Microsoft

An in-depth perspective on software vulnerabilities and exploits, malicious code threats, and potentially unwanted software

Microsoft Security Intelligence Report

Volume 15

January through June, 2013

Nepal

The statistics presented here are generated by Microsoft security programs and services running on computers in Nepal in 2Q13 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.

In previous volumes of the *Microsoft Security Intelligence Report*, malware prevalence was measured by *infection rate*, defined as the number of computers cleaned for every 1,000 executions of the Microsoft Malicious Software Removal Tool (*computers cleaned per mille*, or *CCM*). To provide a more accurate picture of the malware landscape, the CCM metric is being replaced by a measure of *encounter rate*, defined as the percent of computers running Microsoft real-time security products that detect malware each quarter.

The encounter rate for a population is typically much greater than its infection rate, because real-time security software blocks most malware before it can infect the computer. To help put encounter rates in context, this volume of the report includes data for both encounter rate and infection rate.

Infection rate statistics for Nepal

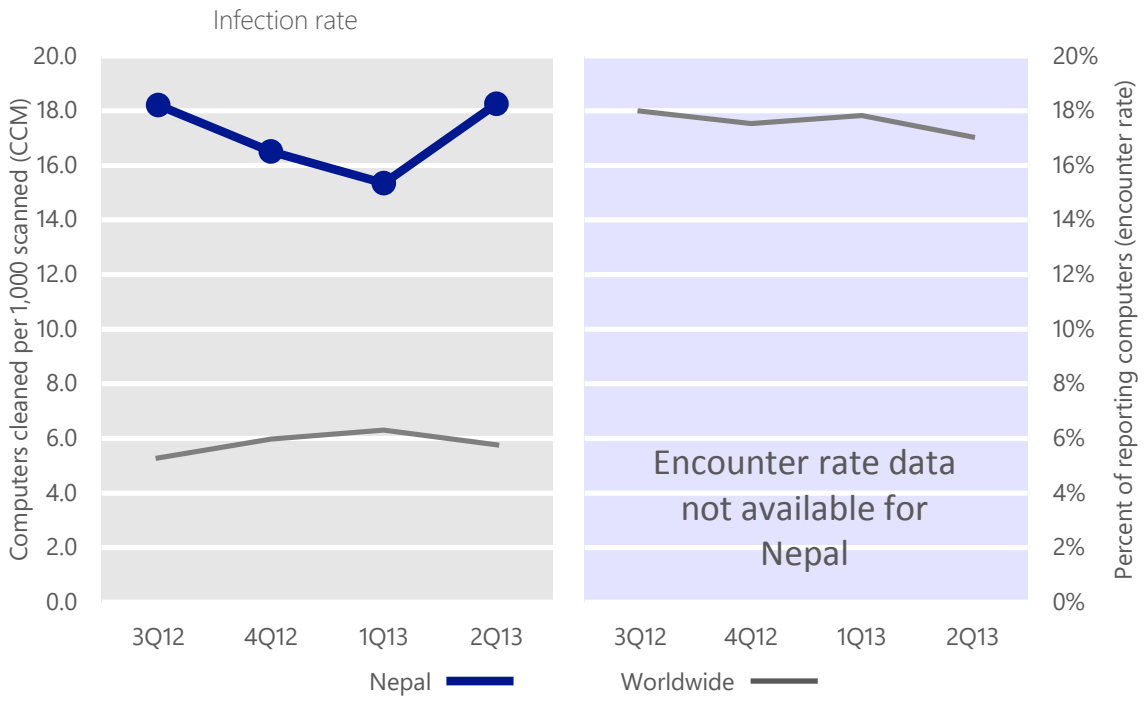
Metric	3Q12	4Q12	1Q13	2Q13
CCM, Nepal	18.2	16.5	15.3	18.3
Worldwide average CCM	*5.3*	*6.0*	*6.3*	*5.8*
Encounter rate, Nepal	N/A	N/A	N/A	N/A
Worldwide average encounter rate	*18.0%*	*17.5%*	*17.8%*	*17.0%*

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

Infection and encounter rate trends

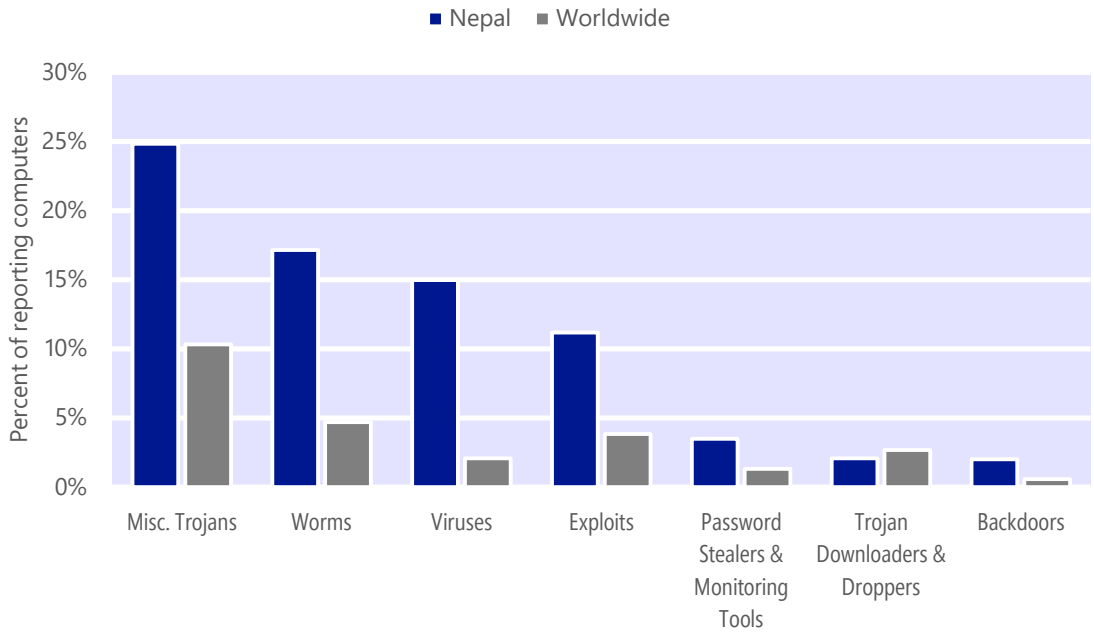
The MSRT cleaned malware on 18.3 of every 1,000 computers scanned in Nepal in 2Q13 (a CCM score of 18.3, compared to the 2Q13 worldwide average CCM of 5.8). In 2Q13, N/A percent of computers in Nepal encountered malware, compared to the 2Q13 worldwide average of 21.7% percent. The following figure shows the infection and encounter rate trends for Nepal over the last four quarters, compared to the world as a whole.

Malware infection and encounter trends in Nepal and worldwide



Threat categories

Malware and potentially unwanted software categories in Nepal in 2Q13, by percentage of computers reporting detections



- The most common category in Nepal in 2Q13 was Miscellaneous Trojans. It was encountered by 24.9 percent of all computers there, up from 24.0 percent in 1Q13.
- The second most common category in Nepal in 2Q13 was Worms. It was encountered by 17.2 percent of all computers there, up from 15.6 percent in 1Q13.
- The third most common category in Nepal in 2Q13 was Viruses, which was encountered by 17.2 percent of all computers there, up from 14.6 percent in 1Q13.

Threat families

The top 10 malware families in Nepal in 2Q13

	Family	Most significant category	% of reporting computers
1	Win32/Ramnit	Misc. Trojans	10.9%
2	INF/Autorun	Misc. Trojans	10.4%
3	Win32/CplLnk	Exploits	9.9%
4	Win32/Finodes	Misc. Trojans	9.5%
5	Win32/Sality	Viruses	6.8%
6	Win32/Virut	Viruses	6.8%
7	Win32/Nuqel	Worms	3.7%
8	Win32/Obfuscator	Misc. Trojans	3.2%
9	Win32/Yeltminky	Worms	3.1%
10	Win32/Conficker	Worms	2.1%

- The most common threat family in Nepal in 2Q13 was Win32/Ramnit, which affected 10.9 percent of reporting computers in Nepal. 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 second most common threat family in Nepal in 2Q13 was INF/Autorun, which affected 10.4 percent of reporting computers with detections in Nepal. 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 threat family in Nepal in 2Q13 was Win32/CplLnk, which affected 9.9 percent of reporting computers with detections in Nepal. Win32/CplLnk is a generic detection for specially-crafted malicious shortcut files that attempt to exploit the vulnerability addressed by Microsoft Security Bulletin MS10-046.
- The fourth most common threat family in Nepal in 2Q13 was Win32/Finodes, which affected 9.5 percent of reporting computers with detections in Nepal. Win32/Finodes is a trojan that attempts to contacts one or more remote hosts.

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 Nepal

Metric	3Q12	4Q12	1Q13	2Q13
Phishing sites per 1,000 hosts *(Worldwide)*	N/A *(5.41)*	N/A *(5.10)*	4.74 *(4.56)*	7.11 *(4.24)*
Malware hosting sites per 1,000 hosts *(Worldwide)*	N/A *(9.46)*	N/A *(10.85)*	16.59 *(11.66)*	28.44 *(17.67)*
Drive-by download sites per 1,000 URLs *(Worldwide)*	1.18 *(0.56)*	0.50 *(0.33)*	N/A *(0.50)*	0.03 *(1.12)*

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