Microsoft Security Intelligence Report

Volume 18 | July through December, 2014

Iraq

Microsoft

Iraq

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

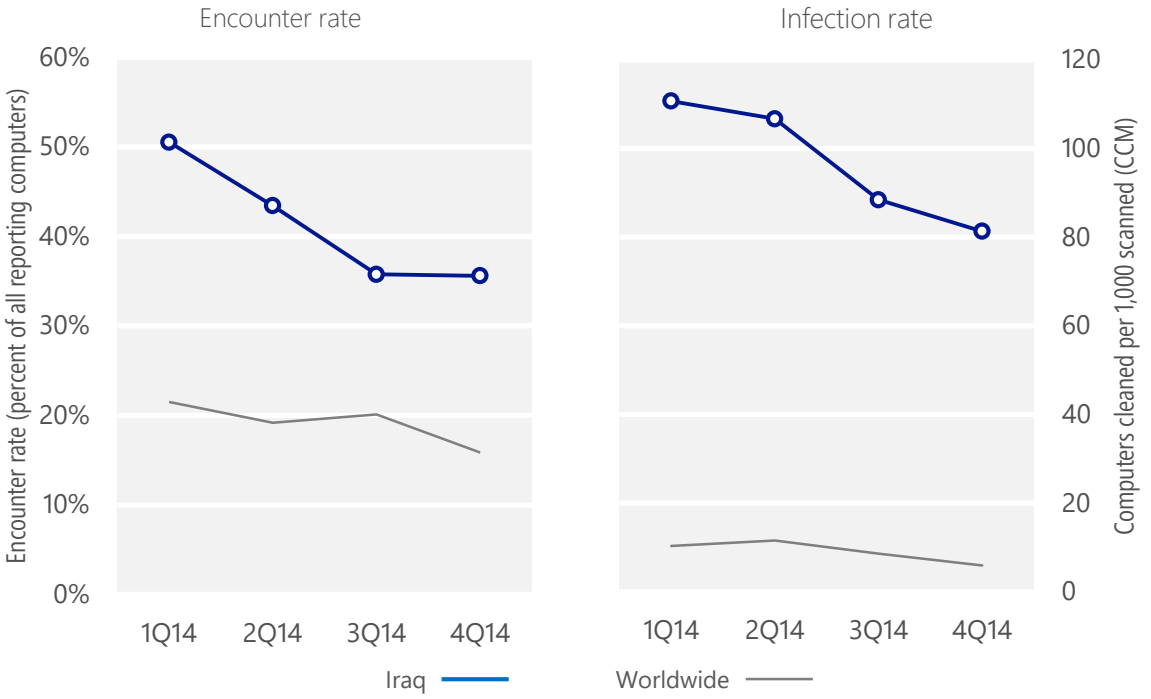
Metric	1Q14	2Q14	3Q14	4Q14
Encounter rate, Iraq	50.5%	43.4%	35.7%	35.6%
Worldwide encounter rate	*21.5%*	*19.2%*	*20.1%*	*15.9%*
CCM, Iraq	110.7	106.7	88.5	81.3
Worldwide CCM	*10.3*	*11.5*	*8.6*	*5.9*

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, 35.6% percent of computers in Iraq encountered malware, compared to the 4Q14 worldwide encounter rate of 15.9 percent. In addition, the MSRT detected and removed malware from 81.3 of every 1,000 unique computers scanned in Iraq in 4Q14 (a CCM score of 81.3, compared to the 4Q14 worldwide CCM of 5.9). The following figure shows the encounter and infection rate trends for Iraq over the last four quarters, compared to the world as a whole.

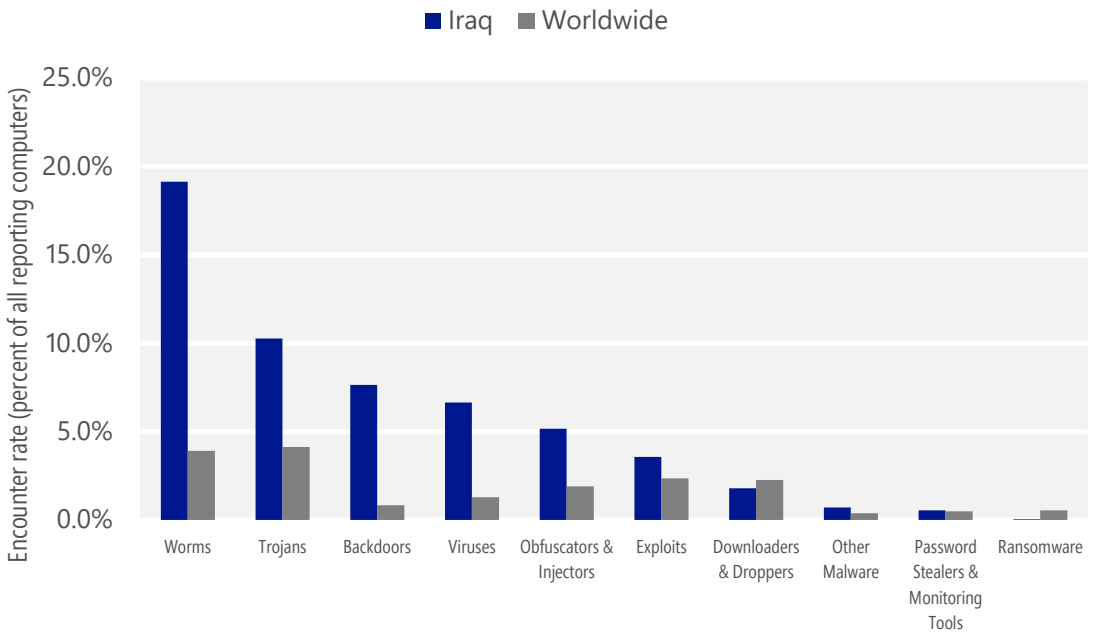
Malware encounter and infection rate trends in Iraq and worldwide



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

Malware categories

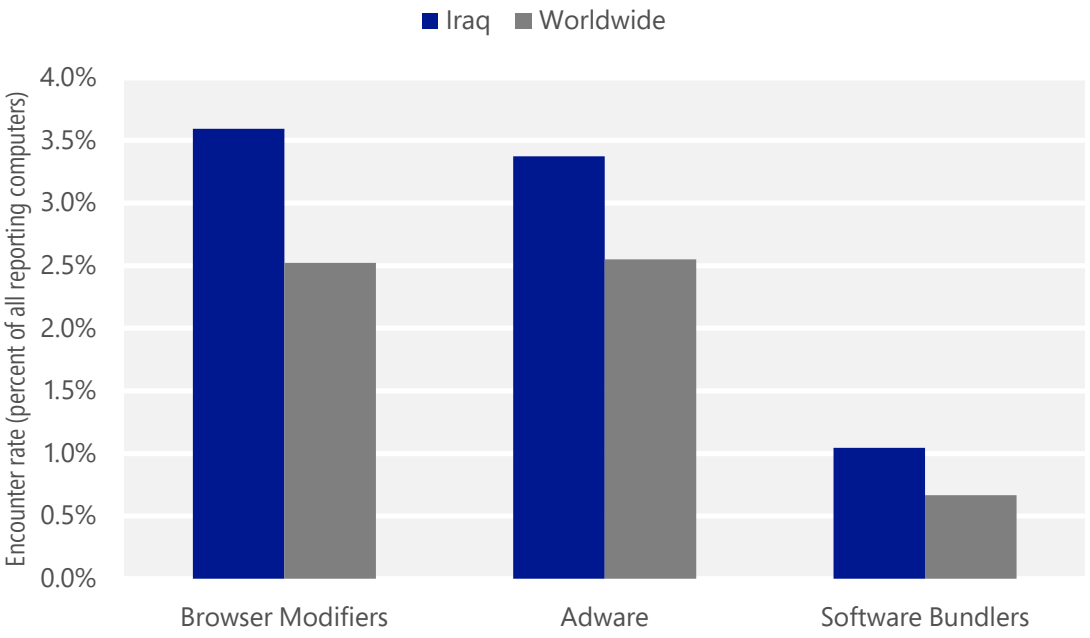
Malware encountered in Iraq in 4Q14, by category



- The most common malware category in Iraq in 4Q14 was Worms. It was encountered by 19.1 percent of all computers there, up from 17.6 percent in 3Q14.
- The second most common malware category in Iraq in 4Q14 was Trojans. It was encountered by 10.3 percent of all computers there, down from 11.6 percent in 3Q14.
- The third most common malware category in Iraq in 4Q14 was Backdoors, which was encountered by 7.6 percent of all computers there, down from 8.3 percent in 3Q14.

Unwanted software categories

Unwanted software encountered in Iraq in 4Q14, by category



- The most common unwanted software category in Iraq in 4Q14 was Browser Modifiers. It was encountered by 3.6 percent of all computers there, down from 4.8 percent in 3Q14.
- The second most common unwanted software category in Iraq in 4Q14 was Adware. It was encountered by 3.4 percent of all computers there, up from 1.0 percent in 3Q14.
- The third most common unwanted software category in Iraq 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 Iraq in 4Q14

	Family	Most significant category	% of reporting computers
1	VBS/Jenxcus	Worms	10.6%
2	INF/Autorun	Obfuscators & Injectors	7.4%
3	MSIL/Bladabindi	Backdoors	6.1%
4	Win32/Wecykler	Worms	4.5%
5	Win32/Sality	Viruses	3.5%
6	Win32/Ramnit	Trojans	3.0%
7	Win32/CplLnk	Exploits	3.0%
8	Win32/Gamarue	Worms	2.4%
9	Win32/Vermis	Worms	1.8%
10	Win32/Sulunch	Trojans	1.5%

- The most common malware family encountered in Iraq in 4Q14 was VBS/Jenxcus, which was encountered by 10.6 percent of reporting computers there. 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 malware family encountered in Iraq in 4Q14 was INF/Autorun, which was encountered by 7.4 percent of reporting computers there. INF/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The third most common malware family encountered in Iraq in 4Q14 was MSIL/Bladabindi, which was encountered by 6.1 percent of reporting computers there. 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.
- The fourth most common malware family encountered in Iraq in 4Q14 was Win32/Wecykler, which was encountered by 4.5 percent of reporting computers there. Win32/Wecykler is a family of worms that spread via removable drives, such as USB drives; they?may stop security processes and other processes on the computer, and log keystrokes which they later send to a remote attacker.

Top unwanted software families by encounter rate

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

	Family	Most significant category	% of reporting computers
1	Win32/Couponruc	Browser Modifiers	2.5%
2	Win32/Brya	Adware	1.4%
3	Win32/Defaulttab	Browser Modifiers	1.1%
4	Win32/BetterSurf	Adware	1.0%
5	Win32/Gofileexpress	Software Bundlers	0.8%

- The most common unwanted software family encountered in Iraq in 4Q14 was Win32/Couponruc, which was encountered by 2.5 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 Iraq in 4Q14 was Win32/Brya, which was encountered by 1.4 percent of reporting computers there. Win32/Brya is a program that shows ads that the user cannot control as they browse the web. It does not have a working uninstaller.
- The third most common unwanted software family encountered in Iraq in 4Q14 was Win32/Defaulttab, which was encountered by 1.1 percent of reporting computers there. Win32/Defaulttab is a browser modifier that redirects web browser searches and prevents the user from changing browser settings.

Top threat families by infection rate

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

	Family	Most significant category	Infection rate (CCM)
1	VBS/Jenxcus	Worms	25.1
2	Win32/Sality	Viruses	16.4
3	MSIL/Bladabindi	Backdoors	14.9
4	Win32/Wecykler	Worms	10.9
5	Win32/Ramnit	Trojans	7.8
6	Win32/Gamarue	Worms	4.1
7	Win32/Brontok	Worms	3.9
8	Win32/Dorkbot	Worms	2.8
9	Win32/Folstart	Worms	2.6
10	Win32/Nuqel	Worms	2.4

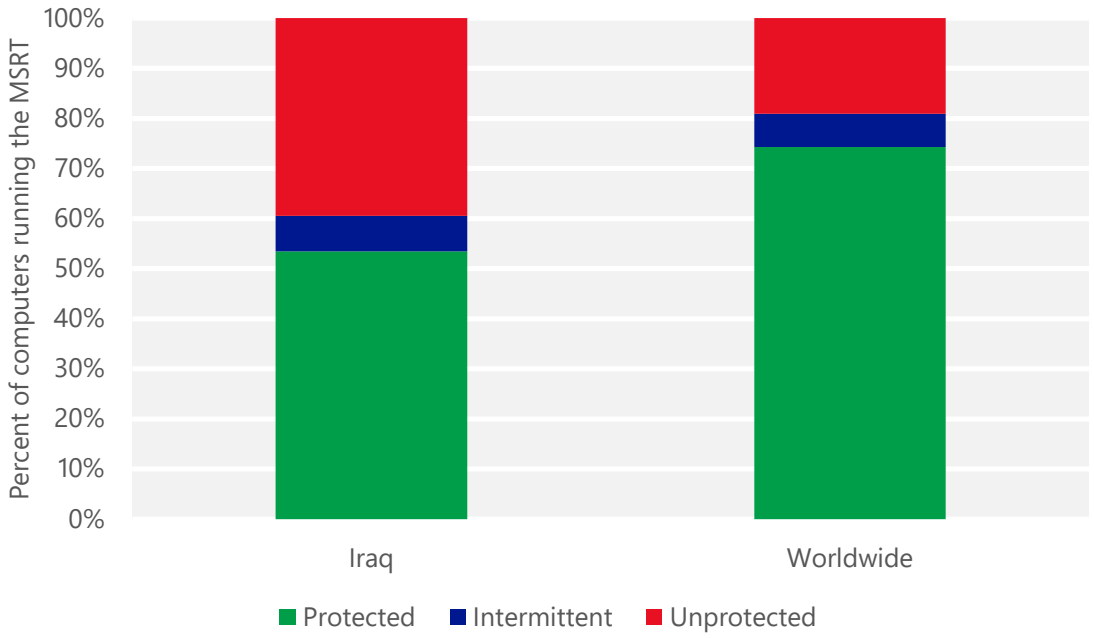
- The most common threat family infecting computers in Iraq in 4Q14 was VBS/Jenxcus, which was detected and removed from 25.1 of every 1,000 unique computers scanned by the MSRT. VBS/Jenxcus is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
- The second most common threat family infecting computers in Iraq in 4Q14 was Win32/Sality, which was detected and removed from 16.4 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 Iraq in 4Q14 was MSIL/Bladabindi, which was detected and removed from 14.9 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.
- The fourth most common threat family infecting computers in Iraq in 4Q14 was Win32/Wecykler, which was detected and removed from 10.9 of every 1,000 unique computers scanned by the MSRT. Win32/Wecykler is a family of worms that spread via removable drives, such as USB drives; they?may stop security processes and other processes on the computer, and log keystrokes which they later send to a remote attacker.

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



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