

Microsoft Security Intelligence Report

Volume 16 | July through December, 2013

Malaysia

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 © 2014 Microsoft Corporation. All rights reserved.

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

Malaysia

The statistics presented here are generated by Microsoft security programs and services running on computers in Malaysia 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 succeeds 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 Malaysia

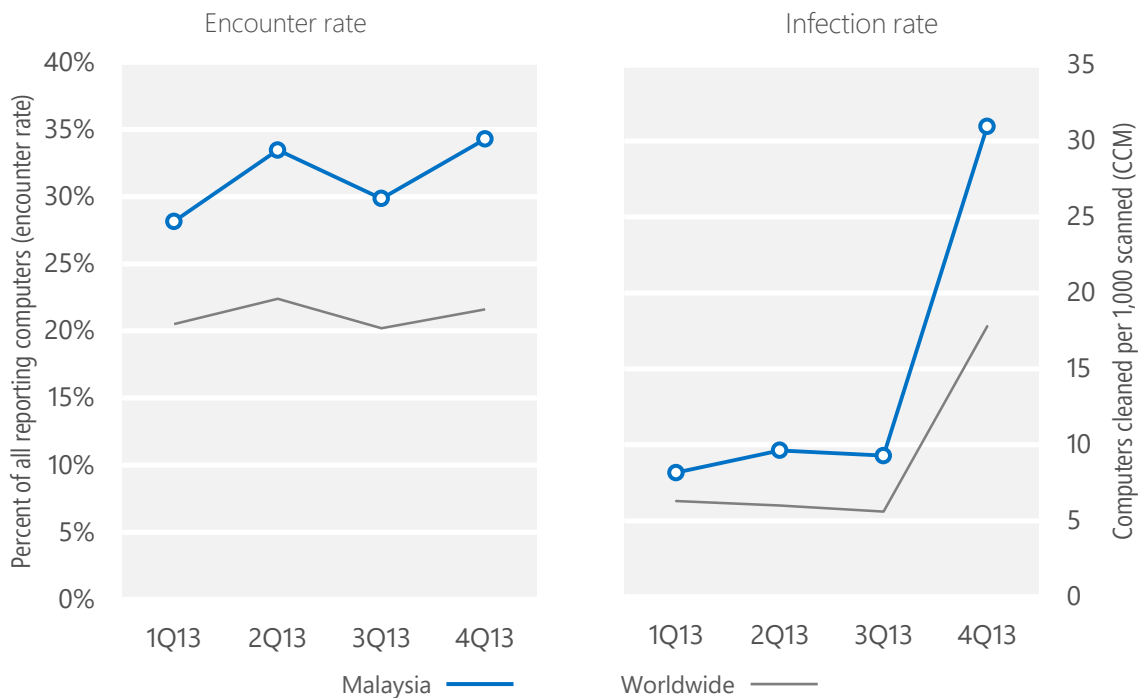
Metric	1Q13	2Q13	3Q13	4Q13
CCM, Malaysia	8.2	9.6	9.3	31.0
Worldwide CCM	6.3	6.9	5.6	17.8
Encounter rate, Malaysia	28.2%	33.5%	29.9%	34.3%
Worldwide encounter rate	20.5%	22.4%	20.2%	21.6%

See the *Security Intelligence Report* website at www.microsoft.com/sir for more information about threats in Malaysia and around the world, and for explanations of the methods and terms used here.

Encounter and infection rate trends

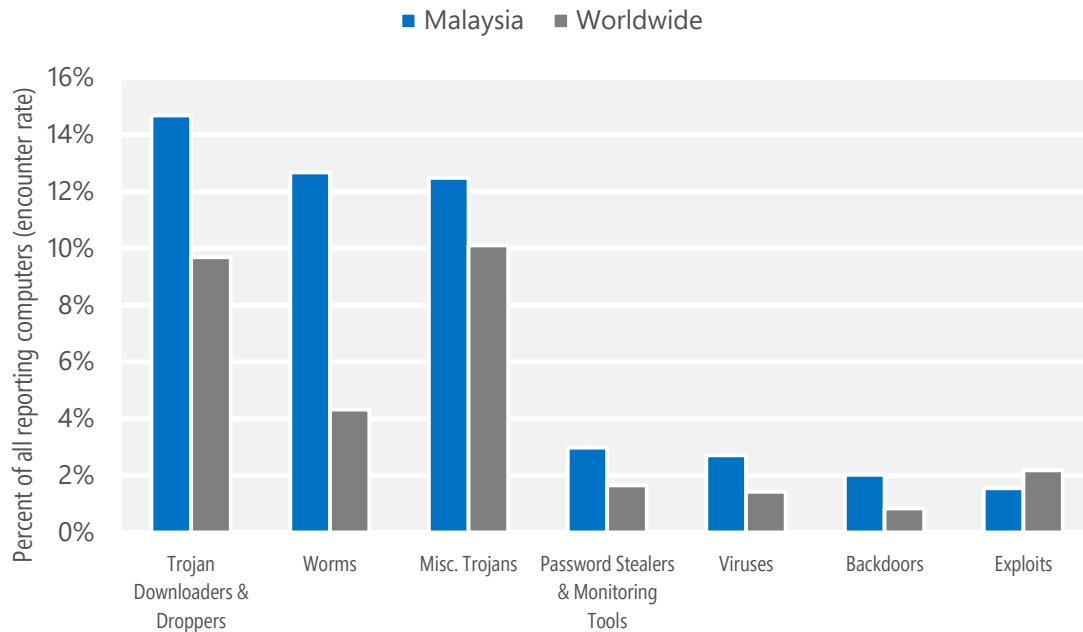
In 4Q13, 34.3% percent of computers in Malaysia encountered malware, compared to the 4Q13 worldwide encounter rate of 21.6% percent. In addition, the MSRT detected and removed malware from 31.0 of every 1,000 unique computers scanned in Malaysia in 4Q13 (a CCM score of 31.0, compared to the 4Q13 worldwide CCM of 17.8). The following figure shows the encounter and infection rate trends for Malaysia over the last four quarters, compared to the world as a whole.

Malware encounter and infection rate trends in Malaysia and worldwide



Threat categories

Malware encountered in Malaysia in 4Q13, by threat category



- The most common category in Malaysia in 4Q13 was Trojan Downloaders & Droppers. It was encountered by 14.7 percent of all computers there, down from 15.7 percent in 3Q13.
- The second most common category in Malaysia in 4Q13 was Worms. It was encountered by 12.7 percent of all computers there, down from 14.7 percent in 3Q13.
- The third most common category in Malaysia in 4Q13 was Miscellaneous Trojans, which was encountered by 12.5 percent of all computers there, up from 3.5 percent in 3Q13.

Top threat families by encounter rate

The top 10 malware families encountered in Malaysia in 4Q13

	Family	Most significant category	% of reporting computers
1	Win32/Rotbrow	Trojan Downloaders & Droppers	9.8%
2	Win32/Brantall	Trojan Downloaders & Droppers	6.1%
3	Win32/Gamarue	Worms	4.3%
4	VBS/Jenxcus	Worms	3.8%
5	Win32/Obfuscator	Misc. Trojans	3.5%
6	INF/Autorun	Worms	3.3%
7	Win32/Dorkbot	Worms	2.8%
8	JS/Faceliker	Misc. Trojans	2.0%
9	Win32/Sality	Viruses	1.6%
10	Win32/Detplock	Misc. Trojans	1.2%

- The most common threat family encountered in Malaysia in 4Q13 was [Win32/Rotbrow](#), which affected 9.8 percent of reporting computers in Malaysia. [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 second most common threat family encountered in Malaysia in 4Q13 was [Win32/Brantall](#), which affected 6.1 percent of reporting computers with detections in Malaysia. [Win32/Brantall](#) is a family of trojans that download and install other programs, including Win32/Sefnit and Win32/Rotbrow. Brantall often pretends to be an installer for other, legitimate programs.
- The third most common threat family encountered in Malaysia in 4Q13 was [Win32/Gamarue](#), which affected 4.3 percent of reporting computers with detections in Malaysia. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The fourth most common threat family encountered in Malaysia in 4Q13 was [VBS/Jenxcus](#), which affected 3.8 percent of reporting computers with detections in Malaysia. [VBS/Jenxcus](#) is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.

Top threat families by infection rate

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

	Family	Most significant category	Infection rate (CCM)
1	Win32/Rotbrow	Trojan Downloaders & Droppers	22.2
2	Win32/Sefnit	Misc. Trojans	4.0
3	Win32/Gamarue	Worms	2.1
4	Win32/Sality	Viruses	1.6
5	Win32/Dorkbot	Worms	0.9
6	Win32/Ramnit	Misc. Trojans	0.6
7	Win32/Lethic	Misc. Trojans	0.4
8	Win32/Pramro	Misc. Trojans	0.3
9	Win32/Nugel	Worms	0.2
10	Win32/Sirefef	Misc. Trojans	0.2

- The most common threat family infecting computers in Malaysia in 4Q13 was [Win32/Rotbrow](#), which was detected and removed from 22.2 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 second most common threat family infecting computers in Malaysia in 4Q13 was [Win32/Sefnit](#), which was detected and removed from 4.0 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.
- The third most common threat family infecting computers in Malaysia in 4Q13 was [Win32/Gamarue](#), which was detected and removed from 2.1 of every 1,000 unique computers scanned by the MSRT. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The fourth most common threat family infecting computers in Malaysia in 4Q13 was [Win32/Sality](#), which was detected and removed from 1.6 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.

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 Malaysia

Metric	1Q13	2Q13	3Q13	4Q13
Phishing sites per 1,000 hosts (Worldwide)	10.76 (4.56)	8.52 (4.24)	7.81 (3.94)	11.89 (5.48)
Malware hosting sites per 1,000 hosts (Worldwide)	10.22 (11.66)	16.51 (17.67)	17.68 (18.00)	16.68 (18.41)
Drive-by download sites per 1,000 URLs (Worldwide)	0.58 (0.50)	3.40 (1.12)	2.34 (1.09)	0.26 (0.25)



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