Microsoft Security Intelligence Report

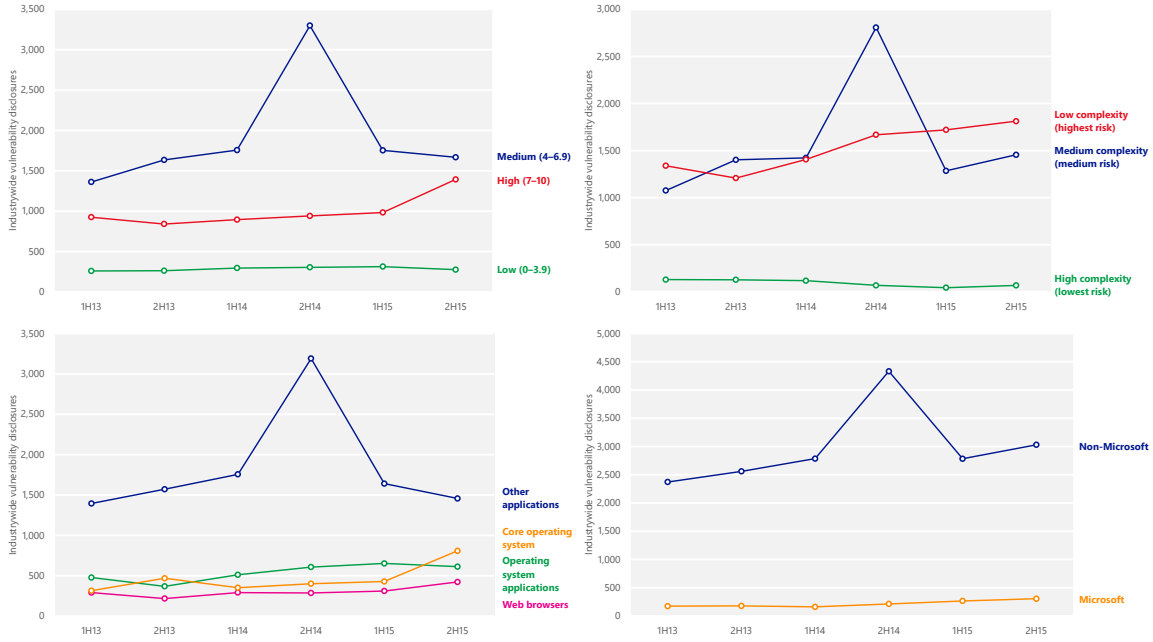
Volume 20 | July through December, 2015

Key Findings Summary

Vulnerabilities

Vulnerability disclosures across the industry increased 9.4 percent between 1H15 and 2H15, to just above 3,300.[1] Disclosures have trended generally upward over the past three years, with the exception of a spike in 2H14 caused by a CERT/CC research project involving SSL vulnerabilities in Android applications.

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, 1H13–2H15

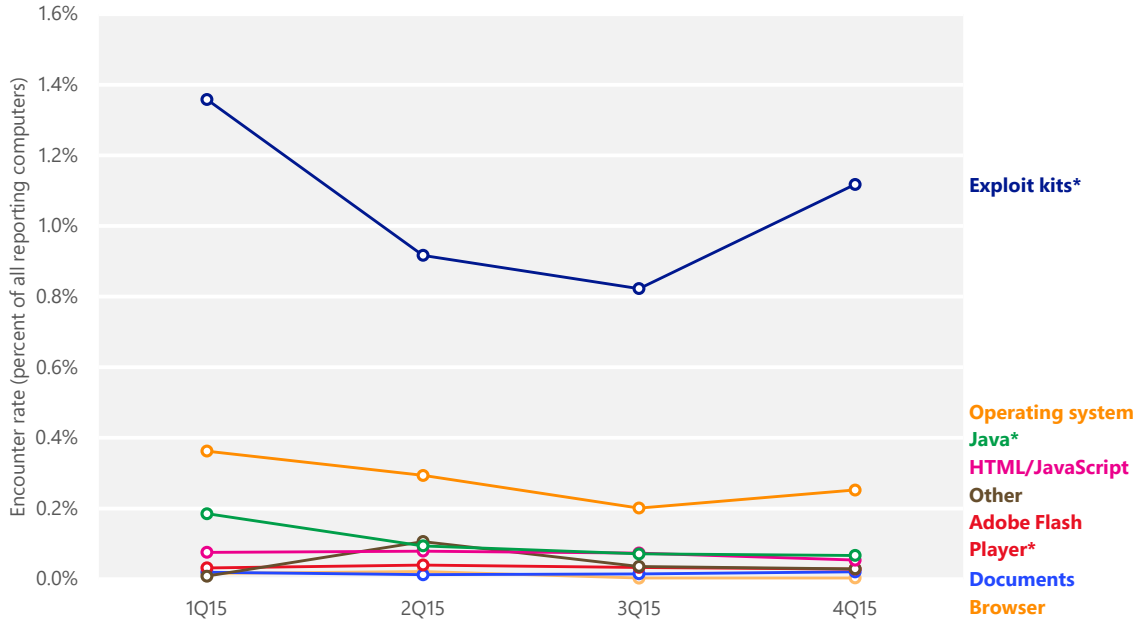


[1] Throughout the report, half-yearly and quarterly time periods are referenced using the *n*H*yy* or *n*Q*yy* formats, where yy indicates the calendar year and n indicates the half or quarter.

Exploits

Figure 2 shows the prevalence of different types of exploits detected by Microsoft antimalware products each quarter in 2015, 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 in 2015



* 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.
- After decreasing steadily for more than a year, encounters with exploit kits increased by more than a third from 3Q15 to 4Q15. They remained the most commonly encountered type of exploit in the second half of the year, with

an encounter rate more than four times that of the next most common type of exploit.

- The number of encounters with exploits that target operating systems increased slightly in 4Q15, but remained lower than in the first half of the year. Operating system exploits were the second most commonly encountered type of exploits during the period.
- Encounters with Java exploits, Adobe Flash Player exploits, and other types of exploits each accounted for less than 0.1 percent of all malware encounters in 2H15.

Exploit families

Figure 3 lists the exploit-related malware families that were detected most often during the second 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 2H15, shaded according to relative prevalence

Exploit	Type	1Q15	2Q15	3Q15	4Q15
Axpergle	Exploit kit	0.86%	0.66%	0.71%	0.92%
CVE-2010-2568 (CplLnk)	Operating system	0.30%	0.23%	0.18%	0.24%
HTML/Meadgive	Exploit kit	0.06%	0.05%	0.07%	0.17%
JS/NeutrinoEK	Exploit kit	0.06%	0.03%	0.01%	0.11%
HTML/IframeRef	Generic	0.07%	0.05%	0.04%	0.05%
JS/Neclu	Exploit kit	0.03%	0.15%	0.05%	0.01%
ShellCode	Other	0.01%	0.02%	0.01%	0.03%
Win32/Sdbby	Other	0.00%	0.09%	0.02%	0.01%
CVE-2012-1723	Java	0.04%	0.02%	0.02%	0.02%
Java/Obfuscator	Java	0.04%	0.05%	0.02%	0.01%

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

- Exploit kits accounted for four of the 10 most commonly encountered exploits during 2H15.
- 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. The vulnerability was first discovered being used by the malware family Win32/Stuxnet in mid-2010, and it has since been exploited by a number of other families, many of which predated the disclosure of the vulnerability and were subsequently adapted to attempt to exploit it. Microsoft published Security Bulletin MS10-046 in August 2010 to address the issue. Windows 8 and subsequently released versions of Windows have never been vulnerable to exploits of CVE-2010-2568.
- 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.
- Win32/Sdbby is a generic detection for malware that bypasses the User Account Control (UAC) prompt to gain administrative privileges on a computer. After briefly becoming the fourth most commonly encountered exploit family in 2Q15, it decreased to much lower levels during the second half of the year.

Malware and unwanted software

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

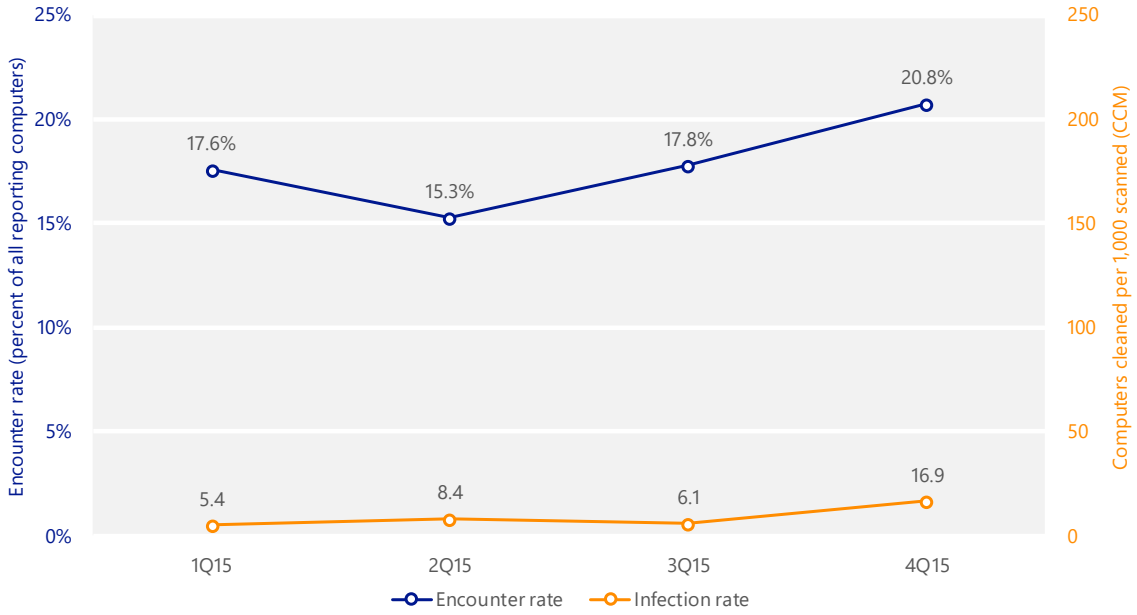
- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter.[3] Only computers whose users have opted in to provide data to Microsoft are considered when calculating encounter rates.
- *Computers cleaned per mille*, or *CCM*, 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

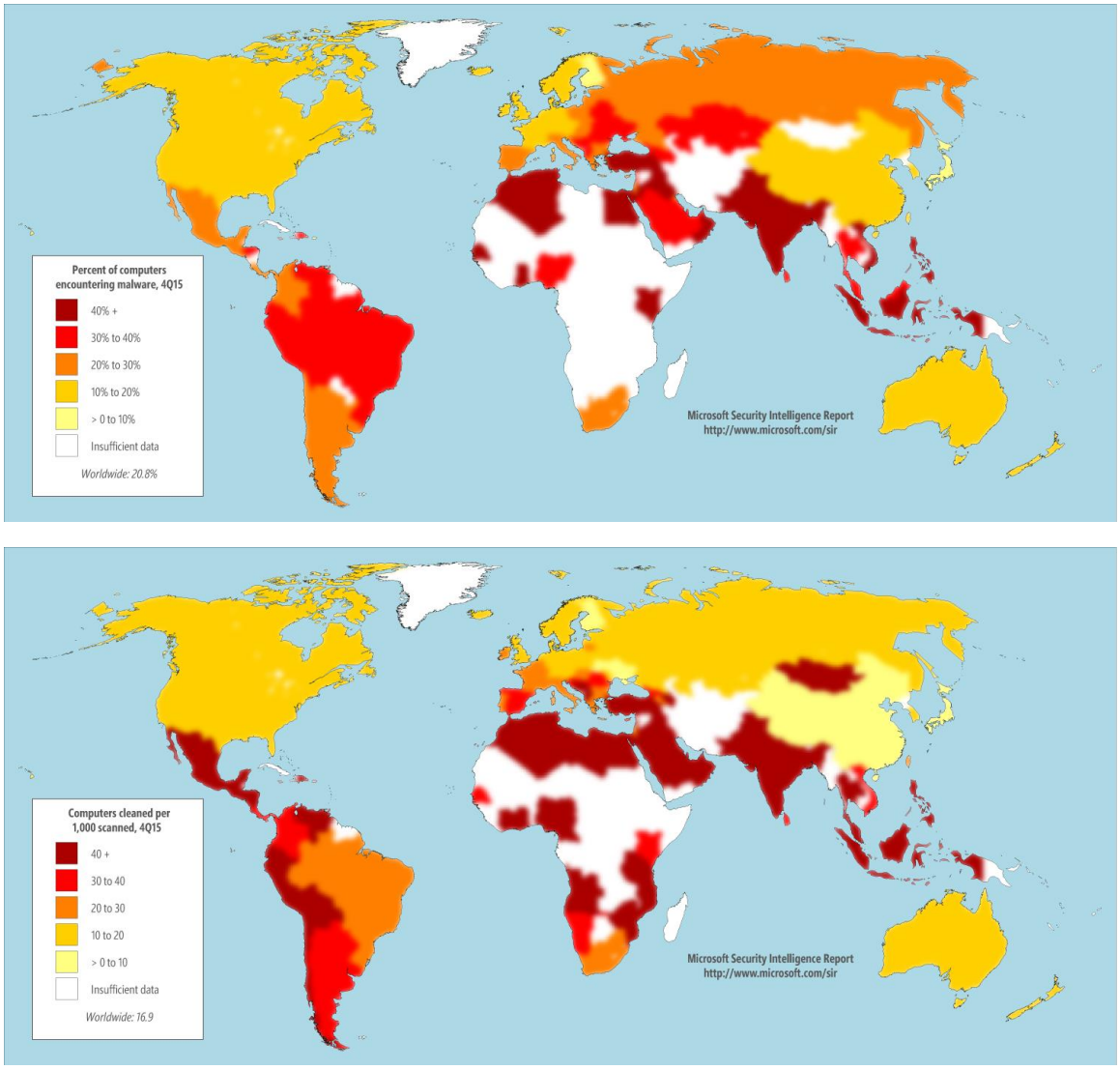


On average, about 17.9 percent of reporting computers worldwide encountered threats in 2015. At the same time, the MSRT removed threats from about 9.2 out of every 1,000 computers, or 0.92 percent.

Malware and unwanted software worldwide

Figure 5 shows the infection and encounter rates for locations around the world in 4Q15.

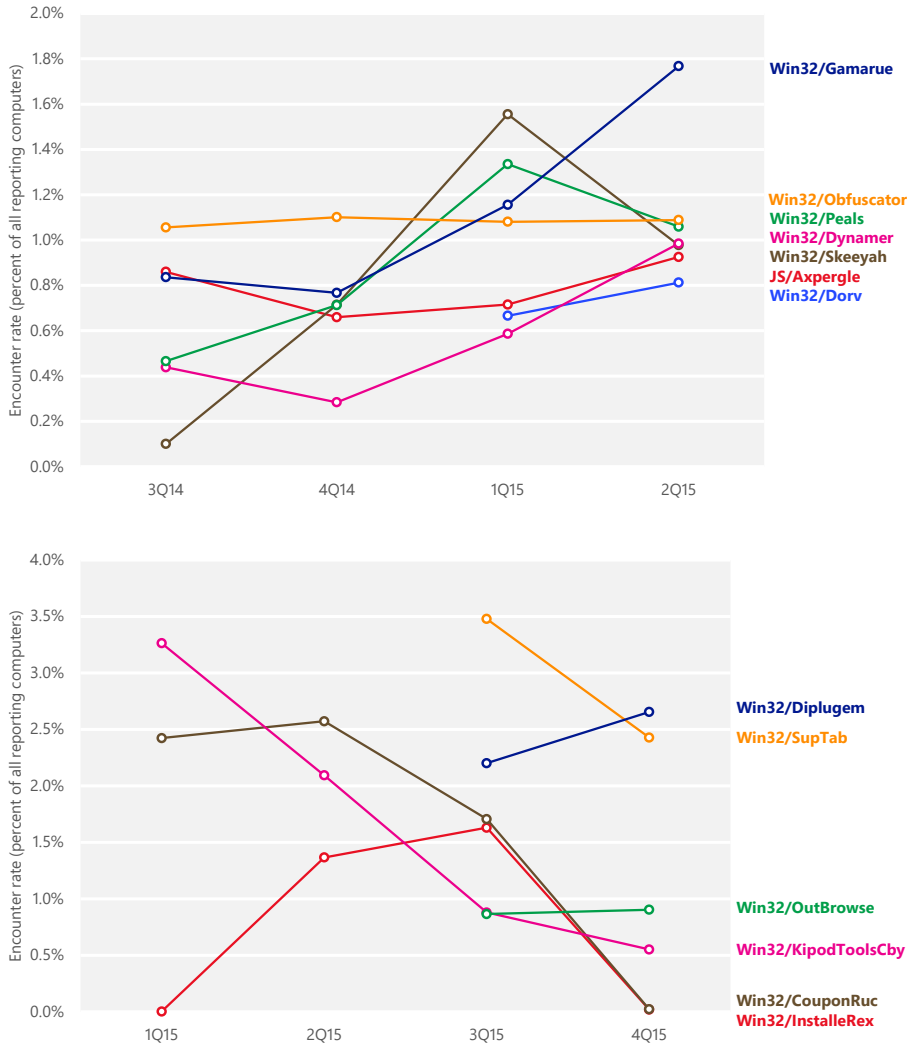
Figure 5. Encounter rates (top) and infection rates (bottom) by country/region in 4Q15



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 2H15.

Figure 6. Encounter rate trends for a number of notable malware families (top) and unwanted software families (bottom) in 2H15

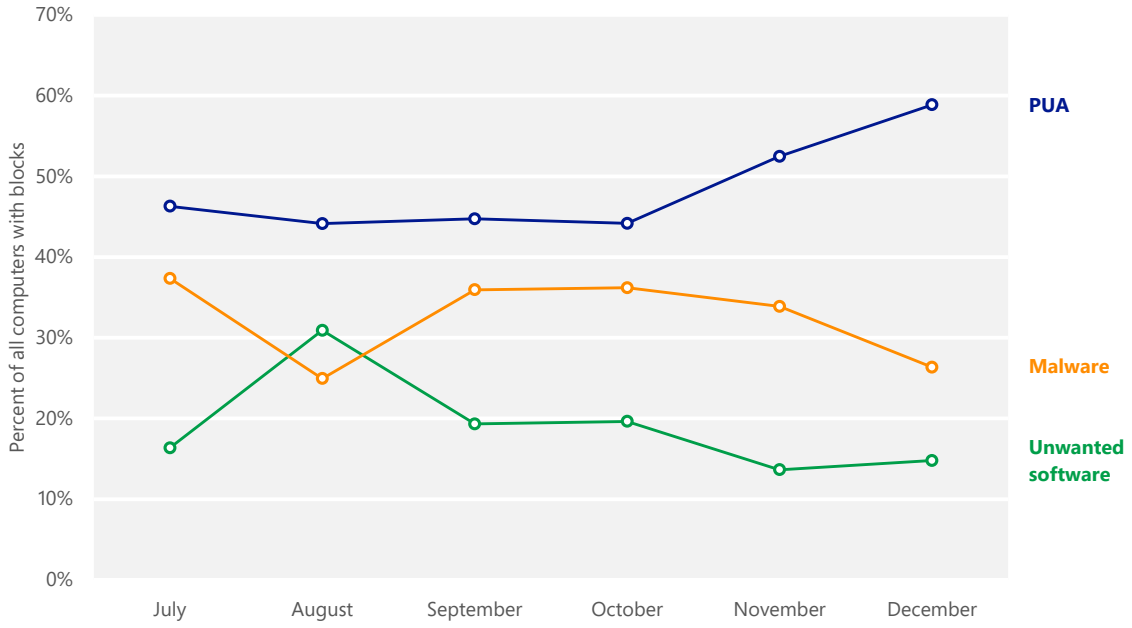


- Win32/Gamarue, the most commonly encountered malware family in 2H15, is a worm that is commonly distributed via exploit kits and social engineering. Gamarue was especially prevalent in southeast Asia and the Middle East, and was rarely detected in North America and western Europe.
- Win32/Skeeyah, Win32/Peals, and Win32/Dynamer are generic detections for a variety of threats that share certain characteristics. All three detections disproportionately affected computers in Russia and Eastern Europe.
- Win32/Obfuscator is a generic detection for programs that have been modified by malware obfuscation tools.
- The three most commonly encountered unwanted software families in 2H15—the browser modifiers Win32/SupTab and Win32/Diplugem, and the software bundler Win32/OutBrowse—were all first encountered in 3Q15.

Potentially unwanted applications in the enterprise

Some programs don't meet the criteria to be considered unwanted software but still exhibit behaviors that may be considered undesirable, particularly in enterprise environments. Microsoft classifies these programs as *potentially unwanted applications* (PUA), and has begun offering enterprise users of System Center Endpoint Protection (SCEP) the ability to block them from being installed on their networks. As Figure 7Error! Reference source not found. shows, PUA can have a bigger impact on an enterprise environment than malware and unwanted software combined.

Figure 7. PUA, malware, and unwanted software blocked during 2H15 pilot project, by month

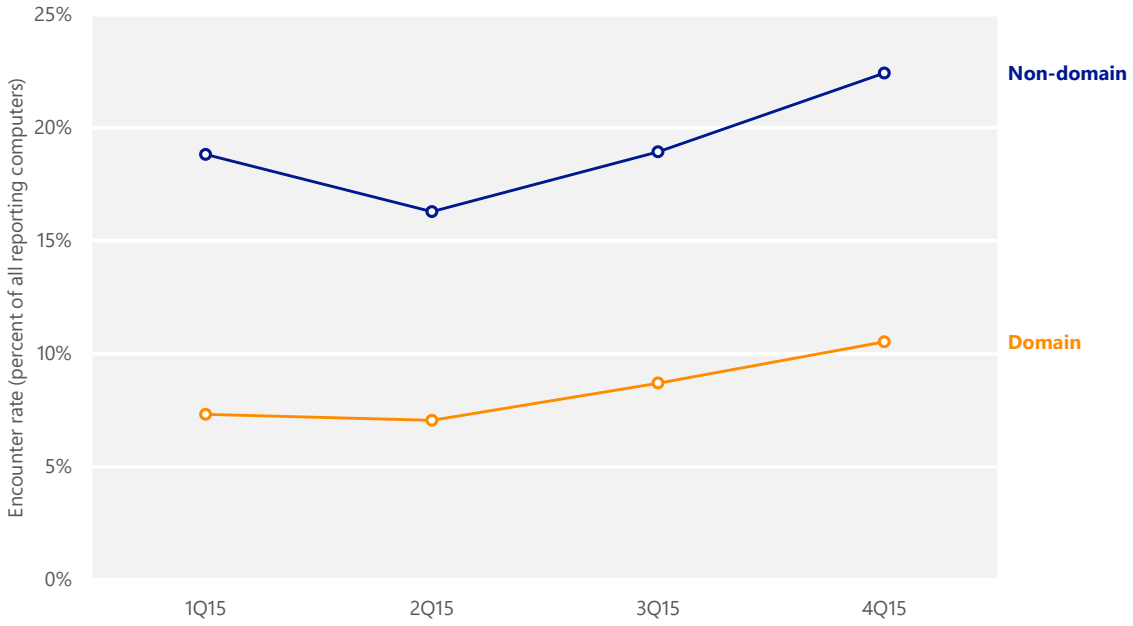


Among the most commonly detected PUA families during a 2H15 pilot project were PUA:Win32/CandyOpen and PUA:Win32/InstallCore, detections for installer programs that were built with software bundler utilities (called OpenCandy and InstallCore, respectively) that offer monetization opportunities to software developers, such as pay-per-install services for programs that offer to download other programs alongside the requested application.

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.

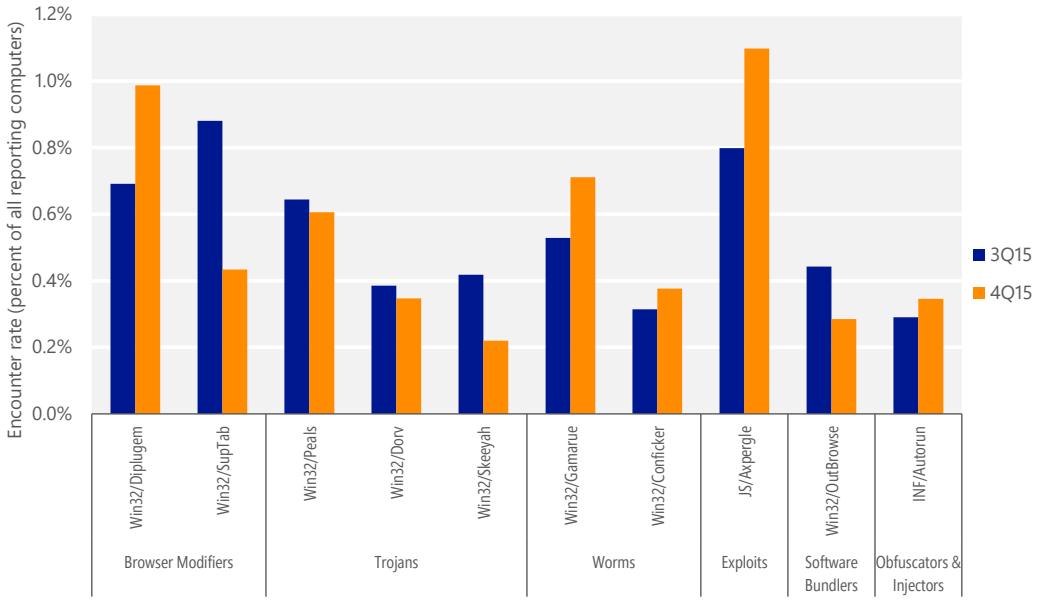
Figure 8. Malware encounter rates for domain-based and non-domain computers in 2015

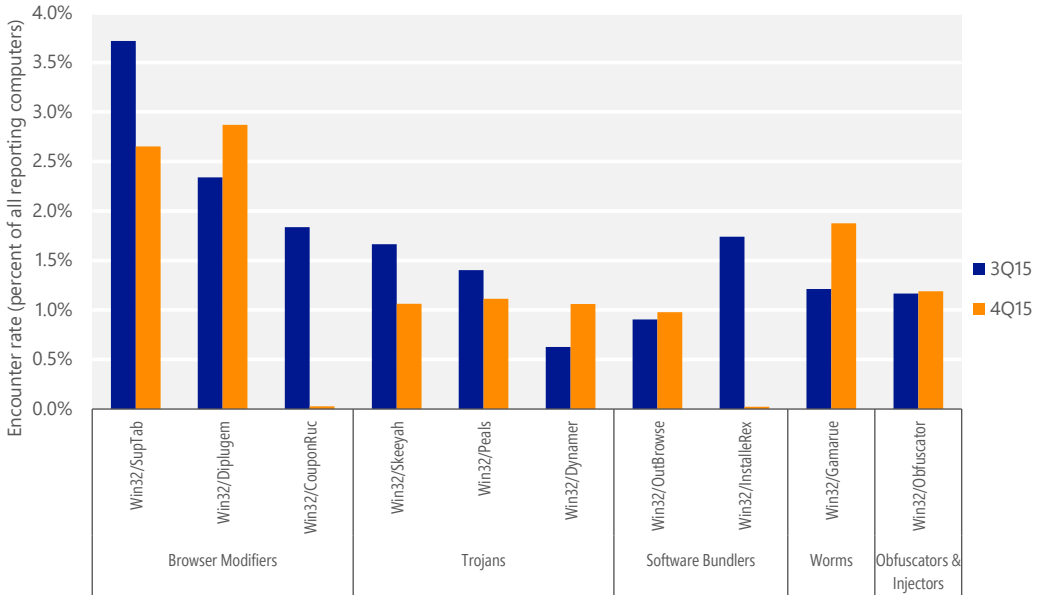


- Enterprise environments typically implement defense-in-depth measures, such as enterprise firewalls, that prevent a certain amount of malware from reaching users' computers. Consequently, enterprise computers tend to encounter malware at a lower rate than consumer computers.

Figure 9 lists the top 10 malware families detected on domain-joined and non-domain computers, respectively, in 2H15.

Figure 9. Quarterly trends for the top 10 malware and unwanted software families detected on domain-joined computers (top) and non-domain computers (bottom) in 2H15, by percent of computers encountering each family



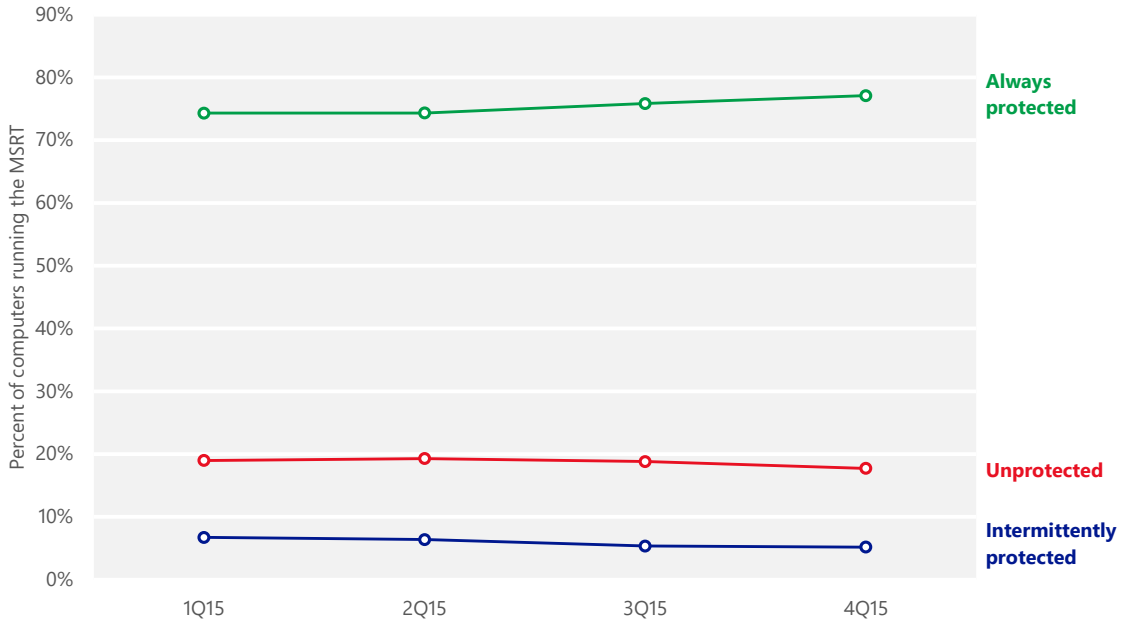


- Six families—Win32/SupTab, Win32/Diplugem, Win32/Gamarue, Win32/Skeeyah, Win32/Peals, and Win32/OutBrowse—were common to both lists. All were more frequently encountered on non-domain computers than on domain-joined computers.
- The four families that were unique to the top 10 list for domain-joined computers but not for non-domain computers are the exploit kit JS/Axpergle, the trojan family Win32/Dorv, the worm family Win32/Conficker, and the generic detection INF/Autorun.
- No ransomware families were among the top 10 families in domain or non-domain environments.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer. Figure 10 shows the percentage of computers worldwide that the MSRT found to be protected or unprotected by real-time security software each quarter in 2015.

Figure 10. Percentage of computers worldwide protected by real-time security software in 2015

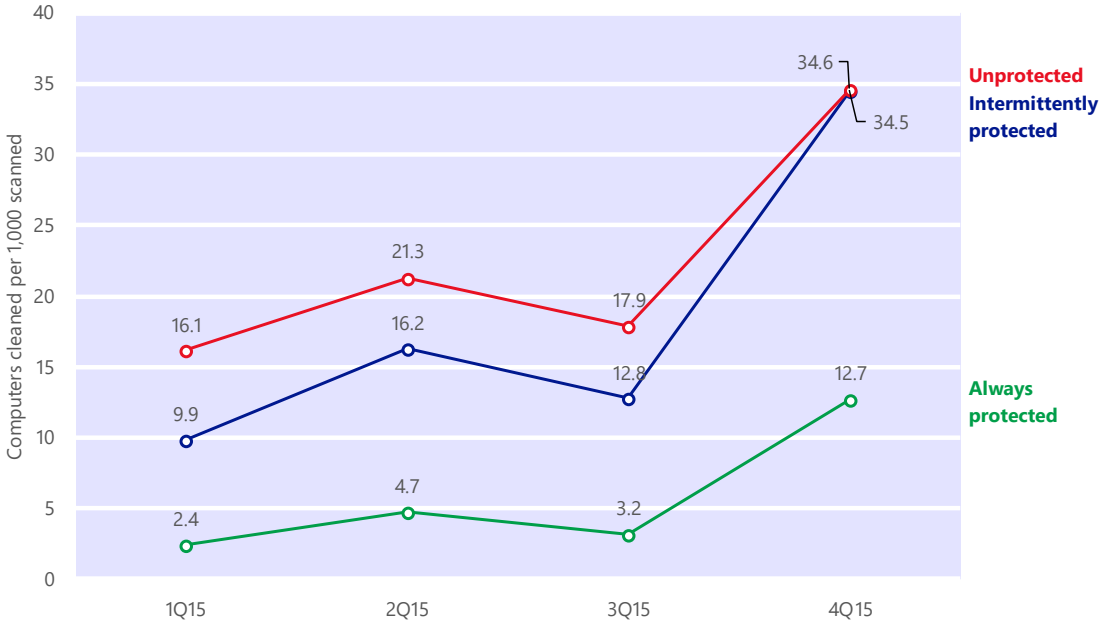


- In Figure 10, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter. "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them. "Unprotected" 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 74.3 percent and 77.1 percent.

As Figure 11 shows, computers that do not run real-time security software are at significantly greater risk of malware infection than computers that do.

Figure 11. Infection rates for protected and unprotected computers in 2015



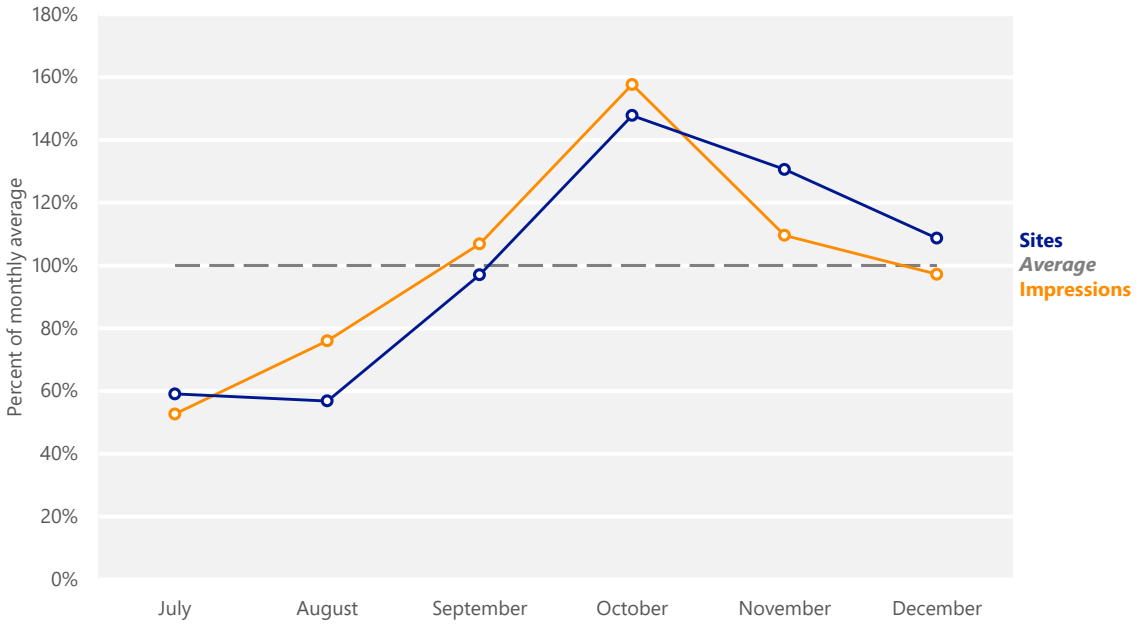
- Infection rates increased significantly for all protection levels in 4Q15 due to Win32/Diplugem. See the full report for more information.
- Computers that were never found to be running real-time security software during 2H15 were between 2.7 and 5.6 times as likely to be infected with malware as computers that were always found to be protected. Computers that were intermittently protected were between 2.7 and 4.0 times more likely to be infected with malware in 2H15 than computers that were always protected.

Malicious websites

Phishing sites

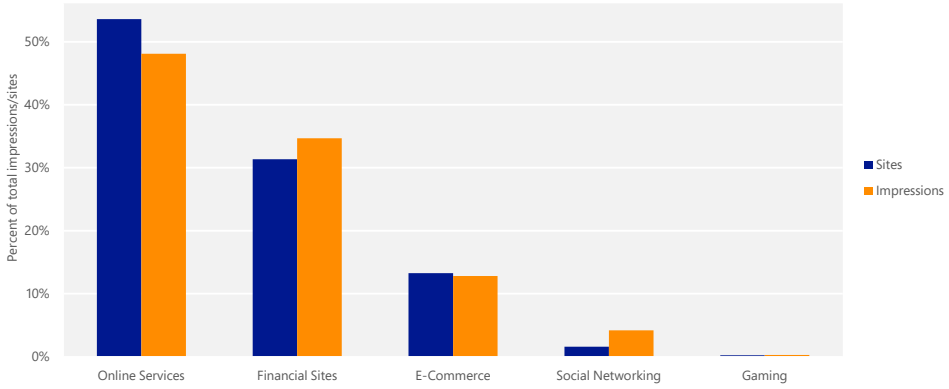
Microsoft gathers information about phishing sites and impressions from *phishing impressions* tracked by SmartScreen Filter in Microsoft Edge and Internet Explorer. A phishing impression is a single instance of a user attempting to visit a known phishing site with SmartScreen Filter enabled and being warned.

Figure 12. Phishing sites and impressions reported by SmartScreen Filter each month in 2H15, relative to the monthly average for each



- Phishing sites that targeted online services received the largest share of impressions during the period, and accounted for the largest number of active phishing URLs.

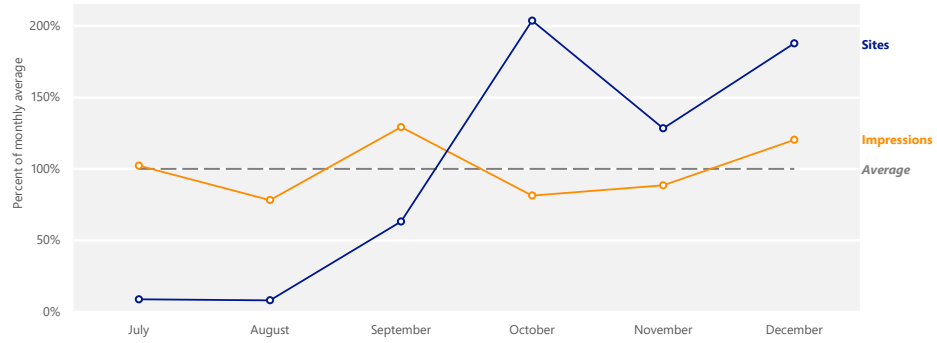
Figure 13. Phishing sites and impressions reported by SmartScreen Filter for each type of phishing site in 2H15



Malware hosting sites

SmartScreen Filter also helps provide protection against sites that are known to host malware. Figure 14 compares the volume of active malware hosting sites in the Microsoft database each month with the volume of malware impressions tracked.

Figure 14. Malware hosting sites and impressions tracked each month in 2H15, relative to the monthly average for each

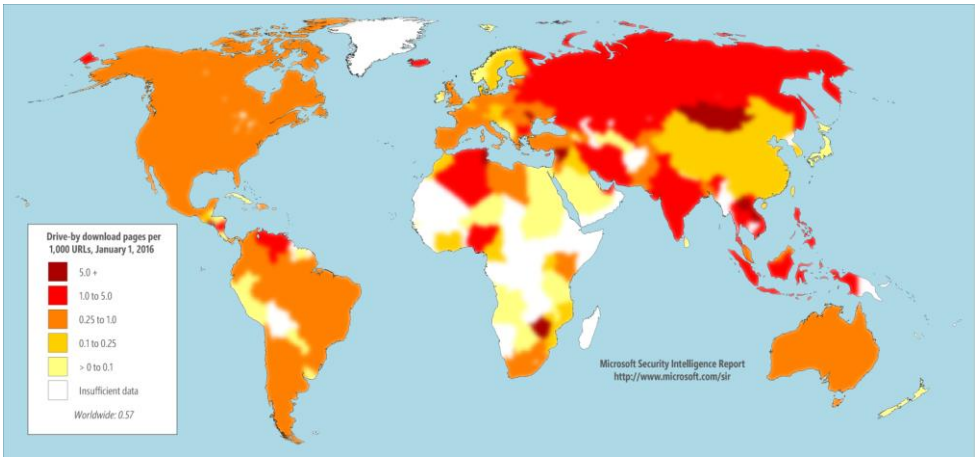


- The number of active malware hosting sites increased by more than 25 times between August and October, correlated with an attack campaign that compromised thousands of sites running the WordPress content management system (CMS) beginning in September.

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 15 shows the concentration of drive-by download pages in countries and regions throughout the world at the end of 4Q15.

Figure 15. Drive-by download pages indexed by Bing at the end of 4Q15 per 1,000 URLs in each country/region



- Significant locations with high concentrations of drive-by download URLs in both quarters include Moldova, with 12.7 drive-by URLs for every 1,000 URLs tracked by Bing at the end of 4Q15; Cyprus, with 2.6; and Russia, with 1.8.

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 security data and analysis for more than 100 individual countries and regions, along with featured intelligence reports on a number of important security topics.