.
- The third most common threat family infecting computers in the Palestinian territories in 4Q14 was Win32/Gamarue, which was detected and removed from 5.2 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 the Palestinian territories in 4Q14 was MSIL/Bladabindi, which was detected and removed from 5.2 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 the Palestinian territories and worldwide protected by real-time security software in 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.09 drive-by download URLs for every 1,000 URLs hosted in the Palestinian territories, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.06 drive-by download URLs for every 1,000 URLs hosted in the Palestinian territories, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in the Palestinian territories and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Palestinian Authority	0.09	0.06
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Panama

The statistics presented here are generated by Microsoft security programs and services running on computers in Panama in 4Q14 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 succeds 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

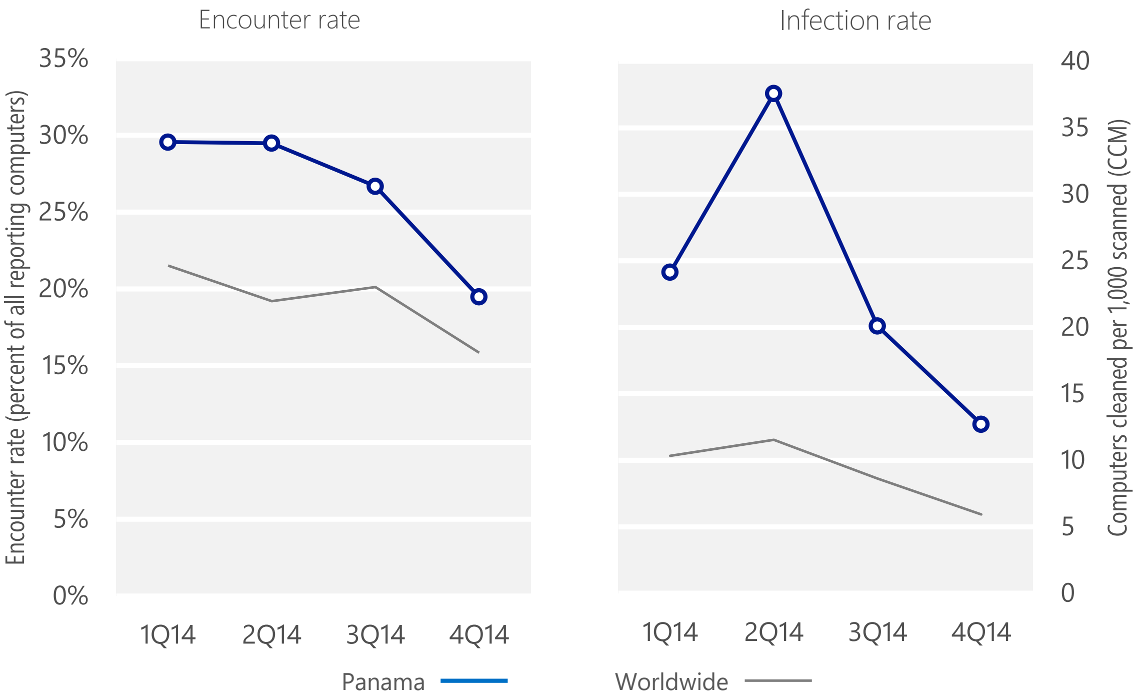
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Panama	29.6%	29.5%	26.7%	19.5%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Panama	24.1	37.6	20.1	12.7
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 19.5% percent of computers in Panama encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 12.7 of every 1,000 unique computers scanned in Panama in 4Q14 (a CCM score of 12.7, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Panama over the last four quarters, compared to the world as a whole.

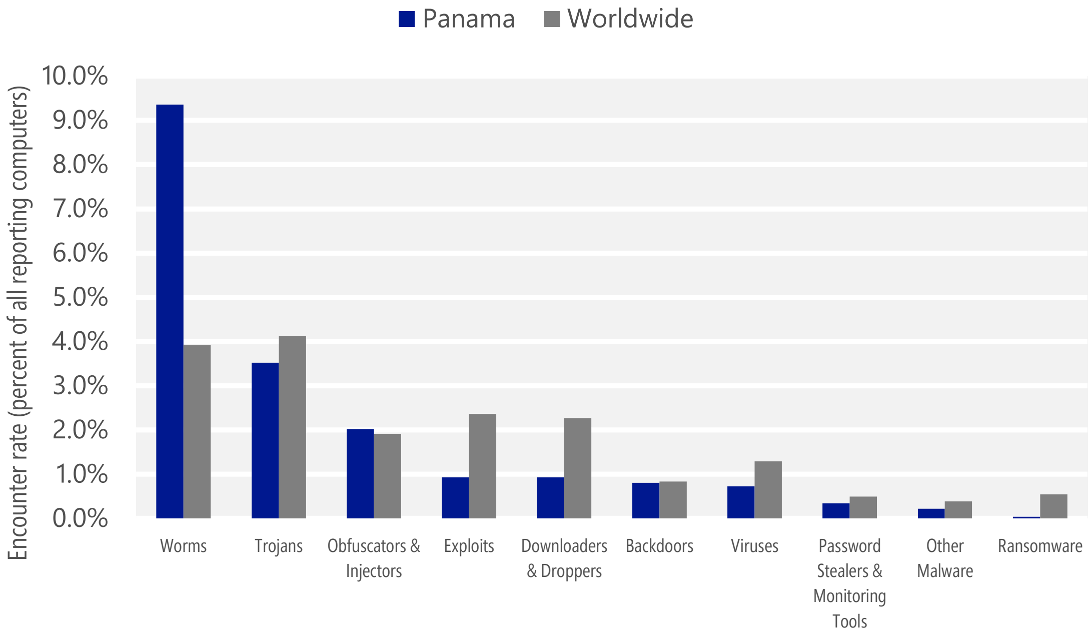
Malware encounter and infection rate trends in Panama and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

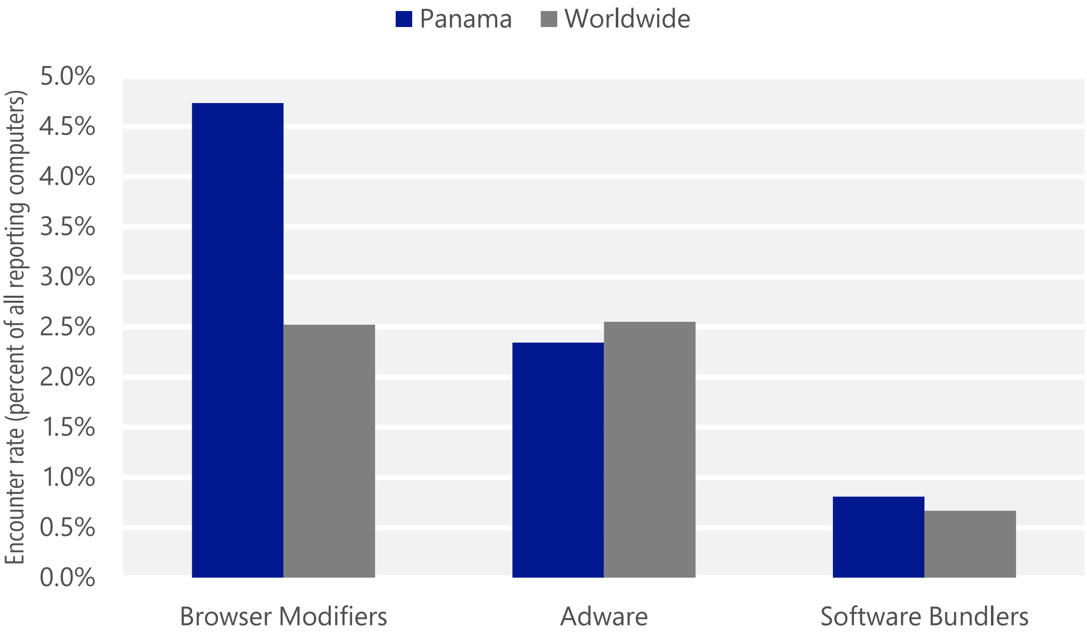
Malware encountered in Panama in 4Q14, by category



- The most common malware category in Panama in 4Q14 was Worms. It was encountered by 9.4 percent of all computers there, down from 14.7 percent in 3Q14.
- The second most common malware category in Panama in 4Q14 was Trojans. It was encountered by 3.5 percent of all computers there, down from 6.2 percent in 3Q14.
- The third most common malware category in Panama in 4Q14 was Obfuscators & Injectors, which was encountered by 2.0 percent of all computers there, down from 2.6 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Panama in 4Q14, by category



- The most common unwanted software category in Panama in 4Q14 was Browser Modifiers. It was encountered by 4.7 percent of all computers there, down from 5.8 percent in 3Q14.
- The second most common unwanted software category in Panama in 4Q14 was Adware. It was encountered by 2.3 percent of all computers there, up from 0.8 percent in 3Q14.
- The third most common unwanted software category in Panama in 4Q14 was Software Bundlers, which was encountered by 0.8 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Panama in 4Q14

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	6.8%
2	Win32/Dorkbot	Worms	1.6%
3	Win32/Obfuscator	Obfuscators & Injectors	0.8%
4	INF/Autorun	Obfuscators & Injectors	0.7%

- The most common malware family encountered in Panama in 4Q14 was VBS/Jenxcus, which was encountered by 6.8 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 Panama in 4Q14 was Win32/Dorkbot, which was encountered by 1.6 percent of reporting computers there. 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 third most common malware family encountered in Panama in 4Q14 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 Panama in 4Q14 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.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Panama in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	3.8%
2	Win32/Defaulttab	Browser Modifiers	1.0%
3	Win32/BetterSurf	Adware	0.9%
4	Win32/Costmin	Adware	0.9%

- The most common unwanted software family encountered in Panama in 4Q14 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 Panama in 4Q14 was Win32/Defaulttab, which was encountered by 1.0 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.
- The third most common unwanted software family encountered in Panama in 4Q14 was Win32/BetterSurf, which was encountered by 0.9 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.

Top threat families by infection rate

The most common malware families by infection rate in Panama in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	8.2
2	Win32/Dorkbot	Worms	0.7
3	Win32/Sality	Viruses	0.6
4	JS/Kilim	Trojans	0.5
5	Win32/Lethic	Trojans	0.4
6	MSIL/Spacekito	Trojans	0.4
7	Win32/Sefnit	Trojans	0.3
8	Win32/Vobfus	Worms	0.3
9	Win32/Brontok	Worms	0.2
10	Win32/Conficker	Worms	0.2

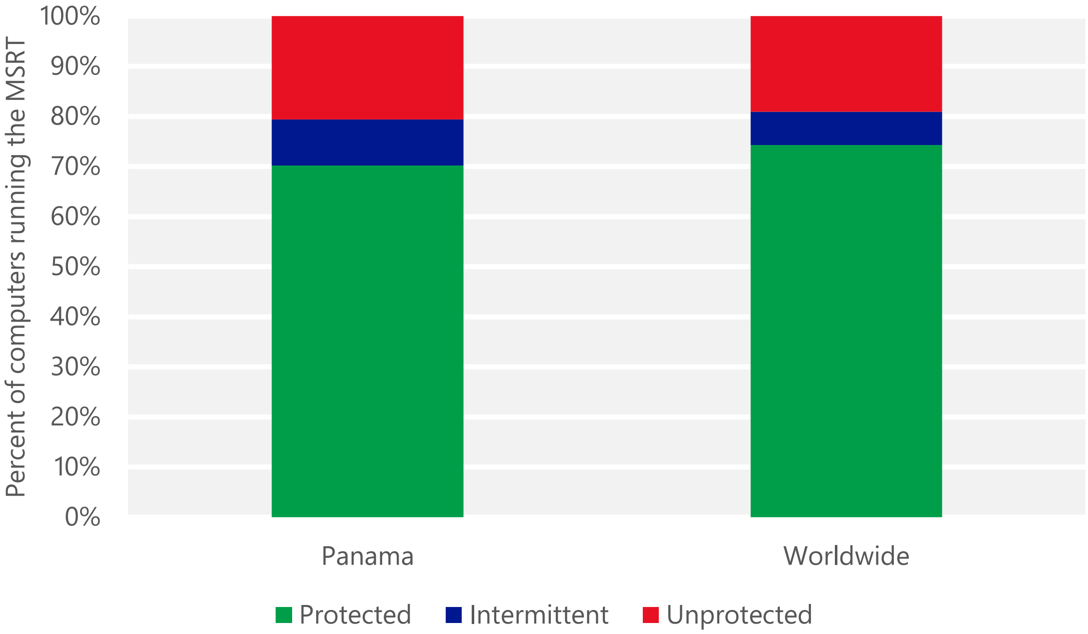
- The most common threat family infecting computers in Panama in 4Q14 was VBS/Jenxcus, which was detected and removed from 8.2 of every 1,000 unique computers scanned by the MSRT. VBS/Jenxcus is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Panama in 4Q14 was Win32/Dorkbot, which was detected and removed from 0.7 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.
- The third most common threat family infecting computers in Panama in 4Q14 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.
- The fourth most common threat family infecting computers in Panama in 4Q14 was JS/Kilim, which was detected and removed from 0.5 of every 1,000 unique computers scanned by the MSRT. JS/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 Panama and worldwide protected by real-time security software in 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 6.61 drive-by download URLs for every 1,000 URLs hosted in Panama, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 4.27 drive-by download URLs for every 1,000 URLs hosted in Panama, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Panama and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Panama	6.61	4.27
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Paraguay

The statistics presented here are generated by Microsoft security programs and services running on computers in Paraguay in 4Q14 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 succeds 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

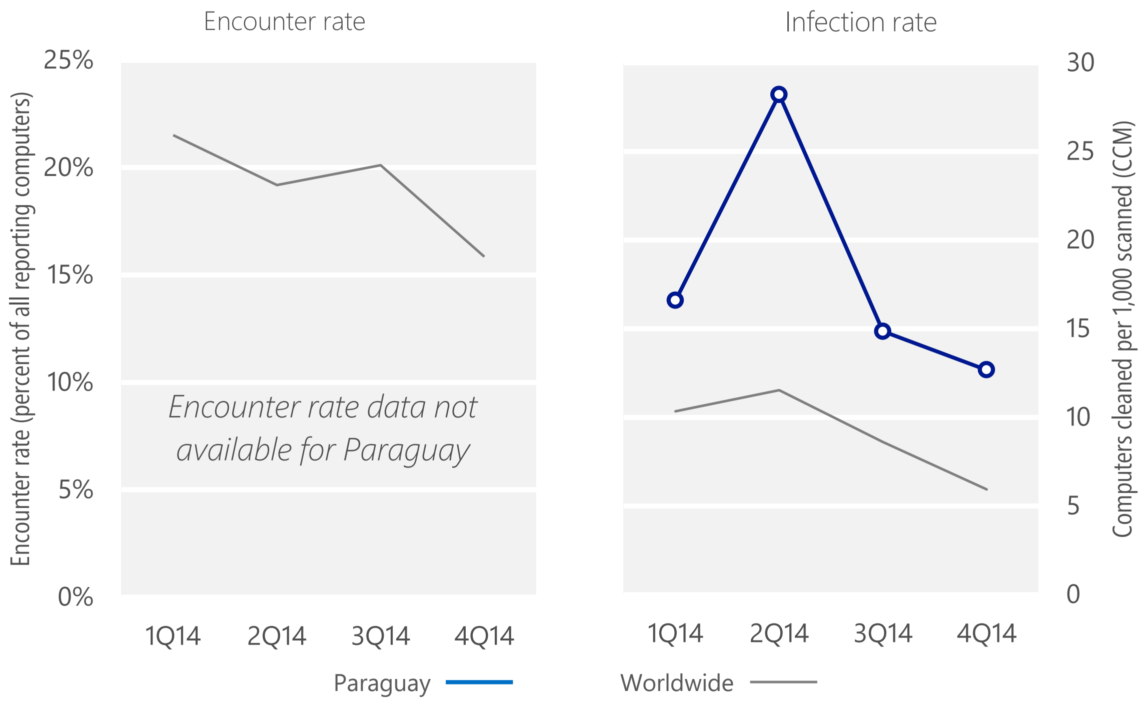
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Paraguay	N/A	N/A	N/A	N/A
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Paraguay	16.6	28.2	14.9	12.7
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, the MSRT detected and removed malware from 12.7 of every 1,000 unique computers scanned in Paraguay in 4Q14 (a CCM score of 12.7, compared to the 4Q14 worldwide CCM of 5.9). 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 18* 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 4Q14

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	5.7
2	Win32/Dorkbot	Worms	1.9
3	Win32/Sality	Viruses	1.1
4	Win32/Lethic	Trojans	1.0
5	Win32/Brontok	Worms	0.8
6	Win32/Sefnit	Trojans	0.6
7	MSIL/Spacekito	Trojans	0.5
8	Win32/Wysotot	Trojans	0.3
9	Win32/Ramnit	Trojans	0.2
10	MSIL/Bladabindi	Backdoors	0.2

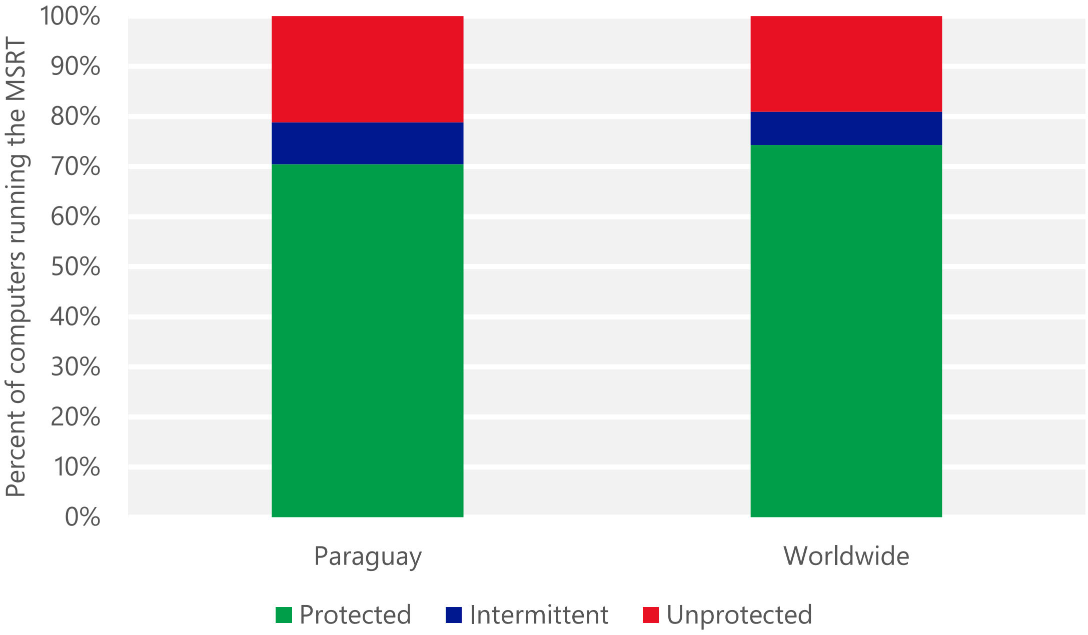
- The most common threat family infecting computers in Paraguay in 4Q14 was VBS/Jenxcus, which was detected and removed from 5.7 of every 1,000 unique computers scanned by the MSRT. VBS/Jenxcus is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Paraguay in 4Q14 was Win32/Dorkbot, which was detected and removed from 1.9 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 third most common threat family infecting computers in Paraguay in 4Q14 was Win32/Sality, which was detected and removed from 1.1 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 Paraguay in 4Q14 was Win32/Lethic, which was detected and removed from 1.0 of every 1,000 unique computers scanned by the MSRT. Win32/Lethic is a trojan that connects to remote servers, which may lead to unauthorized access to an affected system.

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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.05 drive-by download URLs for every 1,000 URLs hosted in Paraguay, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.01 drive-by download URLs for every 1,000 URLs hosted in Paraguay, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Paraguay and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Paraguay	0.05	0.01
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Peru

The statistics presented here are generated by Microsoft security programs and services running on computers in Peru in 4Q14 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 succeds 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

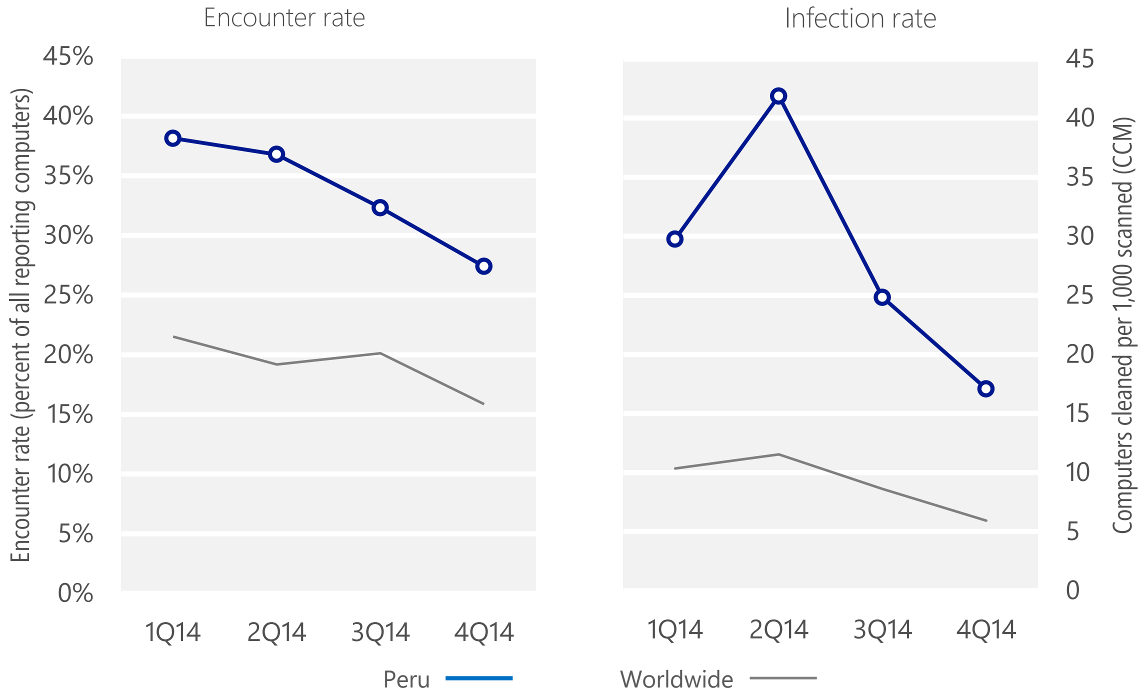
Metric	**1Q14**	**2Q14**	**3Q14**	**4Q14**
Encounter rate, Peru	38.1%	36.8%	32.3%	27.4%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Peru	29.8	41.9	24.8	17.1
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 27.4% percent of computers in Peru encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 17.1 of every 1,000 unique computers scanned in Peru in 4Q14 (a CCM score of 17.1, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Peru over the last four quarters, compared to the world as a whole.

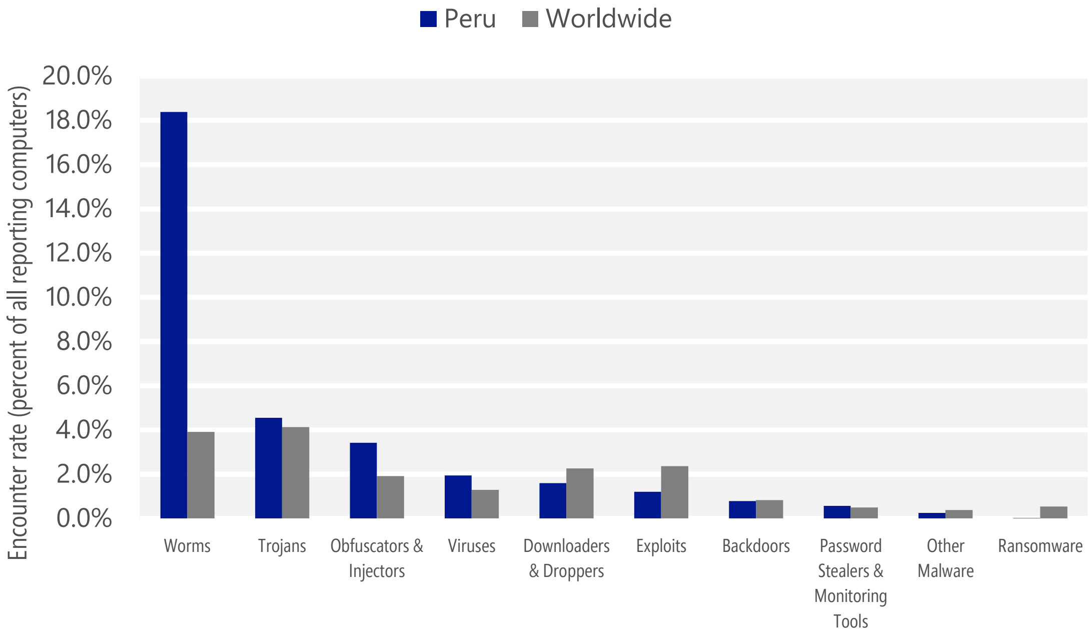
Malware encounter and infection rate trends in Peru and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

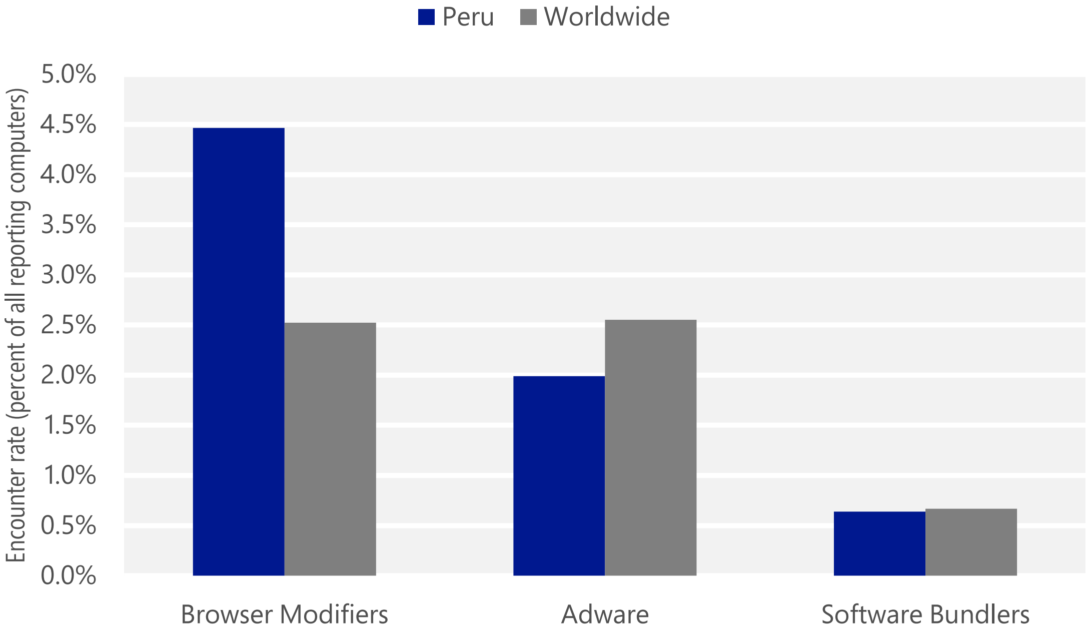
Malware encountered in Peru in 4Q14, by category



- The most common malware category in Peru in 4Q14 was Worms. It was encountered by 18.4 percent of all computers there, down from 20.0 percent in 3Q14.
- The second most common malware category in Peru in 4Q14 was Trojans. It was encountered by 4.6 percent of all computers there, down from 8.3 percent in 3Q14.
- The third most common malware category in Peru in 4Q14 was Obfuscators & Injectors, which was encountered by 3.4 percent of all computers there, down from 3.6 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Peru in 4Q14, by category



- The most common unwanted software category in Peru in 4Q14 was Browser Modifiers. It was encountered by 4.5 percent of all computers there, down from 4.9 percent in 3Q14.
- The second most common unwanted software category in Peru in 4Q14 was Adware. It was encountered by 2.0 percent of all computers there, up from 1.8 percent in 3Q14.
- The third most common unwanted software category in Peru in 4Q14 was Software Bundlers, which was encountered by 0.6 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Peru in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Gamarue	Worms	7.8%
2	VBS/Jenxcus	Worms	6.2%
3	JS/Bondat	Worms	5.3%
4	Win32/Nohad	Worms	2.5%
5	Win32/Yeltminky	Worms	1.5%
6	Win32/CeeInject	Obfuscators & Injectors	1.3%
7	INF/Autorun	Obfuscators & Injectors	1.2%
8	Win32/Vobfus	Worms	1.2%
9	Win32/Obfuscator	Obfuscators & Injectors	1.0%
10	MSIL/Shaskooth	Worms	0.8%

- The most common malware family encountered in Peru in 4Q14 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 Peru in 4Q14 was VBS/Jenxcus, which was encountered by 6.2 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 Peru in 4Q14 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 fourth most common malware family encountered in Peru in 4Q14 was Win32/Nohad, which was encountered by 2.5 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 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	3.7%
2	Win32/Defaulttab	Browser Modifiers	0.8%
3	Win32/Costmin	Adware	0.8%
4	Win32/BetterSurf	Adware	0.8%
5	Win32/Gofileexpress	Software Bundlers	0.3%

- The most common unwanted software family encountered in Peru in 4Q14 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 4Q14 was Win32/Defaulttab, which was encountered by 0.8 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.
- The third most common unwanted software family encountered in Peru in 4Q14 was Win32/Costmin, which was encountered by 0.8 percent of reporting computers there. Win32/Costmin is an adware family that installs itself as a browser extension for Internet Explorer, Mozilla Firefox, and Google Chrome, and displays advertisements as the user browses the Internet.

Top threat families by infection rate

The most common malware families by infection rate in Peru in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	6.6
2	Win32/Gamarue	Worms	5.1
3	Win32/Vobfus	Worms	1.5
4	Win32/Sality	Viruses	0.8
5	Win32/Ramnit	Trojans	0.5
6	MSIL/Spacekito	Trojans	0.4
7	Win32/Yeltminky	Worms	0.4
8	Win32/Dorkbot	Worms	0.3
9	Win32/Sefnit	Trojans	0.3
10	MSIL/Bladabindi	Backdoors	0.3

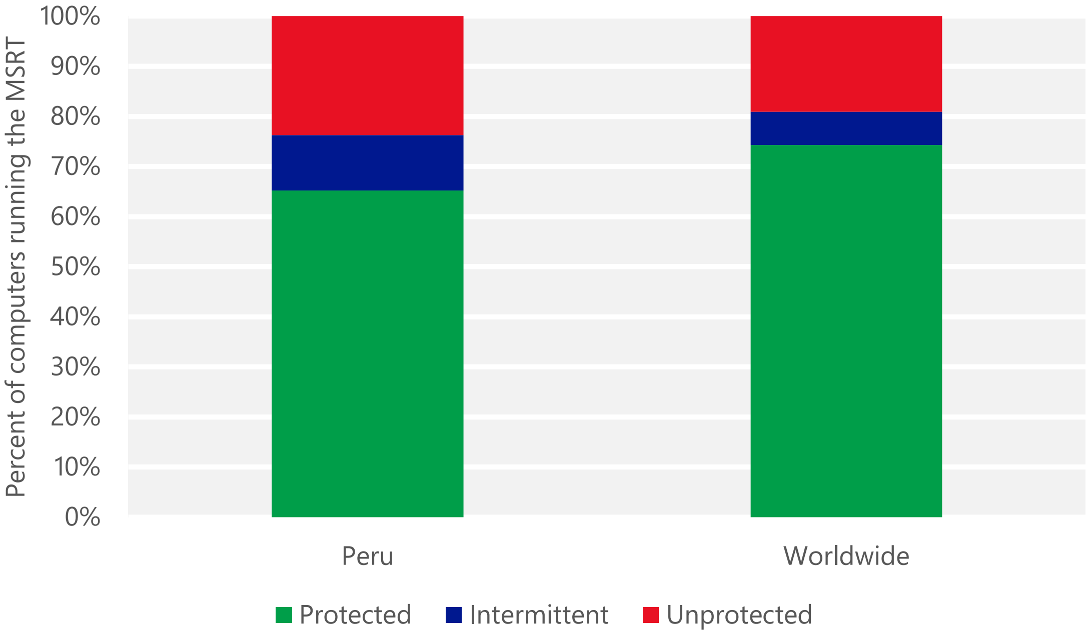
- The most common threat family infecting computers in Peru in 4Q14 was VBS/Jenxcus, which was detected and removed from 6.6 of every 1,000 unique computers scanned by the MSRT. VBS/Jenxcus is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Peru in 4Q14 was Win32/Gamarue, which was detected and removed from 5.1 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 Peru in 4Q14 was Win32/Vobfus, which was detected and removed from 1.5 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.
- The fourth most common threat family infecting computers in Peru in 4Q14 was Win32/Sality, which was detected and removed from 0.8 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.

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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.03 drive-by download URLs for every 1,000 URLs hosted in Peru, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.01 drive-by download URLs for every 1,000 URLs hosted in Peru, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Peru and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Peru	0.03	0.01
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Philippines

The statistics presented here are generated by Microsoft security programs and services running on computers in Philippines in 4Q14 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 succeds 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

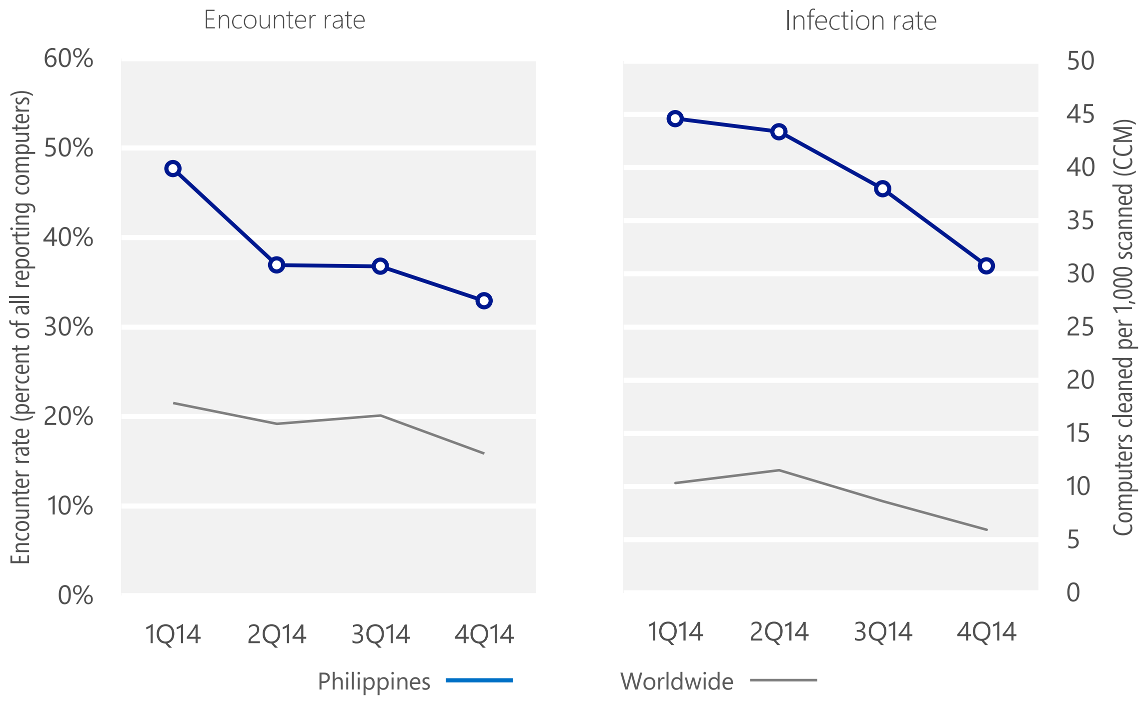
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Philippines	47.7%	36.9%	36.8%	32.9%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Philippines	44.6	43.4	38.0	30.8
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 32.9% percent of computers in Philippines encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 30.8 of every 1,000 unique computers scanned in Philippines in 4Q14 (a CCM score of 30.8, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Philippines over the last four quarters, compared to the world as a whole.

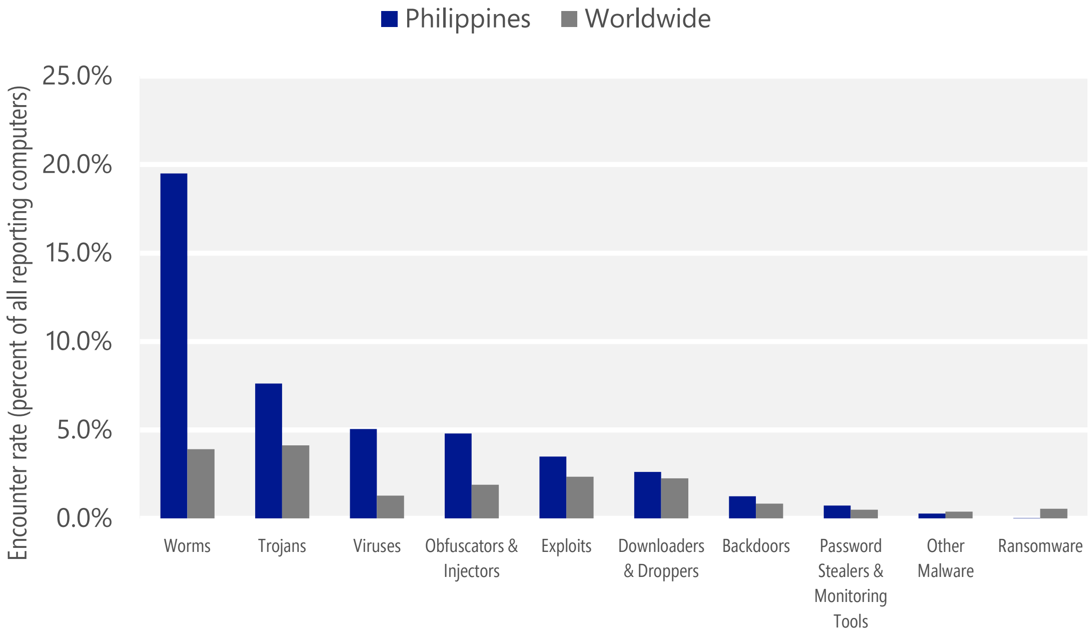
Malware encounter and infection rate trends in Philippines and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

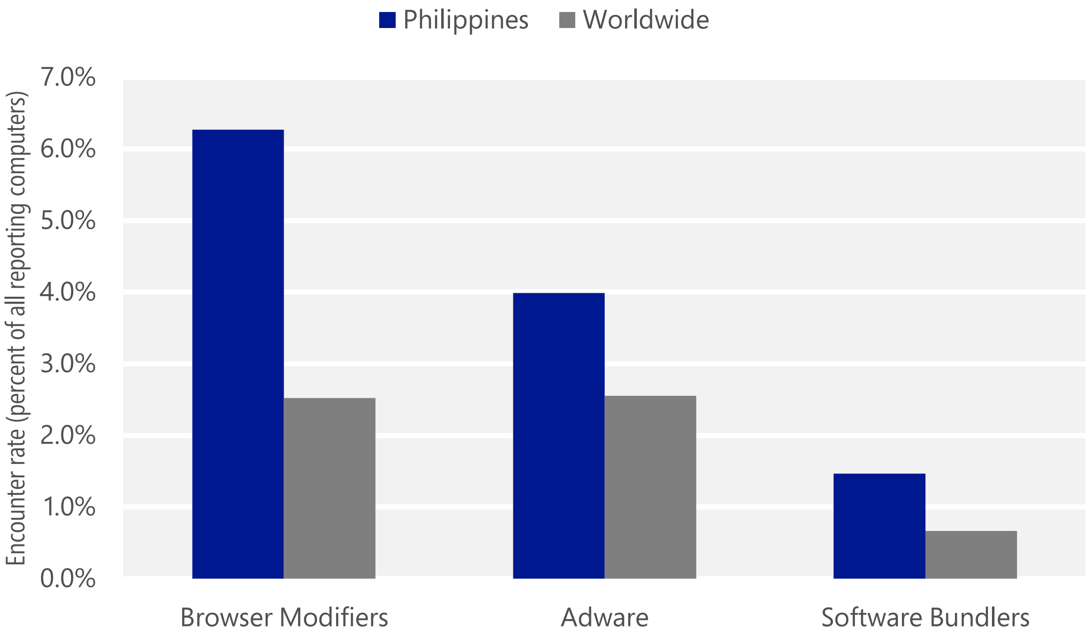
Malware encountered in Philippines in 4Q14, by category



- The most common malware category in Philippines in 4Q14 was Worms. It was encountered by 19.5 percent of all computers there, down from 22.4 percent in 3Q14.
- The second most common malware category in Philippines in 4Q14 was Trojans. It was encountered by 7.6 percent of all computers there, down from 11.7 percent in 3Q14.
- The third most common malware category in Philippines in 4Q14 was Viruses, which was encountered by 5.1 percent of all computers there, down from 5.4 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Philippines in 4Q14, by category



- The most common unwanted software category in Philippines in 4Q14 was Browser Modifiers. It was encountered by 6.3 percent of all computers there, down from 7.3 percent in 3Q14.
- The second most common unwanted software category in Philippines in 4Q14 was Adware. It was encountered by 4.0 percent of all computers there, up from 1.7 percent in 3Q14.
- The third most common unwanted software category in Philippines in 4Q14 was Software Bundlers, which was encountered by 1.5 percent of all computers there, up from 0.2 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Philippines in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Gamarue	Worms	9.0%
2	VBS/Jenxcus	Worms	6.8%
3	INF/Autorun	Obfuscators & Injectors	4.9%
4	Win32/Ramnit	Trojans	3.4%
5	Win32/CplLnk	Exploits	3.2%
6	Win32/Sality	Viruses	3.1%
7	VBS/Cantix	Worms	2.7%
8	Win32/Ippedo	Worms	1.8%
9	Win32/Conficker	Worms	1.4%
10	Win32/Yeltminky	Worms	1.2%

- The most common malware family encountered in Philippines in 4Q14 was Win32/Gamarue, which was encountered by 9.0 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 Philippines in 4Q14 was VBS/Jenxcus, which was encountered by 6.8 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 third most common malware family encountered in Philippines in 4Q14 was INF/Autorun, which was encountered by 4.9 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 fourth most common malware family encountered in Philippines in 4Q14 was Win32/Ramnit, which was encountered by 3.4 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 Philippines in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	4.4%
2	Win32/Defaulttab	Browser Modifiers	2.2%
3	Win32/BetterSurf	Adware	1.5%
4	Win32/Costmin	Adware	1.4%
5	Win32/Gofileexpress	Software Bundlers	0.9%

- The most common unwanted software family encountered in Philippines in 4Q14 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 Philippines in 4Q14 was Win32/Defaulttab, which was encountered by 2.2 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.
- The third most common unwanted software family encountered in Philippines in 4Q14 was Win32/BetterSurf, which was encountered by 1.5 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.

Top threat families by infection rate

The most common malware families by infection rate in Philippines in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Gamarue	Worms	9.9
2	VBS/Jenxcus	Worms	8.1
3	Win32/Sality	Viruses	6.7
4	Win32/Ramnit	Trojans	3.4
5	Win32/Pramro	Trojans	1.3
6	Win32/Brontok	Worms	0.8
7	Win32/Yeltminky	Worms	0.6
8	Win32/Folstart	Worms	0.5
9	JS/Kilim	Trojans	0.5
10	Win32/Sefnit	Trojans	0.4

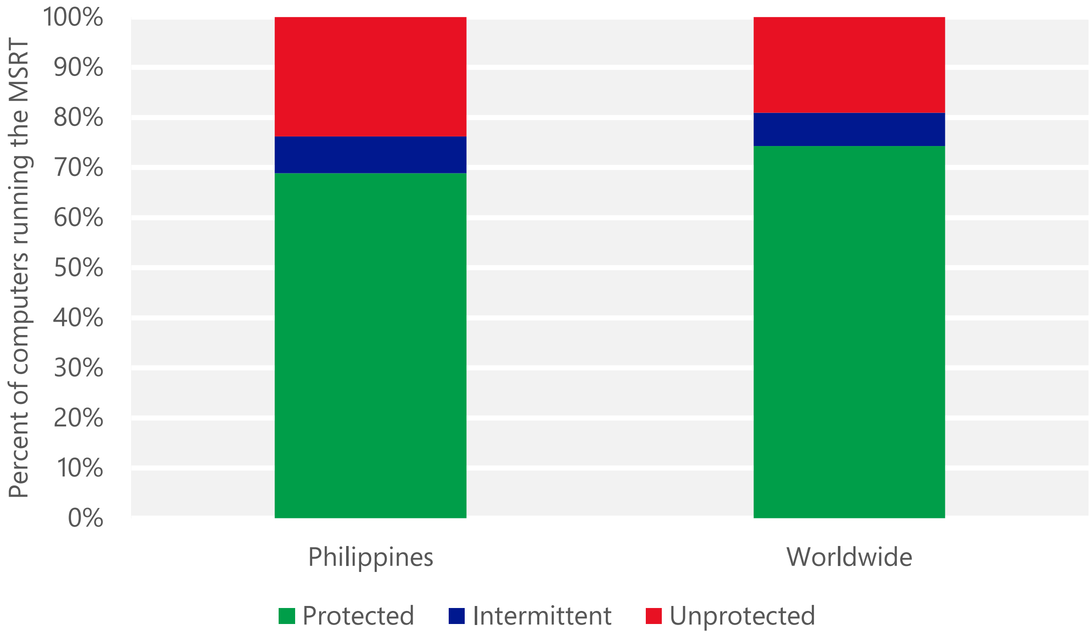
- The most common threat family infecting computers in Philippines in 4Q14 was Win32/Gamarue, which was detected and removed from 9.9 of every 1,000 unique computers scanned by the MSRT. Win32/Gamarue is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed 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 Philippines in 4Q14 was VBS/Jenxcus, which was detected and removed from 8.1 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 Philippines in 4Q14 was Win32/Sality, which was detected and removed from 6.7 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 Philippines in 4Q14 was Win32/Ramnit, which was detected and removed from 3.4 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 Philippines and worldwide protected by real-time security software in 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.57 drive-by download URLs for every 1,000 URLs hosted in Philippines, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.44 drive-by download URLs for every 1,000 URLs hosted in Philippines, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Philippines and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Philippines	0.57	0.44
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Poland

The statistics presented here are generated by Microsoft security programs and services running on computers in Poland in 4Q14 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 succeds 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

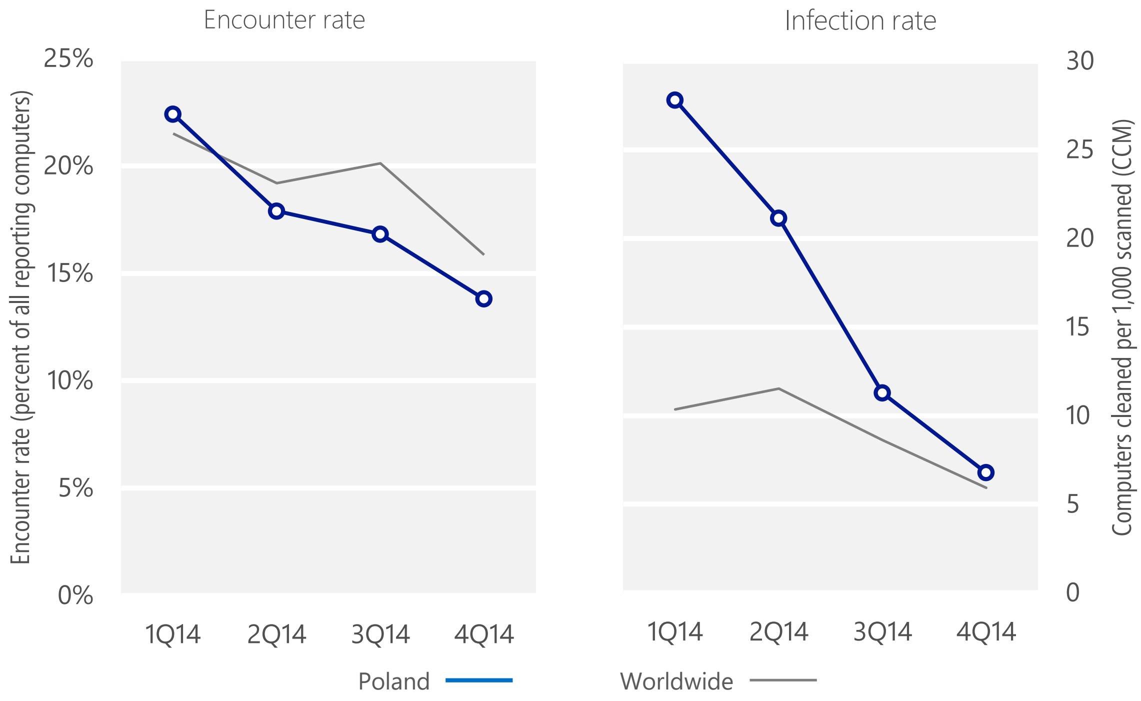
Metric	**1Q14**	**2Q14**	**3Q14**	**4Q14**
Encounter rate, Poland	22.4%	17.9%	16.8%	13.8%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Poland	27.8	21.1	11.3	6.8
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 13.8% percent of computers in Poland encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 6.8 of every 1,000 unique computers scanned in Poland in 4Q14 (a CCM score of 6.8, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Poland over the last four quarters, compared to the world as a whole.

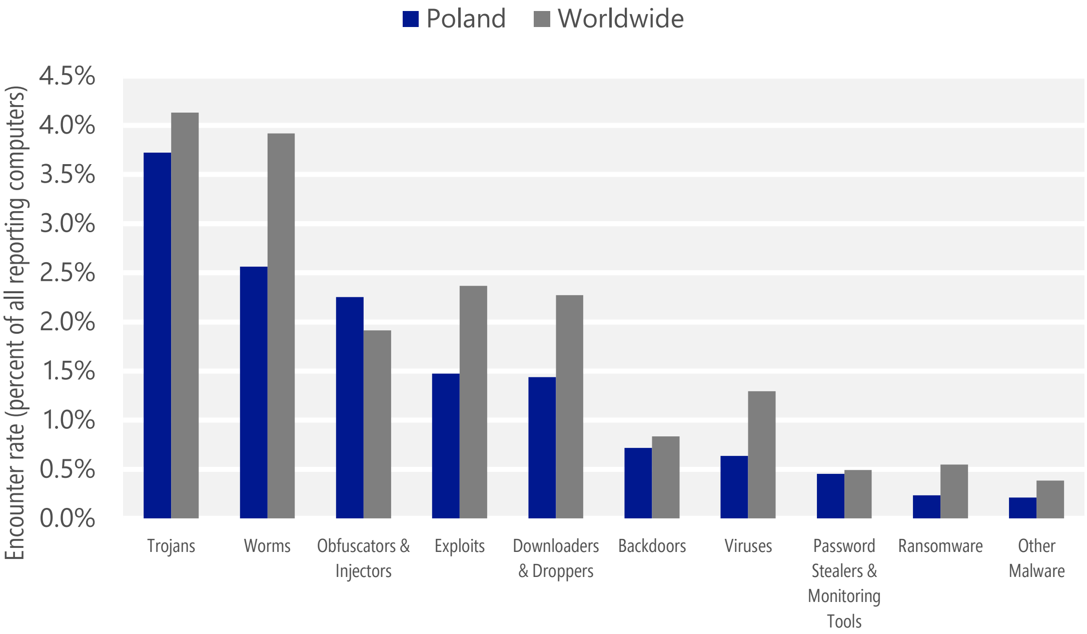
Malware encounter and infection rate trends in Poland and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

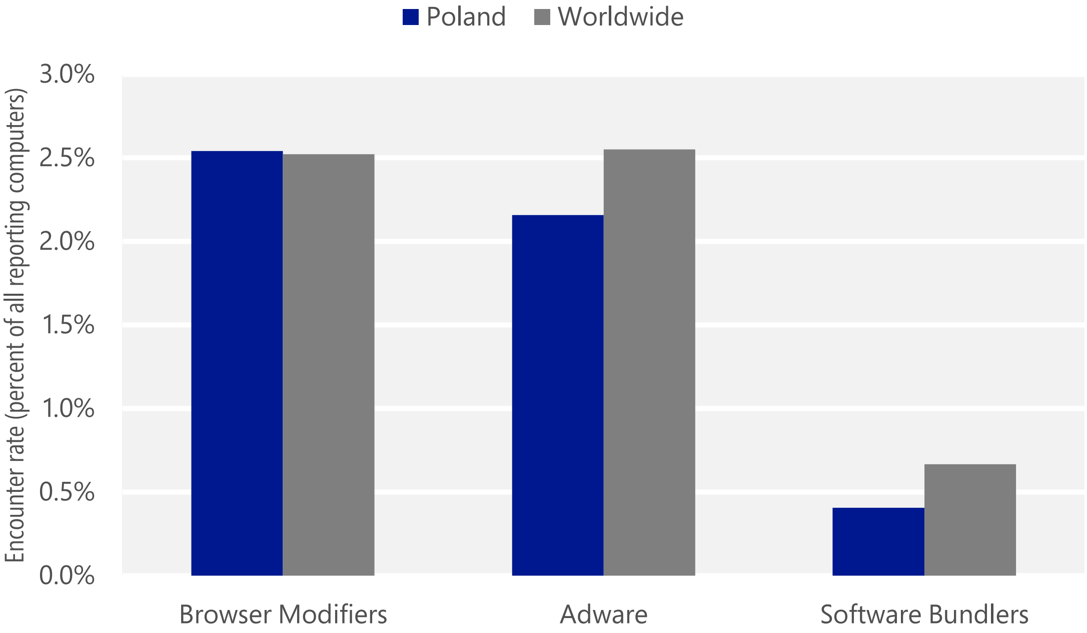
Malware encountered in Poland in 4Q14, by category



- The most common malware category in Poland in 4Q14 was Trojans. It was encountered by 3.7 percent of all computers there, down from 6.5 percent in 3Q14.
- The second most common malware category in Poland in 4Q14 was Worms. It was encountered by 2.6 percent of all computers there, down from 2.7 percent in 3Q14.
- The third most common malware category in Poland in 4Q14 was Obfuscators & Injectors, which was encountered by 2.3 percent of all computers there, down from 2.5 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Poland in 4Q14, by category



- The most common unwanted software category in Poland in 4Q14 was Browser Modifiers. It was encountered by 2.5 percent of all computers there, down from 4.2 percent in 3Q14.
- The second most common unwanted software category in Poland in 4Q14 was Adware. It was encountered by 2.2 percent of all computers there, up from 0.5 percent in 3Q14.
- The third most common unwanted software category in Poland in 4Q14 was Software Bundlers, which was encountered by 0.4 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Poland in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Obfuscator	Obfuscators & Injectors	1.5%
2	INF/Autorun	Obfuscators & Injectors	0.9%
3	JS/Axpergle	Exploits	0.8%
4	JS/Faceliker	Trojans	0.5%
5	Win32/Wysotot	Trojans	0.5%
6	Win32/Brontok	Worms	0.5%
7	Win32/Vobfus	Worms	0.5%
8	Win32/Gamarue	Worms	0.4%
9	Win32/Dynamer	Trojans	0.4%
10	Win32/Conficker	Worms	0.4%

- The most common malware family encountered in Poland in 4Q14 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 Poland in 4Q14 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.
- The third most common malware family encountered in Poland in 4Q14 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 fourth most common malware family encountered in Poland in 4Q14 was JS/Faceliker, which was encountered by 0.5 percent of reporting computers there. JS/Faceliker is a malicious script that ?likes? content on Facebook without the user's knowledge or consent.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Poland in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	2.1%
2	Win32/Pennybee	Adware	0.7%
3	Win32/Defaulttab	Browser Modifiers	0.5%
4	Win32/Costmin	Adware	0.5%
5	Win32/BetterSurf	Adware	0.4%

- The most common unwanted software family encountered in Poland in 4Q14 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 second most common unwanted software family encountered in Poland in 4Q14 was Win32/Pennybee, which was encountered by 0.7 percent of reporting computers there. Win32/Pennybee is adware that shows ads as the user browses the web. It can be installed from the program’s website or bundled with some third-party software installation programs.
- The third most common unwanted software family encountered in Poland in 4Q14 was Win32/Defaulttab, which was encountered by 0.5 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.

Top threat families by infection rate

The most common malware families by infection rate in Poland in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Wysotot	Trojans	1.1
2	Win32/Brontok	Worms	1.0
3	Win32/Sality	Viruses	0.7
4	Win32/Vobfus	Worms	0.7
5	JS/Kilim	Trojans	0.6
6	Win32/Sefnit	Trojans	0.5
7	Win32/Gamarue	Worms	0.3
8	VBS/Jenxcus	Worms	0.3
9	Win32/Tofsee	Backdoors	0.3
10	Win32/Ramnit	Trojans	0.2

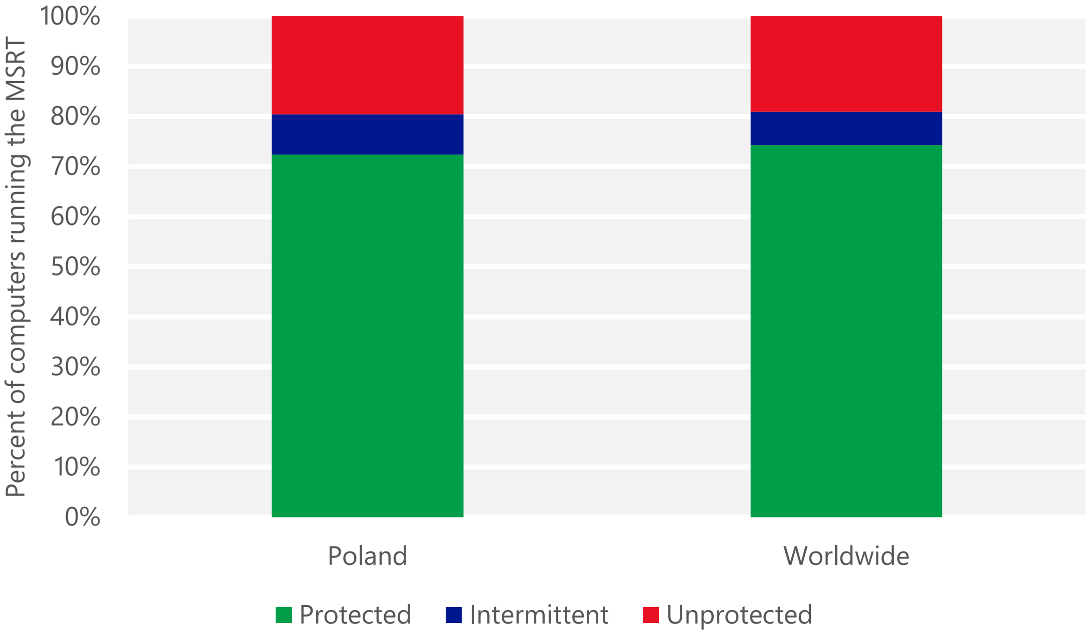
- The most common threat family infecting computers in Poland in 4Q14 was Win32/Wysotot, which was detected and removed from 1.1 of every 1,000 unique computers scanned by the MSRT. Win32/Wysotot is a threat that can change the start page of the user's web browser, and may download and install other files to the computer. It is installed by software bundlers that advertise free software or games.
- The second most common threat family infecting computers in Poland in 4Q14 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.
- The third most common threat family infecting computers in Poland in 4Q14 was Win32/Sality, which was detected and removed from 0.7 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 Poland in 4Q14 was Win32/Vobfus, which was detected and removed from 0.7 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 Poland and worldwide protected by real-time security software in 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.38 drive-by download URLs for every 1,000 URLs hosted in Poland, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.34 drive-by download URLs for every 1,000 URLs hosted in Poland, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Poland and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Poland	0.38	0.34
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Portugal

The statistics presented here are generated by Microsoft security programs and services running on computers in Portugal in 4Q14 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 succeds 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

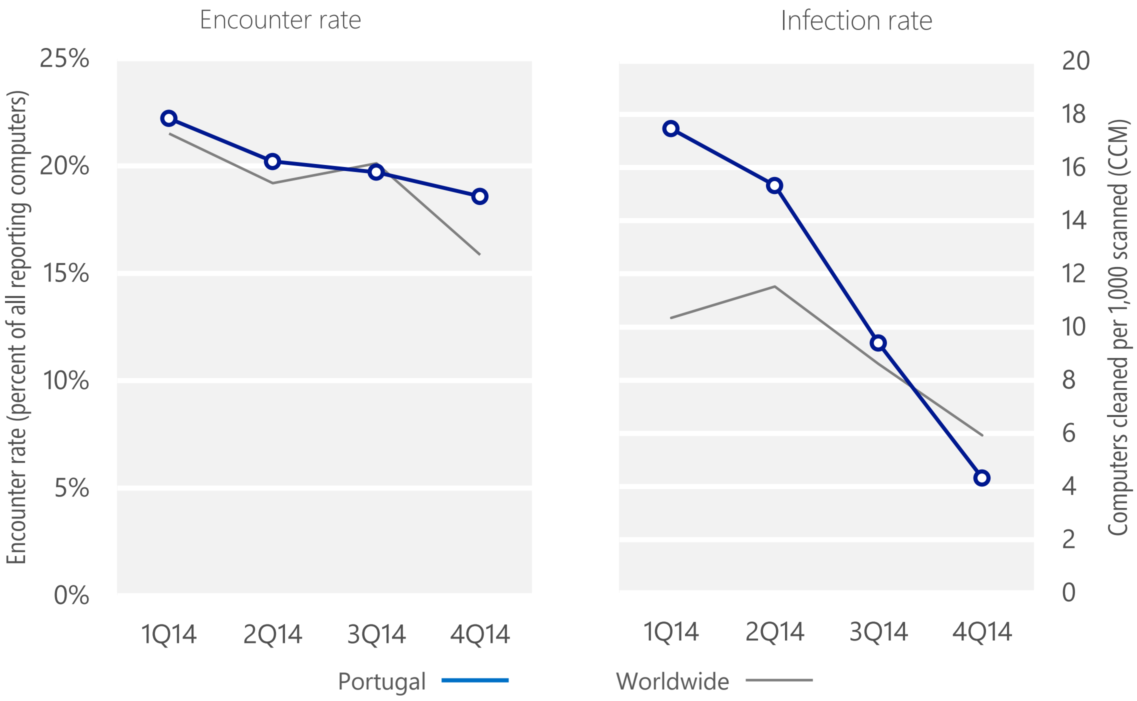
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Portugal	22.2%	20.2%	19.7%	18.6%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Portugal	17.5	15.3	9.4	4.3
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 18.6% percent of computers in Portugal encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 4.3 of every 1,000 unique computers scanned in Portugal in 4Q14 (a CCM score of 4.3, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Portugal over the last four quarters, compared to the world as a whole.

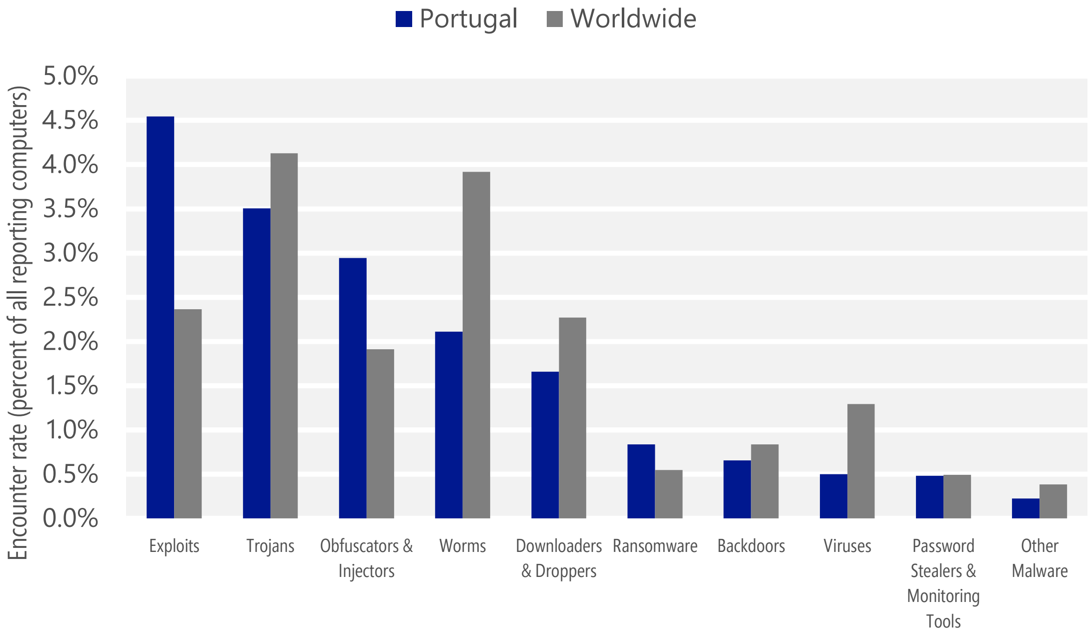
Malware encounter and infection rate trends in Portugal and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

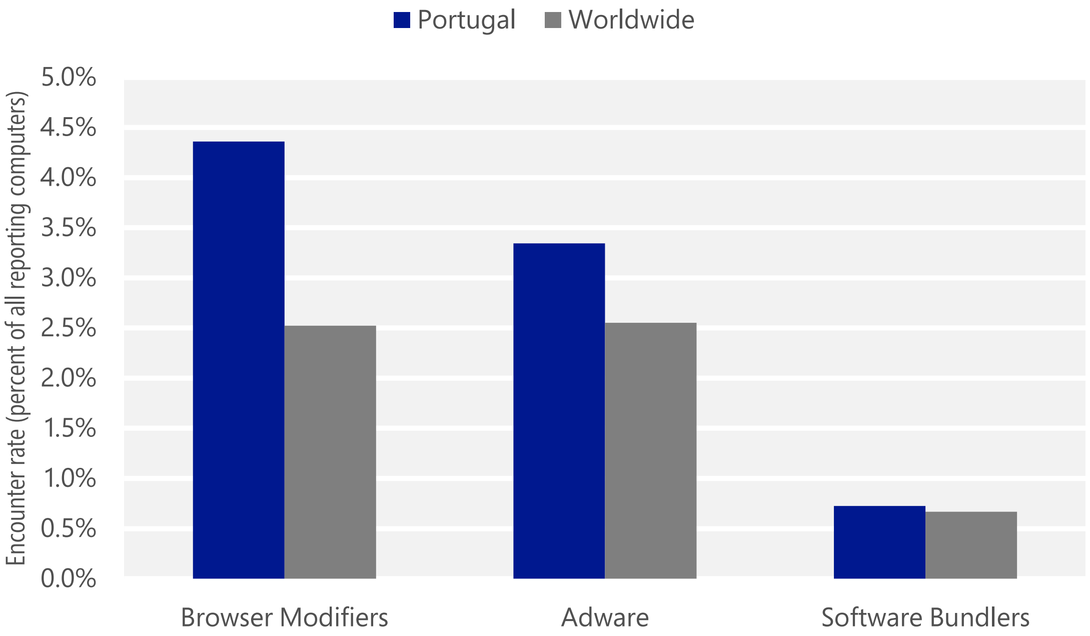
Malware encountered in Portugal in 4Q14, by category



- The most common malware category in Portugal in 4Q14 was Exploits. It was encountered by 4.5 percent of all computers there, down from 6.2 percent in 3Q14.
- The second most common malware category in Portugal in 4Q14 was Trojans. It was encountered by 3.5 percent of all computers there, down from 4.0 percent in 3Q14.
- The third most common malware category in Portugal in 4Q14 was Obfuscators & Injectors, which was encountered by 2.9 percent of all computers there, down from 3.9 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Portugal in 4Q14, by category



- The most common unwanted software category in Portugal in 4Q14 was Browser Modifiers. It was encountered by 4.4 percent of all computers there, down from 6.2 percent in 3Q14.
- The second most common unwanted software category in Portugal in 4Q14 was Adware. It was encountered by 3.3 percent of all computers there, up from 0.5 percent in 3Q14.
- The third most common unwanted software category in Portugal in 4Q14 was Software Bundlers, which was encountered by 0.7 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Portugal in 4Q14

	Family	Most significant category	% of reporting computers
1	JS/Axpergle	Exploits	3.5%
2	Win32/Obfuscator	Obfuscators & Injectors	2.3%
3	INF/Autorun	Obfuscators & Injectors	0.7%
4	Win32/Wysotot	Trojans	0.5%
5	JS/Krypterade	Ransomware	0.5%
6	VBS/Jenxcus	Worms	0.5%
7	Win32/Dynamer	Trojans	0.3%
8	Win32/Brontok	Worms	0.3%
9	Win32/Anogre	Exploits	0.3%
10	Win32/Gamarue	Worms	0.3%

- The most common malware family encountered in Portugal in 4Q14 was JS/Axpergle, which was encountered by 3.5 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 Portugal in 4Q14 was Win32/Obfuscator, which was encountered by 2.3 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 third most common malware family encountered in Portugal in 4Q14 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 fourth most common malware family encountered in Portugal in 4Q14 was Win32/Wysotot, which was encountered by 0.5 percent of reporting computers there. Win32/Wysotot is a threat that can change the start page of the user's web browser, and may download and install other files to the computer. It is installed by software bundlers that advertise free software or games.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Portugal in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	3.3%
2	Win32/Pennybee	Adware	1.1%
3	Win32/Costmin	Adware	1.1%
4	Win32/Defaulttab	Browser Modifiers	1.0%
5	Win32/BetterSurf	Adware	0.7%

- The most common unwanted software family encountered in Portugal in 4Q14 was Win32/Couponruc, which was encountered by 3.3 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 Portugal in 4Q14 was Win32/Pennybee, which was encountered by 1.1 percent of reporting computers there. Win32/Pennybee is adware that shows ads as the user browses the web. It can be installed from the program's website or bundled with some third-party software installation programs.
- The third most common unwanted software family encountered in Portugal in 4Q14 was Win32/Costmin, which was encountered by 1.1 percent of reporting computers there. Win32/Costmin is an adware family that installs itself as a browser extension for Internet Explorer, Mozilla Firefox, and Google Chrome, and displays advertisements as the user browses the Internet.

Top threat families by infection rate

The most common malware families by infection rate in Portugal in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Wysotot	Trojans	0.9
2	VBS/Jenxcus	Worms	0.6
3	Win32/Brontok	Worms	0.4
4	Win32/Sefnit	Trojans	0.4
5	Win32/Ramnit	Trojans	0.2
6	Win32/Vobfus	Worms	0.2
7	MSIL/Bladabindi	Backdoors	0.2
8	Win32/Alureon	Trojans	0.2
9	Win32/Sality	Viruses	0.2
10	JS/Kilim	Trojans	0.1

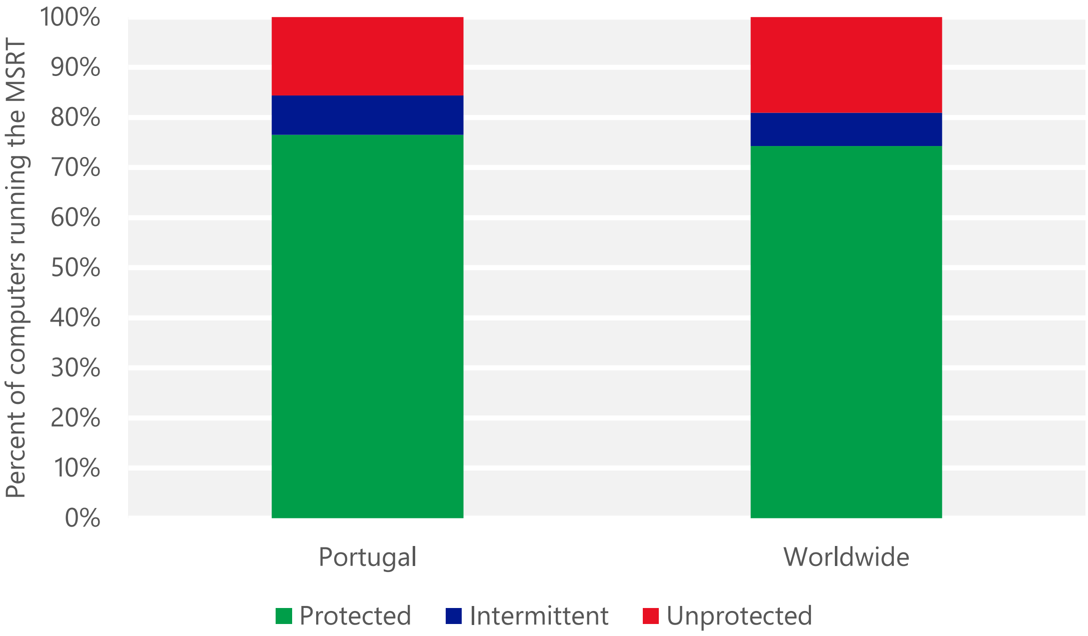
- The most common threat family infecting computers in Portugal in 4Q14 was Win32/Wysotot, which was detected and removed from 0.9 of every 1,000 unique computers scanned by the MSRT. Win32/Wysotot is a threat that can change the start page of the user's web browser, and may download and install other files to the computer. It is installed by software bundlers that advertise free software or games.
- The second most common threat family infecting computers in Portugal in 4Q14 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.
- The third most common threat family infecting computers in Portugal in 4Q14 was Win32/Brontok, which was detected and removed from 0.4 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 Portugal in 4Q14 was Win32/Sefnit, which was detected and removed from 0.4 of every 1,000 unique computers scanned by the MSRT. Win32/Sefnit is a family of trojans that can allow backdoor access, download files, and use the computer and Internet connection for click fraud. Some variants can monitor web browsers and hijack search results.

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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.29 drive-by download URLs for every 1,000 URLs hosted in Portugal, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.43 drive-by download URLs for every 1,000 URLs hosted in Portugal, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Portugal and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Portugal	0.29	0.43
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Puerto Rico

The statistics presented here are generated by Microsoft security programs and services running on computers in Puerto Rico in 4Q14 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 succeds 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

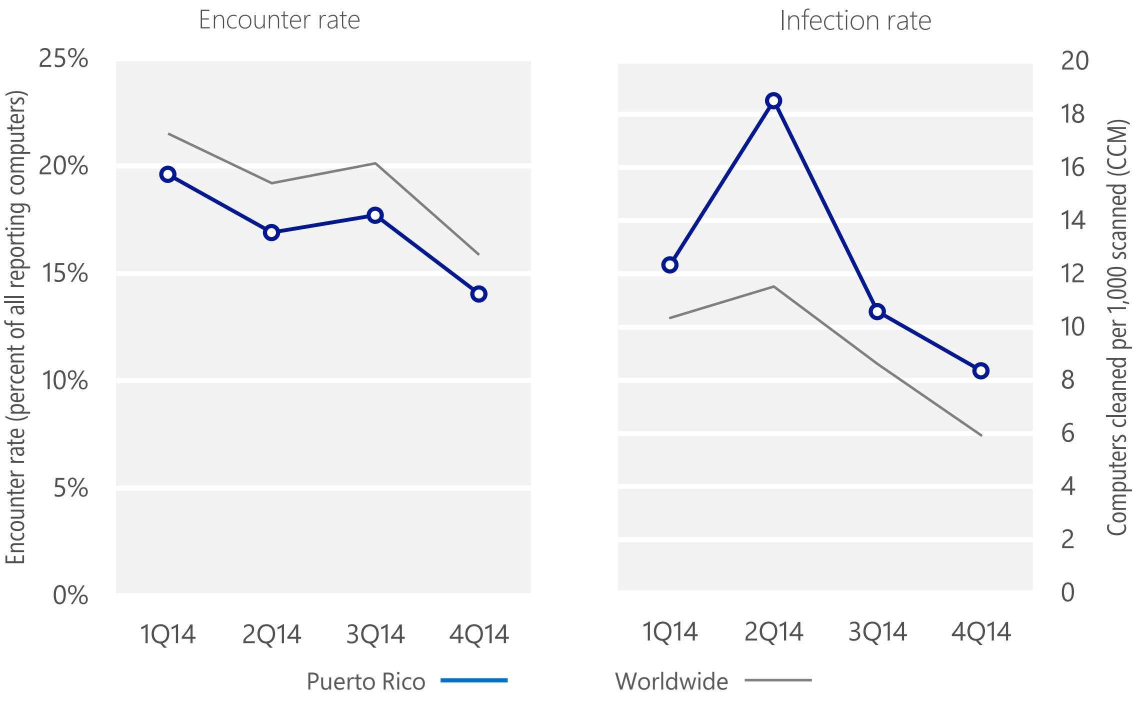
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Puerto Rico	19.6%	16.9%	17.7%	14.0%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Puerto Rico	12.3	18.5	10.6	8.4
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 14.0% percent of computers in Puerto Rico encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 8.4 of every 1,000 unique computers scanned in Puerto Rico in 4Q14 (a CCM score of 8.4, compared to the 4Q14 worldwide CCM of 5.9). 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.

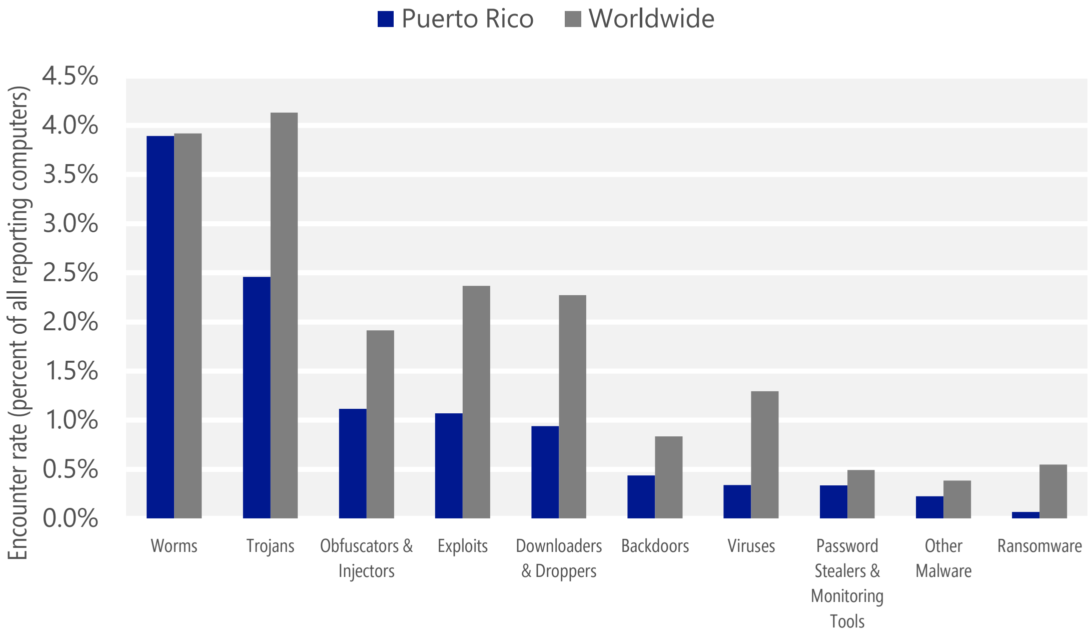
Malware encounter and infection rate trends in Puerto Rico and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

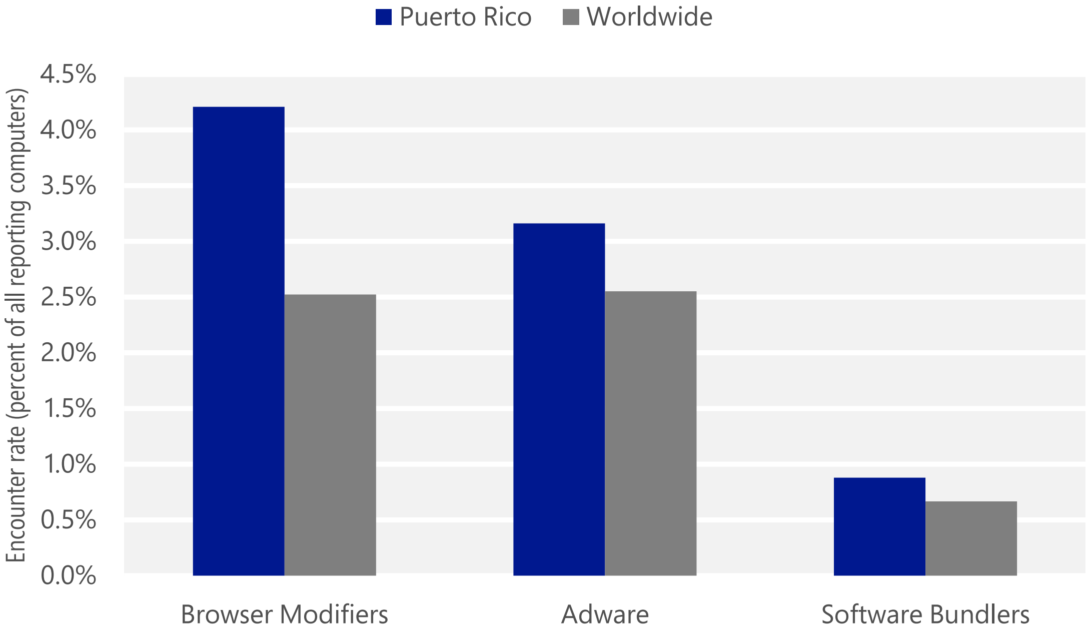
Malware encountered in Puerto Rico in 4Q14, by category



- The most common malware category in Puerto Rico in 4Q14 was Worms. It was encountered by 3.9 percent of all computers there, down from 4.9 percent in 3Q14.
- The second most common malware category in Puerto Rico in 4Q14 was Trojans. It was encountered by 2.5 percent of all computers there, down from 4.3 percent in 3Q14.
- The third most common malware category in Puerto Rico in 4Q14 was Obfuscators & Injectors, which was encountered by 1.1 percent of all computers there, down from 2.6 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Puerto Rico in 4Q14, by category



- The most common unwanted software category in Puerto Rico in 4Q14 was Browser Modifiers. It was encountered by 4.2 percent of all computers there, down from 7.3 percent in 3Q14.
- The second most common unwanted software category in Puerto Rico in 4Q14 was Adware. It was encountered by 3.2 percent of all computers there, up from 0.9 percent in 3Q14.
- The third most common unwanted software category in Puerto Rico in 4Q14 was Software Bundlers, which was encountered by 0.9 percent of all computers there, up from 0.2 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Puerto Rico in 4Q14

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	1.5%
2	INF/Autorun	Obfuscators & Injectors	1.1%
3	Win32/Vobfus	Worms	0.7%
4	Win32/Brontok	Worms	0.6%
5	Win32/Obfuscator	Obfuscators & Injectors	0.5%
6	BAT/Micuda	Trojans	0.4%
7	JS/Axpergle	Exploits	0.3%
8	MSIL/Shaskooth	Worms	0.3%

- The most common malware family encountered in Puerto Rico in 4Q14 was VBS/Jenxcus, which was encountered by 1.5 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 Puerto Rico in 4Q14 was INF/Autorun, which was encountered by 1.1 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 Puerto Rico in 4Q14 was Win32/Vobfus, which was encountered by 0.7 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.
- The fourth most common malware family encountered in Puerto Rico in 4Q14 was Win32/Brontok, which was encountered by 0.6 percent of reporting computers there. 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.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Puerto Rico in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	3.1%
2	Win32/BetterSurf	Adware	1.7%
3	Win32/Defaulttab	Browser Modifiers	1.2%
4	Win32/Costmin	Adware	1.1%
5	Win32/Gofileexpress	Software Bundlers	0.6%

- The most common unwanted software family encountered in Puerto Rico in 4Q14 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 Puerto Rico in 4Q14 was Win32/BetterSurf, which was encountered by 1.7 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.
- The third most common unwanted software family encountered in Puerto Rico in 4Q14 was Win32/Defaulttab, which was encountered by 1.2 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.

Top threat families by infection rate

The most common malware families by infection rate in Puerto Rico in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	3.4
2	Win32/Vobfus	Worms	1.2
3	Win32/Brontok	Worms	1.1
4	Win32/Sefnit	Trojans	0.3
5	Win32/Alureon	Trojans	0.3
6	Win32/Wysotot	Trojans	0.3
7	Win32/Zbot	Password Stealers & Monitoring Tools	0.3
8	Win32/Dorkbot	Worms	0.2
9	Win32/Conficker	Worms	0.2
10	MSIL/Bladabindi	Backdoors	0.1

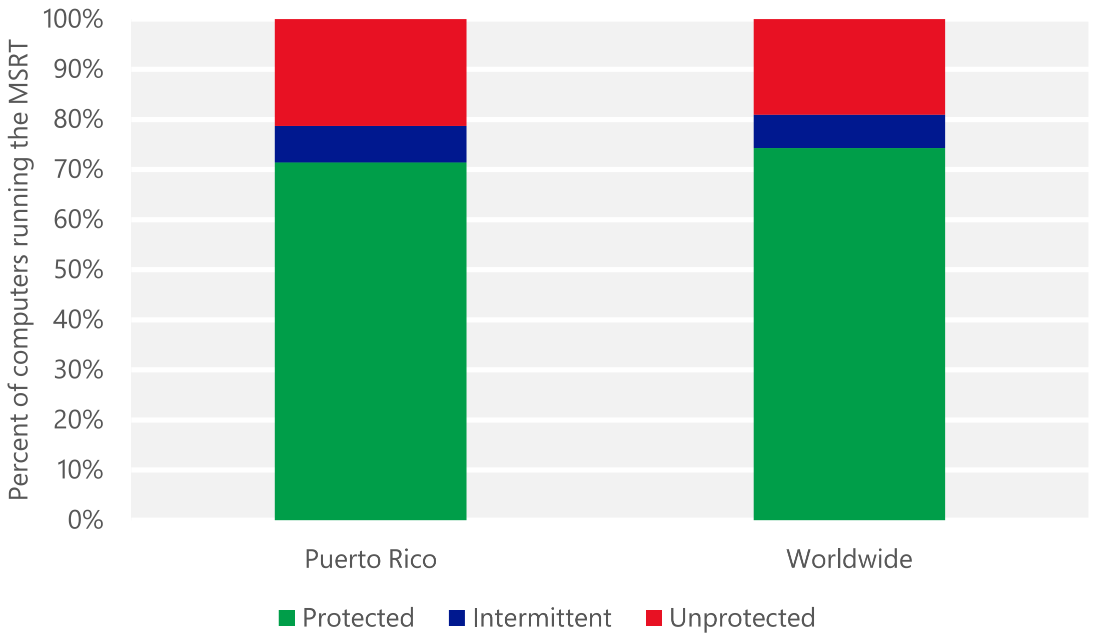
- The most common threat family infecting computers in Puerto Rico in 4Q14 was VBS/Jenxcus, which was detected and removed from 3.4 of every 1,000 unique computers scanned by the MSRT. VBS/Jenxcus is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Puerto Rico in 4Q14 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.
- The third most common threat family infecting computers in Puerto Rico in 4Q14 was Win32/Brontok, which was detected and removed from 1.1 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 Puerto Rico in 4Q14 was Win32/Sefnit, which was detected and removed from 0.3 of every 1,000 unique computers scanned by the MSRT. Win32/Sefnit is a family of trojans that can allow backdoor access, download files, and use the computer and Internet connection for click fraud. Some variants can monitor web browsers and hijack search results.

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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.16 drive-by download URLs for every 1,000 URLs hosted in Puerto Rico, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.01 drive-by download URLs for every 1,000 URLs hosted in Puerto Rico, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Puerto Rico and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Puerto Rico	0.16	0.01
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Qatar

The statistics presented here are generated by Microsoft security programs and services running on computers in Qatar in 4Q14 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 succeds 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

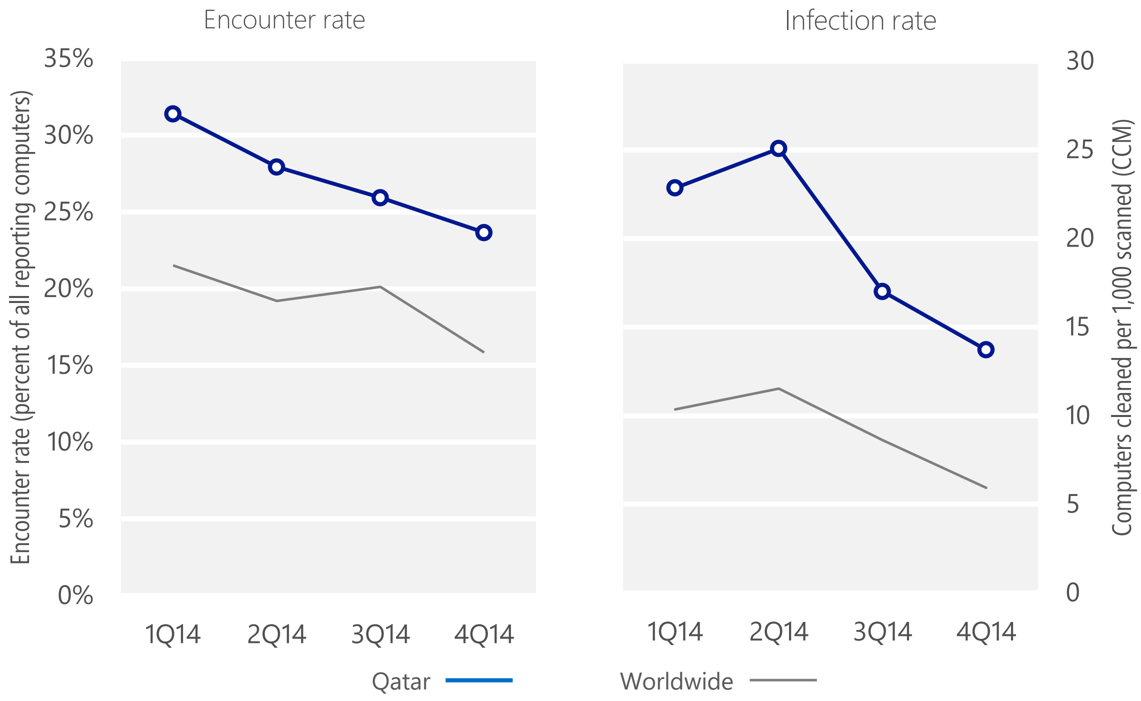
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Qatar	31.4%	27.9%	25.9%	23.7%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Qatar	22.9	25.1	17.0	13.7
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 23.7% percent of computers in Qatar encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 13.7 of every 1,000 unique computers scanned in Qatar in 4Q14 (a CCM score of 13.7, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Qatar over the last four quarters, compared to the world as a whole.

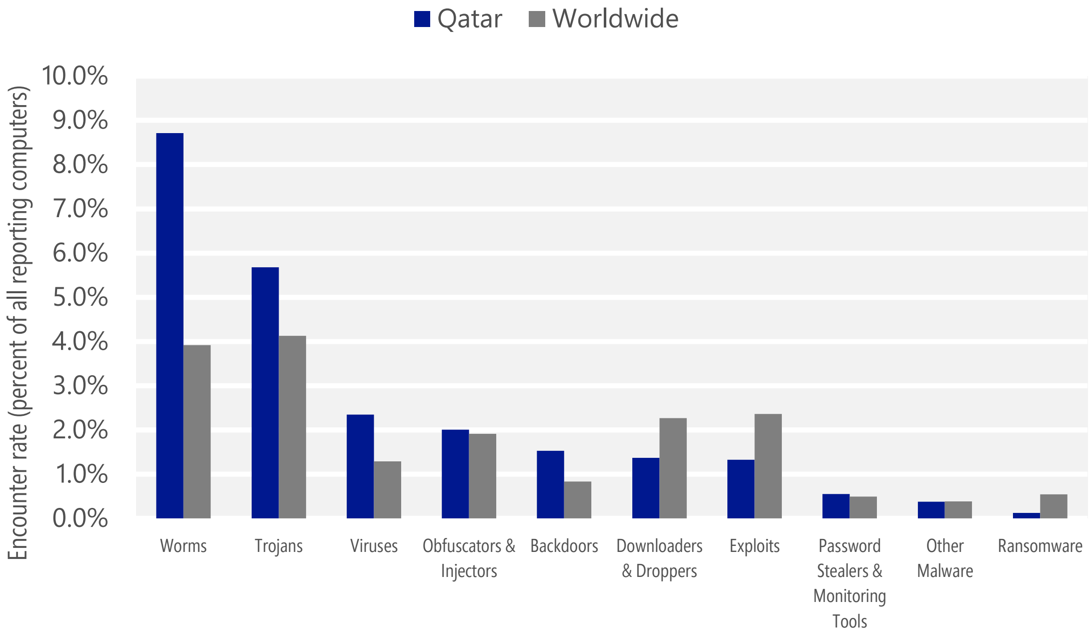
Malware encounter and infection rate trends in Qatar and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

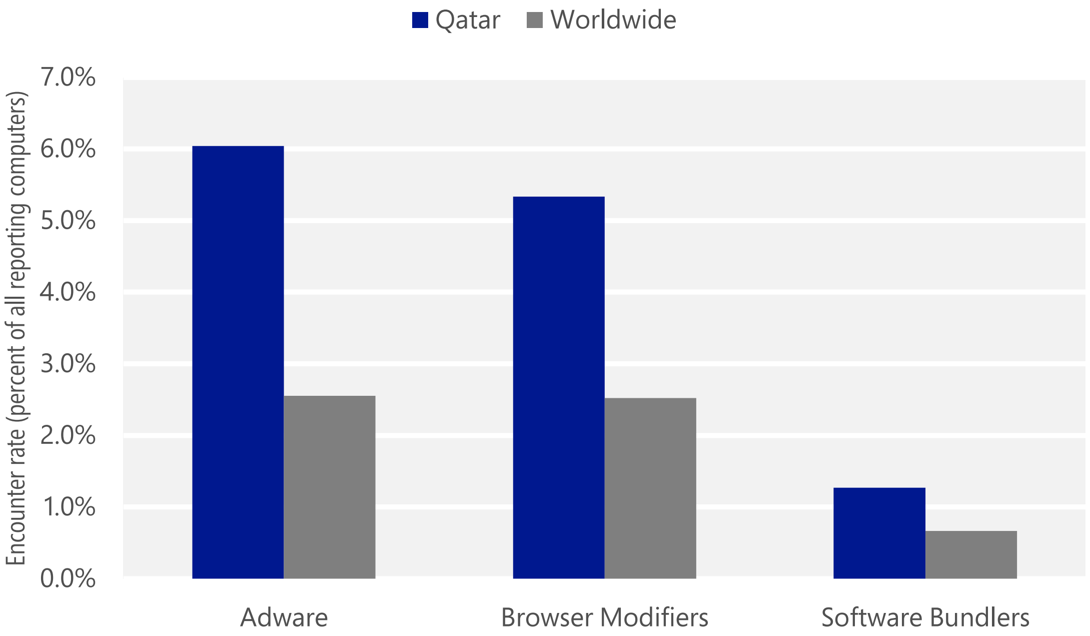
Malware encountered in Qatar in 4Q14, by category



- The most common malware category in Qatar in 4Q14 was Worms. It was encountered by 8.7 percent of all computers there, down from 8.8 percent in 3Q14.
- The second most common malware category in Qatar in 4Q14 was Trojans. It was encountered by 5.7 percent of all computers there, down from 8.2 percent in 3Q14.
- The third most common malware category in Qatar in 4Q14 was Viruses, which was encountered by 2.3 percent of all computers there, down from 3.2 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Qatar in 4Q14, by category



- The most common unwanted software category in Qatar in 4Q14 was Adware. It was encountered by 6.0 percent of all computers there, down from 7.4 percent in 3Q14.
- The second most common unwanted software category in Qatar in 4Q14 was Browser Modifiers. It was encountered by 5.3 percent of all computers there, up from 2.8 percent in 3Q14.
- The third most common unwanted software category in Qatar in 4Q14 was Software Bundlers, which was encountered by 1.3 percent of all computers there, up from 0.2 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Qatar in 4Q14

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	3.0%
2	INF/Autorun	Obfuscators & Injectors	2.0%
3	Win32/Gamarue	Worms	1.2%
4	Win32/Nuqel	Worms	1.0%
5	Win32/Startpage	Trojans	0.8%
6	Win32/Obfuscator	Obfuscators & Injectors	0.8%
7	ALisp/Bursted	Viruses	0.8%
8	Win32/Sality	Viruses	0.7%
9	MSIL/Bladabindi	Backdoors	0.7%
10	ALisp/Copicad	Worms	0.6%

- The most common malware family encountered in Qatar in 4Q14 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 Qatar in 4Q14 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.
- The third most common malware family encountered in Qatar in 4Q14 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 fourth most common malware family encountered in Qatar in 4Q14 was Win32/Nuqel, which was encountered by 1.0 percent of reporting computers there. 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.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Qatar in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	3.6%
2	Win32/Brya	Adware	3.4%
3	Win32/Defaulttab	Browser Modifiers	1.6%
4	Win32/BetterSurf	Adware	1.3%
5	Win32/Costmin	Adware	1.0%

- The most common unwanted software family encountered in Qatar in 4Q14 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 Qatar in 4Q14 was Win32/Brya, which was encountered by 3.4 percent of reporting computers there. Win32/Brya is a program that shows ads that the user cannot control as they browse the web. It does not have a working uninstaller.
- The third most common unwanted software family encountered in Qatar in 4Q14 was Win32/Defaulttab, which was encountered by 1.6 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.

Top threat families by infection rate

The most common malware families by infection rate in Qatar in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	4.5
2	Win32/Sality	Viruses	1.8
3	Win32/Gamarue	Worms	1.4
4	Win32/Nuqel	Worms	1.1
5	MSIL/Bladabindi	Backdoors	0.9
6	Win32/Brontok	Worms	0.5
7	Win32/Ramnit	Trojans	0.4
8	JS/Kilim	Trojans	0.4
9	Win32/Tupym	Worms	0.4
10	Win32/Vobfus	Worms	0.4

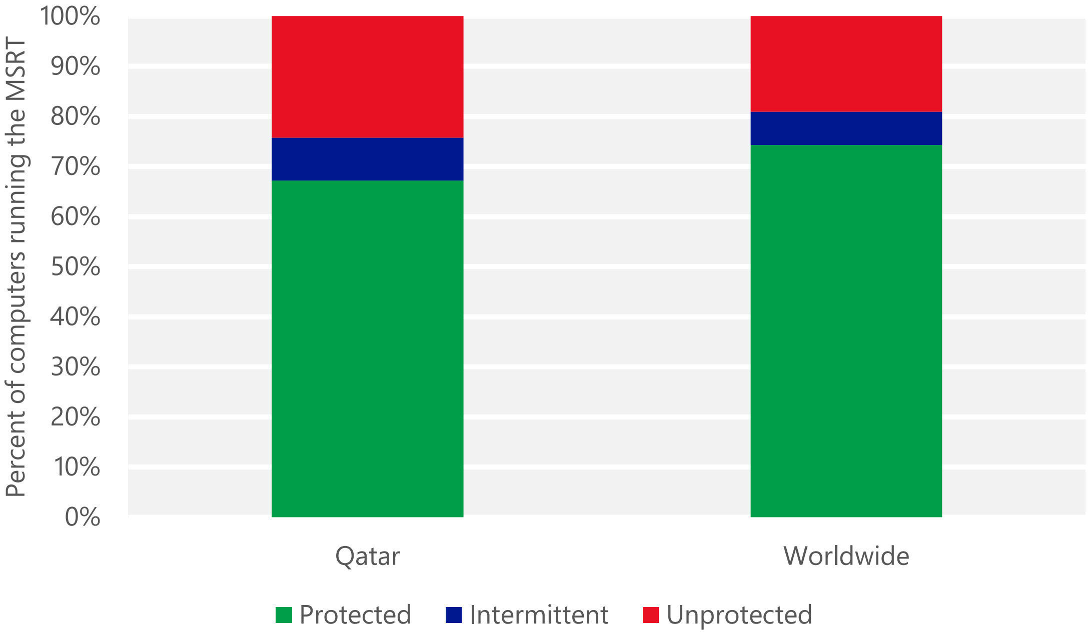
- The most common threat family infecting computers in Qatar in 4Q14 was VBS/Jenxcus, which was detected and removed from 4.5 of every 1,000 unique computers scanned by the MSRT. VBS/Jenxcus is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Qatar in 4Q14 was Win32/Sality, which was detected and removed from 1.8 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 third most common threat family infecting computers in Qatar in 4Q14 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 fourth most common threat family infecting computers in Qatar in 4Q14 was Win32/Nuqel, which was detected and removed from 1.1 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 Qatar and worldwide protected by real-time security software in 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.00 drive-by download URLs for every 1,000 URLs hosted in Qatar, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.00 drive-by download URLs for every 1,000 URLs hosted in Qatar, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Qatar and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Qatar	0.00	0.00
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Romania

The statistics presented here are generated by Microsoft security programs and services running on computers in Romania in 4Q14 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 succeds 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

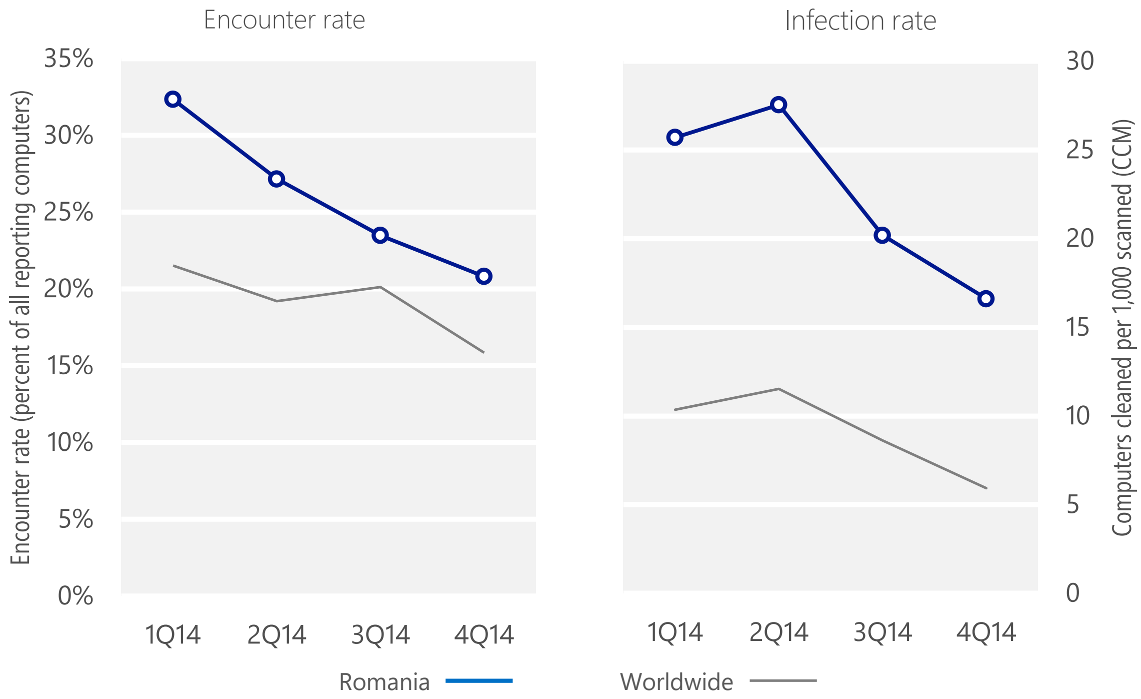
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Romania	32.3%	27.2%	23.5%	20.8%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Romania	25.7	27.5	20.2	16.6
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 20.8% percent of computers in Romania encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 16.6 of every 1,000 unique computers scanned in Romania in 4Q14 (a CCM score of 16.6, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Romania over the last four quarters, compared to the world as a whole.

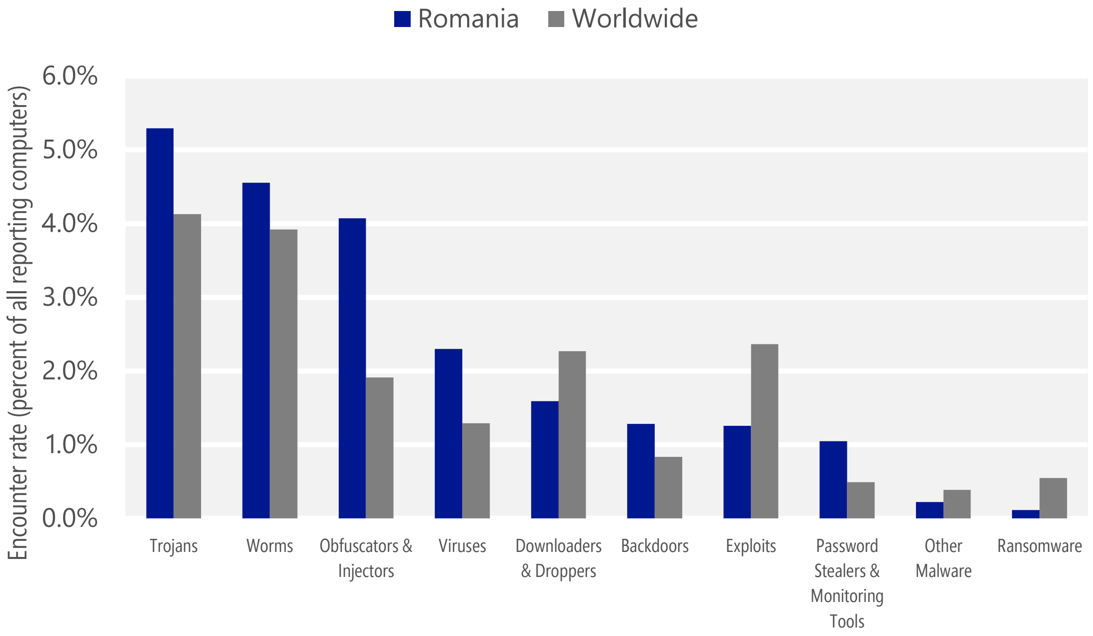
Malware encounter and infection rate trends in Romania and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

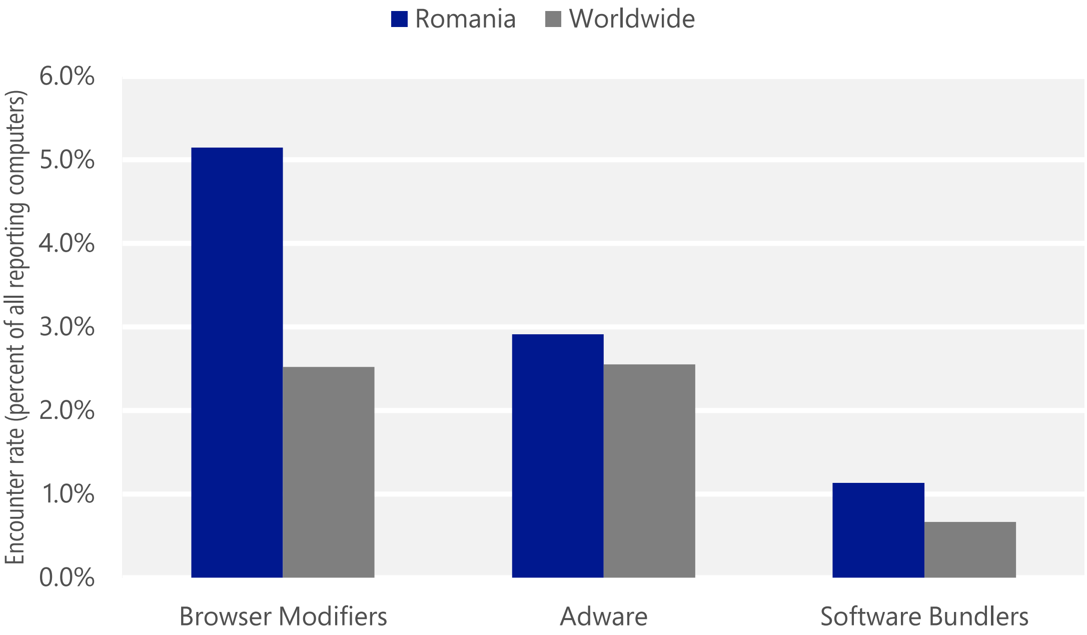
Malware encountered in Romania in 4Q14, by category



- The most common malware category in Romania in 4Q14 was Trojans. It was encountered by 5.3 percent of all computers there, down from 8.6 percent in 3Q14.
- The second most common malware category in Romania in 4Q14 was Worms. It was encountered by 4.6 percent of all computers there, down from 4.6 percent in 3Q14.
- The third most common malware category in Romania in 4Q14 was Obfuscators & Injectors, which was encountered by 4.1 percent of all computers there, down from 4.1 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Romania in 4Q14, by category



- The most common unwanted software category in Romania in 4Q14 was Browser Modifiers. It was encountered by 5.1 percent of all computers there, down from 6.9 percent in 3Q14.
- The second most common unwanted software category in Romania in 4Q14 was Adware. It was encountered by 2.9 percent of all computers there, up from 0.8 percent in 3Q14.
- The third most common unwanted software category in Romania in 4Q14 was Software Bundlers, which was encountered by 1.1 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Romania in 4Q14

	Family	Most significant category	% of reporting computers
1	INF/Autorun	Obfuscators & Injectors	2.1%
2	Win32/Obfuscator	Obfuscators & Injectors	1.9%
3	Win32/Sality	Viruses	1.3%
4	Win32/Brontok	Worms	0.9%
5	Win32/Conficker	Worms	0.9%
6	VBS/Jenxcus	Worms	0.8%
7	Win32/Gamarue	Worms	0.8%
8	Win32/Dynamer	Trojans	0.6%
9	Win32/Neshta	Viruses	0.6%
10	Win32/Ramnit	Trojans	0.5%

- The most common malware family encountered in Romania in 4Q14 was INF/Autorun, which was encountered by 2.1 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 second most common malware family encountered in Romania in 4Q14 was Win32/Obfuscator, which was encountered by 1.9 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 third most common malware family encountered in Romania in 4Q14 was Win32/Sality, which was encountered by 1.3 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 Romania in 4Q14 was Win32/Brontok, which was encountered by 0.9 percent of reporting computers there. 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.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Romania in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	4.0%
2	Win32/Costmin	Adware	1.5%
3	Win32/Defaulttab	Browser Modifiers	1.3%
4	Win32/BetterSurf	Adware	1.2%
5	Win32/Gofileexpress	Software Bundlers	0.9%

- The most common unwanted software family encountered in Romania in 4Q14 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 Romania in 4Q14 was Win32/Costmin, which was encountered by 1.5 percent of reporting computers there. Win32/Costmin is an adware family that installs itself as a browser extension for Internet Explorer, Mozilla Firefox, and Google Chrome, and displays advertisements as the user browses the Internet.
- The third most common unwanted software family encountered in Romania in 4Q14 was Win32/Defaulttab, which was encountered by 1.3 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.

Top threat families by infection rate

The most common malware families by infection rate in Romania in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Sality	Viruses	6.2
2	Win32/Brontok	Worms	2.1
3	Win32/Ramnit	Trojans	1.5
4	Win32/Pramro	Trojans	1.4
5	VBS/Jenxcus	Worms	1.4
6	JS/Kilim	Trojans	1.1
7	Win32/Gamarue	Worms	1.0
8	Win32/Helompy	Worms	0.6
9	Win32/Wysotot	Trojans	0.4
10	Win32/Sefnit	Trojans	0.4

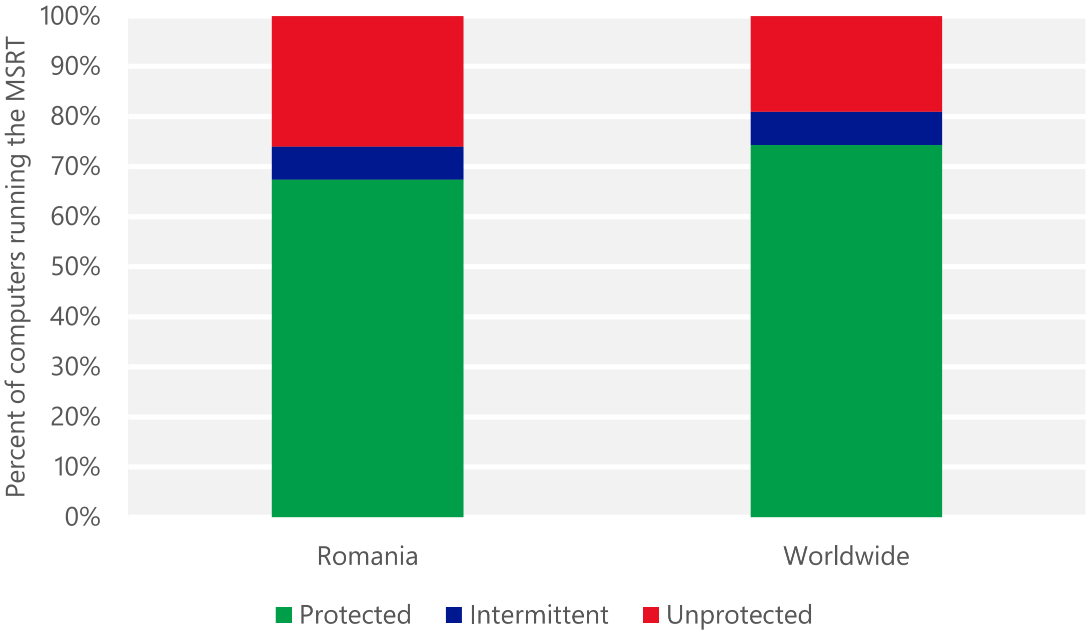
- The most common threat family infecting computers in Romania in 4Q14 was Win32/Sality, which was detected and removed from 6.2 of every 1,000 unique computers scanned by the MSRT. Win32/Sality is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The second most common threat family infecting computers in Romania in 4Q14 was Win32/Brontok, which was detected and removed from 2.1 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 Romania in 4Q14 was Win32/Ramnit, which was detected and removed from 1.5 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 Romania in 4Q14 was Win32/Pramro, which was detected and removed from 1.4 of every 1,000 unique computers scanned by the MSRT. Win32/Pramro is a trojan that creates a proxy on the infected computer for email and HTTP traffic, and is used to send spam email.

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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.24 drive-by download URLs for every 1,000 URLs hosted in Romania, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.23 drive-by download URLs for every 1,000 URLs hosted in Romania, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Romania and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Romania	0.24	0.23
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Russia

The statistics presented here are generated by Microsoft security programs and services running on computers in Russia in 4Q14 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 succeds 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

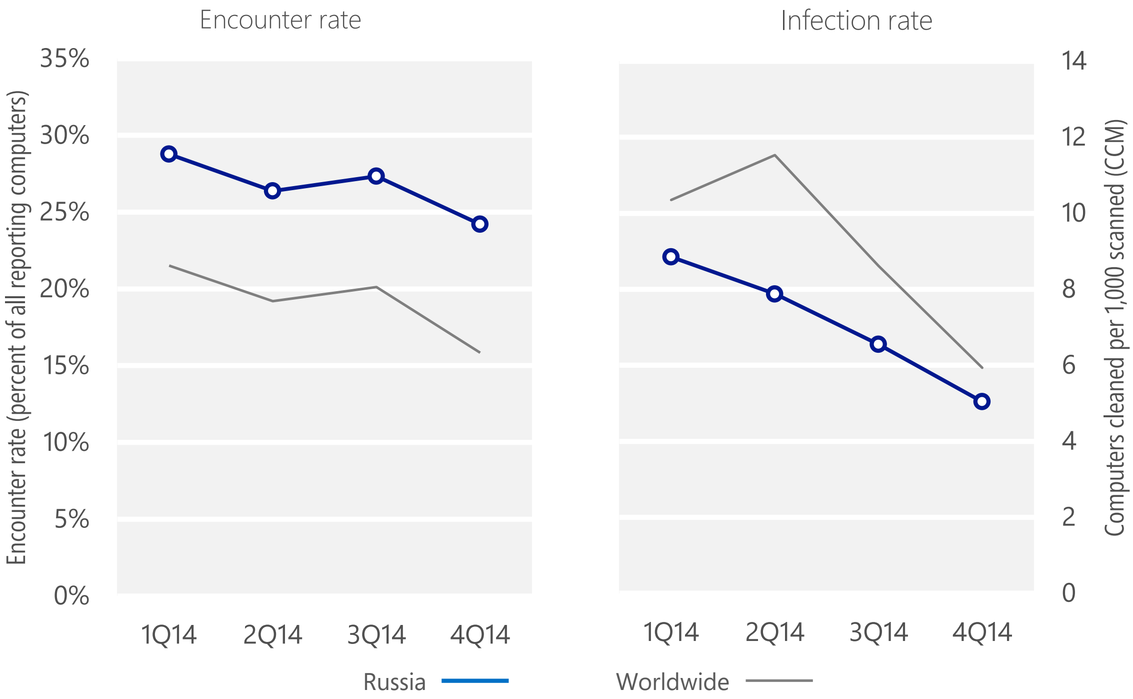
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Russia	28.8%	26.4%	27.3%	24.2%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Russia	8.9	7.9	6.6	5.0
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 24.2% percent of computers in Russia encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 5.0 of every 1,000 unique computers scanned in Russia in 4Q14 (a CCM score of 5.0, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Russia over the last four quarters, compared to the world as a whole.

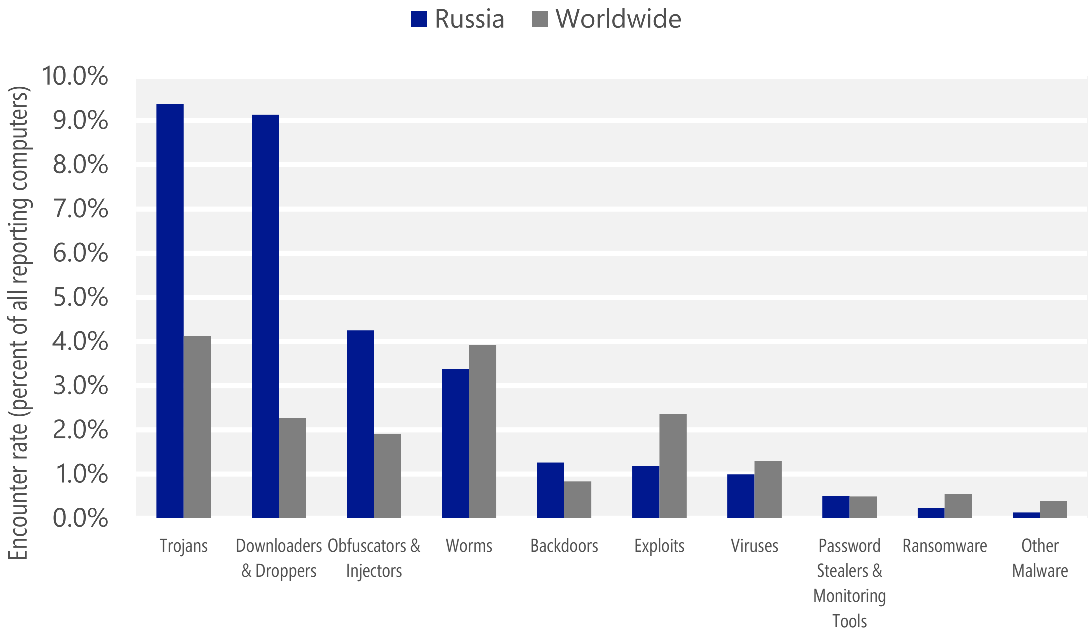
Malware encounter and infection rate trends in Russia and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

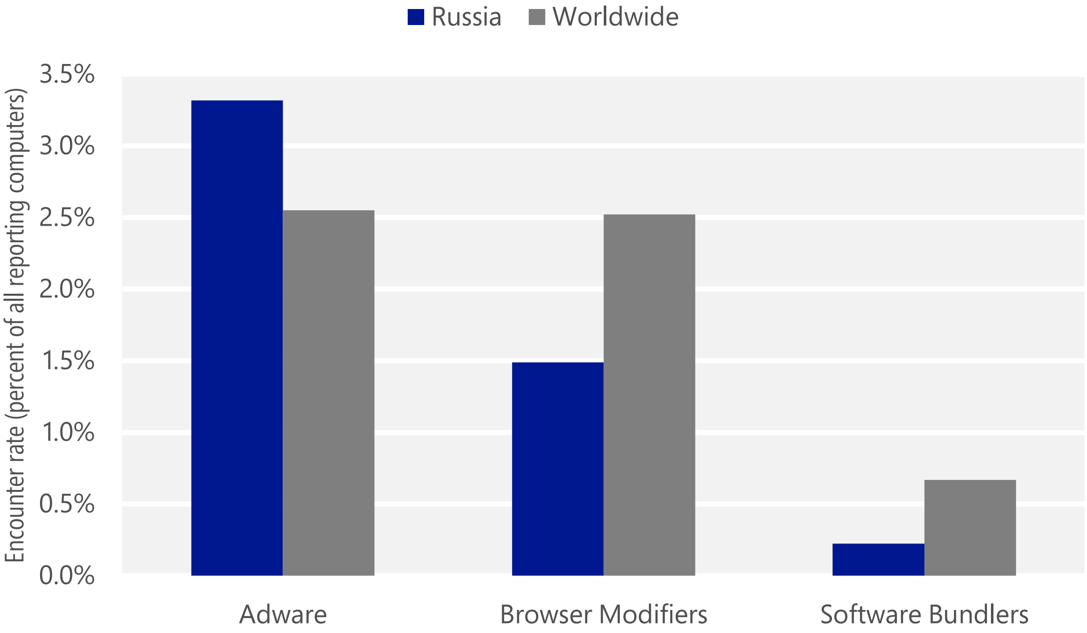
Malware encountered in Russia in 4Q14, by category



- The most common malware category in Russia in 4Q14 was Trojans. It was encountered by 9.4 percent of all computers there, down from 11.9 percent in 3Q14.
- The second most common malware category in Russia in 4Q14 was Downloaders & Droppers. It was encountered by 9.1 percent of all computers there, down from 10.2 percent in 3Q14.
- The third most common malware category in Russia in 4Q14 was Obfuscators & Injectors, which was encountered by 4.3 percent of all computers there, up from 3.9 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Russia in 4Q14, by category



- The most common unwanted software category in Russia in 4Q14 was Adware. It was encountered by 3.3 percent of all computers there, down from 5.3 percent in 3Q14.
- The second most common unwanted software category in Russia in 4Q14 was Browser Modifiers. It was encountered by 1.5 percent of all computers there, up from 0.4 percent in 3Q14.
- The third most common unwanted software category in Russia in 4Q14 was Software Bundlers, which was encountered by 0.2 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Russia in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Ogimant	Downloaders & Droppers	8.1%
2	Win32/Obfuscator	Obfuscators & Injectors	3.6%
3	Win32/Peaac	Trojans	2.9%
4	Win32/Dynamer	Trojans	0.9%
5	Win32/Peals	Trojans	0.8%
6	INF/Autorun	Obfuscators & Injectors	0.8%
7	Win32/Gamarue	Worms	0.7%
8	Win32/Dorkbot	Worms	0.6%
9	JS/Redirector	Trojans	0.5%
10	Win32/Anaki	Trojans	0.5%

- The most common malware family encountered in Russia in 4Q14 was Win32/Ogimant, which was encountered by 8.1 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 second most common malware family encountered in Russia in 4Q14 was Win32/Obfuscator, which was encountered by 3.6 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 Russia in 4Q14 was Win32/Peaac, which was encountered by 2.9 percent of reporting computers there. Win32/Peaac is a generic detection for various threats that display trojan characteristics.
- The fourth most common malware family encountered in Russia in 4Q14 was Win32/Dynamer, which was encountered by 0.9 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 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/BetterSurf	Adware	1.4%
2	Win32/Couponruc	Browser Modifiers	1.3%
3	Win32/Pirrit	Adware	0.9%
4	Win32/Pennybee	Adware	0.8%
5	Win32/Costmin	Adware	0.2%

- The most common unwanted software family encountered in Russia in 4Q14 was Win32/BetterSurf, which was encountered by 1.4 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.
- The second most common unwanted software family encountered in Russia in 4Q14 was Win32/Couponruc, which was encountered by 1.3 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 Russia in 4Q14 was Win32/Pirrit, which was encountered by 0.9 percent of reporting computers there. Win32/Pirrit is a program that shows ads as the user browses the web. It can be downloaded from the program's website or bundled with some third-party software installation programs.

Top threat families by infection rate

The most common malware families by infection rate in Russia in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Gamarue	Worms	0.8
2	Win32/Brontok	Worms	0.6
3	Win32/Dorkbot	Worms	0.6
4	Win32/Ramnit	Trojans	0.5
5	Win32/Sality	Viruses	0.3
6	Win32/Tofsee	Backdoors	0.3
7	Win32/Lethic	Trojans	0.2
8	Win32/Deminnix	Trojans	0.2
9	Win32/Wysotot	Trojans	0.2
10	Win32/Sefnit	Trojans	0.2

- The most common threat family infecting computers in Russia in 4Q14 was Win32/Gamarue, which was detected and removed from 0.8 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 second most common threat family infecting computers in Russia in 4Q14 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 third most common threat family infecting computers in Russia in 4Q14 was Win32/Dorkbot, which was detected and removed from 0.6 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 Russia in 4Q14 was Win32/Ramnit, which was detected and removed from 0.5 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

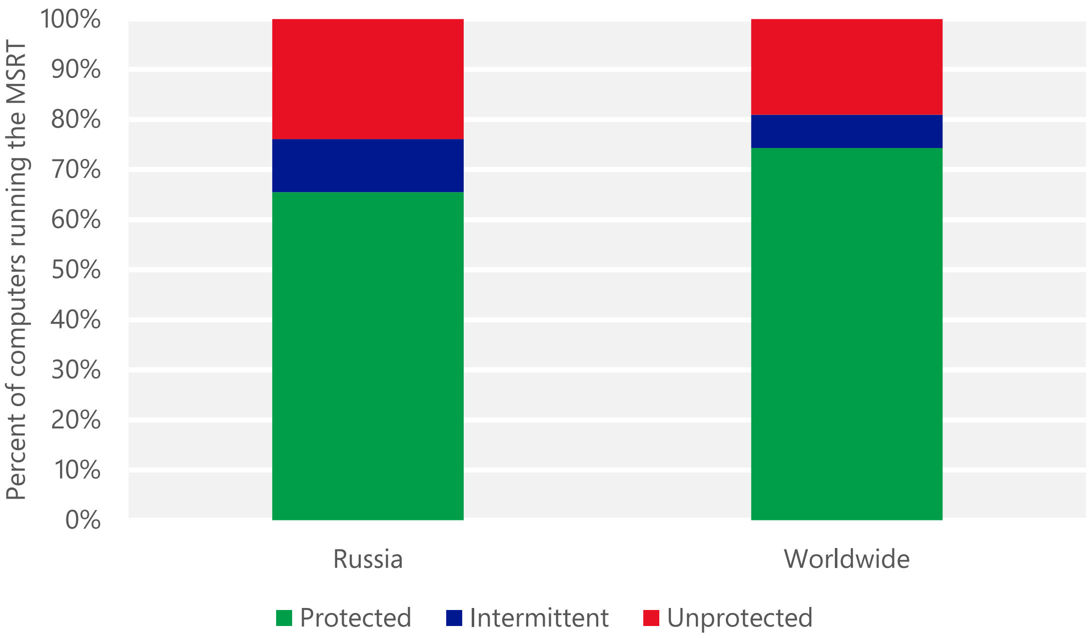
information such as saved FTP credentials and browser cookies. It may also open a backdoor to await instructions from a remote attacker.

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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 2.59 drive-by download URLs for every 1,000 URLs hosted in Russia, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 2.39 drive-by download URLs for every 1,000 URLs hosted in Russia, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Russia and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Russia	2.59	2.39
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Saudi Arabia

The statistics presented here are generated by Microsoft security programs and services running on computers in Saudi Arabia in 4Q14 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 succeds 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

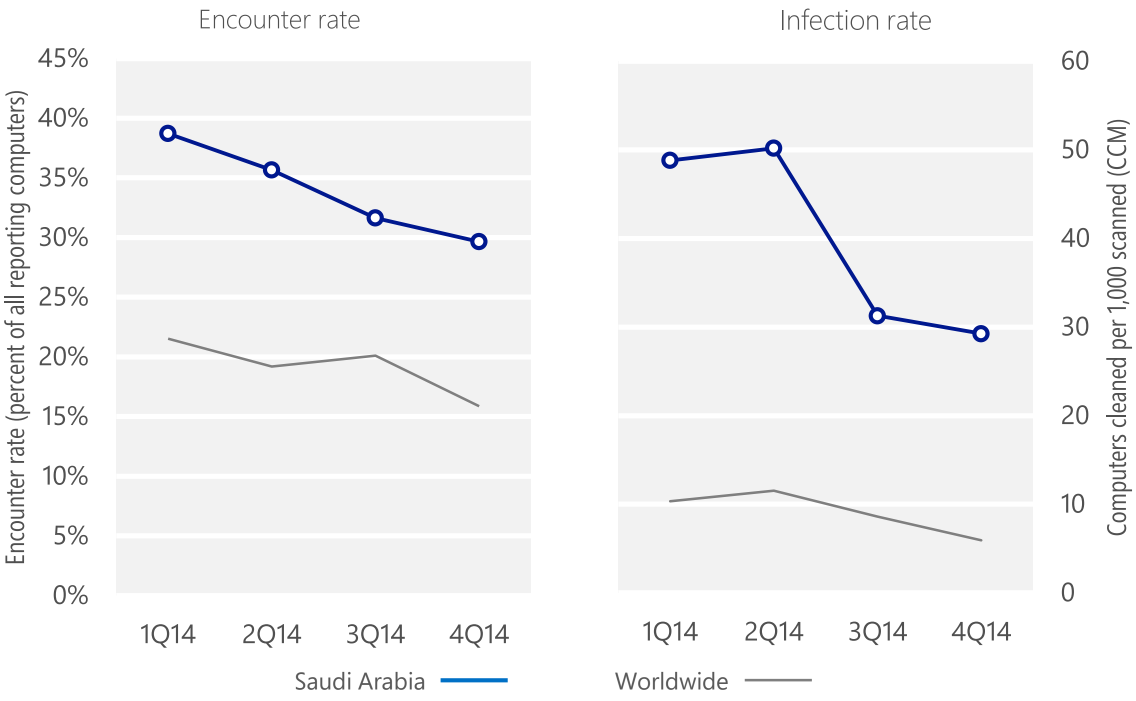
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Saudi Arabia	38.7%	35.7%	31.6%	29.7%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Saudi Arabia	48.8	50.2	31.3	29.3
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 29.7% percent of computers in Saudi Arabia encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 29.3 of every 1,000 unique computers scanned in Saudi Arabia in 4Q14 (a CCM score of 29.3, compared to the 4Q14 worldwide CCM of 5.9). 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.

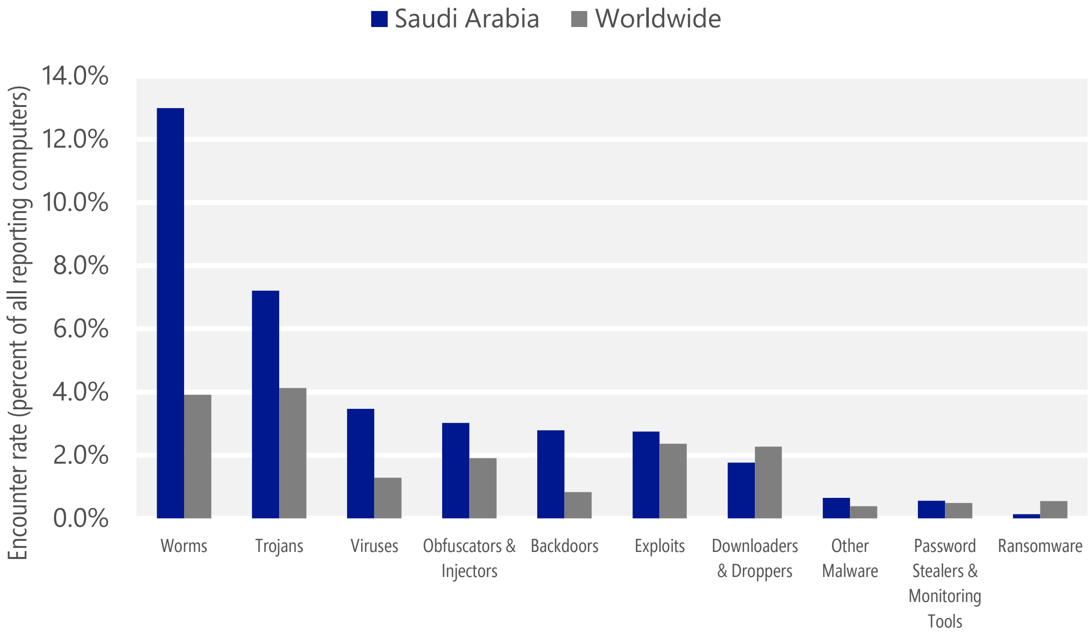
Malware encounter and infection rate trends in Saudi Arabia and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

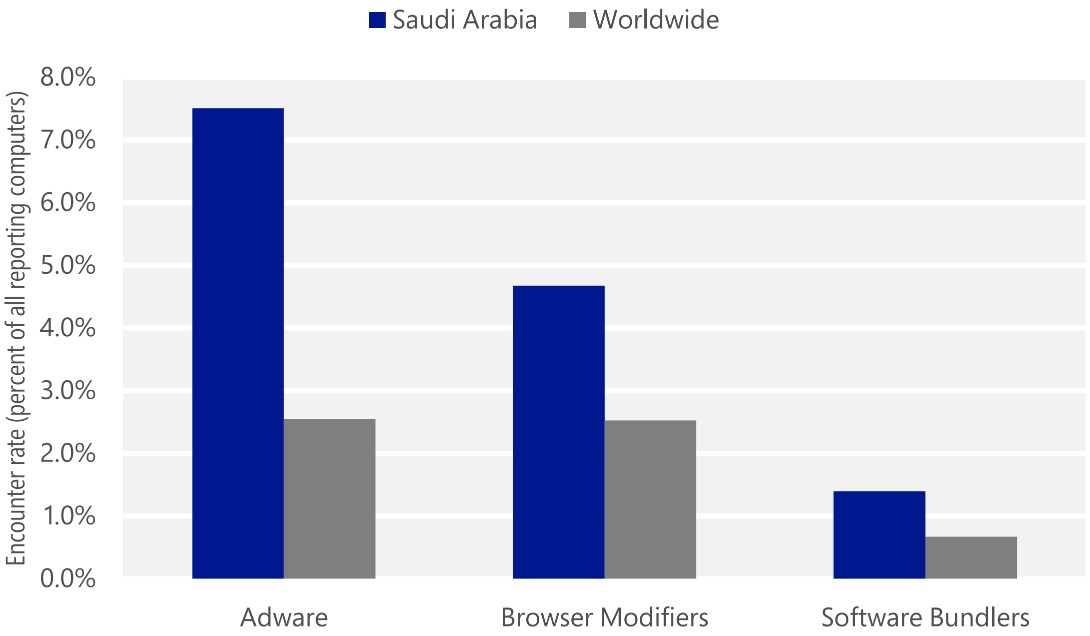
Malware encountered in Saudi Arabia in 4Q14, by category



- The most common malware category in Saudi Arabia in 4Q14 was Worms. It was encountered by 13.0 percent of all computers there, up from 11.1 percent in 3Q14.
- The second most common malware category in Saudi Arabia in 4Q14 was Trojans. It was encountered by 7.2 percent of all computers there, down from 8.9 percent in 3Q14.
- The third most common malware category in Saudi Arabia in 4Q14 was Viruses, which was encountered by 3.5 percent of all computers there, down from 4.5 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Saudi Arabia in 4Q14, by category



- The most common unwanted software category in Saudi Arabia in 4Q14 was Adware. It was encountered by 7.5 percent of all computers there, down from 8.9 percent in 3Q14.
- The second most common unwanted software category in Saudi Arabia in 4Q14 was Browser Modifiers. It was encountered by 4.7 percent of all computers there, up from 3.1 percent in 3Q14.
- The third most common unwanted software category in Saudi Arabia in 4Q14 was Software Bundlers, which was encountered by 1.4 percent of all computers there, up from 0.2 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Saudi Arabia in 4Q14

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	8.2%
2	INF/Autorun	Obfuscators & Injectors	2.7%
3	Win32/Sality	Viruses	1.3%
4	MSIL/Bladabindi	Backdoors	1.3%
5	Win32/CplLnk	Exploits	1.3%
6	JS/Bondat	Worms	1.2%
7	Win32/Ramnit	Trojans	1.2%
8	Win32/Startpage	Trojans	1.0%
9	Win32/Obfuscator	Obfuscators & Injectors	1.0%
10	Win32/Gamarue	Worms	0.9%

- The most common malware family encountered in Saudi Arabia in 4Q14 was VBS/Jenxcus, which was encountered by 8.2 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 4Q14 was INF/Autorun, which was encountered by 2.7 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 Saudi Arabia in 4Q14 was Win32/Sality, which was encountered by 1.3 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 Saudi Arabia in 4Q14 was MSIL/Bladabindi, which was encountered by 1.3 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.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Saudi Arabia in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Brya	Adware	4.6%
2	Win32/Couponruc	Browser Modifiers	3.3%
3	Win32/Costmin	Adware	1.4%
4	Win32/BetterSurf	Adware	1.3%
5	Win32/Defaulttab	Browser Modifiers	1.1%

- The most common unwanted software family encountered in Saudi Arabia in 4Q14 was Win32/Brya, which was encountered by 4.6 percent of reporting computers there. Win32/Brya is a program that shows ads that the user cannot control as they browse the web. It does not have a working uninstaller.
- The second most common unwanted software family encountered in Saudi Arabia in 4Q14 was Win32/Couponruc, which was encountered by 3.3 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 Saudi Arabia in 4Q14 was Win32/Costmin, which was encountered by 1.4 percent of reporting computers there. Win32/Costmin is an adware family that installs itself as a browser extension for Internet Explorer, Mozilla Firefox, and Google Chrome, and displays advertisements as the user browses the Internet.

Top threat families by infection rate

The most common malware families by infection rate in Saudi Arabia in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	16.3
2	Win32/Sality	Viruses	4.0
3	MSIL/Bladabindi	Backdoors	2.4
4	Win32/Ramnit	Trojans	1.4
5	Win32/Gamarue	Worms	0.9
6	Win32/Brontok	Worms	0.7
7	Win32/Pramro	Trojans	0.7
8	Win32/Nuqel	Worms	0.6
9	Win32/Dorkbot	Worms	0.6
10	Win32/Vobfus	Worms	0.6

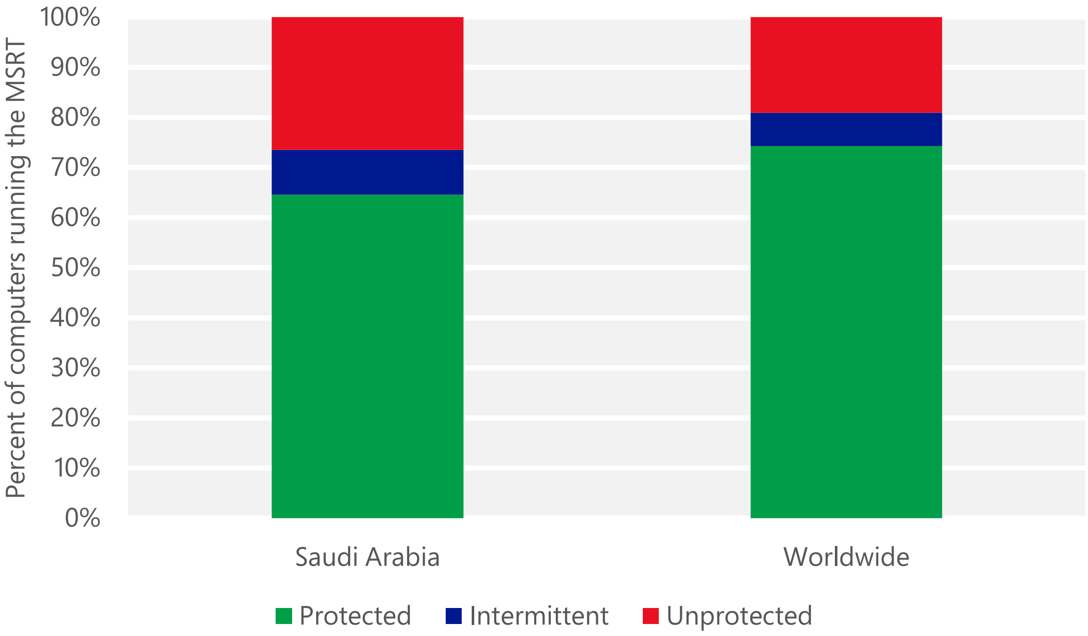
- The most common threat family infecting computers in Saudi Arabia in 4Q14 was VBS/Jenxcus, which was detected and removed from 16.3 of every 1,000 unique computers scanned by the MSRT. VBS/Jenxcus is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Saudi Arabia in 4Q14 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.
- The third most common threat family infecting computers in Saudi Arabia in 4Q14 was MSIL/Bladabindi, which was detected and removed from 2.4 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 Saudi Arabia in 4Q14 was Win32/Ramnit, which was detected and removed from 1.4 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 Saudi Arabia and worldwide protected by real-time security software in 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.12 drive-by download URLs for every 1,000 URLs hosted in Saudi Arabia, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.07 drive-by download URLs for every 1,000 URLs hosted in Saudi Arabia, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Saudi Arabia and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Saudi Arabia	0.12	0.07
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Senegal

The statistics presented here are generated by Microsoft security programs and services running on computers in Senegal in 4Q14 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 succeds 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

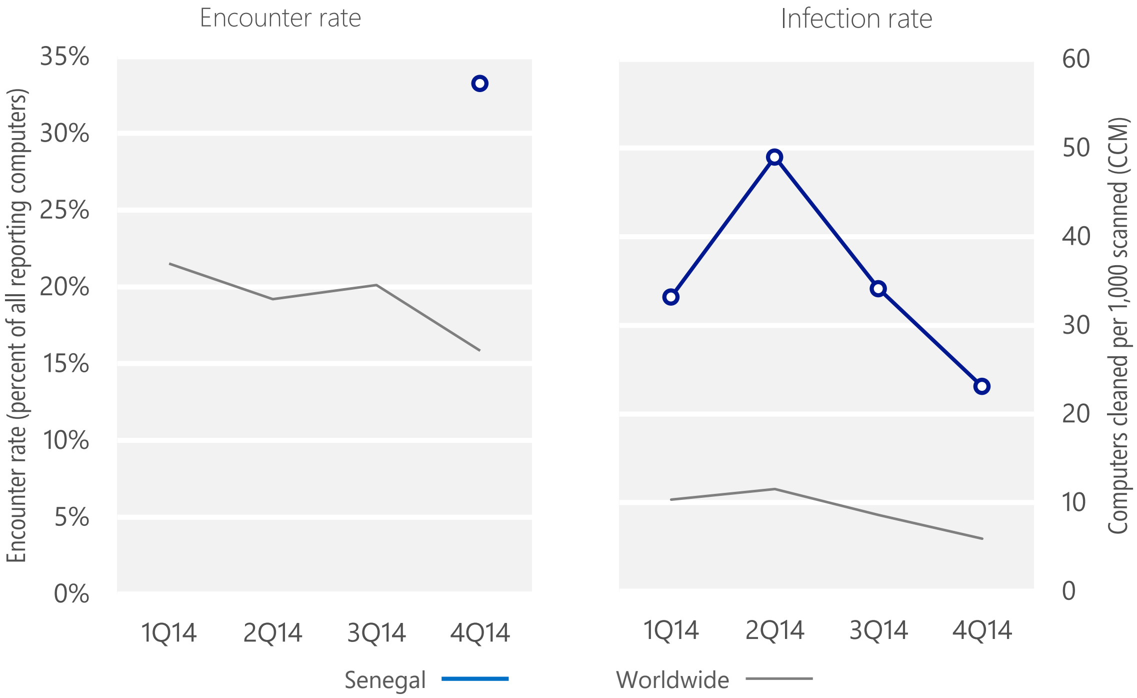
Metric	**1Q14**	**2Q14**	**3Q14**	**4Q14**
Encounter rate, Senegal	N/A	N/A	N/A	33.2%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Senegal	33.2	49.0	34.1	23.1
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 33.2% percent of computers in Senegal encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 23.1 of every 1,000 unique computers scanned in Senegal in 4Q14 (a CCM score of 23.1, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Senegal over the last four quarters, compared to the world as a whole.

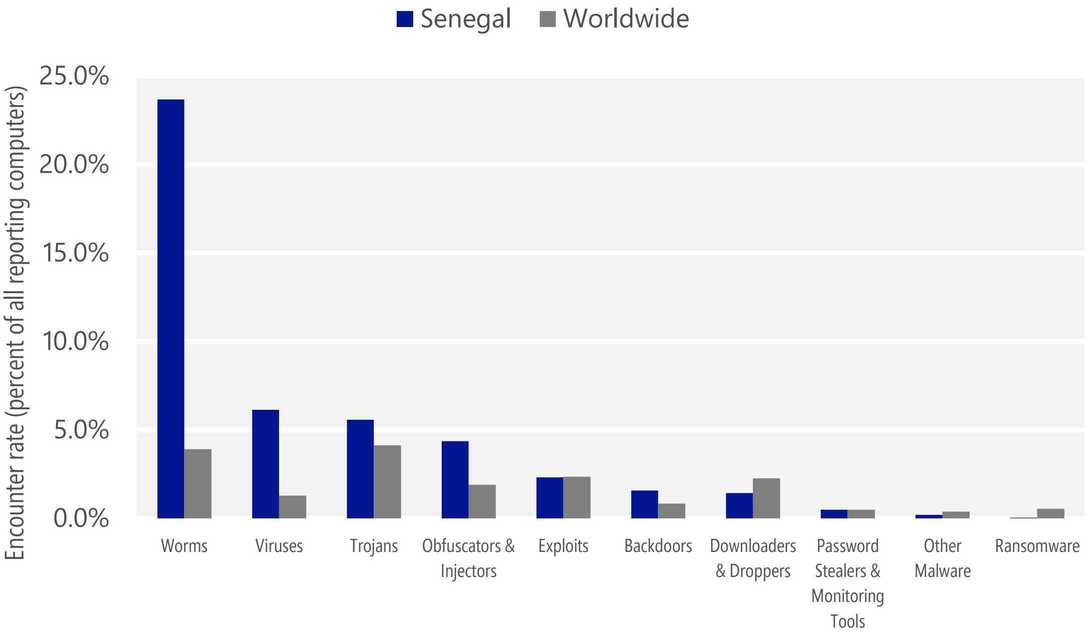
Malware encounter and infection rate trends in Senegal and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

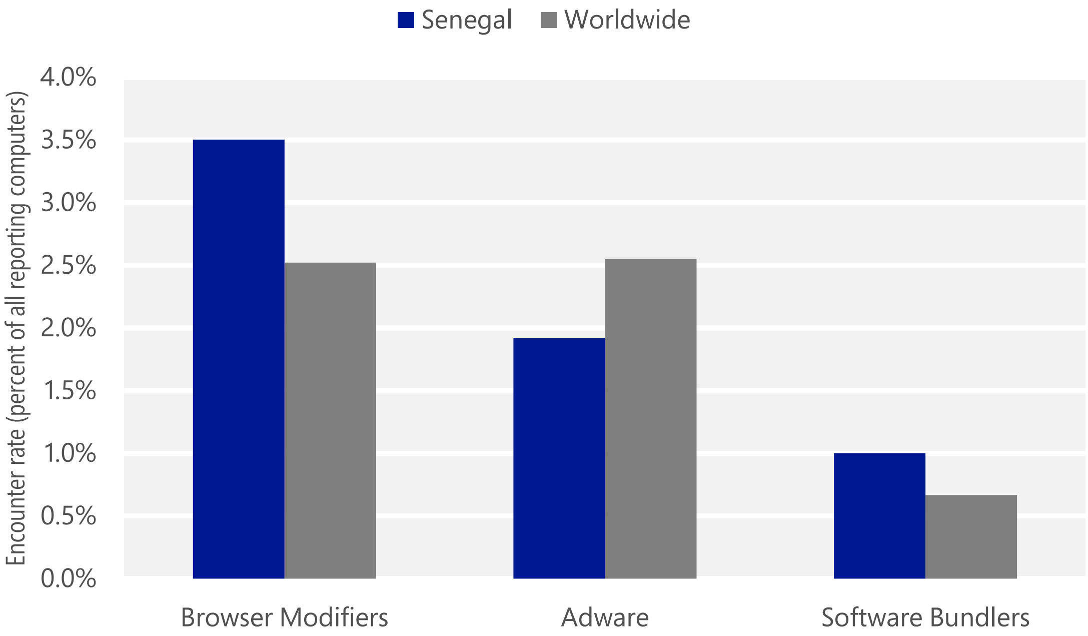
Malware encountered in Senegal in 4Q14, by category



- The most common malware category in Senegal in 4Q14 was Worms. It was encountered by 23.7 percent of all computers there, up from N/A percent in 3Q14.
- The second most common malware category in Senegal in 4Q14 was Viruses. It was encountered by 6.2 percent of all computers there, up from N/A percent in 3Q14.
- The third most common malware category in Senegal in 4Q14 was Trojans, which was encountered by 5.6 percent of all computers there, up from N/A percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Senegal in 4Q14, by category



- The most common unwanted software category in Senegal in 4Q14 was Browser Modifiers. It was encountered by 3.5 percent of all computers there, up from N/A percent in 3Q14.
- The second most common unwanted software category in Senegal in 4Q14 was Adware. It was encountered by 1.9 percent of all computers there, up from N/A percent in 3Q14.
- The third most common unwanted software category in Senegal in 4Q14 was Software Bundlers, which was encountered by 1.0 percent of all computers there, up from N/A percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Senegal in 4Q14

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	11.7%
2	INF/Autorun	Obfuscators & Injectors	6.7%
3	VBS/Rtbot	Worms	5.3%
4	VBS/Cantix	Worms	4.8%
5	Win32/Sality	Viruses	3.4%
6	Win32/Ippedo	Worms	2.8%
7	Win32/Virut	Viruses	2.7%
8	Win32/Macoute	Worms	2.6%
9	Win32/Ramnit	Trojans	2.5%
10	Win32/CplLnk	Exploits	1.8%

- The most common malware family encountered in Senegal in 4Q14 was VBS/Jenxcus, which was encountered by 11.7 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 Senegal in 4Q14 was INF/Autorun, which was encountered by 6.7 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 Senegal in 4Q14 was VBS/Rtbot, which was encountered by 5.3 percent of reporting computers there. VBS/Rtbot is a worm that gives a malicious hacker access to and control of the computer. It spreads through infected removable drives, such as USB flash drives; drops other malware; and modifies computer settings.
- The fourth most common malware family encountered in Senegal in 4Q14 was VBS/Cantix, which was encountered by 4.8 percent of reporting computers there. VBS/Cantix is a worm written in VBScript that spreads via removable drives

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Senegal in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	2.5%
2	Win32/Defaulttab	Browser Modifiers	1.1%

- The most common unwanted software family encountered in Senegal in 4Q14 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 Senegal in 4Q14 was Win32/Defaulttab, which was encountered by 1.1 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.
- The third most common unwanted software family encountered in Senegal in 4Q14 was N/A, which was encountered by percent of reporting computers there.

Top threat families by infection rate

The most common malware families by infection rate in Senegal in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	11.9
2	Win32/Sality	Viruses	5.7
3	Win32/Ramnit	Trojans	1.8
4	Win32/Gamarue	Worms	1.0
5	Win32/Pramro	Trojans	0.6
6	MSIL/Bladabindi	Backdoors	0.6
7	Win32/Yeltminky	Worms	0.6
8	Win32/Vobfus	Worms	0.4
9	Win32/Chir	Viruses	0.3
10	Win32/Sefnit	Trojans	0.3

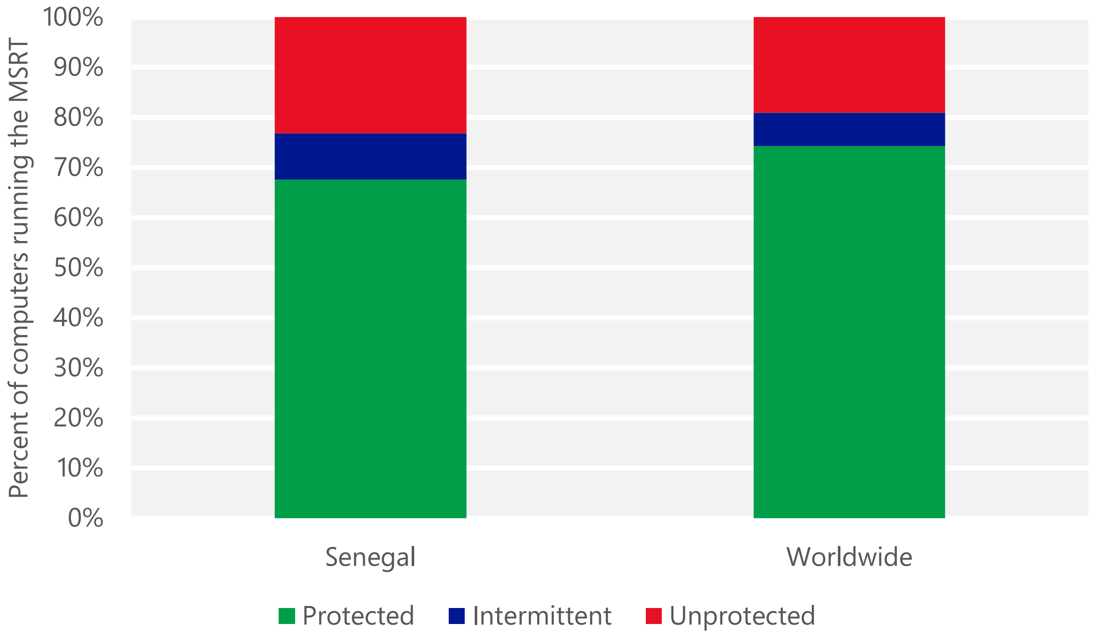
- The most common threat family infecting computers in Senegal in 4Q14 was VBS/Jenxcus, which was detected and removed from 11.9 of every 1,000 unique computers scanned by the MSRT. VBS/Jenxcus is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Senegal in 4Q14 was Win32/Sality, which was detected and removed from 5.7 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 Senegal in 4Q14 was Win32/Ramnit, which was detected and removed from 1.8 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 Senegal in 4Q14 was Win32/Gamarue, which was detected and removed from 1.0 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.

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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.10 drive-by download URLs for every 1,000 URLs hosted in Senegal, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.10 drive-by download URLs for every 1,000 URLs hosted in Senegal, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Senegal and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Senegal	0.10	0.10
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Serbia

The statistics presented here are generated by Microsoft security programs and services running on computers in Serbia in 4Q14 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 succeds 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

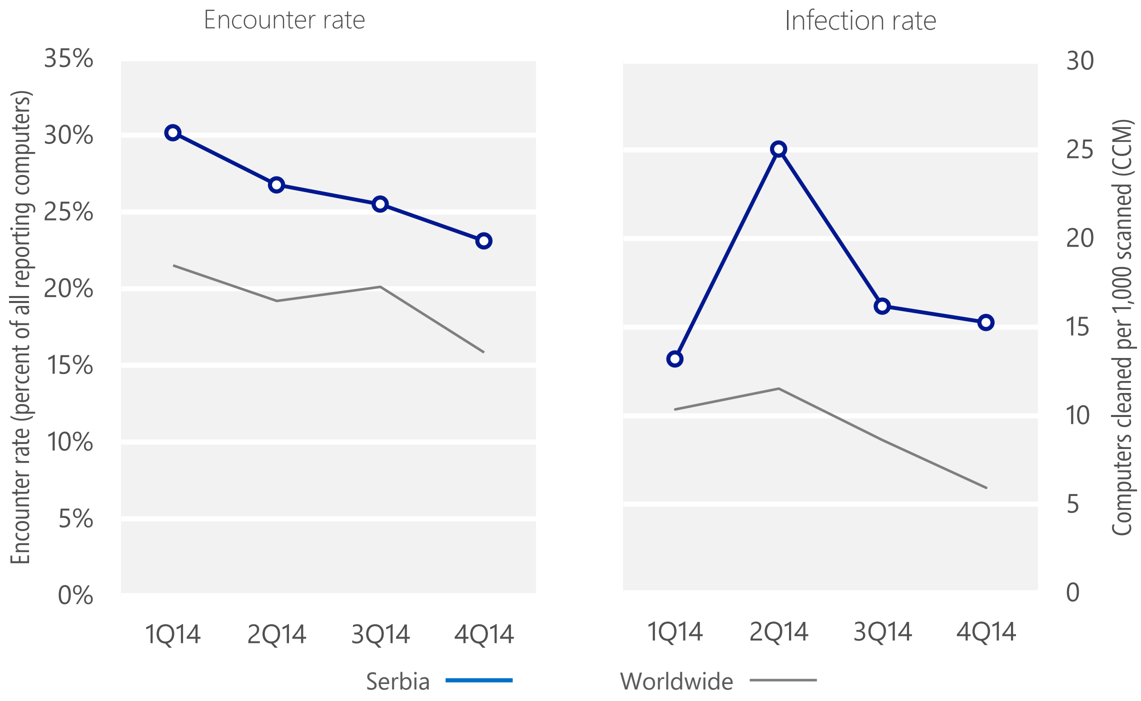
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Serbia	30.2%	26.8%	25.5%	23.1%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Serbia	13.2	25.0	16.2	15.3
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 23.1% percent of computers in Serbia encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 15.3 of every 1,000 unique computers scanned in Serbia in 4Q14 (a CCM score of 15.3, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Serbia over the last four quarters, compared to the world as a whole.

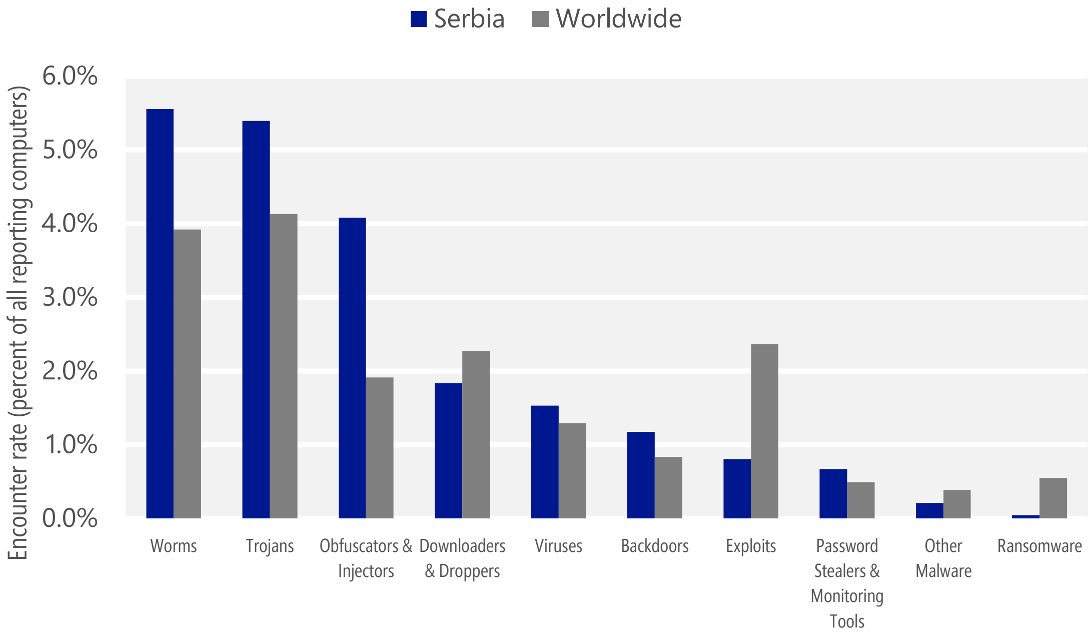
Malware encounter and infection rate trends in Serbia and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

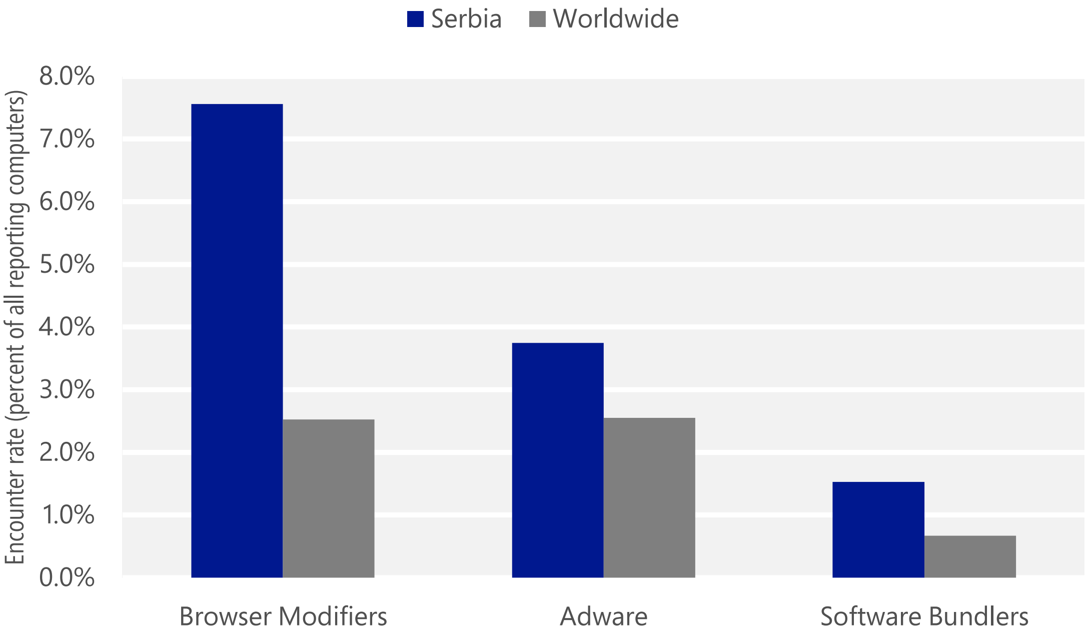
Malware encountered in Serbia in 4Q14, by category



- The most common malware category in Serbia in 4Q14 was Worms. It was encountered by 5.6 percent of all computers there, down from 10.4 percent in 3Q14.
- The second most common malware category in Serbia in 4Q14 was Trojans. It was encountered by 5.4 percent of all computers there, down from 5.5 percent in 3Q14.
- The third most common malware category in Serbia in 4Q14 was Obfuscators & Injectors, which was encountered by 4.1 percent of all computers there, down from 4.2 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Serbia in 4Q14, by category



- The most common unwanted software category in Serbia in 4Q14 was Browser Modifiers. It was encountered by 7.6 percent of all computers there, down from 8.1 percent in 3Q14.
- The second most common unwanted software category in Serbia in 4Q14 was Adware. It was encountered by 3.7 percent of all computers there, up from 0.7 percent in 3Q14.
- The third most common unwanted software category in Serbia in 4Q14 was Software Bundlers, which was encountered by 1.5 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Serbia in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Obfuscator	Obfuscators & Injectors	2.2%
2	INF/Autorun	Obfuscators & Injectors	1.9%
3	VBS/Jenxcus	Worms	1.6%
4	Win32/Gamarue	Worms	1.1%
5	Win32/Sality	Viruses	1.0%
6	Win32/Helompy	Worms	0.9%
7	Win32/Conficker	Worms	0.8%
8	Win32/Dynamer	Trojans	0.5%
9	Win32/Rimecud	Worms	0.4%
10	Win32/VB	Worms	0.4%

- The most common malware family encountered in Serbia in 4Q14 was Win32/Obfuscator, which was encountered by 2.2 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 second most common malware family encountered in Serbia in 4Q14 was INF/Autorun, which was encountered by 1.9 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 Serbia in 4Q14 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 fourth most common malware family encountered in Serbia in 4Q14 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 Serbia in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	5.3%
2	Win32/Defaulttab	Browser Modifiers	2.7%
3	Win32/Costmin	Adware	1.8%
4	Win32/BetterSurf	Adware	1.7%
5	Win32/Gofileexpress	Software Bundlers	1.2%

- The most common unwanted software family encountered in Serbia in 4Q14 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 Serbia in 4Q14 was Win32/Defaulttab, which was encountered by 2.7 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.
- The third most common unwanted software family encountered in Serbia in 4Q14 was Win32/Costmin, which was encountered by 1.8 percent of reporting computers there. Win32/Costmin is an adware family that installs itself as a browser extension for Internet Explorer, Mozilla Firefox, and Google Chrome, and displays advertisements as the user browses the Internet.

Top threat families by infection rate

The most common malware families by infection rate in Serbia in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Sality	Viruses	4.3
2	JS/Kilim	Trojans	3.6
3	VBS/Jenxcus	Worms	1.8
4	Win32/Helompy	Worms	1.6
5	Win32/Gamarue	Worms	0.8
6	Win32/Pramro	Trojans	0.7
7	MSIL/Bladabindi	Backdoors	0.4
8	Win32/Brontok	Worms	0.4
9	Win32/Sefnit	Trojans	0.3
10	Win32/Jeefo	Viruses	0.3

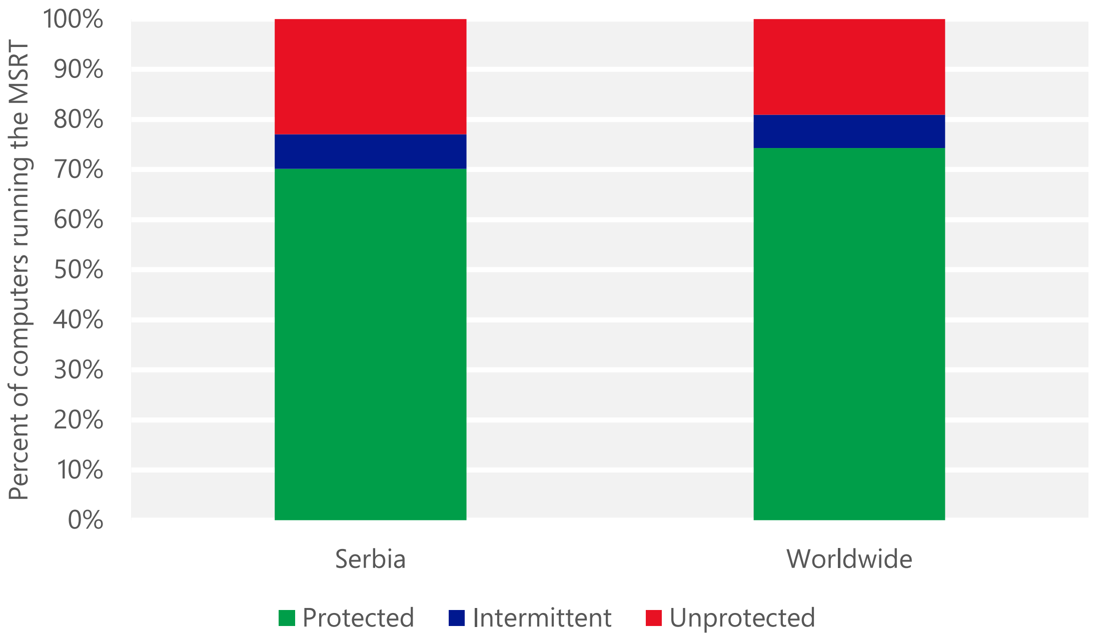
- The most common threat family infecting computers in Serbia in 4Q14 was Win32/Sality, which was detected and removed from 4.3 of every 1,000 unique computers scanned by the MSRT. Win32/Sality is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The second most common threat family infecting computers in Serbia in 4Q14 was JS/Kilim, which was detected and removed from 3.6 of every 1,000 unique computers scanned by the MSRT. JS/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 Serbia in 4Q14 was VBS/Jenxcus, which was detected and removed from 1.8 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 Serbia in 4Q14 was Win32/Helompy, which was detected and removed from 1.6 of every 1,000 unique computers scanned by the MSRT. Win32/Helompy is a worm that spreads via removable drives and attempts to capture and steal authentication details for a number of different websites or online 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 Serbia and worldwide protected by real-time security software in 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.04 drive-by download URLs for every 1,000 URLs hosted in Serbia, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.04 drive-by download URLs for every 1,000 URLs hosted in Serbia, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Serbia and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Serbia	0.04	0.04
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Singapore

The statistics presented here are generated by Microsoft security programs and services running on computers in Singapore in 4Q14 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 succeds 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

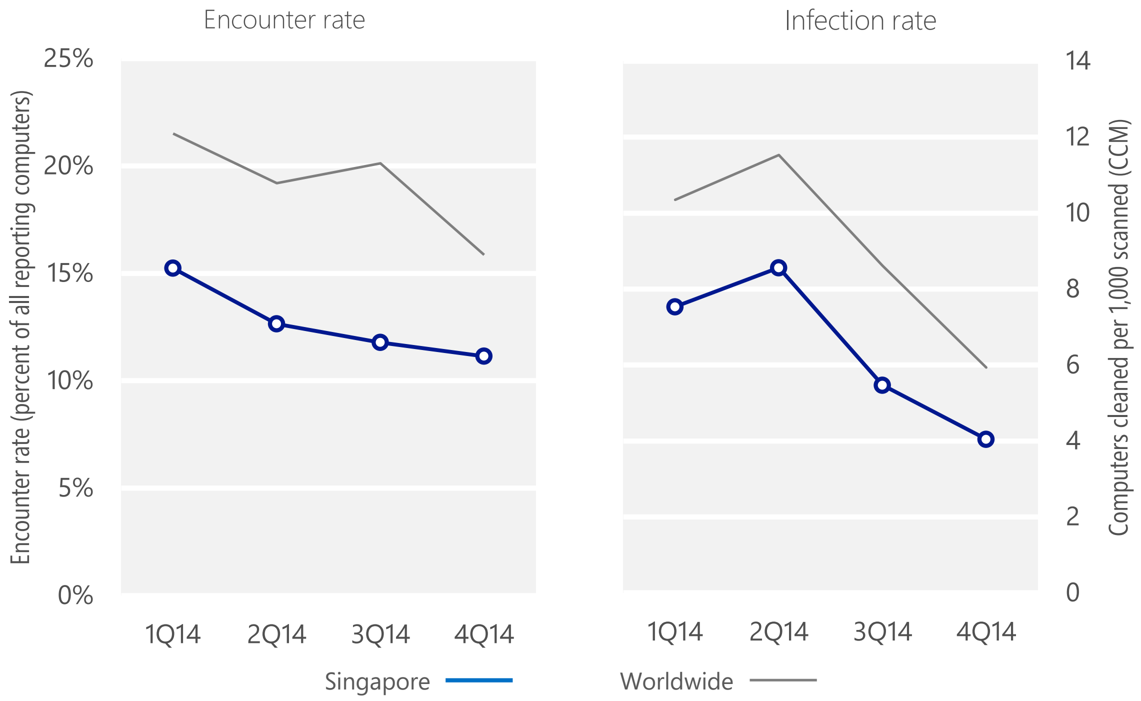
Metric	**1Q14**	**2Q14**	**3Q14**	**4Q14**
Encounter rate, Singapore	15.2%	12.6%	11.8%	11.1%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Singapore	7.5	8.6	5.5	4.0
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 11.1% percent of computers in Singapore encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 4.0 of every 1,000 unique computers scanned in Singapore in 4Q14 (a CCM score of 4.0, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Singapore over the last four quarters, compared to the world as a whole.

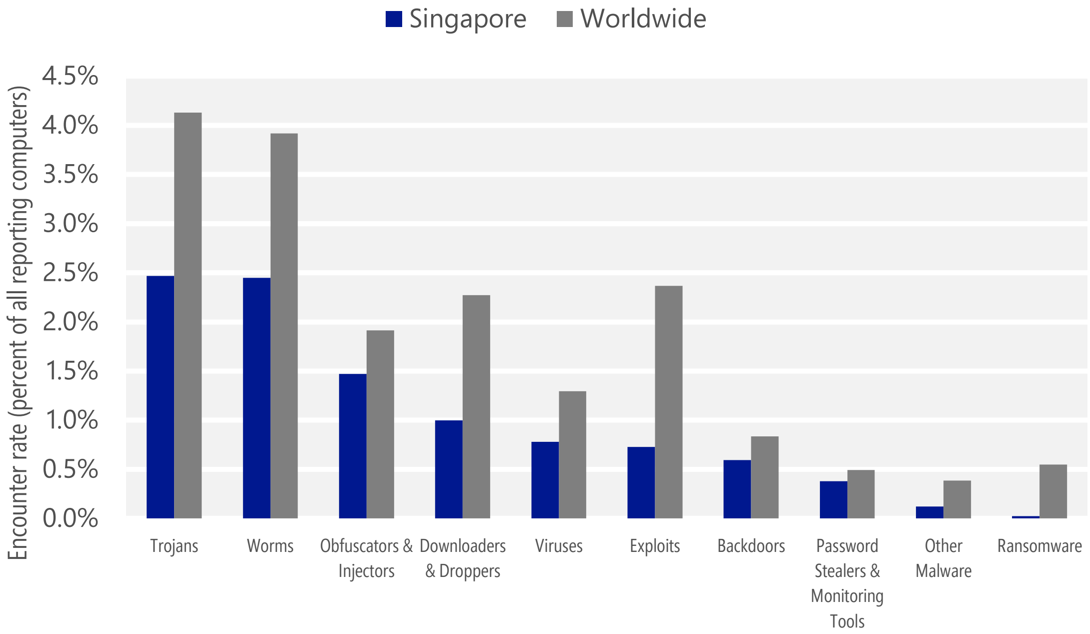
Malware encounter and infection rate trends in Singapore and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

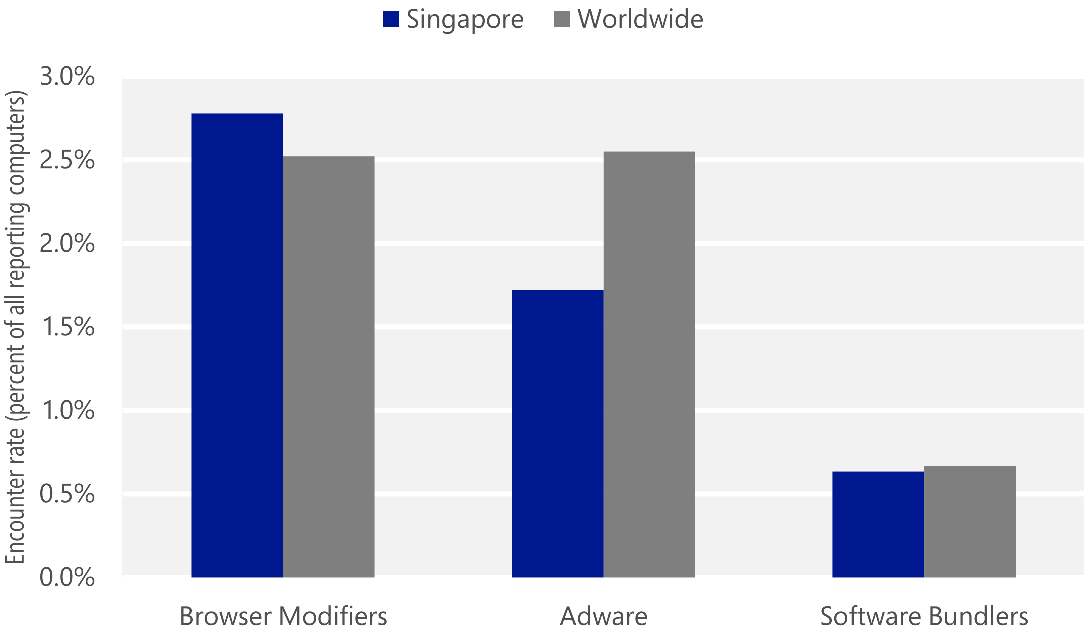
Malware encountered in Singapore in 4Q14, by category



- The most common malware category in Singapore in 4Q14 was Trojans. It was encountered by 2.5 percent of all computers there, down from 3.5 percent in 3Q14.
- The second most common malware category in Singapore in 4Q14 was Worms. It was encountered by 2.4 percent of all computers there, down from 2.8 percent in 3Q14.
- The third most common malware category in Singapore in 4Q14 was Obfuscators & Injectors, which was encountered by 1.5 percent of all computers there, down from 1.6 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Singapore in 4Q14, by category



- The most common unwanted software category in Singapore in 4Q14 was Browser Modifiers. It was encountered by 2.8 percent of all computers there, down from 3.4 percent in 3Q14.
- The second most common unwanted software category in Singapore in 4Q14 was Adware. It was encountered by 1.7 percent of all computers there, up from 0.5 percent in 3Q14.
- The third most common unwanted software category in Singapore in 4Q14 was Software Bundlers, which was encountered by 0.6 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Singapore in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Obfuscator	Obfuscators & Injectors	0.9%
2	INF/Autorun	Obfuscators & Injectors	0.7%
3	Win32/Gamarue	Worms	0.4%
4	VBS/Jenxcus	Worms	0.3%
5	Win32/Dynamer	Trojans	0.3%
6	JS/Faceliker	Trojans	0.3%
7	Win32/Ramnit	Trojans	0.2%
8	Win32/Conficker	Worms	0.2%
9	BAT/Micuda	Trojans	0.2%
10	Win32/Hilgild	Worms	0.2%

- The most common malware family encountered in Singapore in 4Q14 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 Singapore in 4Q14 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 Singapore in 4Q14 was Win32/Gamarue, which was encountered by 0.4 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 fourth most common malware family encountered in Singapore in 4Q14 was VBS/Jenxcus, which was encountered by 0.3 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.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Singapore in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	1.8%
2	Win32/Defaulttab	Browser Modifiers	1.1%
3	Win32/Costmin	Adware	0.7%
4	Win32/BetterSurf	Adware	0.7%
5	Win32/Gofileexpress	Software Bundlers	0.4%

- The most common unwanted software family encountered in Singapore in 4Q14 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 Singapore in 4Q14 was Win32/Defaulttab, which was encountered by 1.1 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.
- The third most common unwanted software family encountered in Singapore in 4Q14 was Win32/Costmin, which was encountered by 0.7 percent of reporting computers there. Win32/Costmin is an adware family that installs itself as a browser extension for Internet Explorer, Mozilla Firefox, and Google Chrome, and displays advertisements as the user browses the Internet.

Top threat families by infection rate

The most common malware families by infection rate in Singapore in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	0.6
2	Win32/Gamarue	Worms	0.5
3	Win32/Sality	Viruses	0.3
4	Win32/Zbot	Password Stealers & Monitoring Tools	0.3
5	Win32/Ramnit	Trojans	0.2
6	Win32/Brontok	Worms	0.2
7	JS/Miuref	Trojans	0.2
8	Win32/Wysotot	Trojans	0.2
9	Win32/Sefnit	Trojans	0.2
10	MSIL/Bladabindi	Backdoors	0.1

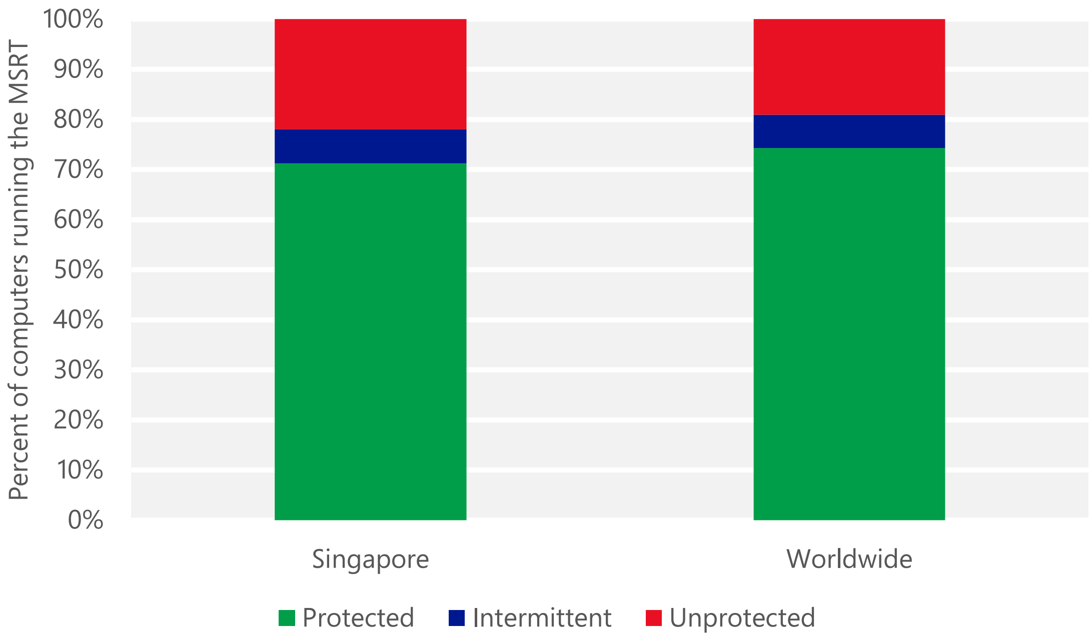
- The most common threat family infecting computers in Singapore in 4Q14 was VBS/Jenxcus, which was detected and removed from 0.6 of every 1,000 unique computers scanned by the MSRT. VBS/Jenxcus is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Singapore in 4Q14 was Win32/Gamarue, which was detected and removed from 0.5 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 Singapore in 4Q14 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.
- The fourth most common threat family infecting computers in Singapore in 4Q14 was Win32/Zbot, which was detected and removed from 0.3 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.

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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 1.14 drive-by download URLs for every 1,000 URLs hosted in Singapore, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 4.22 drive-by download URLs for every 1,000 URLs hosted in Singapore, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Singapore and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Singapore	1.14	4.22
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Slovakia

The statistics presented here are generated by Microsoft security programs and services running on computers in Slovakia in 4Q14 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 succeds 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

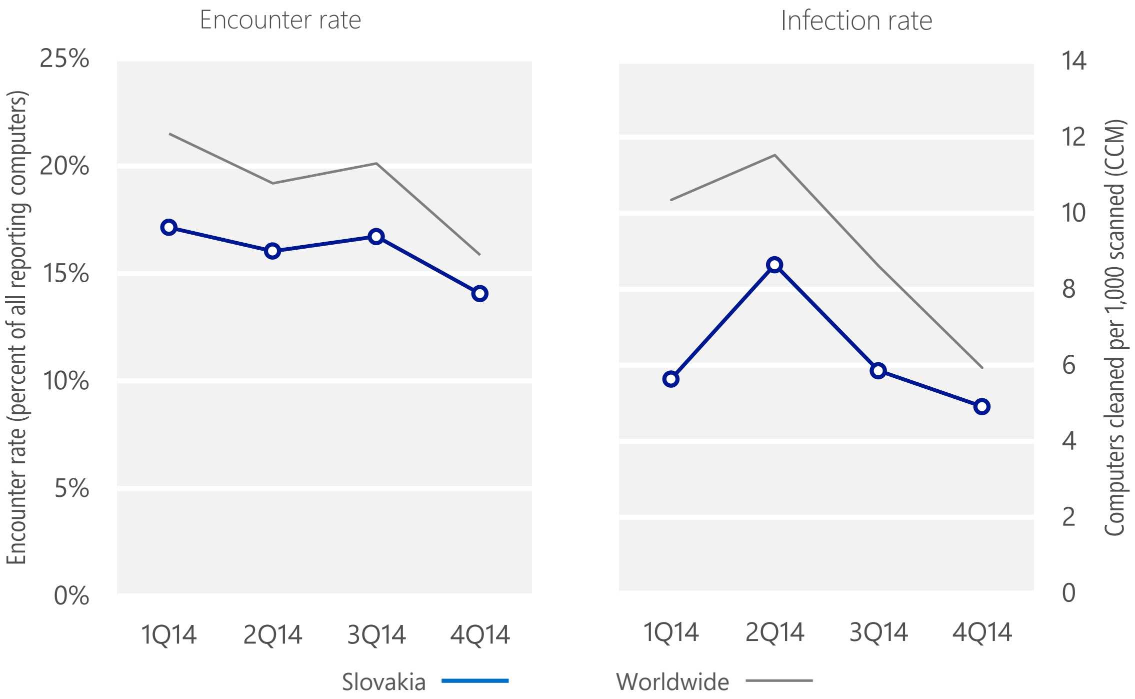
Metric	**1Q14**	**2Q14**	**3Q14**	**4Q14**
Encounter rate, Slovakia	17.1%	16.0%	16.7%	14.1%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Slovakia	5.6	8.6	5.9	4.9
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 14.1% percent of computers in Slovakia encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 4.9 of every 1,000 unique computers scanned in Slovakia in 4Q14 (a CCM score of 4.9, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Slovakia over the last four quarters, compared to the world as a whole.

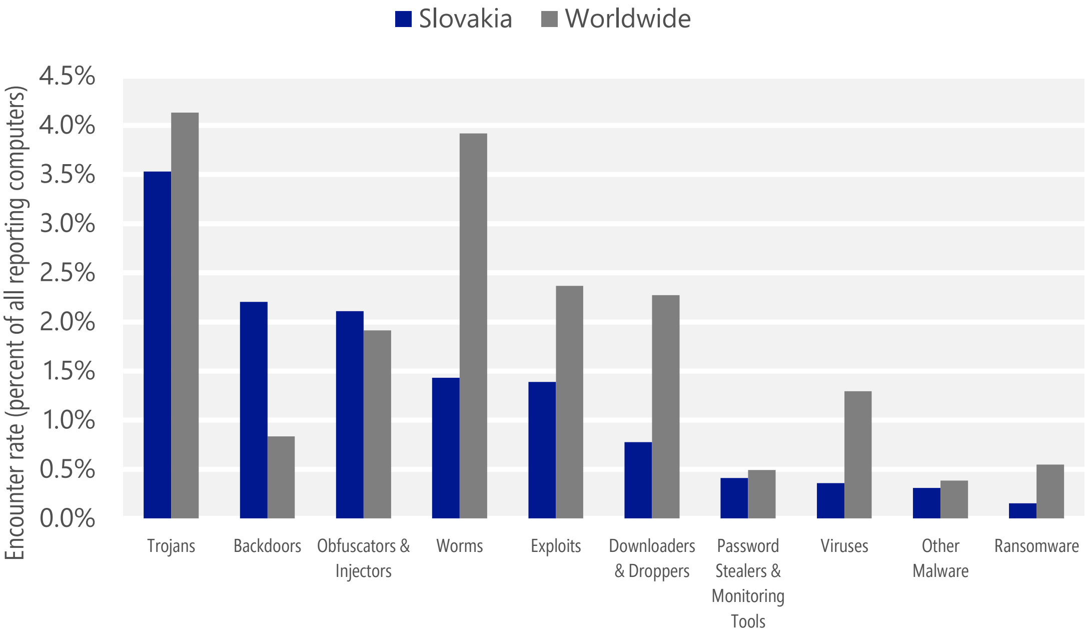
Malware encounter and infection rate trends in Slovakia and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

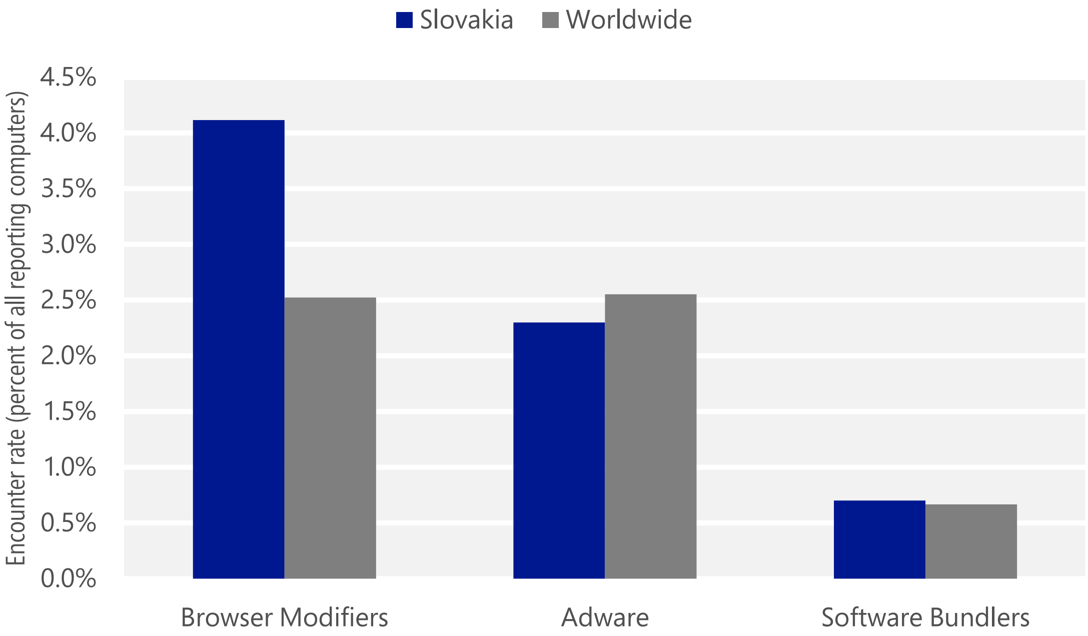
Malware encountered in Slovakia in 4Q14, by category



- The most common malware category in Slovakia in 4Q14 was Trojans. It was encountered by 3.5 percent of all computers there, down from 6.3 percent in 3Q14.
- The second most common malware category in Slovakia in 4Q14 was Backdoors. It was encountered by 2.2 percent of all computers there, up from 2.1 percent in 3Q14.
- The third most common malware category in Slovakia in 4Q14 was Obfuscators & Injectors, which was encountered by 2.1 percent of all computers there, up from 2.0 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Slovakia in 4Q14, by category



- The most common unwanted software category in Slovakia in 4Q14 was Browser Modifiers. It was encountered by 4.1 percent of all computers there, down from 5.4 percent in 3Q14.
- The second most common unwanted software category in Slovakia in 4Q14 was Adware. It was encountered by 2.3 percent of all computers there, up from 0.4 percent in 3Q14.
- The third most common unwanted software category in Slovakia in 4Q14 was Software Bundlers, which was encountered by 0.7 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Slovakia in 4Q14

	Family	Most significant category	% of reporting computers
1	MSIL/Bladabindi	Backdoors	1.6%
2	Win32/Obfuscator	Obfuscators & Injectors	1.5%
3	JS/Axpergle	Exploits	0.8%
4	INF/Autorun	Obfuscators & Injectors	0.5%
5	Win32/Dynamer	Trojans	0.5%
6	VBS/Jenxcus	Worms	0.3%
7	Win32/Anaki	Trojans	0.3%
8	Win32/Gamarue	Worms	0.3%
9	Win32/Emotet	Trojans	0.2%
10	Win32/Anogre	Exploits	0.2%

- The most common malware family encountered in Slovakia in 4Q14 was MSIL/Bladabindi, which was encountered by 1.6 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 second most common malware family encountered in Slovakia in 4Q14 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 third most common malware family encountered in Slovakia in 4Q14 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 fourth most common malware family encountered in Slovakia in 4Q14 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 Slovakia in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	3.1%
2	Win32/Defaulttab	Browser Modifiers	1.1%
3	Win32/BetterSurf	Adware	1.1%
4	Win32/Costmin	Adware	1.1%
5	Win32/Gofileexpress	Software Bundlers	0.6%

- The most common unwanted software family encountered in Slovakia in 4Q14 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 Slovakia in 4Q14 was Win32/Defaulttab, which was encountered by 1.1 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.

- The third most common unwanted software family encountered in Slovakia in 4Q14 was Win32/BetterSurf, which was encountered by 1.1 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.

Top threat families by infection rate

The most common malware families by infection rate in Slovakia in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	MSIL/Bladabindi	Backdoors	1.4
2	JS/Kilim	Trojans	1.2
3	VBS/Jenxcus	Worms	0.5
4	Win32/Brontok	Worms	0.4
5	Win32/Sality	Viruses	0.3
6	Win32/Sefnit	Trojans	0.2
7	Win32/Gamarue	Worms	0.1
8	Win32/Zbot	Password Stealers & Monitoring Tools	0.1
9	Win32/Alureon	Trojans	0.1
10	Win32/Wysotot	Trojans	0.1

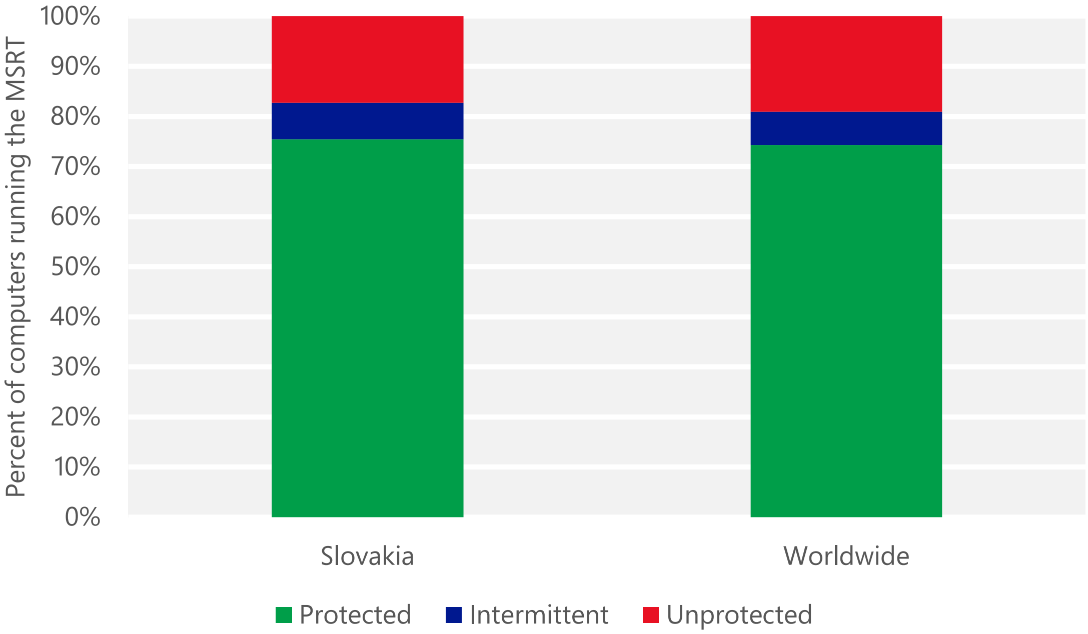
- The most common threat family infecting computers in Slovakia in 4Q14 was MSIL/Bladabindi, which was detected and removed from 1.4 of every 1,000 unique computers scanned by the MSRT. MSIL/Bladabindi is a family of backdoors created by a malicious hacker tool called NJ Rat. The can steal sensitive information, download other malware, and allow backdoor access to an infected computer.
- The second most common threat family infecting computers in Slovakia in 4Q14 was JS/Kilim, which was detected and removed from 1.2 of every 1,000 unique computers scanned by the MSRT. JS/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 Slovakia in 4Q14 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.
- The fourth most common threat family infecting computers in Slovakia in 4Q14 was Win32/Brontok, which was detected and removed from 0.4 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 Slovakia and worldwide protected by real-time security software in 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.22 drive-by download URLs for every 1,000 URLs hosted in Slovakia, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.23 drive-by download URLs for every 1,000 URLs hosted in Slovakia, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Slovakia and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Slovakia	0.22	0.23
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Slovenia

The statistics presented here are generated by Microsoft security programs and services running on computers in Slovenia in 4Q14 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 succeds 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

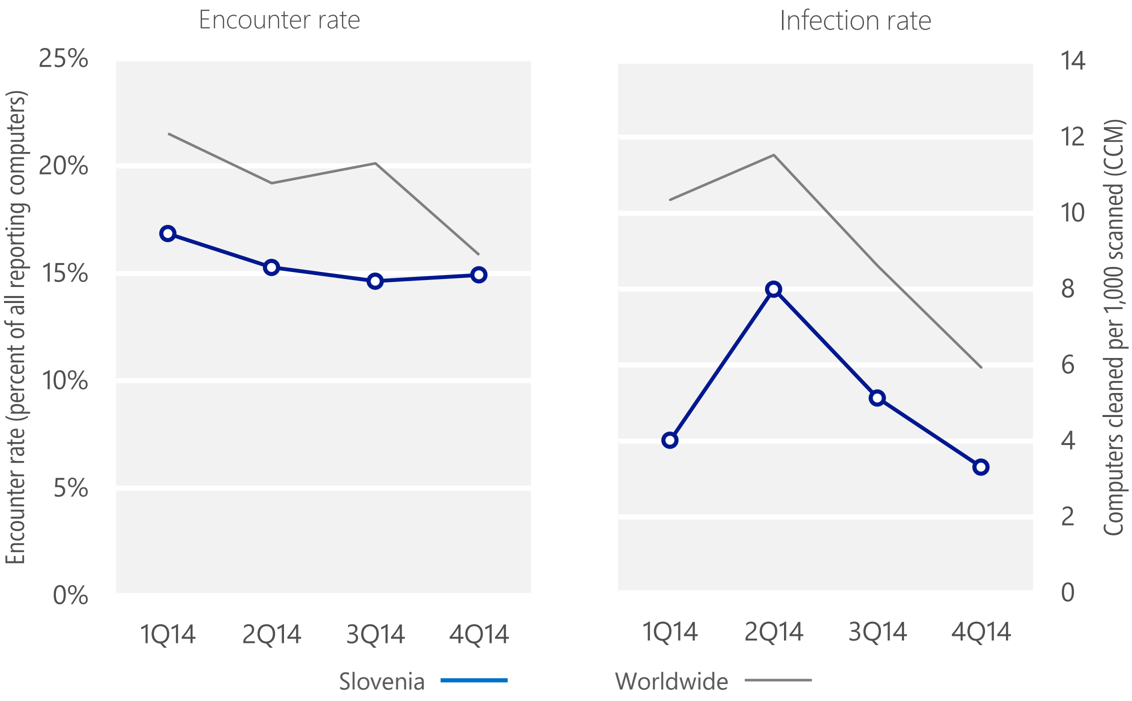
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Slovenia	16.8%	15.3%	14.6%	14.9%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Slovenia	4.0	8.0	5.1	3.3
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 14.9% percent of computers in Slovenia encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 3.3 of every 1,000 unique computers scanned in Slovenia in 4Q14 (a CCM score of 3.3, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Slovenia over the last four quarters, compared to the world as a whole.

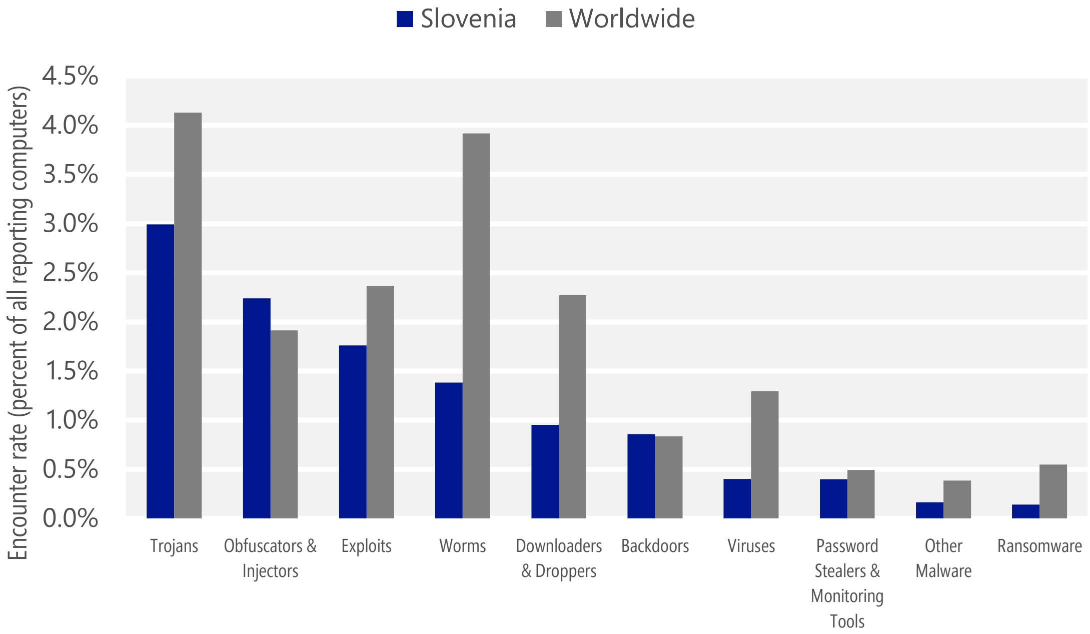
Malware encounter and infection rate trends in Slovenia and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

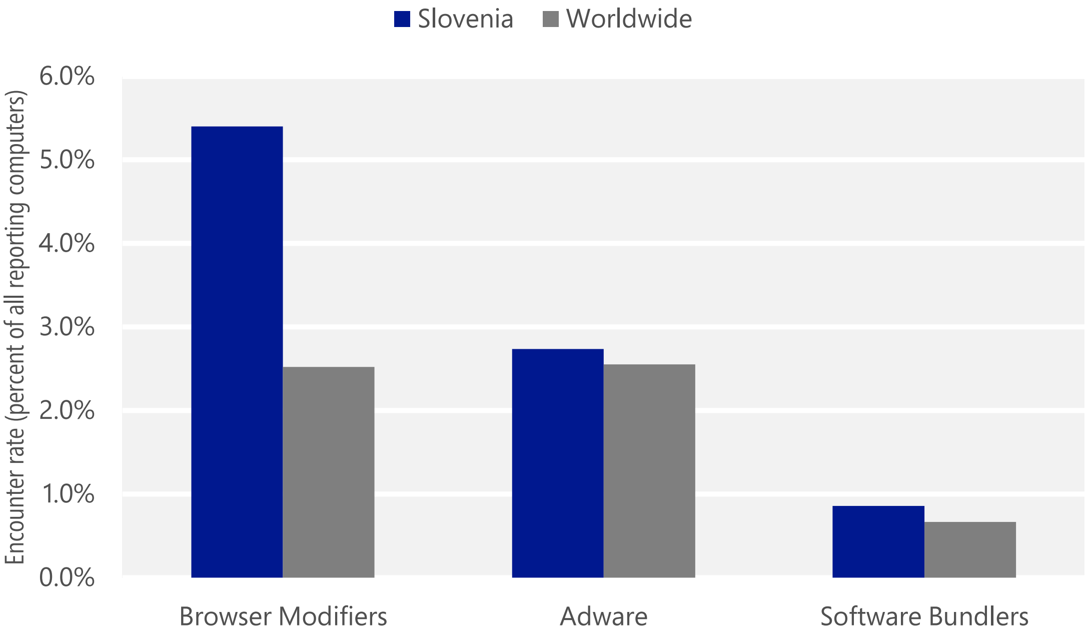
Malware encountered in Slovenia in 4Q14, by category



- The most common malware category in Slovenia in 4Q14 was Trojans. It was encountered by 3.0 percent of all computers there, down from 4.4 percent in 3Q14.
- The second most common malware category in Slovenia in 4Q14 was Obfuscators & Injectors. It was encountered by 2.2 percent of all computers there, down from 2.5 percent in 3Q14.
- The third most common malware category in Slovenia in 4Q14 was Exploits, which was encountered by 1.8 percent of all computers there, down from 2.1 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Slovenia in 4Q14, by category



- The most common unwanted software category in Slovenia in 4Q14 was Browser Modifiers. It was encountered by 5.4 percent of all computers there, down from 5.5 percent in 3Q14.
- The second most common unwanted software category in Slovenia in 4Q14 was Adware. It was encountered by 2.7 percent of all computers there, up from 0.4 percent in 3Q14.
- The third most common unwanted software category in Slovenia in 4Q14 was Software Bundlers, which was encountered by 0.9 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Slovenia in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Obfuscator	Obfuscators & Injectors	1.6%
2	JS/Axpergle	Exploits	1.1%
3	INF/Autorun	Obfuscators & Injectors	0.5%
4	Win32/Emotet	Trojans	0.3%
5	Win32/Conficker	Worms	0.3%
6	Win32/Dynamer	Trojans	0.3%

- The most common malware family encountered in Slovenia in 4Q14 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 Slovenia in 4Q14 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 third most common malware family encountered in Slovenia in 4Q14 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.
- The fourth most common malware family encountered in Slovenia in 4Q14 was Win32/Emotet, which was encountered by 0.3 percent of reporting computers there. 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.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Slovenia in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	3.7%
2	Win32/Defaulttab	Browser Modifiers	1.9%
3	Win32/BetterSurf	Adware	1.2%
4	Win32/Costmin	Adware	1.2%
5	Win32/Gofileexpress	Software Bundlers	0.7%

- The most common unwanted software family encountered in Slovenia in 4Q14 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 Slovenia in 4Q14 was Win32/Defaulttab, which was encountered by 1.9 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.
- The third most common unwanted software family encountered in Slovenia in 4Q14 was Win32/BetterSurf, which was encountered by 1.2 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.

Top threat families by infection rate

The most common malware families by infection rate in Slovenia in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	JS/Kilim	Trojans	0.7
2	Win32/Sality	Viruses	0.3
3	Win32/Sefnit	Trojans	0.2
4	Win32/Ramnit	Trojans	0.2
5	Win32/Alureon	Trojans	0.2
6	Win32/Helompy	Worms	0.1
7	MSIL/Bladabindi	Backdoors	0.1
8	Win32/Zbot	Password Stealers & Monitoring Tools	0.1
9	Win32/Brontok	Worms	0.1
10	Win32/Gamarue	Worms	0.1

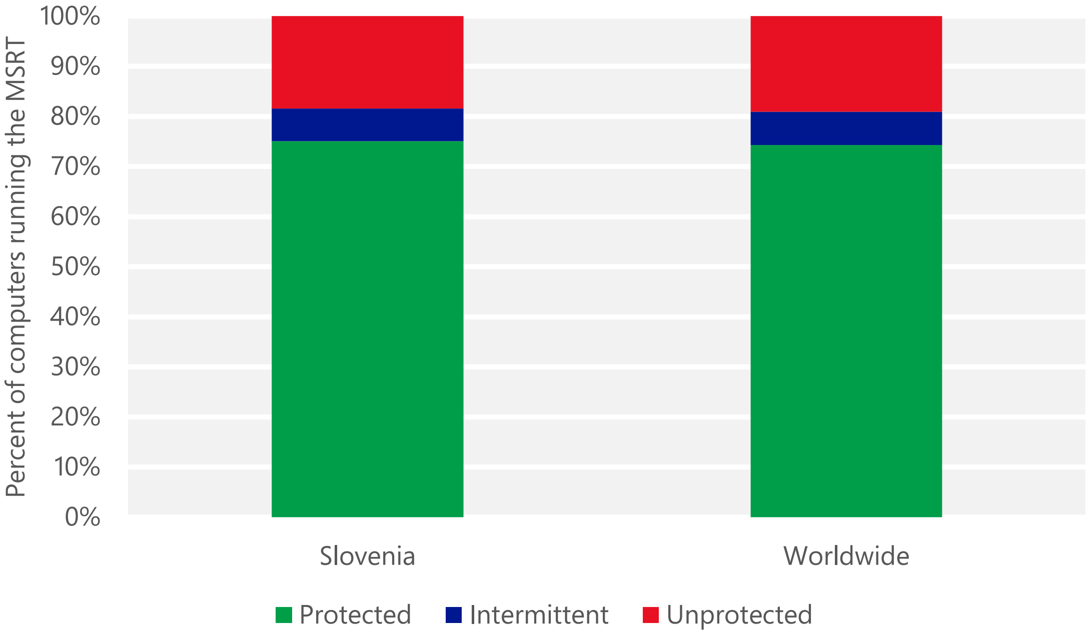
- The most common threat family infecting computers in Slovenia in 4Q14 was JS/Kilim, which was detected and removed from 0.7 of every 1,000 unique computers scanned by the MSRT. JS/Kilim is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks 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 threat family infecting computers in Slovenia in 4Q14 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.
- The third most common threat family infecting computers in Slovenia in 4Q14 was Win32/Sefnit, which was detected and removed from 0.2 of every 1,000 unique computers scanned by the MSRT. Win32/Sefnit is a family of trojans that can allow backdoor access, download files, and use the computer and Internet connection for click fraud. Some variants can monitor web browsers and hijack search results.
- The fourth most common threat family infecting computers in Slovenia in 4Q14 was Win32/Ramnit, which was detected and removed from 0.2 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 Slovenia and worldwide protected by real-time security software in 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.50 drive-by download URLs for every 1,000 URLs hosted in Slovenia, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.56 drive-by download URLs for every 1,000 URLs hosted in Slovenia, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Slovenia and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Slovenia	0.50	0.56
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

South Africa

The statistics presented here are generated by Microsoft security programs and services running on computers in South Africa in 4Q14 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 succeds 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

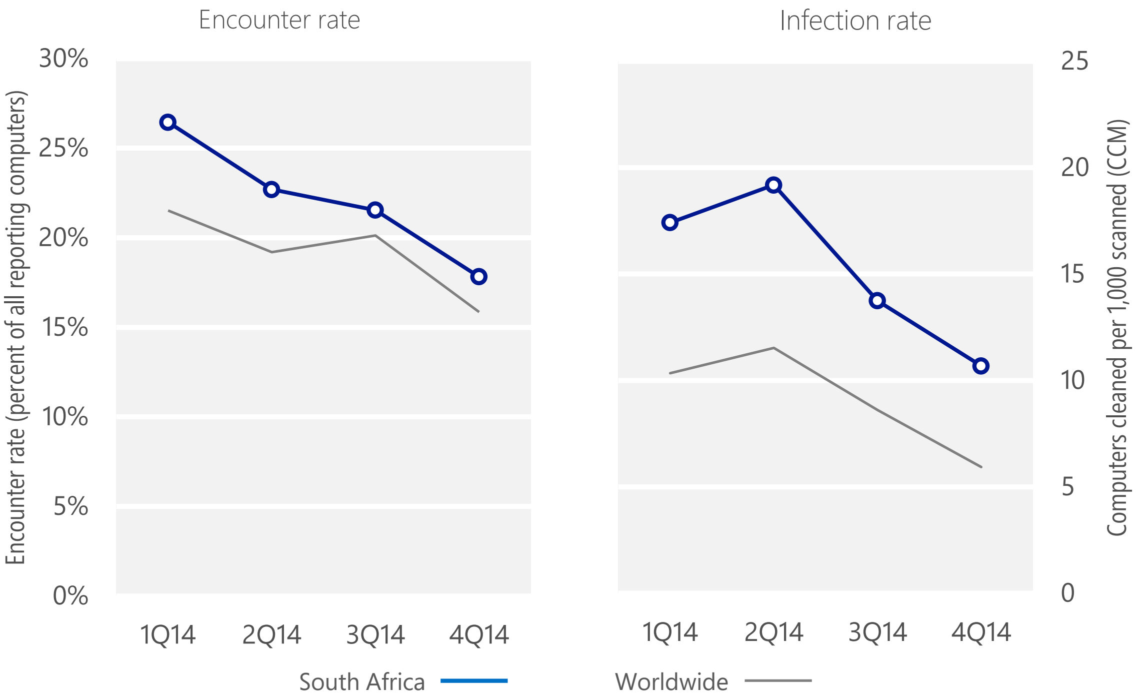
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, South Africa	26.4%	22.7%	21.5%	17.8%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, South Africa	17.4	19.2	13.7	10.7
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 17.8% percent of computers in South Africa encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 10.7 of every 1,000 unique computers scanned in South Africa in 4Q14 (a CCM score of 10.7, compared to the 4Q14 worldwide CCM of 5.9). 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.

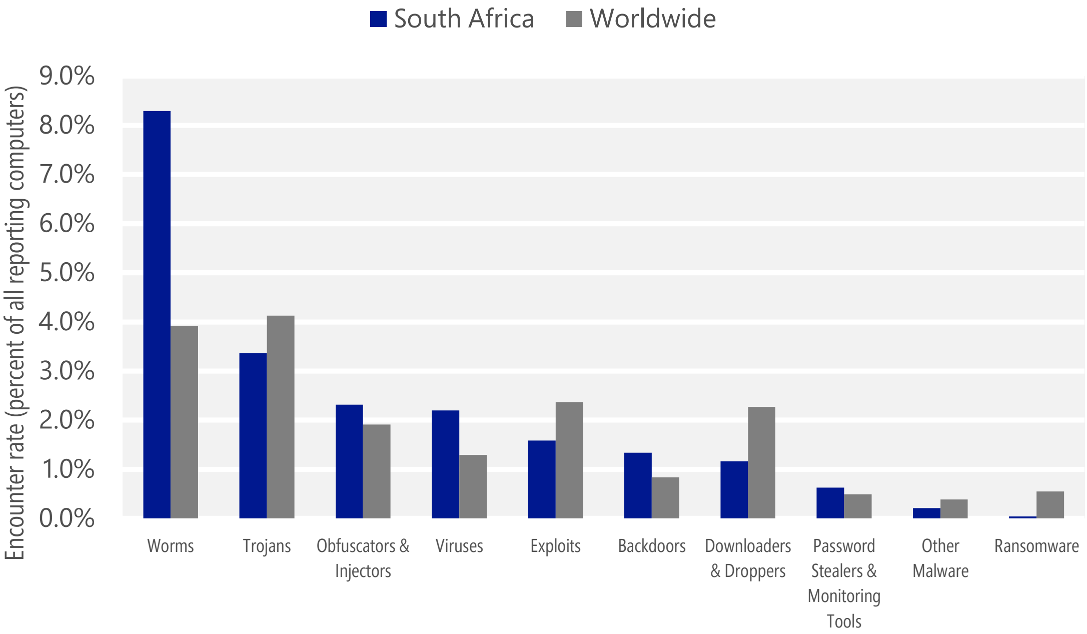
Malware encounter and infection rate trends in South Africa and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

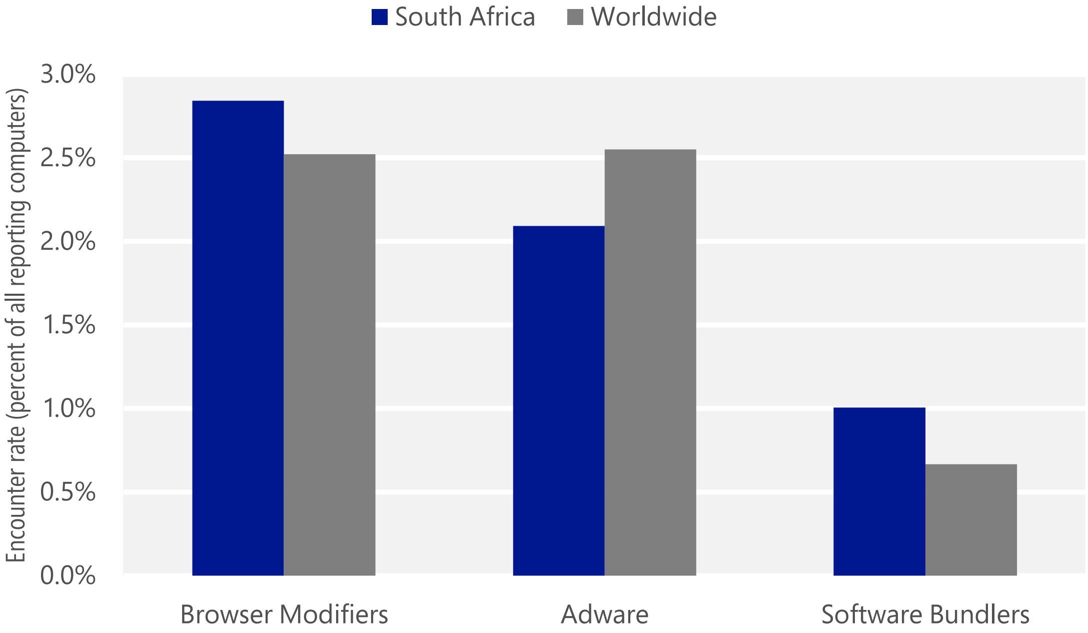
Malware encountered in South Africa in 4Q14, by category



- The most common malware category in South Africa in 4Q14 was Worms. It was encountered by 8.3 percent of all computers there, down from 10.2 percent in 3Q14.
- The second most common malware category in South Africa in 4Q14 was Trojans. It was encountered by 3.4 percent of all computers there, down from 4.9 percent in 3Q14.
- The third most common malware category in South Africa in 4Q14 was Obfuscators & Injectors, which was encountered by 2.3 percent of all computers there, down from 2.7 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in South Africa in 4Q14, by category



- The most common unwanted software category in South Africa in 4Q14 was Browser Modifiers. It was encountered by 2.8 percent of all computers there, down from 5.3 percent in 3Q14.
- The second most common unwanted software category in South Africa in 4Q14 was Adware. It was encountered by 2.1 percent of all computers there, up from 0.7 percent in 3Q14.
- The third most common unwanted software category in South Africa in 4Q14 was Software Bundlers, which was encountered by 1.0 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in South Africa in 4Q14

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	3.6%
2	INF/Autorun	Obfuscators & Injectors	2.2%
3	Win32/Enosch	Worms	1.6%
4	Win32/Vobfus	Worms	0.9%
5	Win32/Virut	Viruses	0.9%
6	Win32/Obfuscator	Obfuscators & Injectors	0.8%
7	Win32/Copali	Worms	0.8%
8	MSIL/Bladabindi	Backdoors	0.7%
9	Win32/Sality	Viruses	0.6%
10	Win32/Ramnit	Trojans	0.6%

- The most common malware family encountered in South Africa in 4Q14 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 South Africa in 4Q14 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.
- The third most common malware family encountered in South Africa in 4Q14 was Win32/Enosch, which was encountered by 1.6 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 4Q14 was Win32/Vobfus, which was encountered by 0.9 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 South Africa in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	2.3%
2	Win32/Costmin	Adware	0.9%
3	Win32/Gofileexpress	Software Bundlers	0.8%
4	Win32/BetterSurf	Adware	0.8%
5	Win32/Defaulttab	Browser Modifiers	0.6%

- The most common unwanted software family encountered in South Africa in 4Q14 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 South Africa in 4Q14 was Win32/Costmin, which was encountered by 0.9 percent of reporting computers there. Win32/Costmin is an adware family that installs itself as a browser extension for Internet Explorer, Mozilla Firefox, and Google Chrome, and displays advertisements as the user browses the Internet.

- The third most common unwanted software family encountered in South Africa in 4Q14 was Win32/Gofileexpress, which was encountered by 0.8 percent of reporting computers there. Win32/Gofileexpress is a software bundler that installs other unwanted software, including Adware:Win32/Lollipop and Adware:Win32/CostMin.

Top threat families by infection rate

The most common malware families by infection rate in South Africa in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	4.4
2	Win32/Sality	Viruses	1.0
3	Win32/Vobfus	Worms	0.9
4	MSIL/Bladabindi	Backdoors	0.6
5	Win32/Chir	Viruses	0.5
6	Win32/Folstart	Worms	0.5
7	Win32/Nuqel	Worms	0.5
8	Win32/Ramnit	Trojans	0.5
9	Win32/Zbot	Password Stealers & Monitoring Tools	0.4
10	Win32/Virut	Viruses	0.3

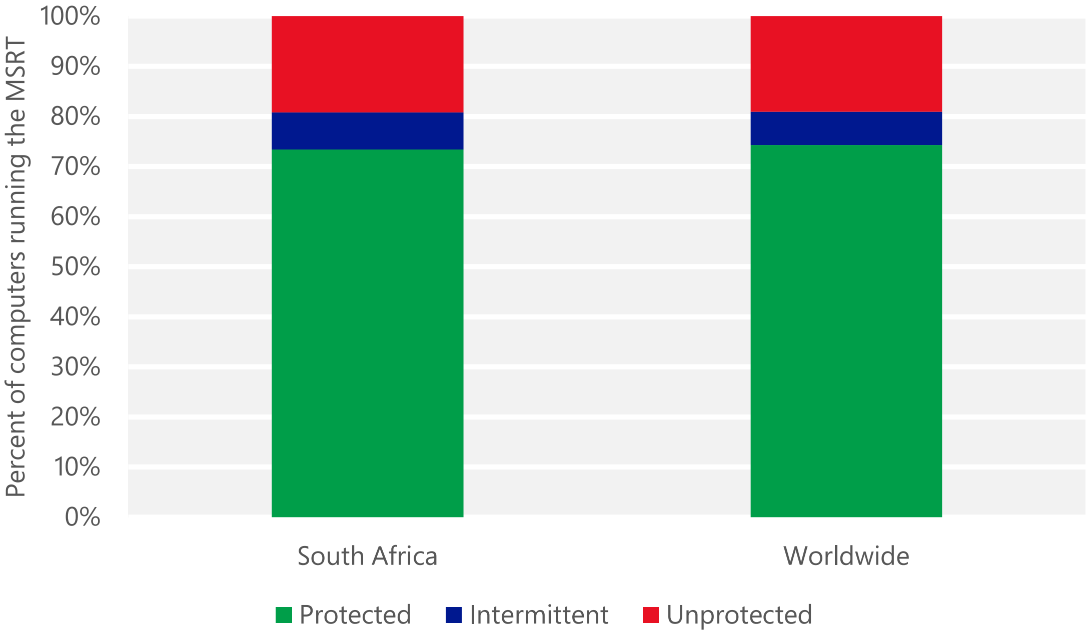
- The most common threat family infecting computers in South Africa in 4Q14 was VBS/Jenxcus, which was detected and removed from 4.4 of every 1,000 unique computers scanned by the MSRT. VBS/Jenxcus is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in South Africa in 4Q14 was Win32/Sality, which was detected and removed from 1.0 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 South Africa in 4Q14 was Win32/Vobfus, which was detected and removed from 0.9 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.
- The fourth most common threat family infecting computers in South Africa in 4Q14 was MSIL/Bladabindi, which was detected and removed from 0.6 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.

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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.12 drive-by download URLs for every 1,000 URLs hosted in South Africa, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.17 drive-by download URLs for every 1,000 URLs hosted in South Africa, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in South Africa and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, South Africa	0.12	0.17
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Spain

The statistics presented here are generated by Microsoft security programs and services running on computers in Spain in 4Q14 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 succeds 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

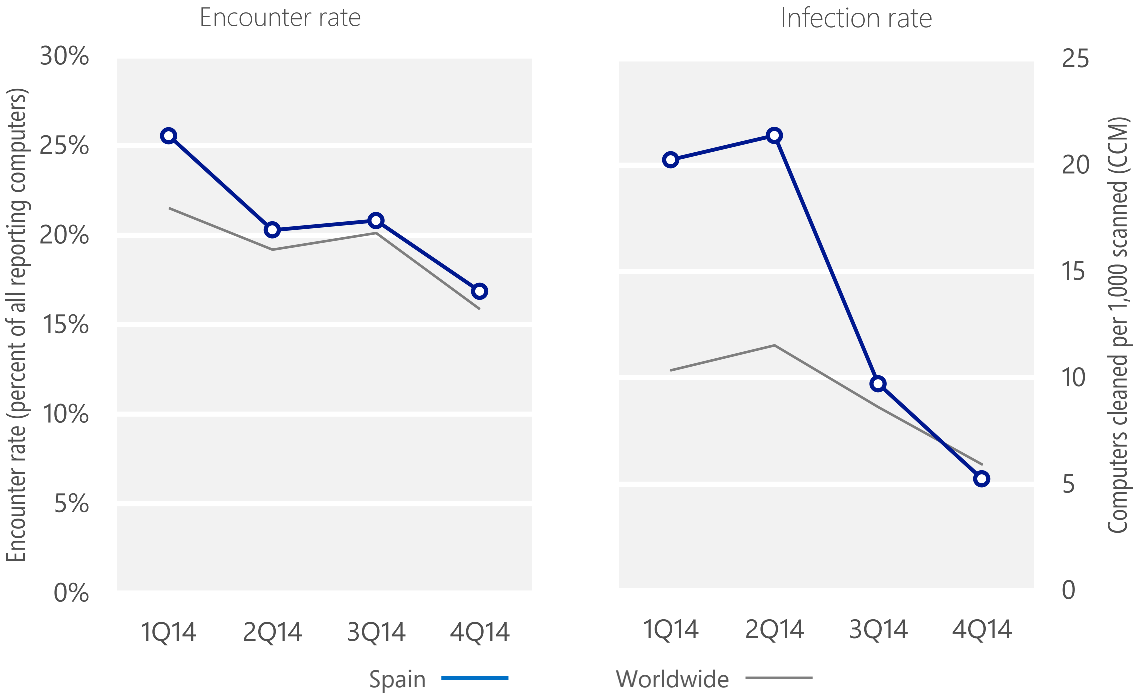
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Spain	25.6%	20.3%	20.8%	16.9%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Spain	20.3	21.4	9.7	5.3
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 16.9% percent of computers in Spain encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 5.3 of every 1,000 unique computers scanned in Spain in 4Q14 (a CCM score of 5.3, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Spain over the last four quarters, compared to the world as a whole.

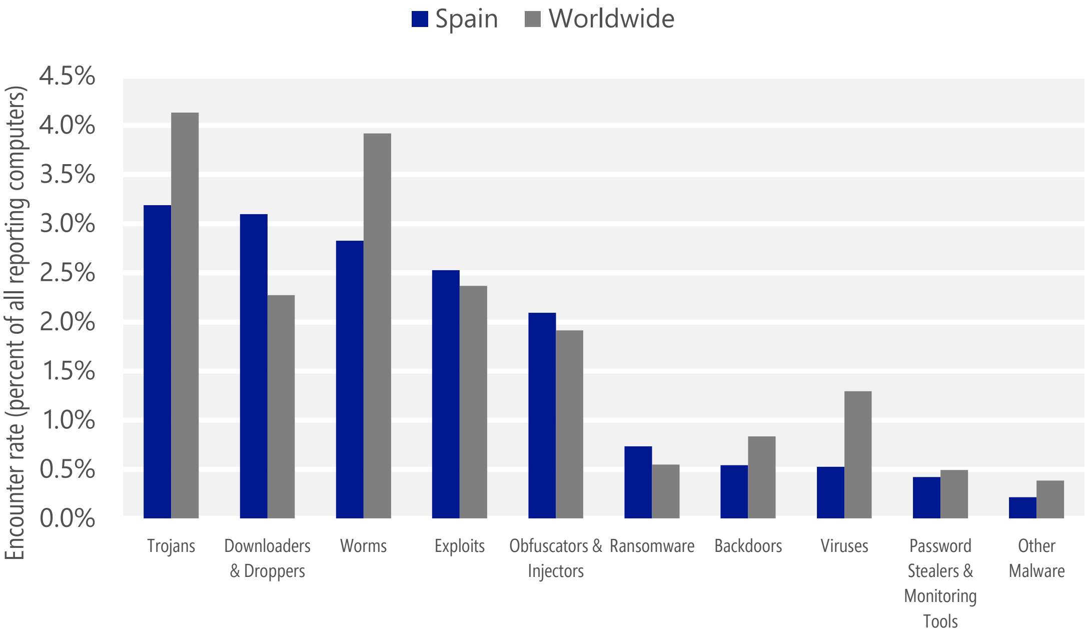
Malware encounter and infection rate trends in Spain and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

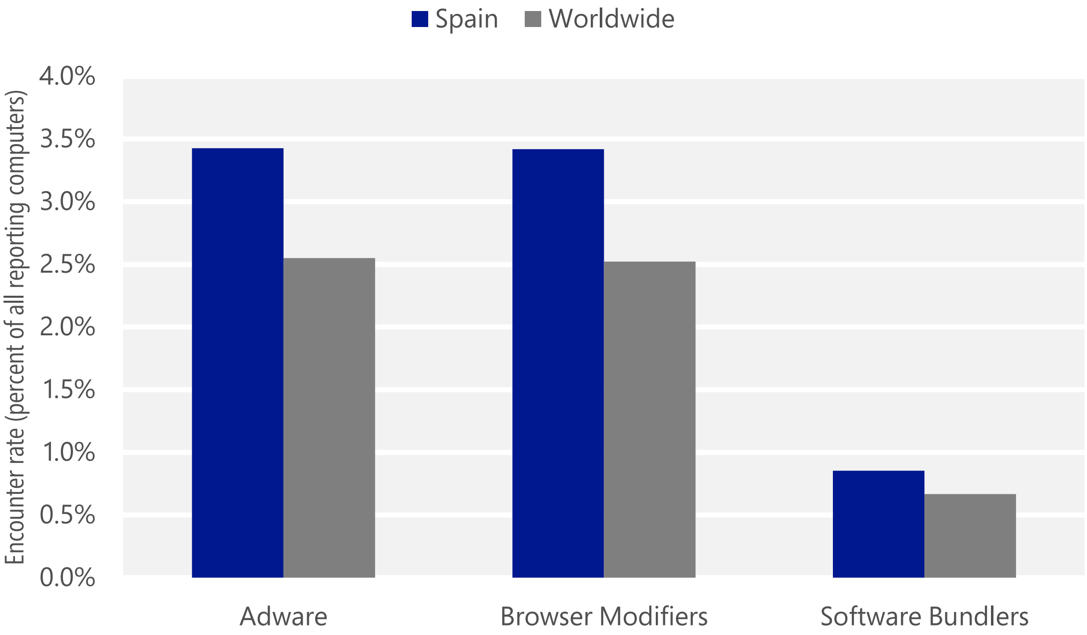
Malware encountered in Spain in 4Q14, by category



- The most common malware category in Spain in 4Q14 was Trojans. It was encountered by 3.2 percent of all computers there, down from 9.4 percent in 3Q14.
- The second most common malware category in Spain in 4Q14 was Downloaders & Droppers. It was encountered by 3.1 percent of all computers there, down from 4.4 percent in 3Q14.
- The third most common malware category in Spain in 4Q14 was Worms, which was encountered by 2.8 percent of all computers there, up from 2.3 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Spain in 4Q14, by category



- The most common unwanted software category in Spain in 4Q14 was Adware. It was encountered by 3.4 percent of all computers there, down from 6.4 percent in 3Q14.
- The second most common unwanted software category in Spain in 4Q14 was Browser Modifiers. It was encountered by 3.4 percent of all computers there, down from 3.9 percent in 3Q14.
- The third most common unwanted software category in Spain in 4Q14 was Software Bundlers, which was encountered by 0.9 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Spain in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Tugspay	Downloaders & Droppers	1.7%
2	Win32/Obfuscator	Obfuscators & Injectors	1.3%
3	JS/Axpergle	Exploits	1.1%
4	INF/Autorun	Obfuscators & Injectors	1.0%
5	Win32/Conficker	Worms	0.7%
6	Win32/Anogre	Exploits	0.6%
7	ASX/Wimad	Downloaders & Droppers	0.5%
8	JS/Krypterade	Ransomware	0.5%
9	Win32/Wysotot	Trojans	0.4%
10	VBS/Jenxcus	Worms	0.4%

- The most common malware family encountered in Spain in 4Q14 was Win32/Tugspay, which was encountered by 1.7 percent of reporting computers there. Win32/Tugspay is a downloader that spreads by posing as an installer for legitimate software, such as a Java update, or through other malware. When installed, it downloads unwanted software to the computer.
- The second most common malware family encountered in Spain in 4Q14 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 third most common malware family encountered in Spain in 4Q14 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 fourth most common malware family encountered in Spain in 4Q14 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.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Spain in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	3.2%
2	Win32/Costmin	Adware	1.4%
3	Win32/BetterSurf	Adware	0.9%
4	Win32/Pennybee	Adware	0.3%
5	Win32/Gofileexpress	Software Bundlers	0.3%

- The most common unwanted software family encountered in Spain in 4Q14 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 Spain in 4Q14 was Win32/Costmin, which was encountered by 1.4 percent of reporting computers there. Win32/Costmin is an adware family that installs itself as a browser extension for Internet Explorer, Mozilla Firefox, and Google Chrome, and displays advertisements as the user browses the Internet.
- The third most common unwanted software family encountered in Spain in 4Q14 was Win32/BetterSurf, which was encountered by 0.9 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.

Top threat families by infection rate

The most common malware families by infection rate in Spain in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Wysotot	Trojans	1.0
2	Win32/Sefnit	Trojans	0.8
3	VBS/Jenxcus	Worms	0.5
4	Win32/Brontok	Worms	0.3
5	Win32/Alureon	Trojans	0.3
6	Win32/Sality	Viruses	0.2
7	Win32/Zbot	Password Stealers & Monitoring Tools	0.2
8	Win32/Conficker	Worms	0.2
9	Win32/Sirefef	Trojans	0.2
10	Win32/Ramnit	Trojans	0.2

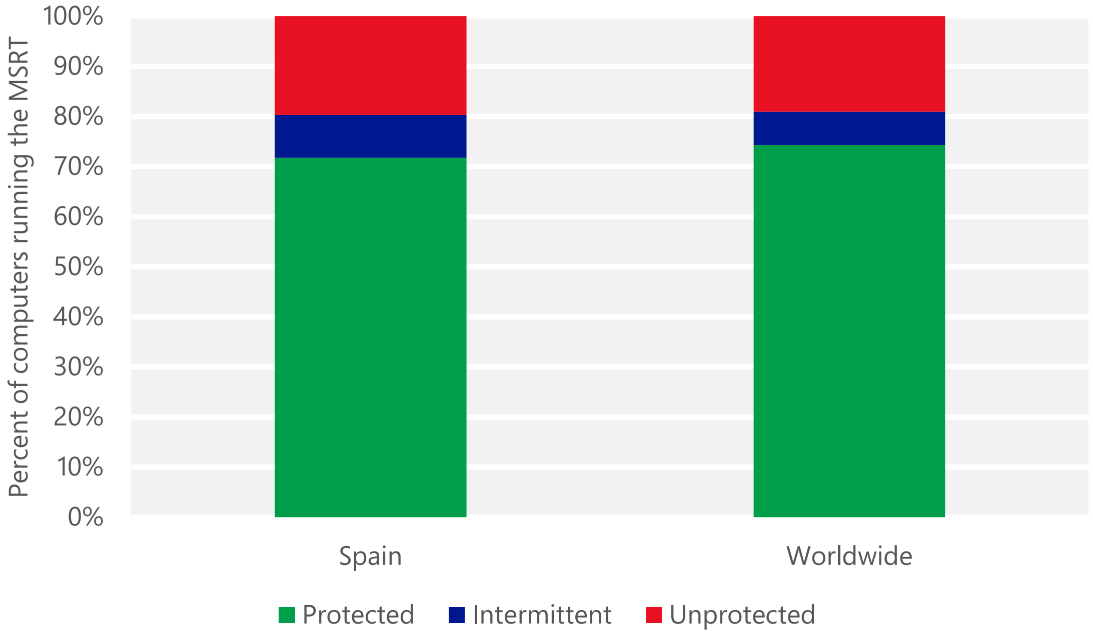
- The most common threat family infecting computers in Spain in 4Q14 was Win32/Wysotot, which was detected and removed from 1.0 of every 1,000 unique computers scanned by the MSRT. Win32/Wysotot is a threat that can change the start page of the user's web browser, and may download and install other files to the computer. It is installed by software bundlers that advertise free software or games.
- The second most common threat family infecting computers in Spain in 4Q14 was Win32/Sefnit, which was detected and removed from 0.8 of every 1,000 unique computers scanned by the MSRT. Win32/Sefnit is a family of trojans that can allow backdoor access, download files, and use the computer and Internet connection for click fraud. Some variants can monitor web browsers and hijack search results.
- The third most common threat family infecting computers in Spain in 4Q14 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.
- The fourth most common threat family infecting computers in Spain in 4Q14 was Win32/Brontok, which was detected and removed from 0.3 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 Spain and worldwide protected by real-time security software in 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.26 drive-by download URLs for every 1,000 URLs hosted in Spain, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.21 drive-by download URLs for every 1,000 URLs hosted in Spain, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Spain and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Spain	0.26	0.21
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Sri Lanka

The statistics presented here are generated by Microsoft security programs and services running on computers in Sri Lanka in 4Q14 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 succeds 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

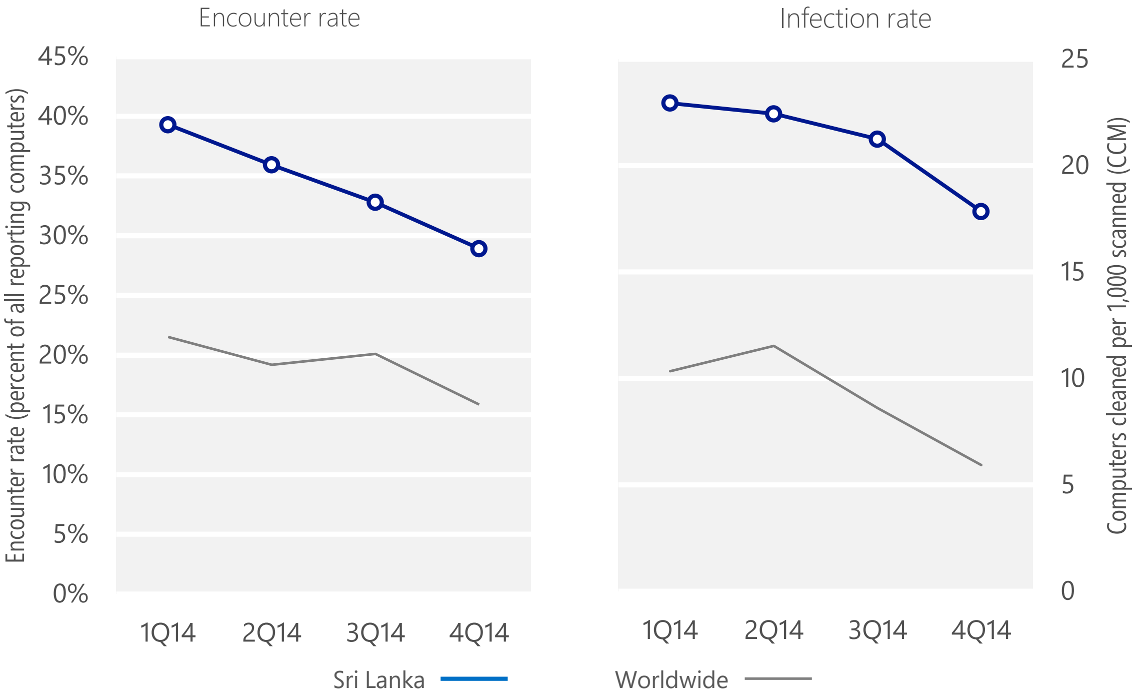
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Sri Lanka	39.3%	35.9%	32.8%	28.9%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Sri Lanka	22.9	22.4	21.2	17.8
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 28.9% percent of computers in Sri Lanka encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 17.8 of every 1,000 unique computers scanned in Sri Lanka in 4Q14 (a CCM score of 17.8, compared to the 4Q14 worldwide CCM of 5.9). 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.

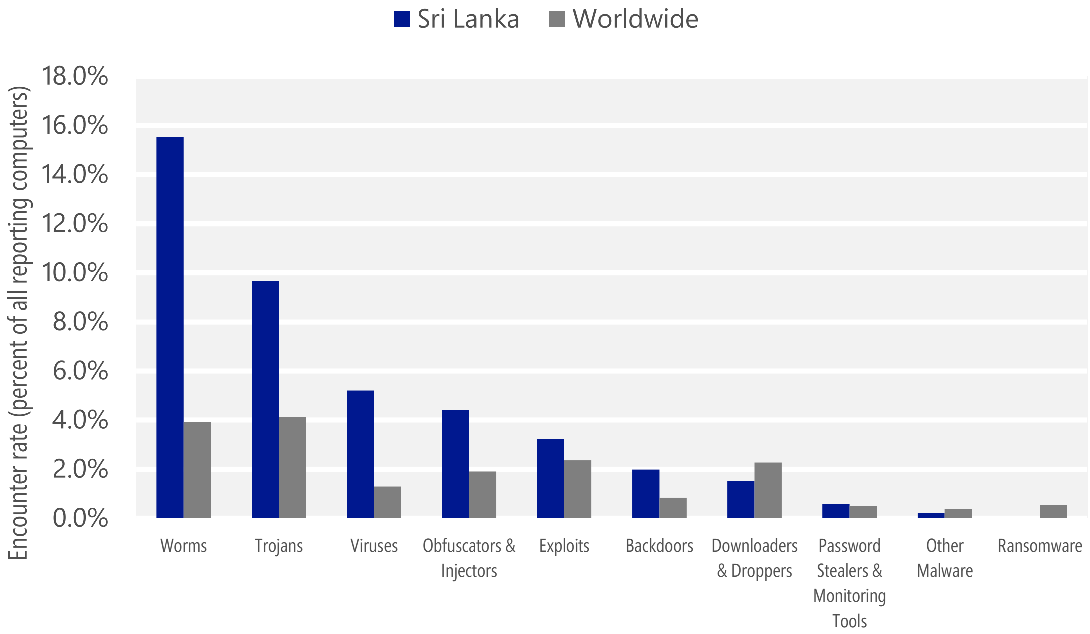
Malware encounter and infection rate trends in Sri Lanka and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

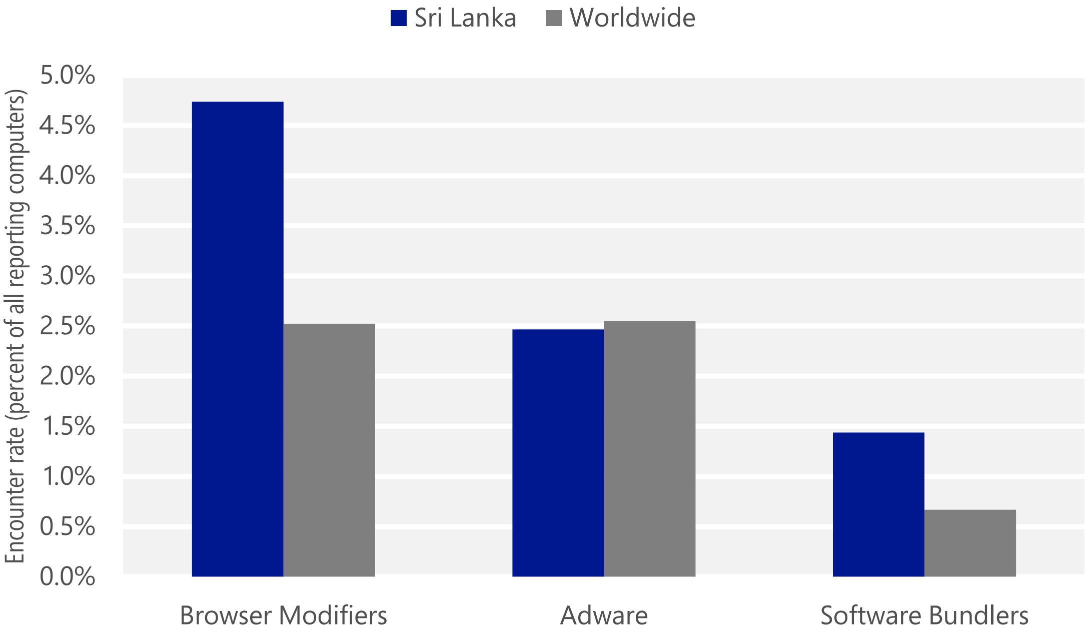
Malware encountered in Sri Lanka in 4Q14, by category



- The most common malware category in Sri Lanka in 4Q14 was Worms. It was encountered by 15.5 percent of all computers there, down from 16.7 percent in 3Q14.
- The second most common malware category in Sri Lanka in 4Q14 was Trojans. It was encountered by 9.7 percent of all computers there, down from 13.9 percent in 3Q14.
- The third most common malware category in Sri Lanka in 4Q14 was Viruses, which was encountered by 5.2 percent of all computers there, down from 6.4 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Sri Lanka in 4Q14, by category



- The most common unwanted software category in Sri Lanka in 4Q14 was Browser Modifiers. It was encountered by 4.7 percent of all computers there, down from 5.4 percent in 3Q14.
- The second most common unwanted software category in Sri Lanka in 4Q14 was Adware. It was encountered by 2.5 percent of all computers there, up from 0.8 percent in 3Q14.
- The third most common unwanted software category in Sri Lanka in 4Q14 was Software Bundlers, which was encountered by 1.4 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Sri Lanka in 4Q14

	Family	Most significant category	% of reporting computers
1	INF/Autorun	Obfuscators & Injectors	7.8%
2	VBS/Jenxcus	Worms	4.6%
3	Win32/Ippedo	Worms	4.2%
4	Win32/Sality	Viruses	3.0%
5	Win32/CplLnk	Exploits	2.7%
6	Win32/Ramnit	Trojans	2.5%
7	Win32/Arande	Trojans	2.5%
8	Win32/Nuqel	Worms	2.5%
9	Win32/Dorkbot	Worms	2.0%
10	Win32/Delicium	Viruses	1.5%

- The most common malware family encountered in Sri Lanka in 4Q14 was INF/Autorun, which was encountered by 7.8 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 second most common malware family encountered in Sri Lanka in 4Q14 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 third most common malware family encountered in Sri Lanka in 4Q14 was Win32/Ippedo, which was encountered by 4.2 percent of reporting computers there. Win32/Ippedo is a worm that can send sensitive information to a malicious hacker. It spreads through infected removable drives, such as USB flash drives.
- The fourth most common malware family encountered in Sri Lanka in 4Q14 was Win32/Sality, which was encountered by 3.0 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 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	3.0%
2	Win32/Defaulttab	Browser Modifiers	1.9%
3	Win32/BetterSurf	Adware	1.3%
4	Win32/Gofileexpress	Software Bundlers	1.1%
5	Win32/Costmin	Adware	0.9%

- The most common unwanted software family encountered in Sri Lanka in 4Q14 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 second most common unwanted software family encountered in Sri Lanka in 4Q14 was Win32/Defaulttab, which was encountered by 1.9 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.

- The third most common unwanted software family encountered in Sri Lanka in 4Q14 was Win32/BetterSurf, which was encountered by 1.3 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.

Top threat families by infection rate

The most common malware families by infection rate in Sri Lanka in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Sality	Viruses	5.2
2	VBS/Jenxcus	Worms	4.3
3	Win32/Nuqel	Worms	1.7
4	Win32/Ramnit	Trojans	1.2
5	Win32/Dorkbot	Worms	1.2
6	Win32/Chir	Viruses	0.9
7	Win32/Gamarue	Worms	0.7
8	Win32/Lethic	Trojans	0.5
9	Win32/Parite	Viruses	0.5
10	Win32/Babonock	Worms	0.5

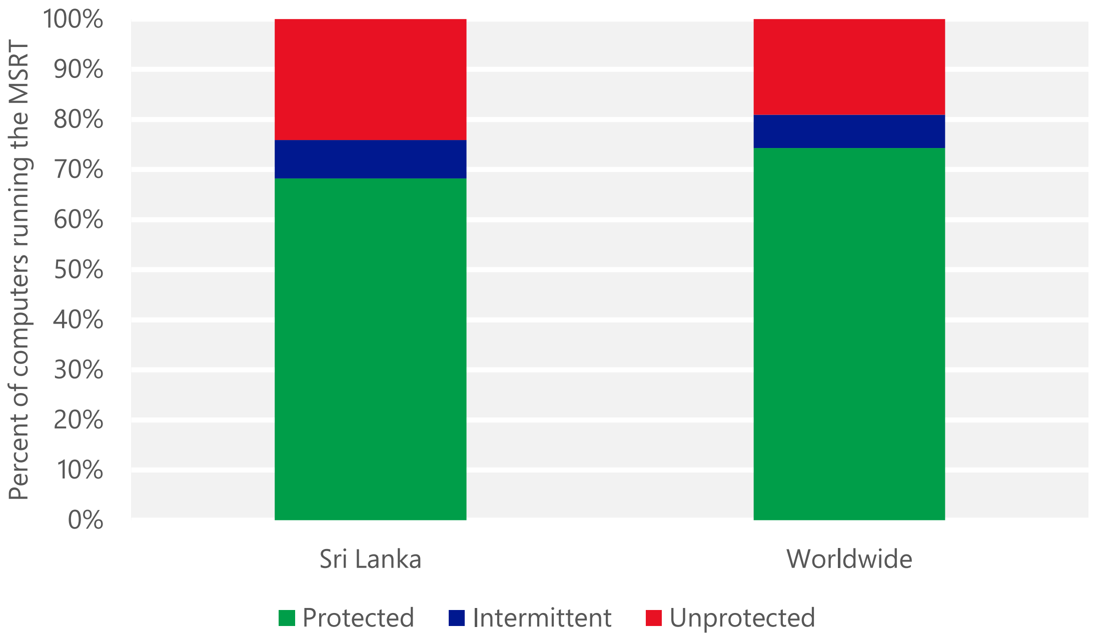
- The most common threat family infecting computers in Sri Lanka in 4Q14 was Win32/Sality, which was detected and removed from 5.2 of every 1,000 unique computers scanned by the MSRT. Win32/Sality is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The second most common threat family infecting computers in Sri Lanka in 4Q14 was VBS/Jenxcus, which was detected and removed from 4.3 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 Sri Lanka in 4Q14 was Win32/Nuqel, which was detected and removed from 1.7 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 Sri Lanka in 4Q14 was Win32/Ramnit, which was detected and removed from 1.2 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 Sri Lanka and worldwide protected by real-time security software in 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.07 drive-by download URLs for every 1,000 URLs hosted in Sri Lanka, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.41 drive-by download URLs for every 1,000 URLs hosted in Sri Lanka, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Sri Lanka and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Sri Lanka	0.07	0.41
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Sweden

The statistics presented here are generated by Microsoft security programs and services running on computers in Sweden in 4Q14 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 succeds 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

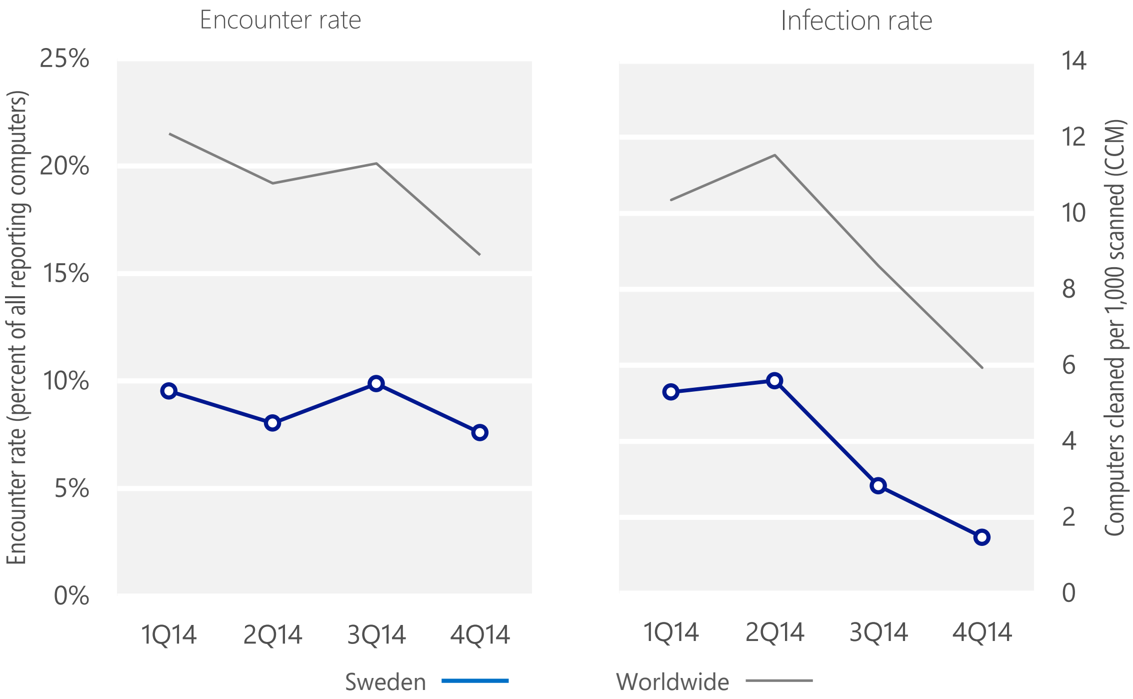
Metric	**1Q14**	**2Q14**	**3Q14**	**4Q14**
Encounter rate, Sweden	9.5%	8.0%	9.9%	7.6%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Sweden	5.3	5.6	2.8	1.5
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 7.6% percent of computers in Sweden encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 1.5 of every 1,000 unique computers scanned in Sweden in 4Q14 (a CCM score of 1.5, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Sweden over the last four quarters, compared to the world as a whole.

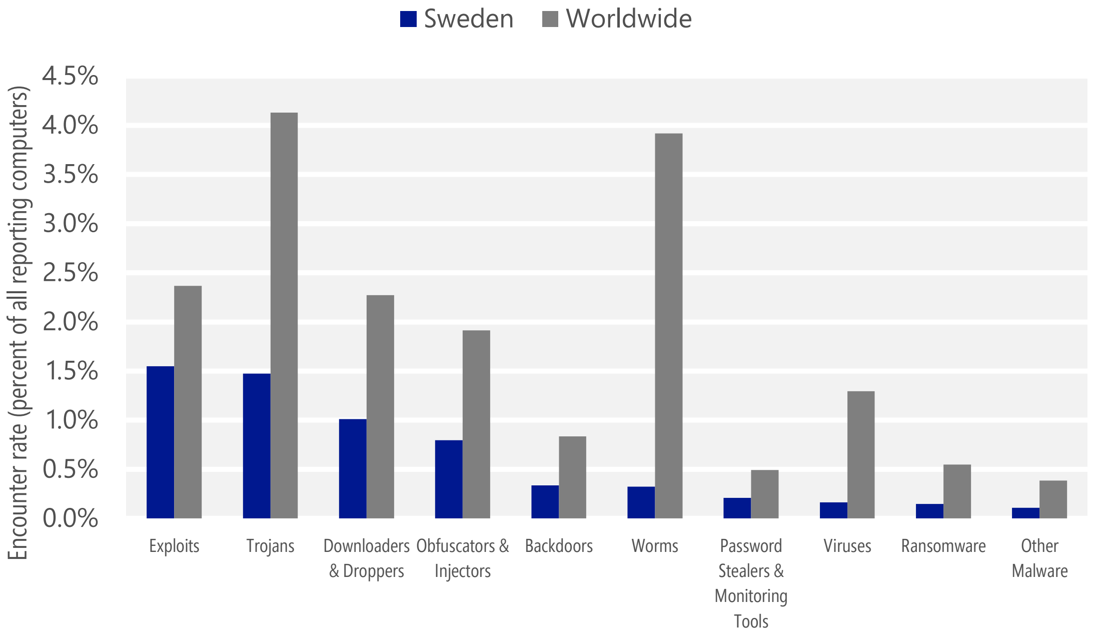
Malware encounter and infection rate trends in Sweden and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

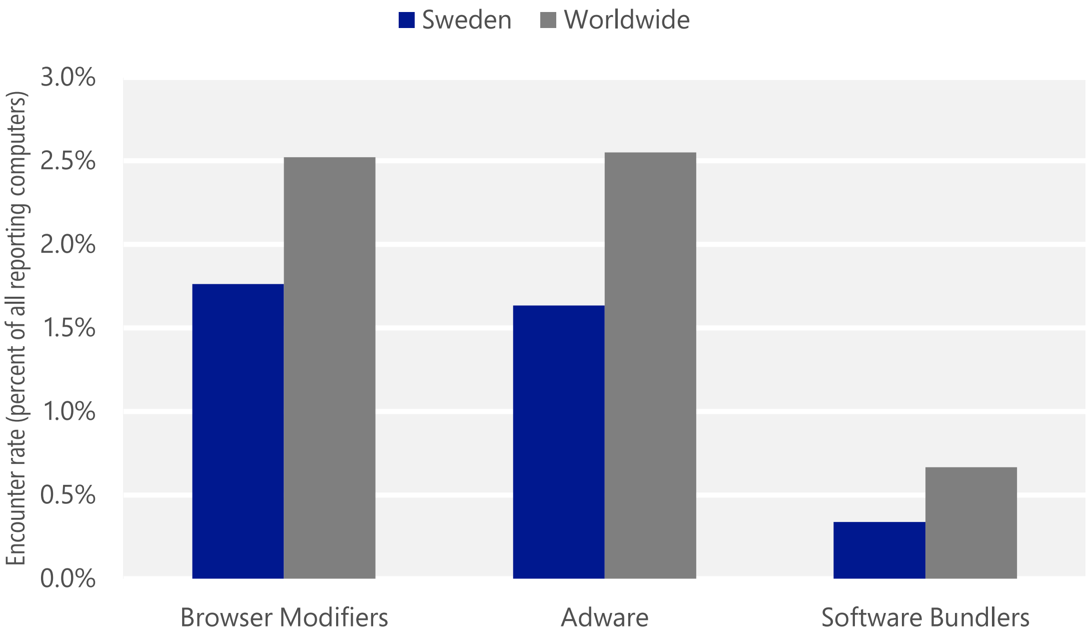
Malware encountered in Sweden in 4Q14, by category



- The most common malware category in Sweden in 4Q14 was Exploits. It was encountered by 1.5 percent of all computers there, down from 2.4 percent in 3Q14.
- The second most common malware category in Sweden in 4Q14 was Trojans. It was encountered by 1.5 percent of all computers there, down from 2.2 percent in 3Q14.
- The third most common malware category in Sweden in 4Q14 was Downloaders & Droppers, which was encountered by 1.0 percent of all computers there, down from 1.5 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Sweden in 4Q14, by category



- The most common unwanted software category in Sweden in 4Q14 was Browser Modifiers. It was encountered by 1.8 percent of all computers there, down from 3.7 percent in 3Q14.
- The second most common unwanted software category in Sweden in 4Q14 was Adware. It was encountered by 1.6 percent of all computers there, up from 1.0 percent in 3Q14.
- The third most common unwanted software category in Sweden in 4Q14 was Software Bundlers, which was encountered by 0.3 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Sweden in 4Q14

	Family	Most significant category	% of reporting computers
1	JS/Axpergle	Exploits	0.9%
2	Win32/Obfuscator	Obfuscators & Injectors	0.7%
3	JS/Faceliker	Trojans	0.2%
4	Win32/Tugspay	Downloaders & Droppers	0.2%
5	JS/Fiexp	Exploits	0.2%
6	MSIL/Pristapi	Downloaders & Droppers	0.2%
7	Win32/Dynamer	Trojans	0.2%
8	Win32/Vatsics	Downloaders & Droppers	0.1%
9	Win32/Wysotot	Trojans	0.1%
10	JS/Astsan	Exploits	0.1%

- The most common malware family encountered in Sweden in 4Q14 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 Sweden in 4Q14 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 third most common malware family encountered in Sweden in 4Q14 was JS/Faceliker, which was encountered by 0.2 percent of reporting computers there. JS/Faceliker is a malicious script that ?likes? content on Facebook without the user’s knowledge or consent.
- The fourth most common malware family encountered in Sweden in 4Q14 was Win32/Tugspay, which was encountered by 0.2 percent of reporting computers there. Win32/Tugspay is a downloader that spreads by posing as an installer for legitimate software, such as a Java update, or through other malware. When installed, it downloads unwanted software to the computer.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Sweden in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	1.5%
2	Win32/Costmin	Adware	0.6%
3	Win32/Pennybee	Adware	0.4%
4	Win32/BetterSurf	Adware	0.3%
5	Win32/Defaulttab	Browser Modifiers	0.3%

- The most common unwanted software family encountered in Sweden in 4Q14 was Win32/Couponruc, which was encountered by 1.5 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 Sweden in 4Q14 was Win32/Costmin, which was encountered by 0.6 percent of reporting computers there. Win32/Costmin is an adware family that installs itself as a browser extension for Internet Explorer, Mozilla Firefox, and Google Chrome, and displays advertisements as the user browses the Internet.
- The third most common unwanted software family encountered in Sweden in 4Q14 was Win32/Pennybee, which was encountered by 0.4 percent of reporting computers there. Win32/Pennybee is adware that shows ads as the user browses the web. It can be installed from the program's website or bundled with some third-party software installation programs.

Top threat families by infection rate

The most common malware families by infection rate in Sweden in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Wysotot	Trojans	0.2
2	Win32/Sefnit	Trojans	0.2
3	MSIL/Bladabindi	Backdoors	0.1
4	Win32/Alureon	Trojans	0.1
5	JS/Miuref	Trojans	0.1
6	Win32/Zbot	Password Stealers & Monitoring Tools	0.1
7	VBS/Jenxcus	Worms	0.1
8	Win32/Sality	Viruses	0.1
9	Win32/Brontok	Worms	0.1
10	Win32/Sirefef	Trojans	0.1

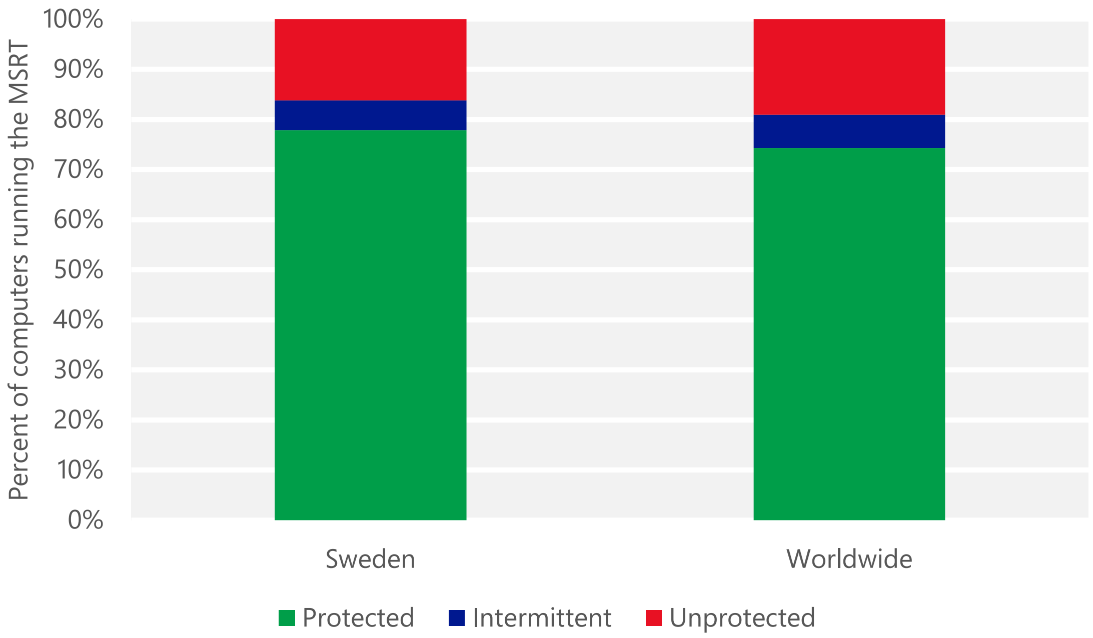
- The most common threat family infecting computers in Sweden in 4Q14 was Win32/Wysotot, which was detected and removed from 0.2 of every 1,000 unique computers scanned by the MSRT. Win32/Wysotot is a threat that can change the start page of the user's web browser, and may download and install other files to the computer. It is installed by software bundlers that advertise free software or games.
- The second most common threat family infecting computers in Sweden in 4Q14 was Win32/Sefnit, which was detected and removed from 0.2 of every 1,000 unique computers scanned by the MSRT. Win32/Sefnit is a family of trojans that can allow backdoor access, download files, and use the computer and Internet connection for click fraud. Some variants can monitor web browsers and hijack search results.
- The third most common threat family infecting computers in Sweden in 4Q14 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.
- The fourth most common threat family infecting computers in Sweden in 4Q14 was Win32/Alureon, which was detected and removed from 0.1 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.

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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.86 drive-by download URLs for every 1,000 URLs hosted in Sweden, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.03 drive-by download URLs for every 1,000 URLs hosted in Sweden, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Sweden and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Sweden	0.86	0.03
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Switzerland

The statistics presented here are generated by Microsoft security programs and services running on computers in Switzerland in 4Q14 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 succeds 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

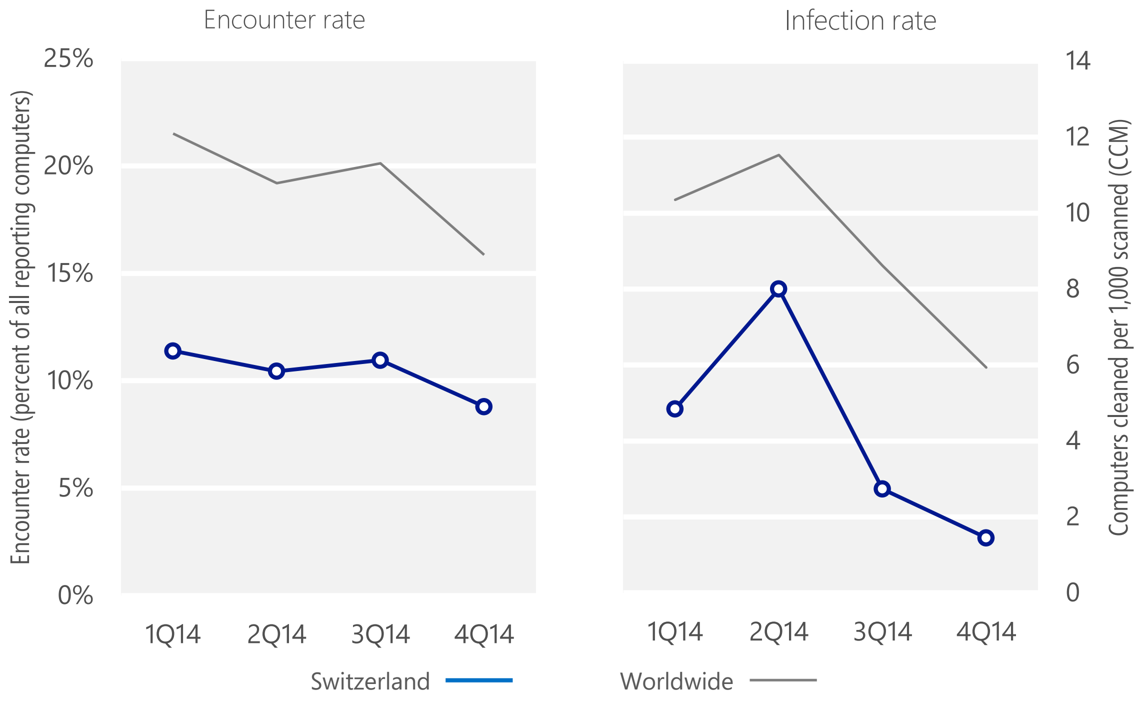
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Switzerland	11.4%	10.4%	11.0%	8.8%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Switzerland	4.8	8.0	2.7	1.5
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 8.8% percent of computers in Switzerland encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 1.5 of every 1,000 unique computers scanned in Switzerland in 4Q14 (a CCM score of 1.5, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Switzerland over the last four quarters, compared to the world as a whole.

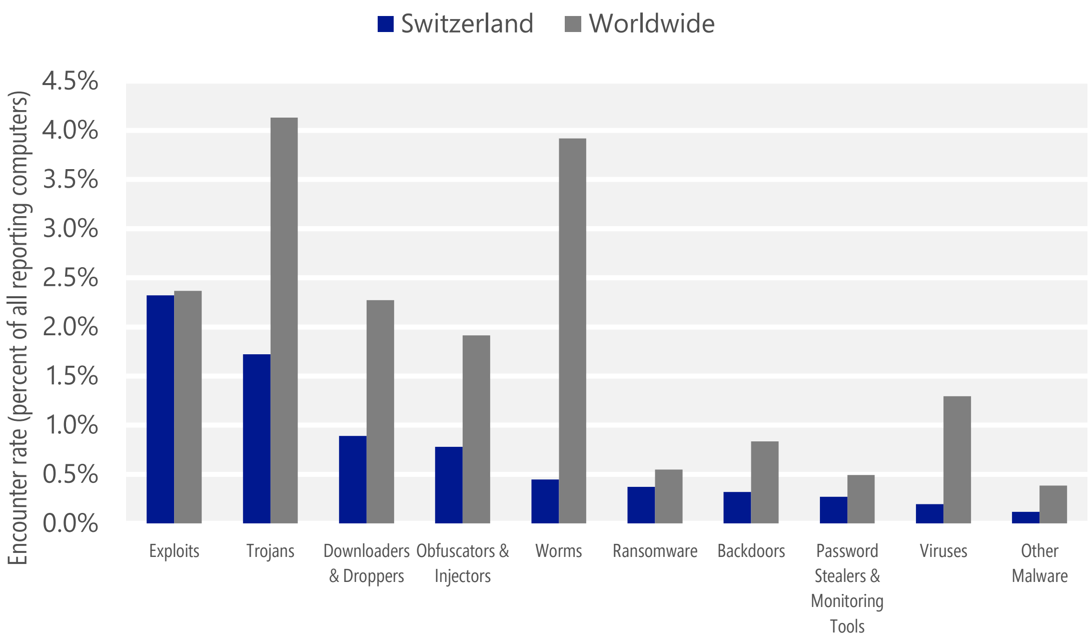
Malware encounter and infection rate trends in Switzerland and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

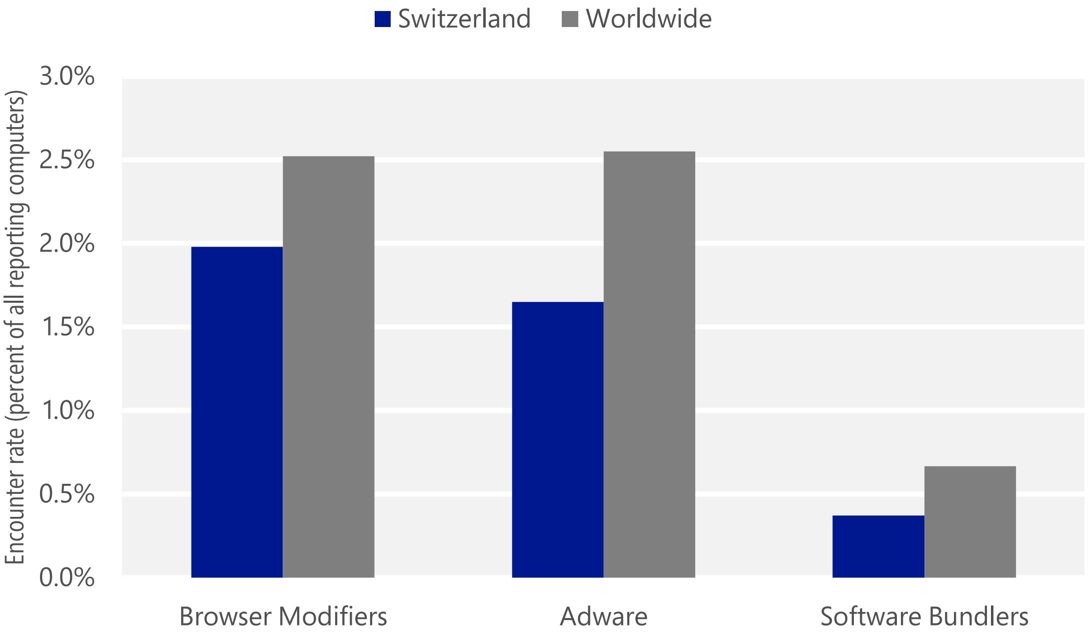
Malware encountered in Switzerland in 4Q14, by category



- The most common malware category in Switzerland in 4Q14 was Exploits. It was encountered by 2.3 percent of all computers there, down from 2.6 percent in 3Q14.
- The second most common malware category in Switzerland in 4Q14 was Trojans. It was encountered by 1.7 percent of all computers there, down from 2.3 percent in 3Q14.
- The third most common malware category in Switzerland in 4Q14 was Downloaders & Droppers, which was encountered by 0.9 percent of all computers there, down from 2.2 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Switzerland in 4Q14, by category



- The most common unwanted software category in Switzerland in 4Q14 was Browser Modifiers. It was encountered by 2.0 percent of all computers there, down from 4.0 percent in 3Q14.
- The second most common unwanted software category in Switzerland in 4Q14 was Adware. It was encountered by 1.7 percent of all computers there, up from 0.6 percent in 3Q14.
- The third most common unwanted software category in Switzerland in 4Q14 was Software Bundlers, which was encountered by 0.4 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Switzerland in 4Q14

	Family	Most significant category	% of reporting computers
1	JS/Axpergle	Exploits	1.4%
2	Win32/Obfuscator	Obfuscators & Injectors	0.6%
3	JS/Neclu	Exploits	0.2%
4	Win32/Emotet	Trojans	0.2%
5	JS/Fiexp	Exploits	0.2%
6	JS/Krypterade	Ransomware	0.2%
7	ASX/Wimad	Downloaders & Droppers	0.2%
8	Win32/Dynamer	Trojans	0.1%
9	JS/Astsan	Exploits	0.1%
10	Win32/Reveton	Ransomware	0.1%

- The most common malware family encountered in Switzerland in 4Q14 was JS/Axpergle, which was encountered by 1.4 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 second most common malware family encountered in Switzerland in 4Q14 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 Switzerland in 4Q14 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 Switzerland in 4Q14 was Win32/Emotet, which was encountered by 0.2 percent of reporting computers there. 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.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Switzerland in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	1.7%
2	Win32/Costmin	Adware	0.7%
3	Win32/BetterSurf	Adware	0.4%
4	Win32/Pirrit	Adware	0.3%
5	Win32/Defaulttab	Browser Modifiers	0.2%

- The most common unwanted software family encountered in Switzerland in 4Q14 was Win32/Couponruc, which was encountered by 1.7 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 Switzerland in 4Q14 was Win32/Costmin, which was encountered by 0.7 percent of reporting computers there. Win32/Costmin is an adware family that installs itself as a browser extension for Internet Explorer, Mozilla Firefox, and Google Chrome, and displays advertisements as the user browses the Internet.
- The third most common unwanted software family encountered in Switzerland in 4Q14 was Win32/BetterSurf, which was encountered by 0.4 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.

Top threat families by infection rate

The most common malware families by infection rate in Switzerland in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Sefnit	Trojans	0.2
2	Win32/Wysotot	Trojans	0.2
3	Win32/Zbot	Password Stealers & Monitoring Tools	0.1
4	Win32/Alureon	Trojans	0.1
5	JS/Miuref	Trojans	0.1
6	VBS/Jenxcus	Worms	0.1
7	Win32/Gamarue	Worms	<0.1
8	MSIL/Bladabindi	Backdoors	<0.1
9	Win32/Ramnit	Trojans	<0.1
10	Win32/Sality	Viruses	<0.1

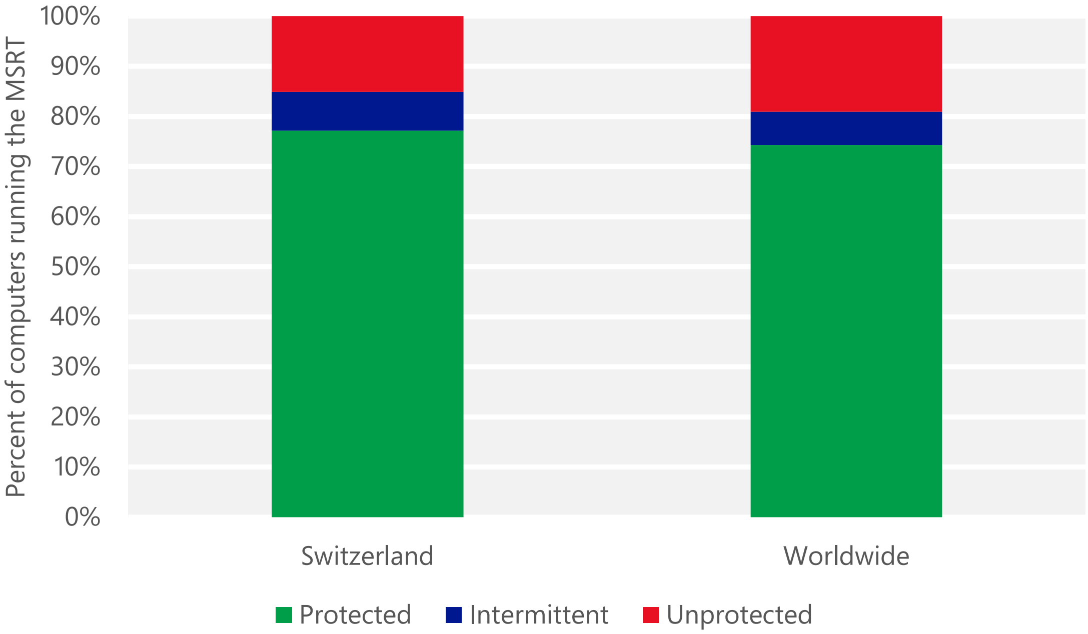
- The most common threat family infecting computers in Switzerland in 4Q14 was Win32/Sefnit, which was detected and removed from 0.2 of every 1,000 unique computers scanned by the MSRT. Win32/Sefnit is a family of trojans that can allow backdoor access, download files, and use the computer and Internet connection for click fraud. Some variants can monitor web browsers and hijack search results.
- The second most common threat family infecting computers in Switzerland in 4Q14 was Win32/Wysotot, which was detected and removed from 0.2 of every 1,000 unique computers scanned by the MSRT. Win32/Wysotot is a threat that can change the start page of the user's web browser, and may download and install other files to the computer. It is installed by software bundlers that advertise free software or games.
- The third most common threat family infecting computers in Switzerland in 4Q14 was Win32/Zbot, which was detected and removed from 0.1 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 fourth most common threat family infecting computers in Switzerland in 4Q14 was Win32/Alureon, which was detected and removed from 0.1 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.

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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.12 drive-by download URLs for every 1,000 URLs hosted in Switzerland, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.10 drive-by download URLs for every 1,000 URLs hosted in Switzerland, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Switzerland and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Switzerland	0.12	0.10
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Taiwan

The statistics presented here are generated by Microsoft security programs and services running on computers in Taiwan in 4Q14 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 succeds 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

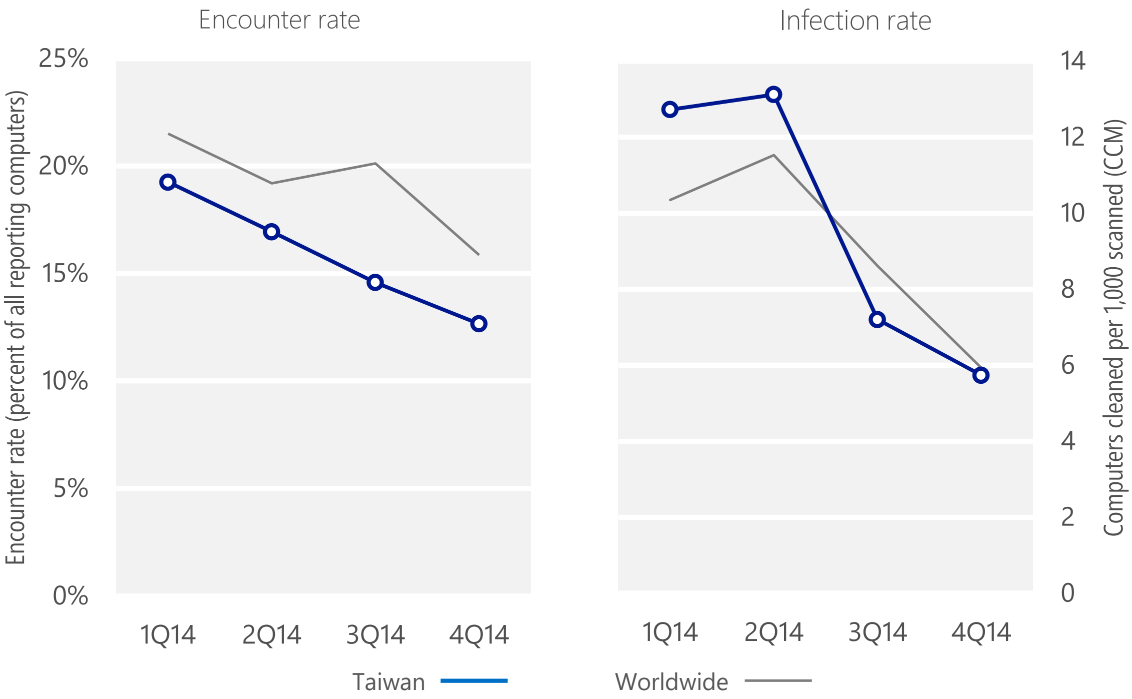
Metric	**1Q14**	**2Q14**	**3Q14**	**4Q14**
Encounter rate, Taiwan	19.3%	16.9%	14.6%	12.7%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Taiwan	12.7	13.1	7.2	5.7
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 12.7% percent of computers in Taiwan encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 5.7 of every 1,000 unique computers scanned in Taiwan in 4Q14 (a CCM score of 5.7, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Taiwan over the last four quarters, compared to the world as a whole.

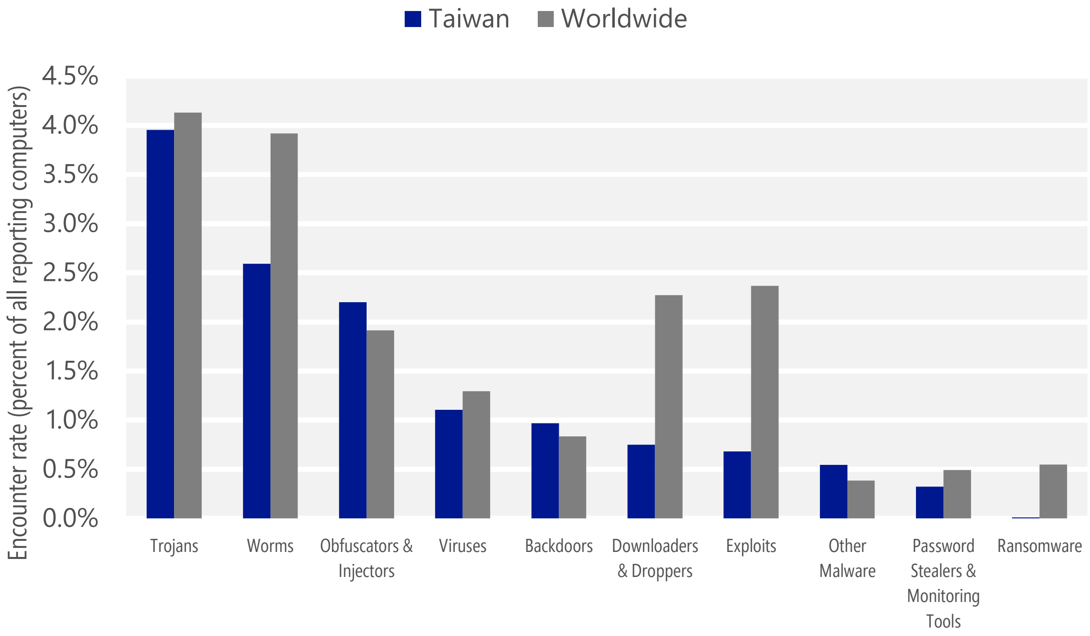
Malware encounter and infection rate trends in Taiwan and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

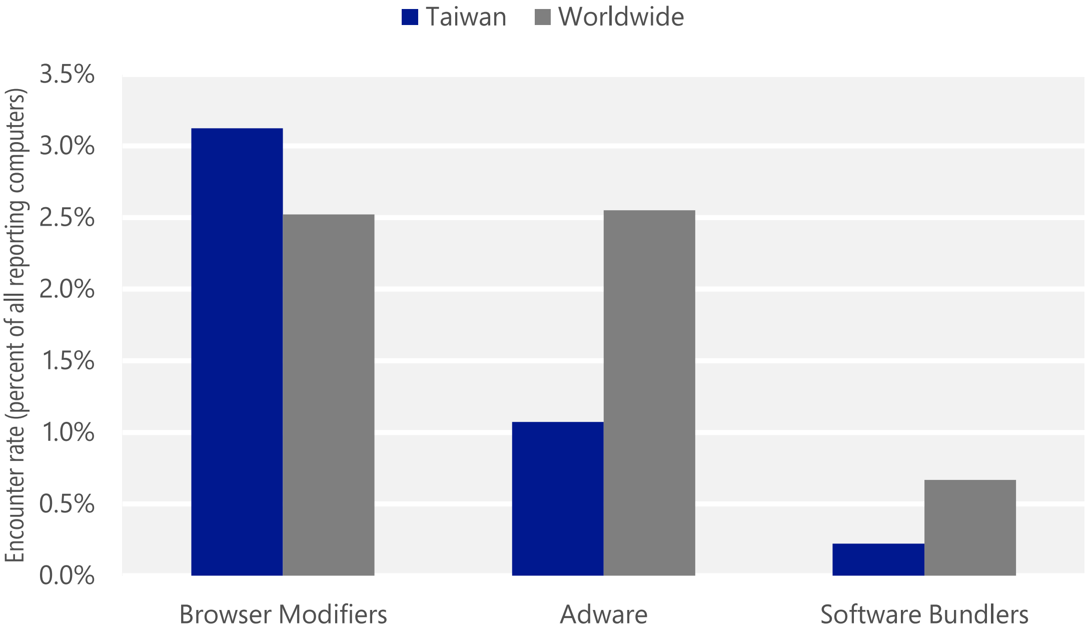
Malware encountered in Taiwan in 4Q14, by category



- The most common malware category in Taiwan in 4Q14 was Trojans. It was encountered by 4.0 percent of all computers there, down from 5.2 percent in 3Q14.
- The second most common malware category in Taiwan in 4Q14 was Worms. It was encountered by 2.6 percent of all computers there, up from 2.5 percent in 3Q14.
- The third most common malware category in Taiwan in 4Q14 was Obfuscators & Injectors, which was encountered by 2.2 percent of all computers there, down from 2.5 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Taiwan in 4Q14, by category



- The most common unwanted software category in Taiwan in 4Q14 was Browser Modifiers. It was encountered by 3.1 percent of all computers there, down from 3.5 percent in 3Q14.
- The second most common unwanted software category in Taiwan in 4Q14 was Adware. It was encountered by 1.1 percent of all computers there, up from 0.2 percent in 3Q14.
- The third most common unwanted software category in Taiwan in 4Q14 was Software Bundlers, which was encountered by 0.2 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Taiwan in 4Q14

	Family	Most significant category	% of reporting computers
1	INF/Autorun	Obfuscators & Injectors	1.5%
2	Win32/Obfuscator	Obfuscators & Injectors	1.0%
3	MSIL/Hakey	Trojans	0.8%
4	Win32/Conficker	Worms	0.6%
5	Win32/Dynamer	Trojans	0.5%
6	Win32/Nitol	Other Malware	0.5%
7	Win32/FlyAgent	Backdoors	0.5%
8	VBS/Jenxcus	Worms	0.4%
9	Win32/Taterf	Worms	0.3%
10	Win32/Rimecud	Worms	0.3%

- The most common malware family encountered in Taiwan in 4Q14 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 second most common malware family encountered in Taiwan in 4Q14 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.
- The third most common malware family encountered in Taiwan in 4Q14 was MSIL/Hakey, which was encountered by 0.8 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.
- The fourth most common malware family encountered in Taiwan in 4Q14 was Win32/Conficker, which was encountered by 0.6 percent of reporting computers there. Win32/Conficker is a worm that spreads by exploiting a vulnerability addressed by Security Bulletin MS08-067. Some variants also spread via removable drives and by exploiting weak passwords. It disables several important system services and security products, and downloads arbitrary files.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Taiwan in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	2.7%
2	Win32/Costmin	Adware	0.7%
3	Win32/Defaulttab	Browser Modifiers	0.4%
4	Win32/BetterSurf	Adware	0.2%
5	Win32/Gofileexpress	Software Bundlers	0.2%

- The most common unwanted software family encountered in Taiwan in 4Q14 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 second most common unwanted software family encountered in Taiwan in 4Q14 was Win32/Costmin, which was encountered by 0.7 percent of reporting computers there. Win32/Costmin is an adware family that installs itself as a browser extension for Internet Explorer, Mozilla Firefox, and Google Chrome, and displays advertisements as the user browses the Internet.
- The third most common unwanted software family encountered in Taiwan in 4Q14 was Win32/Defaulttab, which was encountered by 0.4 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.

Top threat families by infection rate

The most common malware families by infection rate in Taiwan in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Nitol	Other Malware	1.5
2	Win32/Sality	Viruses	0.5
3	Win32/Frethog	Password Stealers & Monitoring Tools	0.4
4	VBS/Jenxcus	Worms	0.4
5	Win32/Wysotot	Trojans	0.3
6	Win32/Hupigon	Backdoors	0.3
7	Win32/Ramnit	Trojans	0.3
8	Win32/Taterf	Worms	0.3
9	Win32/Rimecud	Worms	0.2
10	Win32/Sefnit	Trojans	0.2

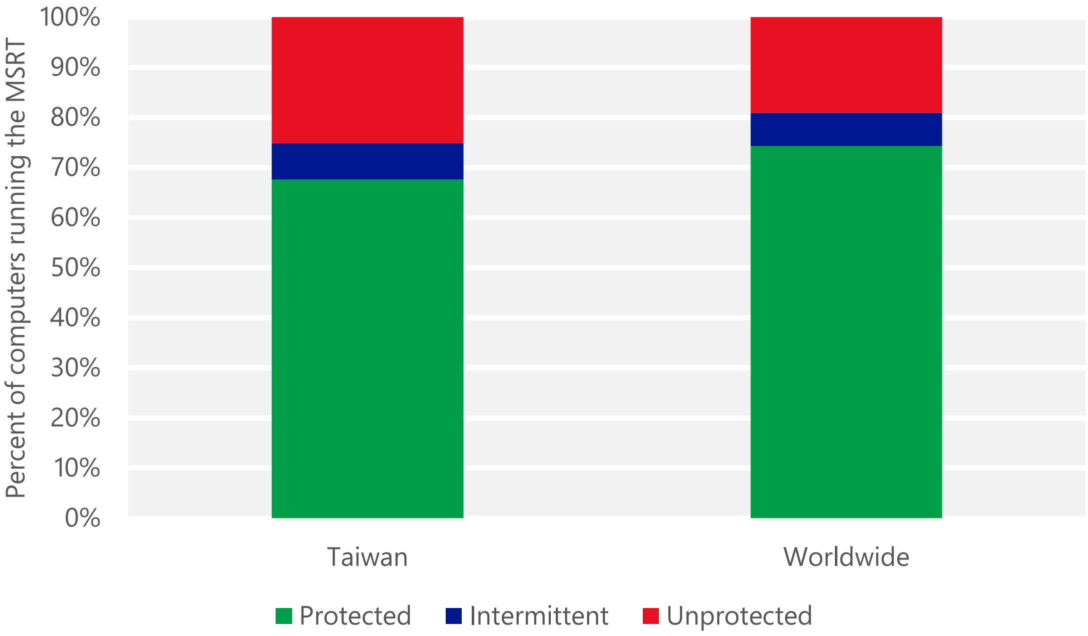
- The most common threat family infecting computers in Taiwan in 4Q14 was Win32/Nitol, which was detected and removed from 1.5 of every 1,000 unique computers scanned by the MSRT. Win32/Nitol is a family of trojans that perform DDoS (distributed denial of service) attacks, allow backdoor access and control, 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 4Q14 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.
- The third most common threat family infecting computers in Taiwan in 4Q14 was Win32/Frethog, which was detected and removed from 0.4 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 Taiwan in 4Q14 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 Taiwan and worldwide protected by real-time security software in 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 11.03 drive-by download URLs for every 1,000 URLs hosted in Taiwan, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 12.07 drive-by download URLs for every 1,000 URLs hosted in Taiwan, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Taiwan and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Taiwan	11.03	12.07
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Tanzania

The statistics presented here are generated by Microsoft security programs and services running on computers in Tanzania in 4Q14 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 succeds 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

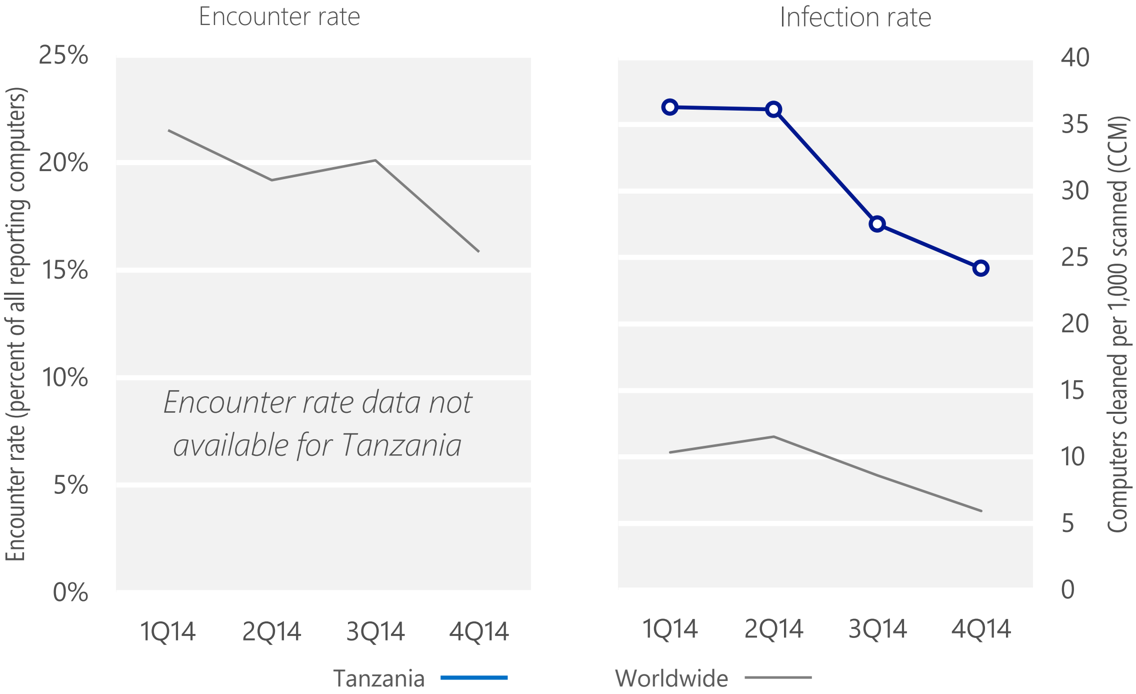
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Tanzania	N/A	N/A	N/A	N/A
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Tanzania	36.3	36.1	27.5	24.2
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, the MSRT detected and removed malware from 24.2 of every 1,000 unique computers scanned in Tanzania in 4Q14 (a CCM score of 24.2, compared to the 4Q14 worldwide CCM of 5.9). 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 18* 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 4Q14

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	8.2
2	Win32/Gamarue	Worms	7.2
3	Win32/Sality	Viruses	4.5
4	Win32/Ramnit	Trojans	2.1
5	Win32/Chir	Viruses	1.0
6	MSIL/Bladabindi	Backdoors	0.5
7	Win32/Zbot	Password Stealers & Monitoring Tools	0.4
8	Win32/Nuqel	Worms	0.3
9	Win32/Dorkbot	Worms	0.3
10	Win32/Virut	Viruses	0.3

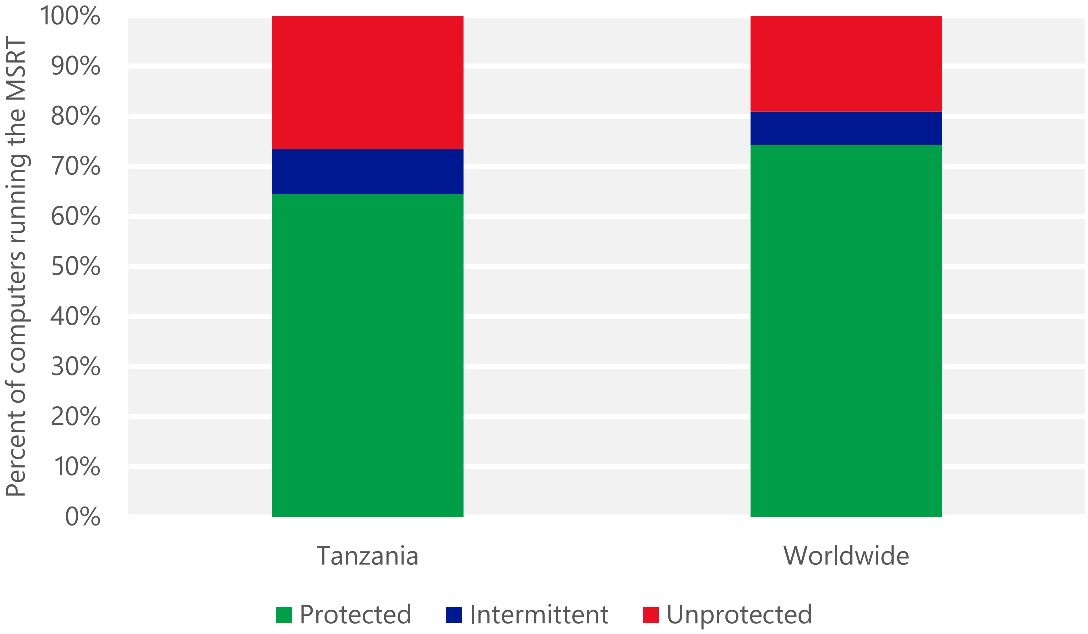
- The most common threat family infecting computers in Tanzania in 4Q14 was VBS/Jenxcus, which was detected and removed from 8.2 of every 1,000 unique computers scanned by the MSRT. VBS/Jenxcus is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Tanzania in 4Q14 was Win32/Gamarue, which was detected and removed from 7.2 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 Tanzania in 4Q14 was Win32/Sality, which was detected and removed from 4.5 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 fourth most common threat family infecting computers in Tanzania in 4Q14 was Win32/Ramnit, which was detected and removed from 2.1 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.

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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 3.65 drive-by download URLs for every 1,000 URLs hosted in Tanzania, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 3.35 drive-by download URLs for every 1,000 URLs hosted in Tanzania, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Tanzania and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Tanzania	3.65	3.35
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Thailand

The statistics presented here are generated by Microsoft security programs and services running on computers in Thailand in 4Q14 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 succeds 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

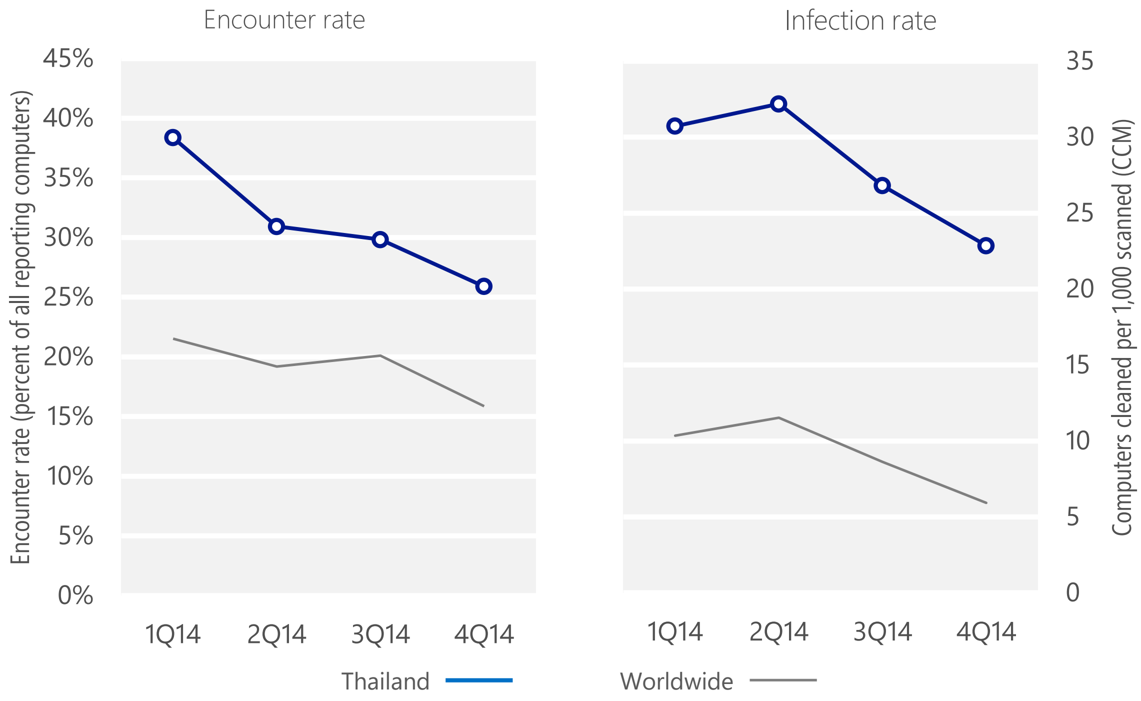
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Thailand	38.4%	30.9%	29.8%	25.9%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Thailand	30.7	32.2	26.8	22.9
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 25.9% percent of computers in Thailand encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 22.9 of every 1,000 unique computers scanned in Thailand in 4Q14 (a CCM score of 22.9, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Thailand over the last four quarters, compared to the world as a whole.

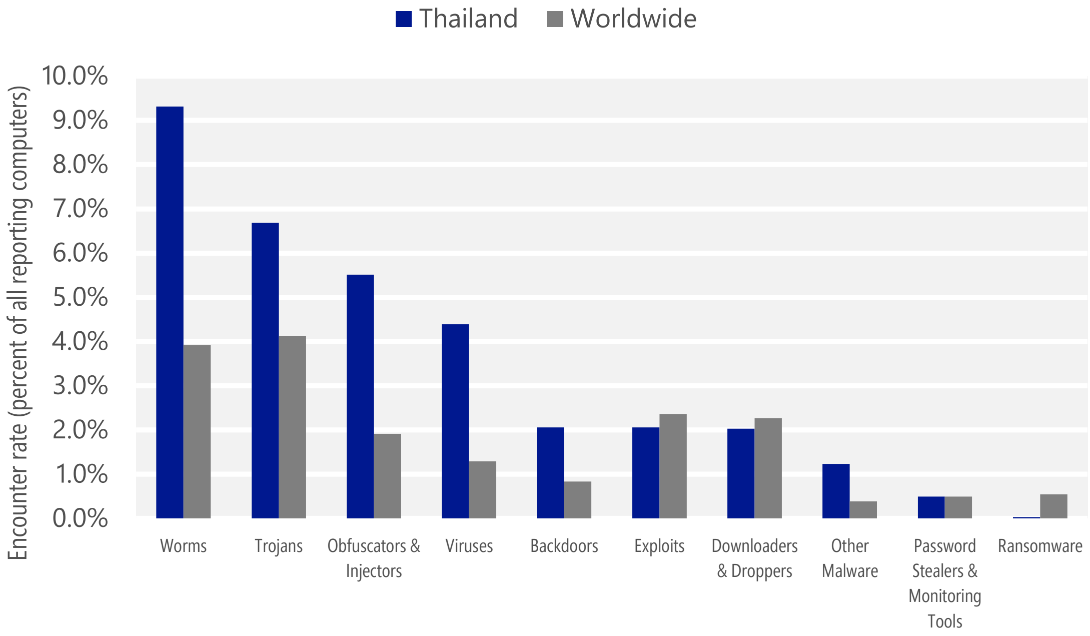
Malware encounter and infection rate trends in Thailand and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

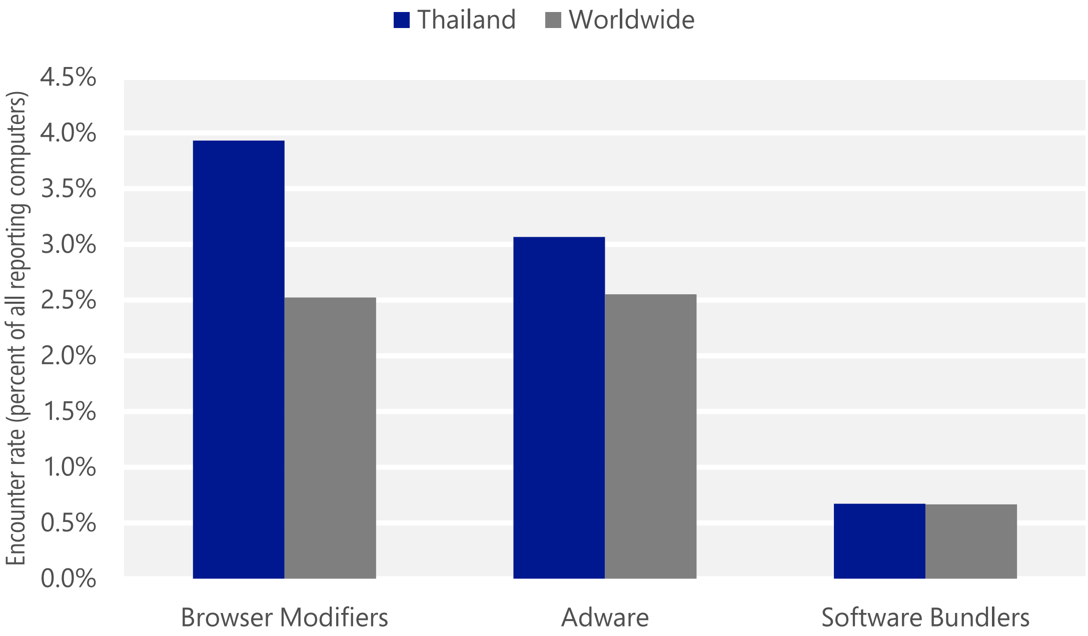
Malware encountered in Thailand in 4Q14, by category



- The most common malware category in Thailand in 4Q14 was Worms. It was encountered by 9.3 percent of all computers there, down from 10.9 percent in 3Q14.
- The second most common malware category in Thailand in 4Q14 was Trojans. It was encountered by 6.7 percent of all computers there, down from 9.5 percent in 3Q14.
- The third most common malware category in Thailand in 4Q14 was Obfuscators & Injectors, which was encountered by 5.5 percent of all computers there, up from 4.9 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Thailand in 4Q14, by category



- The most common unwanted software category in Thailand in 4Q14 was Browser Modifiers. It was encountered by 3.9 percent of all computers there, down from 6.1 percent in 3Q14.
- The second most common unwanted software category in Thailand in 4Q14 was Adware. It was encountered by 3.1 percent of all computers there, up from 0.9 percent in 3Q14.
- The third most common unwanted software category in Thailand in 4Q14 was Software Bundlers, which was encountered by 0.7 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Thailand in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Gamarue	Worms	4.7%
2	Win32/Obfuscator	Obfuscators & Injectors	3.3%
3	INF/Autorun	Obfuscators & Injectors	2.2%
4	Win32/Sality	Viruses	2.2%
5	Win32/Ramnit	Trojans	1.6%
6	VBS/Jenxcus	Worms	1.2%
7	Win32/CplLnk	Exploits	1.0%
8	Win32/Nitol	Other Malware	1.0%
9	Win32/Ceatrg	Trojans	0.9%
10	MSIL/Bladabindi	Backdoors	0.8%

- The most common malware family encountered in Thailand in 4Q14 was Win32/Gamarue, which was encountered by 4.7 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 4Q14 was Win32/Obfuscator, which was encountered by 3.3 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 third most common malware family encountered in Thailand in 4Q14 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.
- The fourth most common malware family encountered in Thailand in 4Q14 was Win32/Sality, which was encountered by 2.2 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 Thailand in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	3.4%
2	Win32/Costmin	Adware	1.3%
3	Win32/BetterSurf	Adware	0.9%
4	Win32/Pennybee	Adware	0.8%
5	Win32/Defaulttab	Browser Modifiers	0.6%

- The most common unwanted software family encountered in Thailand in 4Q14 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 Thailand in 4Q14 was Win32/Costmin, which was encountered by 1.3 percent of reporting computers there. Win32/Costmin is an adware family that installs itself as a browser extension for Internet Explorer, Mozilla Firefox, and Google Chrome, and displays advertisements as the user browses the Internet.
- The third most common unwanted software family encountered in Thailand in 4Q14 was Win32/BetterSurf, which was encountered by 0.9 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.

Top threat families by infection rate

The most common malware families by infection rate in Thailand in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Sality	Viruses	6.8
2	Win32/Gamarue	Worms	4.8
3	Win32/Ramnit	Trojans	3.1
4	Win32/Nitol	Other Malware	2.3
5	MSIL/Bladabindi	Backdoors	2.0
6	VBS/Jenxcus	Worms	1.9
7	Win32/Pramro	Trojans	1.0
8	Win32/Wysotot	Trojans	0.5
9	Win32/Sefnit	Trojans	0.4
10	Win32/Dorkbot	Worms	0.4

- The most common threat family infecting computers in Thailand in 4Q14 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 second most common threat family infecting computers in Thailand in 4Q14 was Win32/Gamarue, which was detected and removed from 4.8 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 Thailand in 4Q14 was Win32/Ramnit, which was detected and removed from 3.1 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 fourth most common threat family infecting computers in Thailand in 4Q14 was Win32/Nitol, which was detected and removed from 2.3 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

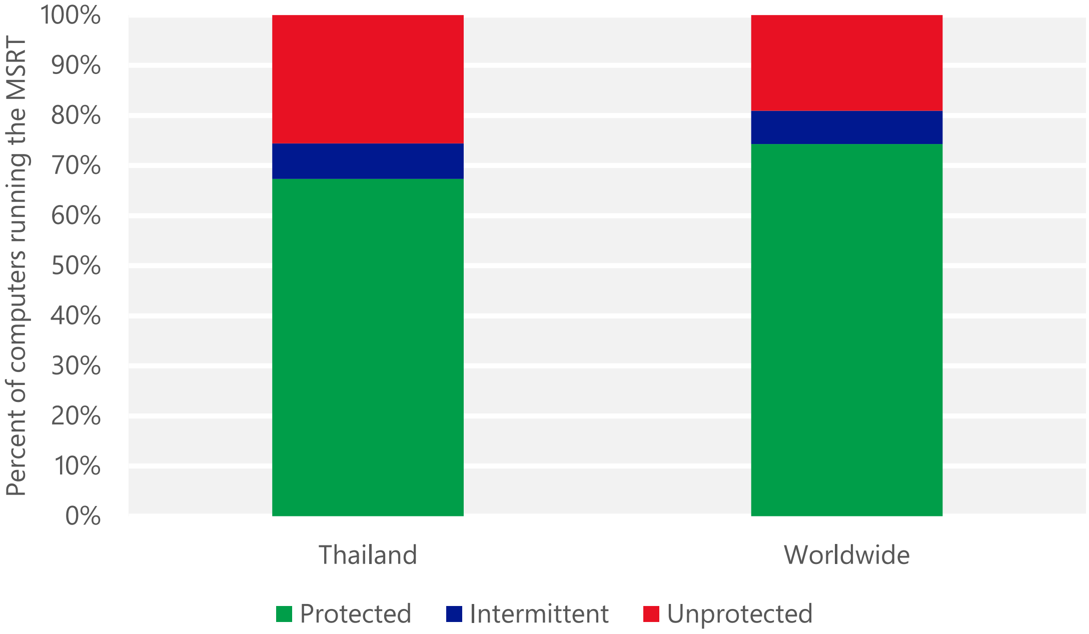
control, download and run files, and perform a number of other malicious activities on the computer.

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 Thailand and worldwide protected by real-time security software in 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 1.21 drive-by download URLs for every 1,000 URLs hosted in Thailand, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.98 drive-by download URLs for every 1,000 URLs hosted in Thailand, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Thailand and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Thailand	1.21	0.98
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Trinidad and Tobago

The statistics presented here are generated by Microsoft security programs and services running on computers in Trinidad and Tobago in 4Q14 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 succeds 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

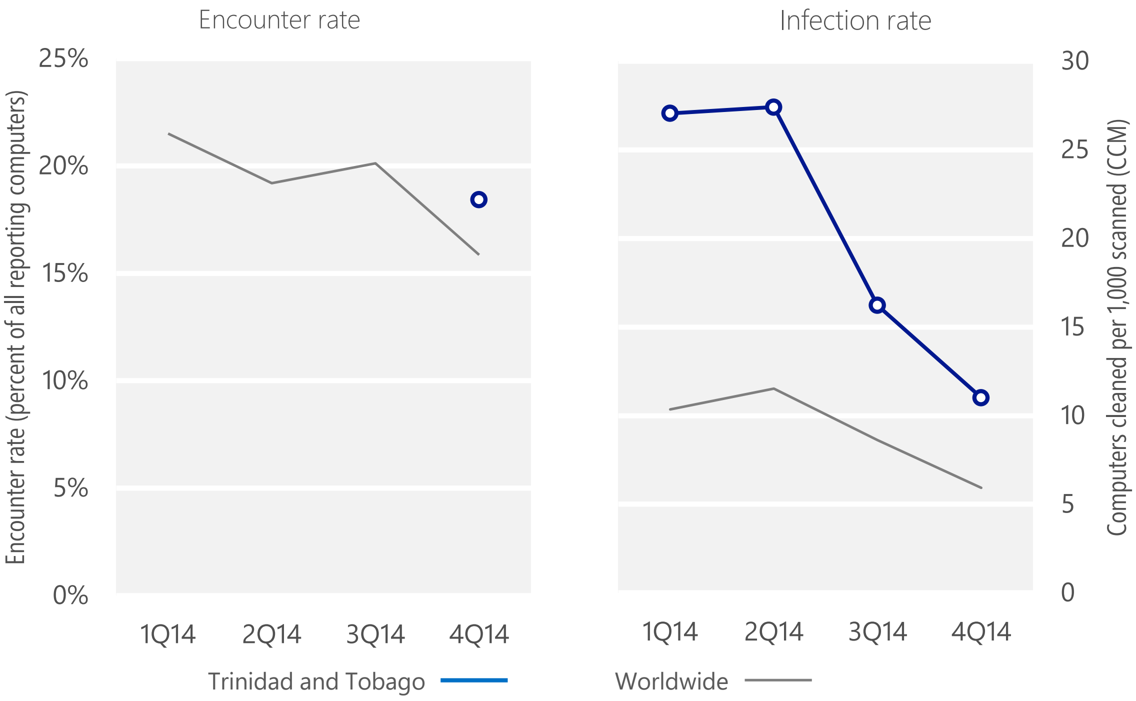
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Trinidad and Tobago	N/A	N/A	N/A	18.4%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Trinidad and Tobago	27.1	27.4	16.2	11.0
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 18.4% percent of computers in Trinidad and Tobago encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 11.0 of every 1,000 unique computers scanned in Trinidad and Tobago in 4Q14 (a CCM score of 11.0, compared to the 4Q14 worldwide CCM of 5.9). 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.

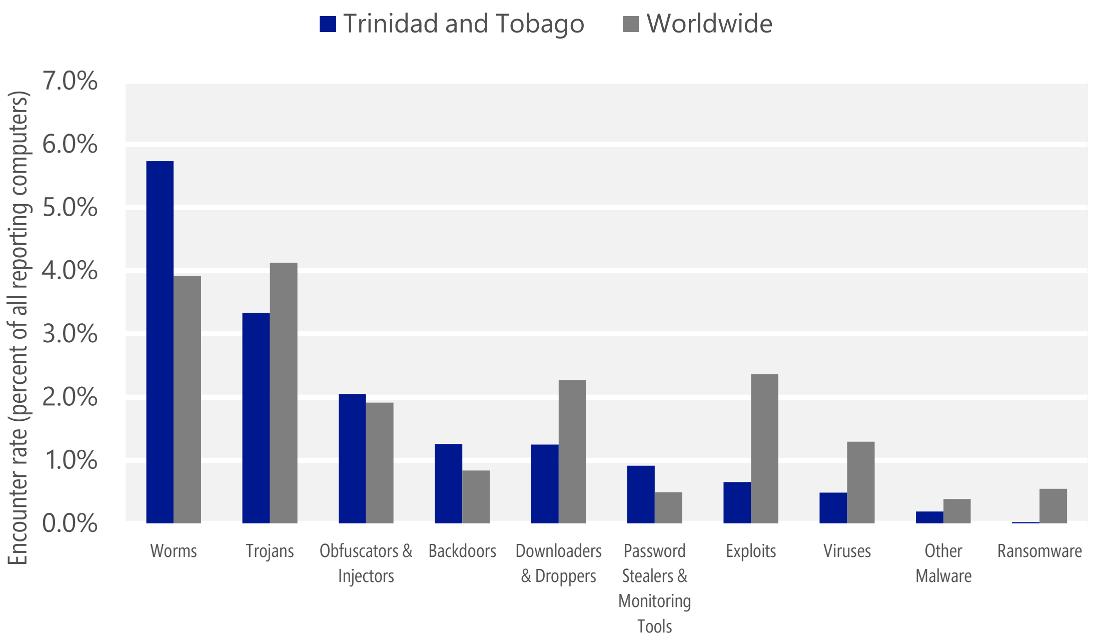
Malware encounter and infection rate trends in Trinidad and Tobago and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

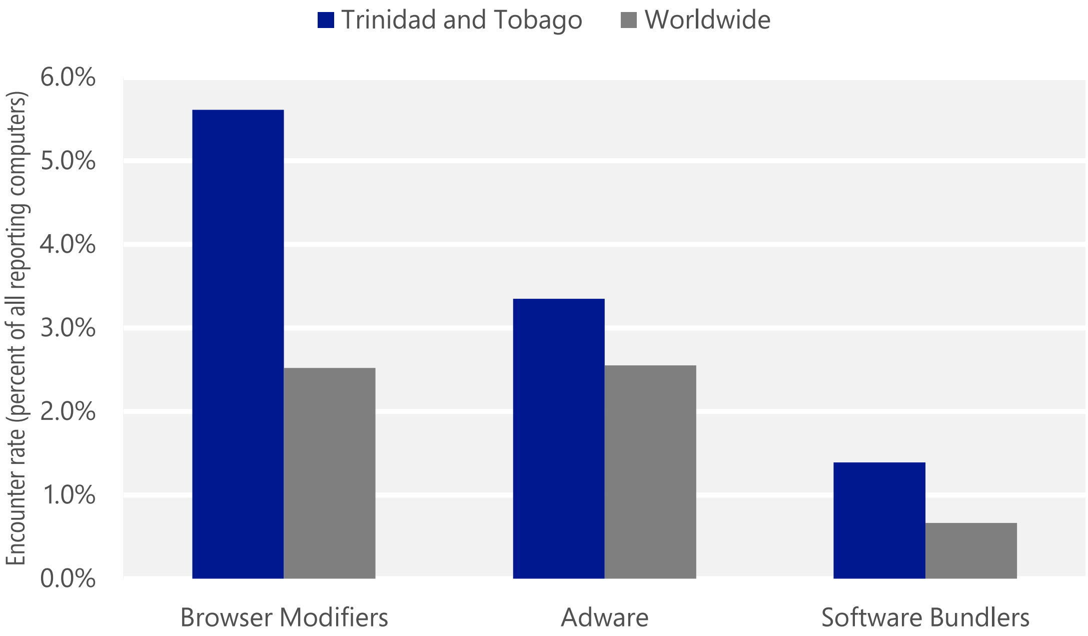
Malware encountered in Trinidad and Tobago in 4Q14, by category



- The most common malware category in Trinidad and Tobago in 4Q14 was Worms. It was encountered by 5.7 percent of all computers there, up from N/A percent in 3Q14.
- The second most common malware category in Trinidad and Tobago in 4Q14 was Trojans. It was encountered by 3.3 percent of all computers there, up from N/A percent in 3Q14.
- The third most common malware category in Trinidad and Tobago in 4Q14 was Obfuscators & Injectors, which was encountered by 2.1 percent of all computers there, up from N/A percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Trinidad and Tobago in 4Q14, by category



- The most common unwanted software category in Trinidad and Tobago in 4Q14 was Browser Modifiers. It was encountered by 5.6 percent of all computers there, up from N/A percent in 3Q14.
- The second most common unwanted software category in Trinidad and Tobago in 4Q14 was Adware. It was encountered by 3.3 percent of all computers there, up from N/A percent in 3Q14.
- The third most common unwanted software category in Trinidad and Tobago in 4Q14 was Software Bundlers, which was encountered by 1.4 percent of all computers there, up from N/A percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Trinidad and Tobago in 4Q14

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	3.9%
2	INF/Autorun	Obfuscators & Injectors	1.0%
3	Win32/Obfuscator	Obfuscators & Injectors	1.0%

- The most common malware family encountered in Trinidad and Tobago in 4Q14 was VBS/Jenxcus, which was encountered by 3.9 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 Trinidad and Tobago in 4Q14 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 third most common malware family encountered in Trinidad and Tobago in 4Q14 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.
- The fourth most common malware family encountered in Trinidad and Tobago in 4Q14 was N/A, which was encountered by percent of reporting computers there.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Trinidad and Tobago in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	3.7%
2	Win32/Defaulttab	Browser Modifiers	2.2%
3	Win32/BetterSurf	Adware	1.6%
4	Win32/Costmin	Adware	1.4%
5	Win32/Gofileexpress	Software Bundlers	1.0%

- The most common unwanted software family encountered in Trinidad and Tobago in 4Q14 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 Trinidad and Tobago in 4Q14 was Win32/Defaulttab, which was encountered by 2.2 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.

- The third most common unwanted software family encountered in Trinidad and Tobago in 4Q14 was Win32/BetterSurf, which was encountered by 1.6 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.

Top threat families by infection rate

The most common malware families by infection rate in Trinidad and Tobago in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	5.8
2	MSIL/Bladabindi	Backdoors	1.0
3	Win32/Brontok	Worms	0.8
4	Win32/IRCbot	Backdoors	0.7
5	Win32/Vobfus	Worms	0.7
6	Win32/Sefnit	Trojans	0.3
7	Win32/Alureon	Trojans	0.3
8	Win32/Dorkbot	Worms	0.2
9	Win32/Conficker	Worms	0.2
10	Win32/Gamarue	Worms	0.2

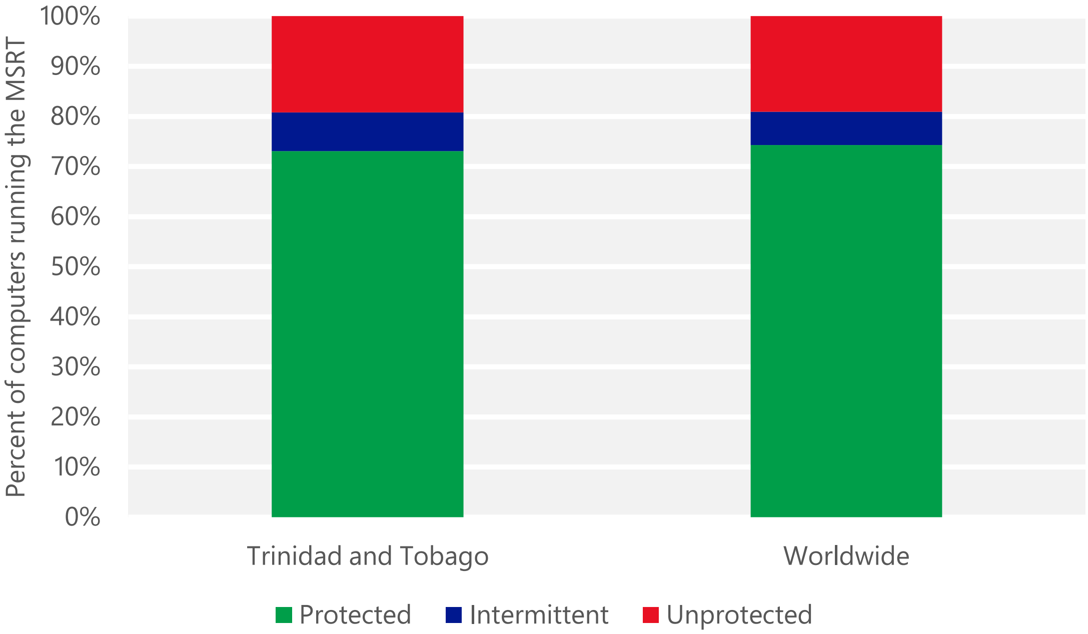
- The most common threat family infecting computers in Trinidad and Tobago in 4Q14 was VBS/Jenxcus, which was detected and removed from 5.8 of every 1,000 unique computers scanned by the MSRT. VBS/Jenxcus is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Trinidad and Tobago in 4Q14 was MSIL/Bladabindi, which was detected and removed from 1.0 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 Trinidad and Tobago in 4Q14 was Win32/Brontok, which was detected and removed from 0.8 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 Trinidad and Tobago in 4Q14 was Win32/IRCbot, which was detected and removed from 0.7 of every 1,000 unique computers scanned by the MSRT. Win32/IRCbot is a large family of backdoor trojans that drops other malicious software and connects to IRC servers to receive commands from 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 Trinidad and Tobago and worldwide protected by real-time security software in 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.00 drive-by download URLs for every 1,000 URLs hosted in Trinidad and Tobago, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.00 drive-by download URLs for every 1,000 URLs hosted in Trinidad and Tobago, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Trinidad and Tobago and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Trinidad and Tobago	0.00	0.00
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Tunisia

The statistics presented here are generated by Microsoft security programs and services running on computers in Tunisia in 4Q14 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 succeds 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

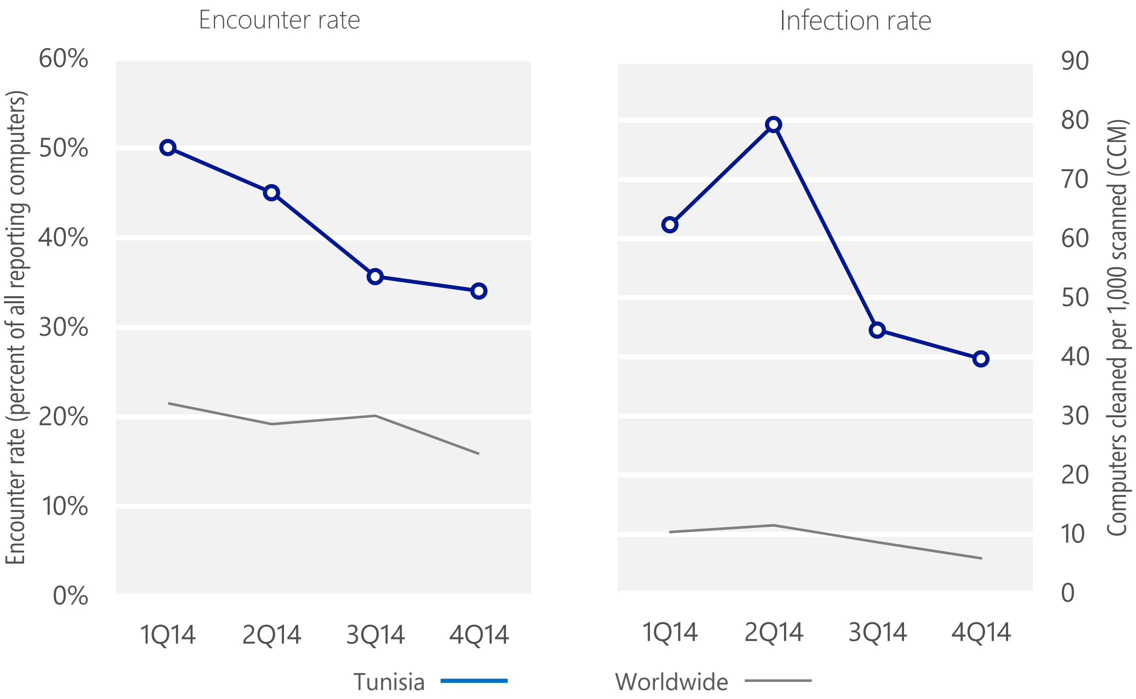
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Tunisia	50.1%	45.0%	35.7%	34.1%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Tunisia	62.3	79.3	44.5	39.7
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 34.1% percent of computers in Tunisia encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 39.7 of every 1,000 unique computers scanned in Tunisia in 4Q14 (a CCM score of 39.7, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Tunisia over the last four quarters, compared to the world as a whole.

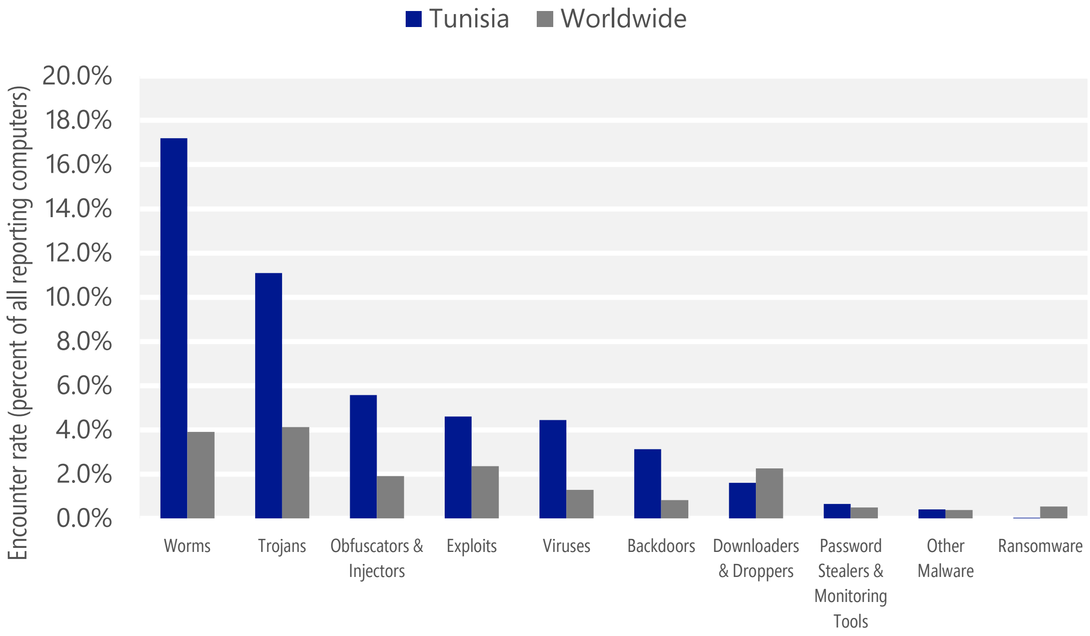
Malware encounter and infection rate trends in Tunisia and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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 4Q14, by category



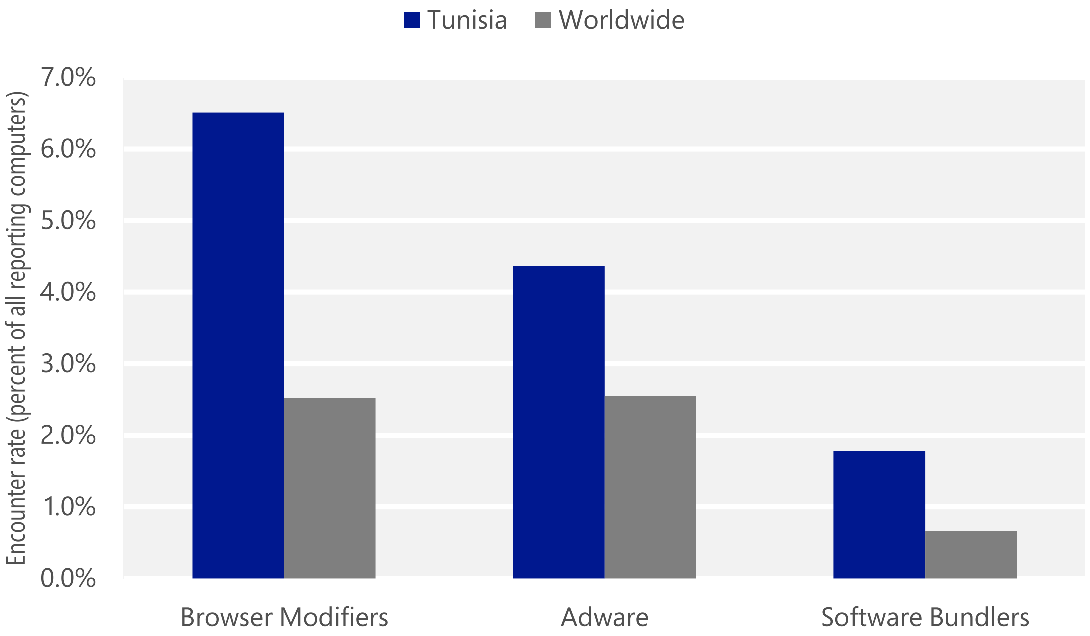
- The most common malware category in Tunisia in 4Q14 was Worms. It was encountered by 17.2 percent of all computers there, up from 16.4 percent in 3Q14.

- The second most common malware category in Tunisia in 4Q14 was Trojans. It was encountered by 11.1 percent of all computers there, down from 14.3 percent in 3Q14.

- The third most common malware category in Tunisia in 4Q14 was Obfuscators & Injectors, which was encountered by 5.6 percent of all computers there, up from 4.9 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Tunisia in 4Q14, by category



- The most common unwanted software category in Tunisia in 4Q14 was Browser Modifiers. It was encountered by 6.5 percent of all computers there, down from 8.0 percent in 3Q14.
- The second most common unwanted software category in Tunisia in 4Q14 was Adware. It was encountered by 4.4 percent of all computers there, up from 0.9 percent in 3Q14.
- The third most common unwanted software category in Tunisia in 4Q14 was Software Bundlers, which was encountered by 1.8 percent of all computers there, up from 0.2 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Tunisia in 4Q14

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	10.4%
2	INF/Autorun	Obfuscators & Injectors	6.0%
3	Win32/CplLnk	Exploits	4.1%
4	Win32/Ramnit	Trojans	4.0%
5	Win32/Sality	Viruses	2.3%
6	JS/Faceliker	Trojans	2.0%
7	MSIL/Bladabindi	Backdoors	1.8%
8	VBS/Rtbot	Worms	1.6%
9	Win32/Vobfus	Worms	1.5%
10	Win32/Obfuscator	Obfuscators & Injectors	1.3%

- The most common malware family encountered in Tunisia in 4Q14 was VBS/Jenxcus, which was encountered by 10.4 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 Tunisia in 4Q14 was INF/Autorun, which was encountered by 6.0 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 Tunisia in 4Q14 was Win32/CplLnk, which was encountered by 4.1 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 Tunisia in 4Q14 was Win32/Ramnit, which was encountered by 4.0 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 Tunisia in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	4.3%
2	Win32/Defaulttab	Browser Modifiers	2.4%
3	Win32/BetterSurf	Adware	2.3%
4	Win32/Gofileexpress	Software Bundlers	1.5%
5	Win32/Costmin	Adware	1.2%

- The most common unwanted software family encountered in Tunisia in 4Q14 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 second most common unwanted software family encountered in Tunisia in 4Q14 was Win32/Defaulttab, which was encountered by 2.4 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.
- The third most common unwanted software family encountered in Tunisia in 4Q14 was Win32/BetterSurf, which was encountered by 2.3 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.

Top threat families by infection rate

The most common malware families by infection rate in Tunisia in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	17.7
2	Win32/Sality	Viruses	7.4
3	Win32/Ramnit	Trojans	6.4
4	MSIL/Bladabindi	Backdoors	2.7
5	JS/Kilim	Trojans	2.2
6	Win32/Vobfus	Worms	1.7
7	Win32/Gamarue	Worms	1.1
8	Win32/Pramro	Trojans	1.0
9	Win32/Sefnit	Trojans	0.8
10	Win32/Dorkbot	Worms	0.7

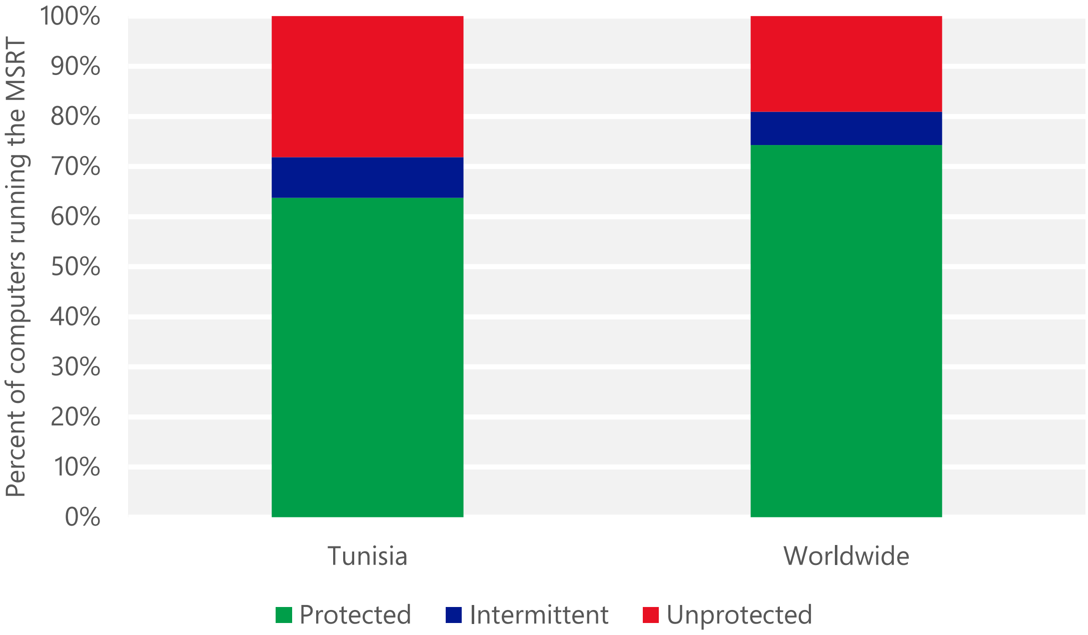
- The most common threat family infecting computers in Tunisia in 4Q14 was VBS/Jenxcus, which was detected and removed from 17.7 of every 1,000 unique computers scanned by the MSRT. VBS/Jenxcus is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Tunisia in 4Q14 was Win32/Sality, which was detected and removed from 7.4 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 Tunisia in 4Q14 was Win32/Ramnit, which was detected and removed from 6.4 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 Tunisia in 4Q14 was MSIL/Bladabindi, which was detected and removed from 2.7 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 Tunisia and worldwide protected by real-time security software in 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 7.56 drive-by download URLs for every 1,000 URLs hosted in Tunisia, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 6.14 drive-by download URLs for every 1,000 URLs hosted in Tunisia, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Tunisia and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Tunisia	7.56	6.14
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Turkey

The statistics presented here are generated by Microsoft security programs and services running on computers in Turkey in 4Q14 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 succeds 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

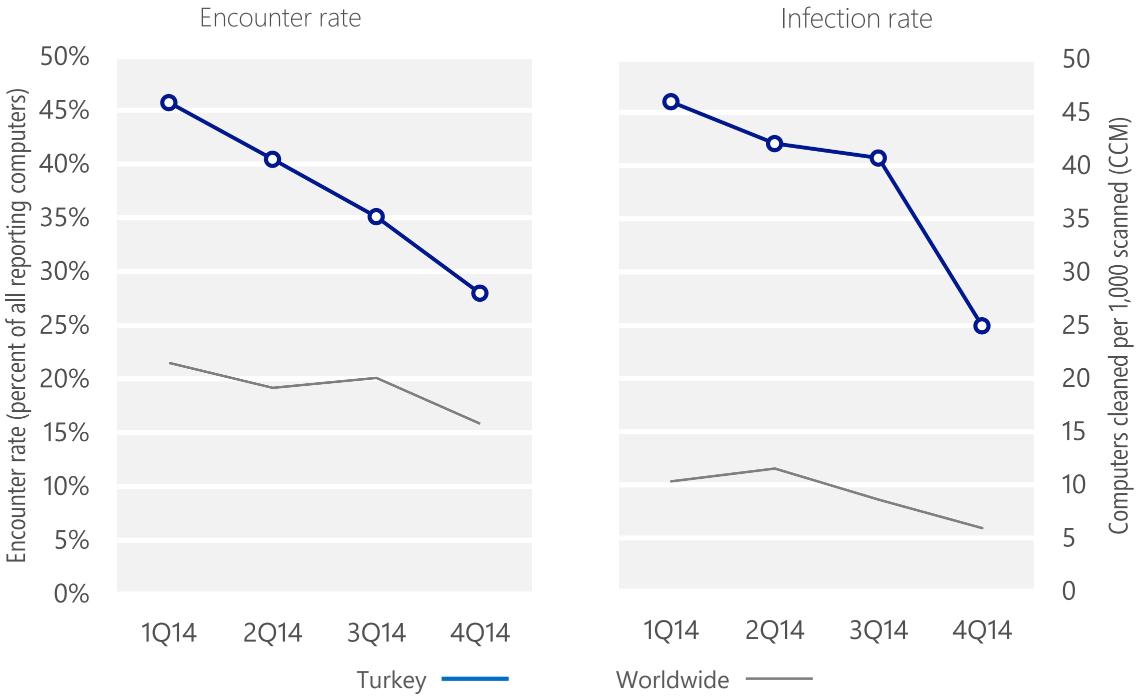
Metric	**1Q14**	**2Q14**	**3Q14**	**4Q14**
Encounter rate, Turkey	45.7%	40.4%	35.1%	28.0%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Turkey	46.0	42.1	40.7	24.9
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 28.0% percent of computers in Turkey encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 24.9 of every 1,000 unique computers scanned in Turkey in 4Q14 (a CCM score of 24.9, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Turkey over the last four quarters, compared to the world as a whole.

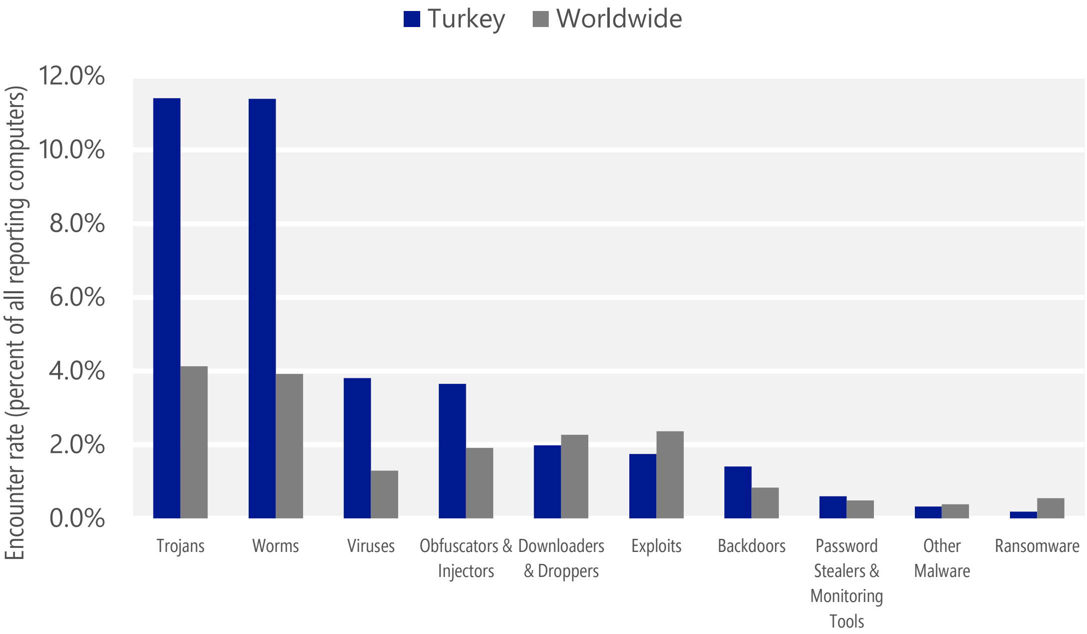
Malware encounter and infection rate trends in Turkey and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

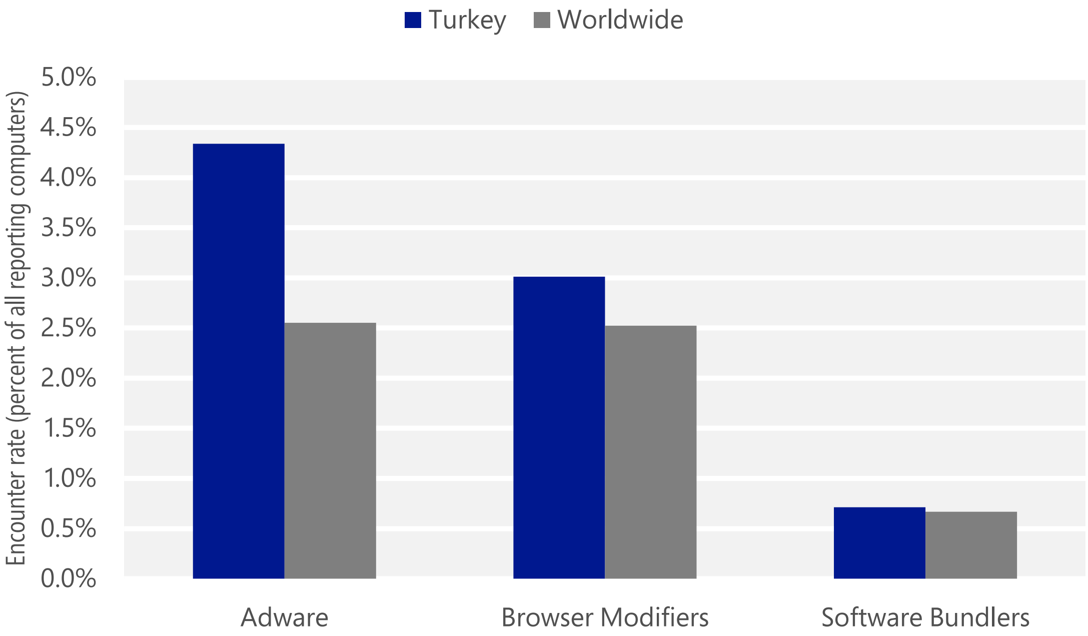
Malware encountered in Turkey in 4Q14, by category



- The most common malware category in Turkey in 4Q14 was Trojans. It was encountered by 11.4 percent of all computers there, down from 18.8 percent in 3Q14.
- The second most common malware category in Turkey in 4Q14 was Worms. It was encountered by 11.4 percent of all computers there, up from 8.2 percent in 3Q14.
- The third most common malware category in Turkey in 4Q14 was Viruses, which was encountered by 3.8 percent of all computers there, down from 4.7 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Turkey in 4Q14, by category



- The most common unwanted software category in Turkey in 4Q14 was Adware. It was encountered by 4.3 percent of all computers there, down from 7.6 percent in 3Q14.
- The second most common unwanted software category in Turkey in 4Q14 was Browser Modifiers. It was encountered by 3.0 percent of all computers there, down from 5.2 percent in 3Q14.
- The third most common unwanted software category in Turkey in 4Q14 was Software Bundlers, which was encountered by 0.7 percent of all computers there, up from 0.0 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Turkey in 4Q14

	Family	Most significant category	% of reporting computers
1	INF/Autorun	Obfuscators & Injectors	5.3%
2	Win32/Gamarue	Worms	3.3%
3	Win32/Sality	Viruses	2.0%
4	Win32/BeeVry	Trojans	1.9%
5	Win32/Obfuscator	Obfuscators & Injectors	1.7%
6	Win32/Ramnit	Trojans	1.6%
7	Win32/Rimod	Trojans	1.4%
8	JS/Kilim	Trojans	1.4%
9	Win32/Nuqel	Worms	1.2%
10	MSIL/Wooniky	Worms	1.2%

- The most common malware family encountered in Turkey in 4Q14 was INF/Autorun, which was encountered by 5.3 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 second most common malware family encountered in Turkey in 4Q14 was Win32/Gamarue, which was encountered by 3.3 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 third most common malware family encountered in Turkey in 4Q14 was Win32/Sality, which was encountered by 2.0 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 Turkey in 4Q14 was Win32/BeeVry, which was encountered by 1.9 percent of reporting computers there. Win32/BeeVry is a trojan that modifies a number of settings to prevent the computer from accessing security-related websites, and lower the computer’s security.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Turkey in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	2.7%
2	Win32/BetterSurf	Adware	1.5%
3	Win32/Pennybee	Adware	1.3%
4	Win32/Costmin	Adware	0.9%
5	Win32/Couponarific	Adware	0.5%

- The most common unwanted software family encountered in Turkey in 4Q14 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 second most common unwanted software family encountered in Turkey in 4Q14 was Win32/BetterSurf, which was encountered by 1.5 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.

- The third most common unwanted software family encountered in Turkey in 4Q14 was Win32/Pennybee, which was encountered by 1.3 percent of reporting computers there. Win32/Pennybee is adware that shows ads as the user browses the web. It can be installed from the program's website or bundled with some third-party software installation programs.

Top threat families by infection rate

The most common malware families by infection rate in Turkey in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Sality	Viruses	4.8
2	JS/Kilim	Trojans	3.8
3	Win32/Gamarue	Worms	3.5
4	Win32/Ramnit	Trojans	3.2
5	Win32/Wysotot	Trojans	2.2
6	Win32/Brontok	Worms	1.7
7	VBS/Jenxcus	Worms	1.5
8	Win32/Helompy	Worms	1.4
9	Win32/Nuqel	Worms	1.2
10	Win32/Pramro	Trojans	1.0

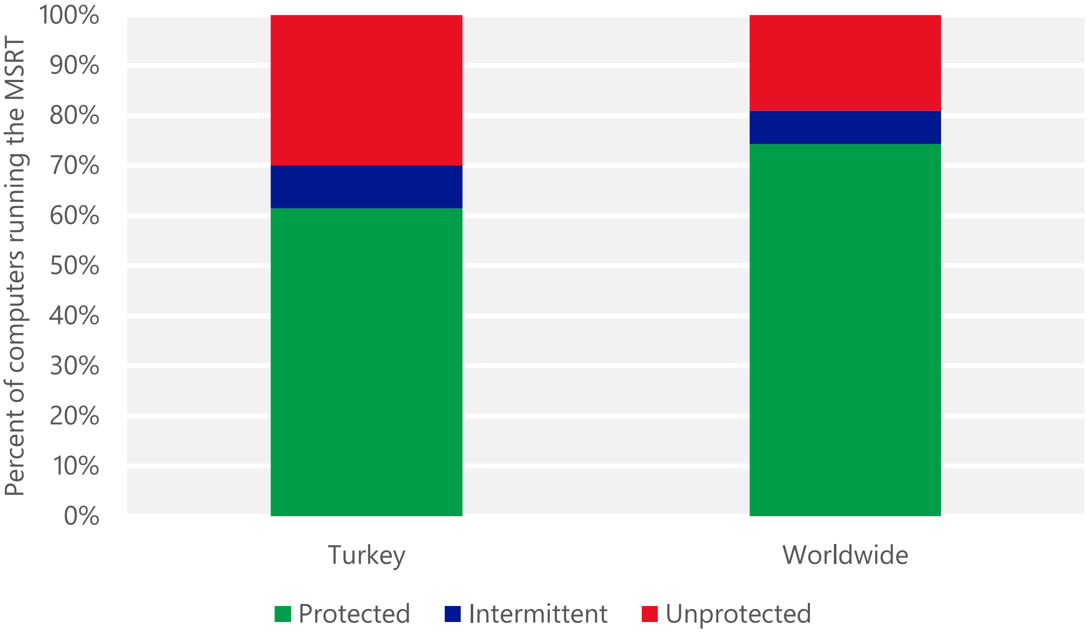
- The most common threat family infecting computers in Turkey in 4Q14 was Win32/Sality, which was detected and removed from 4.8 of every 1,000 unique computers scanned by the MSRT. Win32/Sality is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The second most common threat family infecting computers in Turkey in 4Q14 was JS/Kilim, which was detected and removed from 3.8 of every 1,000 unique computers scanned by the MSRT. JS/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 Turkey in 4Q14 was Win32/Gamarue, which was detected and removed from 3.5 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 Turkey in 4Q14 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 Turkey and worldwide protected by real-time security software in 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.59 drive-by download URLs for every 1,000 URLs hosted in Turkey, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.31 drive-by download URLs for every 1,000 URLs hosted in Turkey, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Turkey and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Turkey	0.59	0.31
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Ukraine

The statistics presented here are generated by Microsoft security programs and services running on computers in Ukraine in 4Q14 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 succeds 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

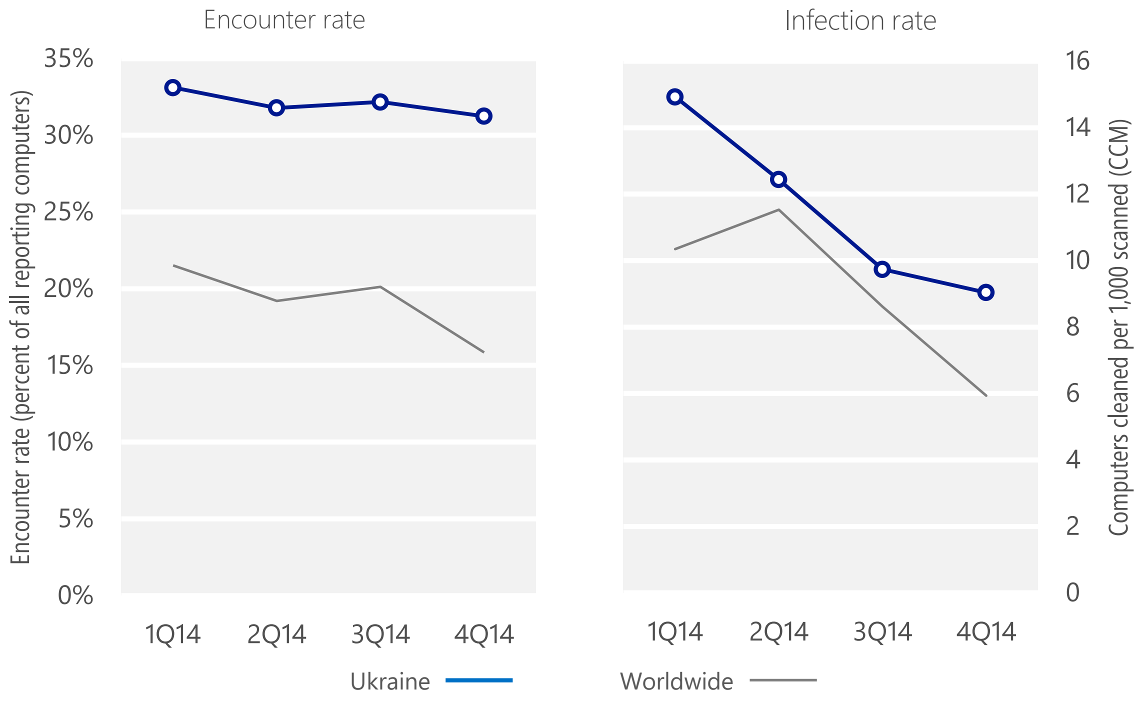
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Ukraine	33.1%	31.8%	32.2%	31.2%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Ukraine	14.9	12.4	9.7	9.0
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 31.2% percent of computers in Ukraine encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 9.0 of every 1,000 unique computers scanned in Ukraine in 4Q14 (a CCM score of 9.0, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Ukraine over the last four quarters, compared to the world as a whole.

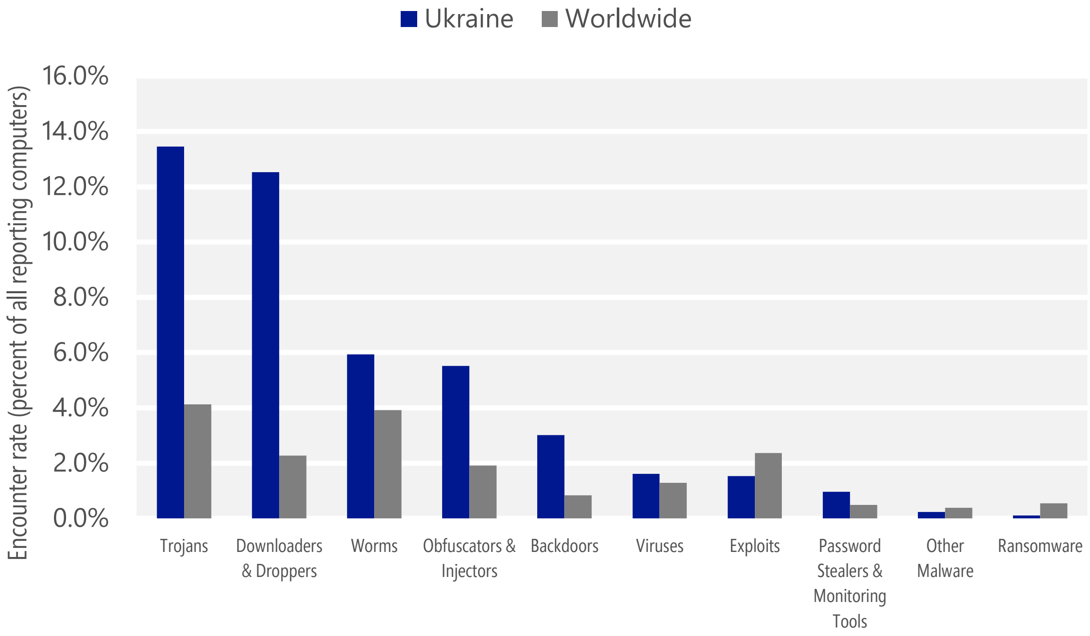
Malware encounter and infection rate trends in Ukraine and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

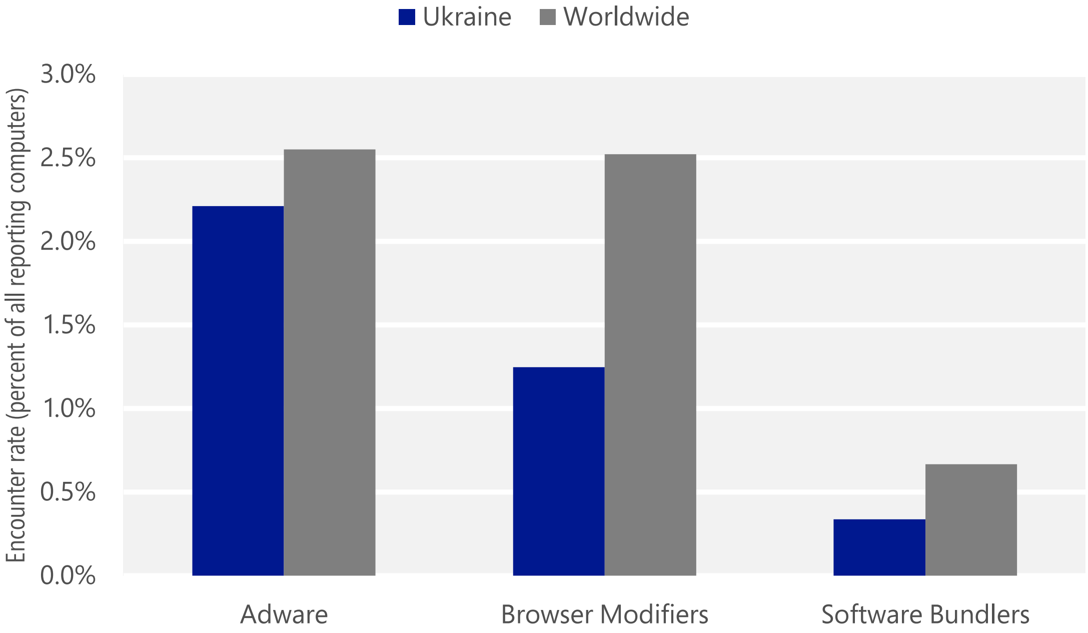
Malware encountered in Ukraine in 4Q14, by category



- The most common malware category in Ukraine in 4Q14 was Trojans. It was encountered by 13.5 percent of all computers there, down from 15.0 percent in 3Q14.
- The second most common malware category in Ukraine in 4Q14 was Downloaders & Droppers. It was encountered by 12.5 percent of all computers there, up from 12.3 percent in 3Q14.
- The third most common malware category in Ukraine in 4Q14 was Worms, which was encountered by 5.9 percent of all computers there, up from 5.3 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Ukraine in 4Q14, by category



- The most common unwanted software category in Ukraine in 4Q14 was Adware. It was encountered by 2.2 percent of all computers there, down from 4.3 percent in 3Q14.
- The second most common unwanted software category in Ukraine in 4Q14 was Browser Modifiers. It was encountered by 1.2 percent of all computers there, up from 0.2 percent in 3Q14.
- The third most common unwanted software category in Ukraine in 4Q14 was Software Bundlers, which was encountered by 0.3 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Ukraine in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Ogimant	Downloaders & Droppers	11.4%
2	Win32/Peaac	Trojans	4.4%
3	Win32/Obfuscator	Obfuscators & Injectors	4.3%
4	Win32/Gamarue	Worms	3.0%
5	Win32/Peals	Trojans	1.5%
6	Win32/Dynamer	Trojans	1.1%
7	Win32/Morix	Backdoors	1.0%
8	INF/Autorun	Obfuscators & Injectors	0.9%
9	Win32/Ramnit	Trojans	0.8%
10	Win32/Anaki	Trojans	0.8%

- The most common malware family encountered in Ukraine in 4Q14 was Win32/Ogimant, which was encountered by 11.4 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 second most common malware family encountered in Ukraine in 4Q14 was Win32/Peaac, which was encountered by 4.4 percent of reporting computers there. Win32/Peaac is a generic detection for various threats that display trojan characteristics.
- The third most common malware family encountered in Ukraine in 4Q14 was Win32/Obfuscator, which was encountered by 4.3 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 Ukraine in 4Q14 was Win32/Gamarue, which was encountered by 3.0 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.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Ukraine in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/BetterSurf	Adware	1.8%
2	Win32/Couponruc	Browser Modifiers	0.8%
3	Win32/Defaulttab	Browser Modifiers	0.4%
4	Win32/Costmin	Adware	0.3%
5	Win32/Gofileexpress	Software Bundlers	0.3%

- The most common unwanted software family encountered in Ukraine in 4Q14 was Win32/BetterSurf, which was encountered by 1.8 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.
- The second most common unwanted software family encountered in Ukraine in 4Q14 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 Ukraine in 4Q14 was Win32/Defaulttab, which was encountered by 0.4 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.

Top threat families by infection rate

The most common malware families by infection rate in Ukraine in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Gamarue	Worms	2.3
2	Win32/Tofsee	Backdoors	1.2
3	Win32/Ramnit	Trojans	1.0
4	Win32/Sality	Viruses	0.8
5	Win32/Deminnix	Trojans	0.6
6	Win32/Helompy	Worms	0.5
7	Win32/Dorkbot	Worms	0.5
8	VBS/Jenxcus	Worms	0.3
9	Win32/Brontok	Worms	0.2
10	Win32/Sefnit	Trojans	0.2

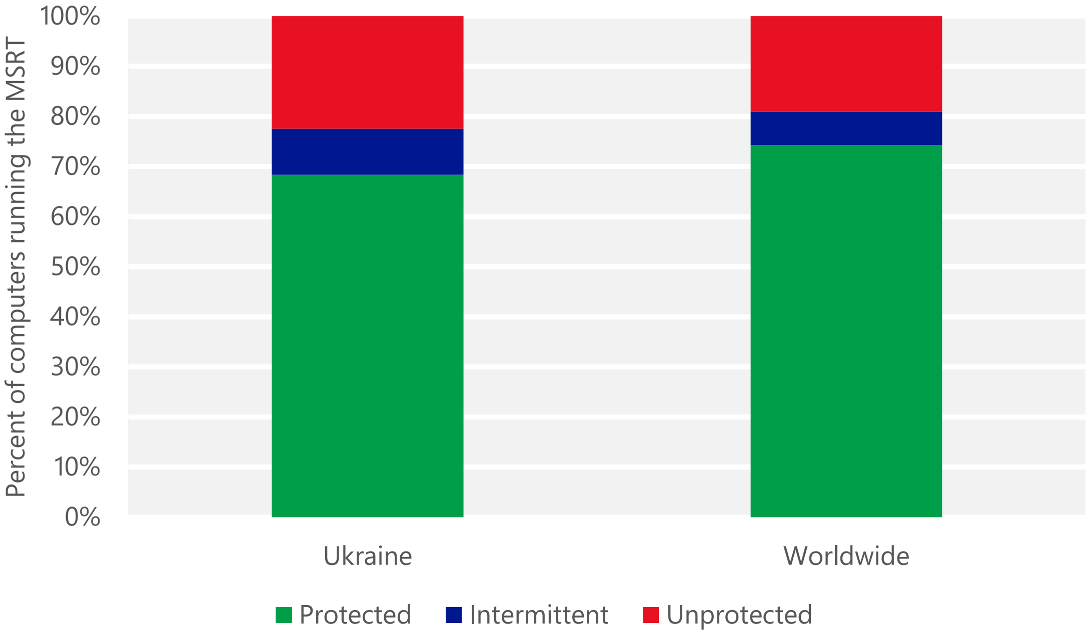
- The most common threat family infecting computers in Ukraine in 4Q14 was Win32/Gamarue, which was detected and removed from 2.3 of every 1,000 unique computers scanned by the MSRT. Win32/Gamarue is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The second most common threat family infecting computers in Ukraine in 4Q14 was Win32/Tofsee, which was detected and removed from 1.2 of every 1,000 unique computers scanned by the MSRT. Win32/Tofsee is a multi-component family of backdoor trojans that act as a spam and traffic relay.
- The third most common threat family infecting computers in Ukraine in 4Q14 was Win32/Ramnit, which was detected and removed from 1.0 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.
- The fourth most common threat family infecting computers in Ukraine in 4Q14 was Win32/Sality, which was detected and removed from 0.8 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.

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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 1.10 drive-by download URLs for every 1,000 URLs hosted in Ukraine, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.40 drive-by download URLs for every 1,000 URLs hosted in Ukraine, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Ukraine and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Ukraine	1.10	0.40
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

United Arab Emirates

The statistics presented here are generated by Microsoft security programs and services running on computers in the United Arab Emirates in 4Q14 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 succeds 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

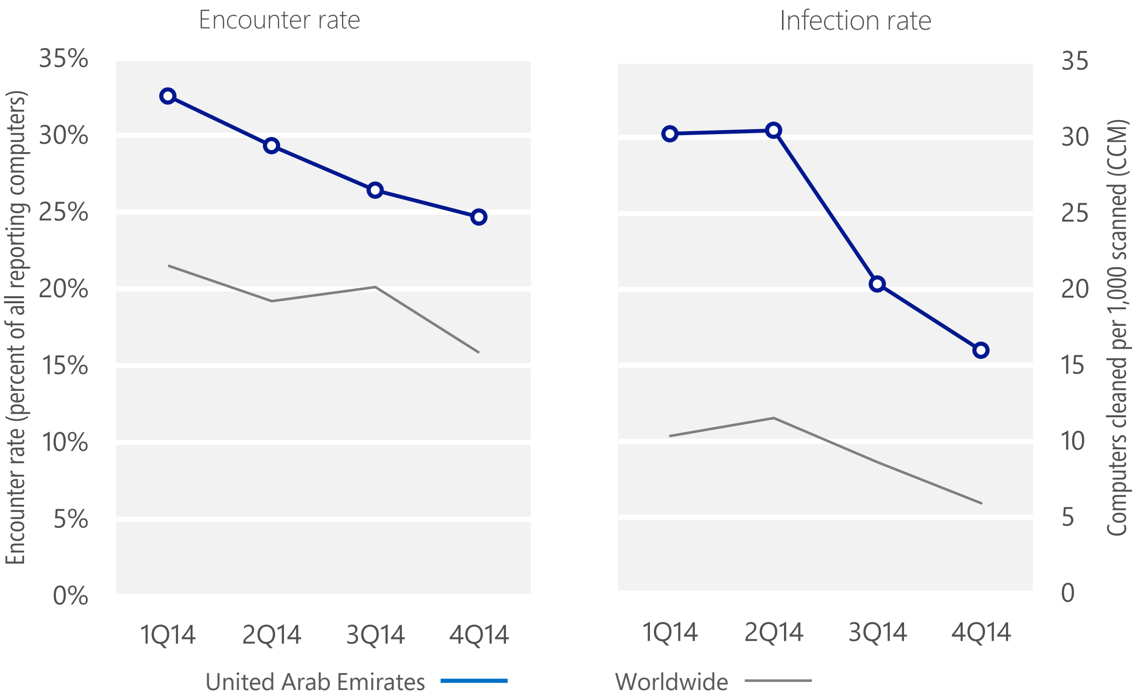
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, United Arab Emirates	32.6%	29.3%	26.4%	24.7%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, United Arab Emirates	30.2	30.5	20.4	16.0
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 24.7% percent of computers in the United Arab Emirates encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 16.0 of every 1,000 unique computers scanned in the United Arab Emirates in 4Q14 (a CCM score of 16.0, compared to the 4Q14 worldwide CCM of 5.9). 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.

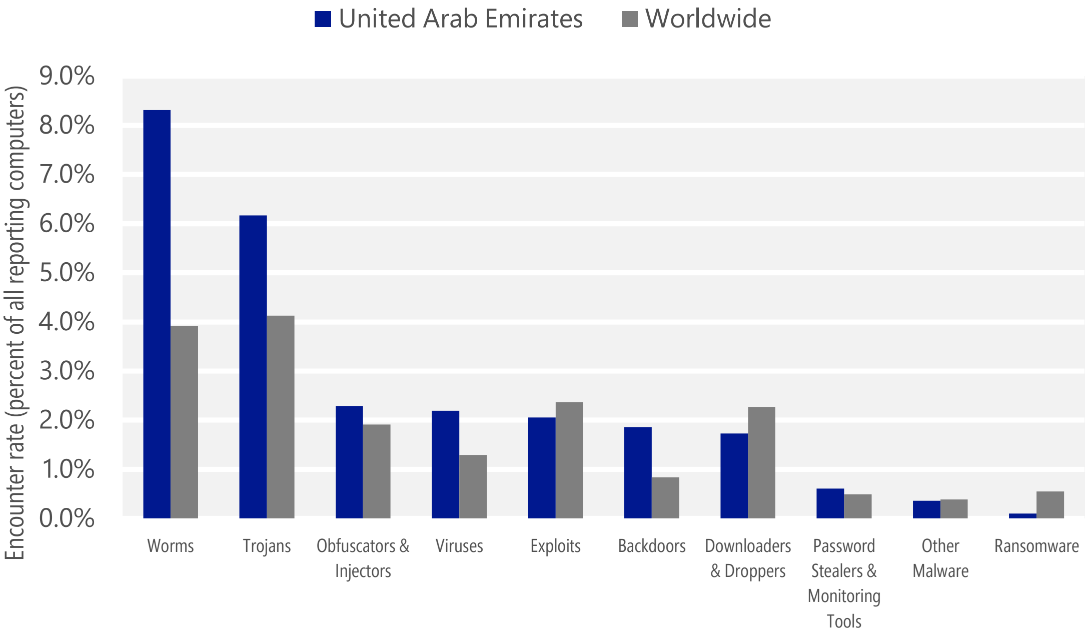
Malware encounter and infection rate trends in the United Arab Emirates and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

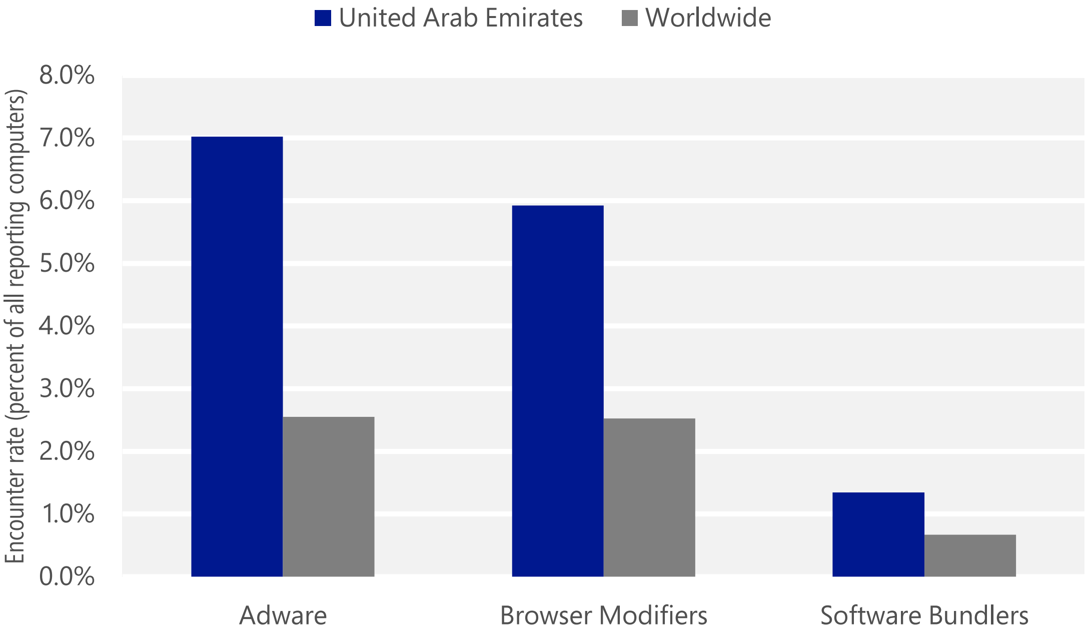
Malware encountered in the United Arab Emirates in 4Q14, by category



- The most common malware category in the United Arab Emirates in 4Q14 was Worms. It was encountered by 8.3 percent of all computers there, down from 8.6 percent in 3Q14.
- The second most common malware category in the United Arab Emirates in 4Q14 was Trojans. It was encountered by 6.2 percent of all computers there, down from 8.3 percent in 3Q14.
- The third most common malware category in the United Arab Emirates in 4Q14 was Obfuscators & Injectors, which was encountered by 2.3 percent of all computers there, down from 3.7 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in the United Arab Emirates in 4Q14, by category



- The most common unwanted software category in the United Arab Emirates in 4Q14 was Adware. It was encountered by 7.0 percent of all computers there, down from 8.7 percent in 3Q14.
- The second most common unwanted software category in the United Arab Emirates in 4Q14 was Browser Modifiers. It was encountered by 5.9 percent of all computers there, up from 1.2 percent in 3Q14.
- The third most common unwanted software category in the United Arab Emirates in 4Q14 was Software Bundlers, which was encountered by 1.3 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in the United Arab Emirates in 4Q14

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	2.9%
2	INF/Autorun	Obfuscators & Injectors	2.0%
3	Win32/Gamarue	Worms	1.6%
4	Win32/Startpage	Trojans	1.1%
5	Win32/Sality	Viruses	0.9%
6	Win32/Obfuscator	Obfuscators & Injectors	0.9%
7	JS/Axpergle	Exploits	0.8%
8	Win32/Nuqel	Worms	0.8%
9	Win32/Ramnit	Trojans	0.8%
10	Win32/CplLnk	Exploits	0.7%

- The most common malware family encountered in the United Arab Emirates in 4Q14 was VBS/Jenxcus, which was encountered by 2.9 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 the United Arab Emirates in 4Q14 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.
- The third most common malware family encountered in the United Arab Emirates in 4Q14 was Win32/Gamarue, which was encountered by 1.6 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 fourth most common malware family encountered in the United Arab Emirates in 4Q14 was Win32/Startpage, which was encountered by 1.1 percent of reporting computers there. Win32/Startpage is a detection for various threats that change the configured start page of the affected user?s web browser and may also perform other malicious actions.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in the United Arab Emirates in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	4.4%
2	Win32/Brya	Adware	4.3%
3	Win32/BetterSurf	Adware	1.3%
4	Win32/Costmin	Adware	1.3%
5	Win32/Defaulttab	Browser Modifiers	1.2%

- The most common unwanted software family encountered in the United Arab Emirates in 4Q14 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 the United Arab Emirates in 4Q14 was Win32/Brya, which was encountered by 4.3 percent of reporting computers there. Win32/Brya is a program that shows ads that the user cannot control as they browse the web. It does not have a working uninstaller.
- The third most common unwanted software family encountered in the United Arab Emirates in 4Q14 was Win32/BetterSurf, which was encountered by 1.3 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.

Top threat families by infection rate

The most common malware families by infection rate in the United Arab Emirates in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	4.6
2	Win32/Sality	Viruses	2.2
3	Win32/Gamarue	Worms	2.1
4	Win32/Ramnit	Trojans	1.2
5	Win32/Nuqel	Worms	1.0
6	MSIL/Bladabindi	Backdoors	0.8
7	Win32/Wysotot	Trojans	0.6
8	Win32/Sefnit	Trojans	0.4
9	Win32/Vobfus	Worms	0.4
10	JS/Kilim	Trojans	0.4

- The most common threat family infecting computers in the United Arab Emirates in 4Q14 was VBS/Jenxcus, which was detected and removed from 4.6 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 the United Arab Emirates in 4Q14 was Win32/Sality, which was detected and removed from 2.2 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.
- The third most common threat family infecting computers in the United Arab Emirates in 4Q14 was Win32/Gamarue, which was detected and removed from 2.1 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 fourth most common threat family infecting computers in the United Arab Emirates in 4Q14 was Win32/Ramnit, which was detected and removed from 1.2 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

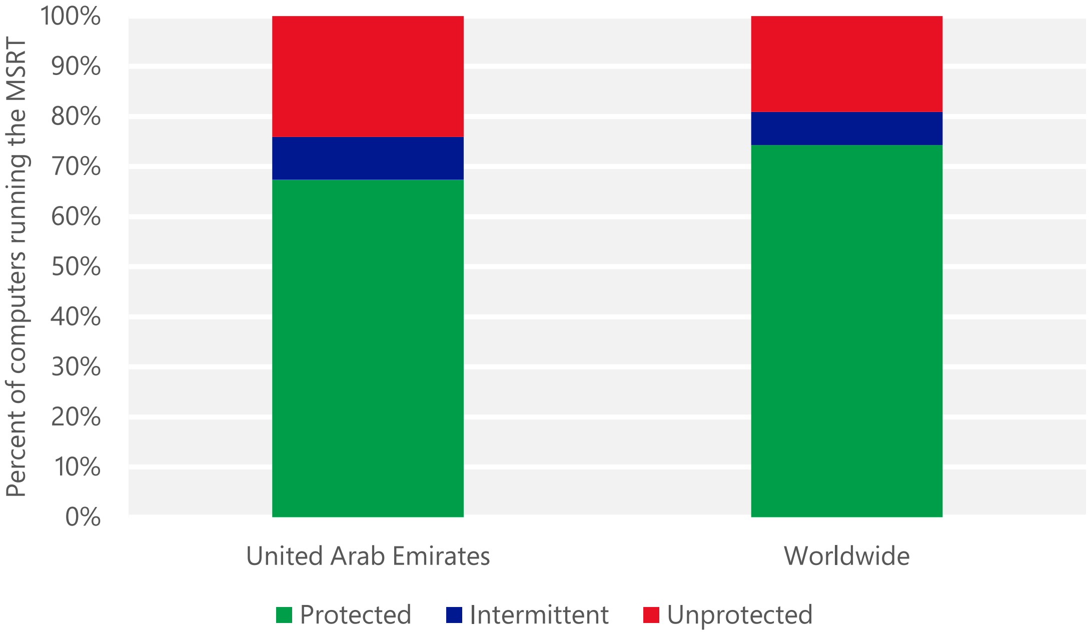
steals sensitive information such as saved FTP credentials and browser cookies. It may also open a backdoor to await instructions from a remote attacker.

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 the United Arab Emirates and worldwide protected by real-time security software in 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.03 drive-by download URLs for every 1,000 URLs hosted in the United Arab Emirates, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.01 drive-by download URLs for every 1,000 URLs hosted in the United Arab Emirates, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in the United Arab Emirates and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, United Arab Emirates	0.03	0.01
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

United Kingdom

The statistics presented here are generated by Microsoft security programs and services running on computers in the United Kingdom in 4Q14 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 succeds 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

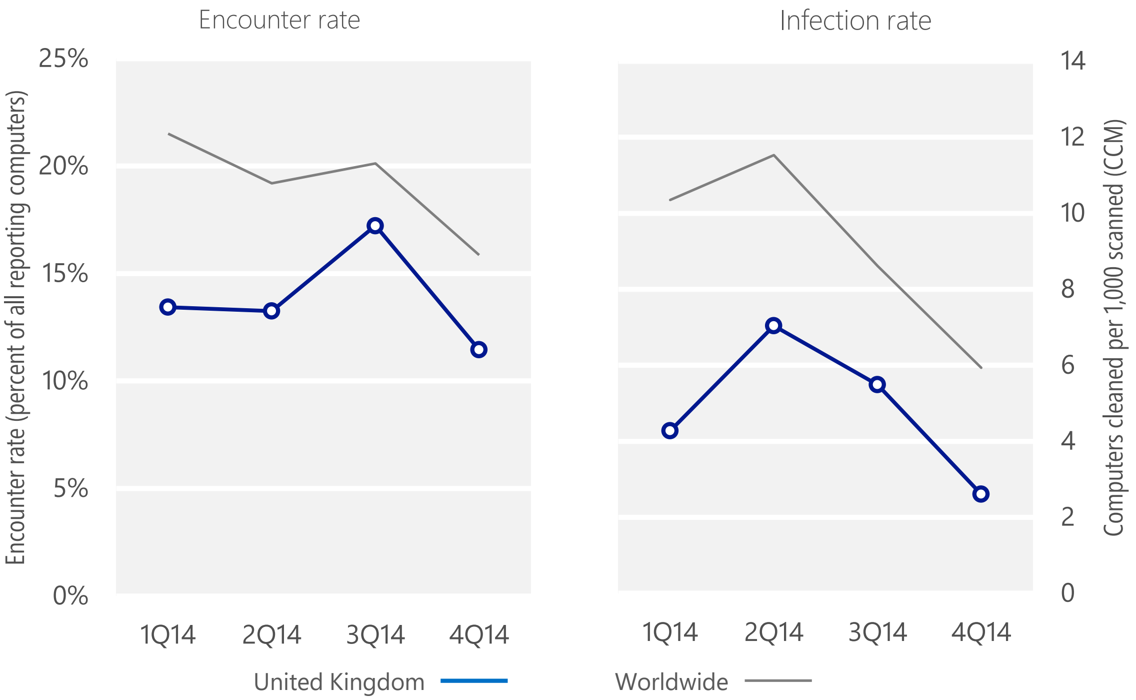
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, United Kingdom	13.4%	13.3%	17.2%	11.5%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, United Kingdom	4.3	7.0	5.5	2.6
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 11.5% percent of computers in the United Kingdom encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 2.6 of every 1,000 unique computers scanned in the United Kingdom in 4Q14 (a CCM score of 2.6, compared to the 4Q14 worldwide CCM of 5.9). 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.

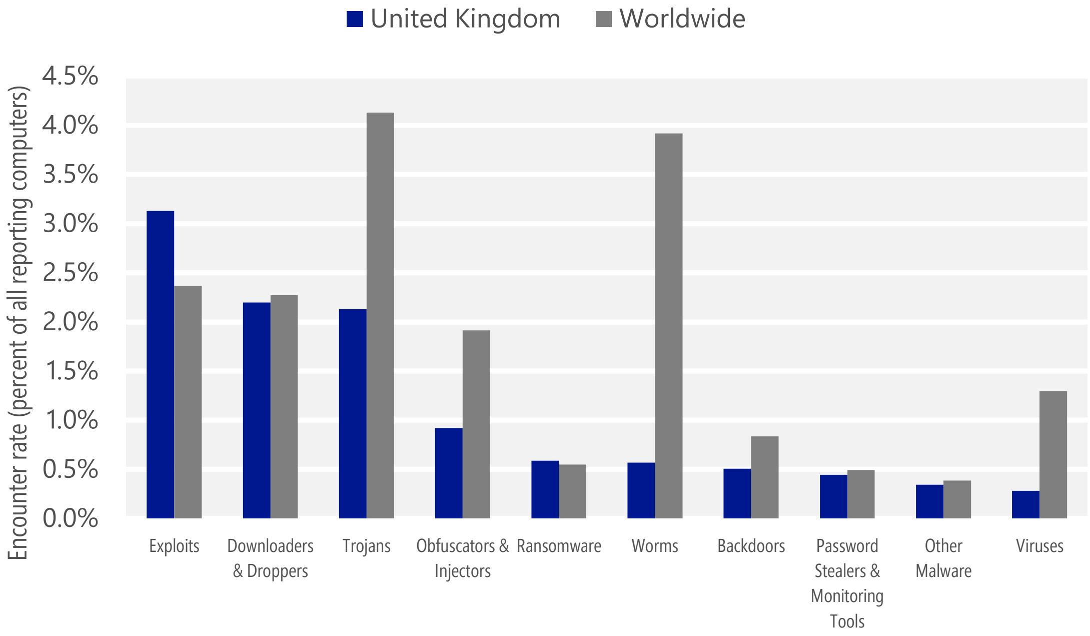
Malware encounter and infection rate trends in the United Kingdom and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

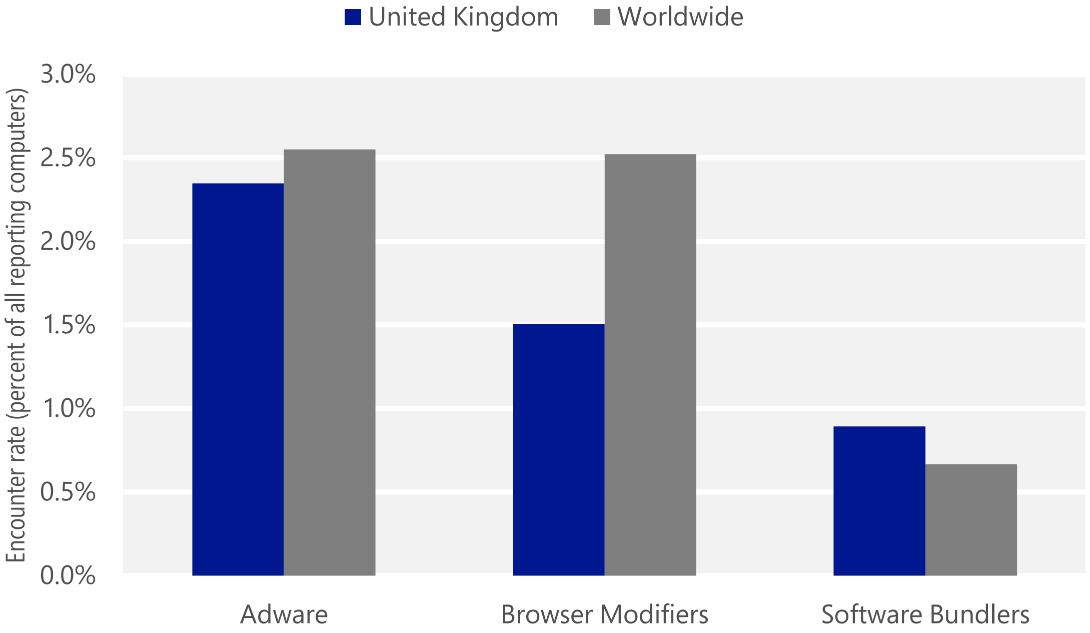
Malware encountered in the United Kingdom in 4Q14, by category



- The most common malware category in the United Kingdom in 4Q14 was Exploits. It was encountered by 3.1 percent of all computers there, down from 6.7 percent in 3Q14.
- The second most common malware category in the United Kingdom in 4Q14 was Downloaders & Droppers. It was encountered by 2.2 percent of all computers there, down from 3.5 percent in 3Q14.
- The third most common malware category in the United Kingdom in 4Q14 was Trojans, which was encountered by 2.1 percent of all computers there, down from 3.0 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in the United Kingdom in 4Q14, by category



- The most common unwanted software category in the United Kingdom in 4Q14 was Adware. It was encountered by 2.3 percent of all computers there, down from 5.1 percent in 3Q14.
- The second most common unwanted software category in the United Kingdom in 4Q14 was Browser Modifiers. It was encountered by 1.5 percent of all computers there, down from 4.0 percent in 3Q14.
- The third most common unwanted software category in the United Kingdom in 4Q14 was Software Bundlers, which was encountered by 0.9 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in the United Kingdom in 4Q14

	Family	Most significant category	% of reporting computers
1	JS/Axpergle	Exploits	1.7%
2	Win32/Tugspay	Downloaders & Droppers	0.9%
3	JS/Fiexp	Exploits	0.8%
4	Win32/Obfuscator	Obfuscators & Injectors	0.8%
5	Win32/Clikug	Trojans	0.6%
6	Win32/Anogre	Exploits	0.6%
7	JS/Krypterade	Ransomware	0.3%
8	Win32/Upatre	Downloaders & Droppers	0.2%
9	Win32/Zbot	Password Stealers & Monitoring Tools	0.2%
10	W97M/Adnel	Downloaders & Droppers	0.2%

- The most common malware family encountered in the United Kingdom in 4Q14 was JS/Axpergle, which was encountered by 1.7 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 the United Kingdom in 4Q14 was Win32/Tugspay, which was encountered by 0.9 percent of reporting computers there. Win32/Tugspay is a downloader that spreads by posing as an installer for legitimate software, such as a Java update, or through other malware. When installed, it downloads unwanted software to the computer.
- The third most common malware family encountered in the United Kingdom in 4Q14 was JS/Fiexp, which was encountered by 0.8 percent of reporting computers there. JS/Fiexp is a detection for the Fiesta exploit kit, which attempts to exploit Java, Adobe Flash Player, Adobe Reader, Silverlight, and Internet Explorer to install malware.
- The fourth most common malware family encountered in the United Kingdom in 4Q14 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 the United Kingdom in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	1.2%
2	Win32/Costmin	Adware	0.7%
3	Win32/Couponarific	Adware	0.4%
4	Win32/BetterSurf	Adware	0.4%
5	Win32/Gofileexpress	Software Bundlers	0.3%

- The most common unwanted software family encountered in the United Kingdom in 4Q14 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 the United Kingdom in 4Q14 was Win32/Costmin, which was encountered by 0.7 percent of reporting computers there. Win32/Costmin is an adware family that installs itself as a browser extension for Internet Explorer, Mozilla Firefox, and Google Chrome, and displays advertisements as the user browses the Internet.
- The third most common unwanted software family encountered in the United Kingdom in 4Q14 was Win32/Couponarific, which was encountered by 0.4 percent of reporting computers there. Win32/Couponarific is a program that shows ads that the user cannot control as they browse the web. It does not have a working uninstaller.

Top threat families by infection rate

The most common malware families by infection rate in the United Kingdom in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Sefnit	Trojans	0.3
2	Win32/Zbot	Password Stealers & Monitoring Tools	0.2
3	Win32/Wysotot	Trojans	0.2
4	JS/Medfos	Trojans	0.2
5	Win32/Ramnit	Trojans	0.2
6	Win32/Caphaw	Backdoors	0.2
7	JS/Miuref	Trojans	0.2
8	Win32/Alureon	Trojans	0.2
9	Win32/Sirefef	Trojans	0.1
10	VBS/Jenxcus	Worms	0.1

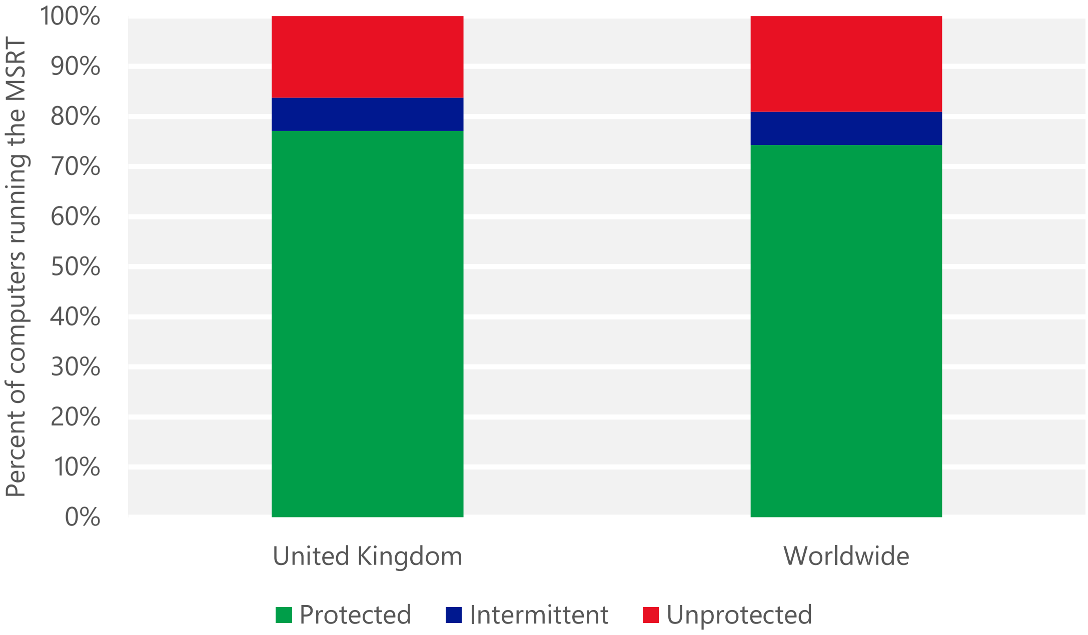
- The most common threat family infecting computers in the United Kingdom in 4Q14 was Win32/Sefnit, which was detected and removed from 0.3 of every 1,000 unique computers scanned by the MSRT. Win32/Sefnit is a family of trojans that can allow backdoor access, download files, and use the computer and Internet connection for click fraud. Some variants can monitor web browsers and hijack search results.
- The second most common threat family infecting computers in the United Kingdom in 4Q14 was Win32/Zbot, which was detected and removed from 0.2 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 third most common threat family infecting computers in the United Kingdom in 4Q14 was Win32/Wysotot, which was detected and removed from 0.2 of every 1,000 unique computers scanned by the MSRT. Win32/Wysotot is a threat that can change the start page of the user's web browser, and may download and install other files to the computer. It is installed by software bundlers that advertise free software or games.
- The fourth most common threat family infecting computers in the United Kingdom in 4Q14 was JS/Medfos, which was detected and removed from 0.2 of every 1,000 unique computers scanned by the MSRT. JS/Medfos is ?A trojan that installs malicious Internet browser extensions and redirects search results from popular search engines.

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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.21 drive-by download URLs for every 1,000 URLs hosted in the United Kingdom, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.79 drive-by download URLs for every 1,000 URLs hosted in the United Kingdom, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in the United Kingdom and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, United Kingdom	0.21	0.79
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

United States

The statistics presented here are generated by Microsoft security programs and services running on computers in the United States in 4Q14 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 succeds 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

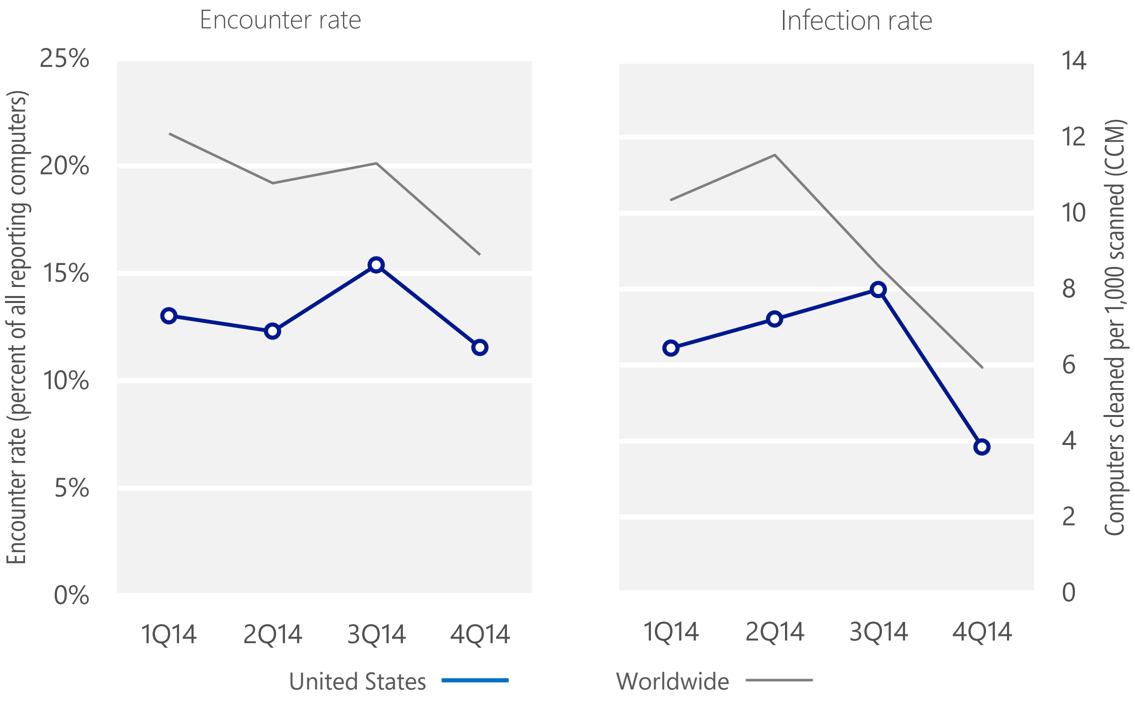
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, United States	13.0%	12.3%	15.4%	11.5%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, United States	6.4	7.2	8.0	3.8
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 11.5% percent of computers in the United States encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 3.8 of every 1,000 unique computers scanned in the United States in 4Q14 (a CCM score of 3.8, compared to the 4Q14 worldwide CCM of 5.9). 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.

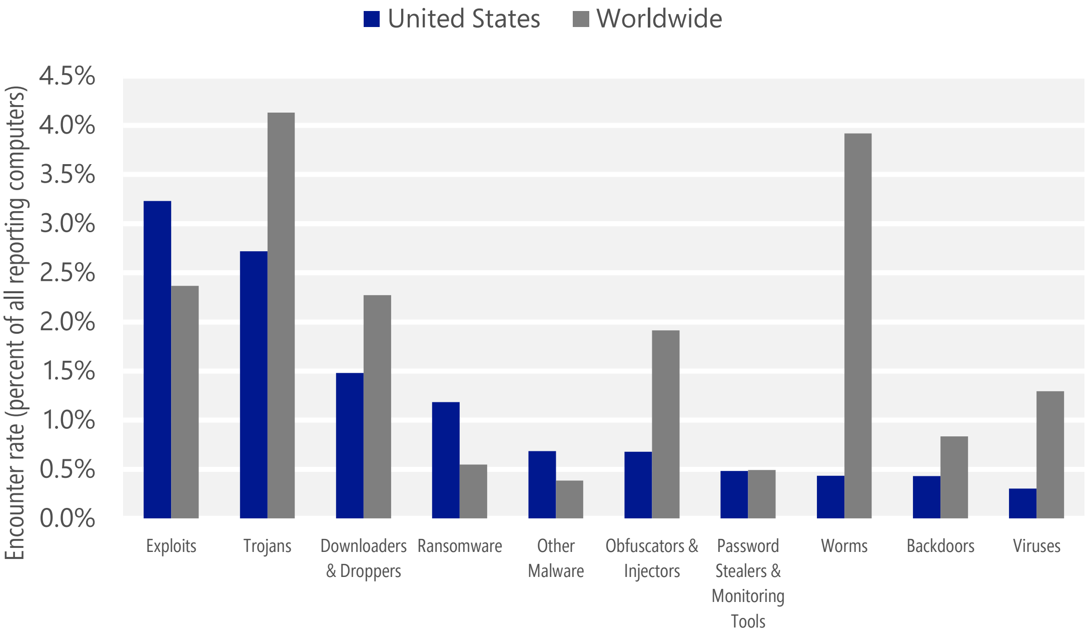
Malware encounter and infection rate trends in the United States and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

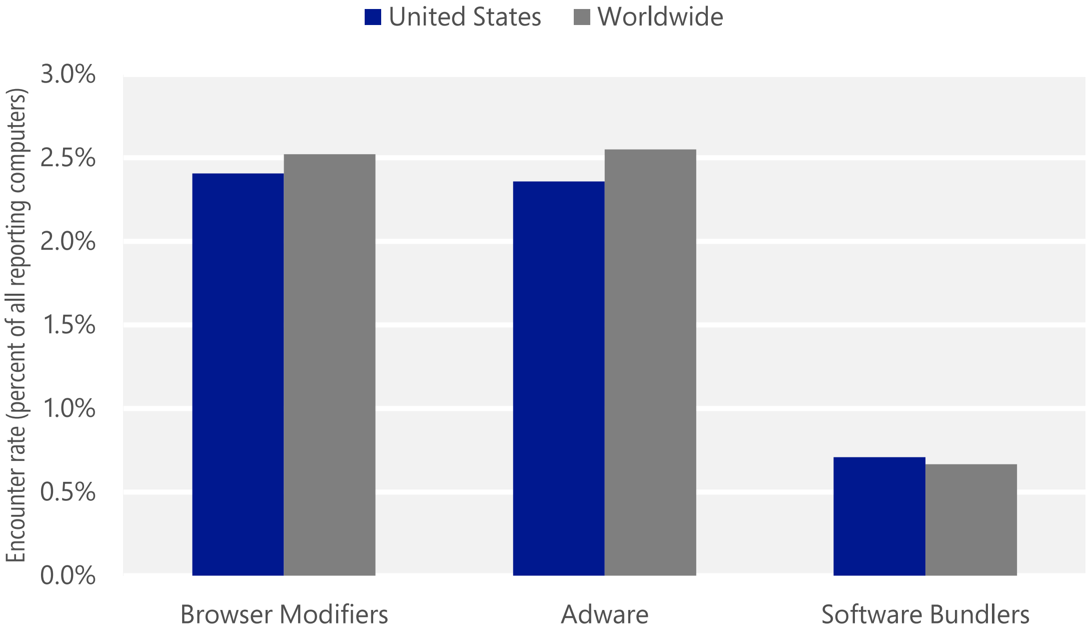
Malware encountered in the United States in 4Q14, by category



- The most common malware category in the United States in 4Q14 was Exploits. It was encountered by 3.2 percent of all computers there, down from 4.0 percent in 3Q14.
- The second most common malware category in the United States in 4Q14 was Trojans. It was encountered by 2.7 percent of all computers there, down from 3.7 percent in 3Q14.
- The third most common malware category in the United States in 4Q14 was Downloaders & Droppers, which was encountered by 1.5 percent of all computers there, down from 3.1 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in the United States in 4Q14, by category



- The most common unwanted software category in the United States in 4Q14 was Browser Modifiers. It was encountered by 2.4 percent of all computers there, down from 5.3 percent in 3Q14.
- The second most common unwanted software category in the United States in 4Q14 was Adware. It was encountered by 2.4 percent of all computers there, down from 2.9 percent in 3Q14.
- The third most common unwanted software category in the United States in 4Q14 was Software Bundlers, which was encountered by 0.7 percent of all computers there, up from 0.4 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in the United States in 4Q14

	Family	Most significant category	% of reporting computers
1	JS/Axpergle	Exploits	1.3%
2	Win32/Anogre	Exploits	1.0%
3	JS/Krypterade	Ransomware	0.8%
4	JS/Fiexp	Exploits	0.6%
5	Win32/Clikug	Trojans	0.6%
6	Win32/Obfuscator	Obfuscators & Injectors	0.5%
7	Win32/Chroject	Trojans	0.4%
8	Win32/Tugspay	Downloaders & Droppers	0.3%
9	Win32/Zbot	Password Stealers & Monitoring Tools	0.3%
10	Win32/Crowti	Ransomware	0.3%

- The most common malware family encountered in the United States in 4Q14 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 second most common malware family encountered in the United States in 4Q14 was Win32/Anogre, which was encountered by 1.0 percent of reporting computers there. Win32/Anogre is a threat that exploits a vulnerability addressed by Microsoft Security Bulletin MS11-087. This vulnerability can allow a hacker to install programs, view, change, or delete data or create new accounts with full administrative privileges.
- The third most common malware family encountered in the United States in 4Q14 was JS/Krypterade, which was encountered by 0.8 percent of reporting computers there. JS/Krypterade is ransomware that fraudulently claims the computer has been used for unlawful activity, locks it, and demands that the user pay to unlock it.
- The fourth most common malware family encountered in the United States in 4Q14 was JS/Fiexp, which was encountered by 0.6 percent of reporting computers there. JS/Fiexp is a detection for the Fiesta exploit kit, which attempts to exploit Java, Adobe Flash Player, Adobe Reader, Silverlight, and Internet Explorer to install malware.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in the United States in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Defaulttab	Browser Modifiers	1.2%
2	Win32/Couponruc	Browser Modifiers	1.1%
3	Win32/Invisiblebrowser	Adware	0.5%
4	Win32/Costmin	Adware	0.5%
5	Win32/Pennybee	Adware	0.4%

- The most common unwanted software family encountered in the United States in 4Q14 was Win32/Defaulttab, which was encountered by 1.2 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.
- The second most common unwanted software family encountered in the United States in 4Q14 was Win32/Couponruc, which was encountered by 1.1 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 States in 4Q14 was Win32/Invisiblebrowser, which was encountered by 0.5 percent of reporting computers there. Win32/Invisiblebrowser is a program that shows ads as the user browses the web. It can be bundled with some third-party software installation programs.

Top threat families by infection rate

The most common malware families by infection rate in the United States in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Alureon	Trojans	1.2
2	Win32/Tracur	Trojans	0.5
3	Win32/Zbot	Password Stealers & Monitoring Tools	0.4
4	JS/Medfos	Trojans	0.3
5	JS/Miuref	Trojans	0.2
6	Win32/Sirefef	Trojans	0.2
7	Win32/Wysotot	Trojans	0.2
8	Win32/Kuluoz	Downloaders & Droppers	0.1
9	Win32/Sefnit	Trojans	0.1
10	Win32/FakeRean	Other Malware	0.1

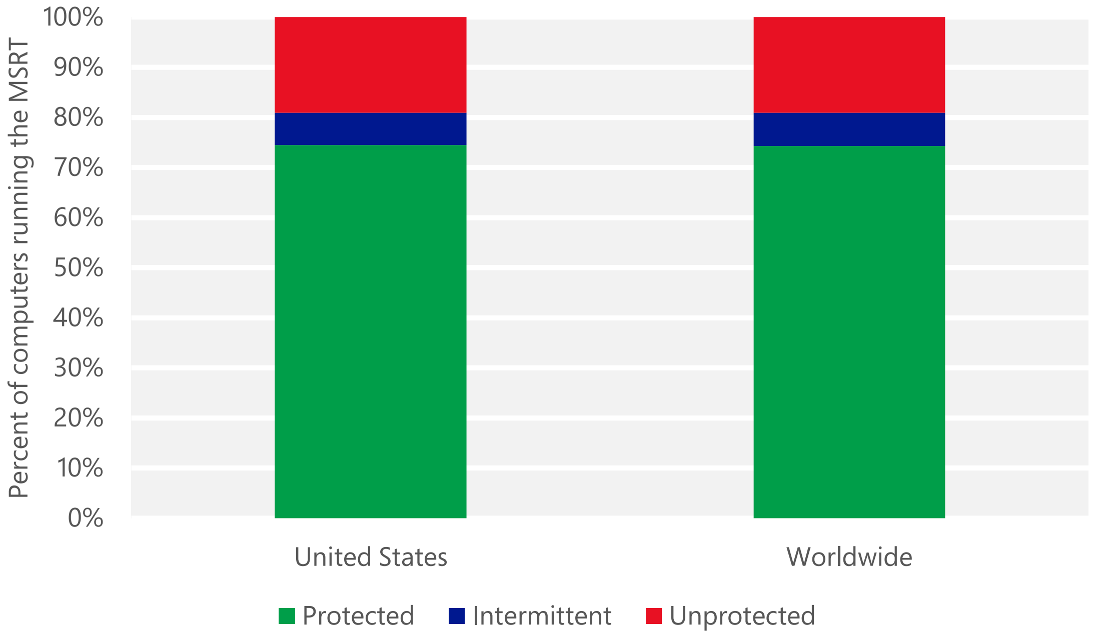
- The most common threat family infecting computers in the United States in 4Q14 was Win32/Alureon, which was detected and removed from 1.2 of every 1,000 unique computers scanned by the MSRT. Win32/Alureon is a data-stealing trojan that gathers confidential information such as user names, passwords, and credit card data from incoming and outgoing Internet traffic. It may also download malicious data and modify DNS settings.
- The second most common threat family infecting computers in the United States in 4Q14 was Win32/Tracur, which was detected and removed from 0.5 of every 1,000 unique computers scanned by the MSRT. Win32/Tracur is a trojan that downloads and executes arbitrary files, redirects web search queries to a malicious URL, and may also install other malware.
- The third most common threat family infecting computers in the United States in 4Q14 was Win32/Zbot, which was detected and removed from 0.4 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 fourth most common threat family infecting computers in the United States in 4Q14 was JS/Medfos, which was detected and removed from 0.3 of every 1,000 unique computers scanned by the MSRT. JS/Medfos is ?A trojan that installs malicious Internet browser extensions and redirects search results from popular search engines.

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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.25 drive-by download URLs for every 1,000 URLs hosted in the United States, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.33 drive-by download URLs for every 1,000 URLs hosted in the United States, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in the United States and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, United States	0.25	0.33
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Uruguay

The statistics presented here are generated by Microsoft security programs and services running on computers in Uruguay in 4Q14 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 succeds 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

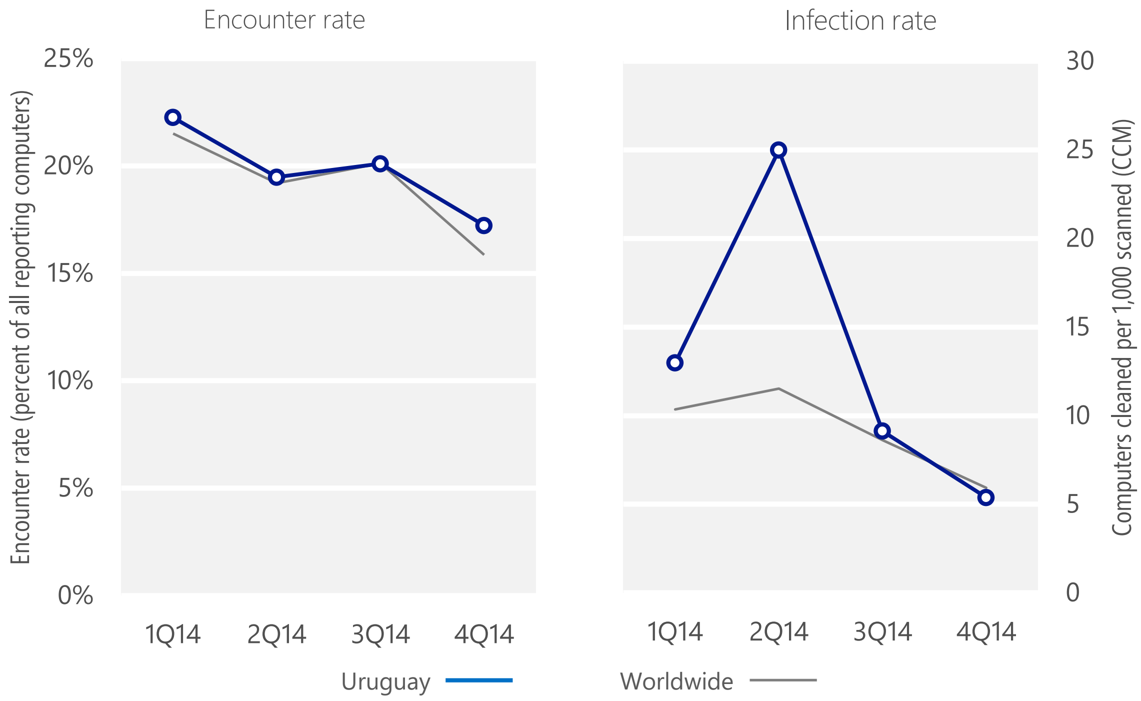
Metric	**1Q14**	**2Q14**	**3Q14**	**4Q14**
Encounter rate, Uruguay	22.3%	19.5%	20.1%	17.2%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Uruguay	13.0	25.0	9.1	5.4
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 17.2% percent of computers in Uruguay encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 5.4 of every 1,000 unique computers scanned in Uruguay in 4Q14 (a CCM score of 5.4, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Uruguay over the last four quarters, compared to the world as a whole.

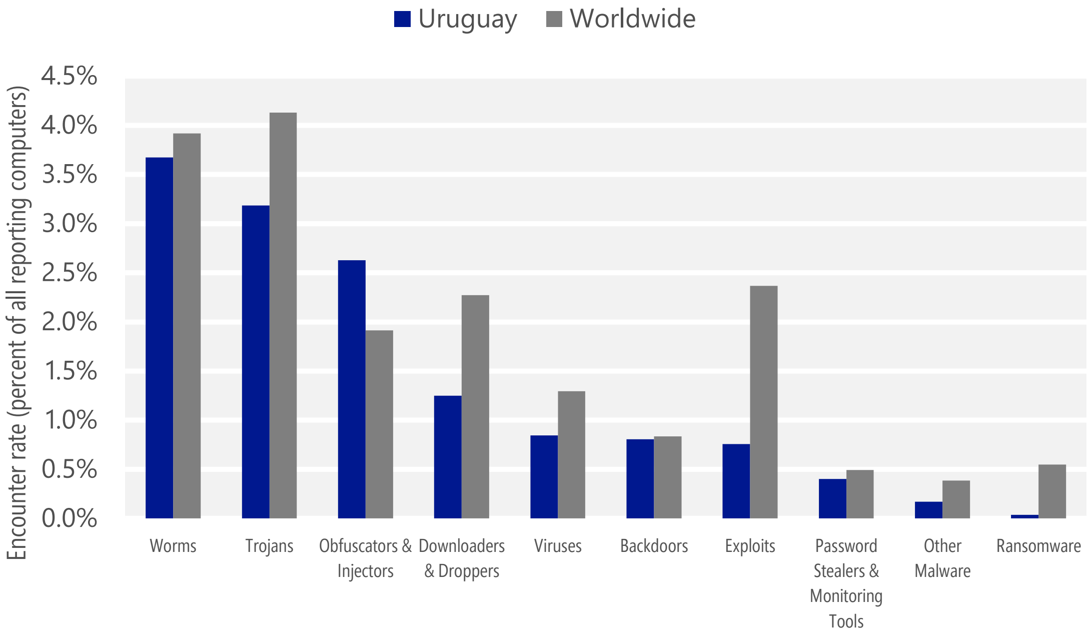
Malware encounter and infection rate trends in Uruguay and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

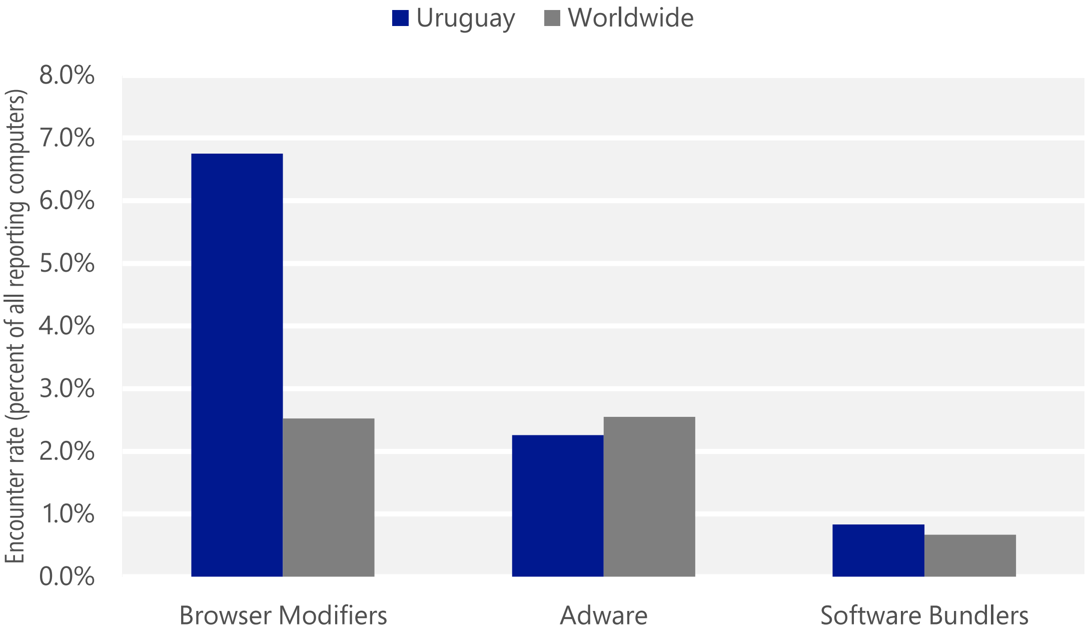
Malware encountered in Uruguay in 4Q14, by category



- The most common malware category in Uruguay in 4Q14 was Worms. It was encountered by 3.7 percent of all computers there, down from 5.6 percent in 3Q14.
- The second most common malware category in Uruguay in 4Q14 was Trojans. It was encountered by 3.2 percent of all computers there, down from 4.2 percent in 3Q14.
- The third most common malware category in Uruguay in 4Q14 was Obfuscators & Injectors, which was encountered by 2.6 percent of all computers there, down from 3.6 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Uruguay in 4Q14, by category



- The most common unwanted software category in Uruguay in 4Q14 was Browser Modifiers. It was encountered by 6.8 percent of all computers there, up from 5.9 percent in 3Q14.
- The second most common unwanted software category in Uruguay in 4Q14 was Adware. It was encountered by 2.3 percent of all computers there, up from 1.9 percent in 3Q14.
- The third most common unwanted software category in Uruguay in 4Q14 was Software Bundlers, which was encountered by 0.8 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Uruguay in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Obfuscator	Obfuscators & Injectors	1.6%
2	INF/Autorun	Obfuscators & Injectors	0.9%
3	JS/Bondat	Worms	0.8%

- The most common malware family encountered in Uruguay in 4Q14 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 4Q14 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.
- The third most common malware family encountered in Uruguay in 4Q14 was JS/Bondat, which was encountered by 0.8 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 fourth most common malware family encountered in Uruguay in 4Q14 was N/A, which was encountered by percent of reporting computers there.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Uruguay in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	5.1%
2	Win32/Defaulttab	Browser Modifiers	1.8%
3	Win32/Costmin	Adware	1.0%
4	Win32/BetterSurf	Adware	0.8%

- The most common unwanted software family encountered in Uruguay in 4Q14 was Win32/Couponruc, which was encountered by 5.1 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 Uruguay in 4Q14 was Win32/Defaulttab, which was encountered by 1.8 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.
- The third most common unwanted software family encountered in Uruguay in 4Q14 was Win32/Costmin, which was encountered by 1.0 percent of reporting computers there. Win32/Costmin is an adware family that installs itself as a browser extension for Internet Explorer, Mozilla Firefox, and Google Chrome, and displays advertisements as the user browses the Internet.

Top threat families by infection rate

The most common malware families by infection rate in Uruguay in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Sality	Viruses	0.7
2	VBS/Jenxcus	Worms	0.6
3	MSIL/Spacekito	Trojans	0.6
4	Win32/Sefnit	Trojans	0.6
5	Win32/Ramnit	Trojans	0.6
6	Win32/Gamarue	Worms	0.2
7	Win32/Dorkbot	Worms	0.2
8	Win32/Wysotot	Trojans	0.2
9	Win32/Conficker	Worms	0.2
10	Win32/Brontok	Worms	0.2

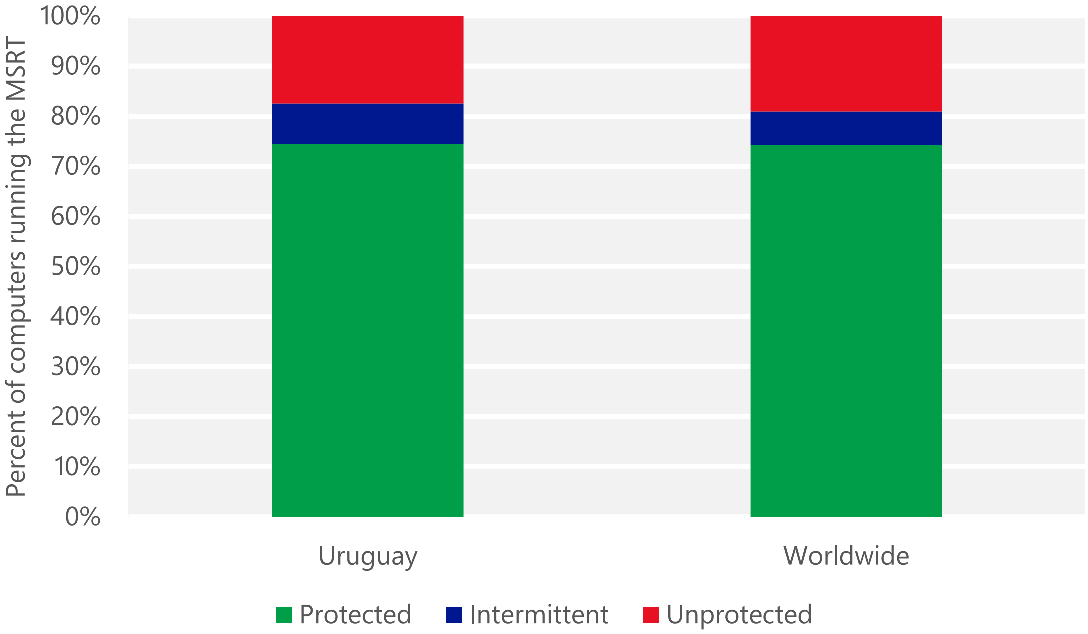
- The most common threat family infecting computers in Uruguay in 4Q14 was Win32/Sality, which was detected and removed from 0.7 of every 1,000 unique computers scanned by the MSRT. Win32/Sality is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The second most common threat family infecting computers in Uruguay in 4Q14 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.
- The third most common threat family infecting computers in Uruguay in 4Q14 was MSIL/Spacekito, which was detected and removed from 0.6 of every 1,000 unique computers scanned by the MSRT. MSIL/Spacekito is a threat that steals information about the computer and installs browser add-ons that display ads.
- The fourth most common threat family infecting computers in Uruguay in 4Q14 was Win32/Sefnit, which was detected and removed from 0.6 of every 1,000 unique computers scanned by the MSRT. Win32/Sefnit is a family of trojans that can allow backdoor access, download files, and use the computer and Internet connection for click fraud. Some variants can monitor web browsers and hijack search results.

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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.03 drive-by download URLs for every 1,000 URLs hosted in Uruguay, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.07 drive-by download URLs for every 1,000 URLs hosted in Uruguay, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Uruguay and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Uruguay	0.03	0.07
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Venezuela

The statistics presented here are generated by Microsoft security programs and services running on computers in Venezuela in 4Q14 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 succeds 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

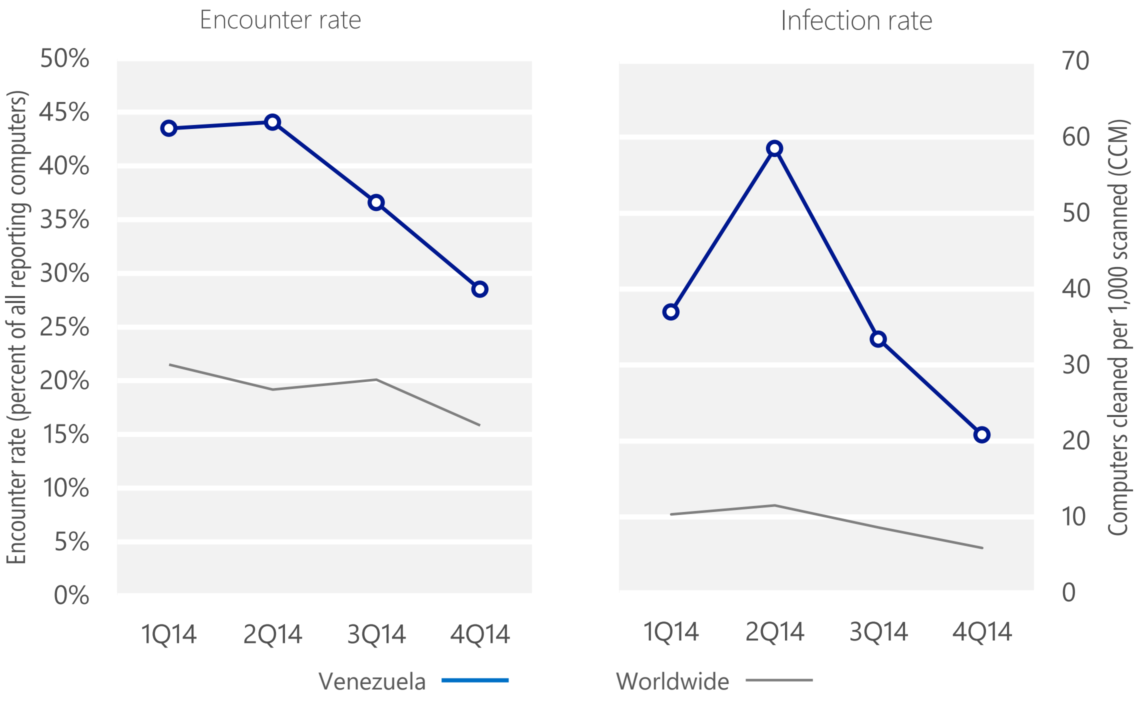
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Venezuela	43.5%	44.1%	36.6%	28.5%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Venezuela	37.0	58.5	33.4	20.8
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 28.5% percent of computers in Venezuela encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 20.8 of every 1,000 unique computers scanned in Venezuela in 4Q14 (a CCM score of 20.8, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Venezuela over the last four quarters, compared to the world as a whole.

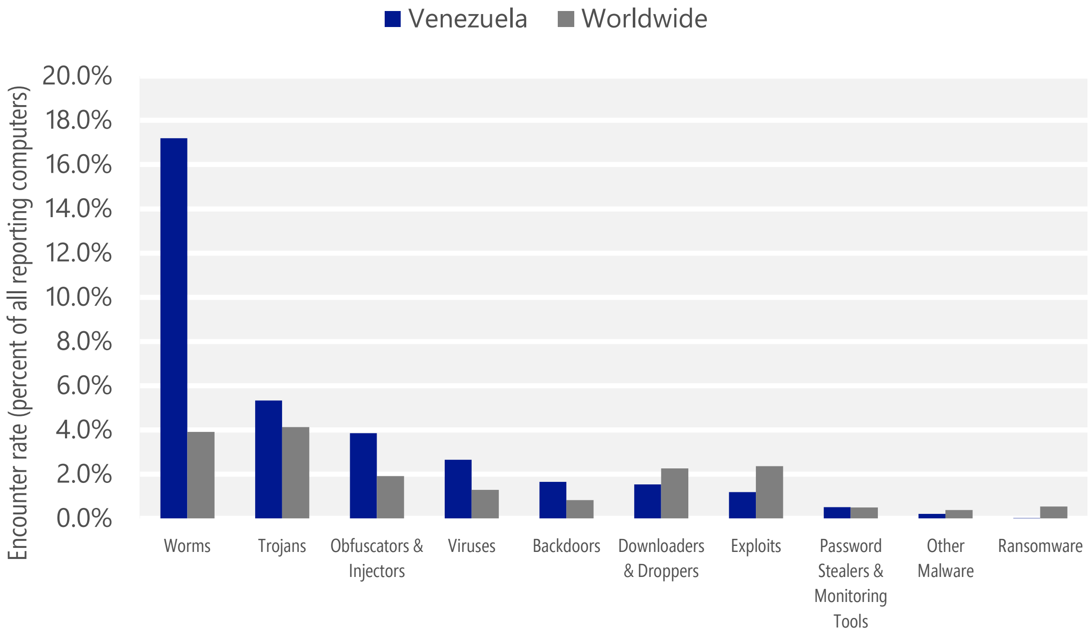
Malware encounter and infection rate trends in Venezuela and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

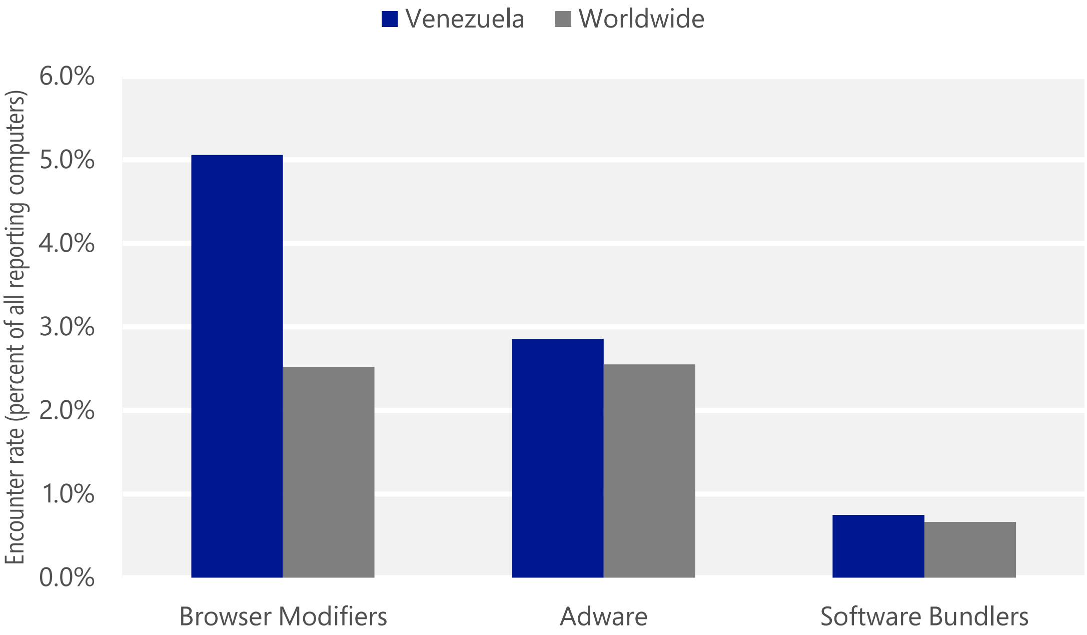
Malware encountered in Venezuela in 4Q14, by category



- The most common malware category in Venezuela in 4Q14 was Worms. It was encountered by 17.2 percent of all computers there, down from 21.6 percent in 3Q14.
- The second most common malware category in Venezuela in 4Q14 was Trojans. It was encountered by 5.3 percent of all computers there, down from 9.9 percent in 3Q14.
- The third most common malware category in Venezuela in 4Q14 was Obfuscators & Injectors, which was encountered by 3.9 percent of all computers there, down from 4.8 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Venezuela in 4Q14, by category



- The most common unwanted software category in Venezuela in 4Q14 was Browser Modifiers. It was encountered by 5.1 percent of all computers there, down from 6.6 percent in 3Q14.
- The second most common unwanted software category in Venezuela in 4Q14 was Adware. It was encountered by 2.9 percent of all computers there, up from 1.7 percent in 3Q14.
- The third most common unwanted software category in Venezuela in 4Q14 was Software Bundlers, which was encountered by 0.8 percent of all computers there, up from 0.2 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Venezuela in 4Q14

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	11.9%
2	INF/Autorun	Obfuscators & Injectors	2.8%
3	JS/Bondat	Worms	2.3%
4	Win32/Conficker	Worms	1.9%
5	Win32/Sality	Viruses	1.4%
6	Win32/Vermis	Worms	1.3%
7	Win32/Dorkbot	Worms	1.1%
8	Win32/Obfuscator	Obfuscators & Injectors	1.1%
9	Win32/Nuqel	Worms	1.0%
10	Win32/Lamin	Worms	1.0%

- The most common malware family encountered in Venezuela in 4Q14 was VBS/Jenxcus, which was encountered by 11.9 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 Venezuela in 4Q14 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 third most common malware family encountered in Venezuela in 4Q14 was JS/Bondat, which was encountered by 2.3 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 fourth most common malware family encountered in Venezuela in 4Q14 was Win32/Conficker, which was encountered by 1.9 percent of reporting computers there. Win32/Conficker is a worm that spreads by exploiting a vulnerability addressed by Security Bulletin MS08-067. Some variants also spread via removable drives and by exploiting weak passwords. It disables several important system services and security products, and downloads arbitrary files.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Venezuela in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	3.9%
2	Win32/BetterSurf	Adware	1.6%
3	Win32/Defaulttab	Browser Modifiers	1.3%
4	Win32/Costmin	Adware	0.9%
5	Win32/Gofileexpress	Software Bundlers	0.3%

- The most common unwanted software family encountered in Venezuela in 4Q14 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 second most common unwanted software family encountered in Venezuela in 4Q14 was Win32/BetterSurf, which was encountered by 1.6 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.
- The third most common unwanted software family encountered in Venezuela in 4Q14 was Win32/Defaulttab, which was encountered by 1.3 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.

Top threat families by infection rate

The most common malware families by infection rate in Venezuela in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	13.0
2	Win32/Sality	Viruses	2.2
3	Win32/Ramnit	Trojans	1.0
4	Win32/Dorkbot	Worms	0.6
5	MSIL/Bladabindi	Backdoors	0.5
6	Win32/Sefnit	Trojans	0.5
7	Win32/Vobfus	Worms	0.5
8	MSIL/Spacekito	Trojans	0.5
9	Win32/Nuqel	Worms	0.5
10	Win32/Pramro	Trojans	0.5

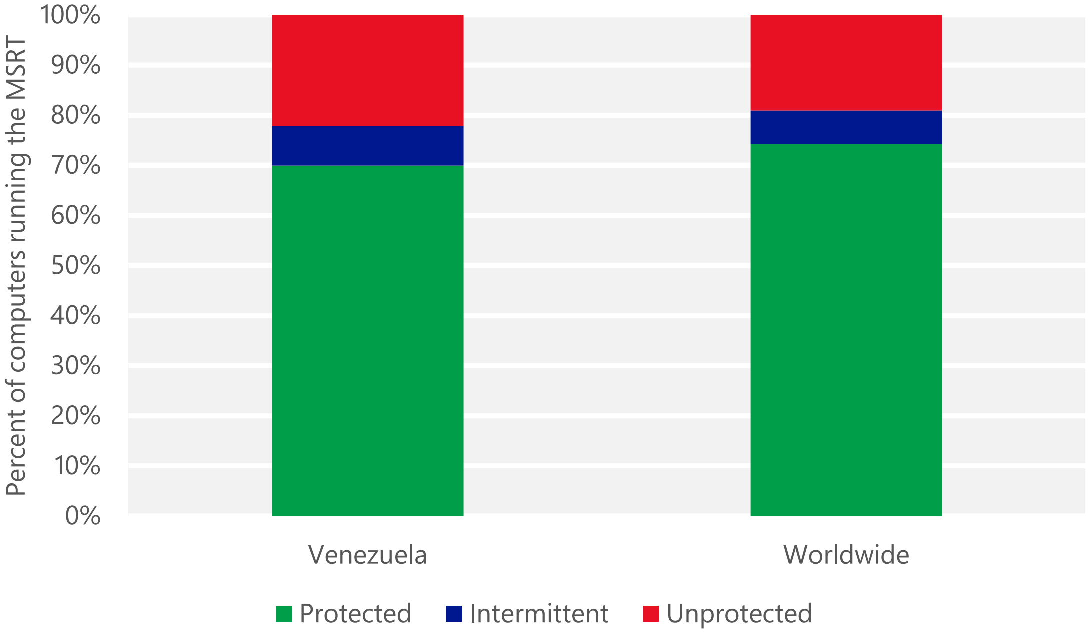
- The most common threat family infecting computers in Venezuela in 4Q14 was VBS/Jenxcus, which was detected and removed from 13.0 of every 1,000 unique computers scanned by the MSRT. VBS/Jenxcus is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Venezuela in 4Q14 was Win32/Sality, which was detected and removed from 2.2 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.
- The third most common threat family infecting computers in Venezuela in 4Q14 was Win32/Ramnit, which was detected and removed from 1.0 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.
- The fourth most common threat family infecting computers in Venezuela in 4Q14 was Win32/Dorkbot, which was detected and removed from 0.6 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 Venezuela and worldwide protected by real-time security software in 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.47 drive-by download URLs for every 1,000 URLs hosted in Venezuela, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.25 drive-by download URLs for every 1,000 URLs hosted in Venezuela, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Venezuela and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Venezuela	0.47	0.25
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Vietnam

The statistics presented here are generated by Microsoft security programs and services running on computers in Vietnam in 4Q14 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 succeds 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

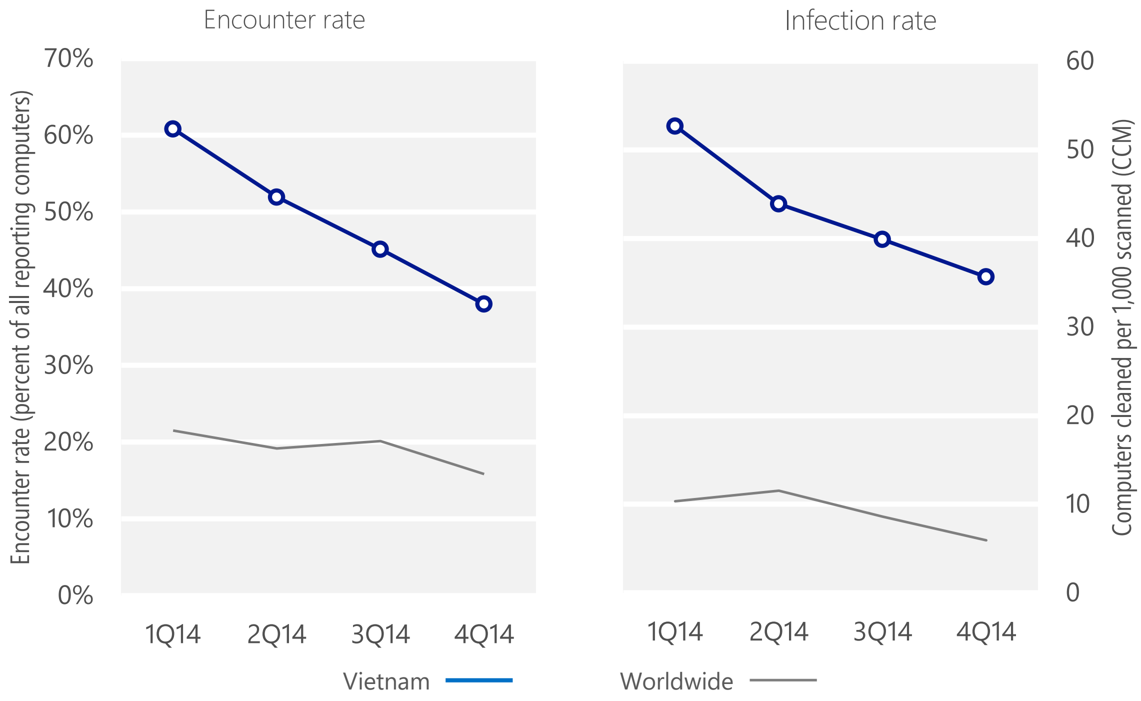
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Vietnam	60.8%	52.0%	45.1%	38.0%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Vietnam	52.7	43.9	39.9	35.7
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, 38.0% percent of computers in Vietnam encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 35.7 of every 1,000 unique computers scanned in Vietnam in 4Q14 (a CCM score of 35.7, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Vietnam over the last four quarters, compared to the world as a whole.

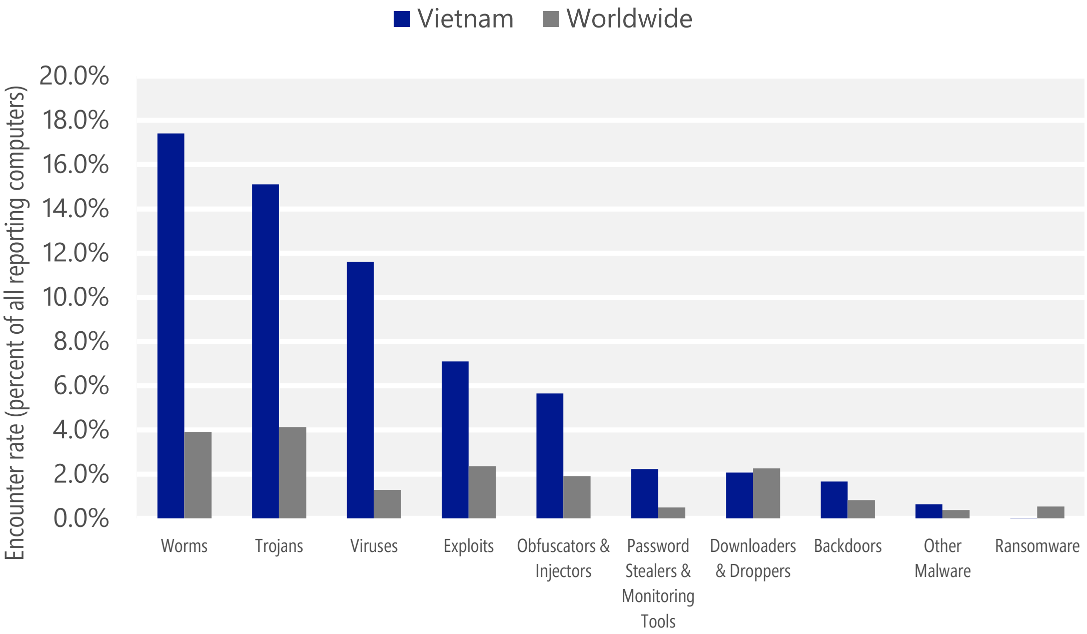
Malware encounter and infection rate trends in Vietnam and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* 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

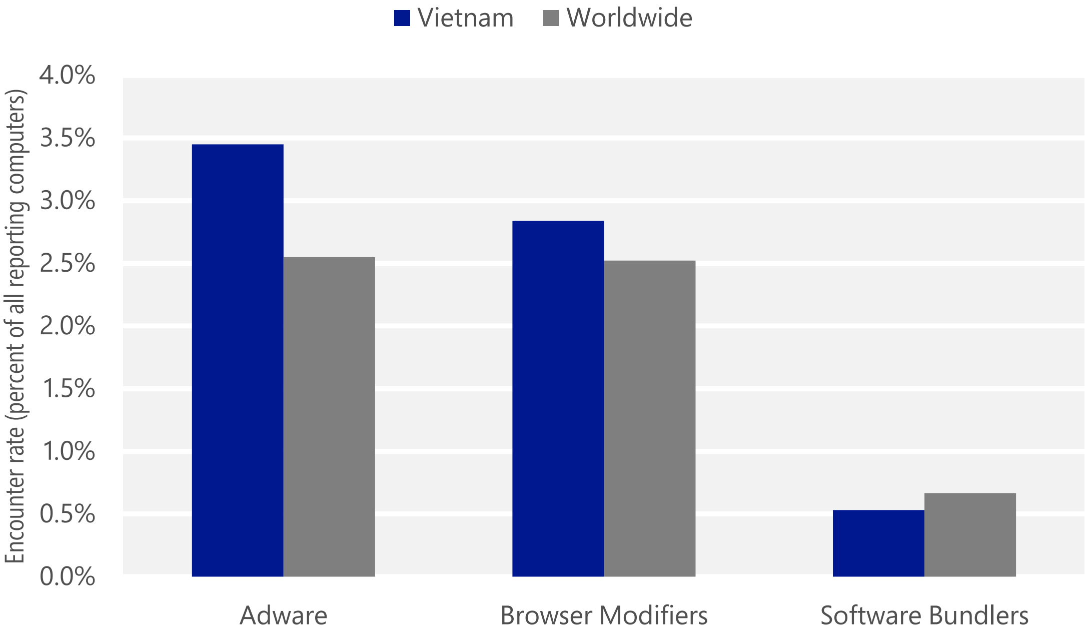
Malware encountered in Vietnam in 4Q14, by category



- The most common malware category in Vietnam in 4Q14 was Worms. It was encountered by 17.4 percent of all computers there, down from 26.3 percent in 3Q14.
- The second most common malware category in Vietnam in 4Q14 was Trojans. It was encountered by 15.1 percent of all computers there, down from 17.1 percent in 3Q14.
- The third most common malware category in Vietnam in 4Q14 was Viruses, which was encountered by 11.6 percent of all computers there, up from 9.3 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Vietnam in 4Q14, by category



- The most common unwanted software category in Vietnam in 4Q14 was Adware. It was encountered by 3.4 percent of all computers there, down from 5.7 percent in 3Q14.
- The second most common unwanted software category in Vietnam in 4Q14 was Browser Modifiers. It was encountered by 2.8 percent of all computers there, up from 0.8 percent in 3Q14.
- The third most common unwanted software category in Vietnam in 4Q14 was Software Bundlers, which was encountered by 0.5 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Vietnam in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Gamarue	Worms	8.3%
2	Win32/CplLnk	Exploits	6.7%
3	Win32/Ramnit	Trojans	6.4%
4	INF/Autorun	Obfuscators & Injectors	6.3%
5	JS/Faceliker	Trojans	4.7%
6	Win32/Sality	Viruses	4.5%
7	DOS/Sigru	Viruses	3.5%
8	VBS/Jenxcus	Worms	3.1%
9	Win32/VB	Worms	2.3%
10	Win32/Conficker	Worms	1.8%

- The most common malware family encountered in Vietnam in 4Q14 was Win32/Gamarue, which was encountered by 8.3 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 4Q14 was Win32/CplLnk, which was encountered by 6.7 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 third most common malware family encountered in Vietnam in 4Q14 was Win32/Ramnit, which was encountered by 6.4 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.
- The fourth most common malware family encountered in Vietnam in 4Q14 was INF/Autorun, which was encountered by 6.3 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 Vietnam in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	2.2%
2	Win32/Pennybee	Adware	1.7%
3	Win32/BetterSurf	Adware	0.8%
4	Win32/Costmin	Adware	0.8%
5	Win32/Defaulttab	Browser Modifiers	0.7%

- The most common unwanted software family encountered in Vietnam in 4Q14 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 Vietnam in 4Q14 was Win32/Pennybee, which was encountered by 1.7 percent of reporting computers there. Win32/Pennybee is adware that shows ads as the user browses the web. It can be installed from the program's website or bundled with some third-party software installation programs.

- The third most common unwanted software family encountered in Vietnam in 4Q14 was Win32/BetterSurf, which was encountered by 0.8 percent of reporting computers there. Win32/BetterSurf is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.

Top threat families by infection rate

The most common malware families by infection rate in Vietnam in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Ramnit	Trojans	9.7
2	Win32/Sality	Viruses	8.1
3	Win32/Gamarue	Worms	7.4
4	VBS/Jenxcus	Worms	3.8
5	Win32/Wysotot	Trojans	2.0
6	Win32/Folstart	Worms	1.4
7	Win32/Pramro	Trojans	1.3
8	Win32/Sefnit	Trojans	0.7
9	Win32/Nitol	Other Malware	0.6
10	Win32/Necurs	Trojans	0.6

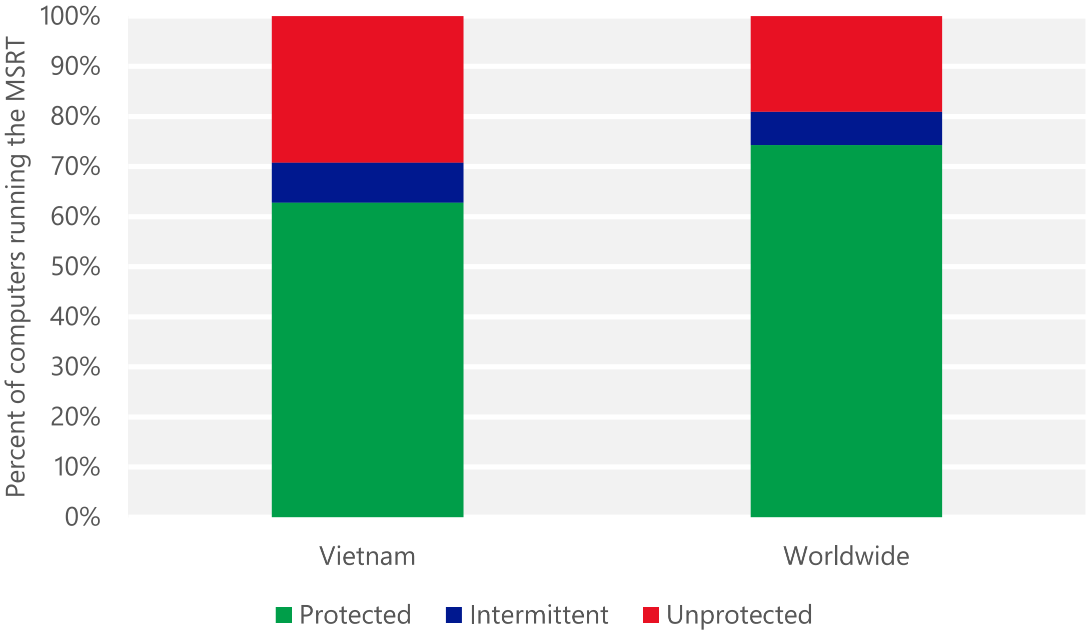
- The most common threat family infecting computers in Vietnam in 4Q14 was Win32/Ramnit, which was detected and removed from 9.7 of every 1,000 unique computers scanned by the MSRT. Win32/Ramnit is a family of multi-component malware that infects executable files, Microsoft Office files, and HTML files. 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 Vietnam in 4Q14 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.
- The third most common threat family infecting computers in Vietnam in 4Q14 was Win32/Gamarue, which was detected and removed from 7.4 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 Vietnam in 4Q14 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.

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 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 10.73 drive-by download URLs for every 1,000 URLs hosted in Vietnam, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 4.10 drive-by download URLs for every 1,000 URLs hosted in Vietnam, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Vietnam and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Vietnam	10.73	4.10
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Zimbabwe

The statistics presented here are generated by Microsoft security programs and services running on computers in Zimbabwe in 4Q14 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 succeds 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

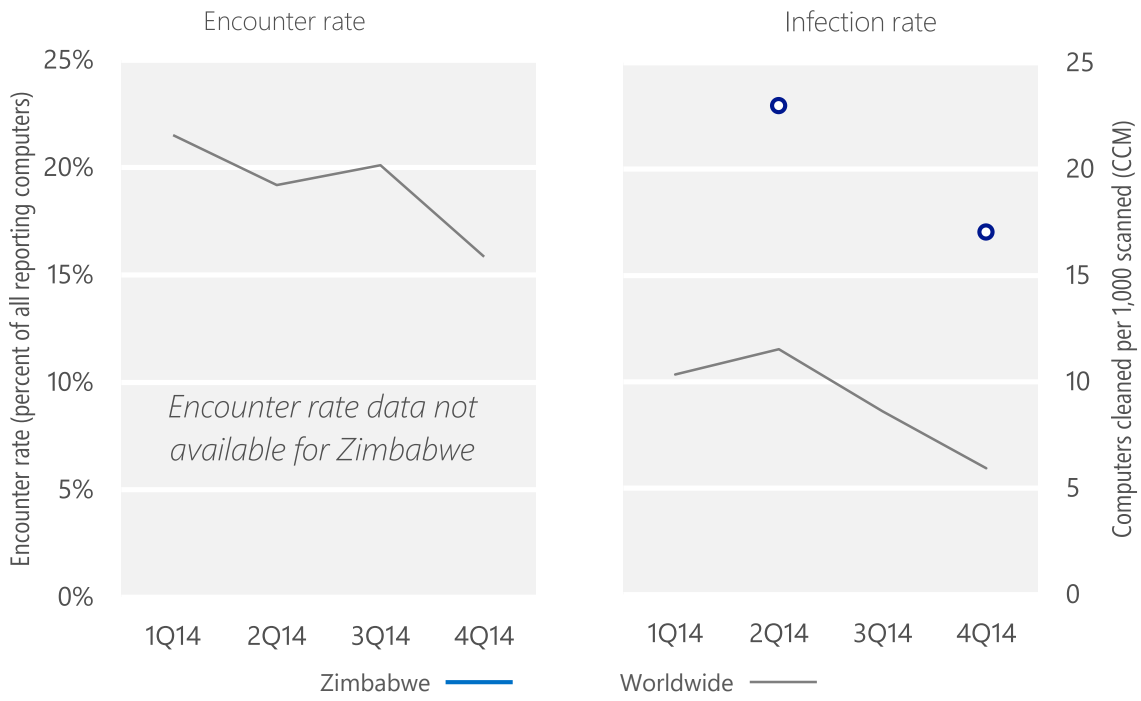
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Zimbabwe	N/A	N/A	N/A	N/A
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Zimbabwe	N/A	23.0	N/A	17.0
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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 4Q14, the MSRT detected and removed malware from 17.0 of every 1,000 unique computers scanned in Zimbabwe in 4Q14 (a CCM score of 17.0, compared to the 4Q14 worldwide CCM of 5.9). 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 18* 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 4Q14

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	6.3
2	Win32/Chir	Viruses	3.8
3	Win32/Sality	Viruses	3.0
4	Win32/Zbot	Password Stealers & Monitoring Tools	1.4
5	Win32/Ramnit	Trojans	0.8
6	Win32/Vobfus	Worms	0.7
7	MSIL/Bladabindi	Backdoors	0.6
8	Win32/Virut	Viruses	0.6
9	Win32/Gamarue	Worms	0.3
10	Win32/Parite	Viruses	0.2

- The most common threat family infecting computers in Zimbabwe in 4Q14 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 second most common threat family infecting computers in Zimbabwe in 4Q14 was Win32/Chir, which was detected and removed from 3.8 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 third most common threat family infecting computers in Zimbabwe in 4Q14 was Win32/Sality, which was detected and removed from 3.0 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 Zimbabwe in 4Q14 was Win32/Zbot, which was detected and removed from 1.4 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.

Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 1.36 drive-by download URLs for every 1,000 URLs hosted in Zimbabwe, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.98 drive-by download URLs for every 1,000 URLs hosted in Zimbabwe, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Zimbabwe and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Zimbabwe	1.36	0.98
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

Microsoft

One Microsoft Way
Redmond, WA 98052-6399
microsoft.com/security