Microsoft

Microsoft Security Intelligence Report

Volume 16 | July through December, 2013

Korea

Korea

The statistics presented here are generated by Microsoft security programs and services running on computers in Korea in 4Q13 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

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

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

Infection rate statistics for Korea

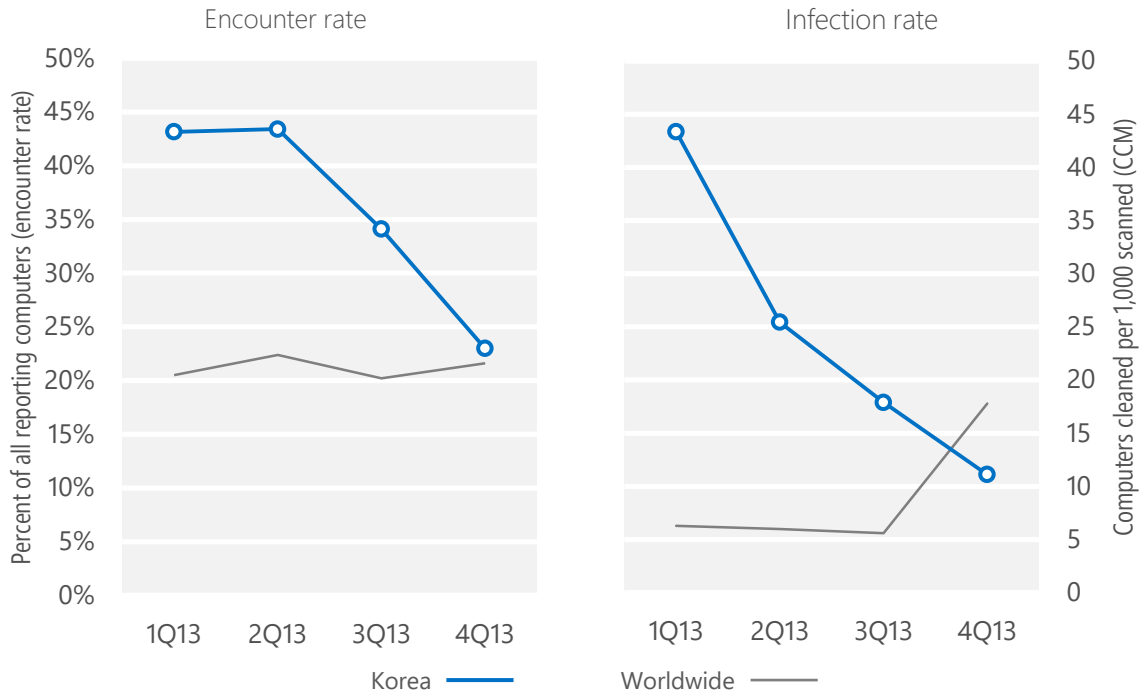
Metric	1Q13	2Q13	3Q13	4Q13
CCM, Korea	43.4	25.4	17.9	11.1
Worldwide CCM	*6.3*	*6.9*	*5.6*	*17.8*
Encounter rate, Korea	43.2%	43.4%	34.1%	23.0%
Worldwide encounter rate	*20.5%*	*22.4%*	*20.2%*	*21.6%*

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.

Encounter and infection rate trends

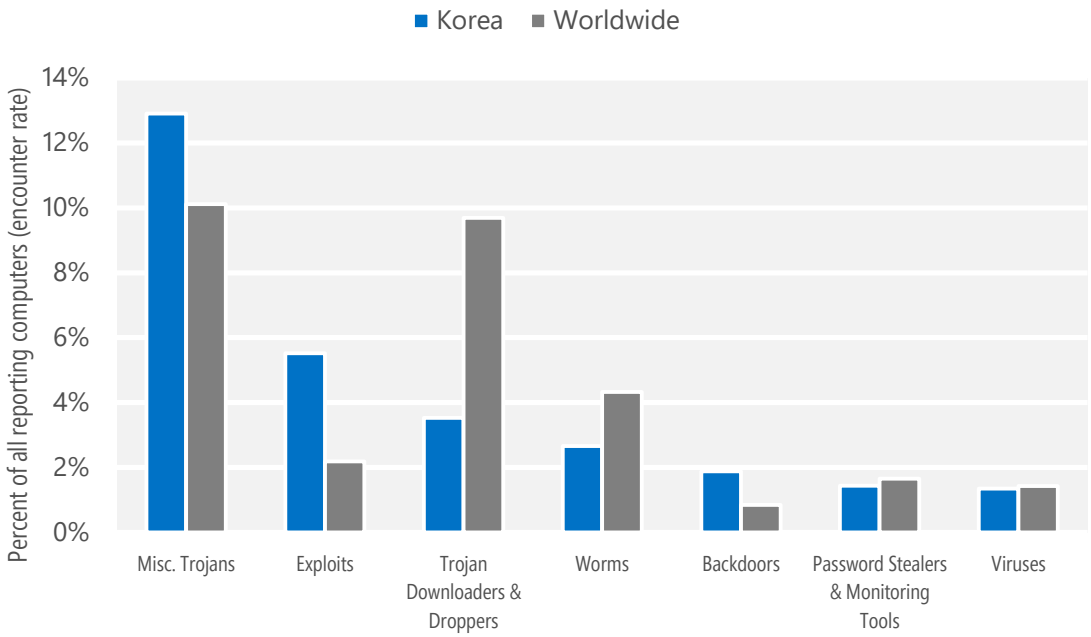
In 4Q13, 23.0% percent of computers in Korea encountered malware, compared to the 4Q13 worldwide encounter rate of 21.6% percent. In addition, the MSRT detected and removed malware from 11.1 of every 1,000 unique computers scanned in Korea in 4Q13 (a CCM score of 11.1, compared to the 4Q13 worldwide CCM of 17.8). The following figure shows the encounter and infection rate trends for Korea over the last four quarters, compared to the world as a whole.

Malware encounter and infection rate trends in Korea and worldwide



Threat categories

Malware encountered in Korea in 4Q13, by threat category



- The most common category in Korea in 4Q13 was Miscellaneous Trojans. It was encountered by 12.9 percent of all computers there, down from 18.2 percent in 3Q13.
- The second most common category in Korea in 4Q13 was Exploits. It was encountered by 5.5 percent of all computers there, down from 16.9 percent in 3Q13.
- The third most common category in Korea in 4Q13 was Trojan Downloaders & Droppers, which was encountered by 3.5 percent of all computers there, down from 5.5 percent in 3Q13.

Top threat families by encounter rate

The top 10 malware families encountered in Korea in 4Q13

	Family	Most significant category	% of reporting computers
1	JS/DonxRef	Exploits	3.1%
2	Win32/Obfuscator	Misc. Trojans	2.2%
3	JS/Redirector	Misc. Trojans	1.8%
4	Win32/Comisproc	Misc. Trojans	1.6%
5	Win32/Onescan	Misc. Trojans	1.4%
6	JS/ShellCode	Exploits	1.4%
7	Win32/Dynamer	Misc. Trojans	1.4%
8	Win32/Sisron	Misc. Trojans	1.3%
9	Win32/Sisproc	Misc. Trojans	1.2%
10	Win32/OnLineGames	Password Stealers & Monitoring Tools	0.9%

- The most common threat family encountered in Korea in 4Q13 was JS/DonxRef, which affected 3.1 percent of reporting computers in Korea. JS/DonxRef is a generic detection for malicious JavaScript objects that construct shellcode. The scripts may try to exploit vulnerabilities in Java, Adobe Flash Player, and Windows.
- The second most common threat family encountered in Korea in 4Q13 was Win32/Obfuscator, which affected 2.2 percent of reporting computers with detections in Korea. Win32/Obfuscator is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The third most common threat family encountered in Korea in 4Q13 was JS/Redirector, which affected 1.8 percent of reporting computers with detections in Korea. JS/Redirector is a detection for a class of JavaScript trojans that redirect users to unexpected websites, which may contain drive-by downloads.
- The fourth most common threat family encountered in Korea in 4Q13 was Win32/Comisproc, which affected 1.6 percent of reporting computers with detections in Korea. Win32/Comisproc is a generic detection for malicious files that drop files in certain folders, such as the Windows system folder, and may take other malicious actions.

Top threat families by infection rate

The top 10 malware families by infection rate in Korea in 4Q13

	Family	Most significant category	Infection rate (CCM)
1	Win32/Onescan	Misc. Trojans	5.1
2	Win32/Rotbrow	Trojan Downloaders & Droppers	2.8
3	Win32/Nitol	Misc. Trojans	1.4
4	Win32/Sefnit	Misc. Trojans	0.3
5	Win32/Virut	Viruses	0.3
6	Win32/Zbot	Password Stealers & Monitoring Tools	0.2
7	Win32/Dorkbot	Worms	0.2
8	Win32/Hupigon	Backdoors	0.2
9	Win32/Parite	Viruses	0.2
10	Win32/Pluzoks	Trojan Downloaders & Droppers	0.1

- The most common threat family infecting computers in Korea in 4Q13 was Win32/Onescan, which was detected and removed from 5.1 of every 1,000 unique computers scanned by the MSRT. Win32/Onescan is a Korean-language rogue security software family distributed under the names One Scan, Siren114, EnPrivacy, PC Trouble, Smart Vaccine, and many others.
- The second most common threat family infecting computers in Korea in 4Q13 was Win32/Rotbrow, which was detected and removed from 2.8 of every 1,000 unique computers scanned by the MSRT. Win32/Rotbrow is a trojan that installs browser add-ons that claim to offer protection from other add-ons. Rotbrow can change the browser's home page, and can install the trojan Win32/Sefnit. It is commonly installed by Win32/Brantall.
- The third most common threat family infecting computers in Korea in 4Q13 was Win32/Nitol, which was detected and removed from 1.4 of every 1,000 unique computers scanned by the MSRT. Win32/Nitol is a family of trojans that perform DDoS (distributed denial of service) attacks, allow backdoor access and control, download and run files, and perform a number of other malicious activities on the computer.
- The fourth most common threat family infecting computers in Korea in 4Q13 was Win32/Sefnit, which was detected and removed from 0.3 of every 1,000 unique computers scanned by the MSRT. Win32/Sefnit is a family of trojans that can allow backdoor access, download files, and use the computer and Internet connection for click fraud. Some variants can monitor web browsers and hijack search results.

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.

Malicious website statistics for Korea

Metric	1Q13	2Q13	3Q13	4Q13
Phishing sites per 1,000 hosts *(Worldwide)*	2.30 *(4.56)*	1.90 *(4.24)*	1.27 *(3.94)*	1.60 *(5.48)*
Malware hosting sites per 1,000 hosts *(Worldwide)*	15.26 *(11.66)*	22.08 *(17.67)*	24.24 *(18.00)*	14.04 *(18.41)*
Drive-by download sites per 1,000 URLs *(Worldwide)*	0.15 *(0.50)*	0.29 *(1.12)*	0.35 *(1.09)*	0.04 *(0.25)*

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