Microsoft

Microsoft Security Intelligence Report

Volume 22 | January through March, 2017

China

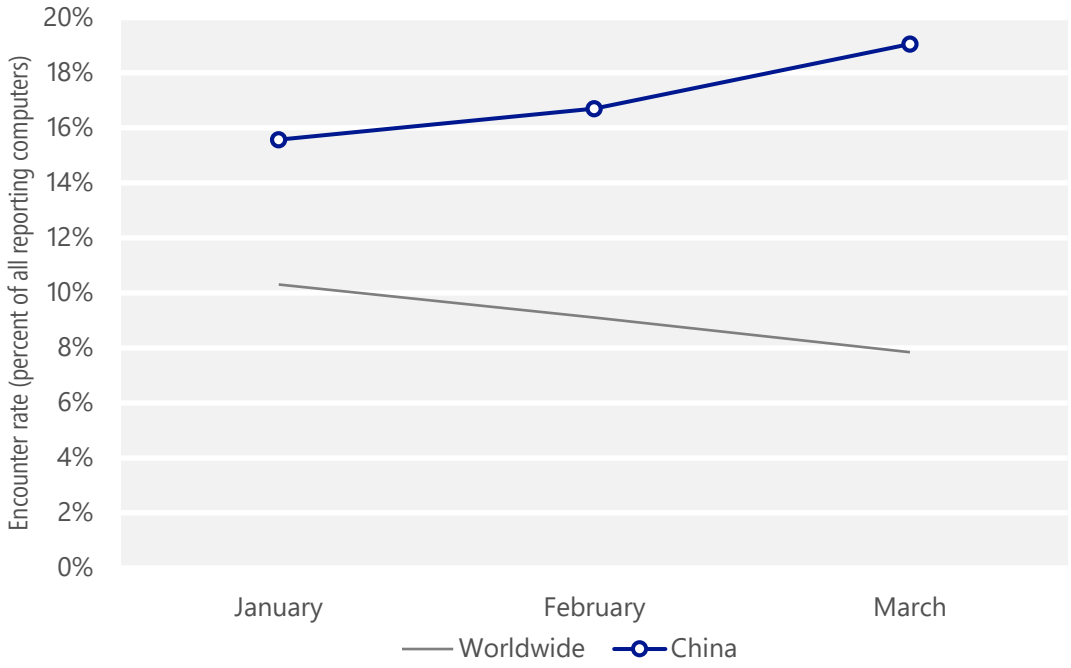
China

The statistics presented here are generated by Microsoft security programs and services running on computers in China in March 2017 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

Encounter rate trends

In March 2017, 19.0 percent of computers in China encountered malware, compared to the March 2017 worldwide encounter rate of 7.8 percent. The following figure shows the encounter and infection rate trends for China over the last three months, compared to the world as a whole.

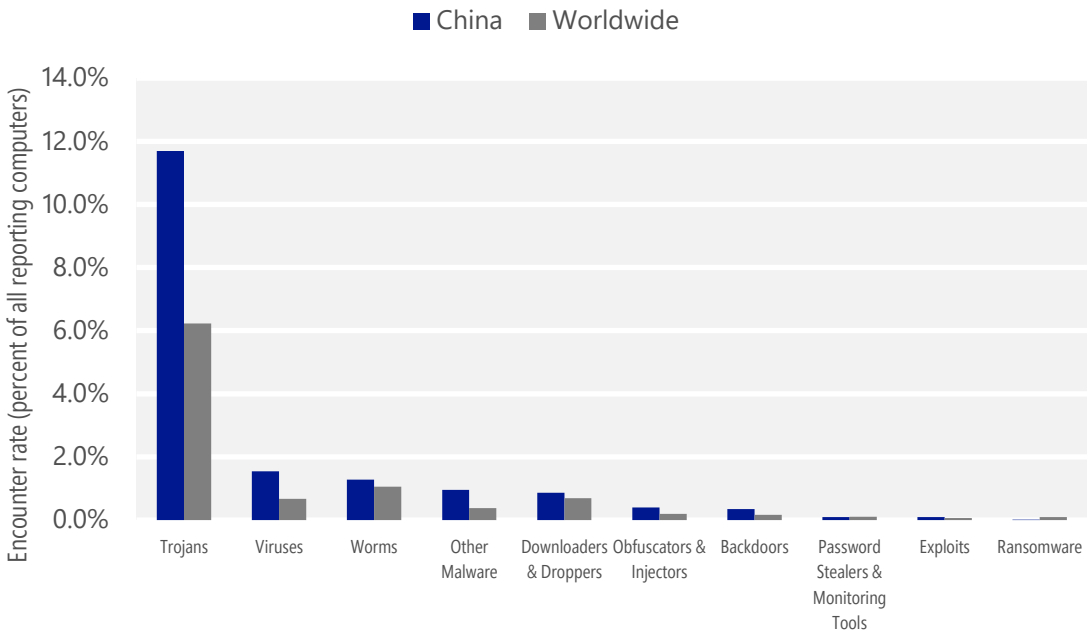
Malware encounter rate trends in China and worldwide



See the full report at http://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.

Malicious software categories

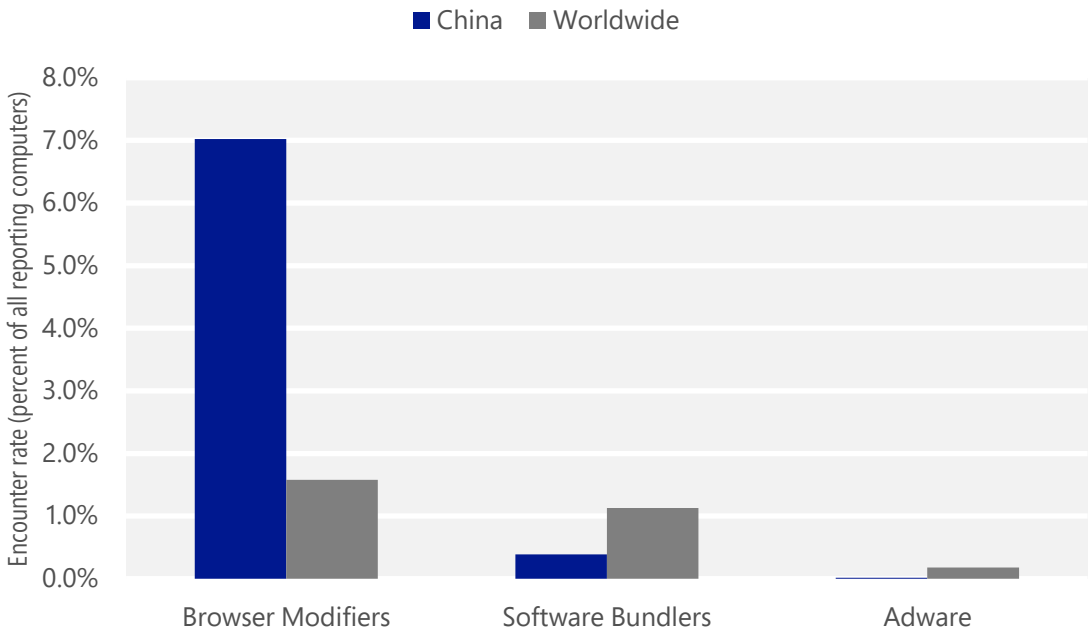
Malicious software encountered in China in March 2017, by category



- The most common malicious software category in China in March 2017 was Trojans. It was encountered by 11.69 percent of all computers there, up from 10.63 percent in February 2017.
- The second most common malicious software category in China in March 2017 was Viruses. It was encountered by 1.54 percent of all computers there, up from 1.42 percent in February 2017.
- The third most common malicious software category in China in March 2017 was Worms, which was encountered by 1.28 percent of all computers there, up from 1.09 percent in February 2017.

Unwanted software categories

Unwanted software encountered in China in March 2017, by category



- The most common unwanted software category in China in March 2017 was Browser Modifiers. It was encountered by 7.02 percent of all computers there, down from 8.69 percent in February 2017.
- The second most common unwanted software category in China in March 2017 was Software Bundlers. It was encountered by 0.39 percent of all computers there, down from 0.40 percent in February 2017.
- The third most common unwanted software category in China in March 2017 was Adware, which was encountered by 0.01 percent of all computers there, unchanged from 0.01 percent in February 2017.

Top malicious software families by encounter rate

The most common malicious software families encountered in China in March 2017

	Family	Most significant category	% of reporting computers
1	Win32/Spursint	Trojans	2.84%
2	Win32/Vigorf	Trojans	1.36%
3	Win32/Fuery	Trojans	1.15%
4	Win32/Ramnit	Viruses	0.94%
5	Win32/Dynamer	Trojans	0.90%
6	Win32/Rundas	Trojans	0.65%
7	Win32/Vigram	Trojans	0.65%
8	Win32/Skeeyah	Trojans	0.64%
9	Win32/Swrort	Trojans	0.43%
10	JS/Redirector	Trojans	0.42%

- The most common malicious software family encountered in China in March 2017 was Win32/Spursint, which was encountered by 2.84 percent of reporting computers there. Win32/Spursint is a cloud-based detection for files that have been automatically identified as malicious by the cloud-based protection feature of Windows Defender.
- The second most common malicious software family encountered in China in March 2017 was Win32/Vigorf, which was encountered by 1.36 percent of reporting computers there. Win32/Vigorf is a generic detection for a variety of threats.
- The third most common malicious software family encountered in China in March 2017 was Win32/Fuery, which was encountered by 1.15 percent of reporting computers there. Win32/Fuery is a cloud-based detection for files that have been automatically identified as malicious by the cloud-based protection feature of Windows Defender.
- The fourth most common malicious software family encountered in China in March 2017 was Win32/Ramnit, which was encountered by 0.94 percent of reporting computers there. Win32/Ramnit is a family of multi-component malware that infects executable files, Microsoft Office files, and HTML files. Win32/Ramnit spreads to removable drives and steals sensitive information such as saved FTP credentials and browser cookies. It may also open a backdoor to await instructions from a remote attacker.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in China in March 2017

	Family	Most significant category	% of reporting computers
1	Win32/Xiazai	Browser Modifiers	3.91%
2	Win32/Qiwmonk	Browser Modifiers	2.21%
3	Win32/Riccietex	Browser Modifiers	0.99%
4	Win32/Ogimant	Software Bundlers	0.08%
5	Win32/Kipidow	Browser Modifiers	0.03%

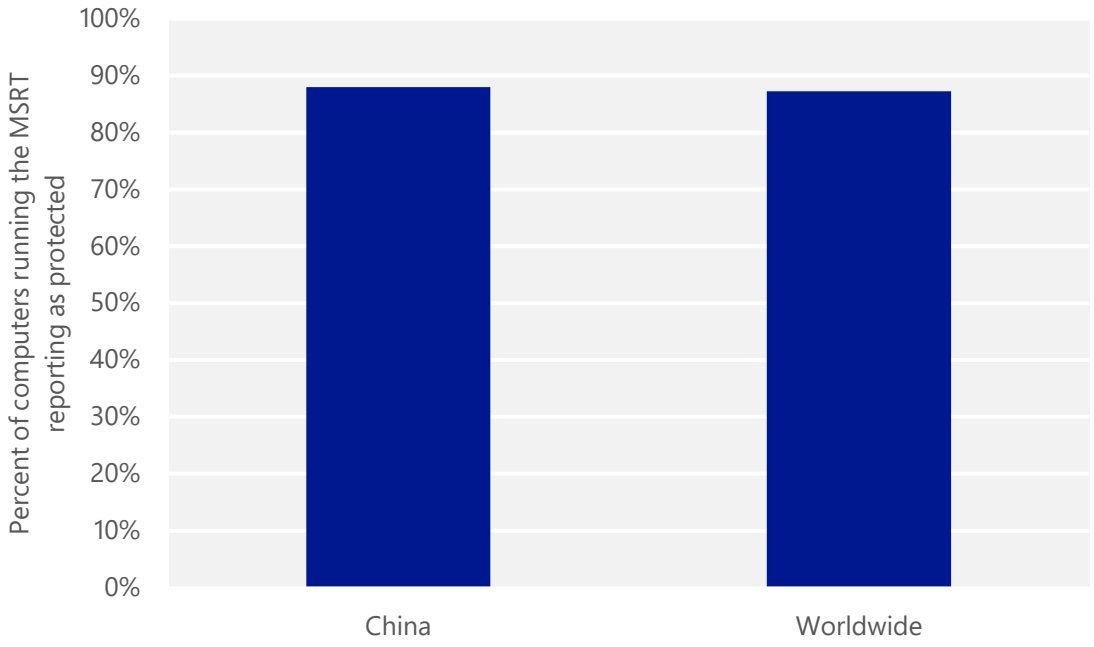
- The most common unwanted software family encountered in China in March 2017 was Win32/Xiazai, which was encountered by 3.91 percent of reporting computers there. Win32/Xiazai is a program that installs unwanted software on the computer at the same time as the software the user is trying to install, without adequate consent.
- The second most common unwanted software family encountered in China in March 2017 was Win32/Qiwmonk, which was encountered by 2.21 percent of reporting computers there. Win32/Qiwmonk is a browser modifier that can change web browser settings and prevent users from changing them back. It can be installed when other software is downloaded from third-party websites, usually claiming to be installers for free software or games that would otherwise have to be paid for.
- The third most common unwanted software family encountered in China in March 2017 was Win32/Riccietex, which was encountered by 0.99 percent of reporting computers there. Win32/Riccietex is a browser modifier that is distributed as an installer for various applications. When used, it alters shortcuts (.lnk files) that open popular browsers and configures them to open a specific website by default.

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.

The figure below shows the percentage of computers worldwide and in China that the MSRT found to be running up-to-date real-time security software in March 2017.

Percent of computers in China and worldwide protected by real-time security software in March 2017



Malicious websites

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

The information presented in this section has been generated from telemetry data produced by Windows Defender SmartScreen in Microsoft Edge and Internet Explorer. See the Malicious Websites section of *Microsoft Security Intelligence Report, Volume 22* for more information about these protections and how the data is collected.

Malicious website statistics for China

Metric	China	Worldwide
Drive-by download pages per 1,000 URLs	0.16	0.17
Phishing sites per 1,000 Internet hosts	0.6	6.3
Malware hosting sites per 1,000 Internet hosts	45.9	14.8

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