Microsoft

Microsoft Security Intelligence Report

Volume 21 | January through June, 2016

Germany

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.

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

Germany

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

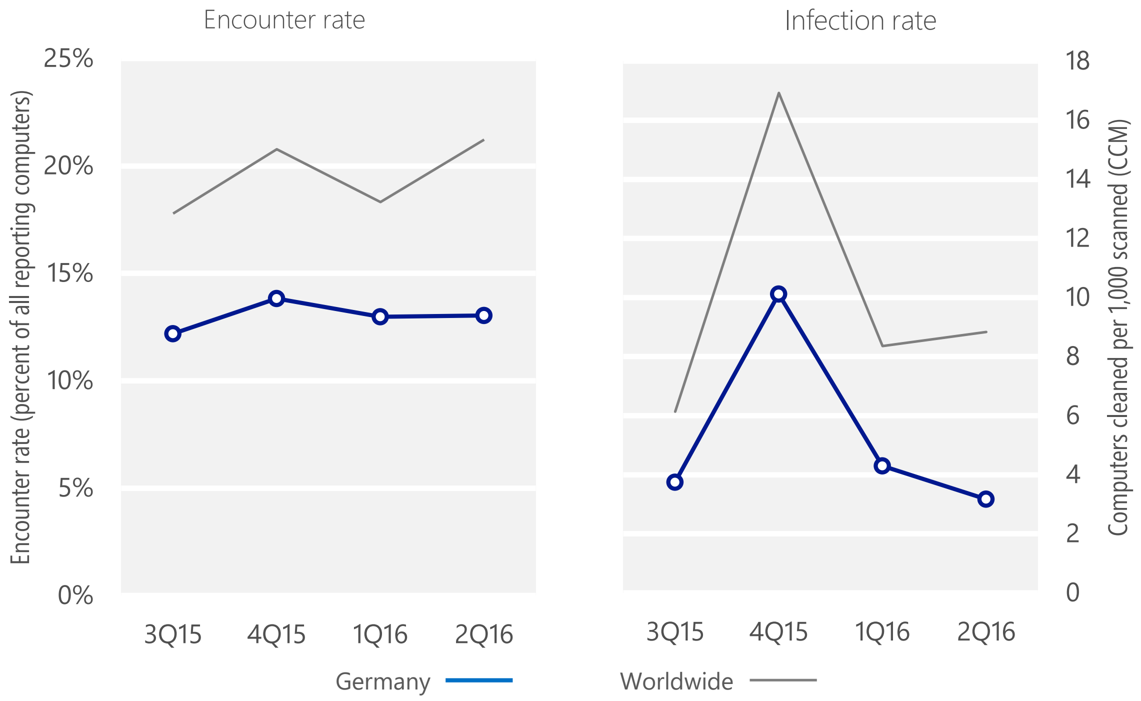
Infection rate statistics for Germany

Metric	3Q15	4Q15	1Q16	2Q16
Encounter rate, Germany	12.2%	13.8%	13.0%	13.0%
Worldwide encounter rate	*17.8%*	*20.8%*	*18.3%*	*21.2%*
CCM, Germany	3.7	10.1	4.3	3.2
Worldwide CCM	*6.1*	*16.9*	*8.4*	*8.8*

Encounter and infection rate trends

In 2Q16, 13.0% of computers in Germany encountered malware, compared to the 2Q16 worldwide encounter rate of 20.8 percent. In addition, the MSRT detected and removed malware from 3.2 of every 1,000 unique computers scanned in Germany in 2Q16 (a CCM score of 3.2, compared to the 2Q16 worldwide CCM of 16.9). The following figure shows the encounter and infection rate trends for Germany over the last four quarters, compared to the world as a whole.

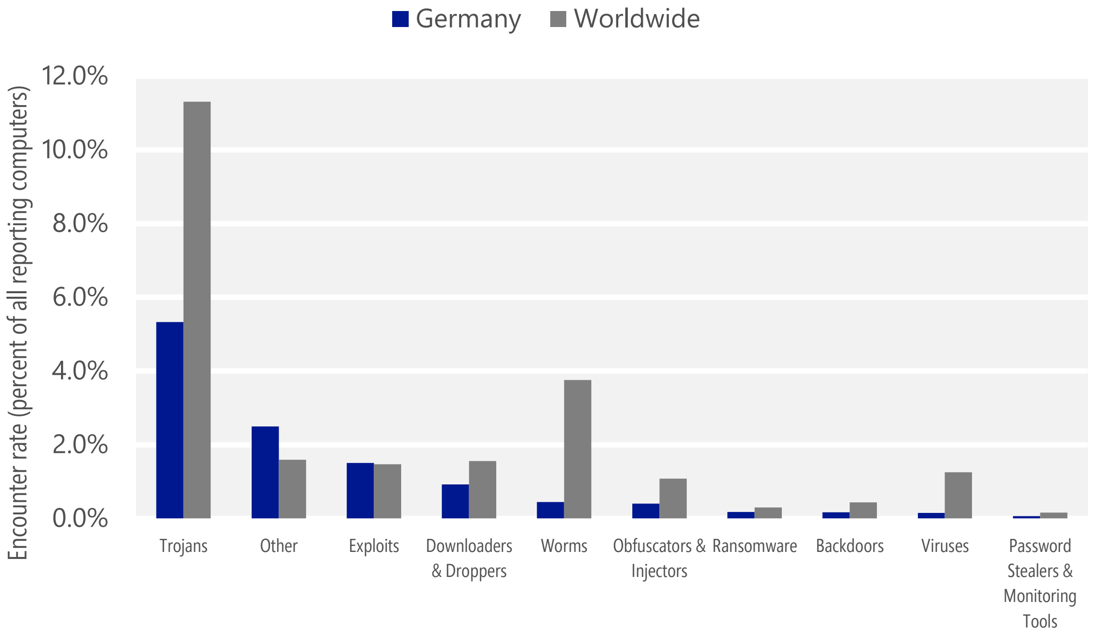
Malware encounter and infection rate trends in Germany and worldwide



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

Malicious software categories

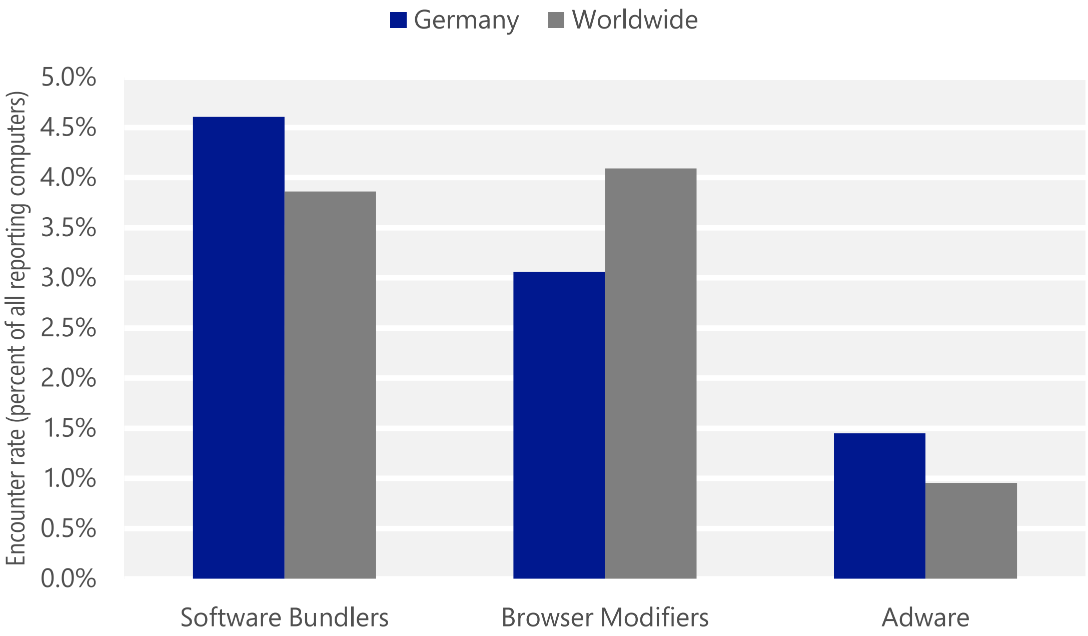
Malicious software encountered in Germany in 2Q16, by category



- The most common malicious software category in Germany in 2Q16 was Trojans. It was encountered by 5.3 percent of all computers there, down from 5.4 percent in 1Q16.
- The second most common malicious software category in Germany in 2Q16 was Exploits. It was encountered by 1.5 percent of all computers there, down from 1.5 percent in 1Q16.
- The third most common malicious software category in Germany in 2Q16 was Downloaders & Droppers, which was encountered by 0.9 percent of all computers there, down from 1.4 percent in 1Q16.

Unwanted software categories

Unwanted software encountered in Germany in 2Q16, by category



- The most common unwanted software category in Germany in 2Q16 was Software Bundlers. It was encountered by 4.6 percent of all computers there, up from 4.3 percent in 1Q16.
- The second most common unwanted software category in Germany in 2Q16 was Browser Modifiers. It was encountered by 3.1 percent of all computers there, down from 3.7 percent in 1Q16.
- The third most common unwanted software category in Germany in 2Q16 was Adware, which was encountered by 1.5 percent of all computers there, up from 1.0 percent in 1Q16.

Top malicious software families by encounter rate

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

	Family	Most significant category	% of reporting computers
1	JS/Axpergle	Exploits	0.8%
2	Win32/Xadupi	Trojans	0.6%
3	Win32/Dynamer	Trojans	0.5%
4	Win32/Skeeyah	Trojans	0.4%
5	Win32/Spursint	Trojans	0.3%
6	Win32/Peals	Trojans	0.3%
7	Win32/Rundas	Trojans	0.3%
8	JS/NeutrinoEK	Exploits	0.3%
9	Win32/Obfuscator	Obfuscators & Injectors	0.2%
10	JS/Nemucod	Downloaders & Droppers	0.2%

- The most common malicious software family encountered in Germany in 2Q16 was JS/Axpergle, which was encountered by 0.8 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 Germany in 2Q16 was Win32/Xadupi, which was encountered by 0.6 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 third most common malicious software family encountered in Germany in 2Q16 was Win32/Dynamer, which was encountered by 0.5 percent of reporting computers there. Win32/Dynamer is a generic detection for a variety of threats.
- The fourth most common malicious software family encountered in Germany in 2Q16 was Win32/Skeeyah, which was encountered by 0.4 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 Germany in 2Q16

	Family	Most significant category	% of reporting computers
1	Win32/Bervisec	Software Bundlers	2.0%
2	Win32/Sasquor	Browser Modifiers	0.8%
3	Win32/SupTab	Browser Modifiers	0.8%
4	Win32/Stallmonitz	Software Bundlers	0.8%
5	Win32/Adposhel	Adware	0.8%

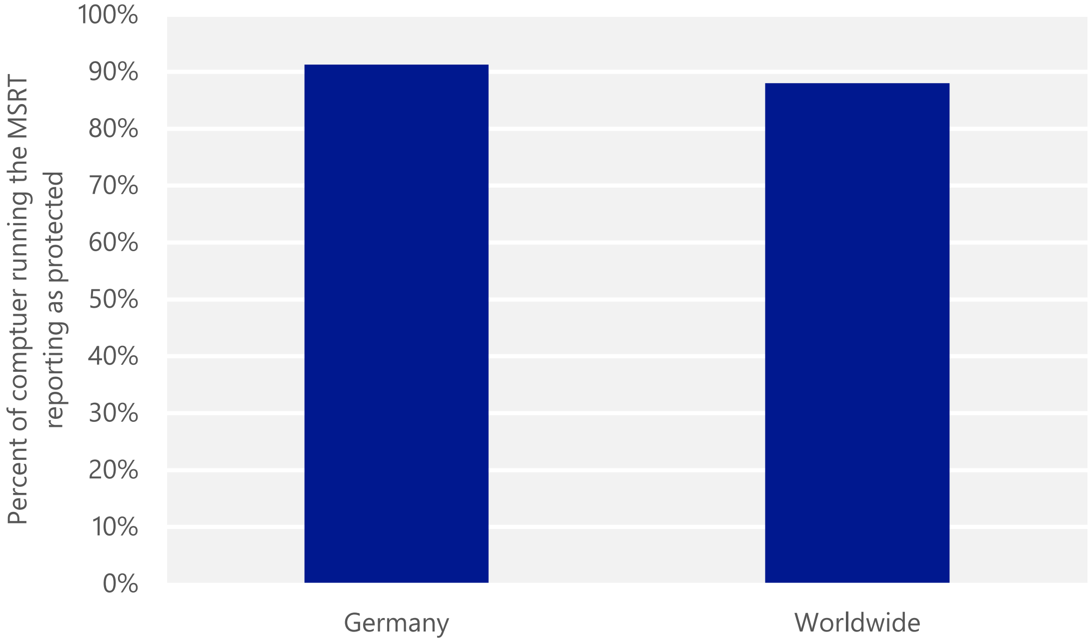
- The most common unwanted software family encountered in Germany in 2Q16 was Win32/Bervisec, which was encountered by 2.0 percent of reporting computers there. Win32/Bervisec is a software bundler that is typically distributed on German-language websites as an installer for legitimate applications. Some versions also install the browser modifier Win32/Sasquor.
- The second most common unwanted software family encountered in Germany in 2Q16 was Win32/Sasquor, which was encountered by 0.8 percent of reporting computers there. Win32/Sasquor is a browser modifier that modifies search and home page settings, and installs services and scheduled tasks to prevent the user from changing them back. It can also download additional malware, including Win32/SupTab and Win32/Xadupi.
- The third most common unwanted software family encountered in Germany in 2Q16 was Win32/SupTab, which was encountered by 0.8 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.

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

Percent of computers in Germany 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 Germany

Metric	1Q16	2Q16
Drive-by download pages per 1,000 URLs *(Worldwide)*	0.21 *(0.38)*	0.28 *(0.55)*
Phishing sites per 1,000 Internet hosts *(Worldwide)*	6.23 *(6.2)*	5.83 *(6.2)*
Malware hosting sites per 1,000 Internet hosts *(Worldwide)*	13.64 *(21.5)*	18.35 *(27.7)*

Microsoft

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