



Microsoft Security Intelligence Report

Volume 18 | July through December, 2014

Georgia

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 © 2015 Microsoft Corporation. All rights reserved.

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

Georgia

The statistics presented here are generated by Microsoft security programs and services running on computers in Georgia in 4Q14 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 Georgia

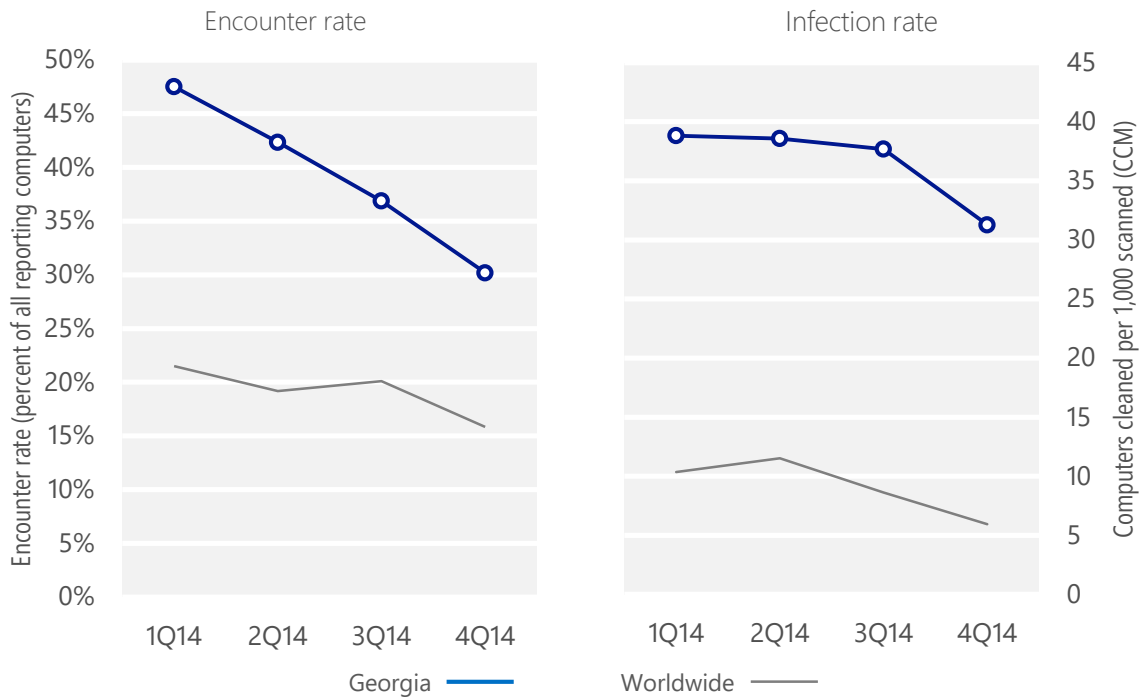
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Georgia	47.5%	42.3%	36.9%	30.2%
<i>Worldwide encounter rate</i>	<i>21.5%</i>	<i>19.2%</i>	<i>20.1%</i>	<i>15.9%</i>
CCM, Georgia	38.8	38.6	37.7	31.3
<i>Worldwide CCM</i>	<i>10.3</i>	<i>11.5</i>	<i>8.6</i>	<i>5.9</i>

Encounter and infection rates reported here do not include totals for the Brantall, Filcote, 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 4Q14, 30.2% percent of computers in Georgia encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 31.3 of every 1,000 unique computers scanned in Georgia in 4Q14 (a CCM score of 31.3, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Georgia over the last four quarters, compared to the world as a whole.

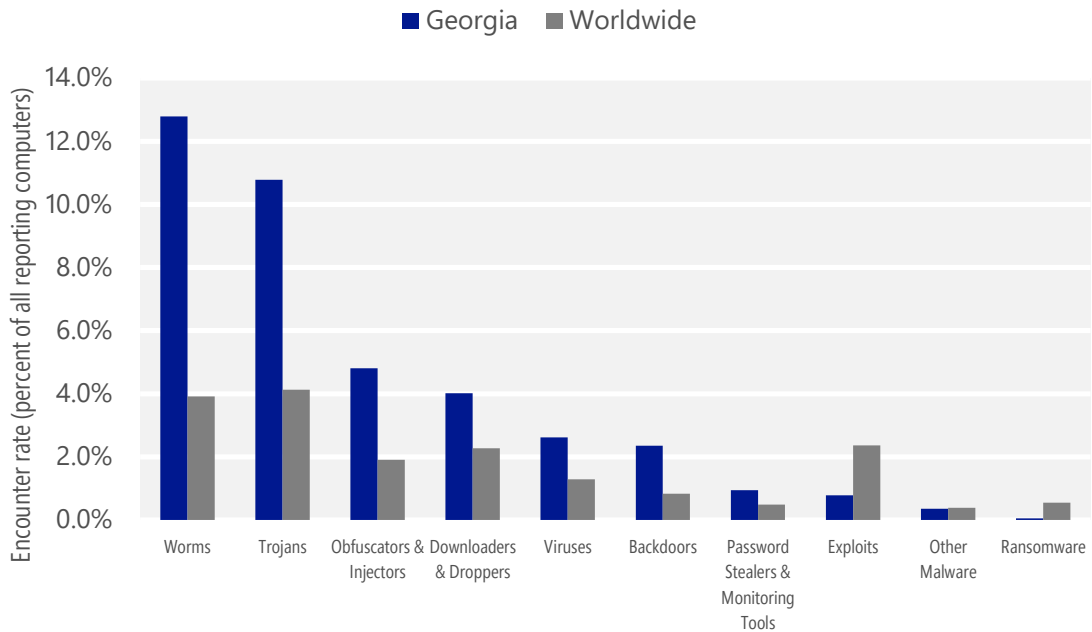
Malware encounter and infection rate trends in Georgia and worldwide



See the Worldwide Threat Assessment section of [Microsoft Security Intelligence Report, Volume 18](#) at www.microsoft.com/sir for more information about threats in Georgia and around the world, and for explanations of the methods and terms used here.

Malware categories

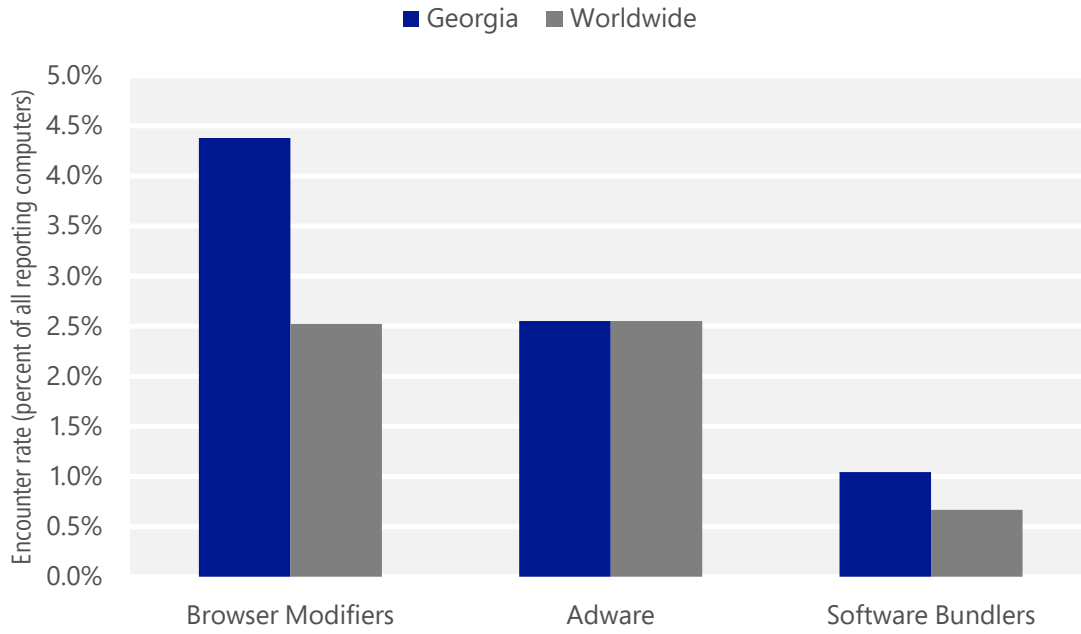
Malware encountered in Georgia in 4Q14, by category



- The most common malware category in Georgia in 4Q14 was Worms. It was encountered by 12.8 percent of all computers there, down from 18.5 percent in 3Q14.
- The second most common malware category in Georgia in 4Q14 was Trojans. It was encountered by 10.8 percent of all computers there, down from 13.5 percent in 3Q14.
- The third most common malware category in Georgia in 4Q14 was Obfuscators & Injectors, which was encountered by 4.8 percent of all computers there, down from 7.0 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Georgia in 4Q14, by category



- The most common unwanted software category in Georgia in 4Q14 was Browser Modifiers. It was encountered by 4.4 percent of all computers there, down from 5.8 percent in 3Q14.
- The second most common unwanted software category in Georgia in 4Q14 was Adware. It was encountered by 2.6 percent of all computers there, up from 0.5 percent in 3Q14.
- The third most common unwanted software category in Georgia in 4Q14 was Software Bundlers, which was encountered by 1.0 percent of all computers there, up from 0.1 percent in 3Q14.

Top malware families by encounter rate

The most common malware families encountered in Georgia in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Gamarue	Worms	4.6%
2	JS/Kilim	Trojans	3.7%
3	Win32/Tophos	Worms	3.1%
4	Win32/Obfuscator	Obfuscators & Injectors	2.7%
5	Win32/Ogimant	Downloaders & Droppers	2.3%
6	INF/Autorun	Obfuscators & Injectors	2.2%
7	Win32/Brontok	Worms	2.1%
8	Win32/Sality	Viruses	1.3%
9	Win32/Peaac	Trojans	1.2%
10	Win32/Vermis	Worms	1.2%

- The most common malware family encountered in Georgia in 4Q14 was [Win32/Gamarue](#), which was encountered by 4.6 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 Georgia in 4Q14 was [JS/Kilim](#), which was encountered by 3.7 percent of reporting computers there. [JS/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The third most common malware family encountered in Georgia in 4Q14 was [Win32/Tophos](#), which was encountered by 3.1 percent of reporting computers there. [Win32/Tophos](#) is a worm that copies itself to network shares and removable drives, displays an adult-oriented image, and may download additional malware.
- The fourth most common malware family encountered in Georgia in 4Q14 was [Win32/Obfuscator](#), which was encountered by 2.7 percent of reporting computers there. [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.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Georgia in 4Q14

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	3.6%
2	Win32/BetterSurf	Adware	1.5%
3	Win32/Costmin	Adware	1.0%
4	Win32/Defaulttab	Browser Modifiers	0.9%
5	Win32/Gofilexpress	Software Bundlers	0.8%

- The most common unwanted software family encountered in Georgia in 4Q14 was [Win32/Couponruc](#), which was encountered by 3.6 percent of reporting computers there. [Win32/Couponruc](#) is a browser modifier that changes browser settings and may also modify some computer and Internet settings.
- The second most common unwanted software family encountered in Georgia in 4Q14 was [Win32/BetterSurf](#), which was encountered by 1.5 percent of reporting computers there. [Win32/BetterSurf](#) is adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.
- The third most common unwanted software family encountered in Georgia in 4Q14 was [Win32/Costmin](#), which was encountered by 1.0 percent of reporting computers there. [Win32/Costmin](#) is an adware family that installs itself as a browser extension for Internet Explorer, Mozilla Firefox, and Google Chrome, and displays advertisements as the user browses the Internet.

Top threat families by infection rate

The most common malware families by infection rate in Georgia in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	JS/Kilim	Trojans	7.0
2	Win32/Gamarue	Worms	6.0
3	Win32/Sality	Viruses	4.3
4	Win32/Brontok	Worms	3.8
5	Win32/Ramnit	Trojans	2.3
6	Win32/Jeefo	Viruses	2.0
7	Win32/Dorkbot	Worms	1.4
8	Win32/Helompy	Worms	1.4
9	Win32/Nuqel	Worms	1.4
10	Win32/Lethic	Trojans	0.8

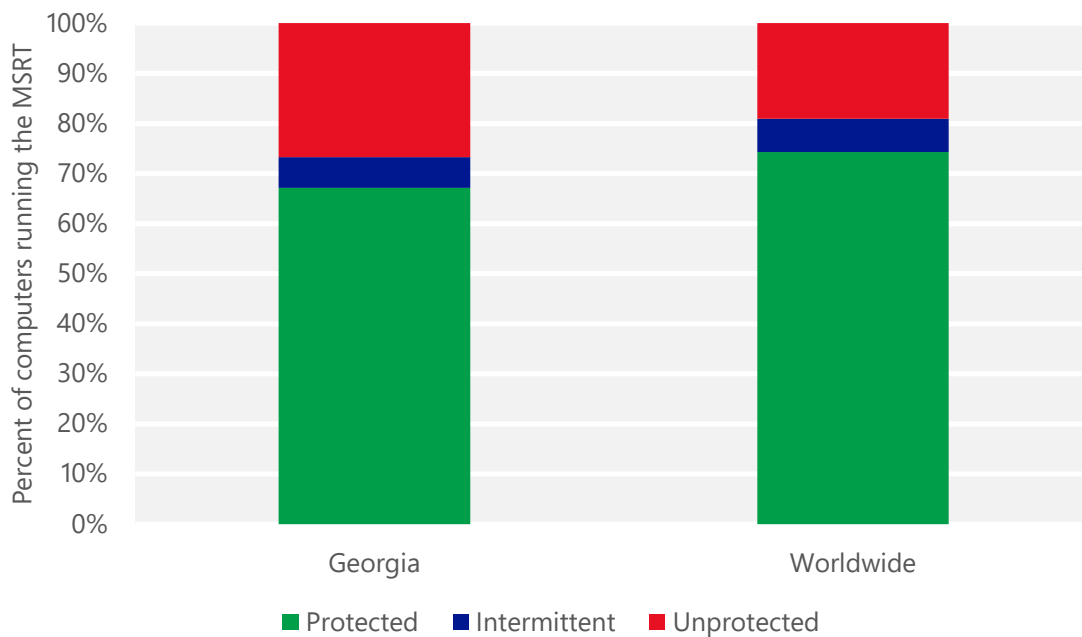
- The most common threat family infecting computers in Georgia in 4Q14 was [JS/Kilim](#), which was detected and removed from 7.0 of every 1,000 unique computers scanned by the MSRT. [JS/Kilim](#) is a trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
- The second most common threat family infecting computers in Georgia in 4Q14 was [Win32/Gamarue](#), which was detected and removed from 6.0 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 Georgia in 4Q14 was [Win32/Sality](#), which was detected and removed from 4.3 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 Georgia in 4Q14 was [Win32/Brontok](#), which was detected and removed from 3.8 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.

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 Georgia and worldwide protected by real-time security software in 4Q14



Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes the web, pages are assessed for malicious elements or malicious behavior. Clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software.

At the end of 3Q14, Bing detected 0.16 drive-by download URLs for every 1,000 URLs hosted in Georgia, compared to 0.41 worldwide. At the end of 4Q14, Bing detected 0.19 drive-by download URLs for every 1,000 URLs hosted in Georgia, compared to 0.45 worldwide.

Drive-by download pages per 1,000 URLs hosted in Georgia and worldwide

Metric	October 1, 2014	January 1, 2015
Drive-by download pages per 1,000 URLs, Georgia	0.16	0.19
<i>Drive-by download pages per 1,000 URLs worldwide</i>	<i>0.41</i>	<i>0.45</i>



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