Microsoft Security Intelligence Report

Volume 18 | July through December, 2014

United States

Microsoft

United States

The statistics presented here are generated by Microsoft security programs and services running on computers in the United States in 4Q14 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

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

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

Infection rate statistics for the United States

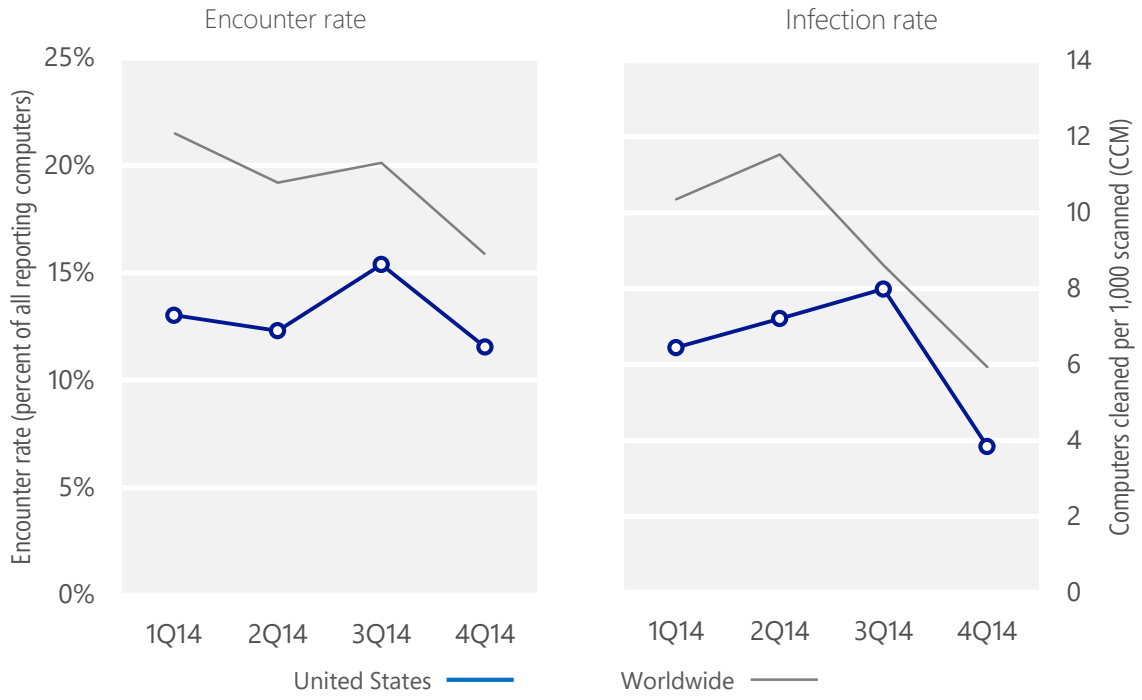
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, United States	13.0%	12.3%	15.4%	11.5%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, United States	6.4	7.2	8.0	3.8
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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

Encounter and infection rate trends

In 4Q14, 11.5% percent of computers in the United States encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 3.8 of every 1,000 unique computers scanned in the United States in 4Q14 (a CCM score of 3.8, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for the United States over the last four quarters, compared to the world as a whole.

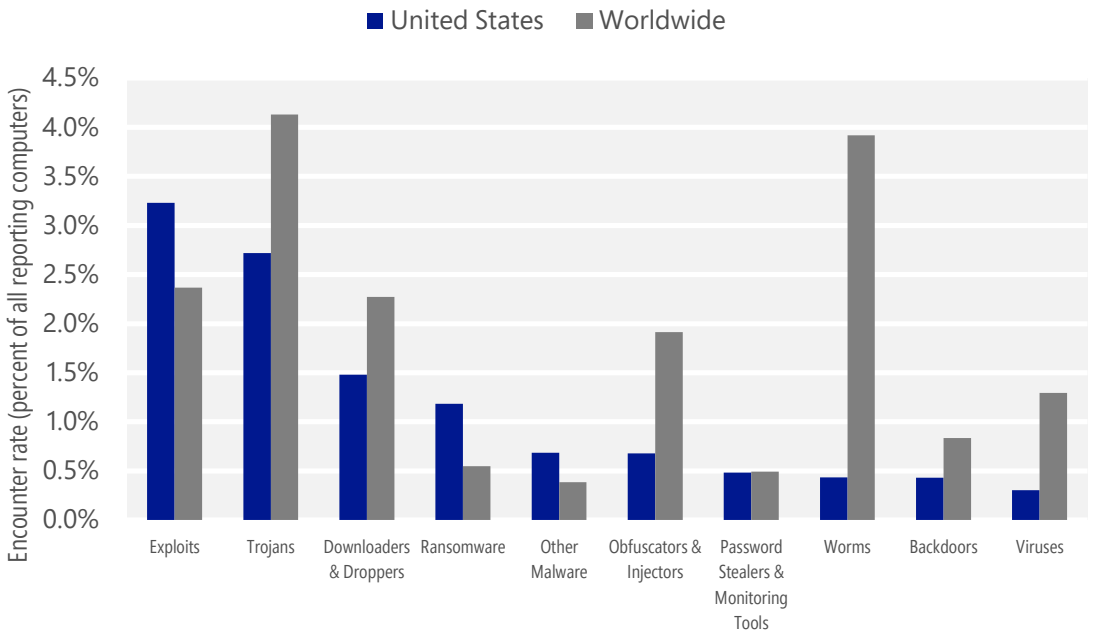
Malware encounter and infection rate trends in the United States and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 18* at www.microsoft.com/sir for more information about threats in the United States and around the world, and for explanations of the methods and terms used here.

Malware categories

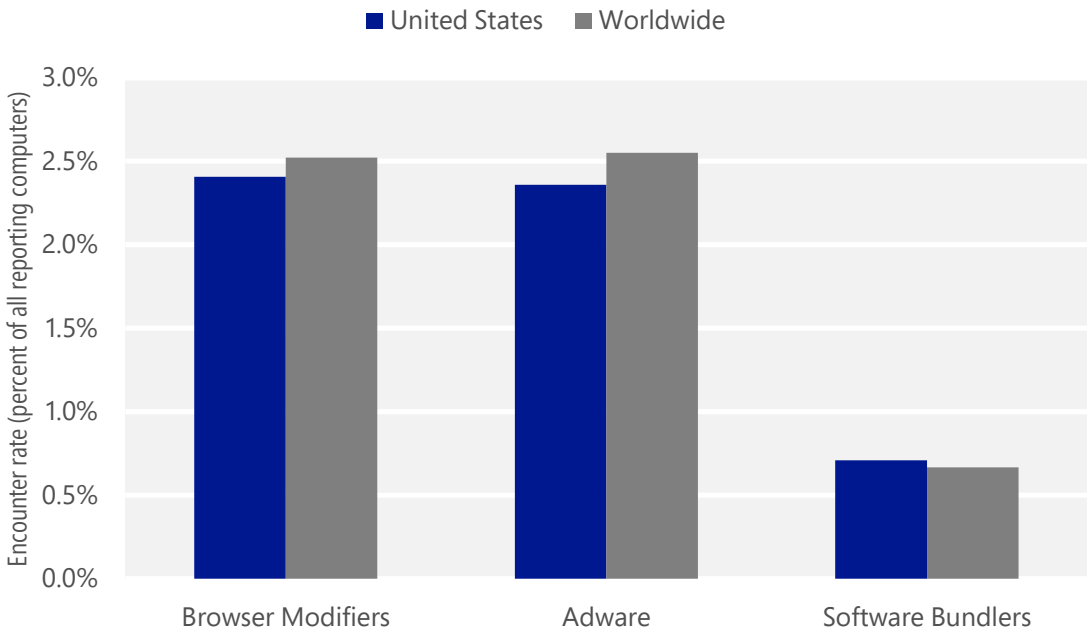
Malware encountered in the United States in 4Q14, by category



- The most common malware category in the United States in 4Q14 was Exploits. It was encountered by 3.2 percent of all computers there, down from 4.0 percent in 3Q14.
- The second most common malware category in the United States in 4Q14 was Trojans. It was encountered by 2.7 percent of all computers there, down from 3.7 percent in 3Q14.
- The third most common malware category in the United States in 4Q14 was Downloaders & Droppers, which was encountered by 1.5 percent of all computers there, down from 3.1 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in the United States in 4Q14, by category



- The most common unwanted software category in the United States in 4Q14 was Browser Modifiers. It was encountered by 2.4 percent of all computers there, down from 5.3 percent in 3Q14.
- The second most common unwanted software category in the United States in 4Q14 was Adware. It was encountered by 2.4 percent of all computers there, down from 2.9 percent in 3Q14.
- The third most common unwanted software category in the United States in 4Q14 was Software Bundlers, which was encountered by 0.7 percent of all computers there, up from 0.4 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in the United States in 4Q14

	Family	Most significant category	% of reporting computers
1	JS/Axpergle	Exploits	1.3%
2	Win32/Anogre	Exploits	1.0%
3	JS/Krypterade	Ransomware	0.8%
4	JS/Fiexp	Exploits	0.6%
5	Win32/Clikug	Trojans	0.6%
6	Win32/Obfuscator	Obfuscators & Injectors	0.5%
7	Win32/Chroject	Trojans	0.4%
8	Win32/Tugspay	Downloaders & Droppers	0.3%
9	Win32/Zbot	Password Stealers & Monitoring Tools	0.3%
10	Win32/Crowti	Ransomware	0.3%

- The most common malware family encountered in the United States in 4Q14 was JS/Axpergle, which was encountered by 1.3 percent of reporting computers there. JS/Axpergle is a detection for the Angler exploit kit, which exploits vulnerabilities in recent versions of Internet Explorer, Silverlight, Adobe Flash Player, and Java to install malware.
- The second most common malware family encountered in the United States in 4Q14 was Win32/Anogre, which was encountered by 1.0 percent of reporting computers there. Win32/Anogre is a threat that exploits a vulnerability addressed by Microsoft Security Bulletin MS11-087. This vulnerability can allow a hacker to install programs, view, change, or delete data or create new accounts with full administrative privileges.
- The third most common malware family encountered in the United States in 4Q14 was JS/Krypterade, which was encountered by 0.8 percent of reporting computers there. JS/Krypterade is ransomware that fraudulently claims the computer has been used for unlawful activity, locks it, and demands that the user pay to unlock it.
- The fourth most common malware family encountered in the United States in 4Q14 was JS/Fiexp, which was encountered by 0.6 percent of reporting computers there. JS/Fiexp is a detection for the Fiesta exploit kit, which attempts to exploit Java, Adobe Flash Player, Adobe Reader, Silverlight, and Internet Explorer to install malware.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in the United States in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Defaulttab	Browser Modifiers	1.2%
2	Win32/Couponruc	Browser Modifiers	1.1%
3	Win32/Invisiblebrowser	Adware	0.5%
4	Win32/Costmin	Adware	0.5%
5	Win32/Pennybee	Adware	0.4%

- The most common unwanted software family encountered in the United States in 4Q14 was Win32/Defaulttab, which was encountered by 1.2 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.
- The second most common unwanted software family encountered in the United States in 4Q14 was Win32/Couponruc, which was encountered by 1.1 percent of reporting computers there. Win32/Couponruc is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The third most common unwanted software family encountered in the United States in 4Q14 was Win32/Invisiblebrowser, which was encountered by 0.5 percent of reporting computers there. Win32/Invisiblebrowser is a program that shows ads as the user browses the web. It can be bundled with some third-party software installation programs.

Top threat families by infection rate

The most common malware families by infection rate in the United States in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Alureon	Trojans	1.2
2	Win32/Tracur	Trojans	0.5
3	Win32/Zbot	Password Stealers & Monitoring Tools	0.4
4	JS/Medfos	Trojans	0.3
5	JS/Miuref	Trojans	0.2
6	Win32/Sirefef	Trojans	0.2
7	Win32/Wysotot	Trojans	0.2
8	Win32/Kuluoz	Downloaders & Droppers	0.1
9	Win32/Sefnit	Trojans	0.1
10	Win32/FakeRean	Other Malware	0.1

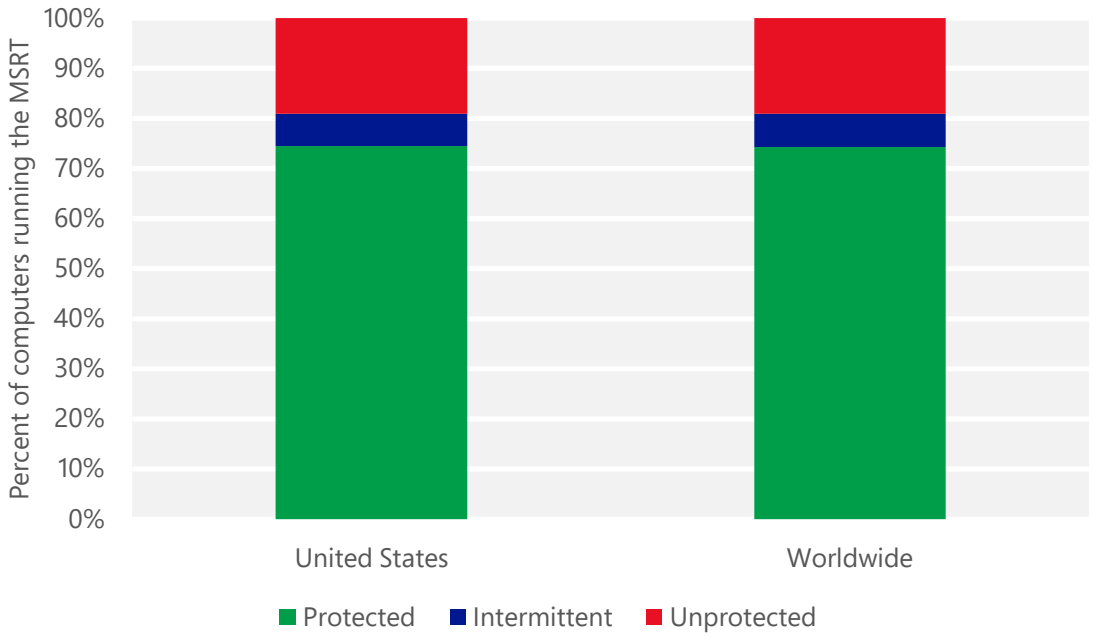
- The most common threat family infecting computers in the United States in 4Q14 was Win32/Alureon, which was detected and removed from 1.2 of every 1,000 unique computers scanned by the MSRT. Win32/Alureon is a data-stealing trojan that gathers confidential information such as user names, passwords, and credit card data from incoming and outgoing Internet traffic. It may also download malicious data and modify DNS settings.
- The second most common threat family infecting computers in the United States in 4Q14 was Win32/Tracur, which was detected and removed from 0.5 of every 1,000 unique computers scanned by the MSRT. Win32/Tracur is a trojan that downloads and executes arbitrary files, redirects web search queries to a malicious URL, and may also install other malware.
- The third most common threat family infecting computers in the United States in 4Q14 was Win32/Zbot, which was detected and removed from 0.4 of every 1,000 unique computers scanned by the MSRT. Win32/Zbot is a family of password stealing trojans that also contains backdoor functionality allowing unauthorized access and control of an affected computer.
- The fourth most common threat family infecting computers in the United States in 4Q14 was JS/Medfos, which was detected and removed from 0.3 of every 1,000 unique computers scanned by the MSRT. JS/Medfos is ?A trojan that installs malicious Internet browser extensions and redirects search results from popular search engines.

Security software use

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

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

Percent of computers in the United States and worldwide protected by real-time security software in 4Q14



Drive-by download sites

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

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

At the end of 3Q14, Bing detected 0.25 drive-by download URLs for every 1,000 URLs hosted in the United States, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.33 drive-by download URLs for every 1,000 URLs hosted in the United States, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in the United States and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, United States	0.25	0.33
Drive-by download pages per 1,000 URLs worldwide	*0.41*	*0.45*

One Microsoft Way
Redmond, WA 98052-6399
microsoft.com/security