Microsoft Security Intelligence Report

Volume 18 | July through December, 2014

China

Microsoft

China

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

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

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

Infection rate statistics for China

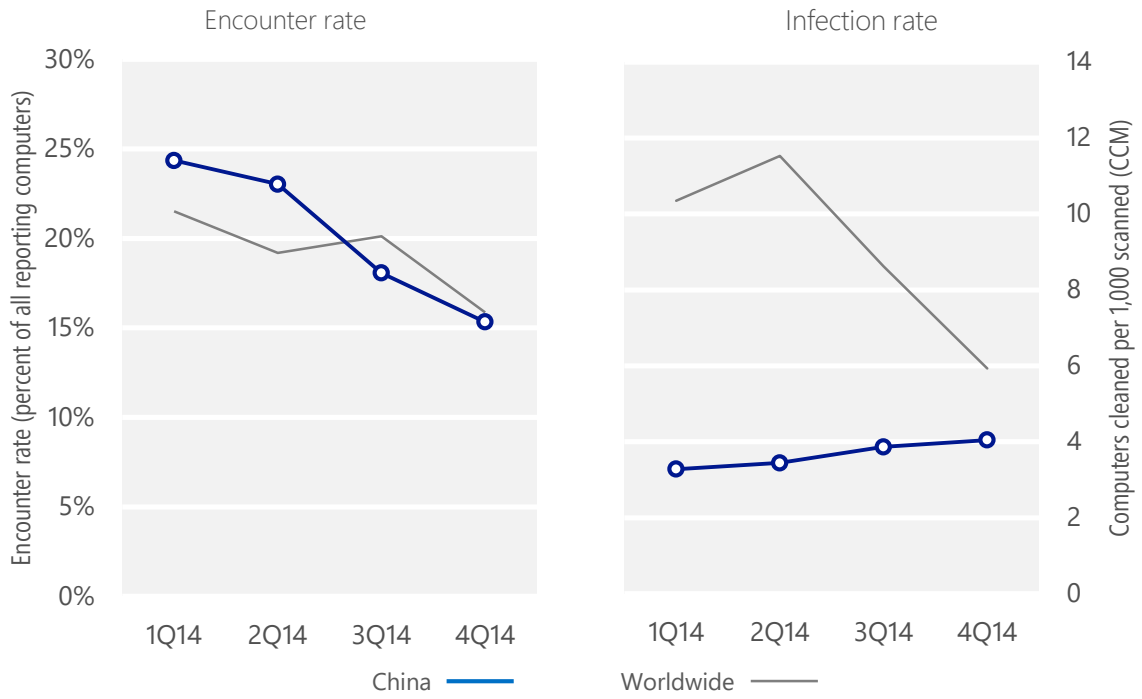
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, China	24.4%	23.0%	18.1%	15.3%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, China	3.3	3.4	3.9	4.0
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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

Encounter and infection rate trends

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

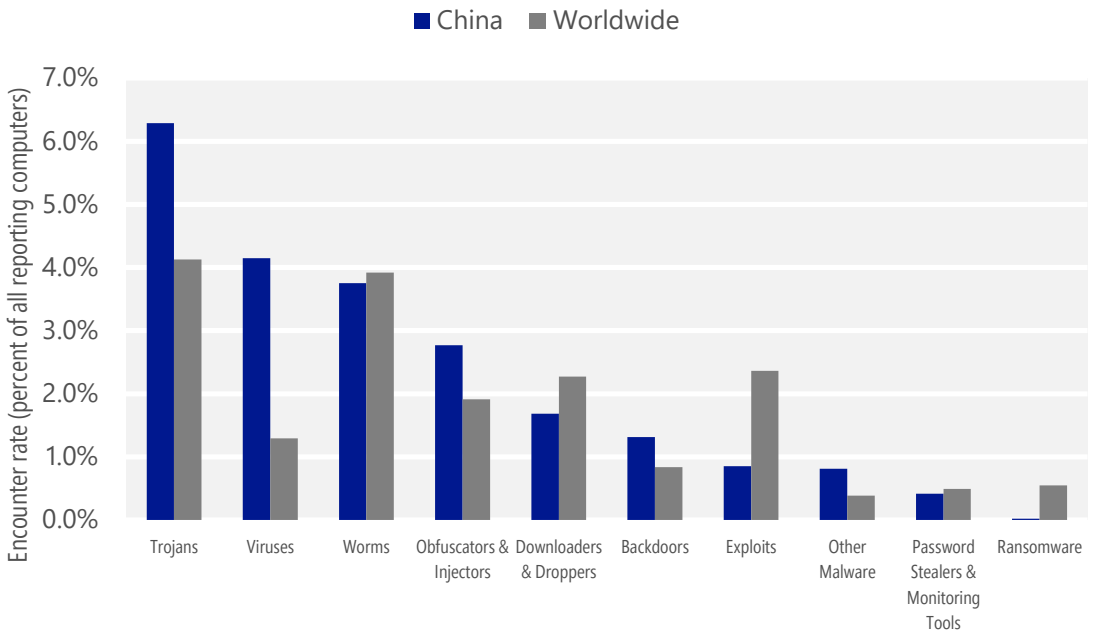
Malware encounter and infection rate trends in China and worldwide



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

Malware categories

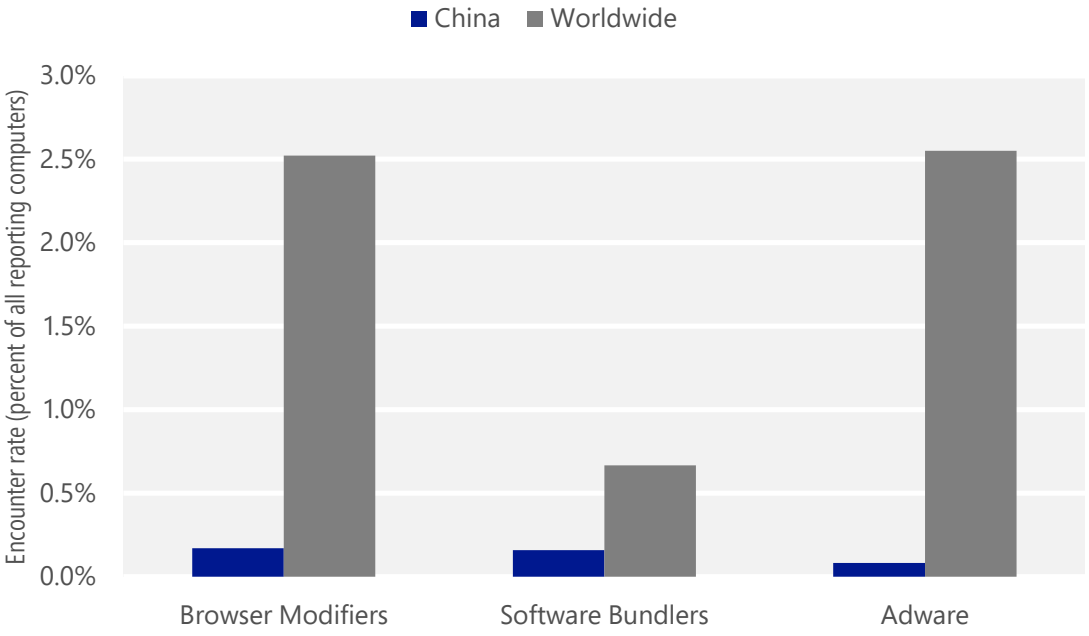
Malware encountered in China in 4Q14, by category



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

Unwanted software categories

Unwanted software encountered in China in 4Q14, by category



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

Top malware families by encounter rate

The most common malware families encountered in China in 4Q14

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

- The most common malware family encountered in China in 4Q14 was Win32/Obfuscator, which was encountered by 2.2 percent of reporting computers there. Win32/Obfuscator is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The second most common malware family encountered in China in 4Q14 was INF/Autorun, which was encountered by 1.1 percent of reporting computers there. INF/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The third most common malware family encountered in China in 4Q14 was Win32/Dynamer, which was encountered by 0.9 percent of reporting computers there. Win32/Dynamer is a generic detection for a variety of threats.
- The fourth most common malware family encountered in China in 4Q14 was DOS/JackTheRipper, which was encountered by 0.9 percent of reporting computers there. DOS/JackTheRipper is a virus that can stop some files from working correctly in Windows XP and earlier operating systems. It spreads by infecting the master boot record (MBR) on connected hard disks and floppy disks.

Top unwanted software families by encounter rate

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

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

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

Top threat families by infection rate

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

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

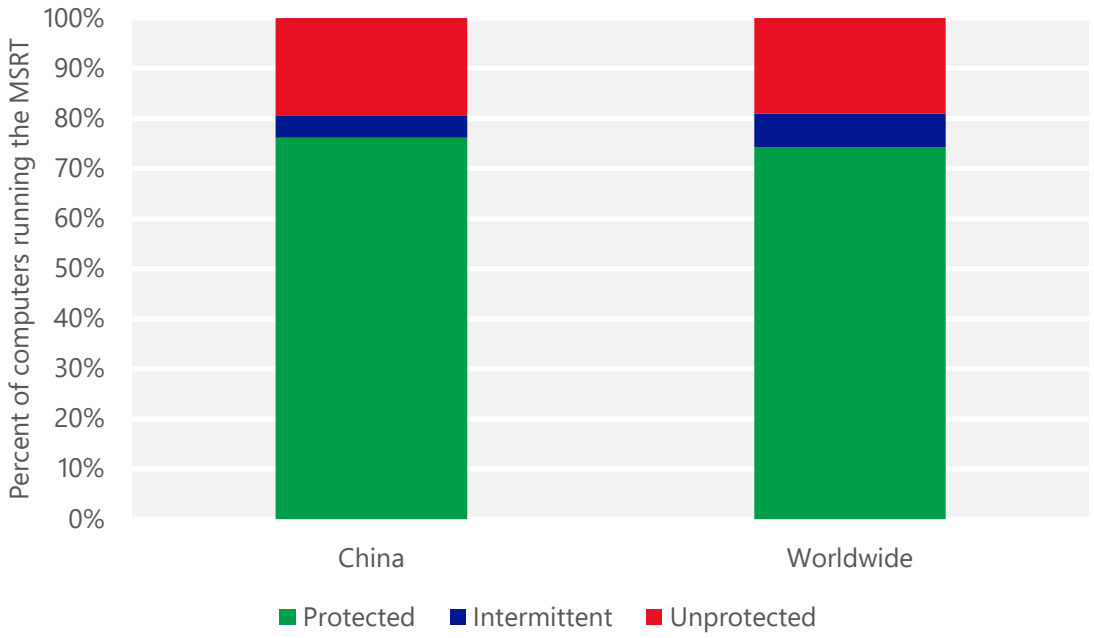
- The most common threat family infecting computers in China in 4Q14 was Win32/Nitol, which was detected and removed from 1.3 of every 1,000 unique computers scanned by the MSRT. Win32/Nitol is a family of trojans that perform DDoS (distributed denial of service) attacks, allow backdoor access and control, download and run files, and perform a number of other malicious activities on the computer.
- The second most common threat family infecting computers in China in 4Q14 was Win32/Frethog, which was detected and removed from 0.8 of every 1,000 unique computers scanned by the MSRT. Win32/Frethog is a large family of password-stealing trojans that targets confidential data, such as account information, from massively multiplayer online games.
- The third most common threat family infecting computers in China in 4Q14 was Win32/Ramnit, which was detected and removed from 0.7 of every 1,000 unique computers scanned by the MSRT. Win32/Ramnit is a family of multi-component malware that infects executable files, Microsoft Office files, and HTML files. Win32/Ramnit spreads to removable drives and steals sensitive information such as saved FTP credentials and browser cookies. It may also open a backdoor to await instructions from a remote attacker.
- The fourth most common threat family infecting computers in China in 4Q14 was Win32/Sality, which was detected and removed from 0.3 of every 1,000 unique computers scanned by the MSRT. Win32/Sality is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.

Security software use

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

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

Percent of computers in China and worldwide protected by real-time security software in 4Q14



Drive-by download sites

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

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

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

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

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

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