Microsoft

Microsoft Security Intelligence Report

Volume 22 | January through March, 2017

Russia

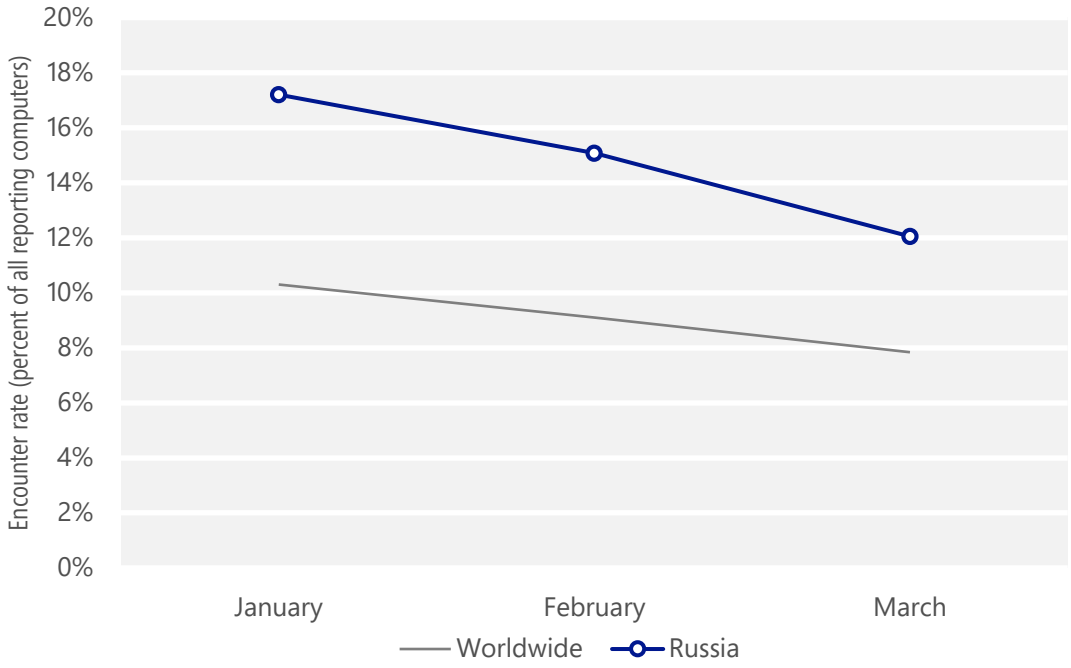
Russia

The statistics presented here are generated by Microsoft security programs and services running on computers in Russia in March 2017 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.

Encounter rate trends

In March 2017, 12.0 percent of computers in Russia encountered malware, compared to the March 2017 worldwide encounter rate of 7.8 percent. The following figure shows the encounter and infection rate trends for Russia over the last three months, compared to the world as a whole.

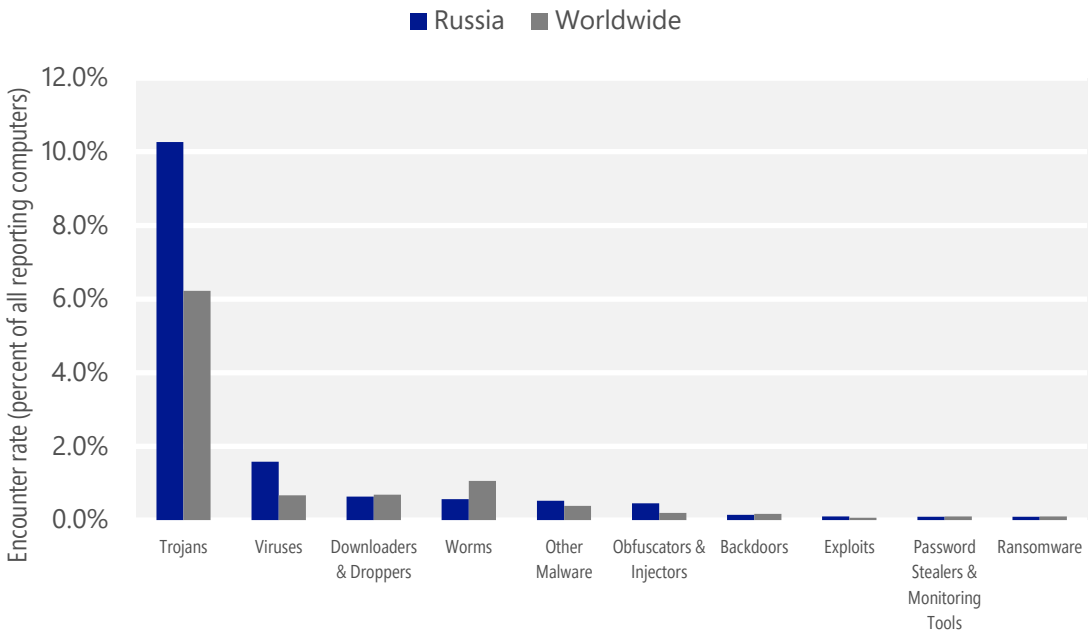
Malware encounter rate trends in Russia and worldwide



See the full report at http://www.microsoft.com/sir for more information about threats in Russia and around the world, and for explanations of the methods and terms used here.

Malicious software categories

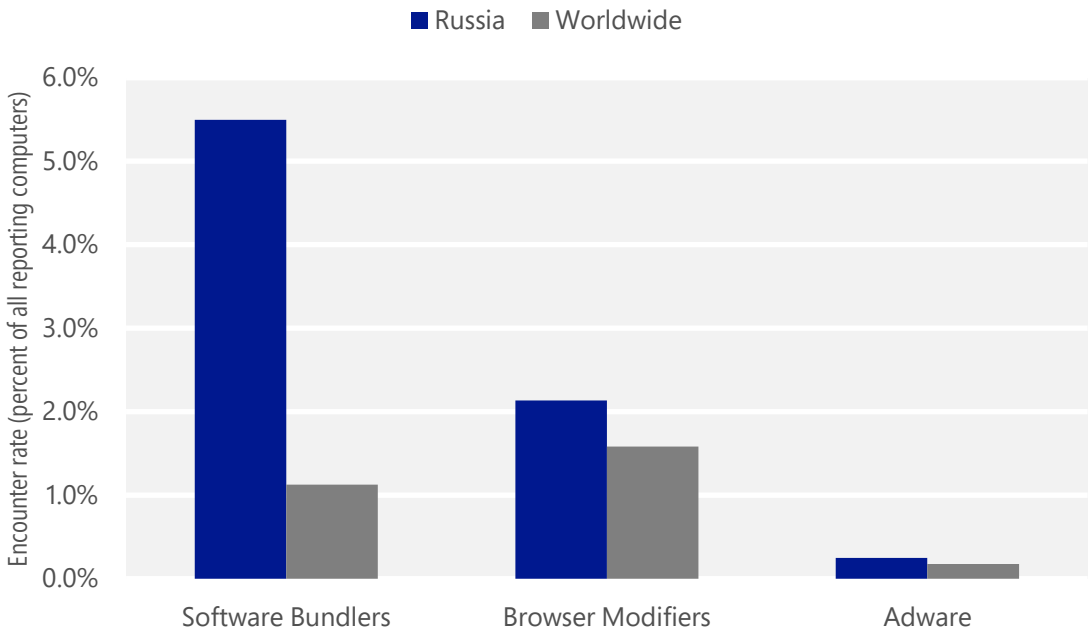
Malicious software encountered in Russia in March 2017, by category



- The most common malicious software category in Russia in March 2017 was Trojans. It was encountered by 10.26 percent of all computers there, down from 10.58 percent in February 2017.
- The second most common malicious software category in Russia in March 2017 was Viruses. It was encountered by 1.59 percent of all computers there, down from 1.60 percent in February 2017.
- The third most common malicious software category in Russia in March 2017 was Downloaders & Droppers, which was encountered by 0.64 percent of all computers there, down from 0.82 percent in February 2017.

Unwanted software categories

Unwanted software encountered in Russia in March 2017, by category



- The most common unwanted software category in Russia in March 2017 was Software Bundlers. It was encountered by 5.49 percent of all computers there, down from 5.51 percent in February 2017.
- The second most common unwanted software category in Russia in March 2017 was Browser Modifiers. It was encountered by 2.14 percent of all computers there, down from 2.61 percent in February 2017.
- The third most common unwanted software category in Russia in March 2017 was Adware, which was encountered by 0.25 percent of all computers there, down from 0.34 percent in February 2017.

Top malicious software families by encounter rate

The most common malicious software families encountered in Russia in March 2017

	Family	Most significant category	% of reporting computers
1	Win32/Fuery	Trojans	1.31%
2	Win32/Skeeyah	Trojans	1.12%
3	Win32/Spursint	Trojans	1.09%
4	Win32/Vigorf	Trojans	1.04%
5	Win32/Dynamer	Trojans	0.72%
6	Win32/Mupad	Trojans	0.62%
7	Win32/Rundas	Trojans	0.57%
8	Win32/Swrort	Trojans	0.44%
9	Win32/Neshta	Viruses	0.32%
10	Win32/Obfuscator	Obfuscators & Injectors	0.31%

- The most common malicious software family encountered in Russia in March 2017 was Win32/Fuery, which was encountered by 1.31 percent of reporting computers there. Win32/Fuery is a cloud-based detection for files that have been automatically identified as malicious by the cloud-based protection feature of Windows Defender.
- The second most common malicious software family encountered in Russia in March 2017 was Win32/Skeeyah, which was encountered by 1.12 percent of reporting computers there. Win32/Skeeyah is a generic detection for various threats that display trojan characteristics.
- The third most common malicious software family encountered in Russia in March 2017 was Win32/Spursint, which was encountered by 1.09 percent of reporting computers there. Win32/Spursint is a cloud-based detection for files that have been automatically identified as malicious by the cloud-based protection feature of Windows Defender.
- The fourth most common malicious software family encountered in Russia in March 2017 was Win32/Vigorf, which was encountered by 1.04 percent of reporting computers there. Win32/Vigorf is a generic detection for a variety of threats.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Russia in March 2017

	Family	Most significant category	% of reporting computers
1	Win32/FileTour	Software Bundlers	1.85%
2	Win32/Ogimant	Software Bundlers	1.26%
3	Win32/DLHelper	Software Bundlers	0.90%
4	Win32/Foxiebro	Browser Modifiers	0.67%
5	Win32/ICLoader	Software Bundlers	0.45%

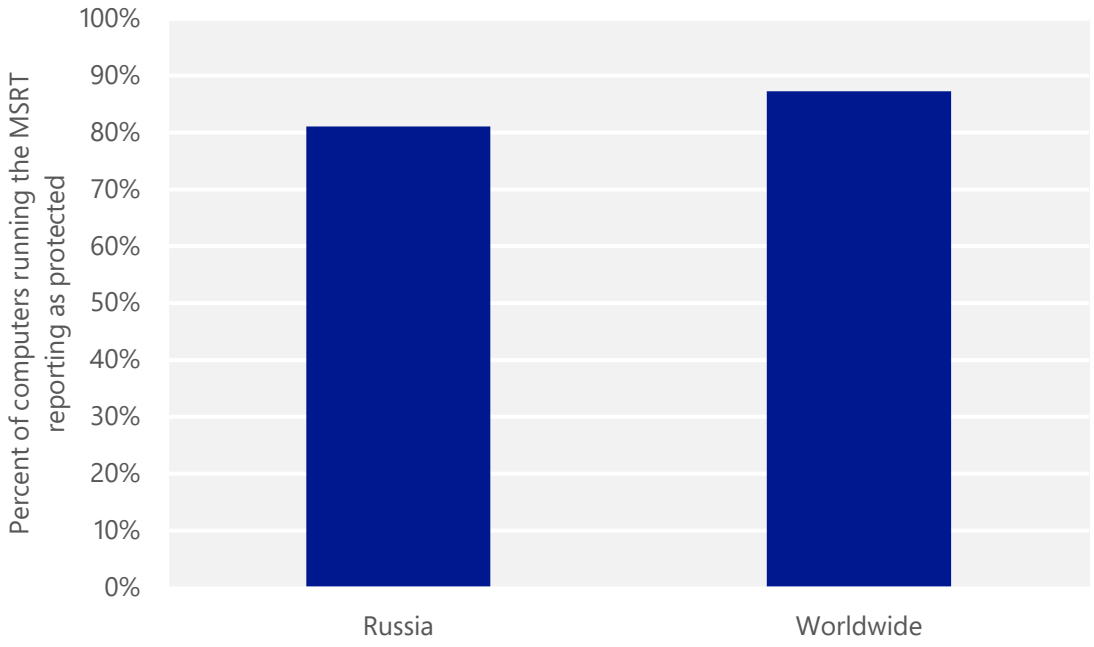
- The most common unwanted software family encountered in Russia in March 2017 was Win32/FileTour, which was encountered by 1.85 percent of reporting computers there. Win32/FileTour is a software bundler that may offer to download torrent files. It installs unwanted software on the computer, sometimes including web browsers and mail programs.
- The second most common unwanted software family encountered in Russia in March 2017 was Win32/Ogimant, which was encountered by 1.26 percent of reporting computers there. Win32/Ogimant is a threat that claims to help download items from the Internet, but actually downloads and runs files that are specified by a remote attacker.
- The third most common unwanted software family encountered in Russia in March 2017 was Win32/DLHelper, which was encountered by 0.90 percent of reporting computers there. Win32/DLHelper is a software bundler that is often distributed as a mountable .iso disk file. It installs unwanted software alongside the desired applications, including Win32/Pokavampo.

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 Russia that the MSRT found to be running up-to-date real-time security software in March 2017.

Percent of computers in Russia and worldwide protected by real-time security software in March 2017



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 Windows Defender SmartScreen in Microsoft Edge and Internet Explorer. See the Malicious Websites section of *Microsoft Security Intelligence Report, Volume 22* for more information about these protections and how the data is collected.

Malicious website statistics for Russia

Metric	Russia	Worldwide
Drive-by download pages per 1,000 URLs	0.59	0.17
Phishing sites per 1,000 Internet hosts	6.0	6.3
Malware hosting sites per 1,000 Internet hosts	13.9	14.8

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