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

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.

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

Belarus

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

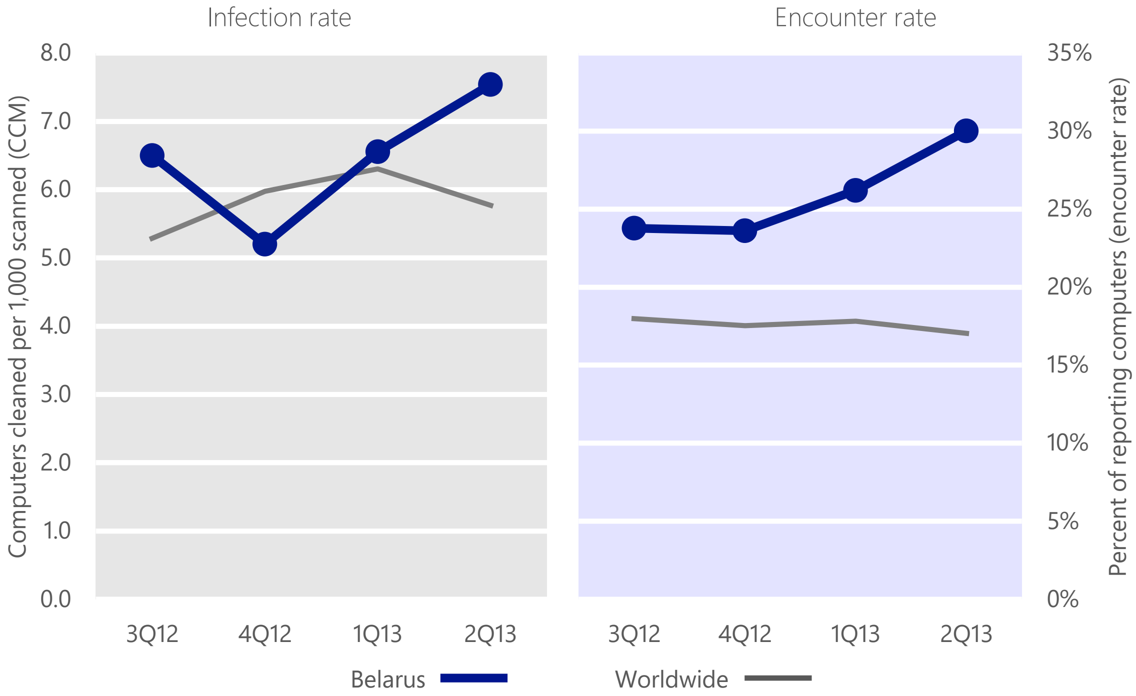
Metric	3Q12	4Q12	1Q13	2Q13
CCM, Belarus	6.5	5.2	6.6	7.5
Worldwide average CCM	*5.3*	*6.0*	*6.3*	*5.8*
Encounter rate, Belarus	23.8%	23.6%	26.2%	30.0%
Worldwide average encounter rate	*18.0%*	*17.5%*	*17.8%*	*17.0%*

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

Infection and encounter rate trends

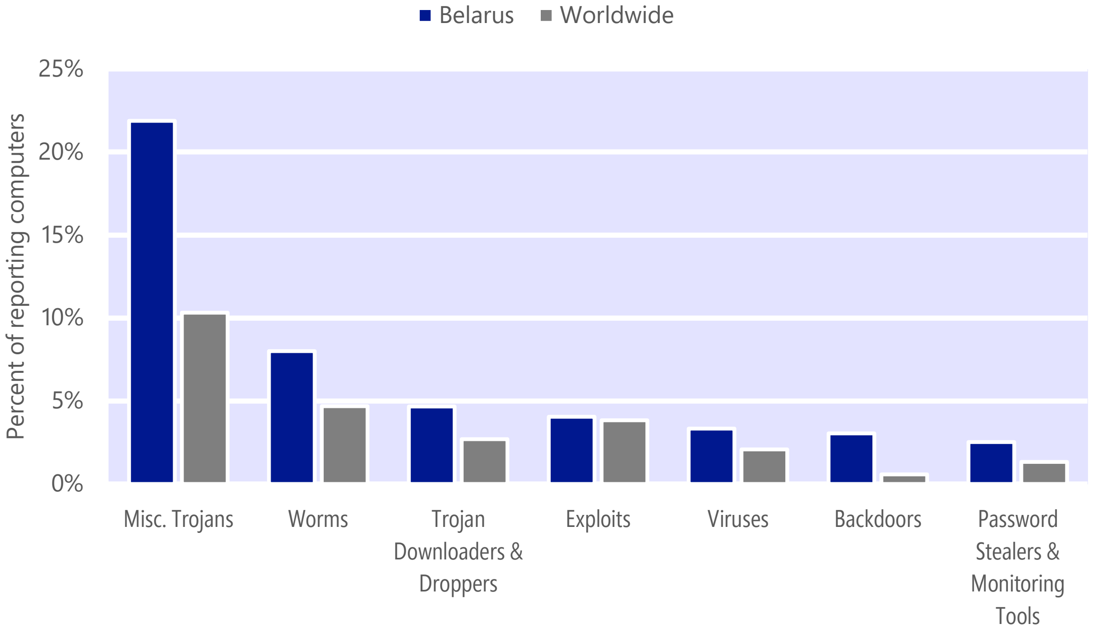
The MSRT cleaned malware on 7.5 of every 1,000 computers scanned in Belarus in 2Q13 (a CCM score of 7.5, compared to the 2Q13 worldwide average CCM of 5.8). In 2Q13, 30.0% percent of computers in Belarus encountered malware, compared to the 2Q13 worldwide average of 21.7% percent. The following figure shows the infection and encounter rate trends for Belarus over the last four quarters, compared to the world as a whole.

Malware infection and encounter trends in Belarus and worldwide



Threat categories

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



- The most common category in Belarus in 2Q13 was Miscellaneous Trojans. It was encountered by 21.9 percent of all computers there, up from 19.3 percent in 1Q13.
- The second most common category in Belarus in 2Q13 was Worms. It was encountered by 8.0 percent of all computers there, up from 5.7 percent in 1Q13.
- The third most common category in Belarus in 2Q13 was Trojan Downloaders & Droppers, which was encountered by 8.0 percent of all computers there, down from 5.0 percent in 1Q13.

Threat families

The top 10 malware families in Belarus in 2Q13

	Family	Most significant category	% of reporting computers
1	Win32/Obfuscator	Misc. Trojans	6.6%
2	Win32/Dorkbot	Worms	3.2%
3	BAT/Qhost	Misc. Trojans	2.6%
4	Win32/Dynamer	Misc. Trojans	1.8%
5	JS/Tadtruss	Misc. Trojans	1.8%
6	Win32/Gamarue	Worms	1.7%
7	INF/Autorun	Misc. Trojans	1.6%
8	Win32/Zipparch	Misc. Trojans	1.5%
9	JS/Redirector	Misc. Trojans	1.2%
10	Win32/Orsam	Misc. Trojans	1.2%

- The most common threat family in Belarus in 2Q13 was Win32/Obfuscator, which affected 6.6 percent of reporting computers in Belarus. 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 threat family in Belarus in 2Q13 was Win32/Dorkbot, which affected 3.2 percent of reporting computers with detections in Belarus. Win32/Dorkbot is a worm that spreads via instant messaging and removable drives. It also contains backdoor functionality that allows unauthorized access and control of the affected computer. Win32/Dorkbot may be distributed from compromised or malicious websites using PDF or browser exploits.
- The third most common threat family in Belarus in 2Q13 was BAT/Qhost, which affected 2.6 percent of reporting computers with detections in Belarus. BAT/Qhost is a generic detection for trojans that modify the HOSTS file on the computer to redirect or limit Internet traffic to certain sites.
- The fourth most common threat family in Belarus in 2Q13 was Win32/Dynamer, which affected 1.8 percent of reporting computers with detections in Belarus. Win32/Dynamer is a generic detection for a variety of threats.

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 Belarus

Metric	3Q12	4Q12	1Q13	2Q13
Phishing sites per 1,000 hosts *(Worldwide)*	11.01 *(5.41)*	13.38 *(5.10)*	13.63 *(4.56)*	14.65 *(4.24)*
Malware hosting sites per 1,000 hosts *(Worldwide)*	10.62 *(9.46)*	13.77 *(10.85)*	22.83 *(11.66)*	31.35 *(17.67)*
Drive-by download sites per 1,000 URLs *(Worldwide)*	3.67 *(0.56)*	1.31 *(0.33)*	2.04 *(0.50)*	5.63 *(1.12)*

Microsoft

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