

Microsoft Security Intelligence Report

Regional Threat Assessment – Volume 13

January through June, 2012

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 website references, may change without notice. You bear the risk of using it.

Copyright © 2012 Microsoft Corporation. All rights reserved.

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

Table of Contents

Albania.....	5
Algeria.....	13
Angola	21
Argentina.....	29
Australia	37
Austria.....	45
Bahamas, The.....	53
Bahrain.....	61
Bangladesh.....	69
Belarus	77
Belgium	85
Bolivia.....	93
Brazil.....	101
Bulgaria	109
Canada.....	117
Chile.....	125
China	133
Colombia	141
Costa Rica.....	149
Croatia	157
Cyprus.....	165
Czech Republic.....	173
Denmark	181
Dominican Republic.....	189
Ecuador	197
Egypt	205

El Salvador	213
Estonia	221
Finland.....	229
France	237
Georgia.....	245
Germany	253
Greece	261
Guatemala.....	269
Honduras.....	277
Hong Kong S.A.R.....	285
Hungary	293
Iceland	301
India.....	309
Indonesia	317
Iraq.....	325
Ireland.....	333
Israel	341
Italy	349
Jamaica.....	357
Japan.....	365
Jordan.....	373
Kazakhstan.....	381
Kenya	389
Korea.....	397
Kuwait.....	405
Latvia.....	413
Lebanon.....	421
Lithuania.....	429
Luxembourg.....	437
Macao S.A.R.....	445
Malaysia	453

Malta	461
Mexico	469
Moldova.....	477
Morocco.....	485
Nepal.....	493
Netherlands	501
New Zealand	509
Nicaragua	517
Nigeria	525
Norway	533
Oman	541
Pakistan	549
Palestinian Authority.....	557
Panama.....	565
Paraguay	573
Peru.....	581
Philippines.....	589
Poland.....	597
Portugal.....	605
Puerto Rico.....	613
Qatar.....	621
Romania	629
Russia.....	637
Saudi Arabia	645
Senegal	653
Singapore	661
Slovakia	669
Slovenia	677
South Africa	685
Spain.....	693
Sri Lanka.....	701

Sweden.....	709
Switzerland	717
Syria.....	725
Taiwan	733
Tanzania.....	741
Thailand	749
Trinidad and Tobago.....	757
Tunisia	765
Turkey.....	773
Uganda.....	781
Ukraine.....	789
United Arab Emirates.....	797
United Kingdom	805
United States.....	813
Uruguay	821
Venezuela.....	829
Vietnam.....	837

Albania

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Albania in 2Q12 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.

Infection rate statistics for Albania

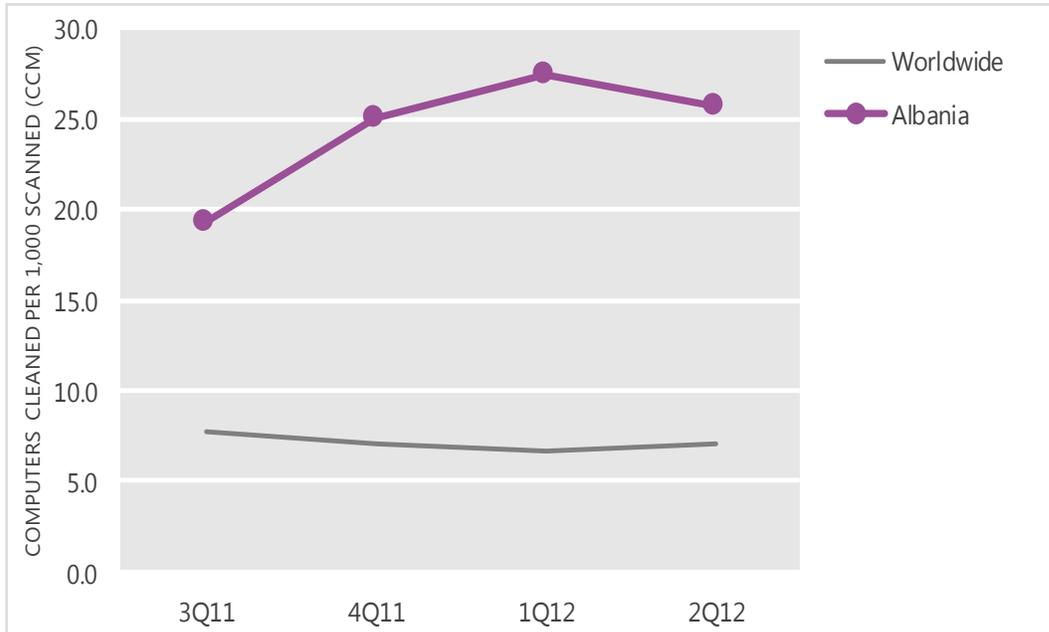
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	19.3	25.0	27.5	25.7
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

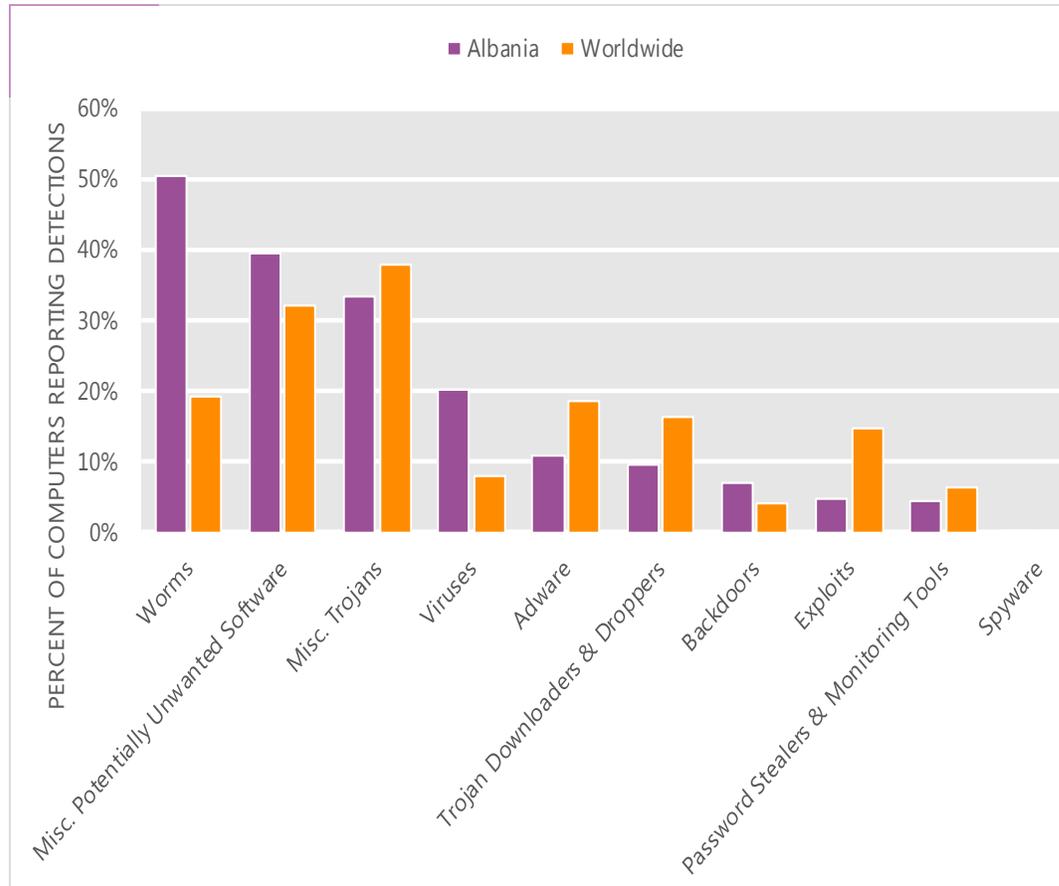
The MSRT detected malware on 25.7 of every 1,000 computers scanned in Albania in 2Q12 (a CCM score of 25.7, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Albania over the last four quarters, compared to the world as a whole.

CCM infection trends in Albania and worldwide



Threat categories

Malware and potentially unwanted software categories in Albania in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Albania in 2Q12 was Worms. It affected 50.5 percent of all computers with detections there, up from 48.7 percent in 1Q12.
- The second most common category in Albania in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 39.3 percent of all computers with detections there, up from 38.5 percent in 1Q12.
- The third most common category in Albania in 2Q12 was Miscellaneous Trojans, which affected 33.2 percent of all computers with detections there, down from 35.3 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Albania in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Autorun	Worms	23.3%
2	Win32/Sality	Viruses	20.7%
3	Win32/Helompy	Worms	20.2%
4	Win32/Rimecud	Worms	12.1%
5	Win32/Keygen	Misc. Potentially Unwanted Software	11.3%
6	Win32/Conficker	Worms	11.1%
7	Win32/Vobfus	Worms	8.8%
8	Win32/Dorkbot	Worms	6.3%
9	Win32/Hotbar	Adware	4.5%
10	JS/Pornpop	Adware	4.1%

- The most common threat family in Albania in 2Q12 was [Win32/Autorun](#), which affected 23.3 percent of computers with detections in Albania. [Win32/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 threat family in Albania in 2Q12 was [Win32/Sality](#), which affected 20.7 percent of computers with detections in Albania. [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 in Albania in 2Q12 was [Win32/Helompy](#), which affected 20.2 percent of computers with detections in Albania. [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 in Albania in 2Q12 was [Win32/Rimecud](#), which affected 12.1 percent of computers with detections in Albania. [Win32/Rimecud](#) is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Albania

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	N/A (1.6)	N/A (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	2.85 (3.9)	2.85 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	N/A (0.7)	N/A (0.9)

Update service usage

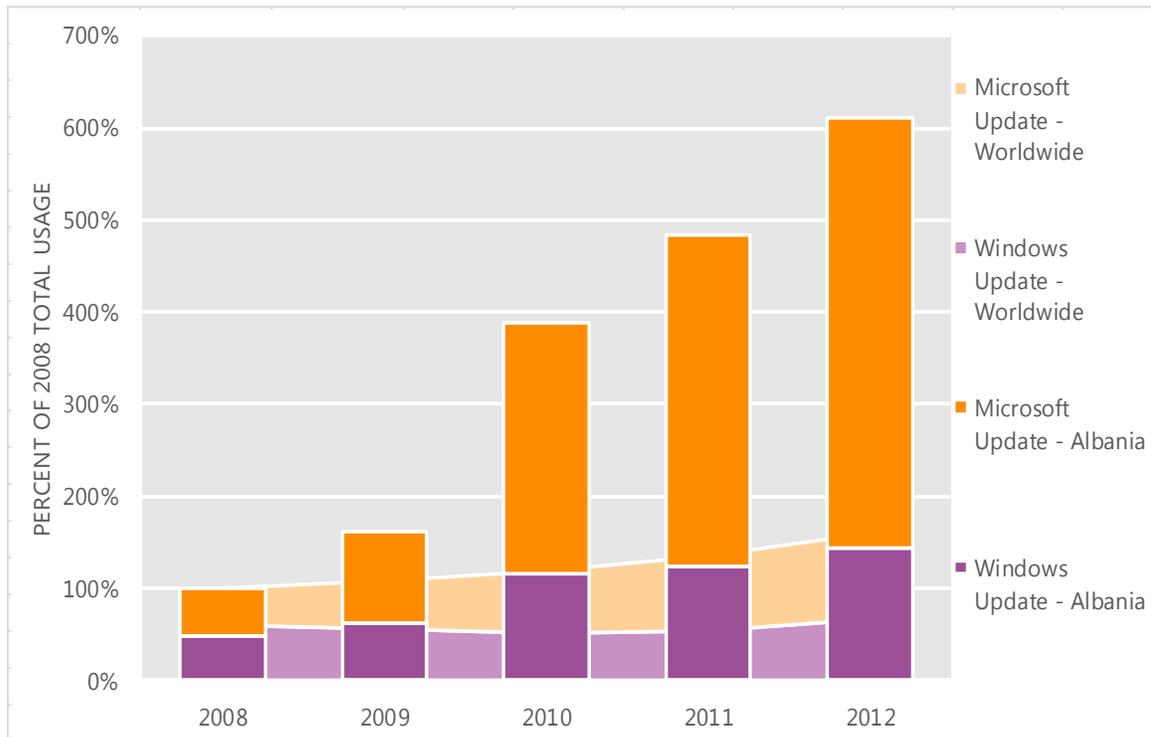
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Albania and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Albania over the last four years, indexed to the total usage for both services in Albania in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Albania was up 26.1 percent from 2011, and up 511.3 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Albania in 2012, 76.4 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Algeria

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Algeria in 2Q12 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.

Infection rate statistics for Algeria

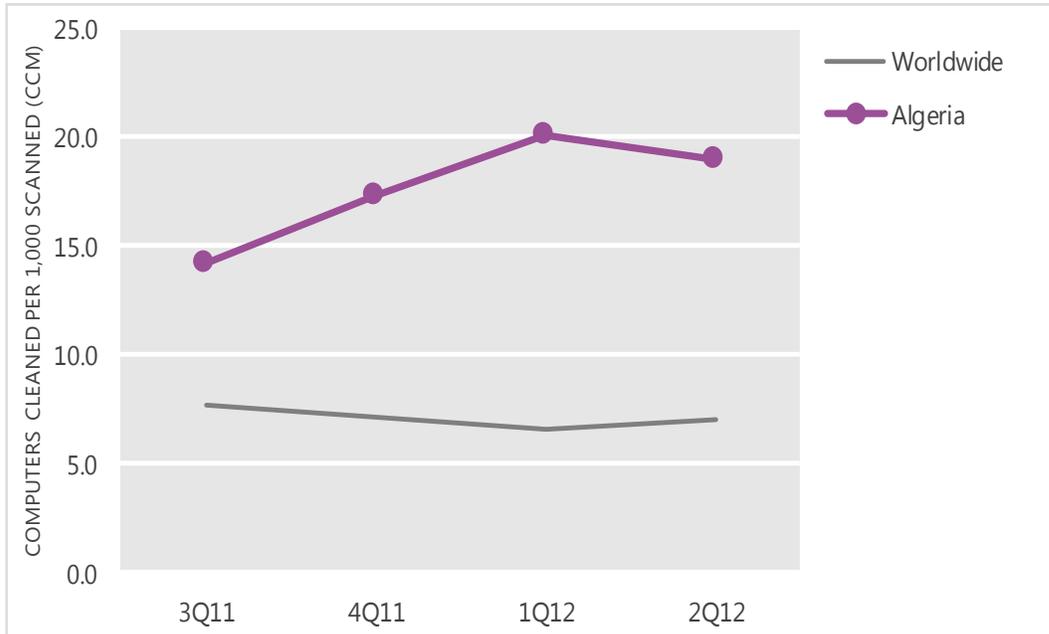
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	14.2	17.3	20.1	19.0
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

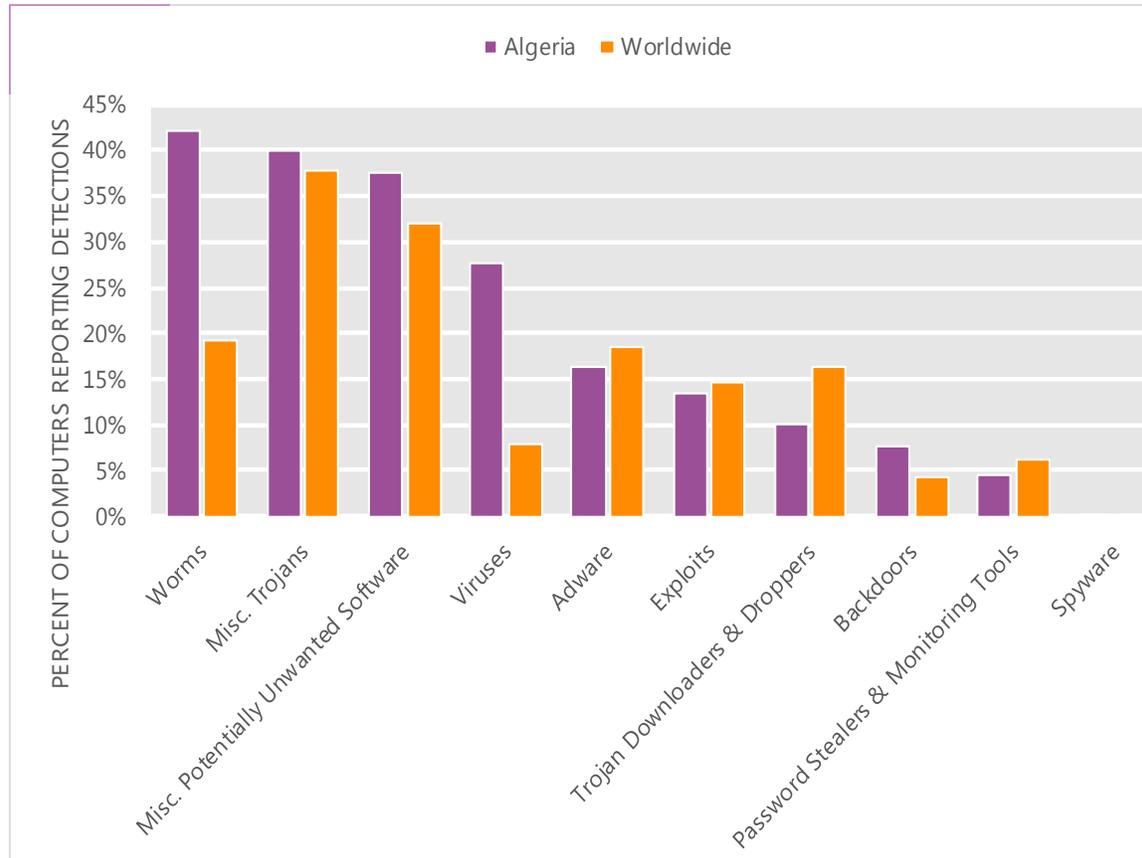
The MSRT detected malware on 19.0 of every 1,000 computers scanned in Algeria in 2Q12 (a CCM score of 19.0, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Algeria over the last four quarters, compared to the world as a whole.

CCM infection trends in Algeria and worldwide



Threat categories

Malware and potentially unwanted software categories in Algeria in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Algeria in 2Q12 was Worms. It affected 42.1 percent of all computers with detections there, up from 41.2 percent in 1Q12.
- The second most common category in Algeria in 2Q12 was Miscellaneous Trojans. It affected 40.0 percent of all computers with detections there, up from 38.7 percent in 1Q12.
- The third most common category in Algeria in 2Q12 was Miscellaneous Potentially Unwanted Software, which affected 37.6 percent of all computers with detections there, down from 40.4 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Algeria in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Ramnit	Misc. Trojans	18.9%
2	Win32/Sality	Viruses	18.4%
3	Win32/Autorun	Worms	17.2%
4	Win32/Keygen	Misc. Potentially Unwanted Software	13.9%
5	Win32/Vobfus	Worms	12.9%
6	Win32/CplLnk	Exploits	12.0%
7	Win32/Dorkbot	Worms	9.3%
8	Win32/Yeltminky	Worms	6.7%
9	Win32/Mabezat	Viruses	5.9%
10	Win32/Hotbar	Adware	5.1%

- The most common threat family in Algeria in 2Q12 was [Win32/Ramnit](#), which affected 18.9 percent of computers with detections in Algeria. [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 in Algeria in 2Q12 was [Win32/Sality](#), which affected 18.4 percent of computers with detections in Algeria. [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 in Algeria in 2Q12 was [Win32/Autorun](#), which affected 17.2 percent of computers with detections in Algeria. [Win32/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 threat family in Algeria in 2Q12 was [Win32/Keygen](#), which affected 13.9 percent of computers with detections in Algeria. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Algeria

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	0.46 (1.6)	0.92 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	1.73 (3.9)	1.96 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.11 (0.7)	0.12 (0.9)

Update service usage

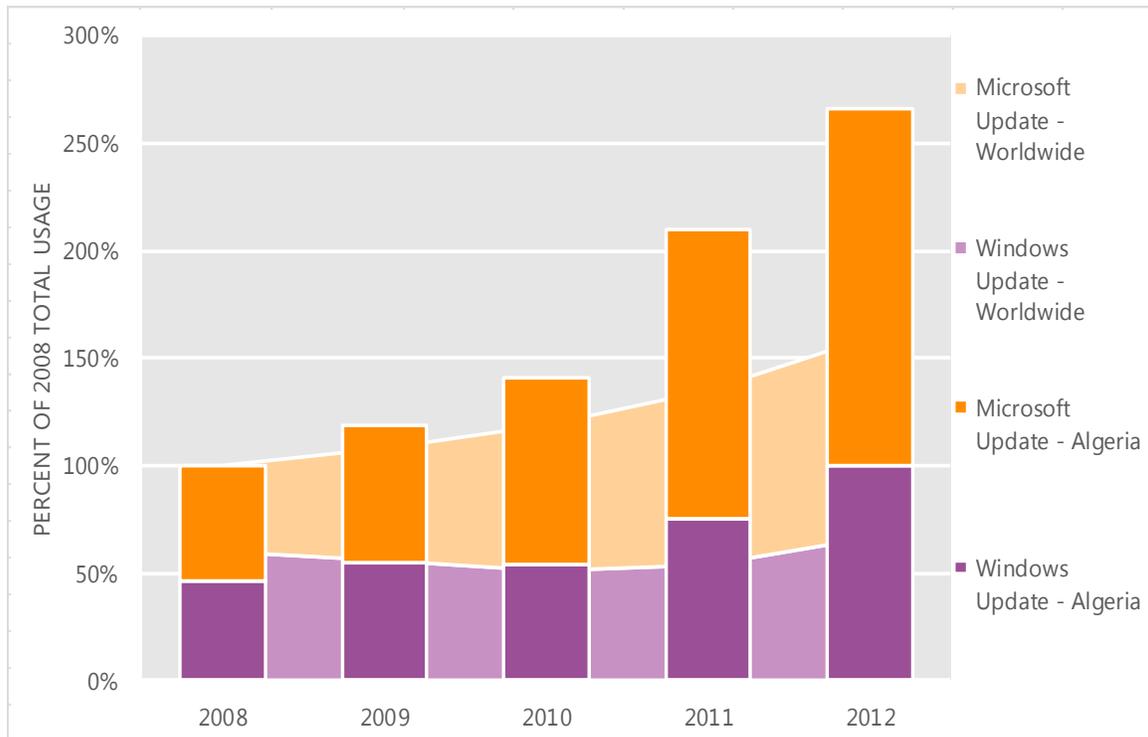
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Algeria and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Algeria over the last four years, indexed to the total usage for both services in Algeria in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Algeria was up 26.9 percent from 2011, and up 166.6 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Algeria in 2012, 62.6 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Angola

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Angola in 2Q12 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.

Infection rate statistics for Angola

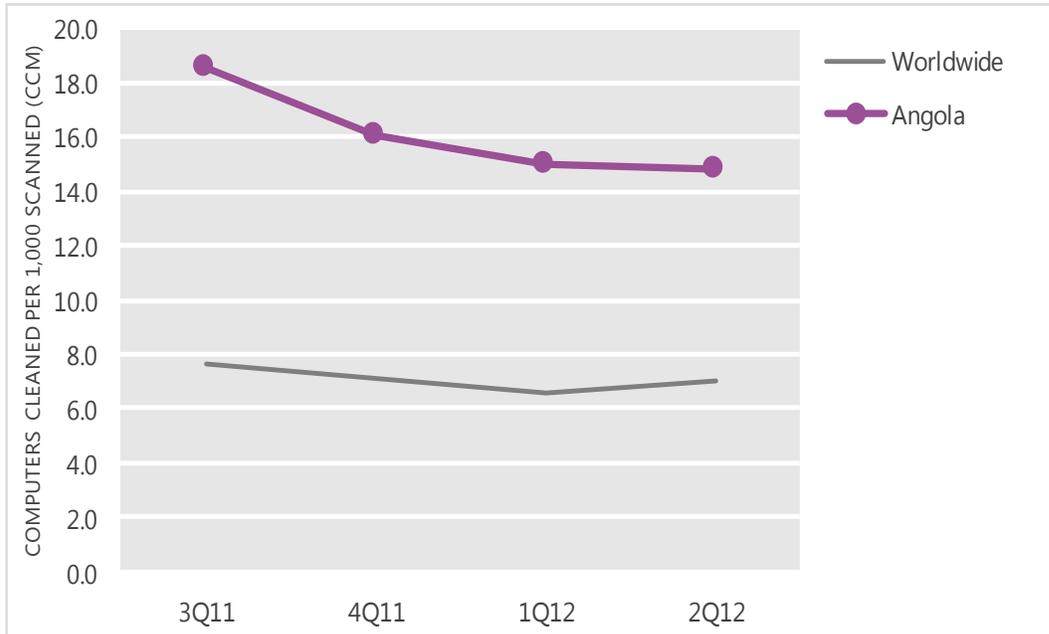
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	18.6	16.1	15.0	14.8
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

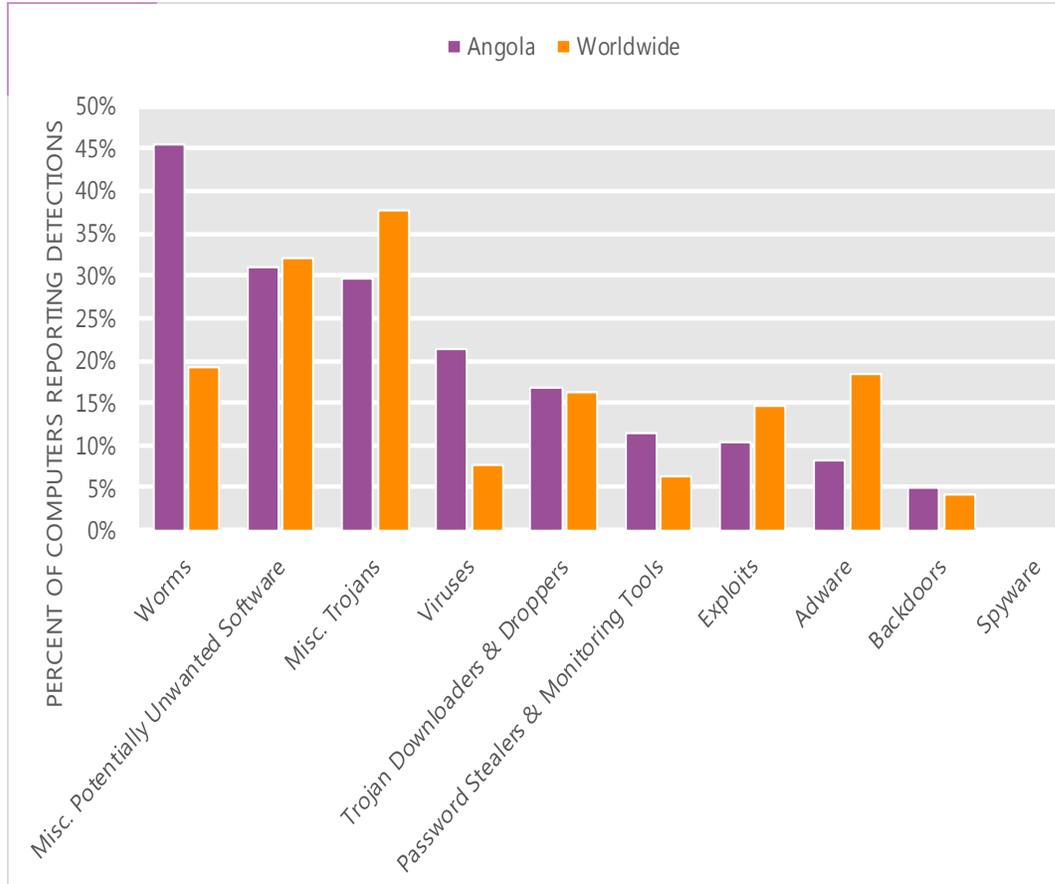
The MSRT detected malware on 14.8 of every 1,000 computers scanned in Angola in 2Q12 (a CCM score of 14.8, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Angola over the last four quarters, compared to the world as a whole.

CCM infection trends in Angola and worldwide



Threat categories

Malware and potentially unwanted software categories in Angola in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Angola in 2Q12 was Worms. It affected 45.4 percent of all computers with detections there, up from 44.1 percent in 1Q12.
- The second most common category in Angola in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 31.0 percent of all computers with detections there, up from 27.1 percent in 1Q12.
- The third most common category in Angola in 2Q12 was Miscellaneous Trojans, which affected 29.6 percent of all computers with detections there, up from 28.1 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Angola in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Vobfus	Worms	27.2%
2	Win32/Autorun	Worms	17.0%
3	Win32/Ramnit	Misc. Trojans	10.0%
4	Win32/Virut	Viruses	8.9%
5	Win32/CplLnk	Exploits	7.7%
6	Win32/Chir	Worms	7.0%
7	Win32/Dorkbot	Worms	6.8%
8	Win32/Keygen	Misc. Potentially Unwanted Software	5.6%
9	Win32/Bancos	Password Stealers & Monitoring Tools	5.0%
10	Win32/Sirefef	Misc. Trojans	4.7%

- The most common threat family in Angola in 2Q12 was [Win32/Vobfus](#), which affected 27.2 percent of computers with detections in Angola. [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 second most common threat family in Angola in 2Q12 was [Win32/Autorun](#), which affected 17.0 percent of computers with detections in Angola. [Win32/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 threat family in Angola in 2Q12 was [Win32/Ramnit](#), which affected 10.0 percent of computers with detections in Angola. [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 in Angola in 2Q12 was [Win32/Virut](#), which affected 8.9 percent of computers with detections in Angola. [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.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Angola

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	N/A (1.6)	N/A (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	N/A (3.9)	N/A (4.4)
Drive-by download per 1,000 URLs (Worldwide)	N/A (0.7)	N/A (0.9)

Update service usage

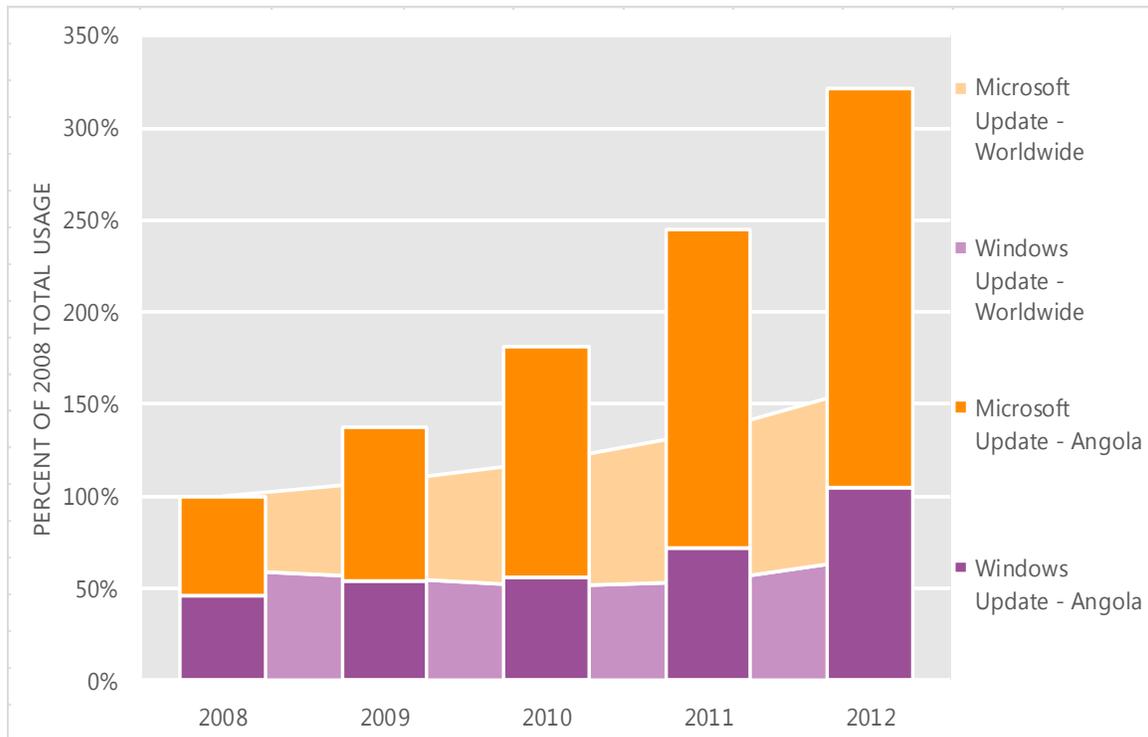
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Angola and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Angola over the last four years, indexed to the total usage for both services in Angola in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Angola was up 31.3 percent from 2011, and up 221.5 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Angola in 2012, 67.5 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Argentina

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Argentina in 2Q12 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.

Infection rate statistics for Argentina

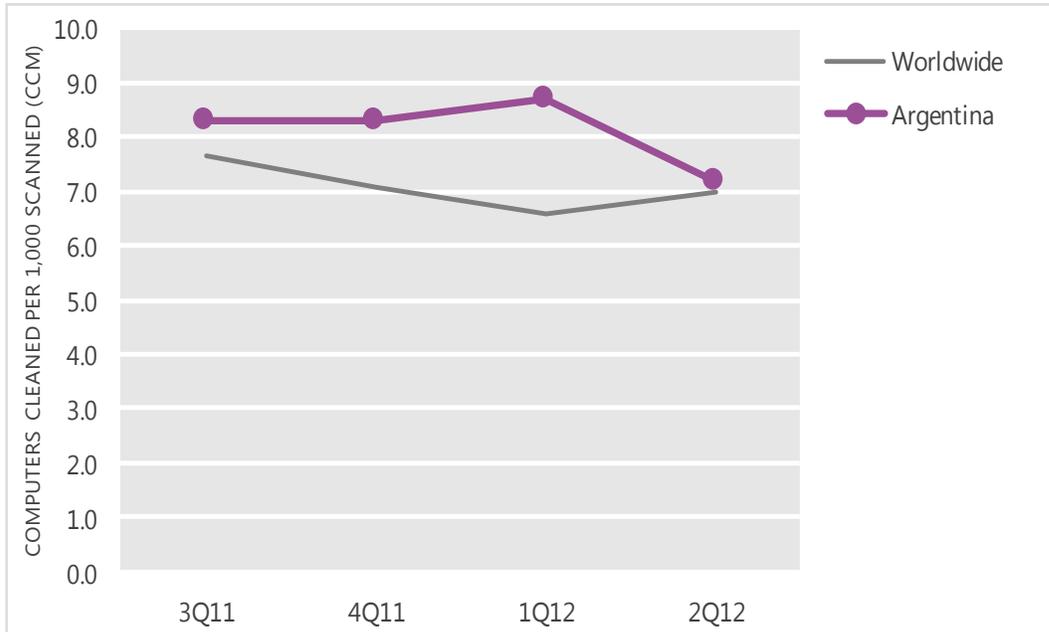
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	8.3	8.3	8.7	7.2
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

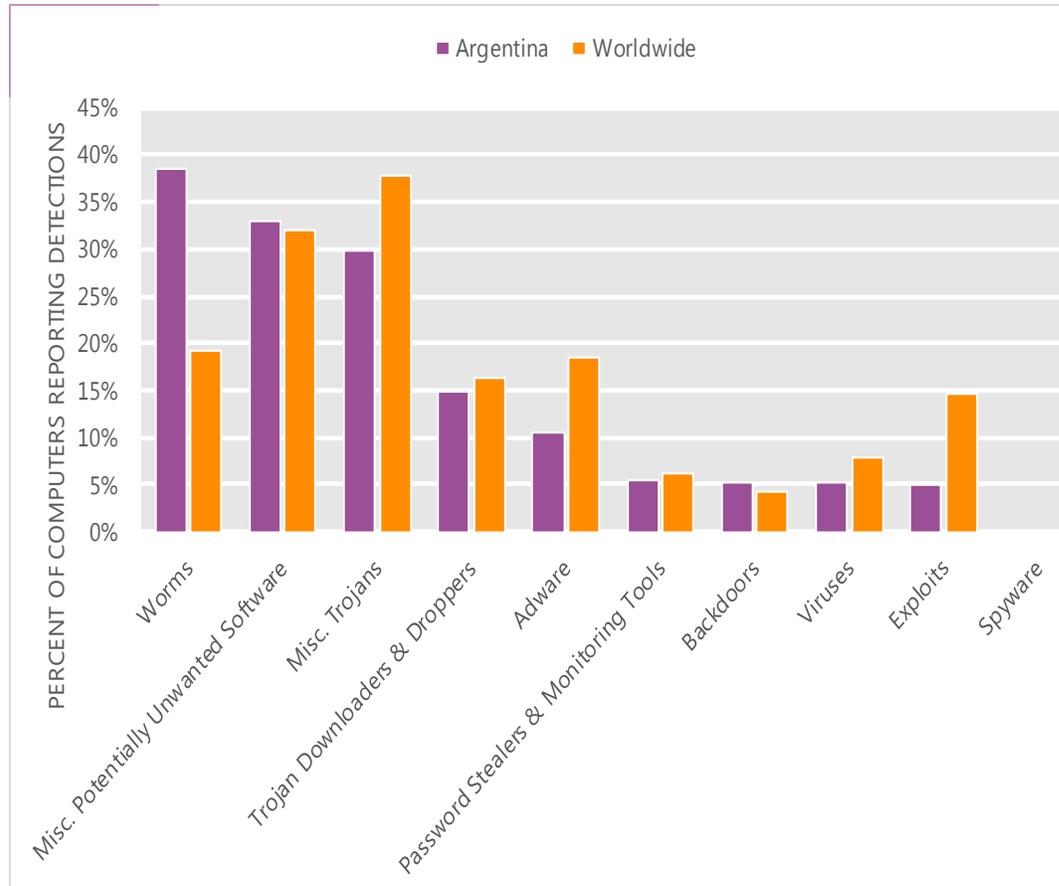
The MSRT detected malware on 7.2 of every 1,000 computers scanned in Argentina in 2Q12 (a CCM score of 7.2, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Argentina over the last four quarters, compared to the world as a whole.

CCM infection trends in Argentina and worldwide



Threat categories

Malware and potentially unwanted software categories in Argentina in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Argentina in 2Q12 was Worms. It affected 38.4 percent of all computers with detections there, down from 43.4 percent in 1Q12.
- The second most common category in Argentina in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 33.0 percent of all computers with detections there, down from 33.0 percent in 1Q12.
- The third most common category in Argentina in 2Q12 was Miscellaneous Trojans, which affected 29.8 percent of all computers with detections there, up from 24.2 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Argentina in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Dorkbot	Worms	16.0%
2	Win32/Keygen	Misc. Potentially Unwanted Software	10.9%
3	Win32/Autorun	Worms	9.7%
4	JS/Redirector	Misc. Trojans	6.8%
5	IRC/Prune	Worms	6.7%
6	ASX/Wimad	Trojan Downloaders & Droppers	6.4%
7	Win32/Conficker	Worms	6.1%
8	JS/Pornpop	Adware	4.4%
9	Win32/Sality	Viruses	3.4%
10	Win32/VBInject	Misc. Potentially Unwanted Software	3.1%

- The most common threat family in Argentina in 2Q12 was [Win32/Dorkbot](#), which affected 16.0 percent of computers with detections in Argentina. [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 second most common threat family in Argentina in 2Q12 was [Win32/Keygen](#), which affected 10.9 percent of computers with detections in Argentina. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The third most common threat family in Argentina in 2Q12 was [Win32/Autorun](#), which affected 9.7 percent of computers with detections in Argentina. [Win32/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 threat family in Argentina in 2Q12 was [JS/Redirector](#), which affected 6.8 percent of computers with detections in Argentina. [JS/Redirector](#) is a detection for a class of JavaScript trojans that redirect users to unexpected websites, which may contain drive-by downloads.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Argentina

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	1.04 (1.6)	1.30 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	1.88 (3.9)	2.25 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.27 (0.7)	0.58 (0.9)

Update service usage

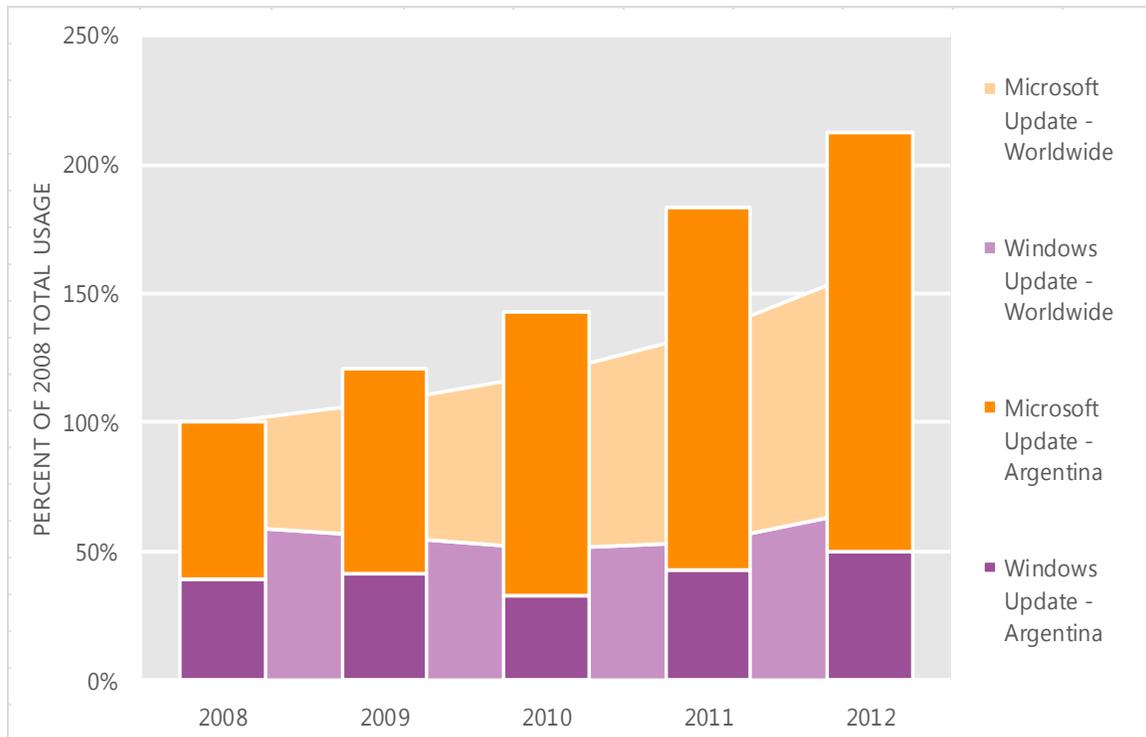
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Argentina and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Argentina over the last four years, indexed to the total usage for both services in Argentina in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Argentina was up 16.1 percent from 2011, and up 112.9 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Argentina in 2012, 76.6 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Australia

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Australia in 2Q12 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.

Infection rate statistics for Australia

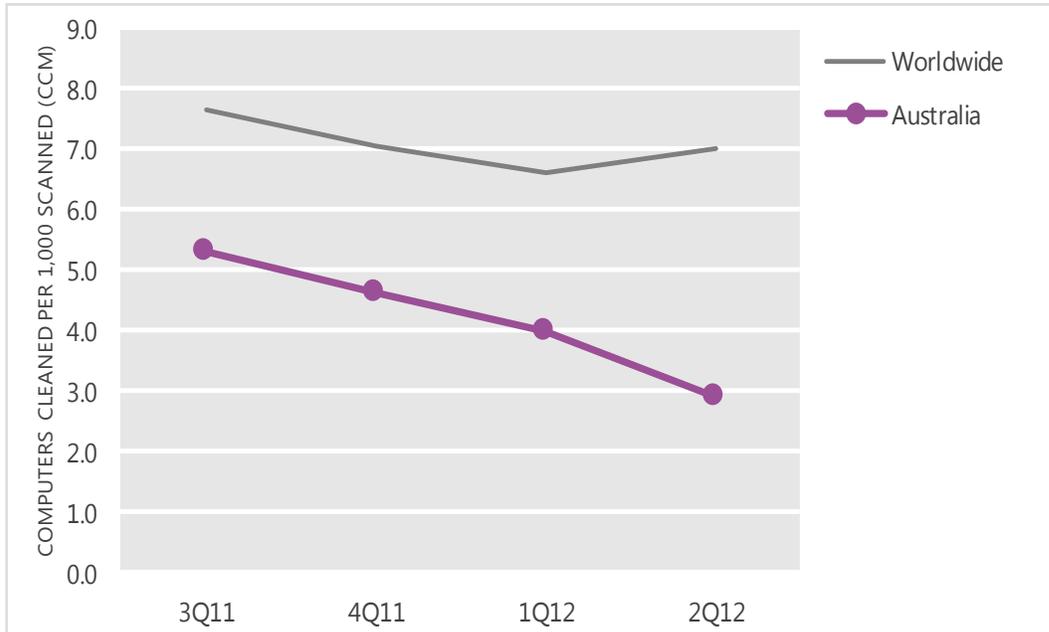
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	5.3	4.6	4.0	2.9
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

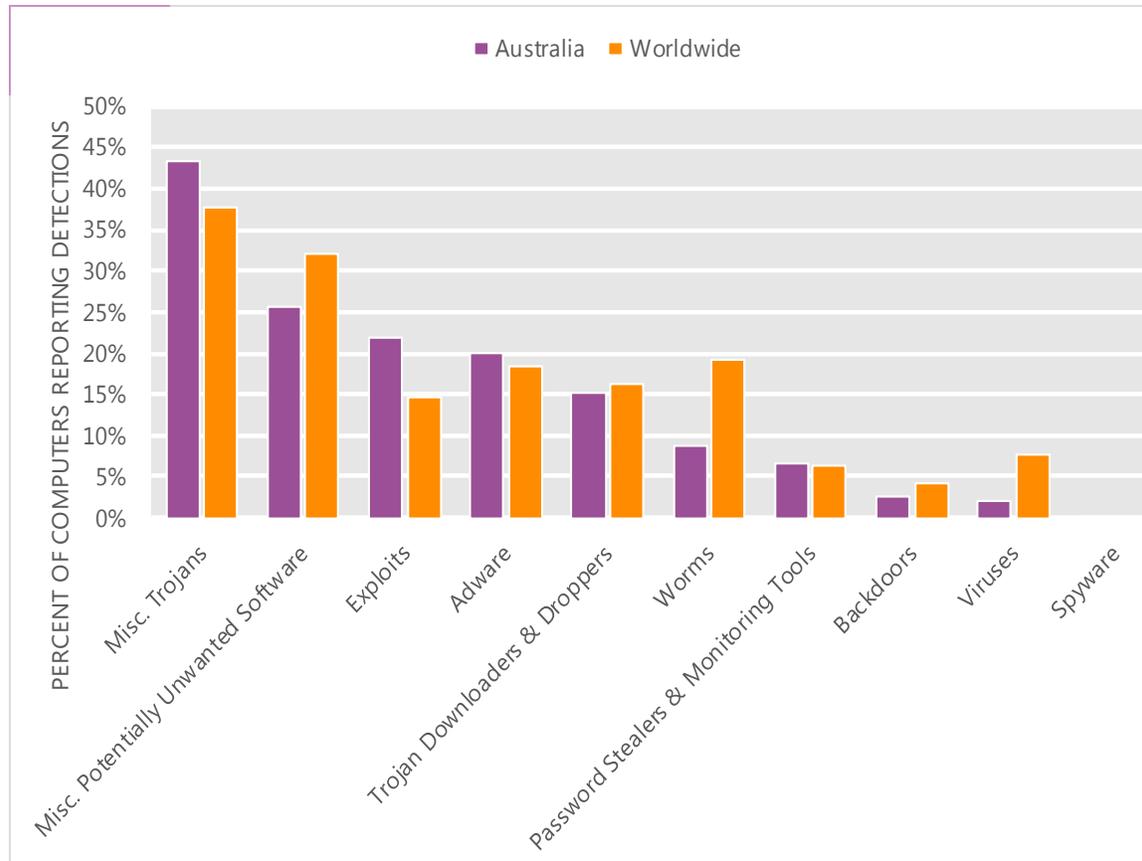
The MSRT detected malware on 2.9 of every 1,000 computers scanned in Australia in 2Q12 (a CCM score of 2.9, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Australia over the last four quarters, compared to the world as a whole.

CCM infection trends in Australia and worldwide



Threat categories

Malware and potentially unwanted software categories in Australia in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Australia in 2Q12 was Miscellaneous Trojans. It affected 43.3 percent of all computers with detections there, up from 41.2 percent in 1Q12.
- The second most common category in Australia in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 25.5 percent of all computers with detections there, up from 24.5 percent in 1Q12.
- The third most common category in Australia in 2Q12 was Exploits, which affected 21.9 percent of all computers with detections there, down from 22.4 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Australia in 2Q12

	Family	Most significant category	% of computers with detections
1	Java/Blacole	Exploits	9.5%
2	Win32/FakePAV	Misc. Trojans	8.6%
3	Win32/Keygen	Misc. Potentially Unwanted Software	8.5%
4	ASX/Wimad	Trojan Downloaders & Droppers	7.5%
5	JS/BlacoleRef	Misc. Trojans	7.4%
6	Win32/Hotbar	Adware	7.0%
7	Java/CVE-2012-0507	Exploits	6.6%
8	JS/Pornpop	Adware	6.5%
9	Win32/Winwebsec	Misc. Trojans	6.0%
10	JS/IframeRef	Misc. Trojans	5.5%

- The most common threat family in Australia in 2Q12 was [Java/Blacole](#), which affected 9.5 percent of computers with detections in Australia. [Java/Blacole](#) is an exploit pack, also known as Blackhole, that is installed on a compromised web server by an attacker and includes a number of exploits that target browser software. If a vulnerable computer browses a compromised website that contains the exploit pack, various malware may be downloaded and run.
- The second most common threat family in Australia in 2Q12 was [Win32/FakePAV](#), which affected 8.6 percent of computers with detections in Australia. [Win32/FakePAV](#) is a rogue security software family that often masquerades as Microsoft Security Essentials or other legitimate antimalware products.
- The third most common threat family in Australia in 2Q12 was [Win32/Keygen](#), which affected 8.5 percent of computers with detections in Australia. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The fourth most common threat family in Australia in 2Q12 was [ASX/Wimad](#), which affected 7.5 percent of computers with detections in Australia. [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.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Australia

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	1.70 (1.6)	1.98 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	2.39 (3.9)	2.65 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.33 (0.7)	0.69 (0.9)

Update service usage

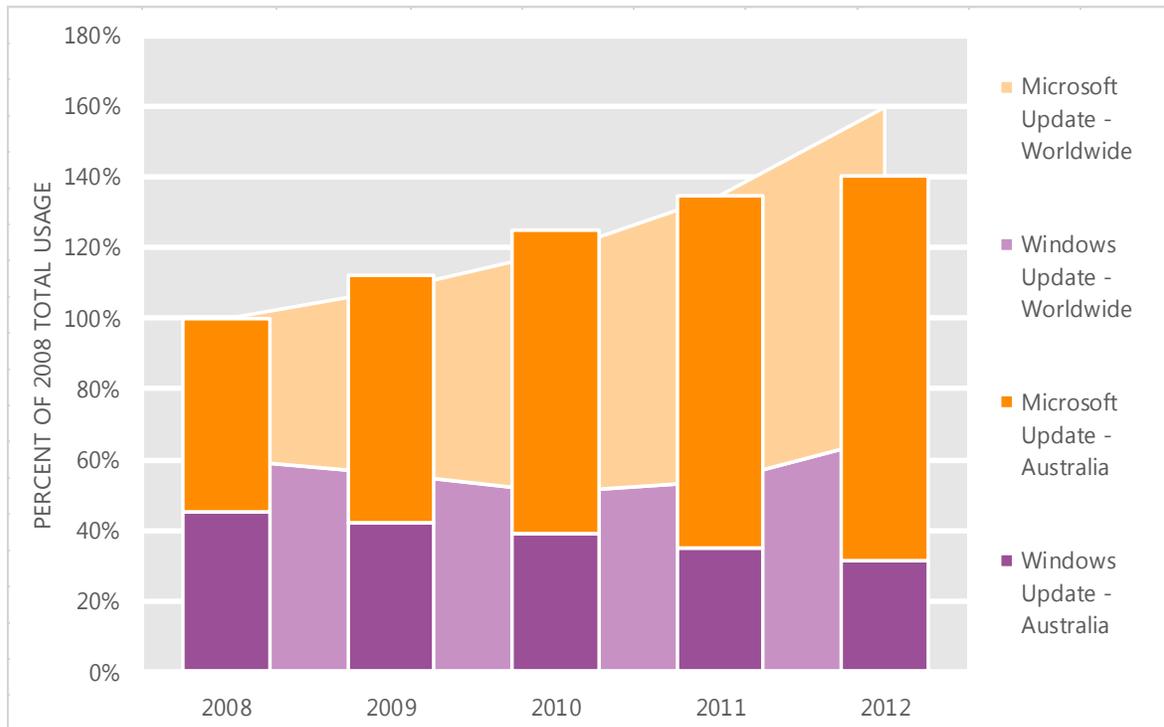
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Australia and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Australia over the last four years, indexed to the total usage for both services in Australia in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Australia was up 4.1 percent from 2011, and up 40.3 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Australia in 2012, 77.5 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Austria

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Austria in 2Q12 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.

Infection rate statistics for Austria

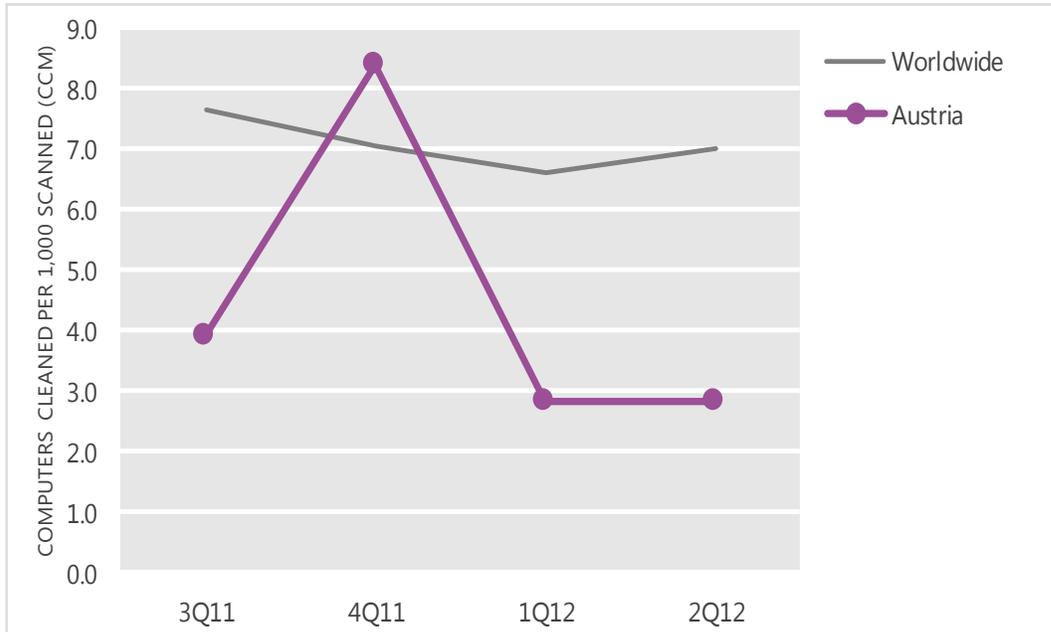
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	3.9	8.4	2.8	2.8
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

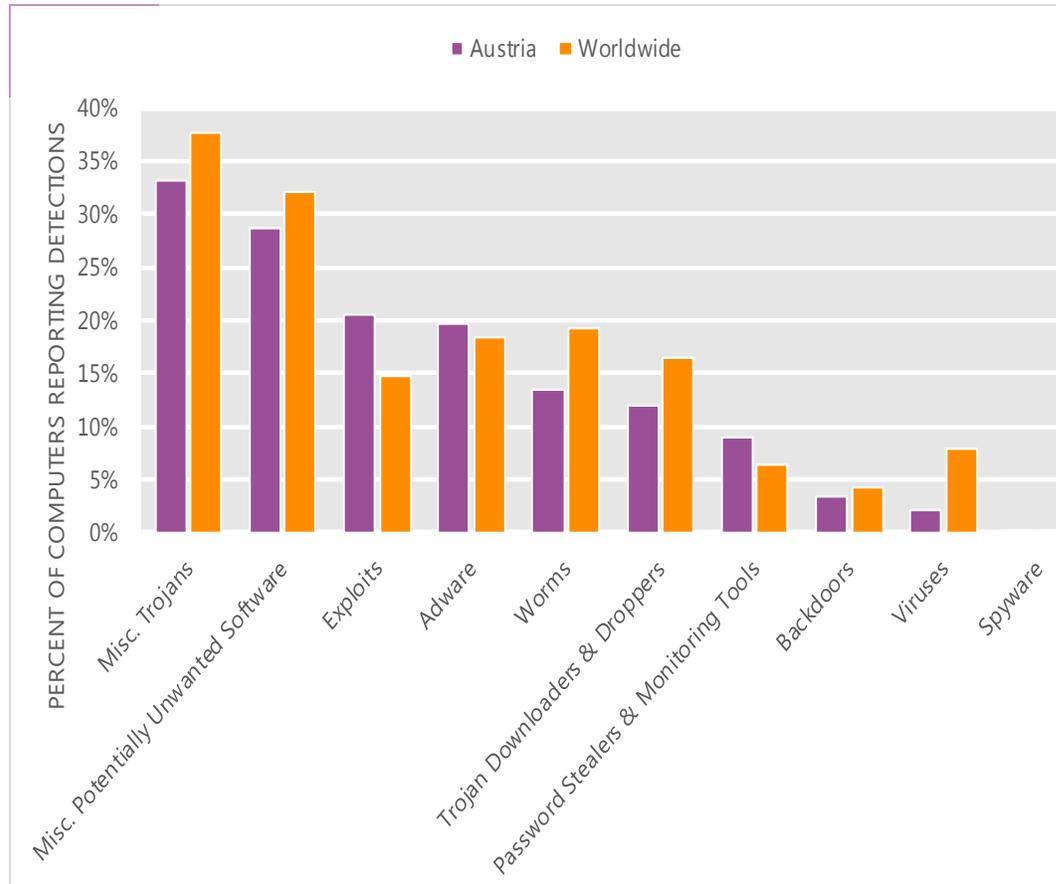
The MSRT detected malware on 2.8 of every 1,000 computers scanned in Austria in 2Q12 (a CCM score of 2.8, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Austria over the last four quarters, compared to the world as a whole.

CCM infection trends in Austria and worldwide



Threat categories

Malware and potentially unwanted software categories in Austria in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Austria in 2Q12 was Miscellaneous Trojans. It affected 33.3 percent of all computers with detections there, up from 29.8 percent in 1Q12.
- The second most common category in Austria in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 28.6 percent of all computers with detections there, down from 32.5 percent in 1Q12.
- The third most common category in Austria in 2Q12 was Exploits, which affected 20.4 percent of all computers with detections there, up from 15.5 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Austria in 2Q12

	Family	Most significant category	% of computers with detections
1	Java/Blacole	Exploits	13.1%
2	JS/Pornpop	Adware	11.4%
3	Win32/Keygen	Misc. Potentially Unwanted Software	10.3%
4	Java/CVE-2012-0507	Exploits	4.6%
5	JS/IframeRef	Misc. Trojans	4.4%
6	JS/BlacoleRef	Misc. Trojans	4.4%
7	ASX/Wimad	Trojan Downloaders & Droppers	3.8%
8	Win32/Banker	Password Stealers & Monitoring Tools	3.8%
9	Win32/Sirefef	Misc. Trojans	3.6%
10	Win32/Pdfjsc	Exploits	3.5%

- The most common threat family in Austria in 2Q12 was [Java/Blacole](#), which affected 13.1 percent of computers with detections in Austria. [Java/Blacole](#) is an exploit pack, also known as Blackhole, that is installed on a compromised web server by an attacker and includes a number of exploits that target browser software. If a vulnerable computer browses a compromised website that contains the exploit pack, various malware may be downloaded and run.
- The second most common threat family in Austria in 2Q12 was [JS/Pornpop](#), which affected 11.4 percent of computers with detections in Austria. [JS/Pornpop](#) is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The third most common threat family in Austria in 2Q12 was [Win32/Keygen](#), which affected 10.3 percent of computers with detections in Austria. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The fourth most common threat family in Austria in 2Q12 was [Java/CVE-2012-0507](#), which affected 4.6 percent of computers with detections in Austria. [Java/CVE-2012-0507](#) is a detection for a malicious Java applet that exploits the Java Runtime Environment (JRE) vulnerability described in CVE-2012-0507, addressed by an Oracle security update in February 2012.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Austria

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	0.86 (1.6)	1.25 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	2.74 (3.9)	3.21 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.03 (0.7)	0.12 (0.9)

Update service usage

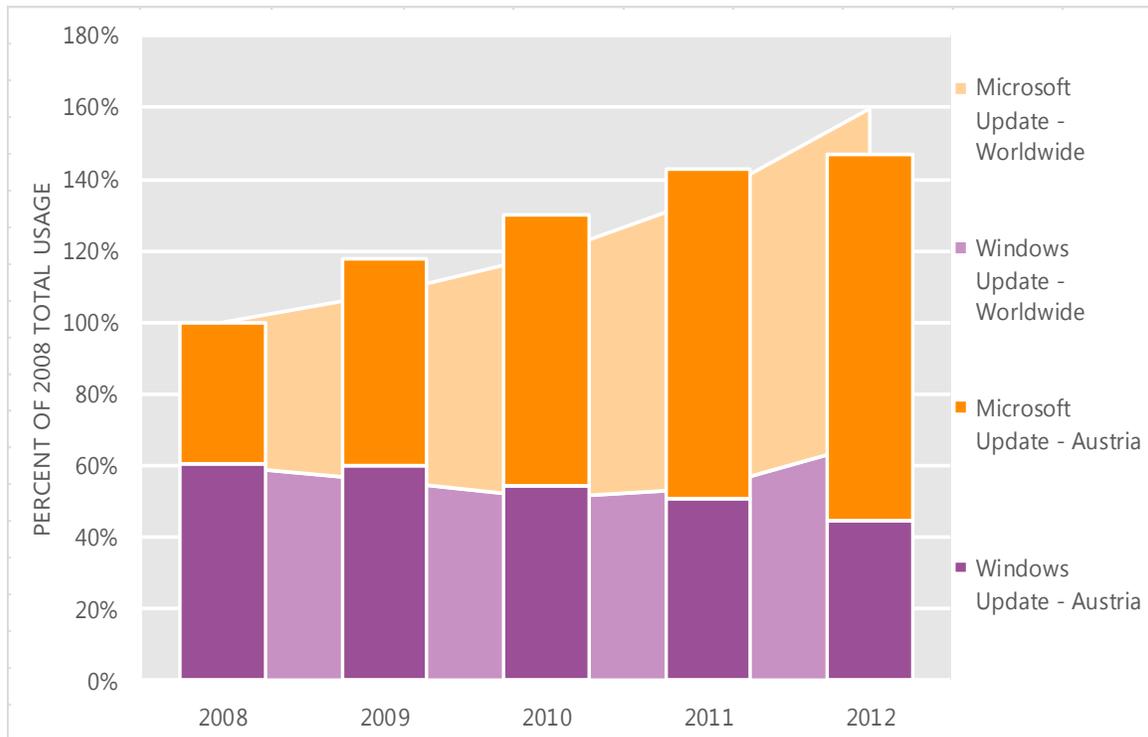
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Austria and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Austria over the last four years, indexed to the total usage for both services in Austria in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Austria was up 2.8 percent from 2011, and up 46.7 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Austria in 2012, 69.5 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Bahamas, The

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in the Bahamas in 2Q12 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.

Infection rate statistics for the Bahamas

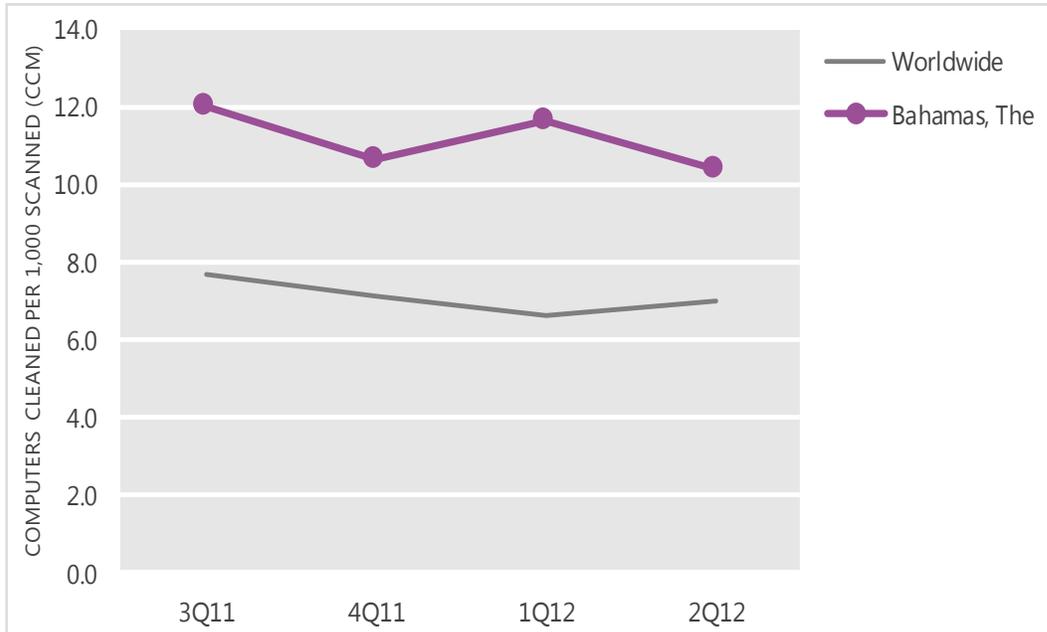
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	12.0	10.6	11.6	10.4
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

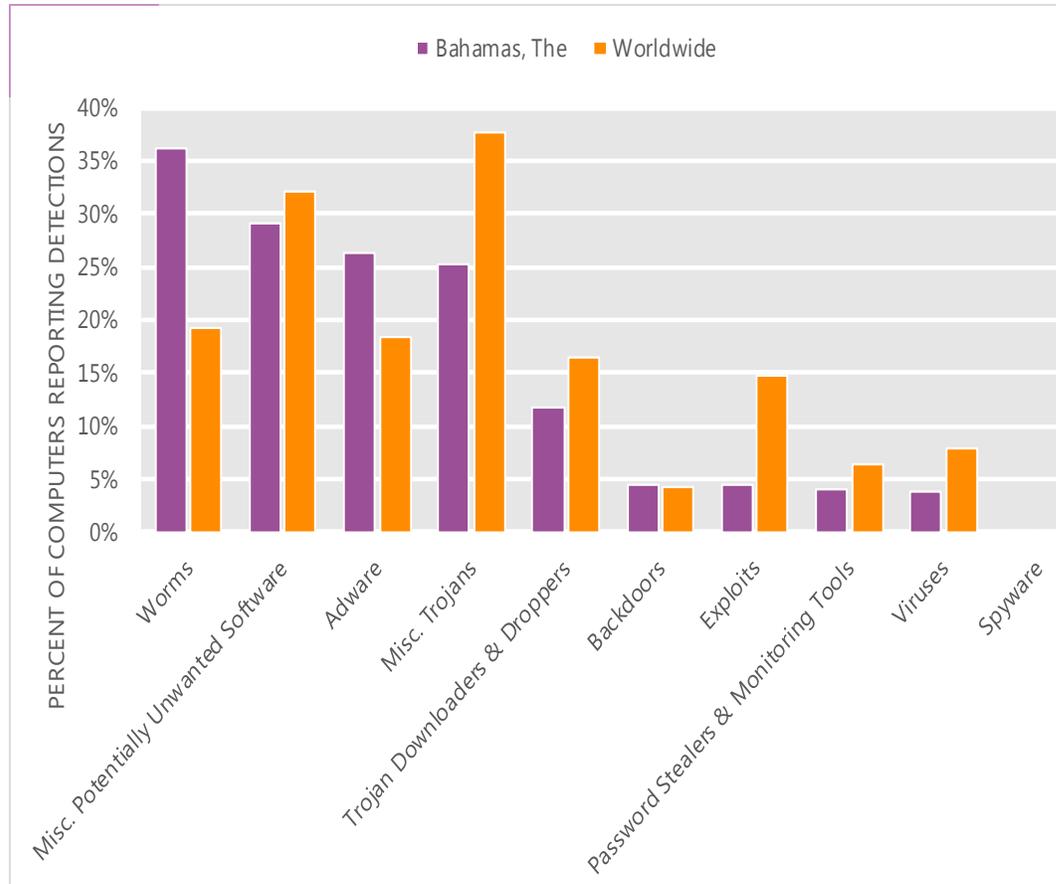
The MSRT detected malware on 10.4 of every 1,000 computers scanned in the Bahamas in 2Q12 (a CCM score of 10.4, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for the Bahamas over the last four quarters, compared to the world as a whole.

CCM infection trends in the Bahamas and worldwide



Threat categories

Malware and potentially unwanted software categories in the Bahamas in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in the Bahamas in 2Q12 was Worms. It affected 36.3 percent of all computers with detections there, down from 36.7 percent in 1Q12.
- The second most common category in the Bahamas in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 29.1 percent of all computers with detections there, up from 28.7 percent in 1Q12.
- The third most common category in the Bahamas in 2Q12 was Adware, which affected 26.2 percent of all computers with detections there, down from 33.2 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in the Bahamas in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Hotbar	Adware	17.9%
2	Win32/Zwangi	Misc. Potentially Unwanted Software	13.0%
3	Win32/Autorun	Worms	12.1%
4	Win32/Vobfus	Worms	11.1%
5	Win32/Dorkbot	Worms	8.4%
6	ASX/Wimad	Trojan Downloaders & Droppers	6.4%
7	JS/IframeRef	Misc. Trojans	5.4%
8	Win32/Hamweq	Worms	4.9%
9	Win32/Keygen	Misc. Potentially Unwanted Software	4.9%
10	JS/Pornpop	Adware	4.5%

- The most common threat family in the Bahamas in 2Q12 was [Win32/Hotbar](#), which affected 17.9 percent of computers with detections in the Bahamas. [Win32/Hotbar](#) is adware that displays a dynamic toolbar and targeted pop-up ads based on its monitoring of web-browsing activity.
- The second most common threat family in the Bahamas in 2Q12 was [Win32/Zwangi](#), which affected 13.0 percent of computers with detections in the Bahamas. [Win32/Zwangi](#) is a program that runs as a service in the background and modifies web browser settings to visit a particular website.
- The third most common threat family in the Bahamas in 2Q12 was [Win32/Autorun](#), which affected 12.1 percent of computers with detections in the Bahamas. [Win32/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 threat family in the Bahamas in 2Q12 was [Win32/Vobfus](#), which affected 11.1 percent of computers with detections in the Bahamas. [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.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for the Bahamas

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	N/A (1.6)	N/A (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	N/A (3.9)	N/A (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.17 (0.7)	0.26 (0.9)

Update service usage

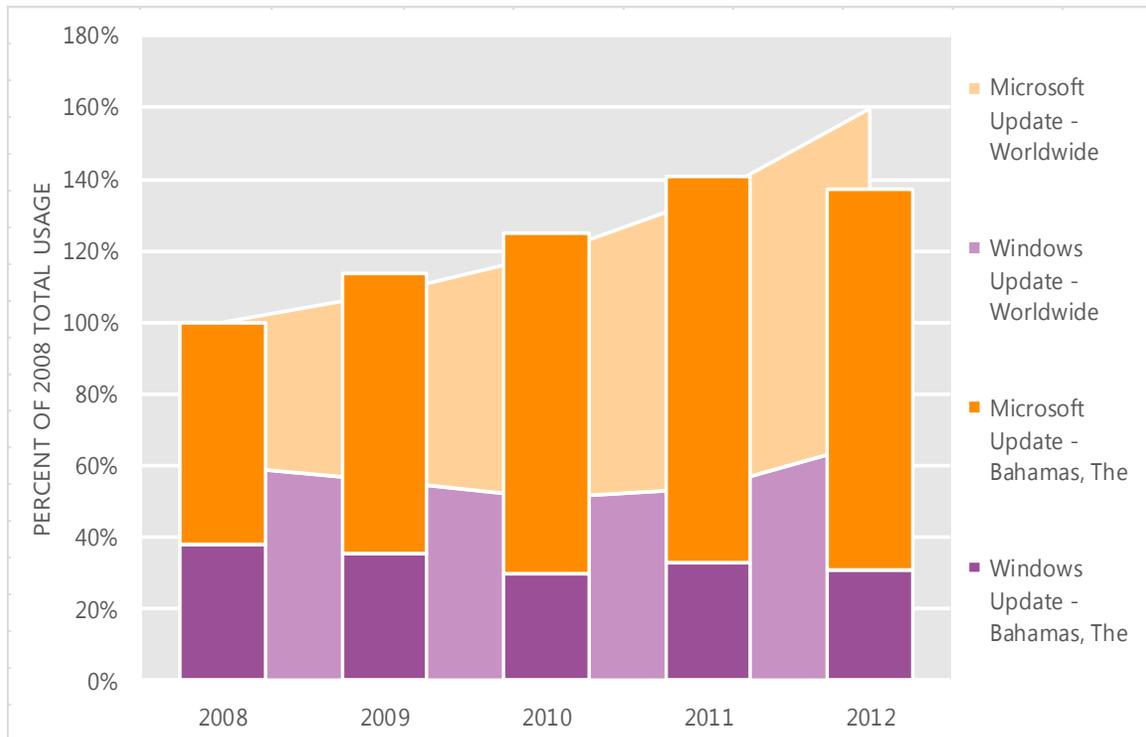
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in the Bahamas and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in the Bahamas over the last four years, indexed to the total usage for both services in the Bahamas in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in the Bahamas was down 2.7 percent from 2011, and up 37.1 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in the Bahamas in 2012, 77.7 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Bahrain

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Bahrain in 2Q12 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.

Infection rate statistics for Bahrain

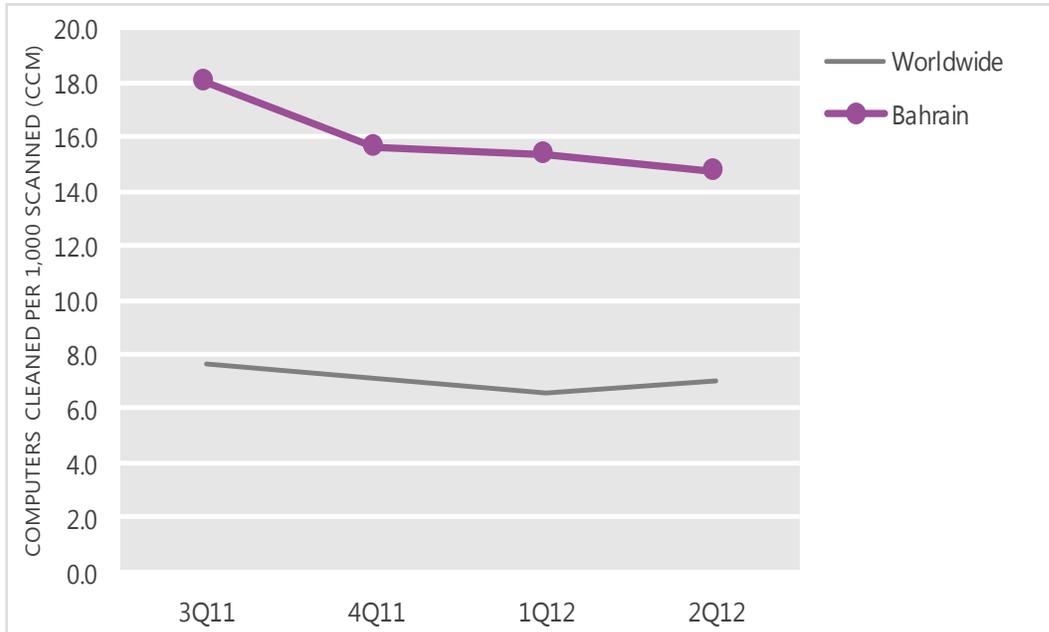
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	18.0	15.6	15.4	14.7
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

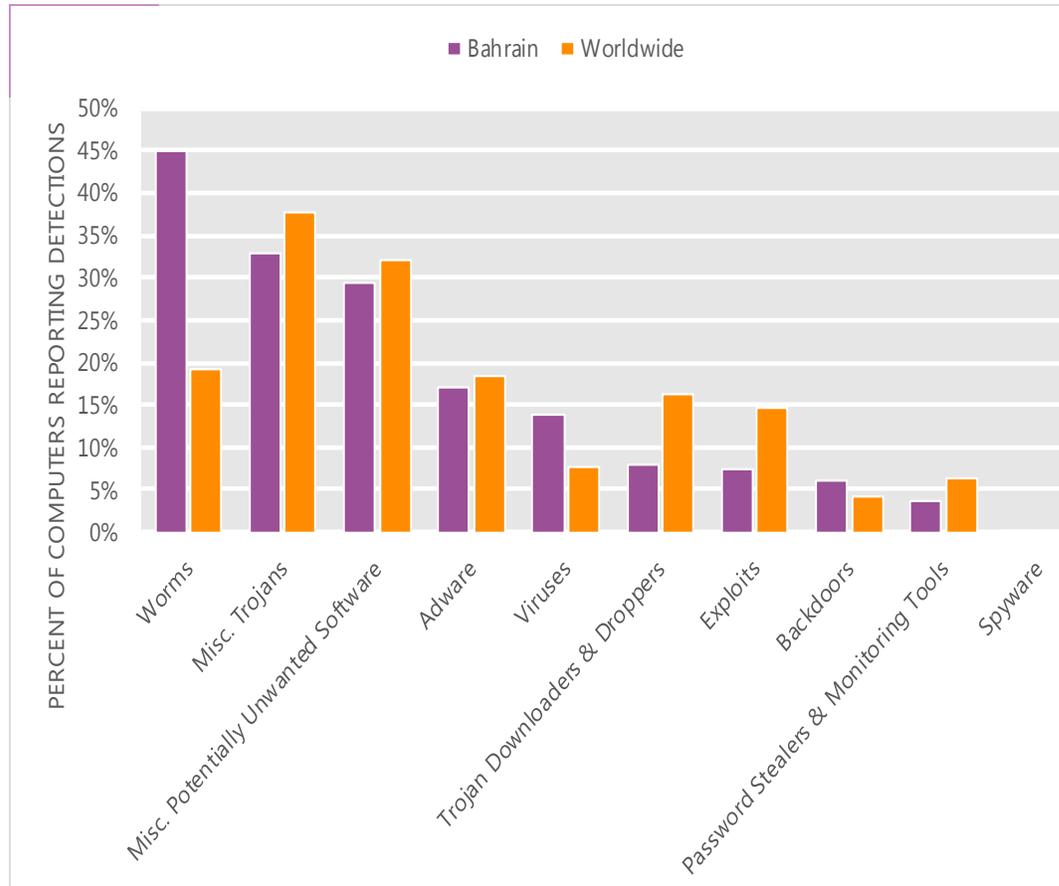
The MSRT detected malware on 14.7 of every 1,000 computers scanned in Bahrain in 2Q12 (a CCM score of 14.7, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Bahrain over the last four quarters, compared to the world as a whole.

CCM infection trends in Bahrain and worldwide



Threat categories

Malware and potentially unwanted software categories in Bahrain in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Bahrain in 2Q12 was Worms. It affected 44.9 percent of all computers with detections there, down from 45.0 percent in 1Q12.
- The second most common category in Bahrain in 2Q12 was Miscellaneous Trojans. It affected 33.0 percent of all computers with detections there, up from 32.8 percent in 1Q12.
- The third most common category in Bahrain in 2Q12 was Miscellaneous Potentially Unwanted Software, which affected 29.4 percent of all computers with detections there, down from 30.1 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Bahrain in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Nuqel	Worms	16.5%
2	Win32/Autorun	Worms	15.2%
3	Win32/Dorkbot	Worms	11.6%
4	Win32/Keygen	Misc. Potentially Unwanted Software	10.3%
5	Win32/Sality	Viruses	8.5%
6	JS/Paypopup	Adware	7.2%
7	Win32/Rimecud	Worms	6.4%
8	Win32/Vobfus	Worms	5.3%
9	Win32/Hotbar	Adware	5.0%
10	Win32/Ramnit	Misc. Trojans	4.6%

- The most common threat family in Bahrain in 2Q12 was [Win32/Nuqel](#), which affected 16.5 percent of computers with detections in Bahrain. [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 second most common threat family in Bahrain in 2Q12 was [Win32/Autorun](#), which affected 15.2 percent of computers with detections in Bahrain. [Win32/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 threat family in Bahrain in 2Q12 was [Win32/Dorkbot](#), which affected 11.6 percent of computers with detections in Bahrain. [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 in Bahrain in 2Q12 was [Win32/Keygen](#), which affected 10.3 percent of computers with detections in Bahrain. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Bahrain

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	0.53 (1.6)	N/A (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	0.53 (3.9)	2.12 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	N/A (0.7)	N/A (0.9)

Update service usage

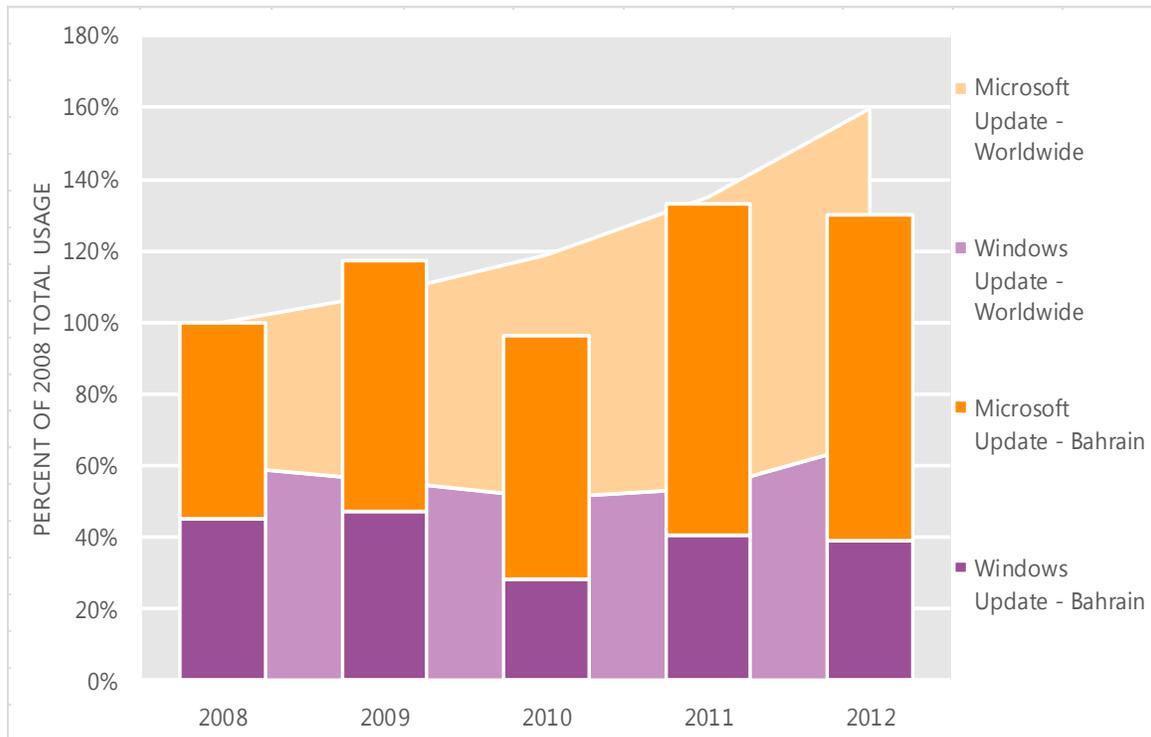
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Bahrain and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Bahrain over the last four years, indexed to the total usage for both services in Bahrain in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Bahrain was down 2.5 percent from 2011, and up 29.9 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Bahrain in 2012, 69.9 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Bangladesh

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Bangladesh in 2Q12 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.

Infection rate statistics for Bangladesh

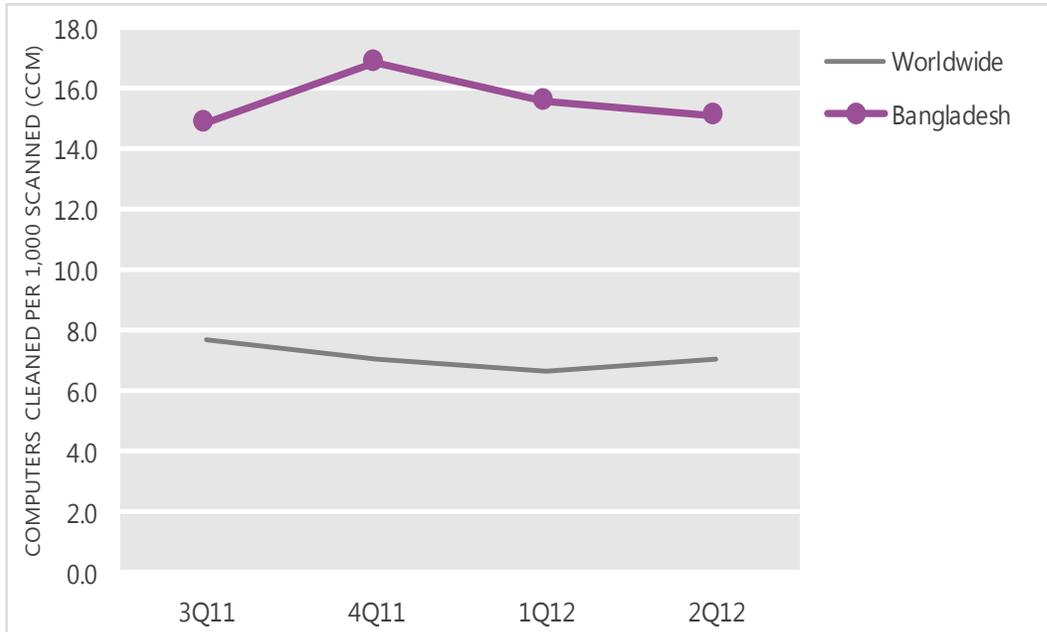
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	14.9	16.9	15.6	15.1
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

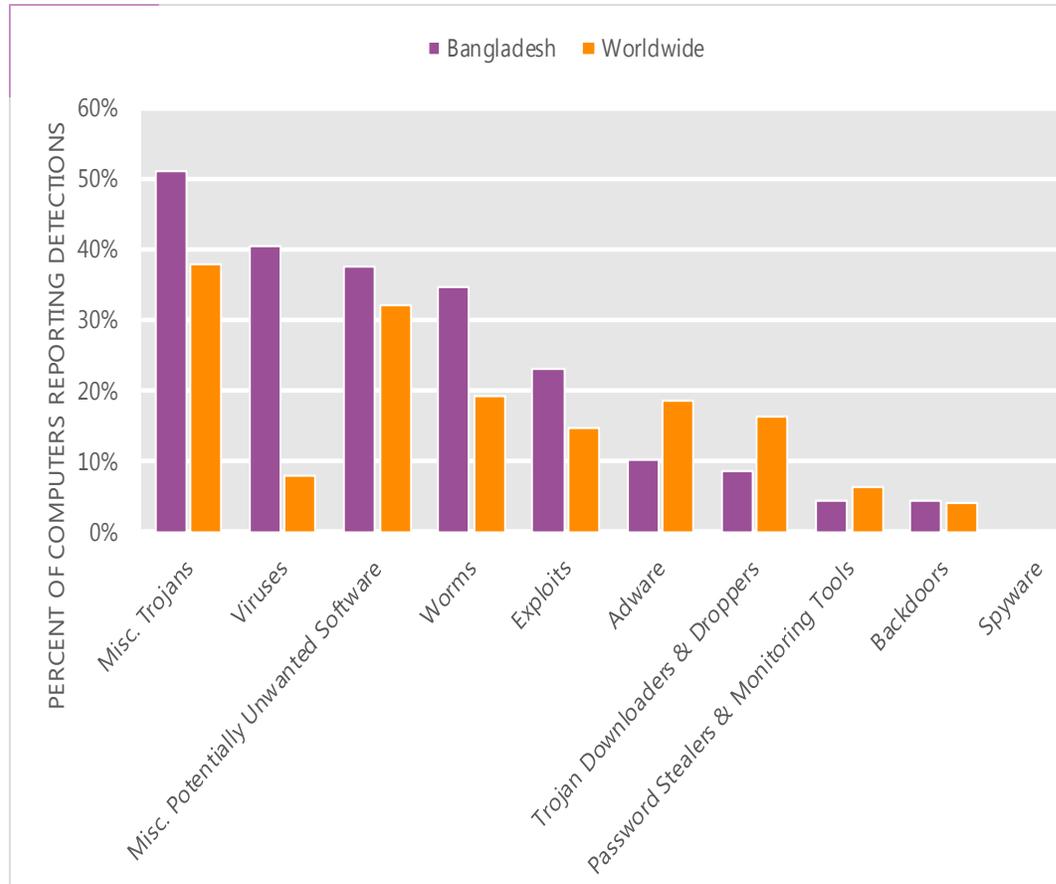
The MSRT detected malware on 15.1 of every 1,000 computers scanned in Bangladesh in 2Q12 (a CCM score of 15.1, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Bangladesh over the last four quarters, compared to the world as a whole.

CCM infection trends in Bangladesh and worldwide



Threat categories

Malware and potentially unwanted software categories in Bangladesh in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Bangladesh in 2Q12 was Miscellaneous Trojans. It affected 51.1 percent of all computers with detections there, down from 53.0 percent in 1Q12.
- The second most common category in Bangladesh in 2Q12 was Viruses. It affected 40.5 percent of all computers with detections there, down from 41.3 percent in 1Q12.
- The third most common category in Bangladesh in 2Q12 was Miscellaneous Potentially Unwanted Software, which affected 37.6 percent of all computers with detections there, up from 36.8 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Bangladesh in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Ramnit	Misc. Trojans	39.2%
2	Win32/Autorun	Worms	22.9%
3	Win32/CplLnk	Exploits	20.6%
4	Win32/Keygen	Misc. Potentially Unwanted Software	20.0%
5	Win32/Sality	Viruses	17.8%
6	Win32/Rimecud	Worms	10.8%
7	Win32/Conficker	Worms	9.2%
8	Win32/Virut	Viruses	8.1%
9	Win32/Dorkbot	Worms	6.4%
10	Win32/VB	Worms	5.6%

- The most common threat family in Bangladesh in 2Q12 was [Win32/Ramnit](#), which affected 39.2 percent of computers with detections in Bangladesh. [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 in Bangladesh in 2Q12 was [Win32/Autorun](#), which affected 22.9 percent of computers with detections in Bangladesh. [Win32/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 threat family in Bangladesh in 2Q12 was [Win32/CplLnk](#), which affected 20.6 percent of computers with detections in Bangladesh. [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 threat family in Bangladesh in 2Q12 was [Win32/Keygen](#), which affected 20.0 percent of computers with detections in Bangladesh. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Bangladesh

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	2.44 (1.6)	0.81 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	2.04 (3.9)	1.22 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.61 (0.7)	0.84 (0.9)

Update service usage

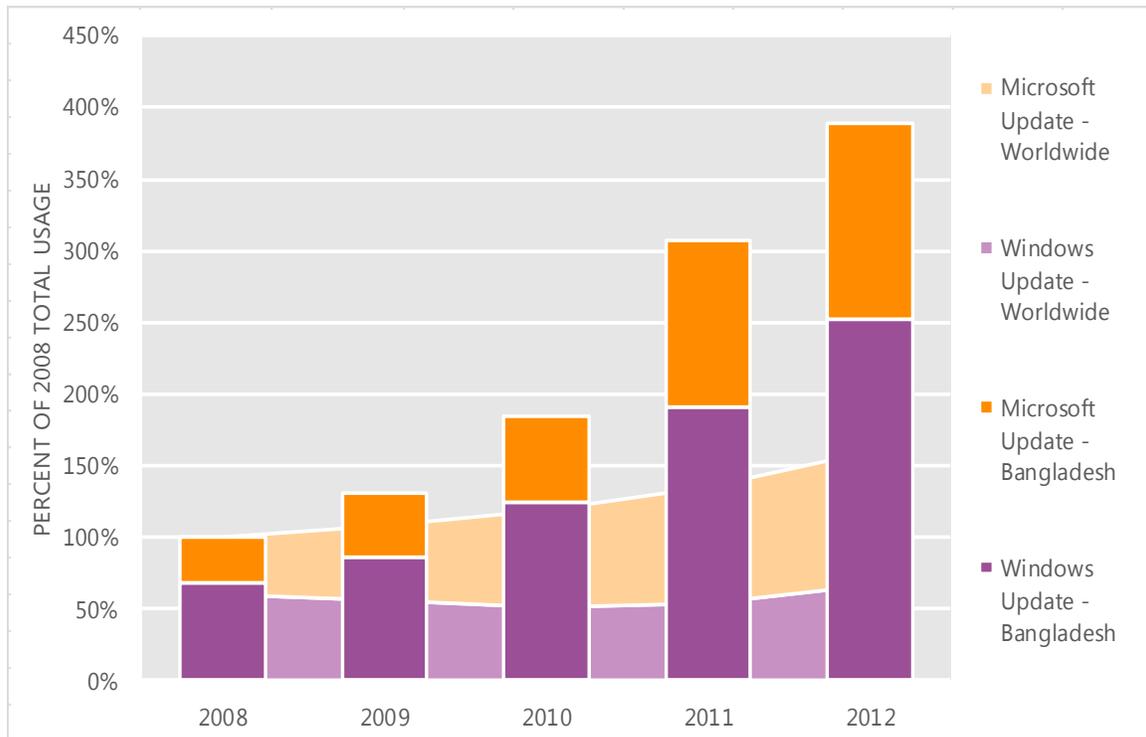
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Bangladesh and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Bangladesh over the last four years, indexed to the total usage for both services in Bangladesh in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Bangladesh was up 26.8 percent from 2011, and up 288.7 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Bangladesh in 2012, 35.2 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Belarus

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Belarus in 2Q12 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.

Infection rate statistics for Belarus

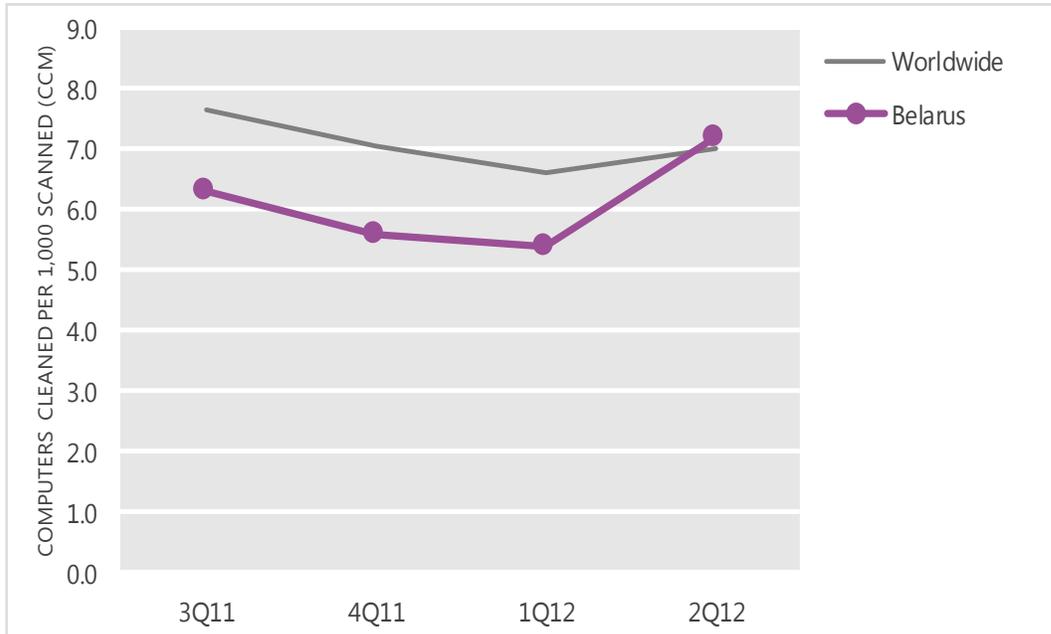
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	6.3	5.6	5.4	7.2
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

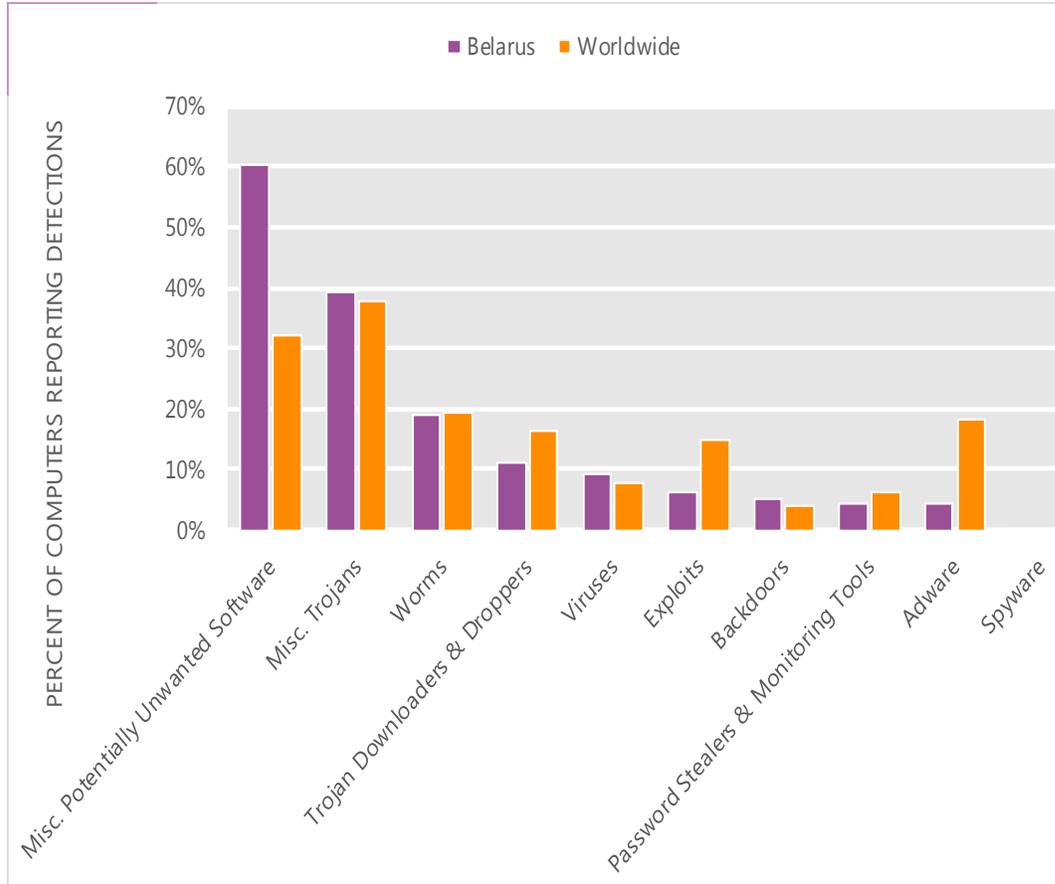
The MSRT detected malware on 7.2 of every 1,000 computers scanned in Belarus in 2Q12 (a CCM score of 7.2, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Belarus over the last four quarters, compared to the world as a whole.

CCM infection trends in Belarus and worldwide



Threat categories

Malware and potentially unwanted software categories in Belarus in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Belarus in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 60.3 percent of all computers with detections there, down from 65.9 percent in 1Q12.
- The second most common category in Belarus in 2Q12 was Miscellaneous Trojans. It affected 39.2 percent of all computers with detections there, up from 34.0 percent in 1Q12.
- The third most common category in Belarus in 2Q12 was Worms, which affected 19.1 percent of all computers with detections there, up from 17.5 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Belarus in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Pameseg	Misc. Potentially Unwanted Software	35.3%
2	Win32/Keygen	Misc. Potentially Unwanted Software	15.4%
3	Win32/Dorkbot	Worms	11.2%
4	Win32/Obfuscator	Misc. Potentially Unwanted Software	7.8%
5	Win32/Vundo	Misc. Trojans	7.1%
6	JS/IframeRef	Misc. Trojans	5.4%
7	Win32/Dynamer	Misc. Trojans	5.0%
8	Win32/Autorun	Worms	4.9%
9	Win32/Rimecud	Worms	3.7%
10	Win32/Ramnit	Misc. Trojans	3.3%

- The most common threat family in Belarus in 2Q12 was [Win32/Pameseg](#), which affected 35.3 percent of computers with detections in Belarus. [Win32/Pameseg](#) is a fake program installer that requires the user to send SMS messages to a premium number to successfully install certain programs.
- The second most common threat family in Belarus in 2Q12 was [Win32/Keygen](#), which affected 15.4 percent of computers with detections in Belarus. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The third most common threat family in Belarus in 2Q12 was [Win32/Dorkbot](#), which affected 11.2 percent of computers with detections in Belarus. [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 in Belarus in 2Q12 was [Win32/Obfuscator](#), which affected 7.8 percent of computers with detections in Belarus. [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.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Belarus

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	7.30 (1.6)	9.61 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	5.77 (3.9)	8.84 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	1.41 (0.7)	1.09 (0.9)

Update service usage

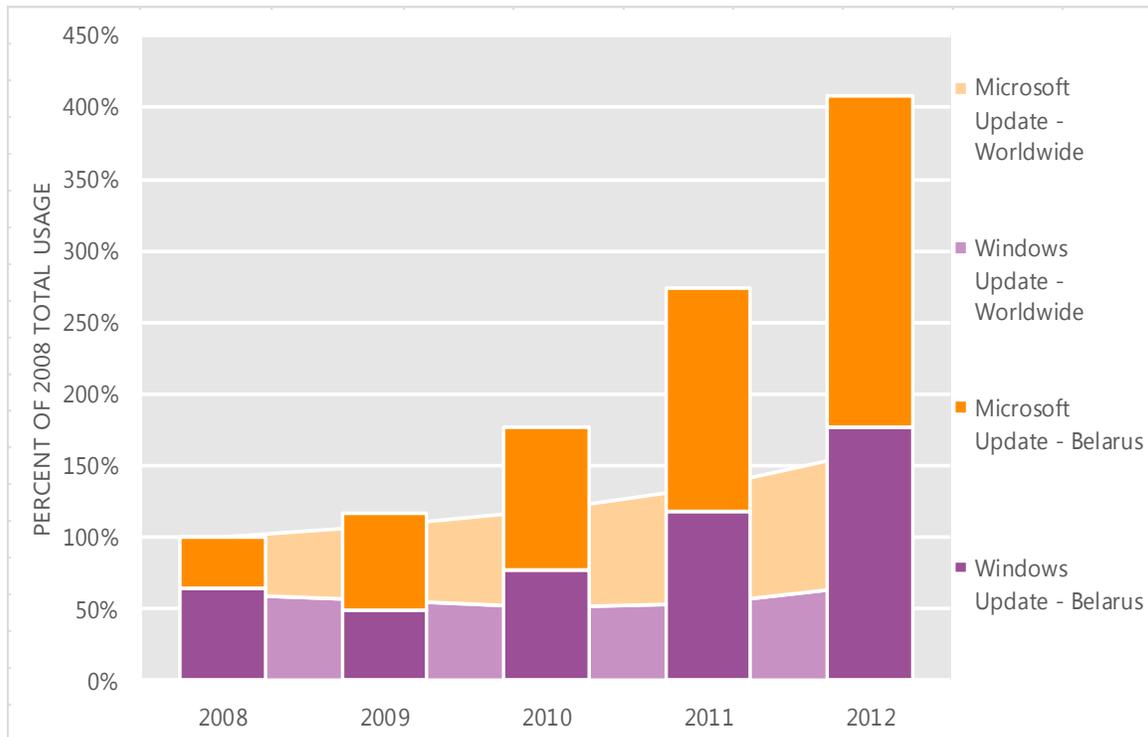
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Belarus and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Belarus over the last four years, indexed to the total usage for both services in Belarus in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Belarus was up 48.5 percent from 2011, and up 307.7 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Belarus in 2012, 56.6 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Belgium

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Belgium in 2Q12 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.

Infection rate statistics for Belgium

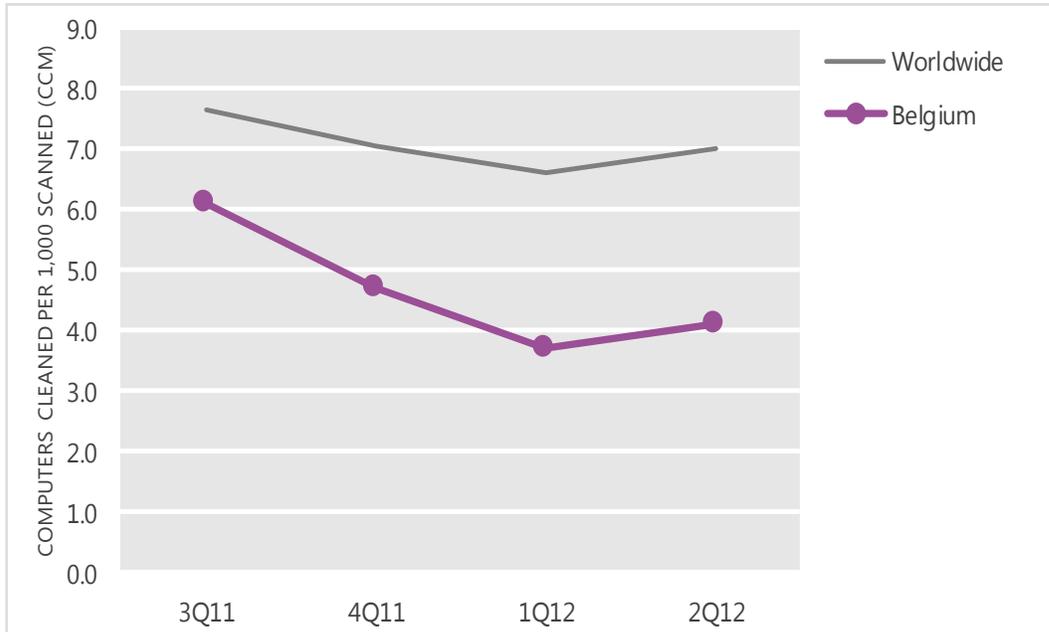
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	6.1	4.7	3.7	4.1
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

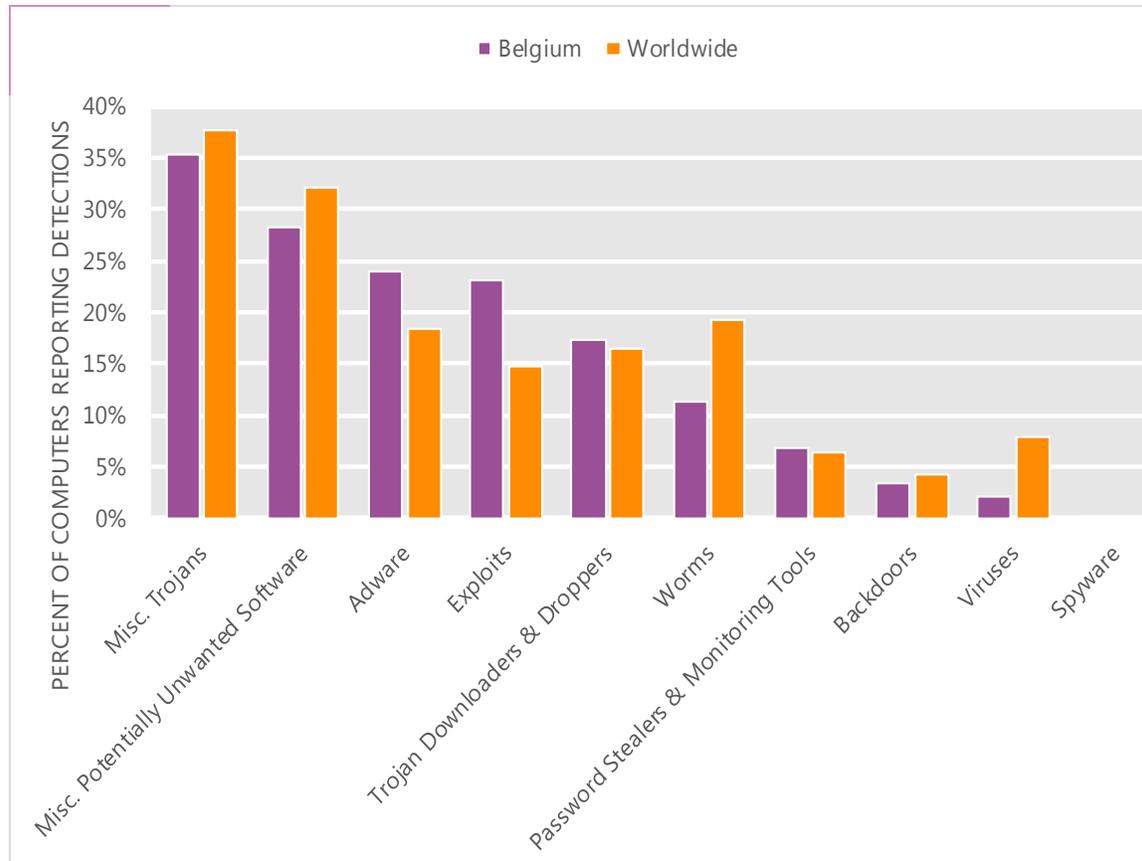
The MSRT detected malware on 4.1 of every 1,000 computers scanned in Belgium in 2Q12 (a CCM score of 4.1, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Belgium over the last four quarters, compared to the world as a whole.

CCM infection trends in Belgium and worldwide



Threat categories

Malware and potentially unwanted software categories in Belgium in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Belgium in 2Q12 was Miscellaneous Trojans. It affected 35.4 percent of all computers with detections there, up from 31.1 percent in 1Q12.
- The second most common category in Belgium in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 28.2 percent of all computers with detections there, down from 30.9 percent in 1Q12.
- The third most common category in Belgium in 2Q12 was Adware, which affected 24.0 percent of all computers with detections there, down from 33.7 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Belgium in 2Q12

	Family	Most significant category	% of computers with detections
1	Java/Blacole	Exploits	15.6%
2	JS/Pornpop	Adware	9.6%
3	ASX/Wimad	Trojan Downloaders & Droppers	9.3%
4	Win32/Hotbar	Adware	8.7%
5	Win32/Keygen	Misc. Potentially Unwanted Software	8.7%
6	Java/CVE-2012-0507	Exploits	6.0%
7	JS/IframeRef	Misc. Trojans	5.4%
8	JS/BlacoleRef	Misc. Trojans	4.8%
9	Win32/Zwangi	Misc. Potentially Unwanted Software	4.2%
10	Win32/Sirefef	Misc. Trojans	4.1%

- The most common threat family in Belgium in 2Q12 was [Java/Blacole](#), which affected 15.6 percent of computers with detections in Belgium. [Java/Blacole](#) is an exploit pack, also known as Blackhole, that is installed on a compromised web server by an attacker and includes a number of exploits that target browser software. If a vulnerable computer browses a compromised website that contains the exploit pack, various malware may be downloaded and run.
- The second most common threat family in Belgium in 2Q12 was [JS/Pornpop](#), which affected 9.6 percent of computers with detections in Belgium. [JS/Pornpop](#) is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The third most common threat family in Belgium in 2Q12 was [ASX/Wimad](#), which affected 9.3 percent of computers with detections in Belgium. [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 threat family in Belgium in 2Q12 was [Win32/Hotbar](#), which affected 8.7 percent of computers with detections in Belgium. [Win32/Hotbar](#) is adware that displays a dynamic toolbar and targeted pop-up ads based on its monitoring of web-browsing activity.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Belgium

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	0.97 (1.6)	1.03 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	1.53 (3.9)	2.31 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.08 (0.7)	0.31 (0.9)

Update service usage

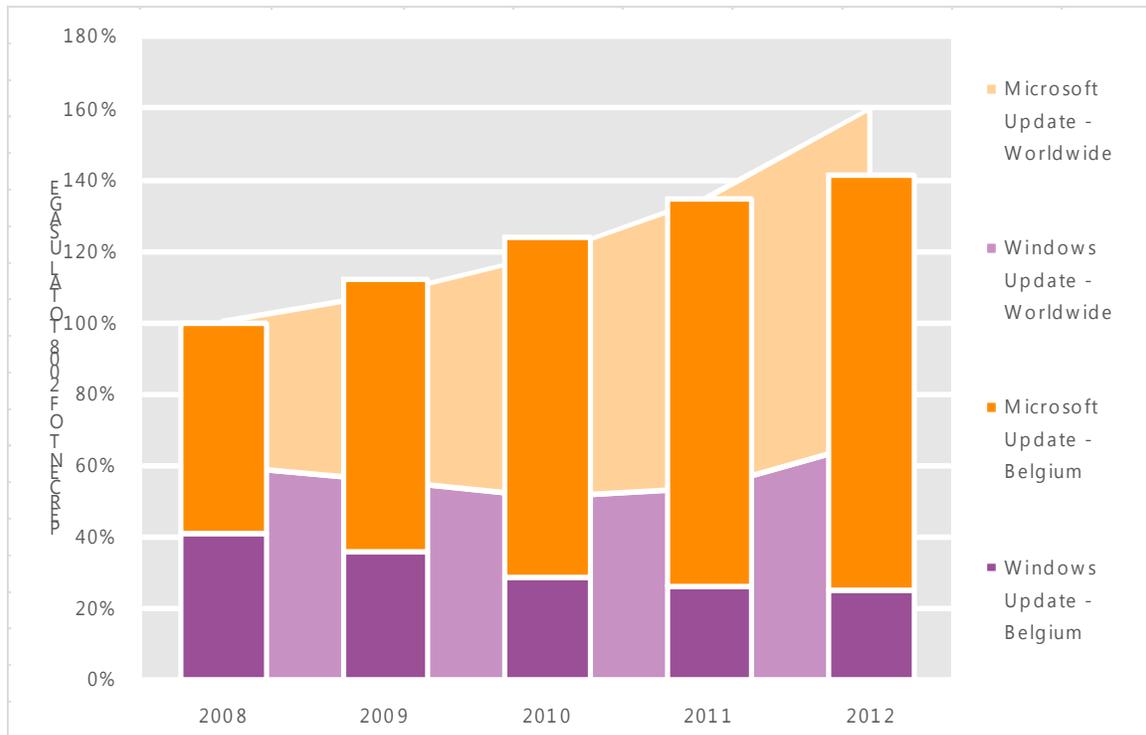
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Belgium and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Belgium over the last four years, indexed to the total usage for both services in Belgium in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Belgium was up 4.9 percent from 2011, and up 41.3 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Belgium in 2012, 82.3 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Bolivia

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Bolivia in 2Q12 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.

Infection rate statistics for Bolivia

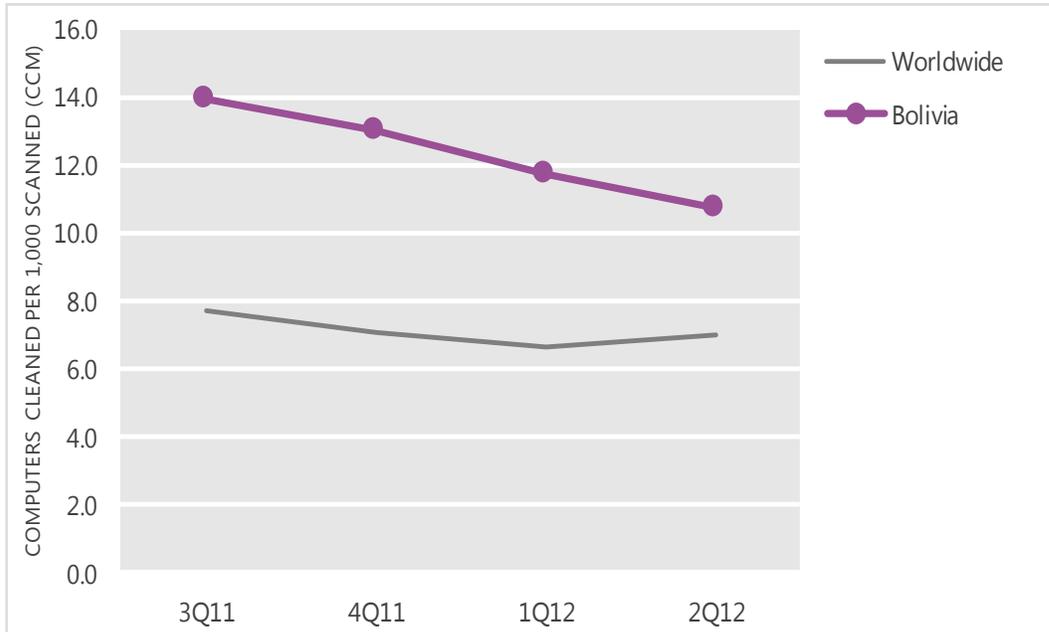
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	13.9	13.0	11.7	10.7
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

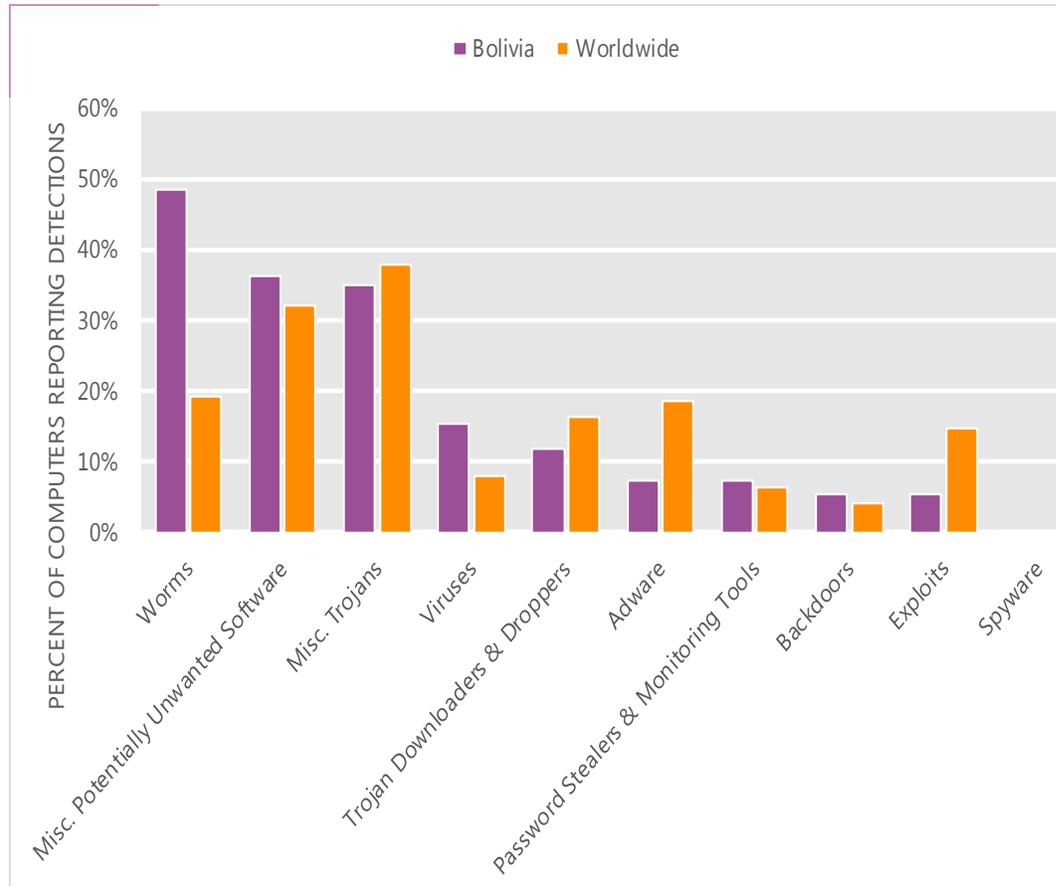
The MSRT detected malware on 10.7 of every 1,000 computers scanned in Bolivia in 2Q12 (a CCM score of 10.7, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Bolivia over the last four quarters, compared to the world as a whole.

CCM infection trends in Bolivia and worldwide



Threat categories

Malware and potentially unwanted software categories in Bolivia in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Bolivia in 2Q12 was Worms. It affected 48.5 percent of all computers with detections there, up from 44.1 percent in 1Q12.
- The second most common category in Bolivia in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 36.2 percent of all computers with detections there, down from 37.5 percent in 1Q12.
- The third most common category in Bolivia in 2Q12 was Miscellaneous Trojans, which affected 34.9 percent of all computers with detections there, up from 33.9 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Bolivia in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Dorkbot	Worms	22.8%
2	Win32/Autorun	Worms	15.1%
3	Win32/Keygen	Misc. Potentially Unwanted Software	14.5%
4	Win32/Sality	Viruses	13.0%
5	Win32/Vobfus	Worms	10.8%
6	Win32/Nuqel	Worms	6.7%
7	Win32/Sohanad	Worms	6.1%
8	Win32/Conficker	Worms	5.2%
9	Win32/Rimecud	Worms	4.9%
10	Win32/VBInject	Misc. Potentially Unwanted Software	4.1%

- The most common threat family in Bolivia in 2Q12 was [Win32/Dorkbot](#), which affected 22.8 percent of computers with detections in Bolivia. [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 second most common threat family in Bolivia in 2Q12 was [Win32/Autorun](#), which affected 15.1 percent of computers with detections in Bolivia. [Win32/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 threat family in Bolivia in 2Q12 was [Win32/Keygen](#), which affected 14.5 percent of computers with detections in Bolivia. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The fourth most common threat family in Bolivia in 2Q12 was [Win32/Sality](#), which affected 13.0 percent of computers with detections in Bolivia. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Bolivia

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	0.35 (1.6)	N/A (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	1.39 (3.9)	1.39 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.07 (0.7)	0.10 (0.9)

Update service usage

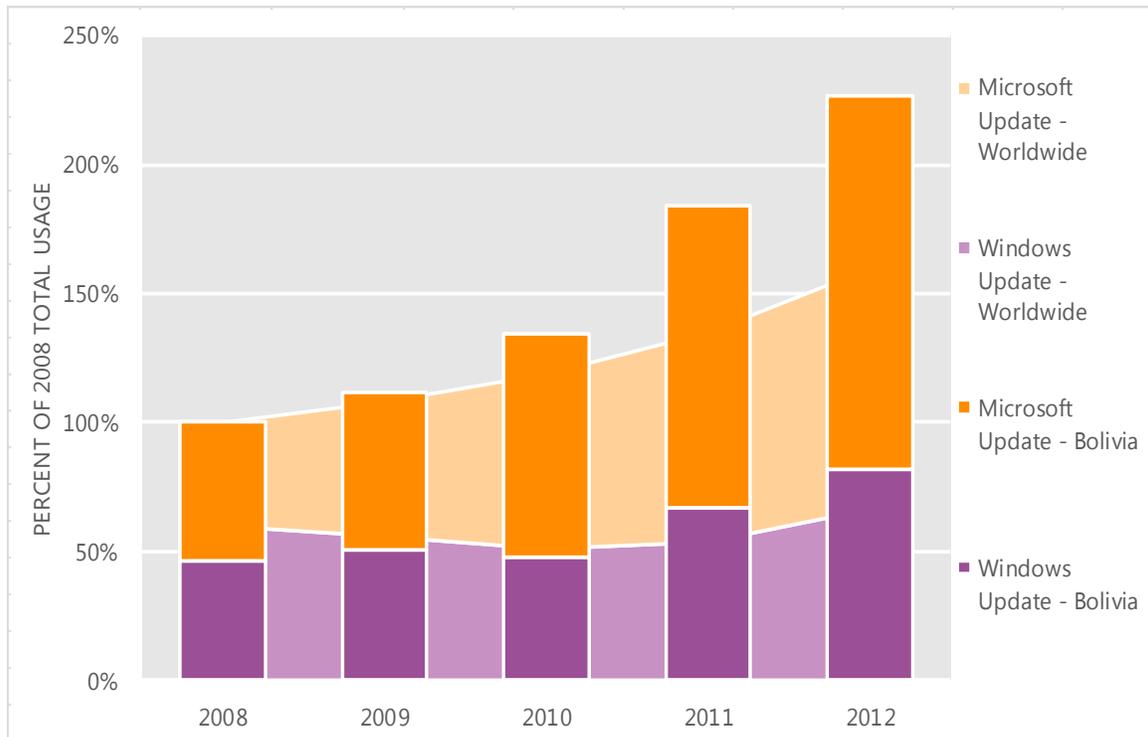
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Bolivia and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Bolivia over the last four years, indexed to the total usage for both services in Bolivia in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Bolivia was up 23.1 percent from 2011, and up 126.5 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Bolivia in 2012, 63.8 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Brazil

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Brazil in 2Q12 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.

Infection rate statistics for Brazil

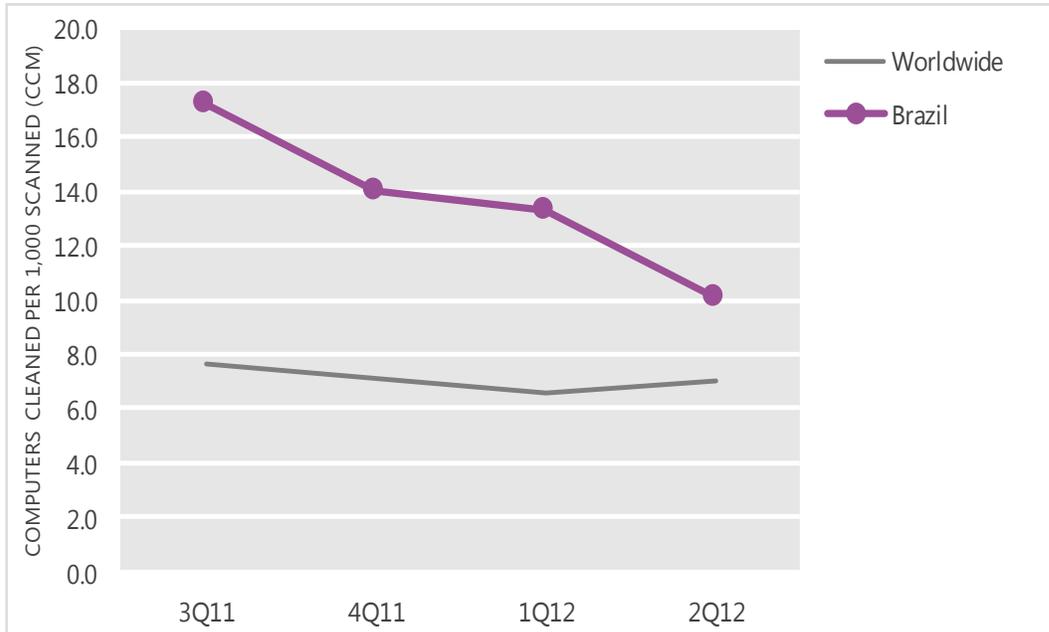
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	17.2	14.0	13.3	10.1
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

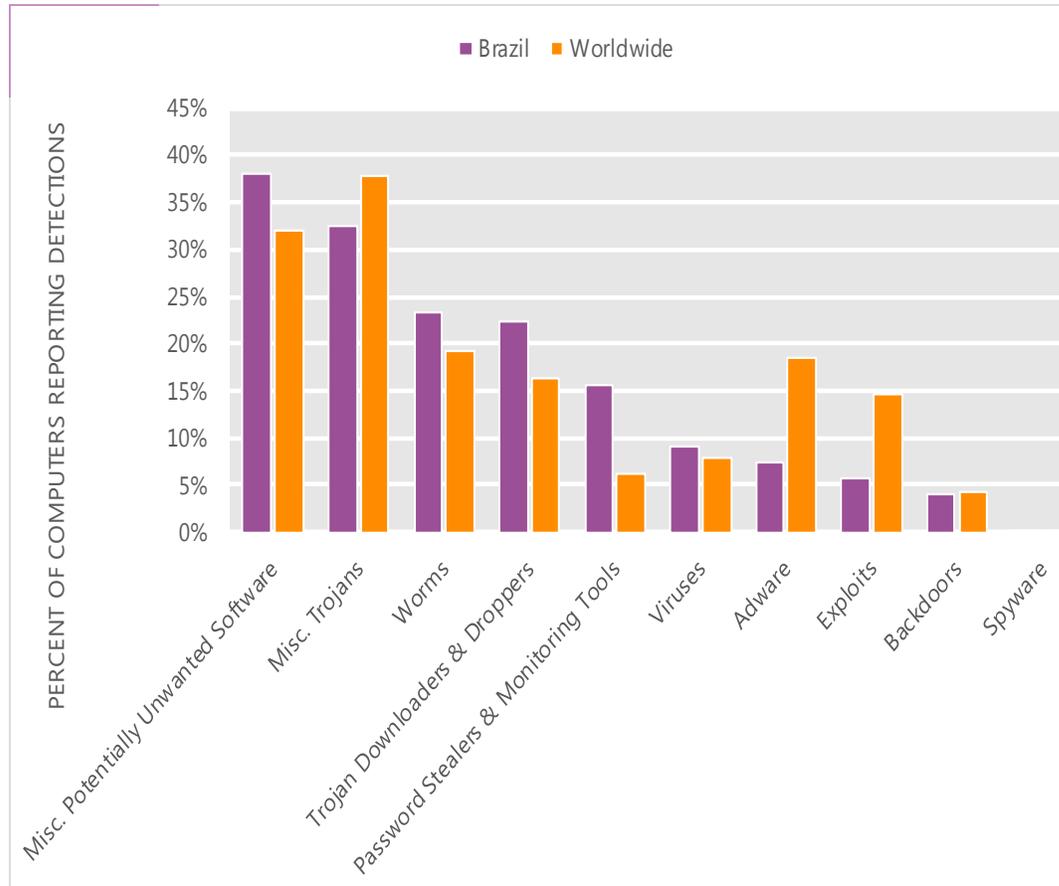
The MSRT detected malware on 10.1 of every 1,000 computers scanned in Brazil in 2Q12 (a CCM score of 10.1, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Brazil over the last four quarters, compared to the world as a whole.

CCM infection trends in Brazil and worldwide



Threat categories

Malware and potentially unwanted software categories in Brazil in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Brazil in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 38.1 percent of all computers with detections there, up from 36.3 percent in 1Q12.
- The second most common category in Brazil in 2Q12 was Miscellaneous Trojans. It affected 32.6 percent of all computers with detections there, up from 29.8 percent in 1Q12.
- The third most common category in Brazil in 2Q12 was Worms, which affected 23.3 percent of all computers with detections there, up from 20.8 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Brazil in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Keygen	Misc. Potentially Unwanted Software	12.0%
2	Win32/Autorun	Worms	10.2%
3	Win32/Bancos	Password Stealers & Monitoring Tools	8.3%
4	Win32/Banload	Trojan Downloaders & Droppers	8.2%
5	Win32/Sality	Viruses	6.5%
6	Win32/Conficker	Worms	5.8%
7	Win32/Banker	Password Stealers & Monitoring Tools	5.2%
8	Win32/Dorkbot	Worms	5.0%
9	Win32/PossibleHostsFileHijack	Misc. Potentially Unwanted Software	4.3%
10	Win32/Obfuscator	Misc. Potentially Unwanted Software	4.2%

- The most common threat family in Brazil in 2Q12 was [Win32/Keygen](#), which affected 12.0 percent of computers with detections in Brazil. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The second most common threat family in Brazil in 2Q12 was [Win32/Autorun](#), which affected 10.2 percent of computers with detections in Brazil. [Win32/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 threat family in Brazil in 2Q12 was [Win32/Bancos](#), which affected 8.3 percent of computers with detections in Brazil. [Win32/Bancos](#) is a data-stealing trojan that captures online banking credentials and relays them to the attacker. Most variants target customers of Brazilian banks.
- The fourth most common threat family in Brazil in 2Q12 was [Win32/Banload](#), which affected 8.2 percent of computers with detections in Brazil. [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.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Brazil

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	1.30 (1.6)	1.68 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	2.05 (3.9)	2.76 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.25 (0.7)	0.36 (0.9)

Update service usage

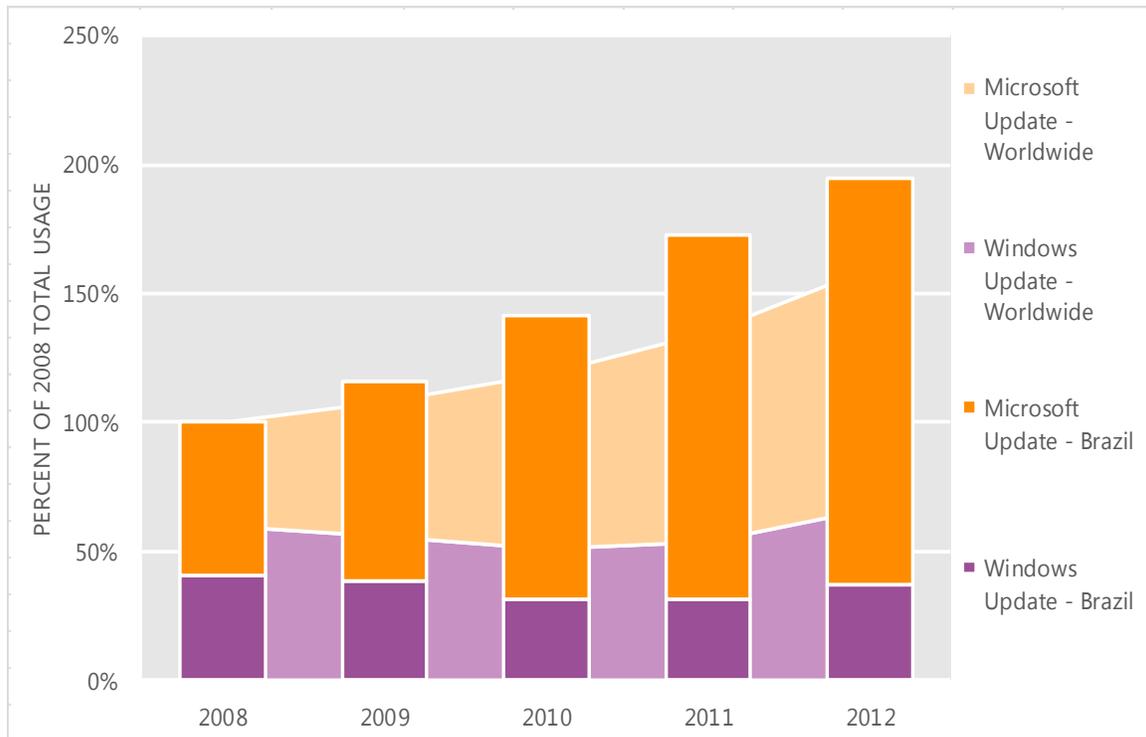
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Brazil and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Brazil over the last four years, indexed to the total usage for both services in Brazil in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Brazil was up 12.7 percent from 2011, and up 94.6 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Brazil in 2012, 81.0 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Bulgaria

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Bulgaria in 2Q12 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.

Infection rate statistics for Bulgaria

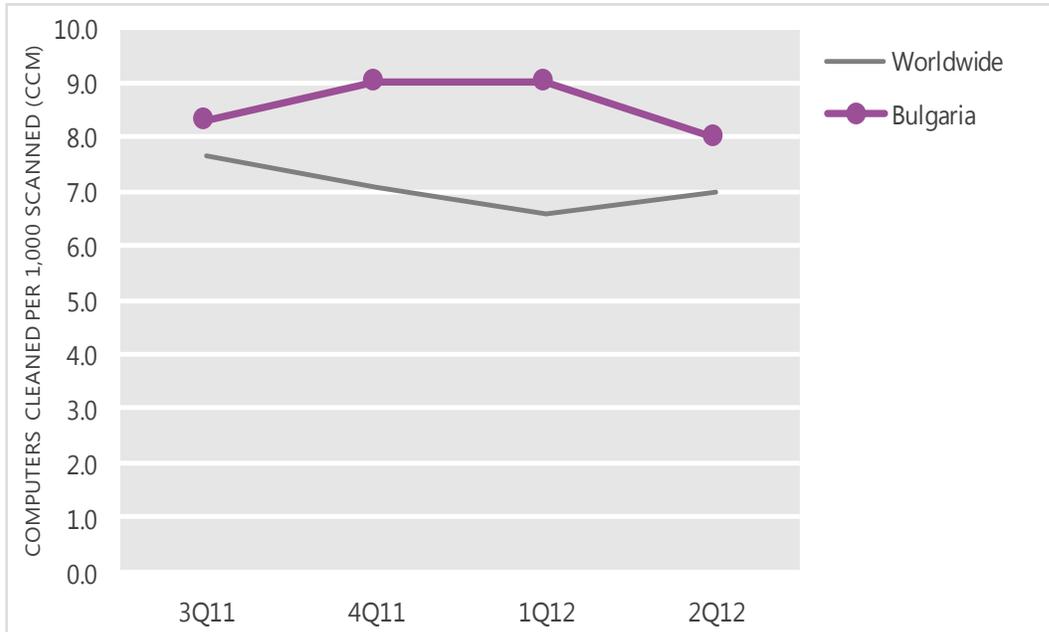
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	8.3	9.0	9.0	8.0
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

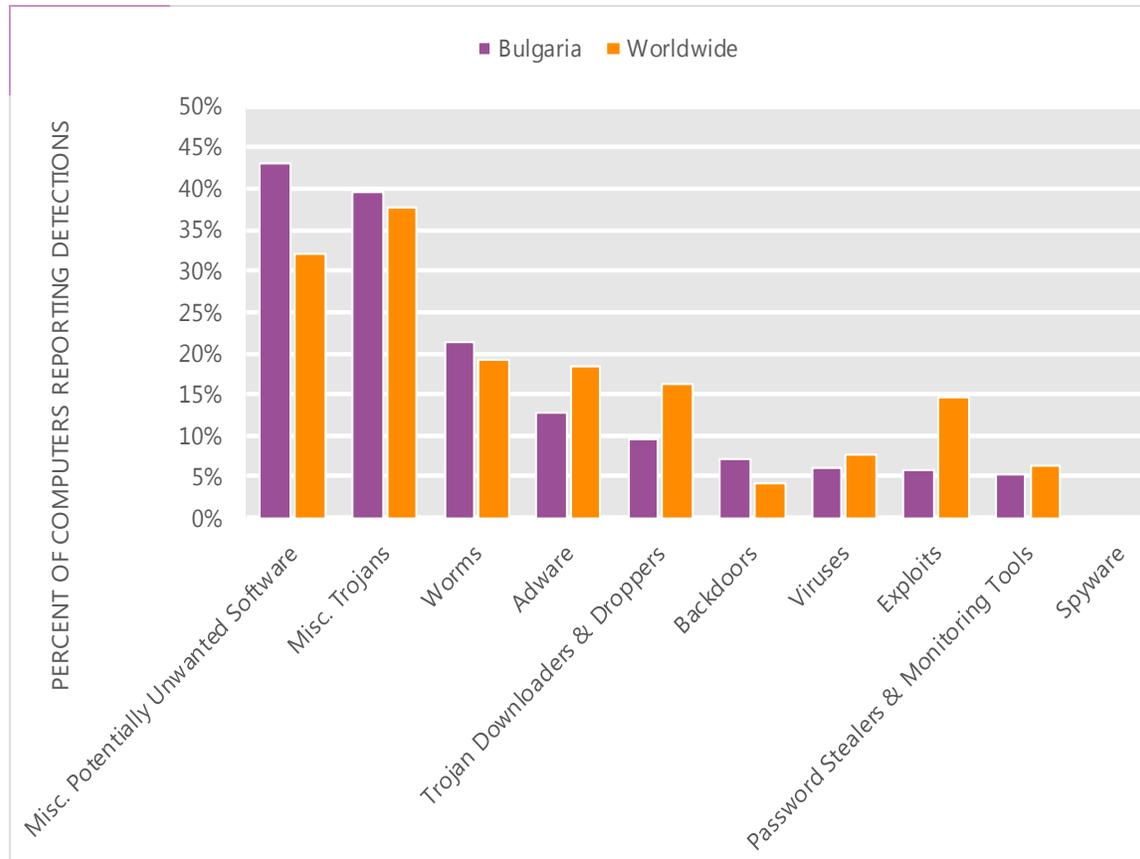
The MSRT detected malware on 8.0 of every 1,000 computers scanned in Bulgaria in 2Q12 (a CCM score of 8.0, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Bulgaria over the last four quarters, compared to the world as a whole.

CCM infection trends in Bulgaria and worldwide



Threat categories

Malware and potentially unwanted software categories in Bulgaria in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Bulgaria in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 43.2 percent of all computers with detections there, down from 43.4 percent in 1Q12.
- The second most common category in Bulgaria in 2Q12 was Miscellaneous Trojans. It affected 39.6 percent of all computers with detections there, up from 39.1 percent in 1Q12.
- The third most common category in Bulgaria in 2Q12 was Worms, which affected 21.4 percent of all computers with detections there, down from 21.5 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Bulgaria in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Keygen	Misc. Potentially Unwanted Software	21.0%
2	Win32/Autorun	Worms	8.1%
3	JS/Pornpop	Adware	6.7%
4	Win32/Conficker	Worms	6.4%
5	Win32/Obfuscator	Misc. Potentially Unwanted Software	5.9%
6	Win32/Rimecud	Worms	5.6%
7	JS/Iframe	Misc. Trojans	5.0%
8	Win32/Sality	Viruses	4.2%
9	JS/IframeRef	Misc. Trojans	3.7%
10	Win32/Killav	Misc. Trojans	3.6%

- The most common threat family in Bulgaria in 2Q12 was [Win32/Keygen](#), which affected 21.0 percent of computers with detections in Bulgaria. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The second most common threat family in Bulgaria in 2Q12 was [Win32/Autorun](#), which affected 8.1 percent of computers with detections in Bulgaria. [Win32/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 threat family in Bulgaria in 2Q12 was [JS/Pornpop](#), which affected 6.7 percent of computers with detections in Bulgaria. [JS/Pornpop](#) is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The fourth most common threat family in Bulgaria in 2Q12 was [Win32/Conficker](#), which affected 6.4 percent of computers with detections in Bulgaria. [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.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Bulgaria

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	2.67 (1.6)	2.57 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	3.02 (3.9)	2.62 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	1.19 (0.7)	1.62 (0.9)

Update service usage

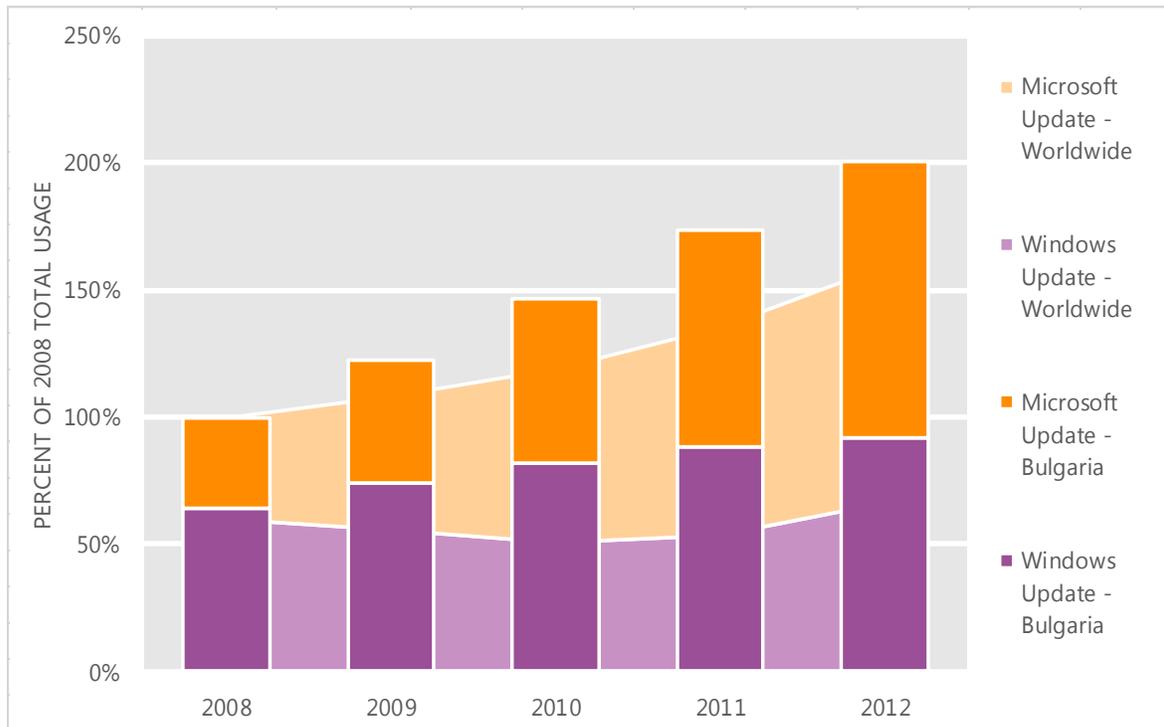
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Bulgaria and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Bulgaria over the last four years, indexed to the total usage for both services in Bulgaria in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Bulgaria was up 15.3 percent from 2011, and up 100.5 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Bulgaria in 2012, 54.2 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Canada

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Canada in 2Q12 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.

Infection rate statistics for Canada

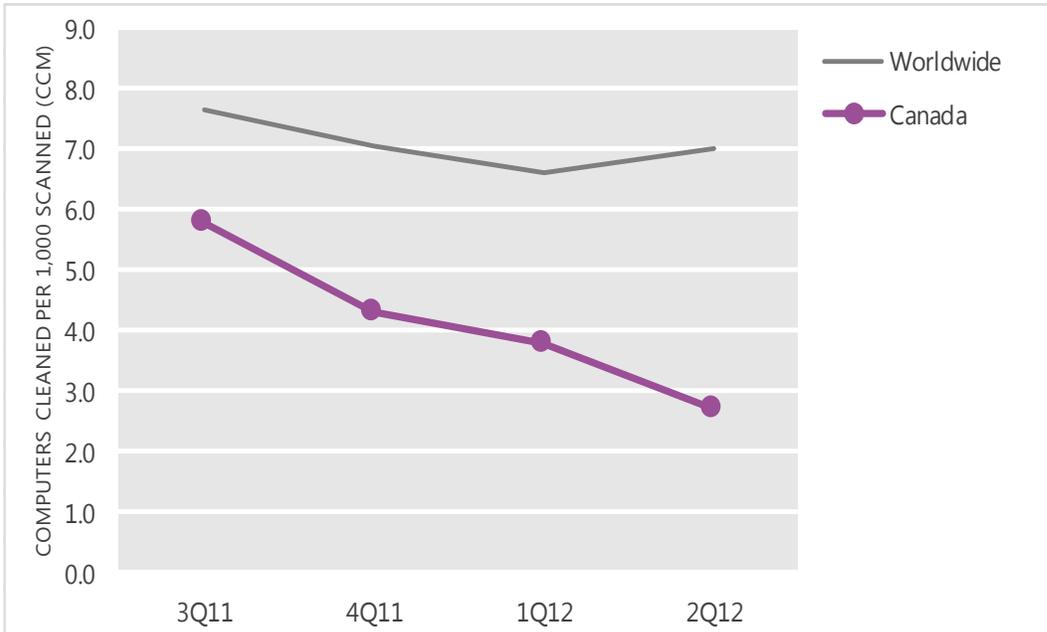
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	5.8	4.3	3.8	2.7
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

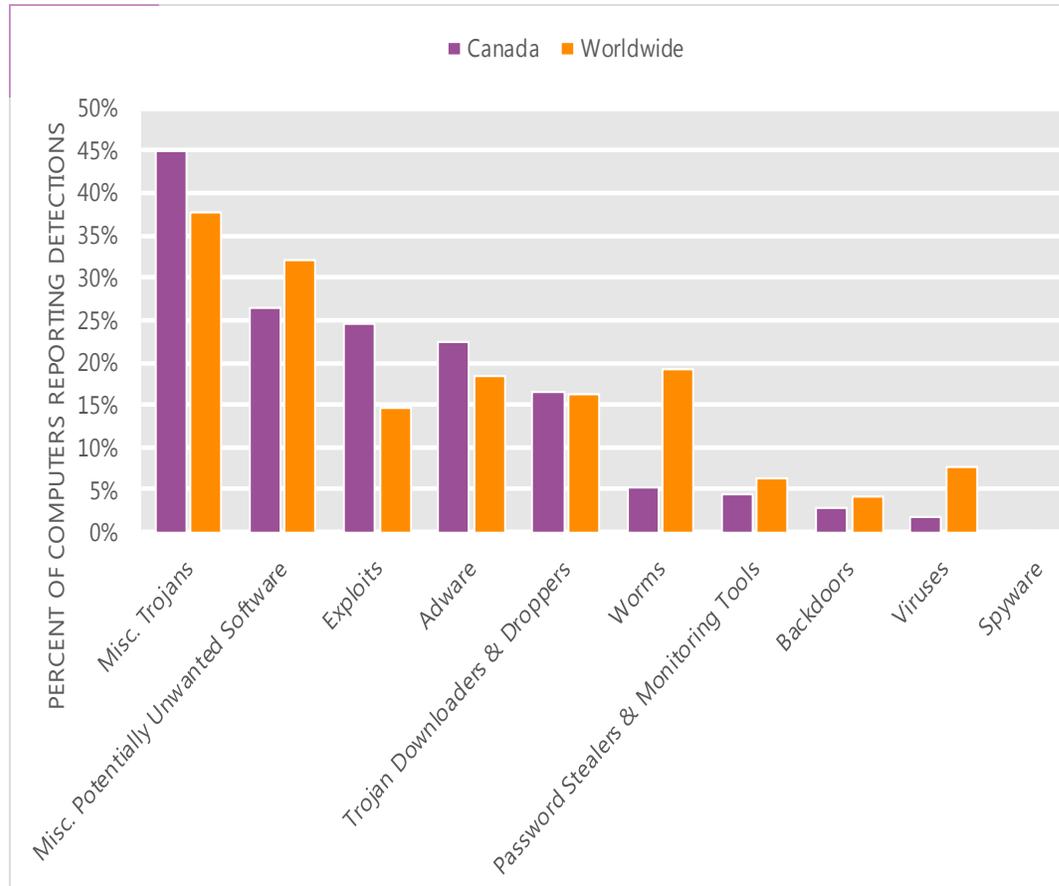
The MSRT detected malware on 2.7 of every 1,000 computers scanned in Canada in 2Q12 (a CCM score of 2.7, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Canada over the last four quarters, compared to the world as a whole.

CCM infection trends in Canada and worldwide



Threat categories

Malware and potentially unwanted software categories in Canada in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Canada in 2Q12 was Miscellaneous Trojans. It affected 45.0 percent of all computers with detections there, up from 36.3 percent in 1Q12.
- The second most common category in Canada in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 26.4 percent of all computers with detections there, up from 25.8 percent in 1Q12.
- The third most common category in Canada in 2Q12 was Exploits, which affected 24.6 percent of all computers with detections there, down from 25.0 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Canada in 2Q12

	Family	Most significant category	% of computers with detections
1	Java/Blacole	Exploits	10.1%
2	JS/IframeRef	Misc. Trojans	9.2%
3	Win32/FakePAV	Misc. Trojans	8.8%
4	Win32/Hotbar	Adware	8.6%
5	JS/Pornpop	Adware	8.0%
6	ASX/Wimad	Trojan Downloaders & Droppers	7.7%
7	Java/CVE-2012-0507	Exploits	7.5%
8	Win32/Keygen	Misc. Potentially Unwanted Software	7.1%
9	Win32/Winwebsec	Misc. Trojans	6.9%
10	Win32/Sirefef	Misc. Trojans	6.8%

- The most common threat family in Canada in 2Q12 was [Java/Blacole](#), which affected 10.1 percent of computers with detections in Canada. [Java/Blacole](#) is an exploit pack, also known as Blackhole, that is installed on a compromised web server by an attacker and includes a number of exploits that target browser software. If a vulnerable computer browses a compromised website that contains the exploit pack, various malware may be downloaded and run.
- The second most common threat family in Canada in 2Q12 was [JS/IframeRef](#), which affected 9.2 percent of computers with detections in Canada. [JS/IframeRef](#) is a generic detection for specially formed IFrame tags that point to remote websites that contain malicious content.
- The third most common threat family in Canada in 2Q12 was [Win32/FakePAV](#), which affected 8.8 percent of computers with detections in Canada. [Win32/FakePAV](#) is a rogue security software family that often masquerades as Microsoft Security Essentials or other legitimate antimalware products.
- The fourth most common threat family in Canada in 2Q12 was [Win32/Hotbar](#), which affected 8.6 percent of computers with detections in Canada. [Win32/Hotbar](#) is adware that displays a dynamic toolbar and targeted pop-up ads based on its monitoring of web-browsing activity.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Canada

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	1.35 (1.6)	1.50 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	2.52 (3.9)	2.62 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.88 (0.7)	0.91 (0.9)

Update service usage

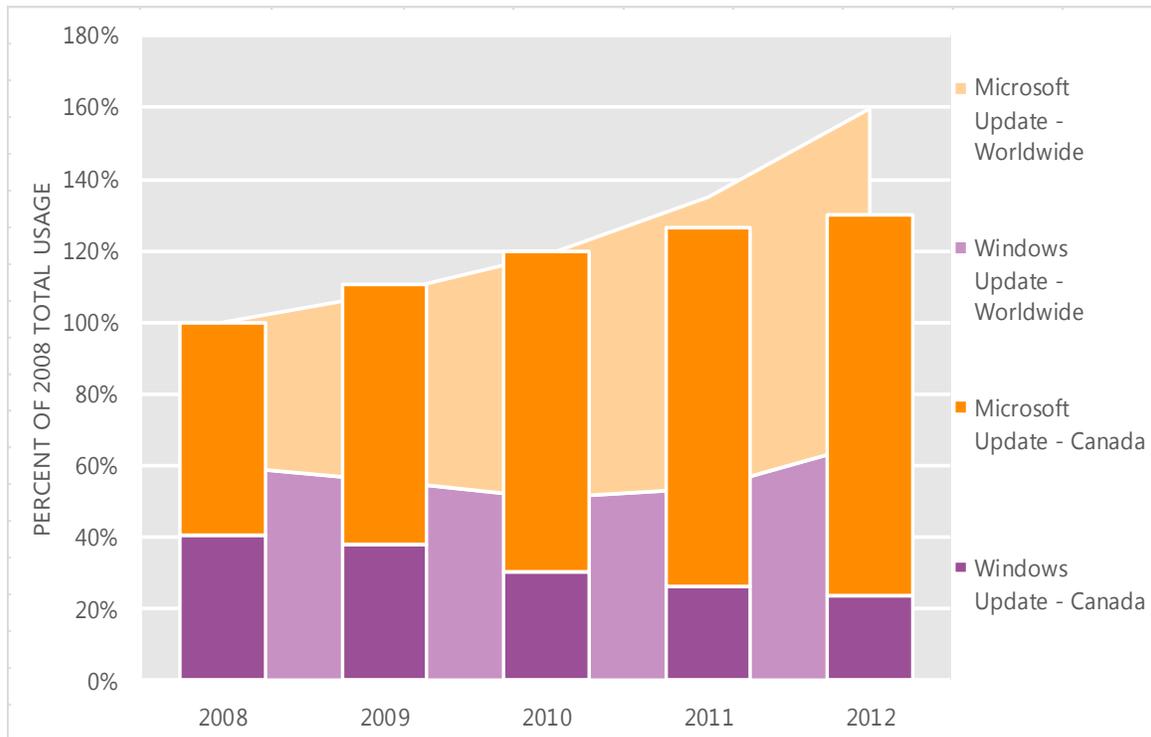
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Canada and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Canada over the last four years, indexed to the total usage for both services in Canada in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Canada was up 2.9 percent from 2011, and up 30.0 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Canada in 2012, 81.7 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Chile

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Chile in 2Q12 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.

Infection rate statistics for Chile

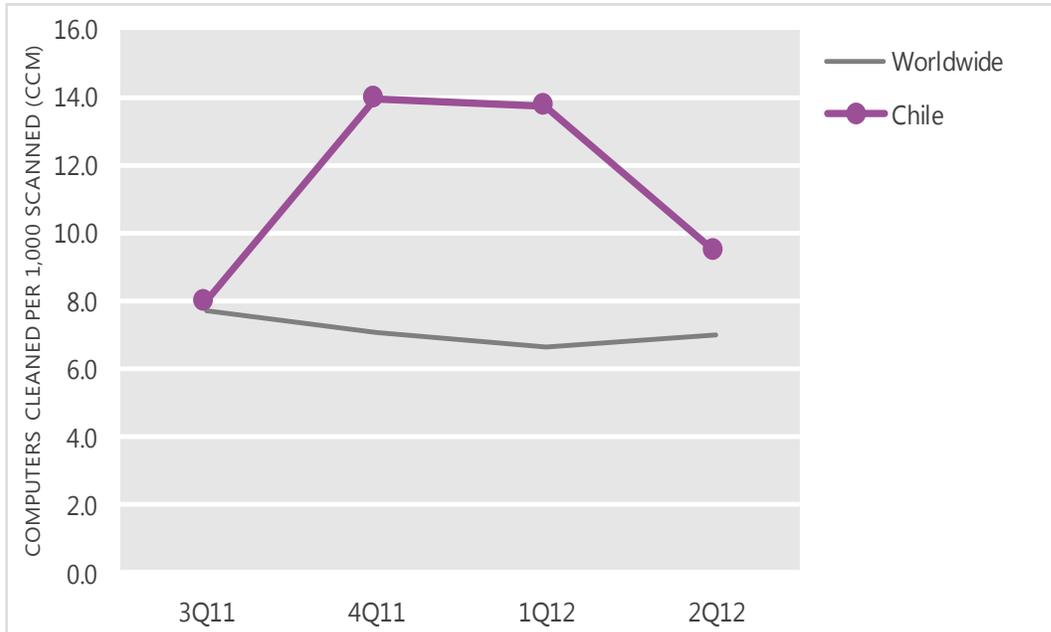
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	7.9	13.9	13.7	9.4
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

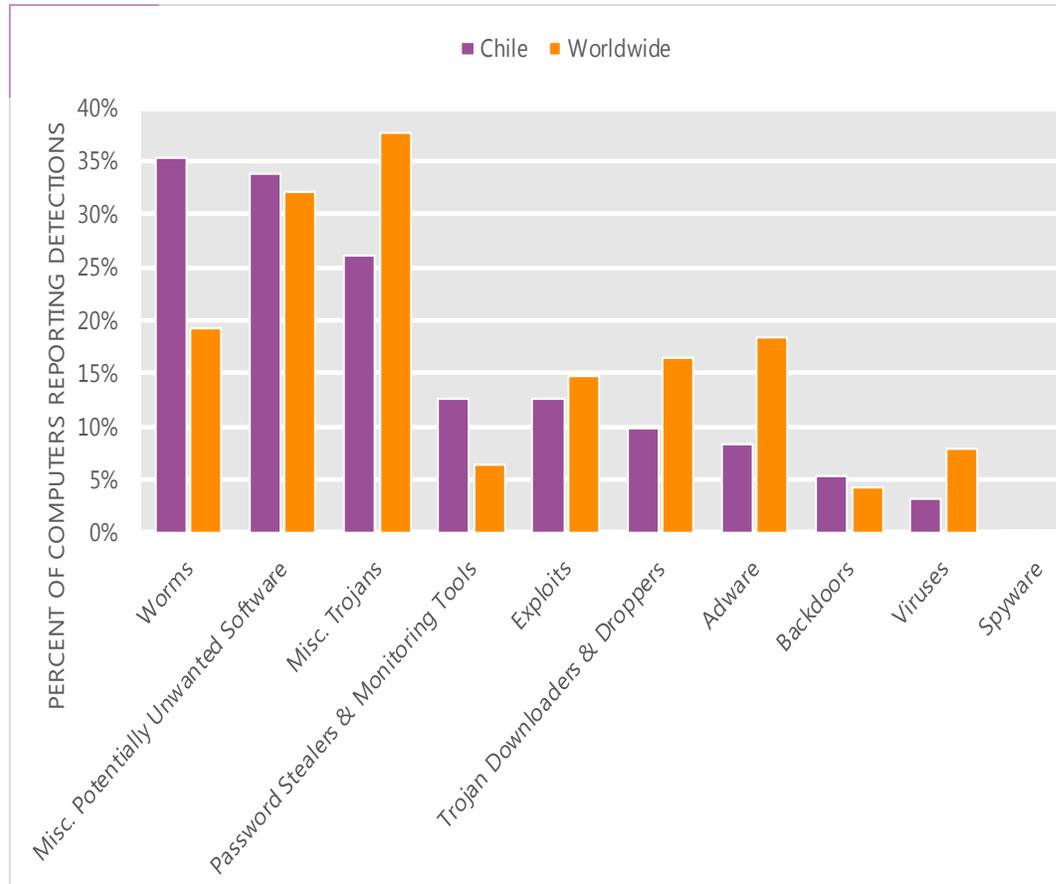
The MSRT detected malware on 9.4 of every 1,000 computers scanned in Chile in 2Q12 (a CCM score of 9.4, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Chile over the last four quarters, compared to the world as a whole.

CCM infection trends in Chile and worldwide



Threat categories

Malware and potentially unwanted software categories in Chile in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Chile in 2Q12 was Worms. It affected 35.3 percent of all computers with detections there, up from 27.3 percent in 1Q12.
- The second most common category in Chile in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 33.7 percent of all computers with detections there, up from 32.7 percent in 1Q12.
- The third most common category in Chile in 2Q12 was Miscellaneous Trojans, which affected 26.1 percent of all computers with detections there, down from 26.8 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Chile in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Dorkbot	Worms	19.6%
2	Win32/Keygen	Misc. Potentially Unwanted Software	10.5%
3	Java/Blacole	Exploits	8.7%
4	Win32/Autorun	Worms	8.0%
5	Win32/Zbot	Password Stealers & Monitoring Tools	7.9%
6	Win32/Conficker	Worms	5.1%
7	Win32/VBInject	Misc. Potentially Unwanted Software	4.0%
8	ASX/Wimad	Trojan Downloaders & Droppers	3.8%
9	JS/Redirector	Misc. Trojans	3.8%
10	Win32/Obfuscator	Misc. Potentially Unwanted Software	3.8%

- The most common threat family in Chile in 2Q12 was [Win32/Dorkbot](#), which affected 19.6 percent of computers with detections in Chile. [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 second most common threat family in Chile in 2Q12 was [Win32/Keygen](#), which affected 10.5 percent of computers with detections in Chile. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The third most common threat family in Chile in 2Q12 was [Java/Blacole](#), which affected 8.7 percent of computers with detections in Chile. [Java/Blacole](#) is an exploit pack, also known as Blackhole, that is installed on a compromised web server by an attacker and includes a number of exploits that target browser software. If a vulnerable computer browses a compromised website that contains the exploit pack, various malware may be downloaded and run.
- The fourth most common threat family in Chile in 2Q12 was [Win32/Autorun](#), which affected 8.0 percent of computers with detections in Chile. [Win32/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.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Chile

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	1.38 (1.6)	1.87 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	2.27 (3.9)	3.99 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	1.40 (0.7)	1.30 (0.9)

Update service usage

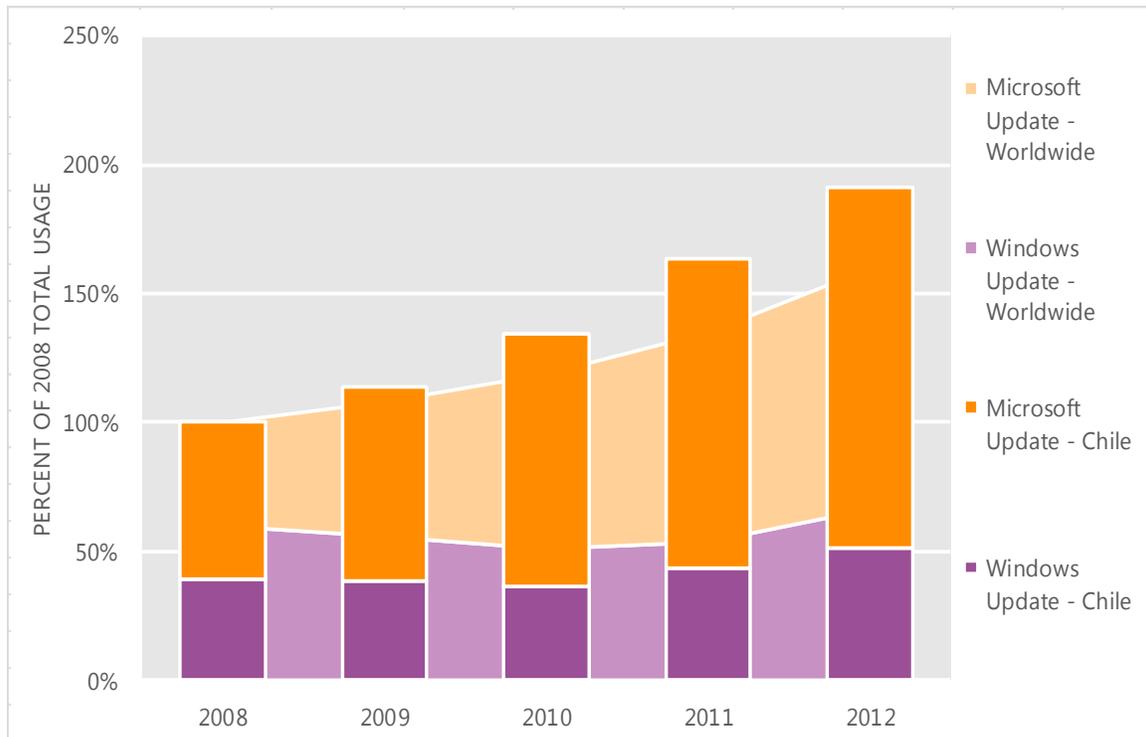
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Chile and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Chile over the last four years, indexed to the total usage for both services in Chile in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Chile was up 17.2 percent from 2011, and up 91.6 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Chile in 2012, 73.3 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

China

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in China in 2Q12 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.

Infection rate statistics for China

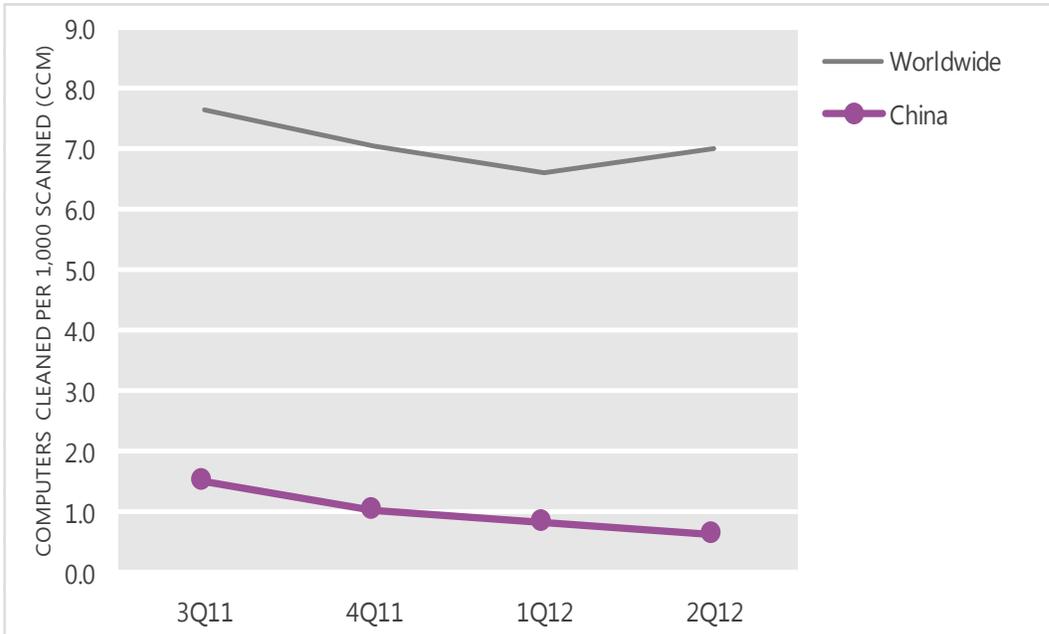
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	1.5	1.0	0.8	0.6
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

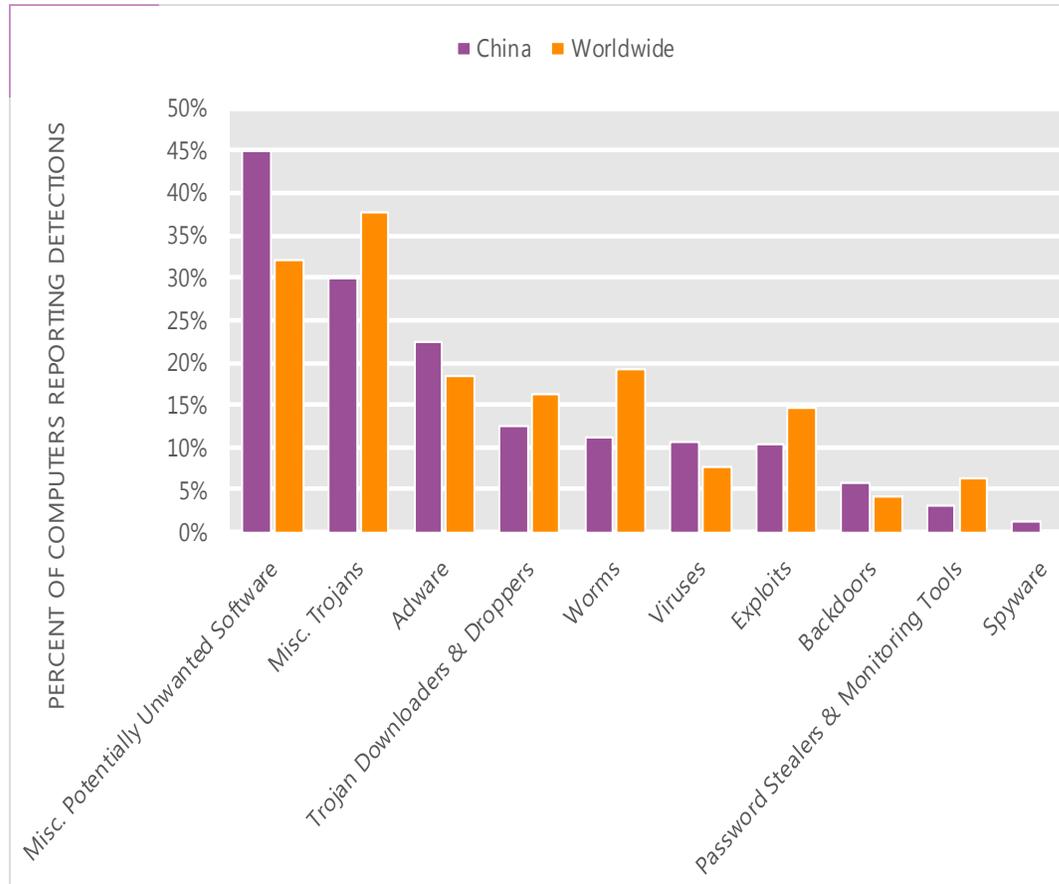
The MSRT detected malware on 0.6 of every 1,000 computers scanned in China in 2Q12 (a CCM score of 0.6, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for China over the last four quarters, compared to the world as a whole.

CCM infection trends in China and worldwide



Threat categories

Malware and potentially unwanted software categories in China in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in China in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 45.0 percent of all computers with detections there, up from 43.7 percent in 1Q12.
- The second most common category in China in 2Q12 was Miscellaneous Trojans. It affected 29.9 percent of all computers with detections there, down from 30.6 percent in 1Q12.
- The third most common category in China in 2Q12 was Adware, which affected 22.4 percent of all computers with detections there, up from 12.2 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in China in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/BaiduSobar	Misc. Potentially Unwanted Software	17.2%
2	JS/Popupper	Adware	16.6%
3	Win32/Keygen	Misc. Potentially Unwanted Software	12.6%
4	JS/IframeRef	Misc. Trojans	6.5%
5	Win32/PossibleHostsFileHijack	Misc. Potentially Unwanted Software	6.1%
6	Win32/Obfuscator	Misc. Potentially Unwanted Software	5.1%
7	Win32/Conficker	Worms	4.2%
8	Win32/Orsam	Misc. Trojans	4.0%
9	Win32/Agent	Misc. Trojans	3.3%
10	Win32/Bumat	Misc. Trojans	3.3%

- The most common threat family in China in 2Q12 was [Win32/BaiduSobar](#), which affected 17.2 percent of computers with detections in China. [Win32/BaiduSobar](#) is a Chinese-language web browser toolbar that delivers pop-up and contextual advertisements, blocks certain other advertisements, and changes the Internet Explorer search page.
- The second most common threat family in China in 2Q12 was [JS/Popupper](#), which affected 16.6 percent of computers with detections in China. [JS/Popupper](#) is a detection for a particular JavaScript script that attempts to display pop-under advertisements.
- The third most common threat family in China in 2Q12 was [Win32/Keygen](#), which affected 12.6 percent of computers with detections in China. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The fourth most common threat family in China in 2Q12 was [JS/IframeRef](#), which affected 6.5 percent of computers with detections in China. [JS/IframeRef](#) is a generic detection for specially formed IFrame tags that point to remote web-sites that contain malicious content.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for China

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	0.53 (1.6)	0.66 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	7.23 (3.9)	8.11 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.28 (0.7)	0.56 (0.9)

Update service usage

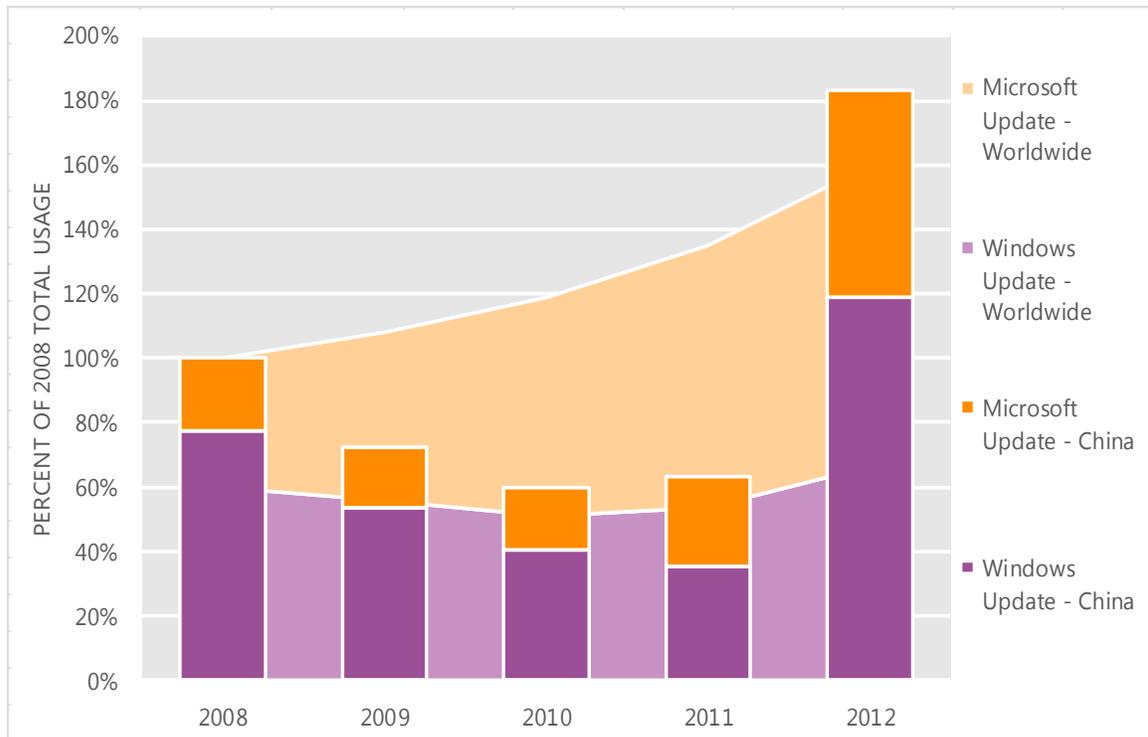
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in China and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in China over the last four years, indexed to the total usage for both services in China in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in China was up 190.2 percent from 2011, and up 83.1 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in China in 2012, 35.2 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Colombia

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Colombia in 2Q12 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.

Infection rate statistics for Colombia

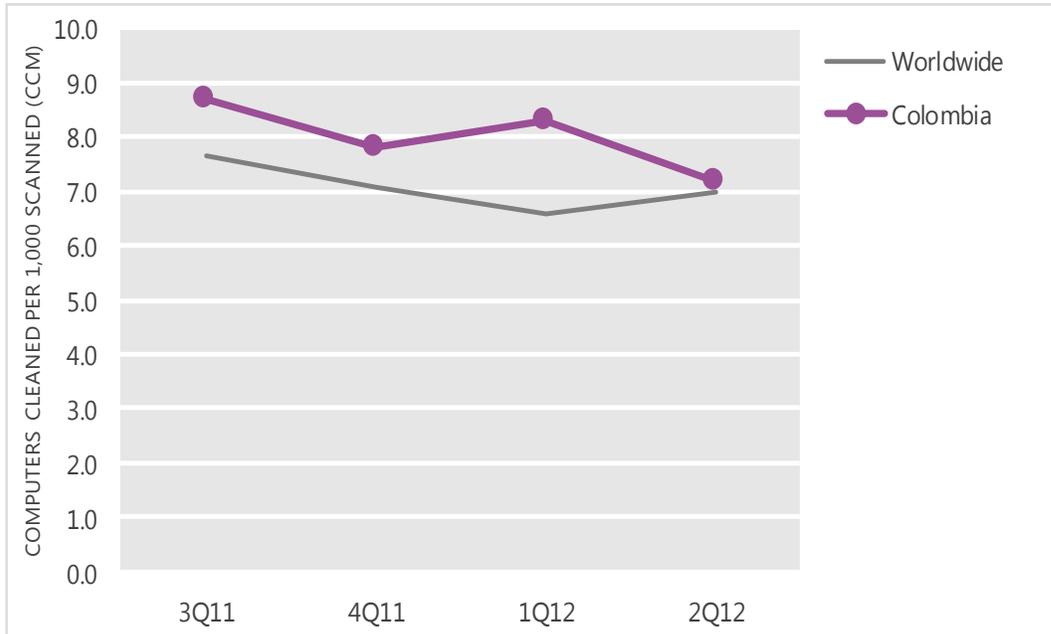
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	8.7	7.8	8.3	7.2
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

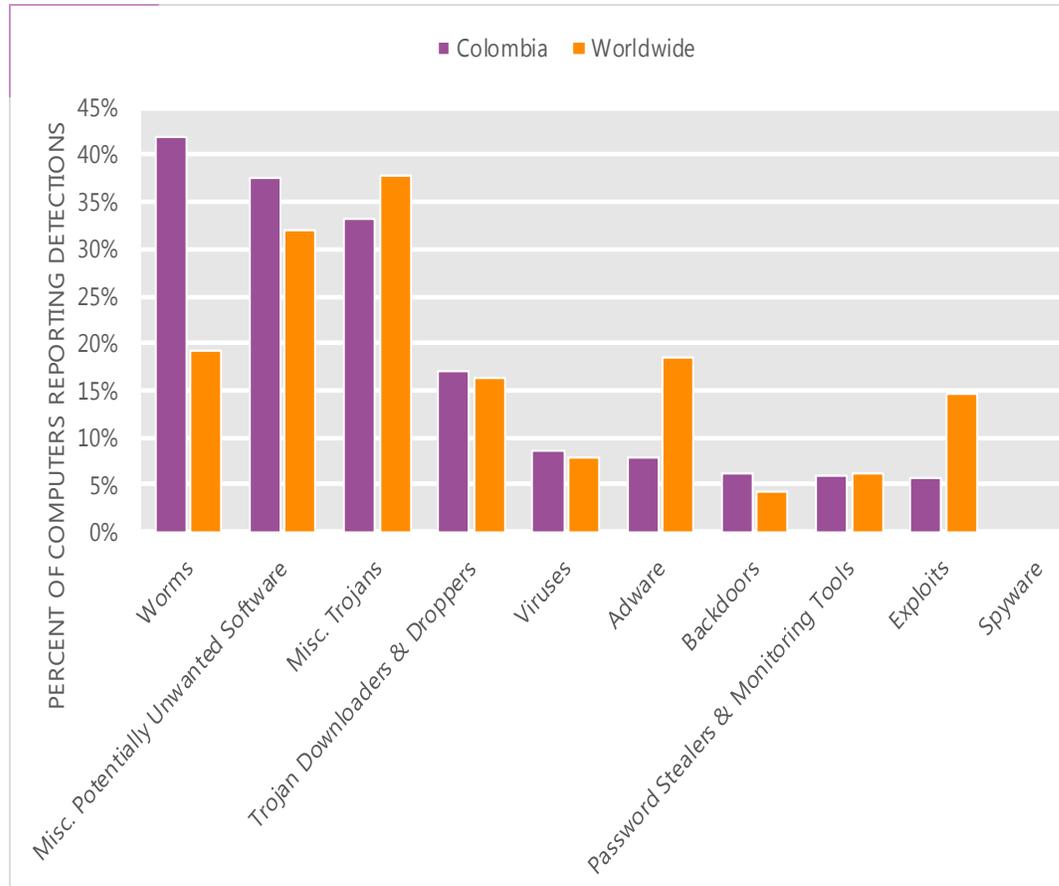
The MSRT detected malware on 7.2 of every 1,000 computers scanned in Colombia in 2Q12 (a CCM score of 7.2, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Colombia over the last four quarters, compared to the world as a whole.

CCM infection trends in Colombia and worldwide



Threat categories

Malware and potentially unwanted software categories in Colombia in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Colombia in 2Q12 was Worms. It affected 41.9 percent of all computers with detections there, down from 42.1 percent in 1Q12.
- The second most common category in Colombia in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 37.5 percent of all computers with detections there, down from 42.7 percent in 1Q12.
- The third most common category in Colombia in 2Q12 was Miscellaneous Trojans, which affected 33.2 percent of all computers with detections there, up from 27.9 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Colombia in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Dorkbot	Worms	25.0%
2	Win32/Keygen	Misc. Potentially Unwanted Software	13.0%
3	Win32/Autorun	Worms	12.3%
4	Win32/Conficker	Worms	7.9%
5	Win32/VBInject	Misc. Potentially Unwanted Software	7.3%
6	Win32/Sality	Viruses	5.7%
7	Win32/Banker	Password Stealers & Monitoring Tools	5.0%
8	JS/Redirector	Misc. Trojans	4.6%
9	ASX/Wimad	Trojan Downloaders & Droppers	4.4%
10	Win32/Silly_P2P	Worms	4.2%

- The most common threat family in Colombia in 2Q12 was [Win32/Dorkbot](#), which affected 25.0 percent of computers with detections in Colombia. [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 second most common threat family in Colombia in 2Q12 was [Win32/Keygen](#), which affected 13.0 percent of computers with detections in Colombia. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The third most common threat family in Colombia in 2Q12 was [Win32/Autorun](#), which affected 12.3 percent of computers with detections in Colombia. [Win32/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 threat family in Colombia in 2Q12 was [Win32/Conficker](#), which affected 7.9 percent of computers with detections in Colombia. [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.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Colombia

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	0.44 (1.6)	0.43 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	0.97 (3.9)	1.49 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.06 (0.7)	0.07 (0.9)

Update service usage

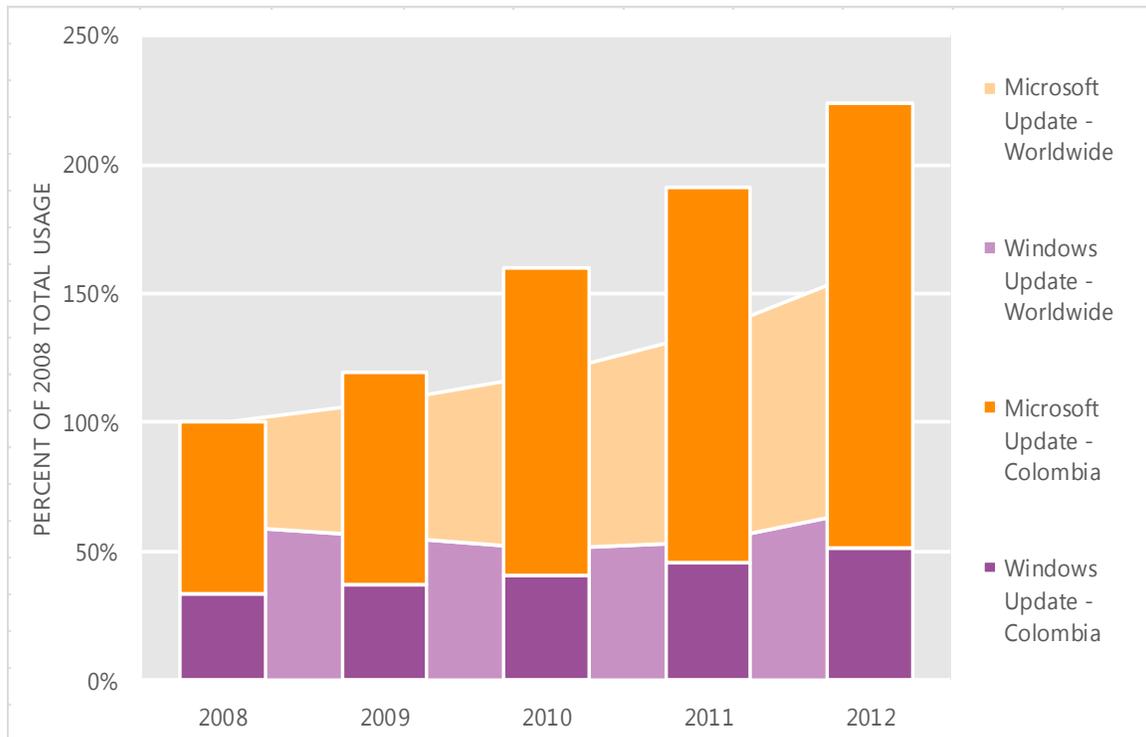
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Colombia and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Colombia over the last four years, indexed to the total usage for both services in Colombia in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Colombia was up 17.1 percent from 2011, and up 124.3 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Colombia in 2012, 77.1 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Costa Rica

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Costa Rica in 2Q12 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.

Infection rate statistics for Costa Rica

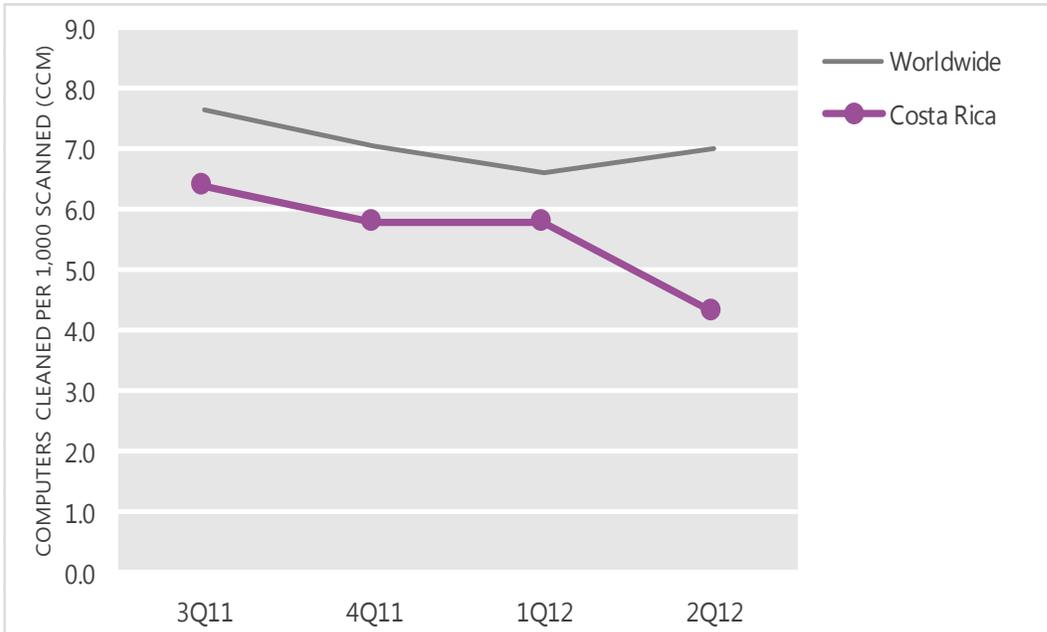
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	6.4	5.8	5.8	4.3
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

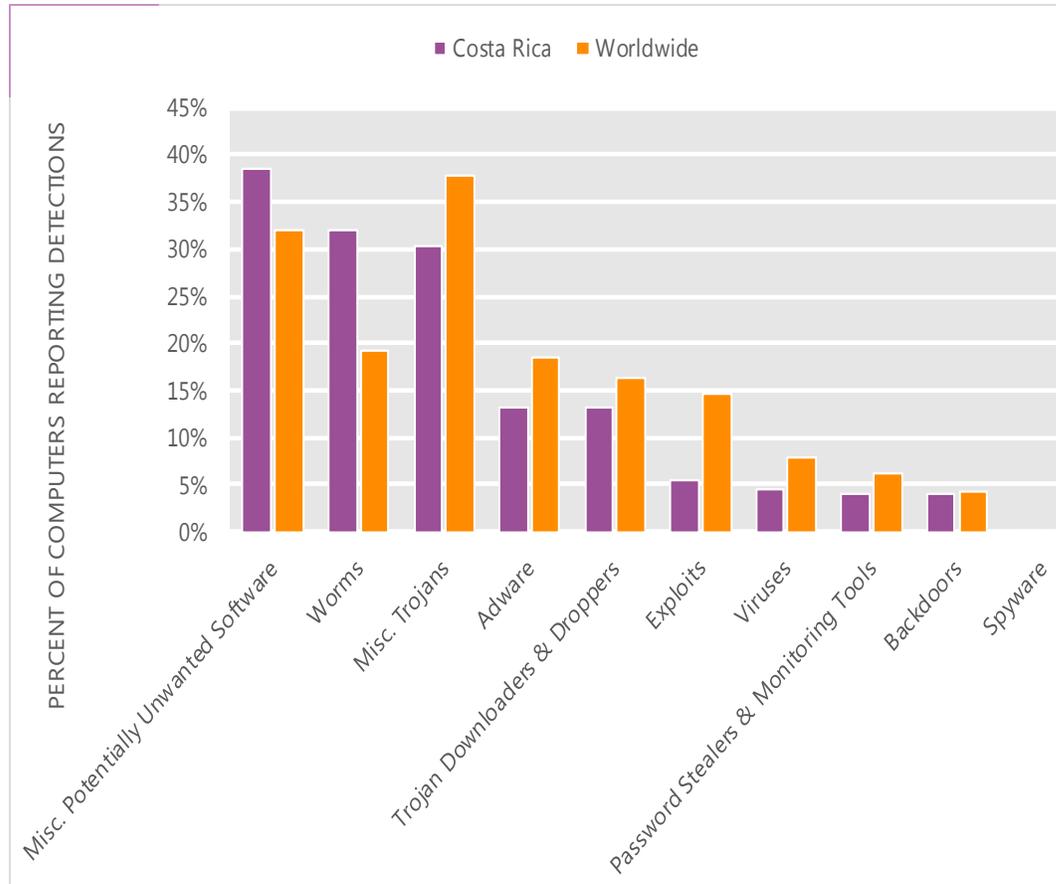
The MSRT detected malware on 4.3 of every 1,000 computers scanned in Costa Rica in 2Q12 (a CCM score of 4.3, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Costa Rica over the last four quarters, compared to the world as a whole.

CCM infection trends in Costa Rica and worldwide



Threat categories

Malware and potentially unwanted software categories in Costa Rica in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Costa Rica in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 38.6 percent of all computers with detections there, down from 42.6 percent in 1Q12.
- The second most common category in Costa Rica in 2Q12 was Worms. It affected 31.9 percent of all computers with detections there, up from 31.6 percent in 1Q12.
- The third most common category in Costa Rica in 2Q12 was Miscellaneous Trojans, which affected 30.4 percent of all computers with detections there, up from 26.8 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Costa Rica in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Dorkbot	Worms	17.8%
2	Win32/Keygen	Misc. Potentially Unwanted Software	14.9%
3	Win32/Autorun	Worms	9.7%
4	JS/Pornpop	Adware	5.1%
5	Win32/Conficker	Worms	4.7%
6	ASX/Wimad	Trojan Downloaders & Droppers	4.4%
7	JS/Redirector	Misc. Trojans	4.4%
8	Win32/Rimecud	Worms	4.3%
9	Win32/VBInject	Misc. Potentially Unwanted Software	3.7%
10	Win32/Zwangi	Misc. Potentially Unwanted Software	3.7%

- The most common threat family in Costa Rica in 2Q12 was [Win32/Dorkbot](#), which affected 17.8 percent of computers with detections in Costa Rica. [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 second most common threat family in Costa Rica in 2Q12 was [Win32/Keygen](#), which affected 14.9 percent of computers with detections in Costa Rica. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The third most common threat family in Costa Rica in 2Q12 was [Win32/Autorun](#), which affected 9.7 percent of computers with detections in Costa Rica. [Win32/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 threat family in Costa Rica in 2Q12 was [JS/Pornpop](#), which affected 5.1 percent of computers with detections in Costa Rica. [JS/Pornpop](#) is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Costa Rica

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	0.43 (1.6)	0.33 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	1.30 (3.9)	2.17 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	1.11 (0.7)	1.04 (0.9)

Update service usage

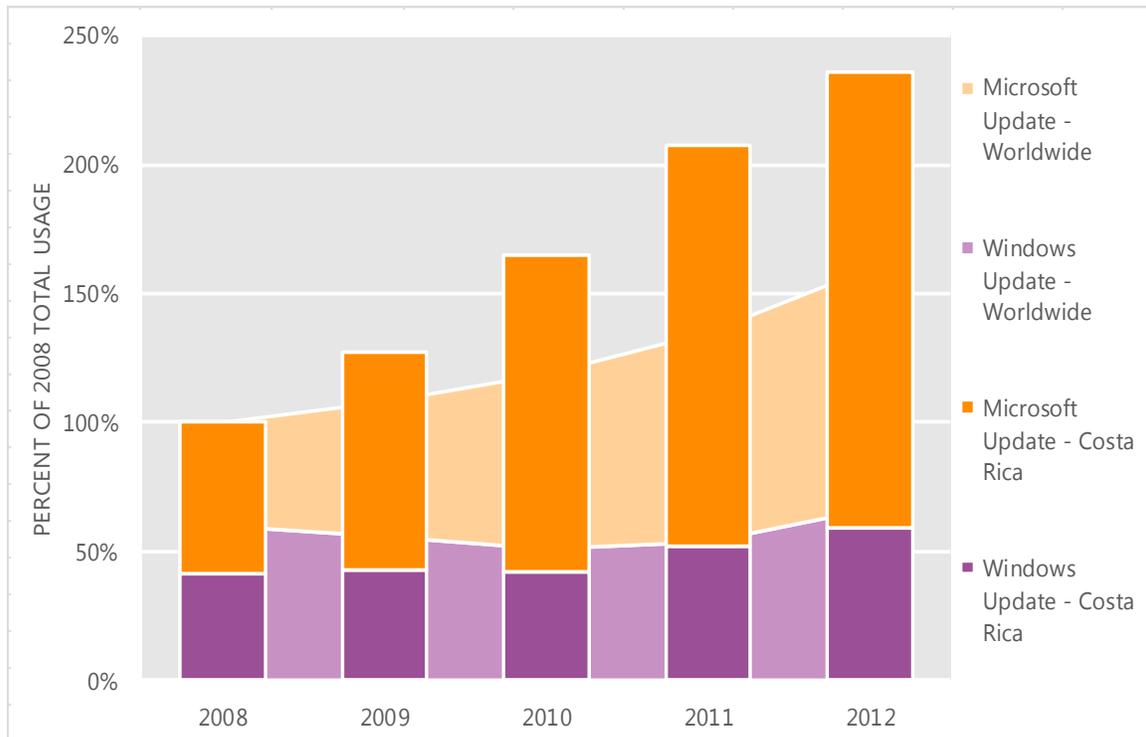
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Costa Rica and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Costa Rica over the last four years, indexed to the total usage for both services in Costa Rica in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Costa Rica was up 13.5 percent from 2011, and up 135.9 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Costa Rica in 2012, 74.9 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Croatia

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Croatia in 2Q12 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.

Infection rate statistics for Croatia

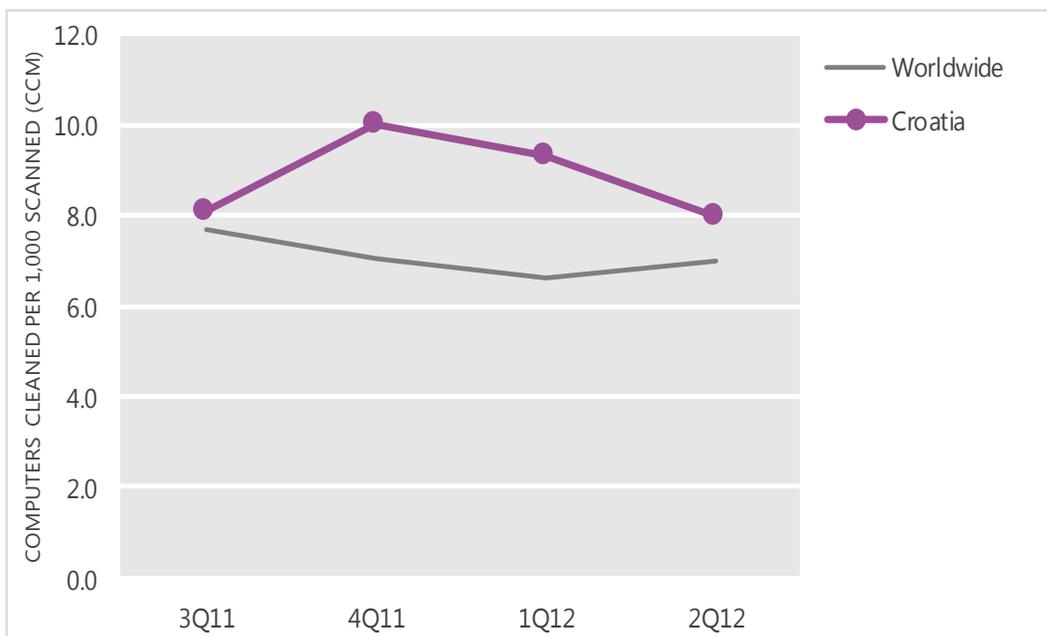
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	8.1	10.0	9.3	8.0
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

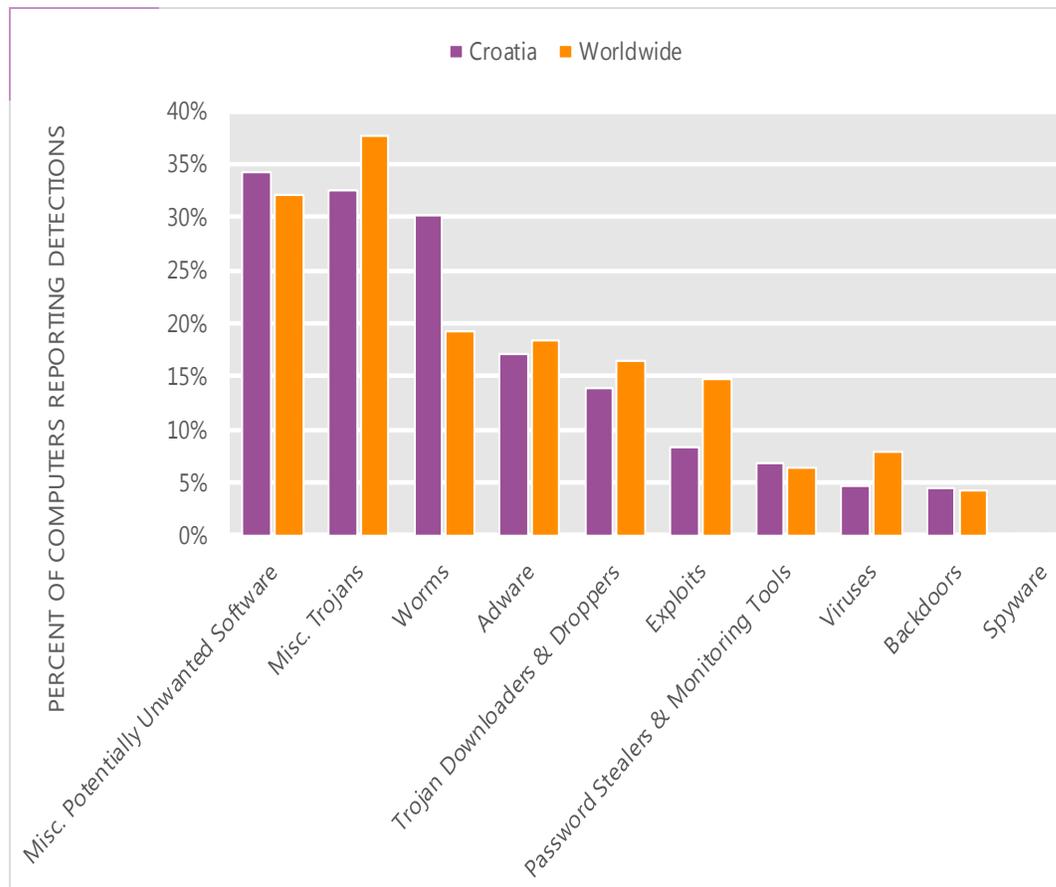
The MSRT detected malware on 8.0 of every 1,000 computers scanned in Croatia in 2Q12 (a CCM score of 8.0, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Croatia over the last four quarters, compared to the world as a whole.

CCM infection trends in Croatia and worldwide



Threat categories

Malware and potentially unwanted software categories in Croatia in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Croatia in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 34.3 percent of all computers with detections there, down from 37.2 percent in 1Q12.
- The second most common category in Croatia in 2Q12 was Miscellaneous Trojans. It affected 32.4 percent of all computers with detections there, down from 32.5 percent in 1Q12.
- The third most common category in Croatia in 2Q12 was Worms, which affected 30.1 percent of all computers with detections there, up from 24.1 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Croatia in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Keygen	Misc. Potentially Unwanted Software	13.2%
2	JS/Pornpop	Adware	8.4%
3	Win32/Autorun	Worms	7.3%
4	Win32/Pushbot	Worms	6.5%
5	Win32/Rimecud	Worms	5.7%
6	Win32/Winwebsec	Misc. Trojans	5.4%
7	Win32/Hotbar	Adware	4.8%
8	ASX/Wimad	Trojan Downloaders & Droppers	4.6%
9	Win32/Zwangi	Misc. Potentially Unwanted Software	4.5%
10	Java/CVE-2012-0507	Exploits	4.4%

- The most common threat family in Croatia in 2Q12 was [Win32/Keygen](#), which affected 13.2 percent of computers with detections in Croatia. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The second most common threat family in Croatia in 2Q12 was [JS/Pornpop](#), which affected 8.4 percent of computers with detections in Croatia. [JS/Pornpop](#) is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The third most common threat family in Croatia in 2Q12 was [Win32/Autorun](#), which affected 7.3 percent of computers with detections in Croatia. [Win32/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 threat family in Croatia in 2Q12 was [Win32/Pushbot](#), which affected 6.5 percent of computers with detections in Croatia. [Win32/Pushbot](#) is a detection for a family of malware that spreads via MSN Messenger, Yahoo! Messenger and AIM when commanded by a remote attacker. It contains backdoor functionality that allows unauthorized access and control of an affected computer.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Croatia

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	0.59 (1.6)	1.06 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	2.25 (3.9)	2.01 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.20 (0.7)	0.26 (0.9)

Update service usage

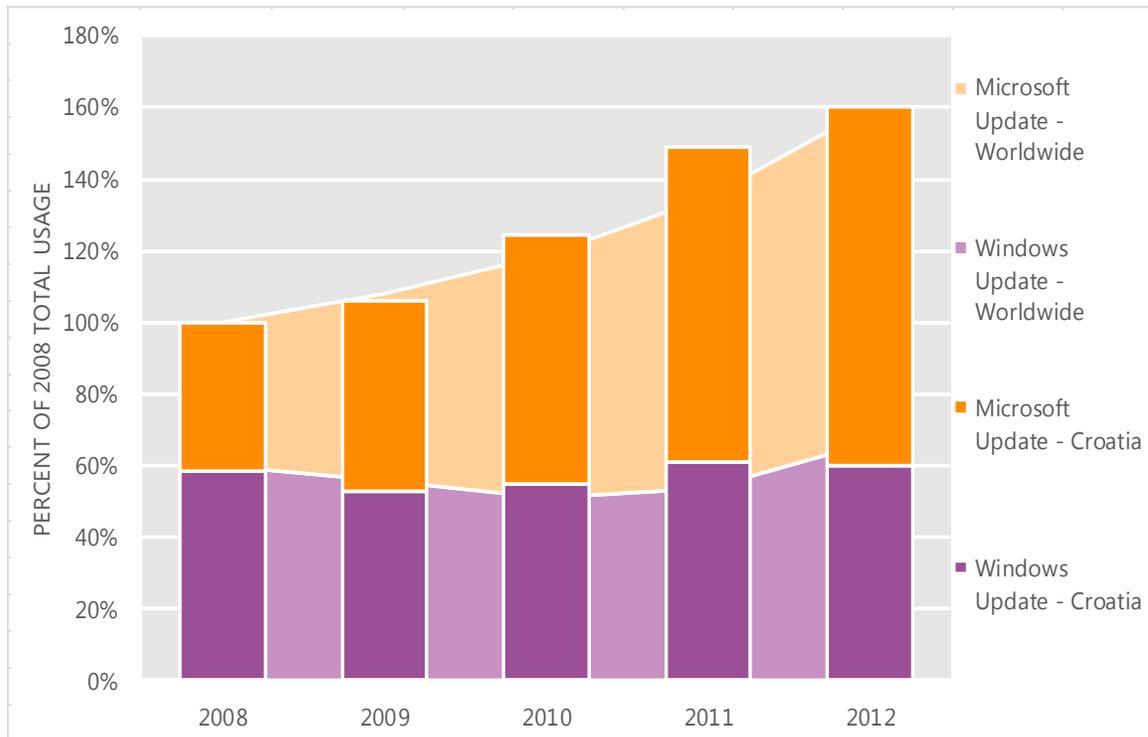
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Croatia and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Croatia over the last four years, indexed to the total usage for both services in Croatia in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Croatia was up 7.7 percent from 2011, and up 60.3 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Croatia in 2012, 62.5 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Cyprus

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Cyprus in 2Q12 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.

Infection rate statistics for Cyprus

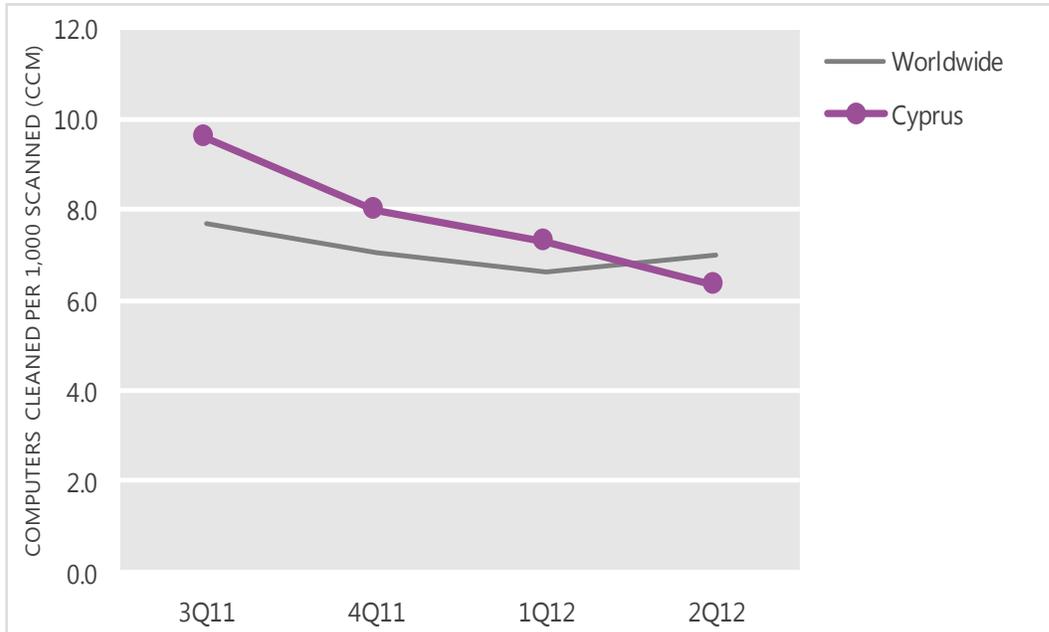
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	9.6	8.0	7.3	6.3
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

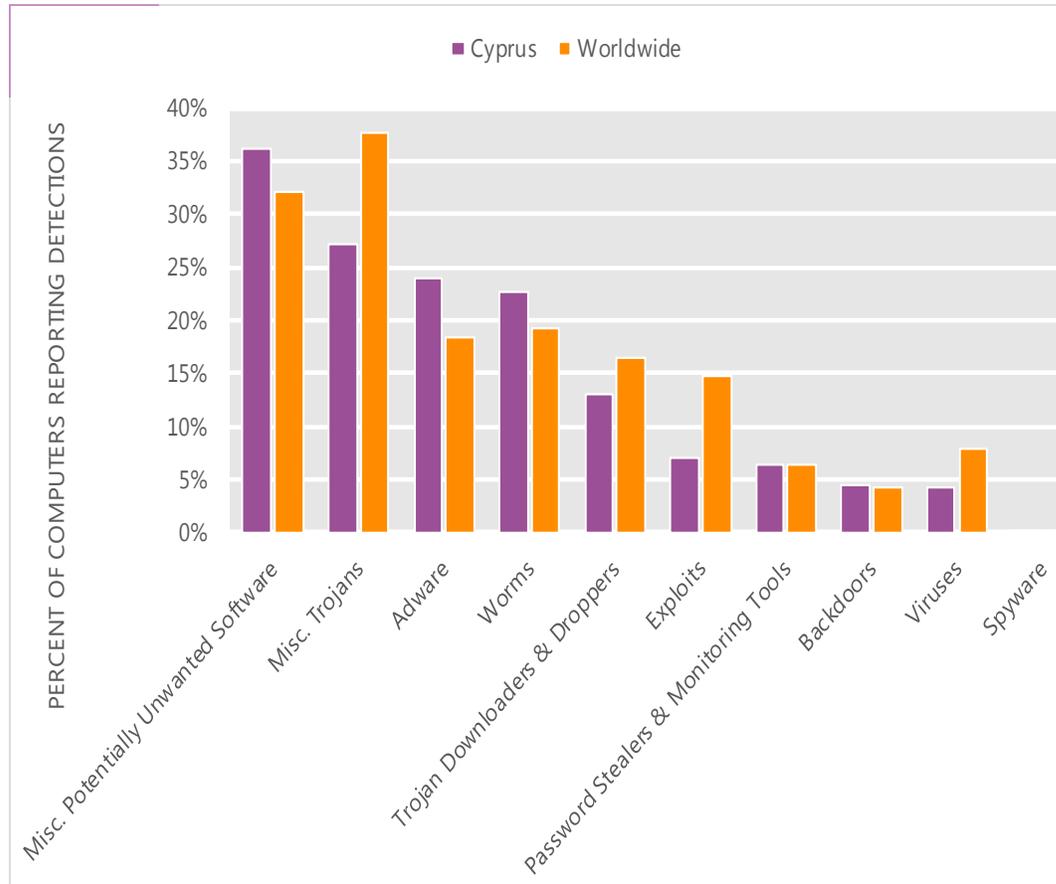
The MSRT detected malware on 6.3 of every 1,000 computers scanned in Cyprus in 2Q12 (a CCM score of 6.3, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Cyprus over the last four quarters, compared to the world as a whole.

CCM infection trends in Cyprus and worldwide



Threat categories

Malware and potentially unwanted software categories in Cyprus in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Cyprus in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 36.2 percent of all computers with detections there, down from 37.6 percent in 1Q12.
- The second most common category in Cyprus in 2Q12 was Miscellaneous Trojans. It affected 27.1 percent of all computers with detections there, down from 27.1 percent in 1Q12.
- The third most common category in Cyprus in 2Q12 was Adware, which affected 24.0 percent of all computers with detections there, down from 30.2 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Cyprus in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Keygen	Misc. Potentially Unwanted Software	11.7%
2	Win32/Hotbar	Adware	10.0%
3	JS/Pornpop	Adware	9.6%
4	Win32/Autorun	Worms	8.6%
5	Win32/Zwangi	Misc. Potentially Unwanted Software	8.1%
6	ASX/Wimad	Trojan Downloaders & Droppers	5.2%
7	Win32/Conficker	Worms	4.9%
8	Win32/Rimecud	Worms	4.0%
9	Win32/Sality	Viruses	3.1%
10	JS/IframeRef	Misc. Trojans	3.1%

- The most common threat family in Cyprus in 2Q12 was [Win32/Keygen](#), which affected 11.7 percent of computers with detections in Cyprus. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The second most common threat family in Cyprus in 2Q12 was [Win32/Hotbar](#), which affected 10.0 percent of computers with detections in Cyprus. [Win32/Hotbar](#) is adware that displays a dynamic toolbar and targeted pop-up ads based on its monitoring of web-browsing activity.
- The third most common threat family in Cyprus in 2Q12 was [JS/Pornpop](#), which affected 9.6 percent of computers with detections in Cyprus. [JS/Pornpop](#) is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The fourth most common threat family in Cyprus in 2Q12 was [Win32/Autorun](#), which affected 8.6 percent of computers with detections in Cyprus. [Win32/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.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Cyprus

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts <i>(Worldwide)</i>	6.11 <i>(1.6)</i>	5.43 <i>(1.8)</i>
Malware hosting sites per 1,000 hosts <i>(Worldwide)</i>	8.14 <i>(3.9)</i>	5.77 <i>(4.4)</i>
Drive-by download per 1,000 URLs <i>(Worldwide)</i>	4.21 <i>(0.7)</i>	6.98 <i>(0.9)</i>

Update service usage

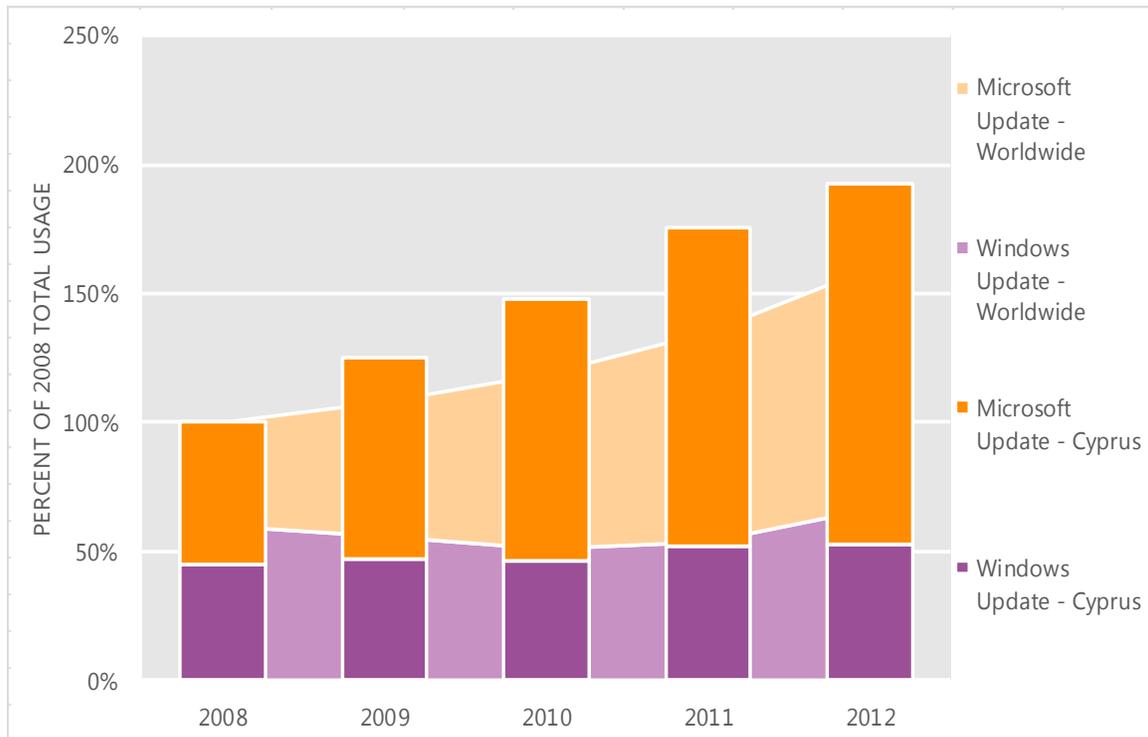
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Cyprus and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Cyprus over the last four years, indexed to the total usage for both services in Cyprus in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Cyprus was up 9.8 percent from 2011, and up 92.7 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Cyprus in 2012, 72.6 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Czech Republic

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in the Czech Republic in 2Q12 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.

Infection rate statistics for the Czech Republic

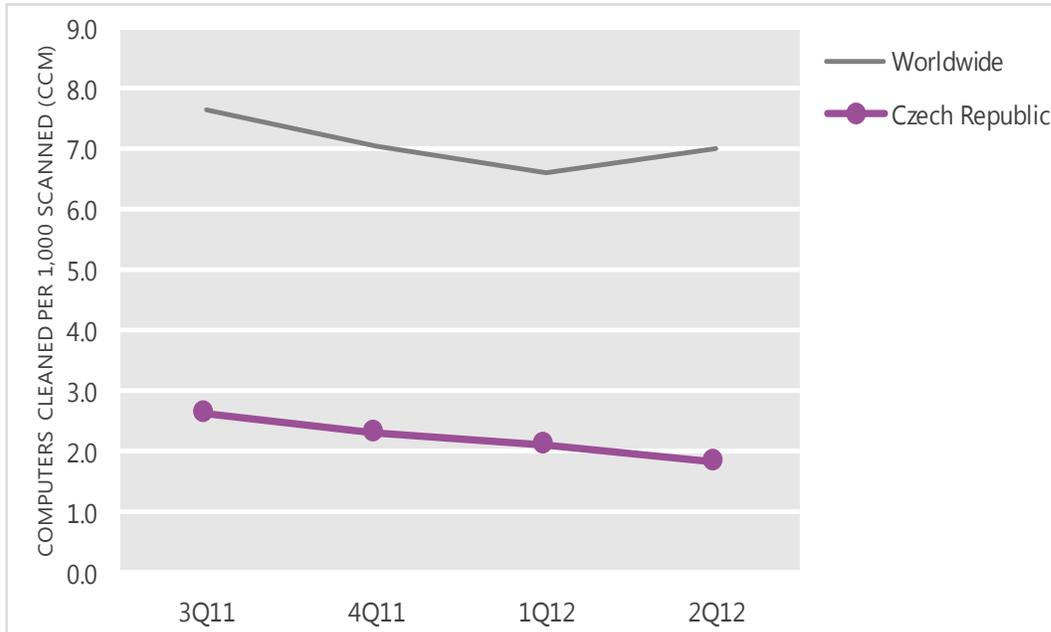
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	2.6	2.3	2.1	1.8
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

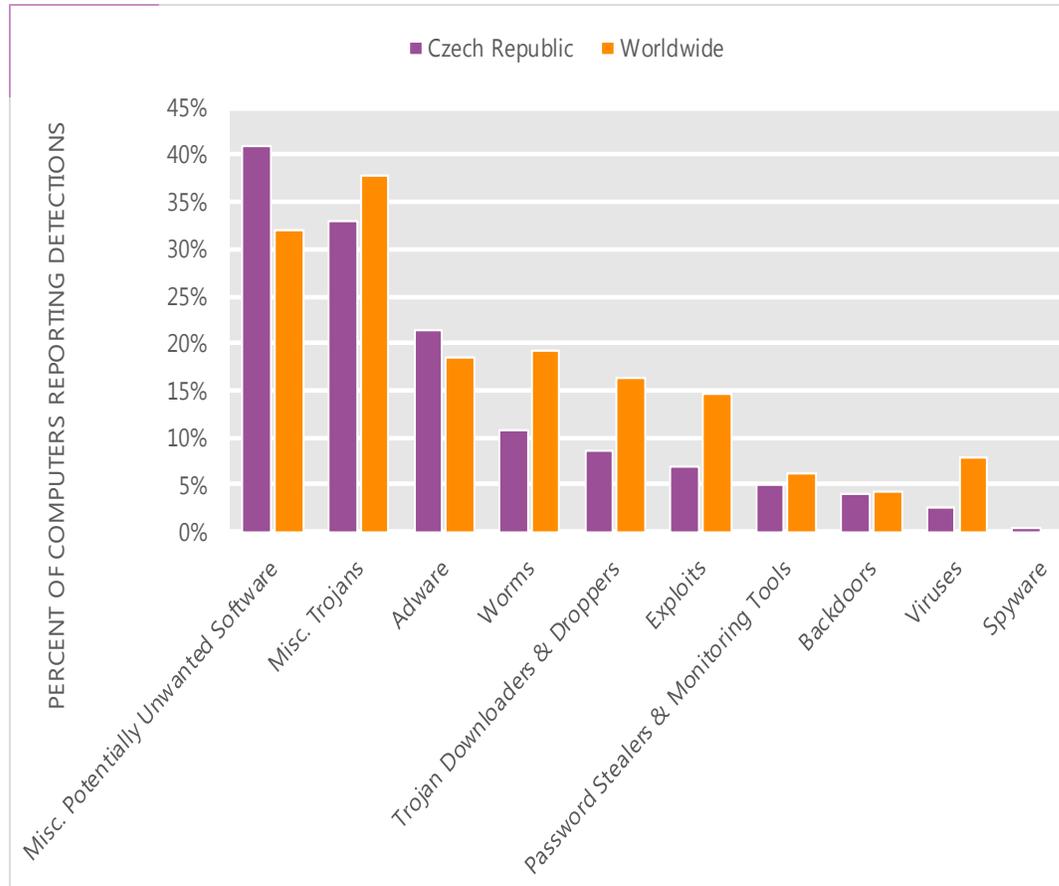
The MSRT detected malware on 1.8 of every 1,000 computers scanned in the Czech Republic in 2Q12 (a CCM score of 1.8, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for the Czech Republic over the last four quarters, compared to the world as a whole.

CCM infection trends in the Czech Republic and worldwide



Threat categories

Malware and potentially unwanted software categories in the Czech Republic in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in the Czech Republic in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 40.9 percent of all computers with detections there, up from 40.1 percent in 1Q12.
- The second most common category in the Czech Republic in 2Q12 was Miscellaneous Trojans. It affected 33.0 percent of all computers with detections there, up from 32.9 percent in 1Q12.
- The third most common category in the Czech Republic in 2Q12 was Adware, which affected 21.5 percent of all computers with detections there, down from 25.7 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in the Czech Republic in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Keygen	Misc. Potentially Unwanted Software	19.3%
2	JS/Pornpop	Adware	9.9%
3	Win32/Obfuscator	Misc. Potentially Unwanted Software	6.0%
4	JS/IframeRef	Misc. Trojans	5.5%
5	Win32/OpenCandy	Adware	4.4%
6	Win32/Hotbar	Adware	4.1%
7	Win32/Dynamer	Misc. Trojans	4.1%
8	Win32/Zwangi	Misc. Potentially Unwanted Software	3.6%
9	Win32/Autorun	Worms	3.3%
10	Win32/Sirefef	Misc. Trojans	3.2%

- The most common threat family in the Czech Republic in 2Q12 was [Win32/Keygen](#), which affected 19.3 percent of computers with detections in the Czech Republic. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The second most common threat family in the Czech Republic in 2Q12 was [JS/Pornpop](#), which affected 9.9 percent of computers with detections in the Czech Republic. [JS/Pornpop](#) is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The third most common threat family in the Czech Republic in 2Q12 was [Win32/Obfuscator](#), which affected 6.0 percent of computers with detections in the Czech Republic. [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 threat family in the Czech Republic in 2Q12 was [JS/IframeRef](#), which affected 5.5 percent of computers with detections in the Czech Republic. [JS/IframeRef](#) is a generic detection for specially formed IFrame tags that point to remote websites that contain malicious content.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for the Czech Republic

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	1.25 (1.6)	1.42 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	2.86 (3.9)	3.03 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.44 (0.7)	0.54 (0.9)

Update service usage

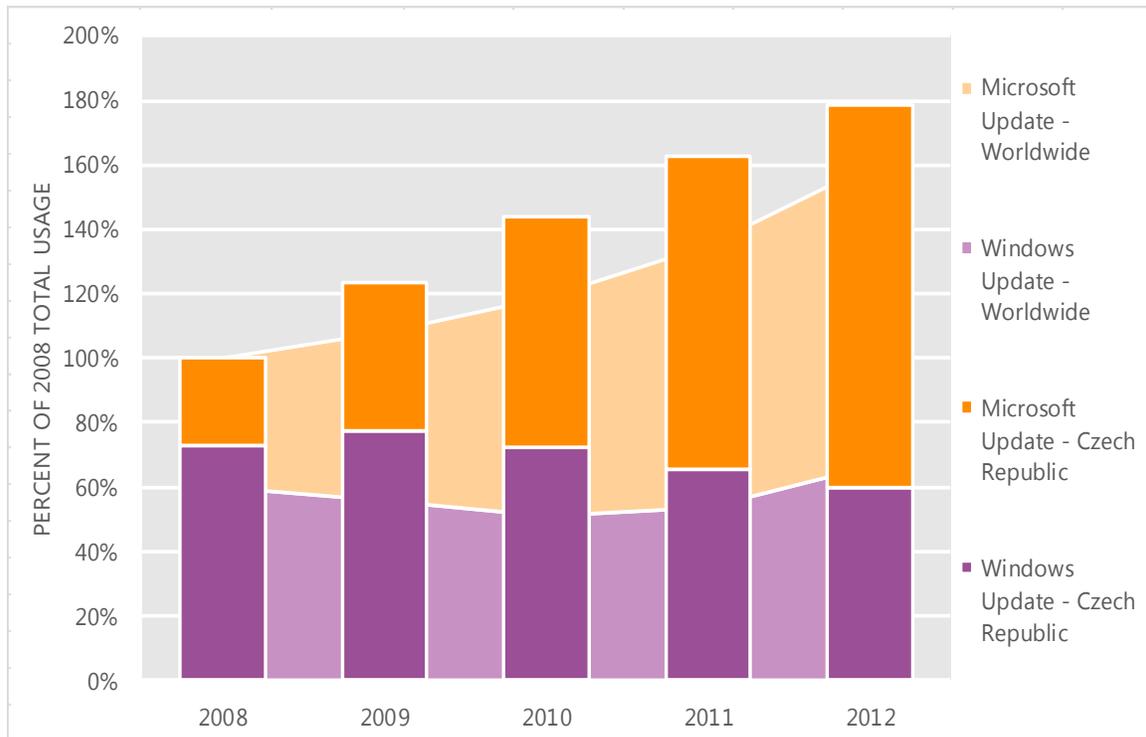
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in the Czech Republic and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in the Czech Republic over the last four years, indexed to the total usage for both services in the Czech Republic in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in the Czech Republic was up 9.7 percent from 2011, and up 78.4 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in the Czech Republic in 2012, 66.4 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Denmark

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Denmark in 2Q12 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.

Infection rate statistics for Denmark

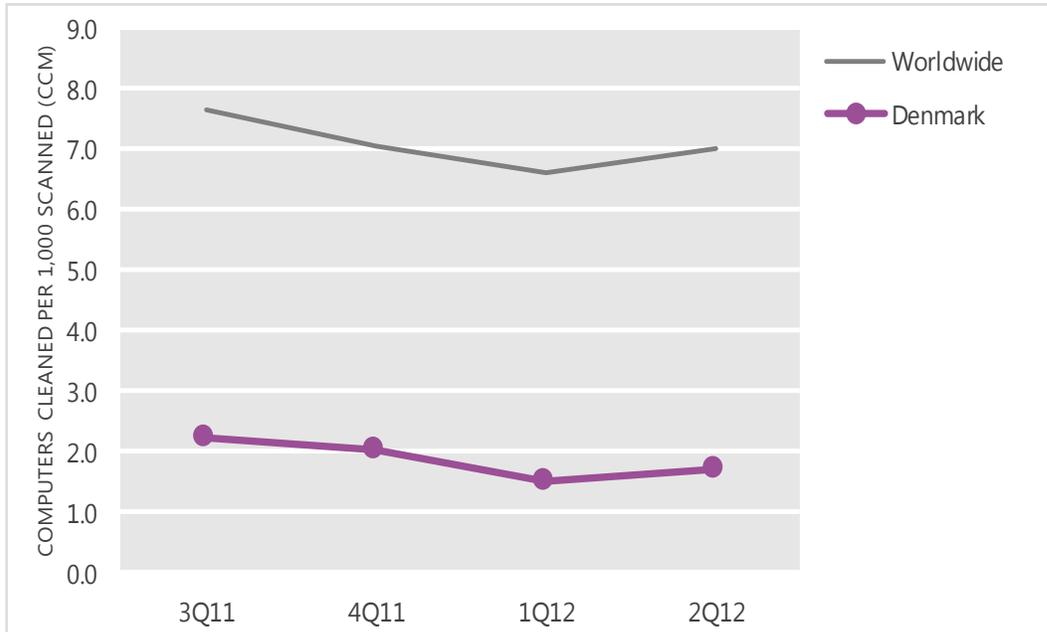
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	2.2	2.0	1.5	1.7
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

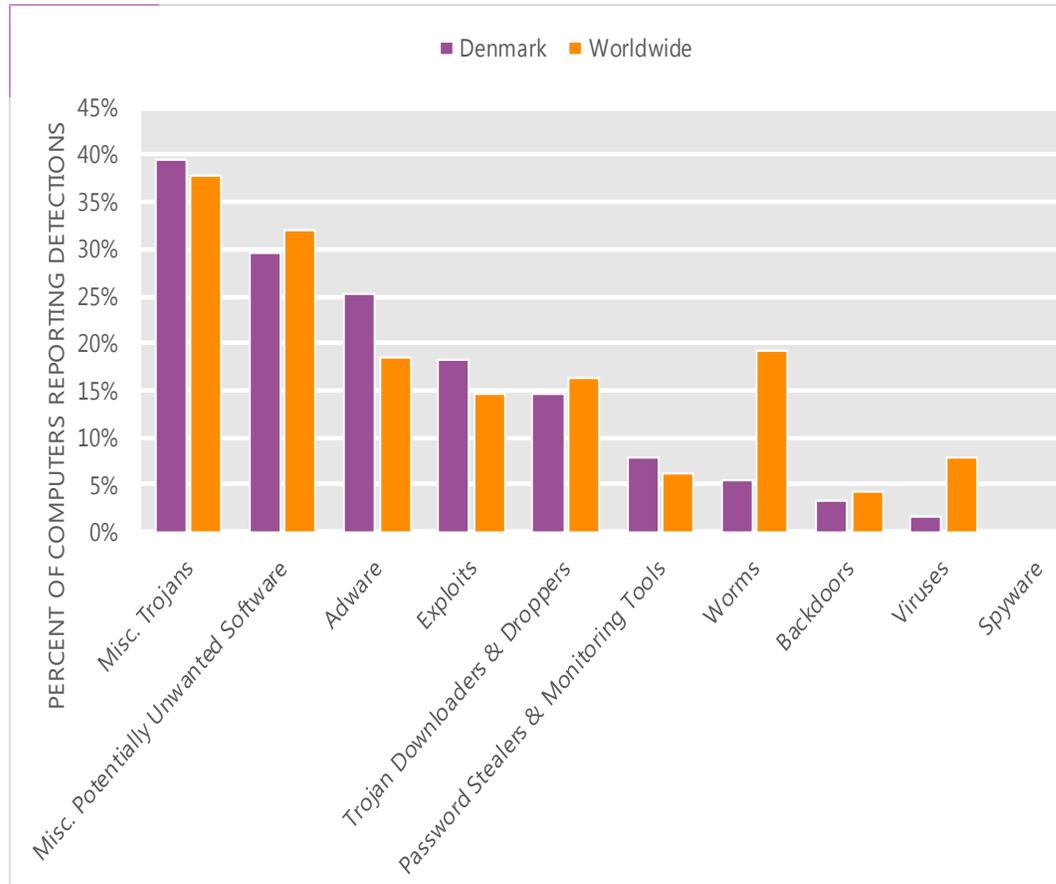
The MSRT detected malware on 1.7 of every 1,000 computers scanned in Denmark in 2Q12 (a CCM score of 1.7, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Denmark over the last four quarters, compared to the world as a whole.

CCM infection trends in Denmark and worldwide



Threat categories

Malware and potentially unwanted software categories in Denmark in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Denmark in 2Q12 was Miscellaneous Trojans. It affected 39.6 percent of all computers with detections there, up from 30.4 percent in 1Q12.
- The second most common category in Denmark in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 29.6 percent of all computers with detections there, down from 34.6 percent in 1Q12.
- The third most common category in Denmark in 2Q12 was Adware, which affected 25.2 percent of all computers with detections there, down from 34.9 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Denmark in 2Q12

	Family	Most significant category	% of computers with detections
1	JS/Pornpop	Adware	13.6%
2	Win32/Keygen	Misc. Potentially Unwanted Software	11.2%
3	Java/Blacole	Exploits	10.3%
4	Win32/Hotbar	Adware	8.9%
5	Win32/Sirefef	Misc. Trojans	8.0%
6	Win32/FakePAV	Misc. Trojans	8.0%
7	JS/IframeRef	Misc. Trojans	5.7%
8	Java/CVE-2012-0507	Exploits	5.4%
9	Win32/Winwebsec	Misc. Trojans	5.0%
10	ASX/Wimad	Trojan Downloaders & Droppers	5.0%

- The most common threat family in Denmark in 2Q12 was [JS/Pornpop](#), which affected 13.6 percent of computers with detections in Denmark. [JS/Pornpop](#) is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The second most common threat family in Denmark in 2Q12 was [Win32/Keygen](#), which affected 11.2 percent of computers with detections in Denmark. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The third most common threat family in Denmark in 2Q12 was [Java/Blacole](#), which affected 10.3 percent of computers with detections in Denmark. [Java/Blacole](#) is an exploit pack, also known as Blackhole, that is installed on a compromised web server by an attacker and includes a number of exploits that target browser software. If a vulnerable computer browses a compromised website that contains the exploit pack, various malware may be downloaded and run.
- The fourth most common threat family in Denmark in 2Q12 was [Win32/Hotbar](#), which affected 8.9 percent of computers with detections in Denmark. [Win32/Hotbar](#) is adware that displays a dynamic toolbar and targeted pop-up ads based on its monitoring of web-browsing activity.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Denmark

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	3.83 (1.6)	4.08 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	3.73 (3.9)	3.83 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.27 (0.7)	0.61 (0.9)

Update service usage

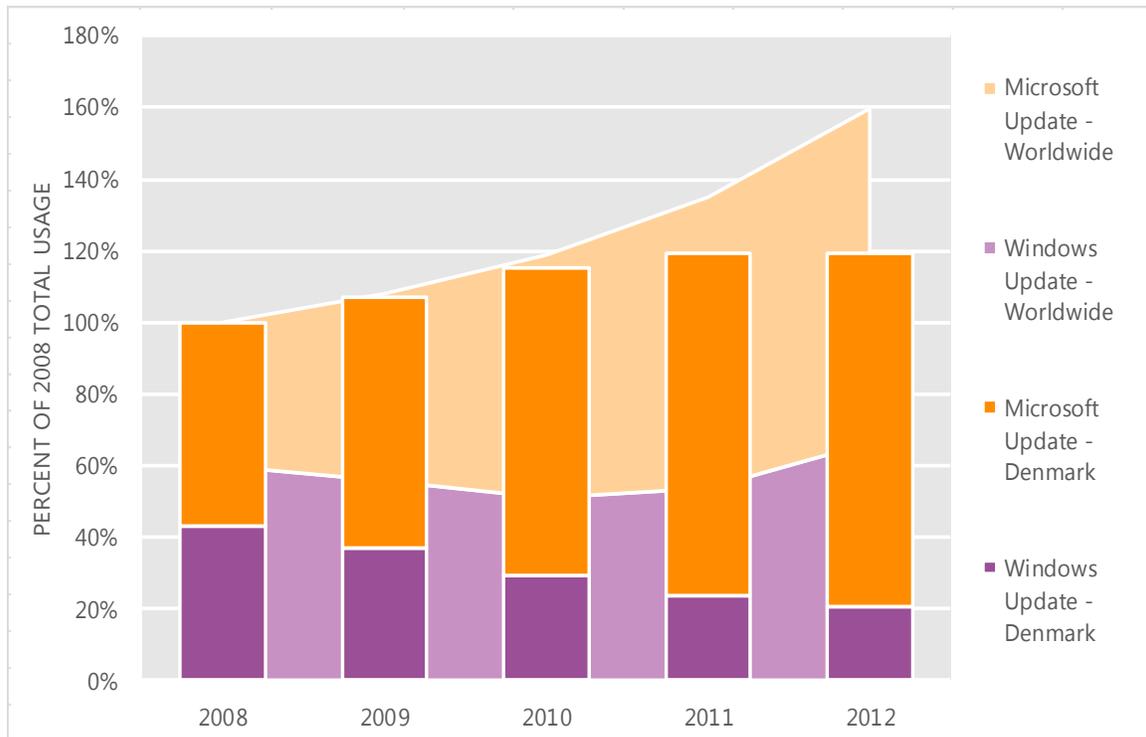
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Denmark and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Denmark over the last four years, indexed to the total usage for both services in Denmark in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Denmark was down 0.0 percent from 2011, and up 19.2 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Denmark in 2012, 82.6 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Dominican Republic

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in the Dominican Republic in 2Q12 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.

Infection rate statistics for the Dominican Republic

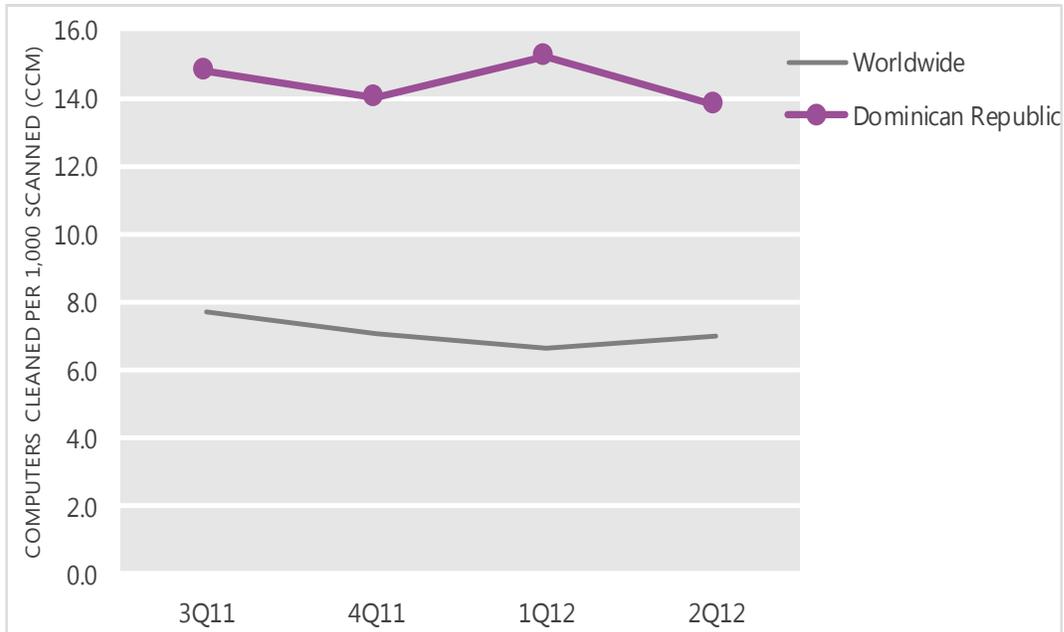
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	14.8	14.0	15.2	13.8
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

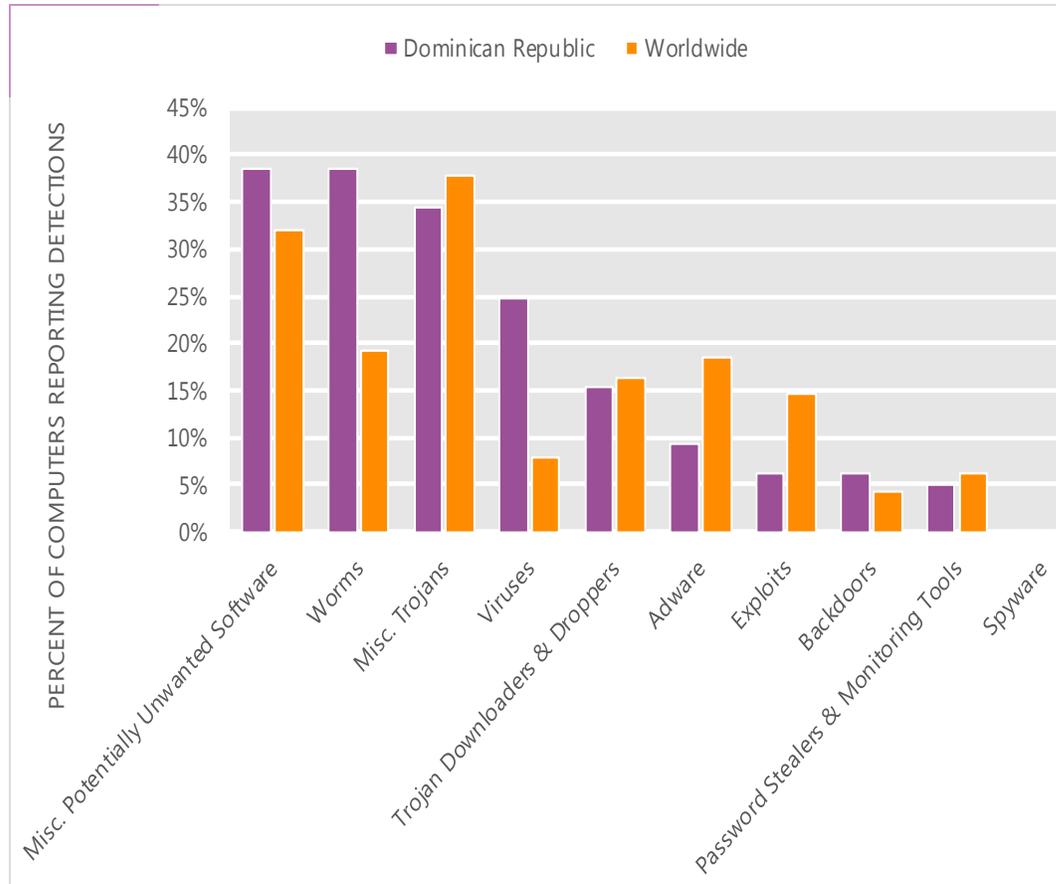
The MSRT detected malware on 13.8 of every 1,000 computers scanned in the Dominican Republic in 2Q12 (a CCM score of 13.8, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for the Dominican Republic over the last four quarters, compared to the world as a whole.

CCM infection trends in the Dominican Republic and worldwide



Threat categories

Malware and potentially unwanted software categories in the Dominican Republic in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in the Dominican Republic in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 38.6 percent of all computers with detections there, down from 40.1 percent in 1Q12.
- The second most common category in the Dominican Republic in 2Q12 was Worms. It affected 38.5 percent of all computers with detections there, down from 38.5 percent in 1Q12.
- The third most common category in the Dominican Republic in 2Q12 was Miscellaneous Trojans, which affected 34.5 percent of all computers with detections there, up from 32.1 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in the Dominican Republic in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Sality	Viruses	23.5%
2	Win32/Autorun	Worms	20.3%
3	Win32/Dorkbot	Worms	10.2%
4	Win32/Keygen	Misc. Potentially Unwanted Software	10.0%
5	Win32/Vobfus	Worms	9.0%
6	Win32/Brontok	Worms	7.0%
7	Win32/Rimecud	Worms	7.0%
8	ASX/Wimad	Trojan Downloaders & Droppers	4.9%
9	Win32/Silly_P2P	Worms	4.8%
10	Win32/Conficker	Worms	4.3%

- The most common threat family in the Dominican Republic in 2Q12 was [Win32/Sality](#), which affected 23.5 percent of computers with detections in the Dominican Republic. [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 in the Dominican Republic in 2Q12 was [Win32/Autorun](#), which affected 20.3 percent of computers with detections in the Dominican Republic. [Win32/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 threat family in the Dominican Republic in 2Q12 was [Win32/Dorkbot](#), which affected 10.2 percent of computers with detections in the Dominican Republic. [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 in the Dominican Republic in 2Q12 was [Win32/Keygen](#), which affected 10.0 percent of computers with detections in the Dominican Republic. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for the Dominican Republic

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	0.47 (1.6)	0.71 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	2.84 (3.9)	1.66 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.00 (0.7)	0.00 (0.9)

Update service usage

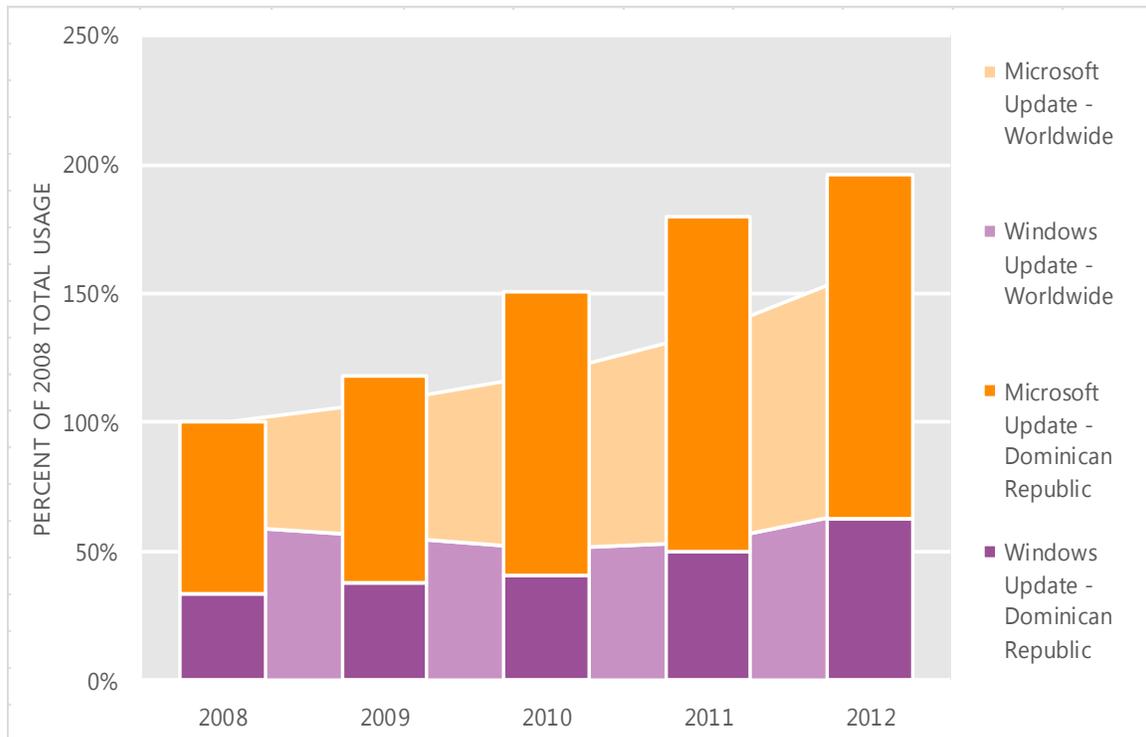
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in the Dominican Republic and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in the Dominican Republic over the last four years, indexed to the total usage for both services in the Dominican Republic in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in the Dominican Republic was up 8.9 percent from 2011, and up 96.2 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in the Dominican Republic in 2012, 68.2 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Ecuador

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Ecuador in 2Q12 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.

Infection rate statistics for Ecuador

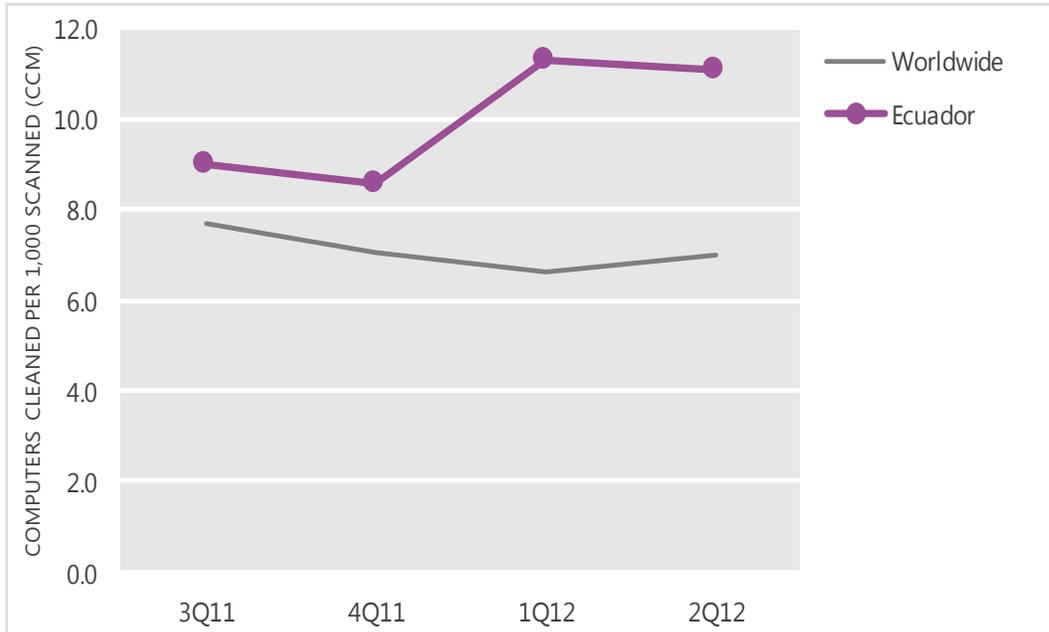
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	9.0	8.6	11.3	11.1
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

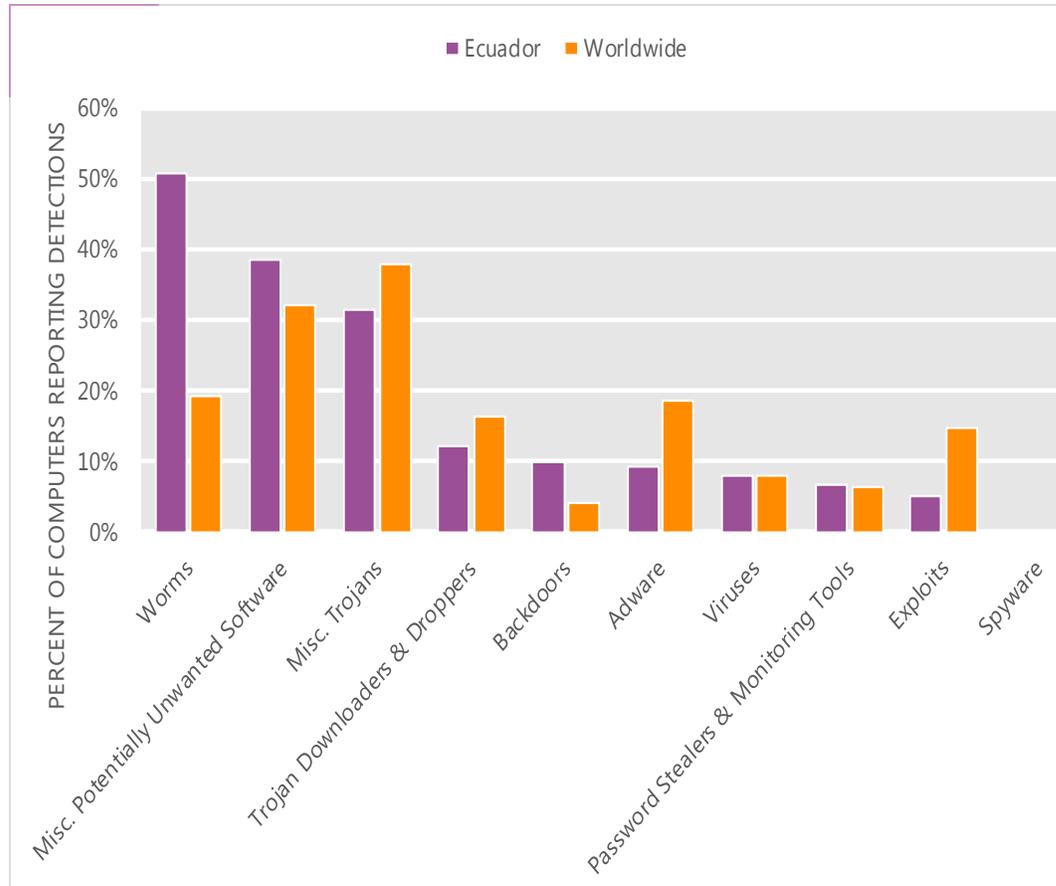
The MSRT detected malware on 11.1 of every 1,000 computers scanned in Ecuador in 2Q12 (a CCM score of 11.1, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Ecuador over the last four quarters, compared to the world as a whole.

CCM infection trends in Ecuador and worldwide



Threat categories

Malware and potentially unwanted software categories in Ecuador in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Ecuador in 2Q12 was Worms. It affected 50.6 percent of all computers with detections there, up from 47.8 percent in 1Q12.
- The second most common category in Ecuador in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 38.6 percent of all computers with detections there, down from 43.5 percent in 1Q12.
- The third most common category in Ecuador in 2Q12 was Miscellaneous Trojans, which affected 31.6 percent of all computers with detections there, up from 25.7 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Ecuador in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Dorkbot	Worms	29.9%
2	Win32/Autorun	Worms	13.2%
3	Win32/Keygen	Misc. Potentially Unwanted Software	12.9%
4	Win32/Vobfus	Worms	11.4%
5	Win32/VBInject	Misc. Potentially Unwanted Software	8.4%
6	Win32/Conficker	Worms	5.5%
7	Win32/Sality	Viruses	5.4%
8	Win32/Sirefef	Misc. Trojans	4.5%
9	Win32/IRCbot	Backdoors	4.0%
10	ASX/Wimad	Trojan Downloaders & Droppers	3.2%

- The most common threat family in Ecuador in 2Q12 was [Win32/Dorkbot](#), which affected 29.9 percent of computers with detections in Ecuador. [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 second most common threat family in Ecuador in 2Q12 was [Win32/Autorun](#), which affected 13.2 percent of computers with detections in Ecuador. [Win32/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 threat family in Ecuador in 2Q12 was [Win32/Keygen](#), which affected 12.9 percent of computers with detections in Ecuador. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The fourth most common threat family in Ecuador in 2Q12 was [Win32/Vobfus](#), which affected 11.4 percent of computers with detections in Ecuador. [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.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Ecuador

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	0.73 (1.6)	0.94 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	0.52 (3.9)	1.15 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.01 (0.7)	0.05 (0.9)

Update service usage

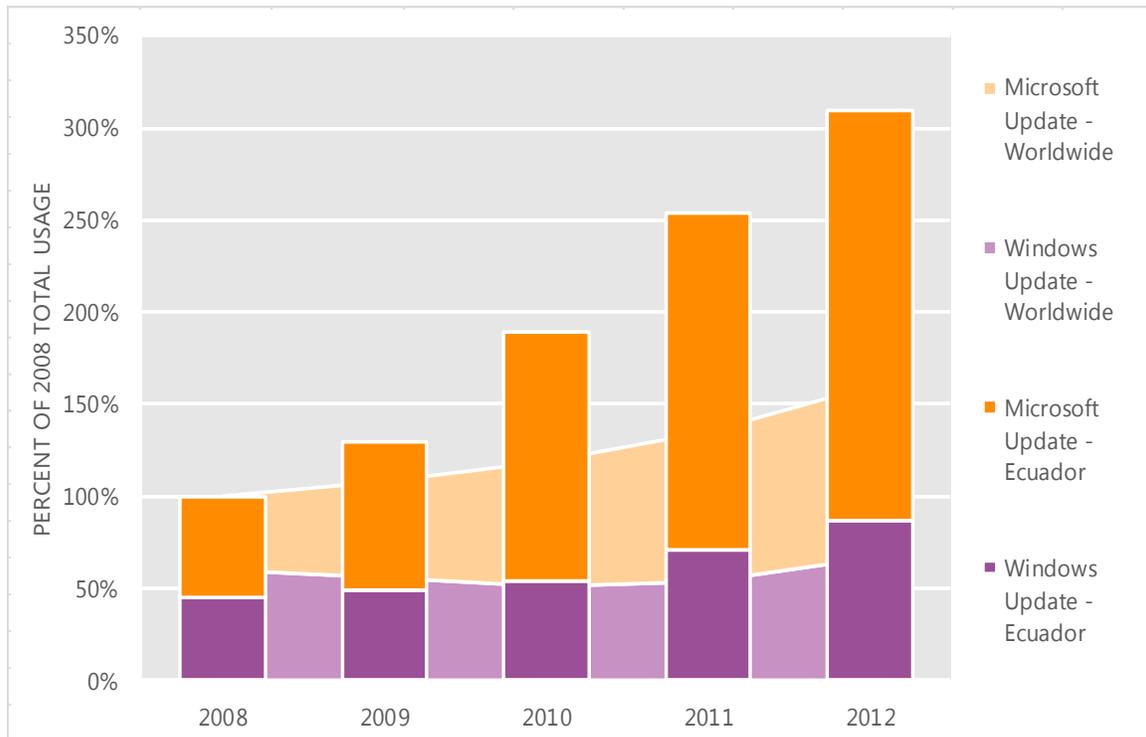
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Ecuador and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Ecuador over the last four years, indexed to the total usage for both services in Ecuador in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Ecuador was up 22.3 percent from 2011, and up 209.9 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Ecuador in 2012, 71.9 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Egypt

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Egypt in 2Q12 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.

Infection rate statistics for Egypt

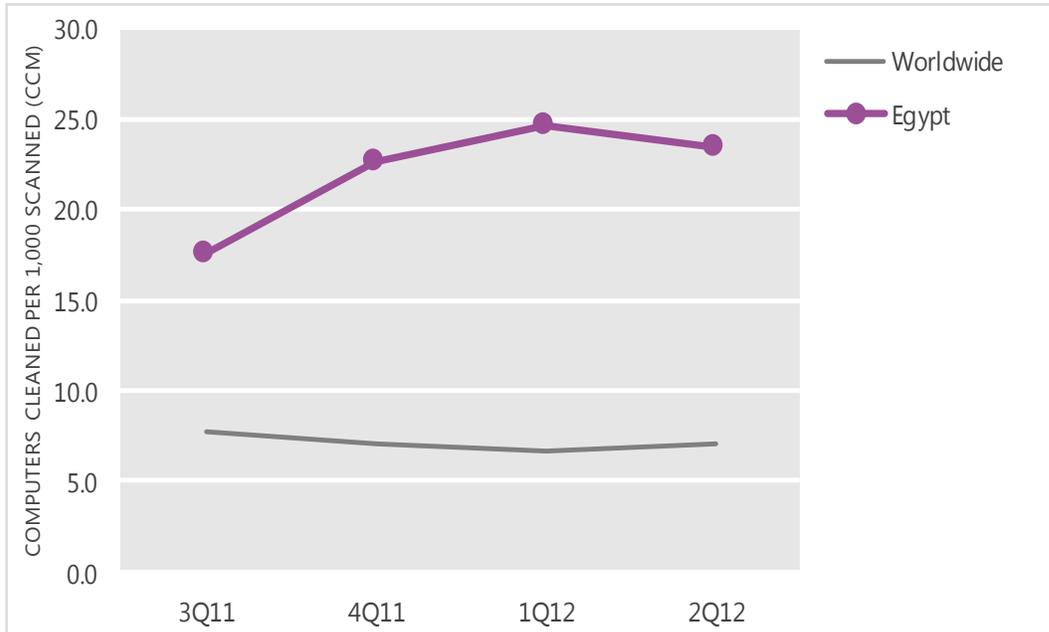
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	17.5	22.7	24.7	23.4
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

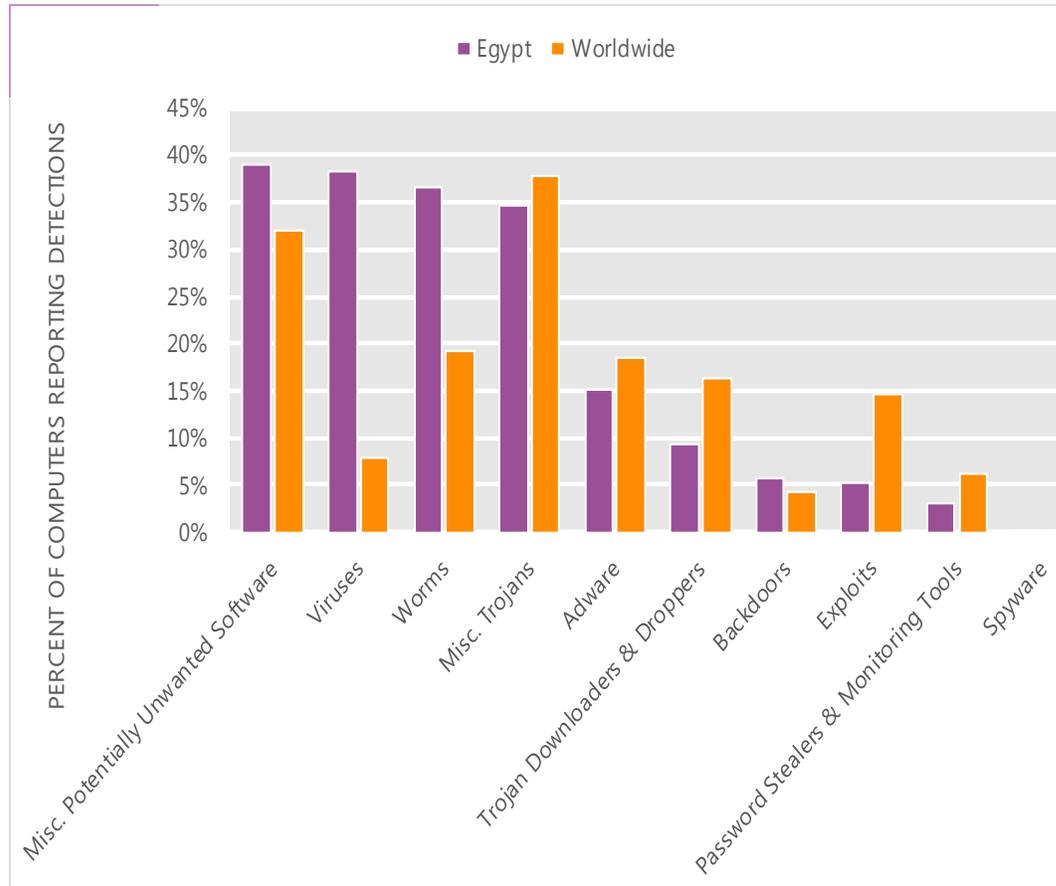
The MSRT detected malware on 23.4 of every 1,000 computers scanned in Egypt in 2Q12 (a CCM score of 23.4, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Egypt over the last four quarters, compared to the world as a whole.

CCM infection trends in Egypt and worldwide



Threat categories

Malware and potentially unwanted software categories in Egypt in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Egypt in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 39.0 percent of all computers with detections there, down from 39.4 percent in 1Q12.
- The second most common category in Egypt in 2Q12 was Viruses. It affected 38.2 percent of all computers with detections there, down from 40.3 percent in 1Q12.
- The third most common category in Egypt in 2Q12 was Worms, which affected 36.5 percent of all computers with detections there, up from 36.3 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Egypt in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Sality	Viruses	34.3%
2	Win32/Autorun	Worms	20.4%
3	Win32/Keygen	Misc. Potentially Unwanted Software	19.1%
4	Win32/Dorkbot	Worms	9.7%
5	Win32/Virut	Viruses	7.4%
6	JS/Paypopup	Adware	6.6%
7	Win32/Pramro	Misc. Trojans	6.5%
8	Win32/Agent	Misc. Trojans	5.9%
9	Win32/Nuqel	Worms	5.5%
10	Win32/Ramnit	Misc. Trojans	5.2%

- The most common threat family in Egypt in 2Q12 was [Win32/Sality](#), which affected 34.3 percent of computers with detections in Egypt. [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 in Egypt in 2Q12 was [Win32/Autorun](#), which affected 20.4 percent of computers with detections in Egypt. [Win32/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 threat family in Egypt in 2Q12 was [Win32/Keygen](#), which affected 19.1 percent of computers with detections in Egypt. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The fourth most common threat family in Egypt in 2Q12 was [Win32/Dorkbot](#), which affected 9.7 percent of computers with detections in Egypt. [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.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Egypt

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	0.51 (1.6)	0.61 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	2.85 (3.9)	3.05 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.05 (0.7)	0.09 (0.9)

Update service usage

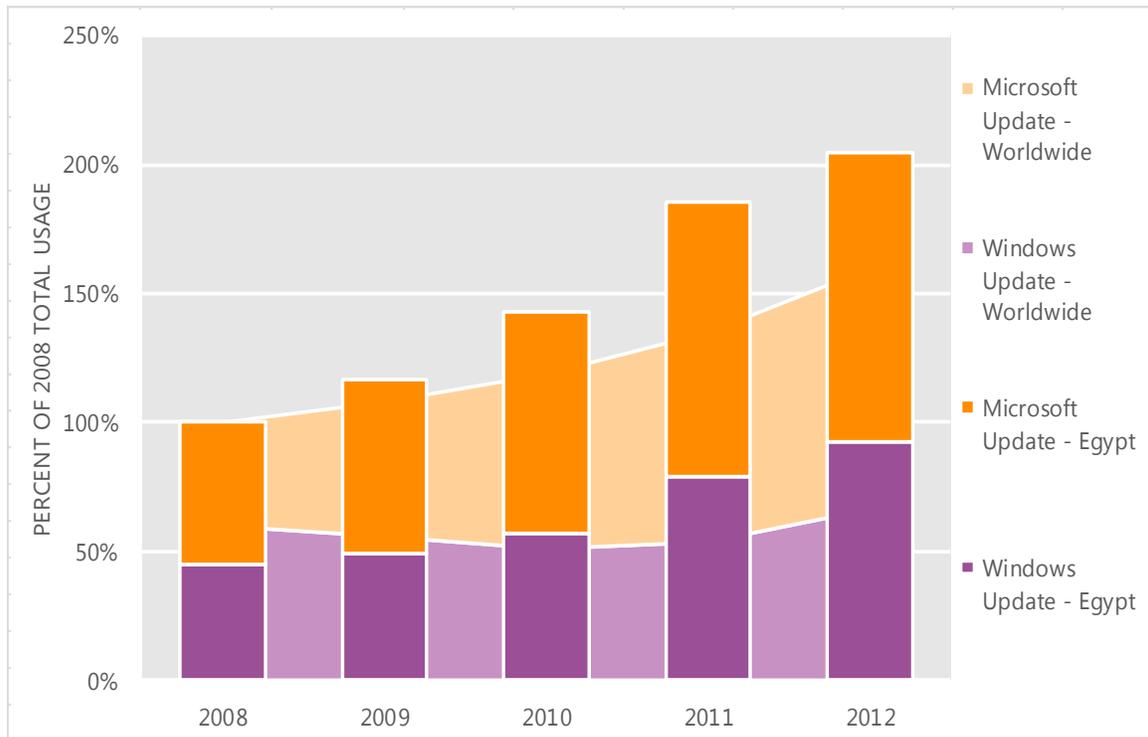
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Egypt and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Egypt over the last four years, indexed to the total usage for both services in Egypt in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Egypt was up 10.2 percent from 2011, and up 104.8 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Egypt in 2012, 54.7 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

El Salvador

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in El Salvador in 2Q12 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.

Infection rate statistics for El Salvador

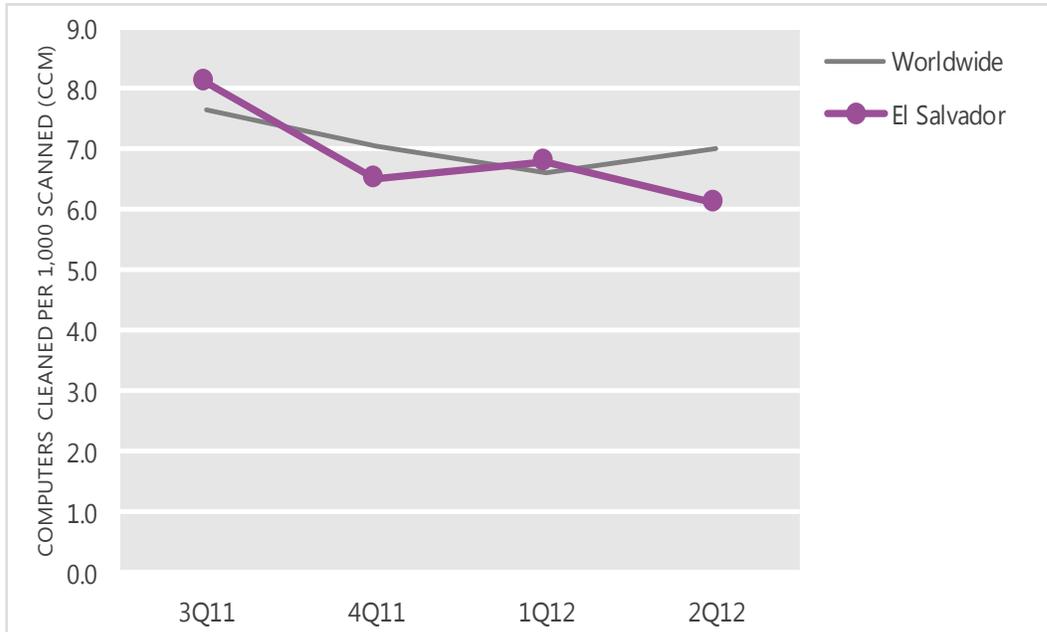
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	8.1	6.5	6.8	6.1
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

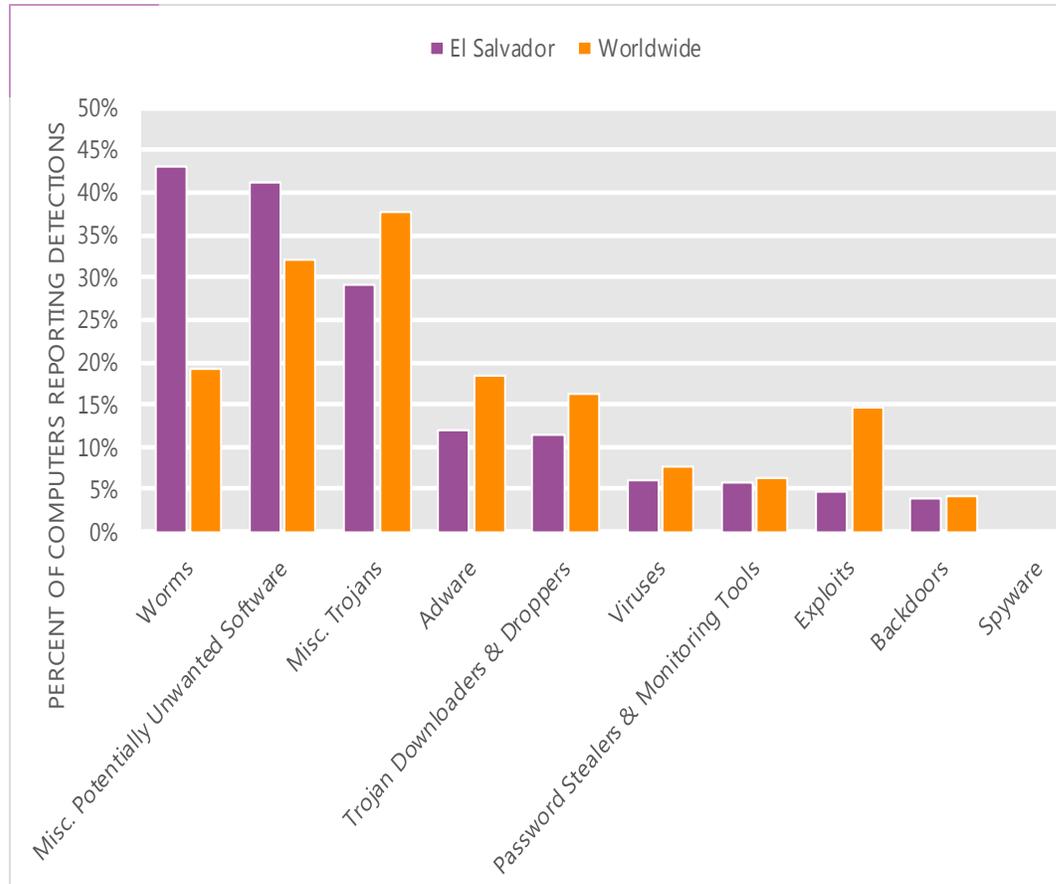
The MSRT detected malware on 6.1 of every 1,000 computers scanned in El Salvador in 2Q12 (a CCM score of 6.1, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for El Salvador over the last four quarters, compared to the world as a whole.

CCM infection trends in El Salvador and worldwide



Threat categories

Malware and potentially unwanted software categories in El Salvador in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in El Salvador in 2Q12 was Worms. It affected 43.0 percent of all computers with detections there, up from 40.3 percent in 1Q12.
- The second most common category in El Salvador in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 41.1 percent of all computers with detections there, down from 45.1 percent in 1Q12.
- The third most common category in El Salvador in 2Q12 was Miscellaneous Trojans, which affected 29.2 percent of all computers with detections there, up from 26.3 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in El Salvador in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Dorkbot	Worms	24.4%
2	Win32/Keygen	Misc. Potentially Unwanted Software	15.7%
3	Win32/Autorun	Worms	14.0%
4	Win32/Vobfus	Worms	7.6%
5	Win32/VBInject	Misc. Potentially Unwanted Software	6.8%
6	Win32/Sality	Viruses	5.4%
7	Win32/Conficker	Worms	4.6%
8	JS/Pornpop	Adware	4.6%
9	Win32/Brontok	Worms	4.5%
10	JS/Redirector	Misc. Trojans	4.2%

- The most common threat family in El Salvador in 2Q12 was [Win32/Dorkbot](#), which affected 24.4 percent of computers with detections in El Salvador. [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 second most common threat family in El Salvador in 2Q12 was [Win32/Keygen](#), which affected 15.7 percent of computers with detections in El Salvador. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The third most common threat family in El Salvador in 2Q12 was [Win32/Autorun](#), which affected 14.0 percent of computers with detections in El Salvador. [Win32/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 threat family in El Salvador in 2Q12 was [Win32/Vobfus](#), which affected 7.6 percent of computers with detections in El Salvador. [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.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for El Salvador

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	0.40 (1.6)	0.40 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	0.40 (3.9)	1.20 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.03 (0.7)	0.00 (0.9)

Update service usage

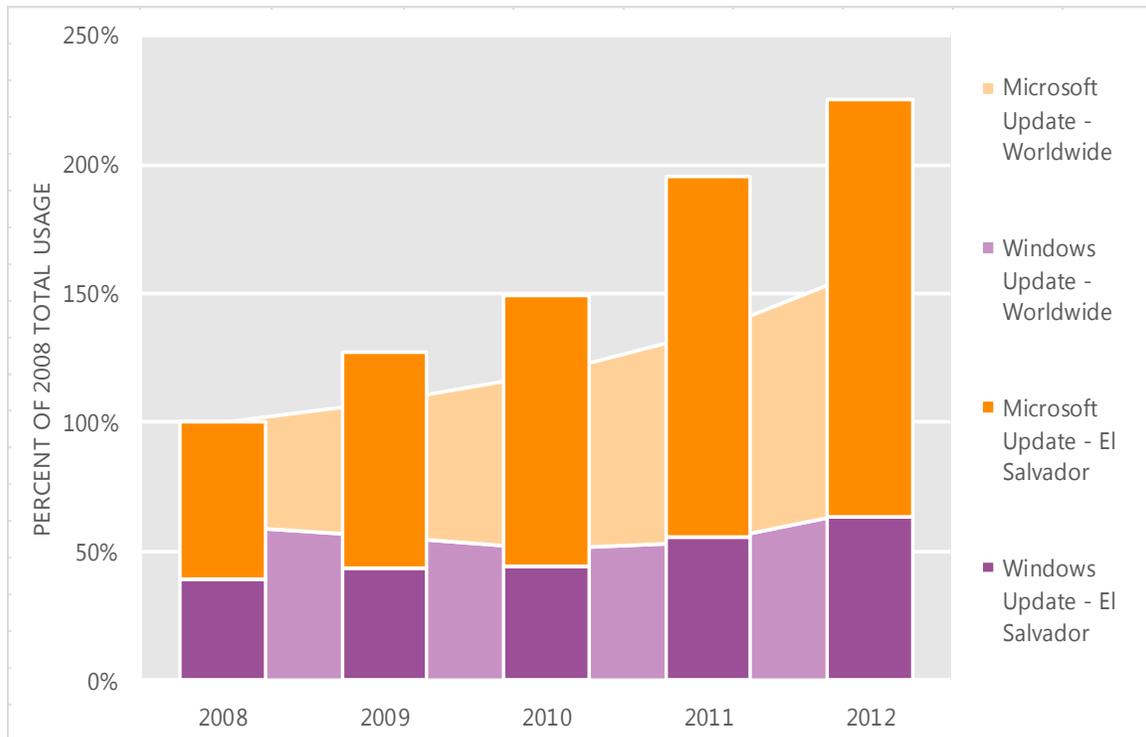
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in El Salvador and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in El Salvador over the last four years, indexed to the total usage for both services in El Salvador in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in El Salvador was up 15.4 percent from 2011, and up 125.4 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in El Salvador in 2012, 72.0 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Estonia

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Estonia in 2Q12 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.

Infection rate statistics for Estonia

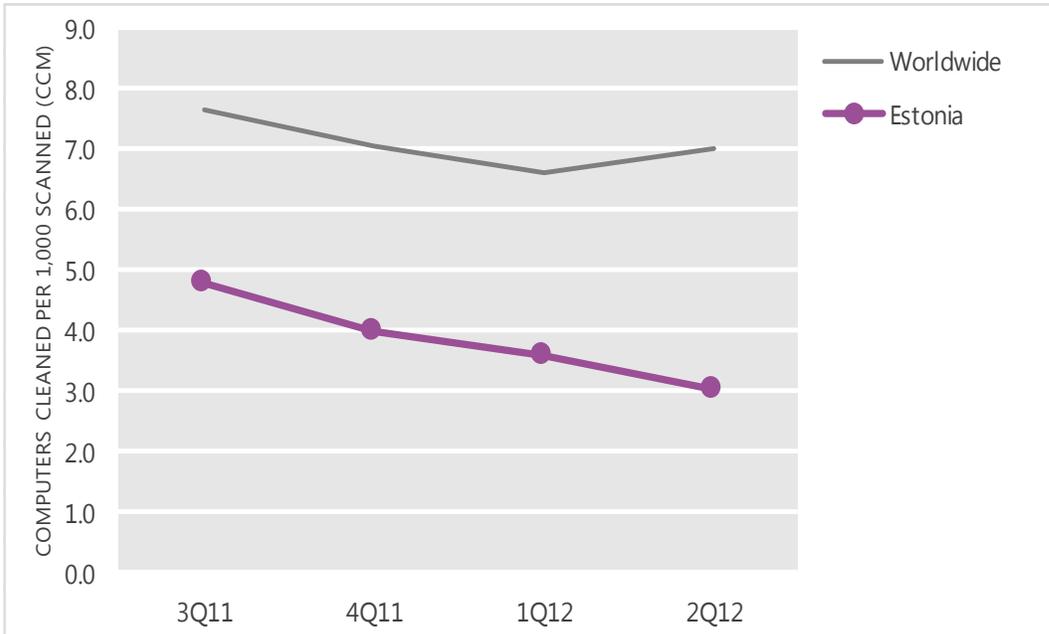
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	4.8	4.0	3.6	3.0
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

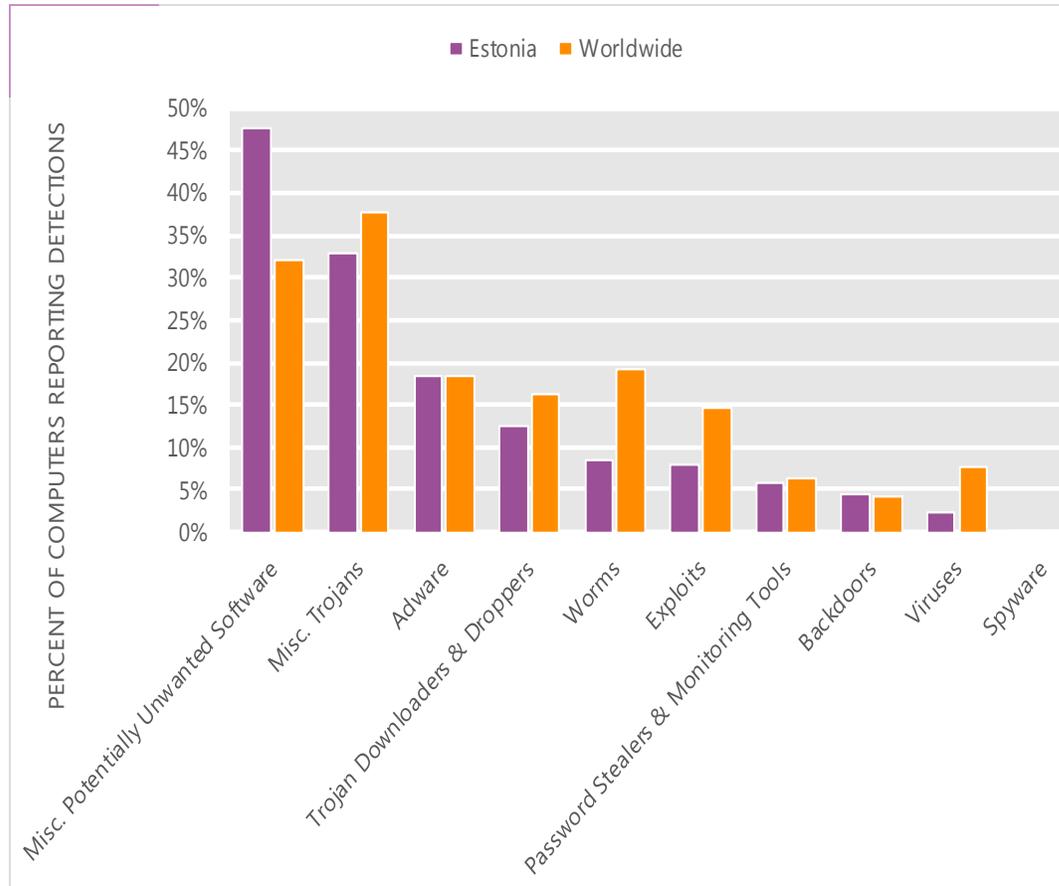
The MSRT detected malware on 3.0 of every 1,000 computers scanned in Estonia in 2Q12 (a CCM score of 3.0, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Estonia over the last four quarters, compared to the world as a whole.

CCM infection trends in Estonia and worldwide



Threat categories

Malware and potentially unwanted software categories in Estonia in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Estonia in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 47.6 percent of all computers with detections there, down from 47.8 percent in 1Q12.
- The second most common category in Estonia in 2Q12 was Miscellaneous Trojans. It affected 32.8 percent of all computers with detections there, up from 29.5 percent in 1Q12.
- The third most common category in Estonia in 2Q12 was Adware, which affected 18.4 percent of all computers with detections there, down from 24.5 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Estonia in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Keygen	Misc. Potentially Unwanted Software	16.8%
2	Win32/Pameseg	Misc. Potentially Unwanted Software	9.5%
3	Win32/Hotbar	Adware	7.4%
4	JS/Pornpop	Adware	7.2%
5	JS/IframeRef	Misc. Trojans	6.8%
6	Win32/Obfuscator	Misc. Potentially Unwanted Software	6.6%
7	Win32/Zwangi	Misc. Potentially Unwanted Software	5.8%
8	ASX/Wimad	Trojan Downloaders & Droppers	5.4%
9	Win32/Dynamer	Misc. Trojans	3.1%
10	JS/Redirector	Misc. Trojans	3.1%

- The most common threat family in Estonia in 2Q12 was [Win32/Keygen](#), which affected 16.8 percent of computers with detections in Estonia. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The second most common threat family in Estonia in 2Q12 was [Win32/Pameseg](#), which affected 9.5 percent of computers with detections in Estonia. [Win32/Pameseg](#) is a fake program installer that requires the user to send SMS messages to a premium number to successfully install certain programs.
- The third most common threat family in Estonia in 2Q12 was [Win32/Hotbar](#), which affected 7.4 percent of computers with detections in Estonia. [Win32/Hotbar](#) is adware that displays a dynamic toolbar and targeted pop-up ads based on its monitoring of web-browsing activity.
- The fourth most common threat family in Estonia in 2Q12 was [JS/Pornpop](#), which affected 7.2 percent of computers with detections in Estonia. [JS/Pornpop](#) is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Estonia

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	1.01 (1.6)	1.21 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	0.60 (3.9)	1.41 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	2.33 (0.7)	0.85 (0.9)

Update service usage

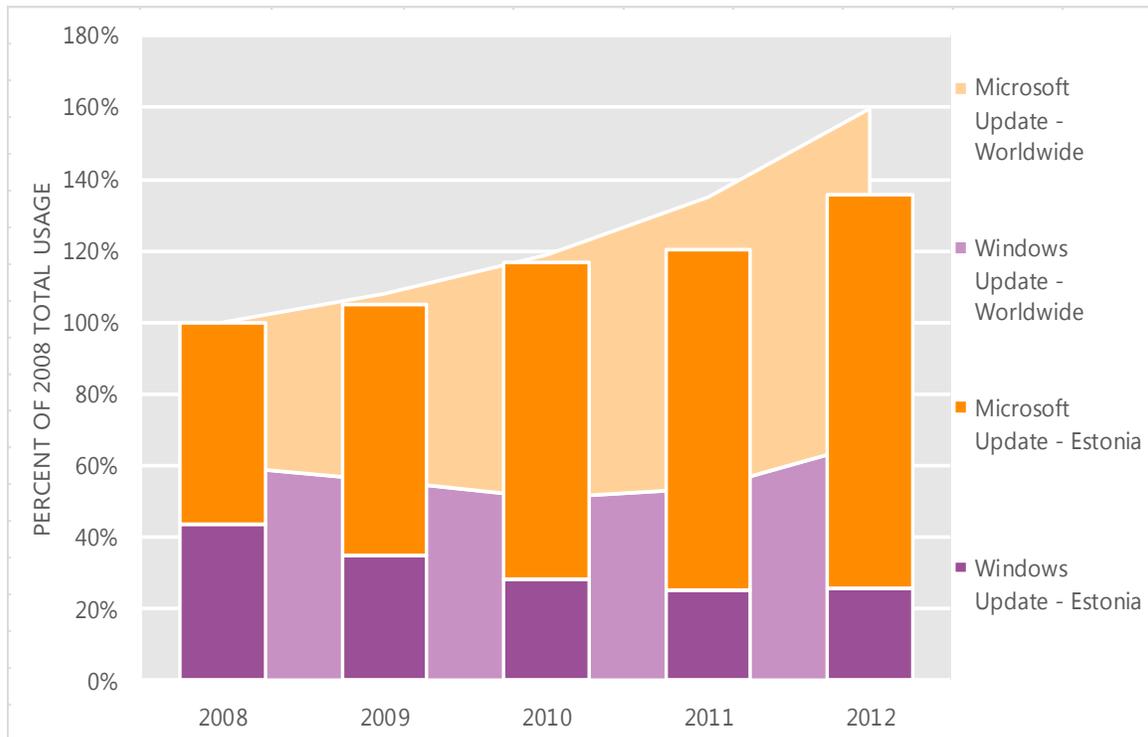
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Estonia and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Estonia over the last four years, indexed to the total usage for both services in Estonia in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Estonia was up 12.5 percent from 2011, and up 35.5 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Estonia in 2012, 81.1 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Finland

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Finland in 2Q12 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.

Infection rate statistics for Finland

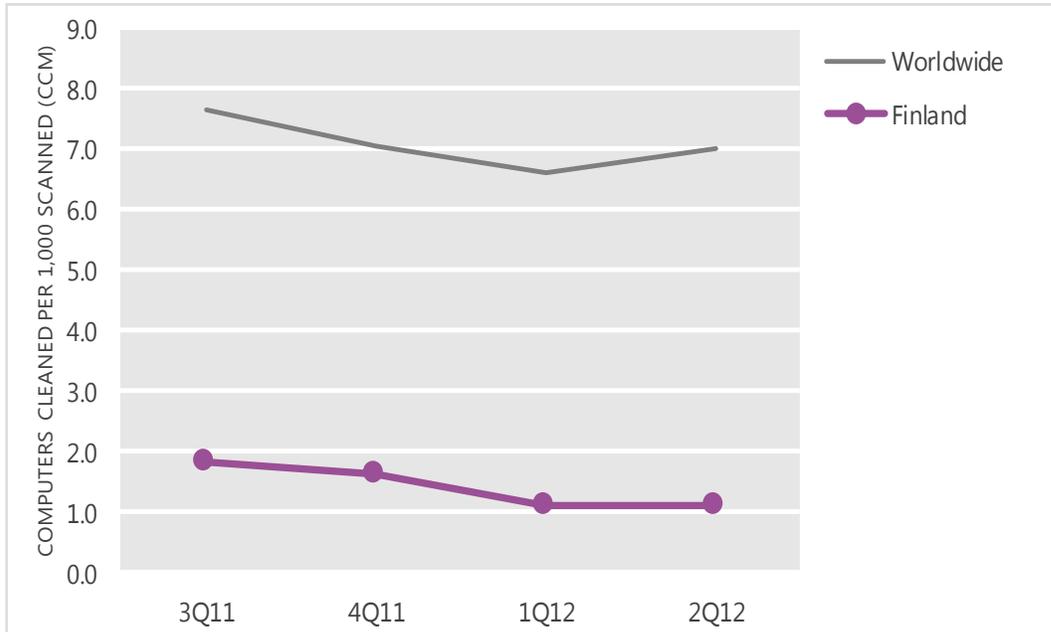
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	1.8	1.6	1.1	1.1
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

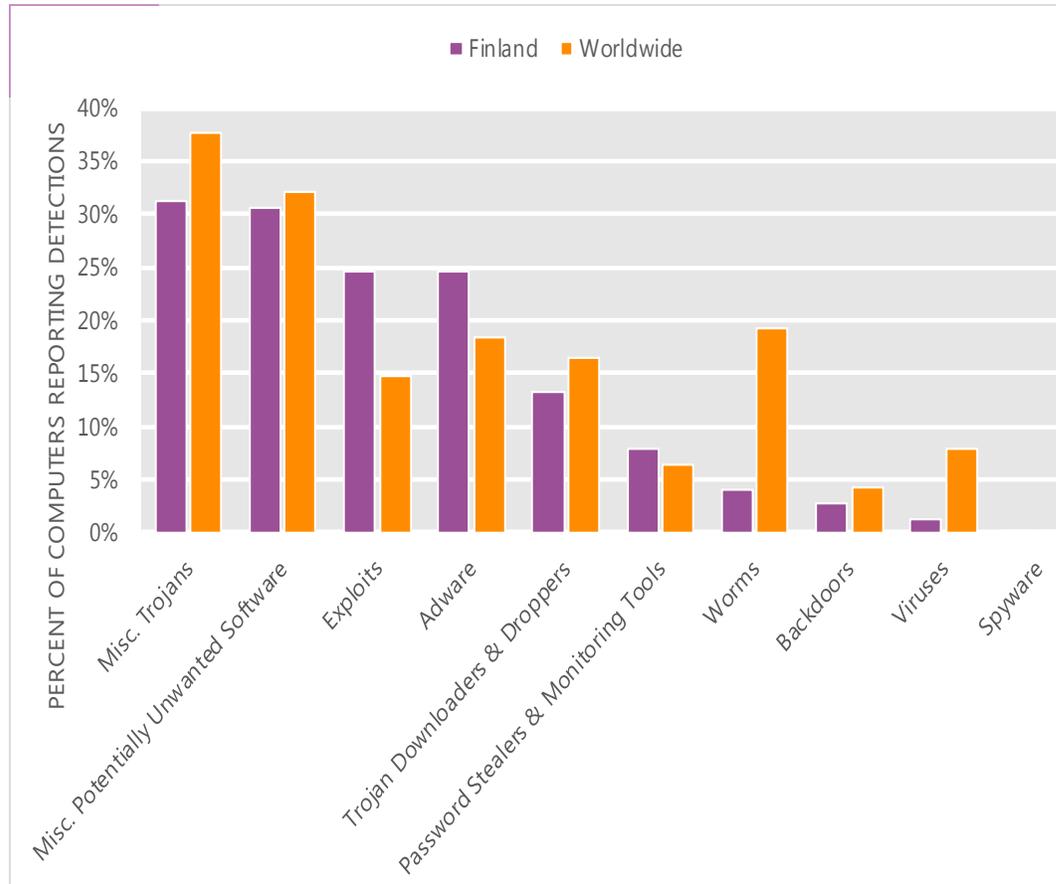
The MSRT detected malware on 1.1 of every 1,000 computers scanned in Finland in 2Q12 (a CCM score of 1.1, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Finland over the last four quarters, compared to the world as a whole.

CCM infection trends in Finland and worldwide



Threat categories

Malware and potentially unwanted software categories in Finland in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Finland in 2Q12 was Miscellaneous Trojans. It affected 31.3 percent of all computers with detections there, up from 28.6 percent in 1Q12.
- The second most common category in Finland in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 30.6 percent of all computers with detections there, down from 35.0 percent in 1Q12.
- The third most common category in Finland in 2Q12 was Exploits, which affected 24.7 percent of all computers with detections there, up from 13.5 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Finland in 2Q12

	Family	Most significant category	% of computers with detections
1	Java/Blacole	Exploits	14.5%
2	Win32/Keygen	Misc. Potentially Unwanted Software	11.3%
3	JS/Pornpop	Adware	11.1%
4	Win32/Hotbar	Adware	8.5%
5	Java/CVE-2012-0507	Exploits	6.7%
6	JS/BlacoleRef	Misc. Trojans	6.5%
7	ASX/Wimad	Trojan Downloaders & Droppers	5.0%
8	JS/IframeRef	Misc. Trojans	4.8%
9	Win32/Zwangi	Misc. Potentially Unwanted Software	4.8%
10	Win32/Pdfjsc	Exploits	4.7%

- The most common threat family in Finland in 2Q12 was [Java/Blacole](#), which affected 14.5 percent of computers with detections in Finland. [Java/Blacole](#) is an exploit pack, also known as Blackhole, that is installed on a compromised web server by an attacker and includes a number of exploits that target browser software. If a vulnerable computer browses a compromised website that contains the exploit pack, various malware may be downloaded and run.
- The second most common threat family in Finland in 2Q12 was [Win32/Keygen](#), which affected 11.3 percent of computers with detections in Finland. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The third most common threat family in Finland in 2Q12 was [JS/Pornpop](#), which affected 11.1 percent of computers with detections in Finland. [JS/Pornpop](#) is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The fourth most common threat family in Finland in 2Q12 was [Win32/Hotbar](#), which affected 8.5 percent of computers with detections in Finland. [Win32/Hotbar](#) is adware that displays a dynamic toolbar and targeted pop-up ads based on its monitoring of web-browsing activity.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Finland

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	0.78 (1.6)	0.78 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	1.96 (3.9)	2.23 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.04 (0.7)	0.21 (0.9)

Update service usage

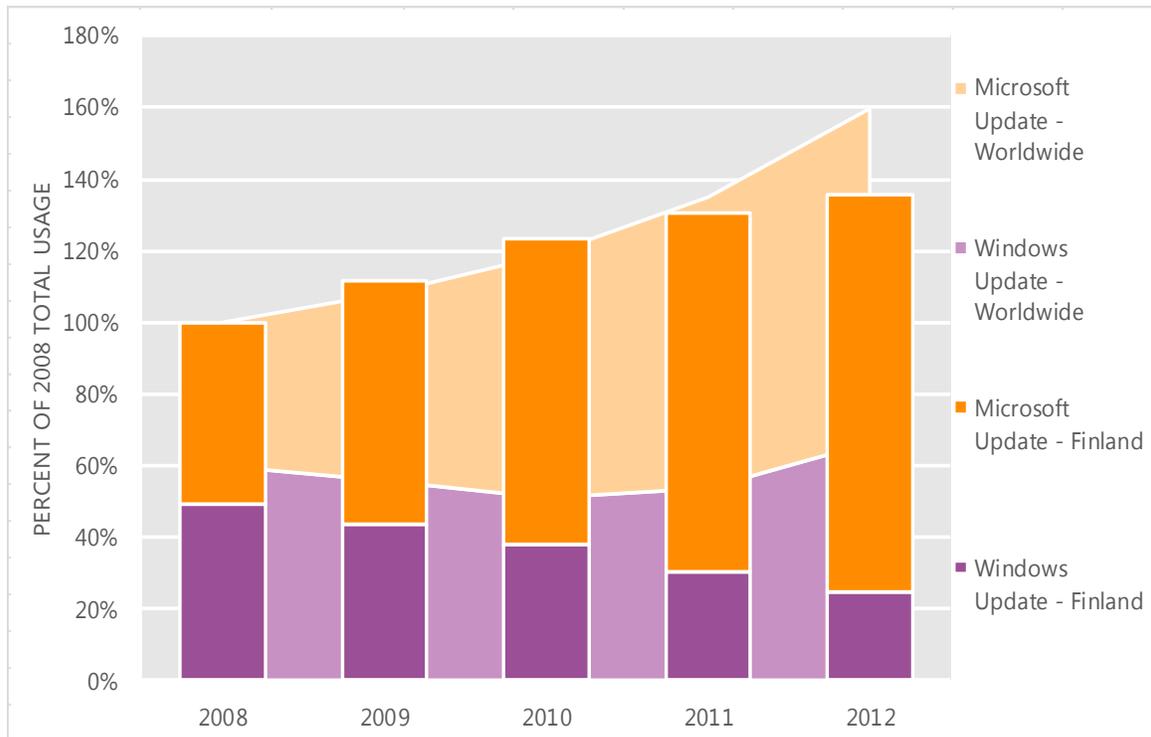
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Finland and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Finland over the last four years, indexed to the total usage for both services in Finland in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Finland was up 4.2 percent from 2011, and up 35.8 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Finland in 2012, 81.8 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

France

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in France in 2Q12 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.

Infection rate statistics for France

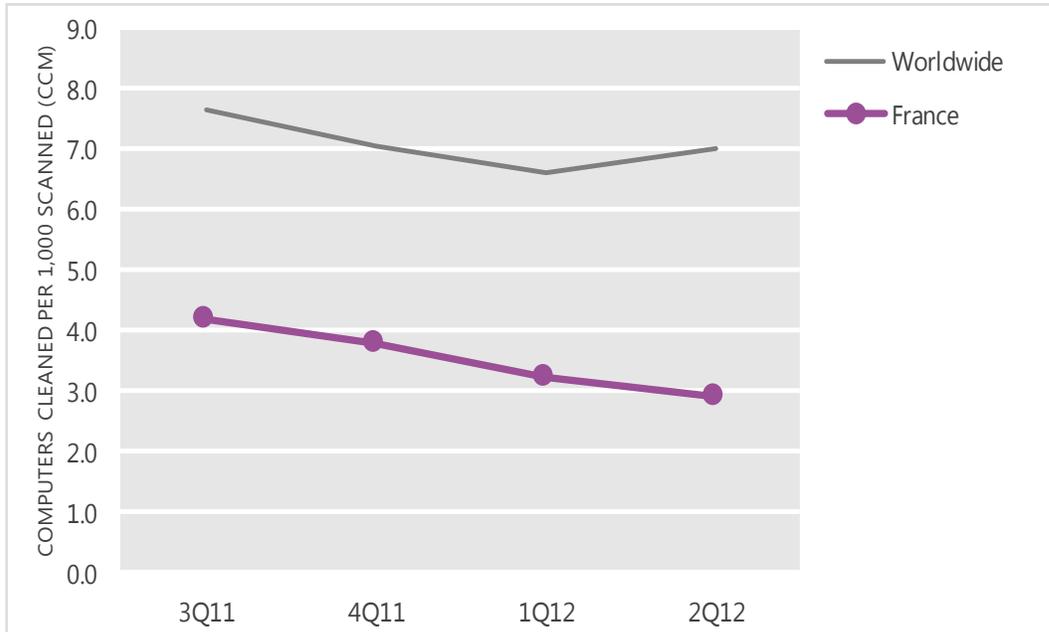
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	4.2	3.8	3.2	2.9
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

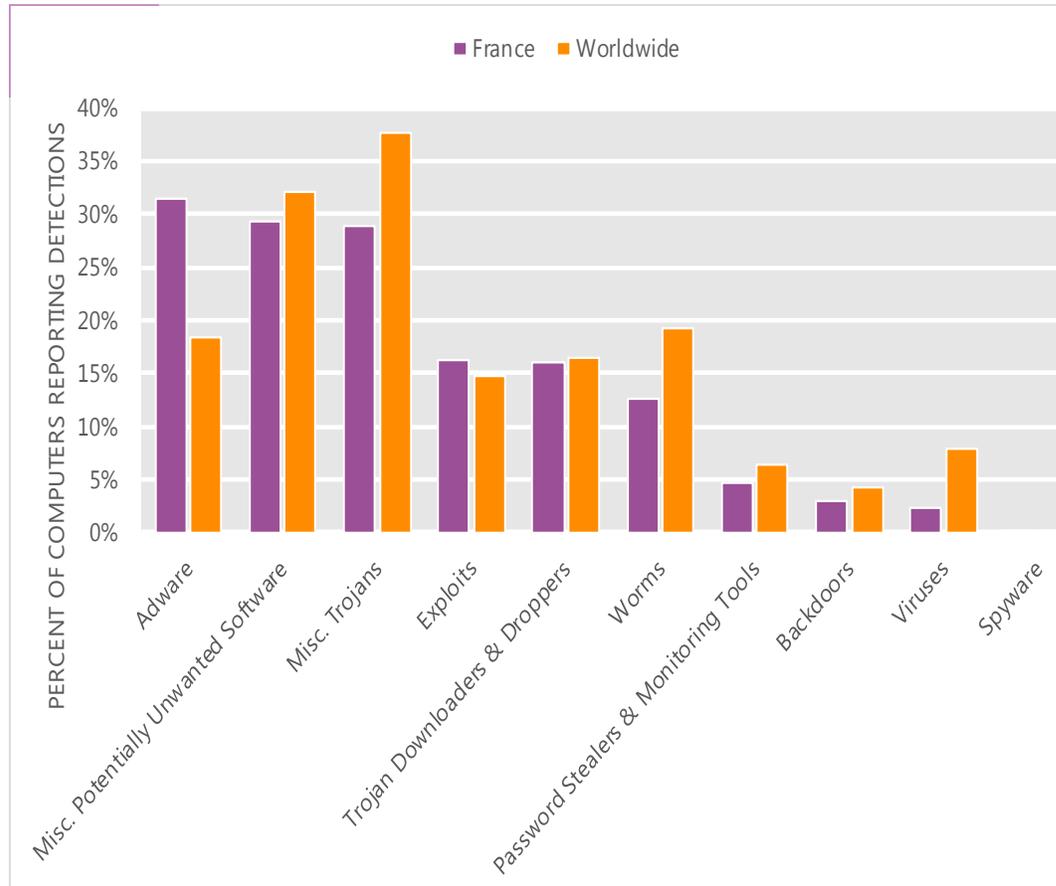
The MSRT detected malware on 2.9 of every 1,000 computers scanned in France in 2Q12 (a CCM score of 2.9, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for France over the last four quarters, compared to the world as a whole.

CCM infection trends in France and worldwide



Threat categories

Malware and potentially unwanted software categories in France in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in France in 2Q12 was Adware. It affected 31.5 percent of all computers with detections there, down from 41.0 percent in 1Q12.
- The second most common category in France in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 29.3 percent of all computers with detections there, down from 29.9 percent in 1Q12.
- The third most common category in France in 2Q12 was Miscellaneous Trojans, which affected 28.8 percent of all computers with detections there, up from 26.2 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in France in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Hotbar	Adware	13.0%
2	Java/Blacole	Exploits	10.0%
3	ASX/Wimad	Trojan Downloaders & Droppers	8.5%
4	Win32/Keygen	Misc. Potentially Unwanted Software	8.1%
5	Win32/Zwangi	Misc. Potentially Unwanted Software	6.1%
6	JS/Pornpop	Adware	5.7%
7	Win32/Autorun	Worms	4.5%
8	JS/IframeRef	Misc. Trojans	3.9%
9	Win32/OpenCandy	Adware	3.8%
10	Win32/Sirefef	Misc. Trojans	3.8%

- The most common threat family in France in 2Q12 was [Win32/Hotbar](#), which affected 13.0 percent of computers with detections in France. [Win32/Hotbar](#) is adware that displays a dynamic toolbar and targeted pop-up ads based on its monitoring of web-browsing activity.
- The second most common threat family in France in 2Q12 was [Java/Blacole](#), which affected 10.0 percent of computers with detections in France. [Java/Blacole](#) is an exploit pack, also known as Blackhole, that is installed on a compromised web server by an attacker and includes a number of exploits that target browser software. If a vulnerable computer browses a compromised website that contains the exploit pack, various malware may be downloaded and run.
- The third most common threat family in France in 2Q12 was [ASX/Wimad](#), which affected 8.5 percent of computers with detections in France. [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 threat family in France in 2Q12 was [Win32/Keygen](#), which affected 8.1 percent of computers with detections in France. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for France

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	1.39 (1.6)	1.42 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	3.74 (3.9)	3.75 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.25 (0.7)	1.11 (0.9)

Update service usage

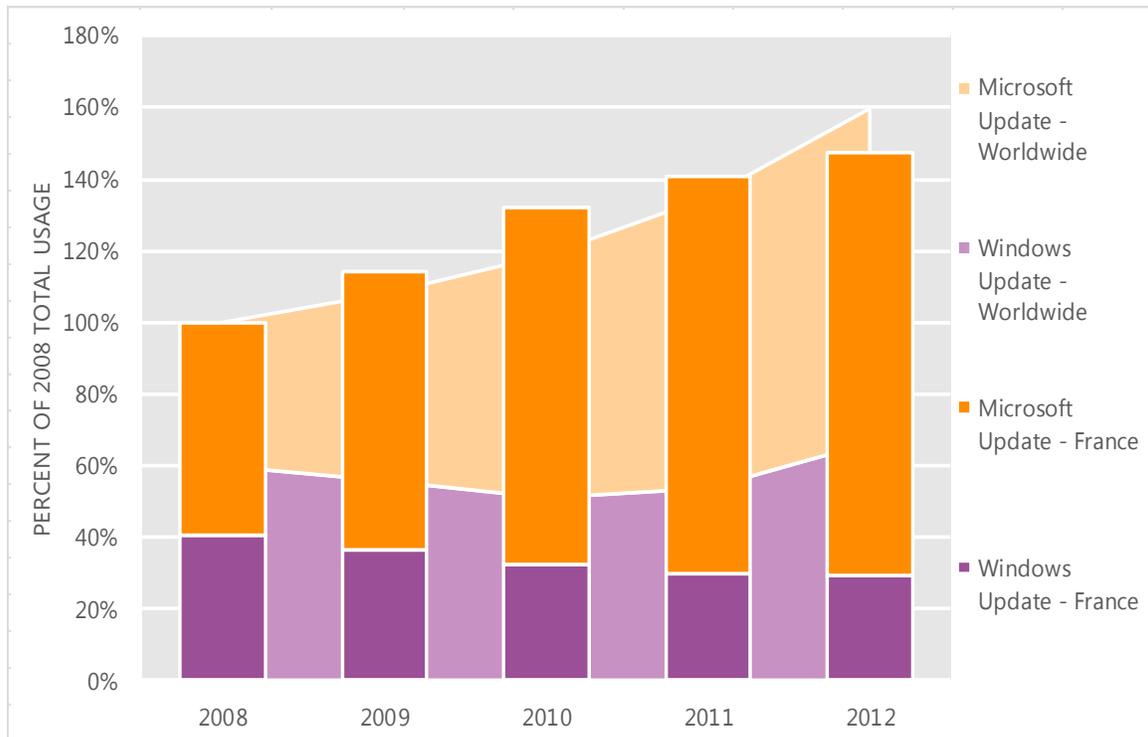
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in France and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in France over the last four years, indexed to the total usage for both services in France in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in France was up 4.8 percent from 2011, and up 47.5 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in France in 2012, 80.3 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Georgia

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Georgia in 2Q12 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.

Infection rate statistics for Georgia

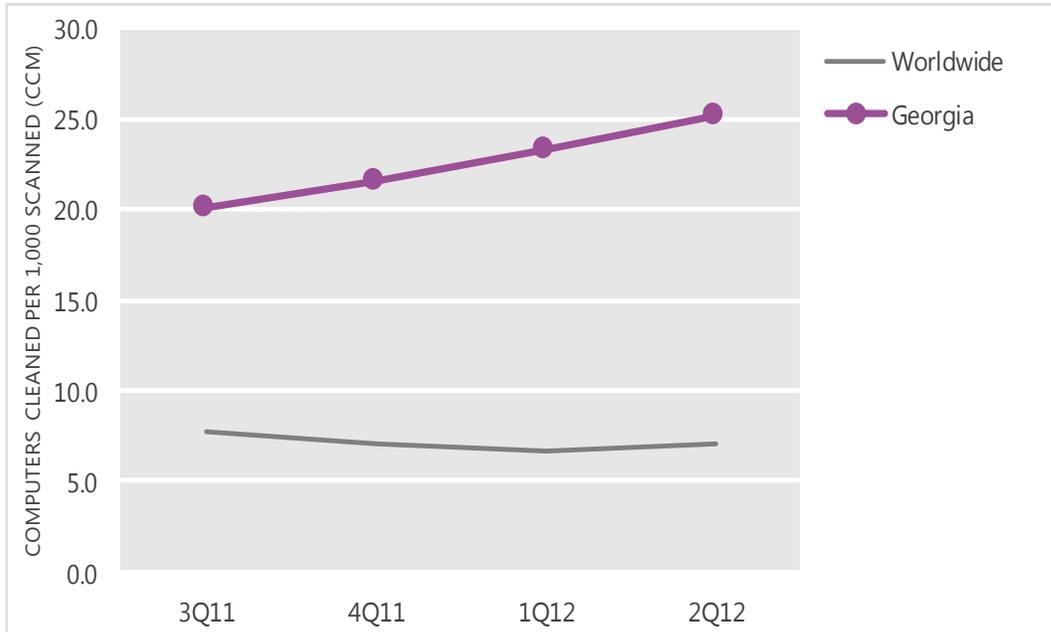
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	20.1	21.6	23.3	25.2
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

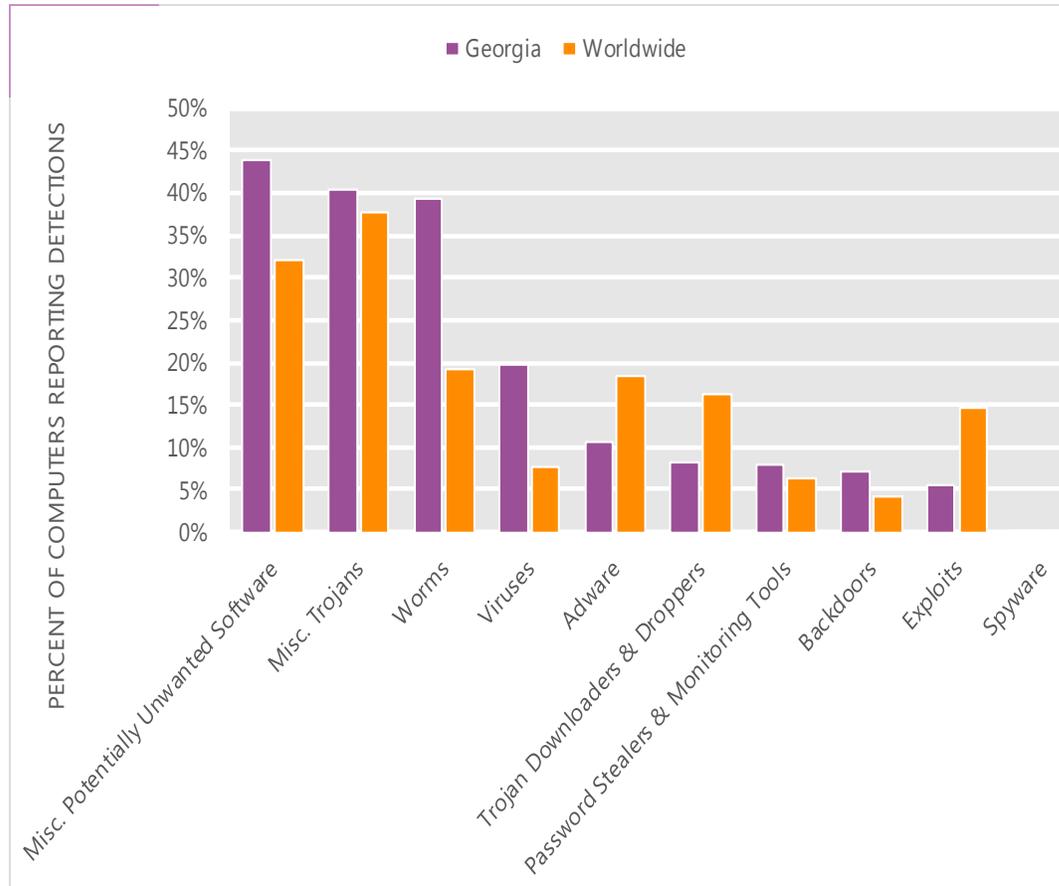
The MSRT detected malware on 25.2 of every 1,000 computers scanned in Georgia in 2Q12 (a CCM score of 25.2, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Georgia over the last four quarters, compared to the world as a whole.

CCM infection trends in Georgia and worldwide



Threat categories

Malware and potentially unwanted software categories in Georgia in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Georgia in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 43.8 percent of all computers with detections there, down from 47.7 percent in 1Q12.
- The second most common category in Georgia in 2Q12 was Miscellaneous Trojans. It affected 40.3 percent of all computers with detections there, up from 35.2 percent in 1Q12.
- The third most common category in Georgia in 2Q12 was Worms, which affected 39.4 percent of all computers with detections there, up from 36.2 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Georgia in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Keygen	Misc. Potentially Unwanted Software	15.9%
2	Win32/Autorun	Worms	15.6%
3	Win32/Dorkbot	Worms	12.1%
4	Win32/Sality	Viruses	11.7%
5	Win32/Pameseg	Misc. Potentially Unwanted Software	7.9%
6	JS/IframeRef	Misc. Trojans	7.5%
7	JS/BlacoleRef	Misc. Trojans	7.0%
8	Win32/Brontok	Worms	6.4%
9	Win32/Verst	Worms	6.3%
10	Win32/Rimecud	Worms	5.8%

- The most common threat family in Georgia in 2Q12 was [Win32/Keygen](#), which affected 15.9 percent of computers with detections in Georgia. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The second most common threat family in Georgia in 2Q12 was [Win32/Autorun](#), which affected 15.6 percent of computers with detections in Georgia. [Win32/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 threat family in Georgia in 2Q12 was [Win32/Dorkbot](#), which affected 12.1 percent of computers with detections in Georgia. [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 in Georgia in 2Q12 was [Win32/Sality](#), which affected 11.7 percent of computers with detections in Georgia. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Georgia

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	0.90 (1.6)	1.63 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	2.90 (3.9)	2.35 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	4.27 (0.7)	4.67 (0.9)

Update service usage

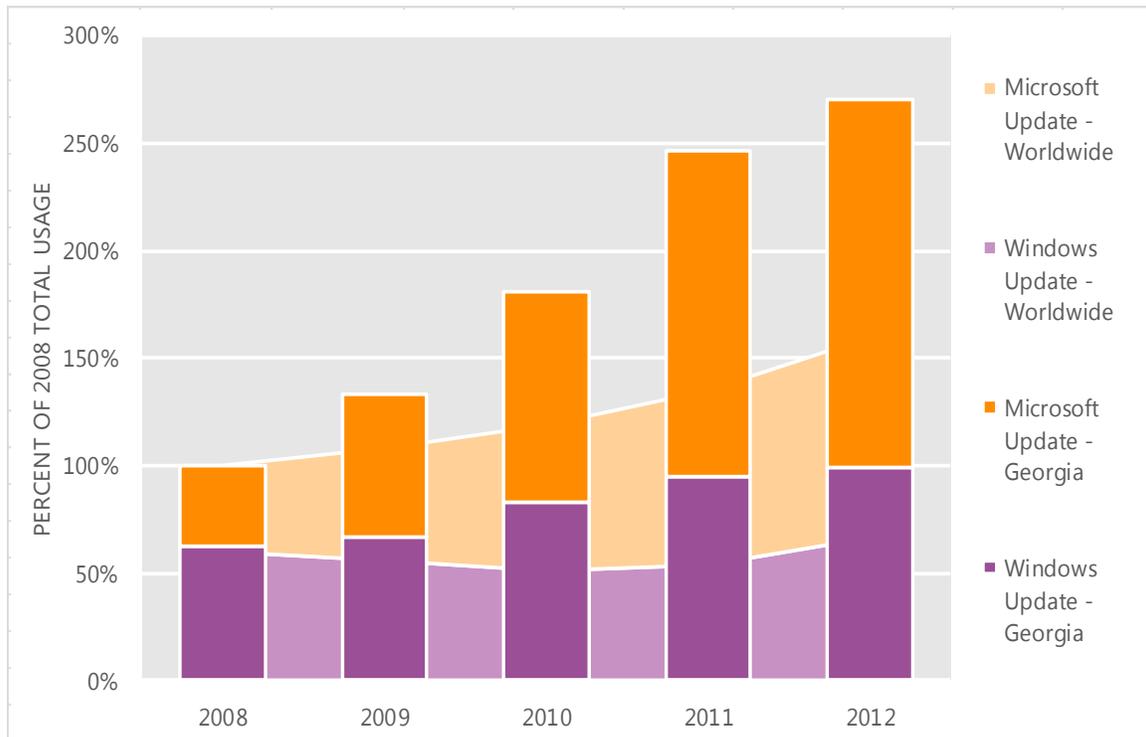
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Georgia and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Georgia over the last four years, indexed to the total usage for both services in Georgia in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Georgia was up 9.8 percent from 2011, and up 170.4 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Georgia in 2012, 63.2 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Germany

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Germany in 2Q12 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.

Infection rate statistics for Germany

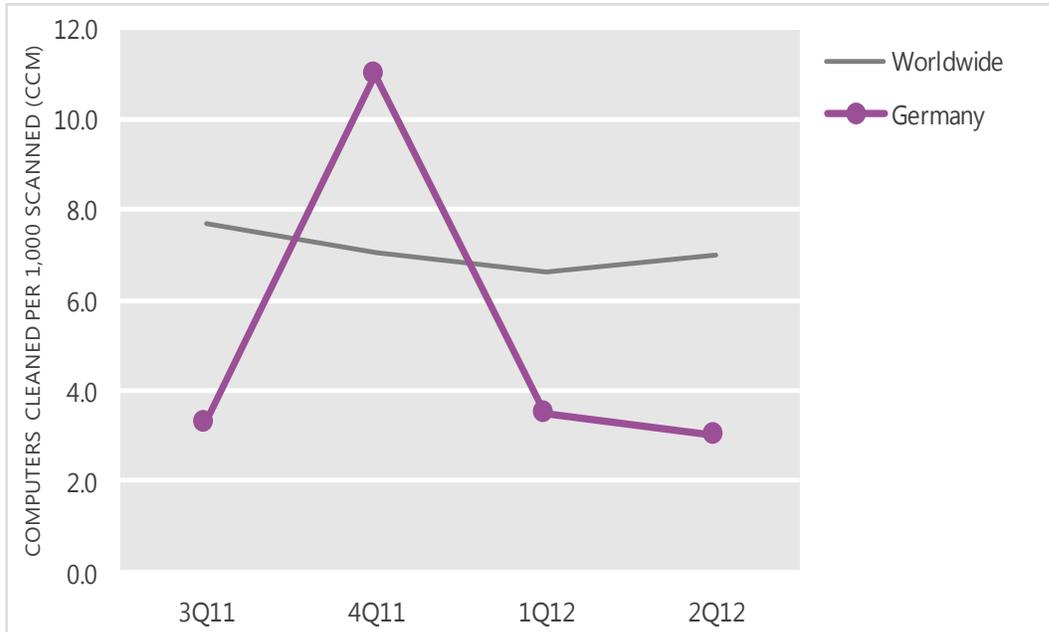
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	3.3	11.0	3.5	3.0
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

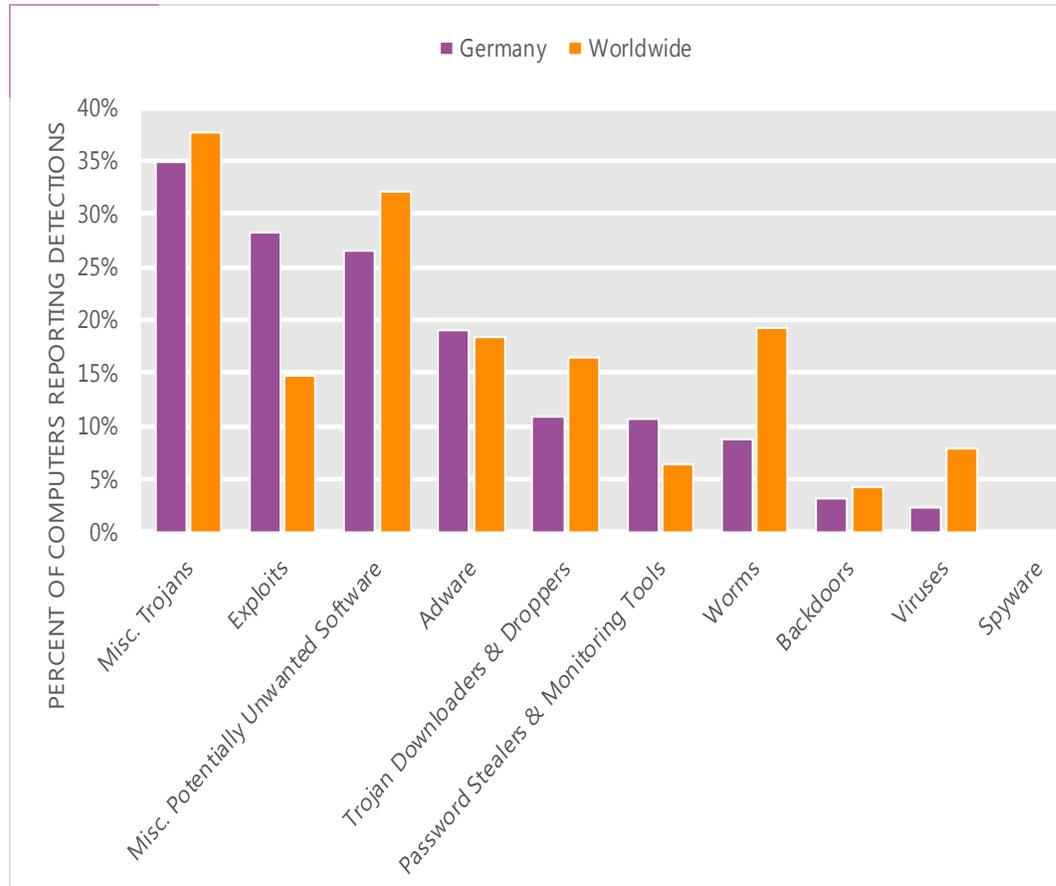
The MSRT detected malware on 3.0 of every 1,000 computers scanned in Germany in 2Q12 (a CCM score of 3.0, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Germany over the last four quarters, compared to the world as a whole.

CCM infection trends in Germany and worldwide



Threat categories

Malware and potentially unwanted software categories in Germany in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Germany in 2Q12 was Miscellaneous Trojans. It affected 35.0 percent of all computers with detections there, up from 31.9 percent in 1Q12.
- The second most common category in Germany in 2Q12 was Exploits. It affected 28.2 percent of all computers with detections there, up from 26.5 percent in 1Q12.
- The third most common category in Germany in 2Q12 was Miscellaneous Potentially Unwanted Software, which affected 26.6 percent of all computers with detections there, down from 28.1 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Germany in 2Q12

	Family	Most significant category	% of computers with detections
1	Java/Blacole	Exploits	19.2%
2	JS/Pornpop	Adware	11.2%
3	Win32/Keygen	Misc. Potentially Unwanted Software	8.4%
4	Java/CVE-2012-0507	Exploits	7.5%
5	Win32/Pdfjsc	Exploits	5.8%
6	Win32/Sirefef	Misc. Trojans	5.7%
7	JS/BlacoleRef	Misc. Trojans	4.2%
8	Win32/Zbot	Password Stealers & Monitoring Tools	3.9%
9	JS/IframeRef	Misc. Trojans	3.8%
10	Win32/Obfuscator	Misc. Potentially Unwanted Software	3.8%

- The most common threat family in Germany in 2Q12 was [Java/Blacole](#), which affected 19.2 percent of computers with detections in Germany. [Java/Blacole](#) is an exploit pack, also known as Blackhole, that is installed on a compromised web server by an attacker and includes a number of exploits that target browser software. If a vulnerable computer browses a compromised website that contains the exploit pack, various malware may be downloaded and run.
- The second most common threat family in Germany in 2Q12 was [JS/Pornpop](#), which affected 11.2 percent of computers with detections in Germany. [JS/Pornpop](#) is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The third most common threat family in Germany in 2Q12 was [Win32/Keygen](#), which affected 8.4 percent of computers with detections in Germany. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The fourth most common threat family in Germany in 2Q12 was [Java/CVE-2012-0507](#), which affected 7.5 percent of computers with detections in Germany. [Java/CVE-2012-0507](#) is a detection for a malicious Java applet that exploits the Java Runtime Environment (JRE) vulnerability described in CVE-2012-0507, addressed by an Oracle security update in February 2012.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Germany

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	1.88 (1.6)	1.99 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	3.04 (3.9)	3.24 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	3.66 (0.7)	3.88 (0.9)

Update service usage

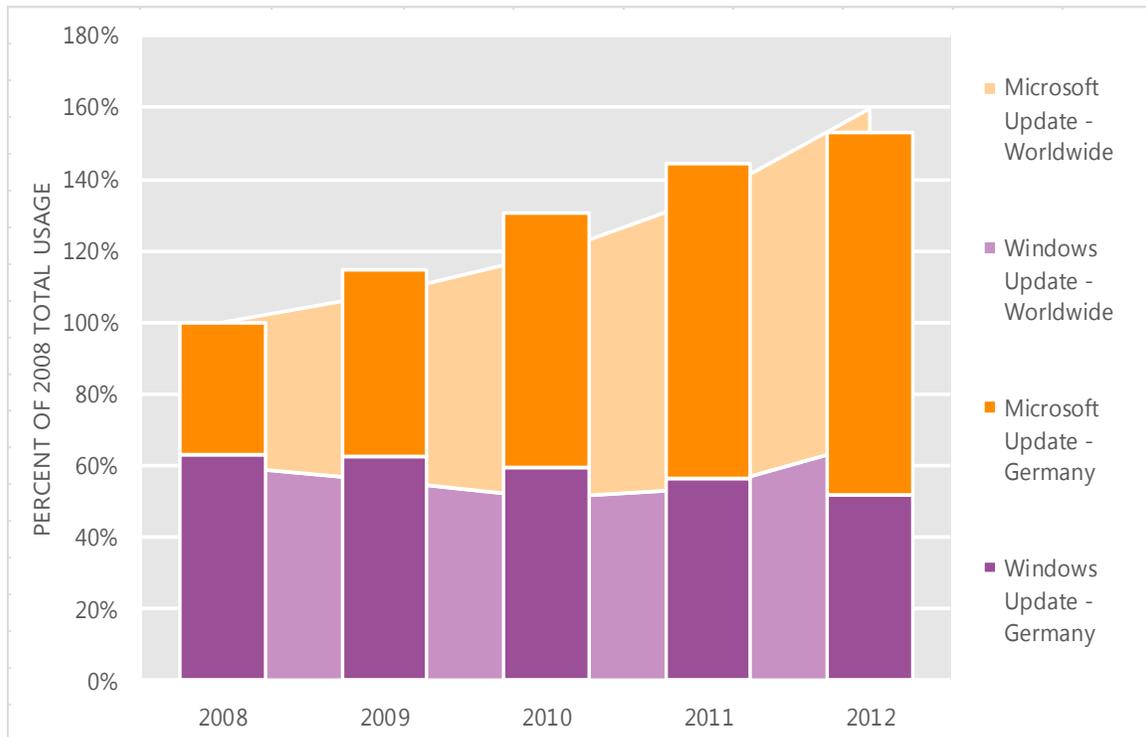
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Germany and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Germany over the last four years, indexed to the total usage for both services in Germany in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Germany was up 5.9 percent from 2011, and up 53.0 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Germany in 2012, 66.1 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Greece

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Greece in 2Q12 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.

Infection rate statistics for Greece

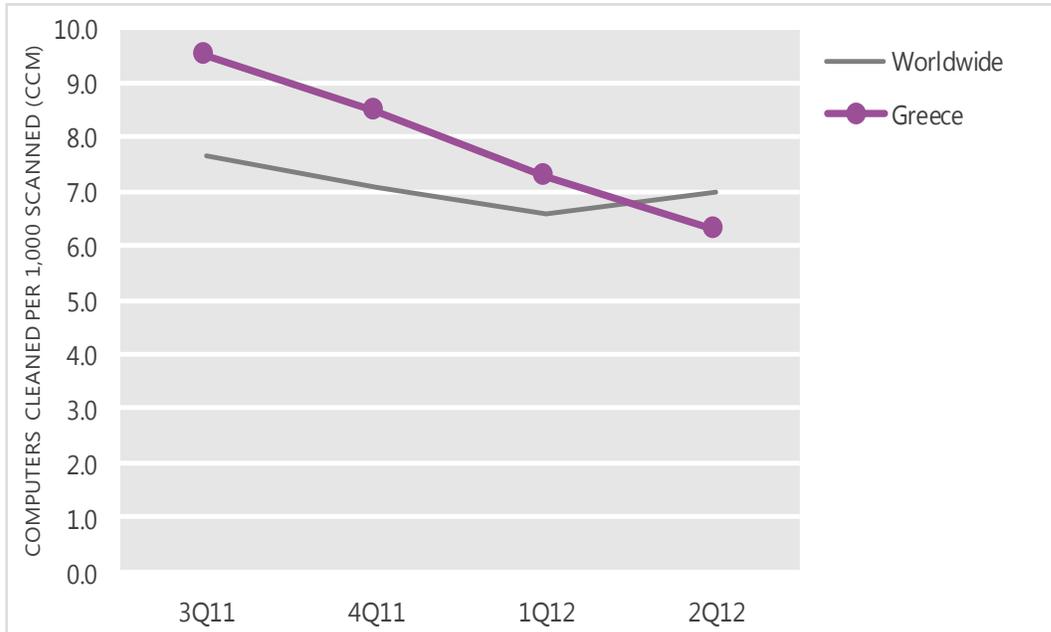
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	9.5	8.5	7.3	6.3
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

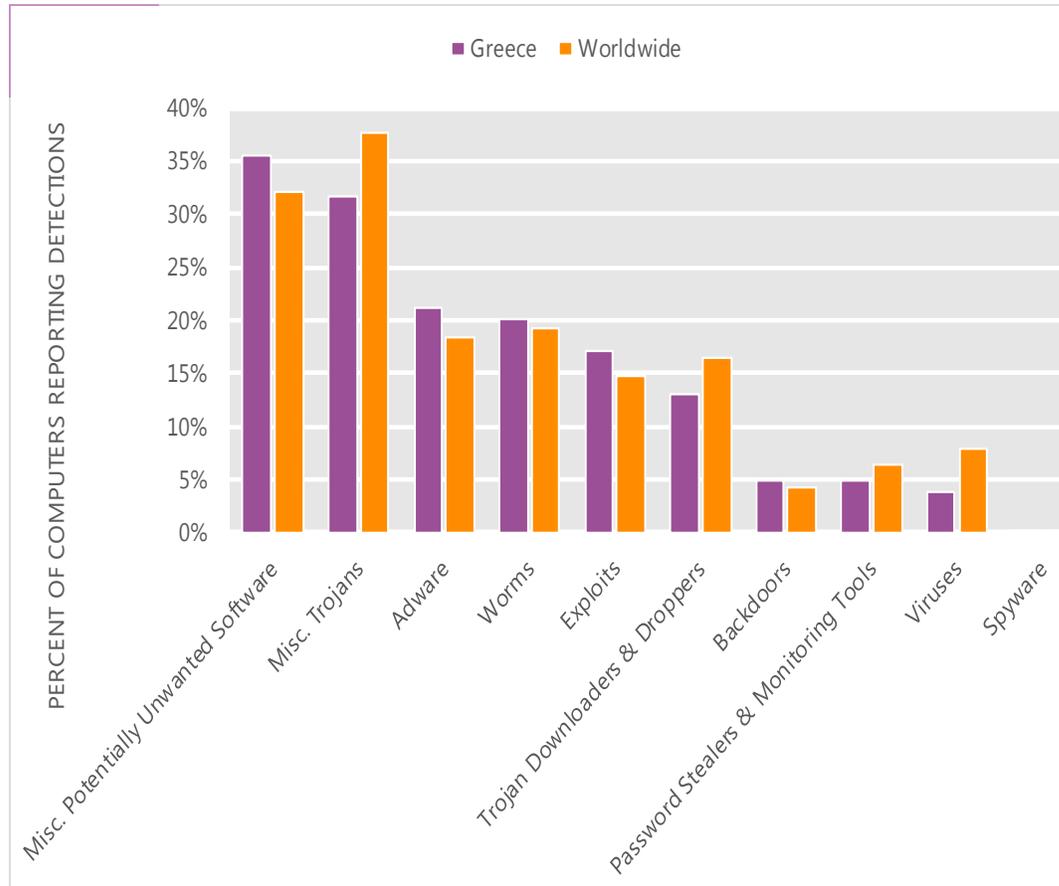
The MSRT detected malware on 6.3 of every 1,000 computers scanned in Greece in 2Q12 (a CCM score of 6.3, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Greece over the last four quarters, compared to the world as a whole.

CCM infection trends in Greece and worldwide



Threat categories

Malware and potentially unwanted software categories in Greece in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Greece in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 35.6 percent of all computers with detections there, down from 36.9 percent in 1Q12.
- The second most common category in Greece in 2Q12 was Miscellaneous Trojans. It affected 31.7 percent of all computers with detections there, up from 28.9 percent in 1Q12.
- The third most common category in Greece in 2Q12 was Adware, which affected 21.1 percent of all computers with detections there, down from 27.8 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Greece in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Keygen	Misc. Potentially Unwanted Software	13.6%
2	JS/Pornpop	Adware	10.5%
3	Java/Blacole	Exploits	10.3%
4	Win32/Autorun	Worms	9.3%
5	Win32/Hotbar	Adware	6.3%
6	Win32/Zwangi	Misc. Potentially Unwanted Software	5.7%
7	ASX/Wimad	Trojan Downloaders & Droppers	4.7%
8	Win32/Pdfjsc	Exploits	4.3%
9	Java/CVE-2012-0507	Exploits	3.9%
10	Win32/Obfuscator	Misc. Potentially Unwanted Software	3.8%

- The most common threat family in Greece in 2Q12 was [Win32/Keygen](#), which affected 13.6 percent of computers with detections in Greece. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The second most common threat family in Greece in 2Q12 was [JS/Pornpop](#), which affected 10.5 percent of computers with detections in Greece. [JS/Pornpop](#) is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The third most common threat family in Greece in 2Q12 was [Java/Blacole](#), which affected 10.3 percent of computers with detections in Greece. [Java/Blacole](#) is an exploit pack, also known as Blackhole, that is installed on a compromised web server by an attacker and includes a number of exploits that target browser software. If a vulnerable computer browses a compromised website that contains the exploit pack, various malware may be downloaded and run.
- The fourth most common threat family in Greece in 2Q12 was [Win32/Autorun](#), which affected 9.3 percent of computers with detections in Greece. [Win32/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.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Greece

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	0.47 (1.6)	0.60 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	1.29 (3.9)	1.01 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.19 (0.7)	0.12 (0.9)

Update service usage

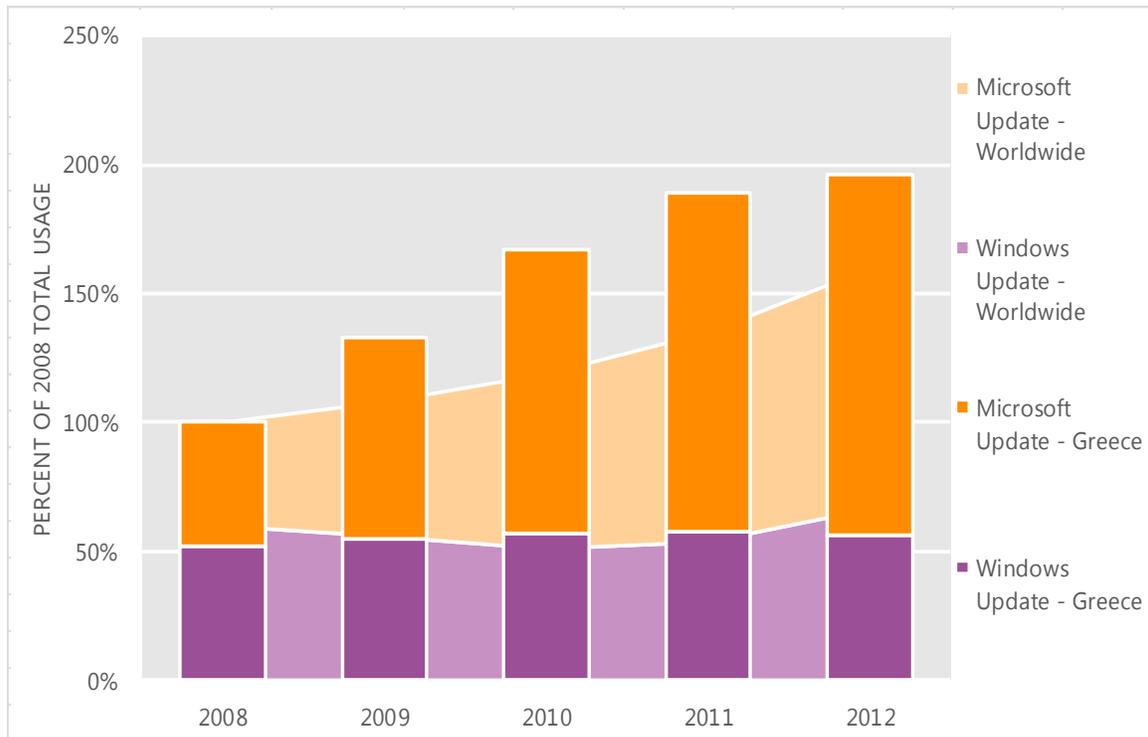
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Greece and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Greece over the last four years, indexed to the total usage for both services in Greece in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Greece was up 4.0 percent from 2011, and up 96.5 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Greece in 2012, 71.3 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Guatemala

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Guatemala in 2Q12 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.

Infection rate statistics for Guatemala

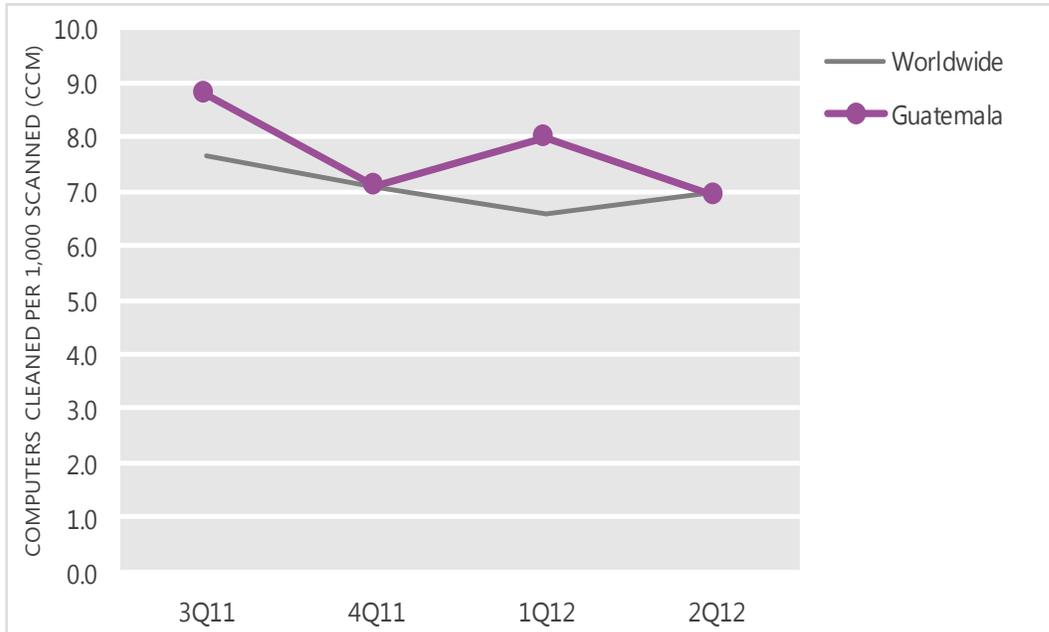
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	8.8	7.1	8.0	6.9
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

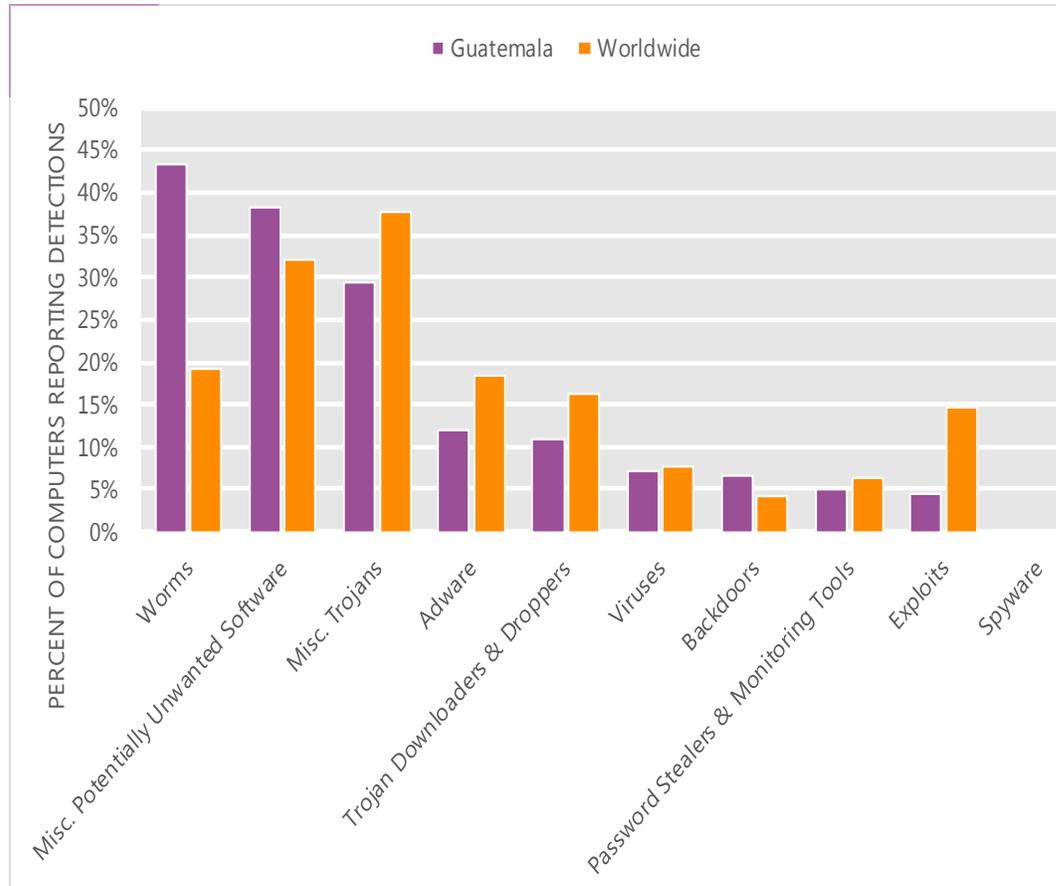
The MSRT detected malware on 6.9 of every 1,000 computers scanned in Guatemala in 2Q12 (a CCM score of 6.9, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Guatemala over the last four quarters, compared to the world as a whole.

CCM infection trends in Guatemala and worldwide



Threat categories

Malware and potentially unwanted software categories in Guatemala in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Guatemala in 2Q12 was Worms. It affected 43.4 percent of all computers with detections there, up from 40.6 percent in 1Q12.
- The second most common category in Guatemala in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 38.2 percent of all computers with detections there, down from 42.5 percent in 1Q12.
- The third most common category in Guatemala in 2Q12 was Miscellaneous Trojans, which affected 29.4 percent of all computers with detections there, up from 26.7 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Guatemala in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Dorkbot	Worms	22.0%
2	Win32/Autorun	Worms	13.9%
3	Win32/Keygen	Misc. Potentially Unwanted Software	13.0%
4	Win32/Vobfus	Worms	9.2%
5	Win32/VBInject	Misc. Potentially Unwanted Software	6.3%
6	Win32/Sality	Viruses	6.2%
7	Win32/Rimecud	Worms	4.7%
8	JS/Pornpop	Adware	4.1%
9	Win32/Conficker	Worms	4.1%
10	ASX/Wimad	Trojan Downloaders & Droppers	3.7%

- The most common threat family in Guatemala in 2Q12 was [Win32/Dorkbot](#), which affected 22.0 percent of computers with detections in Guatemala. [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 second most common threat family in Guatemala in 2Q12 was [Win32/Autorun](#), which affected 13.9 percent of computers with detections in Guatemala. [Win32/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 threat family in Guatemala in 2Q12 was [Win32/Keygen](#), which affected 13.0 percent of computers with detections in Guatemala. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The fourth most common threat family in Guatemala in 2Q12 was [Win32/Vobfus](#), which affected 9.2 percent of computers with detections in Guatemala. [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.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Guatemala

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	N/A (1.6)	0.32 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	0.63 (3.9)	0.95 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.01 (0.7)	N/A (0.9)

Update service usage

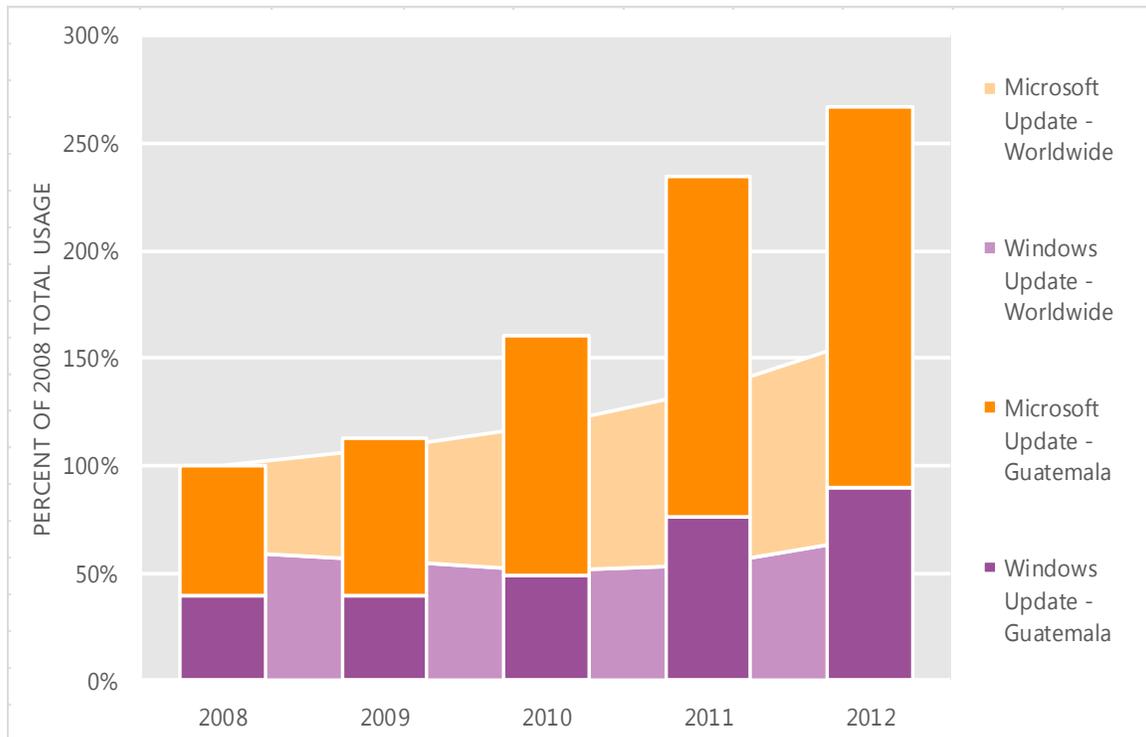
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Guatemala and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Guatemala over the last four years, indexed to the total usage for both services in Guatemala in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Guatemala was up 13.7 percent from 2011, and up 166.7 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Guatemala in 2012, 66.3 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Honduras

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Honduras in 2Q12 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.

Infection rate statistics for Honduras

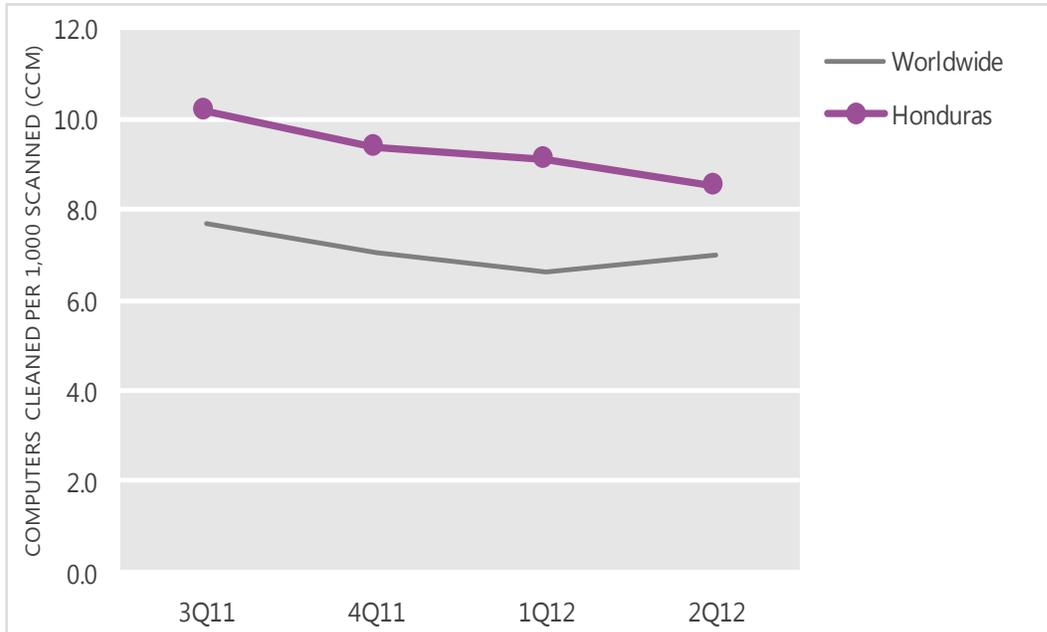
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	10.2	9.4	9.1	8.5
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

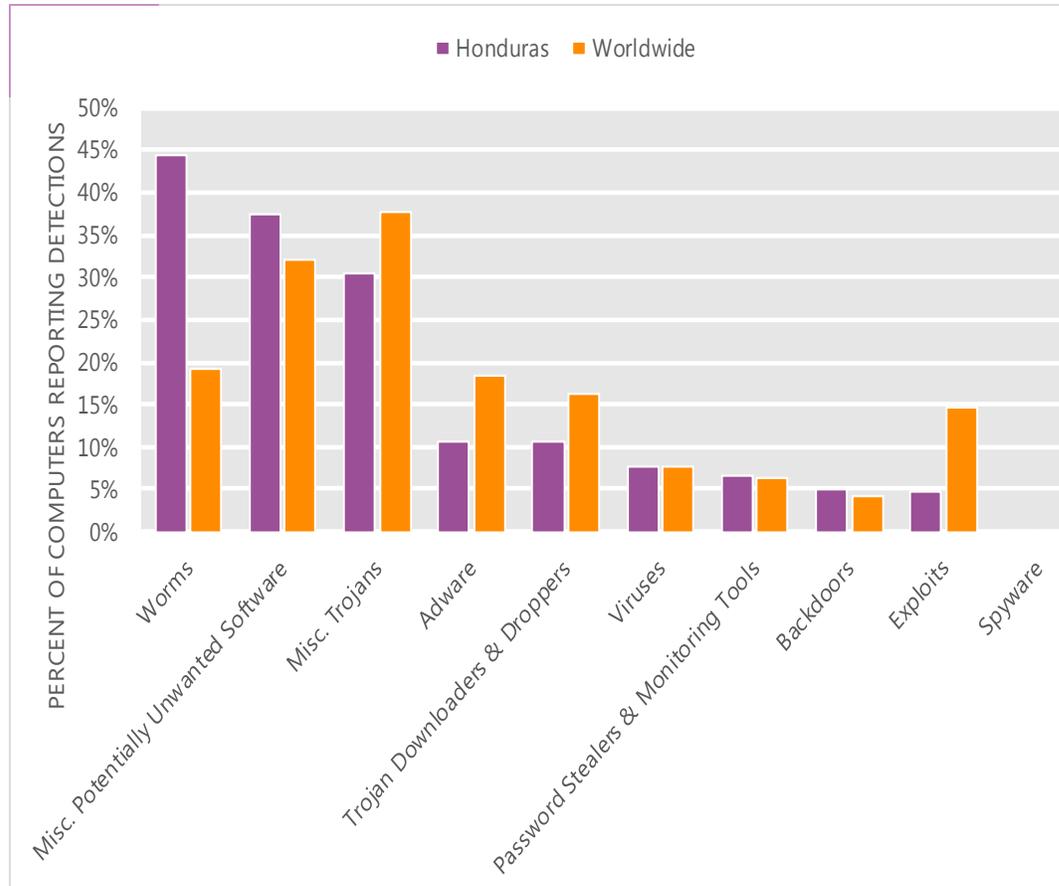
The MSRT detected malware on 8.5 of every 1,000 computers scanned in Honduras in 2Q12 (a CCM score of 8.5, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Honduras over the last four quarters, compared to the world as a whole.

CCM infection trends in Honduras and worldwide



Threat categories

Malware and potentially unwanted software categories in Honduras in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Honduras in 2Q12 was Worms. It affected 44.4 percent of all computers with detections there, up from 40.0 percent in 1Q12.
- The second most common category in Honduras in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 37.5 percent of all computers with detections there, down from 42.2 percent in 1Q12.
- The third most common category in Honduras in 2Q12 was Miscellaneous Trojans, which affected 30.4 percent of all computers with detections there, up from 27.4 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Honduras in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Dorkbot	Worms	16.7%
2	Win32/Autorun	Worms	15.2%
3	Win32/Vobfus	Worms	14.3%
4	Win32/Keygen	Misc. Potentially Unwanted Software	14.2%
5	Win32/Nuqel	Worms	8.3%
6	Win32/Sality	Viruses	5.3%
7	Win32/Rimecud	Worms	4.3%
8	Win32/Conficker	Worms	3.9%
9	JS/Redirector	Misc. Trojans	3.5%
10	Win32/Sirefef	Misc. Trojans	3.4%

- The most common threat family in Honduras in 2Q12 was [Win32/Dorkbot](#), which affected 16.7 percent of computers with detections in Honduras. [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 second most common threat family in Honduras in 2Q12 was [Win32/Autorun](#), which affected 15.2 percent of computers with detections in Honduras. [Win32/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 threat family in Honduras in 2Q12 was [Win32/Vobfus](#), which affected 14.3 percent of computers with detections in Honduras. [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 in Honduras in 2Q12 was [Win32/Keygen](#), which affected 14.2 percent of computers with detections in Honduras. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Honduras

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	N/A (1.6)	N/A (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	1.14 (3.9)	1.71 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	N/A (0.7)	0.23 (0.9)

Update service usage

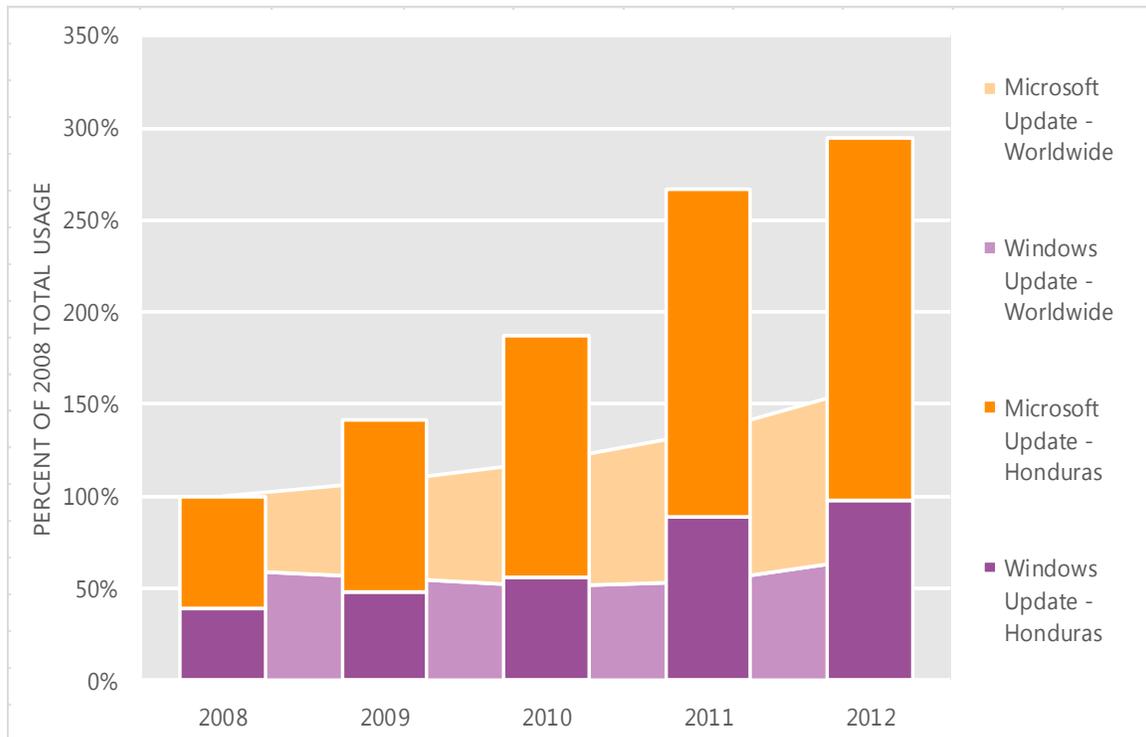
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Honduras and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Honduras over the last four years, indexed to the total usage for both services in Honduras in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Honduras was up 10.7 percent from 2011, and up 194.9 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Honduras in 2012, 66.7 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Hong Kong S.A.R.

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Hong Kong S.A.R. in 2Q12 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.

Infection rate statistics for Hong Kong S.A.R.

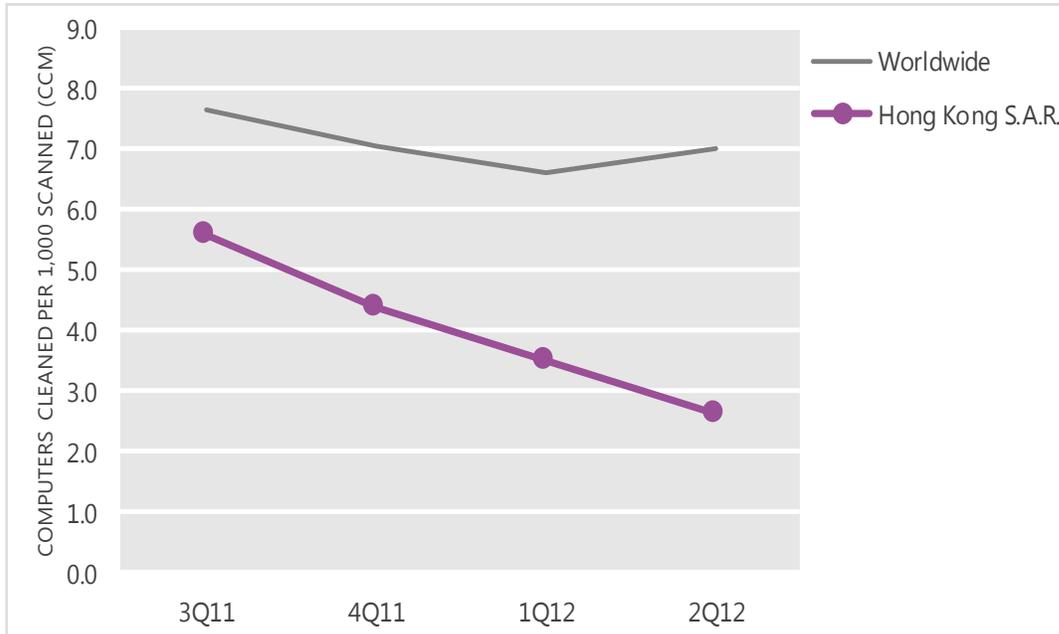
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	5.6	4.4	3.5	2.6
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

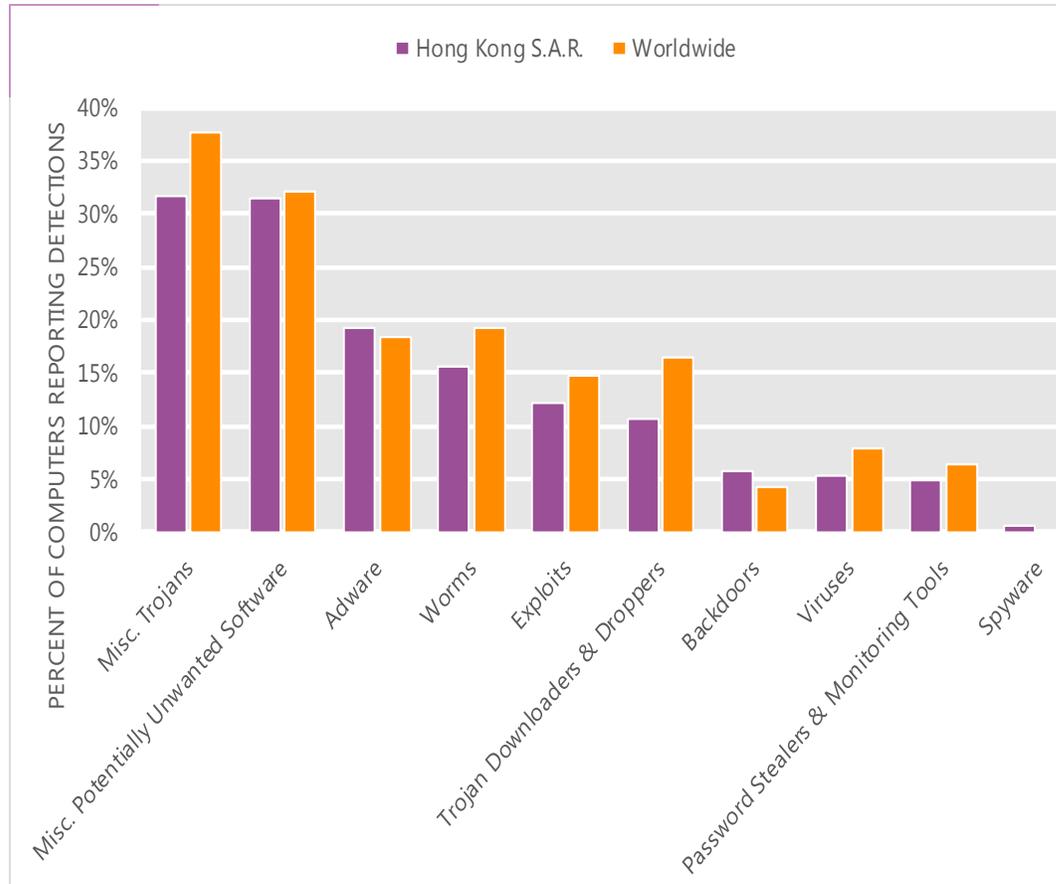
The MSRT detected malware on 2.6 of every 1,000 computers scanned in Hong Kong S.A.R. in 2Q12 (a CCM score of 2.6, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Hong Kong S.A.R. over the last four quarters, compared to the world as a whole.

CCM infection trends in Hong Kong S.A.R. and worldwide



Threat categories

Malware and potentially unwanted software categories in Hong Kong S.A.R. in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Hong Kong S.A.R. in 2Q12 was Miscellaneous Trojans. It affected 31.7 percent of all computers with detections there, up from 30.6 percent in 1Q12.
- The second most common category in Hong Kong S.A.R. in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 31.5 percent of all computers with detections there, down from 35.3 percent in 1Q12.
- The third most common category in Hong Kong S.A.R. in 2Q12 was Adware, which affected 19.3 percent of all computers with detections there, up from 14.1 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Hong Kong S.A.R. in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Keygen	Misc. Potentially Unwanted Software	12.1%
2	JS/IframeRef	Misc. Trojans	11.5%
3	JS/Pornpop	Adware	10.1%
4	Win32/Autorun	Worms	6.5%
5	Win32/Taterf	Worms	3.9%
6	JS/Popupper	Adware	3.3%
7	ASX/Wimad	Trojan Downloaders & Droppers	3.1%
8	Win32/Obfuscator	Misc. Potentially Unwanted Software	3.1%
9	Win32/FakePAV	Misc. Trojans	3.0%
10	Win32/Dynamer	Misc. Trojans	2.9%

- The most common threat family in Hong Kong S.A.R. in 2Q12 was [Win32/Keygen](#), which affected 12.1 percent of computers with detections in Hong Kong S.A.R.. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The second most common threat family in Hong Kong S.A.R. in 2Q12 was [JS/IframeRef](#), which affected 11.5 percent of computers with detections in Hong Kong S.A.R.. [JS/IframeRef](#) is a generic detection for specially formed IFrame tags that point to remote websites that contain malicious content.
- The third most common threat family in Hong Kong S.A.R. in 2Q12 was [JS/Pornpop](#), which affected 10.1 percent of computers with detections in Hong Kong S.A.R.. [JS/Pornpop](#) is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The fourth most common threat family in Hong Kong S.A.R. in 2Q12 was [Win32/Autorun](#), which affected 6.5 percent of computers with detections in Hong Kong S.A.R.. [Win32/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.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Hong Kong S.A.R.

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	1.93 (1.6)	2.41 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	3.63 (3.9)	4.62 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	1.19 (0.7)	0.48 (0.9)

Update service usage

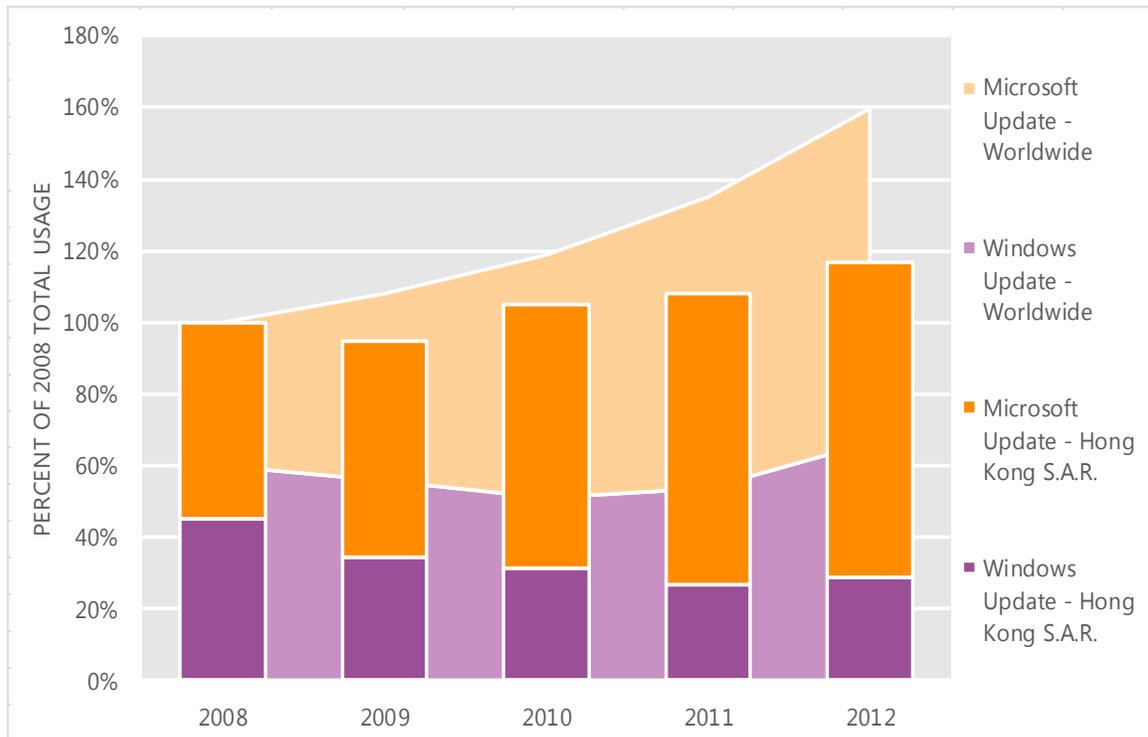
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Hong Kong S.A.R. and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Hong Kong S.A.R. over the last four years, indexed to the total usage for both services in Hong Kong S.A.R. in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Hong Kong S.A.R. was up 8.1 percent from 2011, and up 17.0 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Hong Kong S.A.R. in 2012, 75.6 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Hungary

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Hungary in 2Q12 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.

Infection rate statistics for Hungary

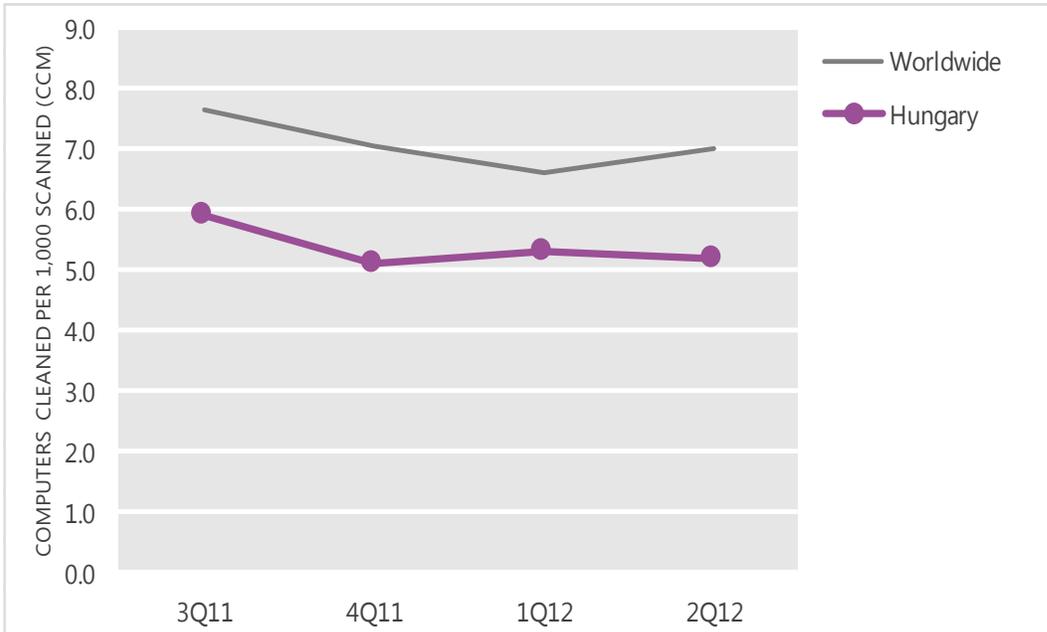
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	5.9	5.1	5.3	5.2
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

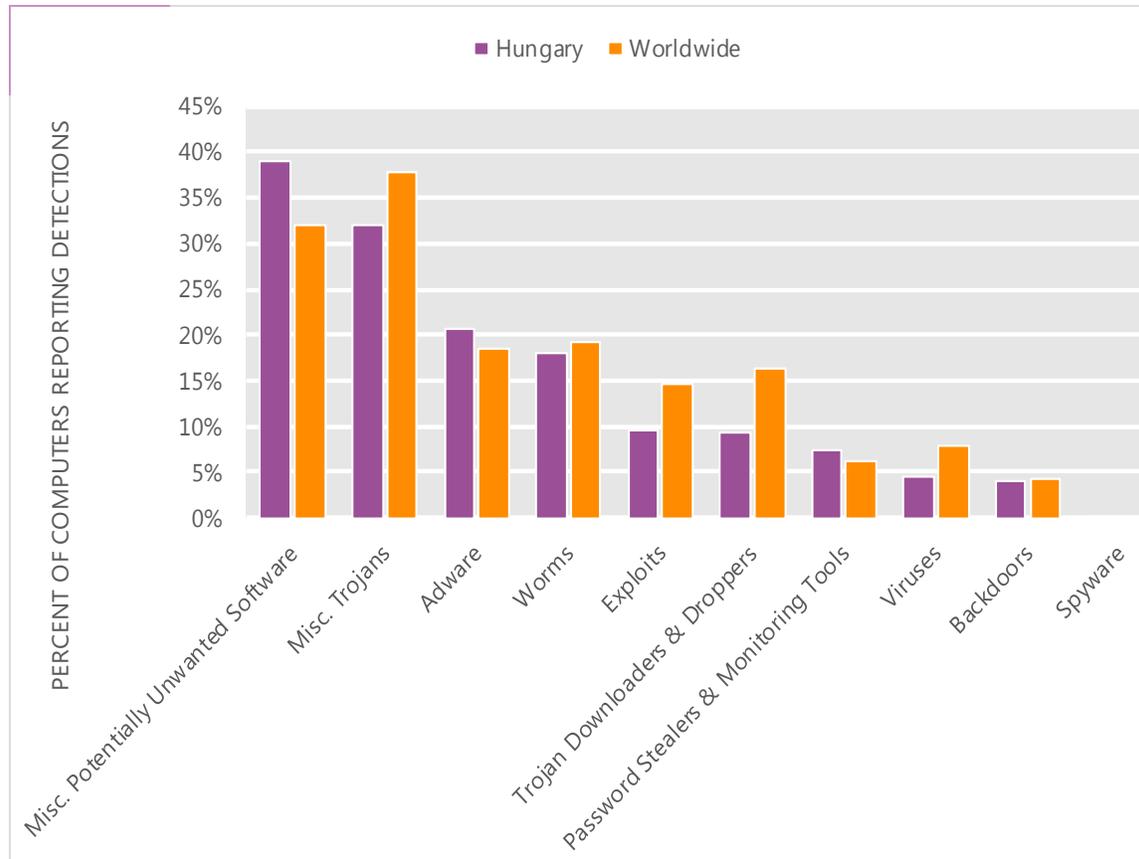
The MSRT detected malware on 5.2 of every 1,000 computers scanned in Hungary in 2Q12 (a CCM score of 5.2, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Hungary over the last four quarters, compared to the world as a whole.

CCM infection trends in Hungary and worldwide



Threat categories

Malware and potentially unwanted software categories in Hungary in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Hungary in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 39.0 percent of all computers with detections there, down from 39.7 percent in 1Q12.
- The second most common category in Hungary in 2Q12 was Miscellaneous Trojans. It affected 31.9 percent of all computers with detections there, down from 32.2 percent in 1Q12.
- The third most common category in Hungary in 2Q12 was Adware, which affected 20.7 percent of all computers with detections there, up from 20.4 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Hungary in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Keygen	Misc. Potentially Unwanted Software	17.1%
2	JS/Pornpop	Adware	11.0%
3	Win32/Autorun	Worms	7.3%
4	JS/IframeRef	Misc. Trojans	5.9%
5	Win32/Conficker	Worms	5.2%
6	Win32/Hotbar	Adware	5.0%
7	Win32/Obfuscator	Misc. Potentially Unwanted Software	4.4%
8	Win32/Zwangi	Misc. Potentially Unwanted Software	3.4%
9	Win32/Cmdow	Misc. Potentially Unwanted Software	3.3%
10	Win32/Dynamer	Misc. Trojans	3.1%

- The most common threat family in Hungary in 2Q12 was [Win32/Keygen](#), which affected 17.1 percent of computers with detections in Hungary. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The second most common threat family in Hungary in 2Q12 was [JS/Pornpop](#), which affected 11.0 percent of computers with detections in Hungary. [JS/Pornpop](#) is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The third most common threat family in Hungary in 2Q12 was [Win32/Autorun](#), which affected 7.3 percent of computers with detections in Hungary. [Win32/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 threat family in Hungary in 2Q12 was [JS/IframeRef](#), which affected 5.9 percent of computers with detections in Hungary. [JS/IframeRef](#) is a generic detection for specially formed IFrame tags that point to remote websites that contain malicious content.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Hungary

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	2.30 (1.6)	2.88 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	3.15 (3.9)	3.11 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	3.84 (0.7)	3.00 (0.9)

Update service usage

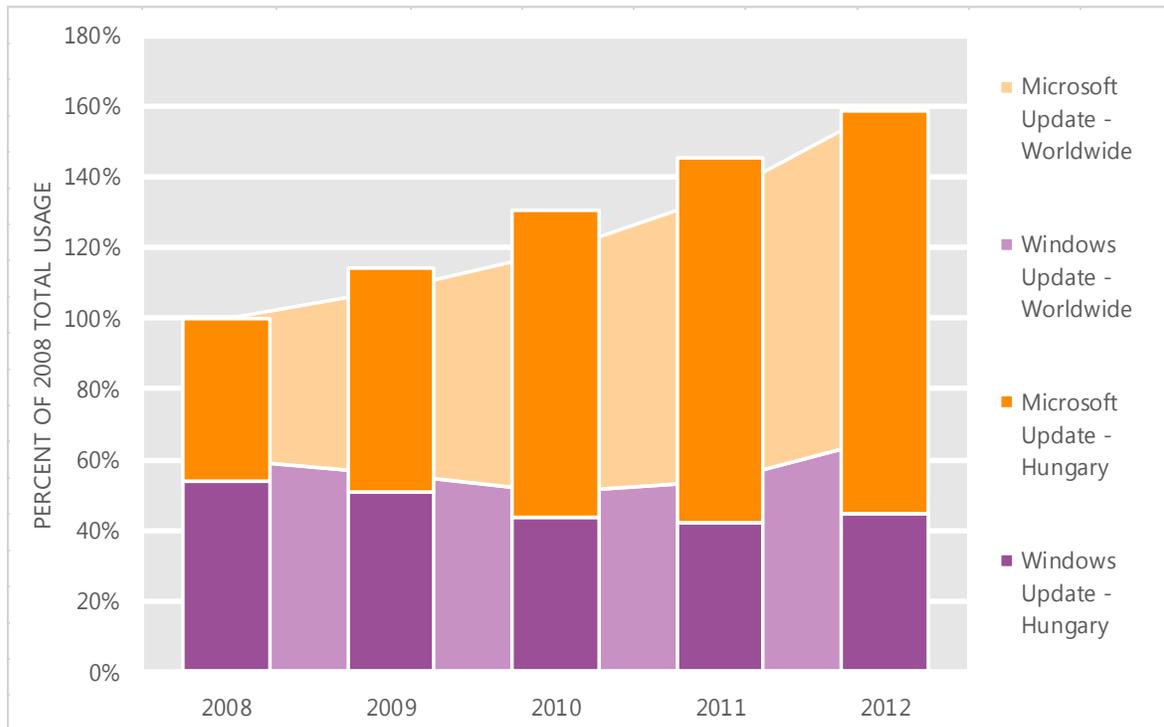
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Hungary and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Hungary over the last four years, indexed to the total usage for both services in Hungary in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Hungary was up 9.1 percent from 2011, and up 58.7 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Hungary in 2012, 72.0 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Iceland

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Iceland in 2Q12 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.

Infection rate statistics for Iceland

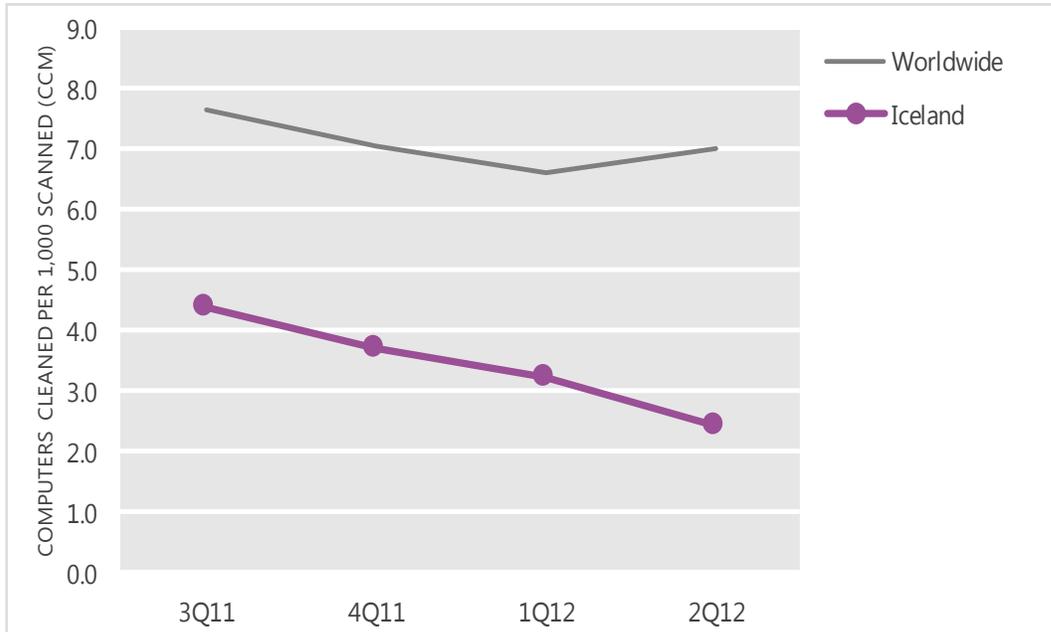
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	4.4	3.7	3.2	2.4
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

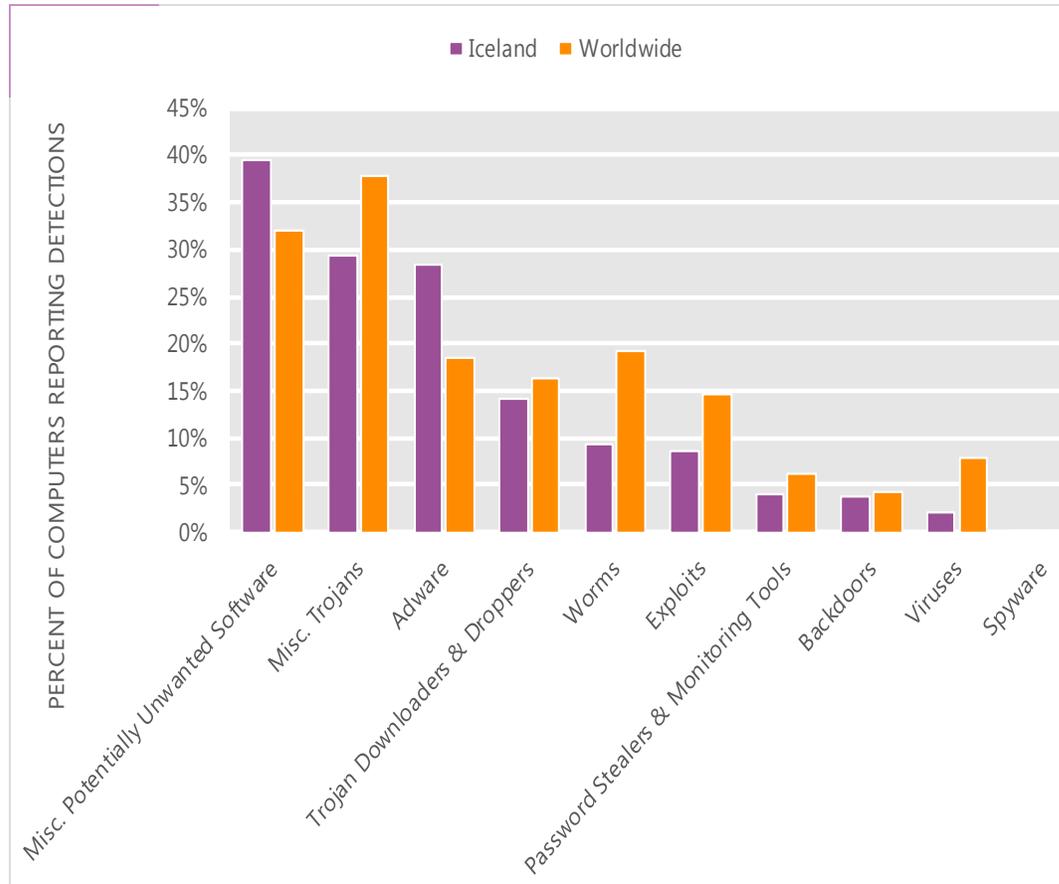
The MSRT detected malware on 2.4 of every 1,000 computers scanned in Iceland in 2Q12 (a CCM score of 2.4, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Iceland over the last four quarters, compared to the world as a whole.

CCM infection trends in Iceland and worldwide



Threat categories

Malware and potentially unwanted software categories in Iceland in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Iceland in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 39.5 percent of all computers with detections there, up from 36.3 percent in 1Q12.
- The second most common category in Iceland in 2Q12 was Miscellaneous Trojans. It affected 29.3 percent of all computers with detections there, down from 34.6 percent in 1Q12.
- The third most common category in Iceland in 2Q12 was Adware, which affected 28.3 percent of all computers with detections there, down from 31.9 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Iceland in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Keygen	Misc. Potentially Unwanted Software	14.5%
2	Win32/Hotbar	Adware	13.4%
3	JS/Pornpop	Adware	10.9%
4	Win32/Zwangi	Misc. Potentially Unwanted Software	9.6%
5	ASX/Wimad	Trojan Downloaders & Droppers	6.8%
6	JS/IframeRef	Misc. Trojans	6.3%
7	Win32/Obfuscator	Misc. Potentially Unwanted Software	3.5%
8	Win32/Sirefef	Misc. Trojans	3.0%
9	Win32/Autorun	Worms	2.9%
10	Java/Blacole	Exploits	2.6%

- The most common threat family in Iceland in 2Q12 was [Win32/Keygen](#), which affected 14.5 percent of computers with detections in Iceland. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The second most common threat family in Iceland in 2Q12 was [Win32/Hotbar](#), which affected 13.4 percent of computers with detections in Iceland. [Win32/Hotbar](#) is adware that displays a dynamic toolbar and targeted pop-up ads based on its monitoring of web-browsing activity.
- The third most common threat family in Iceland in 2Q12 was [JS/Pornpop](#), which affected 10.9 percent of computers with detections in Iceland. [JS/Pornpop](#) is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The fourth most common threat family in Iceland in 2Q12 was [Win32/Zwangi](#), which affected 9.6 percent of computers with detections in Iceland. [Win32/Zwangi](#) is a program that runs as a service in the background and modifies web browser settings to visit a particular website.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Iceland

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	2.97 (1.6)	4.61 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	1.65 (3.9)	2.97 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.49 (0.7)	0.35 (0.9)

Update service usage

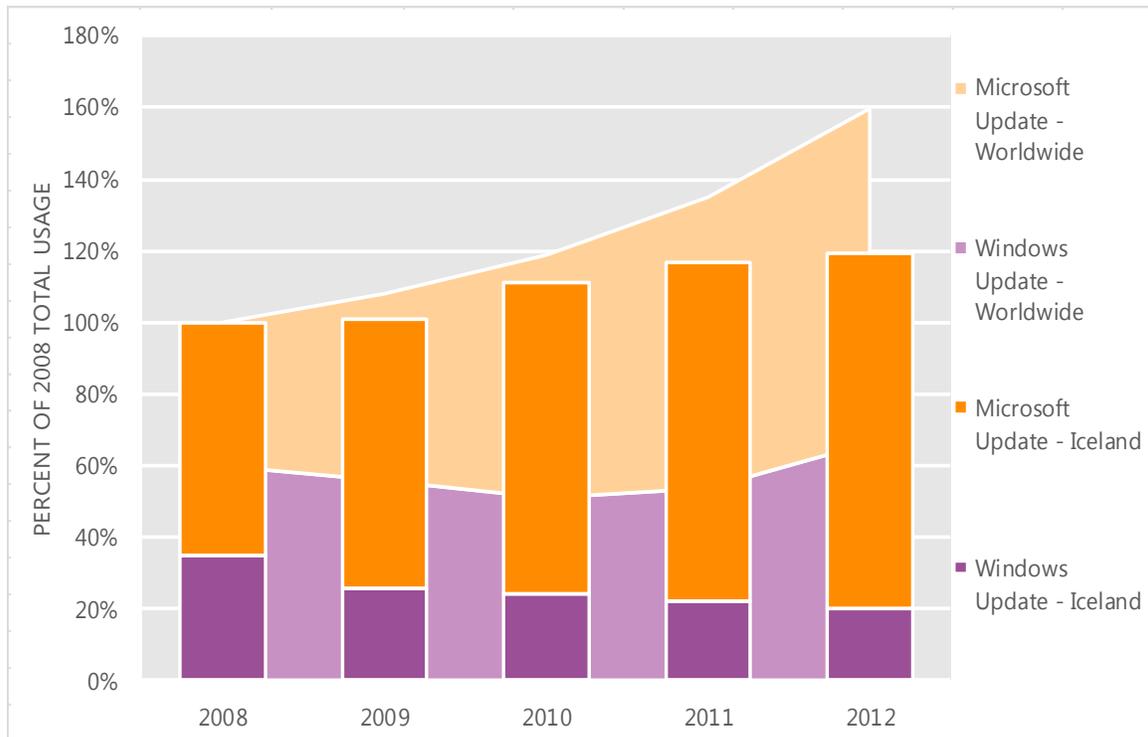
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Iceland and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Iceland over the last four years, indexed to the total usage for both services in Iceland in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Iceland was up 2.3 percent from 2011, and up 19.4 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Iceland in 2012, 83.2 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

India

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in India in 2Q12 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.

Infection rate statistics for India

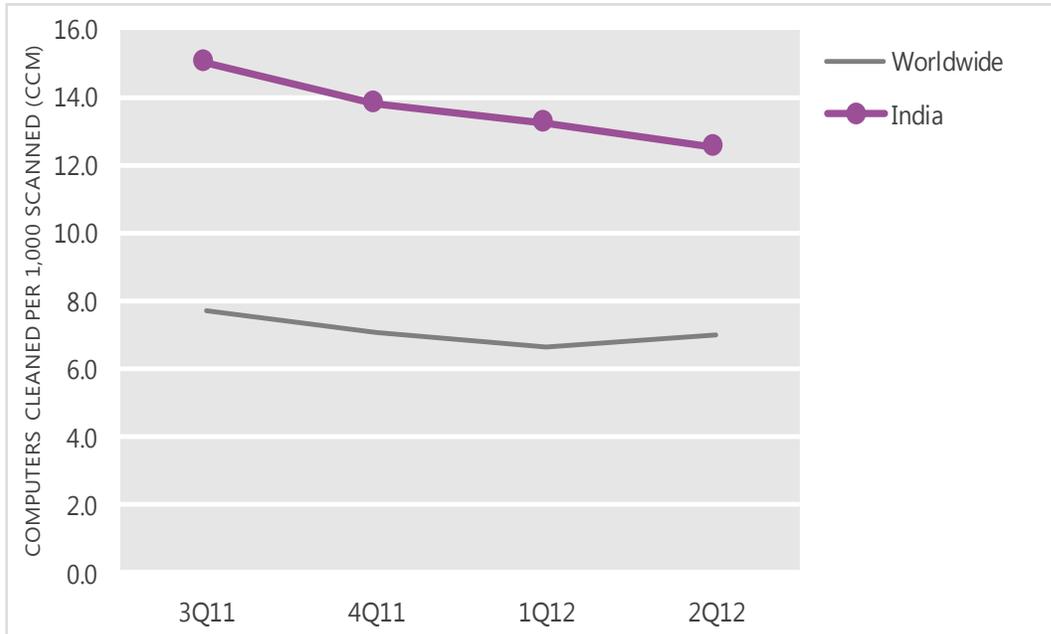
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	15.0	13.8	13.2	12.5
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

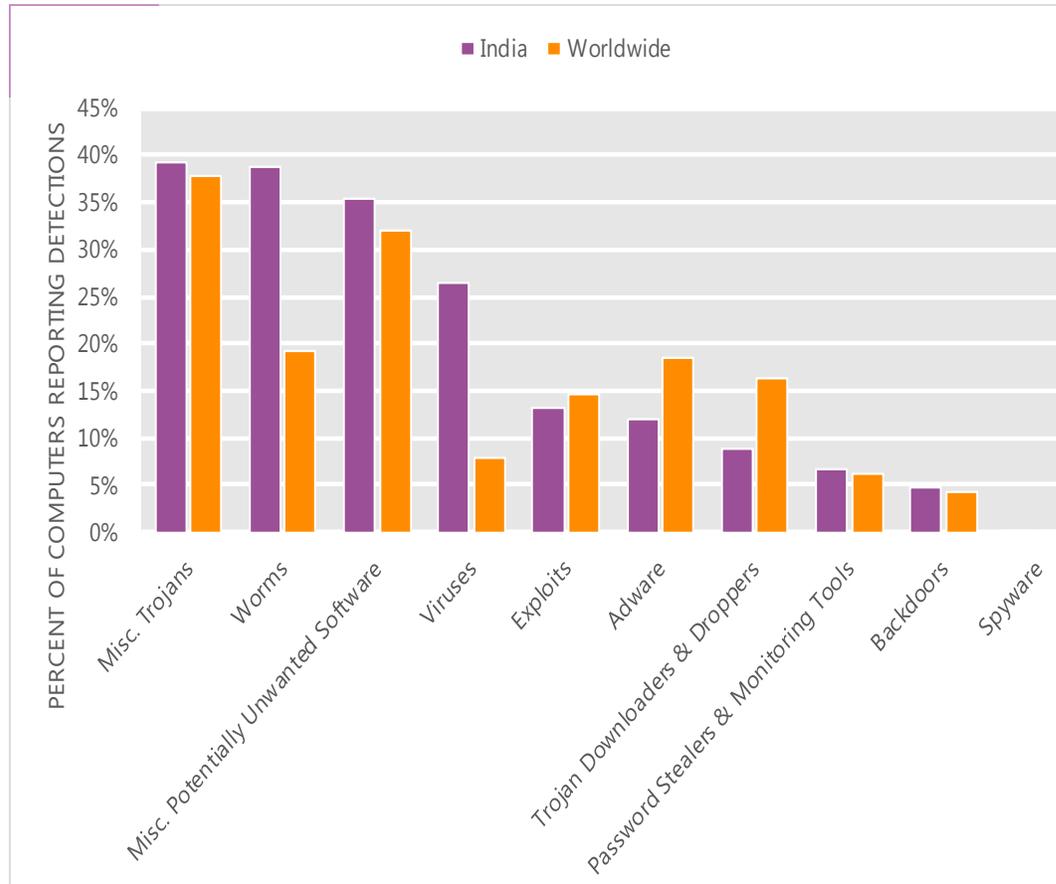
The MSRT detected malware on 12.5 of every 1,000 computers scanned in India in 2Q12 (a CCM score of 12.5, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for India over the last four quarters, compared to the world as a whole.

CCM infection trends in India and worldwide



Threat categories

Malware and potentially unwanted software categories in India in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in India in 2Q12 was Miscellaneous Trojans. It affected 39.2 percent of all computers with detections there, down from 39.4 percent in 1Q12.
- The second most common category in India in 2Q12 was Worms. It affected 38.8 percent of all computers with detections there, down from 40.7 percent in 1Q12.
- The third most common category in India in 2Q12 was Miscellaneous Potentially Unwanted Software, which affected 35.3 percent of all computers with detections there, down from 35.6 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in India in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Autorun	Worms	22.2%
2	Win32/Sality	Viruses	18.8%
3	Win32/Ramnit	Misc. Trojans	13.9%
4	Win32/Keygen	Misc. Potentially Unwanted Software	11.5%
5	Win32/CplLnk	Exploits	9.7%
6	Win32/Rimecud	Worms	9.3%
7	Win32/Nuqel	Worms	8.5%
8	Win32/Virut	Viruses	6.1%
9	Win32/Conficker	Worms	5.2%
10	JS/Pornpop	Adware	5.0%

- The most common threat family in India in 2Q12 was [Win32/Autorun](#), which affected 22.2 percent of computers with detections in India. [Win32/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 threat family in India in 2Q12 was [Win32/Sality](#), which affected 18.8 percent of computers with detections in India. [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 in India in 2Q12 was [Win32/Ramnit](#), which affected 13.9 percent of computers with detections in India. [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 in India in 2Q12 was [Win32/Keygen](#), which affected 11.5 percent of computers with detections in India. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for India

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	0.88 (1.6)	0.84 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	1.48 (3.9)	2.08 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.19 (0.7)	0.69 (0.9)

Update service usage

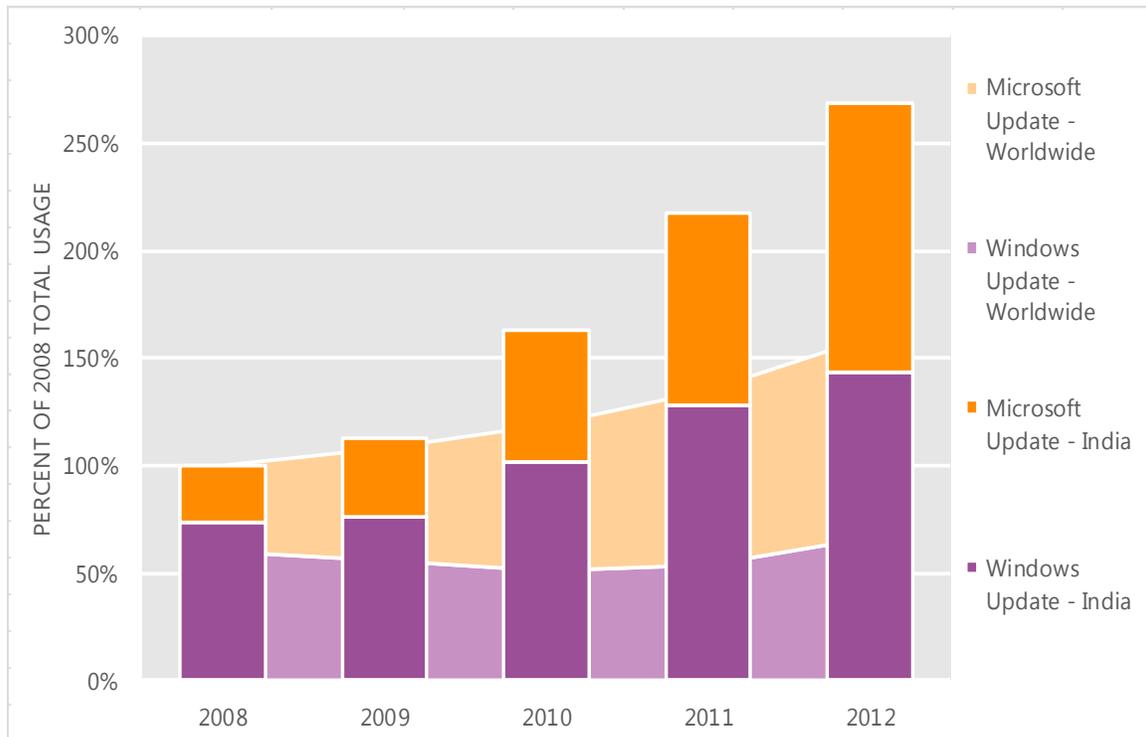
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in India and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in India over the last four years, indexed to the total usage for both services in India in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in India was up 23.5 percent from 2011, and up 169.1 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in India in 2012, 46.8 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Indonesia

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Indonesia in 2Q12 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.

Infection rate statistics for Indonesia

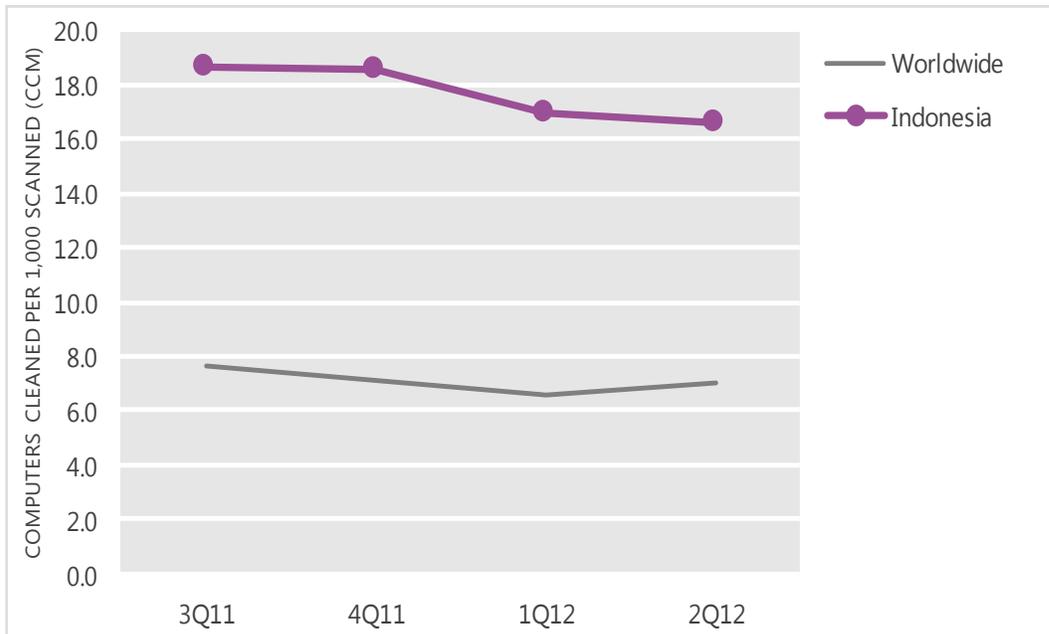
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	18.7	18.6	17.0	16.6
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

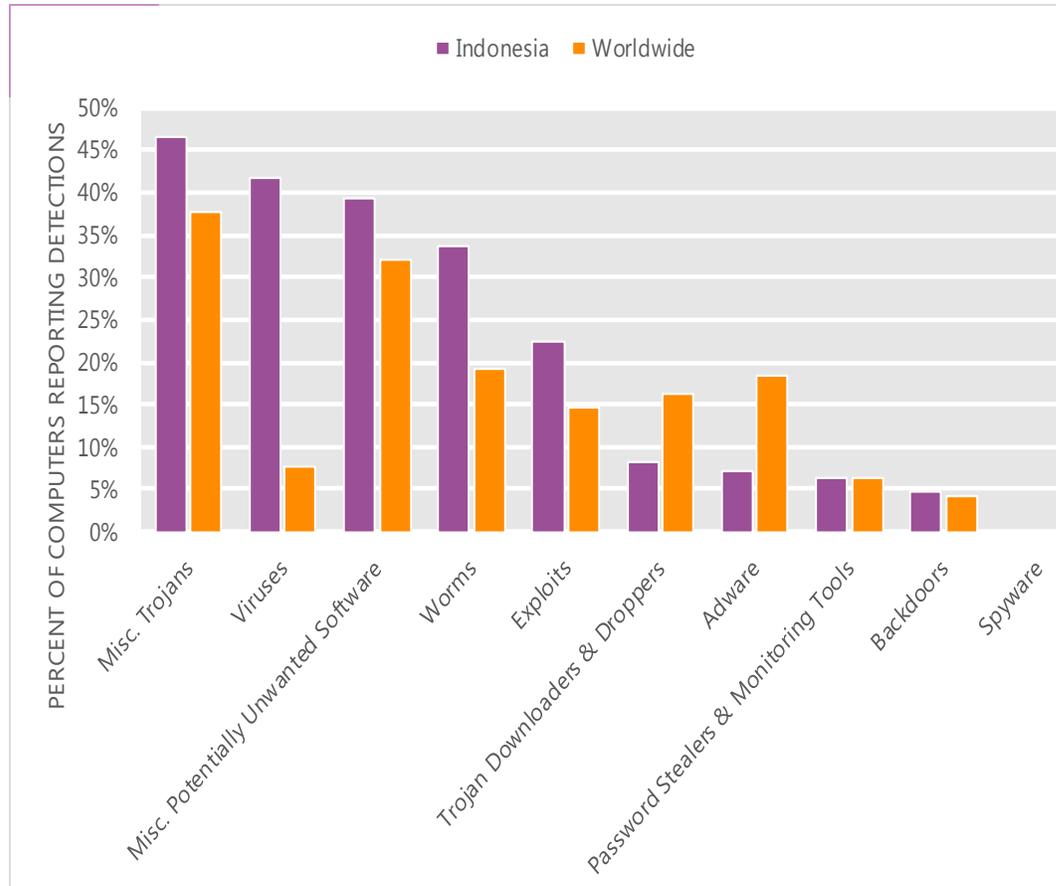
The MSRT detected malware on 16.6 of every 1,000 computers scanned in Indonesia in 2Q12 (a CCM score of 16.6, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Indonesia over the last four quarters, compared to the world as a whole.

CCM infection trends in Indonesia and worldwide



Threat categories

Malware and potentially unwanted software categories in Indonesia in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Indonesia in 2Q12 was Miscellaneous Trojans. It affected 46.6 percent of all computers with detections there, down from 48.8 percent in 1Q12.
- The second most common category in Indonesia in 2Q12 was Viruses. It affected 41.8 percent of all computers with detections there, down from 43.3 percent in 1Q12.
- The third most common category in Indonesia in 2Q12 was Miscellaneous Potentially Unwanted Software, which affected 39.2 percent of all computers with detections there, up from 38.6 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Indonesia in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Ramnit	Misc. Trojans	35.2%
2	Win32/CplLnk	Exploits	19.4%
3	Win32/Keygen	Misc. Potentially Unwanted Software	18.2%
4	Win32/Sality	Viruses	17.4%
5	Win32/Dorkbot	Worms	14.8%
6	Win32/Autorun	Worms	12.1%
7	Win32/Virut	Viruses	11.8%
8	Win32/Conficker	Worms	7.0%
9	Win32/Patch	Misc. Potentially Unwanted Software	4.1%
10	Win32/Slugin	Viruses	4.0%

- The most common threat family in Indonesia in 2Q12 was [Win32/Ramnit](#), which affected 35.2 percent of computers with detections in Indonesia. [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 in Indonesia in 2Q12 was [Win32/CplLnk](#), which affected 19.4 percent of computers with detections in Indonesia. [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 threat family in Indonesia in 2Q12 was [Win32/Keygen](#), which affected 18.2 percent of computers with detections in Indonesia. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The fourth most common threat family in Indonesia in 2Q12 was [Win32/Sality](#), which affected 17.4 percent of computers with detections in Indonesia. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Indonesia

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	2.72 (1.6)	3.51 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	3.64 (3.9)	4.52 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	1.52 (0.7)	2.23 (0.9)

Update service usage

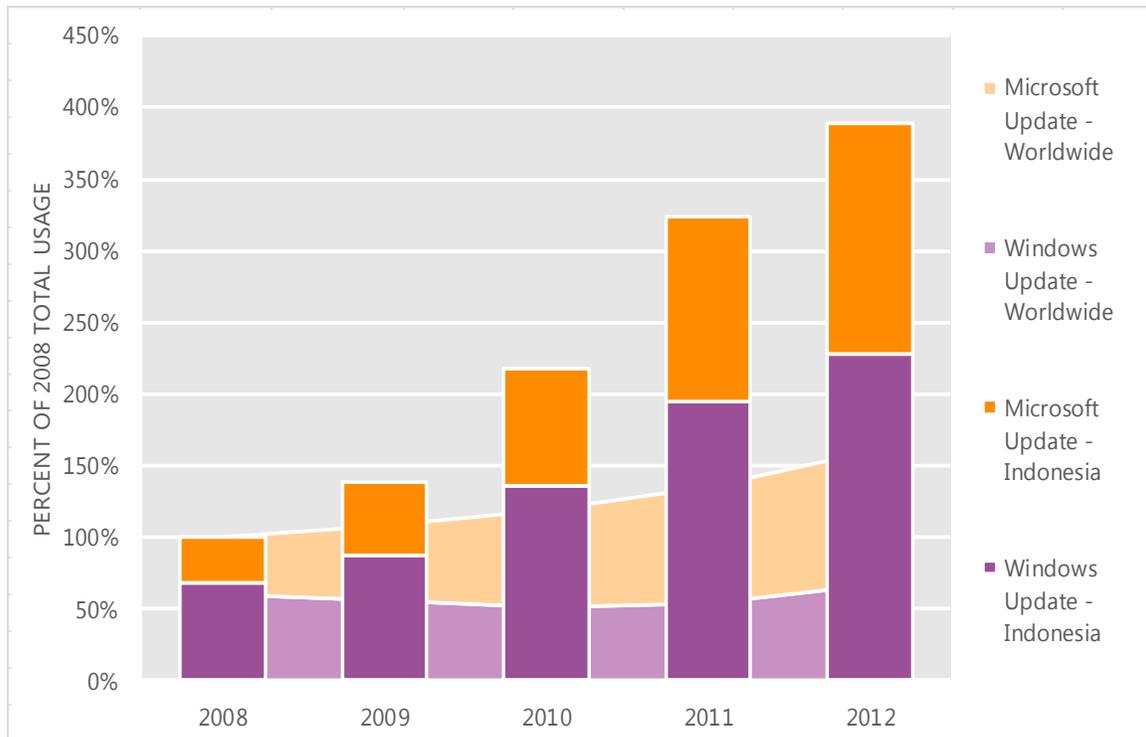
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Indonesia and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Indonesia over the last four years, indexed to the total usage for both services in Indonesia in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Indonesia was up 20.3 percent from 2011, and up 289.7 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Indonesia in 2012, 41.6 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Iraq

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Iraq in 2Q12 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.

Infection rate statistics for Iraq

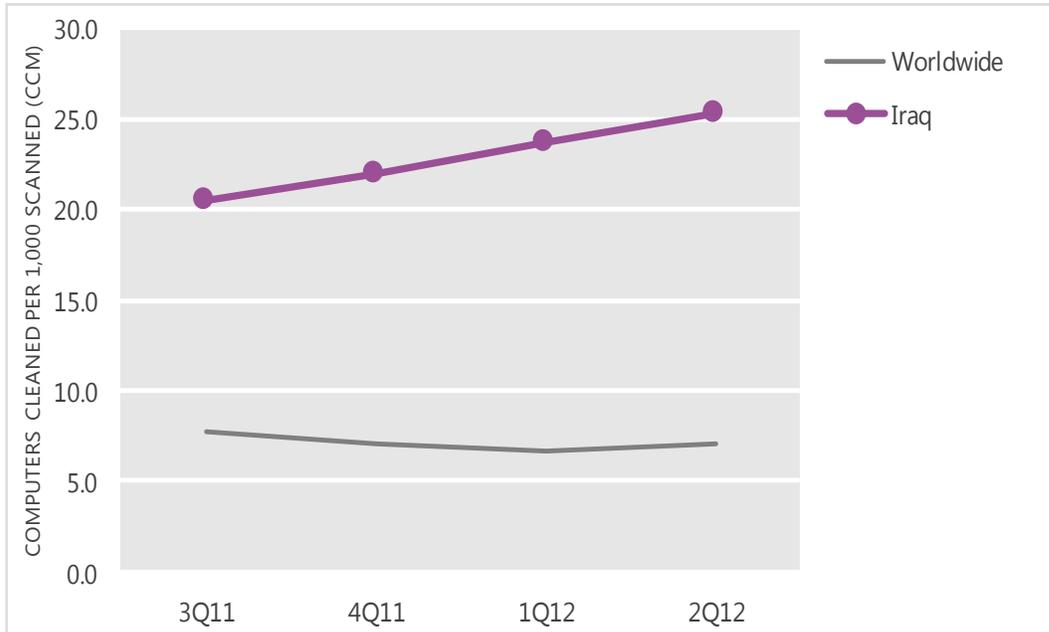
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	20.5	22.0	23.7	25.3
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

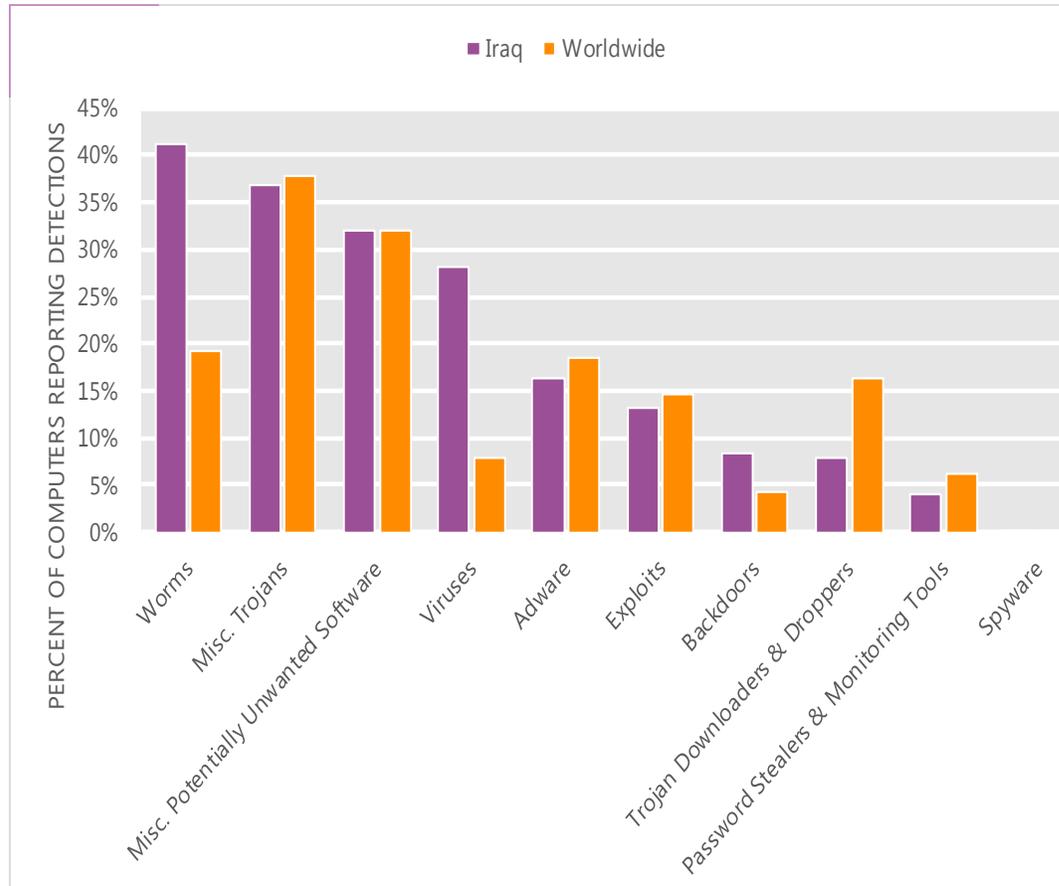
The MSRT detected malware on 25.3 of every 1,000 computers scanned in Iraq in 2Q12 (a CCM score of 25.3, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Iraq over the last four quarters, compared to the world as a whole.

CCM infection trends in Iraq and worldwide



Threat categories

Malware and potentially unwanted software categories in Iraq in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Iraq in 2Q12 was Worms. It affected 41.1 percent of all computers with detections there, up from 38.4 percent in 1Q12.
- The second most common category in Iraq in 2Q12 was Miscellaneous Trojans. It affected 36.8 percent of all computers with detections there, down from 37.1 percent in 1Q12.
- The third most common category in Iraq in 2Q12 was Miscellaneous Potentially Unwanted Software, which affected 31.9 percent of all computers with detections there, down from 36.6 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Iraq in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Autorun	Worms	20.4%
2	Win32/Sality	Viruses	19.8%
3	Win32/Ramnit	Misc. Trojans	16.4%
4	Win32/Keygen	Misc. Potentially Unwanted Software	14.5%
5	Win32/CplLnk	Exploits	11.6%
6	Win32/Dorkbot	Worms	10.8%
7	Win32/Vobfus	Worms	8.7%
8	JS/Paypopup	Adware	6.8%
9	Win32/Brontok	Worms	6.1%
10	JS/Pornpop	Adware	6.1%

- The most common threat family in Iraq in 2Q12 was [Win32/Autorun](#), which affected 20.4 percent of computers with detections in Iraq. [Win32/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 threat family in Iraq in 2Q12 was [Win32/Sality](#), which affected 19.8 percent of computers with detections in Iraq. [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 in Iraq in 2Q12 was [Win32/Ramnit](#), which affected 16.4 percent of computers with detections in Iraq. [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 in Iraq in 2Q12 was [Win32/Keygen](#), which affected 14.5 percent of computers with detections in Iraq. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Iraq

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	N/A (1.6)	N/A (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	N/A (3.9)	N/A (4.4)
Drive-by download per 1,000 URLs (Worldwide)	N/A (0.7)	N/A (0.9)

Update service usage

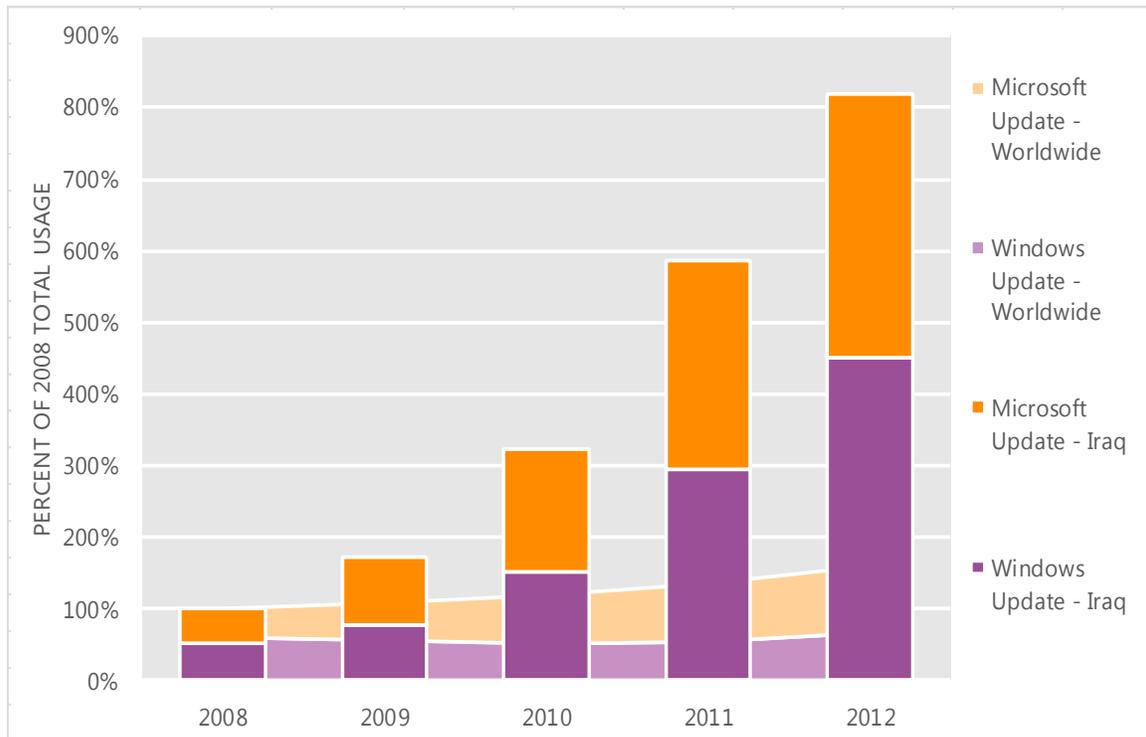
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Iraq and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Iraq over the last four years, indexed to the total usage for both services in Iraq in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Iraq was up 39.9 percent from 2011, and up 719.4 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Iraq in 2012, 44.9 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Ireland

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Ireland in 2Q12 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.

Infection rate statistics for Ireland

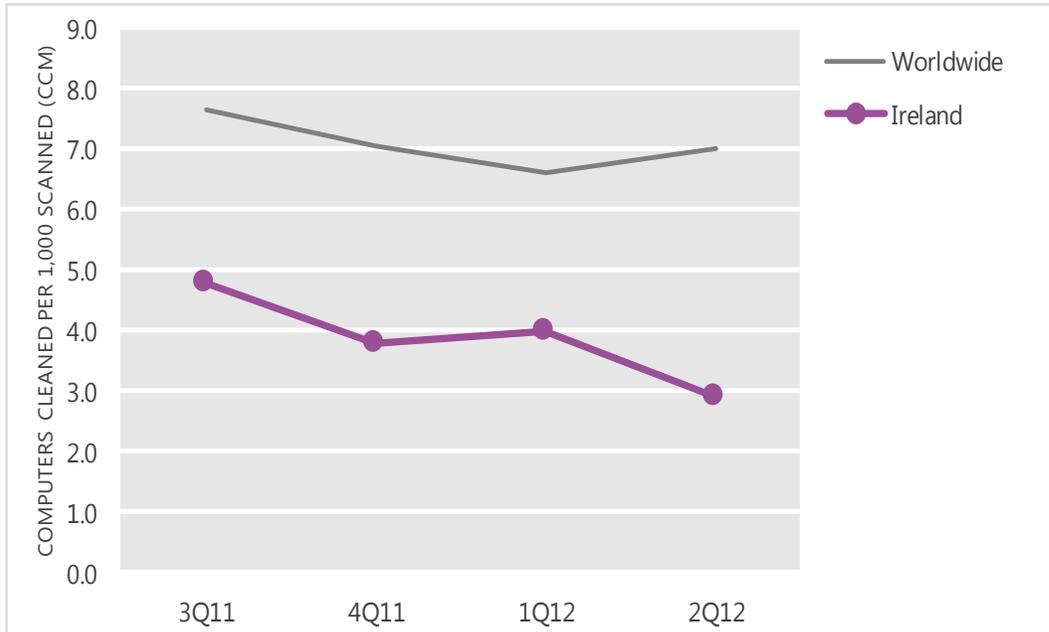
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	4.8	3.8	4.0	2.9
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

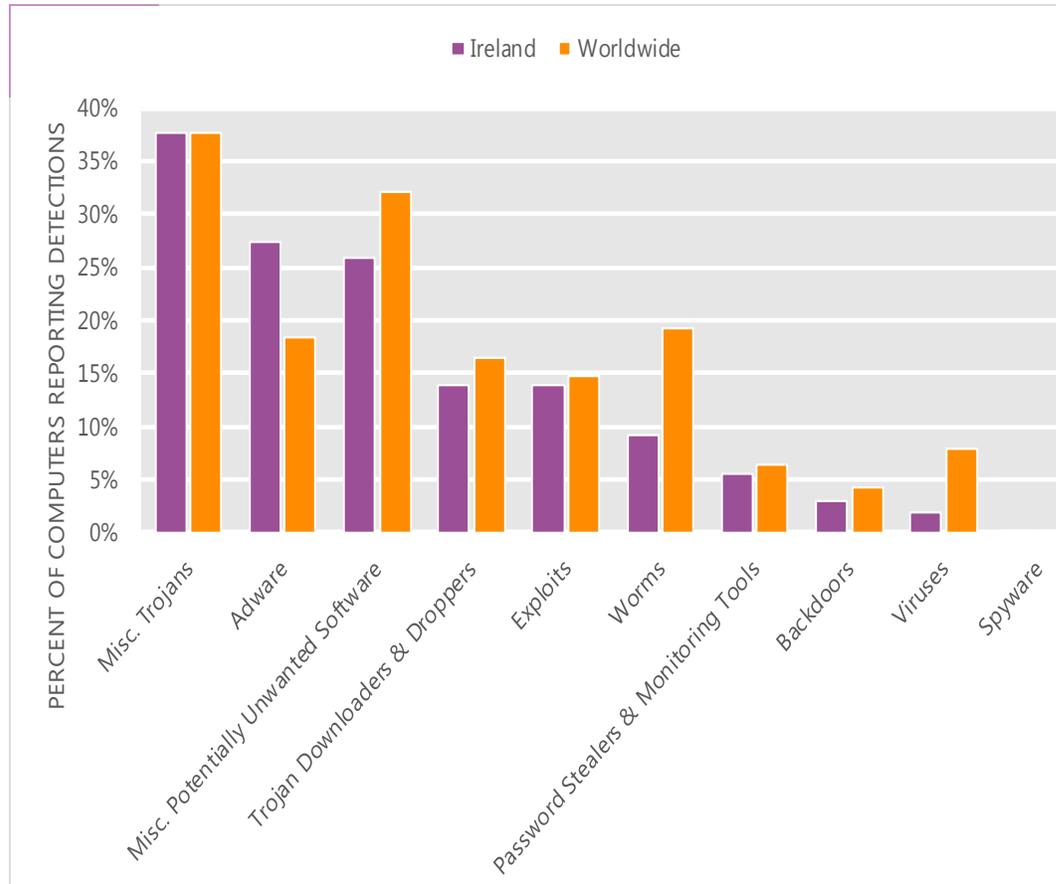
The MSRT detected malware on 2.9 of every 1,000 computers scanned in Ireland in 2Q12 (a CCM score of 2.9, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Ireland over the last four quarters, compared to the world as a whole.

CCM infection trends in Ireland and worldwide



Threat categories

Malware and potentially unwanted software categories in Ireland in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Ireland in 2Q12 was Miscellaneous Trojans. It affected 37.6 percent of all computers with detections there, down from 38.1 percent in 1Q12.
- The second most common category in Ireland in 2Q12 was Adware. It affected 27.4 percent of all computers with detections there, down from 33.5 percent in 1Q12.
- The third most common category in Ireland in 2Q12 was Miscellaneous Potentially Unwanted Software, which affected 25.9 percent of all computers with detections there, up from 23.3 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Ireland in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Hotbar	Adware	14.6%
2	JS/Pornpop	Adware	8.2%
3	Win32/Keygen	Misc. Potentially Unwanted Software	6.8%
4	ASX/Wimad	Trojan Downloaders & Droppers	6.5%
5	Win32/FakePAV	Misc. Trojans	5.9%
6	Win32/Zwangi	Misc. Potentially Unwanted Software	5.7%
7	JS/BlacoleRef	Misc. Trojans	5.4%
8	Java/Blacole	Exploits	5.3%
9	JS/IframeRef	Misc. Trojans	5.1%
10	Win32/Winwebsec	Misc. Trojans	3.2%

- The most common threat family in Ireland in 2Q12 was [Win32/Hotbar](#), which affected 14.6 percent of computers with detections in Ireland. [Win32/Hotbar](#) is adware that displays a dynamic toolbar and targeted pop-up ads based on its monitoring of web-browsing activity.
- The second most common threat family in Ireland in 2Q12 was [JS/Pornpop](#), which affected 8.2 percent of computers with detections in Ireland. [JS/Pornpop](#) is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The third most common threat family in Ireland in 2Q12 was [Win32/Keygen](#), which affected 6.8 percent of computers with detections in Ireland. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The fourth most common threat family in Ireland in 2Q12 was [ASX/Wimad](#), which affected 6.5 percent of computers with detections in Ireland. [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.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Ireland

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	2.92 (1.6)	2.54 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	2.17 (3.9)	3.07 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.70 (0.7)	0.83 (0.9)

Update service usage

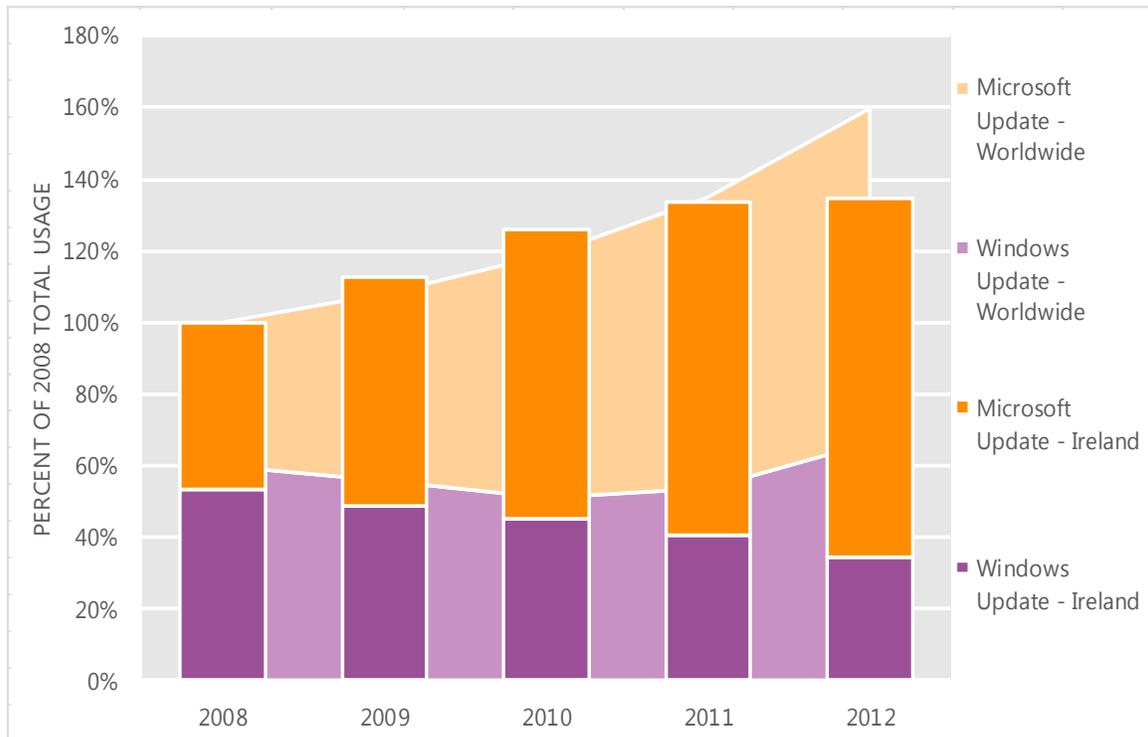
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Ireland and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Ireland over the last four years, indexed to the total usage for both services in Ireland in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Ireland was up 0.7 percent from 2011, and up 34.7 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Ireland in 2012, 74.7 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Israel

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Israel in 2Q12 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.

Infection rate statistics for Israel

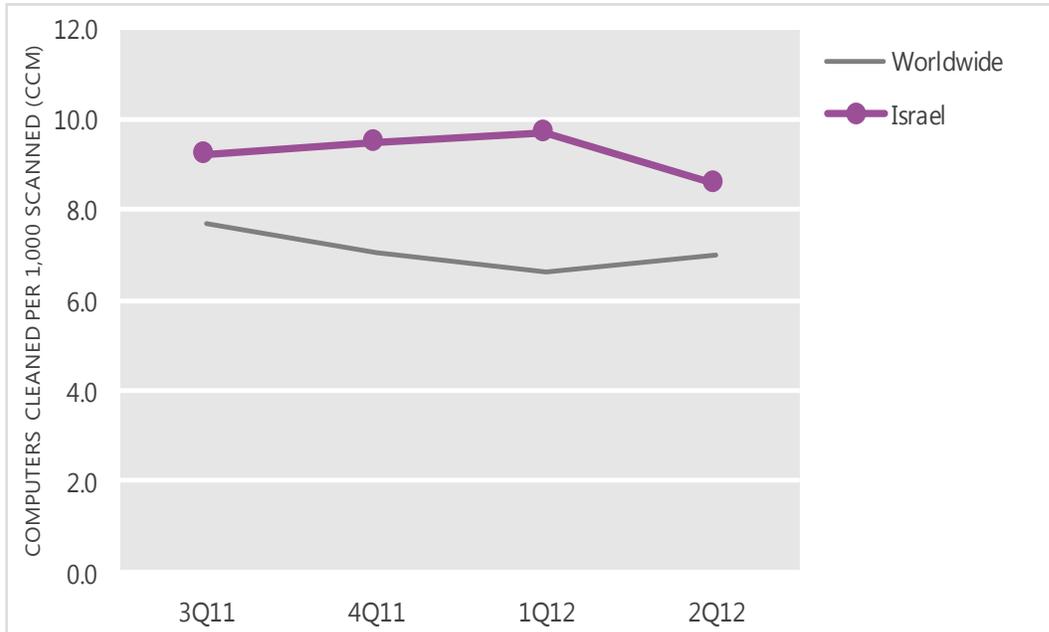
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	9.2	9.5	9.7	8.6
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

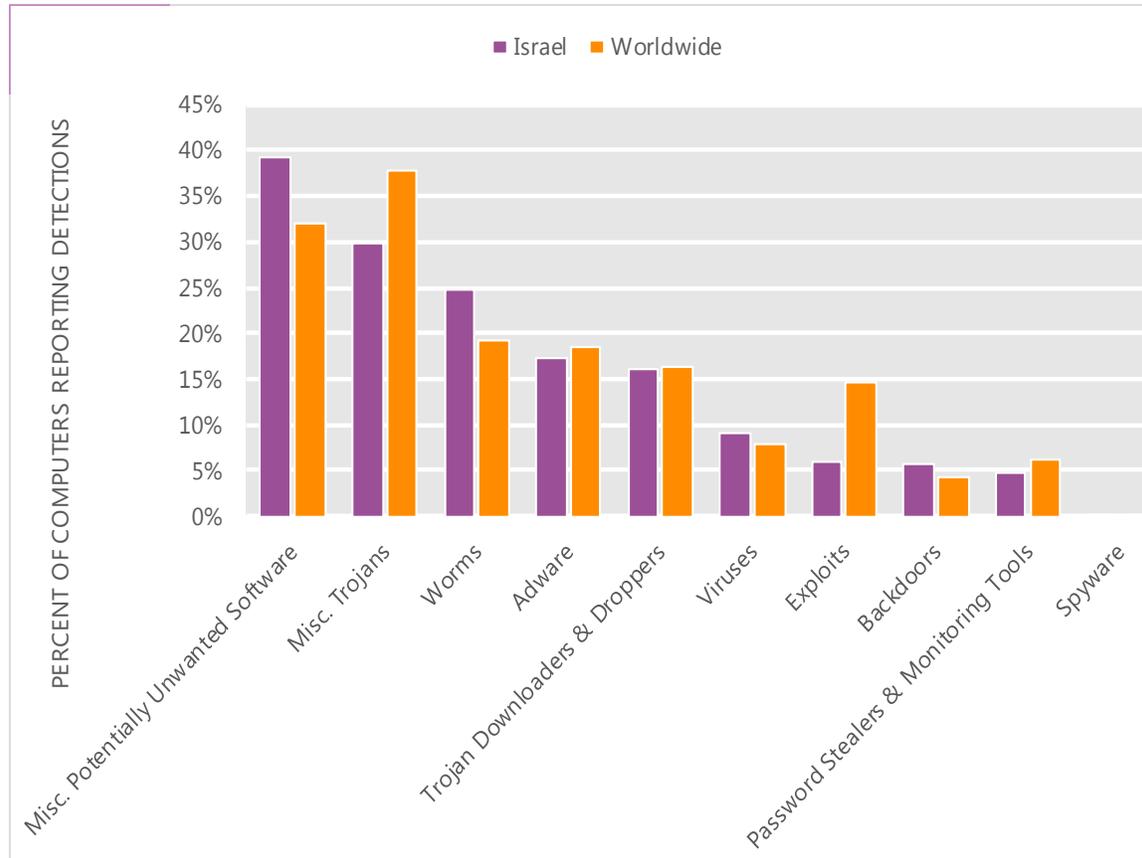
The MSRT detected malware on 8.6 of every 1,000 computers scanned in Israel in 2Q12 (a CCM score of 8.6, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Israel over the last four quarters, compared to the world as a whole.

CCM infection trends in Israel and worldwide



Threat categories

Malware and potentially unwanted software categories in Israel in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Israel in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 39.3 percent of all computers with detections there, up from 38.6 percent in 1Q12.
- The second most common category in Israel in 2Q12 was Miscellaneous Trojans. It affected 29.7 percent of all computers with detections there, up from 28.0 percent in 1Q12.
- The third most common category in Israel in 2Q12 was Worms, which affected 24.8 percent of all computers with detections there, down from 24.8 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Israel in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Keygen	Misc. Potentially Unwanted Software	12.0%
2	Win32/Autorun	Worms	10.4%
3	ASX/Wimad	Trojan Downloaders & Droppers	9.0%
4	Win32/AmmyyAdmin	Misc. Potentially Unwanted Software	6.3%
5	JS/Pornpop	Adware	6.3%
6	Win32/Sality	Viruses	6.0%
7	Win32/Brontok	Worms	5.5%
8	Win32/Hotbar	Adware	5.3%
9	JS/IframeRef	Misc. Trojans	4.5%
10	Win32/Obfuscator	Misc. Potentially Unwanted Software	3.5%

- The most common threat family in Israel in 2Q12 was [Win32/Keygen](#), which affected 12.0 percent of computers with detections in Israel. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The second most common threat family in Israel in 2Q12 was [Win32/Autorun](#), which affected 10.4 percent of computers with detections in Israel. [Win32/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 threat family in Israel in 2Q12 was [ASX/Wimad](#), which affected 9.0 percent of computers with detections in Israel. [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 threat family in Israel in 2Q12 was [Win32/AmmyyAdmin](#), which affected 6.3 percent of computers with detections in Israel. [Win32/AmmyyAdmin](#) is

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Israel

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	0.87 (1.6)	0.87 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	1.62 (3.9)	1.59 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.17 (0.7)	0.41 (0.9)

Update service usage

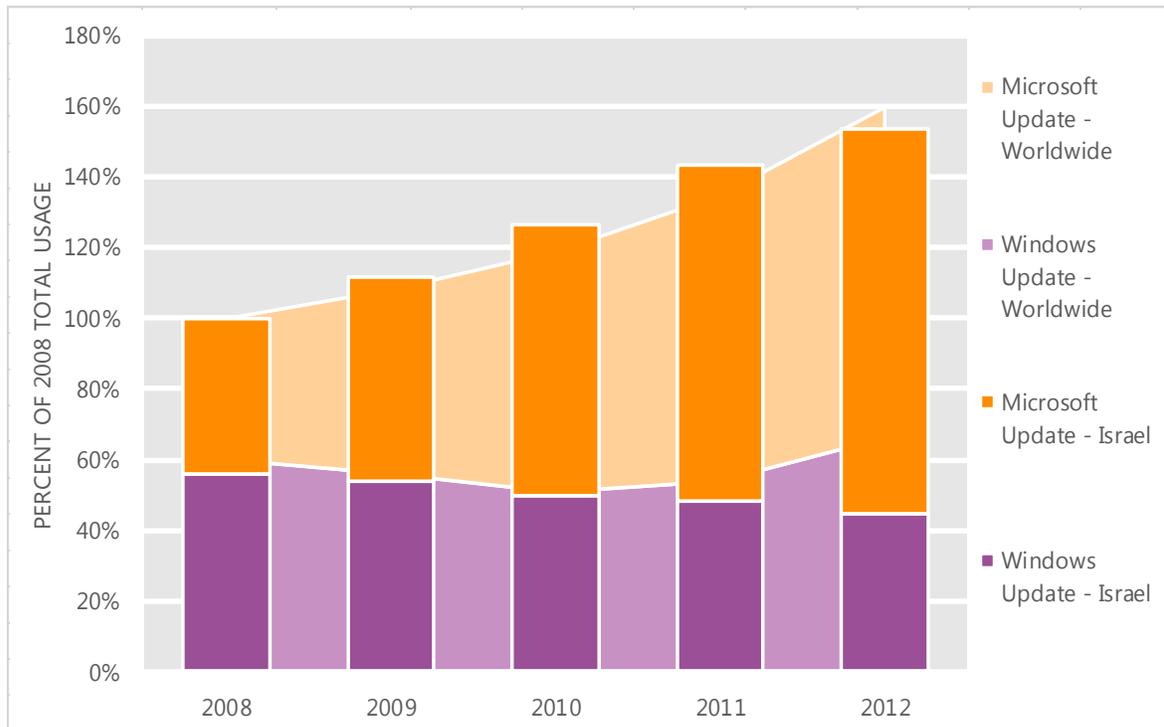
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Israel and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Israel over the last four years, indexed to the total usage for both services in Israel in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Israel was up 7.2 percent from 2011, and up 53.6 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Israel in 2012, 70.8 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Italy

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Italy in 2Q12 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.

Infection rate statistics for Italy

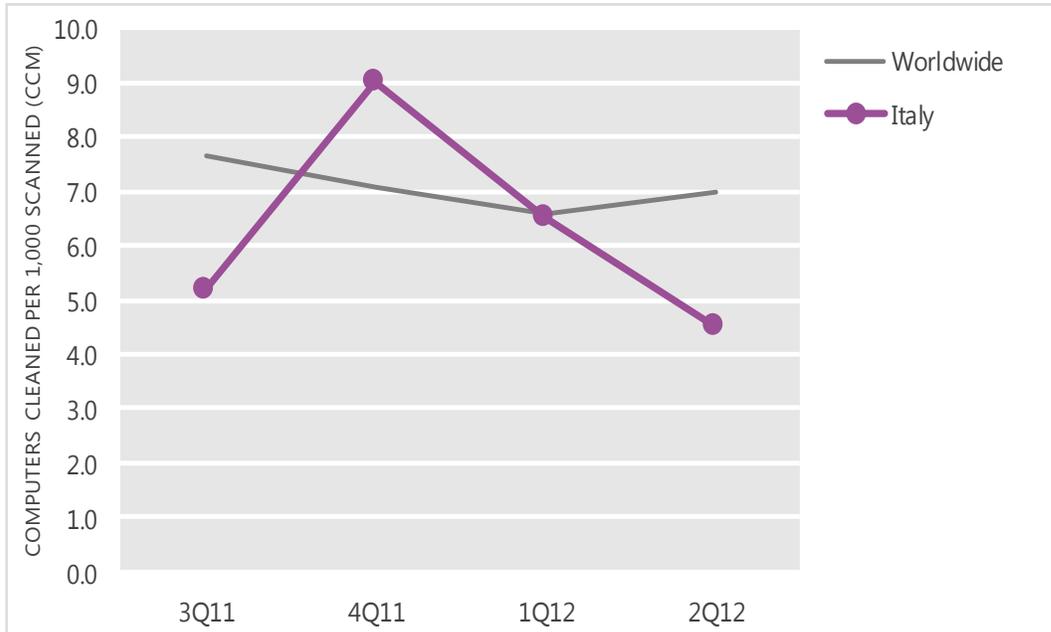
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	5.2	9.0	6.5	4.5
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

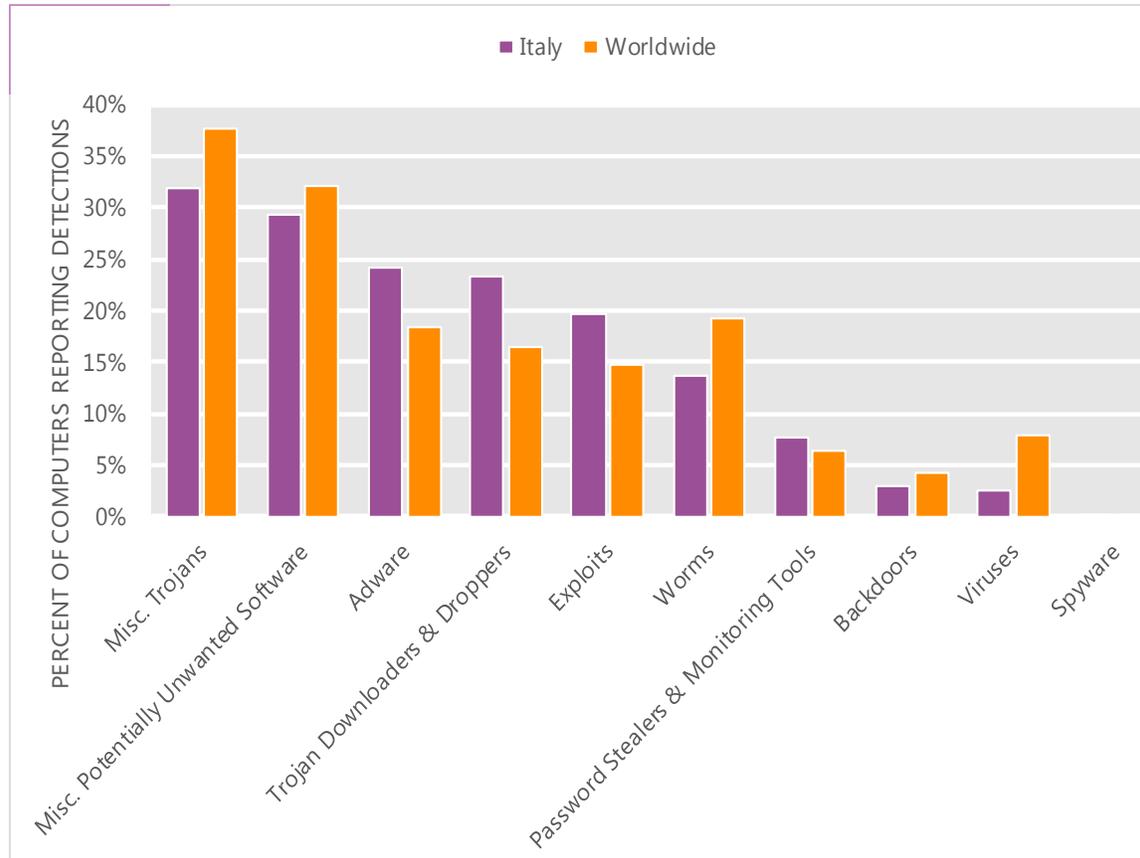
The MSRT detected malware on 4.5 of every 1,000 computers scanned in Italy in 2Q12 (a CCM score of 4.5, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Italy over the last four quarters, compared to the world as a whole.

CCM infection trends in Italy and worldwide



Threat categories

Malware and potentially unwanted software categories in Italy in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Italy in 2Q12 was Miscellaneous Trojans. It affected 31.8 percent of all computers with detections there, down from 32.5 percent in 1Q12.
- The second most common category in Italy in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 29.4 percent of all computers with detections there, up from 29.3 percent in 1Q12.
- The third most common category in Italy in 2Q12 was Adware, which affected 24.1 percent of all computers with detections there, down from 33.4 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Italy in 2Q12

	Family	Most significant category	% of computers with detections
1	ASX/Wimad	Trojan Downloaders & Droppers	17.0%
2	JS/Pornpop	Adware	13.7%
3	Java/Blacole	Exploits	12.5%
4	Win32/Keygen	Misc. Potentially Unwanted Software	8.4%
5	JS/BlacoleRef	Misc. Trojans	5.1%
6	Win32/Autorun	Worms	5.1%
7	Win32/Conficker	Worms	5.0%
8	JS/IframeRef	Misc. Trojans	4.8%
9	Win32/Zbot	Password Stealers & Monitoring Tools	4.7%
10	Win32/Pdfjsc	Exploits	4.3%

- The most common threat family in Italy in 2Q12 was [ASX/Wimad](#), which affected 17.0 percent of computers with detections in Italy. [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 second most common threat family in Italy in 2Q12 was [JS/Pornpop](#), which affected 13.7 percent of computers with detections in Italy. [JS/Pornpop](#) is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The third most common threat family in Italy in 2Q12 was [Java/Blacole](#), which affected 12.5 percent of computers with detections in Italy. [Java/Blacole](#) is an exploit pack, also known as Blackhole, that is installed on a compromised web server by an attacker and includes a number of exploits that target browser software. If a vulnerable computer browses a compromised website that contains the exploit pack, various malware may be downloaded and run.
- The fourth most common threat family in Italy in 2Q12 was [Win32/Keygen](#), which affected 8.4 percent of computers with detections in Italy. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Italy

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	1.63 (1.6)	1.67 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	3.61 (3.9)	3.35 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.69 (0.7)	0.94 (0.9)

Update service usage

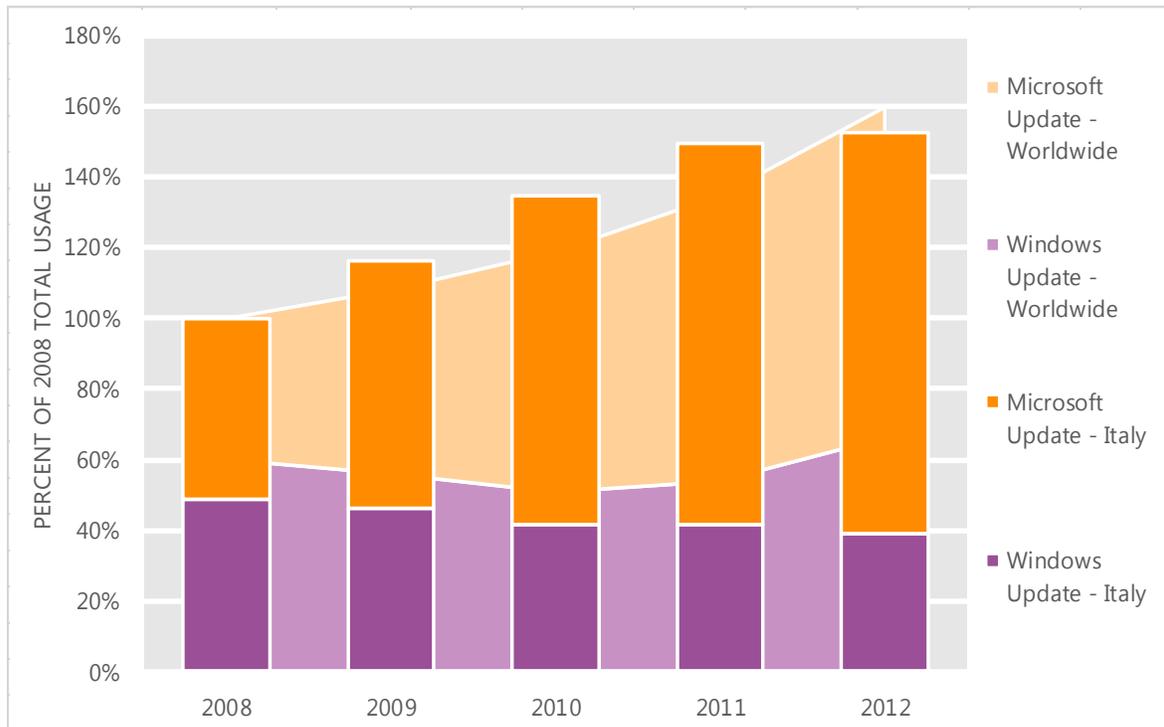
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Italy and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Italy over the last four years, indexed to the total usage for both services in Italy in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Italy was up 1.9 percent from 2011, and up 52.4 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Italy in 2012, 74.5 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Jamaica

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Jamaica in 2Q12 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.

Infection rate statistics for Jamaica

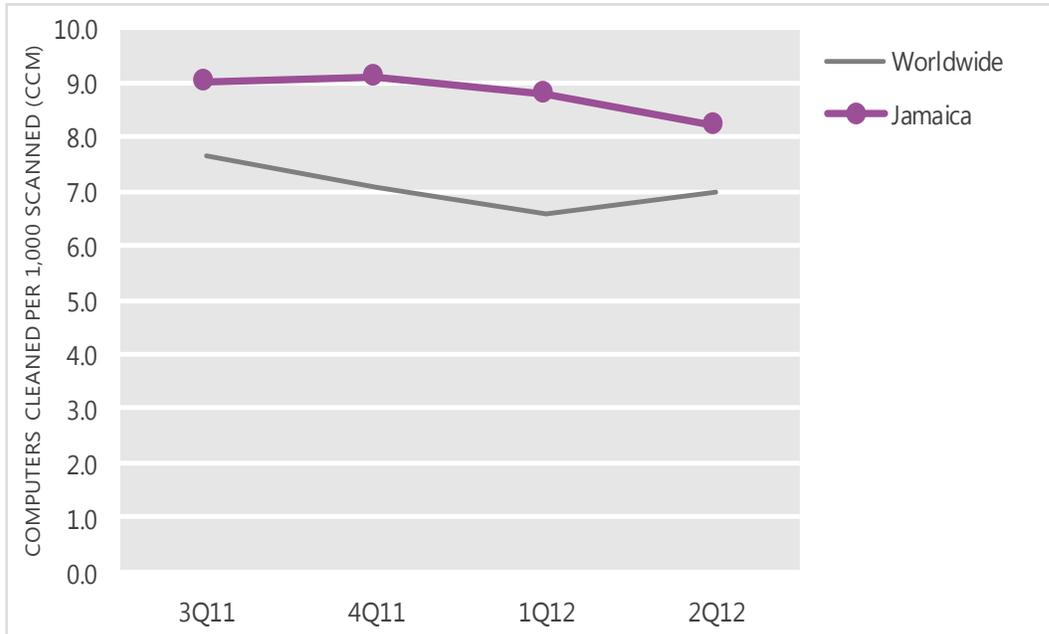
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	9.0	9.1	8.8	8.2
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

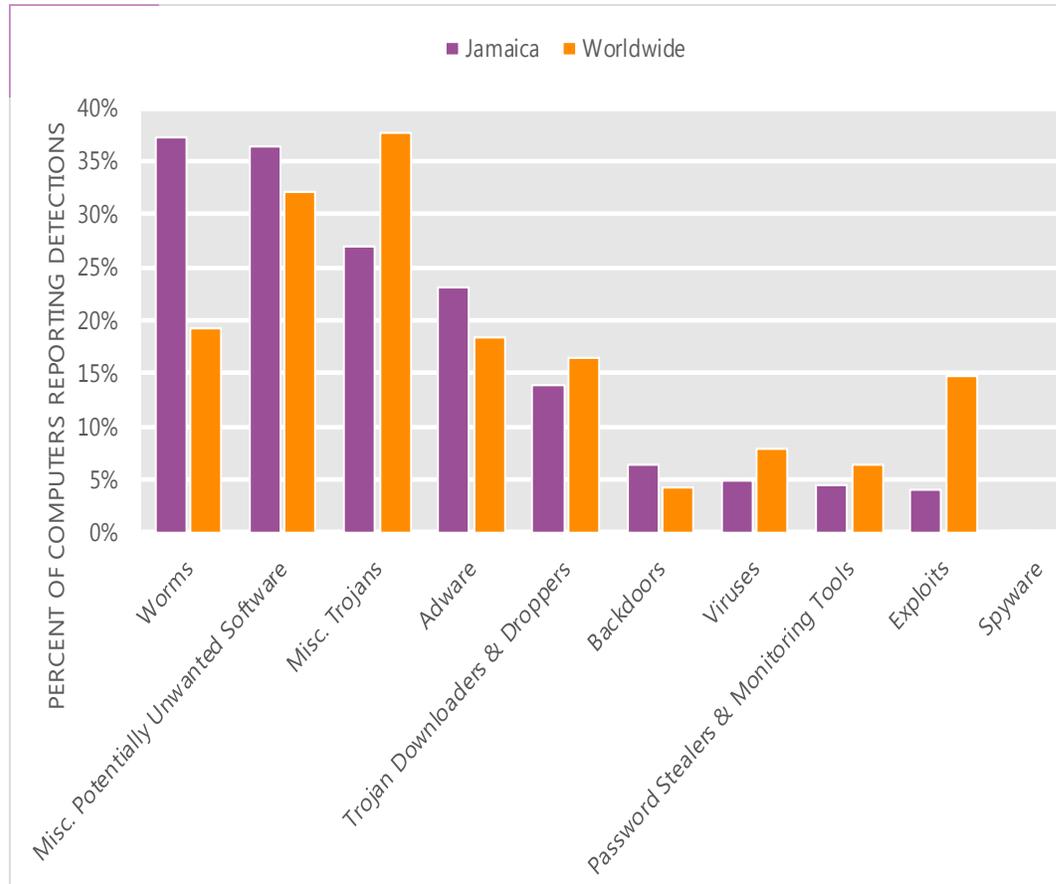
The MSRT detected malware on 8.2 of every 1,000 computers scanned in Jamaica in 2Q12 (a CCM score of 8.2, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Jamaica over the last four quarters, compared to the world as a whole.

CCM infection trends in Jamaica and worldwide



Threat categories

Malware and potentially unwanted software categories in Jamaica in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Jamaica in 2Q12 was Worms. It affected 37.2 percent of all computers with detections there, down from 39.9 percent in 1Q12.
- The second most common category in Jamaica in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 36.3 percent of all computers with detections there, up from 35.1 percent in 1Q12.
- The third most common category in Jamaica in 2Q12 was Miscellaneous Trojans, which affected 27.0 percent of all computers with detections there, up from 25.8 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Jamaica in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Vobfus	Worms	17.2%
2	Win32/Hotbar	Adware	15.0%
3	Win32/Autorun	Worms	13.8%
4	Win32/Zwangi	Misc. Potentially Unwanted Software	10.0%
5	Win32/Keygen	Misc. Potentially Unwanted Software	9.3%
6	Win32/Dorkbot	Worms	6.1%
7	Win32/Rimecud	Worms	5.8%
8	ASX/Wimad	Trojan Downloaders & Droppers	5.7%
9	Win32/Sirefef	Misc. Trojans	5.0%
10	Win32/Brontok	Worms	4.3%

- The most common threat family in Jamaica in 2Q12 was [Win32/Vobfus](#), which affected 17.2 percent of computers with detections in Jamaica. [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 second most common threat family in Jamaica in 2Q12 was [Win32/Hotbar](#), which affected 15.0 percent of computers with detections in Jamaica. [Win32/Hotbar](#) is adware that displays a dynamic toolbar and targeted pop-up ads based on its monitoring of web-browsing activity.
- The third most common threat family in Jamaica in 2Q12 was [Win32/Autorun](#), which affected 13.8 percent of computers with detections in Jamaica. [Win32/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 threat family in Jamaica in 2Q12 was [Win32/Zwangi](#), which affected 10.0 percent of computers with detections in Jamaica. [Win32/Zwangi](#) is a program that runs as a service in the background and modifies web browser settings to visit a particular website.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Jamaica

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	N/A (1.6)	N/A (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	0.53 (3.9)	1.59 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	N/A (0.7)	N/A (0.9)

Update service usage

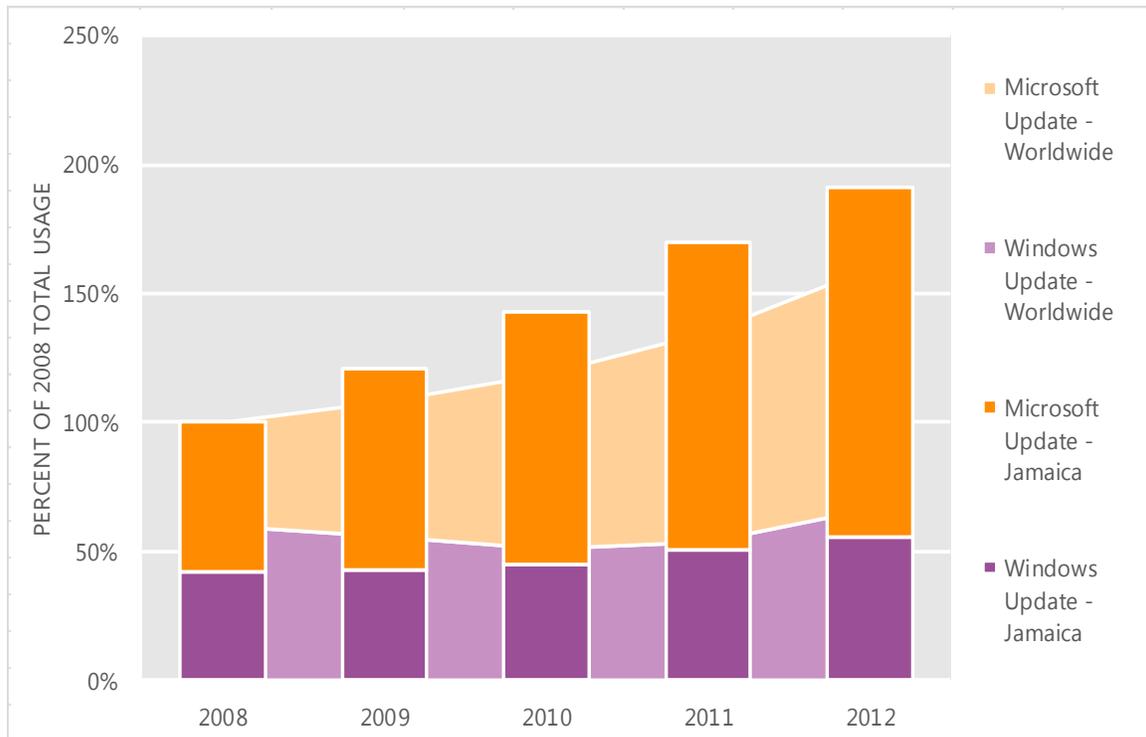
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Jamaica and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Jamaica over the last four years, indexed to the total usage for both services in Jamaica in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Jamaica was up 12.4 percent from 2011, and up 91.3 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Jamaica in 2012, 71.1 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Japan

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Japan in 2Q12 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.

Infection rate statistics for Japan

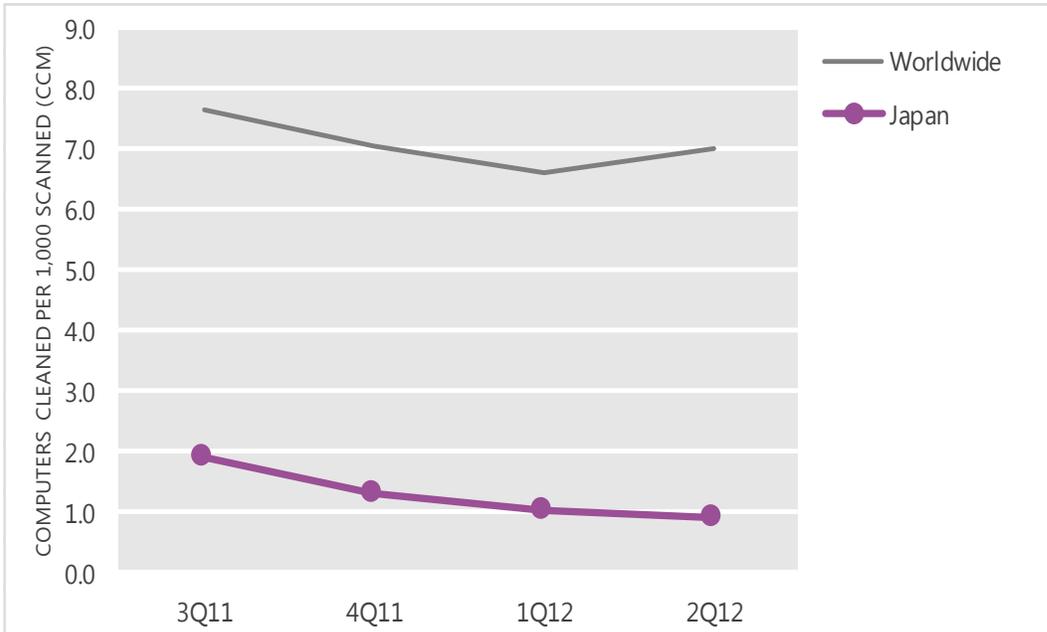
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	1.9	1.3	1.0	0.9
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

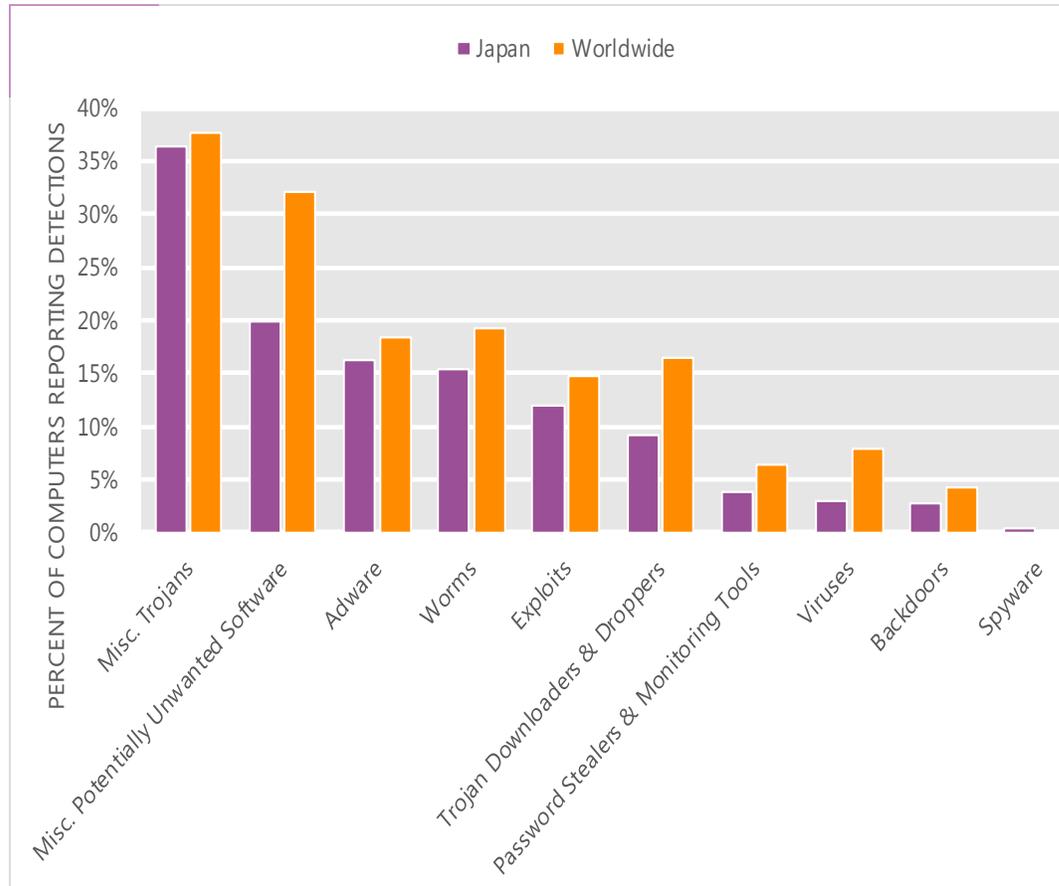
The MSRT detected malware on 0.9 of every 1,000 computers scanned in Japan in 2Q12 (a CCM score of 0.9, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Japan over the last four quarters, compared to the world as a whole.

CCM infection trends in Japan and worldwide



Threat categories

Malware and potentially unwanted software categories in Japan in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Japan in 2Q12 was Miscellaneous Trojans. It affected 36.5 percent of all computers with detections there, up from 26.5 percent in 1Q12.
- The second most common category in Japan in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 19.9 percent of all computers with detections there, down from 23.5 percent in 1Q12.
- The third most common category in Japan in 2Q12 was Adware, which affected 16.2 percent of all computers with detections there, down from 37.7 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Japan in 2Q12

	Family	Most significant category	% of computers with detections
1	JS/IframeRef	Misc. Trojans	10.5%
2	JS/Pornpop	Adware	9.5%
3	Win32/Autorun	Worms	6.2%
4	Win32/Keygen	Misc. Potentially Unwanted Software	5.9%
5	Java/Blacole	Exploits	5.5%
6	JS/Iframe	Misc. Trojans	4.9%
7	Win32/Sirefef	Misc. Trojans	3.8%
8	Win32/Conficker	Worms	3.7%
9	Win32/Taterf	Worms	3.7%
10	Win32/OpenCandy	Adware	3.6%

- The most common threat family in Japan in 2Q12 was [JS/IframeRef](#), which affected 10.5 percent of computers with detections in Japan. [JS/IframeRef](#) is a generic detection for specially formed IFrame tags that point to remote websites that contain malicious content.
- The second most common threat family in Japan in 2Q12 was [JS/Pornpop](#), which affected 9.5 percent of computers with detections in Japan. [JS/Pornpop](#) is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The third most common threat family in Japan in 2Q12 was [Win32/Autorun](#), which affected 6.2 percent of computers with detections in Japan. [Win32/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 threat family in Japan in 2Q12 was [Win32/Keygen](#), which affected 5.9 percent of computers with detections in Japan. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Japan

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	0.89 (1.6)	0.93 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	2.74 (3.9)	3.06 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.10 (0.7)	0.18 (0.9)

Update service usage

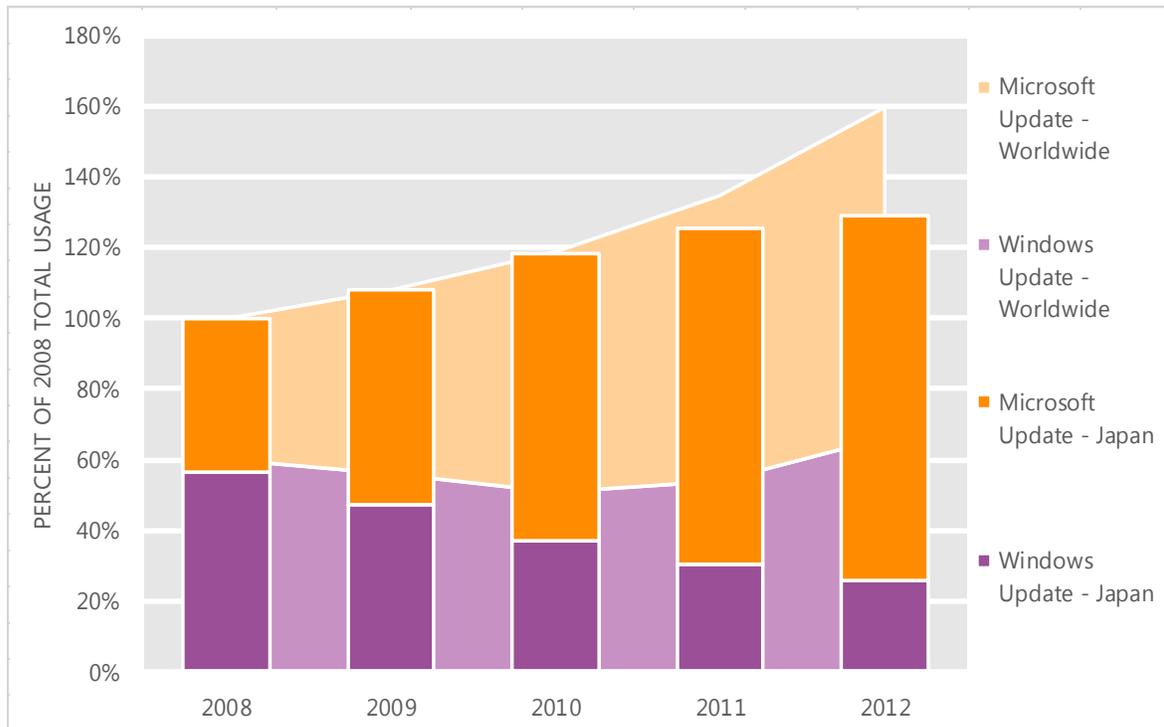
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Japan and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Japan over the last four years, indexed to the total usage for both services in Japan in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Japan was up 2.9 percent from 2011, and up 29.1 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Japan in 2012, 80.2 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Jordan

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Jordan in 2Q12 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.

Infection rate statistics for Jordan

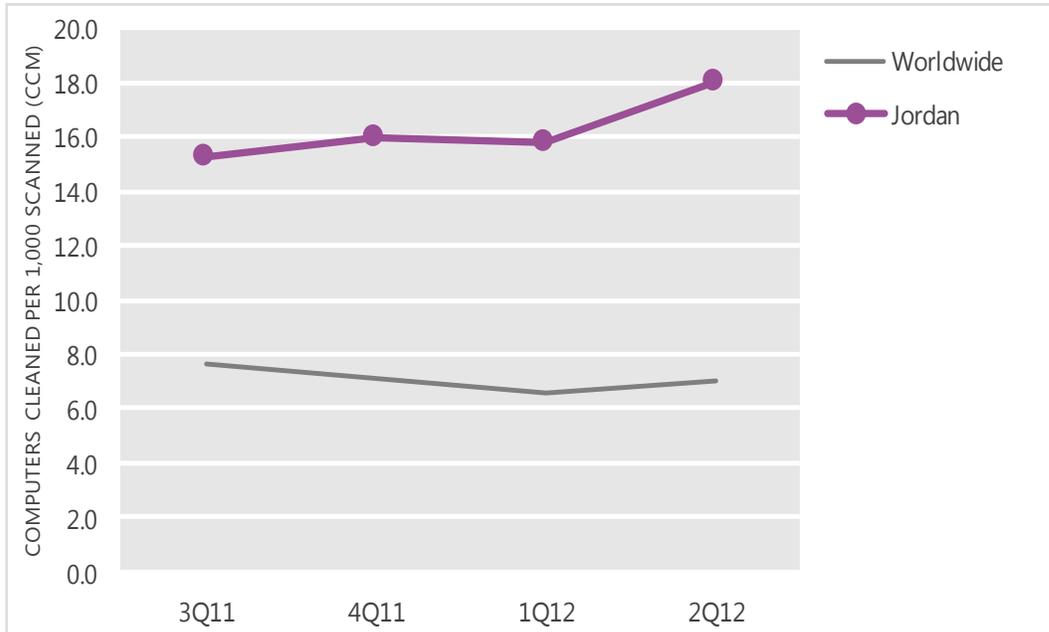
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	15.3	16.0	15.8	18.0
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

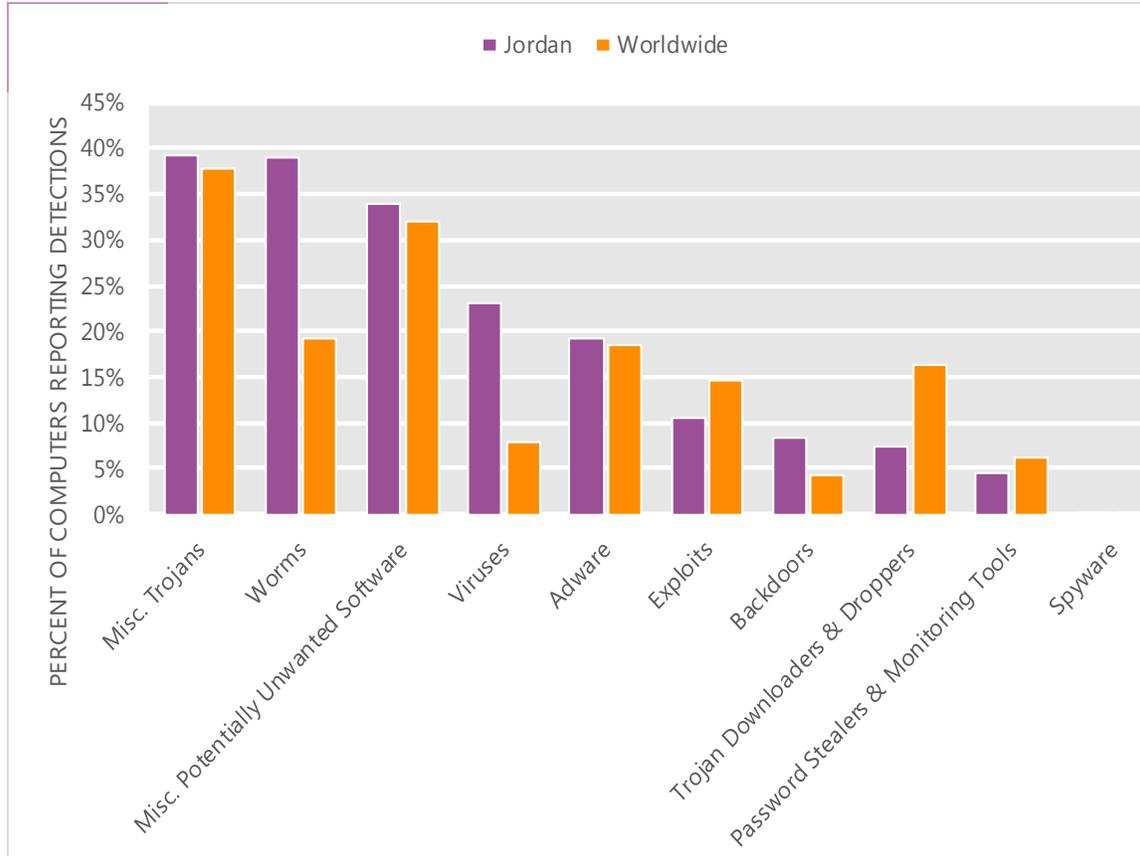
The MSRT detected malware on 18.0 of every 1,000 computers scanned in Jordan in 2Q12 (a CCM score of 18.0, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Jordan over the last four quarters, compared to the world as a whole.

CCM infection trends in Jordan and worldwide



Threat categories

Malware and potentially unwanted software categories in Jordan in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Jordan in 2Q12 was Miscellaneous Trojans. It affected 39.1 percent of all computers with detections there, down from 40.0 percent in 1Q12.
- The second most common category in Jordan in 2Q12 was Worms. It affected 39.0 percent of all computers with detections there, up from 38.2 percent in 1Q12.
- The third most common category in Jordan in 2Q12 was Miscellaneous Potentially Unwanted Software, which affected 34.0 percent of all computers with detections there, down from 35.1 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Jordan in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Autorun	Worms	20.7%
2	Win32/Sality	Viruses	16.8%
3	Win32/Keygen	Misc. Potentially Unwanted Software	13.6%
4	Win32/Vobfus	Worms	10.3%
5	JS/Paypopup	Adware	8.9%
6	Win32/Ramnit	Misc. Trojans	8.9%
7	Win32/CplLnk	Exploits	8.2%
8	Win32/Dorkbot	Worms	7.9%
9	JS/Pornpop	Adware	5.9%
10	Win32/Conficker	Worms	5.4%

- The most common threat family in Jordan in 2Q12 was [Win32/Autorun](#), which affected 20.7 percent of computers with detections in Jordan. [Win32/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 threat family in Jordan in 2Q12 was [Win32/Sality](#), which affected 16.8 percent of computers with detections in Jordan. [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 in Jordan in 2Q12 was [Win32/Keygen](#), which affected 13.6 percent of computers with detections in Jordan. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The fourth most common threat family in Jordan in 2Q12 was [Win32/Vobfus](#), which affected 10.3 percent of computers with detections in Jordan. [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.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Jordan

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	N/A (1.6)	0.38 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	1.14 (3.9)	1.52 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.43 (0.7)	0.42 (0.9)

Update service usage

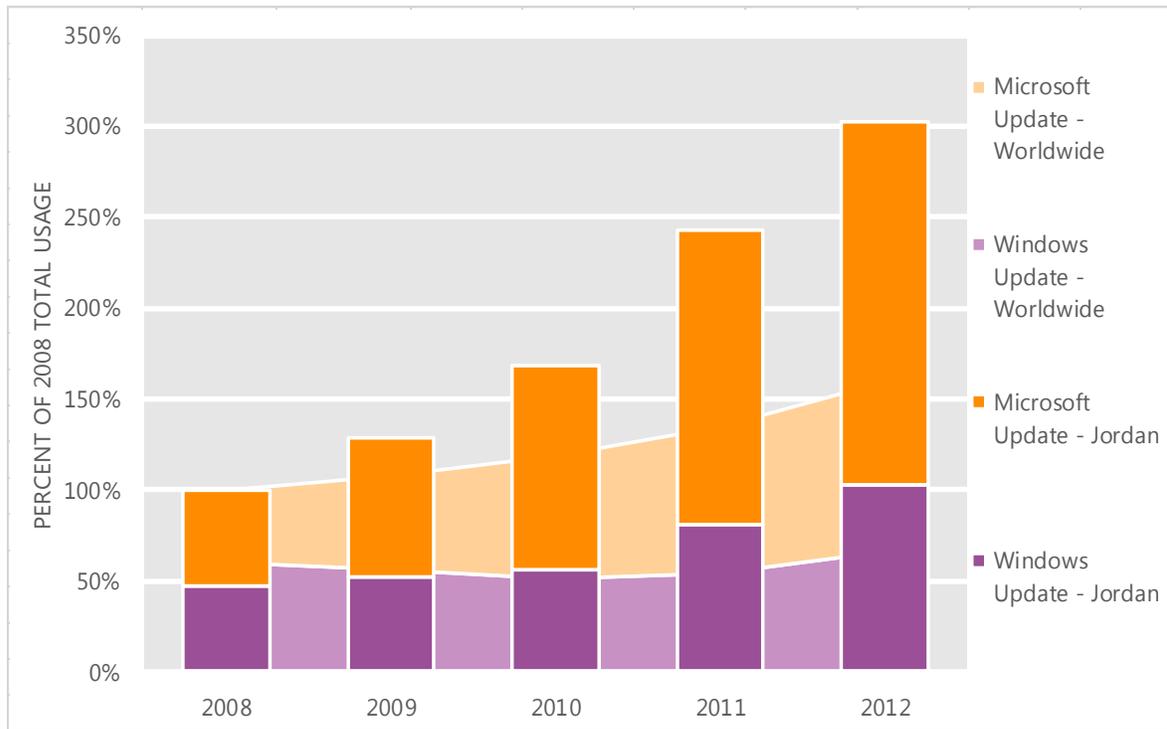
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Jordan and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Jordan over the last four years, indexed to the total usage for both services in Jordan in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Jordan was up 24.2 percent from 2011, and up 202.4 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Jordan in 2012, 65.9 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Kazakhstan

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Kazakhstan in 2Q12 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.

Infection rate statistics for Kazakhstan

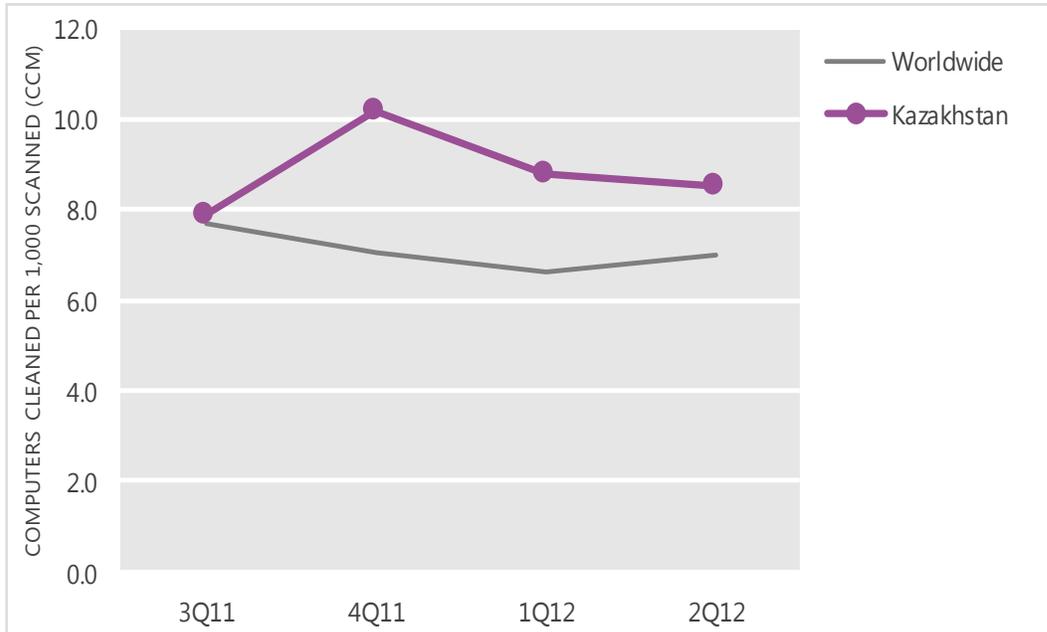
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	7.9	10.2	8.8	8.5
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

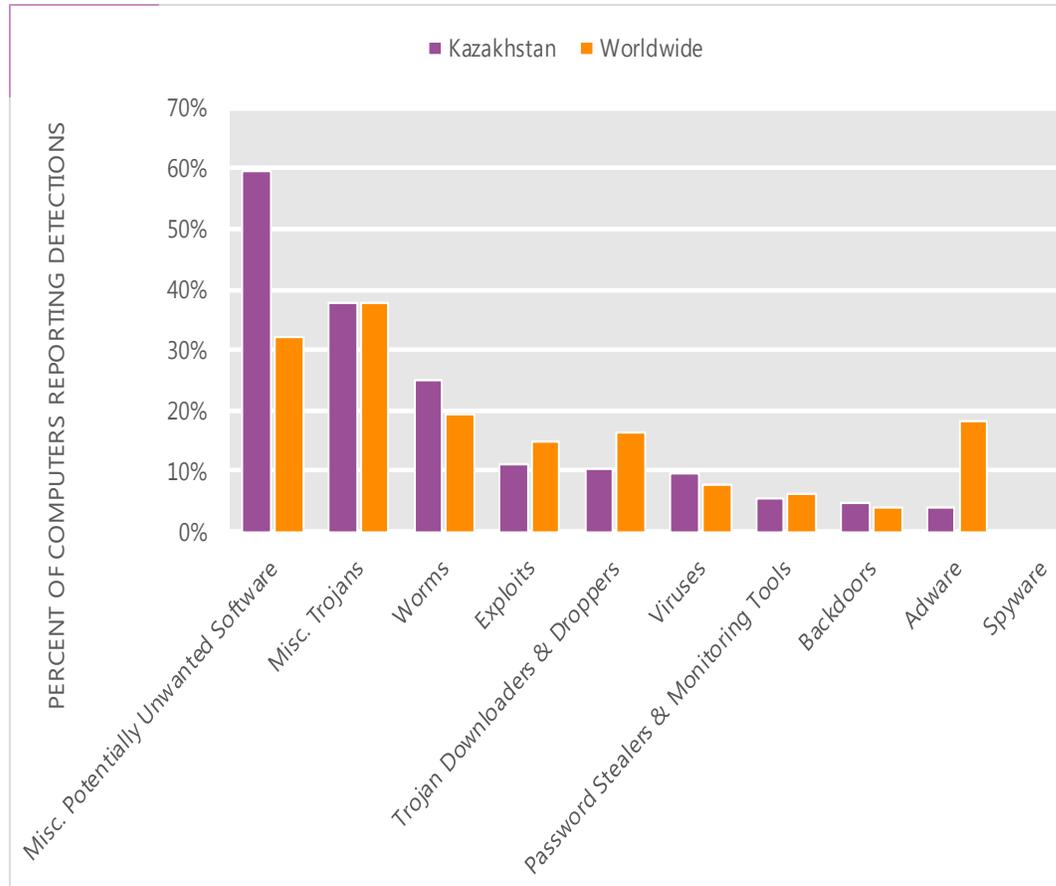
The MSRT detected malware on 8.5 of every 1,000 computers scanned in Kazakhstan in 2Q12 (a CCM score of 8.5, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Kazakhstan over the last four quarters, compared to the world as a whole.

CCM infection trends in Kazakhstan and worldwide



Threat categories

Malware and potentially unwanted software categories in Kazakhstan in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Kazakhstan in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 59.5 percent of all computers with detections there, down from 62.6 percent in 1Q12.
- The second most common category in Kazakhstan in 2Q12 was Miscellaneous Trojans. It affected 37.6 percent of all computers with detections there, up from 36.0 percent in 1Q12.
- The third most common category in Kazakhstan in 2Q12 was Worms, which affected 25.1 percent of all computers with detections there, up from 24.7 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Kazakhstan in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Pameseg	Misc. Potentially Unwanted Software	34.9%
2	Win32/Vobfus	Worms	12.4%
3	Win32/Keygen	Misc. Potentially Unwanted Software	12.3%
4	Win32/Autorun	Worms	9.8%
5	Win32/Obfuscator	Misc. Potentially Unwanted Software	7.4%
6	Win32/Vundo	Misc. Trojans	5.9%
7	Win32/CplLnk	Exploits	5.8%
8	Win32/Ramnit	Misc. Trojans	4.4%
9	Win32/Rimecud	Worms	4.1%
10	Win32/Dynamer	Misc. Trojans	4.1%

- The most common threat family in Kazakhstan in 2Q12 was [Win32/Pameseg](#), which affected 34.9 percent of computers with detections in Kazakhstan. [Win32/Pameseg](#) is a fake program installer that requires the user to send SMS messages to a premium number to successfully install certain programs.
- The second most common threat family in Kazakhstan in 2Q12 was [Win32/Vobfus](#), which affected 12.4 percent of computers with detections in Kazakhstan. [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 in Kazakhstan in 2Q12 was [Win32/Keygen](#), which affected 12.3 percent of computers with detections in Kazakhstan. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The fourth most common threat family in Kazakhstan in 2Q12 was [Win32/Autorun](#), which affected 9.8 percent of computers with detections in Kazakhstan. [Win32/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.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Kazakhstan

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	6.71 (1.6)	8.44 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	5.63 (3.9)	7.58 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	1.00 (0.7)	2.56 (0.9)

Update service usage

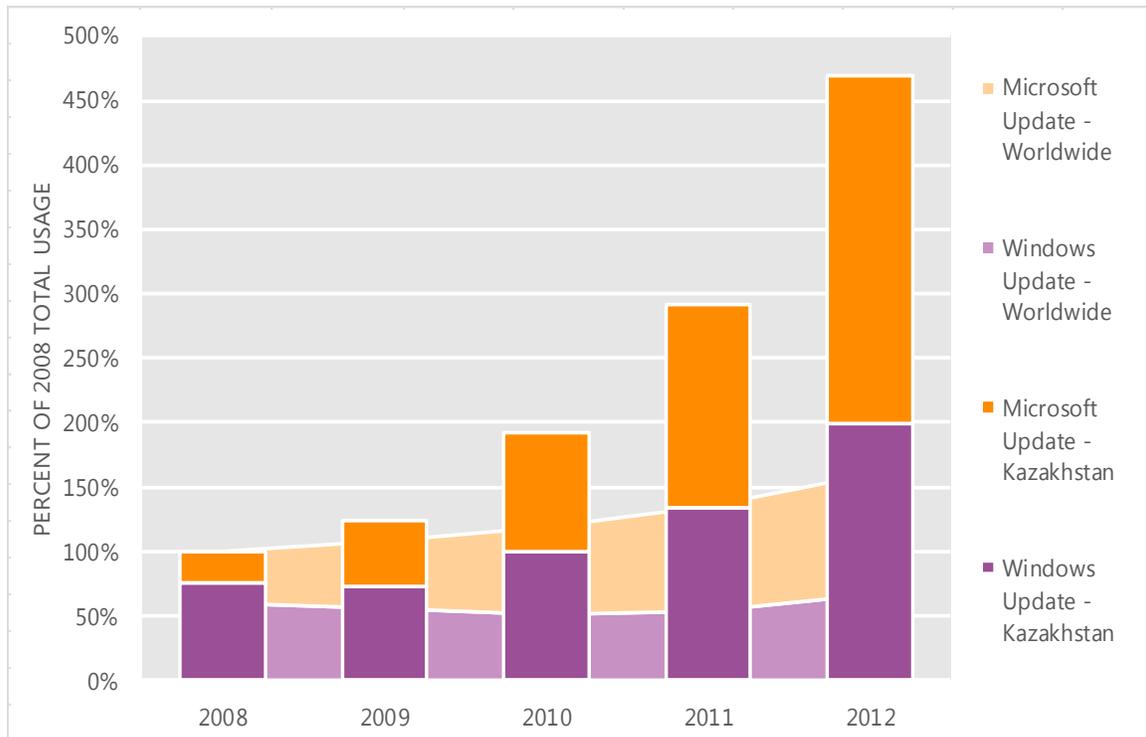
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Kazakhstan and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Kazakhstan over the last four years, indexed to the total usage for both services in Kazakhstan in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Kazakhstan was up 60.6 percent from 2011, and up 369.3 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Kazakhstan in 2012, 57.6 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Kenya

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Kenya in 2Q12 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.

Infection rate statistics for Kenya

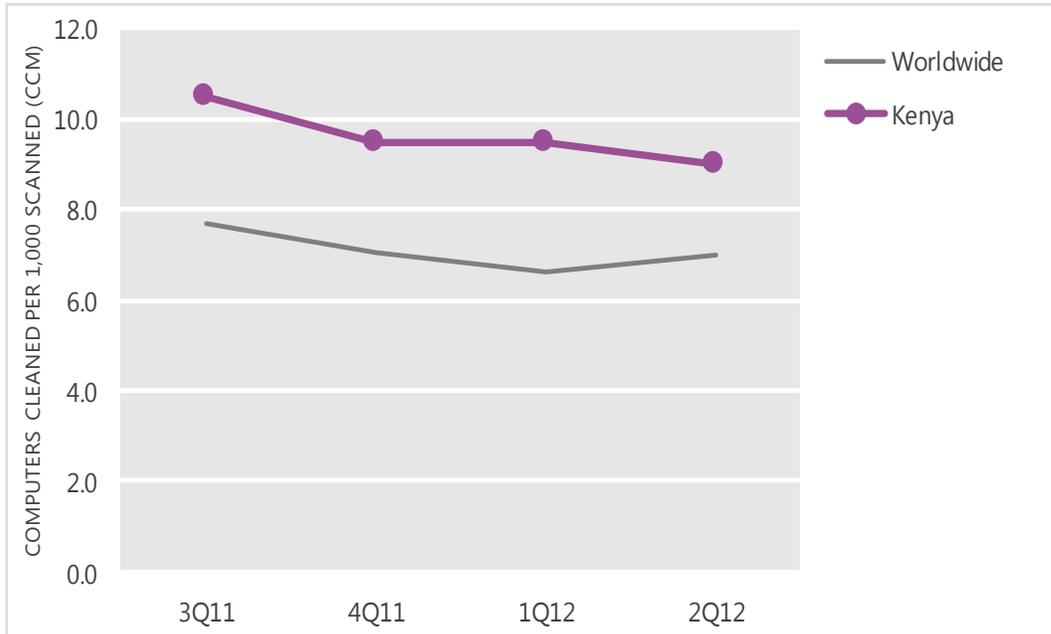
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	10.5	9.5	9.5	9.0
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

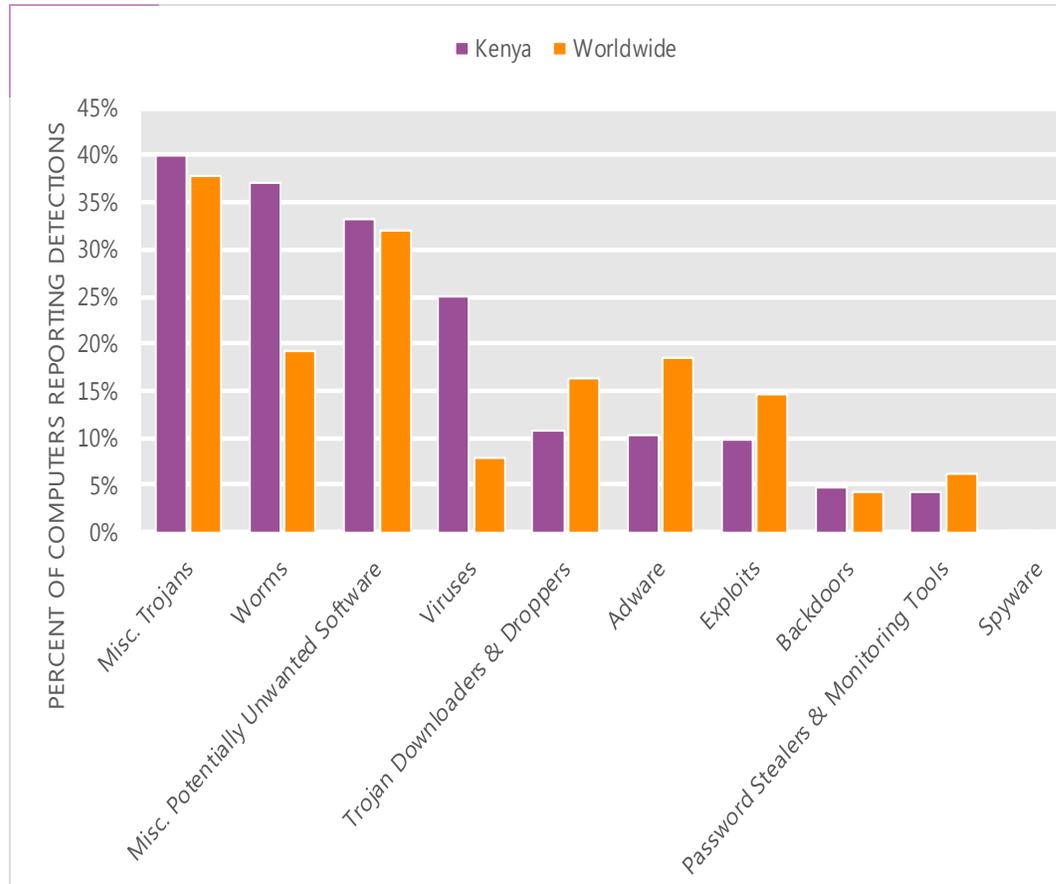
The MSRT detected malware on 9.0 of every 1,000 computers scanned in Kenya in 2Q12 (a CCM score of 9.0, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Kenya over the last four quarters, compared to the world as a whole.

CCM infection trends in Kenya and worldwide



Threat categories

Malware and potentially unwanted software categories in Kenya in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Kenya in 2Q12 was Miscellaneous Trojans. It affected 40.0 percent of all computers with detections there, up from 36.9 percent in 1Q12.
- The second most common category in Kenya in 2Q12 was Worms. It affected 37.0 percent of all computers with detections there, down from 37.8 percent in 1Q12.
- The third most common category in Kenya in 2Q12 was Miscellaneous Potentially Unwanted Software, which affected 33.1 percent of all computers with detections there, up from 32.0 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Kenya in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Autorun	Worms	20.2%
2	Win32/Sality	Viruses	18.9%
3	Win32/Vobfus	Worms	11.3%
4	Win32/Comame	Misc. Trojans	10.1%
5	Win32/Keygen	Misc. Potentially Unwanted Software	9.4%
6	Win32/Rimecud	Worms	7.6%
7	Win32/Dorkbot	Worms	7.2%
8	Win32/CplLnk	Exploits	6.8%
9	Win32/Virut	Viruses	6.4%
10	Win32/Ramnit	Misc. Trojans	6.3%

- The most common threat family in Kenya in 2Q12 was [Win32/Autorun](#), which affected 20.2 percent of computers with detections in Kenya. [Win32/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 threat family in Kenya in 2Q12 was [Win32/Sality](#), which affected 18.9 percent of computers with detections in Kenya. [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 in Kenya in 2Q12 was [Win32/Vobfus](#), which affected 11.3 percent of computers with detections in Kenya. [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 in Kenya in 2Q12 was [Win32/Comame](#), which affected 10.1 percent of computers with detections in Kenya. [Win32/Comame](#) is a generic detection for a variety of threats.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Kenya

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	3.87 (1.6)	1.66 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	1.11 (3.9)	3.87 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.09 (0.7)	1.19 (0.9)

Update service usage

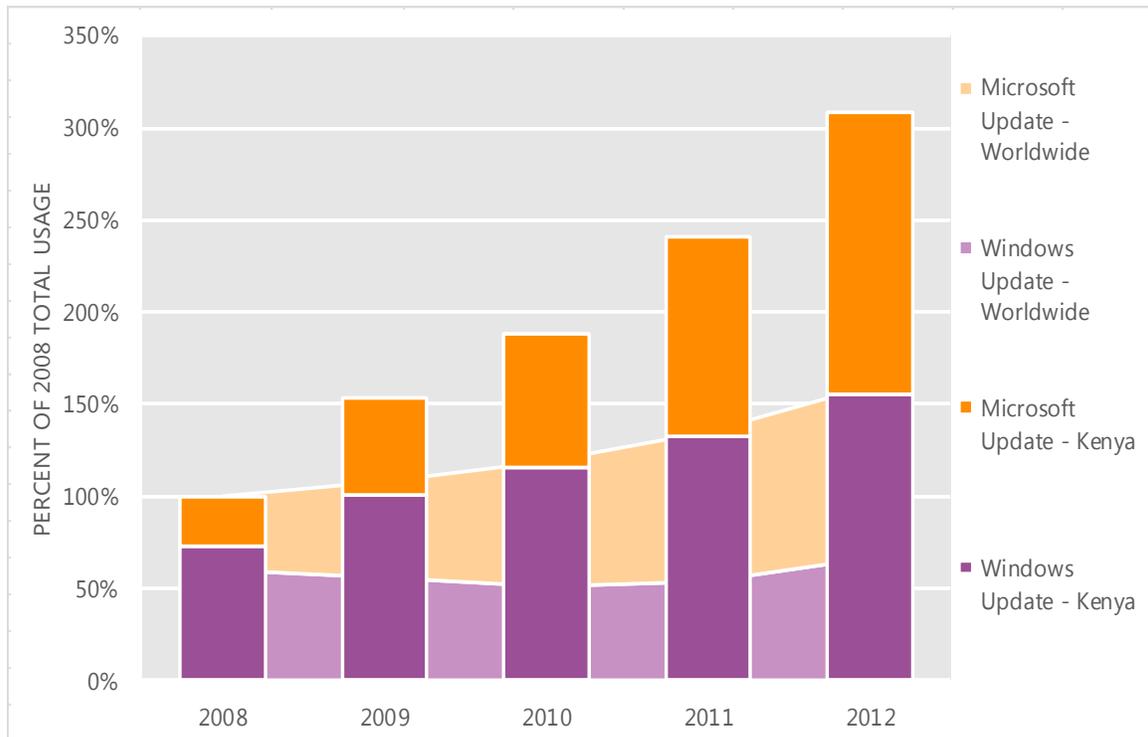
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Kenya and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Kenya over the last four years, indexed to the total usage for both services in Kenya in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Kenya was up 28.5 percent from 2011, and up 209.0 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Kenya in 2012, 49.7 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Korea

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Korea in 2Q12 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.

Infection rate statistics for Korea

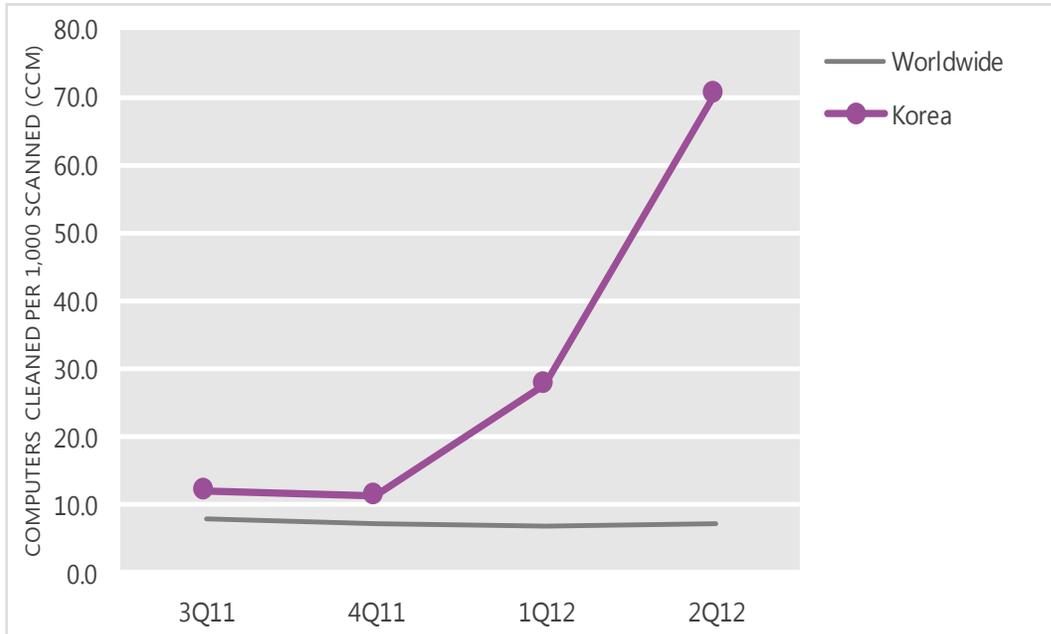
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	12.0	11.1	27.5	70.4
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

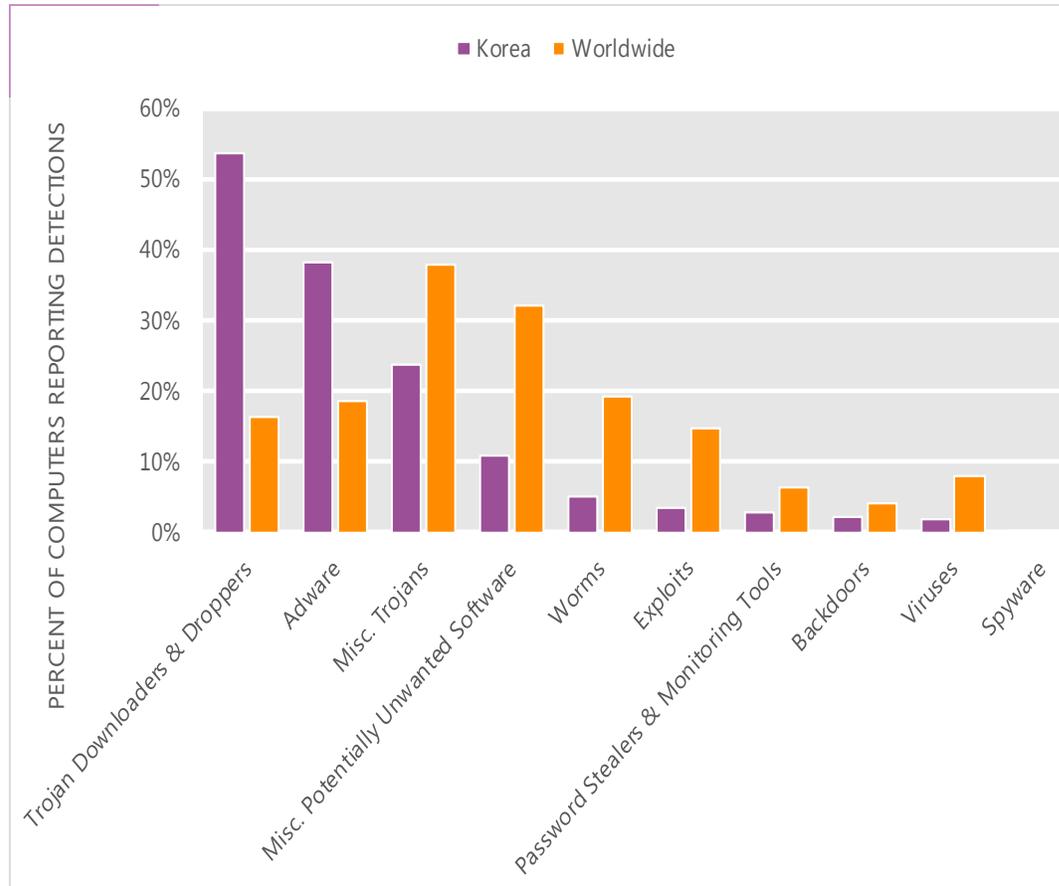
The MSRT detected malware on 70.4 of every 1,000 computers scanned in Korea in 2Q12 (a CCM score of 70.4, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Korea over the last four quarters, compared to the world as a whole.

CCM infection trends in Korea and worldwide



Threat categories

Malware and potentially unwanted software categories in Korea in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Korea in 2Q12 was Trojan Downloaders & Droppers. It affected 53.8 percent of all computers with detections there, up from 23.5 percent in 1Q12.
- The second most common category in Korea in 2Q12 was Adware. It affected 38.0 percent of all computers with detections there, down from 53.6 percent in 1Q12.
- The third most common category in Korea in 2Q12 was Miscellaneous Trojans, which affected 23.6 percent of all computers with detections there, down from 25.2 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Korea in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Pluzoks	Trojan Downloaders & Droppers	46.5%
2	Win32/Onescan	Misc. Trojans	17.6%
3	Win32/Wizpop	Adware	11.4%
4	Win32/FineTop	Adware	7.5%
5	Win32/Funpop	Adware	6.2%
6	Win32/EasyOn	Adware	5.9%
7	Win32/WTool	Adware	5.8%
8	Win32/Addendum	Adware	5.4%
9	Win32/TopGuide	Misc. Potentially Unwanted Software	5.1%
10	Win32/SideTab	Adware	5.0%

- The most common threat family in Korea in 2Q12 was [Win32/Pluzoks](#), which affected 46.5 percent of computers with detections in Korea. [Win32/Pluzoks](#) is a trojan that silently downloads and installs other programs without consent. This could include the installation of additional malware or malware components.
- The second most common threat family in Korea in 2Q12 was [Win32/Onescan](#), which affected 17.6 percent of computers with detections in Korea. [Win32/Onescan](#) is a Korean-language rogue security software family distributed under the names One Scan, Siren114, EnPrivacy, PC Trouble, My Vaccine, and many others.
- The third most common threat family in Korea in 2Q12 was [Win32/Wizpop](#), which affected 11.4 percent of computers with detections in Korea. [Win32/Wizpop](#) is adware that may track user search habits and download executable programs without user consent.
- The fourth most common threat family in Korea in 2Q12 was [Win32/FineTop](#), which affected 7.5 percent of computers with detections in Korea. [Win32/FineTop](#) is adware that may display pop-up advertisements when certain keywords are present in viewed web pages.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Korea

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	0.62 (1.6)	0.79 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	3.17 (3.9)	3.20 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	4.73 (0.7)	3.06 (0.9)

Update service usage

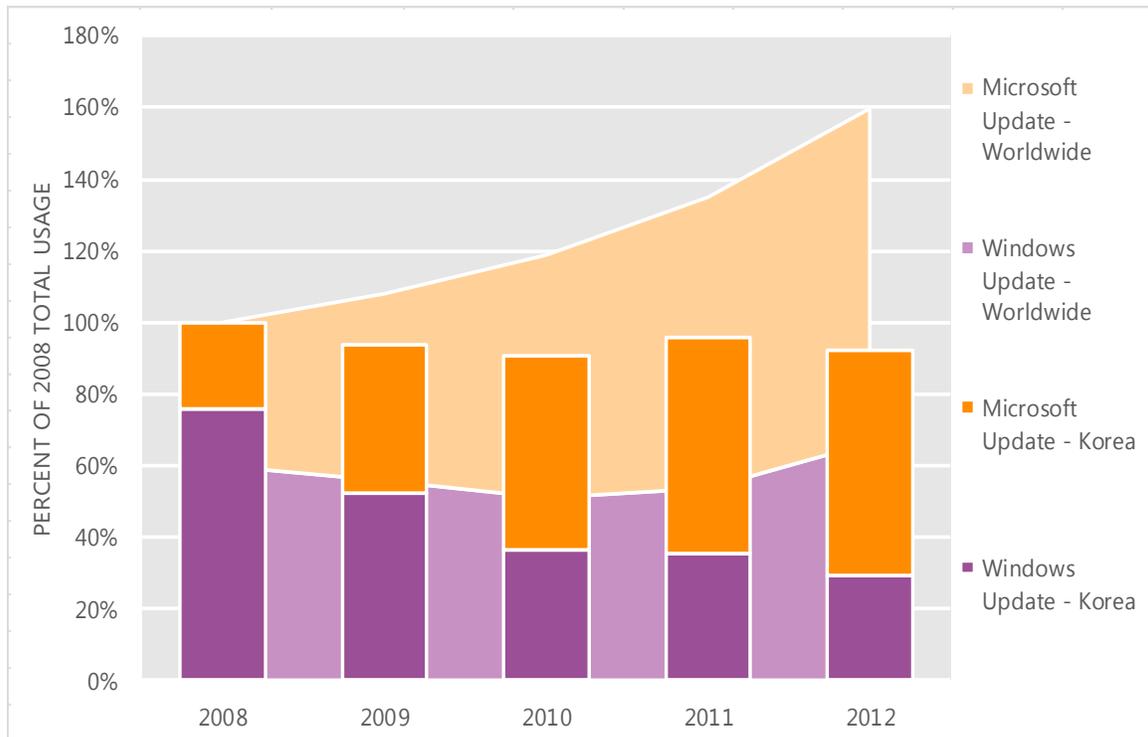
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Korea and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Korea over the last four years, indexed to the total usage for both services in Korea in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Korea was down 3.9 percent from 2011, and down 8.0 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Korea in 2012, 68.3 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Kuwait

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Kuwait in 2Q12 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.

Infection rate statistics for Kuwait

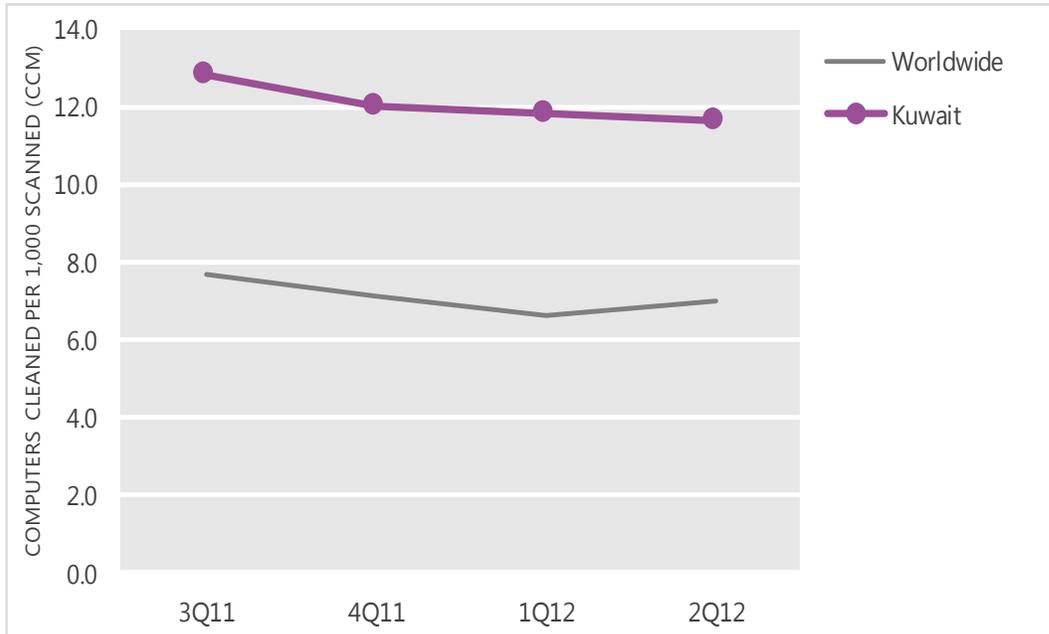
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	12.8	12.0	11.8	11.6
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

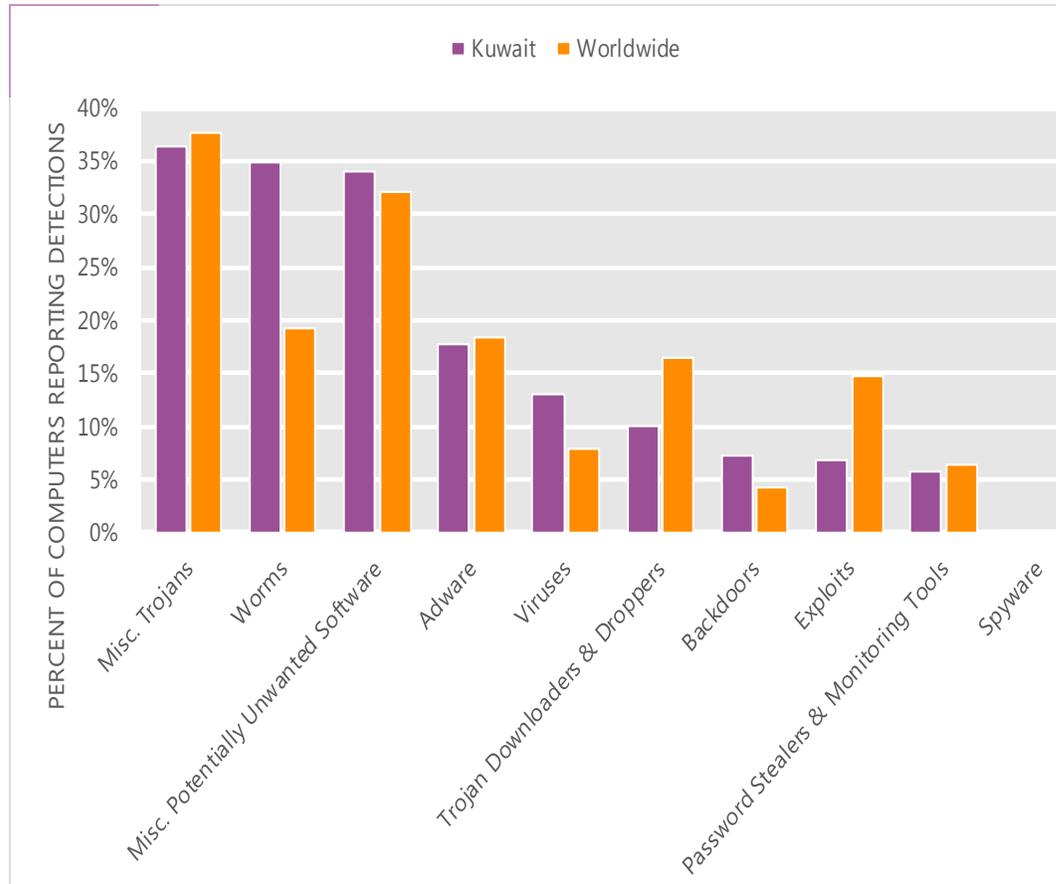
The MSRT detected malware on 11.6 of every 1,000 computers scanned in Kuwait in 2Q12 (a CCM score of 11.6, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Kuwait over the last four quarters, compared to the world as a whole.

CCM infection trends in Kuwait and worldwide



Threat categories

Malware and potentially unwanted software categories in Kuwait in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Kuwait in 2Q12 was Miscellaneous Trojans. It affected 36.5 percent of all computers with detections there, down from 37.0 percent in 1Q12.
- The second most common category in Kuwait in 2Q12 was Worms. It affected 34.9 percent of all computers with detections there, up from 34.0 percent in 1Q12.
- The third most common category in Kuwait in 2Q12 was Miscellaneous Potentially Unwanted Software, which affected 34.0 percent of all computers with detections there, up from 33.1 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Kuwait in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Autorun	Worms	14.5%
2	Win32/Keygen	Misc. Potentially Unwanted Software	13.1%
3	Win32/Sality	Viruses	10.1%
4	Win32/Dorkbot	Worms	7.3%
5	Win32/Rimecud	Worms	7.3%
6	JS/Paypopup	Adware	7.1%
7	Win32/Vobfus	Worms	6.7%
8	Win32/Hotbar	Adware	5.6%
9	Win32/Zwangi	Misc. Potentially Unwanted Software	4.0%
10	Win32/Giframe	Misc. Trojans	3.6%

- The most common threat family in Kuwait in 2Q12 was [Win32/Autorun](#), which affected 14.5 percent of computers with detections in Kuwait. [Win32/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 threat family in Kuwait in 2Q12 was [Win32/Keygen](#), which affected 13.1 percent of computers with detections in Kuwait. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The third most common threat family in Kuwait in 2Q12 was [Win32/Sality](#), which affected 10.1 percent of computers with detections in Kuwait. [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 in Kuwait in 2Q12 was [Win32/Dorkbot](#), which affected 7.3 percent of computers with detections in Kuwait. [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.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Kuwait

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	0.27 (1.6)	0.09 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	0.36 (3.9)	0.72 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.11 (0.7)	0.05 (0.9)

Update service usage

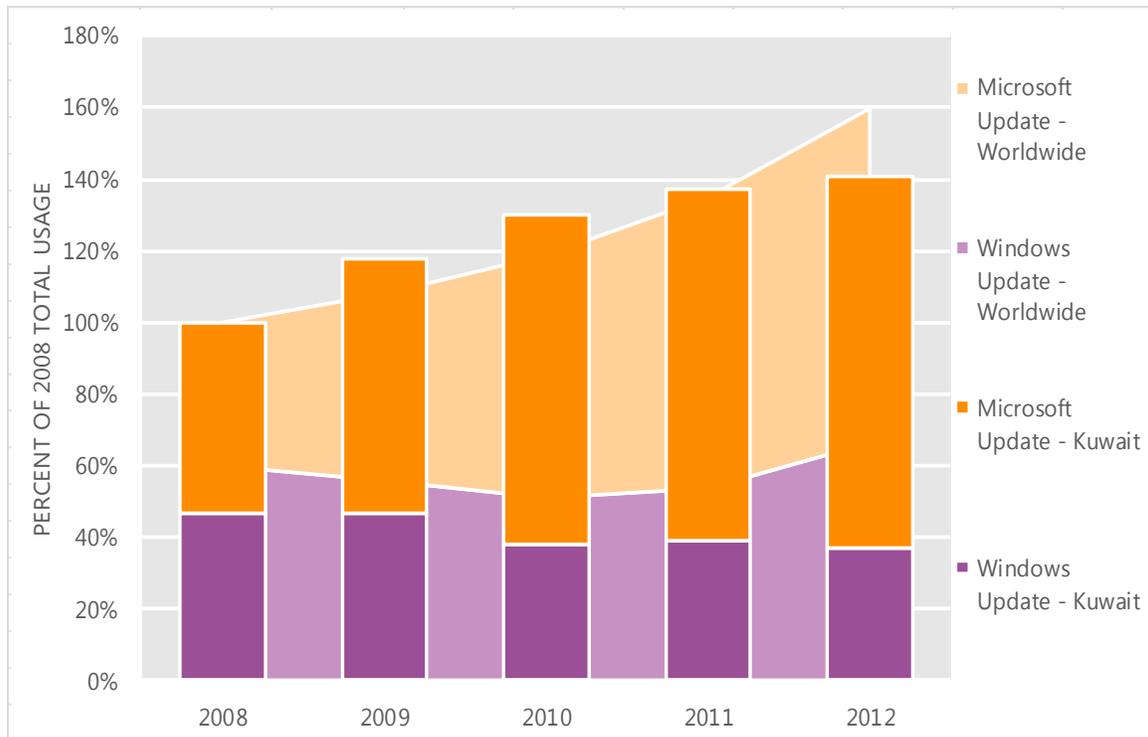
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Kuwait and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Kuwait over the last four years, indexed to the total usage for both services in Kuwait in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Kuwait was up 2.5 percent from 2011, and up 40.7 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Kuwait in 2012, 73.8 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Latvia

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Latvia in 2Q12 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.

Infection rate statistics for Latvia

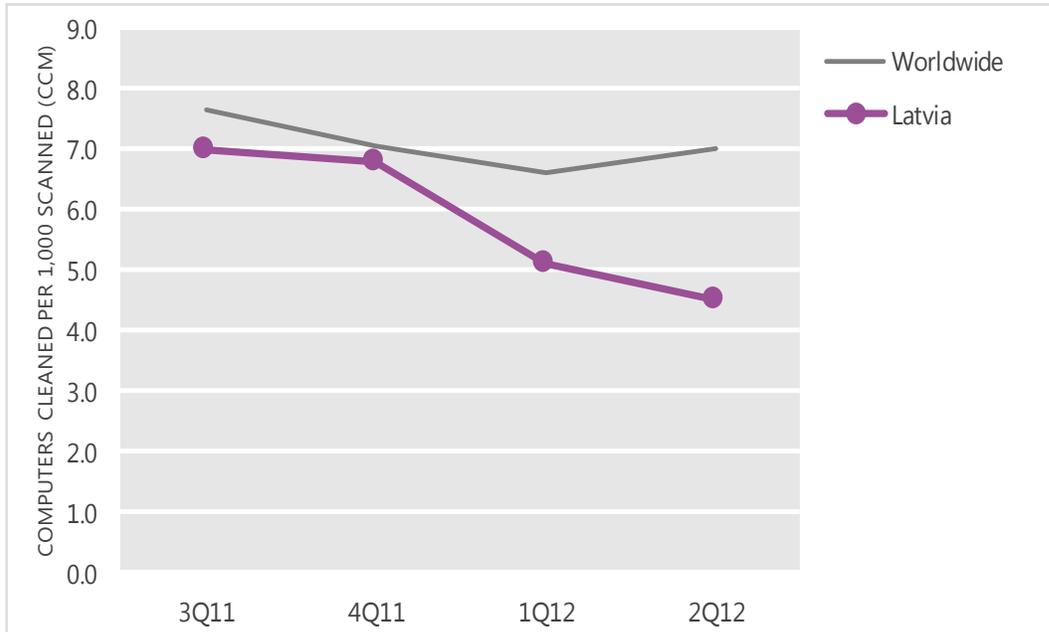
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	7.0	6.8	5.1	4.5
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

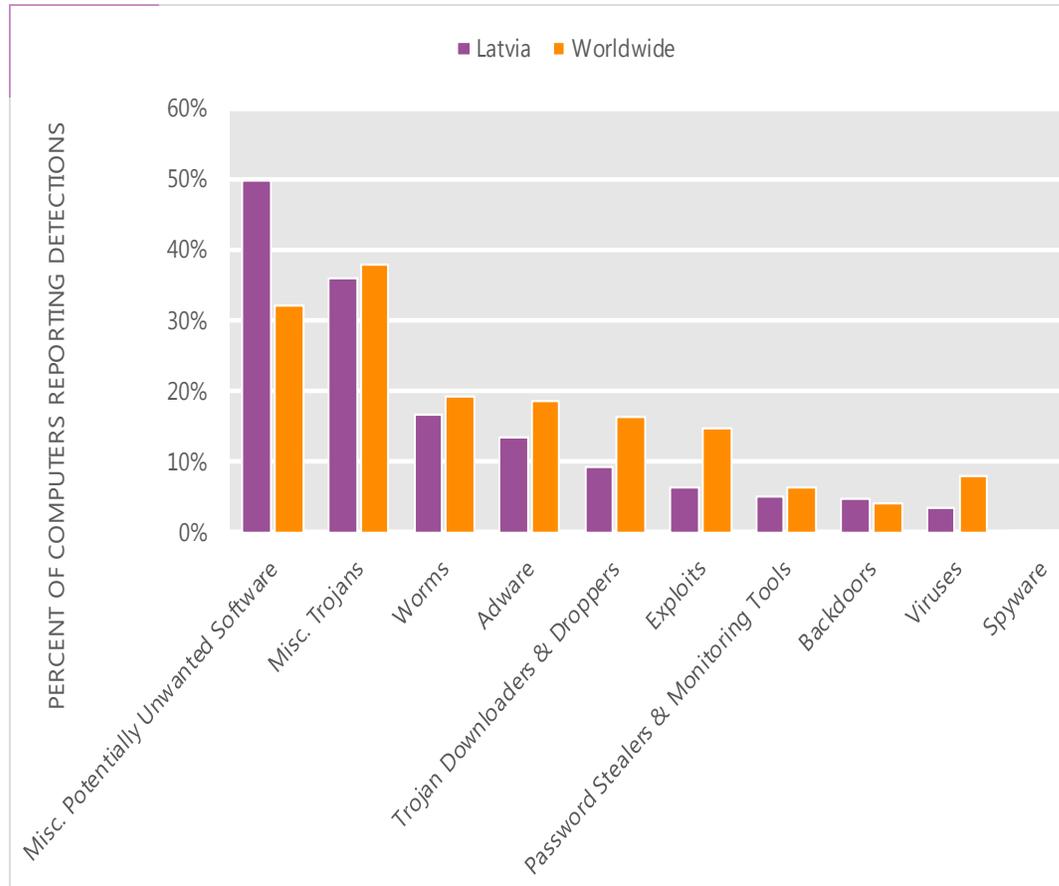
The MSRT detected malware on 4.5 of every 1,000 computers scanned in Latvia in 2Q12 (a CCM score of 4.5, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Latvia over the last four quarters, compared to the world as a whole.

CCM infection trends in Latvia and worldwide



Threat categories

Malware and potentially unwanted software categories in Latvia in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Latvia in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 49.7 percent of all computers with detections there, down from 52.6 percent in 1Q12.
- The second most common category in Latvia in 2Q12 was Miscellaneous Trojans. It affected 35.8 percent of all computers with detections there, up from 32.4 percent in 1Q12.
- The third most common category in Latvia in 2Q12 was Worms, which affected 16.7 percent of all computers with detections there, down from 17.6 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Latvia in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Keygen	Misc. Potentially Unwanted Software	17.3%
2	Win32/Pameseg	Misc. Potentially Unwanted Software	12.2%
3	Win32/Autorun	Worms	6.6%
4	Win32/Obfuscator	Misc. Potentially Unwanted Software	6.5%
5	JS/IframeRef	Misc. Trojans	6.2%
6	JS/Pornpop	Adware	5.4%
7	Win32/Hotbar	Adware	4.8%
8	Win32/Conficker	Worms	4.5%
9	Win32/Zwangi	Misc. Potentially Unwanted Software	4.2%
10	Win32/Dynamer	Misc. Trojans	4.0%

- The most common threat family in Latvia in 2Q12 was [Win32/Keygen](#), which affected 17.3 percent of computers with detections in Latvia. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The second most common threat family in Latvia in 2Q12 was [Win32/Pameseg](#), which affected 12.2 percent of computers with detections in Latvia. [Win32/Pameseg](#) is a fake program installer that requires the user to send SMS messages to a premium number to successfully install certain programs.
- The third most common threat family in Latvia in 2Q12 was [Win32/Autorun](#), which affected 6.6 percent of computers with detections in Latvia. [Win32/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 threat family in Latvia in 2Q12 was [Win32/Obfuscator](#), which affected 6.5 percent of computers with detections in Latvia. [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.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Latvia

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	1.08 (1.6)	1.26 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	7.17 (3.9)	7.17 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	2.16 (0.7)	2.88 (0.9)

Update service usage

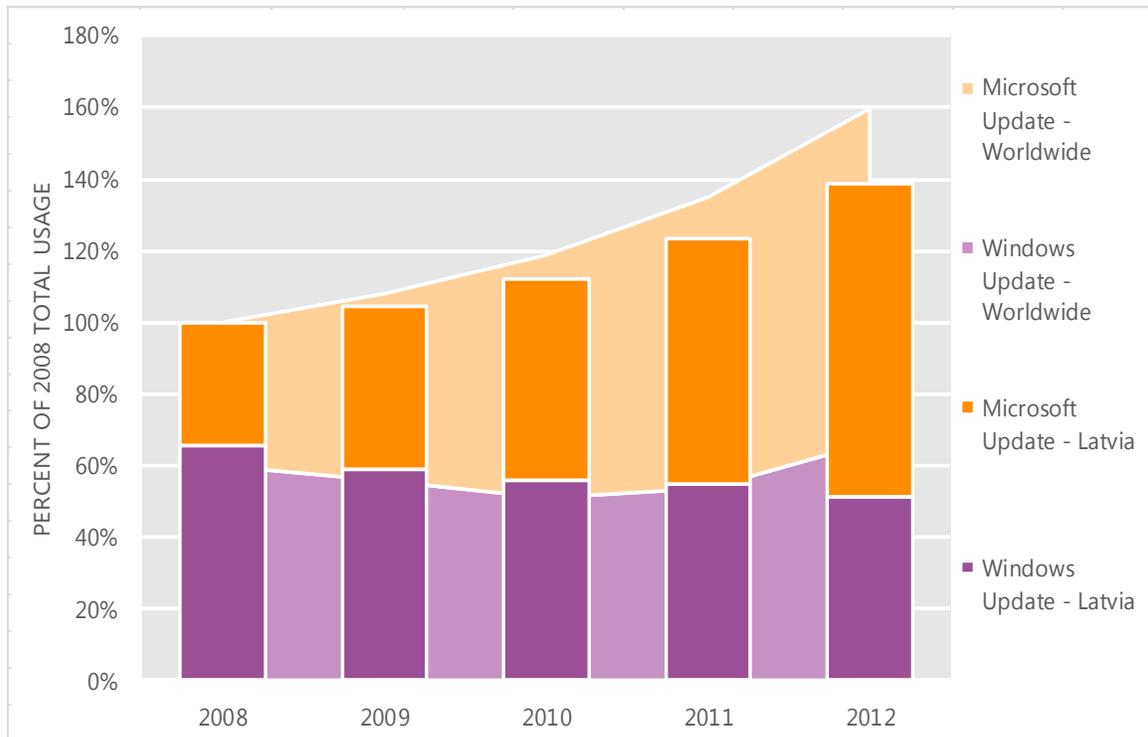
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Latvia and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Latvia over the last four years, indexed to the total usage for both services in Latvia in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Latvia was up 12.3 percent from 2011, and up 38.8 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Latvia in 2012, 62.9 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Lebanon

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Lebanon in 2Q12 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.

Infection rate statistics for Lebanon

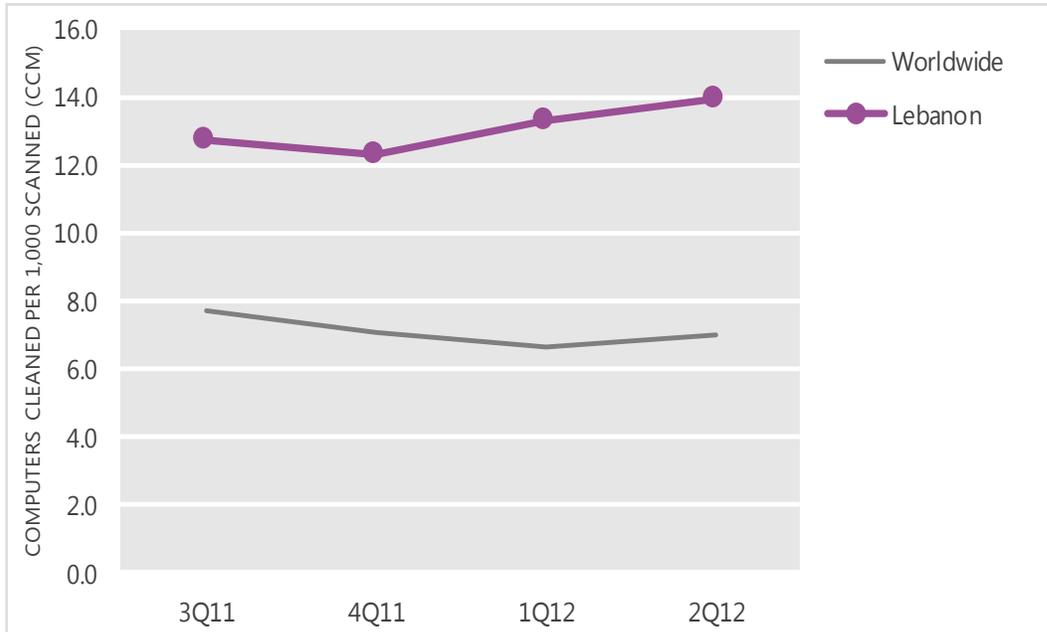
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	12.7	12.3	13.3	13.9
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

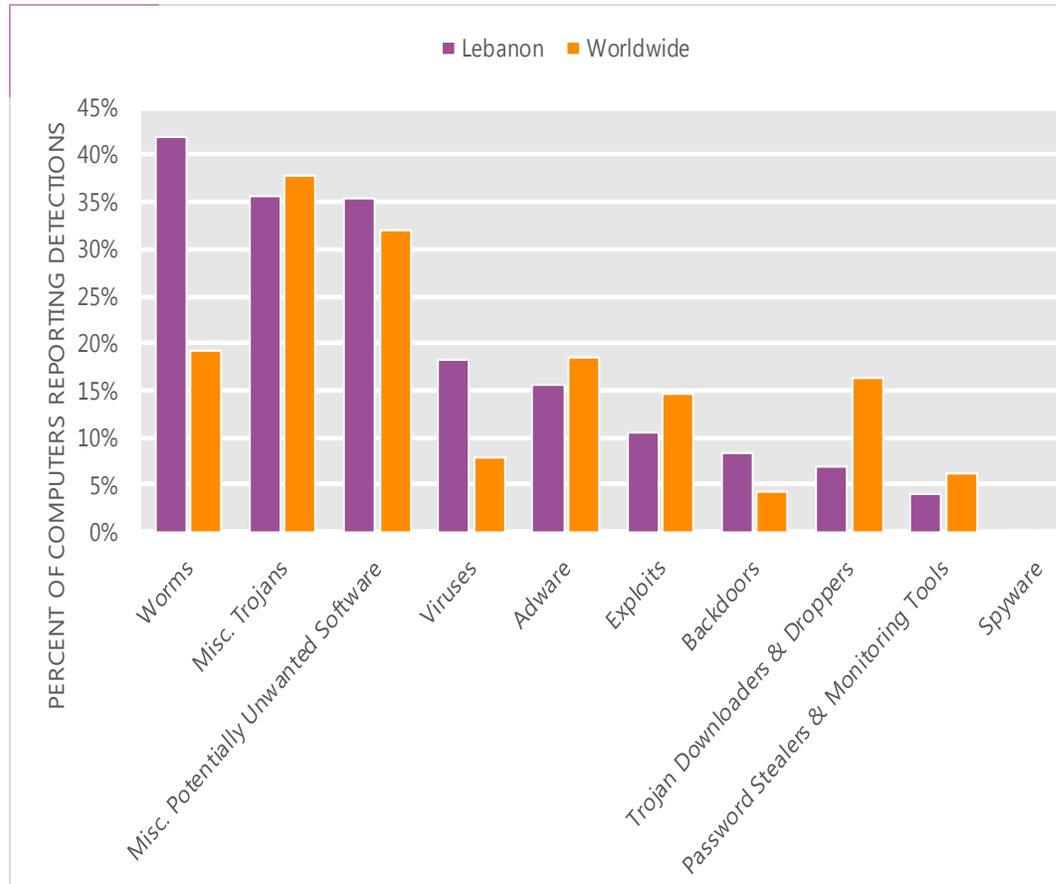
The MSRT detected malware on 13.9 of every 1,000 computers scanned in Lebanon in 2Q12 (a CCM score of 13.9, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Lebanon over the last four quarters, compared to the world as a whole.

CCM infection trends in Lebanon and worldwide



Threat categories

Malware and potentially unwanted software categories in Lebanon in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Lebanon in 2Q12 was Worms. It affected 41.9 percent of all computers with detections there, up from 40.4 percent in 1Q12.
- The second most common category in Lebanon in 2Q12 was Miscellaneous Trojans. It affected 35.5 percent of all computers with detections there, down from 35.8 percent in 1Q12.
- The third most common category in Lebanon in 2Q12 was Miscellaneous Potentially Unwanted Software, which affected 35.5 percent of all computers with detections there, down from 37.4 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Lebanon in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Autorun	Worms	20.6%
2	Win32/Sality	Viruses	13.6%
3	Win32/Keygen	Misc. Potentially Unwanted Software	13.2%
4	Win32/Dorkbot	Worms	10.6%
5	Win32/Ramnit	Misc. Trojans	8.9%
6	Win32/CplLnk	Exploits	7.8%
7	Win32/Rimecud	Worms	7.7%
8	JS/Pornpop	Adware	6.2%
9	Win32/Vobfus	Worms	6.1%
10	Win32/Nuqel	Worms	6.0%

- The most common threat family in Lebanon in 2Q12 was [Win32/Autorun](#), which affected 20.6 percent of computers with detections in Lebanon. [Win32/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 threat family in Lebanon in 2Q12 was [Win32/Sality](#), which affected 13.6 percent of computers with detections in Lebanon. [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 in Lebanon in 2Q12 was [Win32/Keygen](#), which affected 13.2 percent of computers with detections in Lebanon. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The fourth most common threat family in Lebanon in 2Q12 was [Win32/Dorkbot](#), which affected 10.6 percent of computers with detections in Lebanon. [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.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Lebanon

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	1.00 (1.6)	1.00 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	1.33 (3.9)	1.33 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.01 (0.7)	0.01 (0.9)

Update service usage

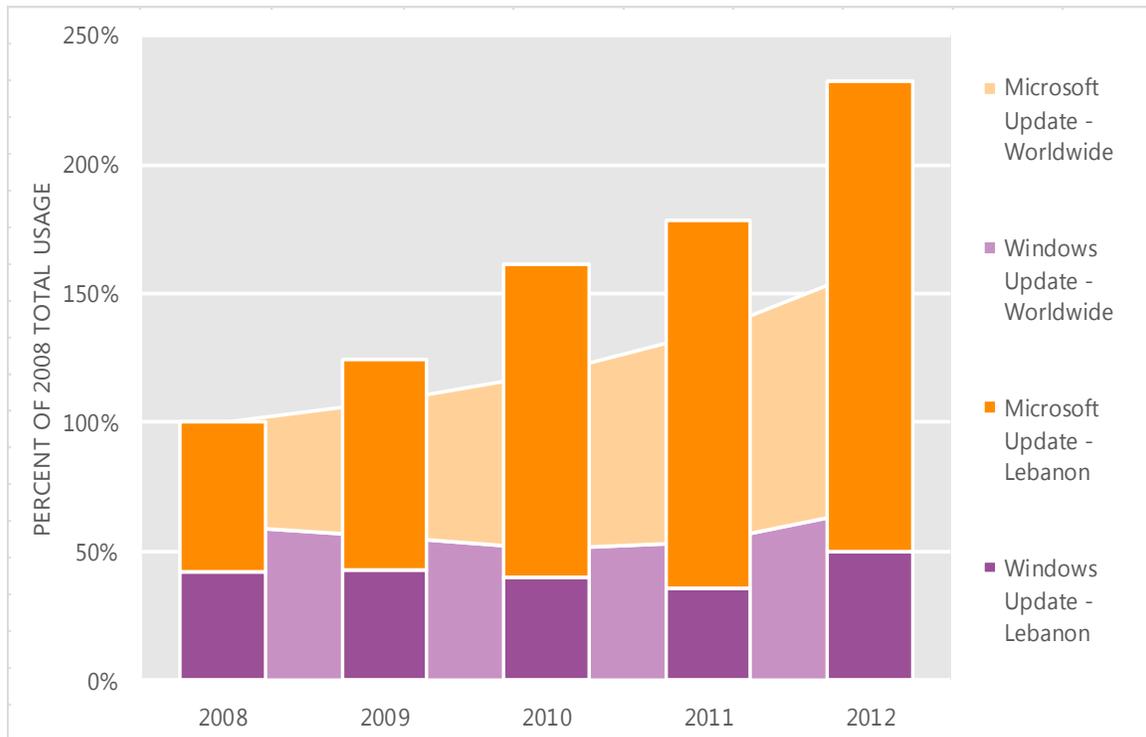
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Lebanon and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Lebanon over the last four years, indexed to the total usage for both services in Lebanon in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Lebanon was up 30.3 percent from 2011, and up 132.2 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Lebanon in 2012, 78.7 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Lithuania

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Lithuania in 2Q12 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.

Infection rate statistics for Lithuania

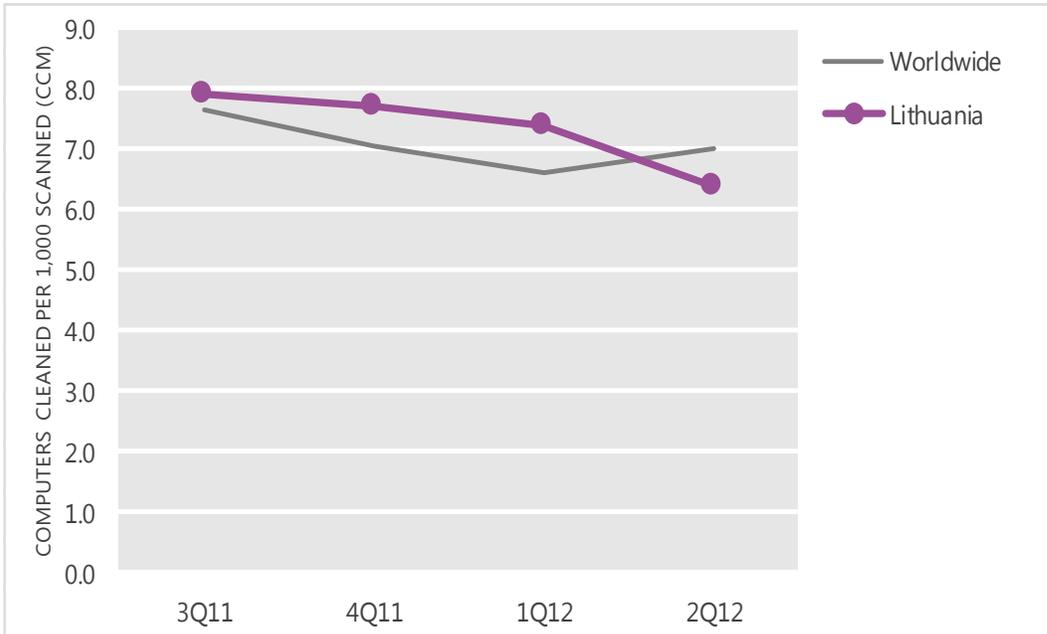
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	7.9	7.7	7.4	6.4
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

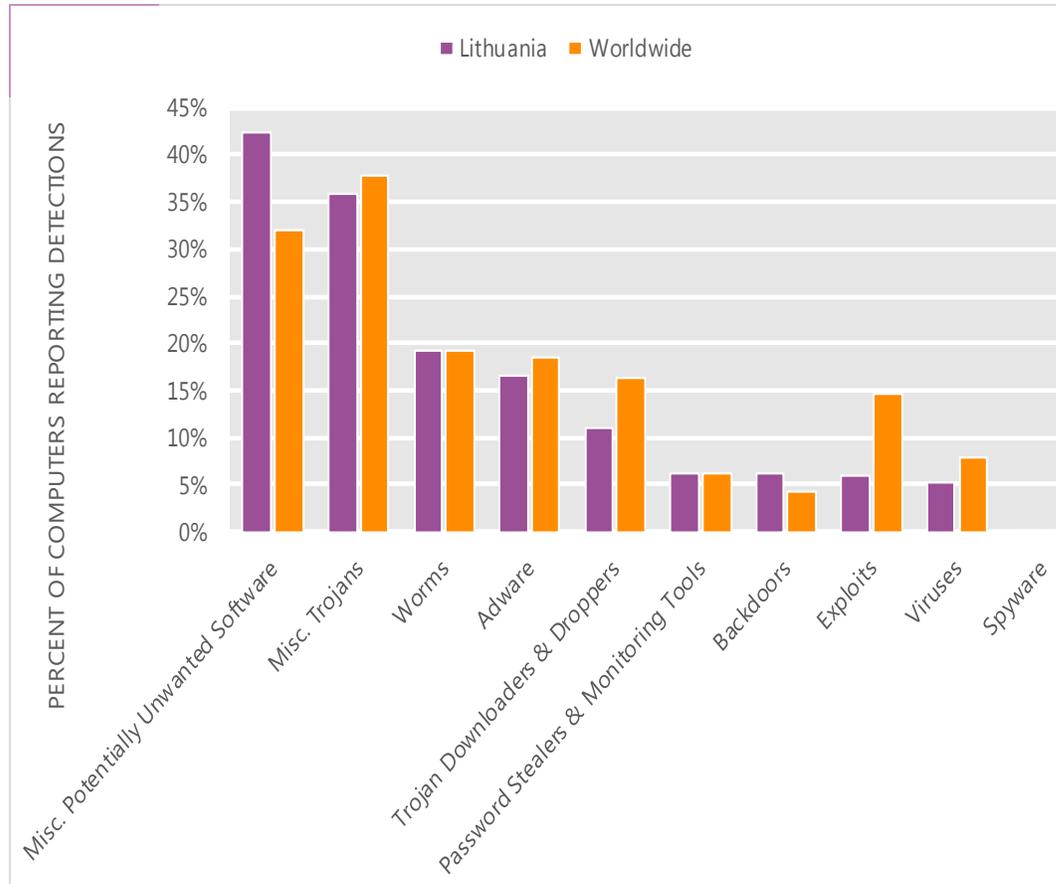
The MSRT detected malware on 6.4 of every 1,000 computers scanned in Lithuania in 2Q12 (a CCM score of 6.4, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Lithuania over the last four quarters, compared to the world as a whole.

CCM infection trends in Lithuania and worldwide



Threat categories

Malware and potentially unwanted software categories in Lithuania in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Lithuania in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 42.3 percent of all computers with detections there, down from 44.1 percent in 1Q12.
- The second most common category in Lithuania in 2Q12 was Miscellaneous Trojans. It affected 35.9 percent of all computers with detections there, up from 33.5 percent in 1Q12.
- The third most common category in Lithuania in 2Q12 was Worms, which affected 19.2 percent of all computers with detections there, up from 18.7 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Lithuania in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Keygen	Misc. Potentially Unwanted Software	17.1%
2	Win32/Autorun	Worms	6.5%
3	JS/Pornpop	Adware	6.5%
4	JS/IframeRef	Misc. Trojans	6.3%
5	Win32/Obfuscator	Misc. Potentially Unwanted Software	5.4%
6	Win32/Hotbar	Adware	5.0%
7	Win32/Rimecud	Worms	4.6%
8	Win32/Zwangi	Misc. Potentially Unwanted Software	4.3%
9	Win32/Pameseg	Misc. Potentially Unwanted Software	3.8%
10	Win32/Conficker	Worms	3.8%

- The most common threat family in Lithuania in 2Q12 was [Win32/Keygen](#), which affected 17.1 percent of computers with detections in Lithuania. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The second most common threat family in Lithuania in 2Q12 was [Win32/Autorun](#), which affected 6.5 percent of computers with detections in Lithuania. [Win32/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 threat family in Lithuania in 2Q12 was [JS/Pornpop](#), which affected 6.5 percent of computers with detections in Lithuania. [JS/Pornpop](#) is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The fourth most common threat family in Lithuania in 2Q12 was [JS/IframeRef](#), which affected 6.3 percent of computers with detections in Lithuania. [JS/IframeRef](#) is a generic detection for specially formed IFrame tags that point to remote websites that contain malicious content.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Lithuania

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	2.52 (1.6)	3.21 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	5.62 (3.9)	4.59 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	2.23 (0.7)	4.89 (0.9)

Update service usage

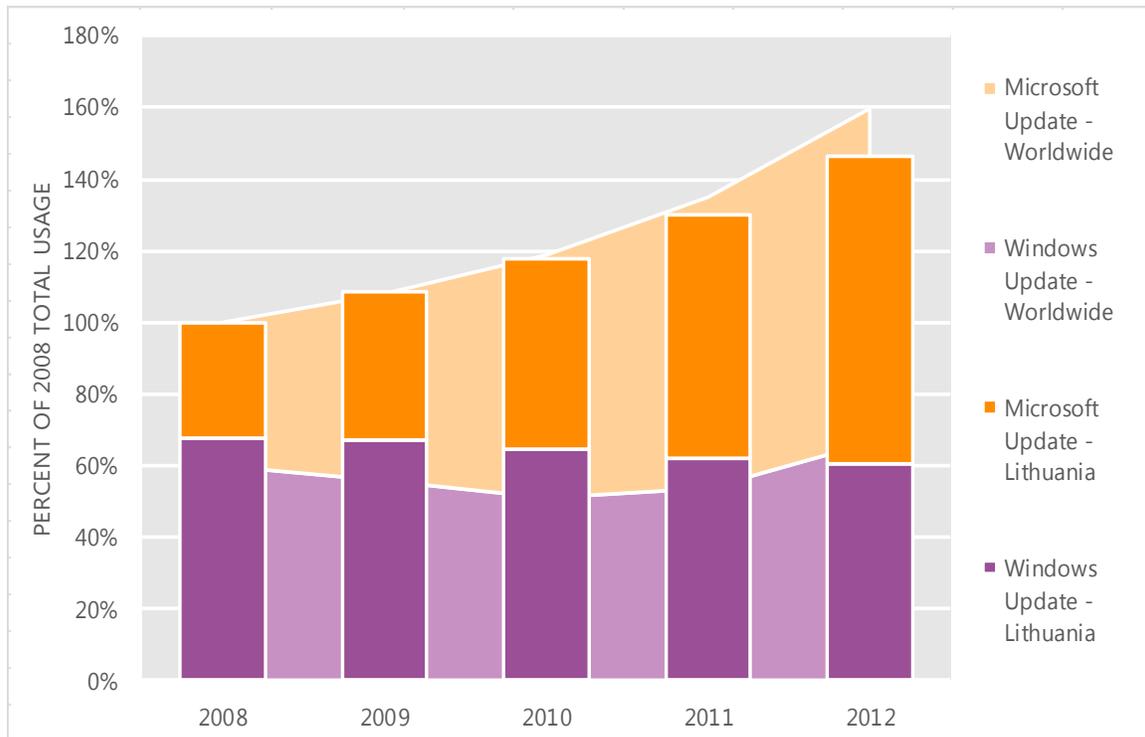
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Lithuania and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Lithuania over the last four years, indexed to the total usage for both services in Lithuania in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Lithuania was up 12.5 percent from 2011, and up 46.2 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Lithuania in 2012, 58.6 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Luxembourg

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Luxembourg in 2Q12 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.

Infection rate statistics for Luxembourg

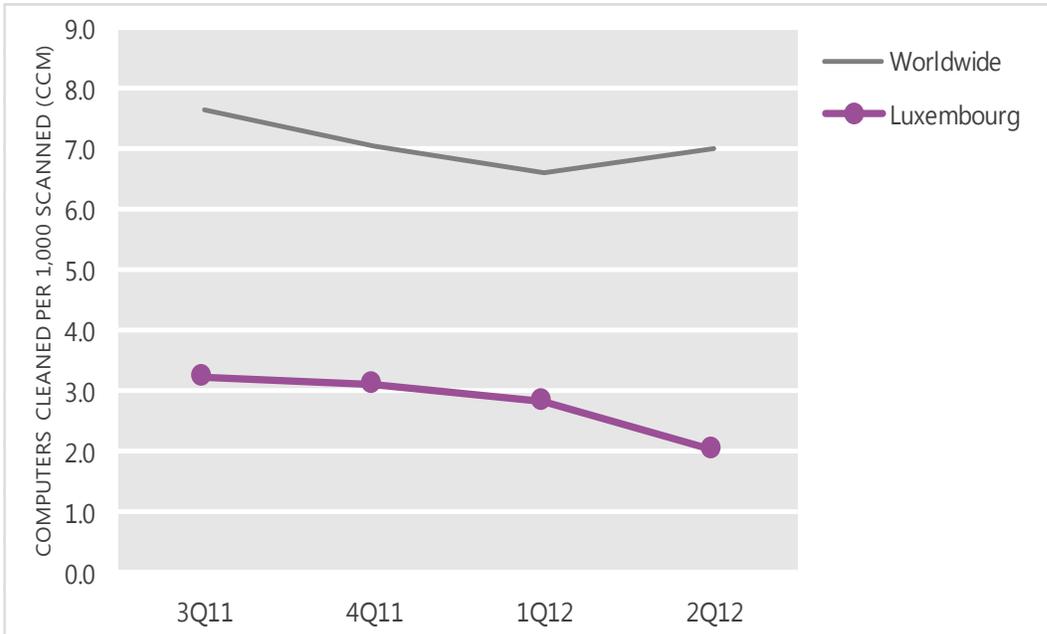
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	3.2	3.1	2.8	2.0
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

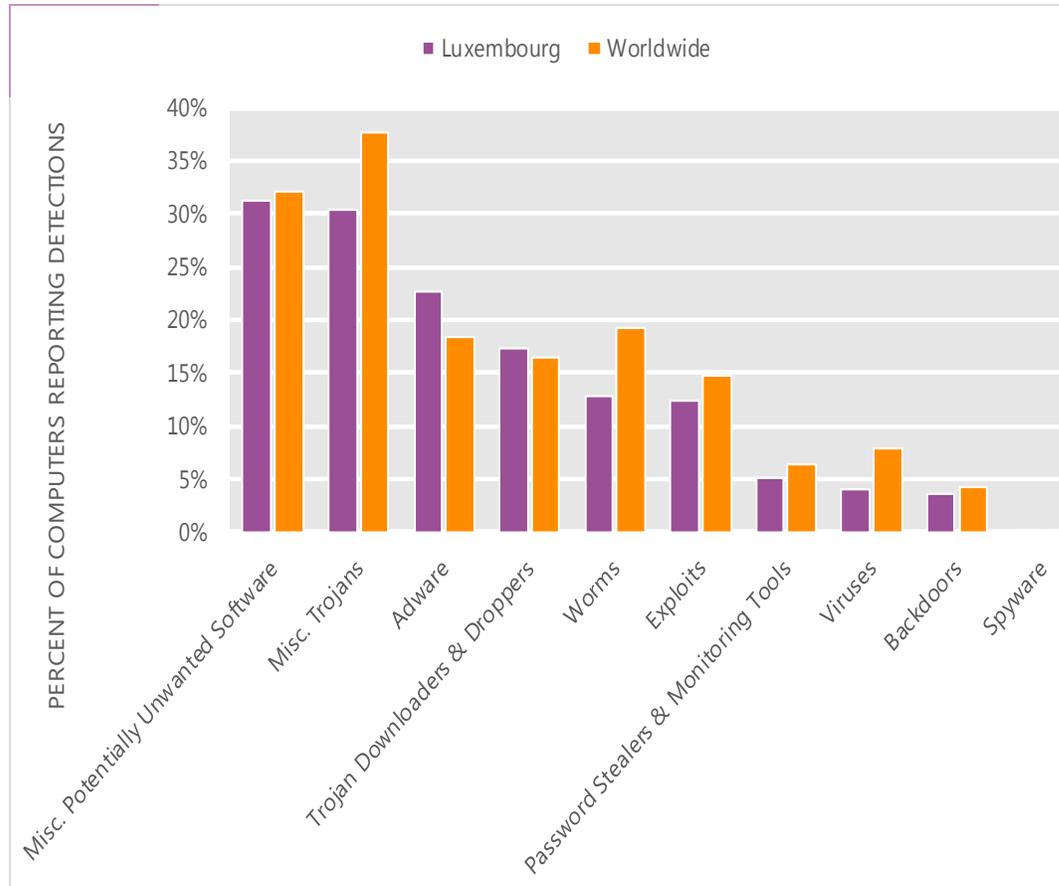
The MSRT detected malware on 2.0 of every 1,000 computers scanned in Luxembourg in 2Q12 (a CCM score of 2.0, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Luxembourg over the last four quarters, compared to the world as a whole.

CCM infection trends in Luxembourg and worldwide



Threat categories

Malware and potentially unwanted software categories in Luxembourg in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Luxembourg in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 31.3 percent of all computers with detections there, down from 32.3 percent in 1Q12.
- The second most common category in Luxembourg in 2Q12 was Miscellaneous Trojans. It affected 30.3 percent of all computers with detections there, up from 27.4 percent in 1Q12.
- The third most common category in Luxembourg in 2Q12 was Adware, which affected 22.6 percent of all computers with detections there, down from 29.6 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Luxembourg in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Keygen	Misc. Potentially Unwanted Software	9.8%
2	ASX/Wimad	Trojan Downloaders & Droppers	9.6%
3	JS/Pornpop	Adware	9.4%
4	Win32/Hotbar	Adware	7.0%
5	Java/Blacole	Exploits	6.4%
6	JS/IframeRef	Misc. Trojans	4.4%
7	Win32/Autorun	Worms	4.3%
8	Win32/Zwangi	Misc. Potentially Unwanted Software	3.8%
9	Win32/Sirefef	Misc. Trojans	3.4%
10	Win32/OpenCandy	Adware	3.1%

- The most common threat family in Luxembourg in 2Q12 was [Win32/Keygen](#), which affected 9.8 percent of computers with detections in Luxembourg. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The second most common threat family in Luxembourg in 2Q12 was [ASX/Wimad](#), which affected 9.6 percent of computers with detections in Luxembourg. [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 third most common threat family in Luxembourg in 2Q12 was [JS/Pornpop](#), which affected 9.4 percent of computers with detections in Luxembourg. [JS/Pornpop](#) is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The fourth most common threat family in Luxembourg in 2Q12 was [Win32/Hotbar](#), which affected 7.0 percent of computers with detections in Luxembourg. [Win32/Hotbar](#) is adware that displays a dynamic toolbar and targeted pop-up ads based on its monitoring of web-browsing activity.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Luxembourg

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	1.20 (1.6)	1.40 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	3.00 (3.9)	4.20 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.34 (0.7)	1.10 (0.9)

Update service usage

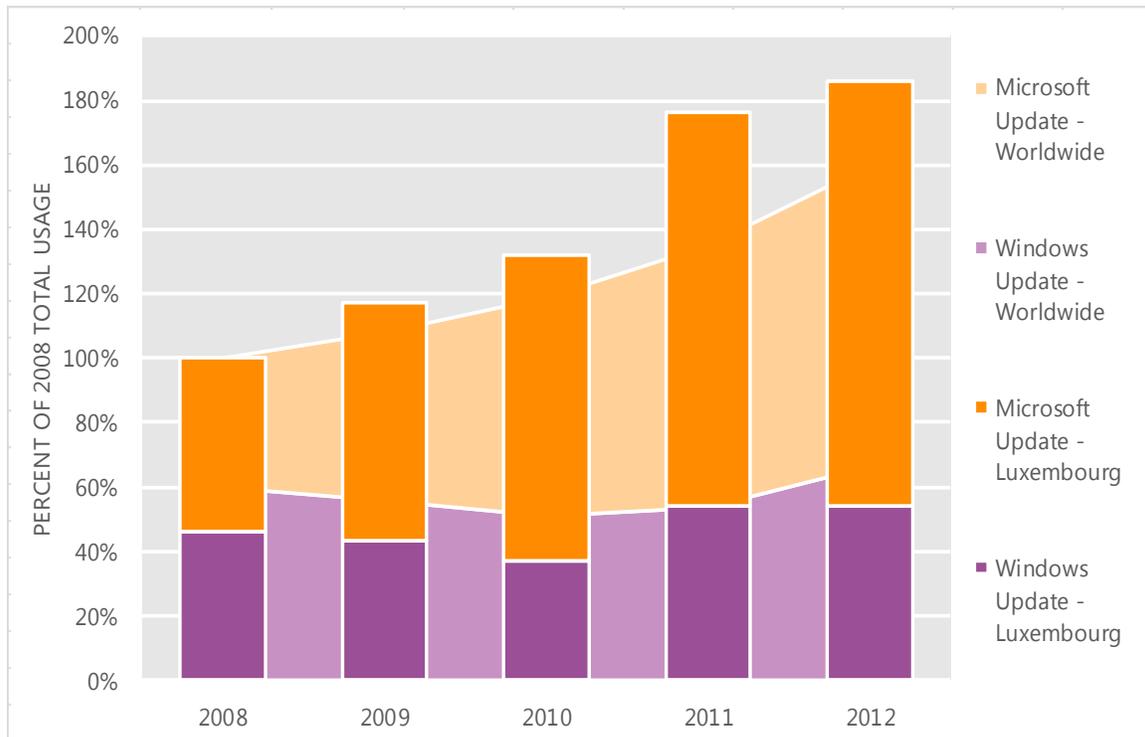
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Luxembourg and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Luxembourg over the last four years, indexed to the total usage for both services in Luxembourg in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Luxembourg was up 5.4 percent from 2011, and up 86.0 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Luxembourg in 2012, 70.8 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Macao S.A.R.

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Macao S.A.R. in 2Q12 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.

Infection rate statistics for Macao S.A.R.

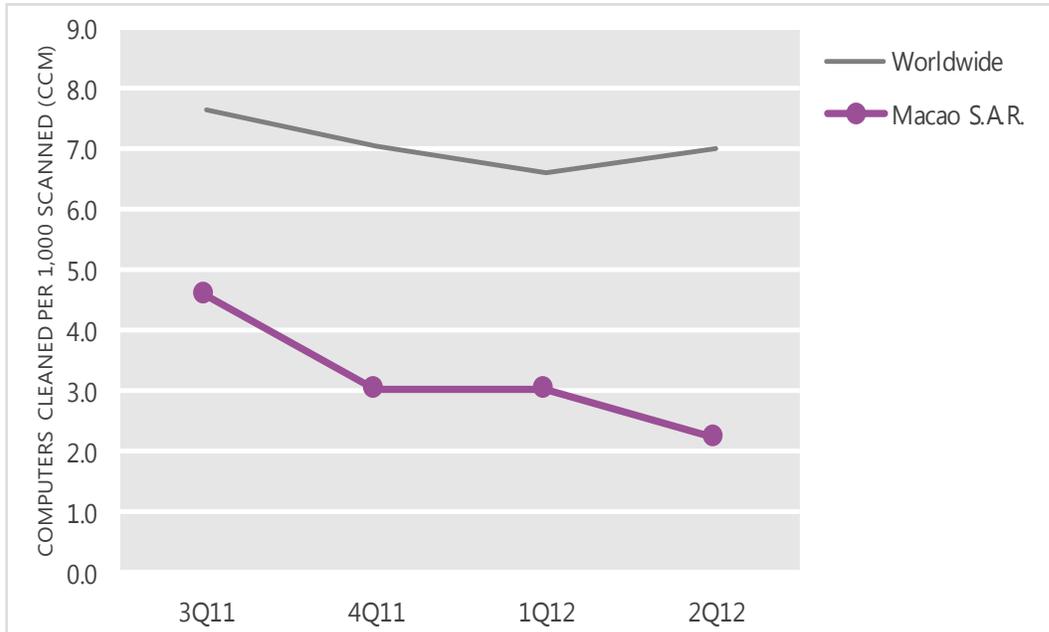
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	4.6	3.0	3.0	2.2
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

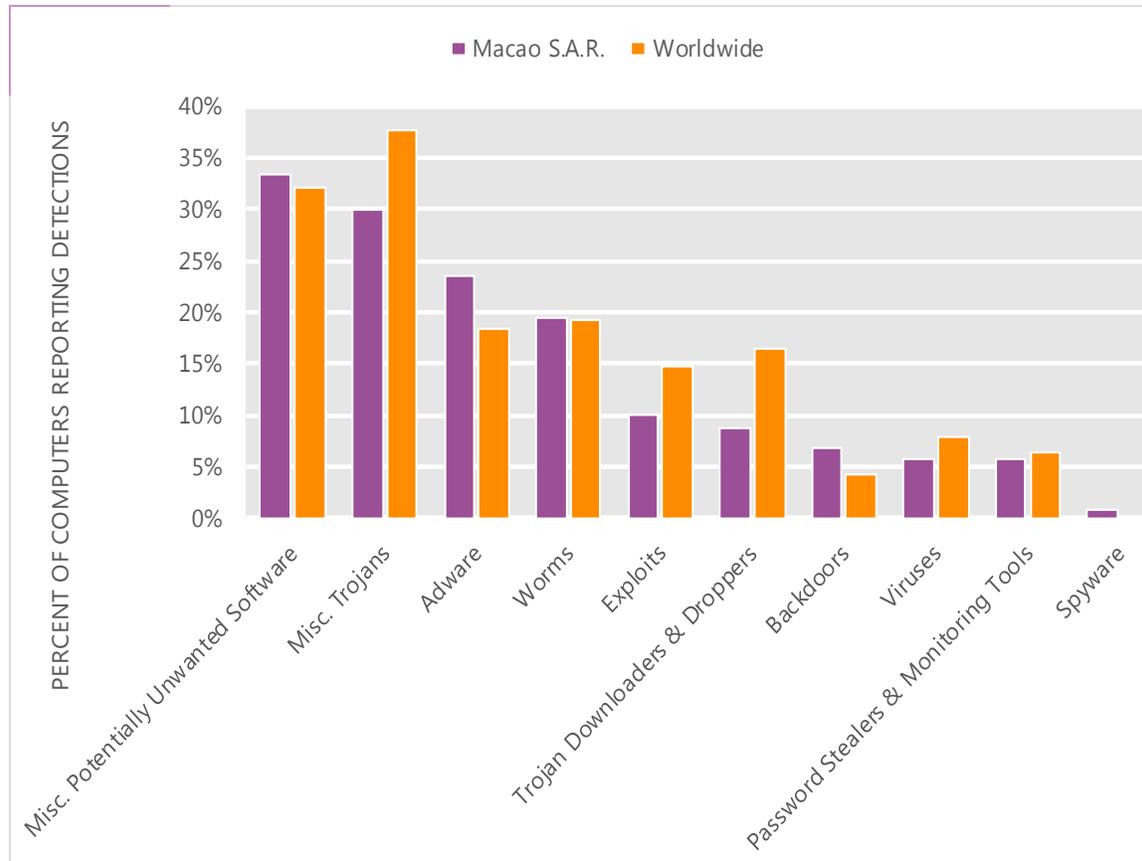
The MSRT detected malware on 2.2 of every 1,000 computers scanned in Macao S.A.R. in 2Q12 (a CCM score of 2.2, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Macao S.A.R. over the last four quarters, compared to the world as a whole.

CCM infection trends in Macao S.A.R. and worldwide



Threat categories

Malware and potentially unwanted software categories in Macao S.A.R. in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Macao S.A.R. in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 33.3 percent of all computers with detections there, down from 37.6 percent in 1Q12.
- The second most common category in Macao S.A.R. in 2Q12 was Miscellaneous Trojans. It affected 29.9 percent of all computers with detections there, down from 30.8 percent in 1Q12.
- The third most common category in Macao S.A.R. in 2Q12 was Adware, which affected 23.5 percent of all computers with detections there, up from 17.3 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Macao S.A.R. in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Keygen	Misc. Potentially Unwanted Software	12.0%
2	JS/Pornpop	Adware	10.3%
3	JS/IframeRef	Misc. Trojans	9.8%
4	Win32/Autorun	Worms	7.3%
5	JS/Popupper	Adware	6.1%
6	Win32/Conficker	Worms	6.0%
7	Win32/BaiduSobar	Misc. Potentially Unwanted Software	4.5%
8	Win32/Hotbar	Adware	4.1%
9	Win32/Obfuscator	Misc. Potentially Unwanted Software	3.6%
10	Win32/Taterf	Worms	3.3%

- The most common threat family in Macao S.A.R. in 2Q12 was [Win32/Keygen](#), which affected 12.0 percent of computers with detections in Macao S.A.R.. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The second most common threat family in Macao S.A.R. in 2Q12 was [JS/Pornpop](#), which affected 10.3 percent of computers with detections in Macao S.A.R.. [JS/Pornpop](#) is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The third most common threat family in Macao S.A.R. in 2Q12 was [JS/IframeRef](#), which affected 9.8 percent of computers with detections in Macao S.A.R.. [JS/IframeRef](#) is a generic detection for specially formed IFrame tags that point to remote websites that contain malicious content.
- The fourth most common threat family in Macao S.A.R. in 2Q12 was [Win32/Autorun](#), which affected 7.3 percent of computers with detections in Macao S.A.R.. [Win32/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.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Macao S.A.R.

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	N/A (1.6)	N/A (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	1.29 (3.9)	1.94 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.02 (0.7)	0.03 (0.9)

Update service usage

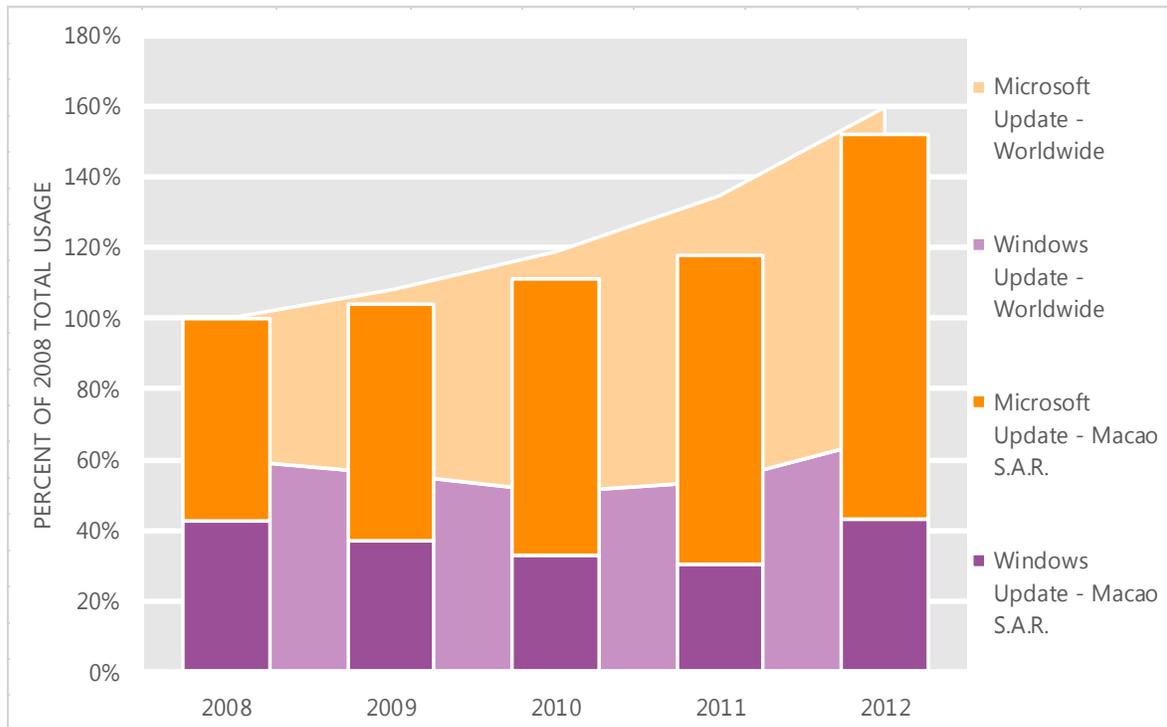
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Macao S.A.R. and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Macao S.A.R. over the last four years, indexed to the total usage for both services in Macao S.A.R. in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Macao S.A.R. was up 29.1 percent from 2011, and up 52.0 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Macao S.A.R. in 2012, 71.7 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Malaysia

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Malaysia in 2Q12 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.

Infection rate statistics for Malaysia

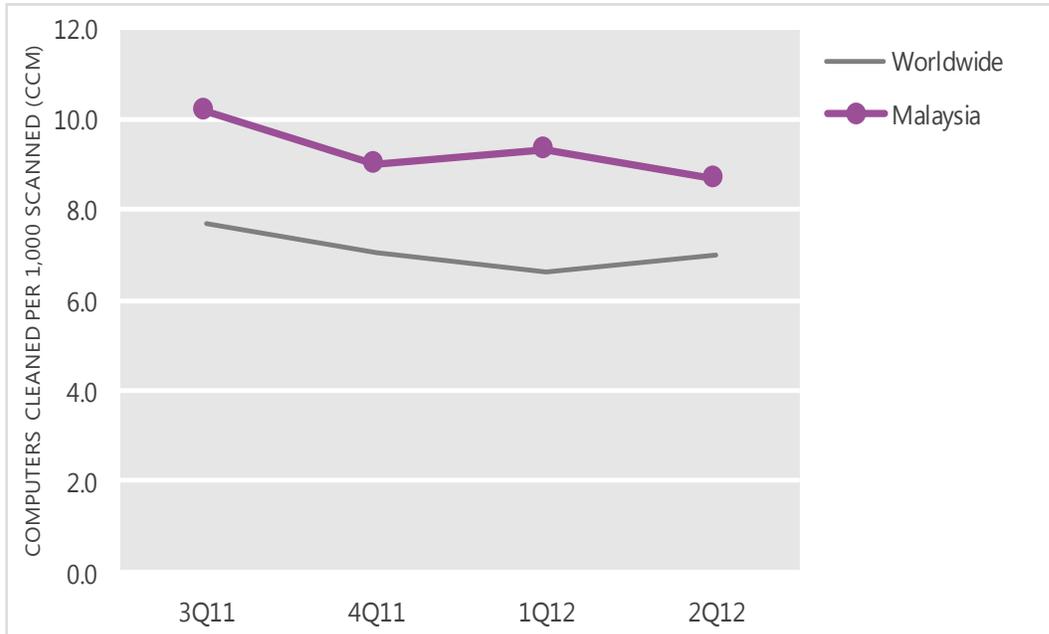
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	10.2	9.0	9.3	8.7
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

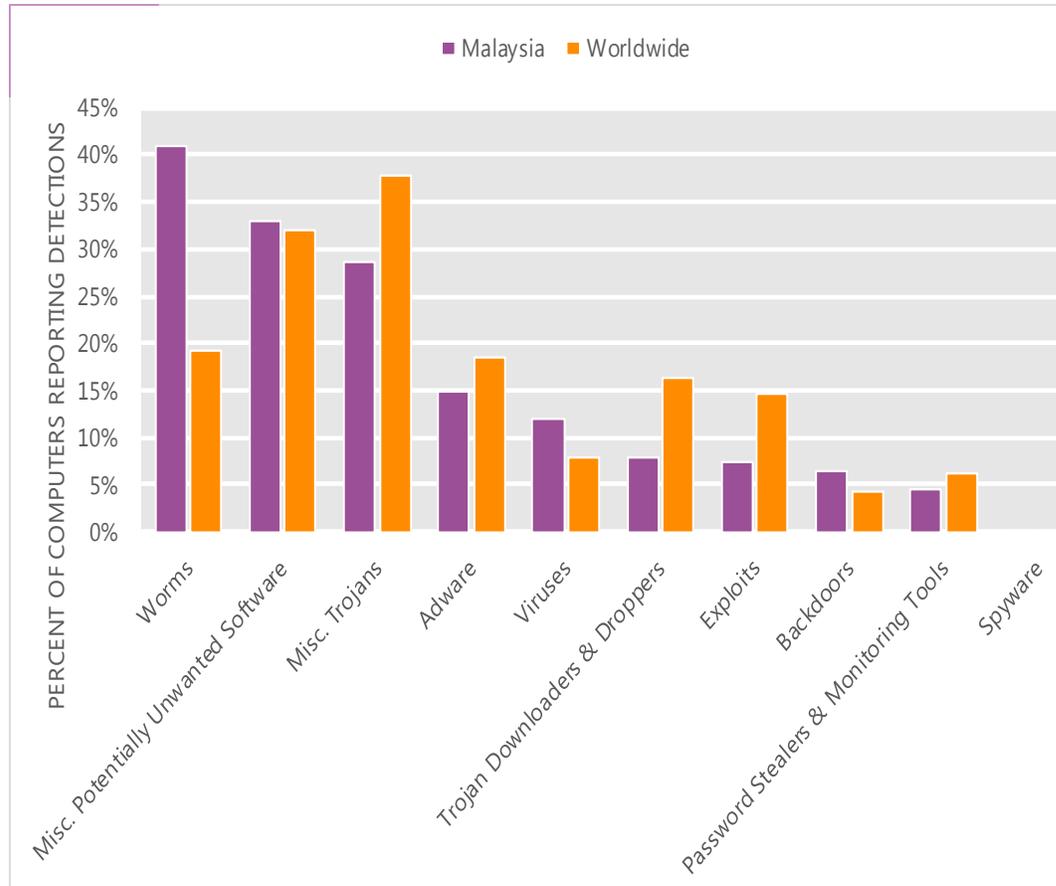
The MSRT detected malware on 8.7 of every 1,000 computers scanned in Malaysia in 2Q12 (a CCM score of 8.7, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Malaysia over the last four quarters, compared to the world as a whole.

CCM infection trends in Malaysia and worldwide



Threat categories

Malware and potentially unwanted software categories in Malaysia in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Malaysia in 2Q12 was Worms. It affected 40.8 percent of all computers with detections there, up from 40.3 percent in 1Q12.
- The second most common category in Malaysia in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 33.0 percent of all computers with detections there, down from 33.1 percent in 1Q12.
- The third most common category in Malaysia in 2Q12 was Miscellaneous Trojans, which affected 28.6 percent of all computers with detections there, down from 29.0 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Malaysia in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Dorkbot	Worms	15.3%
2	Win32/Autorun	Worms	14.5%
3	Win32/Keygen	Misc. Potentially Unwanted Software	11.0%
4	Win32/Sality	Viruses	9.3%
5	Win32/Conficker	Worms	6.5%
6	Win32/Hotbar	Adware	5.1%
7	JS/Pornpop	Adware	5.1%
8	JS/IframeRef	Misc. Trojans	4.1%
9	Win32/Nuqel	Worms	4.0%
10	Win32/Zwangi	Misc. Potentially Unwanted Software	3.8%

- The most common threat family in Malaysia in 2Q12 was [Win32/Dorkbot](#), which affected 15.3 percent of computers with detections in Malaysia. [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 second most common threat family in Malaysia in 2Q12 was [Win32/Autorun](#), which affected 14.5 percent of computers with detections in Malaysia. [Win32/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 threat family in Malaysia in 2Q12 was [Win32/Keygen](#), which affected 11.0 percent of computers with detections in Malaysia. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The fourth most common threat family in Malaysia in 2Q12 was [Win32/Sality](#), which affected 9.3 percent of computers with detections in Malaysia. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Malaysia

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	0.63 (1.6)	0.98 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	0.83 (3.9)	1.27 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	2.81 (0.7)	5.72 (0.9)

Update service usage

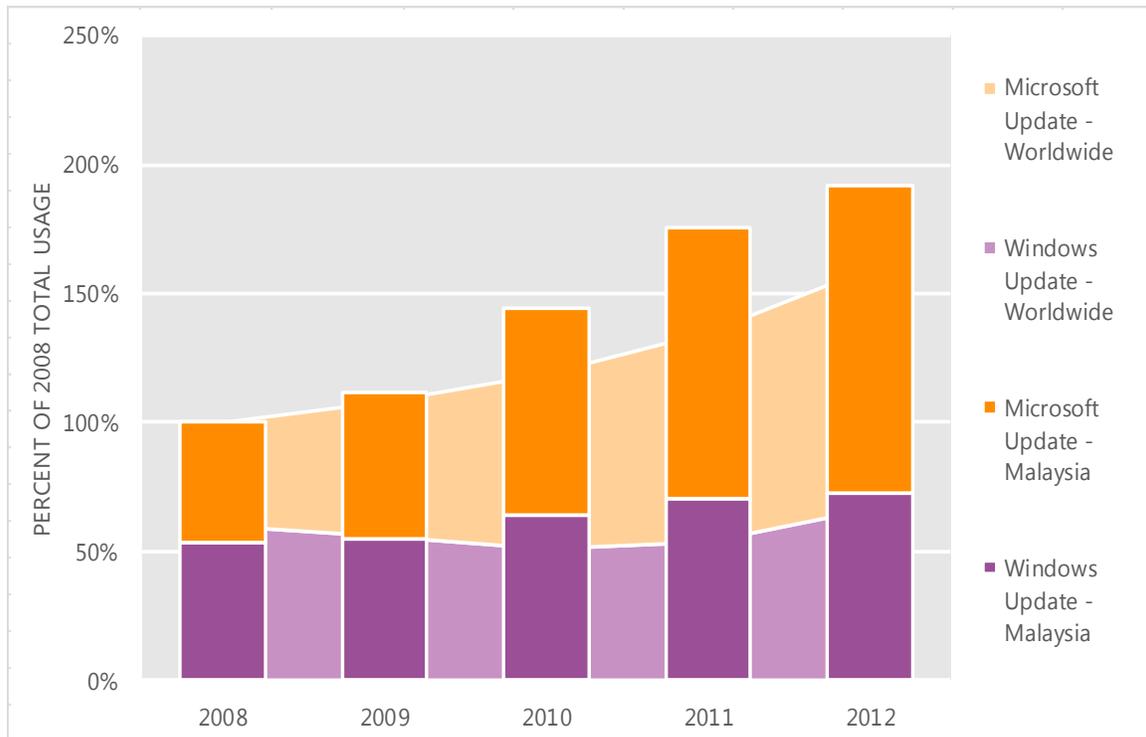
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Malaysia and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Malaysia over the last four years, indexed to the total usage for both services in Malaysia in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Malaysia was up 9.1 percent from 2011, and up 91.9 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Malaysia in 2012, 62.2 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Malta

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Malta in 2Q12 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.

Infection rate statistics for Malta

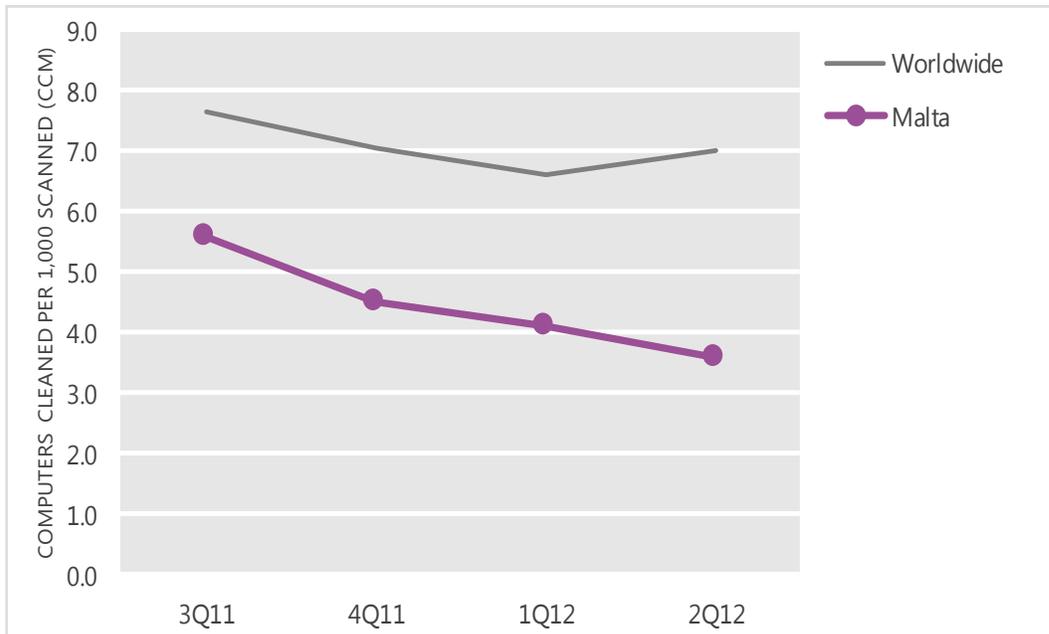
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	5.6	4.5	4.1	3.6
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

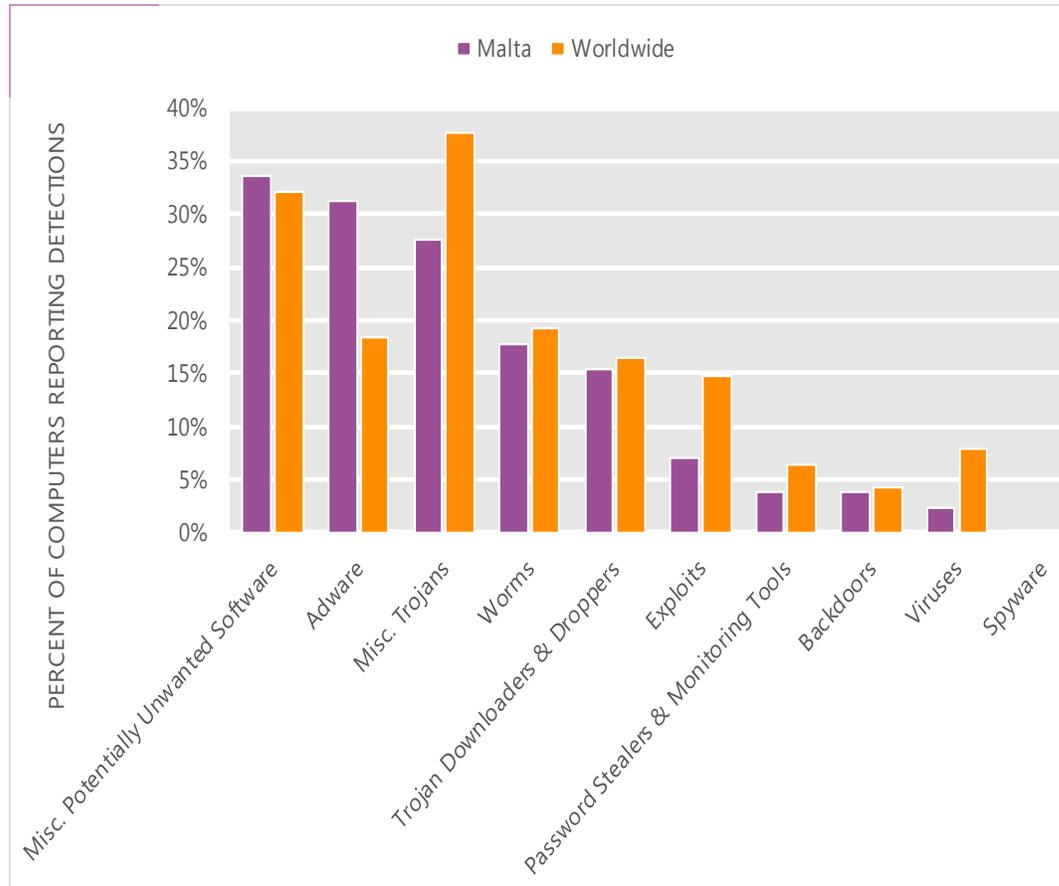
The MSRT detected malware on 3.6 of every 1,000 computers scanned in Malta in 2Q12 (a CCM score of 3.6, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Malta over the last four quarters, compared to the world as a whole.

CCM infection trends in Malta and worldwide



Threat categories

Malware and potentially unwanted software categories in Malta in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Malta in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 33.5 percent of all computers with detections there, up from 32.5 percent in 1Q12.
- The second most common category in Malta in 2Q12 was Adware. It affected 31.1 percent of all computers with detections there, down from 38.9 percent in 1Q12.
- The third most common category in Malta in 2Q12 was Miscellaneous Trojans, which affected 27.6 percent of all computers with detections there, up from 25.2 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Malta in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Hotbar	Adware	15.3%
2	Win32/Keygen	Misc. Potentially Unwanted Software	11.4%
3	JS/Pornpop	Adware	10.8%
4	ASX/Wimad	Trojan Downloaders & Droppers	9.6%
5	Win32/Autorun	Worms	8.2%
6	Win32/Zwangi	Misc. Potentially Unwanted Software	7.8%
7	JS/IframeRef	Misc. Trojans	4.1%
8	Win32/Rimecud	Worms	3.3%
9	Win32/Conficker	Worms	2.8%
10	Win32/Wpakill	Misc. Potentially Unwanted Software	2.7%

- The most common threat family in Malta in 2Q12 was [Win32/Hotbar](#), which affected 15.3 percent of computers with detections in Malta. [Win32/Hotbar](#) is adware that displays a dynamic toolbar and targeted pop-up ads based on its monitoring of web-browsing activity.
- The second most common threat family in Malta in 2Q12 was [Win32/Keygen](#), which affected 11.4 percent of computers with detections in Malta. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The third most common threat family in Malta in 2Q12 was [JS/Pornpop](#), which affected 10.8 percent of computers with detections in Malta. [JS/Pornpop](#) is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The fourth most common threat family in Malta in 2Q12 was [ASX/Wimad](#), which affected 9.6 percent of computers with detections in Malta. [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.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Malta

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	0.79 (1.6)	0.40 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	1.58 (3.9)	1.58 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.00 (0.7)	0.00 (0.9)

Update service usage

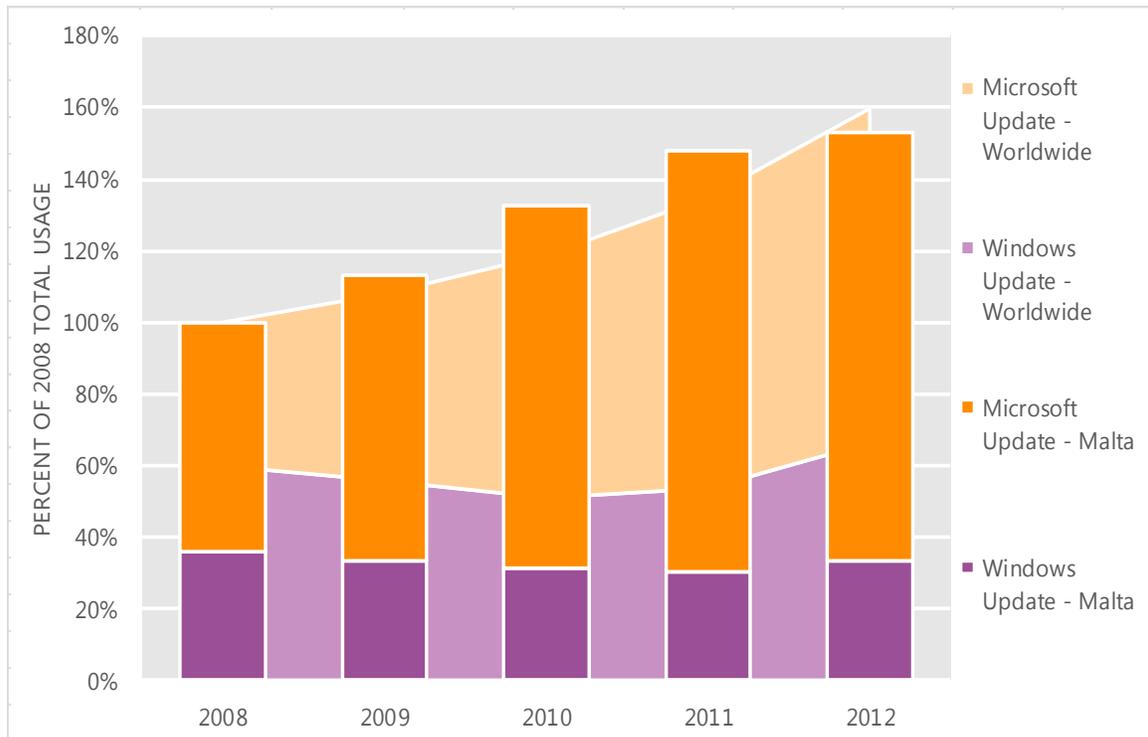
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Malta and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Malta over the last four years, indexed to the total usage for both services in Malta in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Malta was up 3.6 percent from 2011, and up 53.1 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Malta in 2012, 78.3 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Mexico

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Mexico in 2Q12 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.

Infection rate statistics for Mexico

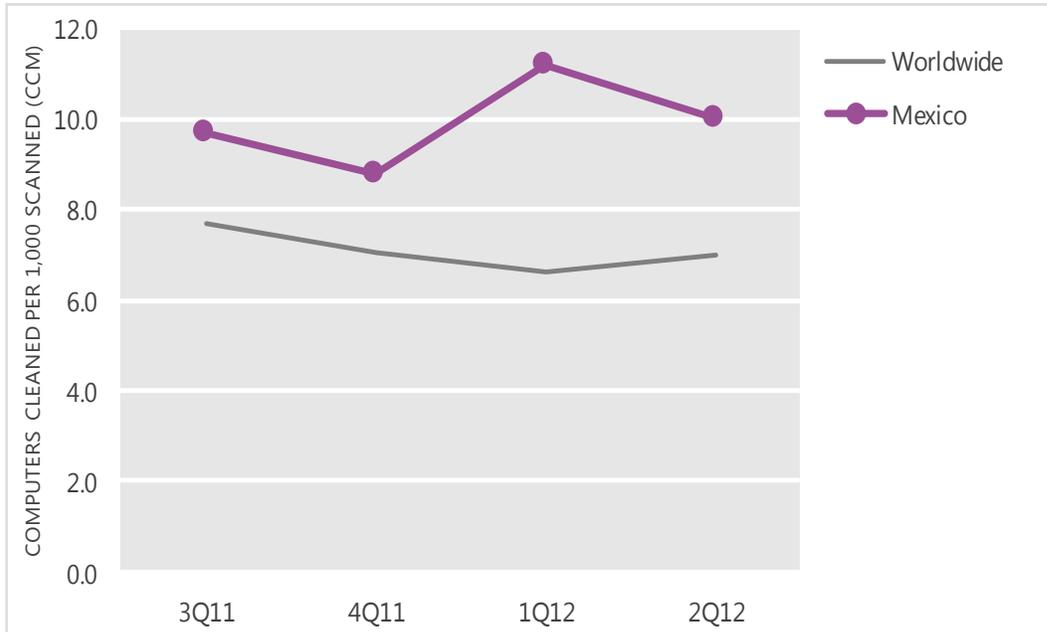
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	9.7	8.8	11.2	10.0
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

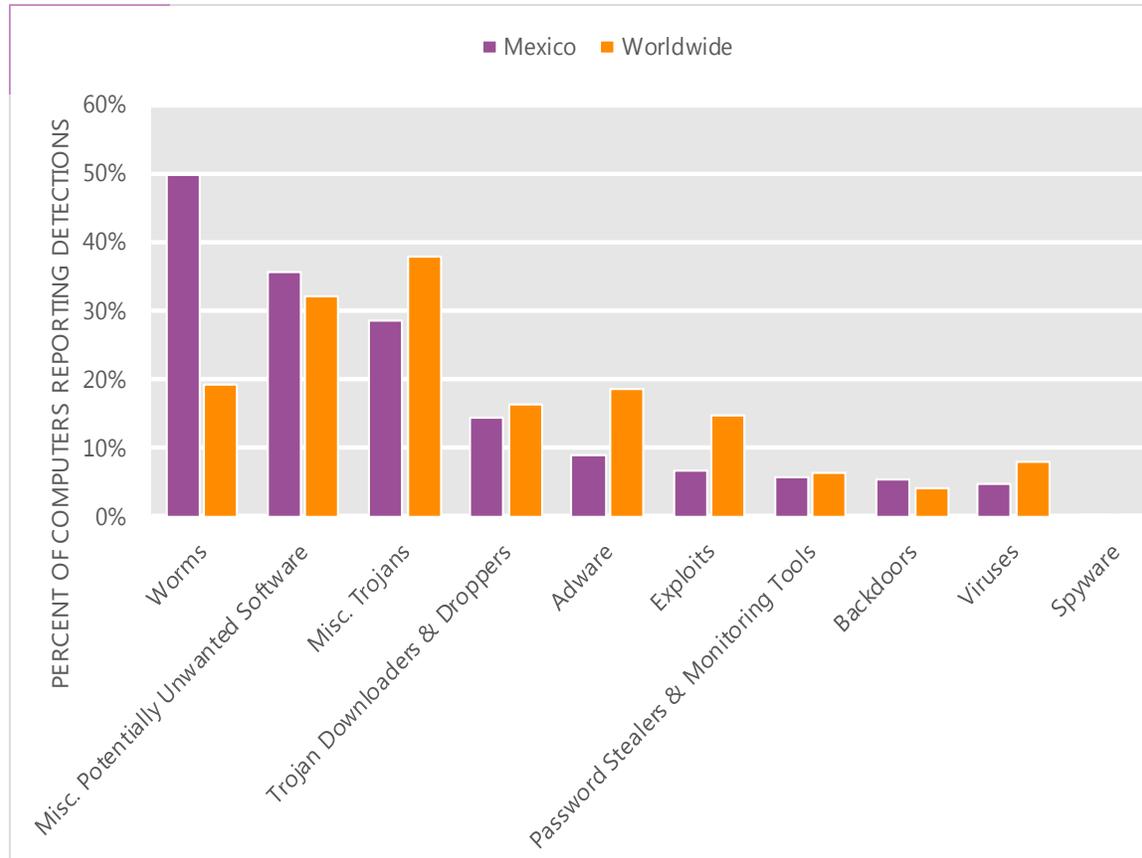
The MSRT detected malware on 10.0 of every 1,000 computers scanned in Mexico in 2Q12 (a CCM score of 10.0, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Mexico over the last four quarters, compared to the world as a whole.

CCM infection trends in Mexico and worldwide



Threat categories

Malware and potentially unwanted software categories in Mexico in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Mexico in 2Q12 was Worms. It affected 49.7 percent of all computers with detections there, up from 48.6 percent in 1Q12.
- The second most common category in Mexico in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 35.4 percent of all computers with detections there, down from 38.5 percent in 1Q12.
- The third most common category in Mexico in 2Q12 was Miscellaneous Trojans, which affected 28.7 percent of all computers with detections there, up from 26.4 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Mexico in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Dorkbot	Worms	25.7%
2	Win32/Autorun	Worms	14.4%
3	Win32/Keygen	Misc. Potentially Unwanted Software	10.8%
4	Win32/Vobfus	Worms	9.2%
5	Win32/VBInject	Misc. Potentially Unwanted Software	7.5%
6	Win32/Conficker	Worms	6.3%
7	ASX/Wimad	Trojan Downloaders & Droppers	5.1%
8	Win32/Brontok	Worms	5.0%
9	Win32/Rimecud	Worms	4.0%
10	Win32/Sirefef	Misc. Trojans	3.8%

- The most common threat family in Mexico in 2Q12 was [Win32/Dorkbot](#), which affected 25.7 percent of computers with detections in Mexico. [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 second most common threat family in Mexico in 2Q12 was [Win32/Autorun](#), which affected 14.4 percent of computers with detections in Mexico. [Win32/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 threat family in Mexico in 2Q12 was [Win32/Keygen](#), which affected 10.8 percent of computers with detections in Mexico. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The fourth most common threat family in Mexico in 2Q12 was [Win32/Vobfus](#), which affected 9.2 percent of computers with detections in Mexico. [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.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Mexico

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	0.74 (1.6)	0.60 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	1.20 (3.9)	1.47 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.01 (0.7)	0.02 (0.9)

Update service usage

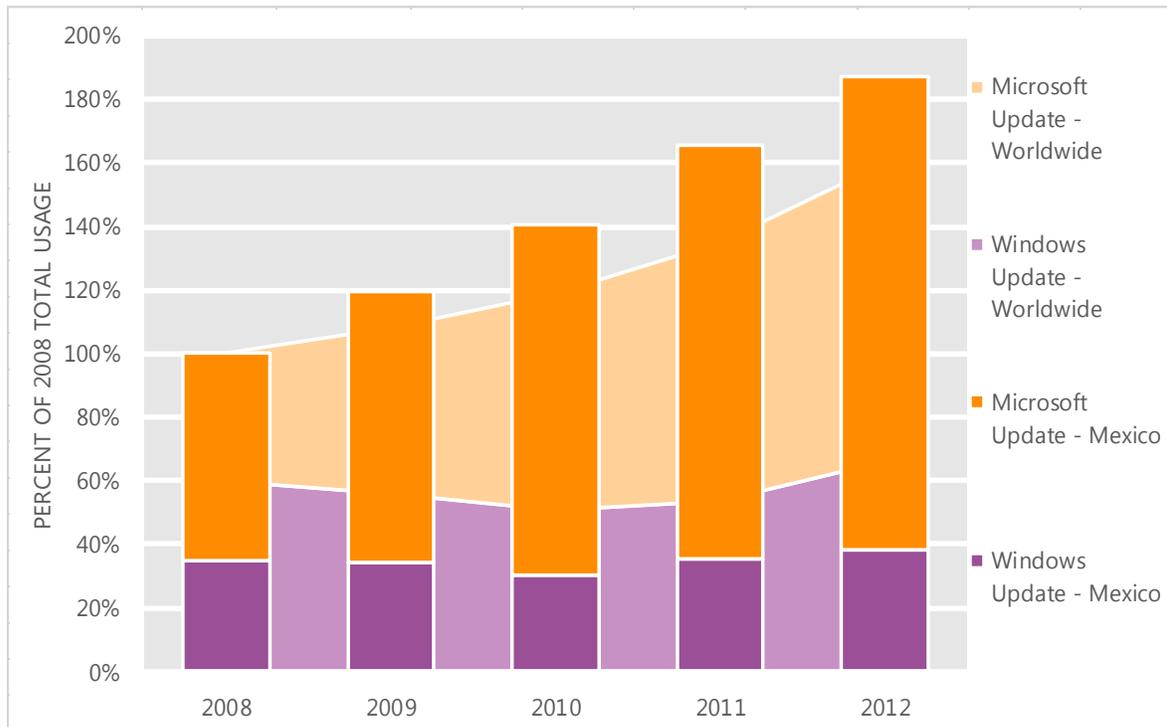
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Mexico and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Mexico over the last four years, indexed to the total usage for both services in Mexico in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Mexico was up 12.8 percent from 2011, and up 87.1 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Mexico in 2012, 79.5 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Moldova

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Moldova in 2Q12 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.

Infection rate statistics for Moldova

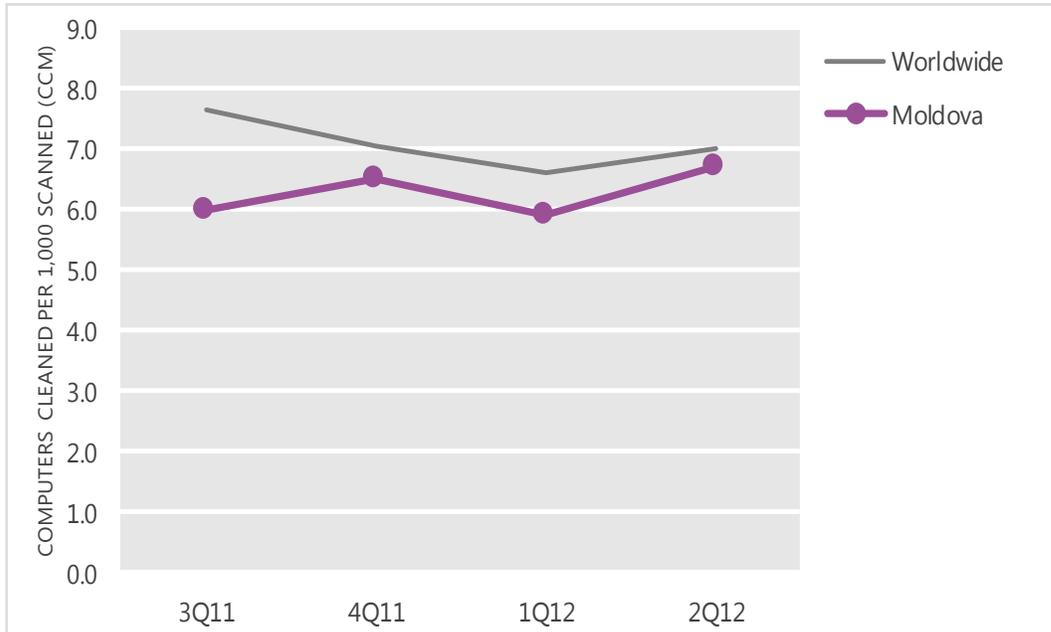
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	6.0	6.5	5.9	6.7
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

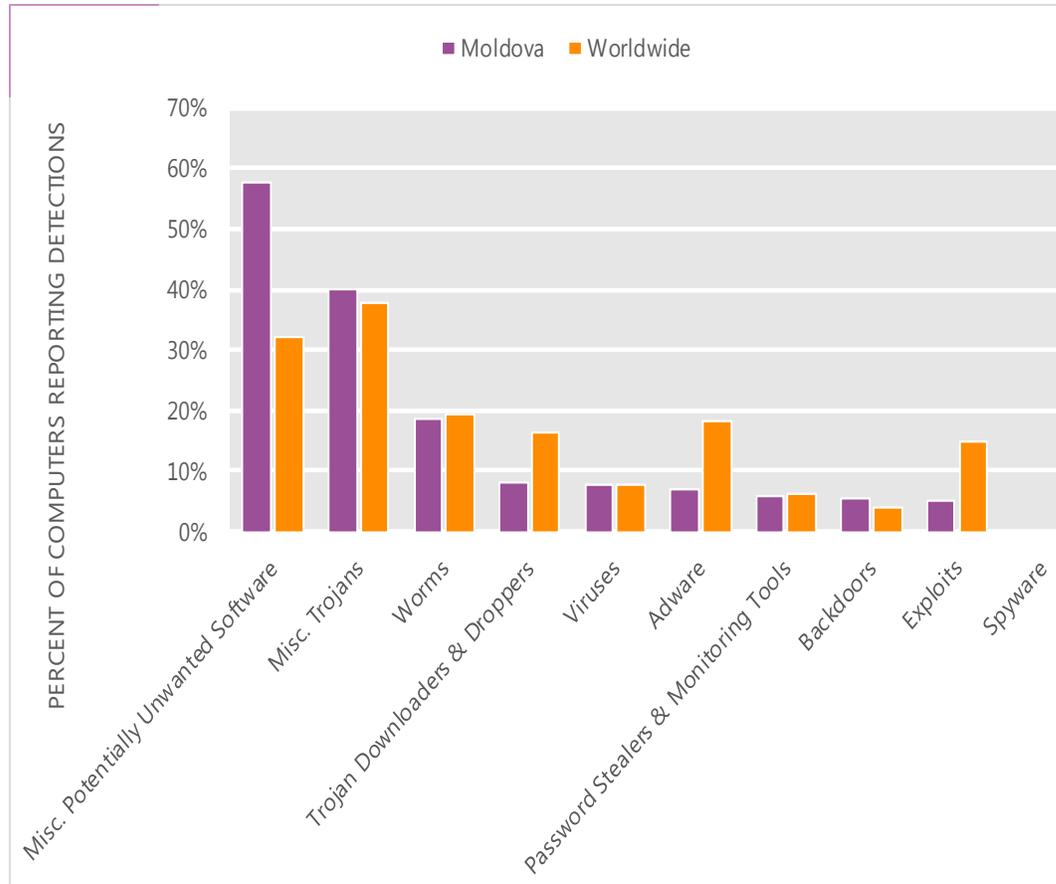
The MSRT detected malware on 6.7 of every 1,000 computers scanned in Moldova in 2Q12 (a CCM score of 6.7, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Moldova over the last four quarters, compared to the world as a whole.

CCM infection trends in Moldova and worldwide



Threat categories

Malware and potentially unwanted software categories in Moldova in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Moldova in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 57.6 percent of all computers with detections there, down from 62.1 percent in 1Q12.
- The second most common category in Moldova in 2Q12 was Miscellaneous Trojans. It affected 40.2 percent of all computers with detections there, up from 37.2 percent in 1Q12.
- The third most common category in Moldova in 2Q12 was Worms, which affected 18.7 percent of all computers with detections there, down from 19.4 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Moldova in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Pameseg	Misc. Potentially Unwanted Software	24.3%
2	Win32/Keygen	Misc. Potentially Unwanted Software	15.5%
3	Win32/Qhosts	Misc. Trojans	8.0%
4	Win32/Obfuscator	Misc. Potentially Unwanted Software	7.1%
5	Win32/Gendows	Misc. Potentially Unwanted Software	6.4%
6	Win32/Autorun	Worms	6.3%
7	Win32/Dorkbot	Worms	4.6%
8	Win32/Sality	Viruses	3.8%
9	Win32/Dynamer	Misc. Trojans	3.4%
10	Win32/Rimecud	Worms	3.3%

- The most common threat family in Moldova in 2Q12 was [Win32/Pameseg](#), which affected 24.3 percent of computers with detections in Moldova. [Win32/Pameseg](#) is a fake program installer that requires the user to send SMS messages to a premium number to successfully install certain programs.
- The second most common threat family in Moldova in 2Q12 was [Win32/Keygen](#), which affected 15.5 percent of computers with detections in Moldova. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The third most common threat family in Moldova in 2Q12 was [Win32/Qhosts](#), which affected 8.0 percent of computers with detections in Moldova. [Win32/Qhosts](#) is a trojan that modifies the computer's HOSTS file to prevent access to certain websites. It may be dropped by other malware as a payload.
- The fourth most common threat family in Moldova in 2Q12 was [Win32/Obfuscator](#), which affected 7.1 percent of computers with detections in Moldova. [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.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Moldova

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	1.59 (1.6)	1.90 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	4.76 (3.9)	5.07 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.33 (0.7)	2.01 (0.9)

Update service usage

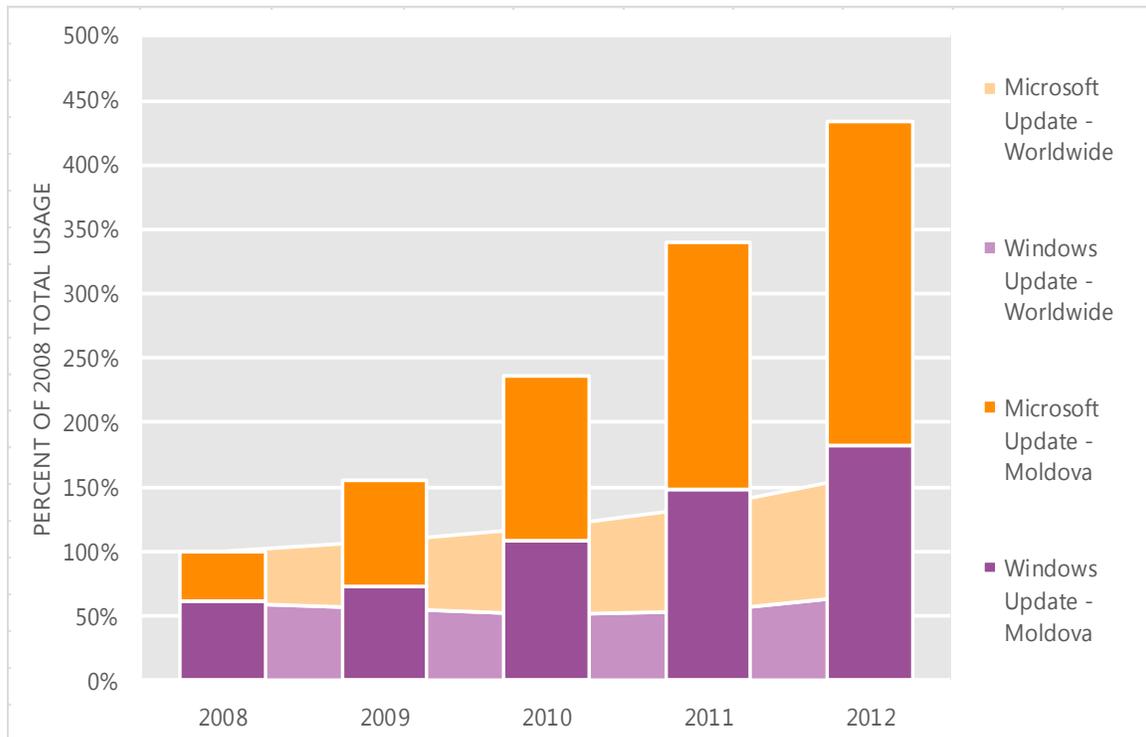
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Moldova and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Moldova over the last four years, indexed to the total usage for both services in Moldova in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Moldova was up 27.6 percent from 2011, and up 334.1 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Moldova in 2012, 57.9 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Morocco

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Morocco in 2Q12 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.

Infection rate statistics for Morocco

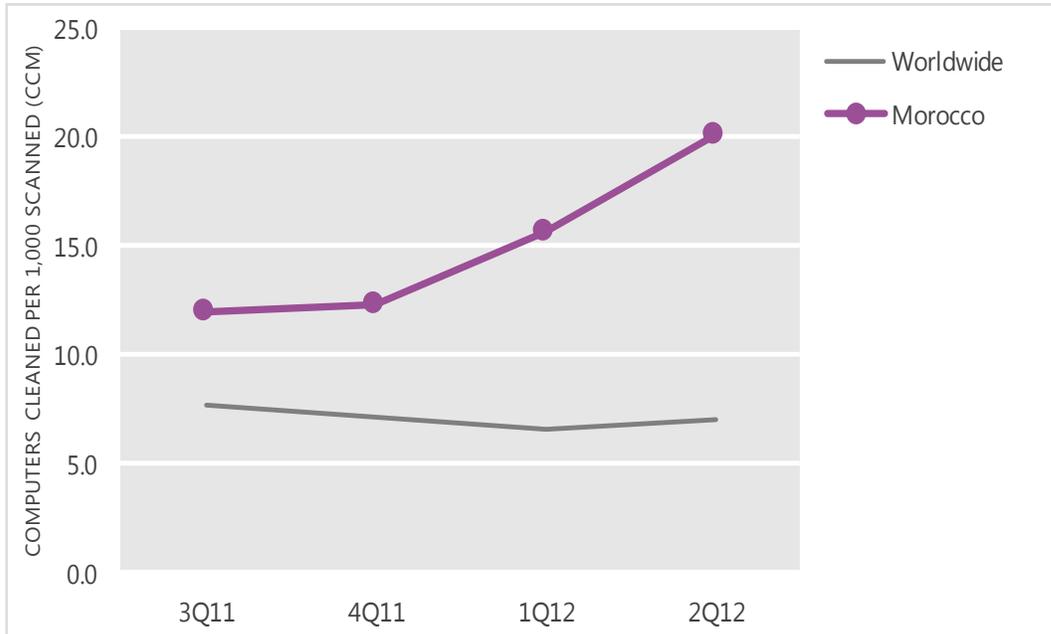
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	12.0	12.3	15.6	20.1
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

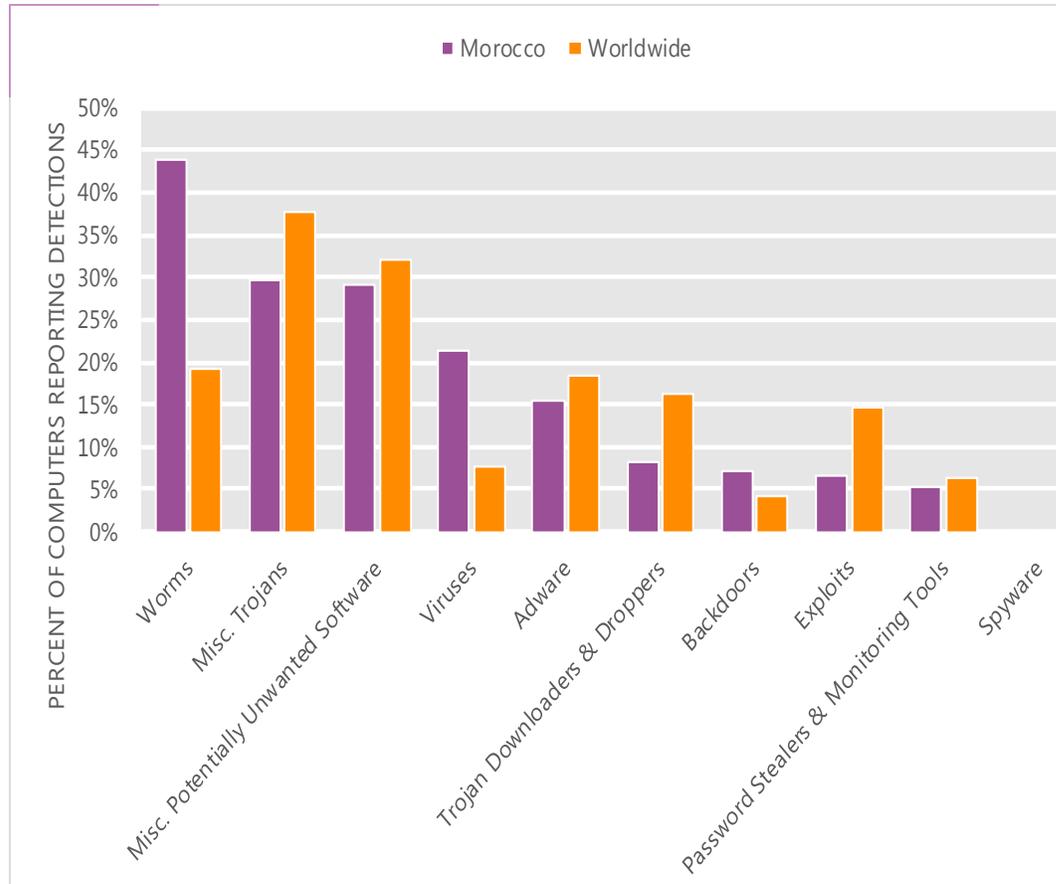
The MSRT detected malware on 20.1 of every 1,000 computers scanned in Morocco in 2Q12 (a CCM score of 20.1, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Morocco over the last four quarters, compared to the world as a whole.

CCM infection trends in Morocco and worldwide



Threat categories

Malware and potentially unwanted software categories in Morocco in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Morocco in 2Q12 was Worms. It affected 43.9 percent of all computers with detections there, up from 35.4 percent in 1Q12.
- The second most common category in Morocco in 2Q12 was Miscellaneous Trojans. It affected 29.7 percent of all computers with detections there, up from 29.3 percent in 1Q12.
- The third most common category in Morocco in 2Q12 was Miscellaneous Potentially Unwanted Software, which affected 29.0 percent of all computers with detections there, down from 34.8 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Morocco in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Sality	Viruses	15.6%
2	Win32/Yeltminky	Worms	13.9%
3	Win32/Autorun	Worms	11.1%
4	Win32/Dorkbot	Worms	10.5%
5	Win32/Keygen	Misc. Potentially Unwanted Software	10.0%
6	Win32/Ramnit	Misc. Trojans	7.5%
7	Win32/Mabezat	Viruses	6.4%
8	Win32/Hotbar	Adware	5.9%
9	Win32/CplLnk	Exploits	5.0%
10	Win32/Vobfus	Worms	5.0%

- The most common threat family in Morocco in 2Q12 was [Win32/Sality](#), which affected 15.6 percent of computers with detections in Morocco. [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 in Morocco in 2Q12 was [Win32/Yeltminky](#), which affected 13.9 percent of computers with detections in Morocco. [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 in Morocco in 2Q12 was [Win32/Autorun](#), which affected 11.1 percent of computers with detections in Morocco. [Win32/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 threat family in Morocco in 2Q12 was [Win32/Dorkbot](#), which affected 10.5 percent of computers with detections in Morocco. [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.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Morocco

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	4.43 (1.6)	1.72 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	6.29 (3.9)	3.43 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.02 (0.7)	0.21 (0.9)

Update service usage

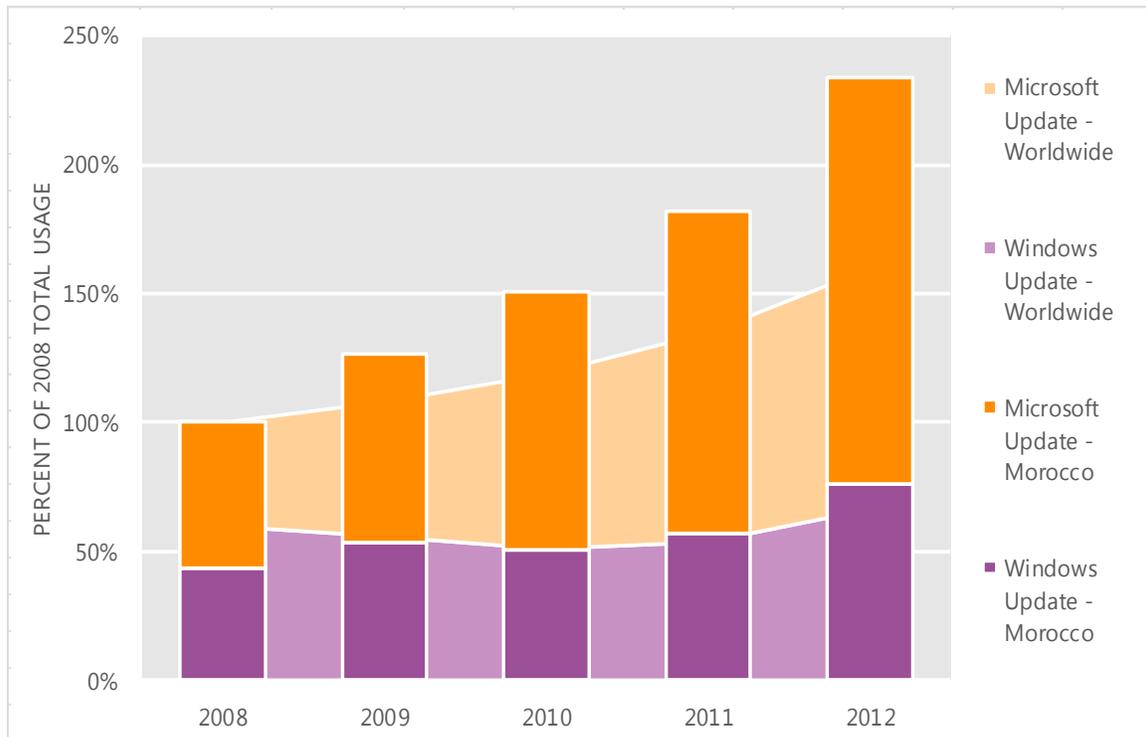
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Morocco and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Morocco over the last four years, indexed to the total usage for both services in Morocco in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Morocco was up 28.2 percent from 2011, and up 133.7 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Morocco in 2012, 67.4 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Nepal

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Nepal in 2Q12 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.

Infection rate statistics for Nepal

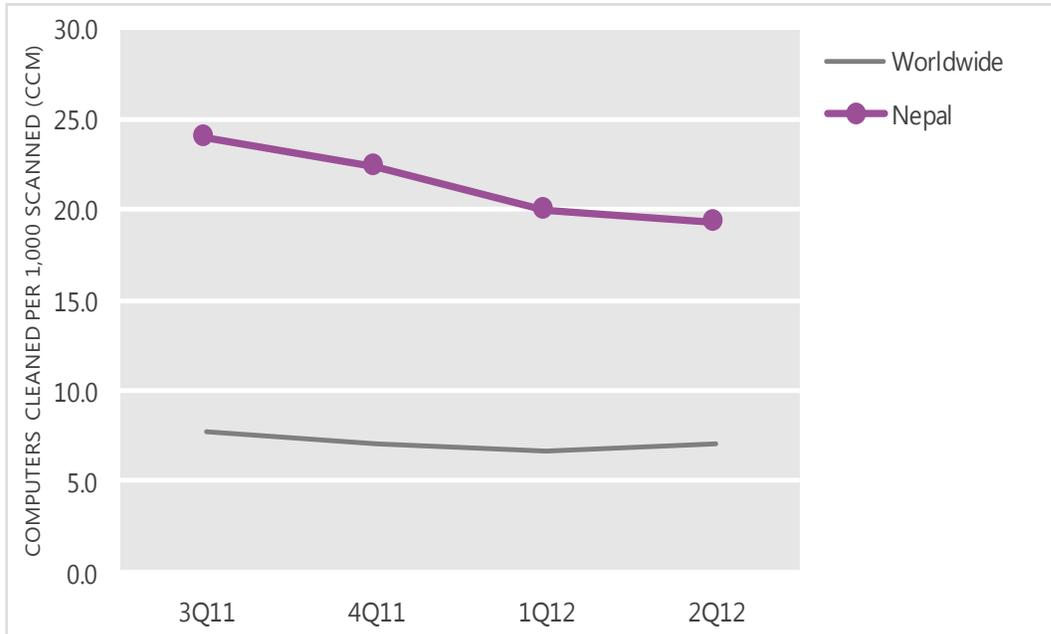
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	24.0	22.4	20.0	19.3
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

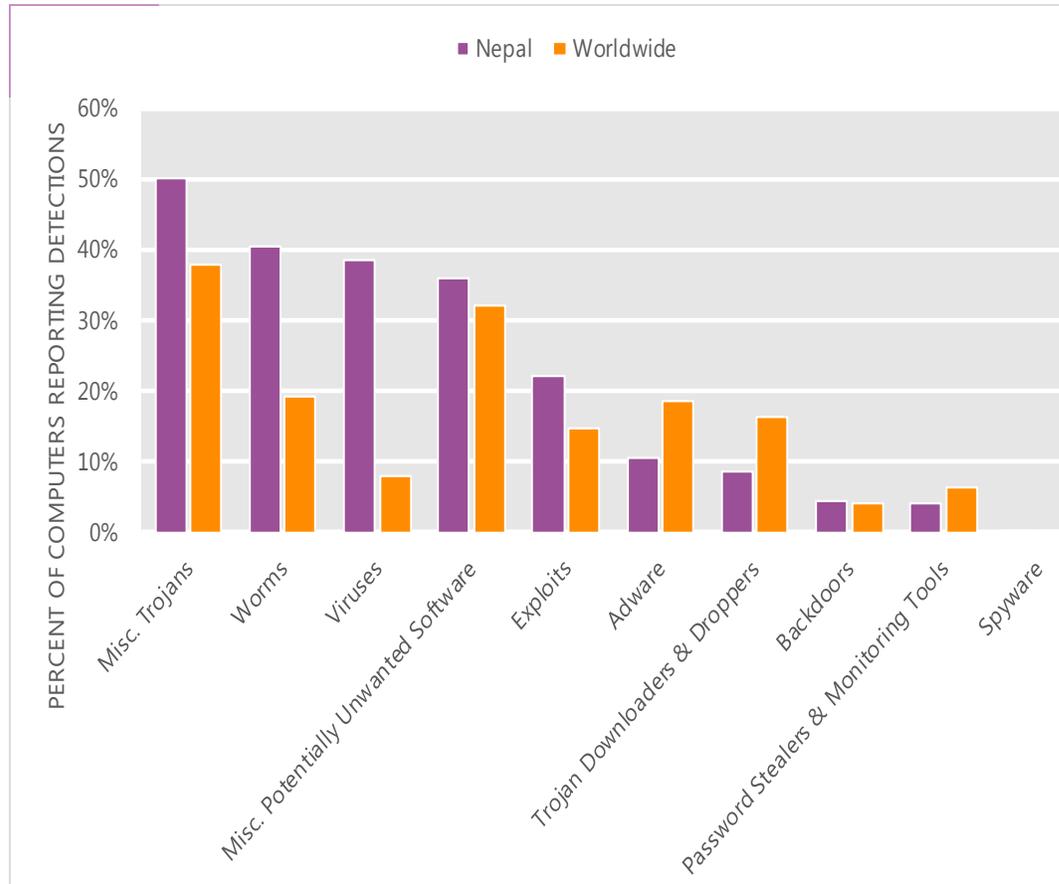
The MSRT detected malware on 19.3 of every 1,000 computers scanned in Nepal in 2Q12 (a CCM score of 19.3, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Nepal over the last four quarters, compared to the world as a whole.

CCM infection trends in Nepal and worldwide



Threat categories

Malware and potentially unwanted software categories in Nepal in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Nepal in 2Q12 was Miscellaneous Trojans. It affected 50.0 percent of all computers with detections there, down from 51.4 percent in 1Q12.
- The second most common category in Nepal in 2Q12 was Worms. It affected 40.4 percent of all computers with detections there, up from 40.3 percent in 1Q12.
- The third most common category in Nepal in 2Q12 was Viruses, which affected 38.5 percent of all computers with detections there, down from 39.3 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Nepal in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Ramnit	Misc. Trojans	29.2%
2	Win32/Autorun	Worms	24.8%
3	Win32/Sality	Viruses	24.1%
4	Win32/CplLnk	Exploits	19.5%
5	Win32/Virut	Viruses	15.4%
6	Win32/Finodes	Misc. Trojans	14.6%
7	Win32/Keygen	Misc. Potentially Unwanted Software	13.6%
8	Win32/Nuqel	Worms	9.5%
9	Win32/Rimecud	Worms	7.9%
10	Win32/Conficker	Worms	6.0%

- The most common threat family in Nepal in 2Q12 was [Win32/Ramnit](#), which affected 29.2 percent of computers with detections in Nepal. [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 in Nepal in 2Q12 was [Win32/Autorun](#), which affected 24.8 percent of computers with detections in Nepal. [Win32/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 threat family in Nepal in 2Q12 was [Win32/Sality](#), which affected 24.1 percent of computers with detections in Nepal. [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 in Nepal in 2Q12 was [Win32/CplLnk](#), which affected 19.5 percent of computers with detections in Nepal. [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.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Nepal

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	N/A (1.6)	N/A (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	N/A (3.9)	N/A (4.4)
Drive-by download per 1,000 URLs (Worldwide)	6.01 (0.7)	1.19 (0.9)

Update service usage

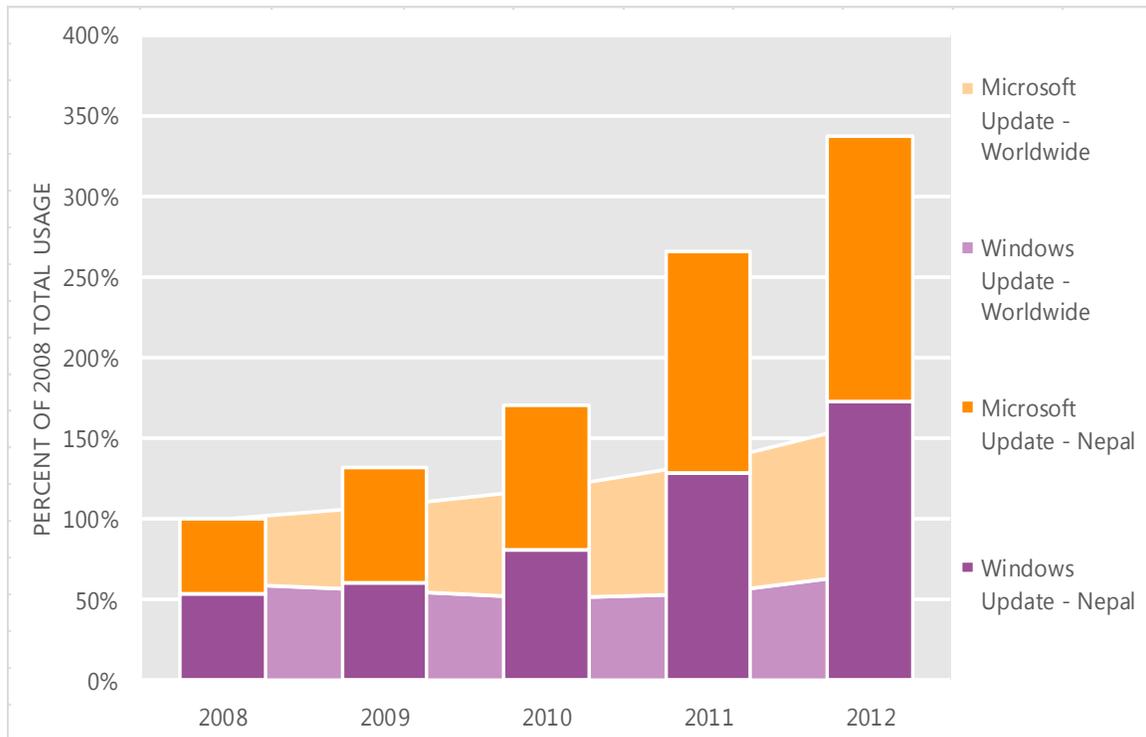
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Nepal and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Nepal over the last four years, indexed to the total usage for both services in Nepal in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Nepal was up 27.2 percent from 2011, and up 238.3 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Nepal in 2012, 48.9 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Netherlands

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in the Netherlands in 2Q12 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.

Infection rate statistics for the Netherlands

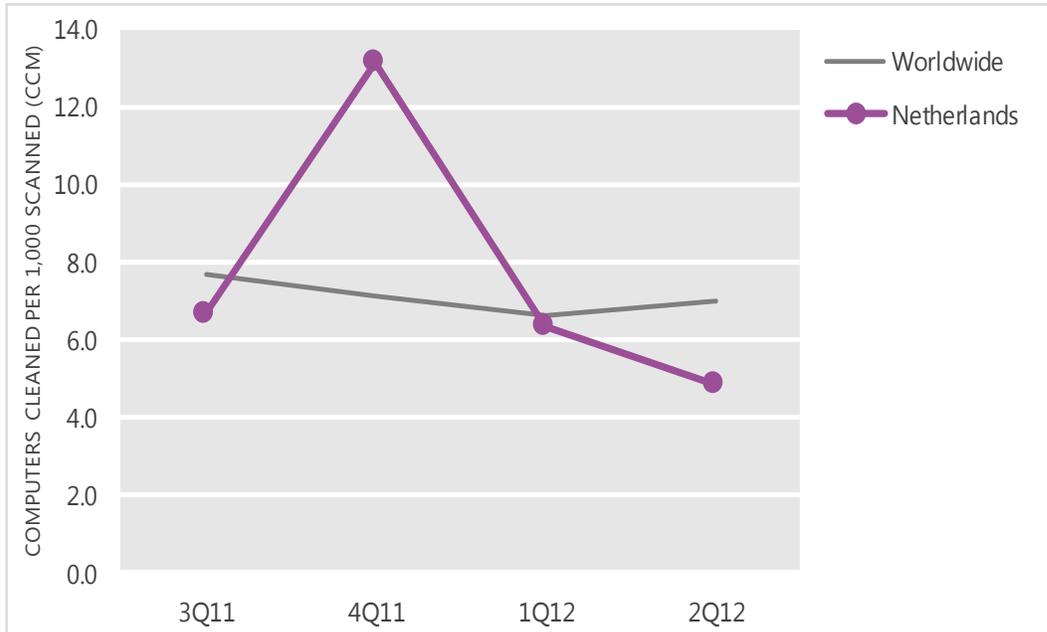
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	6.6	13.1	6.3	4.8
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

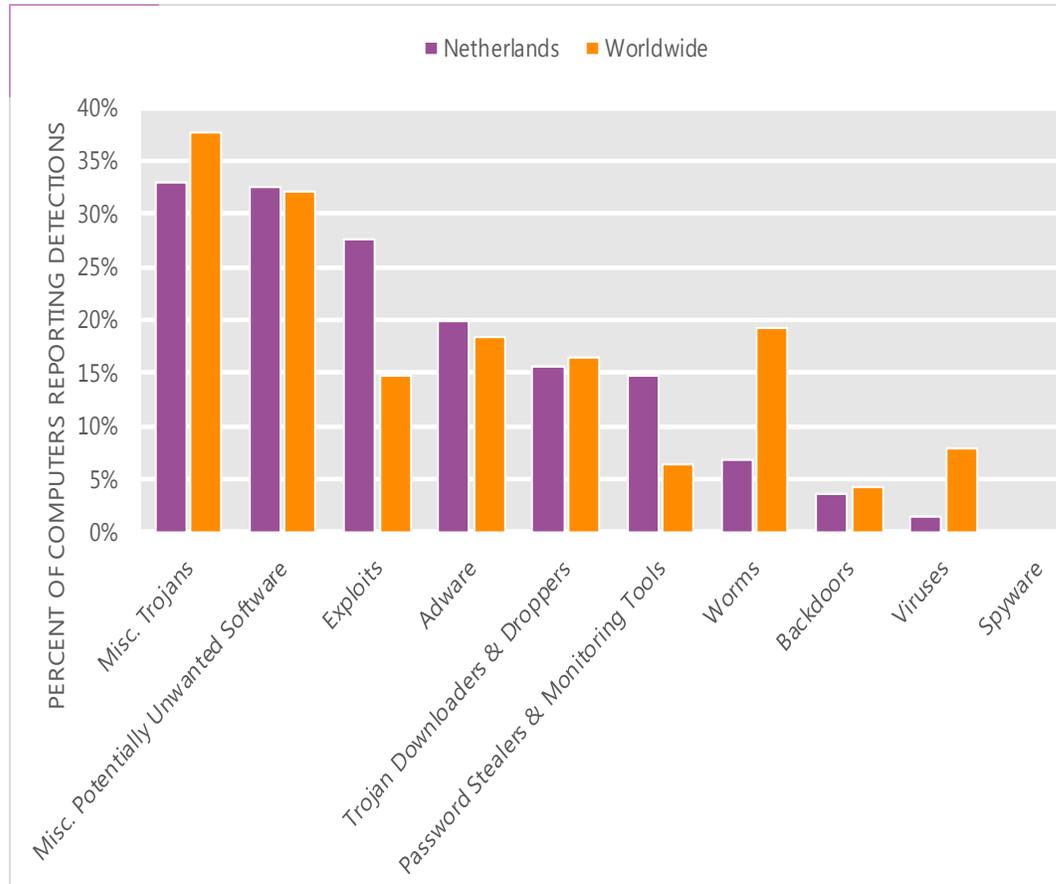
The MSRT detected malware on 4.8 of every 1,000 computers scanned in the Netherlands in 2Q12 (a CCM score of 4.8, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for the Netherlands over the last four quarters, compared to the world as a whole.

CCM infection trends in the Netherlands and worldwide



Threat categories

Malware and potentially unwanted software categories in the Netherlands in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in the Netherlands in 2Q12 was Miscellaneous Trojans. It affected 33.0 percent of all computers with detections there, up from 31.8 percent in 1Q12.
- The second most common category in the Netherlands in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 32.5 percent of all computers with detections there, up from 32.1 percent in 1Q12.
- The third most common category in the Netherlands in 2Q12 was Exploits, which affected 27.5 percent of all computers with detections there, up from 27.1 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in the Netherlands in 2Q12

	Family	Most significant category	% of computers with detections
1	Java/Blacole	Exploits	18.9%
2	Win32/Keygen	Misc. Potentially Unwanted Software	11.2%
3	Win32/Zbot	Password Stealers & Monitoring Tools	10.8%
4	JS/IframeRef	Misc. Trojans	8.9%
5	JS/Pornpop	Adware	8.8%
6	ASX/Wimad	Trojan Downloaders & Droppers	8.1%
7	JS/BlacoleRef	Misc. Trojans	7.4%
8	Win32/Hotbar	Adware	7.4%
9	Java/CVE-2012-0507	Exploits	6.3%
10	Win32/Obfuscator	Misc. Potentially Unwanted Software	6.3%

- The most common threat family in the Netherlands in 2Q12 was [Java/Blacole](#), which affected 18.9 percent of computers with detections in the Netherlands. [Java/Blacole](#) is an exploit pack, also known as Blackhole, that is installed on a compromised web server by an attacker and includes a number of exploits that target browser software. If a vulnerable computer browses a compromised website that contains the exploit pack, various malware may be downloaded and run.
- The second most common threat family in the Netherlands in 2Q12 was [Win32/Keygen](#), which affected 11.2 percent of computers with detections in the Netherlands. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The third most common threat family in the Netherlands in 2Q12 was [Win32/Zbot](#), which affected 10.8 percent of computers with detections in the Netherlands. [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 in the Netherlands in 2Q12 was [JS/IframeRef](#), which affected 8.9 percent of computers with detections in the Netherlands. [JS/IframeRef](#) is a generic detection for specially formed IFrame tags that point to remote websites that contain malicious content.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for the Netherlands

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	1.74 (1.6)	1.68 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	3.07 (3.9)	2.95 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	1.09 (0.7)	2.28 (0.9)

Update service usage

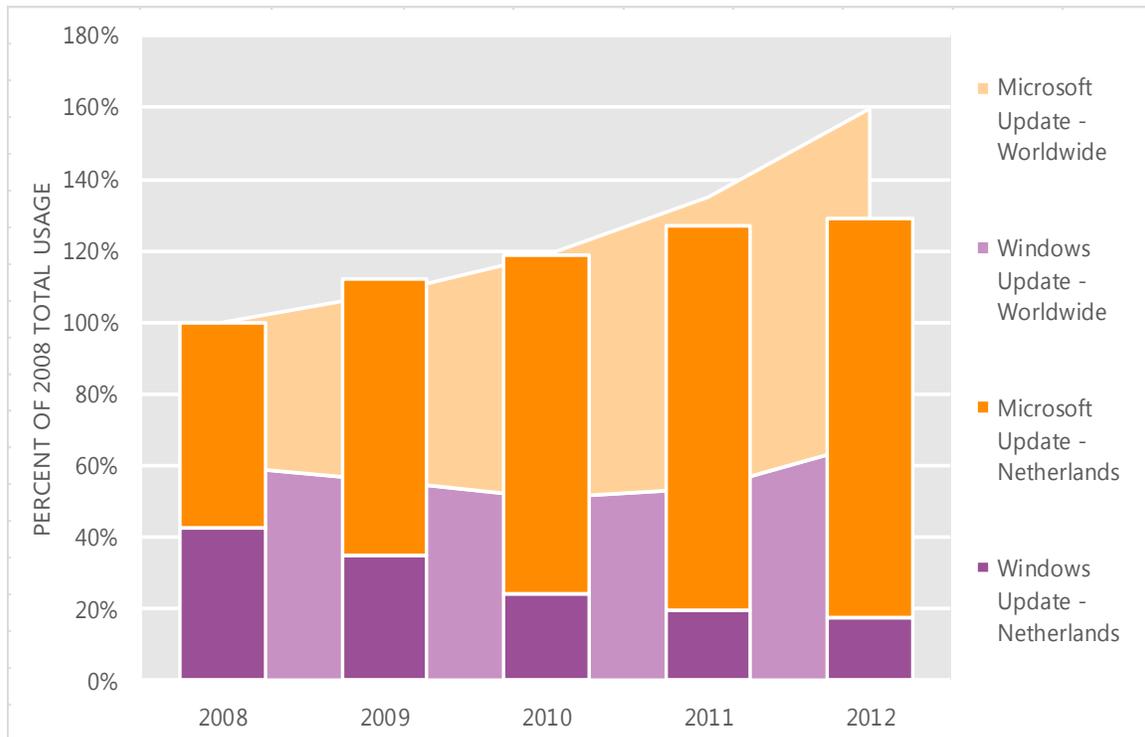
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in the Netherlands and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in the Netherlands over the last four years, indexed to the total usage for both services in the Netherlands in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in the Netherlands was up 1.6 percent from 2011, and up 29.2 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in the Netherlands in 2012, 86.6 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

New Zealand

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in New Zealand in 2Q12 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.

Infection rate statistics for New Zealand

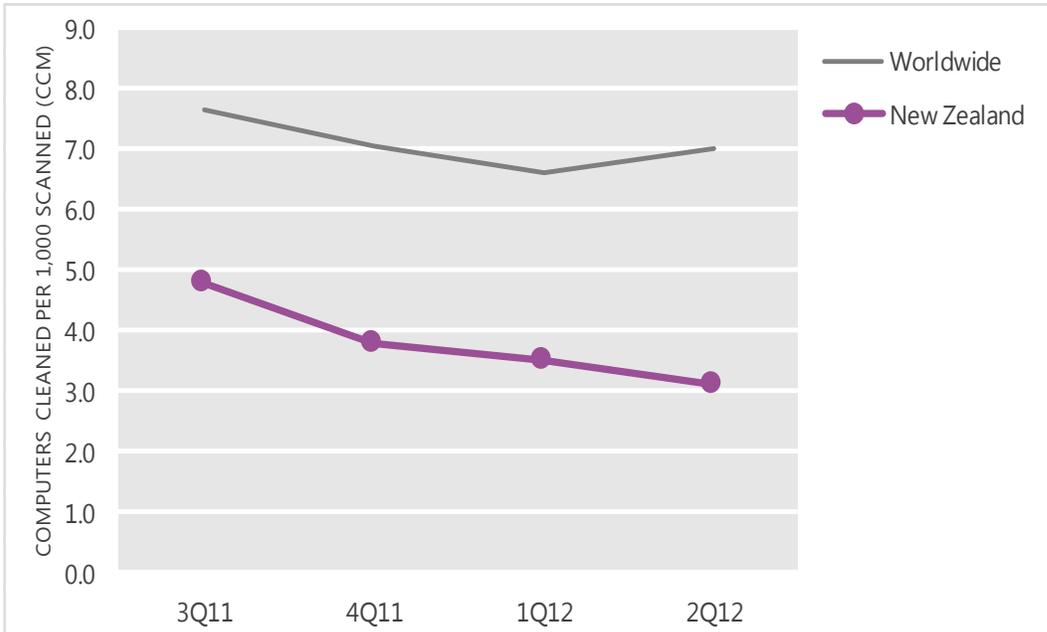
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	4.8	3.8	3.5	3.1
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

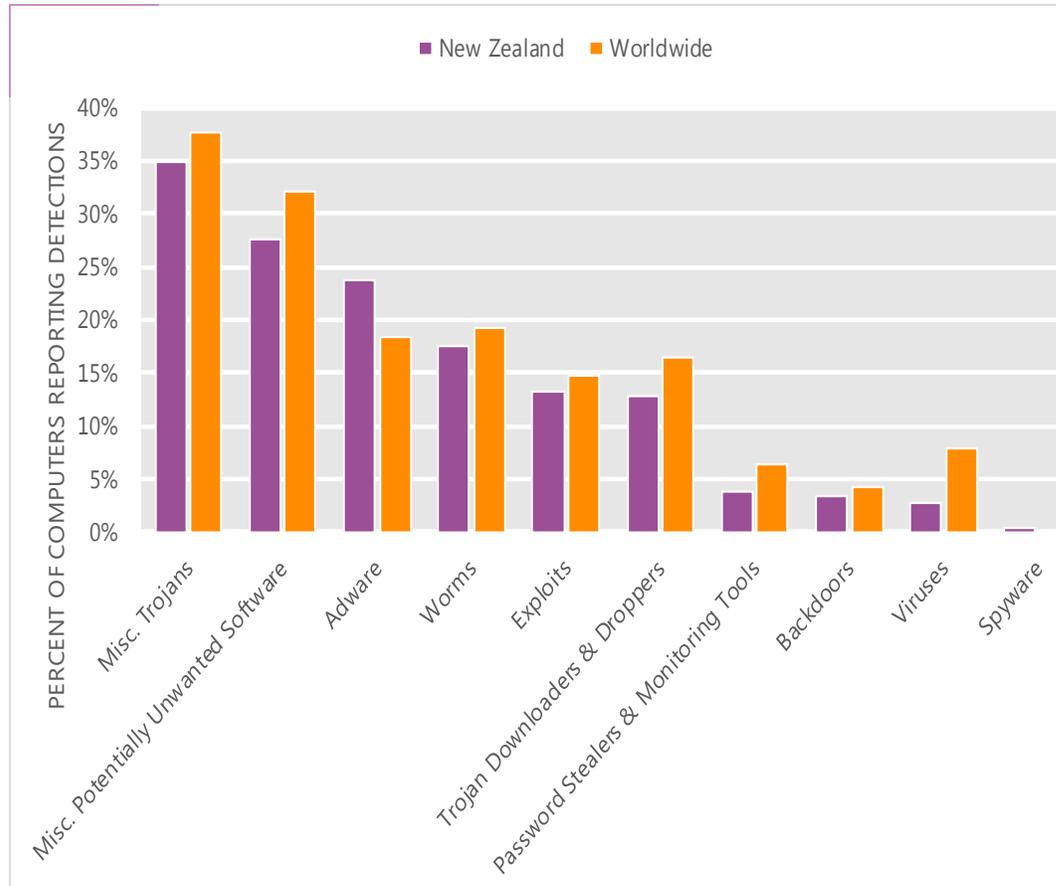
The MSRT detected malware on 3.1 of every 1,000 computers scanned in New Zealand in 2Q12 (a CCM score of 3.1, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for New Zealand over the last four quarters, compared to the world as a whole.

CCM infection trends in New Zealand and worldwide



Threat categories

Malware and potentially unwanted software categories in New Zealand in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in New Zealand in 2Q12 was Miscellaneous Trojans. It affected 34.9 percent of all computers with detections there, up from 32.9 percent in 1Q12.
- The second most common category in New Zealand in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 27.6 percent of all computers with detections there, up from 27.2 percent in 1Q12.
- The third most common category in New Zealand in 2Q12 was Adware, which affected 23.6 percent of all computers with detections there, down from 30.7 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in New Zealand in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Hotbar	Adware	9.8%
2	Win32/FakePAV	Misc. Trojans	8.5%
3	JS/Pornpop	Adware	8.5%
4	Win32/Keygen	Misc. Potentially Unwanted Software	7.9%
5	Win32/Autorun	Worms	6.5%
6	Java/Blacole	Exploits	5.8%
7	ASX/Wimad	Trojan Downloaders & Droppers	5.6%
8	JS/IframeRef	Misc. Trojans	4.9%
9	Win32/Vobfus	Worms	4.9%
10	Win32/Zwangi	Misc. Potentially Unwanted Software	4.0%

- The most common threat family in New Zealand in 2Q12 was [Win32/Hotbar](#), which affected 9.8 percent of computers with detections in New Zealand. [Win32/Hotbar](#) is adware that displays a dynamic toolbar and targeted pop-up ads based on its monitoring of web-browsing activity.
- The second most common threat family in New Zealand in 2Q12 was [Win32/FakePAV](#), which affected 8.5 percent of computers with detections in New Zealand. [Win32/FakePAV](#) is a rogue security software family that often masquerades as Microsoft Security Essentials or other legitimate antimalware products.
- The third most common threat family in New Zealand in 2Q12 was [JS/Pornpop](#), which affected 8.5 percent of computers with detections in New Zealand. [JS/Pornpop](#) is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The fourth most common threat family in New Zealand in 2Q12 was [Win32/Keygen](#), which affected 7.9 percent of computers with detections in New Zealand. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for New Zealand

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	0.92 (1.6)	0.69 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	1.58 (3.9)	1.92 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.78 (0.7)	0.08 (0.9)

Update service usage

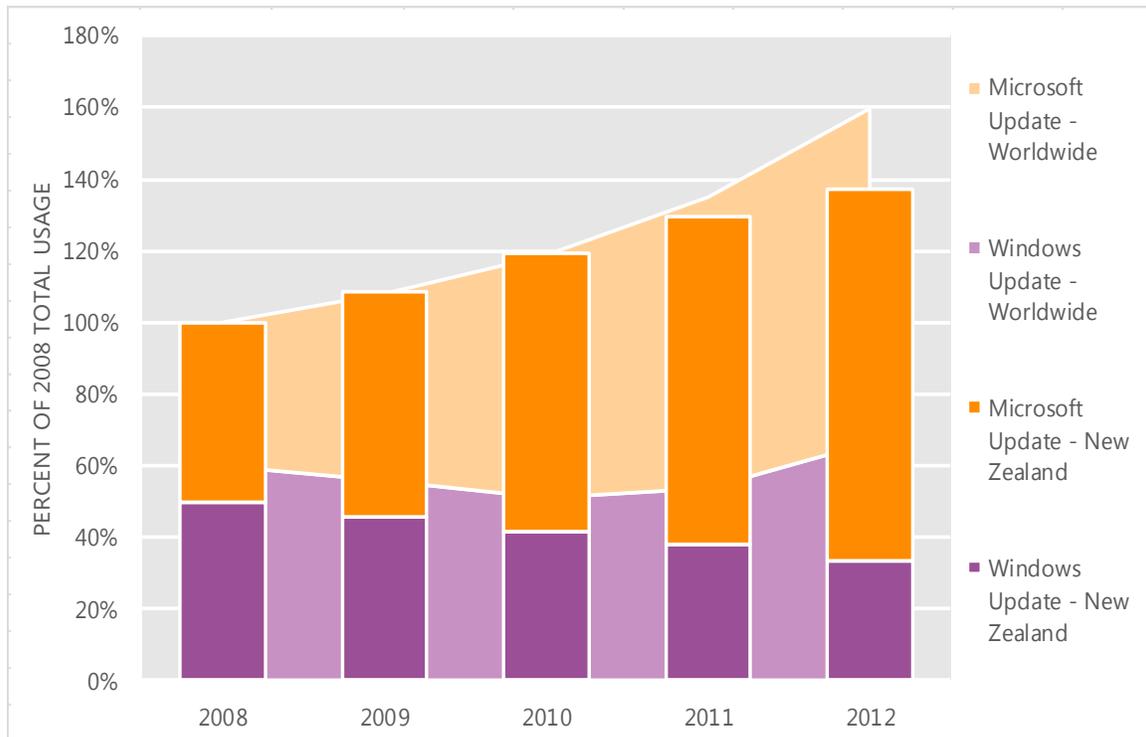
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in New Zealand and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in New Zealand over the last four years, indexed to the total usage for both services in New Zealand in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in New Zealand was up 6.1 percent from 2011, and up 37.3 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in New Zealand in 2012, 75.6 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Nicaragua

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Nicaragua in 2Q12 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.

Infection rate statistics for Nicaragua

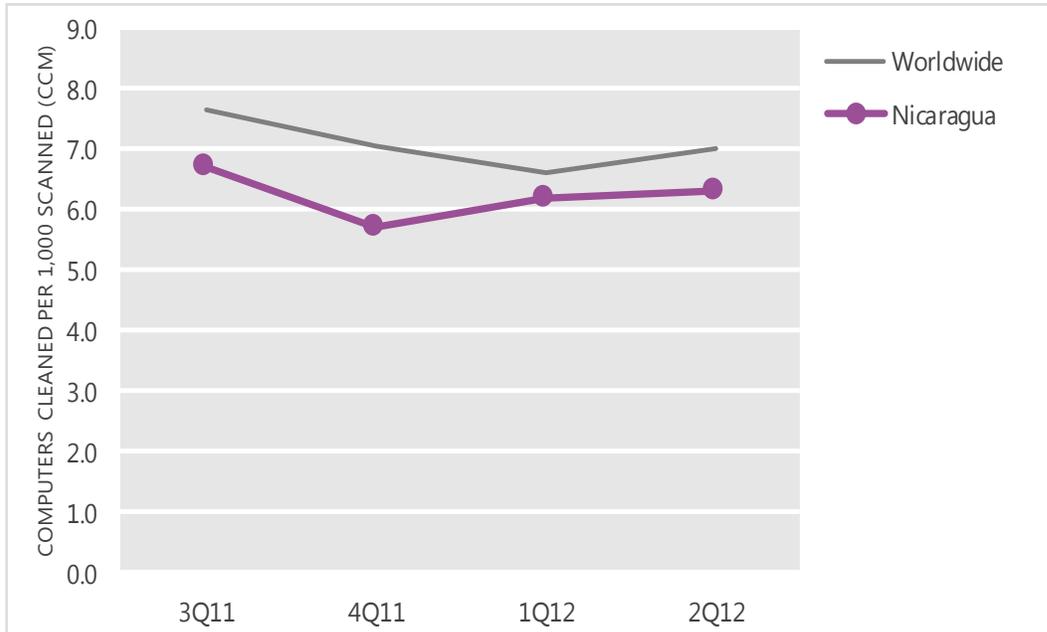
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	6.7	5.7	6.2	6.3
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

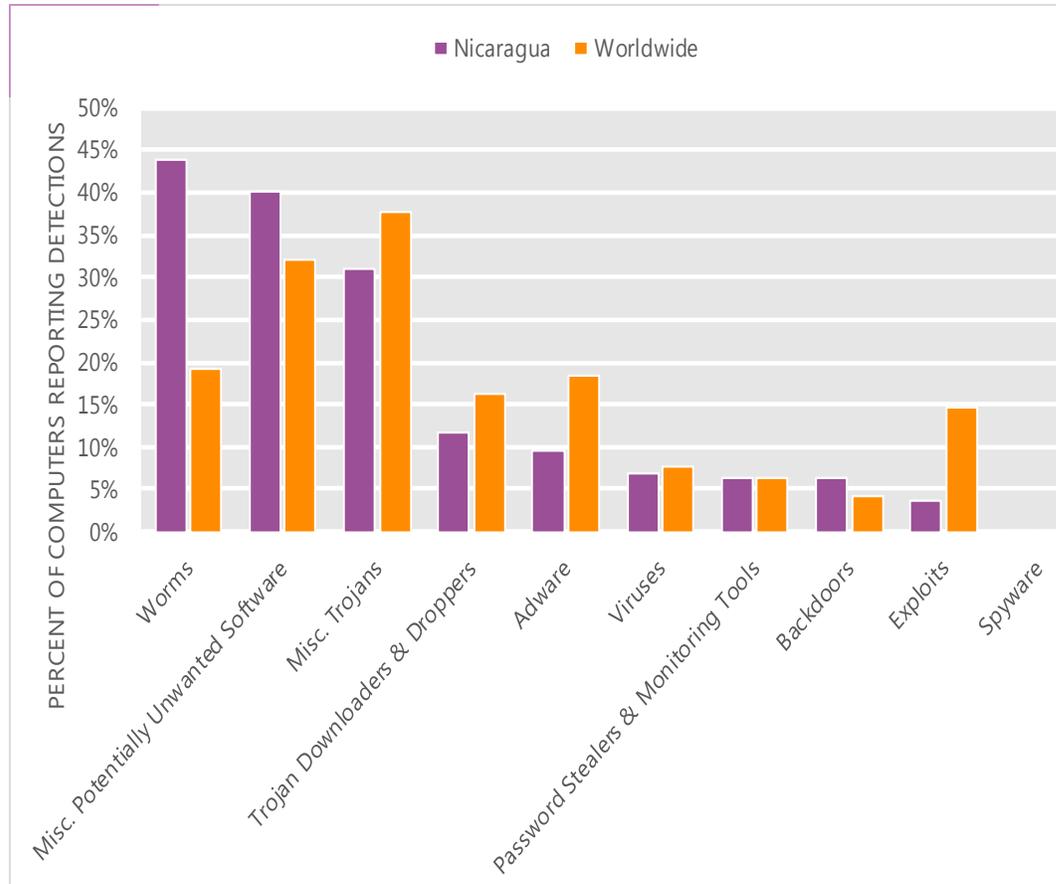
The MSRT detected malware on 6.3 of every 1,000 computers scanned in Nicaragua in 2Q12 (a CCM score of 6.3, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Nicaragua over the last four quarters, compared to the world as a whole.

CCM infection trends in Nicaragua and worldwide



Threat categories

Malware and potentially unwanted software categories in Nicaragua in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Nicaragua in 2Q12 was Worms. It affected 44.0 percent of all computers with detections there, up from 41.7 percent in 1Q12.
- The second most common category in Nicaragua in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 40.2 percent of all computers with detections there, down from 44.8 percent in 1Q12.
- The third most common category in Nicaragua in 2Q12 was Miscellaneous Trojans, which affected 30.9 percent of all computers with detections there, up from 28.6 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Nicaragua in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Dorkbot	Worms	24.3%
2	Win32/Keygen	Misc. Potentially Unwanted Software	17.9%
3	Win32/Autorun	Worms	9.6%
4	Win32/Conficker	Worms	7.5%
5	Win32/Vobfus	Worms	6.7%
6	Win32/VBInject	Misc. Potentially Unwanted Software	6.2%
7	Win32/Rimecud	Worms	5.5%
8	Win32/Yeltminky	Worms	4.6%
9	Win32/Sality	Viruses	4.0%
10	Win32/Wpakill	Misc. Potentially Unwanted Software	3.8%

- The most common threat family in Nicaragua in 2Q12 was [Win32/Dorkbot](#), which affected 24.3 percent of computers with detections in Nicaragua. [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 second most common threat family in Nicaragua in 2Q12 was [Win32/Keygen](#), which affected 17.9 percent of computers with detections in Nicaragua. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The third most common threat family in Nicaragua in 2Q12 was [Win32/Autorun](#), which affected 9.6 percent of computers with detections in Nicaragua. [Win32/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 threat family in Nicaragua in 2Q12 was [Win32/Conficker](#), which affected 7.5 percent of computers with detections in Nicaragua. [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.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Nicaragua

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	N/A (1.6)	N/A (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	N/A (3.9)	N/A (4.4)
Drive-by download per 1,000 URLs (Worldwide)	N/A (0.7)	N/A (0.9)

Update service usage

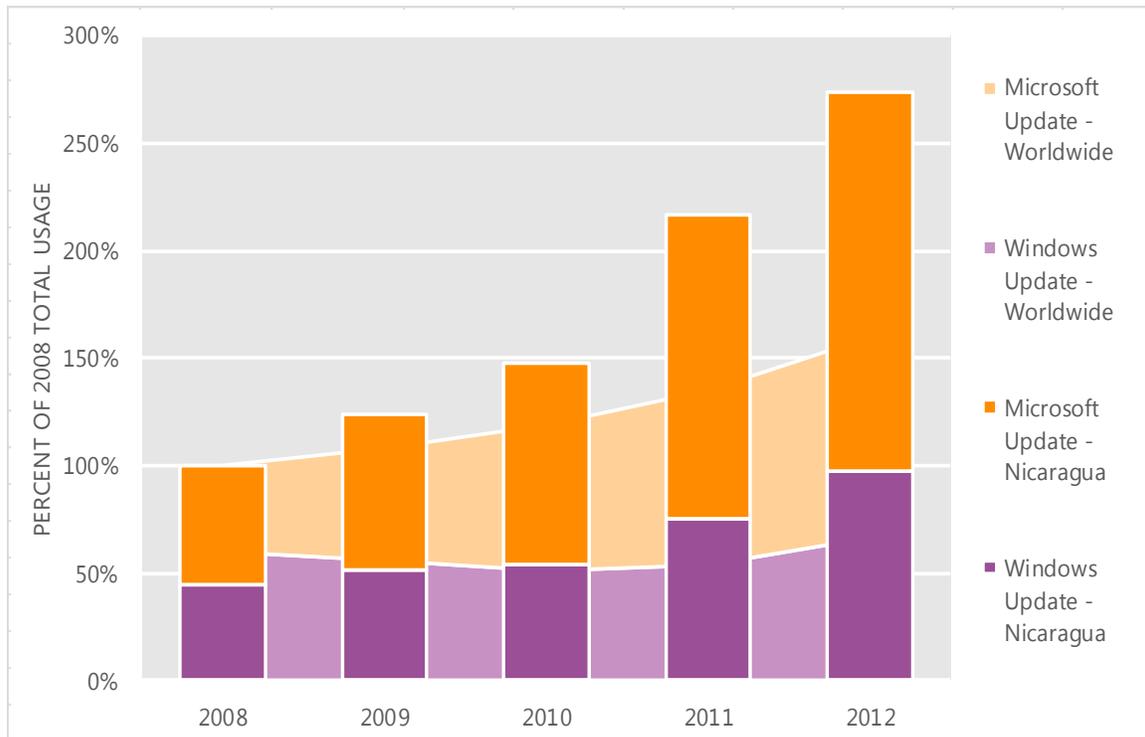
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Nicaragua and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Nicaragua over the last four years, indexed to the total usage for both services in Nicaragua in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Nicaragua was up 26.3 percent from 2011, and up 173.5 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Nicaragua in 2012, 64.3 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Nigeria

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Nigeria in 2Q12 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.

Infection rate statistics for Nigeria

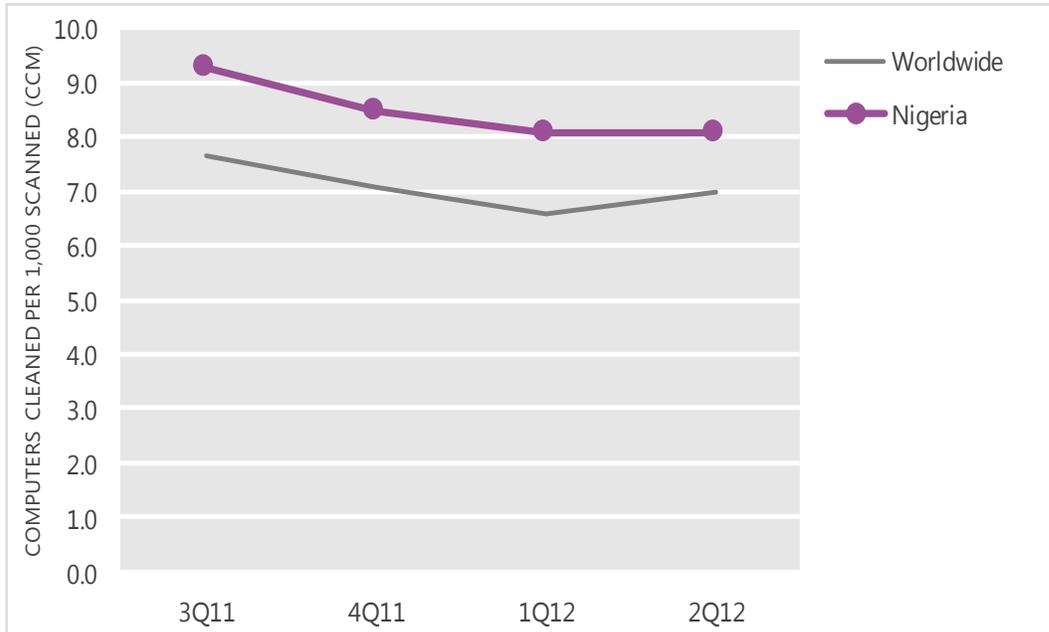
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	9.3	8.5	8.1	8.1
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

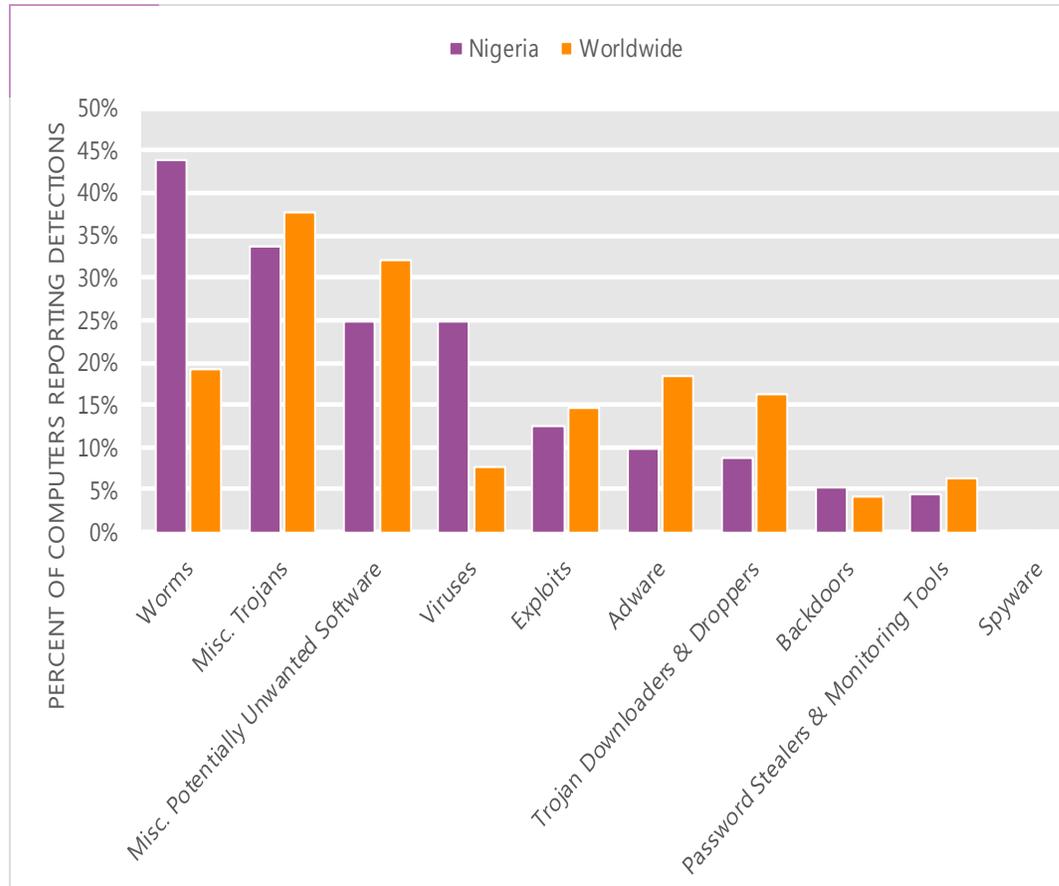
The MSRT detected malware on 8.1 of every 1,000 computers scanned in Nigeria in 2Q12 (a CCM score of 8.1, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Nigeria over the last four quarters, compared to the world as a whole.

CCM infection trends in Nigeria and worldwide



Threat categories

Malware and potentially unwanted software categories in Nigeria in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Nigeria in 2Q12 was Worms. It affected 43.8 percent of all computers with detections there, down from 45.2 percent in 1Q12.
- The second most common category in Nigeria in 2Q12 was Miscellaneous Trojans. It affected 33.8 percent of all computers with detections there, up from 31.0 percent in 1Q12.
- The third most common category in Nigeria in 2Q12 was Miscellaneous Potentially Unwanted Software, which affected 24.9 percent of all computers with detections there, up from 23.2 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Nigeria in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Vobfus	Worms	16.6%
2	Win32/Autorun	Worms	16.6%
3	Win32/Sality	Viruses	13.7%
4	Win32/Rimecud	Worms	10.4%
5	Win32/Ramnit	Misc. Trojans	9.8%
6	Win32/CplLnk	Exploits	9.8%
7	Win32/Virut	Viruses	9.6%
8	Win32/Conficker	Worms	7.9%
9	Win32/Keygen	Misc. Potentially Unwanted Software	6.0%
10	Win32/Dorkbot	Worms	5.7%

- The most common threat family in Nigeria in 2Q12 was [Win32/Vobfus](#), which affected 16.6 percent of computers with detections in Nigeria. [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 second most common threat family in Nigeria in 2Q12 was [Win32/Autorun](#), which affected 16.6 percent of computers with detections in Nigeria. [Win32/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 threat family in Nigeria in 2Q12 was [Win32/Sality](#), which affected 13.7 percent of computers with detections in Nigeria. [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 in Nigeria in 2Q12 was [Win32/Rimecud](#), which affected 10.4 percent of computers with detections in Nigeria. [Win32/Rimecud](#) is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Nigeria

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	N/A (1.6)	1.57 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	1.57 (3.9)	4.71 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	N/A (0.7)	0.04 (0.9)

Update service usage

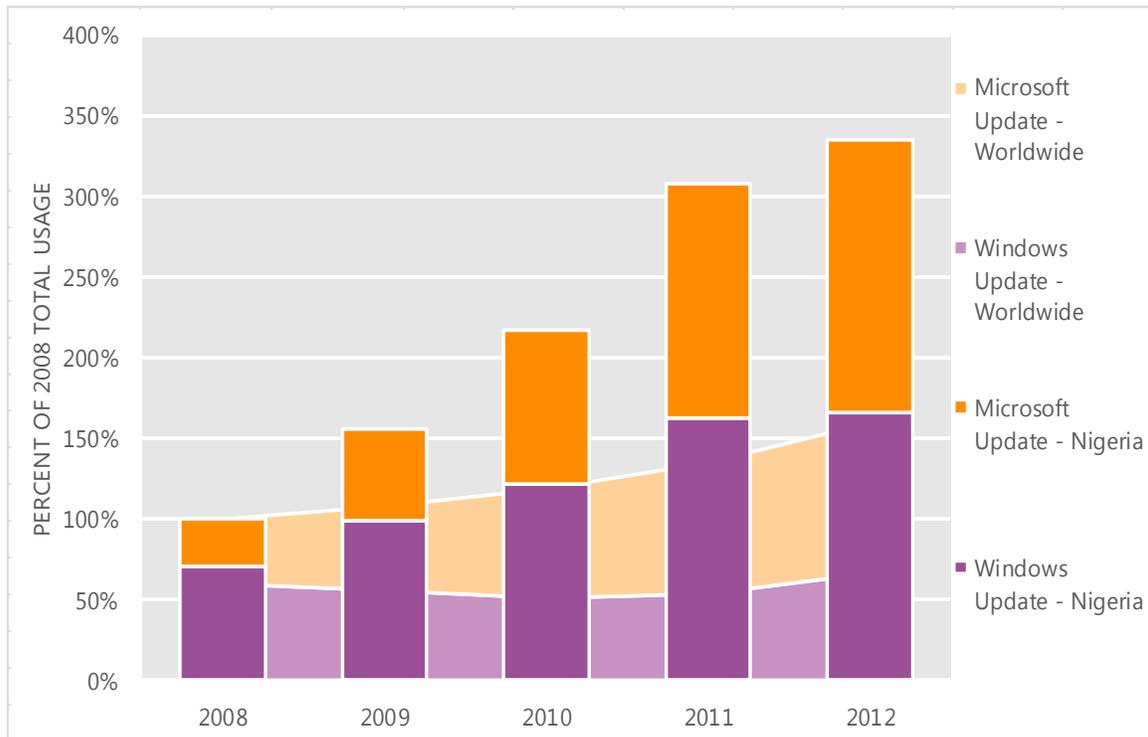
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Nigeria and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Nigeria over the last four years, indexed to the total usage for both services in Nigeria in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Nigeria was up 8.9 percent from 2011, and up 235.8 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Nigeria in 2012, 50.4 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Norway

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Norway in 2Q12 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.

Infection rate statistics for Norway

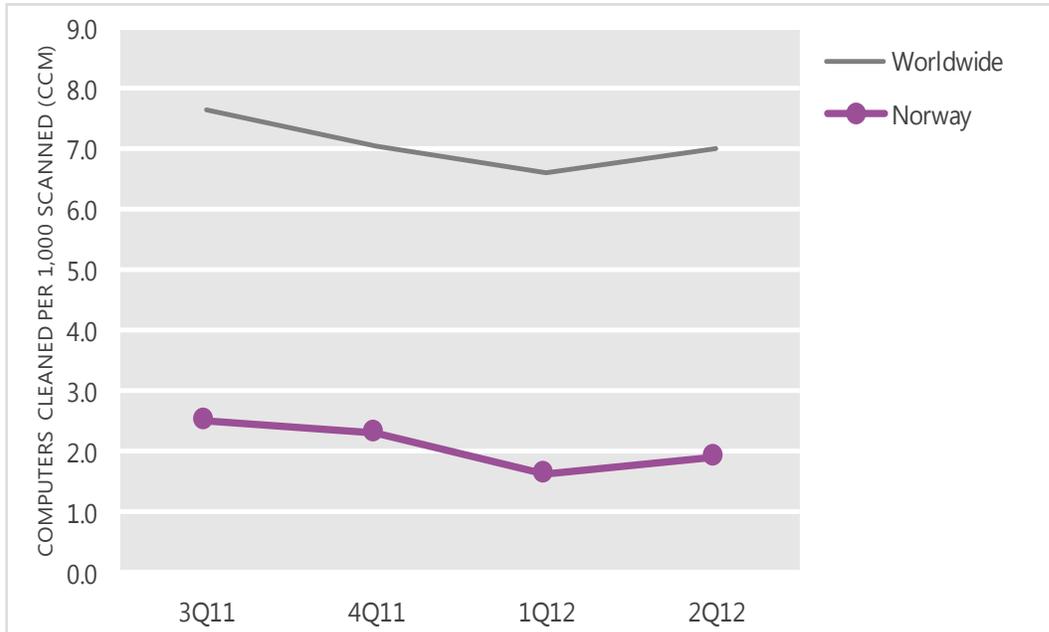
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	2.5	2.3	1.6	1.9
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

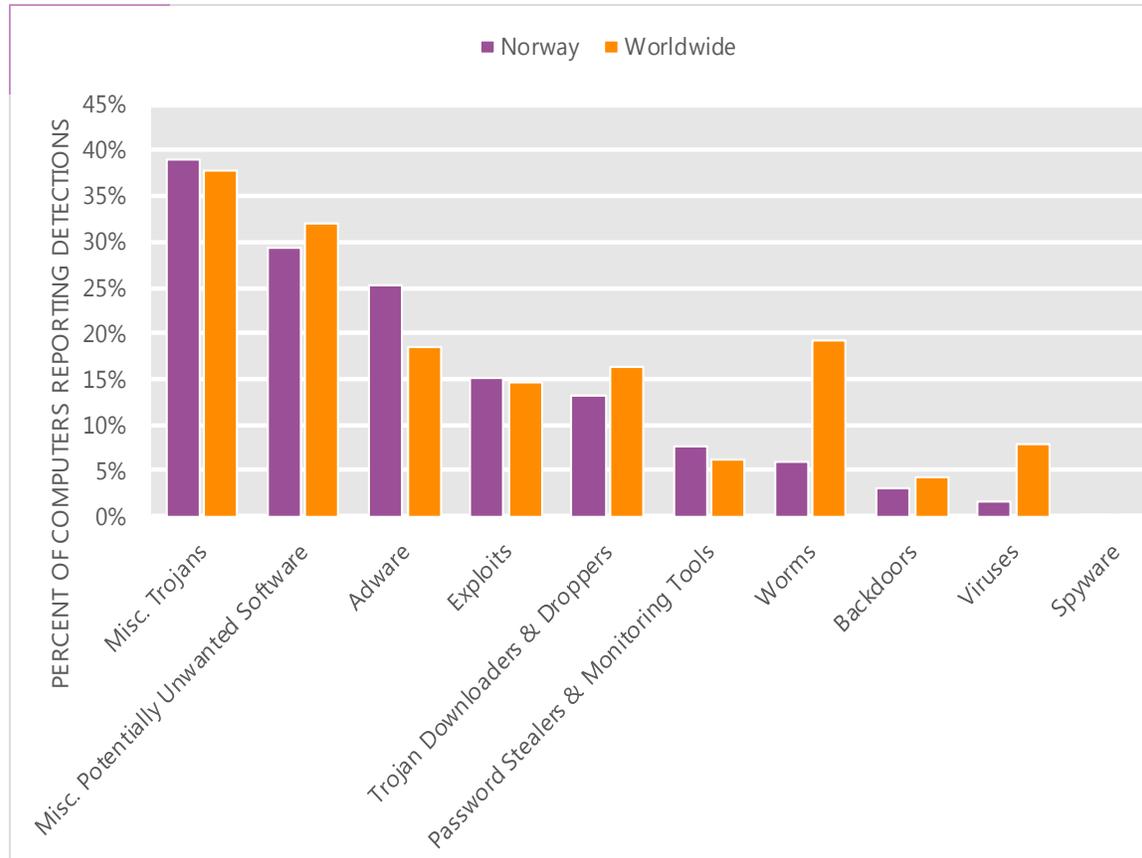
The MSRT detected malware on 1.9 of every 1,000 computers scanned in Norway in 2Q12 (a CCM score of 1.9, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Norway over the last four quarters, compared to the world as a whole.

CCM infection trends in Norway and worldwide



Threat categories

Malware and potentially unwanted software categories in Norway in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Norway in 2Q12 was Miscellaneous Trojans. It affected 39.0 percent of all computers with detections there, up from 31.6 percent in 1Q12.
- The second most common category in Norway in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 29.2 percent of all computers with detections there, down from 31.3 percent in 1Q12.
- The third most common category in Norway in 2Q12 was Adware, which affected 25.2 percent of all computers with detections there, down from 35.0 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Norway in 2Q12

	Family	Most significant category	% of computers with detections
1	JS/Pornpop	Adware	11.4%
2	Win32/Keygen	Misc. Potentially Unwanted Software	10.3%
3	Win32/Hotbar	Adware	9.2%
4	Win32/FakePAV	Misc. Trojans	8.7%
5	Win32/Winwebsec	Misc. Trojans	7.1%
6	ASX/Wimad	Trojan Downloaders & Droppers	6.6%
7	JS/IframeRef	Misc. Trojans	6.0%
8	JS/BlacoleRef	Misc. Trojans	5.6%
9	Java/CVE-2012-0507	Exploits	5.5%
10	Java/Blacole	Exploits	5.2%

- The most common threat family in Norway in 2Q12 was [JS/Pornpop](#), which affected 11.4 percent of computers with detections in Norway. [JS/Pornpop](#) is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The second most common threat family in Norway in 2Q12 was [Win32/Keygen](#), which affected 10.3 percent of computers with detections in Norway. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The third most common threat family in Norway in 2Q12 was [Win32/Hotbar](#), which affected 9.2 percent of computers with detections in Norway. [Win32/Hotbar](#) is adware that displays a dynamic toolbar and targeted pop-up ads based on its monitoring of web-browsing activity.
- The fourth most common threat family in Norway in 2Q12 was [Win32/FakePAV](#), which affected 8.7 percent of computers with detections in Norway. [Win32/FakePAV](#) is a rogue security software family that often masquerades as Microsoft Security Essentials or other legitimate antimalware products.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Norway

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	1.43 (1.6)	1.29 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	2.98 (3.9)	3.53 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.49 (0.7)	0.77 (0.9)

Update service usage

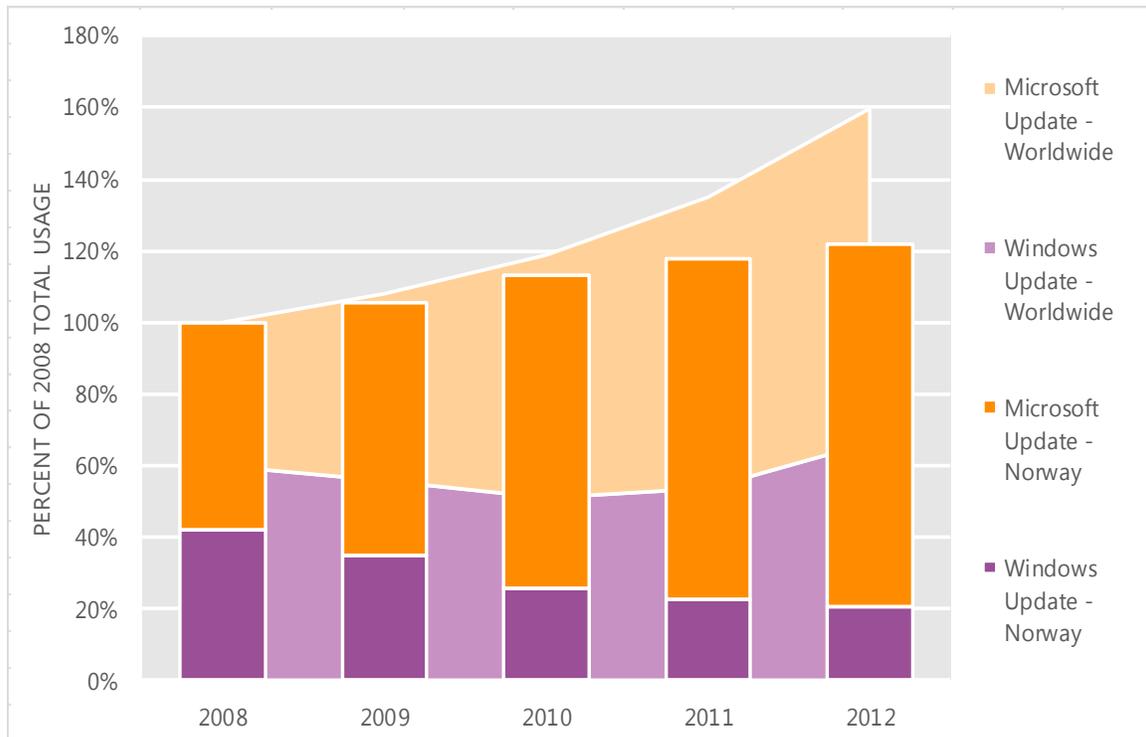
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Norway and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Norway over the last four years, indexed to the total usage for both services in Norway in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Norway was up 3.6 percent from 2011, and up 21.7 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Norway in 2012, 83.1 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Oman

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Oman in 2Q12 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.

Infection rate statistics for Oman

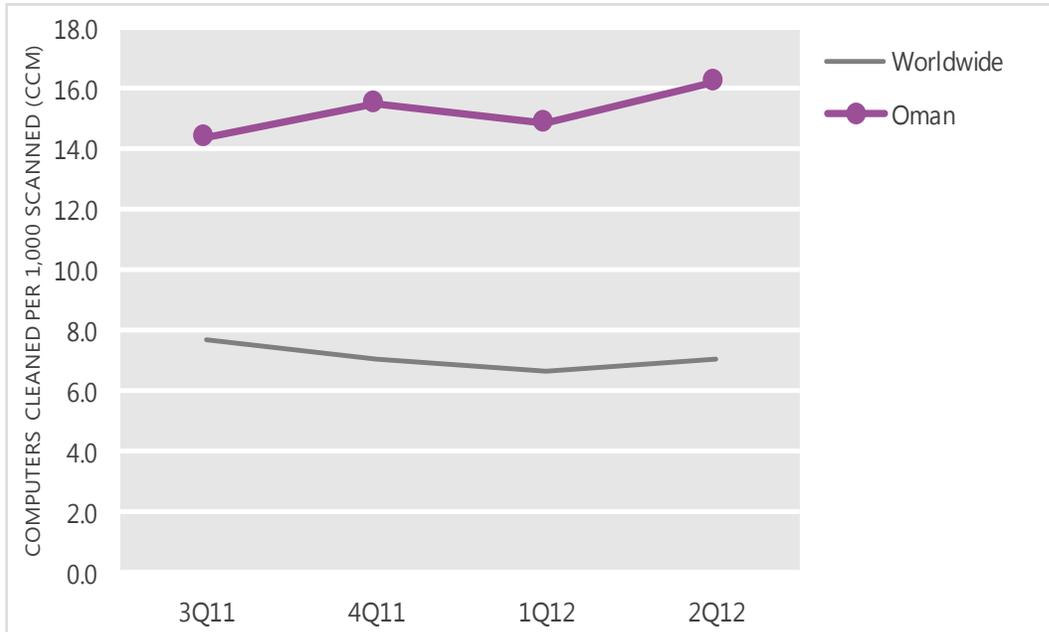
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	14.4	15.5	14.9	16.2
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

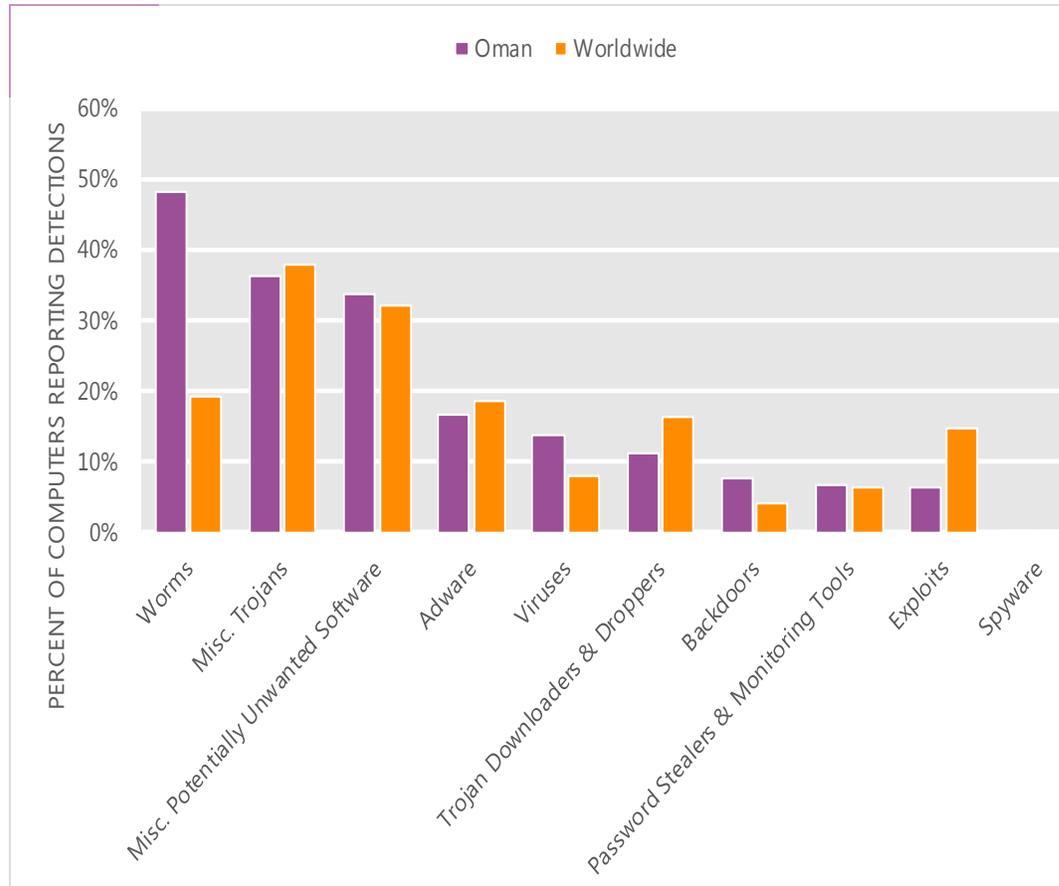
The MSRT detected malware on 16.2 of every 1,000 computers scanned in Oman in 2Q12 (a CCM score of 16.2, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Oman over the last four quarters, compared to the world as a whole.

CCM infection trends in Oman and worldwide



Threat categories

Malware and potentially unwanted software categories in Oman in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Oman in 2Q12 was Worms. It affected 48.1 percent of all computers with detections there, up from 46.0 percent in 1Q12.
- The second most common category in Oman in 2Q12 was Miscellaneous Trojans. It affected 36.2 percent of all computers with detections there, up from 35.9 percent in 1Q12.
- The third most common category in Oman in 2Q12 was Miscellaneous Potentially Unwanted Software, which affected 33.7 percent of all computers with detections there, up from 33.5 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Oman in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Vobfus	Worms	24.2%
2	Win32/Autorun	Worms	19.0%
3	Win32/Keygen	Misc. Potentially Unwanted Software	11.0%
4	JS/Paypopup	Adware	8.8%
5	Win32/Sality	Viruses	8.2%
6	Win32/Sirefef	Misc. Trojans	6.7%
7	Win32/Dorkbot	Worms	6.6%
8	Win32/Nuqel	Worms	6.6%
9	Win32/Agent	Misc. Trojans	4.8%
10	Win32/Gamarue	Worms	4.7%

- The most common threat family in Oman in 2Q12 was [Win32/Vobfus](#), which affected 24.2 percent of computers with detections in Oman. [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 second most common threat family in Oman in 2Q12 was [Win32/Autorun](#), which affected 19.0 percent of computers with detections in Oman. [Win32/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 threat family in Oman in 2Q12 was [Win32/Keygen](#), which affected 11.0 percent of computers with detections in Oman. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The fourth most common threat family in Oman in 2Q12 was [JS/Paypopup](#), which affected 8.8 percent of computers with detections in Oman. [JS/Paypopup](#) is a detection for specially-crafted JavaScript-enabled objects that attempt to display pop-up and pop-under advertisements in new browser windows.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Oman

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	2.23 (1.6)	0.28 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	1.95 (3.9)	1.95 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.00 (0.7)	0.00 (0.9)

Update service usage

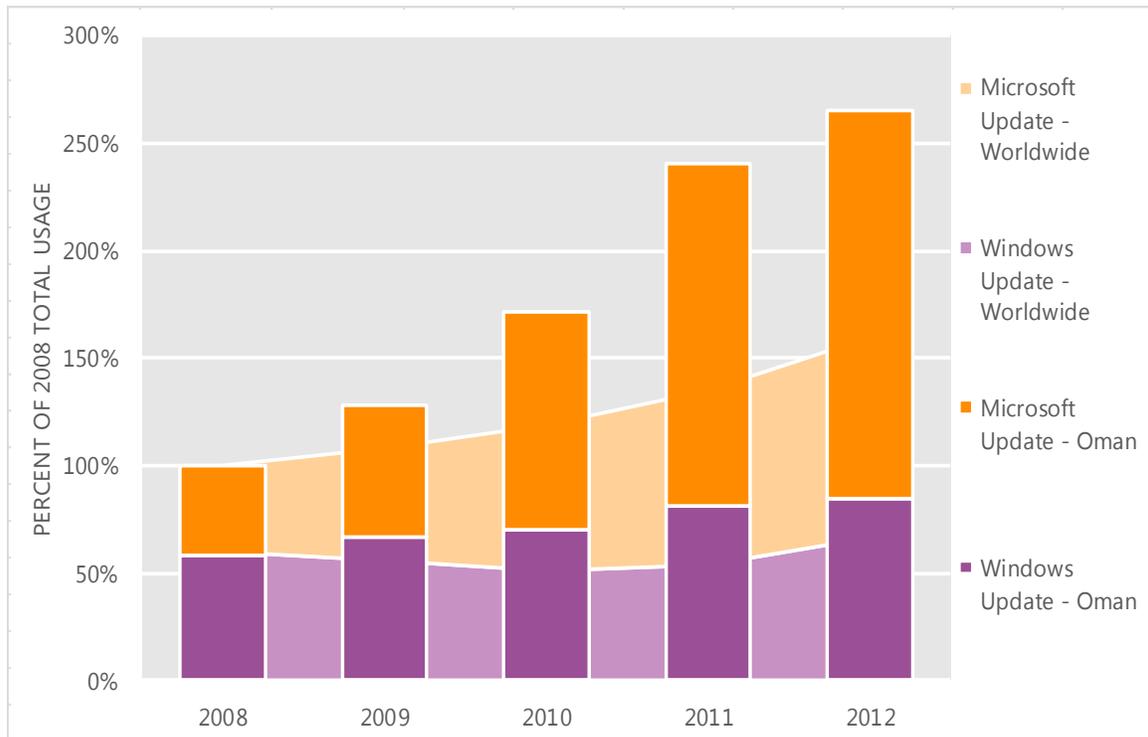
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Oman and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Oman over the last four years, indexed to the total usage for both services in Oman in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Oman was up 10.3 percent from 2011, and up 165.0 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Oman in 2012, 68.0 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Pakistan

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Pakistan in 2Q12 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.

Infection rate statistics for Pakistan

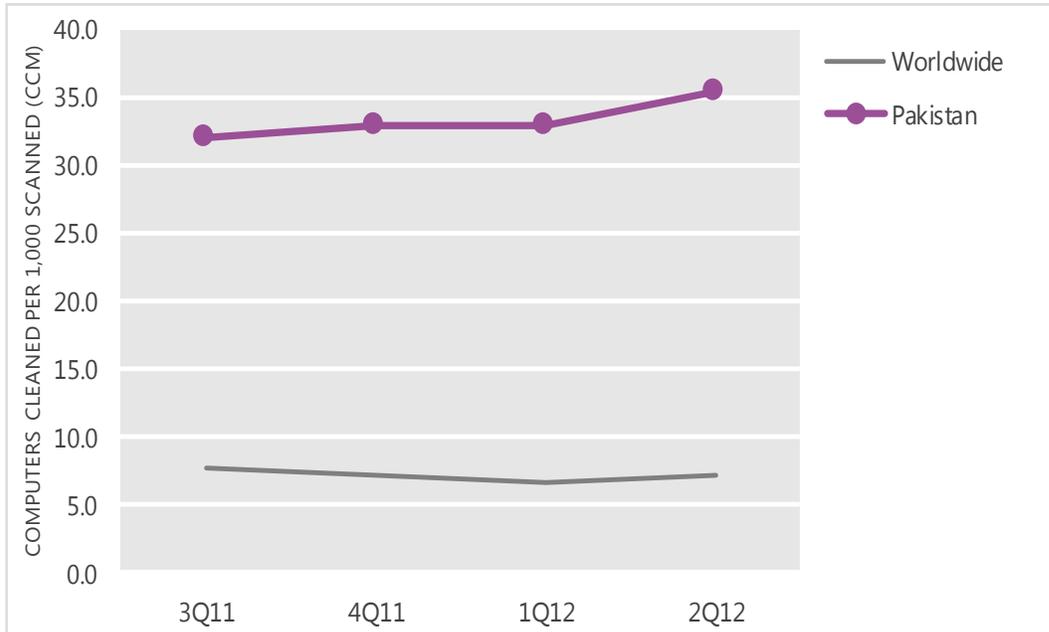
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	31.9	32.9	32.8	35.3
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

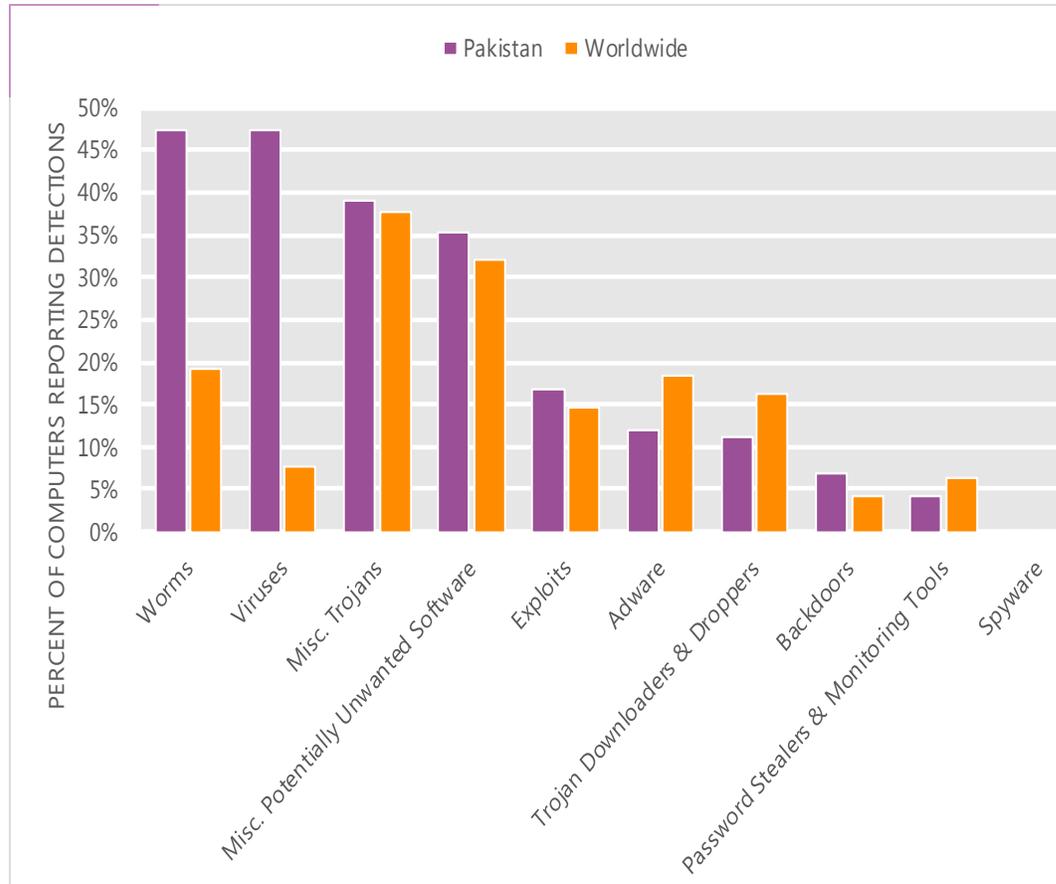
The MSRT detected malware on 35.3 of every 1,000 computers scanned in Pakistan in 2Q12 (a CCM score of 35.3, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Pakistan over the last four quarters, compared to the world as a whole.

CCM infection trends in Pakistan and worldwide



Threat categories

Malware and potentially unwanted software categories in Pakistan in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Pakistan in 2Q12 was Worms. It affected 47.4 percent of all computers with detections there, up from 43.5 percent in 1Q12.
- The second most common category in Pakistan in 2Q12 was Viruses. It affected 47.4 percent of all computers with detections there, down from 49.1 percent in 1Q12.
- The third most common category in Pakistan in 2Q12 was Miscellaneous Trojans, which affected 39.1 percent of all computers with detections there, down from 40.2 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Pakistan in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Sality	Viruses	30.1%
2	Win32/Autorun	Worms	29.0%
3	Win32/Ramnit	Misc. Trojans	20.1%
4	Win32/Virut	Viruses	15.1%
5	Win32/Keygen	Misc. Potentially Unwanted Software	13.2%
6	Win32/Chir	Worms	13.2%
7	Win32/CplLnk	Exploits	12.9%
8	Win32/VB	Worms	8.9%
9	Win32/Conficker	Worms	7.4%
10	Win32/Rimecud	Worms	6.8%

- The most common threat family in Pakistan in 2Q12 was [Win32/Sality](#), which affected 30.1 percent of computers with detections in Pakistan. [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 in Pakistan in 2Q12 was [Win32/Autorun](#), which affected 29.0 percent of computers with detections in Pakistan. [Win32/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 threat family in Pakistan in 2Q12 was [Win32/Ramnit](#), which affected 20.1 percent of computers with detections in Pakistan. [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 in Pakistan in 2Q12 was [Win32/Virut](#), which affected 15.1 percent of computers with detections in Pakistan. [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.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Pakistan

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	1.78 (1.6)	0.55 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	1.85 (3.9)	1.72 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.18 (0.7)	0.71 (0.9)

Update service usage

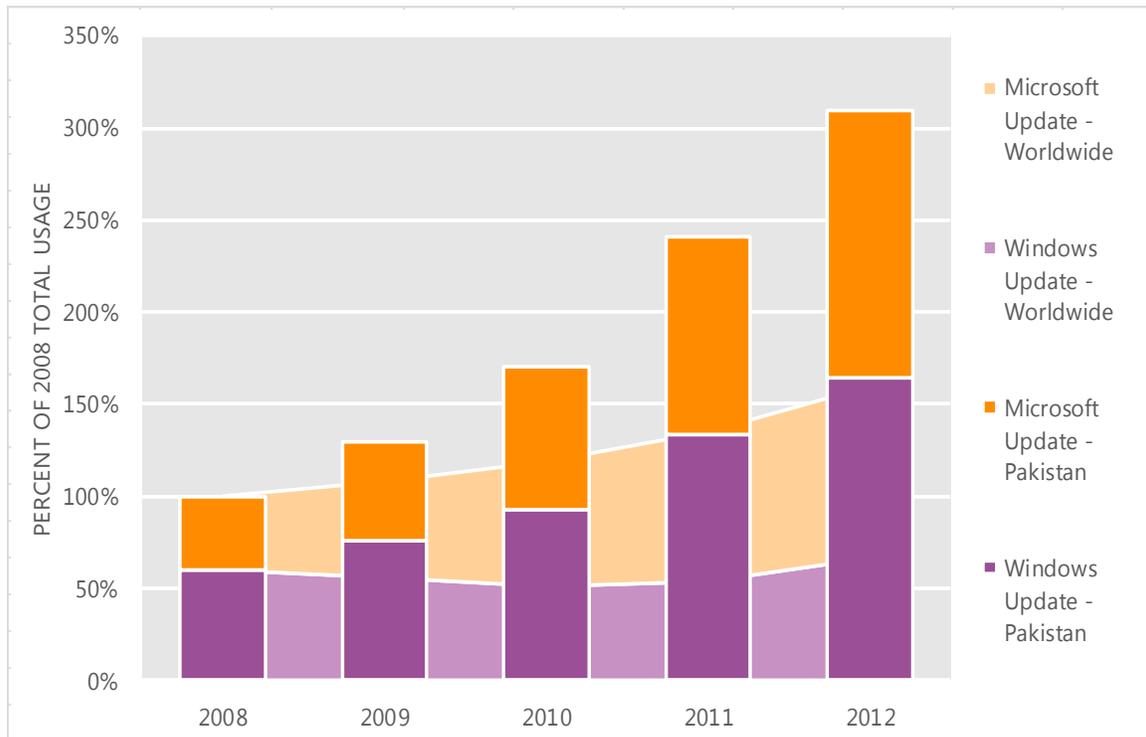
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Pakistan and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Pakistan over the last four years, indexed to the total usage for both services in Pakistan in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Pakistan was up 28.5 percent from 2011, and up 209.7 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Pakistan in 2012, 47.0 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Palestinian Authority

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

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 2Q12 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geo-location to determine country or region.

Infection rate statistics for the Palestinian territories

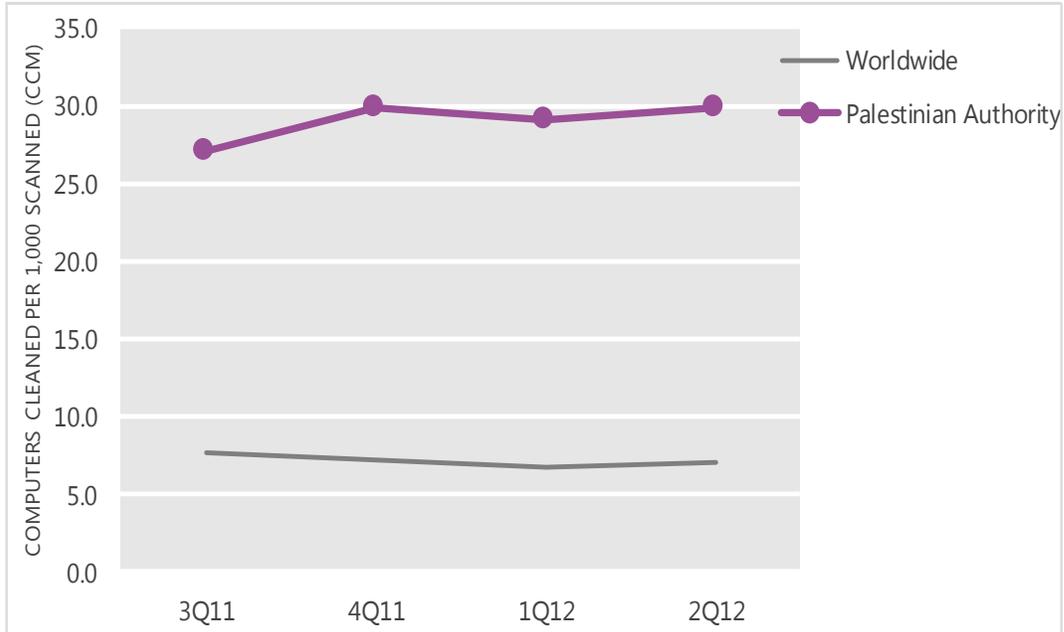
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	27.1	29.9	29.1	29.8
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

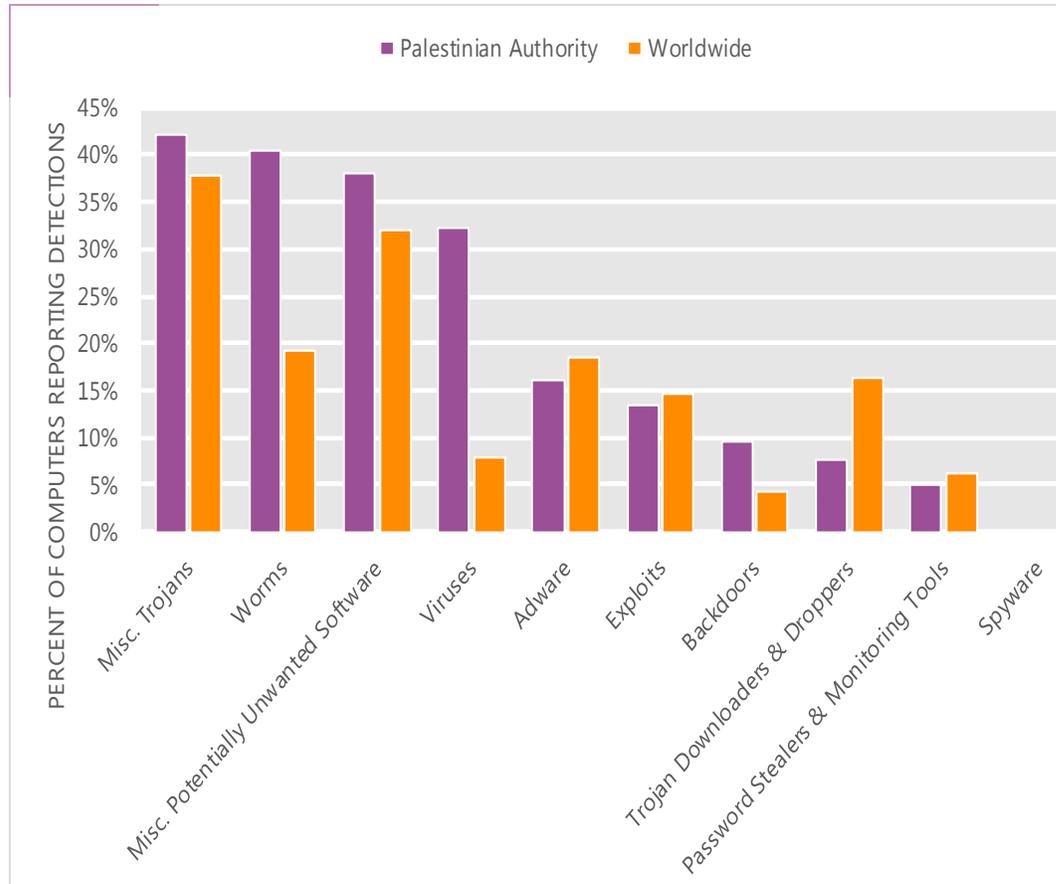
The MSRT detected malware on 29.8 of every 1,000 computers scanned in the Palestinian territories in 2Q12 (a CCM score of 29.8, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for the Palestinian territories over the last four quarters, compared to the world as a whole.

CCM infection trends in the Palestinian territories and worldwide



Threat categories

Malware and potentially unwanted software categories in the Palestinian territories in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in the Palestinian territories in 2Q12 was Miscellaneous Trojans. It affected 42.1 percent of all computers with detections there, up from 42.0 percent in 1Q12.
- The second most common category in the Palestinian territories in 2Q12 was Worms. It affected 40.3 percent of all computers with detections there, up from 38.8 percent in 1Q12.
- The third most common category in the Palestinian territories in 2Q12 was Miscellaneous Potentially Unwanted Software, which affected 38.1 percent of all computers with detections there, down from 38.5 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in the Palestinian territories in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Sality	Viruses	24.8%
2	Win32/Autorun	Worms	20.4%
3	Win32/Keygen	Misc. Potentially Unwanted Software	16.9%
4	Win32/Vobfus	Worms	12.6%
5	Win32/Ramnit	Misc. Trojans	12.5%
6	Win32/CplLnk	Exploits	11.4%
7	JS/Paypopup	Adware	9.2%
8	Win32/Virut	Viruses	7.2%
9	Win32/Dorkbot	Worms	6.4%
10	Win32/Sulunch	Misc. Trojans	6.2%

- The most common threat family in the Palestinian territories in 2Q12 was [Win32/Sality](#), which affected 24.8 percent of computers with detections in the Palestinian territories. [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 in the Palestinian territories in 2Q12 was [Win32/Autorun](#), which affected 20.4 percent of computers with detections in the Palestinian territories. [Win32/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 threat family in the Palestinian territories in 2Q12 was [Win32/Keygen](#), which affected 16.9 percent of computers with detections in the Palestinian territories. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The fourth most common threat family in the Palestinian territories in 2Q12 was [Win32/Vobfus](#), which affected 12.6 percent of computers with detections in the Palestinian territories. [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.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for the Palestinian territories

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	0.24 (1.6)	0.37 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	0.37 (3.9)	0.37 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.06 (0.7)	0.20 (0.9)

Update service usage

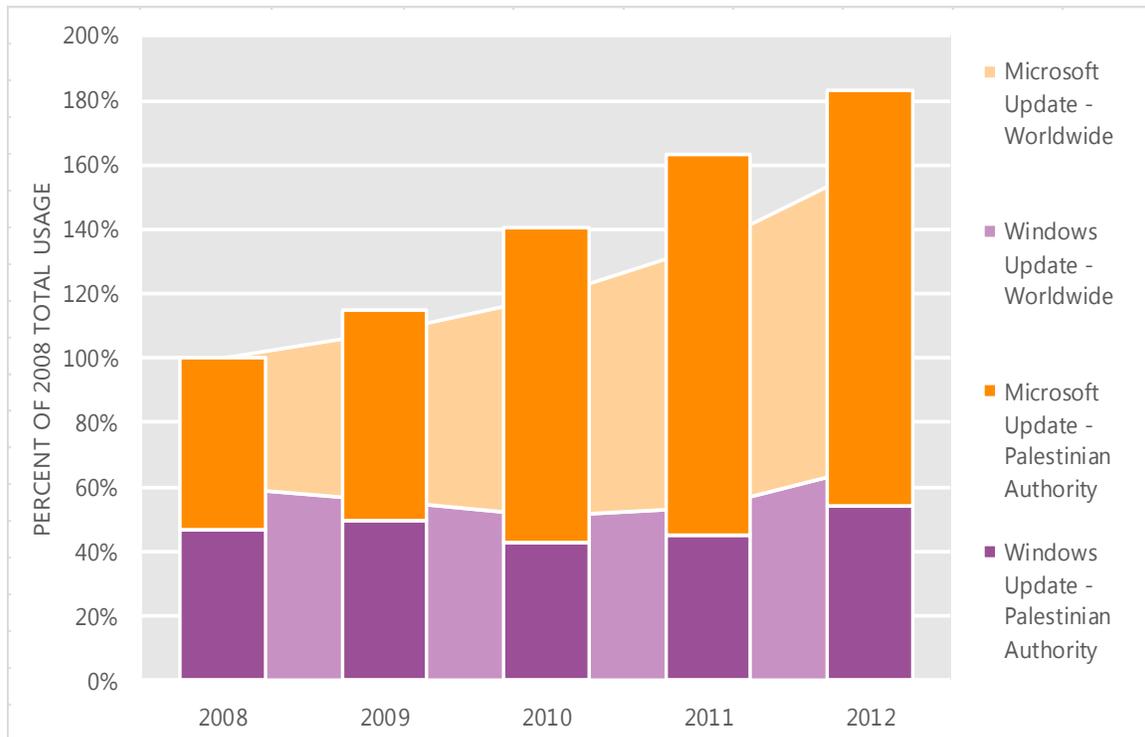
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in the Palestinian territories and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in the Palestinian territories over the last four years, indexed to the total usage for both services in the Palestinian territories in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in the Palestinian territories was up 12.4 percent from 2011, and up 83.2 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in the Palestinian territories in 2012, 70.3 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Panama

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Panama in 2Q12 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.

Infection rate statistics for Panama

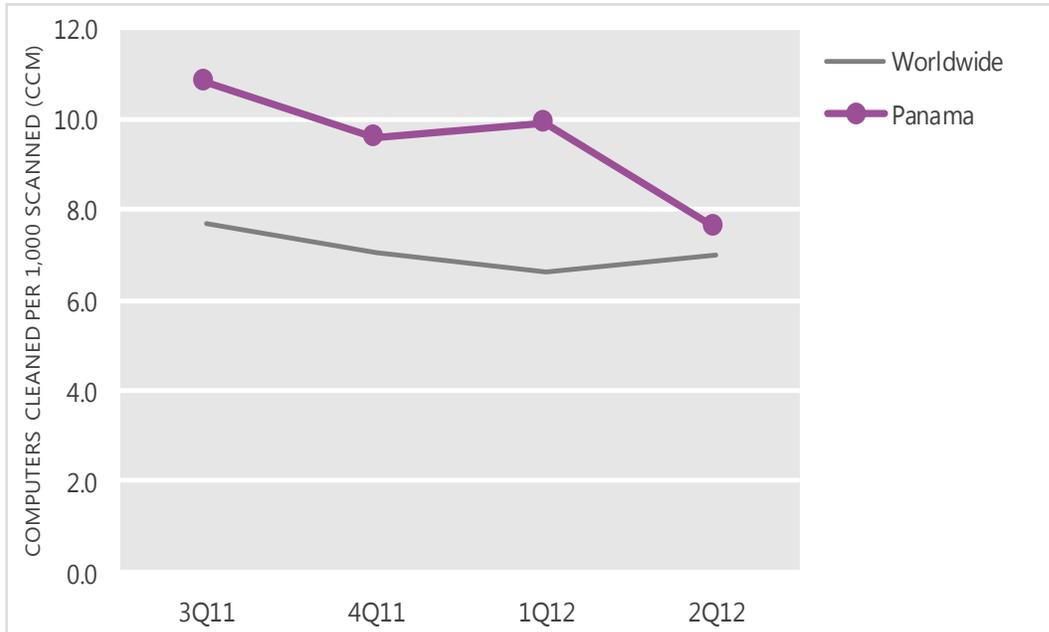
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	10.8	9.6	9.9	7.6
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

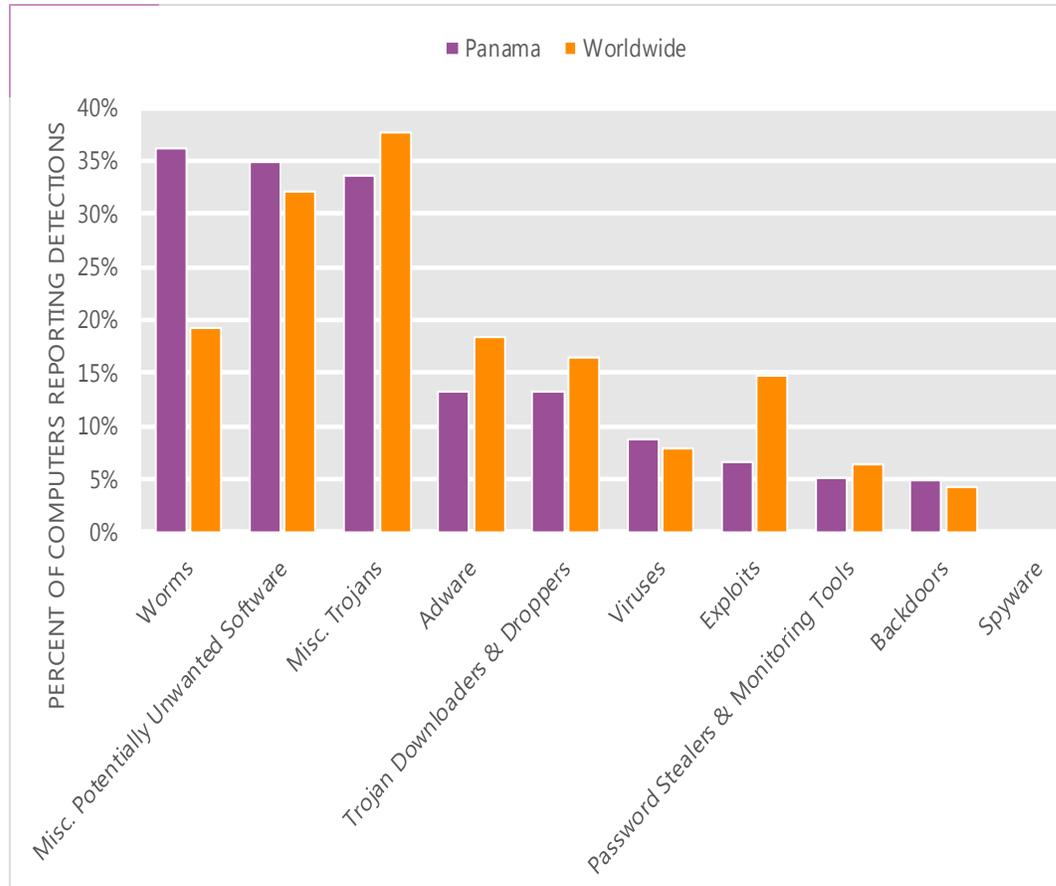
The MSRT detected malware on 7.6 of every 1,000 computers scanned in Panama in 2Q12 (a CCM score of 7.6, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Panama over the last four quarters, compared to the world as a whole.

CCM infection trends in Panama and worldwide



Threat categories

Malware and potentially unwanted software categories in Panama in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Panama in 2Q12 was Worms. It affected 36.1 percent of all computers with detections there, up from 32.8 percent in 1Q12.
- The second most common category in Panama in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 34.9 percent of all computers with detections there, down from 36.1 percent in 1Q12.
- The third most common category in Panama in 2Q12 was Miscellaneous Trojans, which affected 33.7 percent of all computers with detections there, up from 30.3 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Panama in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Dorkbot	Worms	18.0%
2	Win32/Autorun	Worms	11.4%
3	Win32/Keygen	Misc. Potentially Unwanted Software	10.3%
4	Win32/Vobfus	Worms	8.1%
5	Win32/Sality	Viruses	7.1%
6	JS/Pornpop	Adware	5.5%
7	Win32/Conficker	Worms	4.9%
8	ASX/Wimad	Trojan Downloaders & Droppers	4.8%
9	JS/IframeRef	Misc. Trojans	4.6%
10	Win32/VBInject	Misc. Potentially Unwanted Software	4.6%

- The most common threat family in Panama in 2Q12 was [Win32/Dorkbot](#), which affected 18.0 percent of computers with detections in Panama. [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 second most common threat family in Panama in 2Q12 was [Win32/Autorun](#), which affected 11.4 percent of computers with detections in Panama. [Win32/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 threat family in Panama in 2Q12 was [Win32/Keygen](#), which affected 10.3 percent of computers with detections in Panama. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The fourth most common threat family in Panama in 2Q12 was [Win32/Vobfus](#), which affected 8.1 percent of computers with detections in Panama. [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.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Panama

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	1.86 (1.6)	1.86 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	2.17 (3.9)	2.64 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	2.80 (0.7)	2.84 (0.9)

Update service usage

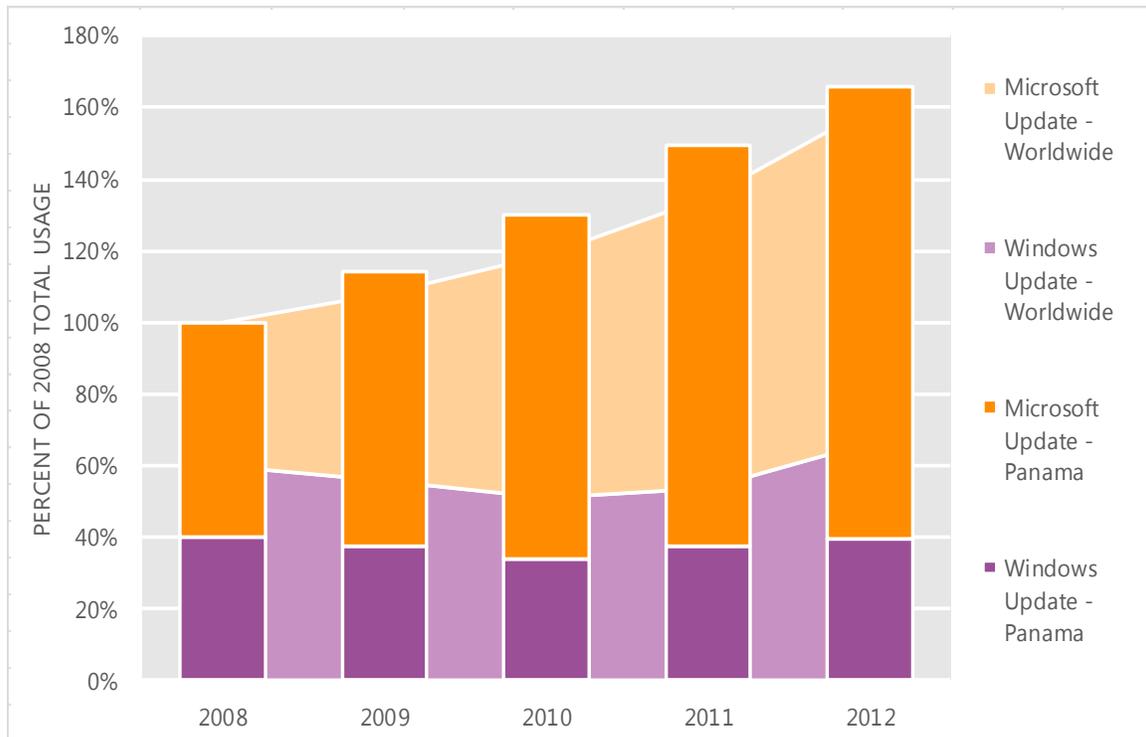
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Panama and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Panama over the last four years, indexed to the total usage for both services in Panama in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Panama was up 10.8 percent from 2011, and up 65.9 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Panama in 2012, 76.1 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Paraguay

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Paraguay in 2Q12 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.

Infection rate statistics for Paraguay

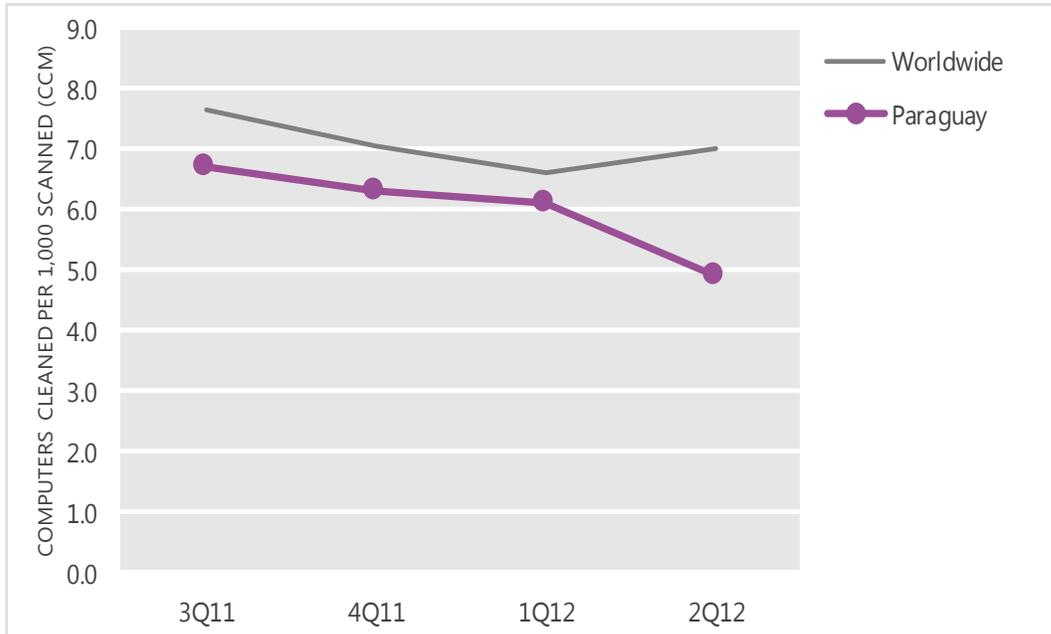
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	6.7	6.3	6.1	4.9
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

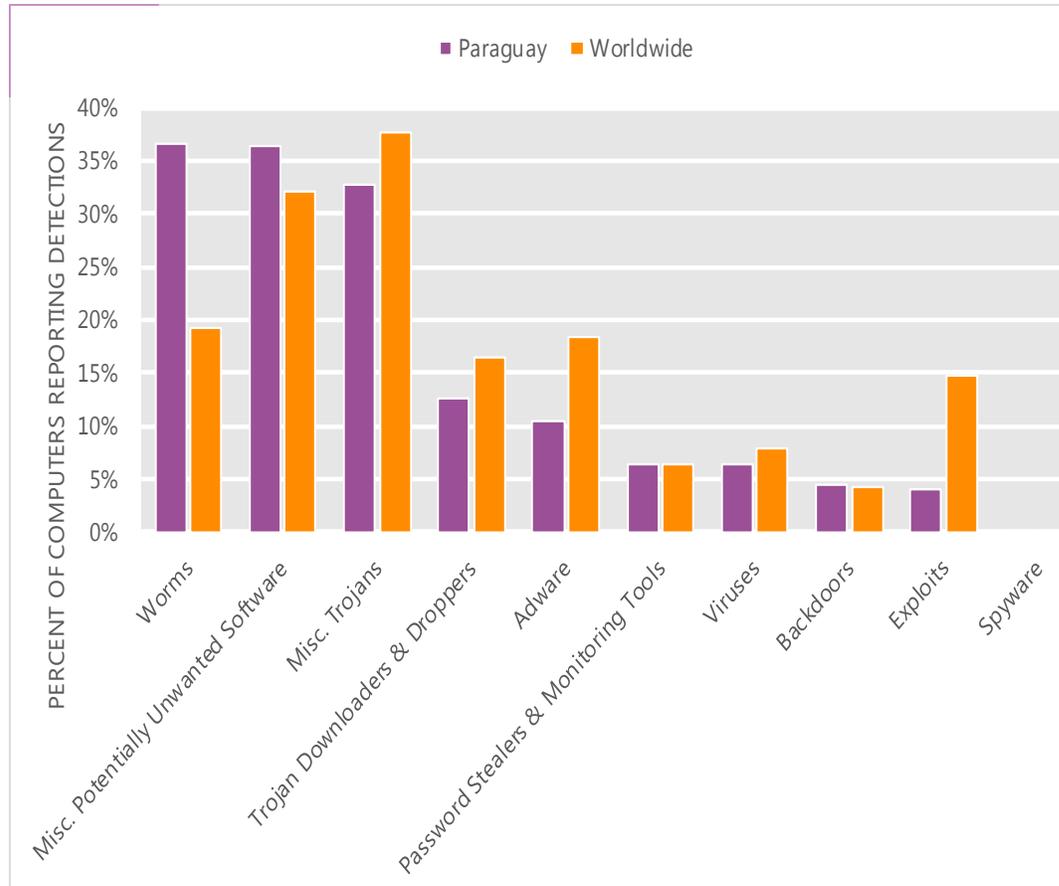
The MSRT detected malware on 4.9 of every 1,000 computers scanned in Paraguay in 2Q12 (a CCM score of 4.9, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Paraguay over the last four quarters, compared to the world as a whole.

CCM infection trends in Paraguay and worldwide



Threat categories

Malware and potentially unwanted software categories in Paraguay in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Paraguay in 2Q12 was Worms. It affected 36.5 percent of all computers with detections there, up from 32.8 percent in 1Q12.
- The second most common category in Paraguay in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 36.4 percent of all computers with detections there, down from 39.6 percent in 1Q12.
- The third most common category in Paraguay in 2Q12 was Miscellaneous Trojans, which affected 32.8 percent of all computers with detections there, up from 25.8 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Paraguay in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Dorkbot	Worms	18.6%
2	Win32/Keygen	Misc. Potentially Unwanted Software	13.6%
3	Win32/Autorun	Worms	10.8%
4	JS/Iframe	Misc. Trojans	7.8%
5	Win32/Sality	Viruses	4.4%
6	JS/Pornpop	Adware	3.8%
7	Win32/VBInject	Misc. Potentially Unwanted Software	3.6%
8	Win32/Wpakill	Misc. Potentially Unwanted Software	3.6%
9	JS/Redirector	Misc. Trojans	3.5%
10	Win32/Conficker	Worms	3.5%

- The most common threat family in Paraguay in 2Q12 was [Win32/Dorkbot](#), which affected 18.6 percent of computers with detections in Paraguay. [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 second most common threat family in Paraguay in 2Q12 was [Win32/Keygen](#), which affected 13.6 percent of computers with detections in Paraguay. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The third most common threat family in Paraguay in 2Q12 was [Win32/Autorun](#), which affected 10.8 percent of computers with detections in Paraguay. [Win32/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 threat family in Paraguay in 2Q12 was [JS/Iframe](#), which affected 7.8 percent of computers with detections in Paraguay. [JS/Iframe](#) is an exploit that targets a vulnerability in Internet Explorer 5.01 and 5.5. Microsoft released Security Bulletin MS01-020 in March 2001 to address the vulnerability.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Paraguay

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	N/A (1.6)	1.49 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	6.69 (3.9)	2.97 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.30 (0.7)	0.41 (0.9)

Update service usage

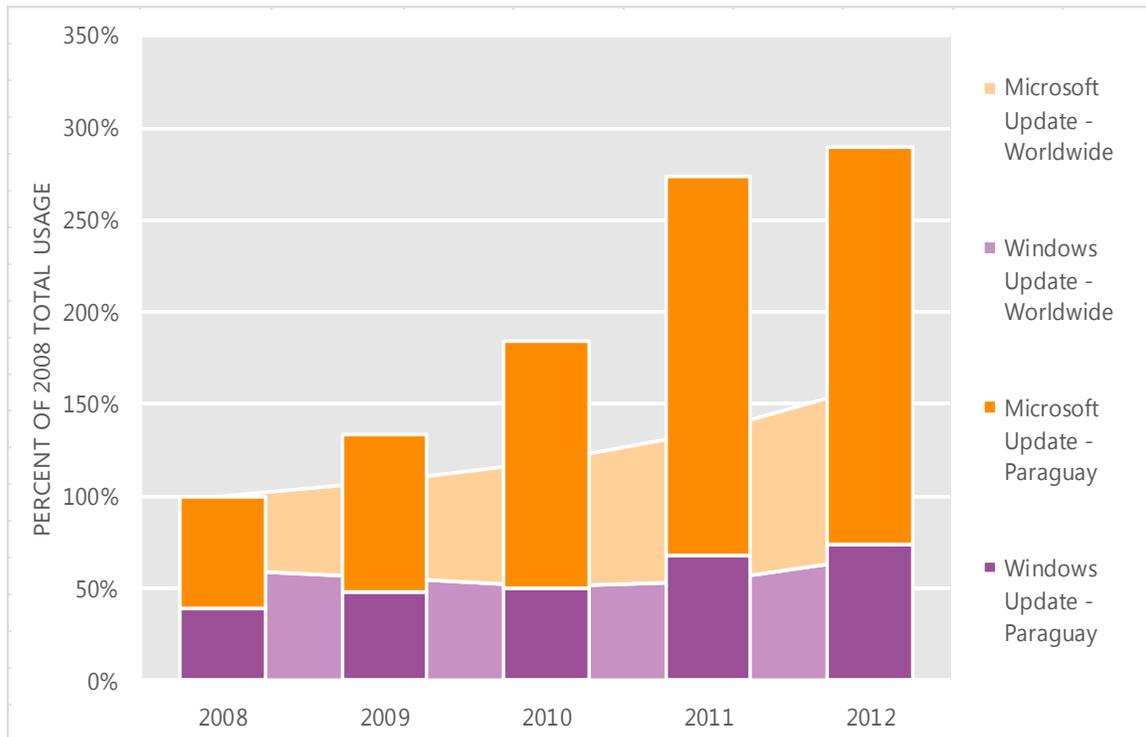
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Paraguay and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Paraguay over the last four years, indexed to the total usage for both services in Paraguay in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Paraguay was up 6.0 percent from 2011, and up 189.9 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Paraguay in 2012, 74.5 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Peru

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Peru in 2Q12 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.

Infection rate statistics for Peru

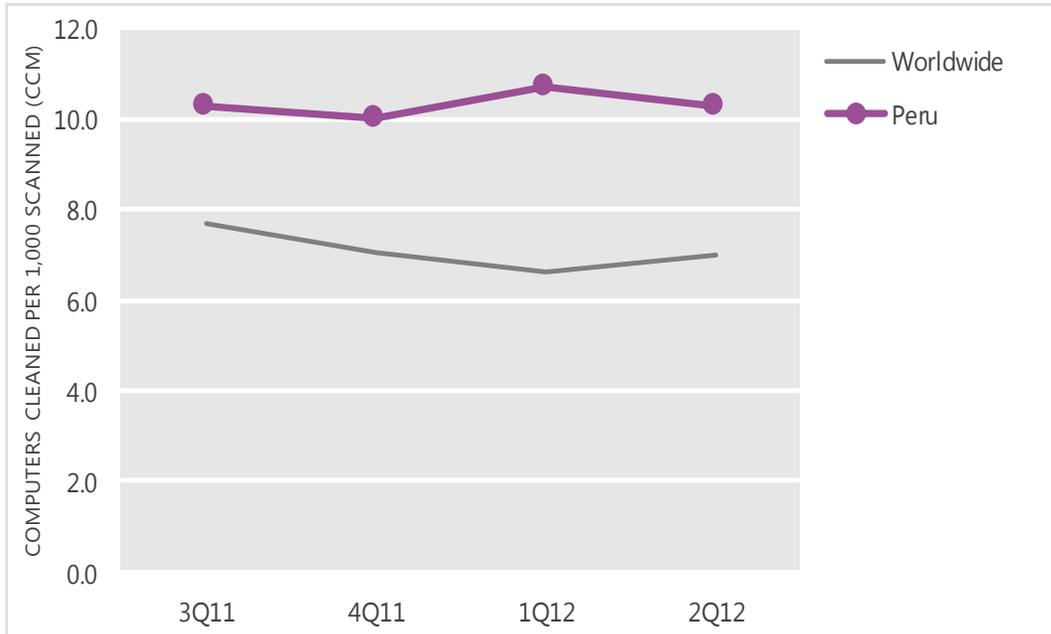
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	10.3	10.0	10.7	10.3
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

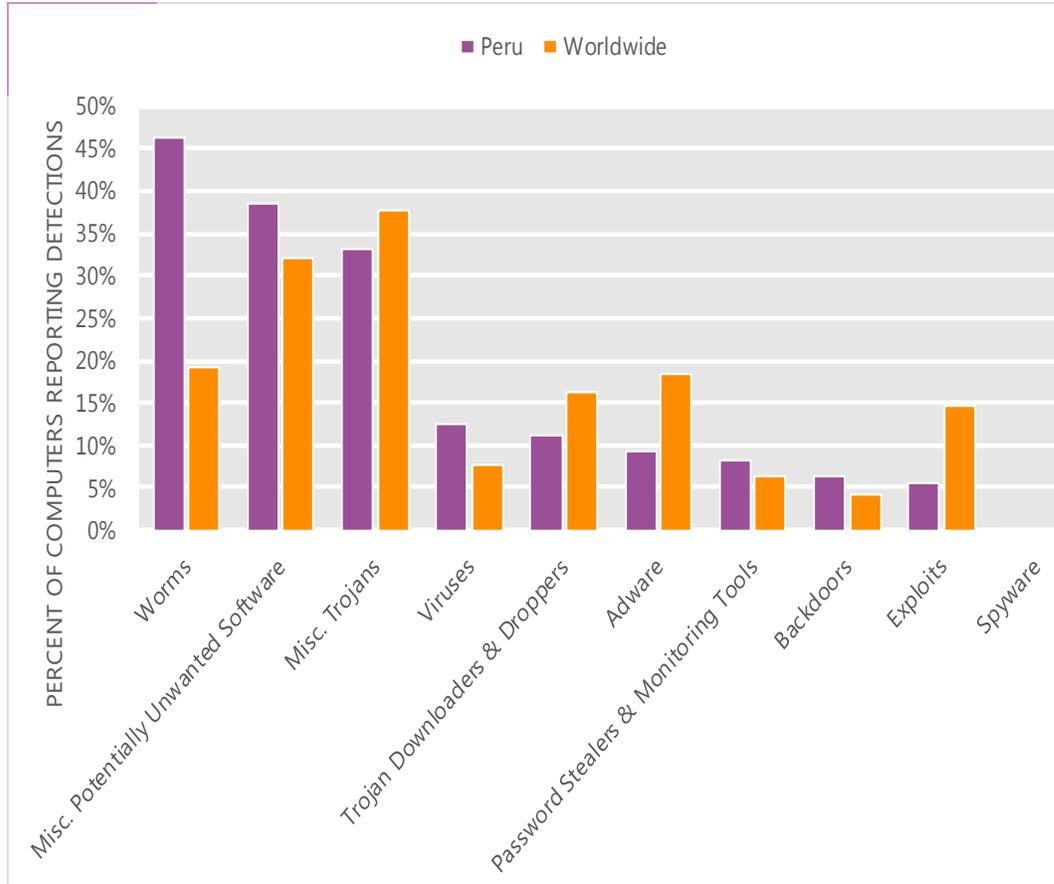
The MSRT detected malware on 10.3 of every 1,000 computers scanned in Peru in 2Q12 (a CCM score of 10.3, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Peru over the last four quarters, compared to the world as a whole.

CCM infection trends in Peru and worldwide



Threat categories

Malware and potentially unwanted software categories in Peru in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Peru in 2Q12 was Worms. It affected 46.2 percent of all computers with detections there, up from 41.9 percent in 1Q12.
- The second most common category in Peru in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 38.4 percent of all computers with detections there, down from 41.0 percent in 1Q12.
- The third most common category in Peru in 2Q12 was Miscellaneous Trojans, which affected 33.0 percent of all computers with detections there, up from 27.9 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Peru in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Dorkbot	Worms	21.4%
2	Win32/Keygen	Misc. Potentially Unwanted Software	15.5%
3	Win32/Autorun	Worms	12.6%
4	Win32/Vobfus	Worms	9.3%
5	Win32/Conficker	Worms	7.2%
6	Win32/VBIject	Misc. Potentially Unwanted Software	6.2%
7	Win32/Sality	Viruses	5.8%
8	Win32/Yeltminky	Worms	5.3%
9	Win32/Nuqel	Worms	5.2%
10	JS/IframeRef	Misc. Trojans	4.7%

- The most common threat family in Peru in 2Q12 was [Win32/Dorkbot](#), which affected 21.4 percent of computers with detections in Peru. [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 second most common threat family in Peru in 2Q12 was [Win32/Keygen](#), which affected 15.5 percent of computers with detections in Peru. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The third most common threat family in Peru in 2Q12 was [Win32/Autorun](#), which affected 12.6 percent of computers with detections in Peru. [Win32/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 threat family in Peru in 2Q12 was [Win32/Vobfus](#), which affected 9.3 percent of computers with detections in Peru. [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.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Peru

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	1.04 (1.6)	0.23 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	0.58 (3.9)	1.16 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.00 (0.7)	0.01 (0.9)

Update service usage

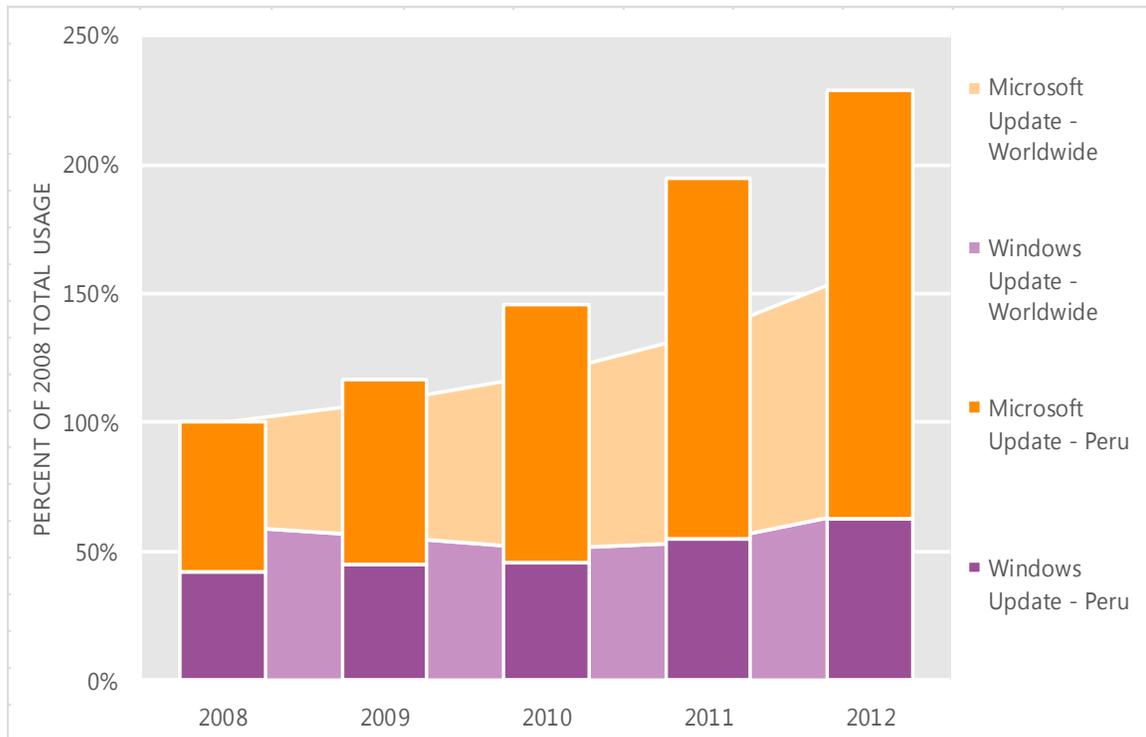
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Peru and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Peru over the last four years, indexed to the total usage for both services in Peru in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Peru was up 17.4 percent from 2011, and up 129.0 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Peru in 2012, 72.5 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Philippines

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Philippines in 2Q12 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.

Infection rate statistics for Philippines

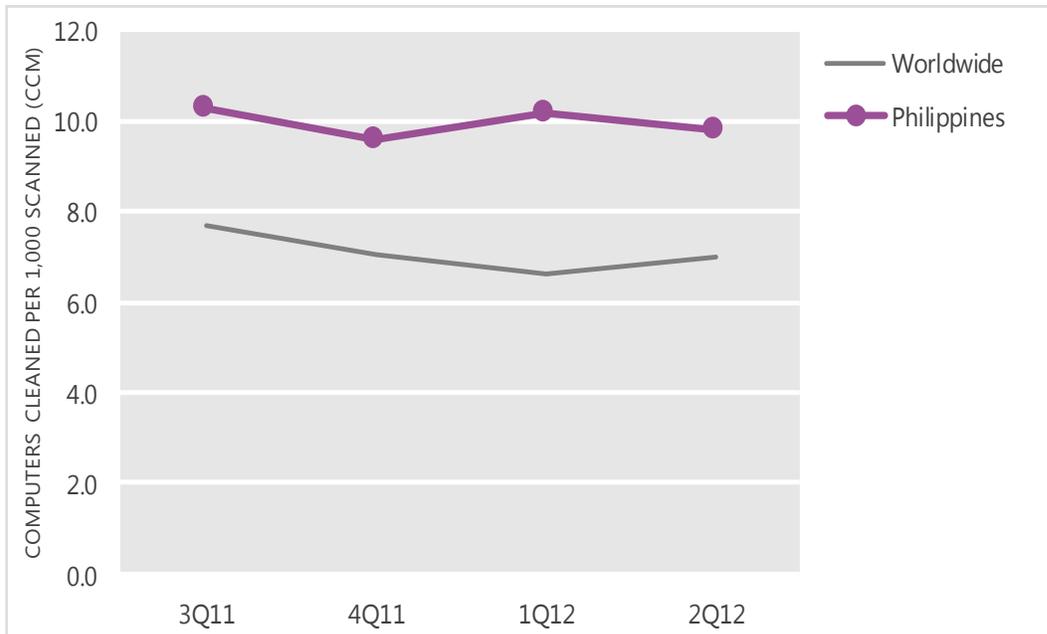
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	10.3	9.6	10.2	9.8
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

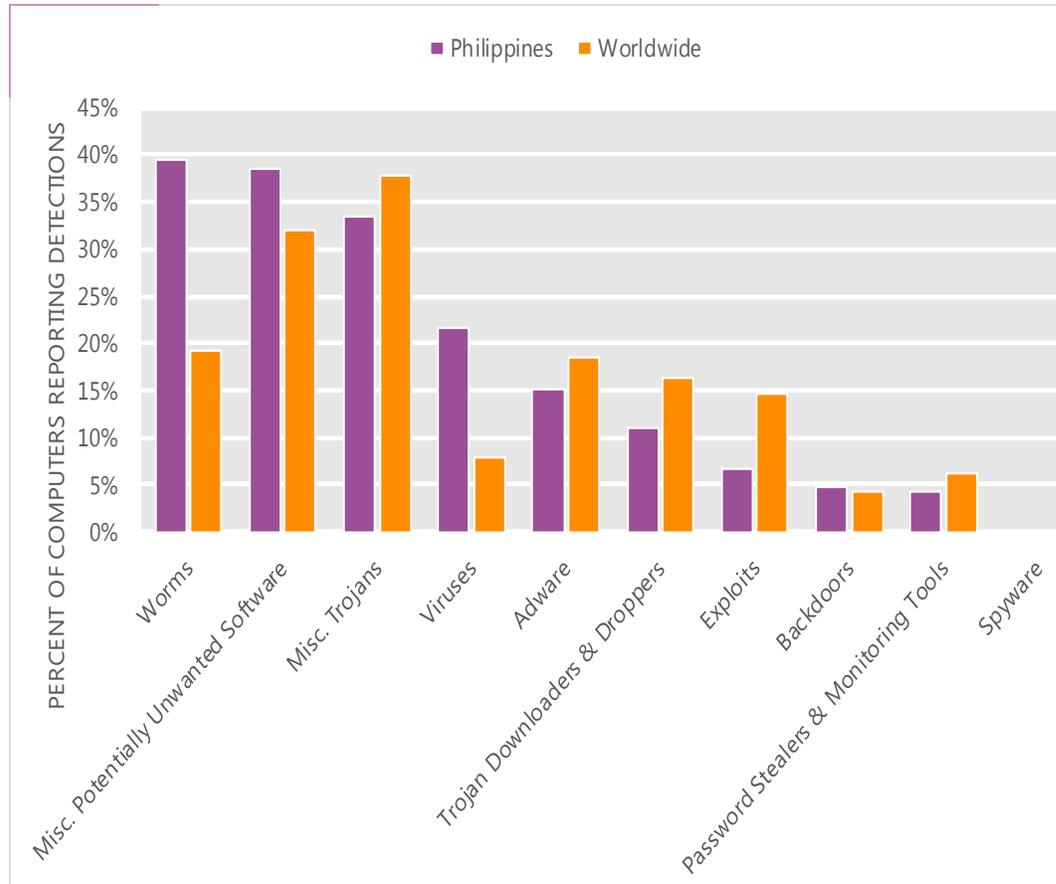
The MSRT detected malware on 9.8 of every 1,000 computers scanned in Philippines in 2Q12 (a CCM score of 9.8, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Philippines over the last four quarters, compared to the world as a whole.

CCM infection trends in Philippines and worldwide



Threat categories

Malware and potentially unwanted software categories in Philippines in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Philippines in 2Q12 was Worms. It affected 39.4 percent of all computers with detections there, down from 43.2 percent in 1Q12.
- The second most common category in Philippines in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 38.4 percent of all computers with detections there, up from 38.3 percent in 1Q12.
- The third most common category in Philippines in 2Q12 was Miscellaneous Trojans, which affected 33.4 percent of all computers with detections there, down from 35.9 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Philippines in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Sality	Viruses	18.0%
2	Win32/Autorun	Worms	16.1%
3	Win32/Keygen	Misc. Potentially Unwanted Software	13.0%
4	Win32/Dorkbot	Worms	11.5%
5	Win32/Conficker	Worms	9.4%
6	Win32/Hotbar	Adware	9.2%
7	Win32/Nuqel	Worms	6.5%
8	Win32/Rimecud	Worms	6.4%
9	Win32/Zwangi	Misc. Potentially Unwanted Software	6.1%
10	Win32/Vobfus	Worms	5.3%

- The most common threat family in Philippines in 2Q12 was [Win32/Sality](#), which affected 18.0 percent of computers with detections in Philippines. [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 in Philippines in 2Q12 was [Win32/Autorun](#), which affected 16.1 percent of computers with detections in Philippines. [Win32/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 threat family in Philippines in 2Q12 was [Win32/Keygen](#), which affected 13.0 percent of computers with detections in Philippines. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The fourth most common threat family in Philippines in 2Q12 was [Win32/Dorkbot](#), which affected 11.5 percent of computers with detections in Philippines. [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.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Philippines

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	0.44 (1.6)	0.88 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	1.43 (3.9)	1.76 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.01 (0.7)	0.04 (0.9)

Update service usage

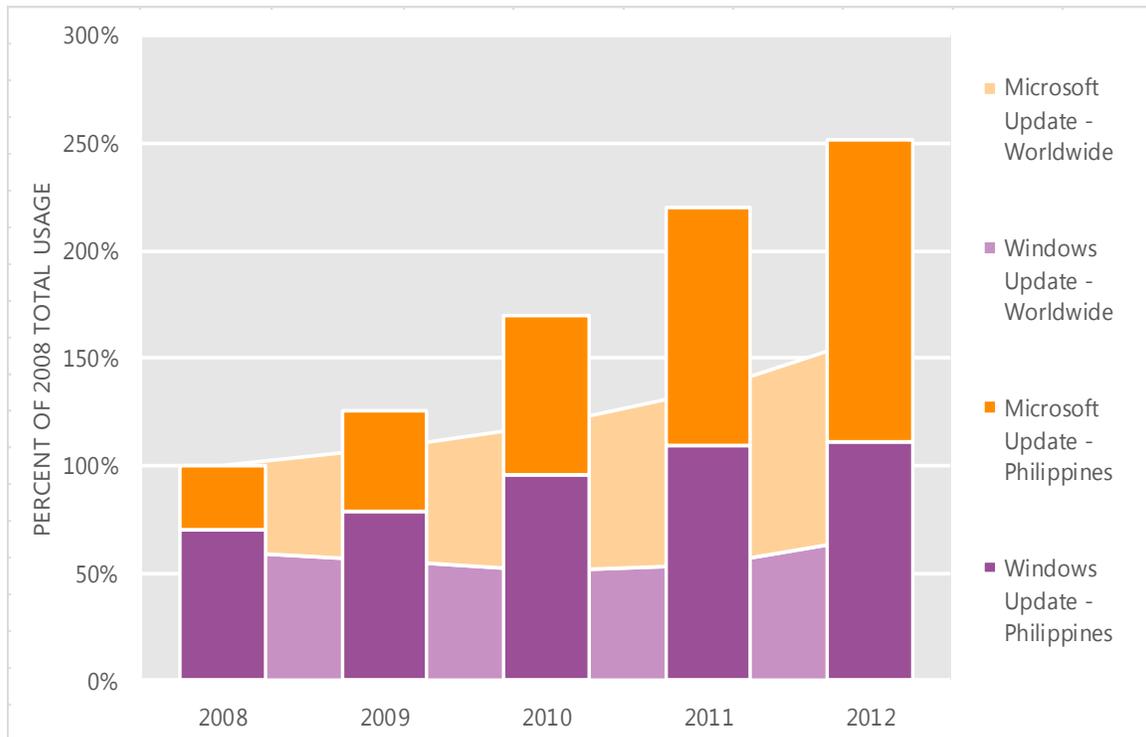
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Philippines and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Philippines over the last four years, indexed to the total usage for both services in Philippines in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Philippines was up 14.0 percent from 2011, and up 151.3 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Philippines in 2012, 55.8 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Poland

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Poland in 2Q12 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.

Infection rate statistics for Poland

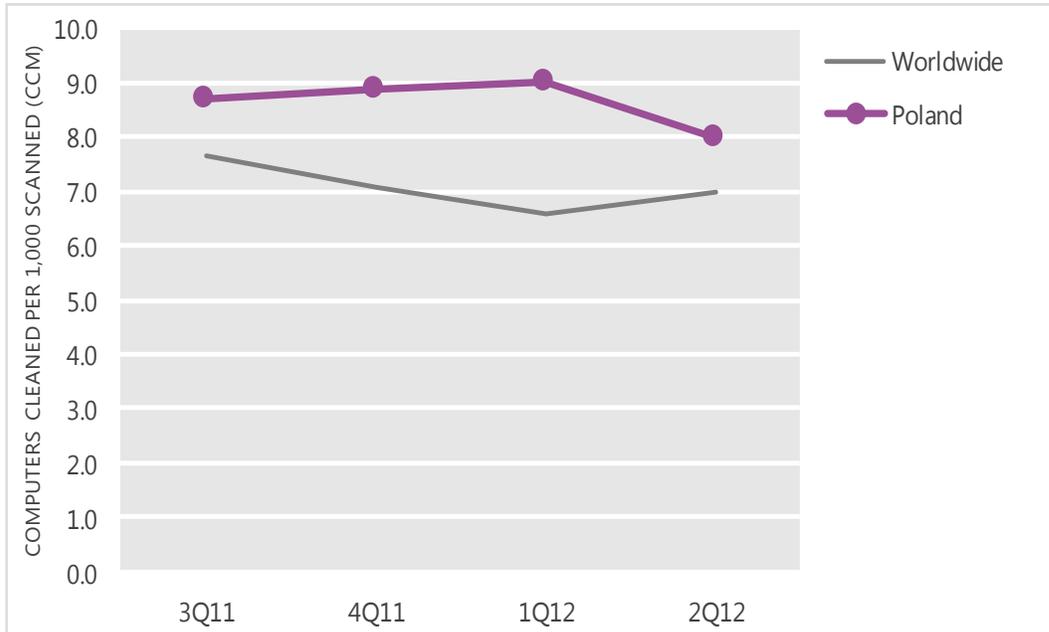
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	8.7	8.9	9.0	8.0
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

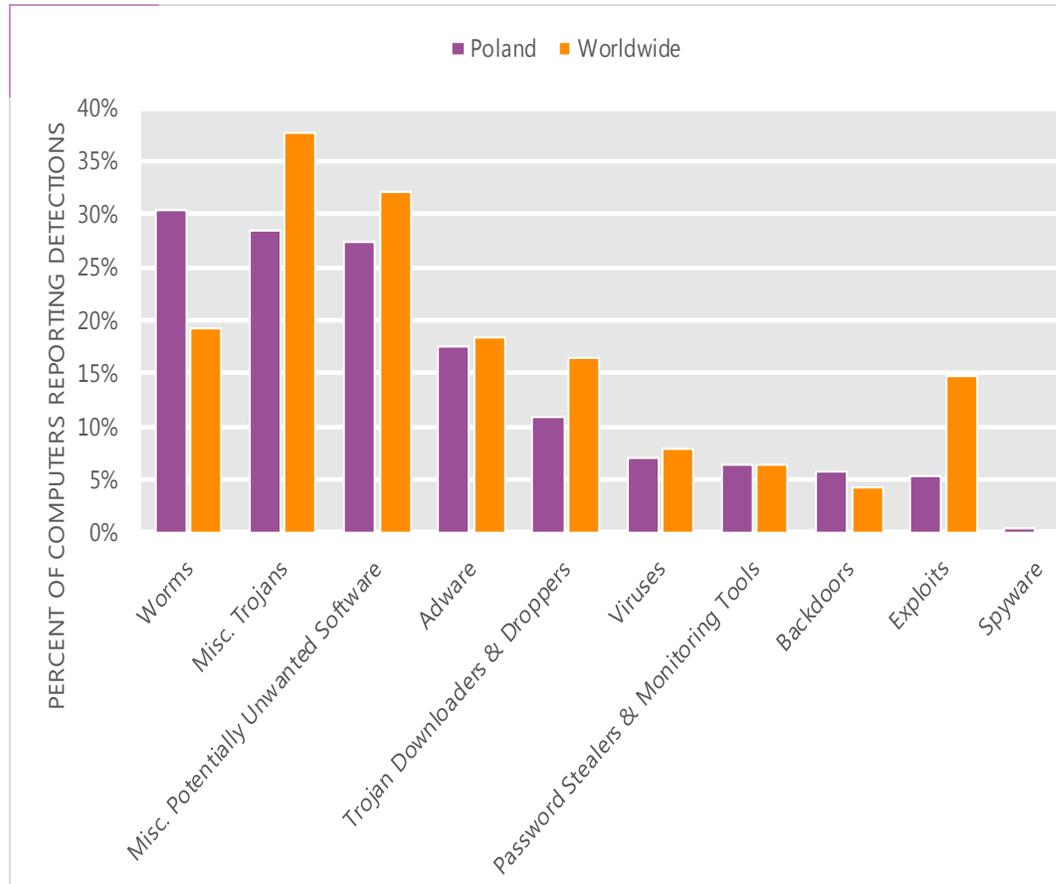
The MSRT detected malware on 8.0 of every 1,000 computers scanned in Poland in 2Q12 (a CCM score of 8.0, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Poland over the last four quarters, compared to the world as a whole.

CCM infection trends in Poland and worldwide



Threat categories

Malware and potentially unwanted software categories in Poland in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Poland in 2Q12 was Worms. It affected 30.3 percent of all computers with detections there, up from 25.0 percent in 1Q12.
- The second most common category in Poland in 2Q12 was Miscellaneous Trojans. It affected 28.5 percent of all computers with detections there, down from 30.9 percent in 1Q12.
- The third most common category in Poland in 2Q12 was Miscellaneous Potentially Unwanted Software, which affected 27.3 percent of all computers with detections there, down from 29.2 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Poland in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Autorun	Worms	8.4%
2	Win32/Keygen	Misc. Potentially Unwanted Software	8.2%
3	Win32/AdRotator	Adware	7.7%
4	Win32/Sality	Viruses	5.1%
5	Win32/Vobfus	Worms	5.1%
6	Win32/Brontok	Worms	4.4%
7	JS/Iframe	Misc. Trojans	3.9%
8	Win32/Taterf	Worms	3.8%
9	JS/Pornpop	Adware	3.7%
10	ASX/Wimad	Trojan Downloaders & Droppers	3.4%

- The most common threat family in Poland in 2Q12 was [Win32/Autorun](#), which affected 8.4 percent of computers with detections in Poland. [Win32/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 threat family in Poland in 2Q12 was [Win32/Keygen](#), which affected 8.2 percent of computers with detections in Poland. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The third most common threat family in Poland in 2Q12 was [Win32/AdRotator](#), which affected 7.7 percent of computers with detections in Poland. [Win32/AdRotator](#) is adware that “rotates” advertisements among sponsors, as the name suggests. AdRotator contacts remote websites to deliver updated content. It also displays fake error messages that encourage users to download and install additional applications.
- The fourth most common threat family in Poland in 2Q12 was [Win32/Sality](#), which affected 5.1 percent of computers with detections in Poland. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Poland

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	2.27 (1.6)	2.85 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	2.03 (3.9)	2.72 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.51 (0.7)	0.76 (0.9)

Update service usage

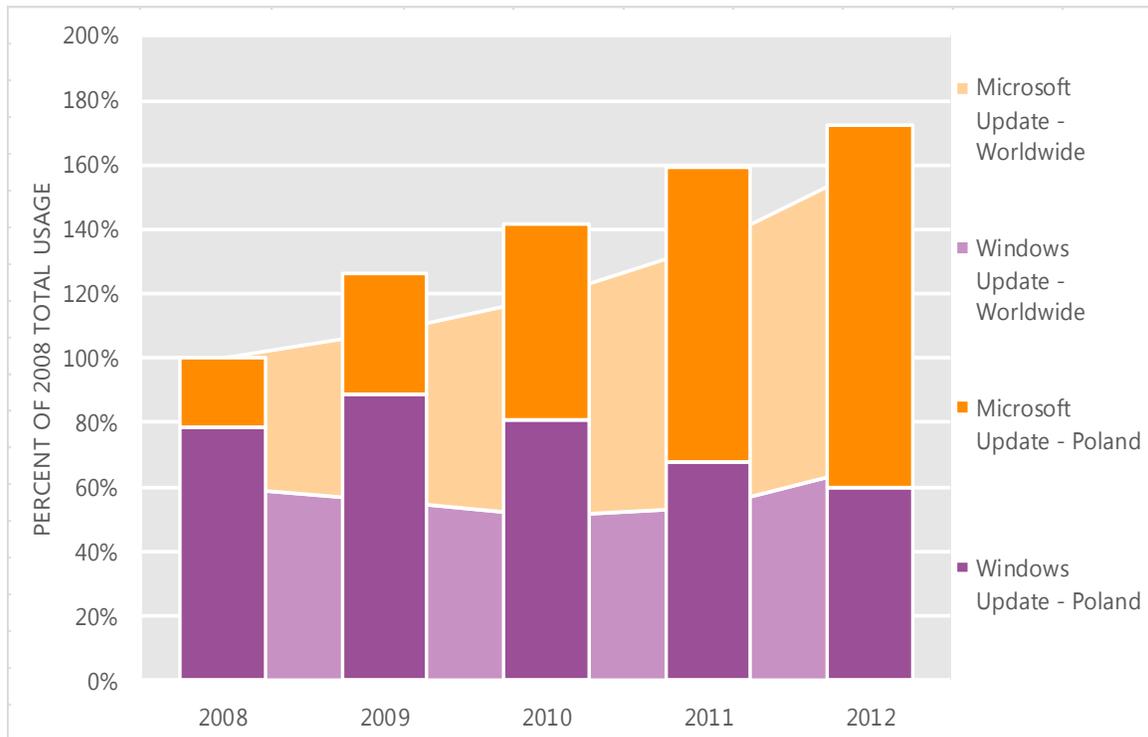
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Poland and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Poland over the last four years, indexed to the total usage for both services in Poland in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Poland was up 8.3 percent from 2011, and up 72.2 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Poland in 2012, 65.1 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Portugal

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Portugal in 2Q12 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.

Infection rate statistics for Portugal

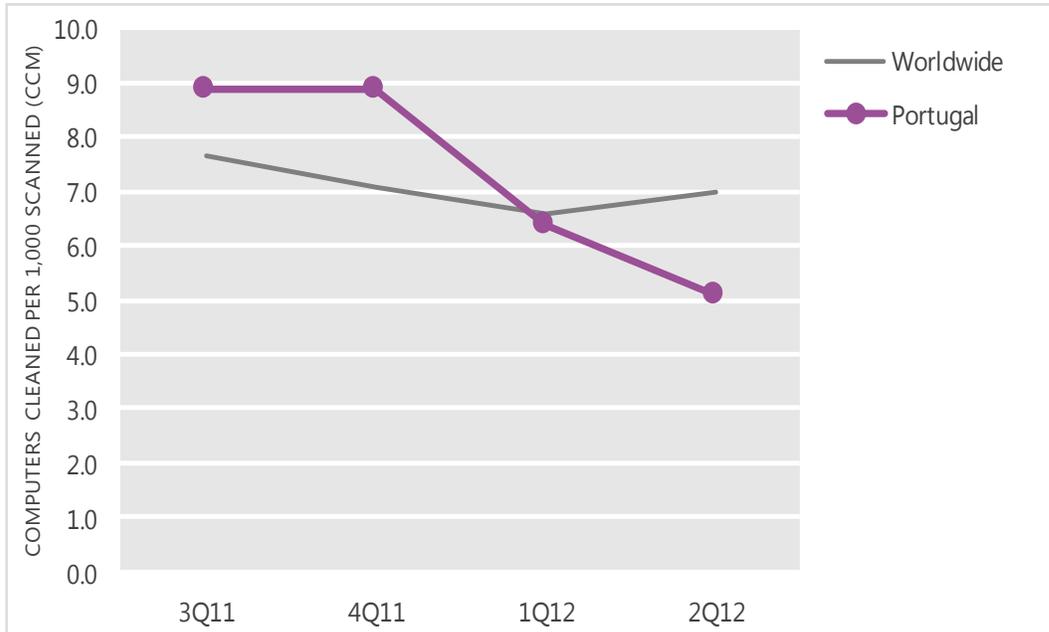
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	8.9	8.9	6.4	5.1
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

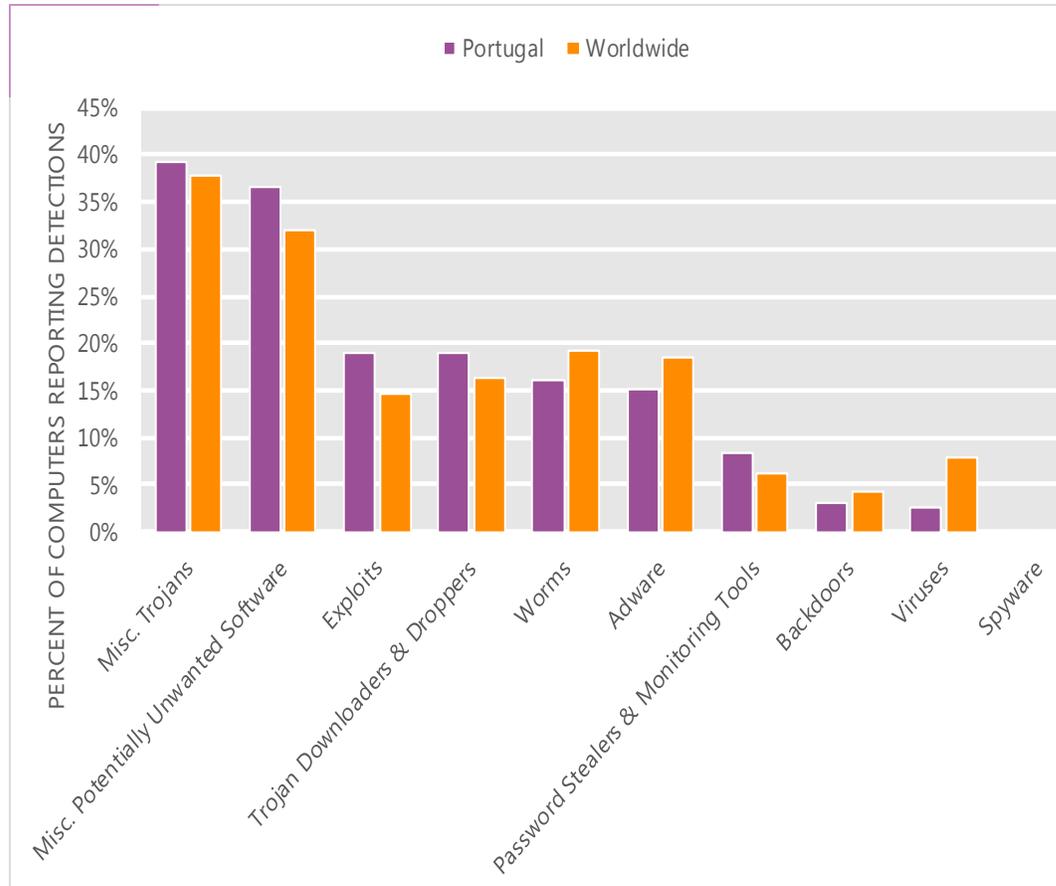
The MSRT detected malware on 5.1 of every 1,000 computers scanned in Portugal in 2Q12 (a CCM score of 5.1, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Portugal over the last four quarters, compared to the world as a whole.

CCM infection trends in Portugal and worldwide



Threat categories

Malware and potentially unwanted software categories in Portugal in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Portugal in 2Q12 was Miscellaneous Trojans. It affected 39.2 percent of all computers with detections there, up from 36.2 percent in 1Q12.
- The second most common category in Portugal in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 36.6 percent of all computers with detections there, down from 37.2 percent in 1Q12.
- The third most common category in Portugal in 2Q12 was Exploits, which affected 19.0 percent of all computers with detections there, up from 15.8 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Portugal in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Keygen	Misc. Potentially Unwanted Software	12.9%
2	Java/Blacole	Exploits	12.0%
3	Win32/Autorun	Worms	7.3%
4	JS/Pornpop	Adware	7.3%
5	ASX/Wimad	Trojan Downloaders & Droppers	6.3%
6	JS/BlacoleRef	Misc. Trojans	6.3%
7	JS/Iframe	Misc. Trojans	5.4%
8	Java/CVE-2012-0507	Exploits	5.3%
9	Win32/Obfuscator	Misc. Potentially Unwanted Software	4.7%
10	Win32/Hotbar	Adware	4.5%

- The most common threat family in Portugal in 2Q12 was [Win32/Keygen](#), which affected 12.9 percent of computers with detections in Portugal. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The second most common threat family in Portugal in 2Q12 was [Java/Blacole](#), which affected 12.0 percent of computers with detections in Portugal. [Java/Blacole](#) is an exploit pack, also known as Blackhole, that is installed on a compromised web server by an attacker and includes a number of exploits that target browser software. If a vulnerable computer browses a compromised website that contains the exploit pack, various malware may be downloaded and run.
- The third most common threat family in Portugal in 2Q12 was [Win32/Autorun](#), which affected 7.3 percent of computers with detections in Portugal. [Win32/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 threat family in Portugal in 2Q12 was [JS/Pornpop](#), which affected 7.3 percent of computers with detections in Portugal. [JS/Pornpop](#) is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Portugal

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	0.65 (1.6)	0.76 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	1.79 (3.9)	1.41 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	1.19 (0.7)	1.85 (0.9)

Update service usage

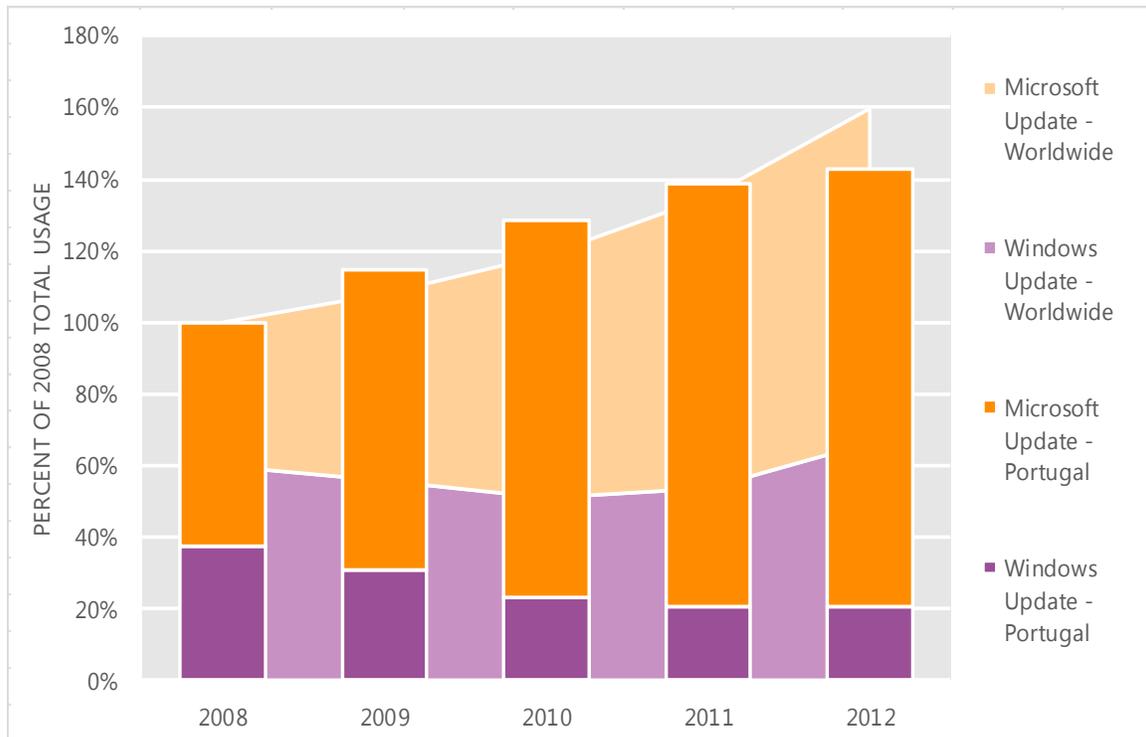
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Portugal and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Portugal over the last four years, indexed to the total usage for both services in Portugal in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Portugal was up 2.9 percent from 2011, and up 42.7 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Portugal in 2012, 85.5 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Puerto Rico

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Puerto Rico in 2Q12 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.

Infection rate statistics for Puerto Rico

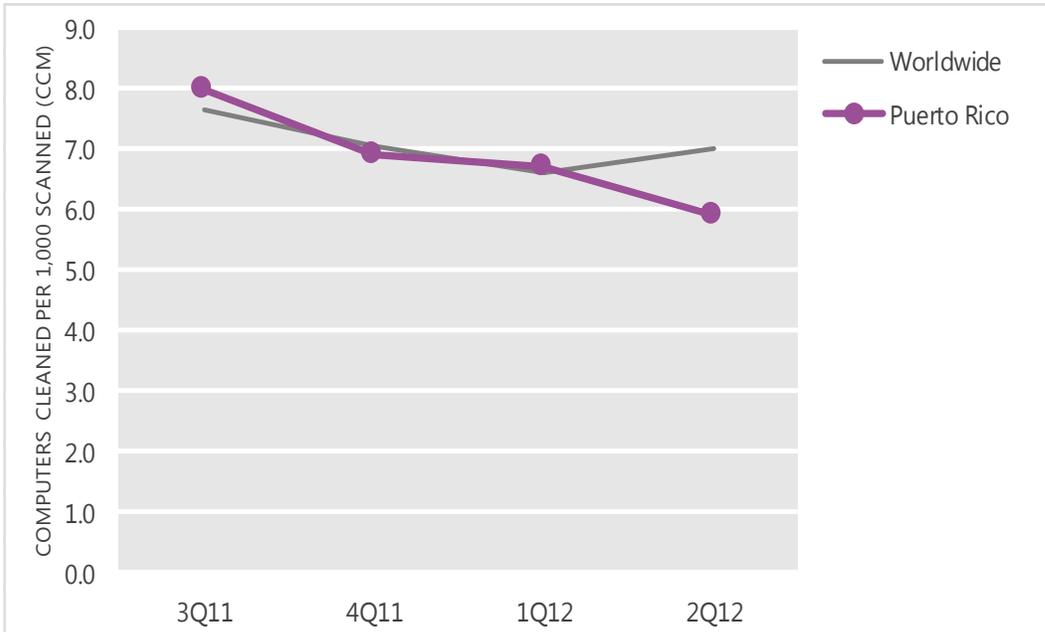
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	8.0	6.9	6.7	5.9
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

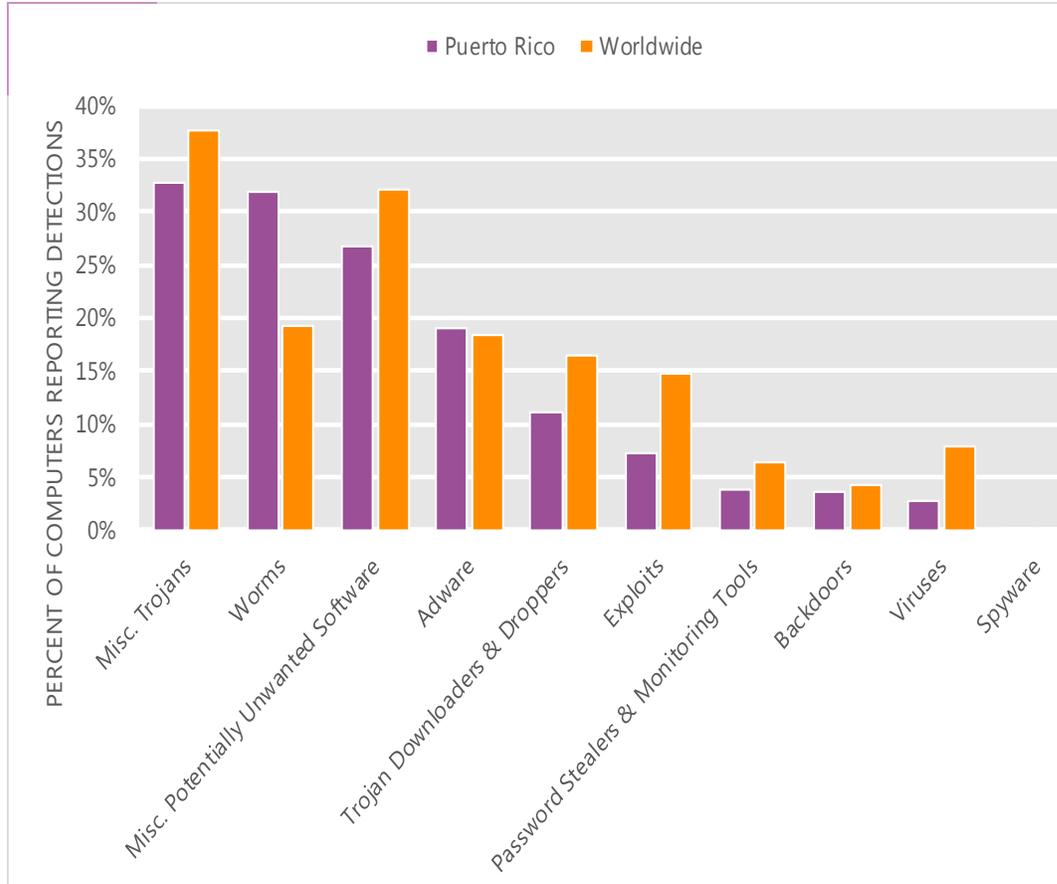
The MSRT detected malware on 5.9 of every 1,000 computers scanned in Puerto Rico in 2Q12 (a CCM score of 5.9, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Puerto Rico over the last four quarters, compared to the world as a whole.

CCM infection trends in Puerto Rico and worldwide



Threat categories

Malware and potentially unwanted software categories in Puerto Rico in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Puerto Rico in 2Q12 was Miscellaneous Trojans. It affected 32.7 percent of all computers with detections there, up from 28.0 percent in 1Q12.
- The second most common category in Puerto Rico in 2Q12 was Worms. It affected 31.9 percent of all computers with detections there, down from 33.3 percent in 1Q12.
- The third most common category in Puerto Rico in 2Q12 was Miscellaneous Potentially Unwanted Software, which affected 26.7 percent of all computers with detections there, down from 27.4 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Puerto Rico in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Autorun	Worms	11.5%
2	Win32/Vobfus	Worms	10.6%
3	Win32/Hotbar	Adware	8.3%
4	Win32/Keygen	Misc. Potentially Unwanted Software	6.6%
5	Win32/Zwangi	Misc. Potentially Unwanted Software	6.4%
6	JS/Pornpop	Adware	6.4%
7	JS/IframeRef	Misc. Trojans	6.0%
8	Win32/Brontok	Worms	5.8%
9	Win32/FakePAV	Misc. Trojans	5.1%
10	ASX/Wimad	Trojan Downloaders & Droppers	3.9%

- The most common threat family in Puerto Rico in 2Q12 was [Win32/Autorun](#), which affected 11.5 percent of computers with detections in Puerto Rico. [Win32/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 threat family in Puerto Rico in 2Q12 was [Win32/Vobfus](#), which affected 10.6 percent of computers with detections in Puerto Rico. [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 in Puerto Rico in 2Q12 was [Win32/Hotbar](#), which affected 8.3 percent of computers with detections in Puerto Rico. [Win32/Hotbar](#) is adware that displays a dynamic toolbar and targeted pop-up ads based on its monitoring of web-browsing activity.
- The fourth most common threat family in Puerto Rico in 2Q12 was [Win32/Keygen](#), which affected 6.6 percent of computers with detections in Puerto Rico. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Puerto Rico

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	0.47 (1.6)	0.94 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	0.71 (3.9)	1.89 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.02 (0.7)	0.17 (0.9)

Update service usage

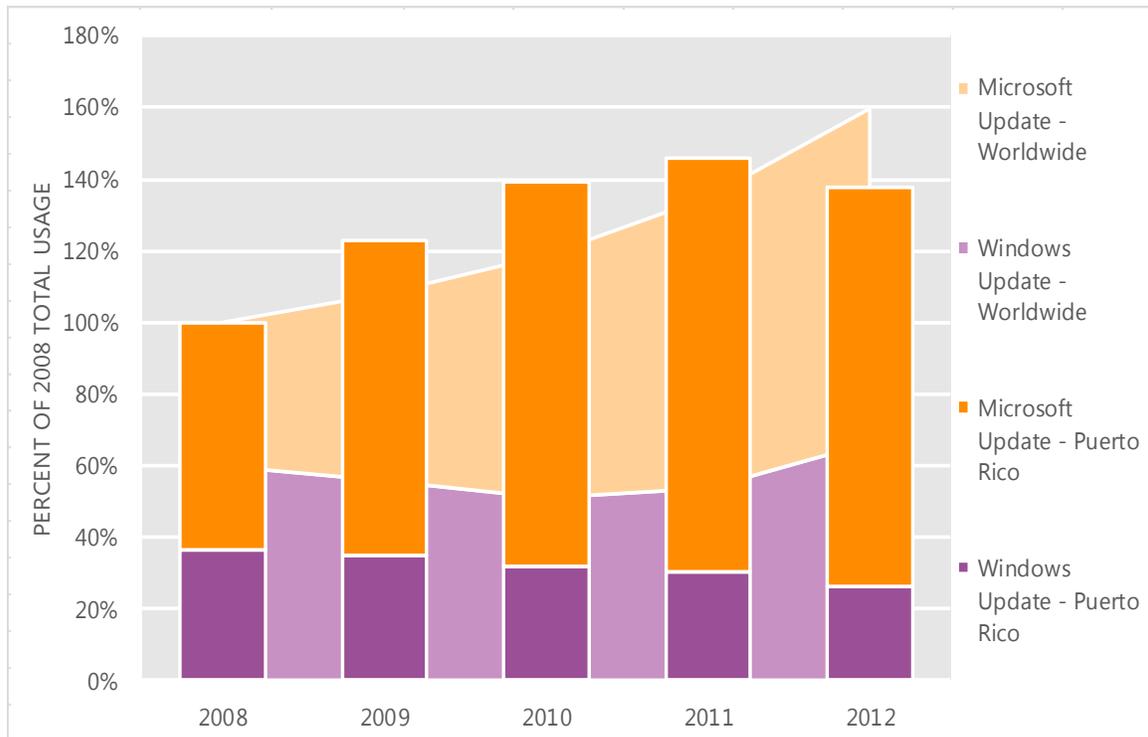
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Puerto Rico and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Puerto Rico over the last four years, indexed to the total usage for both services in Puerto Rico in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Puerto Rico was down 5.9 percent from 2011, and up 37.6 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Puerto Rico in 2012, 80.9 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Qatar

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Qatar in 2Q12 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.

Infection rate statistics for Qatar

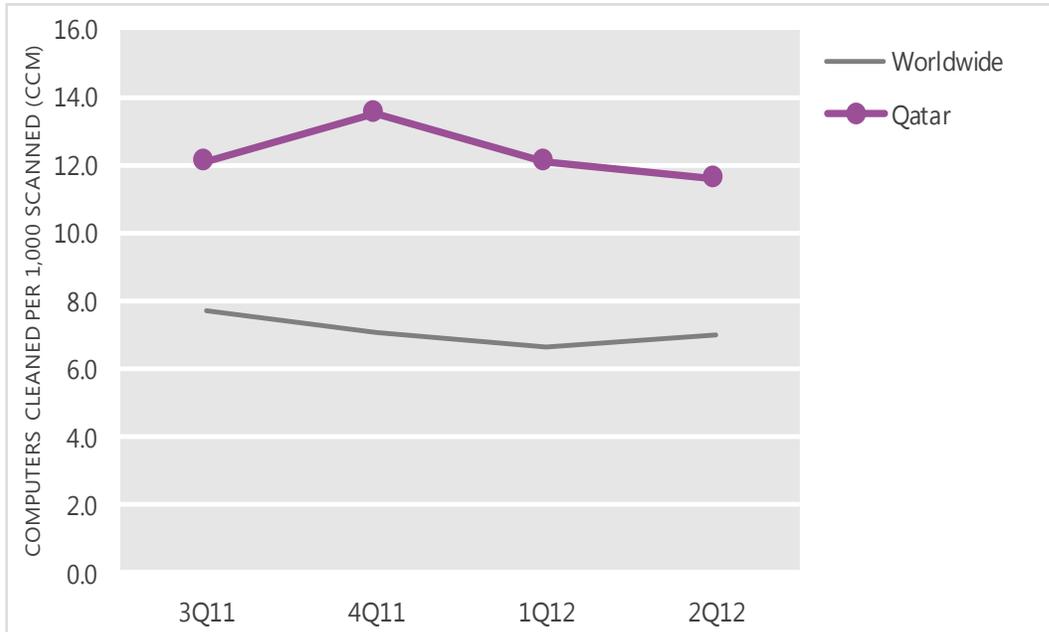
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	12.1	13.5	12.1	11.6
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

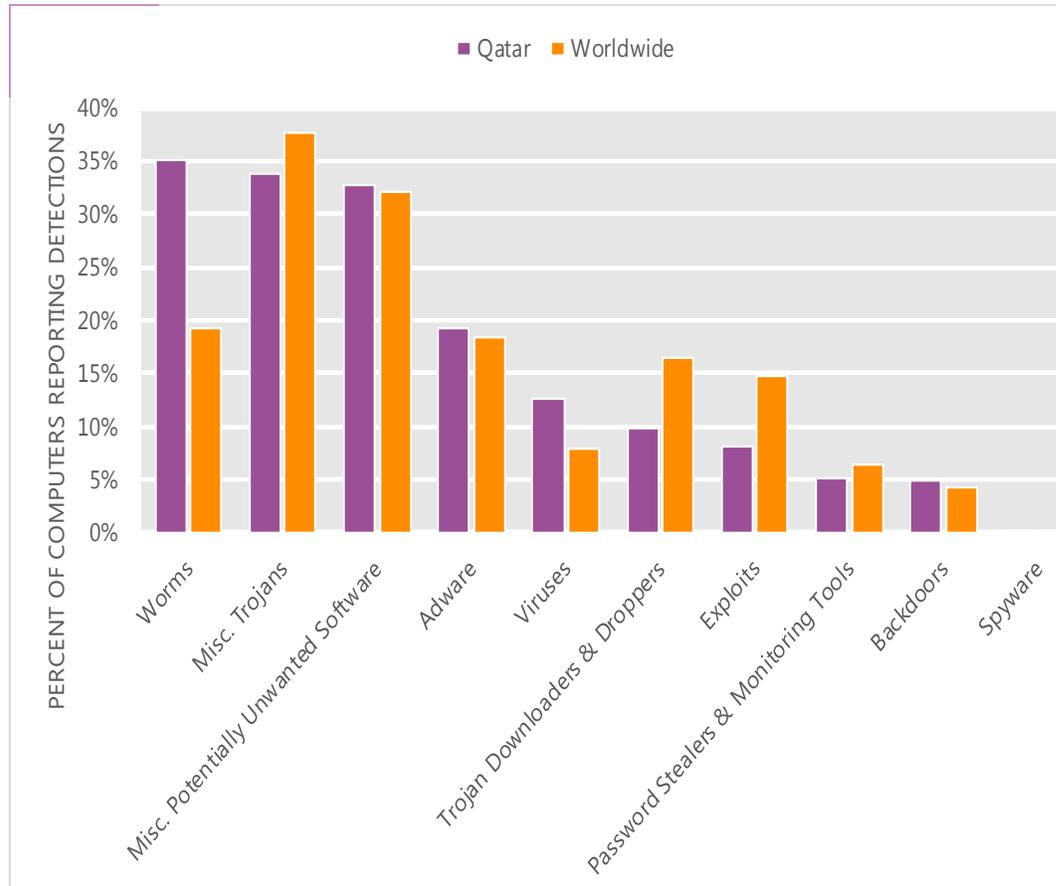
The MSRT detected malware on 11.6 of every 1,000 computers scanned in Qatar in 2Q12 (a CCM score of 11.6, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Qatar over the last four quarters, compared to the world as a whole.

CCM infection trends in Qatar and worldwide



Threat categories

Malware and potentially unwanted software categories in Qatar in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Qatar in 2Q12 was Worms. It affected 35.1 percent of all computers with detections there, down from 35.7 percent in 1Q12.
- The second most common category in Qatar in 2Q12 was Miscellaneous Trojans. It affected 33.7 percent of all computers with detections there, down from 34.9 percent in 1Q12.
- The third most common category in Qatar in 2Q12 was Miscellaneous Potentially Unwanted Software, which affected 32.8 percent of all computers with detections there, up from 32.7 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Qatar in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Autorun	Worms	15.2%
2	Win32/Keygen	Misc. Potentially Unwanted Software	11.3%
3	Win32/Hotbar	Adware	8.3%
4	Win32/Sality	Viruses	8.1%
5	Win32/Nuqel	Worms	7.3%
6	Win32/Zwangi	Misc. Potentially Unwanted Software	6.1%
7	Win32/Dorkbot	Worms	5.8%
8	Win32/Rimecud	Worms	5.5%
9	JS/Paypopup	Adware	5.0%
10	JS/IframeRef	Misc. Trojans	4.6%

- The most common threat family in Qatar in 2Q12 was [Win32/Autorun](#), which affected 15.2 percent of computers with detections in Qatar. [Win32/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 threat family in Qatar in 2Q12 was [Win32/Keygen](#), which affected 11.3 percent of computers with detections in Qatar. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The third most common threat family in Qatar in 2Q12 was [Win32/Hotbar](#), which affected 8.3 percent of computers with detections in Qatar. [Win32/Hotbar](#) is adware that displays a dynamic toolbar and targeted pop-up ads based on its monitoring of web-browsing activity.
- The fourth most common threat family in Qatar in 2Q12 was [Win32/Sality](#), which affected 8.1 percent of computers with detections in Qatar. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Qatar

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	1.09 (1.6)	0.73 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	3.28 (3.9)	4.00 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.02 (0.7)	0.05 (0.9)

Update service usage

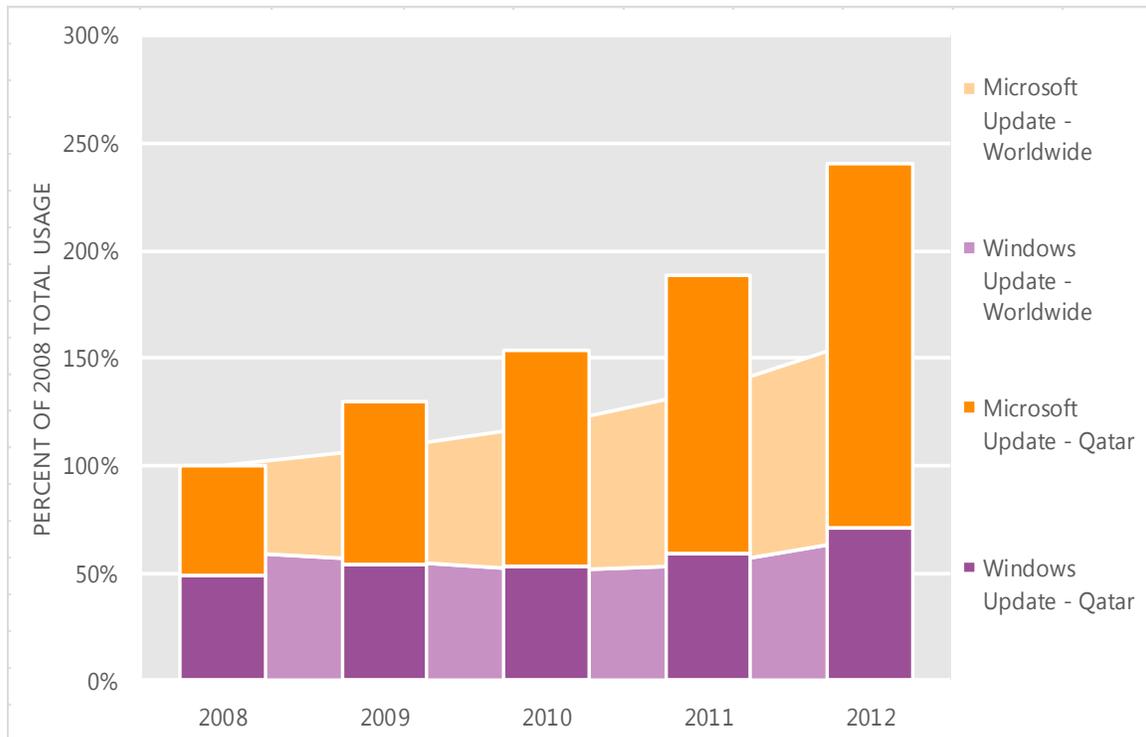
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Qatar and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Qatar over the last four years, indexed to the total usage for both services in Qatar in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Qatar was up 27.2 percent from 2011, and up 140.4 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Qatar in 2012, 70.4 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Romania

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Romania in 2Q12 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.

Infection rate statistics for Romania

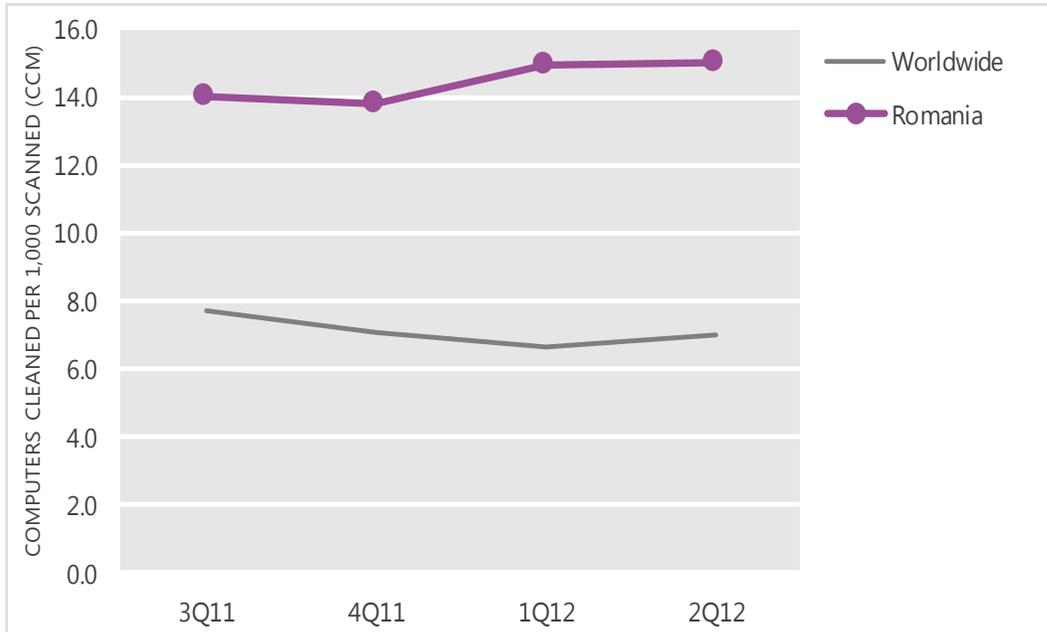
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	14.0	13.8	14.9	15.0
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

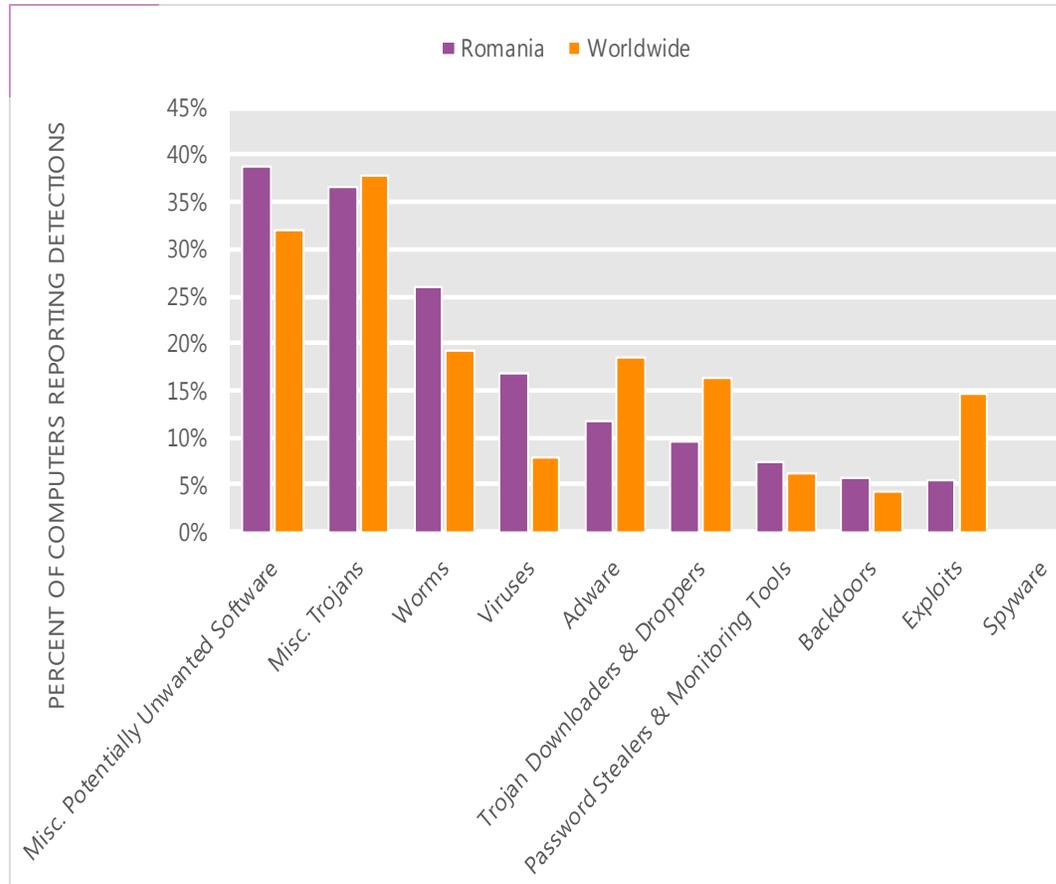
The MSRT detected malware on 15.0 of every 1,000 computers scanned in Romania in 2Q12 (a CCM score of 15.0, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Romania over the last four quarters, compared to the world as a whole.

CCM infection trends in Romania and worldwide



Threat categories

Malware and potentially unwanted software categories in Romania in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Romania in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 38.6 percent of all computers with detections there, down from 39.4 percent in 1Q12.
- The second most common category in Romania in 2Q12 was Miscellaneous Trojans. It affected 36.7 percent of all computers with detections there, down from 37.8 percent in 1Q12.
- The third most common category in Romania in 2Q12 was Worms, which affected 26.1 percent of all computers with detections there, up from 23.8 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Romania in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Sality	Viruses	15.3%
2	Win32/Keygen	Misc. Potentially Unwanted Software	14.7%
3	Win32/Autorun	Worms	11.6%
4	Win32/Conficker	Worms	6.7%
5	Win32/Pramro	Misc. Trojans	5.6%
6	JS/Pornpop	Adware	5.2%
7	Win32/Rimecud	Worms	4.3%
8	Win32/Obfuscator	Misc. Potentially Unwanted Software	4.1%
9	Win32/Brontok	Worms	3.5%
10	Win32/Wpkill	Misc. Potentially Unwanted Software	3.5%

- The most common threat family in Romania in 2Q12 was [Win32/Sality](#), which affected 15.3 percent of computers with detections in Romania. [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 in Romania in 2Q12 was [Win32/Keygen](#), which affected 14.7 percent of computers with detections in Romania. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The third most common threat family in Romania in 2Q12 was [Win32/Autorun](#), which affected 11.6 percent of computers with detections in Romania. [Win32/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 threat family in Romania in 2Q12 was [Win32/Conficker](#), which affected 6.7 percent of computers with detections in Romania. [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.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Romania

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	3.22 (1.6)	3.81 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	4.87 (3.9)	5.46 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	3.40 (0.7)	2.54 (0.9)

Update service usage

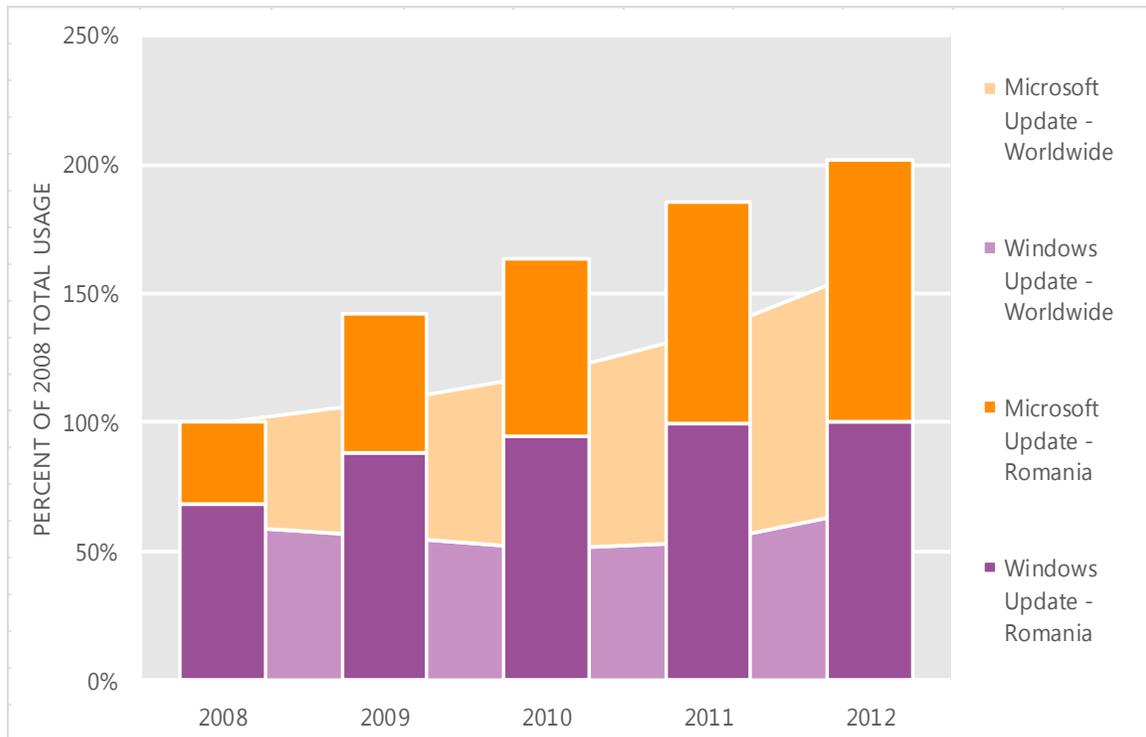
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Romania and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Romania over the last four years, indexed to the total usage for both services in Romania in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Romania was up 8.8 percent from 2011, and up 101.8 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Romania in 2012, 50.4 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Russia

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Russia in 2Q12 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.

Infection rate statistics for Russia

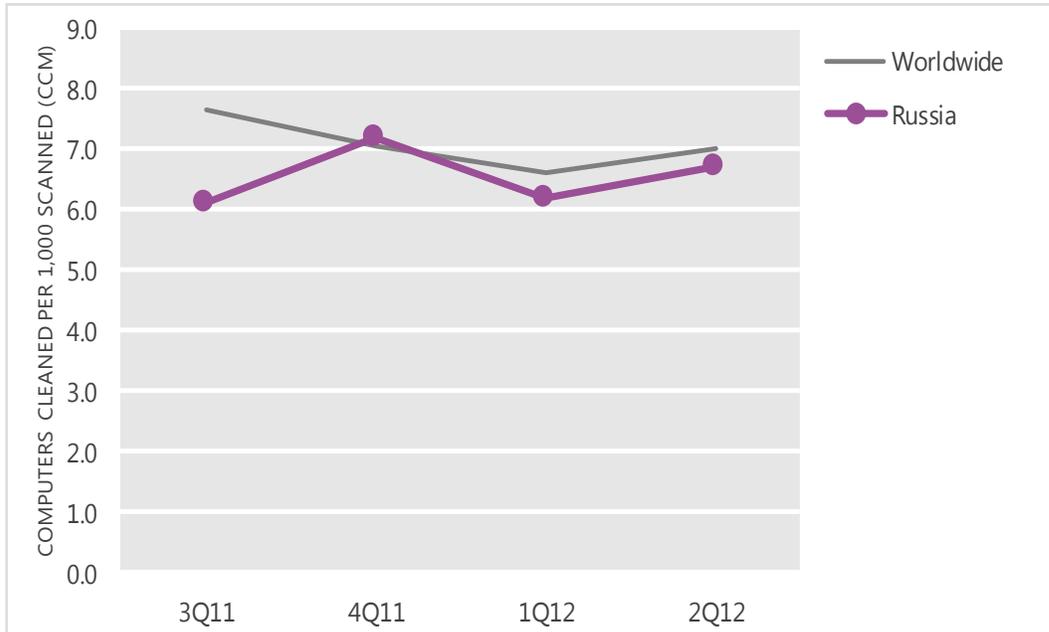
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	6.1	7.2	6.2	6.7
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

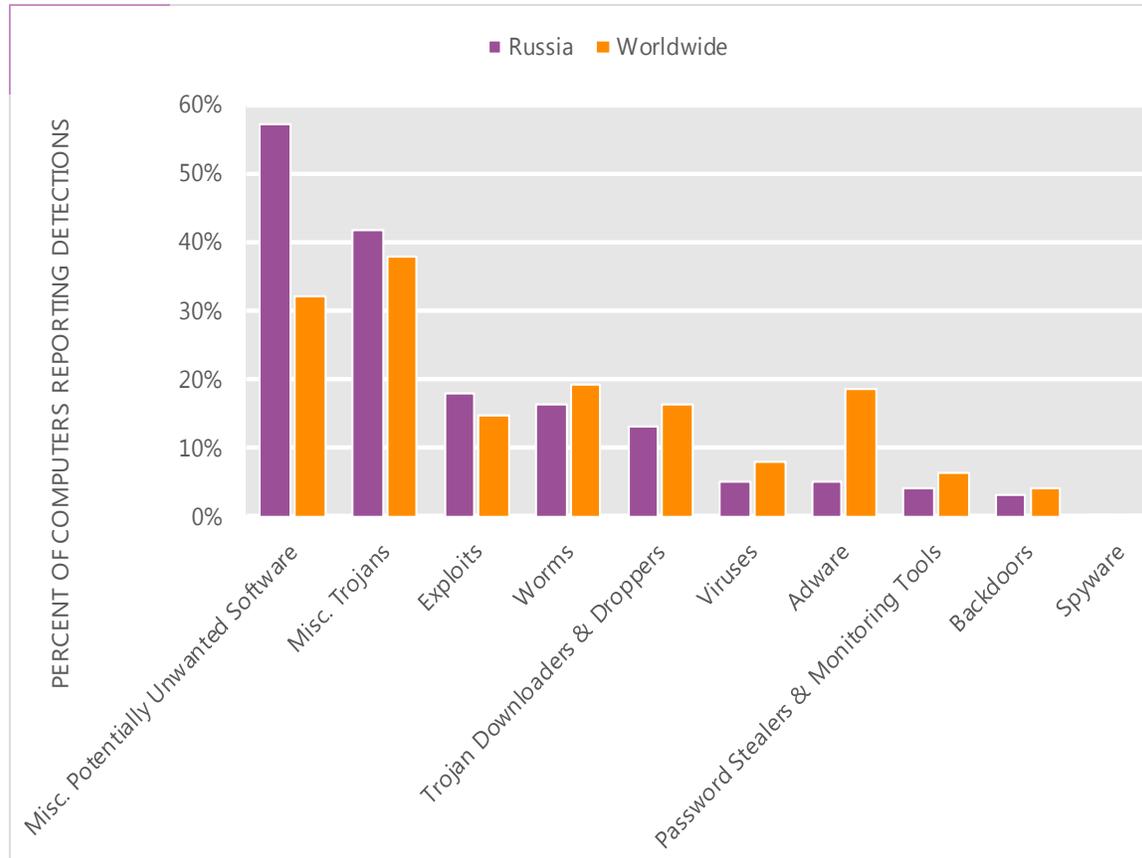
The MSRT detected malware on 6.7 of every 1,000 computers scanned in Russia in 2Q12 (a CCM score of 6.7, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Russia over the last four quarters, compared to the world as a whole.

CCM infection trends in Russia and worldwide



Threat categories

Malware and potentially unwanted software categories in Russia in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Russia in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 57.1 percent of all computers with detections there, down from 60.1 percent in 1Q12.
- The second most common category in Russia in 2Q12 was Miscellaneous Trojans. It affected 41.8 percent of all computers with detections there, up from 36.0 percent in 1Q12.
- The third most common category in Russia in 2Q12 was Exploits, which affected 17.8 percent of all computers with detections there, down from 18.4 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Russia in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Pameseg	Misc. Potentially Unwanted Software	29.0%
2	Win32/Keygen	Misc. Potentially Unwanted Software	12.6%
3	Win32/Obfuscator	Misc. Potentially Unwanted Software	11.0%
4	Java/Blacole	Exploits	9.3%
5	Win32/Vundo	Misc. Trojans	8.3%
6	HTML/SMSFakerweb	Misc. Trojans	7.1%
7	Win32/Carberp	Trojan Downloaders & Droppers	6.1%
8	Win32/Dorkbot	Worms	5.9%
9	Win32/Autorun	Worms	5.3%
10	JS/IframeRef	Misc. Trojans	4.3%

- The most common threat family in Russia in 2Q12 was [Win32/Pameseg](#), which affected 29.0 percent of computers with detections in Russia. [Win32/Pameseg](#) is a fake program installer that requires the user to send SMS messages to a premium number to successfully install certain programs.
- The second most common threat family in Russia in 2Q12 was [Win32/Keygen](#), which affected 12.6 percent of computers with detections in Russia. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The third most common threat family in Russia in 2Q12 was [Win32/Obfuscator](#), which affected 11.0 percent of computers with detections in Russia. [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 threat family in Russia in 2Q12 was [Java/Blacole](#), which affected 9.3 percent of computers with detections in Russia. [Java/Blacole](#) is an exploit pack, also known as Blackhole, that is installed on a compromised web server by an attacker and includes a number of exploits that target browser software. If a vulnerable computer browses a compromised website that contains the exploit pack, various malware may be downloaded and run.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Russia

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	3.03 (1.6)	3.46 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	7.46 (3.9)	7.69 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	2.02 (0.7)	2.66 (0.9)

Update service usage

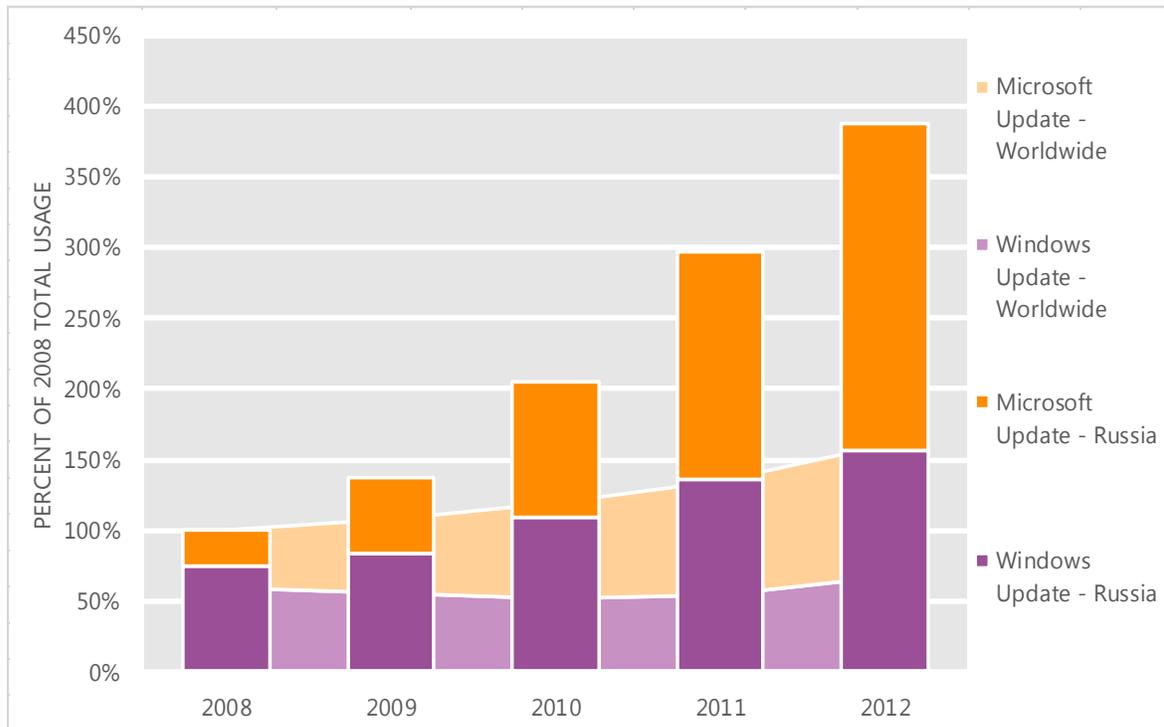
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Russia and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Russia over the last four years, indexed to the total usage for both services in Russia in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Russia was up 30.7 percent from 2011, and up 287.7 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Russia in 2012, 59.7 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Saudi Arabia

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Saudi Arabia in 2Q12 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.

Infection rate statistics for Saudi Arabia

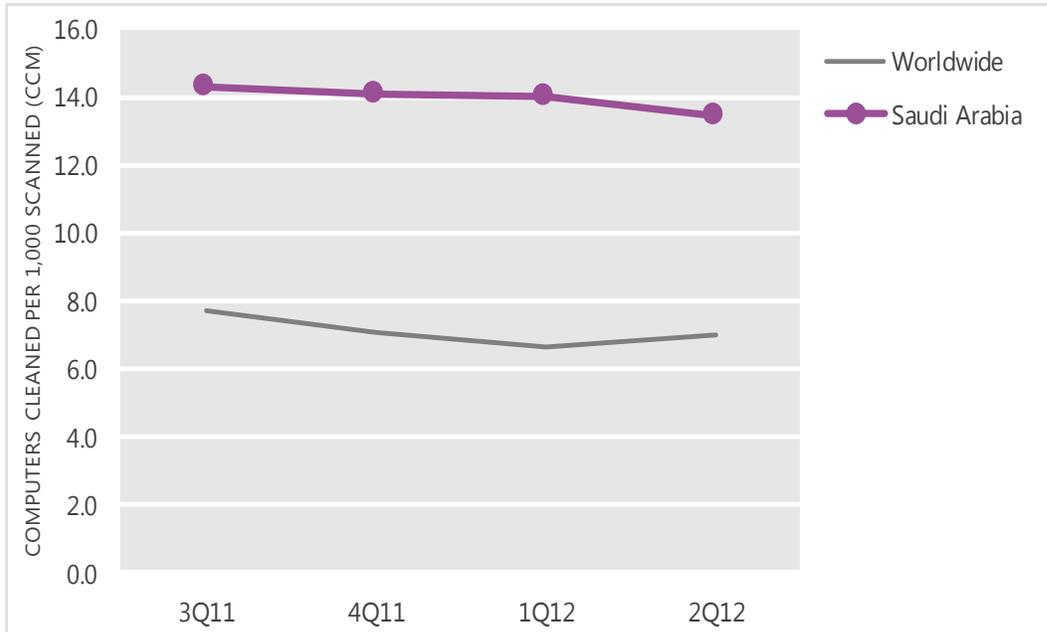
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	14.3	14.1	14.0	13.4
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

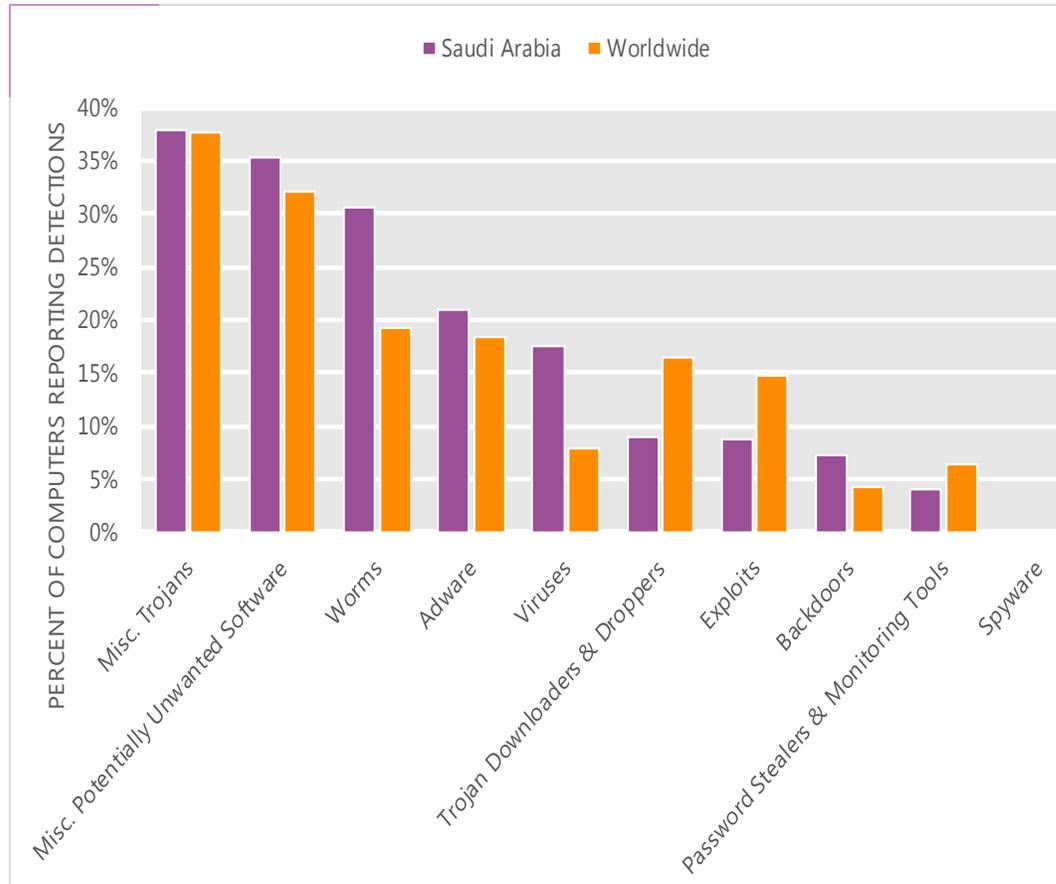
The MSRT detected malware on 13.4 of every 1,000 computers scanned in Saudi Arabia in 2Q12 (a CCM score of 13.4, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Saudi Arabia over the last four quarters, compared to the world as a whole.

CCM infection trends in Saudi Arabia and worldwide



Threat categories

Malware and potentially unwanted software categories in Saudi Arabia in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Saudi Arabia in 2Q12 was Miscellaneous Trojans. It affected 37.8 percent of all computers with detections there, down from 39.1 percent in 1Q12.
- The second most common category in Saudi Arabia in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 35.2 percent of all computers with detections there, down from 35.8 percent in 1Q12.
- The third most common category in Saudi Arabia in 2Q12 was Worms, which affected 30.5 percent of all computers with detections there, up from 30.5 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Saudi Arabia in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Keygen	Misc. Potentially Unwanted Software	14.5%
2	Win32/Autorun	Worms	13.1%
3	JS/Paypopup	Adware	11.9%
4	Win32/Sality	Viruses	11.1%
5	Win32/Ramnit	Misc. Trojans	6.4%
6	Win32/Agent	Misc. Trojans	6.0%
7	Win32/Dorkbot	Worms	5.7%
8	Win32/CplLnk	Exploits	5.1%
9	Win32/Hotbar	Adware	4.5%
10	Win32/Rimecud	Worms	4.2%

- The most common threat family in Saudi Arabia in 2Q12 was [Win32/Keygen](#), which affected 14.5 percent of computers with detections in Saudi Arabia. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The second most common threat family in Saudi Arabia in 2Q12 was [Win32/Autorun](#), which affected 13.1 percent of computers with detections in Saudi Arabia. [Win32/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 threat family in Saudi Arabia in 2Q12 was [JS/Paypopup](#), which affected 11.9 percent of computers with detections in Saudi Arabia. [JS/Paypopup](#) is a detection for specially-crafted JavaScript-enabled objects that attempt to display pop-up and pop-under advertisements in new browser windows.
- The fourth most common threat family in Saudi Arabia in 2Q12 was [Win32/Sality](#), which affected 11.1 percent of computers with detections in Saudi Arabia. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Saudi Arabia

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	1.49 (1.6)	0.62 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	2.17 (3.9)	2.17 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.01 (0.7)	0.22 (0.9)

Update service usage

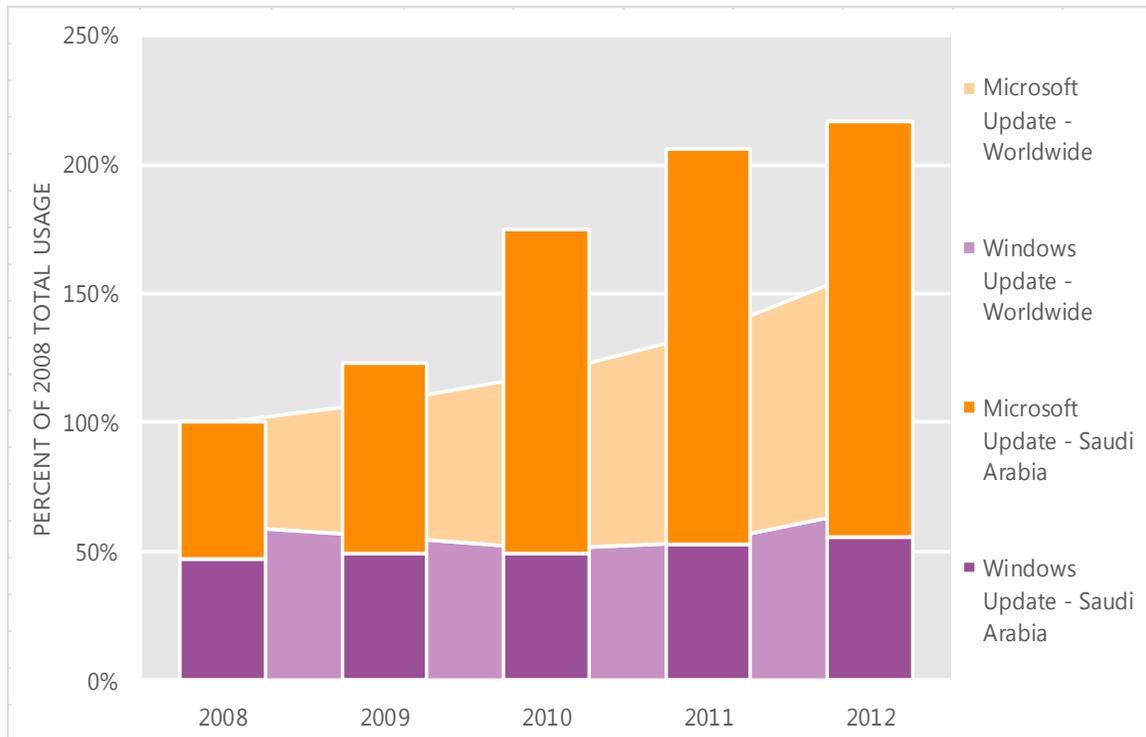
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Saudi Arabia and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Saudi Arabia over the last four years, indexed to the total usage for both services in Saudi Arabia in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Saudi Arabia was up 5.2 percent from 2011, and up 116.6 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Saudi Arabia in 2012, 74.2 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Senegal

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Senegal in 2Q12 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.

Infection rate statistics for Senegal

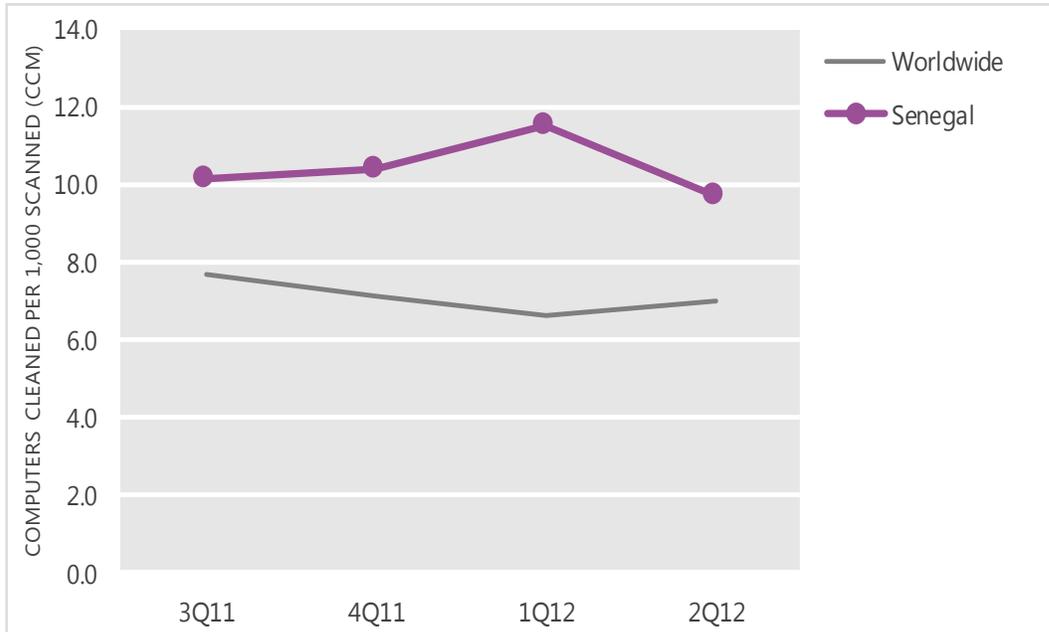
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	10.1	10.4	11.5	9.7
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

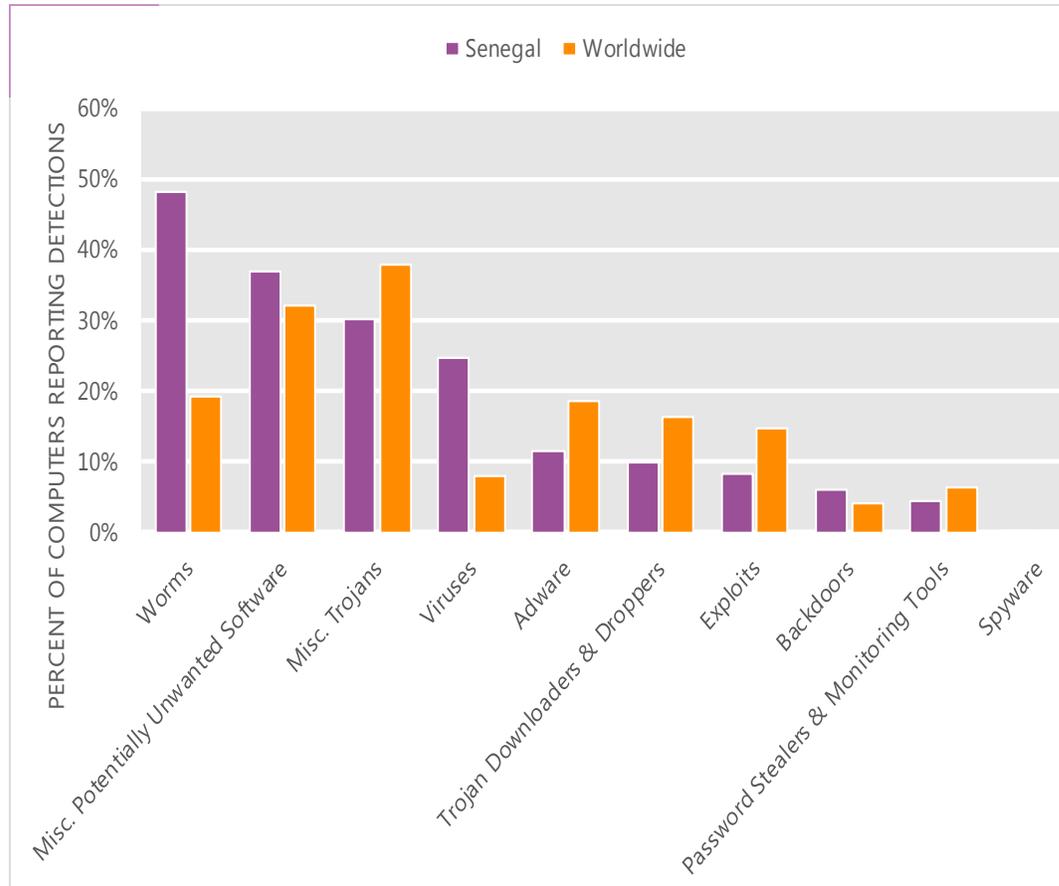
The MSRT detected malware on 9.7 of every 1,000 computers scanned in Senegal in 2Q12 (a CCM score of 9.7, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Senegal over the last four quarters, compared to the world as a whole.

CCM infection trends in Senegal and worldwide



Threat categories

Malware and potentially unwanted software categories in Senegal in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Senegal in 2Q12 was Worms. It affected 48.1 percent of all computers with detections there, up from 46.8 percent in 1Q12.
- The second most common category in Senegal in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 36.9 percent of all computers with detections there, down from 37.1 percent in 1Q12.
- The third most common category in Senegal in 2Q12 was Miscellaneous Trojans, which affected 30.2 percent of all computers with detections there, up from 29.2 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Senegal in 2Q12

	Family	Most significant category	% of computers with detections
1	VBS/Cinera	Worms	20.4%
2	Win32/Autorun	Worms	19.7%
3	Win32/Sality	Viruses	17.2%
4	Win32/Vobfus	Worms	14.4%
5	Win32/Keygen	Misc. Potentially Unwanted Software	9.5%
6	Win32/Dorkbot	Worms	7.6%
7	Win32/Ramnit	Misc. Trojans	6.4%
8	Win32/CplLnk	Exploits	5.9%
9	Win32/Mabezat	Viruses	5.6%
10	Win32/Hotbar	Adware	5.4%

- The most common threat family in Senegal in 2Q12 was [VBS/Cinera](#), which affected 20.4 percent of computers with detections in Senegal. [VBS/Cinera](#) is a self-propagating VBScript worm that spreads via removable drives and displays images of the attacker's choice.
- The second most common threat family in Senegal in 2Q12 was [Win32/Autorun](#), which affected 19.7 percent of computers with detections in Senegal. [Win32/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 threat family in Senegal in 2Q12 was [Win32/Sality](#), which affected 17.2 percent of computers with detections in Senegal. [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 in Senegal in 2Q12 was [Win32/Vobfus](#), which affected 14.4 percent of computers with detections in Senegal. [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.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Senegal

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	N/A (1.6)	N/A (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	N/A (3.9)	N/A (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.02 (0.7)	N/A (0.9)

Update service usage

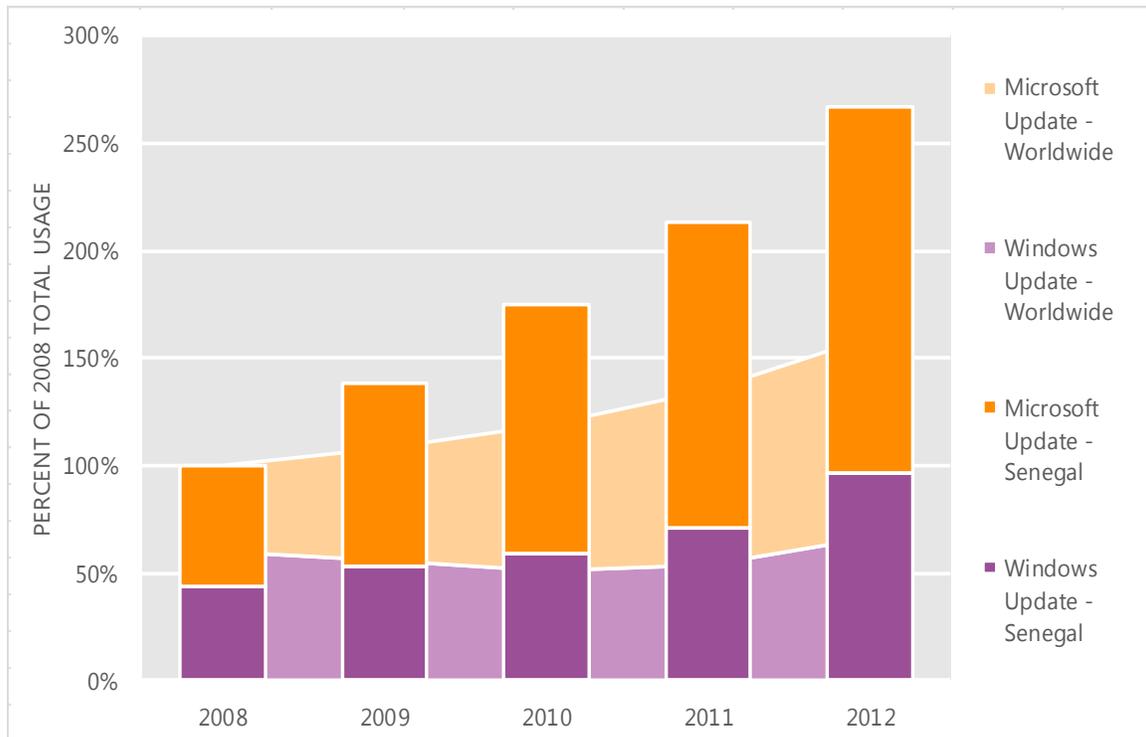
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Senegal and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Senegal over the last four years, indexed to the total usage for both services in Senegal in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Senegal was up 25.5 percent from 2011, and up 167.3 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Senegal in 2012, 63.9 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Singapore

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Singapore in 2Q12 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.

Infection rate statistics for Singapore

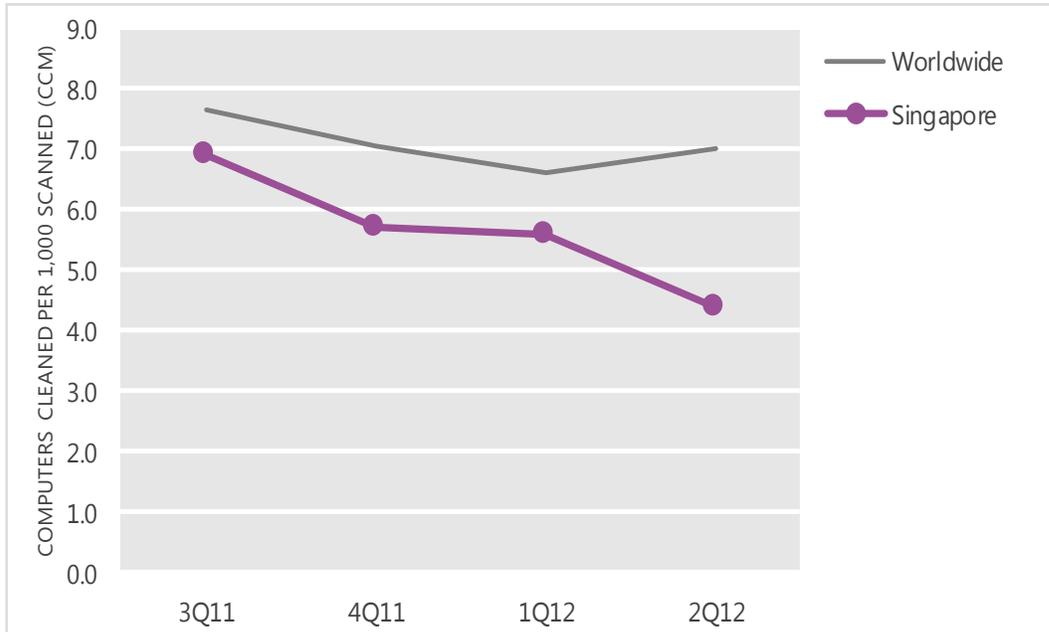
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	6.9	5.7	5.6	4.4
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

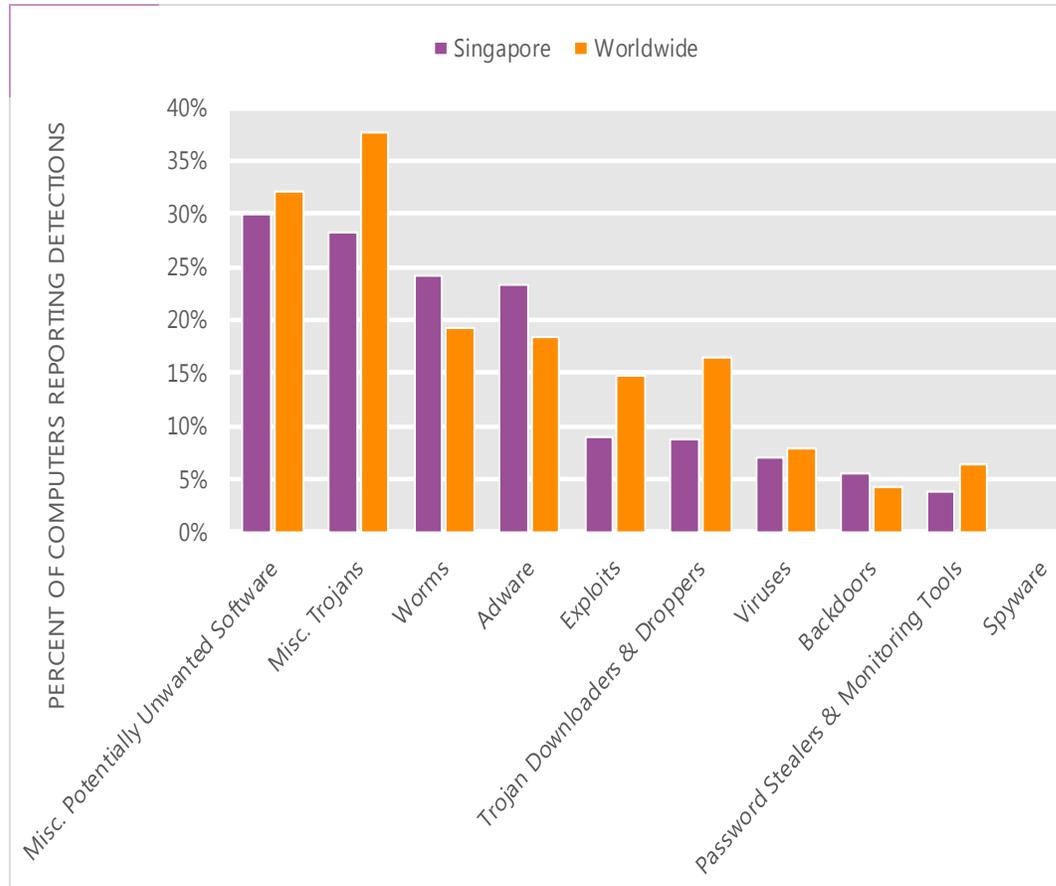
The MSRT detected malware on 4.4 of every 1,000 computers scanned in Singapore in 2Q12 (a CCM score of 4.4, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Singapore over the last four quarters, compared to the world as a whole.

CCM infection trends in Singapore and worldwide



Threat categories

Malware and potentially unwanted software categories in Singapore in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Singapore in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 30.0 percent of all computers with detections there, down from 30.5 percent in 1Q12.
- The second most common category in Singapore in 2Q12 was Miscellaneous Trojans. It affected 28.2 percent of all computers with detections there, up from 26.3 percent in 1Q12.
- The third most common category in Singapore in 2Q12 was Worms, which affected 24.2 percent of all computers with detections there, down from 26.0 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Singapore in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Hotbar	Adware	9.5%
2	Win32/Autorun	Worms	9.5%
3	Win32/Keygen	Misc. Potentially Unwanted Software	9.4%
4	JS/Pornpop	Adware	7.6%
5	JS/IframeRef	Misc. Trojans	6.7%
6	Win32/Zwangi	Misc. Potentially Unwanted Software	6.1%
7	Win32/Dorkbot	Worms	5.9%
8	Win32/Conficker	Worms	3.4%
9	Win32/OpenCandy	Adware	3.4%
10	Win32/Sality	Viruses	3.2%

- The most common threat family in Singapore in 2Q12 was [Win32/Hotbar](#), which affected 9.5 percent of computers with detections in Singapore. [Win32/Hotbar](#) is adware that displays a dynamic toolbar and targeted pop-up ads based on its monitoring of web-browsing activity.
- The second most common threat family in Singapore in 2Q12 was [Win32/Autorun](#), which affected 9.5 percent of computers with detections in Singapore. [Win32/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 threat family in Singapore in 2Q12 was [Win32/Keygen](#), which affected 9.4 percent of computers with detections in Singapore. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The fourth most common threat family in Singapore in 2Q12 was [JS/Pornpop](#), which affected 7.6 percent of computers with detections in Singapore. [JS/Pornpop](#) is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Singapore

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	1.12 (1.6)	1.10 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	2.74 (3.9)	5.02 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.77 (0.7)	1.36 (0.9)

Update service usage

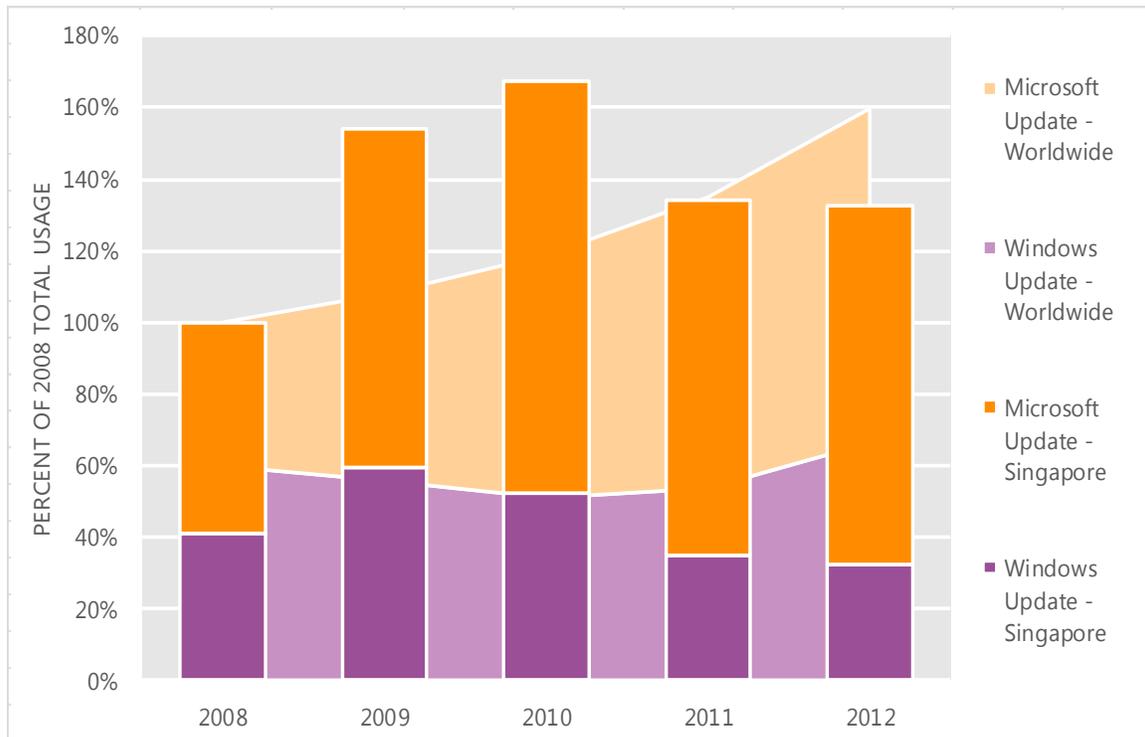
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Singapore and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Singapore over the last four years, indexed to the total usage for both services in Singapore in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Singapore was down 1.3 percent from 2011, and up 32.4 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Singapore in 2012, 75.5 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Slovakia

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Slovakia in 2Q12 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.

Infection rate statistics for Slovakia

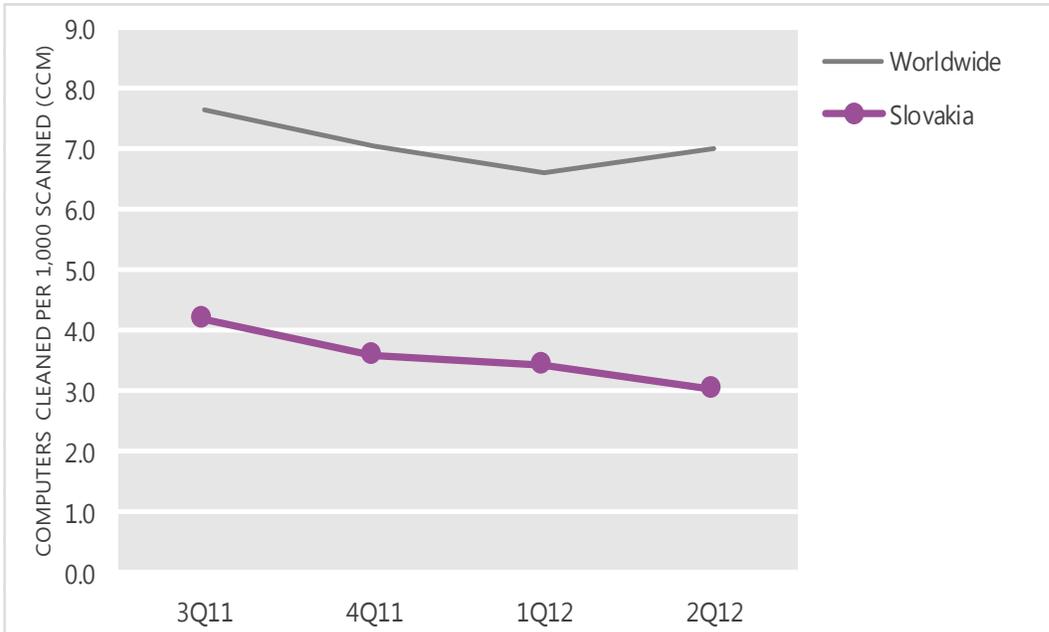
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	4.2	3.6	3.4	3.0
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

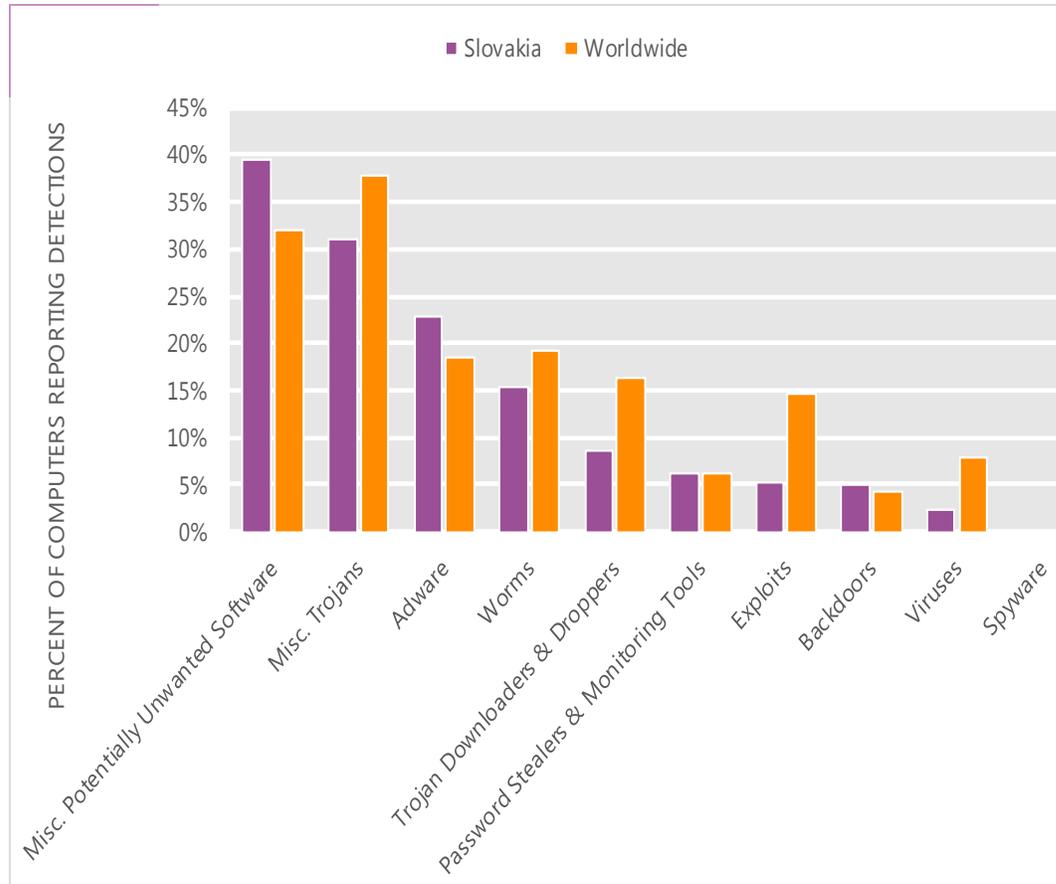
The MSRT detected malware on 3.0 of every 1,000 computers scanned in Slovakia in 2Q12 (a CCM score of 3.0, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Slovakia over the last four quarters, compared to the world as a whole.

CCM infection trends in Slovakia and worldwide



Threat categories

Malware and potentially unwanted software categories in Slovakia in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Slovakia in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 39.5 percent of all computers with detections there, up from 39.2 percent in 1Q12.
- The second most common category in Slovakia in 2Q12 was Miscellaneous Trojans. It affected 31.1 percent of all computers with detections there, up from 30.1 percent in 1Q12.
- The third most common category in Slovakia in 2Q12 was Adware, which affected 22.9 percent of all computers with detections there, down from 28.7 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Slovakia in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Keygen	Misc. Potentially Unwanted Software	17.3%
2	JS/Pornpop	Adware	9.6%
3	Win32/Autorun	Worms	7.2%
4	Win32/Hotbar	Adware	5.0%
5	Win32/Zwangi	Misc. Potentially Unwanted Software	4.8%
6	Win32/Obfuscator	Misc. Potentially Unwanted Software	4.2%
7	Win32/OpenCandy	Adware	3.9%
8	Win32/Dynamer	Misc. Trojans	3.6%
9	JS/IframeRef	Misc. Trojans	3.3%
10	Win32/GamePlayLabs	Adware	2.9%

- The most common threat family in Slovakia in 2Q12 was [Win32/Keygen](#), which affected 17.3 percent of computers with detections in Slovakia. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The second most common threat family in Slovakia in 2Q12 was [JS/Pornpop](#), which affected 9.6 percent of computers with detections in Slovakia. [JS/Pornpop](#) is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The third most common threat family in Slovakia in 2Q12 was [Win32/Autorun](#), which affected 7.2 percent of computers with detections in Slovakia. [Win32/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 threat family in Slovakia in 2Q12 was [Win32/Hotbar](#), which affected 5.0 percent of computers with detections in Slovakia. [Win32/Hotbar](#) is adware that displays a dynamic toolbar and targeted pop-up ads based on its monitoring of web-browsing activity.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Slovakia

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	1.60 (1.6)	2.23 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	1.52 (3.9)	1.52 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.75 (0.7)	0.29 (0.9)

Update service usage

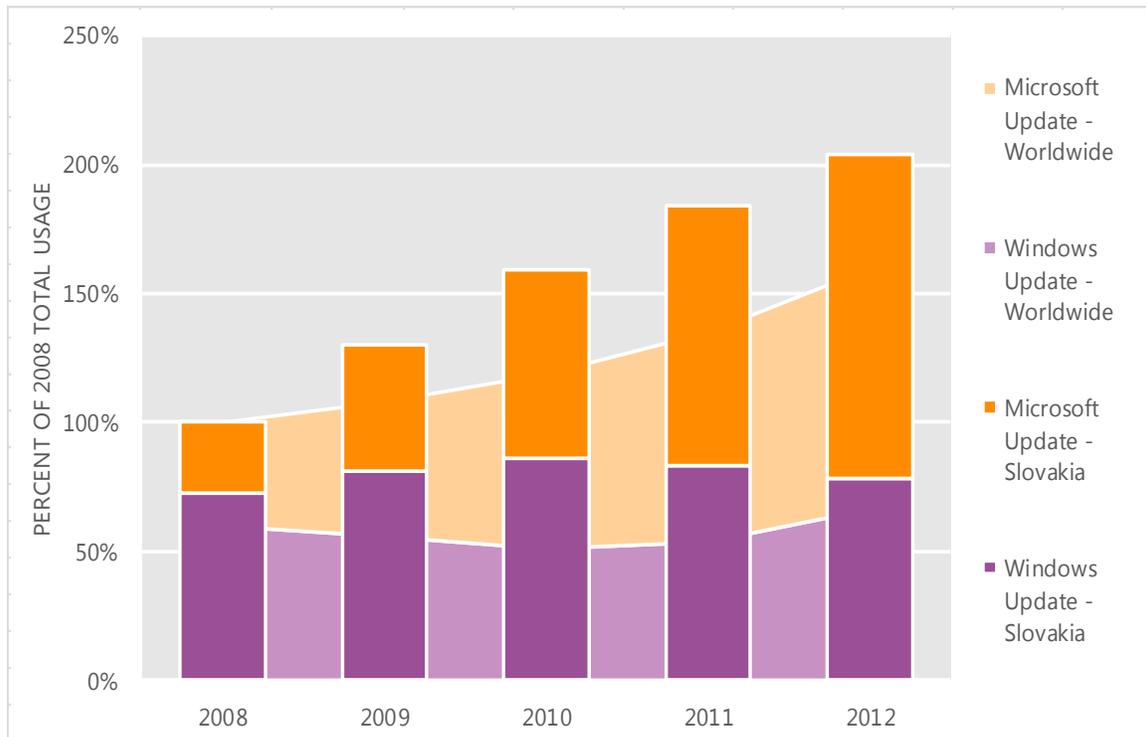
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Slovakia and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Slovakia over the last four years, indexed to the total usage for both services in Slovakia in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Slovakia was up 10.8 percent from 2011, and up 103.8 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Slovakia in 2012, 61.4 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Slovenia

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Slovenia in 2Q12 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.

Infection rate statistics for Slovenia

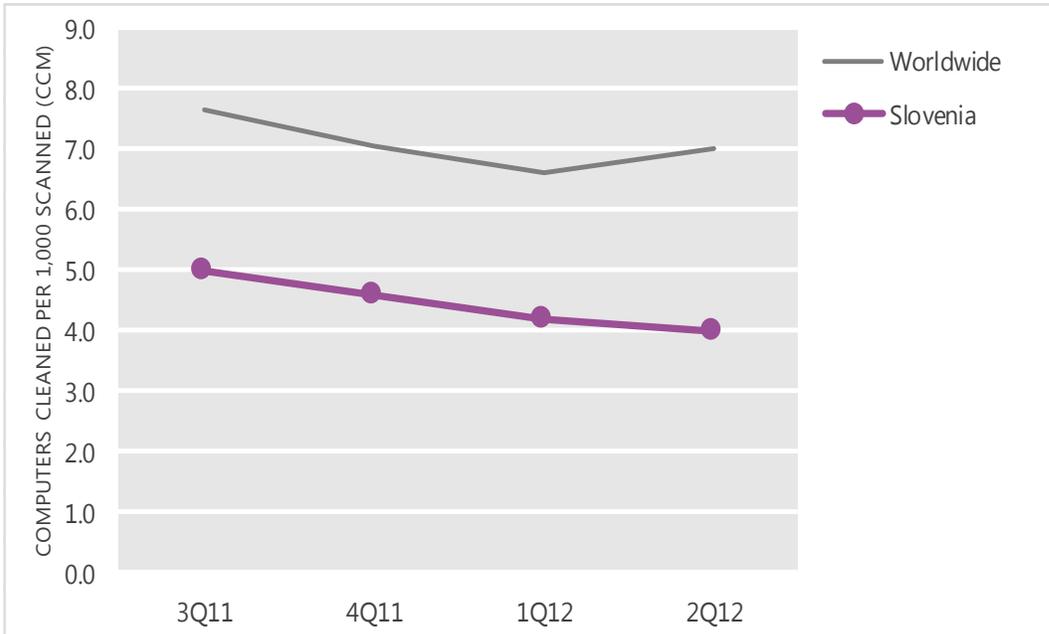
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	5.0	4.6	4.2	4.0
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

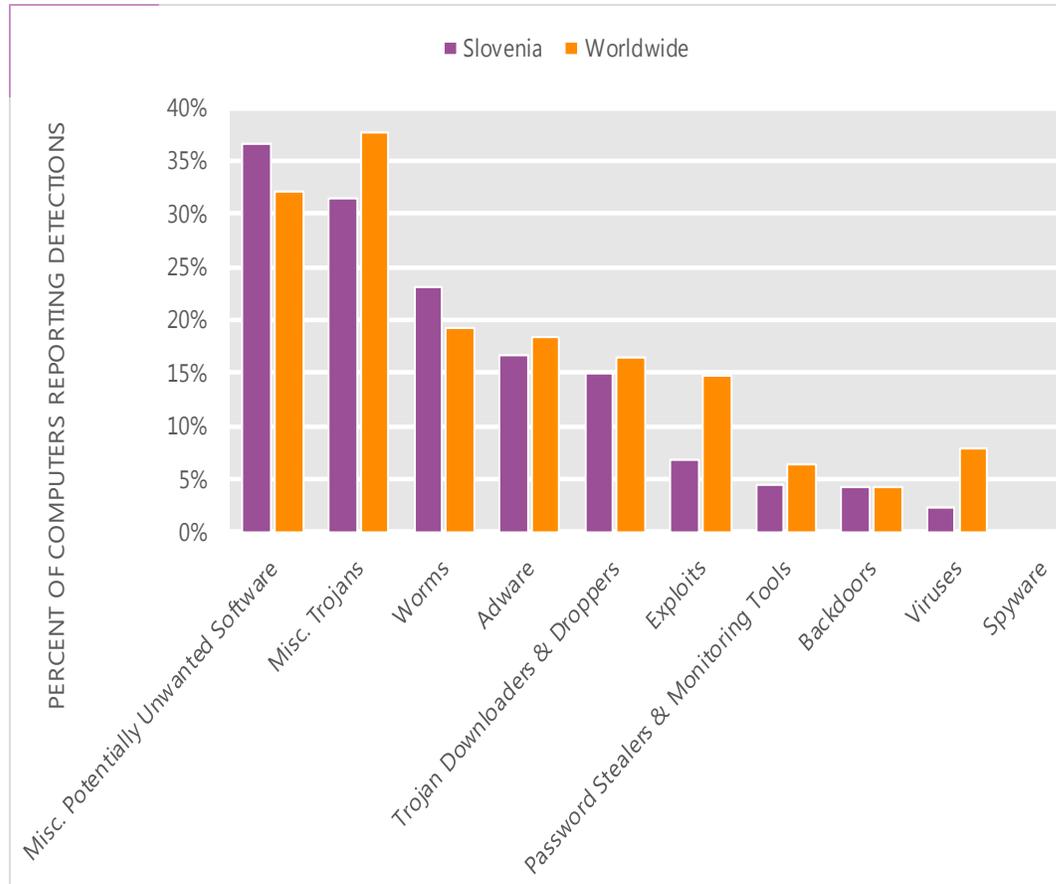
The MSRT detected malware on 4.0 of every 1,000 computers scanned in Slovenia in 2Q12 (a CCM score of 4.0, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Slovenia over the last four quarters, compared to the world as a whole.

CCM infection trends in Slovenia and worldwide



Threat categories

Malware and potentially unwanted software categories in Slovenia in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Slovenia in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 36.6 percent of all computers with detections there, down from 40.4 percent in 1Q12.
- The second most common category in Slovenia in 2Q12 was Miscellaneous Trojans. It affected 31.4 percent of all computers with detections there, down from 32.3 percent in 1Q12.
- The third most common category in Slovenia in 2Q12 was Worms, which affected 23.0 percent of all computers with detections there, up from 14.2 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Slovenia in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Keygen	Misc. Potentially Unwanted Software	15.9%
2	ASX/Wimad	Trojan Downloaders & Droppers	8.4%
3	Win32/Pushbot	Worms	7.4%
4	JS/Pornpop	Adware	7.1%
5	Win32/Autorun	Worms	5.0%
6	Win32/Hotbar	Adware	5.0%
7	Win32/Zwangi	Misc. Potentially Unwanted Software	4.5%
8	Win32/Obfuscator	Misc. Potentially Unwanted Software	3.8%
9	JS/IframeRef	Misc. Trojans	3.5%
10	Win32/Conficker	Worms	3.2%

- The most common threat family in Slovenia in 2Q12 was [Win32/Keygen](#), which affected 15.9 percent of computers with detections in Slovenia. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The second most common threat family in Slovenia in 2Q12 was [ASX/Wimad](#), which affected 8.4 percent of computers with detections in Slovenia. [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 third most common threat family in Slovenia in 2Q12 was [Win32/Pushbot](#), which affected 7.4 percent of computers with detections in Slovenia. [Win32/Pushbot](#) is a detection for a family of malware that spreads via MSN Messenger, Yahoo! Messenger and AIM when commanded by a remote attacker. It contains backdoor functionality that allows unauthorized access and control of an affected computer.
- The fourth most common threat family in Slovenia in 2Q12 was [JS/Pornpop](#), which affected 7.1 percent of computers with detections in Slovenia. [JS/Pornpop](#) is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Slovenia

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	0.60 (1.6)	1.08 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	1.45 (3.9)	1.33 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.15 (0.7)	0.65 (0.9)

Update service usage

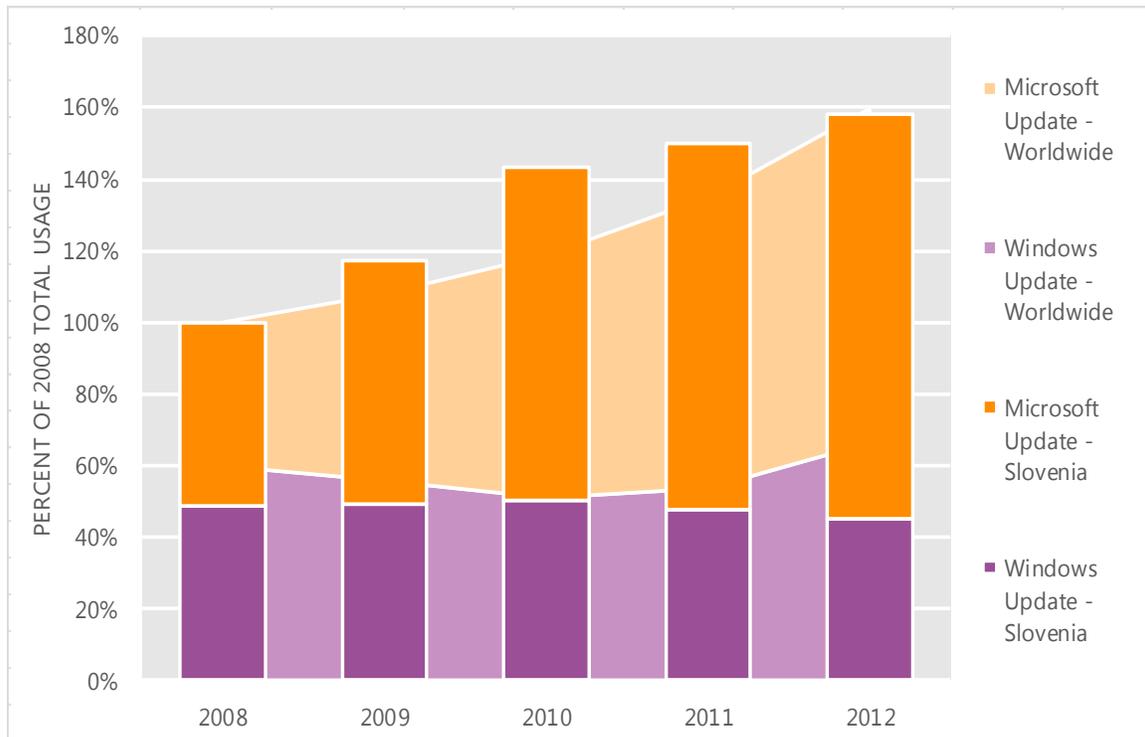
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Slovenia and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Slovenia over the last four years, indexed to the total usage for both services in Slovenia in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Slovenia was up 5.6 percent from 2011, and up 58.4 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Slovenia in 2012, 71.4 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

South Africa

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in South Africa in 2Q12 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.

Infection rate statistics for South Africa

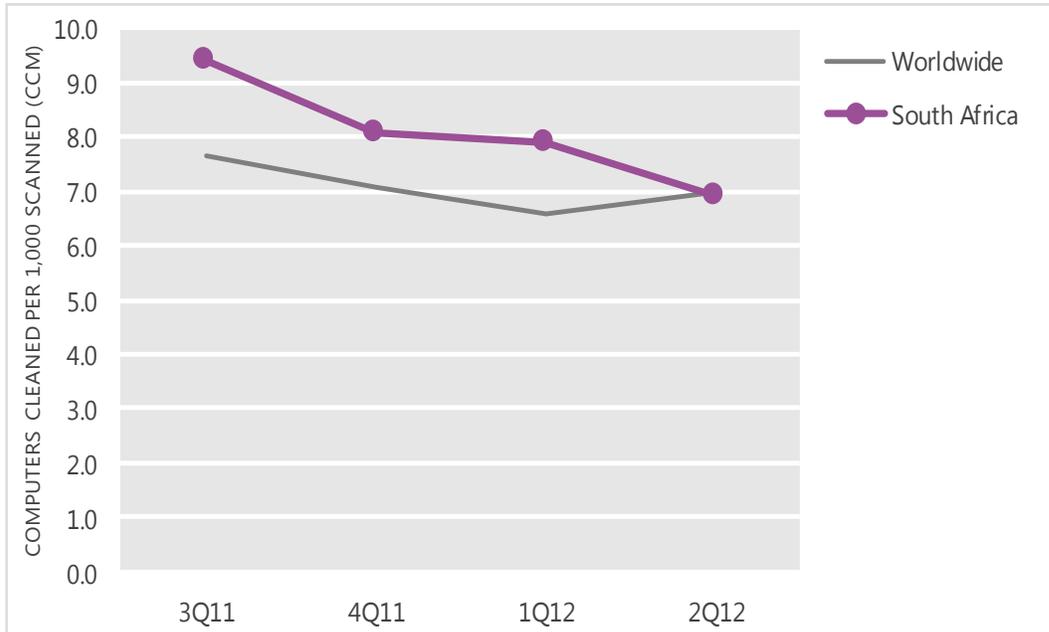
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	9.4	8.1	7.9	6.9
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

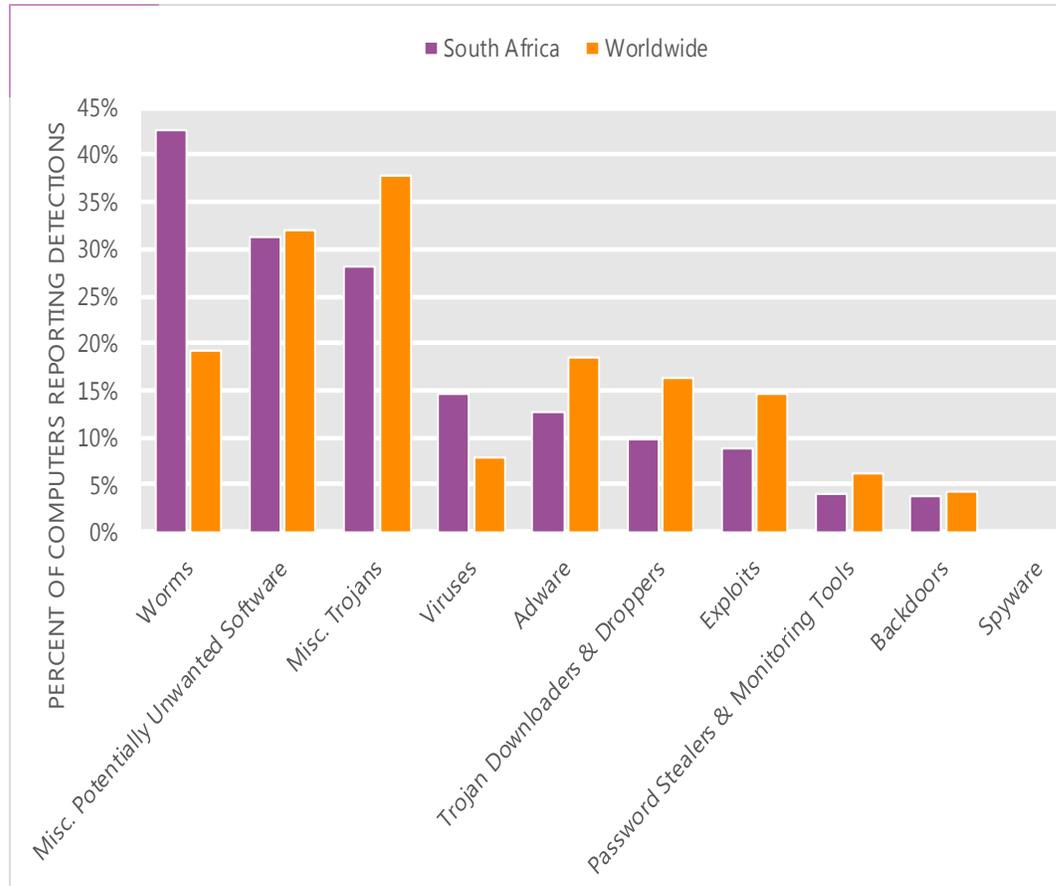
The MSRT detected malware on 6.9 of every 1,000 computers scanned in South Africa in 2Q12 (a CCM score of 6.9, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for South Africa over the last four quarters, compared to the world as a whole.

CCM infection trends in South Africa and worldwide



Threat categories

Malware and potentially unwanted software categories in South Africa in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in South Africa in 2Q12 was Worms. It affected 42.5 percent of all computers with detections there, down from 43.1 percent in 1Q12.
- The second most common category in South Africa in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 31.3 percent of all computers with detections there, up from 30.2 percent in 1Q12.
- The third most common category in South Africa in 2Q12 was Miscellaneous Trojans, which affected 28.1 percent of all computers with detections there, up from 24.9 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in South Africa in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Autorun	Worms	17.9%
2	Win32/Vobfus	Worms	12.8%
3	Win32/Keygen	Misc. Potentially Unwanted Software	9.2%
4	Win32/Rimecud	Worms	8.5%
5	Win32/Virut	Viruses	5.7%
6	Win32/Nuqel	Worms	5.5%
7	JS/Pornpop	Adware	5.3%
8	Win32/Sality	Viruses	5.2%
9	Win32/Dorkbot	Worms	4.7%
10	Win32/Mabezat	Viruses	4.1%

- The most common threat family in South Africa in 2Q12 was [Win32/Autorun](#), which affected 17.9 percent of computers with detections in South Africa. [Win32/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 threat family in South Africa in 2Q12 was [Win32/Vobfus](#), which affected 12.8 percent of computers with detections in South Africa. [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 in South Africa in 2Q12 was [Win32/Keygen](#), which affected 9.2 percent of computers with detections in South Africa. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The fourth most common threat family in South Africa in 2Q12 was [Win32/Rimecud](#), which affected 8.5 percent of computers with detections in South Africa. [Win32/Rimecud](#) is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for South Africa

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	1.95 (1.6)	2.48 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	3.38 (3.9)	3.67 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.17 (0.7)	0.55 (0.9)

Update service usage

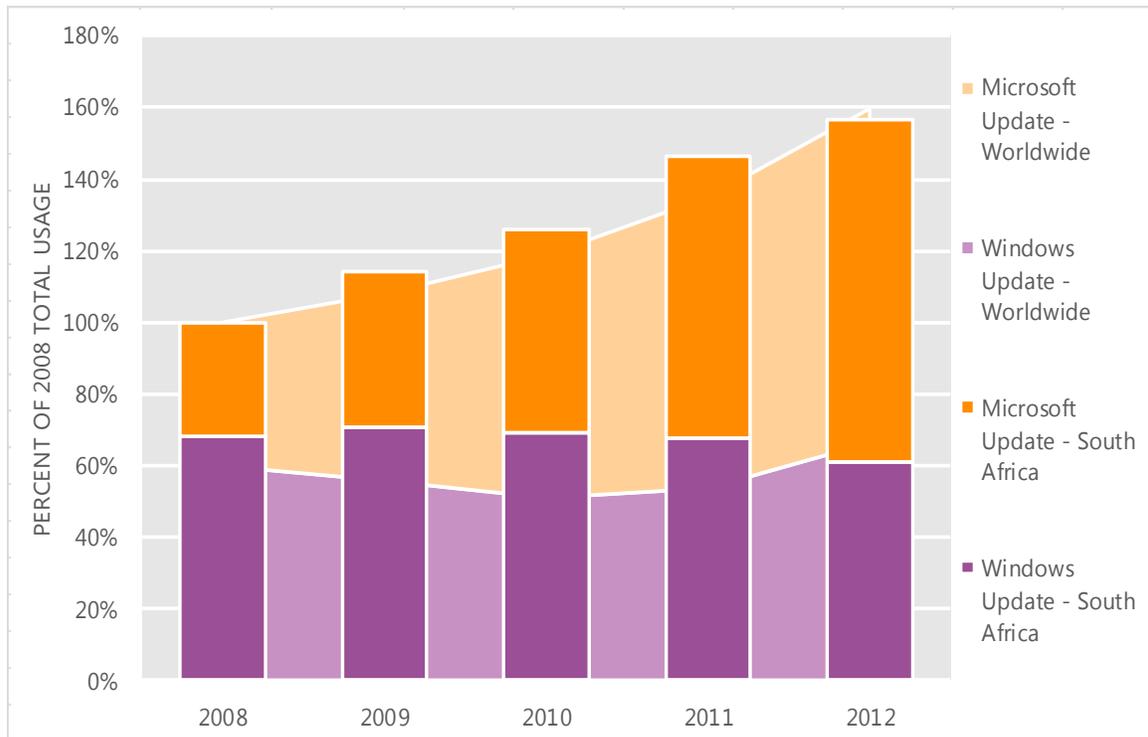
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in South Africa and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in South Africa over the last four years, indexed to the total usage for both services in South Africa in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in South Africa was up 7.0 percent from 2011, and up 56.5 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in South Africa in 2012, 61.1 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Spain

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Spain in 2Q12 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.

Infection rate statistics for Spain

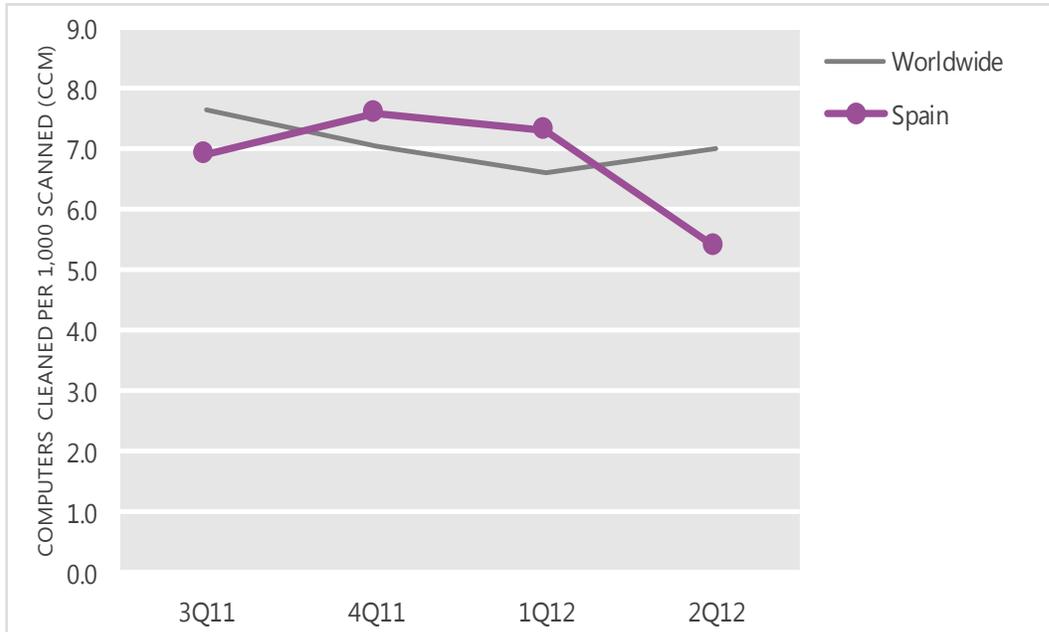
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	6.9	7.6	7.3	5.4
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

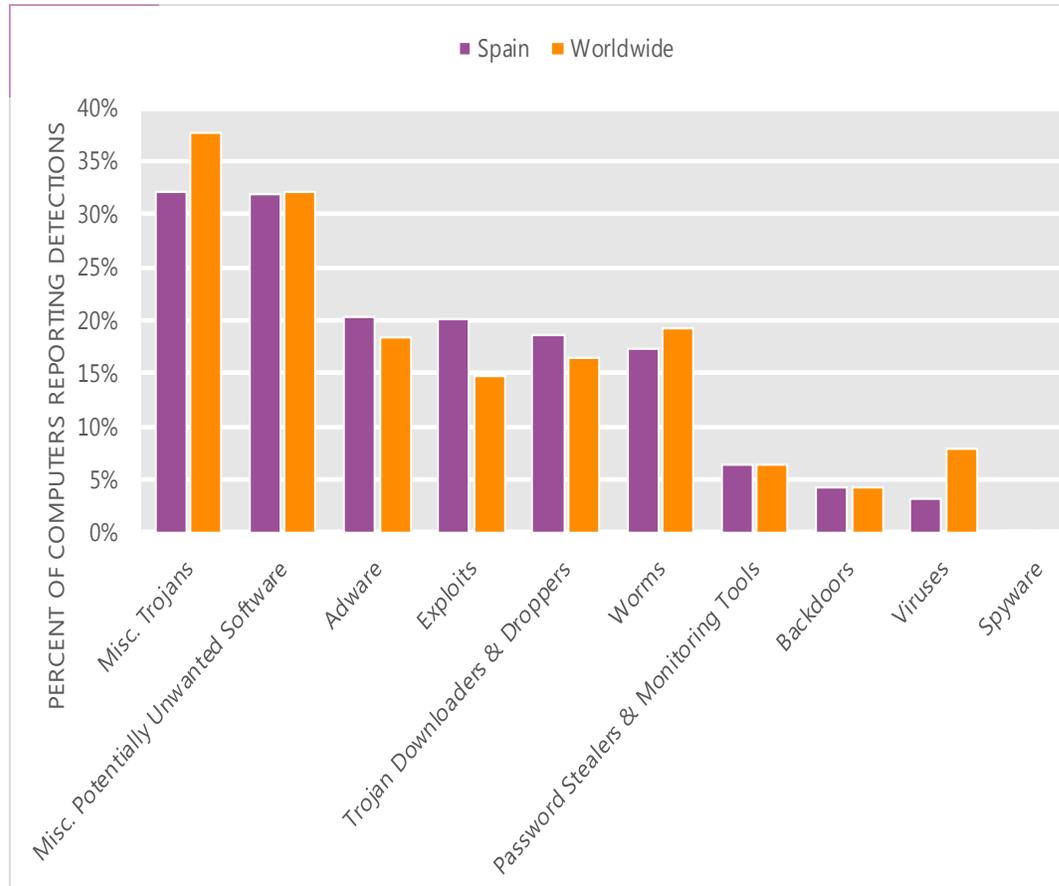
The MSRT detected malware on 5.4 of every 1,000 computers scanned in Spain in 2Q12 (a CCM score of 5.4, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Spain over the last four quarters, compared to the world as a whole.

CCM infection trends in Spain and worldwide



Threat categories

Malware and potentially unwanted software categories in Spain in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Spain in 2Q12 was Miscellaneous Trojans. It affected 32.1 percent of all computers with detections there, down from 32.7 percent in 1Q12.
- The second most common category in Spain in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 32.0 percent of all computers with detections there, down from 32.7 percent in 1Q12.
- The third most common category in Spain in 2Q12 was Adware, which affected 20.3 percent of all computers with detections there, down from 21.7 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Spain in 2Q12

	Family	Most significant category	% of computers with detections
1	Java/Blacole	Exploits	12.4%
2	Win32/Keygen	Misc. Potentially Unwanted Software	10.3%
3	ASX/Wimad	Trojan Downloaders & Droppers	9.3%
4	Win32/Autorun	Worms	6.4%
5	Java/CVE-2012-0507	Exploits	6.3%
6	JS/Redirector	Misc. Trojans	4.5%
7	Win32/Hotbar	Adware	4.5%
8	Win32/Conficker	Worms	4.4%
9	JS/Pornpop	Adware	4.4%
10	Win32/Sirefef	Misc. Trojans	3.9%

- The most common threat family in Spain in 2Q12 was [Java/Blacole](#), which affected 12.4 percent of computers with detections in Spain. [Java/Blacole](#) is an exploit pack, also known as Blackhole, that is installed on a compromised web server by an attacker and includes a number of exploits that target browser software. If a vulnerable computer browses a compromised website that contains the exploit pack, various malware may be downloaded and run.
- The second most common threat family in Spain in 2Q12 was [Win32/Keygen](#), which affected 10.3 percent of computers with detections in Spain. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The third most common threat family in Spain in 2Q12 was [ASX/Wimad](#), which affected 9.3 percent of computers with detections in Spain. [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 threat family in Spain in 2Q12 was [Win32/Autorun](#), which affected 6.4 percent of computers with detections in Spain. [Win32/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.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Spain

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	1.75 (1.6)	1.98 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	3.96 (3.9)	4.42 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.46 (0.7)	0.70 (0.9)

Update service usage

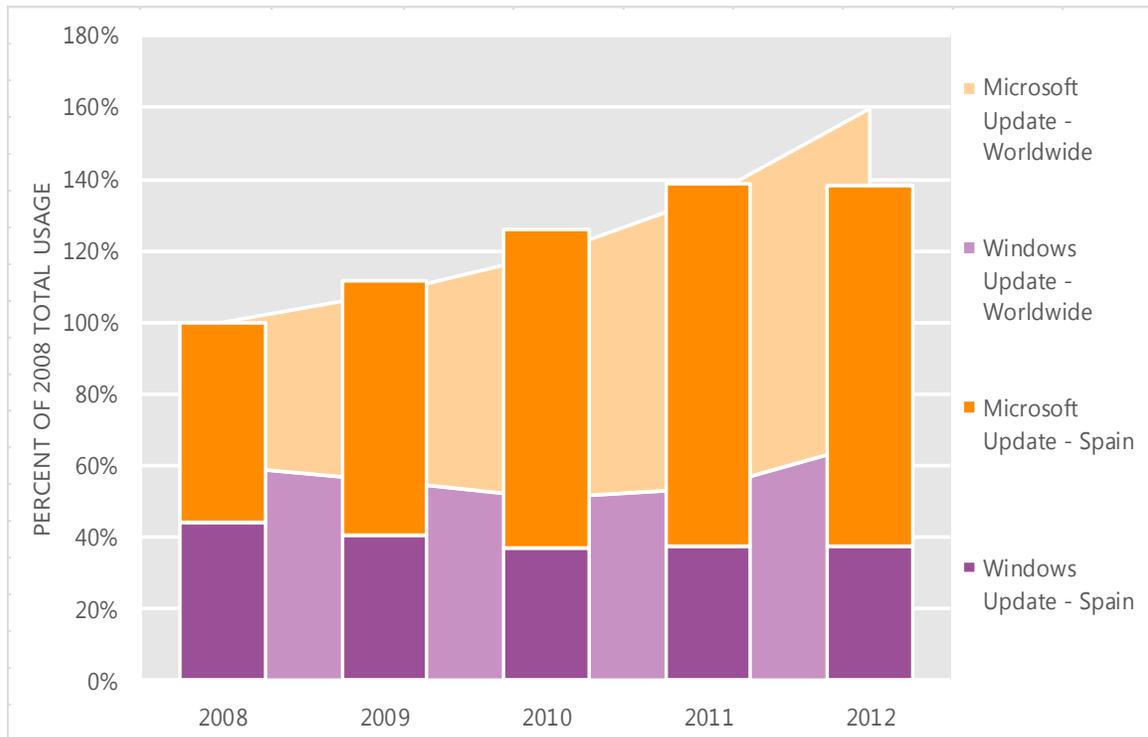
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Spain and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Spain over the last four years, indexed to the total usage for both services in Spain in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Spain was down 0.4 percent from 2011, and up 38.3 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Spain in 2012, 72.9 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Sri Lanka

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Sri Lanka in 2Q12 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.

Infection rate statistics for Sri Lanka

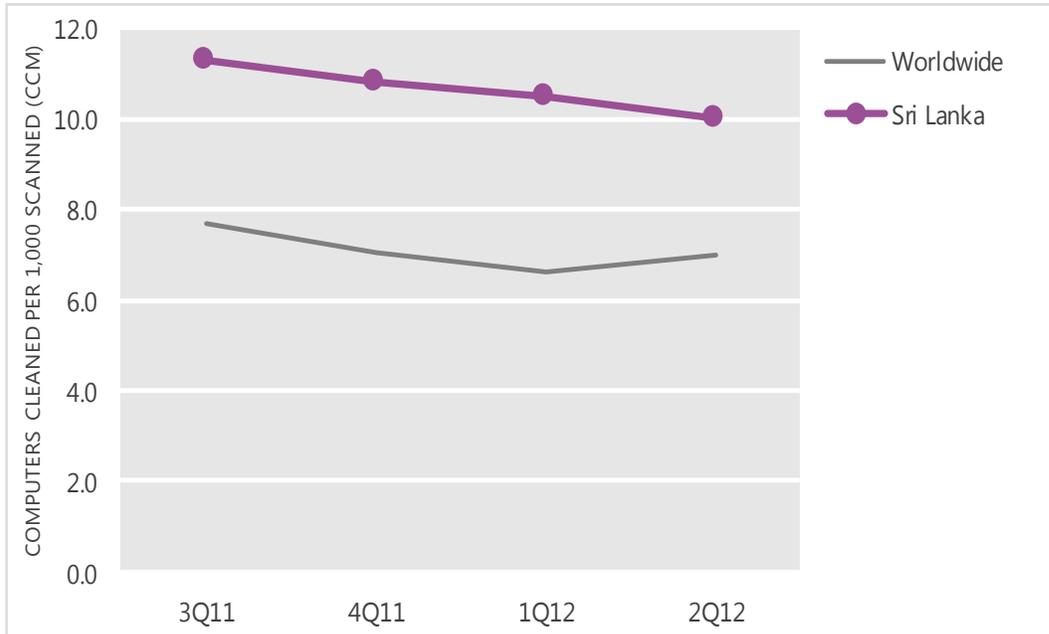
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	11.3	10.8	10.5	10.0
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

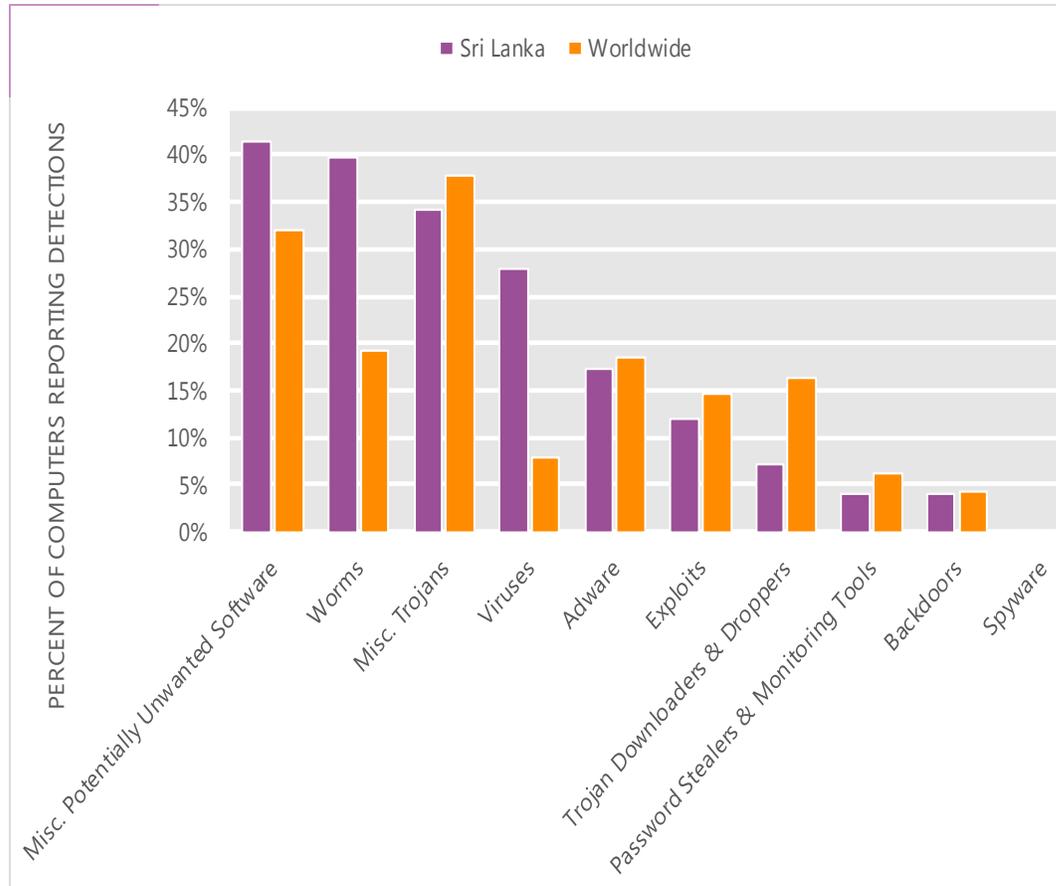
The MSRT detected malware on 10.0 of every 1,000 computers scanned in Sri Lanka in 2Q12 (a CCM score of 10.0, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Sri Lanka over the last four quarters, compared to the world as a whole.

CCM infection trends in Sri Lanka and worldwide



Threat categories

Malware and potentially unwanted software categories in Sri Lanka in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Sri Lanka in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 41.3 percent of all computers with detections there, down from 41.9 percent in 1Q12.
- The second most common category in Sri Lanka in 2Q12 was Worms. It affected 39.7 percent of all computers with detections there, down from 41.8 percent in 1Q12.
- The third most common category in Sri Lanka in 2Q12 was Miscellaneous Trojans, which affected 34.2 percent of all computers with detections there, down from 36.0 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Sri Lanka in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Autorun	Worms	27.8%
2	Win32/Sality	Viruses	20.9%
3	Win32/Keygen	Misc. Potentially Unwanted Software	16.9%
4	Win32/Nuqel	Worms	10.7%
5	JS/Pornpop	Adware	10.1%
6	Win32/Ramnit	Misc. Trojans	9.1%
7	Win32/CplLnk	Exploits	8.9%
8	Win32/Delicious	Viruses	8.8%
9	Win32/Dorkbot	Worms	8.3%
10	Win32/Rimecud	Worms	7.4%

- The most common threat family in Sri Lanka in 2Q12 was [Win32/Autorun](#), which affected 27.8 percent of computers with detections in Sri Lanka. [Win32/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 threat family in Sri Lanka in 2Q12 was [Win32/Sality](#), which affected 20.9 percent of computers with detections in Sri Lanka. [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 in Sri Lanka in 2Q12 was [Win32/Keygen](#), which affected 16.9 percent of computers with detections in Sri Lanka. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The fourth most common threat family in Sri Lanka in 2Q12 was [Win32/Nuqel](#), which affected 10.7 percent of computers with detections in Sri Lanka. [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.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Sri Lanka

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	N/A (1.6)	0.40 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	1.21 (3.9)	2.01 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.00 (0.7)	N/A (0.9)

Update service usage

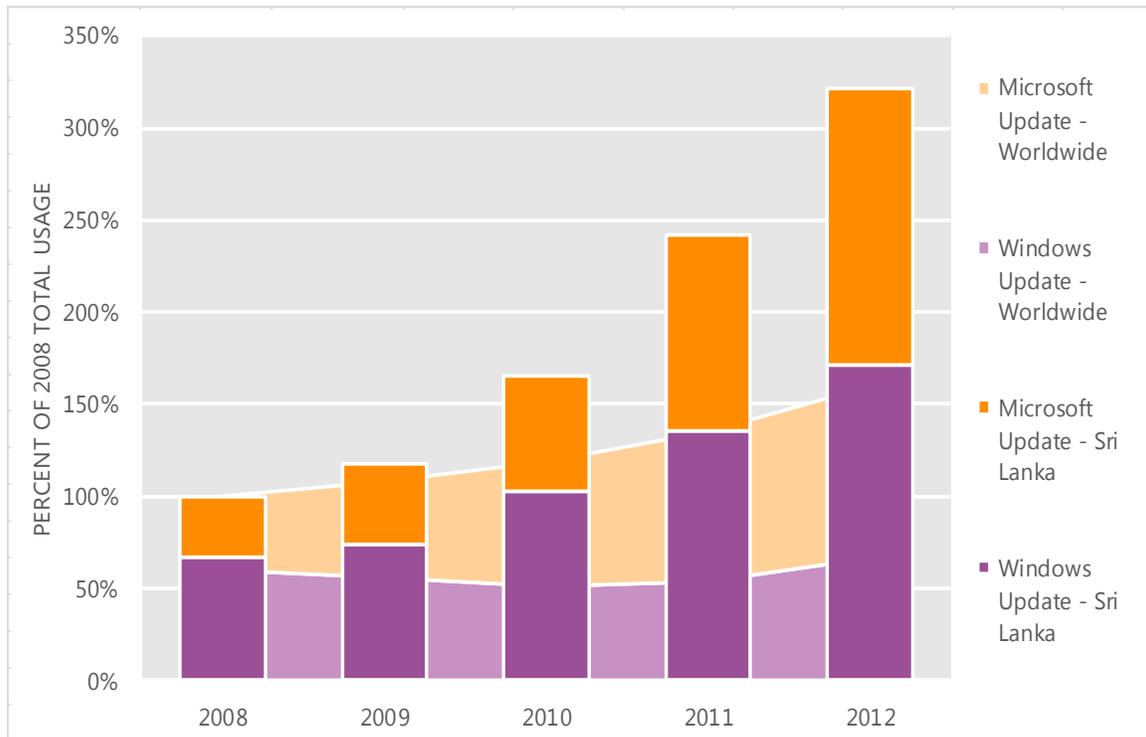
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Sri Lanka and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Sri Lanka over the last four years, indexed to the total usage for both services in Sri Lanka in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Sri Lanka was up 32.9 percent from 2011, and up 221.8 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Sri Lanka in 2012, 46.8 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Sweden

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Sweden in 2Q12 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.

Infection rate statistics for Sweden

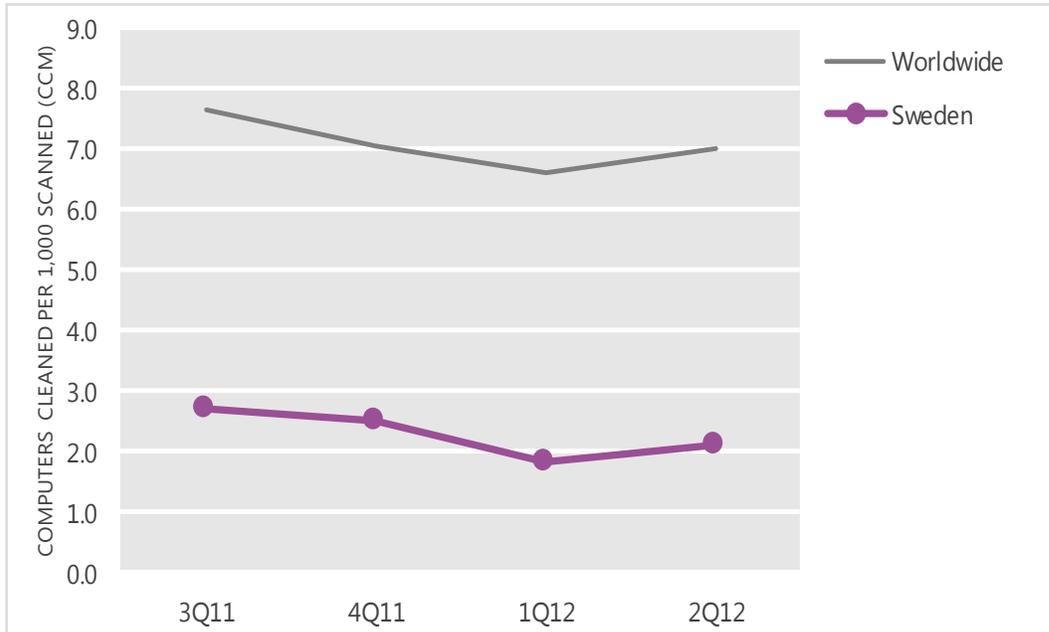
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	2.7	2.5	1.8	2.1
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

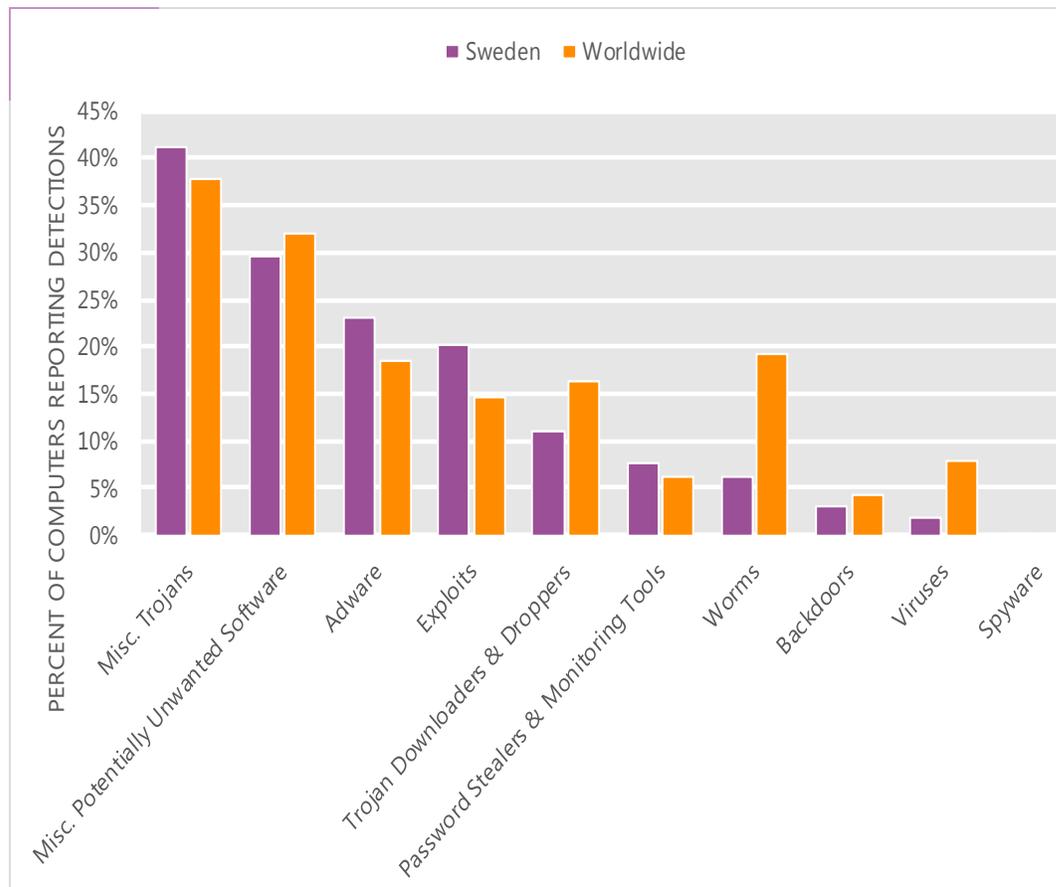
The MSRT detected malware on 2.1 of every 1,000 computers scanned in Sweden in 2Q12 (a CCM score of 2.1, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Sweden over the last four quarters, compared to the world as a whole.

CCM infection trends in Sweden and worldwide



Threat categories

Malware and potentially unwanted software categories in Sweden in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Sweden in 2Q12 was Miscellaneous Trojans. It affected 41.2 percent of all computers with detections there, up from 31.7 percent in 1Q12.
- The second most common category in Sweden in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 29.5 percent of all computers with detections there, down from 32.4 percent in 1Q12.
- The third most common category in Sweden in 2Q12 was Adware, which affected 23.2 percent of all computers with detections there, down from 31.8 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Sweden in 2Q12

	Family	Most significant category	% of computers with detections
1	Java/Blacole	Exploits	11.7%
2	Win32/Keygen	Misc. Potentially Unwanted Software	11.3%
3	JS/Pornpop	Adware	11.0%
4	Win32/Hotbar	Adware	8.2%
5	Win32/FakePAV	Misc. Trojans	8.0%
6	JS/IframeRef	Misc. Trojans	6.9%
7	JS/BlacoleRef	Misc. Trojans	6.4%
8	Java/CVE-2012-0507	Exploits	5.4%
9	Win32/Winwebsec	Misc. Trojans	5.4%
10	Win32/Sirefef	Misc. Trojans	4.2%

- The most common threat family in Sweden in 2Q12 was [Java/Blacole](#), which affected 11.7 percent of computers with detections in Sweden. [Java/Blacole](#) is an exploit pack, also known as Blackhole, that is installed on a compromised web server by an attacker and includes a number of exploits that target browser software. If a vulnerable computer browses a compromised website that contains the exploit pack, various malware may be downloaded and run.
- The second most common threat family in Sweden in 2Q12 was [Win32/Keygen](#), which affected 11.3 percent of computers with detections in Sweden. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The third most common threat family in Sweden in 2Q12 was [JS/Pornpop](#), which affected 11.0 percent of computers with detections in Sweden. [JS/Pornpop](#) is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The fourth most common threat family in Sweden in 2Q12 was [Win32/Hotbar](#), which affected 8.2 percent of computers with detections in Sweden. [Win32/Hotbar](#) is adware that displays a dynamic toolbar and targeted pop-up ads based on its monitoring of web-browsing activity.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Sweden

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	1.79 (1.6)	1.47 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	2.81 (3.9)	3.45 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.17 (0.7)	0.43 (0.9)

Update service usage

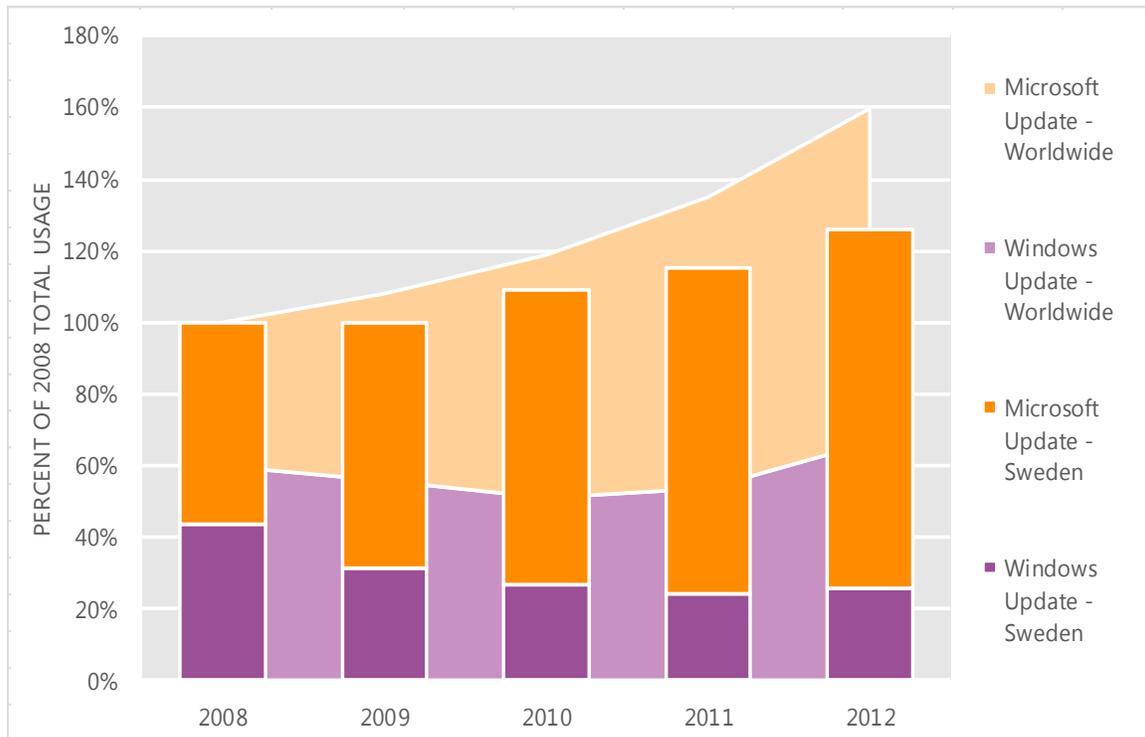
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Sweden and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Sweden over the last four years, indexed to the total usage for both services in Sweden in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Sweden was up 9.0 percent from 2011, and up 25.8 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Sweden in 2012, 79.5 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Switzerland

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Switzerland in 2Q12 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.

Infection rate statistics for Switzerland

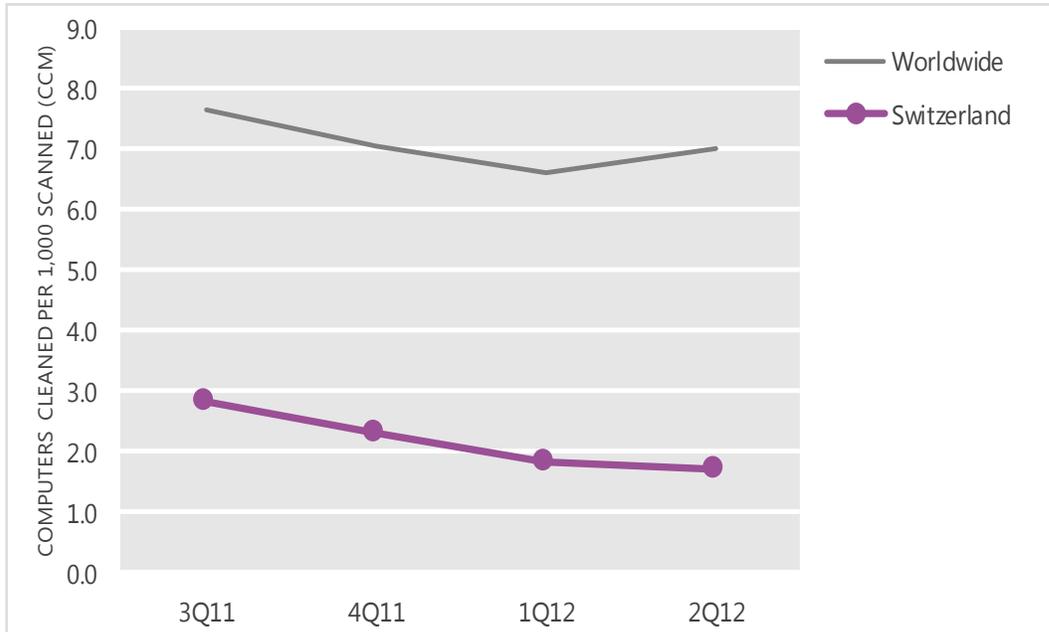
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	2.8	2.3	1.8	1.7
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

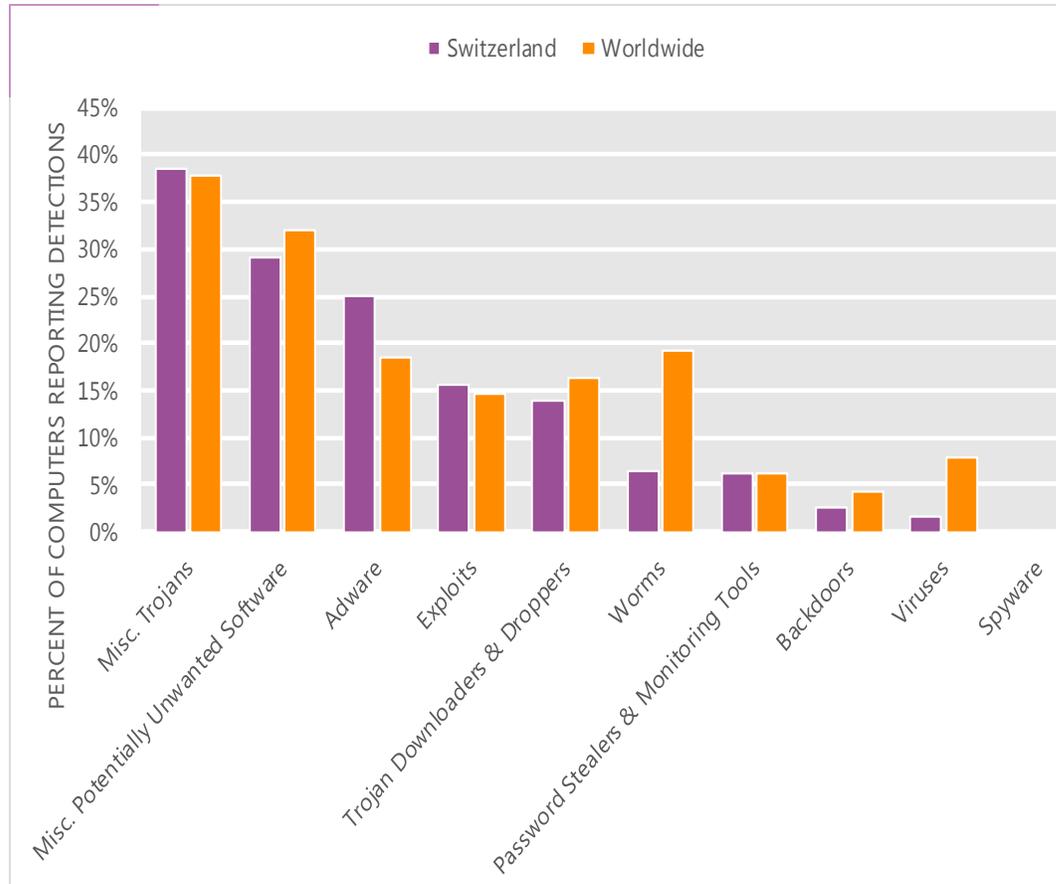
The MSRT detected malware on 1.7 of every 1,000 computers scanned in Switzerland in 2Q12 (a CCM score of 1.7, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Switzerland over the last four quarters, compared to the world as a whole.

CCM infection trends in Switzerland and worldwide



Threat categories

Malware and potentially unwanted software categories in Switzerland in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Switzerland in 2Q12 was Miscellaneous Trojans. It affected 38.6 percent of all computers with detections there, up from 30.4 percent in 1Q12.
- The second most common category in Switzerland in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 29.0 percent of all computers with detections there, down from 31.9 percent in 1Q12.
- The third most common category in Switzerland in 2Q12 was Adware, which affected 25.1 percent of all computers with detections there, down from 34.9 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Switzerland in 2Q12

	Family	Most significant category	% of computers with detections
1	JS/Pornpop	Adware	12.9%
2	Win32/Keygen	Misc. Potentially Unwanted Software	8.2%
3	JS/BlacoleRef	Misc. Trojans	8.1%
4	Win32/FakePAV	Misc. Trojans	7.5%
5	Java/Blacole	Exploits	6.3%
6	Win32/Hotbar	Adware	6.3%
7	JS/IframeRef	Misc. Trojans	6.2%
8	ASX/Wimad	Trojan Downloaders & Droppers	6.1%
9	Win32/Obfuscator	Misc. Potentially Unwanted Software	4.5%
10	Java/CVE-2012-0507	Exploits	4.2%

- The most common threat family in Switzerland in 2Q12 was [JS/Pornpop](#), which affected 12.9 percent of computers with detections in Switzerland. [JS/Pornpop](#) is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The second most common threat family in Switzerland in 2Q12 was [Win32/Keygen](#), which affected 8.2 percent of computers with detections in Switzerland. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The third most common threat family in Switzerland in 2Q12 was [JS/BlacoleRef](#), which affected 8.1 percent of computers with detections in Switzerland. [JS/BlacoleRef](#) is an obfuscated script, often found inserted into compromised websites, that uses a hidden inline frame to redirect the browser to a Blacole exploit server.
- The fourth most common threat family in Switzerland in 2Q12 was [Win32/FakePAV](#), which affected 7.5 percent of computers with detections in Switzerland. [Win32/FakePAV](#) is a rogue security software family that often masquerades as Microsoft Security Essentials or other legitimate antimalware products.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Switzerland

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	0.99 (1.6)	1.14 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	2.13 (3.9)	2.39 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.26 (0.7)	0.36 (0.9)

Update service usage

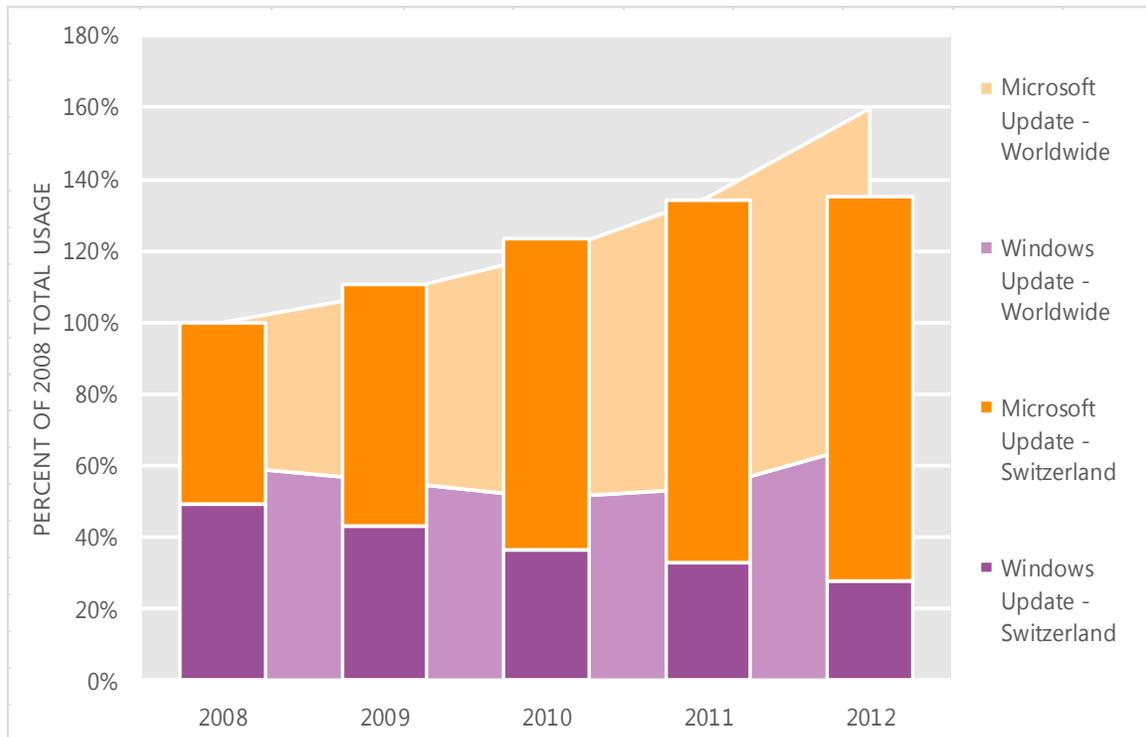
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Switzerland and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Switzerland over the last four years, indexed to the total usage for both services in Switzerland in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Switzerland was up 0.8 percent from 2011, and up 35.3 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Switzerland in 2012, 79.4 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Syria

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Syria in 2Q12 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.

Infection rate statistics for Syria

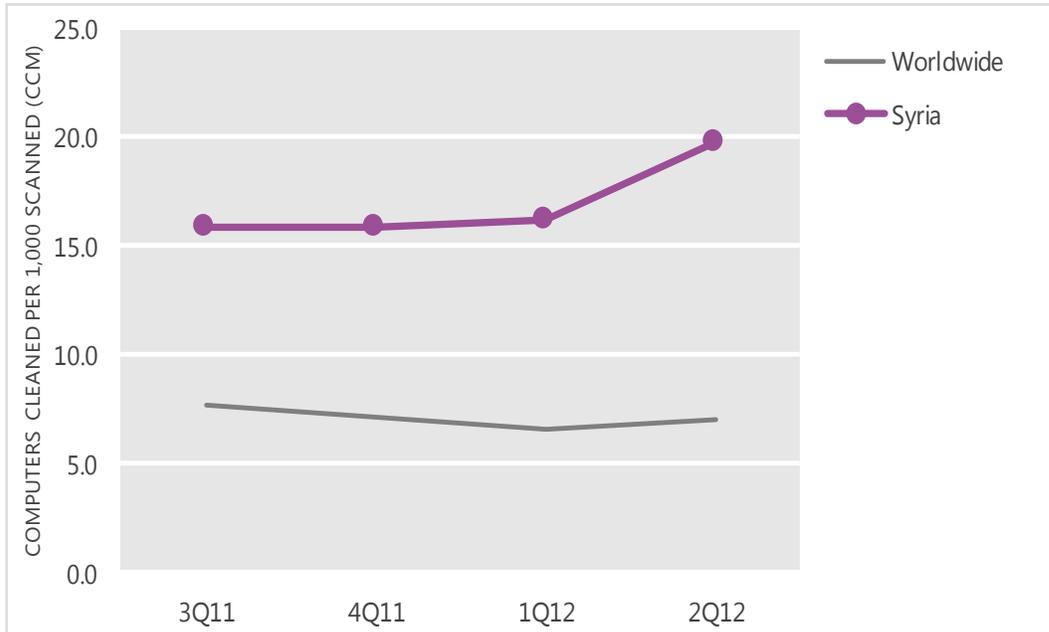
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	15.9	15.9	16.2	19.8
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website at www.microsoft.com/sir for more information about threats in Syria and around the world, and for explanations of the methods and terms used here.

Infection trends (CCM)

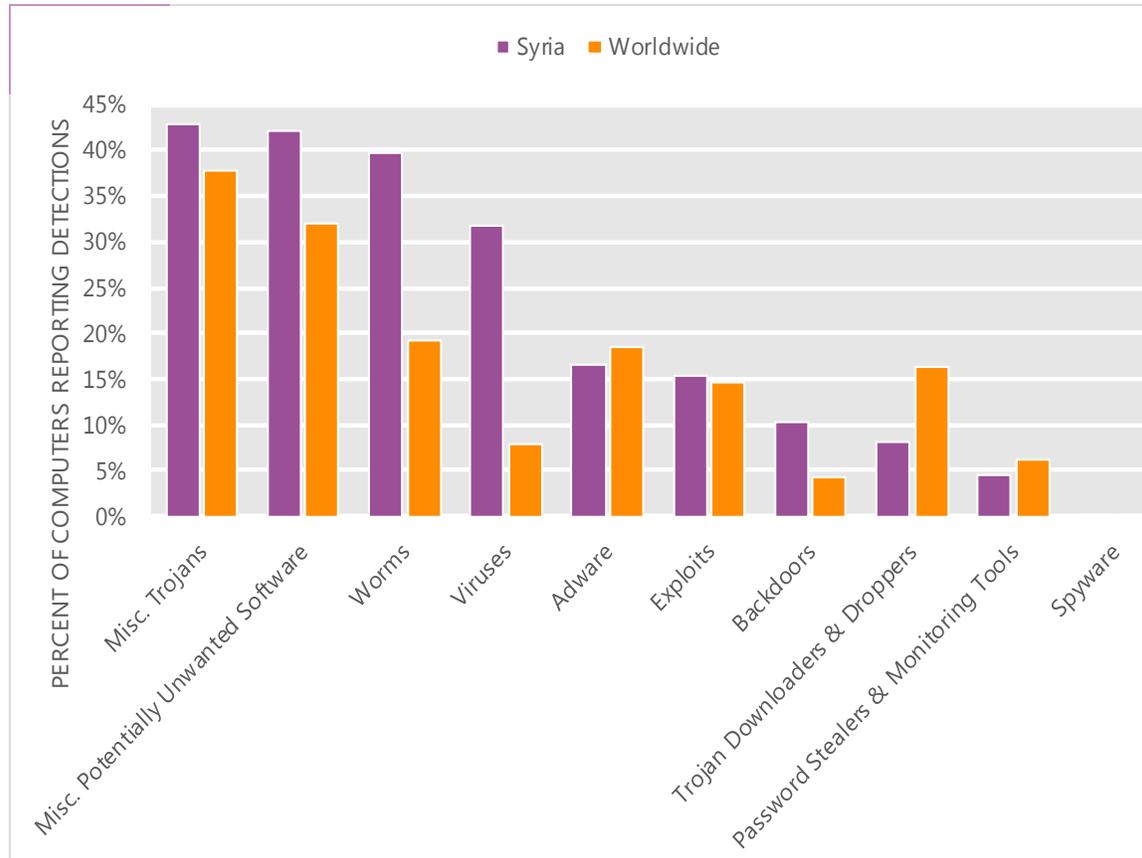
The MSRT detected malware on 19.8 of every 1,000 computers scanned in Syria in 2Q12 (a CCM score of 19.8, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Syria over the last four quarters, compared to the world as a whole.

CCM infection trends in Syria and worldwide



Threat categories

Malware and potentially unwanted software categories in Syria in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Syria in 2Q12 was Miscellaneous Trojans. It affected 42.8 percent of all computers with detections there, up from 42.4 percent in 1Q12.
- The second most common category in Syria in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 42.2 percent of all computers with detections there, down from 42.8 percent in 1Q12.
- The third most common category in Syria in 2Q12 was Worms, which affected 39.6 percent of all computers with detections there, up from 38.6 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Syria in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Sality	Viruses	22.5%
2	Win32/Keygen	Misc. Potentially Unwanted Software	22.3%
3	Win32/Autorun	Worms	19.4%
4	Win32/Ramnit	Misc. Trojans	18.4%
5	Win32/CplLnk	Exploits	13.1%
6	Win32/Dorkbot	Worms	11.9%
7	Win32/Virut	Viruses	9.1%
8	JS/Paypopup	Adware	8.5%
9	Win32/Nuqel	Worms	6.2%
10	Win32/Agent	Misc. Trojans	5.8%

- The most common threat family in Syria in 2Q12 was [Win32/Sality](#), which affected 22.5 percent of computers with detections in Syria. [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 in Syria in 2Q12 was [Win32/Keygen](#), which affected 22.3 percent of computers with detections in Syria. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The third most common threat family in Syria in 2Q12 was [Win32/Autorun](#), which affected 19.4 percent of computers with detections in Syria. [Win32/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 threat family in Syria in 2Q12 was [Win32/Ramnit](#), which affected 18.4 percent of computers with detections in Syria. [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.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Syria

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	0.37 (1.6)	1.12 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	2.25 (3.9)	3.37 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.13 (0.7)	0.17 (0.9)

Update service usage

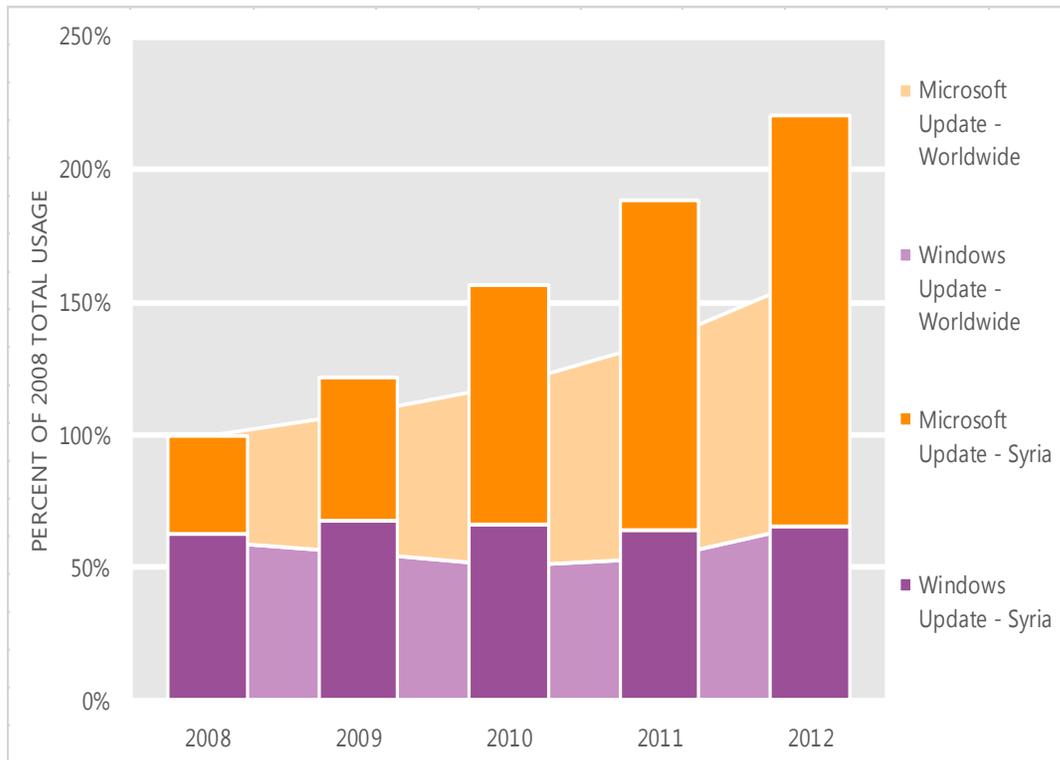
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Syria and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Syria over the last four years, indexed to the total usage for both services in Syria in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Syria was up 17.1 percent from 2011, and up 120.7 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Syria in 2012, 70.3 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Taiwan

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Taiwan in 2Q12 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.

Infection rate statistics for Taiwan

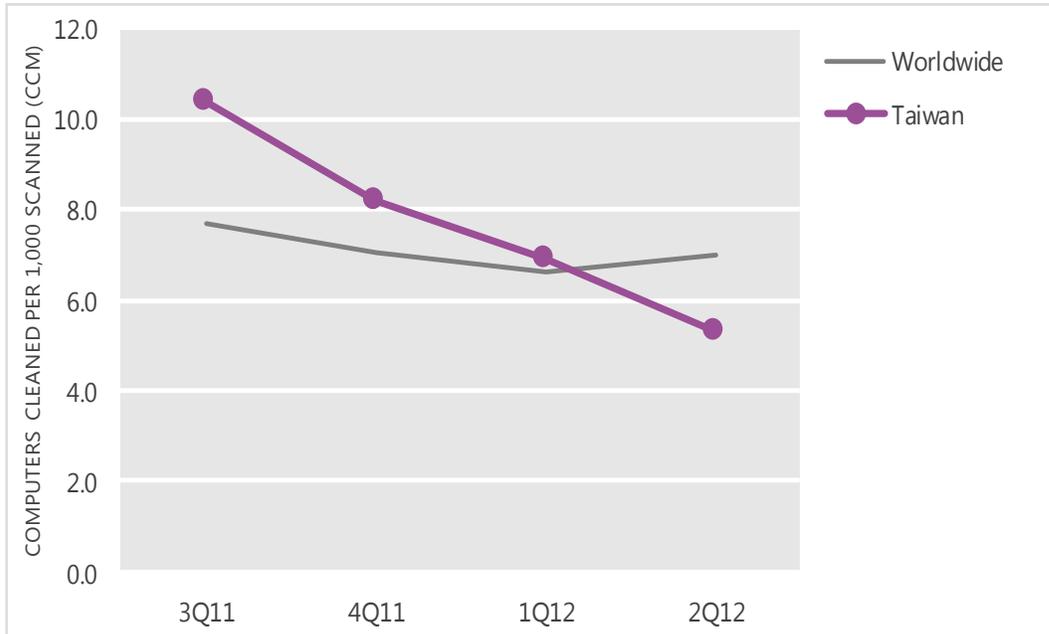
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	10.4	8.2	6.9	5.3
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

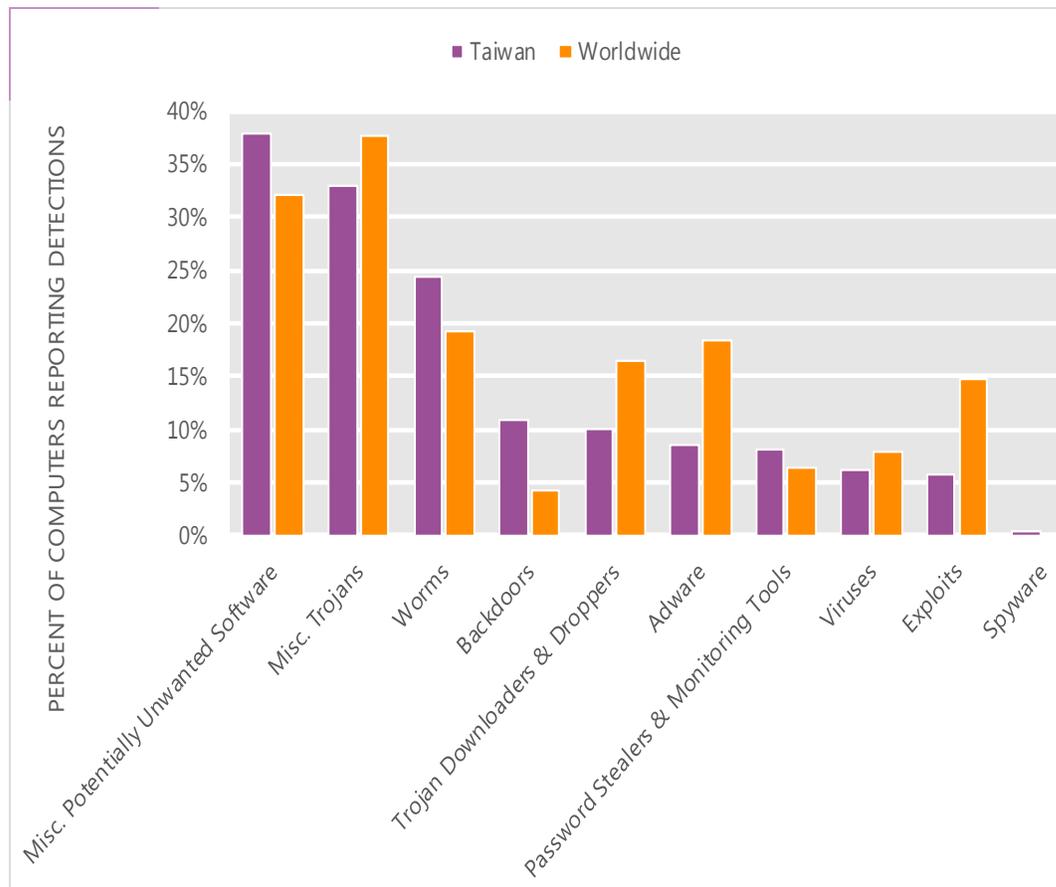
The MSRT detected malware on 5.3 of every 1,000 computers scanned in Taiwan in 2Q12 (a CCM score of 5.3, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Taiwan over the last four quarters, compared to the world as a whole.

CCM infection trends in Taiwan and worldwide



Threat categories

Malware and potentially unwanted software categories in Taiwan in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Taiwan in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 37.9 percent of all computers with detections there, down from 40.6 percent in 1Q12.
- The second most common category in Taiwan in 2Q12 was Miscellaneous Trojans. It affected 33.0 percent of all computers with detections there, up from 30.5 percent in 1Q12.
- The third most common category in Taiwan in 2Q12 was Worms, which affected 24.5 percent of all computers with detections there, down from 26.2 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Taiwan in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Keygen	Misc. Potentially Unwanted Software	16.8%
2	Win32/Autorun	Worms	12.7%
3	JS/IframeRef	Misc. Trojans	8.6%
4	Win32/Taterf	Worms	7.4%
5	Win32/Rimecud	Worms	6.0%
6	Win32/Conficker	Worms	5.9%
7	Win32/FlyAgent	Backdoors	3.7%
8	JS/Pornpop	Adware	3.7%
9	ASX/Wimad	Trojan Downloaders & Droppers	3.5%
10	Win32/Hupigon	Backdoors	3.5%

- The most common threat family in Taiwan in 2Q12 was [Win32/Keygen](#), which affected 16.8 percent of computers with detections in Taiwan. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The second most common threat family in Taiwan in 2Q12 was [Win32/Autorun](#), which affected 12.7 percent of computers with detections in Taiwan. [Win32/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 threat family in Taiwan in 2Q12 was [JS/IframeRef](#), which affected 8.6 percent of computers with detections in Taiwan. [JS/IframeRef](#) is a generic detection for specially formed IFrame tags that point to remote websites that contain malicious content.
- The fourth most common threat family in Taiwan in 2Q12 was [Win32/Taterf](#), which affected 7.4 percent of computers with detections in Taiwan. [Win32/Taterf](#) is a family of worms that spread through mapped drives to steal login and account details for popular online games.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Taiwan

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	0.44 (1.6)	0.42 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	1.54 (3.9)	1.65 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.60 (0.7)	0.66 (0.9)

Update service usage

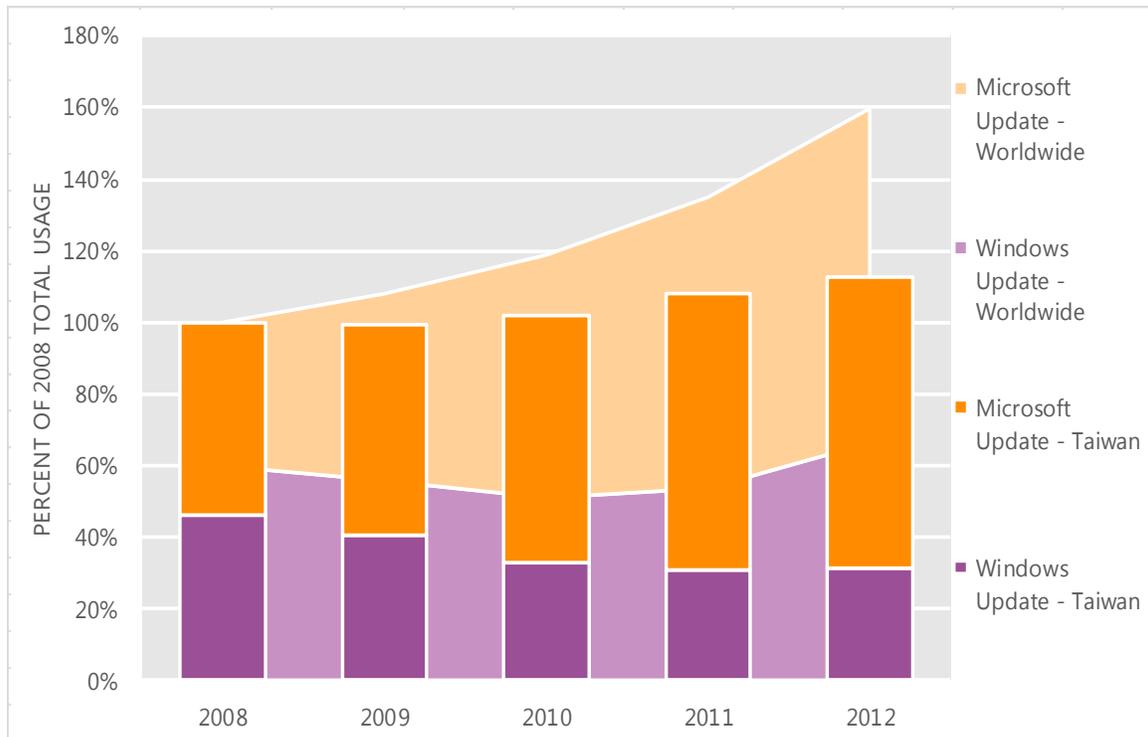
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Taiwan and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Taiwan over the last four years, indexed to the total usage for both services in Taiwan in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Taiwan was up 4.2 percent from 2011, and up 12.8 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Taiwan in 2012, 72.2 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Tanzania

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Tanzania in 2Q12 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.

Infection rate statistics for Tanzania

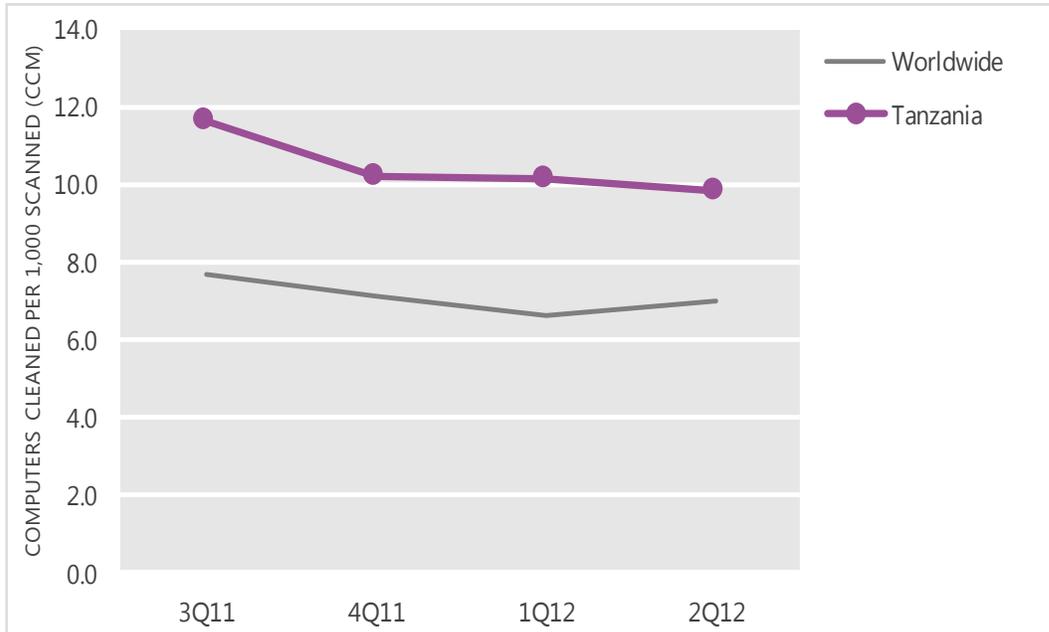
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	11.6	10.2	10.1	9.8
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

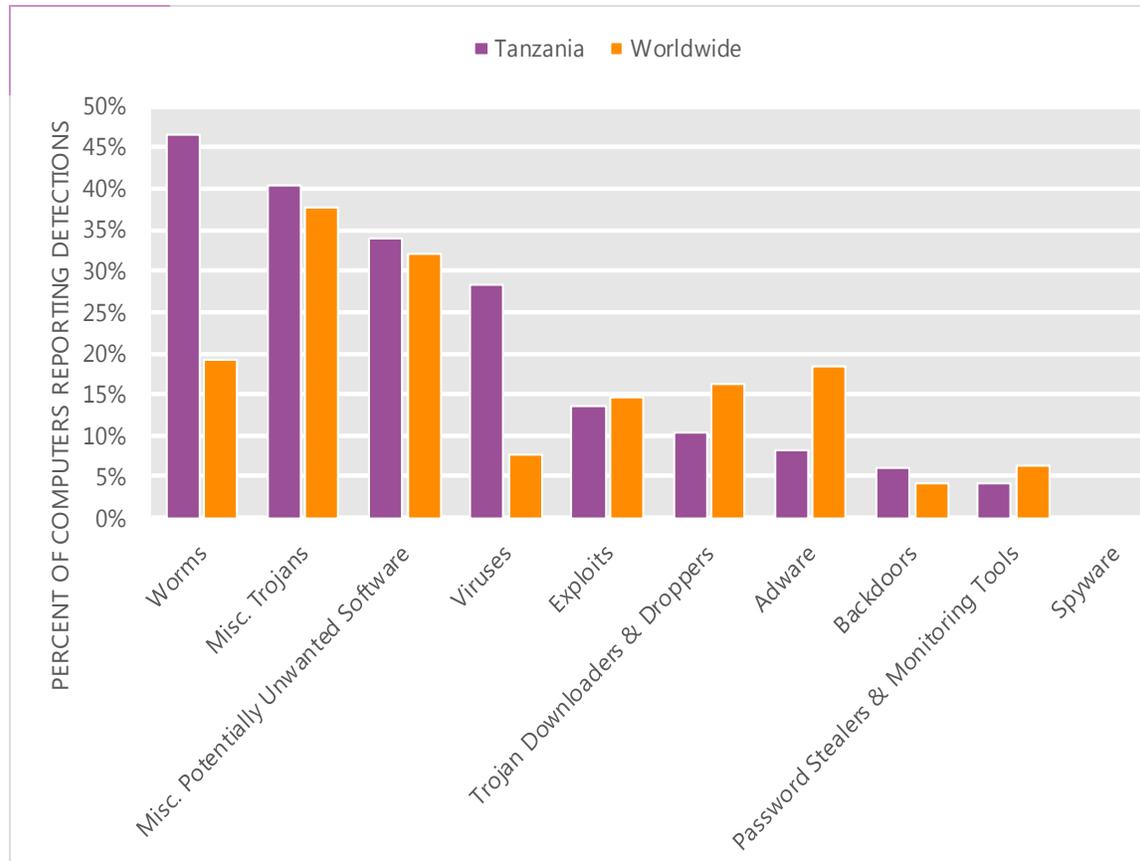
The MSRT detected malware on 9.8 of every 1,000 computers scanned in Tanzania in 2Q12 (a CCM score of 9.8, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Tanzania over the last four quarters, compared to the world as a whole.

CCM infection trends in Tanzania and worldwide



Threat categories

Malware and potentially unwanted software categories in Tanzania in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Tanzania in 2Q12 was Worms. It affected 46.6 percent of all computers with detections there, up from 44.4 percent in 1Q12.
- The second most common category in Tanzania in 2Q12 was Miscellaneous Trojans. It affected 40.3 percent of all computers with detections there, down from 42.0 percent in 1Q12.
- The third most common category in Tanzania in 2Q12 was Miscellaneous Potentially Unwanted Software, which affected 33.9 percent of all computers with detections there, up from 31.9 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Tanzania in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Autorun	Worms	20.7%
2	Win32/Vobfus	Worms	17.7%
3	Win32/Ramnit	Misc. Trojans	15.9%
4	Win32/Dorkbot	Worms	13.9%
5	Win32/Sality	Viruses	12.6%
6	Win32/Virut	Viruses	11.8%
7	Win32/CplLnk	Exploits	10.6%
8	Win32/Rimecud	Worms	10.4%
9	Win32/Keygen	Misc. Potentially Unwanted Software	8.3%
10	Win32/Nuqel	Worms	5.1%

- The most common threat family in Tanzania in 2Q12 was [Win32/Autorun](#), which affected 20.7 percent of computers with detections in Tanzania. [Win32/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 threat family in Tanzania in 2Q12 was [Win32/Vobfus](#), which affected 17.7 percent of computers with detections in Tanzania. [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 in Tanzania in 2Q12 was [Win32/Ramnit](#), which affected 15.9 percent of computers with detections in Tanzania. [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 in Tanzania in 2Q12 was [Win32/Dorkbot](#), which affected 13.9 percent of computers with detections in Tanzania. [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.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Tanzania

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	N/A (1.6)	N/A (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	N/A (3.9)	N/A (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.22 (0.7)	2.60 (0.9)

Update service usage

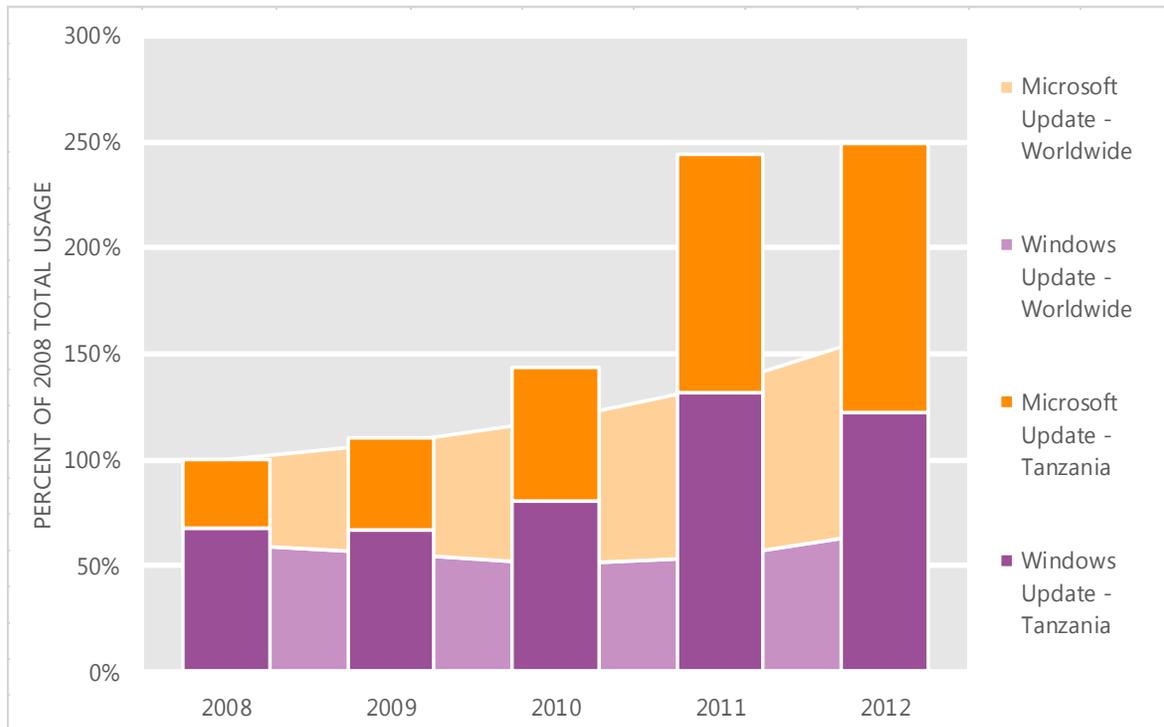
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Tanzania and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Tanzania over the last four years, indexed to the total usage for both services in Tanzania in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Tanzania was up 2.2 percent from 2011, and up 149.1 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Tanzania in 2012, 50.8 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Thailand

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Thailand in 2Q12 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.

Infection rate statistics for Thailand

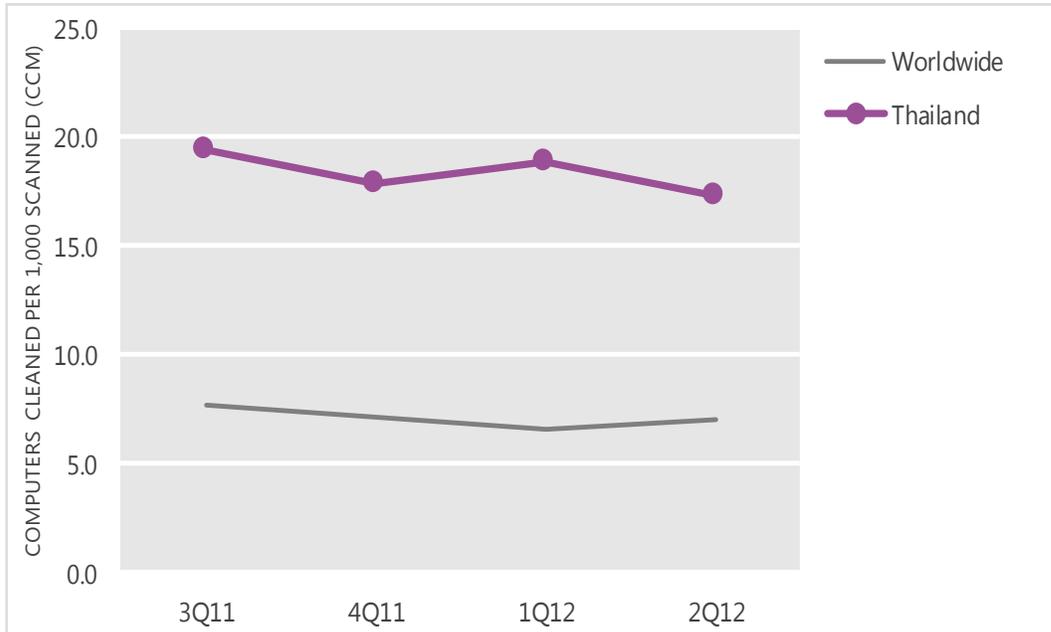
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	19.4	17.9	18.9	17.3
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

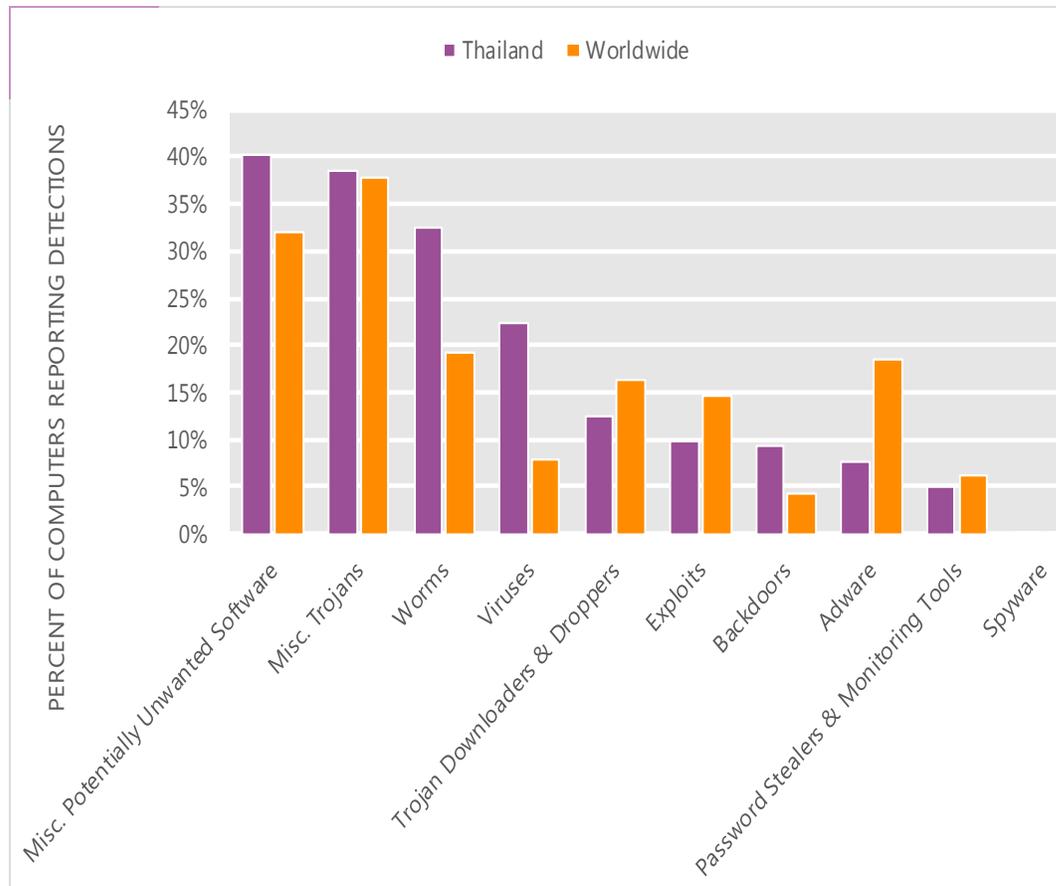
The MSRT detected malware on 17.3 of every 1,000 computers scanned in Thailand in 2Q12 (a CCM score of 17.3, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Thailand over the last four quarters, compared to the world as a whole.

CCM infection trends in Thailand and worldwide



Threat categories

Malware and potentially unwanted software categories in Thailand in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Thailand in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 40.1 percent of all computers with detections there, down from 42.7 percent in 1Q12.
- The second most common category in Thailand in 2Q12 was Miscellaneous Trojans. It affected 38.5 percent of all computers with detections there, up from 37.6 percent in 1Q12.
- The third most common category in Thailand in 2Q12 was Worms, which affected 32.4 percent of all computers with detections there, down from 34.3 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Thailand in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Keygen	Misc. Potentially Unwanted Software	20.8%
2	Win32/Sality	Viruses	17.2%
3	Win32/Autorun	Worms	13.5%
4	Win32/Dorkbot	Worms	8.8%
5	Win32/Ramnit	Misc. Trojans	5.7%
6	Win32/Nuqel	Worms	5.6%
7	Win32/Conficker	Worms	5.5%
8	Win32/Dynamer	Misc. Trojans	5.0%
9	JS/IframeRef	Misc. Trojans	4.9%
10	Win32/Wpkill	Misc. Potentially Unwanted Software	4.0%

- The most common threat family in Thailand in 2Q12 was [Win32/Keygen](#), which affected 20.8 percent of computers with detections in Thailand. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The second most common threat family in Thailand in 2Q12 was [Win32/Sality](#), which affected 17.2 percent of computers with detections in Thailand. [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 in Thailand in 2Q12 was [Win32/Autorun](#), which affected 13.5 percent of computers with detections in Thailand. [Win32/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 threat family in Thailand in 2Q12 was [Win32/Dorkbot](#), which affected 8.8 percent of computers with detections in Thailand. [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.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Thailand

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	0.65 (1.6)	0.58 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	1.00 (3.9)	1.18 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.85 (0.7)	2.61 (0.9)

Update service usage

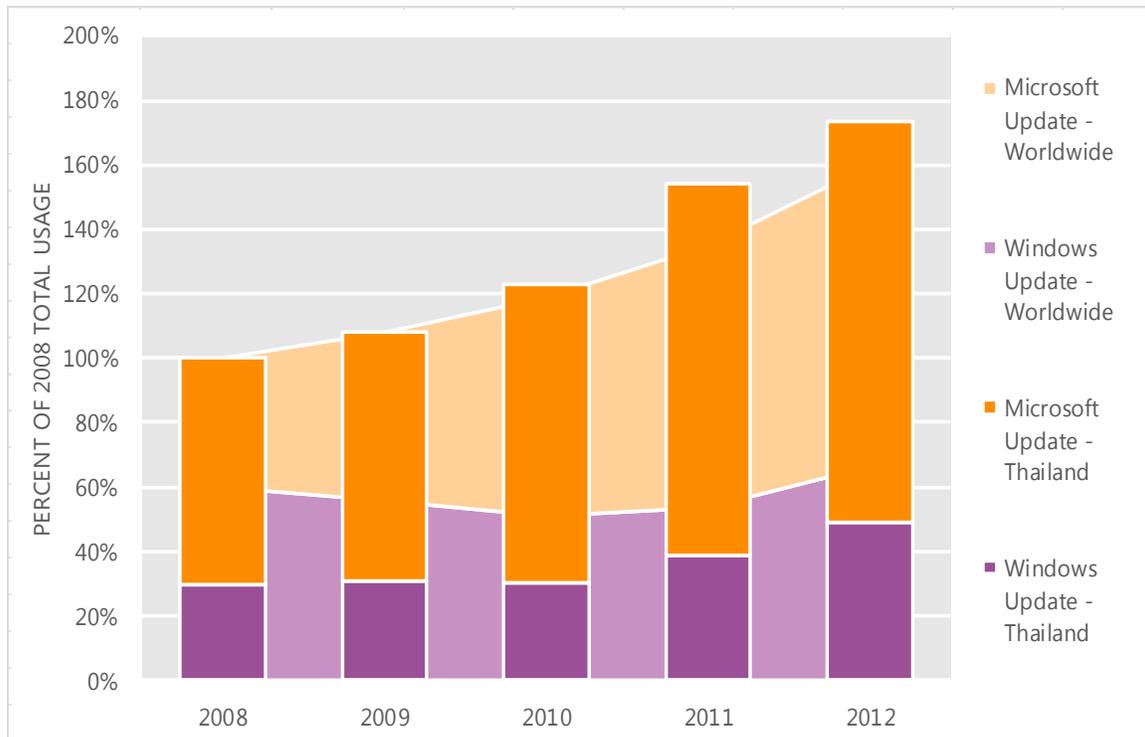
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Thailand and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Thailand over the last four years, indexed to the total usage for both services in Thailand in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Thailand was up 12.7 percent from 2011, and up 73.7 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Thailand in 2012, 71.8 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Trinidad and Tobago

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Trinidad and Tobago in 2Q12 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.

Infection rate statistics for Trinidad and Tobago

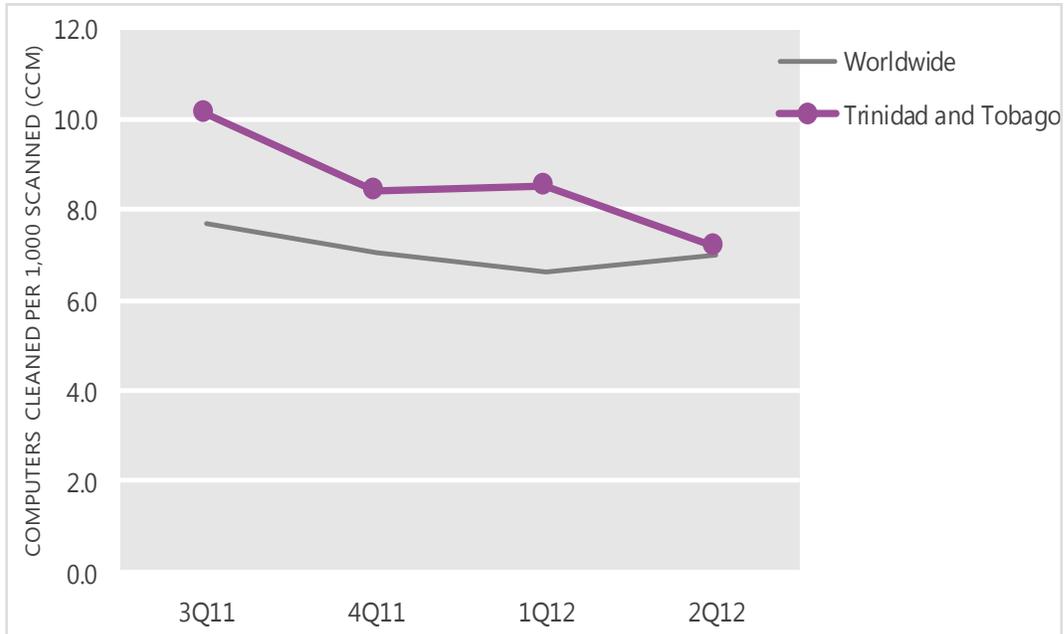
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	10.1	8.4	8.5	7.2
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

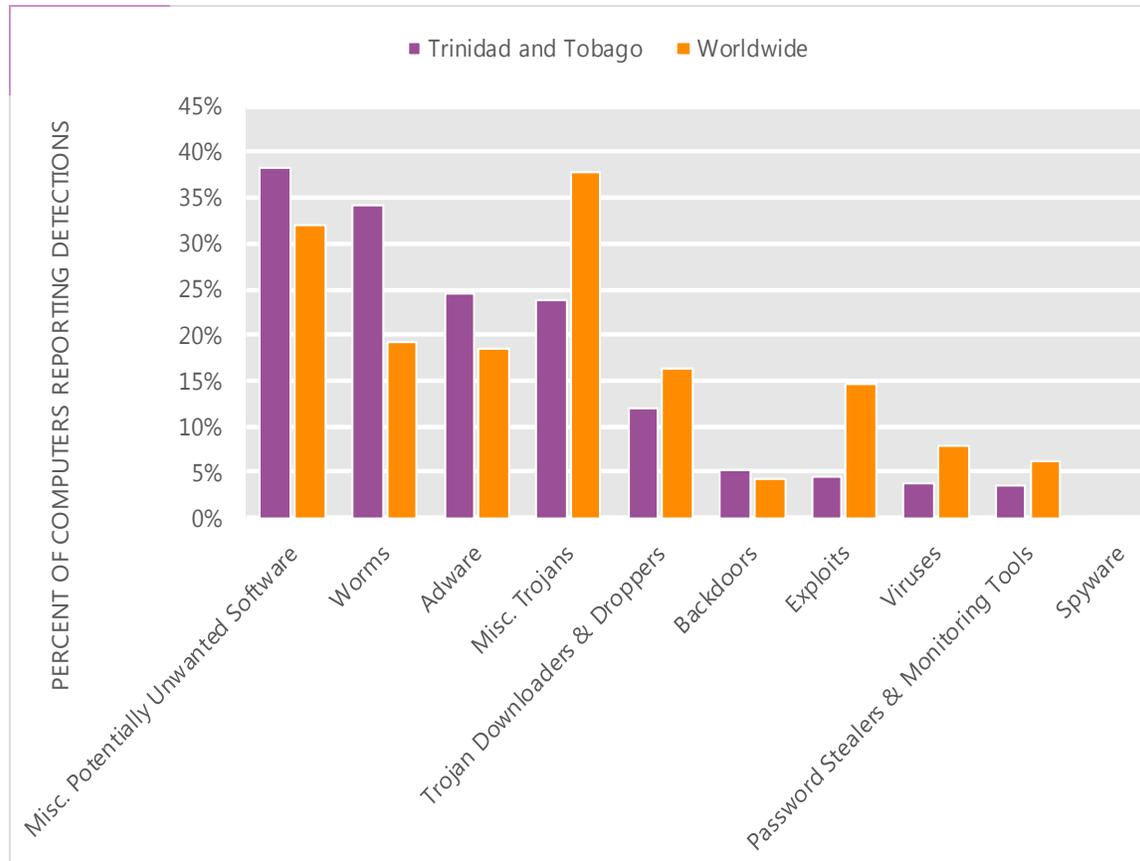
The MSRT detected malware on 7.2 of every 1,000 computers scanned in Trinidad and Tobago in 2Q12 (a CCM score of 7.2, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Trinidad and Tobago over the last four quarters, compared to the world as a whole.

CCM infection trends in Trinidad and Tobago and worldwide



Threat categories

Malware and potentially unwanted software categories in Trinidad and Tobago in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Trinidad and Tobago in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 38.3 percent of all computers with detections there, up from 37.8 percent in 1Q12.
- The second most common category in Trinidad and Tobago in 2Q12 was Worms. It affected 34.1 percent of all computers with detections there, down from 36.6 percent in 1Q12.
- The third most common category in Trinidad and Tobago in 2Q12 was Adware, which affected 24.4 percent of all computers with detections there, down from 31.5 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Trinidad and Tobago in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Hotbar	Adware	14.6%
2	Win32/Autorun	Worms	14.5%
3	Win32/Vobfus	Worms	12.0%
4	Win32/Keygen	Misc. Potentially Unwanted Software	10.4%
5	Win32/Zwangi	Misc. Potentially Unwanted Software	9.7%
6	Win32/Dorkbot	Worms	7.3%
7	JS/Pornpop	Adware	6.4%
8	Win32/VBInject	Misc. Potentially Unwanted Software	6.3%
9	ASX/Wimad	Trojan Downloaders & Droppers	5.0%
10	Win32/Brontok	Worms	4.4%

- The most common threat family in Trinidad and Tobago in 2Q12 was [Win32/Hotbar](#), which affected 14.6 percent of computers with detections in Trinidad and Tobago. [Win32/Hotbar](#) is adware that displays a dynamic toolbar and targeted pop-up ads based on its monitoring of web-browsing activity.
- The second most common threat family in Trinidad and Tobago in 2Q12 was [Win32/Autorun](#), which affected 14.5 percent of computers with detections in Trinidad and Tobago. [Win32/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 threat family in Trinidad and Tobago in 2Q12 was [Win32/Vobfus](#), which affected 12.0 percent of computers with detections in Trinidad and Tobago. [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 in Trinidad and Tobago in 2Q12 was [Win32/Keygen](#), which affected 10.4 percent of computers with detections in Trinidad and Tobago. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Trinidad and Tobago

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	1.35 (1.6)	0.45 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	1.35 (3.9)	1.80 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	N/A (0.7)	0.47 (0.9)

Update service usage

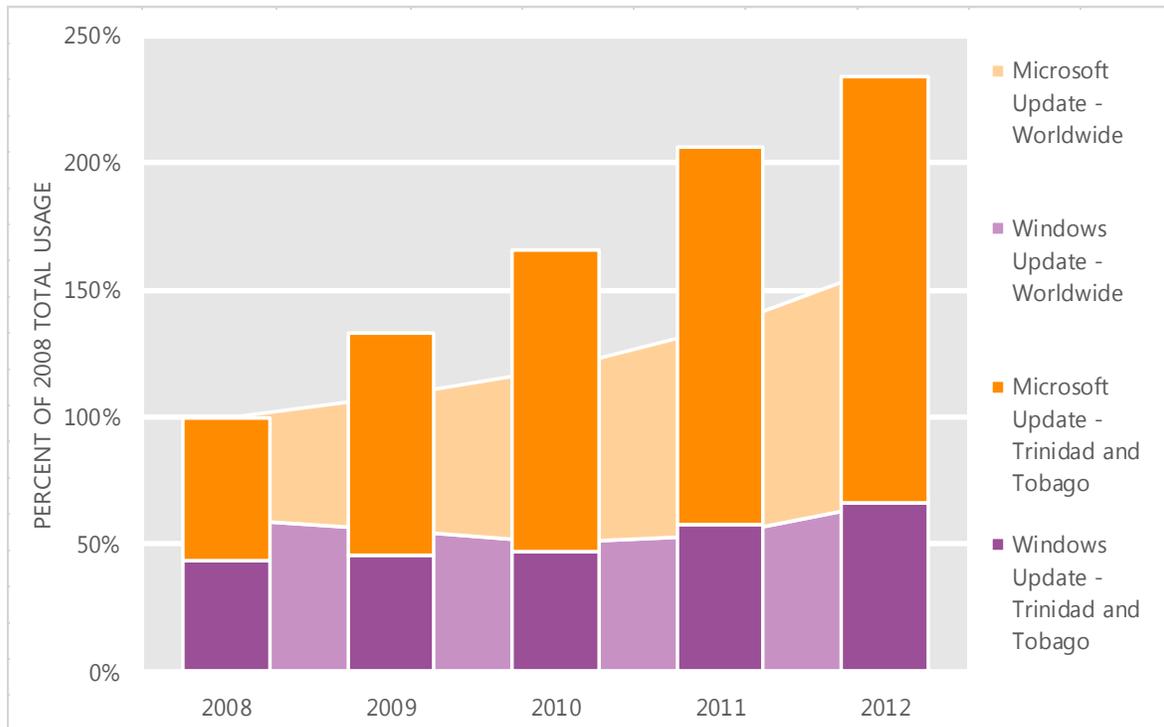
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Trinidad and Tobago and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Trinidad and Tobago over the last four years, indexed to the total usage for both services in Trinidad and Tobago in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Trinidad and Tobago was up 13.4 percent from 2011, and up 133.8 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Trinidad and Tobago in 2012, 71.6 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Tunisia

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Tunisia in 2Q12 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.

Infection rate statistics for Tunisia

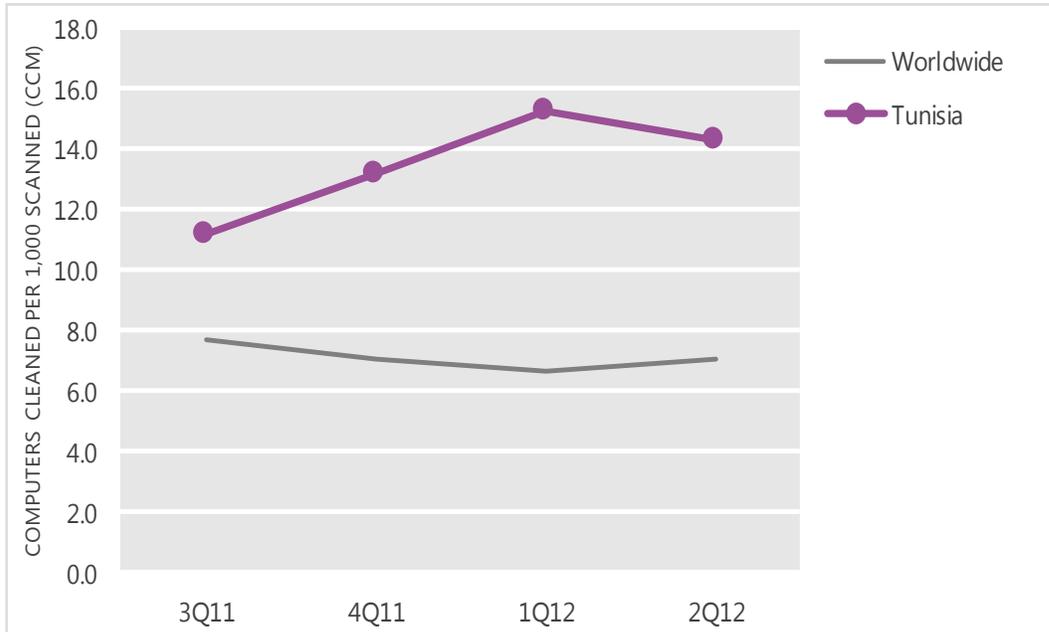
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	11.2	13.2	15.3	14.3
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

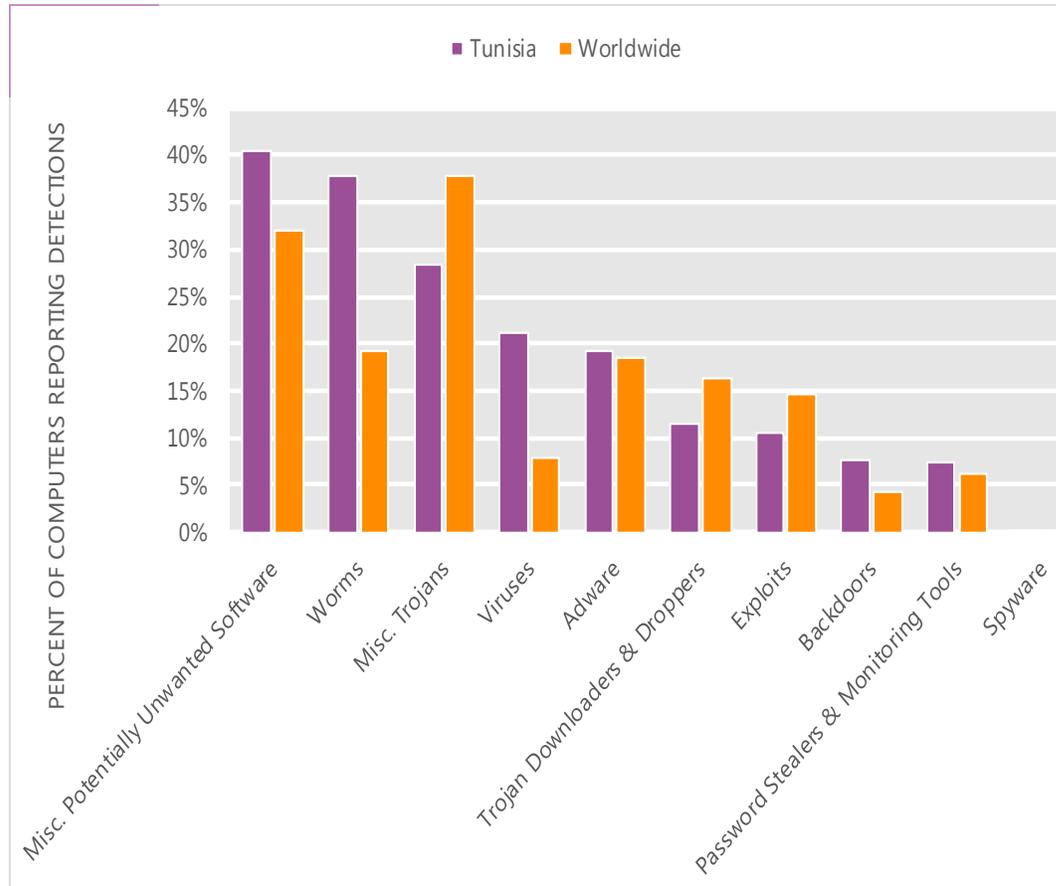
The MSRT detected malware on 14.3 of every 1,000 computers scanned in Tunisia in 2Q12 (a CCM score of 14.3, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Tunisia over the last four quarters, compared to the world as a whole.

CCM infection trends in Tunisia and worldwide



Threat categories

Malware and potentially unwanted software categories in Tunisia in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Tunisia in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 40.4 percent of all computers with detections there, down from 40.6 percent in 1Q12.
- The second most common category in Tunisia in 2Q12 was Worms. It affected 37.8 percent of all computers with detections there, up from 36.2 percent in 1Q12.
- The third most common category in Tunisia in 2Q12 was Miscellaneous Trojans, which affected 28.4 percent of all computers with detections there, up from 27.1 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Tunisia in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Autorun	Worms	17.8%
2	Win32/Vobfus	Worms	14.2%
3	Win32/Sality	Viruses	12.4%
4	Win32/Keygen	Misc. Potentially Unwanted Software	11.9%
5	Win32/Hotbar	Adware	9.8%
6	Win32/Ramnit	Misc. Trojans	9.5%
7	Win32/CplLnk	Exploits	8.8%
8	Win32/Mabezat	Viruses	8.3%
9	Win32/Zwangi	Misc. Potentially Unwanted Software	6.9%
10	Win32/Dorkbot	Worms	6.8%

- The most common threat family in Tunisia in 2Q12 was [Win32/Autorun](#), which affected 17.8 percent of computers with detections in Tunisia. [Win32/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 threat family in Tunisia in 2Q12 was [Win32/Vobfus](#), which affected 14.2 percent of computers with detections in Tunisia. [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 in Tunisia in 2Q12 was [Win32/Sality](#), which affected 12.4 percent of computers with detections in Tunisia. [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 in Tunisia in 2Q12 was [Win32/Keygen](#), which affected 11.9 percent of computers with detections in Tunisia. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Tunisia

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	0.79 (1.6)	1.79 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	2.98 (3.9)	3.57 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	N/A (0.7)	0.00 (0.9)

Update service usage

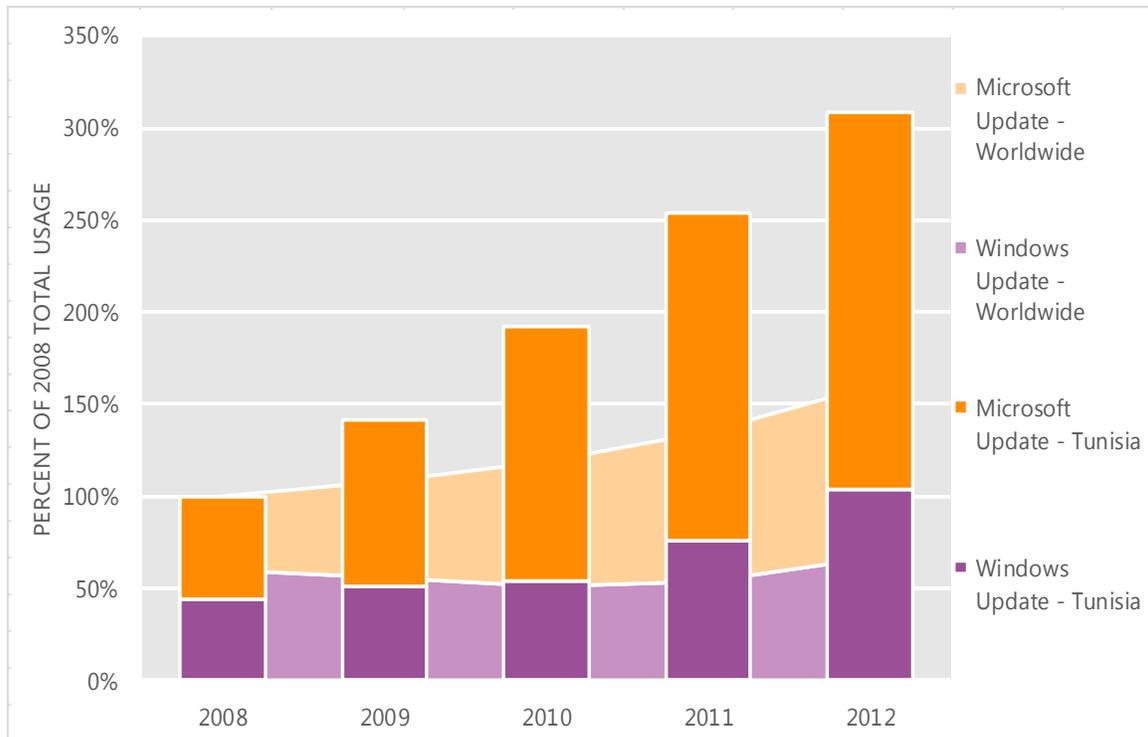
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Tunisia and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Tunisia over the last four years, indexed to the total usage for both services in Tunisia in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Tunisia was up 21.3 percent from 2011, and up 208.4 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Tunisia in 2012, 66.2 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Turkey

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Turkey in 2Q12 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.

Infection rate statistics for Turkey

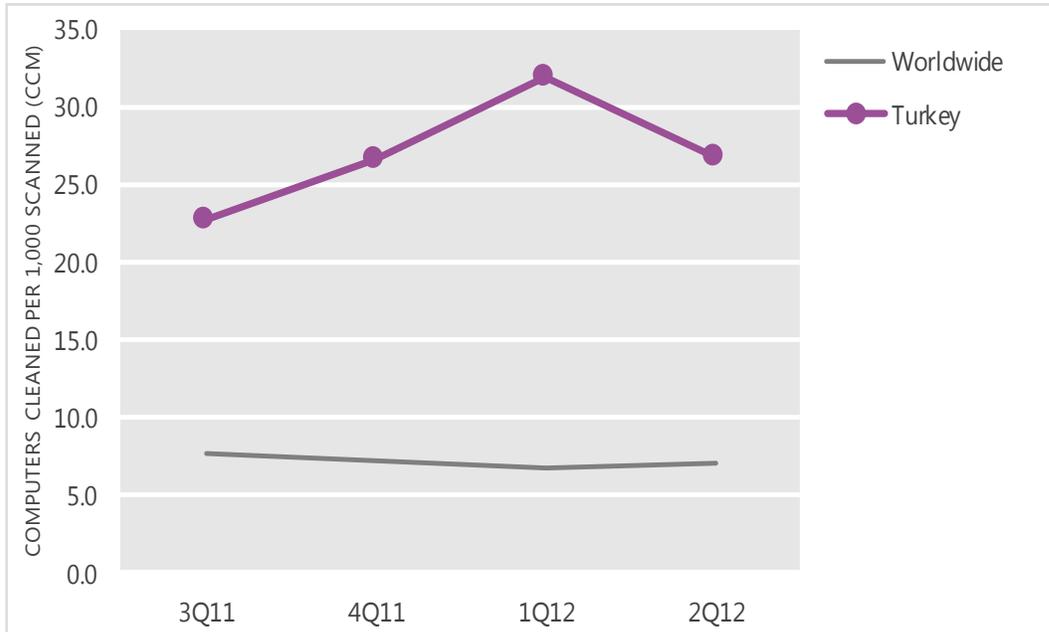
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	22.7	26.6	31.9	26.7
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

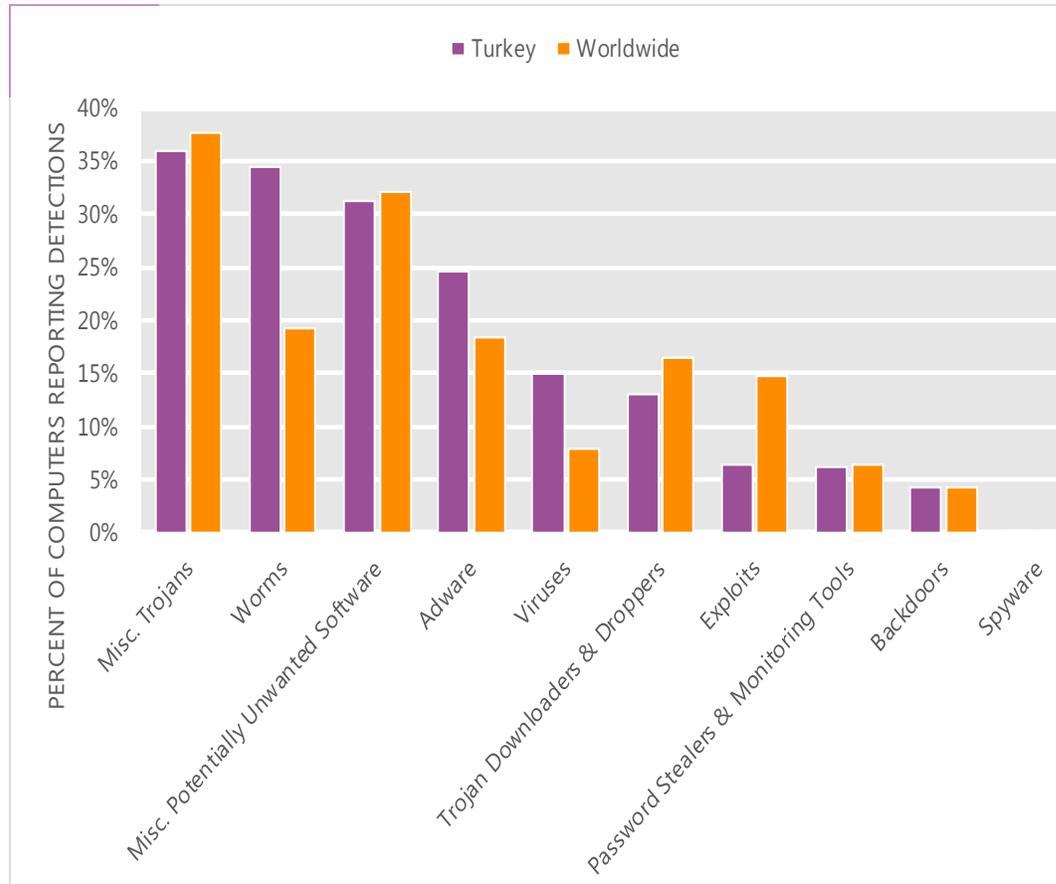
The MSRT detected malware on 26.7 of every 1,000 computers scanned in Turkey in 2Q12 (a CCM score of 26.7, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Turkey over the last four quarters, compared to the world as a whole.

CCM infection trends in Turkey and worldwide



Threat categories

Malware and potentially unwanted software categories in Turkey in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Turkey in 2Q12 was Miscellaneous Trojans. It affected 35.9 percent of all computers with detections there, down from 36.7 percent in 1Q12.
- The second most common category in Turkey in 2Q12 was Worms. It affected 34.5 percent of all computers with detections there, up from 34.3 percent in 1Q12.
- The third most common category in Turkey in 2Q12 was Miscellaneous Potentially Unwanted Software, which affected 31.2 percent of all computers with detections there, up from 31.1 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Turkey in 2Q12

	Family	Most significant category	% of computers with detections
1	JS/Pornpop	Adware	22.0%
2	Win32/Autorun	Worms	12.8%
3	Win32/Helompy	Worms	12.3%
4	Win32/Sality	Viruses	12.1%
5	Win32/Keygen	Misc. Potentially Unwanted Software	10.5%
6	Win32/Nuqel	Worms	7.7%
7	ASX/Wimad	Trojan Downloaders & Droppers	5.3%
8	JS/Iframe	Misc. Trojans	5.3%
9	Win32/Brontok	Worms	4.3%
10	Win32/Conficker	Worms	4.0%

- The most common threat family in Turkey in 2Q12 was [JS/Pornpop](#), which affected 22.0 percent of computers with detections in Turkey. [JS/Pornpop](#) is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The second most common threat family in Turkey in 2Q12 was [Win32/Autorun](#), which affected 12.8 percent of computers with detections in Turkey. [Win32/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 threat family in Turkey in 2Q12 was [Win32/Helompy](#), which affected 12.3 percent of computers with detections in Turkey. [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 in Turkey in 2Q12 was [Win32/Sality](#), which affected 12.1 percent of computers with detections in Turkey. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Turkey

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	1.47 (1.6)	1.52 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	2.46 (3.9)	2.72 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.51 (0.7)	2.56 (0.9)

Update service usage

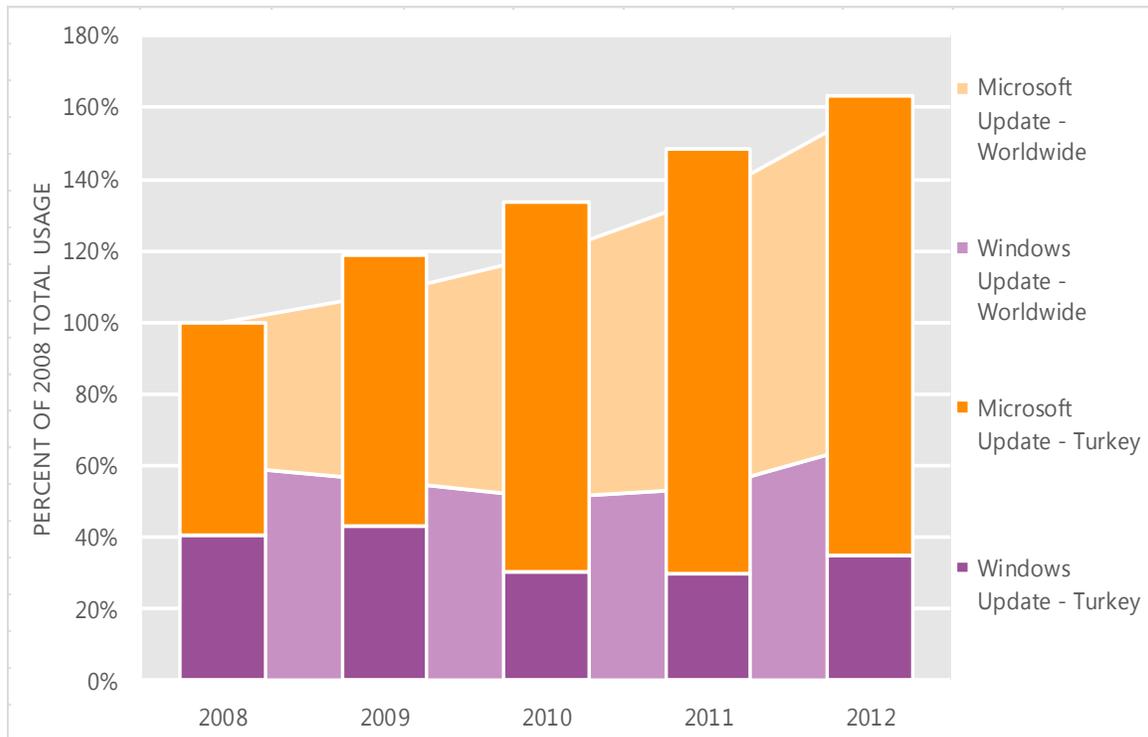
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Turkey and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Turkey over the last four years, indexed to the total usage for both services in Turkey in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Turkey was up 10.1 percent from 2011, and up 63.4 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Turkey in 2012, 78.6 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Uganda

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Uganda in 2Q12 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.

Infection rate statistics for Uganda

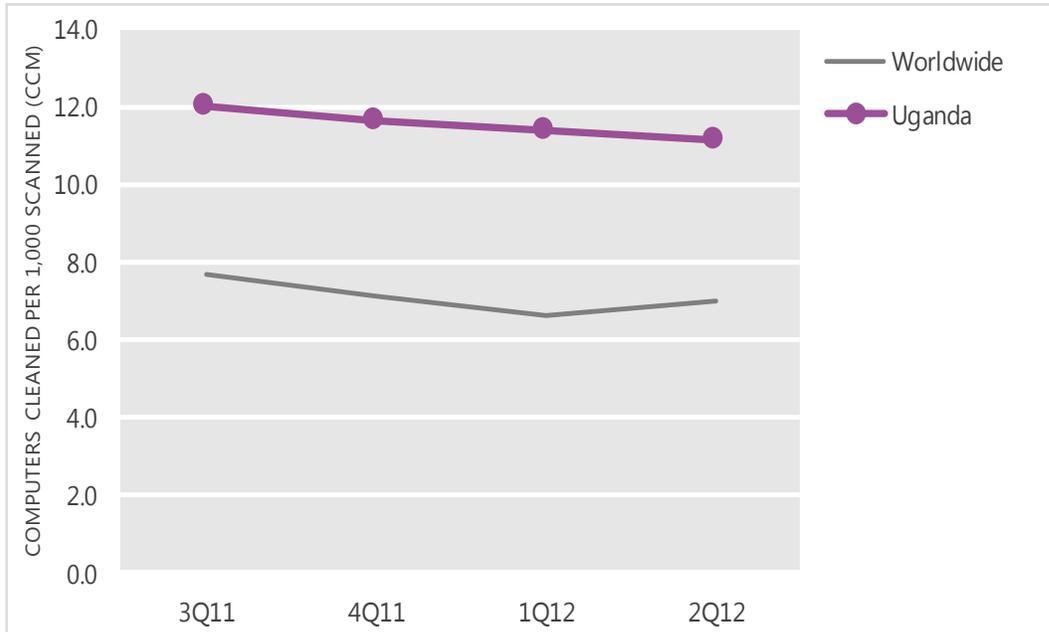
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	12.0	11.6	11.4	11.1
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website at www.microsoft.com/sir for more information about threats in Uganda and around the world, and for explanations of the methods and terms used here.

Infection trends (CCM)

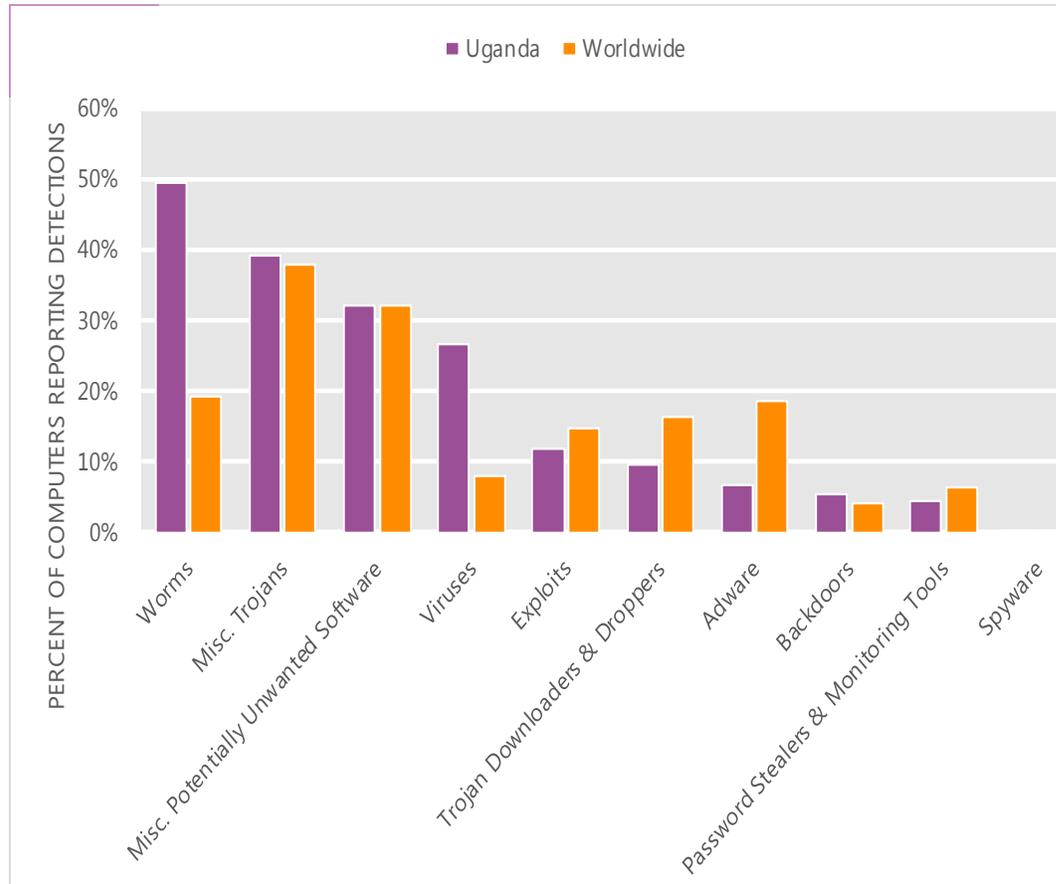
The MSRT detected malware on 11.1 of every 1,000 computers scanned in Uganda in 2Q12 (a CCM score of 11.1, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Uganda over the last four quarters, compared to the world as a whole.

CCM infection trends in Uganda and worldwide



Threat categories

Malware and potentially unwanted software categories in Uganda in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Uganda in 2Q12 was Worms. It affected 49.6 percent of all computers with detections there, down from 49.8 percent in 1Q12.
- The second most common category in Uganda in 2Q12 was Miscellaneous Trojans. It affected 39.3 percent of all computers with detections there, up from 36.5 percent in 1Q12.
- The third most common category in Uganda in 2Q12 was Miscellaneous Potentially Unwanted Software, which affected 32.0 percent of all computers with detections there, up from 31.1 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Uganda in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Vobfus	Worms	21.5%
2	Win32/Autorun	Worms	19.9%
3	Win32/Sality	Viruses	17.1%
4	Win32/Dorkbot	Worms	14.7%
5	Win32/Ramnit	Misc. Trojans	13.0%
6	Win32/CplLnk	Exploits	9.4%
7	Win32/Rimecud	Worms	9.1%
8	Win32/Virut	Viruses	8.4%
9	Win32/Keygen	Misc. Potentially Unwanted Software	7.4%
10	Win32/Nuqel	Worms	5.5%

- The most common threat family in Uganda in 2Q12 was [Win32/Vobfus](#), which affected 21.5 percent of computers with detections in Uganda. [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 second most common threat family in Uganda in 2Q12 was [Win32/Autorun](#), which affected 19.9 percent of computers with detections in Uganda. [Win32/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 threat family in Uganda in 2Q12 was [Win32/Sality](#), which affected 17.1 percent of computers with detections in Uganda. [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 in Uganda in 2Q12 was [Win32/Dorkbot](#), which affected 14.7 percent of computers with detections in Uganda. [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.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Uganda

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	N/A (1.6)	N/A (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	N/A (3.9)	N/A (4.4)
Drive-by download per 1,000 URLs (Worldwide)	N/A (0.7)	N/A (0.9)

Update service usage

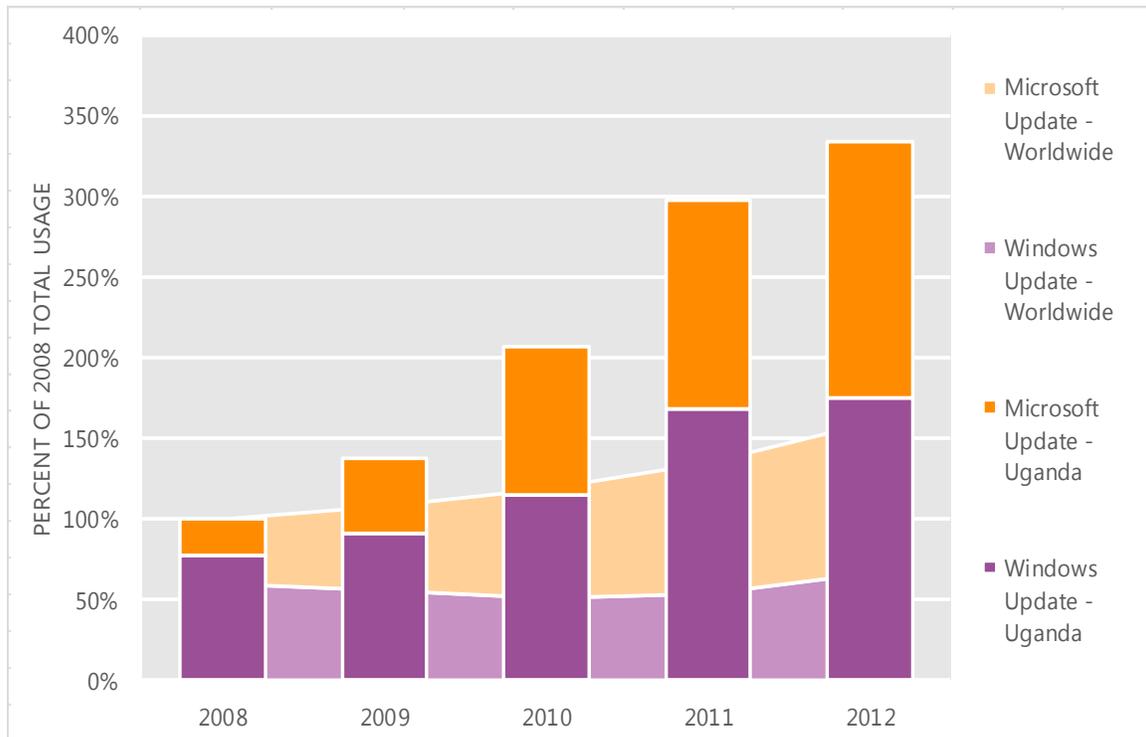
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Uganda and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Uganda over the last four years, indexed to the total usage for both services in Uganda in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Uganda was up 12.3 percent from 2011, and up 234.7 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Uganda in 2012, 47.5 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Ukraine

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Ukraine in 2Q12 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.

Infection rate statistics for Ukraine

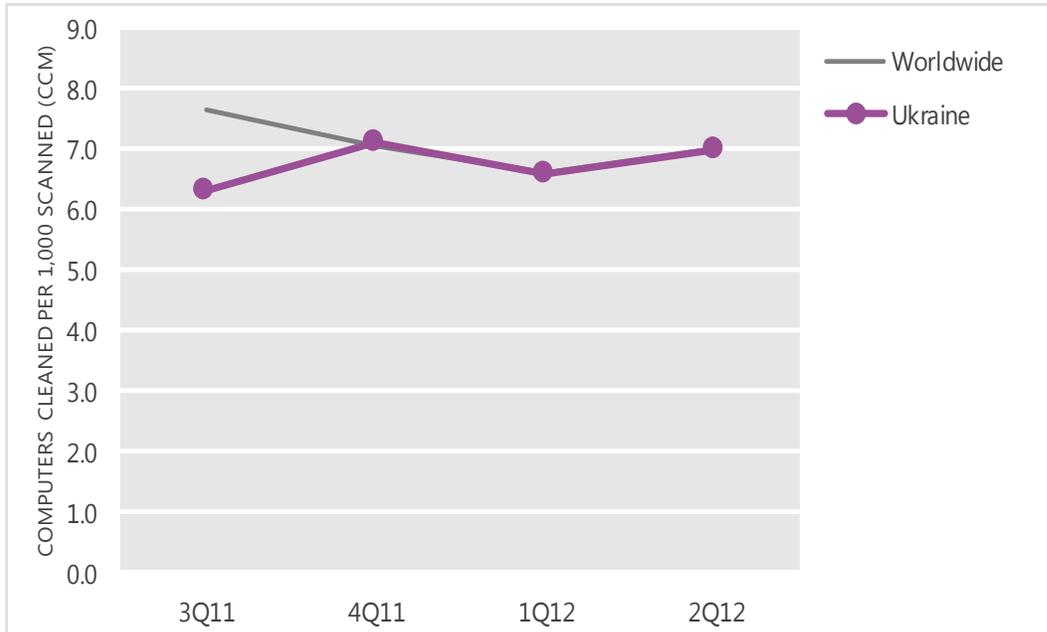
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	6.3	7.1	6.6	7.0
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

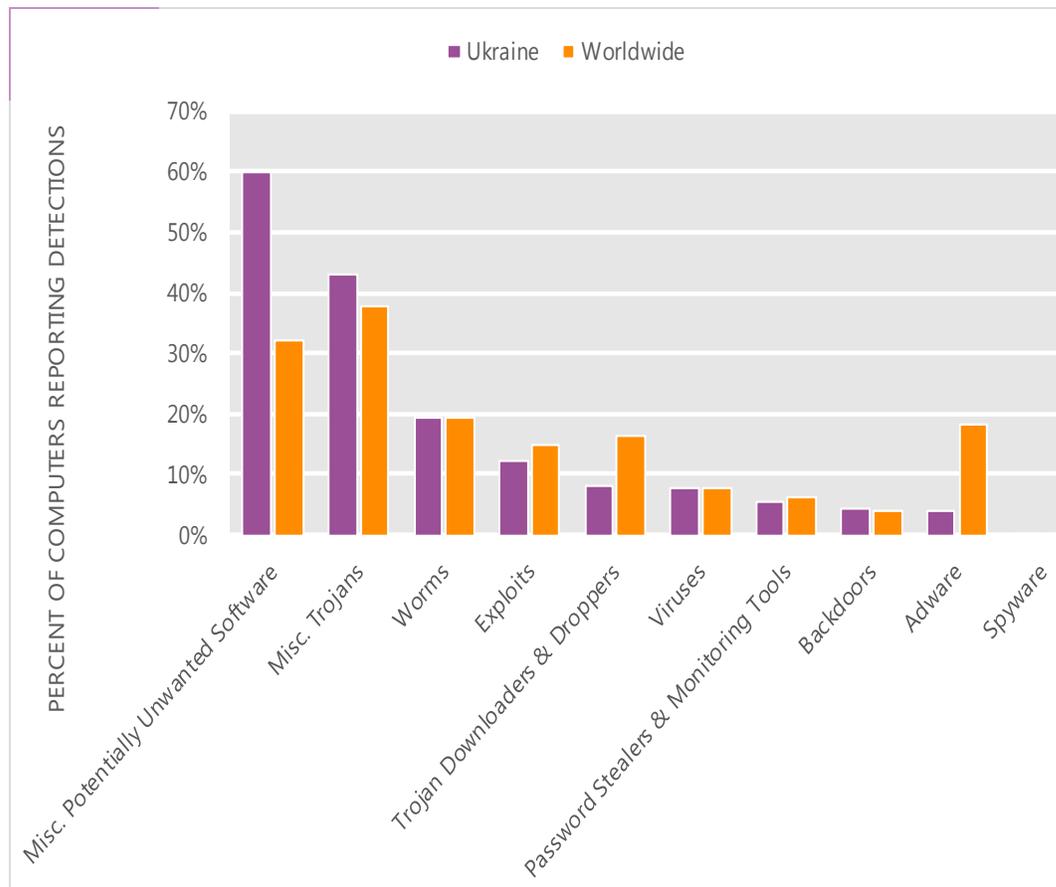
The MSRT detected malware on 7.0 of every 1,000 computers scanned in Ukraine in 2Q12 (a CCM score of 7.0, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Ukraine over the last four quarters, compared to the world as a whole.

CCM infection trends in Ukraine and worldwide



Threat categories

Malware and potentially unwanted software categories in Ukraine in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Ukraine in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 60.0 percent of all computers with detections there, down from 65.4 percent in 1Q12.
- The second most common category in Ukraine in 2Q12 was Miscellaneous Trojans. It affected 42.9 percent of all computers with detections there, up from 39.6 percent in 1Q12.
- The third most common category in Ukraine in 2Q12 was Worms, which affected 19.2 percent of all computers with detections there, down from 19.2 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Ukraine in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Pameseg	Misc. Potentially Unwanted Software	31.6%
2	Win32/Keygen	Misc. Potentially Unwanted Software	15.8%
3	Win32/Obfuscator	Misc. Potentially Unwanted Software	9.2%
4	Win32/Dorkbot	Worms	8.8%
5	JS/IframeRef	Misc. Trojans	8.1%
6	Win32/Vundo	Misc. Trojans	6.7%
7	Win32/Autorun	Worms	6.2%
8	Java/Blacole	Exploits	4.7%
9	Win32/Dynamer	Misc. Trojans	4.6%
10	Win32/Rimecud	Worms	4.6%

- The most common threat family in Ukraine in 2Q12 was [Win32/Pameseg](#), which affected 31.6 percent of computers with detections in Ukraine. [Win32/Pameseg](#) is a fake program installer that requires the user to send SMS messages to a premium number to successfully install certain programs.
- The second most common threat family in Ukraine in 2Q12 was [Win32/Keygen](#), which affected 15.8 percent of computers with detections in Ukraine. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The third most common threat family in Ukraine in 2Q12 was [Win32/Obfuscator](#), which affected 9.2 percent of computers with detections in Ukraine. [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 threat family in Ukraine in 2Q12 was [Win32/Dorkbot](#), which affected 8.8 percent of computers with detections in Ukraine. [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.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Ukraine

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	2.77 (1.6)	3.11 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	9.52 (3.9)	8.10 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	2.76 (0.7)	5.11 (0.9)

Update service usage

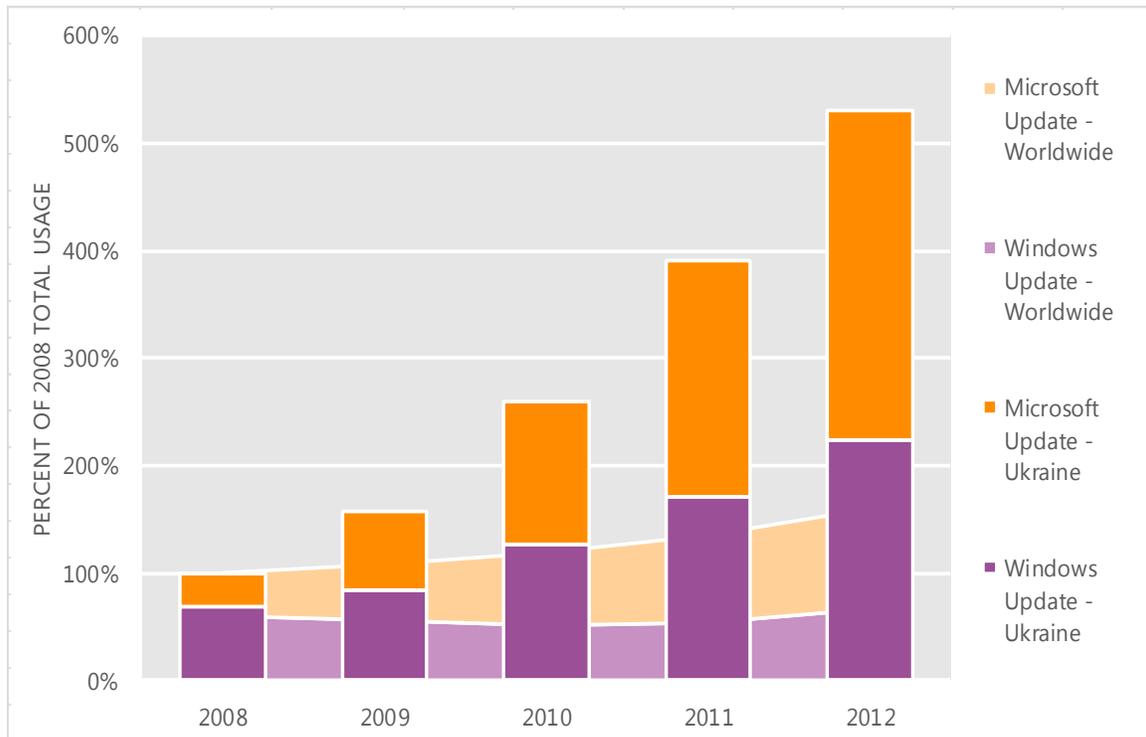
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Ukraine and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Ukraine over the last four years, indexed to the total usage for both services in Ukraine in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Ukraine was up 35.5 percent from 2011, and up 430.1 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Ukraine in 2012, 57.9 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

United Arab Emirates

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in the United Arab Emirates in 2Q12 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.

Infection rate statistics for the United Arab Emirates

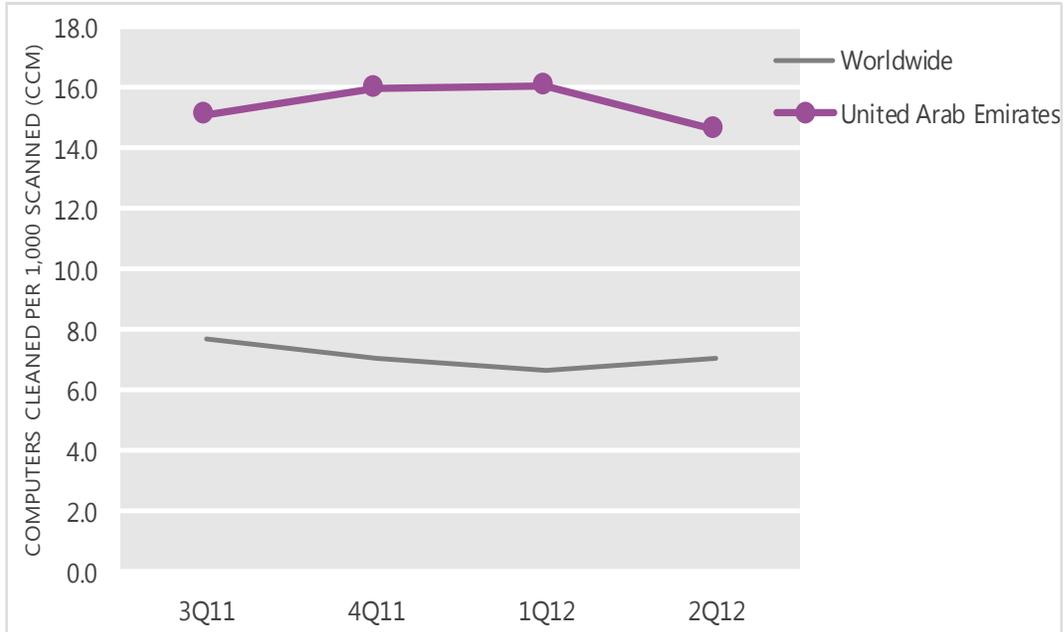
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	15.1	16.0	16.1	14.6
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

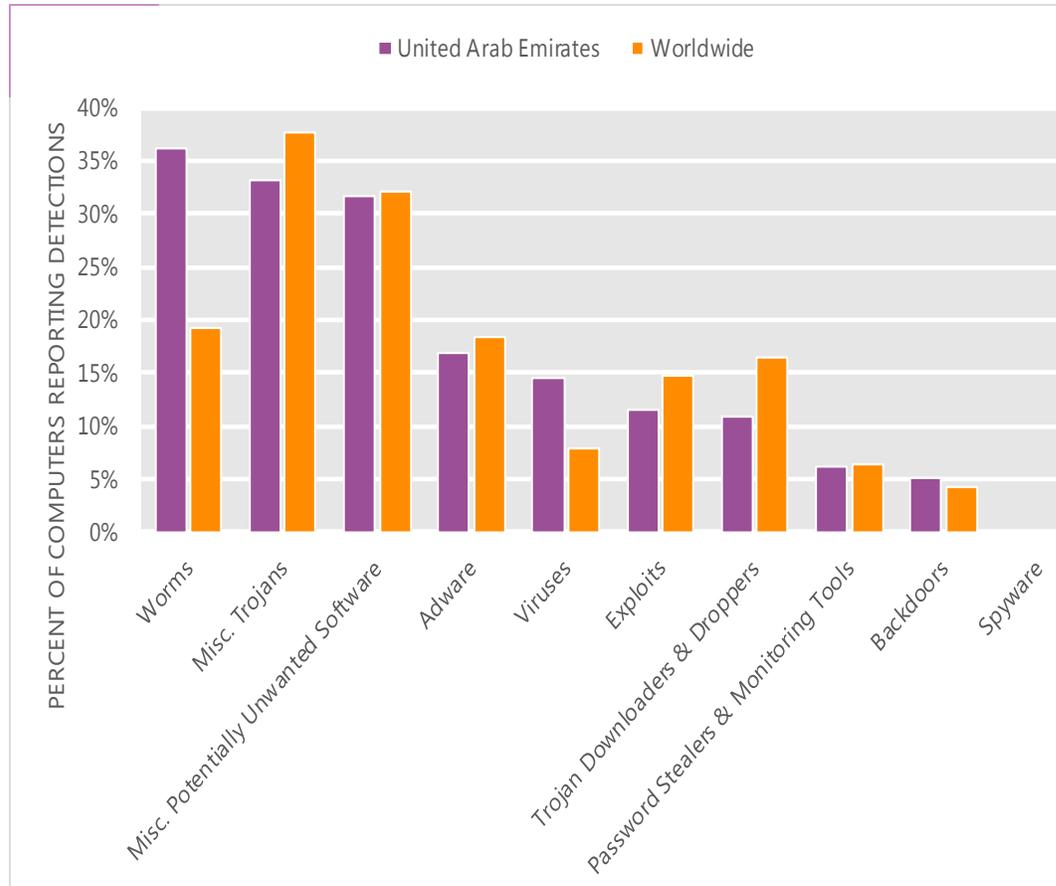
The MSRT detected malware on 14.6 of every 1,000 computers scanned in the United Arab Emirates in 2Q12 (a CCM score of 14.6, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for the United Arab Emirates over the last four quarters, compared to the world as a whole.

CCM infection trends in the United Arab Emirates and worldwide



Threat categories

Malware and potentially unwanted software categories in the United Arab Emirates in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in the United Arab Emirates in 2Q12 was Worms. It affected 36.3 percent of all computers with detections there, down from 36.3 percent in 1Q12.
- The second most common category in the United Arab Emirates in 2Q12 was Miscellaneous Trojans. It affected 33.2 percent of all computers with detections there, up from 32.2 percent in 1Q12.
- The third most common category in the United Arab Emirates in 2Q12 was Miscellaneous Potentially Unwanted Software, which affected 31.6 percent of all computers with detections there, up from 30.3 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in the United Arab Emirates in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Autorun	Worms	15.3%
2	Win32/Keygen	Misc. Potentially Unwanted Software	10.5%
3	Win32/Sality	Viruses	9.4%
4	Win32/Hotbar	Adware	8.1%
5	Win32/Nuqel	Worms	8.0%
6	Win32/Vobfus	Worms	5.9%
7	Win32/Zwangi	Misc. Potentially Unwanted Software	5.0%
8	Win32/Dorkbot	Worms	4.6%
9	ASX/Wimad	Trojan Downloaders & Droppers	4.6%
10	Win32/Rimecud	Worms	4.6%

- The most common threat family in the United Arab Emirates in 2Q12 was [Win32/Autorun](#), which affected 15.3 percent of computers with detections in the United Arab Emirates. [Win32/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 threat family in the United Arab Emirates in 2Q12 was [Win32/Keygen](#), which affected 10.5 percent of computers with detections in the United Arab Emirates. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The third most common threat family in the United Arab Emirates in 2Q12 was [Win32/Sality](#), which affected 9.4 percent of computers with detections in the United Arab Emirates. [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 in the United Arab Emirates in 2Q12 was [Win32/Hotbar](#), which affected 8.1 percent of computers with detections in the United Arab Emirates. [Win32/Hotbar](#) is adware that displays a dynamic toolbar and targeted pop-up ads based on its monitoring of web-browsing activity.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for the United Arab Emirates

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	0.57 (1.6)	0.57 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	1.37 (3.9)	2.05 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.06 (0.7)	0.05 (0.9)

Update service usage

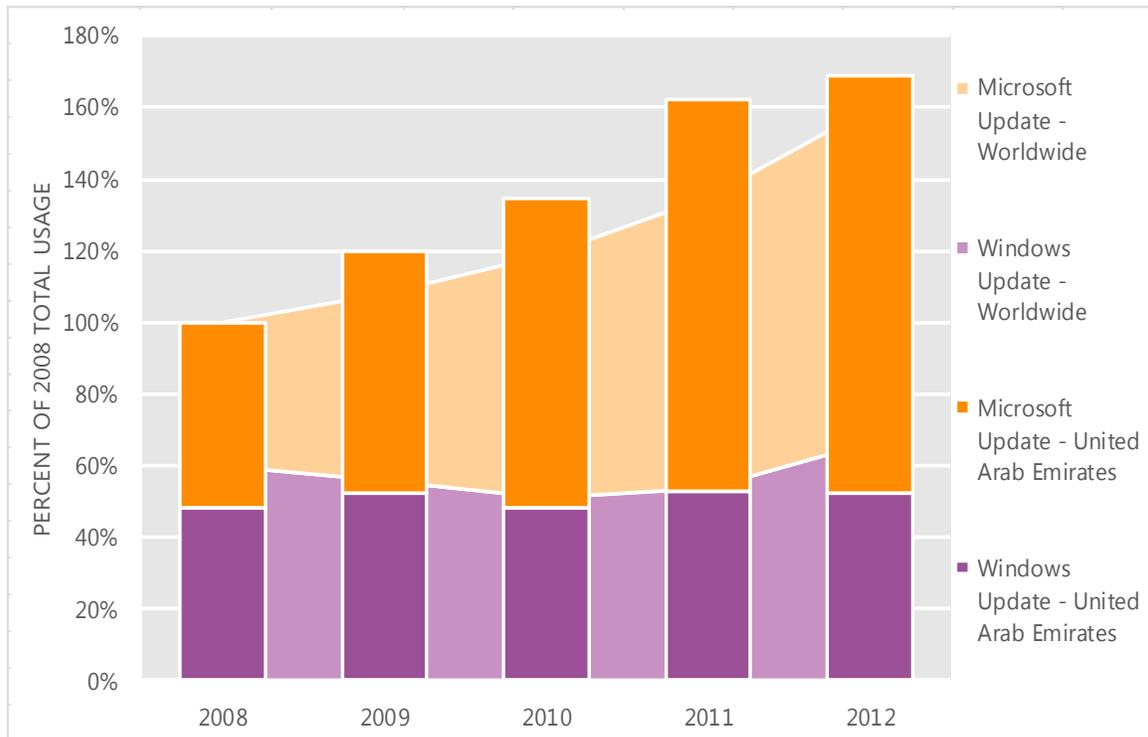
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in the United Arab Emirates and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in the United Arab Emirates over the last four years, indexed to the total usage for both services in the United Arab Emirates in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in the United Arab Emirates was up 4.4 percent from 2011, and up 69.2 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in the United Arab Emirates in 2012, 69.0 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

United Kingdom

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in the United Kingdom in 2Q12 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.

Infection rate statistics for the United Kingdom

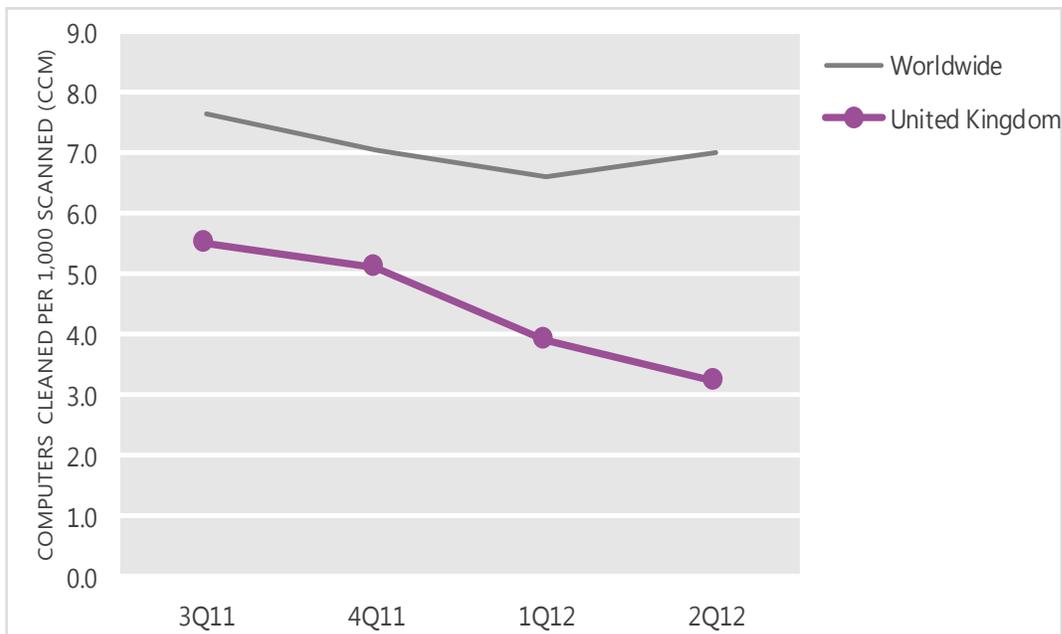
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	5.5	5.1	3.9	3.2
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

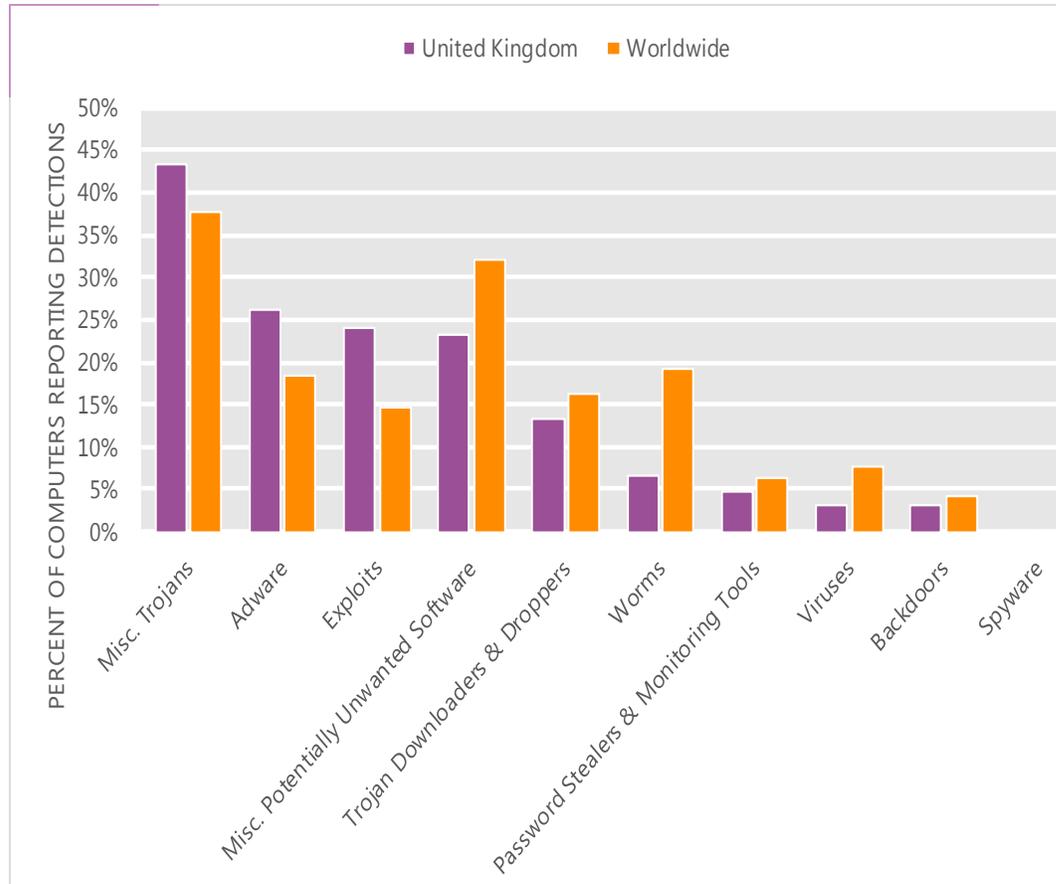
The MSRT detected malware on 3.2 of every 1,000 computers scanned in the United Kingdom in 2Q12 (a CCM score of 3.2, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for the United Kingdom over the last four quarters, compared to the world as a whole.

CCM infection trends in the United Kingdom and worldwide



Threat categories

Malware and potentially unwanted software categories in the United Kingdom in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in the United Kingdom in 2Q12 was Miscellaneous Trojans. It affected 43.2 percent of all computers with detections there, down from 44.5 percent in 1Q12.
- The second most common category in the United Kingdom in 2Q12 was Adware. It affected 26.1 percent of all computers with detections there, down from 34.8 percent in 1Q12.
- The third most common category in the United Kingdom in 2Q12 was Exploits, which affected 24.0 percent of all computers with detections there, up from 22.2 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in the United Kingdom in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Hotbar	Adware	13.0%
2	Java/Blacole	Exploits	11.5%
3	JS/BlacoleRef	Misc. Trojans	10.4%
4	JS/Pornpop	Adware	8.3%
5	Win32/Keygen	Misc. Potentially Unwanted Software	7.1%
6	JS/IframeRef	Misc. Trojans	6.9%
7	Win32/FakePAV	Misc. Trojans	6.6%
8	Win32/Pdfjsc	Exploits	5.9%
9	Java/CVE-2012-0507	Exploits	5.7%
10	ASX/Wimad	Trojan Downloaders & Droppers	5.4%

- The most common threat family in the United Kingdom in 2Q12 was [Win32/Hotbar](#), which affected 13.0 percent of computers with detections in the United Kingdom. [Win32/Hotbar](#) is adware that displays a dynamic toolbar and targeted pop-up ads based on its monitoring of web-browsing activity.
- The second most common threat family in the United Kingdom in 2Q12 was [Java/Blacole](#), which affected 11.5 percent of computers with detections in the United Kingdom. [Java/Blacole](#) is an exploit pack, also known as Blackhole, that is installed on a compromised web server by an attacker and includes a number of exploits that target browser software. If a vulnerable computer browses a compromised website that contains the exploit pack, various malware may be downloaded and run.
- The third most common threat family in the United Kingdom in 2Q12 was [JS/BlacoleRef](#), which affected 10.4 percent of computers with detections in the United Kingdom. [JS/BlacoleRef](#) is an obfuscated script, often found inserted into compromised websites, that uses a hidden inline frame to redirect the browser to a Blacole exploit server.
- The fourth most common threat family in the United Kingdom in 2Q12 was [JS/Pornpop](#), which affected 8.3 percent of computers with detections in the United Kingdom. [JS/Pornpop](#) is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for the United Kingdom

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	1.63 (1.6)	1.88 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	2.33 (3.9)	2.97 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.47 (0.7)	0.53 (0.9)

Update service usage

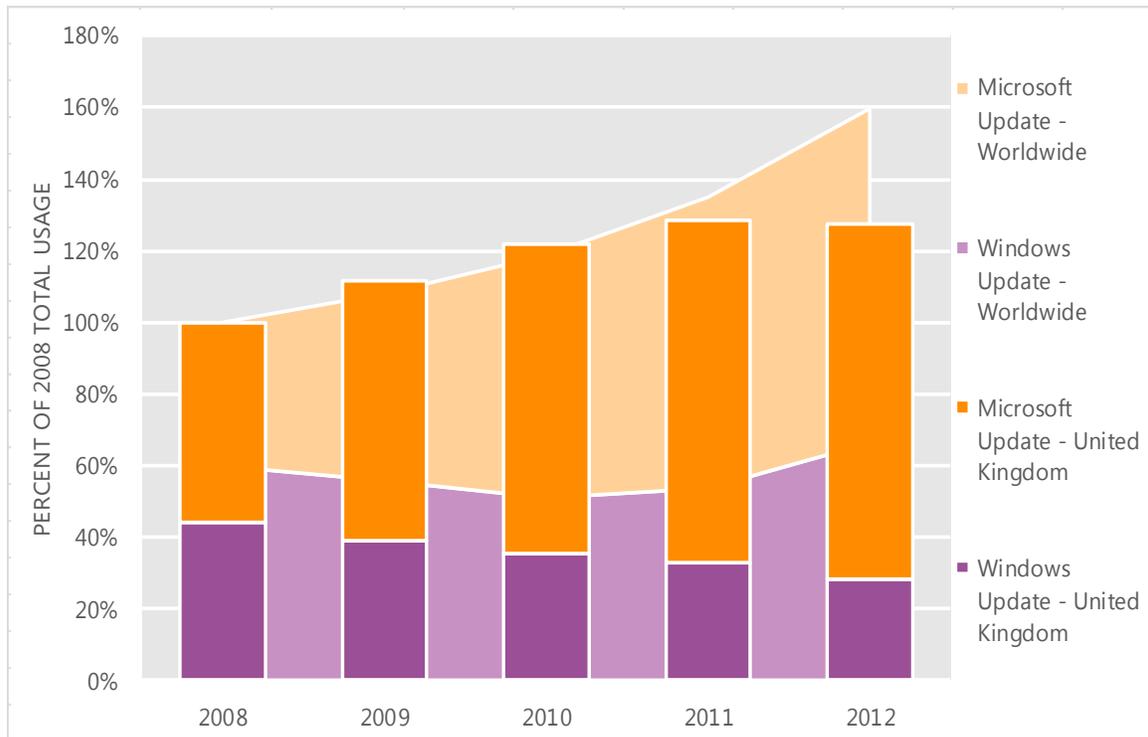
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in the United Kingdom and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in the United Kingdom over the last four years, indexed to the total usage for both services in the United Kingdom in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in the United Kingdom was down 0.9 percent from 2011, and up 27.3 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in the United Kingdom in 2012, 77.8 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

United States

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in the United States in 2Q12 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.

Infection rate statistics for the United States

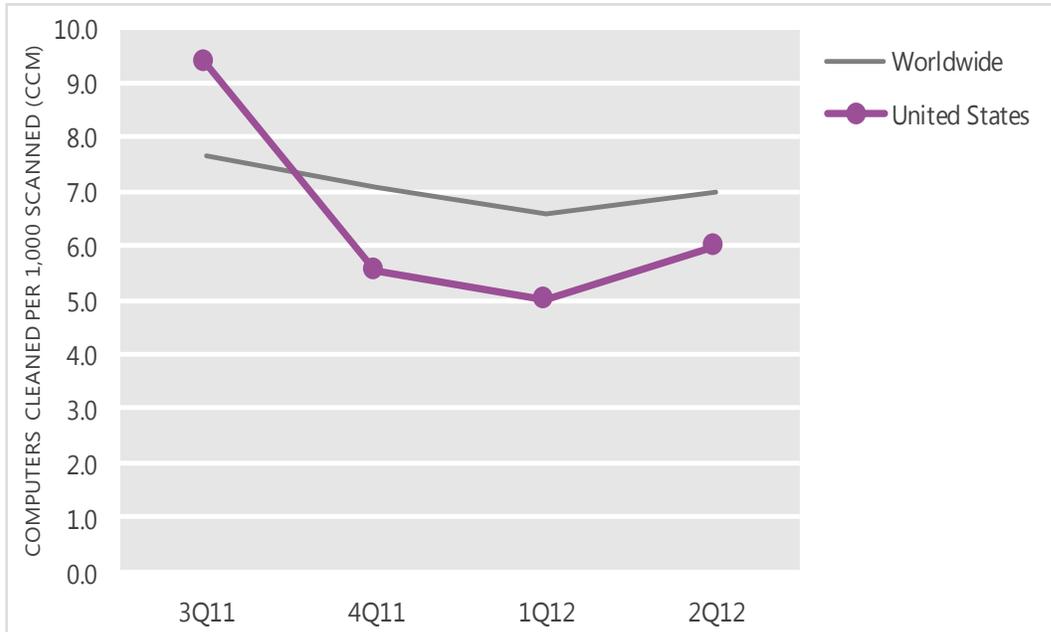
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	9.4	5.5	5.0	6.0
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

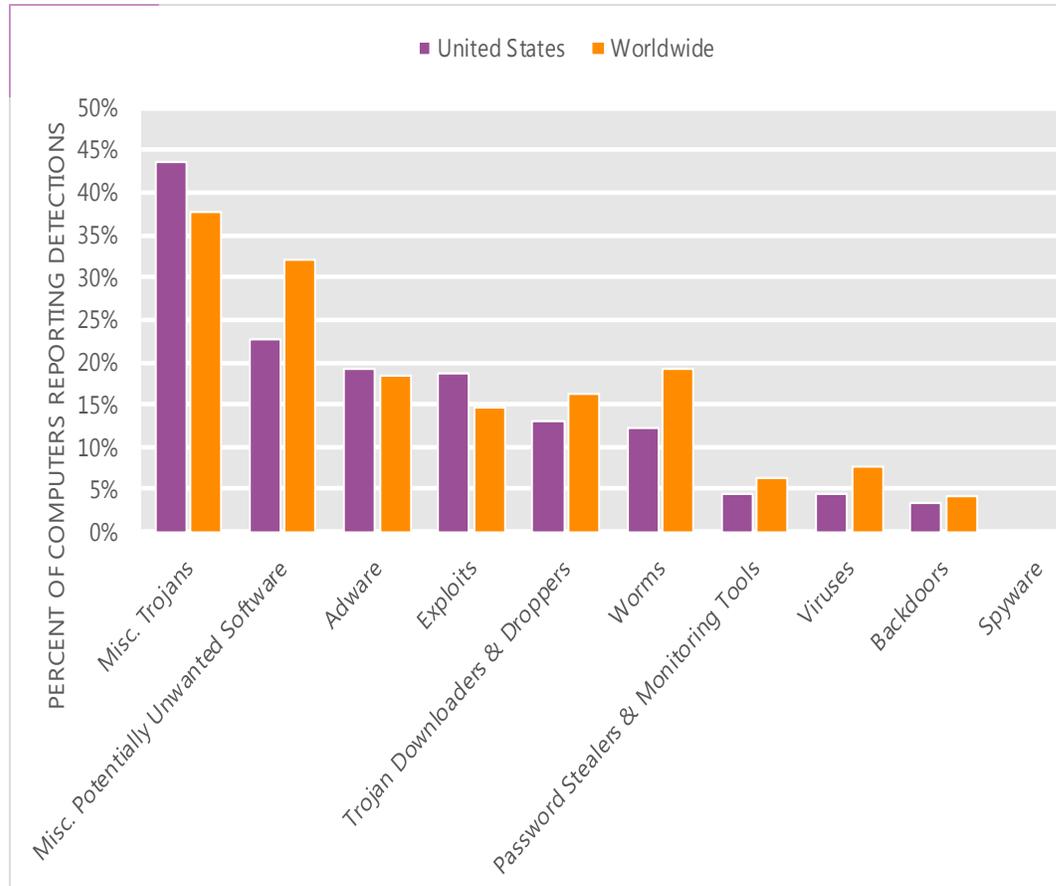
The MSRT detected malware on 6.0 of every 1,000 computers scanned in the United States in 2Q12 (a CCM score of 6.0, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for the United States over the last four quarters, compared to the world as a whole.

CCM infection trends in the United States and worldwide



Threat categories

Malware and potentially unwanted software categories in the United States in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in the United States in 2Q12 was Miscellaneous Trojans. It affected 43.6 percent of all computers with detections there, up from 39.8 percent in 1Q12.
- The second most common category in the United States in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 22.7 percent of all computers with detections there, up from 19.6 percent in 1Q12.
- The third most common category in the United States in 2Q12 was Adware, which affected 19.1 percent of all computers with detections there, down from 31.8 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in the United States in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/FakePAV	Misc. Trojans	9.9%
2	JS/IframeRef	Misc. Trojans	7.1%
3	Java/Blacole	Exploits	6.6%
4	Win32/Hotbar	Adware	5.9%
5	JS/Pornpop	Adware	5.7%
6	Win32/Keygen	Misc. Potentially Unwanted Software	5.5%
7	Win32/Sirefef	Misc. Trojans	5.3%
8	Win32/Autorun	Worms	4.3%
9	Java/CVE-2012-0507	Exploits	4.3%
10	Win32/Pdfjsc	Exploits	4.1%

- The most common threat family in the United States in 2Q12 was [Win32/FakePAV](#), which affected 9.9 percent of computers with detections in the United States. [Win32/FakePAV](#) is a rogue security software family that often masquerades as Microsoft Security Essentials or other legitimate antimalware products.
- The second most common threat family in the United States in 2Q12 was [JS/IframeRef](#), which affected 7.1 percent of computers with detections in the United States. [JS/IframeRef](#) is a generic detection for specially formed IFrame tags that point to remote websites that contain malicious content.
- The third most common threat family in the United States in 2Q12 was [Java/Blacole](#), which affected 6.6 percent of computers with detections in the United States. [Java/Blacole](#) is an exploit pack, also known as Blackhole, that is installed on a compromised web server by an attacker and includes a number of exploits that target browser software. If a vulnerable computer browses a compromised website that contains the exploit pack, various malware may be downloaded and run.
- The fourth most common threat family in the United States in 2Q12 was [Win32/Hotbar](#), which affected 5.9 percent of computers with detections in the United States. [Win32/Hotbar](#) is adware that displays a dynamic toolbar and targeted pop-up ads based on its monitoring of web-browsing activity.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for the United States

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	2.64 (1.6)	2.92 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	4.87 (3.9)	5.65 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.71 (0.7)	0.69 (0.9)

Update service usage

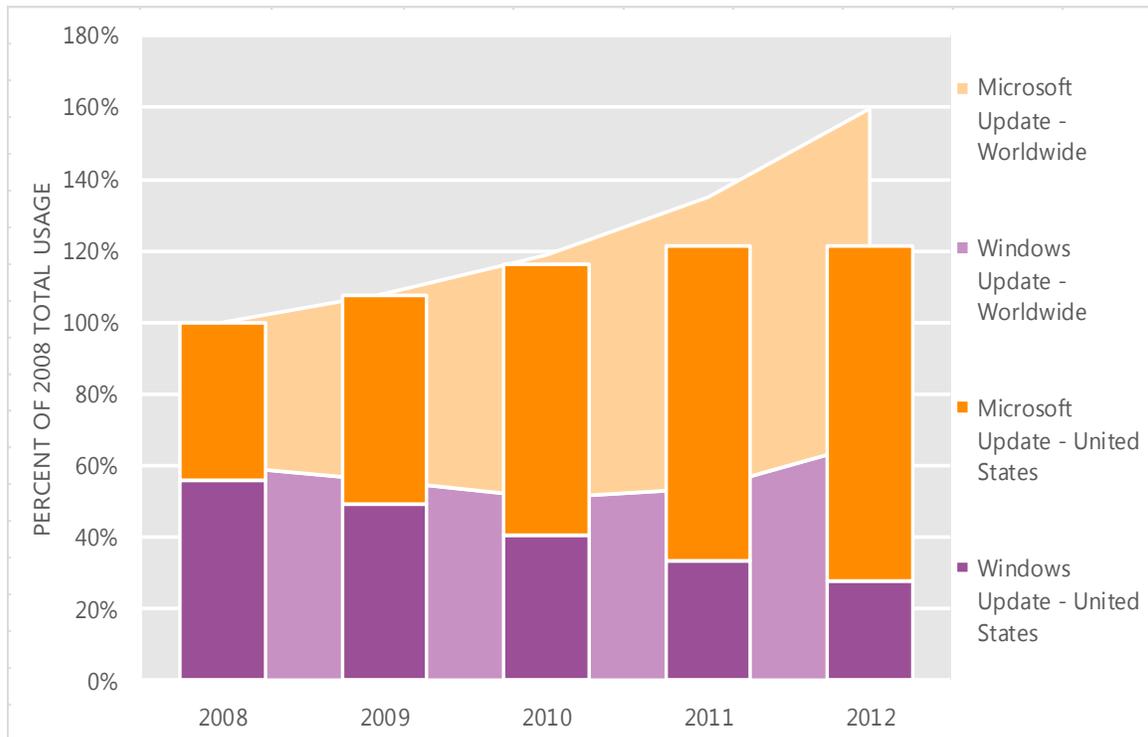
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in the United States and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in the United States over the last four years, indexed to the total usage for both services in the United States in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in the United States was up 0.1 percent from 2011, and up 21.6 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in the United States in 2012, 77.1 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Uruguay

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Uruguay in 2Q12 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.

Infection rate statistics for Uruguay

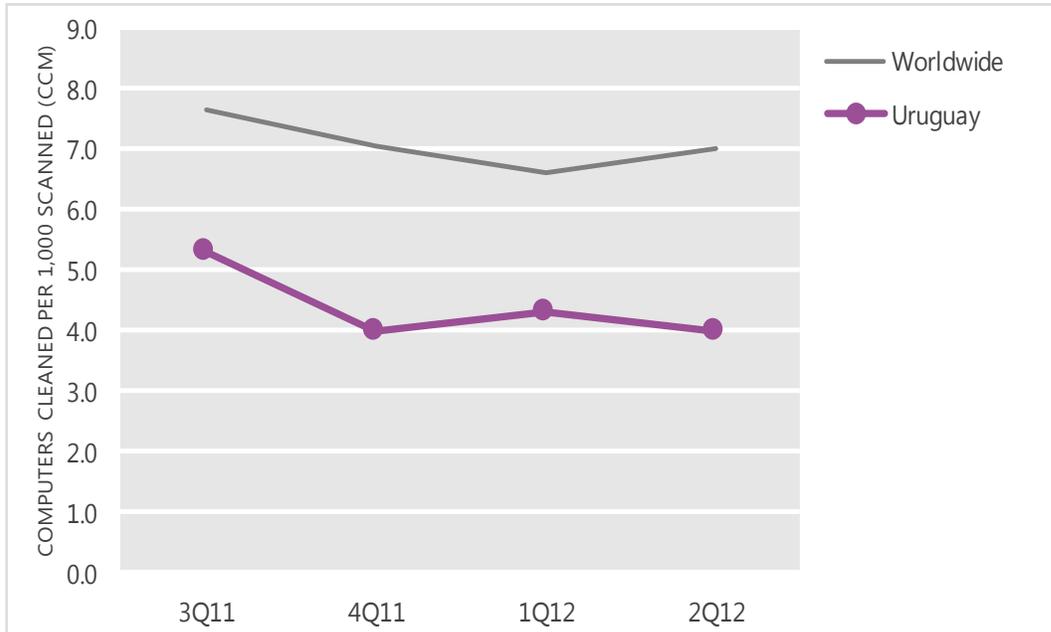
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	5.3	4.0	4.3	4.0
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

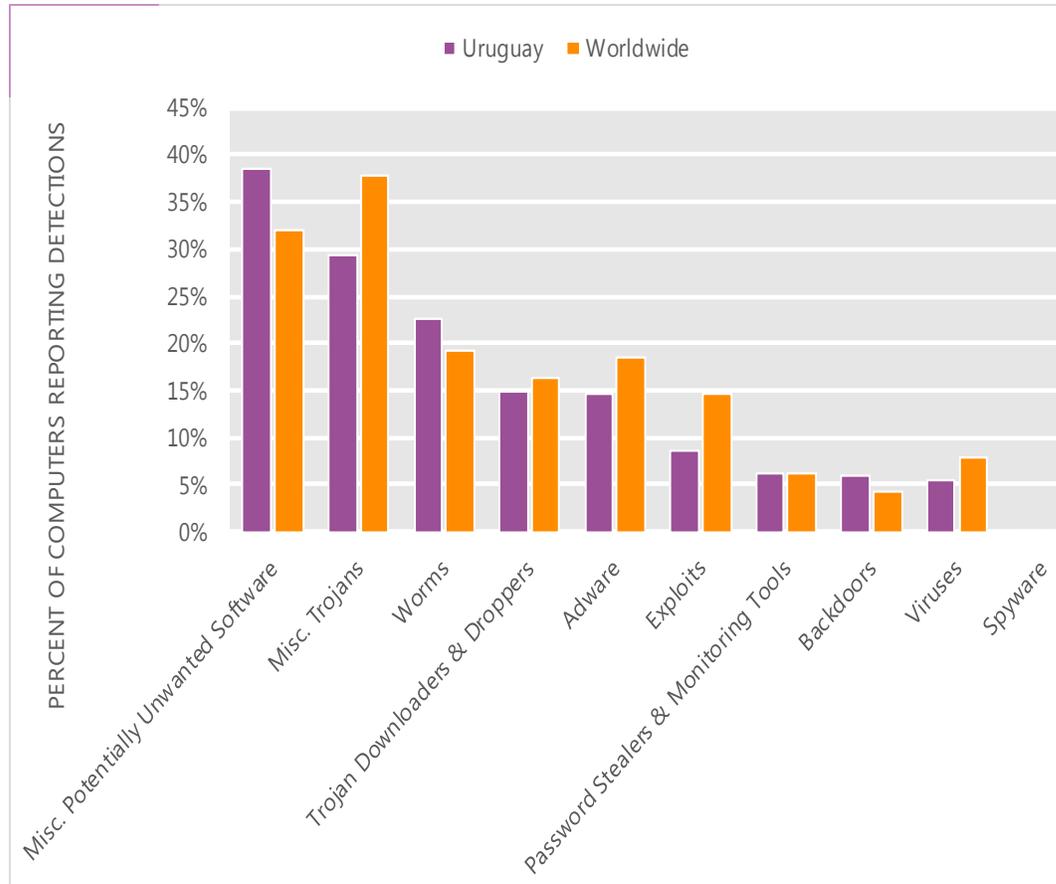
The MSRT detected malware on 4.0 of every 1,000 computers scanned in Uruguay in 2Q12 (a CCM score of 4.0, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Uruguay over the last four quarters, compared to the world as a whole.

CCM infection trends in Uruguay and worldwide



Threat categories

Malware and potentially unwanted software categories in Uruguay in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Uruguay in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 38.4 percent of all computers with detections there, down from 42.1 percent in 1Q12.
- The second most common category in Uruguay in 2Q12 was Miscellaneous Trojans. It affected 29.2 percent of all computers with detections there, up from 25.3 percent in 1Q12.
- The third most common category in Uruguay in 2Q12 was Worms, which affected 22.5 percent of all computers with detections there, up from 21.6 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Uruguay in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Keygen	Misc. Potentially Unwanted Software	13.5%
2	Win32/Autorun	Worms	7.9%
3	Win32/Dorkbot	Worms	7.3%
4	ASX/Wimad	Trojan Downloaders & Droppers	7.0%
5	Win32/Conficker	Worms	6.0%
6	JS/Pornpop	Adware	5.6%
7	JS/Redirector	Misc. Trojans	5.4%
8	Win32/Zwangi	Misc. Potentially Unwanted Software	5.2%
9	Java/Blacole	Exploits	3.8%
10	JS/IframeRef	Misc. Trojans	3.2%

- The most common threat family in Uruguay in 2Q12 was [Win32/Keygen](#), which affected 13.5 percent of computers with detections in Uruguay. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The second most common threat family in Uruguay in 2Q12 was [Win32/Autorun](#), which affected 7.9 percent of computers with detections in Uruguay. [Win32/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 threat family in Uruguay in 2Q12 was [Win32/Dorkbot](#), which affected 7.3 percent of computers with detections in Uruguay. [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 in Uruguay in 2Q12 was [ASX/Wimad](#), which affected 7.0 percent of computers with detections in Uruguay. [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.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Uruguay

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	0.66 (1.6)	0.26 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	1.71 (3.9)	1.32 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.00 (0.7)	0.00 (0.9)

Update service usage

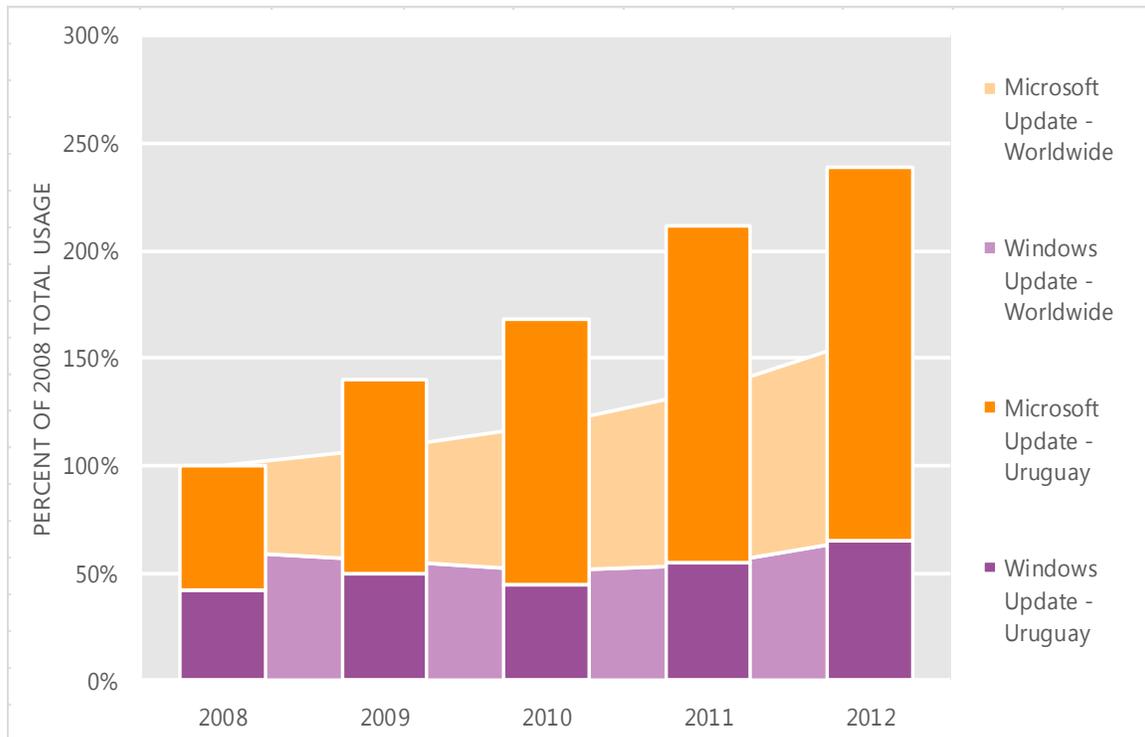
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Uruguay and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Uruguay over the last four years, indexed to the total usage for both services in Uruguay in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Uruguay was up 12.8 percent from 2011, and up 138.8 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Uruguay in 2012, 72.7 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Venezuela

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Venezuela in 2Q12 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.

Infection rate statistics for Venezuela

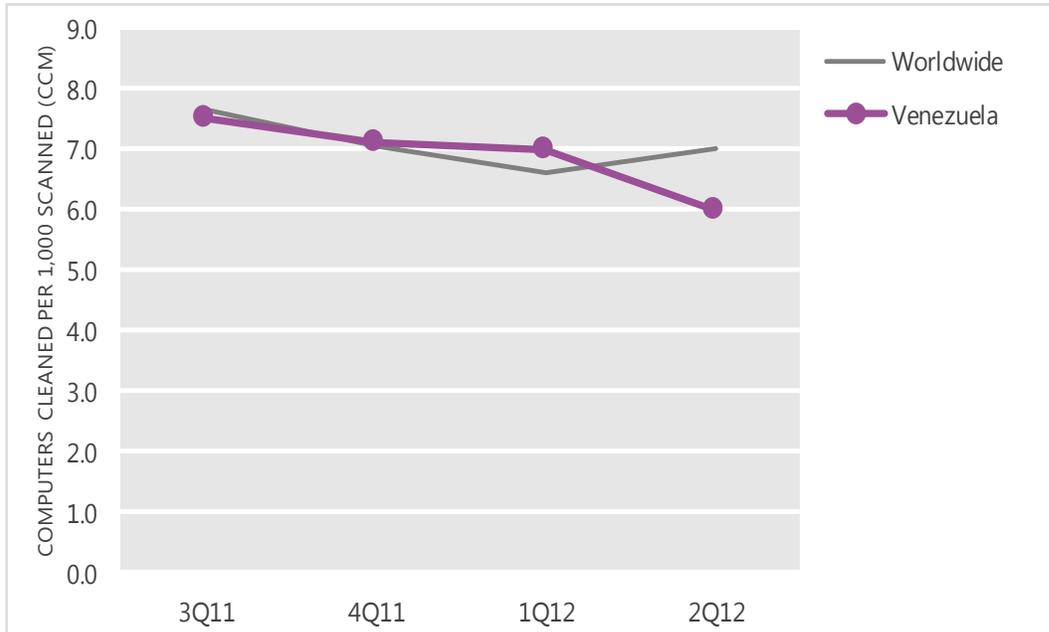
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	7.5	7.1	7.0	6.0
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

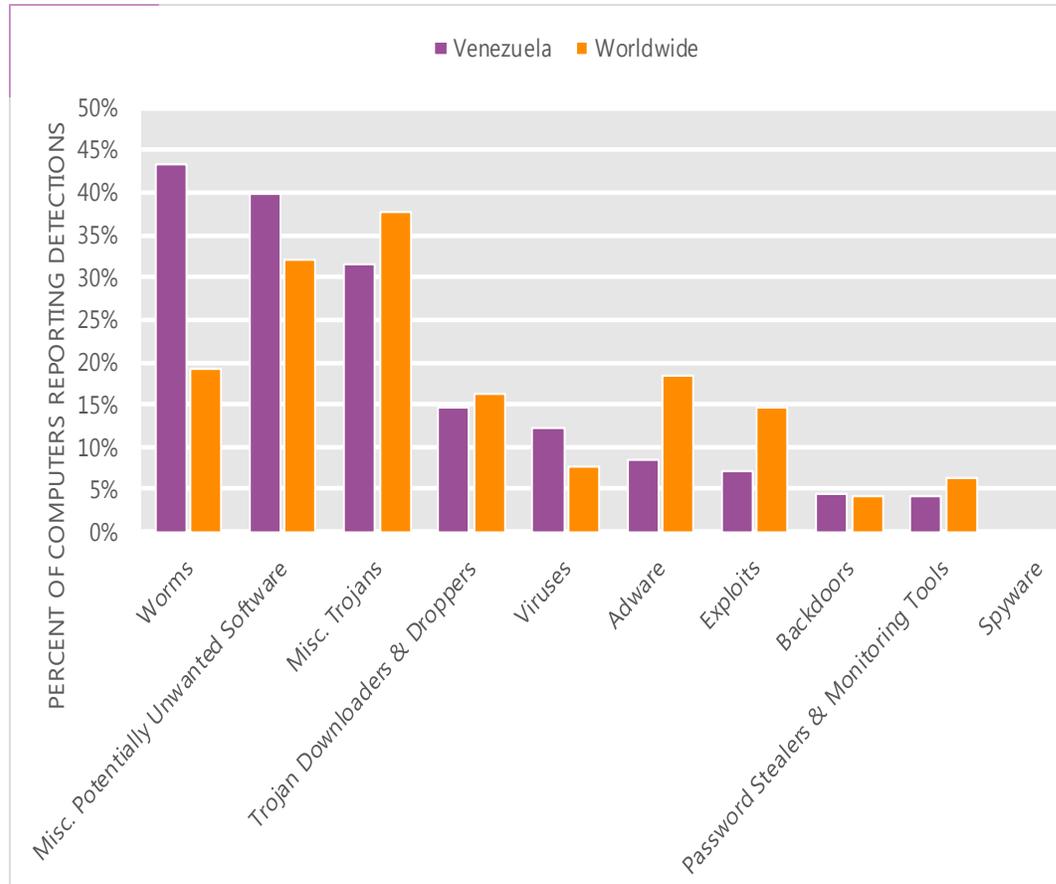
The MSRT detected malware on 6.0 of every 1,000 computers scanned in Venezuela in 2Q12 (a CCM score of 6.0, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Venezuela over the last four quarters, compared to the world as a whole.

CCM infection trends in Venezuela and worldwide



Threat categories

Malware and potentially unwanted software categories in Venezuela in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Venezuela in 2Q12 was Worms. It affected 43.3 percent of all computers with detections there, up from 41.2 percent in 1Q12.
- The second most common category in Venezuela in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 39.9 percent of all computers with detections there, down from 44.1 percent in 1Q12.
- The third most common category in Venezuela in 2Q12 was Miscellaneous Trojans, which affected 31.6 percent of all computers with detections there, up from 29.4 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Venezuela in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Autorun	Worms	17.1%
2	Win32/Dorkbot	Worms	16.3%
3	Win32/Keygen	Misc. Potentially Unwanted Software	12.0%
4	Win32/Conficker	Worms	9.0%
5	Win32/Sality	Viruses	8.4%
6	Win32/Rimecud	Worms	7.2%
7	Win32/Vobfus	Worms	7.0%
8	Win32/Nuqel	Worms	6.8%
9	Win32/Lamin	Worms	5.3%
10	Win32/VBInject	Misc. Potentially Unwanted Software	4.8%

- The most common threat family in Venezuela in 2Q12 was [Win32/Autorun](#), which affected 17.1 percent of computers with detections in Venezuela. [Win32/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 threat family in Venezuela in 2Q12 was [Win32/Dorkbot](#), which affected 16.3 percent of computers with detections in Venezuela. [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 in Venezuela in 2Q12 was [Win32/Keygen](#), which affected 12.0 percent of computers with detections in Venezuela. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The fourth most common threat family in Venezuela in 2Q12 was [Win32/Conficker](#), which affected 9.0 percent of computers with detections in Venezuela. [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.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Venezuela

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	0.50 (1.6)	0.68 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	1.10 (3.9)	1.19 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.37 (0.7)	0.67 (0.9)

Update service usage

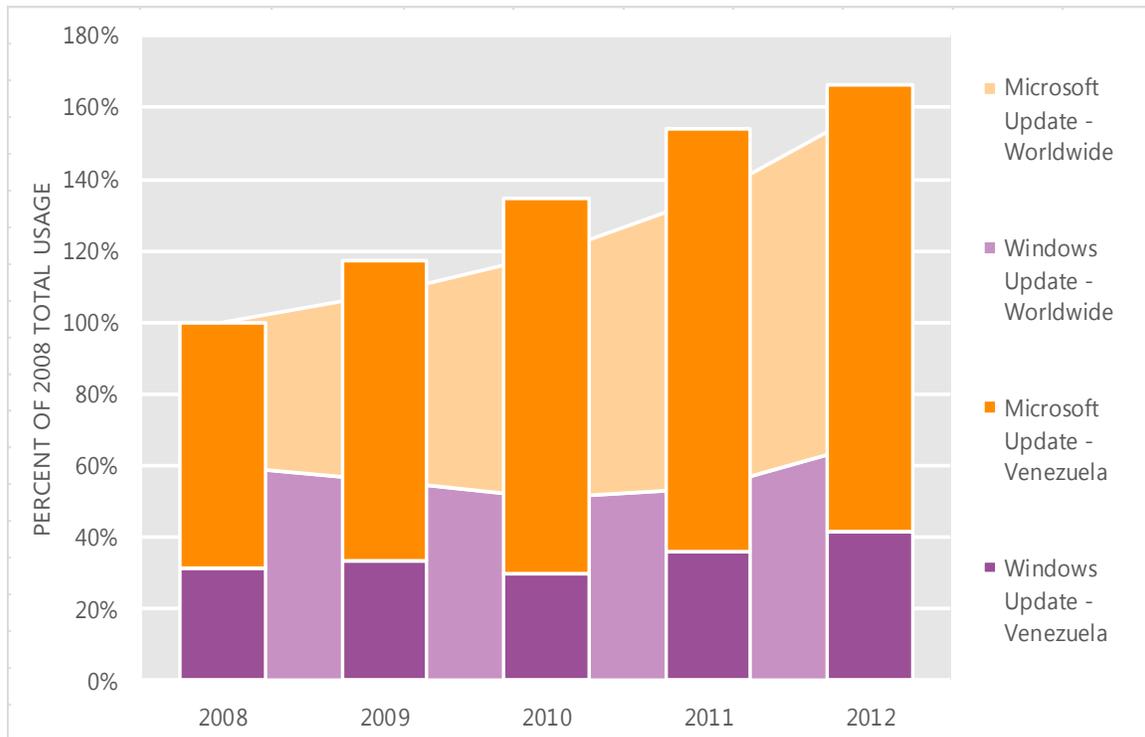
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Venezuela and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Venezuela over the last four years, indexed to the total usage for both services in Venezuela in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Venezuela was up 7.9 percent from 2011, and up 66.2 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Venezuela in 2012, 75.0 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.

Vietnam

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

The statistics presented here are generated by Microsoft security programs and services running on computers in Vietnam in 2Q12 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.

Infection rate statistics for Vietnam

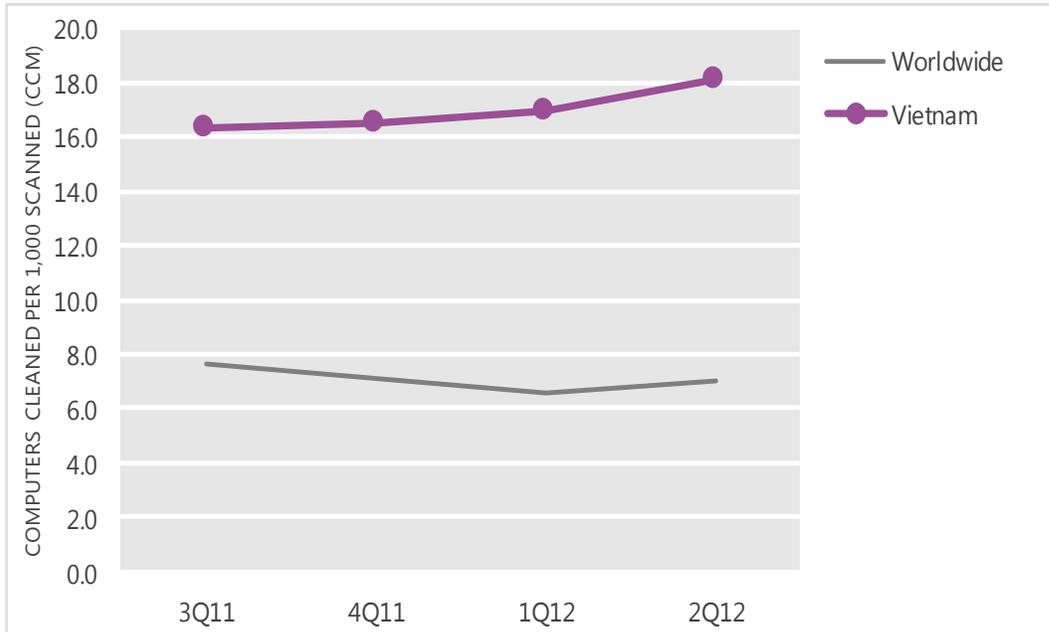
Metric	3Q11	4Q11	1Q12	2Q12
Computers cleaned per 1,000 MSRT executions (CCM)	16.3	16.5	17.0	18.1
Worldwide average CCM	7.7	7.1	6.6	7.0

See the *Security Intelligence Report* website 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.

Infection trends (CCM)

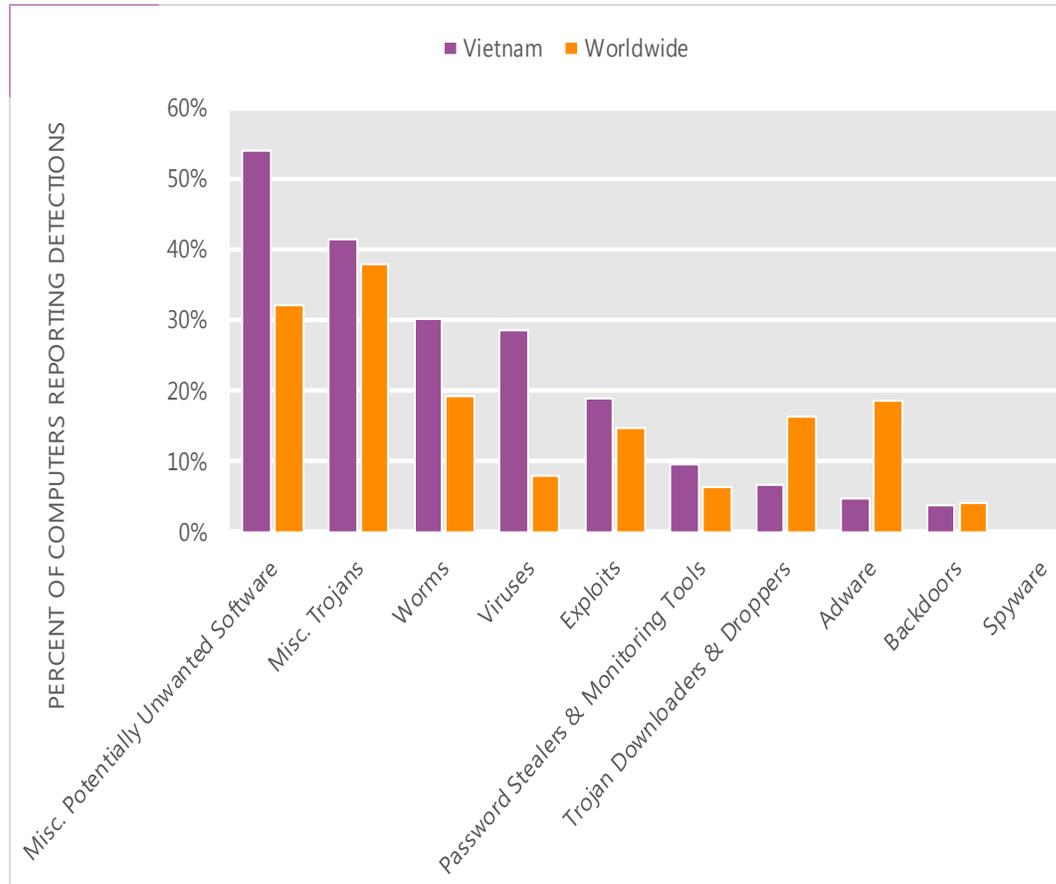
The MSRT detected malware on 18.1 of every 1,000 computers scanned in Vietnam in 2Q12 (a CCM score of 18.1, compared to the 2Q12 worldwide average CCM of 7.0). The following figure shows the CCM trend for Vietnam over the last four quarters, compared to the world as a whole.

CCM infection trends in Vietnam and worldwide



Threat categories

Malware and potentially unwanted software categories in Vietnam in 2Q12, by percentage of computers reporting detections



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Vietnam in 2Q12 was Miscellaneous Potentially Unwanted Software. It affected 54.0 percent of all computers with detections there, down from 58.8 percent in 1Q12.
- The second most common category in Vietnam in 2Q12 was Miscellaneous Trojans. It affected 41.3 percent of all computers with detections there, up from 40.3 percent in 1Q12.
- The third most common category in Vietnam in 2Q12 was Worms, which affected 30.1 percent of all computers with detections there, up from 28.2 percent in 1Q12.

Threat families

The top 10 malware and potentially unwanted software families in Vietnam in 2Q12

	Family	Most significant category	% of computers with detections
1	Win32/Keygen	Misc. Potentially Unwanted Software	26.9%
2	Win32/Ramnit	Misc. Trojans	21.8%
3	Win32/PossibleHostsFileHijack	Misc. Potentially Unwanted Software	17.6%
4	Win32/CplLnk	Exploits	16.1%
5	Win32/Autorun	Worms	15.7%
6	Win32/Sality	Viruses	15.2%
7	Win32/Patch	Misc. Potentially Unwanted Software	10.7%
8	Win32/Conficker	Worms	9.7%
9	Win32/VB	Worms	7.5%
10	Win32/Dynamer	Misc. Trojans	5.4%

- The most common threat family in Vietnam in 2Q12 was [Win32/Keygen](#), which affected 26.9 percent of computers with detections in Vietnam. [Win32/Keygen](#) is a generic detection for tools that generate product keys for various software products.
- The second most common threat family in Vietnam in 2Q12 was [Win32/Ramnit](#), which affected 21.8 percent of computers with detections in Vietnam. [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 in Vietnam in 2Q12 was [Win32/PossibleHostsFileHijack](#), which affected 17.6 percent of computers with detections in Vietnam. [Win32/PossibleHostsFileHijack](#) is an indicator that the computer's HOSTS file may have been modified by malicious or potentially unwanted software, which can cause access to certain Internet domains and websites to be redirected or denied.
- The fourth most common threat family in Vietnam in 2Q12 was [Win32/CplLnk](#), which affected 16.1 percent of computers with detections in Vietnam. [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.

Malicious websites

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

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Vietnam

Metric	1Q12	2Q12
Phishing sites per 1,000 hosts (Worldwide)	2.54 (1.6)	1.86 (1.8)
Malware hosting sites per 1,000 hosts (Worldwide)	3.75 (3.9)	3.99 (4.4)
Drive-by download per 1,000 URLs (Worldwide)	0.70 (0.7)	1.90 (0.9)

Update service usage

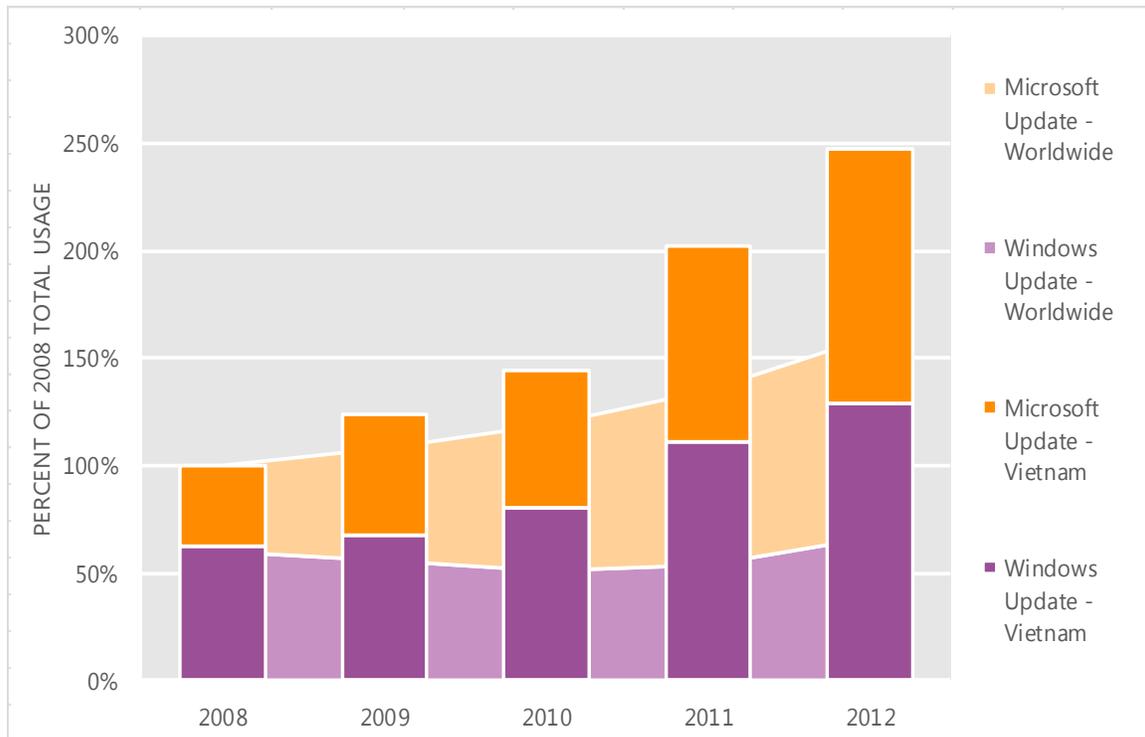
Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in other currently supported versions of Windows) connects to an update service for the list of available updates. After the update client determines which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For end users, Microsoft provides two update services that the update clients can use:

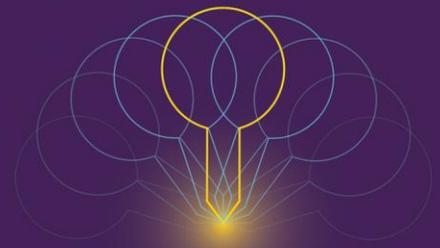
- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update Web site (update.microsoft.com/microsoftupdate). Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers.

Windows Update and Microsoft Update usage in Vietnam and worldwide



- This chart shows the growth in the number of computers connecting to Windows Update and Microsoft Update in Vietnam over the last four years, indexed to the total usage for both services in Vietnam in 2008.
- In 2012, the number of computers connecting to Windows Update and Microsoft Update in Vietnam was up 22.3 percent from 2011, and up 147.6 percent from 2008. By comparison, worldwide use of the two services increased 18.3 percent between 2011 and 2012, and 59.7 percent from 2008 to 2012.
- Of the computers using the two update services in Vietnam in 2012, 47.8 percent were configured to use Microsoft Update, compared to 58.5 percent worldwide.



TwC Next



One Microsoft Way
Redmond, WA 98052-6399
microsoft.com/security