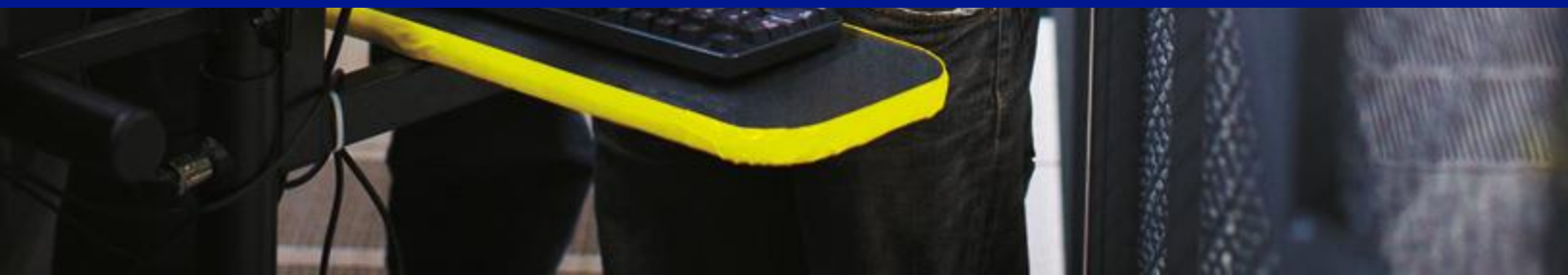




# Microsoft Security Intelligence Report

Volume 20 | July through December, 2015

*Mongolia*



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.

Copyright © 2016 Microsoft Corporation. All rights reserved.

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

# Mongolia

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

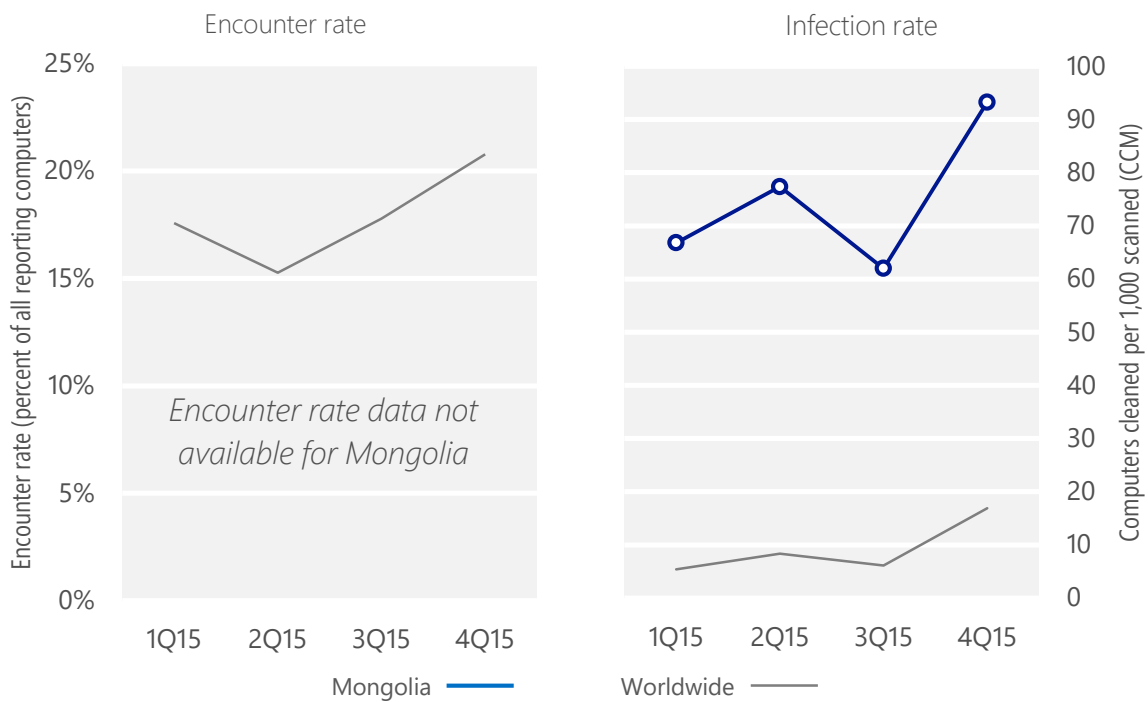
Metric	1Q15	2Q15	3Q15	4Q15
Encounter rate, Mongolia	N/A	N/A	N/A	N/A
Worldwide encounter rate	17.6%	15.3%	17.8%	20.8%
CCM, Mongolia	66.8	77.4	62.0	93.3
Worldwide CCM	5.4	8.4	6.1	16.9

Encounter and infection rates reported here do not include totals for the Brantall, Filcoute, 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, the MSRT detected and removed malware from 93.3 of every 1,000 unique computers scanned in Mongolia in 4Q15 (a CCM score of 93.3, compared to the 4Q15 worldwide CCM of 16.9). The following figure shows the encounter and infection rate trends for Mongolia over the last four quarters, compared to the world as a whole.

Malware encounter and infection rate trends in Mongolia and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 20](#) at [www.microsoft.com/sir](http://www.microsoft.com/sir) for more information about threats in Mongolia and around the world, and for explanations of the methods and terms used here.

## Top threat families by infection rate

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

	Family	Most significant category	Infection rate (CCM)
1	<a href="#">Win32/Gamarue</a>	Worms	36.5
2	<a href="#">Win32/Diplugem</a>	Browser Modifiers	30.8
3	<a href="#">Win32/Sality</a>	Viruses	16.5
4	<a href="#">VBS/Jenxcus</a>	Worms	8.7
5	<a href="#">Win32/Yeltminky</a>	Worms	8.4
6	<a href="#">Win32/Blakamba</a>	Trojans	4.4
7	<a href="#">Win32/Ramnit</a>	Viruses	3.1
8	<a href="#">Win32/Necurs</a>	Trojans	2.5
9	<a href="#">Win32/Virut</a>	Viruses	2.4
10	<a href="#">Win32/Peals</a>	Trojans	1.9

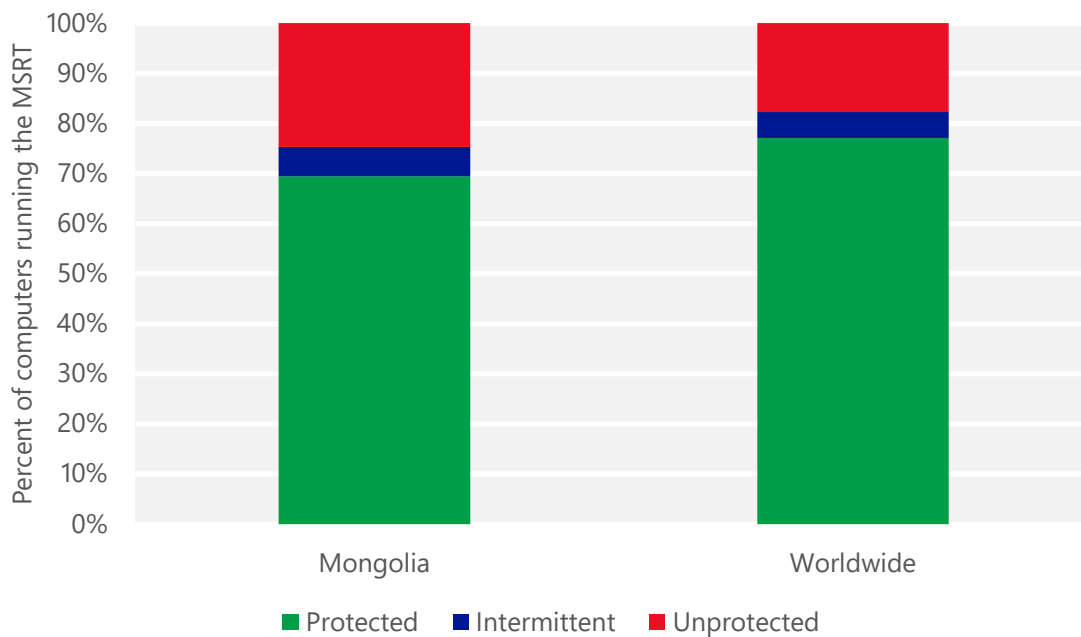
- The most common threat family infecting computers in Mongolia in 4Q15 was [Win32/Gamarue](#), which was detected and removed from 36.5 of every 1,000 unique computers scanned by the MSRT. [Win32/Gamarue](#) is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The second most common threat family infecting computers in Mongolia in 4Q15 was [Win32/Diplugem](#), which was detected and removed from 30.8 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 third most common threat family infecting computers in Mongolia in 4Q15 was [Win32/Sality](#), which was detected and removed from 16.5 of every 1,000 unique computers scanned by the MSRT. [Win32/Sality](#) is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The fourth most common threat family infecting computers in Mongolia in 4Q15 was [VBS/Jenxcus](#), which was detected and removed from 8.7 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.

## 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 Mongolia 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 Mongolia

Metric	3Q15	4Q15
Drive-by download pages per 1,000 URLs (Worldwide)	5.20 (0.22)	10.05 (0.57)
Phishing sites per 100,000 Internet users (Worldwide)	2.29 (4.7)	1.65 (3.9)
Malware hosting sites per 100,000 Internet users (Worldwide)	124.99 (56.2)	52.57 (26.4)



One Microsoft Way  
Redmond, WA 98052-6399  
[microsoft.com/security](https://microsoft.com/security)