Microsoft

Microsoft Security Intelligence Report

Volume 20 | July through December, 2015

Mexico
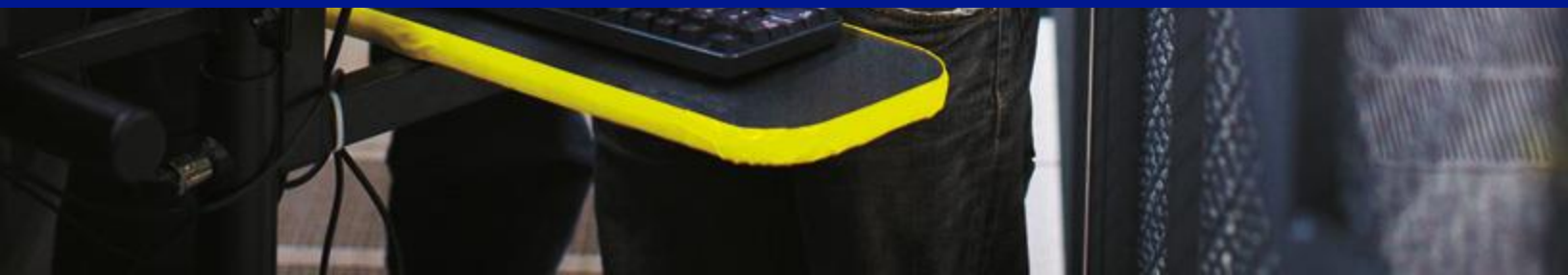
Mexico

The statistics presented here are generated by Microsoft security programs and services running on computers in Mexico in 4Q15 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 Mexico

Metric	1Q15	2Q15	3Q15	4Q15
Encounter rate, Mexico	23.0%	21.2%	23.9%	28.5%
Worldwide encounter rate	*17.6%*	*15.3%*	*17.8%*	*20.8%*
CCM, Mexico	11.4	18.6	11.8	40.9
Worldwide CCM	*5.4*	*8.4*	*6.1*	*16.9*

Encounter and infection rates reported here do not include totals for the Brantall, Filcout, and Rotbrow malware families. See pages 57–64 of *Microsoft Security Intelligence Report, Volume 17* for an explanation of this decision.

Encounter and infection rate trends

In 4Q15, 28.5% of computers in Mexico encountered malware, compared to the 4Q15 worldwide encounter rate of 20.8 percent. In addition, the MSRT detected and removed malware from 40.9 of every 1,000 unique computers scanned in Mexico in 4Q15 (a CCM score of 40.9, compared to the 4Q15 worldwide CCM of 16.9). The following figure shows the encounter and infection rate trends for Mexico over the last four quarters, compared to the world as a whole.

Malware encounter and infection rate trends in Mexico and worldwide
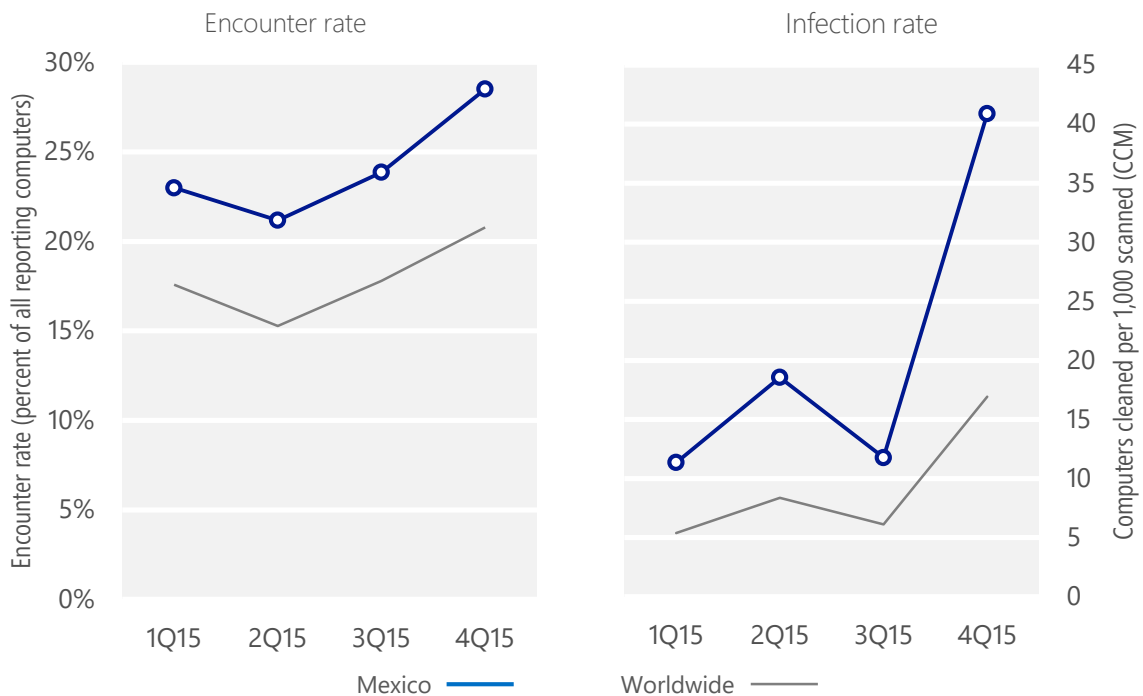
See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 20* at www.microsoft.com/sir for more information about threats in Mexico and around the world, and for explanations of the methods and terms used here.

Malware categories

Malware encountered in Mexico in 4Q15, by category
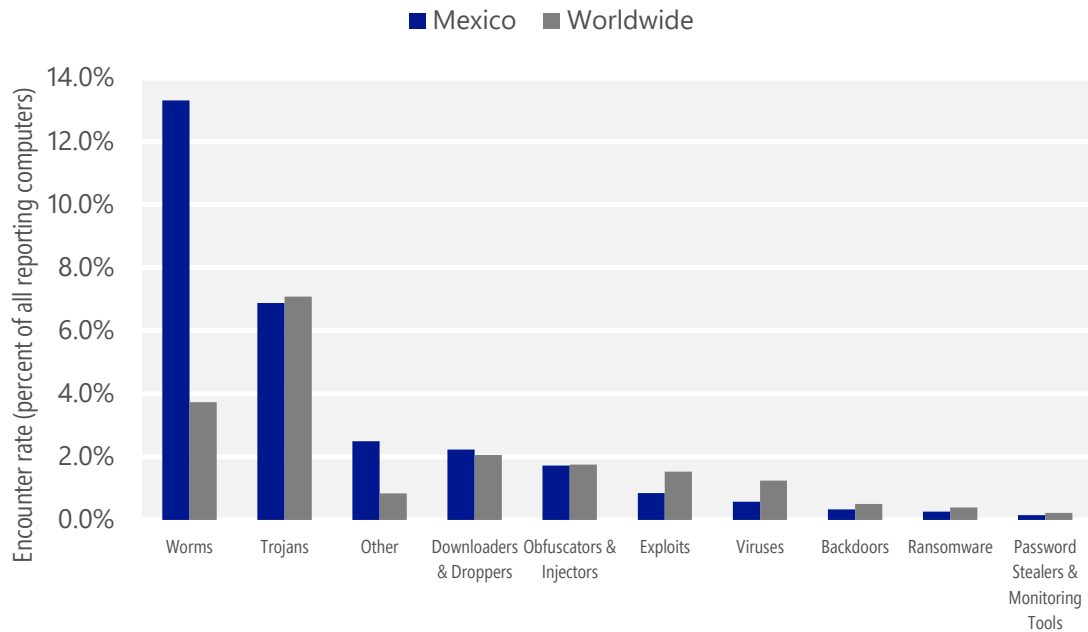
- The most common malware category in Mexico in 4Q15 was Worms. It was encountered by 13.3 percent of all computers there, up from 9.9 percent in 3Q15.

- The second most common malware category in Mexico in 4Q15 was Trojans. It was encountered by 6.9 percent of all computers there, down from 7.7 percent in 3Q15.

- The third most common malware category in Mexico in 4Q15 was Downloaders & Droppers, which was encountered by 2.2 percent of all computers there, down from 2.3 percent in 3Q15.

Unwanted software categories

Unwanted software encountered in Mexico in 4Q15, by category

■ Mexico   ■ Worldwide
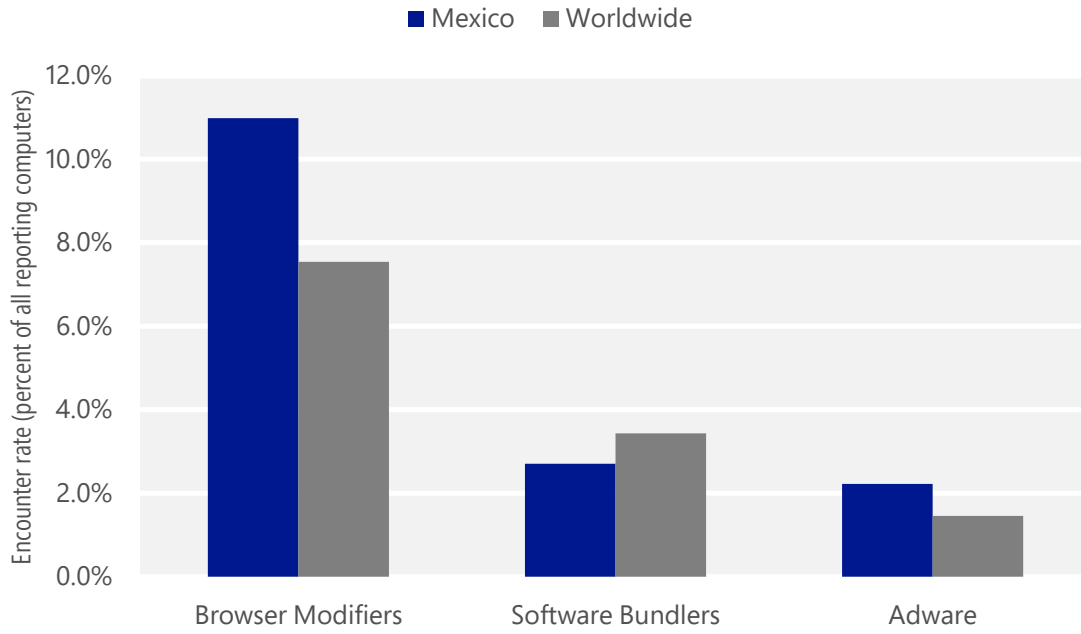
- The most common unwanted software category in Mexico in 4Q15 was Browser Modifiers. It was encountered by 11.0 percent of all computers there, up from 10.7 percent in 3Q15.

- The second most common unwanted software category in Mexico in 4Q15 was Software Bundlers. It was encountered by 2.7 percent of all computers there, down from 3.2 percent in 3Q15.

- The third most common unwanted software category in Mexico in 4Q15 was Adware, which was encountered by 2.2 percent of all computers there, up from 2.0 percent in 3Q15.

Top malware families by encounter rate

The most common malware families encountered in Mexico in 4Q15

	Family	Most significant category	% of reporting computers
1	Win32/Gamarue	Worms	9.3%
2	VBS/Jenxcus	Worms	2.5%
3	Win32/Peals	Trojans	1.9%
4	JS/Bondat	Worms	1.5%
5	Win32/Sventore	Downloaders & Droppers	1.2%
6	INF/Autorun	Obfuscators & Injectors	0.8%
7	Win32/Skeeyah	Trojans	0.6%
8	Win32/Dynamer	Trojans	0.6%
9	Win32/CeeInject	Obfuscators & Injectors	0.5%
10	Win32/Obfuscator	Obfuscators & Injectors	0.5%

- The most common malware family encountered in Mexico in 4Q15 was Win32/Gamarue, which was encountered by 9.3 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 malware family encountered in Mexico in 4Q15 was VBS/Jenxcus, which was encountered by 2.5 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.

- The third most common malware family encountered in Mexico in 4Q15 was Win32/Peals, which was encountered by 1.9 percent of reporting computers there. Win32/Peals is a generic detection for various threats that display trojan characteristics.

- The fourth most common malware family encountered in Mexico in 4Q15 was JS/Bondat, which was encountered by 1.5 percent of reporting computers there. JS/Bondat is a family of threats that collects information about the computer, infects removable drives, and tries to stop the user from accessing files. It spreads by infecting removable drives, such as USB thumb drives and flash drives.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Mexico in 4Q15

	Family	Most significant category	% of reporting computers
1	Win32/SupTab	Browser Modifiers	4.5%
2	Win32/Diplugem	Browser Modifiers	3.6%
3	Win32/Pokki	Browser Modifiers	1.0%
4	Win32/Bayads	Adware	1.0%
5	Win32/EoRezo	Adware	0.7%

- The most common unwanted software family encountered in Mexico in 4Q15 was Win32/SupTab, which was encountered by 4.5 percent of reporting computers there. Win32/SupTab is a browser modifier that installs itself and changes the browser's default search provider, without obtaining the user's consent for either action.

- The second most common unwanted software family encountered in Mexico in 4Q15 was Win32/Diplugem, which was encountered by 3.6 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.

- The third most common unwanted software family encountered in Mexico in 4Q15 was Win32/Pokki, which was encountered by 1.0 percent of reporting computers there. Win32/Pokki is a browser add-on that formerly displayed behaviors of unwanted software. Recent versions of the add-on no longer meet Microsoft detection criteria, and are no longer considered unwanted software.

Top threat families by infection rate

The most common malware families by infection rate in Mexico in 4Q15

|	Family	Most significant category	Infection rate (CCM)
1	Win32/Diplugem	Browser Modifiers	22.6
2	Win32/Gamarue	Worms	12.4
3	VBS/Jenxcus	Worms	2.4
4	Win32/Blakamba	Trojans	1.5
5	Win32/Peals	Trojans	1.1
6	JS/Bondat	Worms	0.7
7	Win32/Brontok	Worms	0.5
8	Win32/Lefgroo	Worms	0.4
9	Win32/Sality	Viruses	0.3
10	Win32/Dorkbot	Worms	0.3

- The most common threat family infecting computers in Mexico in 4Q15 was Win32/Diplugem, which was detected and removed from 22.6 of every 1,000 unique computers scanned by the MSRT. 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.

- The second most common threat family infecting computers in Mexico in 4Q15 was Win32/Gamarue, which was detected and removed from 12.4 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 third most common threat family infecting computers in Mexico in 4Q15 was VBS/Jenxcus, which was detected and removed from 2.4 of every 1,000 unique computers scanned by the MSRT. 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.

- The fourth most common threat family infecting computers in Mexico in 4Q15 was Win32/Blakamba, which was detected and removed from 1.5 of every 1,000 unique computers scanned by the MSRT. Win32/Blakamba is a trojan that can download other malware. It has been observed being installed at the same time as Win32/InstalleRex, a software bundler.

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.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Mexico and worldwide protected by real-time security software in 4Q15
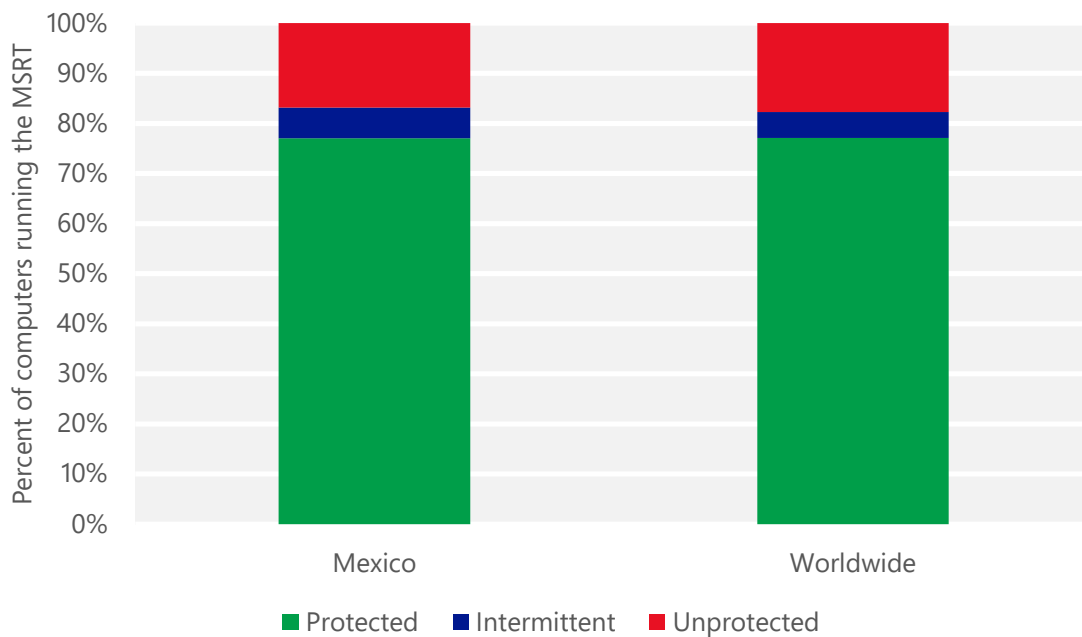
Malicious websites

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.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Microsoft Edge and Internet Explorer. See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 20* for more information about these protections and how the data is collected.

Malicious website statistics for Mexico

Metric	3Q15	4Q15
Drive-by download pages per 1,000 URLs *(Worldwide)*	0.08 *(0.22)*	0.26 *(0.57)*
Phishing sites per 100,000 Internet users *(Worldwide)*	0.87 *(4.7)*	0.75 *(3.9)*
Malware hosting sites per 100,000 Internet users *(Worldwide)*	35.26 *(56.2)*	23.99 *(26.4)*