

Microsoft Security Intelligence Report

Volume 16 | July through December, 2013

Trinidad and Tobago

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.

Trinidad and Tobago

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

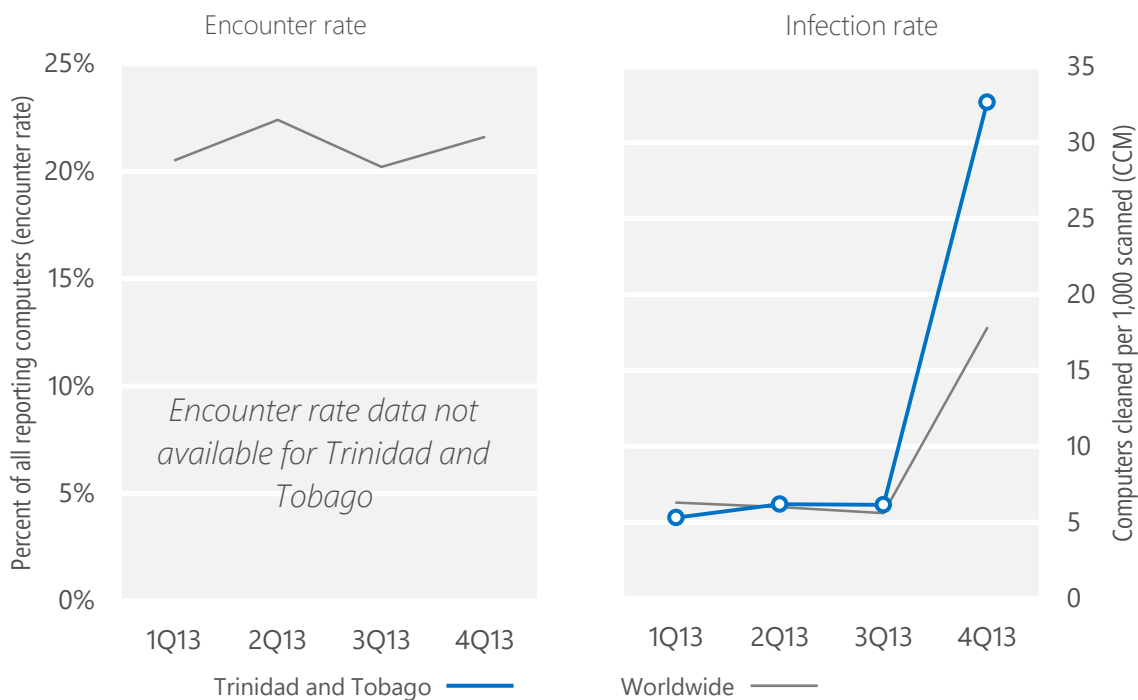
Metric	1Q13	2Q13	3Q13	4Q13
CCM, Trinidad and Tobago	5.3	6.2	6.2	32.7
Worldwide CCM	6.3	6.9	5.6	17.8
Encounter rate, Trinidad and Tobago	N/A	N/A	N/A	N/A
Worldwide encounter rate	20.5%	22.4%	20.2%	21.6%

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

Encounter and infection rate trends

In 4Q13, the MSRT detected and removed malware from 32.7 of every 1,000 unique computers scanned in Trinidad and Tobago in 4Q13 (a CCM score of 32.7, compared to the 4Q13 worldwide CCM of 17.8). The following figure shows the encounter and infection rate trends for Trinidad and Tobago over the last four quarters, compared to the world as a whole.

Malware encounter and infection rate trends in Trinidad and Tobago and worldwide



Top threat families by infection rate

The top 10 malware families by infection rate in Trinidad and Tobago in 4Q13

	Family	Most significant category	Infection rate (CCM)
1	Win32/Rotbrow	Trojan Downloaders & Droppers	27.2
2	Win32/Sefnit	Misc. Trojans	3.5
3	Win32/Vobfus	Worms	0.7
4	Win32/Brontok	Worms	0.6
5	Win32/IRCbot	Backdoors	0.5
6	Win32/Dorkbot	Worms	0.3
7	Win32/Gamarue	Worms	0.3
8	Win32/Sirefef	Misc. Trojans	0.3
9	Win32/Napolar	Misc. Trojans	0.3
10	Win32/Alureon	Misc. Trojans	0.2

- The most common threat family infecting computers in Trinidad and Tobago in 4Q13 was [Win32/Rotbrow](#), which was detected and removed from 27.2 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 Trinidad and Tobago in 4Q13 was [Win32/Sefnit](#), which was detected and removed from 3.5 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 Trinidad and Tobago in 4Q13 was [Win32/Vobfus](#), which was detected and removed from 0.7 of every 1,000 unique computers scanned by the MSRT. [Win32/Vobfus](#) is a family of worms that spreads via network drives and removable drives and download/executes arbitrary files. Downloaded files may include additional malware.
- The fourth most common threat family infecting computers in Trinidad and Tobago in 4Q13 was [Win32/Brontok](#), which was detected and removed from 0.6 of every 1,000 unique computers scanned by the MSRT. [Win32/Brontok](#) is a mass-mailing email worm that spreads by sending copies of itself as email attachments to addresses gathered from files on the infected computer, and by copying itself to removable volumes. Brontok can disable security software, and may conduct DoS attacks against certain websites.

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 Trinidad and Tobago

Metric	1Q13	2Q13	3Q13	4Q13
Phishing sites per 1,000 hosts (Worldwide)	4.18 (4.56)	12.55 (4.24)	4.02 (3.94)	2.01 (5.48)
Malware hosting sites per 1,000 hosts (Worldwide)	23.01 (11.66)	56.49 (17.67)	70.28 (18.00)	68.27 (18.41)
Drive-by download sites per 1,000 URLs (Worldwide)	N/A (0.50)	N/A (1.12)	N/A (1.09)	N/A (0.25)



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