Microsoft Security Intelligence Report

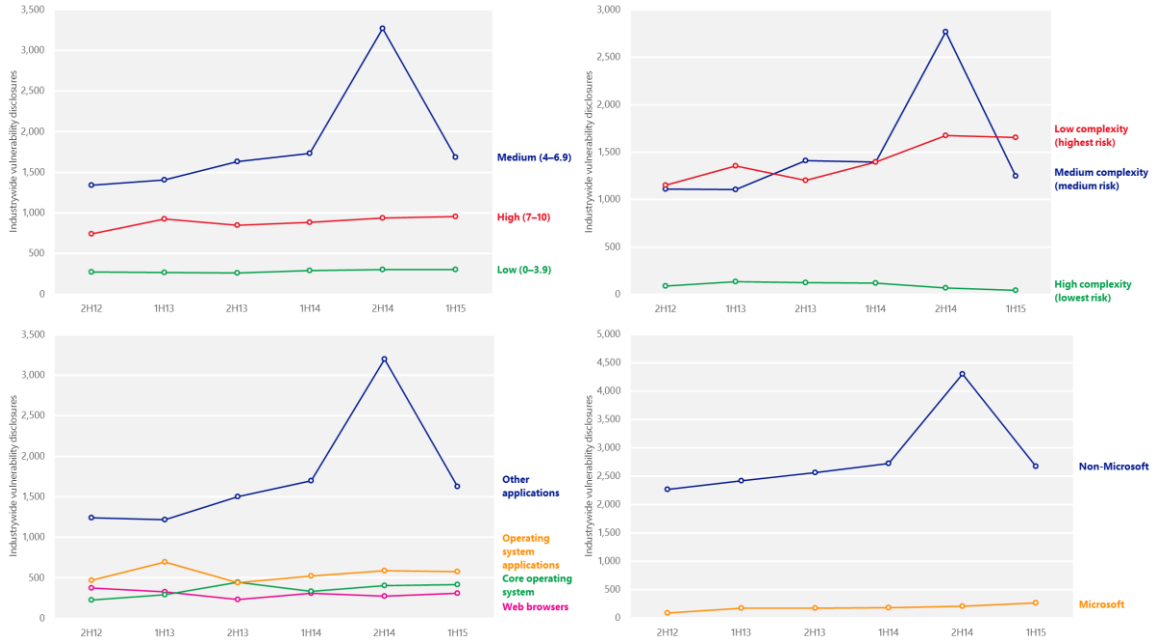
Volume 19 | January through June, 2015

Key Findings Summary

Vulnerabilities

After increasing significantly in 2H14 due to a CERT/CC research project involving SSL vulnerabilities in Android applications, vulnerability disclosures across the industry decreased 34.7 percent in 1H15 to just under 3,000, very close to the level seen a year previously in 1H14. [1]

Figure 1. Trends for vulnerability (CVE) severity, vulnerability complexity, disclosures by type, and disclosures for Microsoft and non-Microsoft products, across the entire software industry, 2H12–1H15

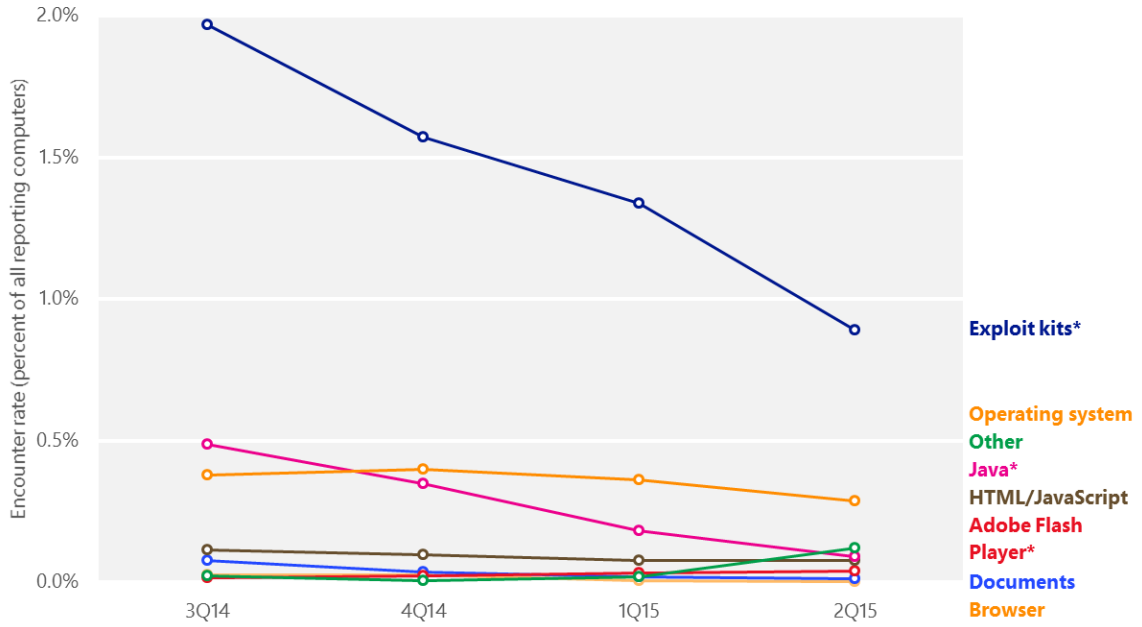


[1] Throughout the report, half-yearly and quarterly time periods are referenced using the *n*H*yy* or *n*Q*yy* formats, where *yy* indicates the calendar year and *n* indicates the half or quarter.

Exploits

Figure 2 shows the prevalence of different types of exploits detected by Microsoft antimalware products from 3Q14 to 2Q15, by encounter rate. *Encounter rate* is the percentage of computers running Microsoft real-time security products that report a malware encounter.

Figure 2. Encounter rates for different types of exploit attempts, 3Q14–2Q15



* Figures for exploit kits, Java, and Adobe Flash Player exploits are affected by IExtensionValidation in Internet Explorer, which blocks many threats before they are encountered. See the full report for more information.

- Computers that report more than one type of exploit are counted for each type detected.
- Encounters with exploit kits decreased by more than a third between 4Q14 and 1Q15, but remained the most commonly encountered type of exploit in

the second half of the year, with an encounter rate more than three times as high as the next most common type of exploit.

- The number of encounters with exploits that target operating systems remained mostly stable in 1H15, becoming the second-most commonly encountered type of exploits during the period.
- Encounters with Java exploits decreased each quarter, becoming the third-most commonly encountered type of exploit in 1H15.

Exploit families

Figure 3 lists the exploit-related malware families that were detected most often during the first half of 2015.

Figure 3. Quarterly encounter rate trends for the exploit families most commonly detected and blocked by Microsoft real-time antimalware products in 1H15, shaded according to relative prevalence

Exploit	Type	3Q14	4Q14	1Q15	2Q15
JS/Axpergle	Exploit kit	0.87%	0.86%	0.85%	0.64%
CVE-2010-2568 (CplLnk)	Operating system	0.35%	0.35%	0.30%	0.23%
JS/Fiexp	Exploit kit	0.31%	0.30%	0.21%	0.05%
Win32/Anogre	Exploit kit	0.60%	0.42%	0.22%	0.04%
JS/Neclu	Exploit kit	0.11%	0.06%	0.03%	0.14%
HTML/IframeRef	Generic	0.10%	0.09%	0.07%	0.05%
HTML/Meadgive	Exploit kit	0.15%	0.08%	0.06%	0.05%
JS/NeutrinoEK	Exploit kit	0.00%	0.01%	0.07%	0.04%
Win32/Sdbby	Other	—	—	0.00%	0.09%
CVE-2014-6332	Operating system	—	0.03%	0.04%	0.05%

Totals for individual vulnerabilities do not include exploits that were detected as part of exploit kits.

- Exploit kits accounted for six of the 10 most commonly encountered exploits during 1H15.

- Exploits targeting the Java Runtime Environment (JRE) have gone from seven of the top 10 individual exploits detected in 2H13 to none in 1H15. A number of changes that have been made to Java and Internet Explorer over the past two years have made it much more difficult for attackers to take advantage of Java-based vulnerabilities, which is the most likely explanation for this significant decrease.
- CVE-2010-2568, the most commonly targeted individual vulnerability in 1H15, is a vulnerability in Windows Shell. Detections are often identified as variants in the Win32/CplLnk family, although several other malware families attempt to exploit the vulnerability as well. An attacker exploits CVE-2010-2568 by creating a malformed shortcut file—typically distributed through social engineering or other methods—that forces a vulnerable computer to load a malicious file when the shortcut icon is displayed in Windows Explorer. Microsoft published Security Bulletin MS10-046 in August 2010 to address the issue.
- HTML/IframeRef is a generic detection for specially formed HTML inline frame (IFrame) tags that redirect to remote websites that contain malicious content. More properly considered exploit downloaders than true exploits, these malicious pages use a variety of techniques to exploit vulnerabilities in browsers and plug-ins. The only commonality is that the attacker uses an inline frame to deliver the exploits to users. The exact exploit delivered and detected by one of these inline frames might be changed frequently.
- CVE-2014-6332 is a vulnerability in Windows Object Linking and Embedding (OLE) that can be used to launch remote attacks on a computer through Internet Explorer in some circumstances. Microsoft released Security Bulletin MS14-064 in November 2014 to address this issue.

Malware and unwanted software

Microsoft uses two different metrics to measure malware and unwanted software prevalence:[2]

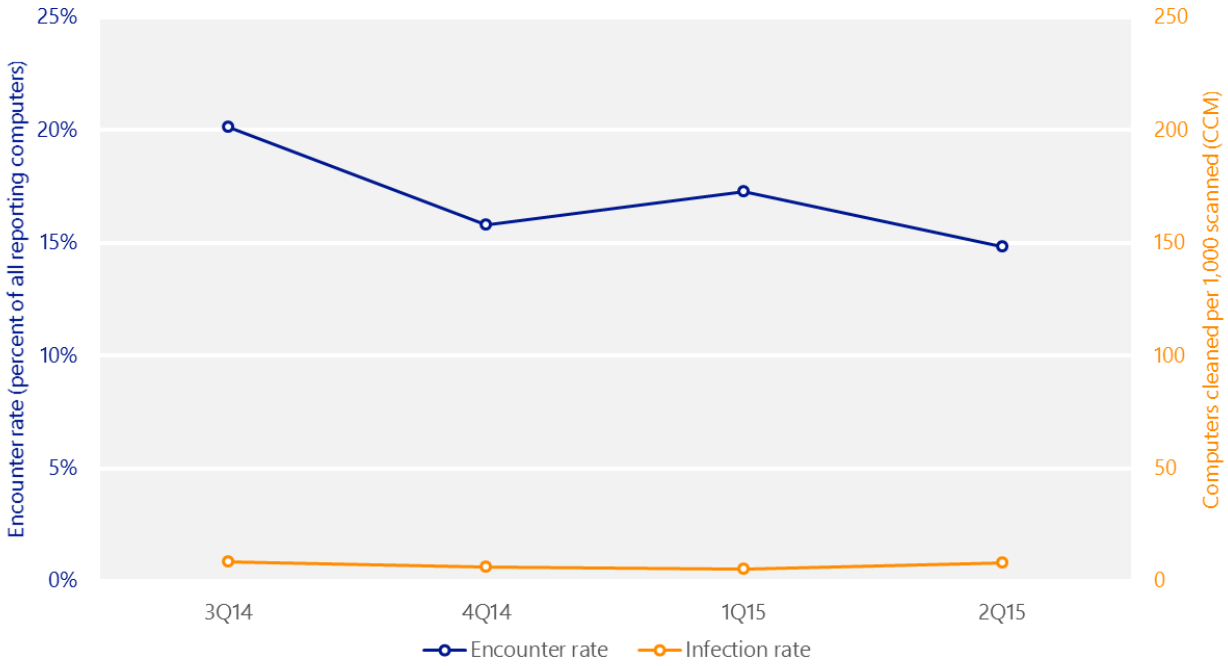
- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter.[3] Only computers whose users have opted in to provide data to Microsoft are considered when calculating encounter rates.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers that run 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. Because it is not a real-time tool, the MSRT only detects and removes threats that are already present on the computer; it does not block infection attempts as they happen.

Figure 4 illustrates the difference between these two metrics.

[2] Encounter and infection rate figures do not include the Brantall, Rotbrow, and Filcout families. See the full report for more information.

[3] Encounter rate does not include threats that are blocked by a web browser before being detected by antimalware software. In particular, IExtensionValidation in Internet Explorer 11 enables security software to block pages containing exploits from loading. (See the full report for more information.) For this reason, encounter rate figures may not fully reflect all of the threats encountered by computer users.

Figure 4. Worldwide encounter and infection rates, 2Q14–2Q15, by quarter

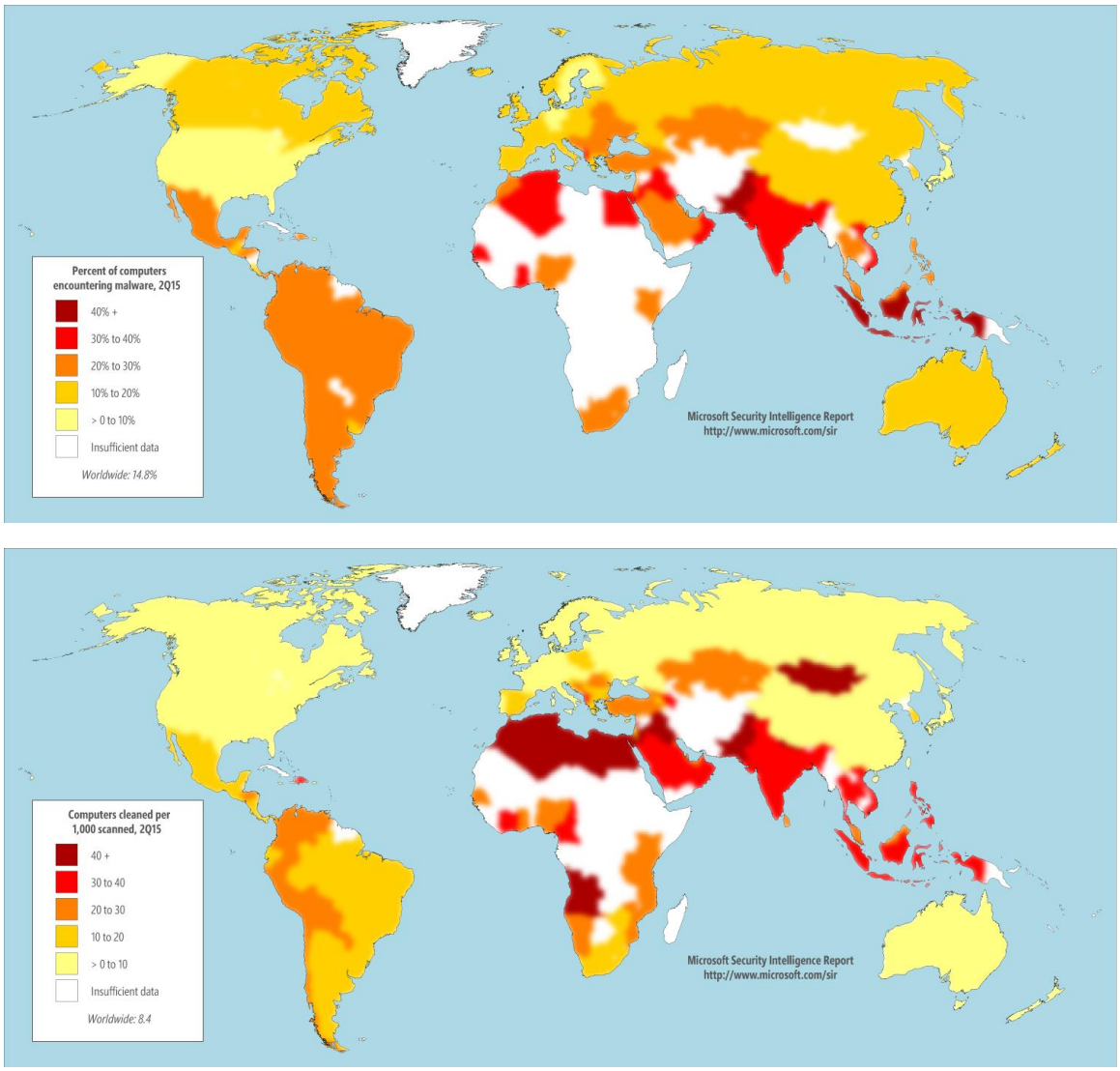


On average, about 17.0 percent of reporting computers worldwide encountered malware over the past four quarters. At the same time, the MSRT removed malware from about 7.1 out of every 1,000 computers, or 0.71 percent.

Malware and unwanted software worldwide

Figure 5 shows the infection and encounter rates in locations around the world in 2Q15.

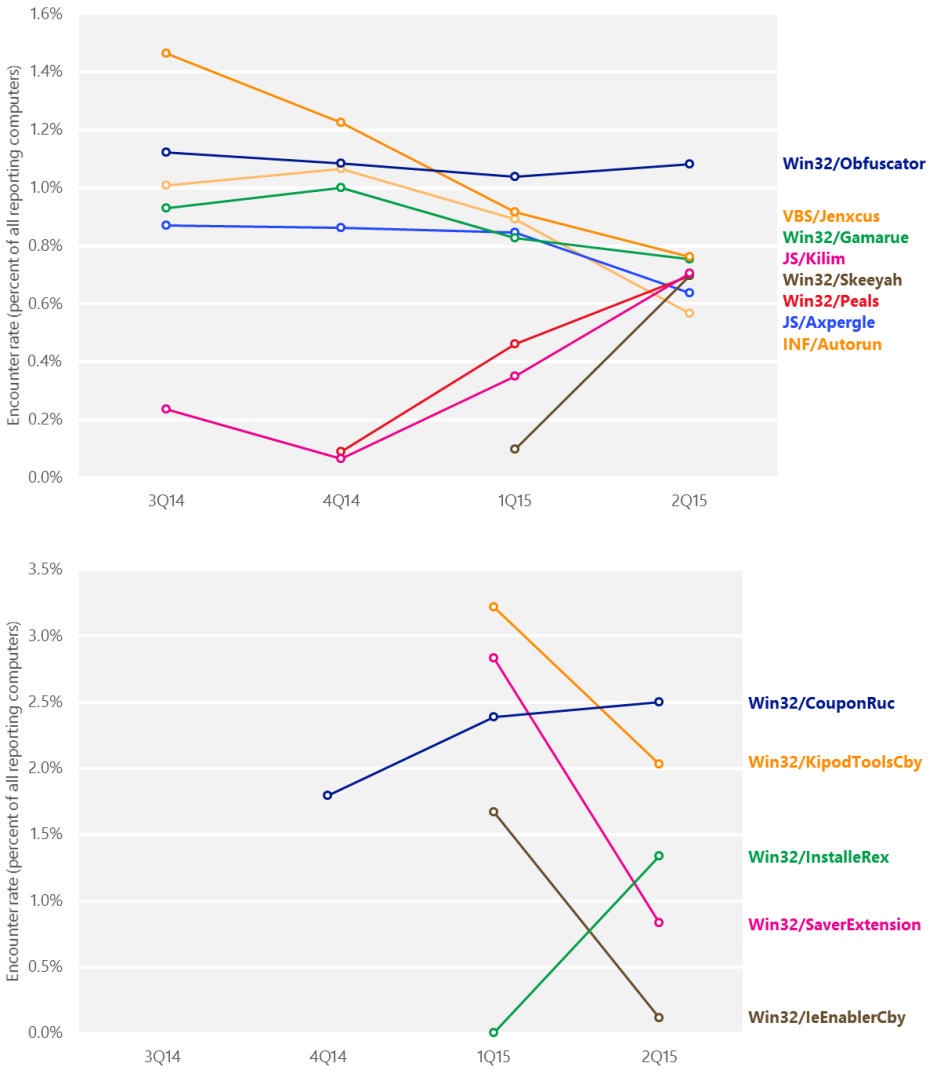
Figure 5. Encounter rates (top) and infection rates (bottom) by country/region in 2Q15



Threat families

Figure 6 shows trends for the top malware and unwanted software families that were detected on computers by Microsoft real-time antimalware products worldwide in 1H15.

Figure 6. Encounter rate trends for a number of notable malware families in 1H15

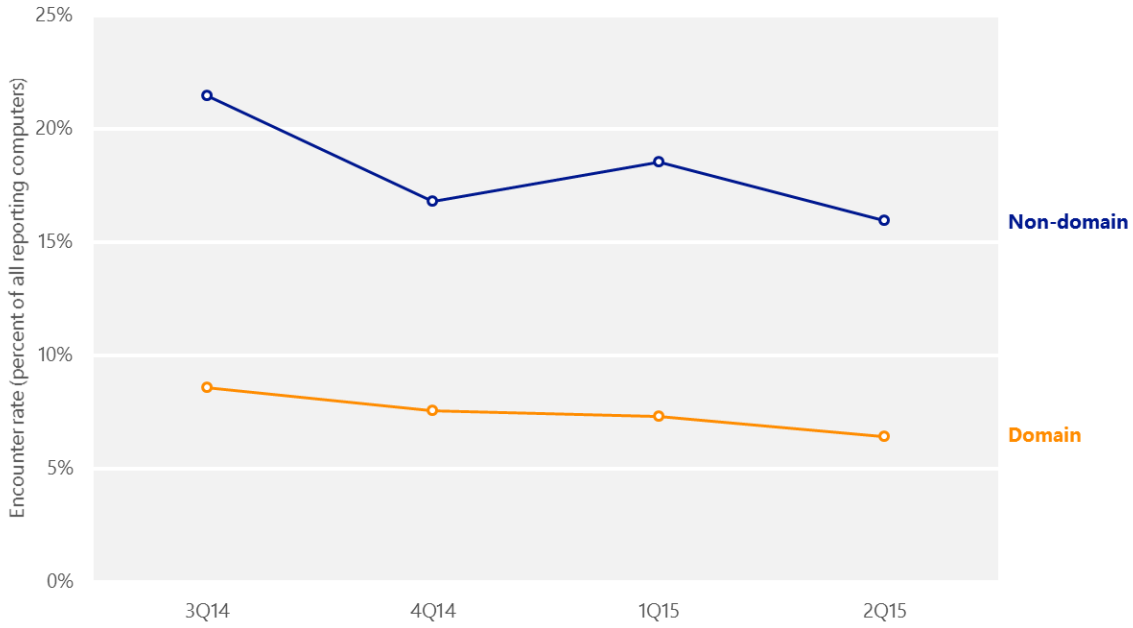


- Win32/Obfuscator, the most commonly encountered threat in 1H15, is a generic detection for programs that have been modified by malware obfuscation tools.
- Encounters involving VBS/Jenxcus declined steadily over the past four quarters, but it remained the second-most commonly encountered family in 1H15. Jenxcus is a worm coded in VBScript that opens a backdoor on an infected computer, enabling an attacker to control it remotely. Encounters involving Jenxcus decreased significantly after the Microsoft Digital Crimes Unit launched a takedown operation in June of 2014 that successfully disrupted the Jenxcus botnet.
- Win32/KipodToolsCby and Win32/IeEnablerCby are browser modifiers that bypass user consent dialogs to install software without the user's explicit permission. Microsoft security products started detecting these browser modifiers in January after Microsoft changed its unwanted software detection criteria to include attempts to bypass user consent for actions such as installing new browser add-ons. KipodToolsCby and IeEnablerCby were both encountered at high levels in 1Q15 as Microsoft security products detected and removed large numbers of installations from previous periods. Encounters subsequently decreased significantly in 2Q15, following the removal of these older installations.
- Win32/CouponRuc is an adware program that installs a browser extension without user consent. It can prevent the user from removing it or other add-ons normally, or changing other browser settings.

Home and enterprise threats

The usage patterns of home users and enterprise users tend to be very different. Analyzing these differences can provide insights into the different ways attackers target enterprise and home users and which threats are more likely to succeed in each environment.

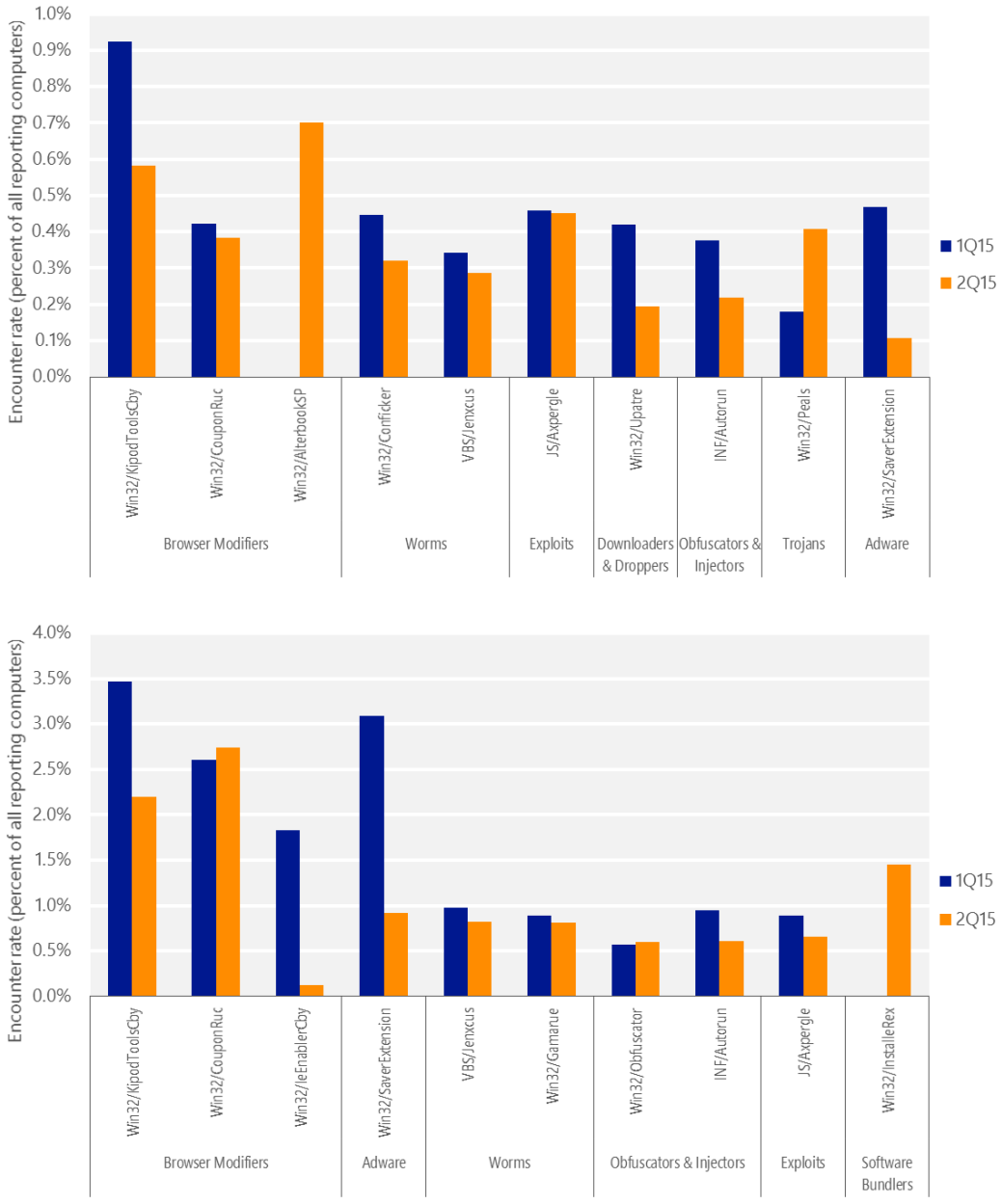
Figure 7. Malware encounter rates for domain-based and non-domain computers, 3Q14–2Q15



- Enterprise environments typically implement defense-in-depth measures, such as enterprise firewalls, that prevent a certain amount of malware from reaching users' computers. Consequently, enterprise computers tend to encounter malware at a lower rate than consumer computers.

Figure 8 lists the top 10 malware families detected on domain-joined and non-domain computers, respectively, in 1H15.

Figure 8. Quarterly trends for the top 10 malware and unwanted software families detected on domain-joined computers (top) and non-domain computers (bottom) in 1H15, by percent of computers encountering each family

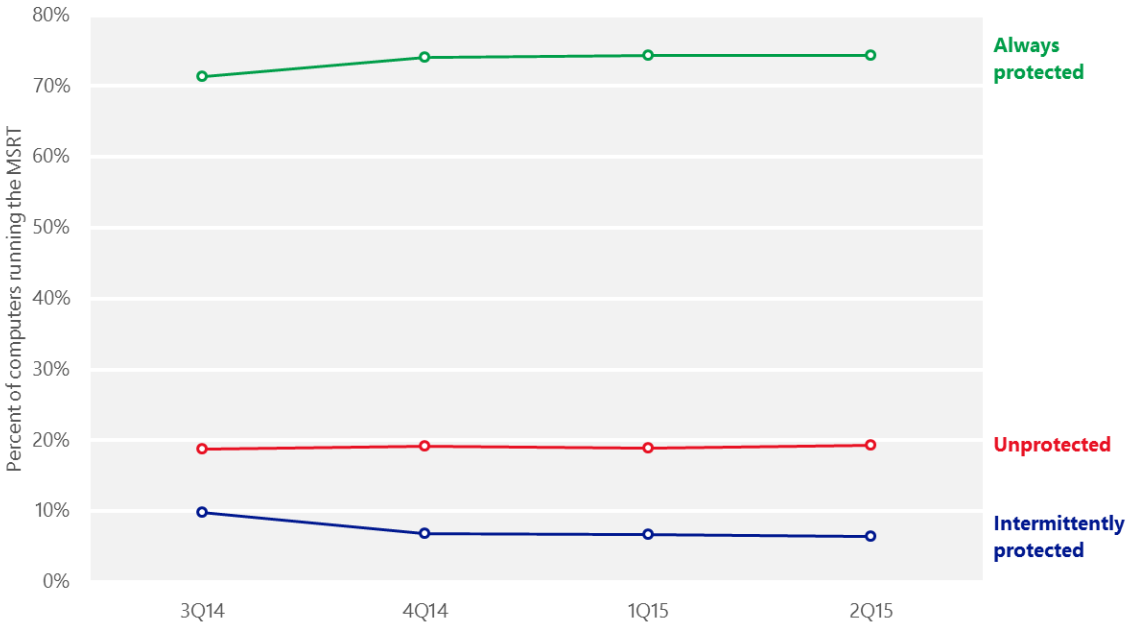


- Six families—INF/Autorun, JS/Axpergle, Win32/CouponRuc, Win32/KipodToolsCby, VBS/Jenxcus, and Win32/SaverExtension—were common to both lists. All were more frequently encountered on non-domain computers than on domain-joined computers.
- The four families that were unique to the top 10 list for domain-joined computers but not for non-domain computers are the worm family Win32/Conficker, the browser modifier Win32/AlterbookSP, the downloader family Win32/Upatre, and the trojan family Win32/Peals.
    - Conficker is a worm that was disrupted several years ago, but continues to be encountered in domain environments because of its use of a built-in list of common and weak passwords to spread between computers.
    - AlterbookSP is a browser add-on that formerly displayed behaviors of unwanted software. Recent versions of the add-on no longer meet Microsoft detection criteria, and are no longer considered unwanted software.
    - Upatre installs malware and unwanted software on the affected computer without the user's consent. It is frequently distributed as an attachment to spam email messages.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer. Figure 9 shows the percentage of computers worldwide that the MSRT found to be protected or unprotected by real-time security software each quarter in 2H14 and 1H215.

Figure 9. Percentage of computers worldwide protected by real-time security software, 3Q14–2Q15

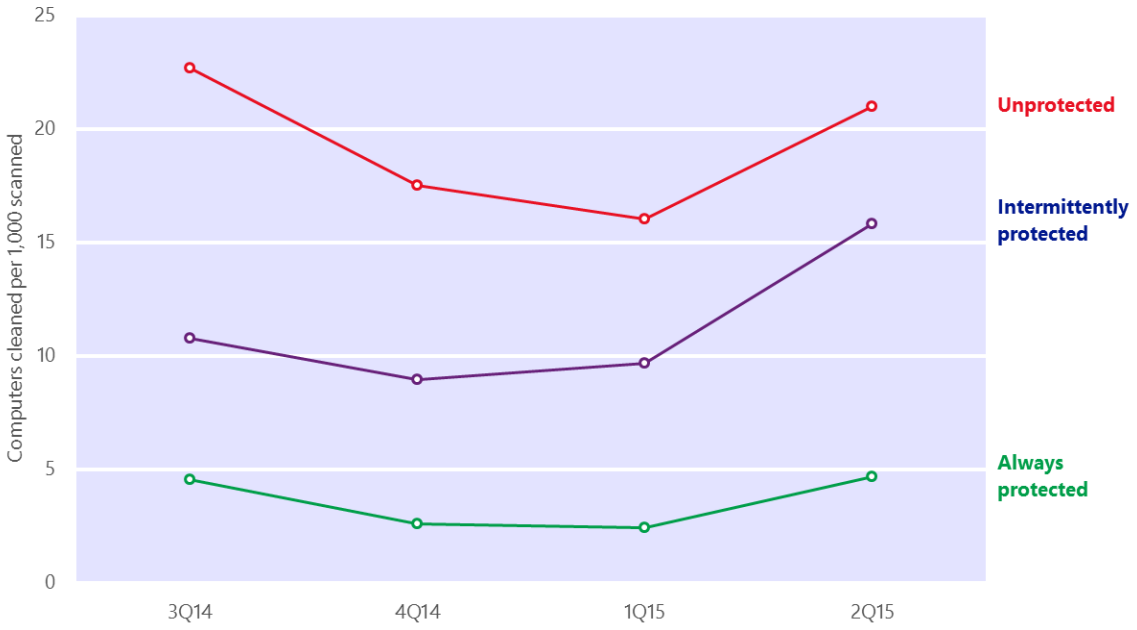


- In Figure 9, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter. "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them. "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

- Overall, about three-fourths of computers worldwide were found to be always protected at every monthly MSRT execution in each of the past four quarters, varying between 71.4 percent and 74.3 percent.
- Computers that never reported running security software accounted for between 18.8 and 19.3 percent of computers worldwide each quarter. Intermittently protected computers accounted for between 6.4 and 9.9 percent of computers each quarter.

As Figure 10 shows, computers that do not run real-time security software are at significantly greater risk of malware infection than computers that do.

Figure 10. Infection rates for protected and unprotected computers, 3Q14–2Q15



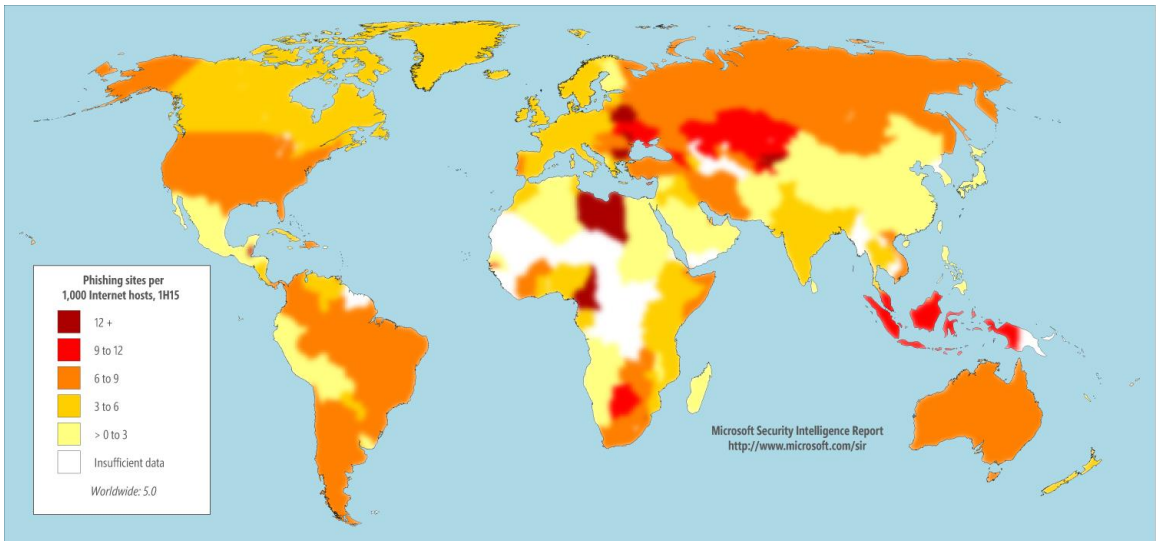
- Computers that were never found to be running real-time security software during 1H15 were about six times as likely to be infected with malware as computers that were always found to be protected. Computers that were intermittently protected were about three times more likely to be infected with malware in 1H15 than computers that were always protected.

Malicious websites

Phishing sites

Phishing impression information from SmartScreen Filter in Internet Explorer includes anonymized information about the IP addresses of the clients making the reports, as well as the IP addresses of the phishing sites themselves.

Figure 11. Phishing sites per 1,000 Internet hosts for locations around the world in 1H15

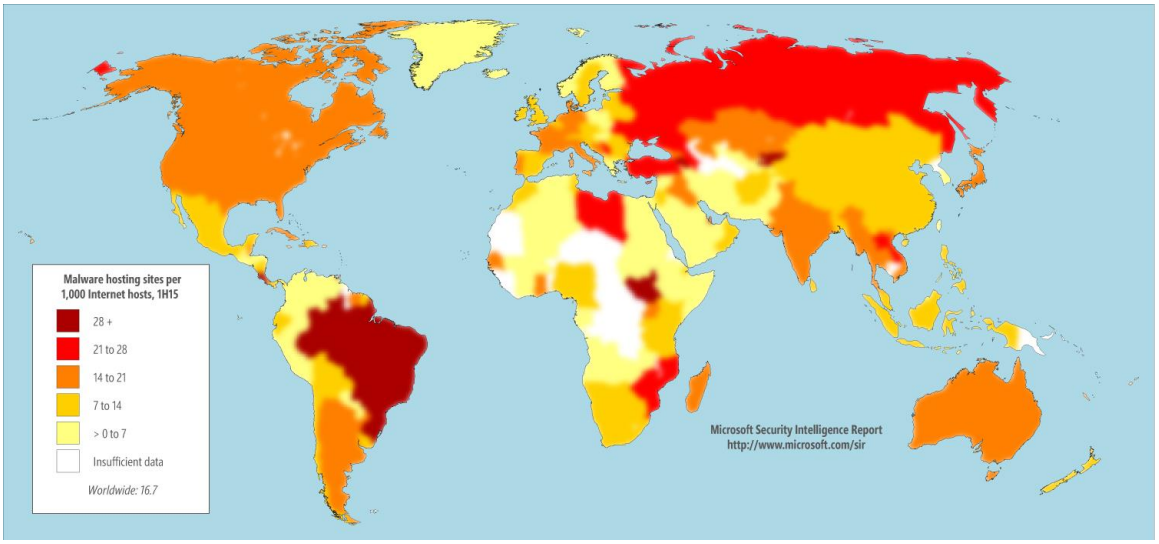


- SmartScreen Filter detected approximately 5.0 phishing sites per 1,000 Internet hosts worldwide in 1H15.
- Locations hosting higher than average concentrations of phishing sites include Bulgaria (98.5 per 1,000 Internet hosts in 1Q15), Libya (15.6), and Belize (14.5). Locations with low concentrations of phishing sites include Taiwan (1.2), the United Arab Emirates (1.4), and Korea (1.6).

Malware hosting sites

SmartScreen Filter helps provide protection against sites that are known to host malware, in addition to phishing sites. SmartScreen Filter uses file and URL reputation data and Microsoft antimalware technologies to determine whether sites distribute unsafe content. Figure 12 shows the geographic distribution of malware hosts and computers reporting impressions in 1H15.

Figure 12. Malware distribution sites per 1,000 Internet hosts for locations around the world in 1H15



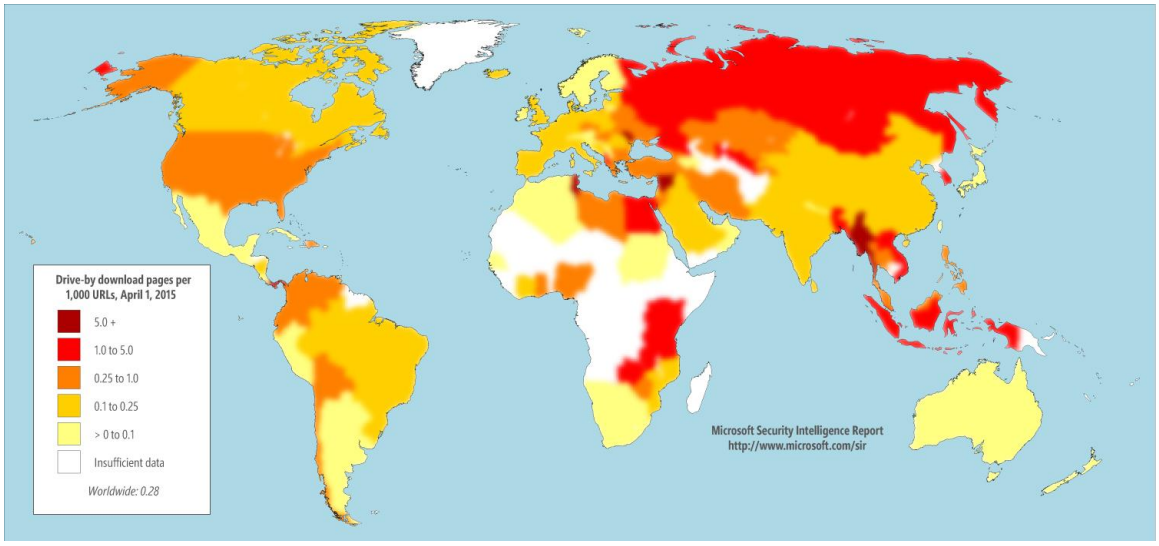
- SmartScreen Filter detected approximately 16.7 malware hosting sites per 1,000 Internet hosts worldwide in 1H15.
- Locations with large concentrations of malware hosting sites included Brazil (41.0 per 1,000 Internet hosts in 1H15), Costa Rica (38.8), and Russia (23.9). Locations with low concentrations of malware hosting sites included Taiwan (2.8), Saudi Arabia (4.3), and Finland (4.4).

Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable

computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Figure 13 shows the concentration of drive-by download pages in countries and regions throughout the world at the end of 2Q15.

Figure 13. Drive-by download pages indexed by Bing at the end of 2Q15 per 1,000 URLs in each country/region



- Significant locations with high concentrations of drive-by download URLs in both quarters include Panama, with 8.7 drive-by URLs for every 1,000 URLs tracked by Bing at the end of 2Q15; Vietnam, with 3.0; and Russia, with 1.7.

This document summarizes the key findings of the report. Visit www.microsoft.com/sir to download the full version, which includes in-depth analysis of the findings summarized here. It also includes featured intelligence reports about banking malware in Brazil and a targeted attack group Microsoft is tracking, as well as security data and analysis for more than 100 individual countries and regions.