

Microsoft Security Intelligence Report

Volume 21 | January through June, 2016

Italy

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.

Italy

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

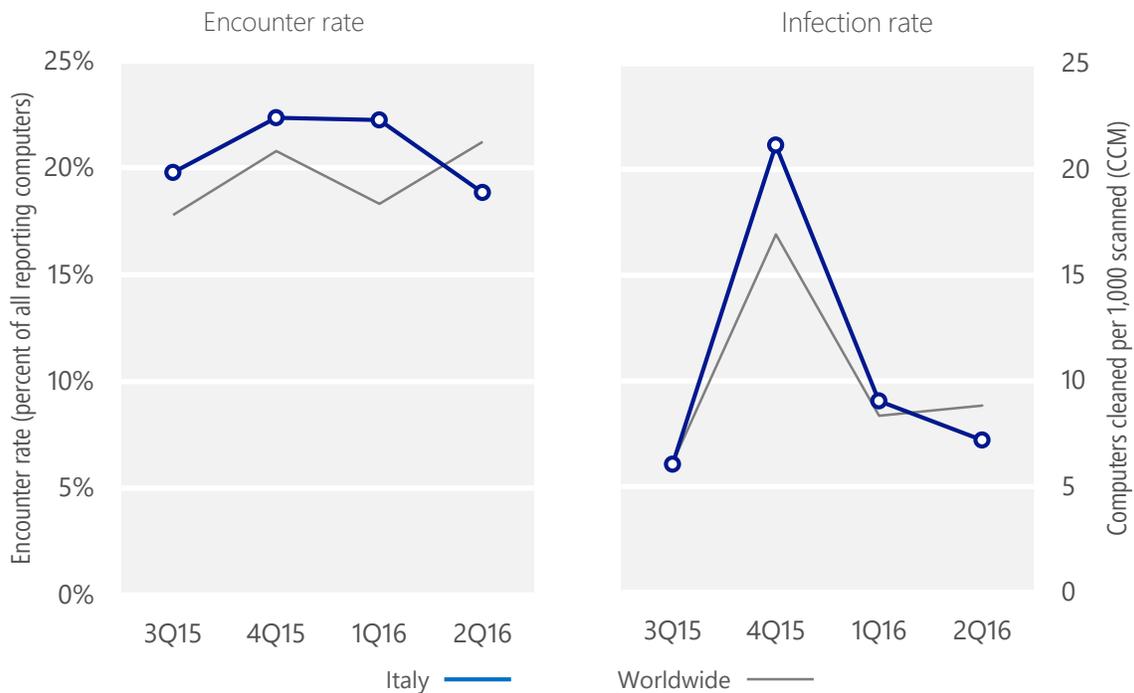
Infection rate statistics for Italy

Metric	3Q15	4Q15	1Q16	2Q16
Encounter rate, Italy	19.8%	22.3%	22.2%	18.8%
<i>Worldwide encounter rate</i>	<i>17.8%</i>	<i>20.8%</i>	<i>18.3%</i>	<i>21.2%</i>
CCM, Italy	6.1	21.1	9.1	7.2
<i>Worldwide CCM</i>	<i>6.1</i>	<i>16.9</i>	<i>8.4</i>	<i>8.8</i>

Encounter and infection rate trends

In 2Q16, 18.8% of computers in Italy encountered malware, compared to the 2Q16 worldwide encounter rate of 20.8 percent. In addition, the MSRT detected and removed malware from 7.2 of every 1,000 unique computers scanned in Italy in 2Q16 (a CCM score of 7.2, compared to the 2Q16 worldwide CCM of 16.9). The following figure shows the encounter and infection rate trends for Italy over the last four quarters, compared to the world as a whole.

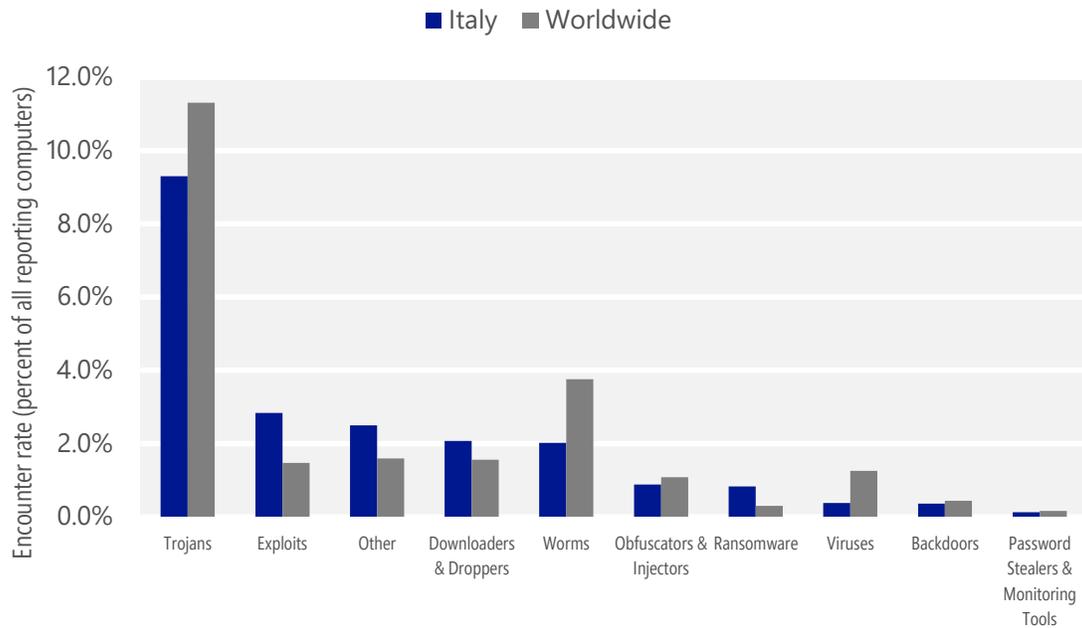
Malware encounter and infection rate trends in Italy and worldwide



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

Malicious software categories

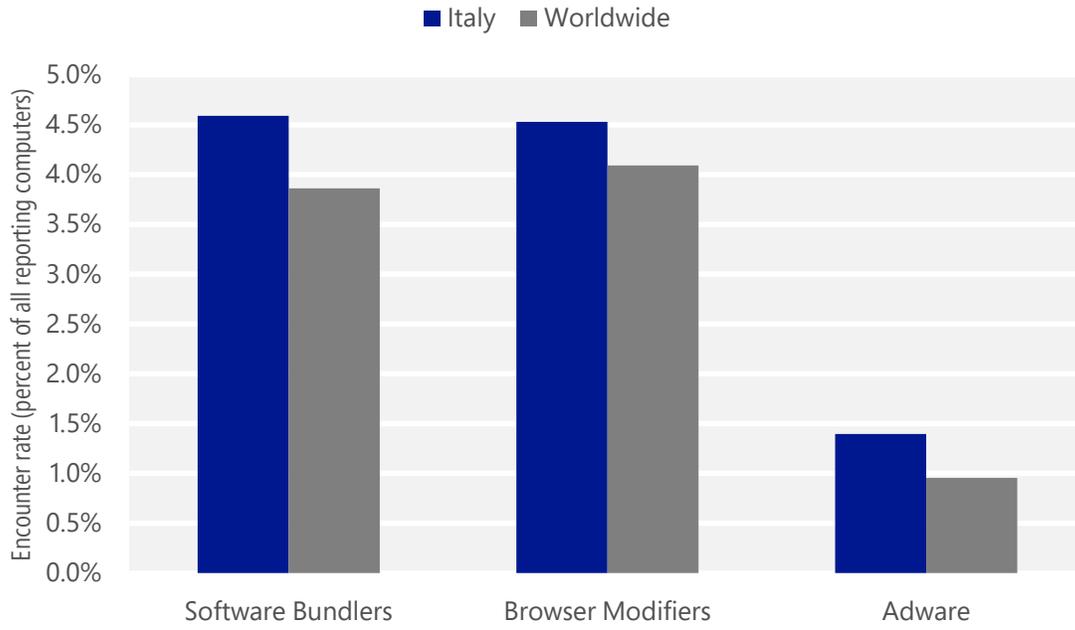
Malicious software encountered in Italy in 2Q16, by category



- The most common malicious software category in Italy in 2Q16 was Trojans. It was encountered by 9.3 percent of all computers there, down from 9.8 percent in 1Q16.
- The second most common malicious software category in Italy in 2Q16 was Exploits. It was encountered by 2.8 percent of all computers there, down from 3.9 percent in 1Q16.
- The third most common malicious software category in Italy in 2Q16 was Downloaders & Droppers, which was encountered by 2.1 percent of all computers there, down from 2.9 percent in 1Q16.

Unwanted software categories

Unwanted software encountered in Italy in 2Q16, by category



- The most common unwanted software category in Italy in 2Q16 was Software Bundlers. It was encountered by 4.6 percent of all computers there, down from 7.5 percent in 1Q16.
- The second most common unwanted software category in Italy in 2Q16 was Browser Modifiers. It was encountered by 4.5 percent of all computers there, down from 6.1 percent in 1Q16.
- The third most common unwanted software category in Italy in 2Q16 was Adware, which was encountered by 1.4 percent of all computers there, down from 1.4 percent in 1Q16.

Top malicious software families by encounter rate

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

	Family	Most significant category	% of reporting computers
1	JS/Axpergle	Exploits	1.7%
2	Win32/Dynamer	Trojans	1.2%
3	Win32/Xadupi	Trojans	0.9%
4	Win32/Skeeyah	Trojans	0.8%
5	Win32/Wpakill	Other Malware	0.8%
6	Win32/Peals	Trojans	0.7%
7	Win32/Spursint	Trojans	0.6%
8	ASX/Wimad	Downloaders & Droppers	0.5%
9	JS/NeutrinoEK	Exploits	0.5%
10	INF/Autorun	Obfuscators & Injectors	0.5%

- The most common malicious software family encountered in Italy in 2Q16 was [JS/Axpergle](#), which was encountered by 1.7 percent of reporting computers there. [JS/Axpergle](#) is a detection for the Angler exploit kit, which exploits vulnerabilities in some versions of Internet Explorer, Silverlight, Adobe Flash Player, and Java to install malware.
- The second most common malicious software family encountered in Italy in 2Q16 was [Win32/Dynamer](#), which was encountered by 1.2 percent of reporting computers there. [Win32/Dynamer](#) is a generic detection for a variety of threats.
- The third most common malicious software family encountered in Italy in 2Q16 was [Win32/Xadupi](#), which was encountered by 0.9 percent of reporting computers there. [Win32/Xadupi](#) is a trojan that poses as a useful application, usually called WinZipper or QKSee, but can silently download and install other malware. It is often installed silently by the browser modifiers Win32/Sasquor and Win32/SupTab.
- The fourth most common malicious software family encountered in Italy in 2Q16 was [Win32/Skeeyah](#), which was encountered by 0.8 percent of reporting computers there. [Win32/Skeeyah](#) is a generic detection for various threats that display trojan characteristics.

Top unwanted software families by encounter rate

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

	Family	Most significant category	% of reporting computers
1	Win32/SupTab	Browser Modifiers	1.2%
2	Win32/Mizenota	Software Bundlers	1.1%
3	Win32/Stallmonitz	Software Bundlers	1.0%
4	Win32/Sasquor	Browser Modifiers	1.0%
5	Win32/Diplugem	Browser Modifiers	0.7%

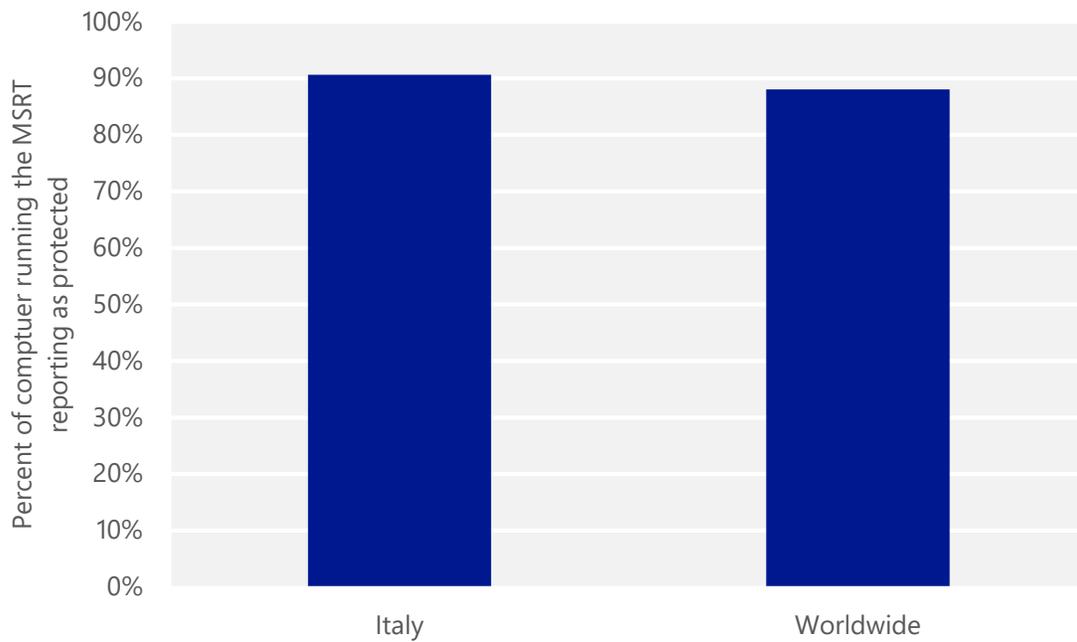
- The most common unwanted software family encountered in Italy in 2Q16 was [Win32/SupTab](#), which was encountered by 1.2 percent of reporting computers there. [Win32/SupTab](#) is a browser modifier that installs itself and changes the browser's default search provider, without obtaining the user's consent for either action.
- The second most common unwanted software family encountered in Italy 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/Sasquor](#), [Win32/Smudplu](#), and others.
- The third most common unwanted software family encountered in Italy in 2Q16 was [Win32/Stallmonitz](#), which was encountered by 1.0 percent of reporting computers there. [Win32/Stallmonitz](#) is a software bundler that installs unwanted software, typically [Win32/InstallMonitizer](#), along with the program desired by the user.

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 Italy that the MSRT found to be running up-to-date real-time security software in 2Q16.

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



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 21](#) for more information about these protections and how the data is collected.

Malicious website statistics for Italy

Metric	1Q16	2Q16
Drive-by download pages per 1,000 URLs (Worldwide)	0.23 (0.38)	0.32 (0.55)
Phishing sites per 1,000 Internet hosts (Worldwide)	6.95 (6.2)	7.44 (6.2)
Malware hosting sites per 1,000 Internet hosts (Worldwide)	14.79 (21.5)	18.68 (27.7)



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