Microsoft Security Intelligence Report

Volume 18 | July through December, 2014

Bahrain

Microsoft

Bahrain

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

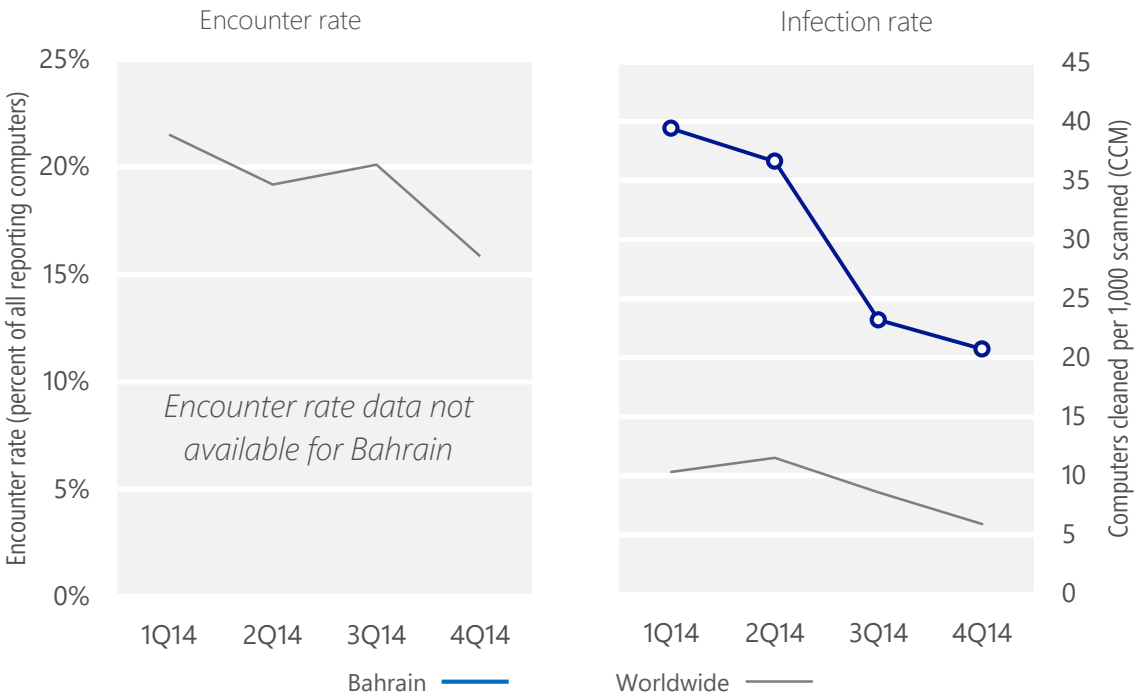
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Bahrain	N/A	N/A	N/A	N/A
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Bahrain	39.4	36.6	23.2	20.7
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

Encounter and infection rates reported here do not include totals for the Brantall, Filcout, 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, the MSRT detected and removed malware from 20.7 of every 1,000 unique computers scanned in Bahrain in 4Q14 (a CCM score of 20.7, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Bahrain over the last four quarters, compared to the world as a whole.

Malware encounter and infection rate trends in Bahrain 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 Bahrain 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 Bahrain in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	8.6
2	Win32/Sality	Viruses	2.4
3	Win32/Nuqel	Worms	2.4
4	MSIL/Bladabindi	Backdoors	1.6
5	Win32/Dorkbot	Worms	1.2
6	Win32/Gamarue	Worms	1.2
7	Win32/Ramnit	Trojans	1.0
8	Win32/Vobfus	Worms	0.4
9	Win32/Brontok	Worms	0.4
10	Win32/Zbot	Password Stealers & Monitoring Tools	0.4

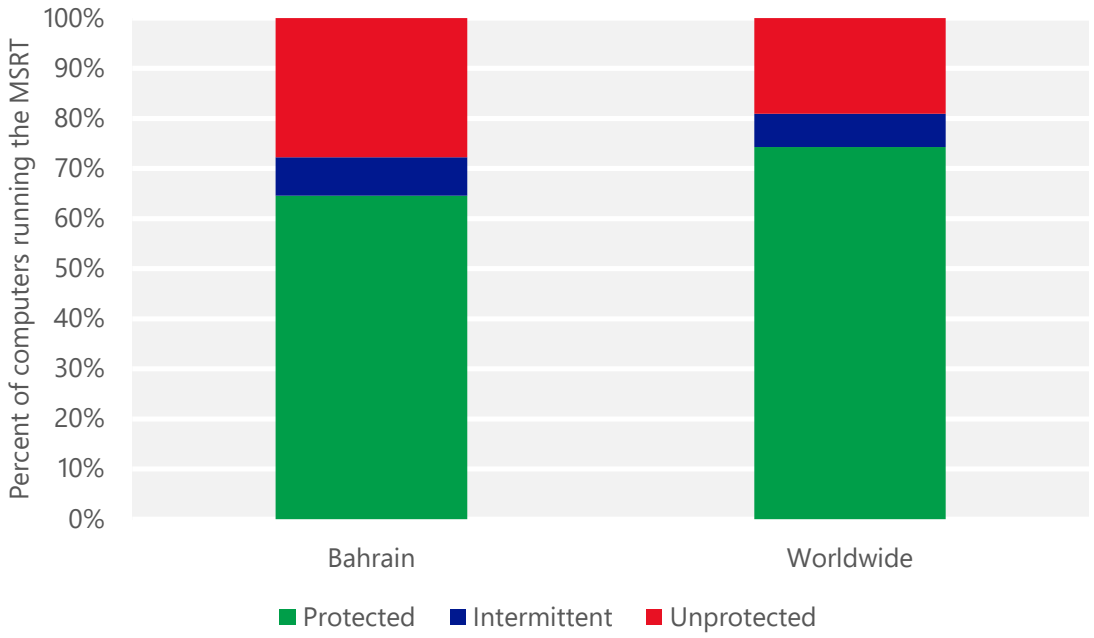
- The most common threat family infecting computers in Bahrain in 4Q14 was VBS/Jenxcus, which was detected and removed from 8.6 of every 1,000 unique computers scanned by the MSRT. VBS/Jenxcus is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Bahrain in 4Q14 was Win32/Sality, which was detected and removed from 2.4 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 third most common threat family infecting computers in Bahrain in 4Q14 was Win32/Nuqel, which was detected and removed from 2.4 of every 1,000 unique computers scanned by the MSRT. Win32/Nuqel is a worm that spreads via mapped drives and certain instant messaging applications. It may modify system settings, connect to certain websites, download arbitrary files, or take other malicious actions.
- The fourth most common threat family infecting computers in Bahrain in 4Q14 was MSIL/Bladabindi, which was detected and removed from 1.6 of every 1,000 unique computers scanned by the MSRT. MSIL/Bladabindi is a family of backdoors created by a malicious hacker tool called NJ Rat. The can steal sensitive information, download other malware, and allow backdoor access to an infected computer.

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



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