Microsoft

Microsoft Security Intelligence Report

Volume 21 | January through June, 2016

Bolivia

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 Web site 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.

Bolivia

The statistics presented here are generated by Microsoft security programs and services running on computers in Bolivia in 2Q16 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.

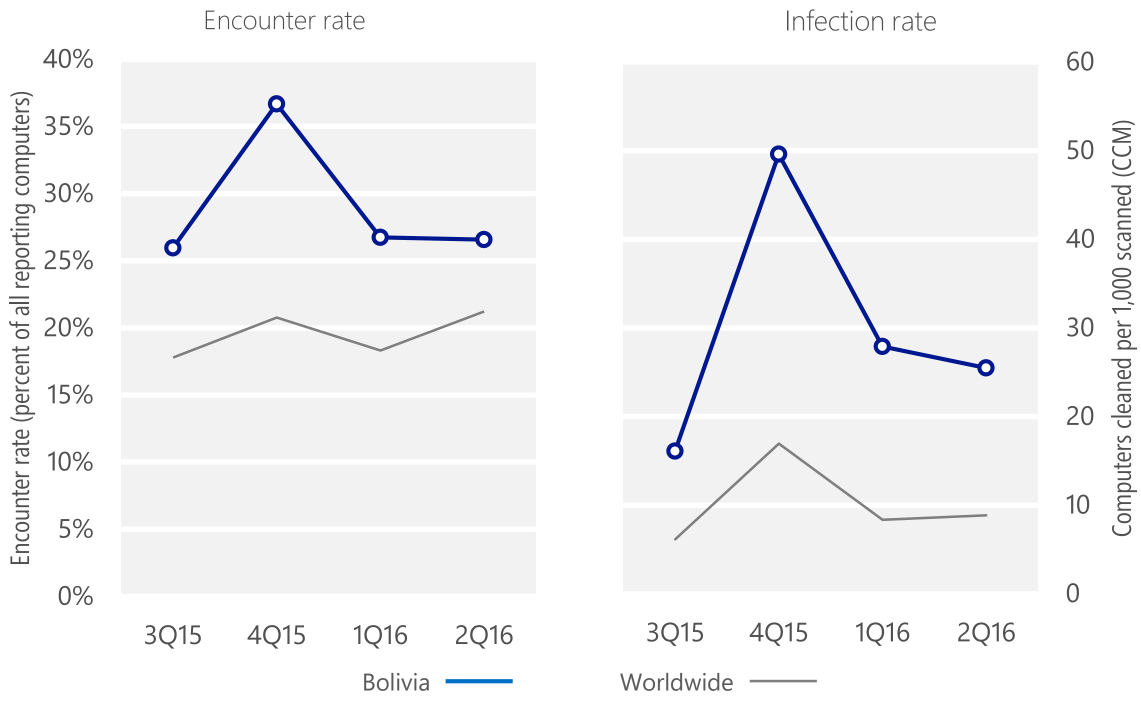
Infection rate statistics for Bolivia

Metric	3Q15	4Q15	1Q16	2Q16
Encounter rate, Bolivia	25.9%	36.7%	26.7%	26.6%
Worldwide encounter rate	*17.8%*	*20.8%*	*18.3%*	*21.2%*
CCM, Bolivia	16.1	49.6	27.9	25.5
Worldwide CCM	*6.1*	*16.9*	*8.4*	*8.8*

Encounter and infection rate trends

In 2Q16, 26.6% of computers in Bolivia encountered malware, compared to the 2Q16 worldwide encounter rate of 20.8 percent. In addition, the MSRT detected and removed malware from 25.5 of every 1,000 unique computers scanned in Bolivia in 2Q16 (a CCM score of 25.5, compared to the 2Q16 worldwide CCM of 16.9). The following figure shows the encounter and infection rate trends for Bolivia over the last four quarters, compared to the world as a whole.

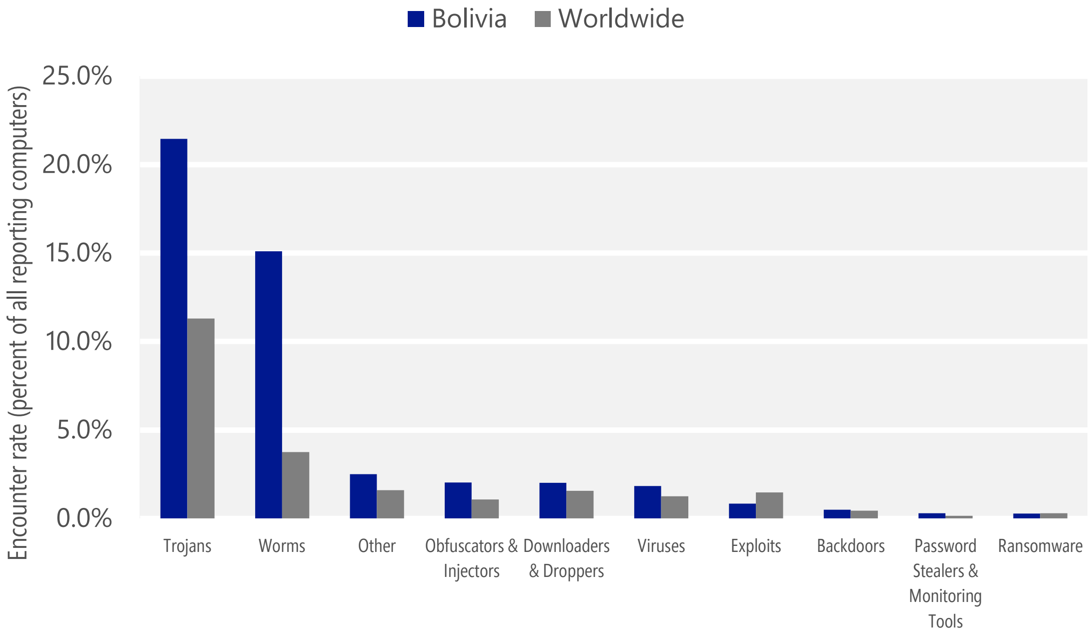
Malware encounter and infection rate trends in Bolivia and worldwide



See the Worldwide Threat Assessment section of Microsoft Security Intelligence Report, Volume 21 at www.microsoft.com/sir for more information about threats in Bolivia and around the world, and for explanations of the methods and terms used here.

Malicious software categories

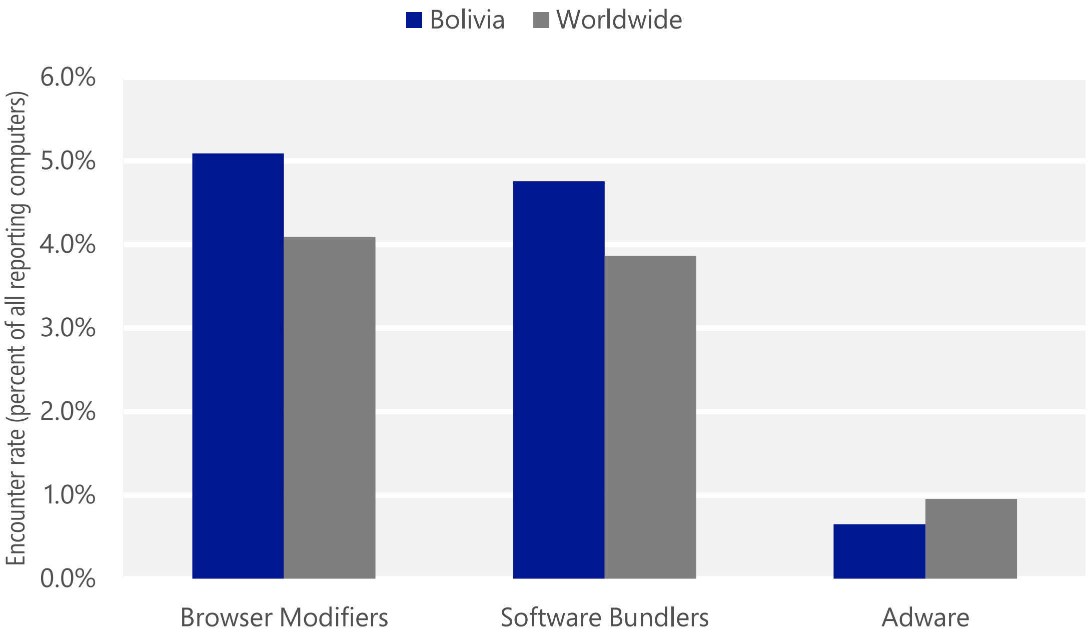
Malicious software encountered in Bolivia in 2Q16, by category



- The most common malicious software category in Bolivia in 2Q16 was Trojans. It was encountered by 21.4 percent of all computers there, up from 20.1 percent in 1Q16.
- The second most common malicious software category in Bolivia in 2Q16 was Worms. It was encountered by 15.1 percent of all computers there, down from 16.5 percent in 1Q16.
- The third most common malicious software category in Bolivia in 2Q16 was Other Malware, which was encountered by 3.1 percent of all computers there, down from 5.0 percent in 1Q16.

Unwanted software categories

Unwanted software encountered in Bolivia in 2Q16, by category



- The most common unwanted software category in Bolivia in 2Q16 was Browser Modifiers. It was encountered by 5.1 percent of all computers there, down from 7.5 percent in 1Q16.
- The second most common unwanted software category in Bolivia in 2Q16 was Software Bundlers. It was encountered by 4.8 percent of all computers there, down from 6.9 percent in 1Q16.
- The third most common unwanted software category in Bolivia in 2Q16 was Adware, which was encountered by 0.7 percent of all computers there, down from 1.0 percent in 1Q16.

Top malicious software families by encounter rate

The most common malicious software families encountered in Bolivia in 2Q16

	Family	Most significant category	% of reporting computers
1	Win32/Gamarue	Worms	7.7%
2	Win32/Lodbak	Trojans	6.1%
3	Win32/Peals	Trojans	2.6%
4	VBS/Jenxcus	Worms	2.0%
5	JS/Bondat	Worms	1.7%
6	Win32/Dynamer	Trojans	1.6%
7	Win32/Spursint	Trojans	1.0%
8	Win32/Skeeyah	Trojans	1.0%
9	INF/Autorun	Obfuscators & Injectors	0.9%
10	Win32/Sality	Viruses	0.8%

- The most common malicious software family encountered in Bolivia in 2Q16 was Win32/Gamarue, which was encountered by 7.7 percent of reporting computers there. 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 second most common malicious software family encountered in Bolivia in 2Q16 was Win32/Lodbak, which was encountered by 6.1 percent of reporting computers there. Win32/Lodbak is a trojan that is usually installed on removable drives by Win32/Gamarue, and which attempts to install Gamarue when the infected removable drive is connected to a computer.
- The third most common malicious software family encountered in Bolivia in 2Q16 was Win32/Peals, which was encountered by 2.6 percent of reporting computers there. Win32/Peals is a generic detection for various threats that display trojan characteristics.
- The fourth most common malicious software family encountered in Bolivia in 2Q16 was VBS/Jenxcus, which was encountered by 2.0 percent of reporting computers there. 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 unwanted software families by encounter rate

The most common unwanted software families encountered in Bolivia in 2Q16

	Family	Most significant category	% of reporting computers
1	Win32/Mizenota	Software Bundlers	1.1%
2	Win32/Sasquor	Browser Modifiers	1.1%
3	Win32/Diplugem	Browser Modifiers	1.0%
4	Win32/SupTab	Browser Modifiers	0.7%
5	Win32/KipodToolsCby	Browser Modifiers	0.7%

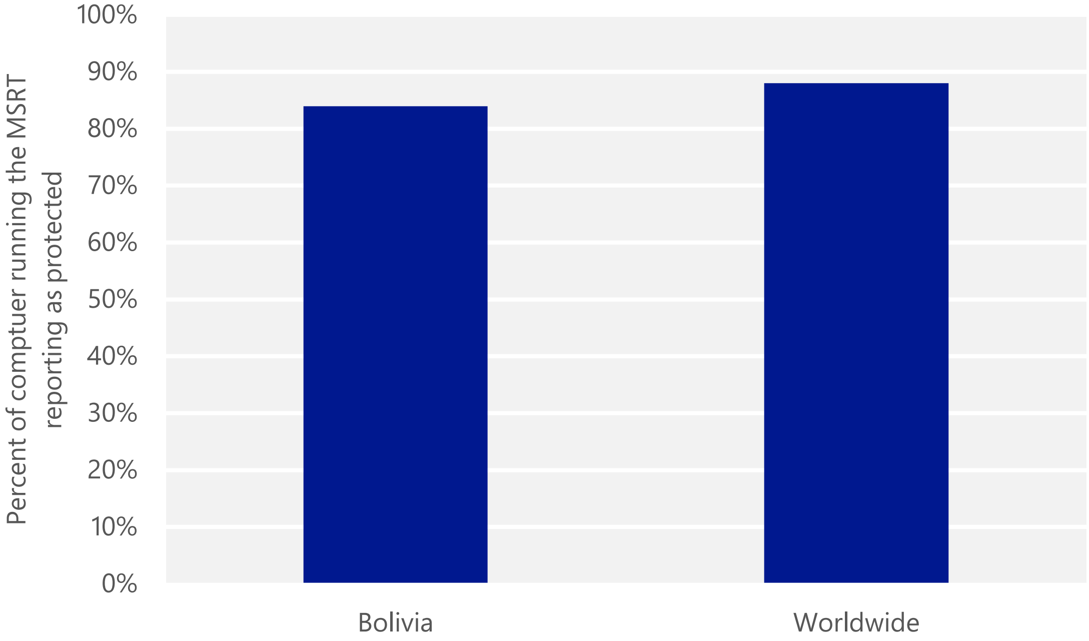
- The most common unwanted software family encountered in Bolivia in 2Q16 was Win32/Mizenota, which was encountered by 1.1 percent of reporting computers there. Win32/Mizenota is a software bundler that installs unwanted software alongside the software the user is trying to install. It has been observed to install Win32/SupTab, Win32/Sasqor, Win32/Smudplu, and others.
- The second most common unwanted software family encountered in Bolivia in 2Q16 was Win32/Sasquor, which was encountered by 1.1 percent of reporting computers there. Win32/Sasquor is a browser modifier that modifies search and home page settings, and installs services and scheduled tasks to prevent the user from changing them back. It can also download additional malware, including Win32/SupTab and Win32/Xadupi.
- The third most common unwanted software family encountered in Bolivia in 2Q16 was Win32/Diplugem, which was encountered by 1.0 percent of reporting computers there. Win32/Diplugem is a browser modifier that installs browser add-ons without obtaining the user's consent. The add-ons show extra advertisements as the user browses the web, and can inject additional ads into web search results pages.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

The figure below shows the percentage of computers worldwide and in Bolivia that the MSRT found to be running up-to-date real-time security software in 2Q16.

Percent of computers in Bolivia and worldwide protected by real-time security software in 2Q16



Microsoft

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