Microsoft Security Intelligence Report

Volume 18 | July through December, 2014

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.

Authors

Dennis Batchelder
Microsoft Malware Protection Center

Joe Blackbird
Microsoft Malware Protection Center

Patti Chrzan
Microsoft Digital Crimes Unit

Elia Florio
Microsoft Malware Protection Center

Chad Foster
Bing

Paul Henry
Wadeware LLC

Jeff Jones
Corporate Communications

Marianne Mallen
Microsoft Malware Protection Center

Nam Ng
Worldwide Cybersecurity & Data Protection

Niall O'Sullivan
Microsoft Digital Crimes Unit

Daryl Pecelj
Microsoft IT Information Security and Risk Management

Ina Ragragio
Microsoft Malware Protection Center

Tim Rains
Worldwide Cybersecurity & Data Protection

Paul Rebriy
Bing

Holly Stewart
Microsoft Malware Protection Center

Jerome Stewart
Microsoft Digital Crimes Unit

Todd Thompson
Microsoft IT Information Security and Risk Management

David "dwizzle" Weston
Operating Systems Group

Contributors

Chun Feng
Microsoft Malware Protection Center

Tanmay Ganacharya
Microsoft Malware Protection Center

Cristin Goodwin
Microsoft Trustworthy Computing

Roger Grimes
Microsoft IT

Satomi Hayakawa
CSS Japan Security Response Team

Ben Hope
Microsoft Malware Protection Center

Yurika Kakiuchi
CSS Japan Security Response Team

Marc Lauricella
Corporate Communications

Jenn LeMond
Microsoft IT

Scott Molenkamp
Microsoft Malware Protection Center

Dolcita Montemayor
Microsoft Malware Protection Center

Daric Morton
Microsoft Services

Cody Nicewanner
Operating Systems Group

Hamish O'Dea
Microsoft Malware Protection Center

Jeong Wook Oh
Microsoft Malware Protection Center

Dmitriy Pletnev
Microsoft Malware Protection Center

Laura A. Robinson
Microsoft IT

Jasmine Sesso
Microsoft Malware Protection Center

Norie Tamura
CSS Japan Security Response Team

Steve Wacker
Wadeware LLC

Vladimir Zubko
Microsoft Malware Protection Center

Table of contents

Mitigating risk 91

Appendixes 103

About this report

The Microsoft Security Intelligence Report (SIR) focuses on software vulnerabilities, software vulnerability exploits, malware, and unwanted software. Past reports and related resources are available for download at www.microsoft.com/sir. We hope that readers find the data, insights, and guidance provided in this report useful in helping them protect their organizations, software, and users.

Reporting period

This volume of the *Microsoft Security Intelligence Report* focuses on the third and fourth quarters of 2014, with trend data for the last several quarters presented on a quarterly basis. Because vulnerability disclosures can be highly inconsistent from quarter to quarter and often occur disproportionately at certain times of the year, statistics about vulnerability disclosures are presented on a half-yearly basis.

Throughout the report, half-yearly and quarterly time periods are referenced using the *n*H*yy* or *n*Q*yy* formats, in which *yy* indicates the calendar year and *n* indicates the half or quarter. For example, 1H14 represents the first half of 2014 (January 1 through June 30), and 4Q13 represents the fourth quarter of 2013 (October 1 through December 31). To avoid confusion, please note the reporting period or periods being referenced when considering the statistics in this report.

Conventions

This report uses the Microsoft Malware Protection Center (MMPC) naming standard for families and variants of malware. For information about this standard, see "Appendix A: Threat naming conventions" on page 105. In this report, any threat or group of threats that share a common unique base name is considered a family for the sake of presentation. This consideration includes threats that may not otherwise be considered families according to common industry practices, such as generic detections. For the purposes of this report, a "threat" is defined as a malware or unwanted software family or variant that is detected by the Microsoft Malware Protection Engine.

Foreword

As I look at the latest data in this volume of the *Microsoft Security Intelligence Report* I can clearly see the threat landscape evolving in at least a few important ways.

First, vulnerability disclosures across the entire industry increased precipitously in the second half of 2014, increasing 56 percent from the first half of the year. 4,512 vulnerabilities were disclosed during the second half of 2014, representing the largest number of vulnerabilities disclosed in any six month period since the Common Vulnerabilities and Exposures system was launched in 1999. This increase is predominantly the result of work performed by the Computer Emergency Response Team (CERT) Coordination Center (CERT/CC) finding almost 1,400 individual CVEs affecting thousands of different publishers of Android apps and code libraries (more details can be found in this report).

Secondly, commercial exploit kits continue to be popular tools among some attackers. The speed at which we see newly discovered exploits get incorporated into commercial exploit kits has accelerated. The timespan between the availability of a security update and when an exploit for the vulnerability is integrated into a commercial exploit kit was significantly reduced in the second half of 2014. It used to take weeks or months for new exploits to appear in exploit kits, but in the second half of 2014 we saw that time period decrease to ten days or less in several cases.

Thirdly, attackers have focused on attacking vulnerabilities in Oracle Java for many years. But that trend changed in the second half of 2014 when Microsoft deployed a new feature in Internet Explorer that blocks the use of out-of-date Java. This helped to blunt the high volume of exploitation attempts on out-of-date Java installations and protect many, many consumers and organizations from these attacks.

The last highlight I'll mention is that newer versions of Windows operating systems are performing better than older versions at mitigating malware and threats. Windows 8.1 and Windows Server 2012 R2 have some of the lowest malware infection rates we have seen and are providing clear security benefits to those people and organizations using them.

You'll get plenty of other insights in this volume of the *Microsoft Security Intelligence Report* and I hope you get real value from the data.

Tim Rains
Chief Security Advisor
Worldwide Cybersecurity & Data Protection

Featured intelligence

The life and times of an exploit

The CVE-2014-6332 vulnerability, a memory corruption issue in Windows OLE, was a focus for attackers in the last quarter of 2014. Initially released by an independent security researcher as a proof-of-concept exploit with fully operational code, it was quickly repurposed by both targeted attack groups and criminal exploit kits alike, despite the availability of a security update addressing the vulnerability.

This section focuses on the details of this exploit, its use by both criminals and targeted attack groups, and the material impact of this and other released exploits. It illustrates how attackers can move quickly to take advantage of newly disclosed vulnerabilities even after they've been addressed with security updates, and demonstrates how swiftly testing and applying updates as they are released remains one of the best ways individuals and organizations can protect themselves from attack.

Disclosure and spread

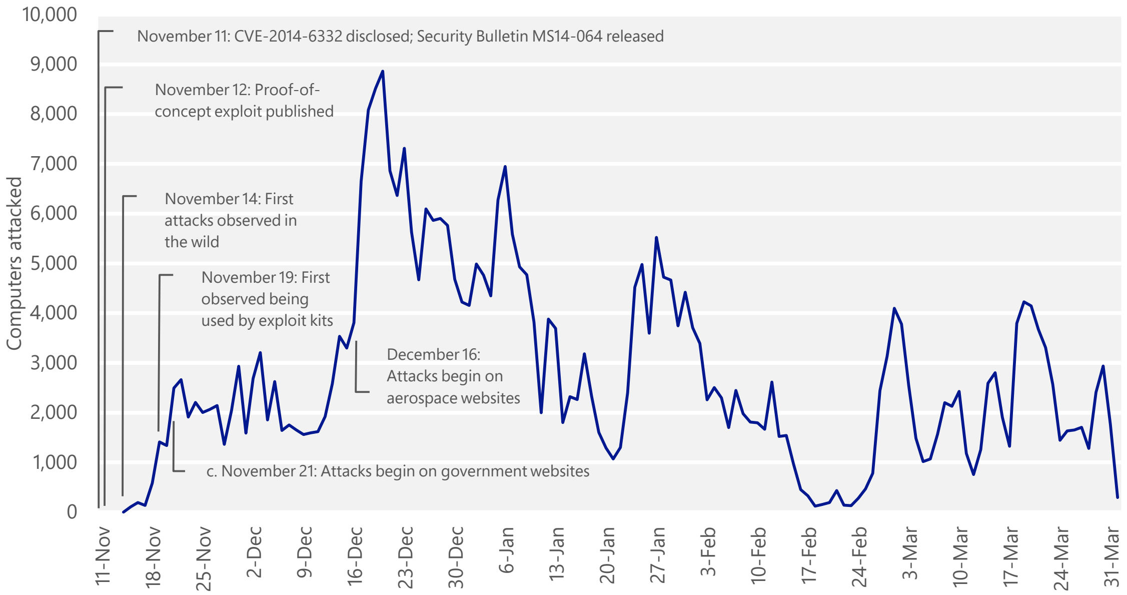
On November 11, 2014, Microsoft released Security Bulletin MS14-064 as part of its regular scheduled monthly security bulletin release (colloquially called "Patch Tuesday.") One of the vulnerabilities addressed by this security bulletin was CVE-2014-6332, a vulnerability in Windows Object Linking and Embedding (OLE) that was privately reported to Microsoft by Robert Freeman of IBM's X-Force security research team. The vulnerability has a CVSS severity score of 9.3 (categorized as "High") and an access complexity score of Medium. (See "Vulnerabilities" beginning on page 13 for more information about vulnerability severity and complexity.) Although it is not a vulnerability in Internet Explorer, a remote attacker could use Internet Explorer to attempt to exploit CVE-2014-6332 on the computer. (If Internet Explorer is in protected mode, which is enabled by default for Internet websites, the exploit requires that the user grant the Windows-based script host permission to run it in order to succeed.) Applying Security Bulletin MS14-064 resolves the issue.

November 12: Initial proof-of-concept exploit released

The day after the security bulletin was released, November 12, an independent security researcher in China published a fully-weaponized proof-of-concept exploit targeting CVE-2014-6332. This exploit was particularly notable because it was the first one known to make use of an exploitation technique developed and published by several different security researchers earlier in 2014.

Dubbed "God Mode" for its supposed resemblance to a video game cheat code, this technique could be used to bypass most memory mitigations by setting a single byte in the Internet Explorer script engine on a compromised computer. Using this technique, the exploit is capable of bypassing exploit mitigations on most versions of Windows—creating a tempting opportunity for both malware creators and targeted attackers.

Figure 1. Number of computers reporting CVE-2014-6332 exploit attempts each day, November 2014–March 2015



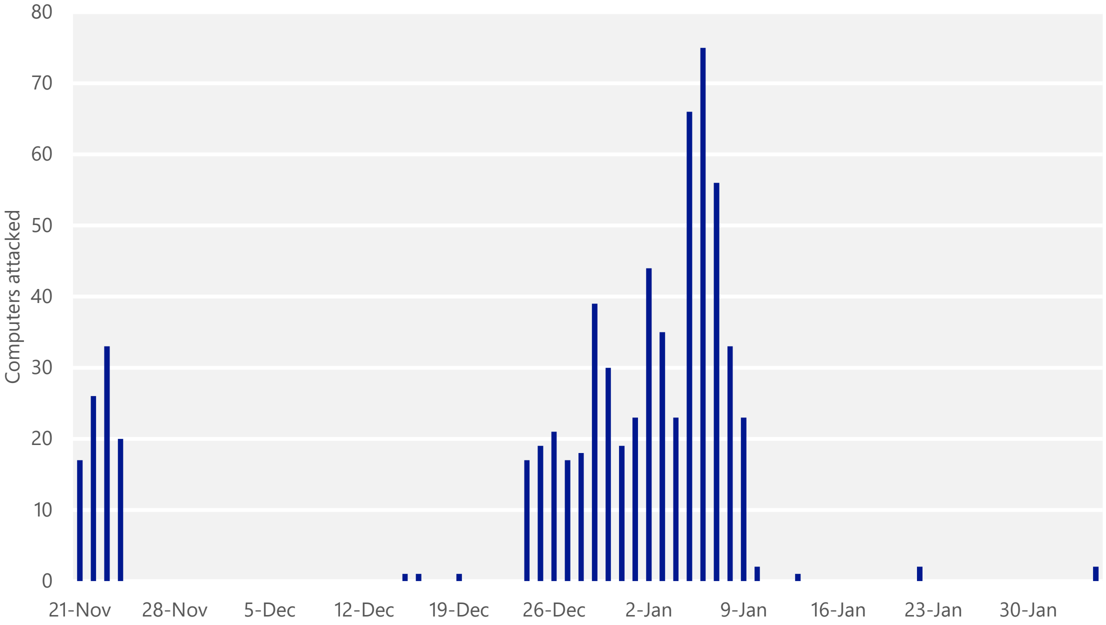
November 14: Watering hole attacks

On November 14, Microsoft began receiving data that showed the CVE-2014-6332 vulnerability and exploit being used in the wild. A review of internal telemetry suggested that several active campaigns were using the exploit in *watering hole attacks* that targeted specific industries and demographic groups by compromising websites used in those communities. Targeted groups included ethnic groups, users of certain government websites, democracy activist organizations, and university-based communities.

Late November: Attacks detected against government and aerospace websites

Microsoft identified an additional targeted attack campaign using CVE-2014-6332 that started in late November with attacks on government websites and spread to aerospace websites the following month. (See page 8 for more information about these attacks.)

Figure 2. Number of computers detected being attacked each day in the campaign against government and aerospace websites, November 2014–February 2015



Late November: CVE-2014-6332 added to exploit kits

CVE-2014-6332 exploits began appearing in exploit kits at around the time of the government website attacks. (See page 25 for more information on exploit kits.) Figure 3 lists the exploit kits that have been observed to include exploits for CVE-2014-6332.

Figure 3. Exploit kits known to target CVE-2014-6332

Exploit kit	Microsoft primary detection name	Date CVE-2014-6332 exploits first observed
Sweet Orange	Win32/Anogre	2014-11-19
Neutrino	JS/Neutrino	2014-11-20
Archie	Win32/Archost	2014-11-24
Flash	JS/Fashack	2014-12-13
Rig	JS/Meadgive	2014-12-18
Angler	JS/Axpergle	2014-12-27
Fiesta	JS/Fiexp	*Unknown*
Kaixin	JS/DonxRef	*Unknown*
Nuclear	JS/Neclu	*Unknown*
Magnitude	HTML/Pangimop	*Unknown*

The reliability of the CVE-2014-6332 exploit has made it one of the primary tools used by attackers, and Microsoft has observed significant variability in the obfuscation schemes attackers use to package the exploit in an effort to avoid detection by security software.

Analysis of CVE-2014-6332 targeted attacks

The script uses the memory corruption vulnerability to modify the property that normally prevents unsafe ActiveX controls from loading.

The CVE-2014-6332 vulnerability involves a bug in the way the VBScript engine in Internet Explorer handles array resizing. A successful exploit of the vulnerability results in memory corruption and enables the attacker to execute certain actions that VBScript is normally prevented from performing in the browser.[1]

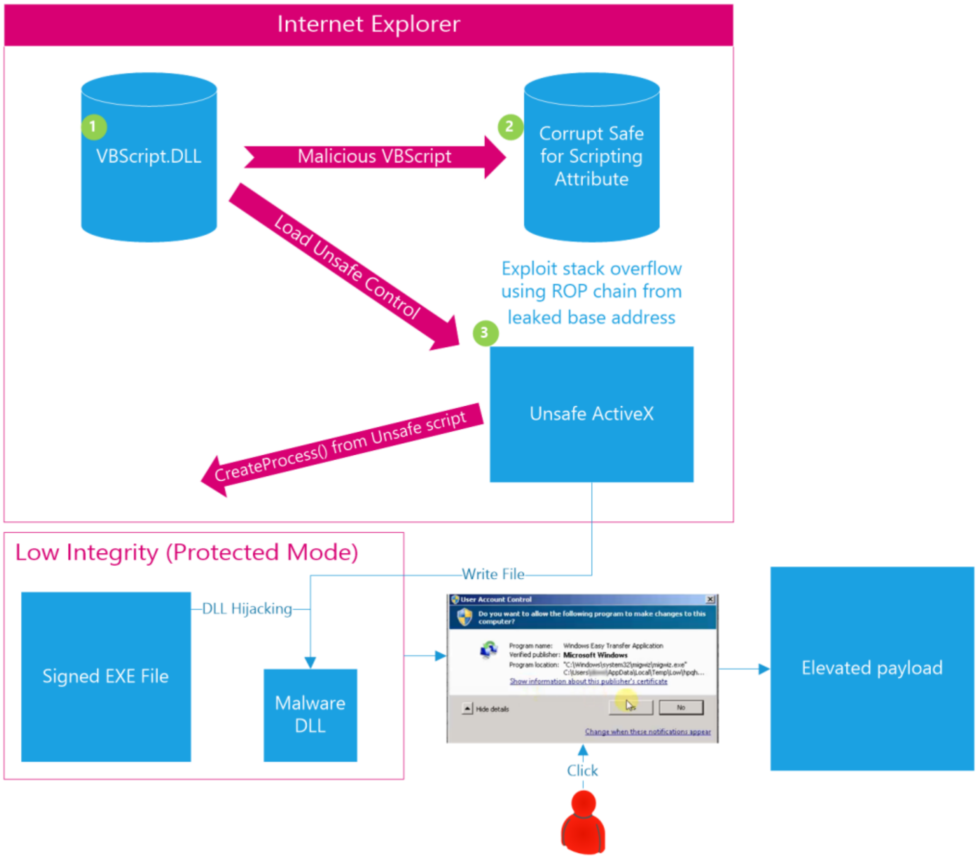
In a typical scenario, the attacker adds a malicious script based on the proof-of-concept code to a compromised webpage. When a user of a vulnerable computer visits the webpage using Internet Explorer, the script uses the memory corruption vulnerability to modify the "Safe for Scripting" property in

[1] Although VBScript is no longer supported in the Internet Explorer 11 document mode, web pages can still be written to use IE5, IE7, IE8, IE9, or IE10 document modes, and the CVE-2014-6332 vulnerability still applies to those document modes. The upcoming Microsoft Edge browser does not use VBScript or binary extensions, and is not susceptible to VBScript vulnerabilities.

memory, which typically prevents unsafe ActiveX controls from loading.

Disabling this property enables the attacker to load the **Wscript.Shell** ActiveX control in Internet Explorer. This control, which enables certain shell operations in VBScript, typically cannot be loaded by scripts on remote web pages because of the potential for abuse, but exploiting CVE-2014-6332 enables the attacker to bypass this restriction. The attacker can now use **Wscript.Shell** to perform a number of actions in Windows—including creating and executing files—without having to bypass additional exploit mitigations.

Figure 4. Mechanics of the CVE-2014-6332 exploit


Internet Explorer
1
VBScript.DLL
Malicious VBScript
2
Corrupt Safe for Scripting Attribute
Load Unsafe Control
Exploit stack overflow using ROP chain from leaked base address
3
Unsafe ActiveX
CreateProcess() from Unsafe script
Low Integrity (Protected Mode)
Write File
DLL Hijacking
Signed EXE File
Malware DLL
Elevated payload
Click

User Account Control

Do you want to allow the following program to make changes to this computer?

Program name: Windows Easy Transfer Application
Verified publisher: Microsoft Windows
Program location: "C:\Windows\system32\migwiz\migwiz.exe" C:\Users\[redacted]\AppData\Local\Temp\Low\hpqh...

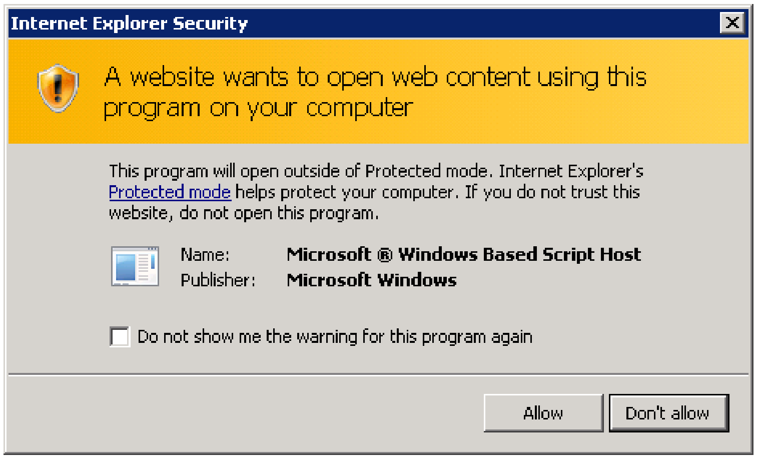
Show information about this publisher's certificate

Hide details
No
Change when these notifications appear

To help improve the attacker's chance of remaining undetected, the exploit writes the payload to an inconspicuous directory on the user's computer, such as C:\ProgramData\Microsoft\Windows\DRM\, and executes the file. Because Internet Explorer's protected mode prevents untrusted webpages from running programs locally, a standard dialog box prompts the user for permission to open the program outside of protected mode. If the user does not grant this permission, the Internet Explorer sandbox prevents the malware from executing.

If the user does grant permission, however, the malware will launch at the user's privilege level, thereby "escaping" the sandbox.

Figure 5. The warning dialog that appears when the exploit attempts to launch from Internet Explorer's protected mode


Internet Explorer Security

A website wants to open web content using this program on your computer

This program will open outside of Protected mode. Internet Explorer's Protected mode helps protect your computer. If you do not trust this website, do not open this program.

Name: Microsoft ® Windows Based Script Host
Publisher: Microsoft Windows

□ Do not show me the warning for this program again

The malware then attempts to connect to a command & control (C&C) server that security researchers have connected to a known espionage group.[2] A different C&C server observed by Microsoft was used in previous watering hole attacks, and has been connected to a different targeted attack group.[3]

Promptly installing security updates remains one of the best ways to defend against newly discovered threats.

The attack can also be packaged in other ways. In the attack on the government and aerospace websites, the CVE-2014-6332 exploit was repackaged within an Adobe Flash file, possibly in an attempt to avoid detection by security software. Interestingly, the exploit author within this campaign also chose to substitute the original "Safe-for-scripting" attack with an Adobe Flash-based return-oriented programming (ROP) exploit payload. The malicious Flash file used to package the exploit strongly resembles one used in a zero-day exploit distributed on forbes.com at around the same time that targeted CVE-2014-

[2] Gavin O'Gorman and Geoff McDonald, "The Elderwood Project," Symantec Corporation, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-elderwood-project.pdf.

[3] Jen Miller-Osborn and Ryan Olsen, "Recent Watering Hole Attacks Attributed to APT Group 'th3bug' Using Poison Ivy," Palo Alto Networks, September 19, 2014, http://researchcenter.paloaltonetworks.com/2014/09/recent-watering-hole-attacks-attributed-apt-group-th3bug-using-poison-ivy/.

9163,[4] a vulnerability in Adobe Flash addressed by Adobe Security Bulletin APSB14-27. The two files share many of the same variable names and display a high degree of code reuse, suggesting that they may have been created by the same malware author, or that the two attacks are connected in some other way.

Guidance: Defending against exploits

The events surrounding the disclosure and exploitation of the CVE-2014-6332 vulnerability demonstrate the risks that computer users worldwide face when updates are not applied quickly and fully working exploits are released to the public. In this case, both targeted attackers and opportunistic criminals quickly took advantage of freely available vulnerability and technique information to infect thousands of unpatched computers by compromising a number of high-profile websites.

In addition, CVE-2014-6332 serves as a reminder that promptly installing all relevant security updates as soon as is practical remains one of the best ways to help defend users and systems against newly discovered threats. Microsoft issued Security Bulletin MS14-064 to address the vulnerability before any exploits targeting the vulnerability were discovered in the wild; computer users and administrators who applied the security update the day it was released faced no risk from any of the subsequently discovered exploits. In fact, most exploit kits rely heavily on vulnerability exploits for which security updates have been available for months or even years—they target computers that do not have the appropriate updates installed, and therefore remain at risk.

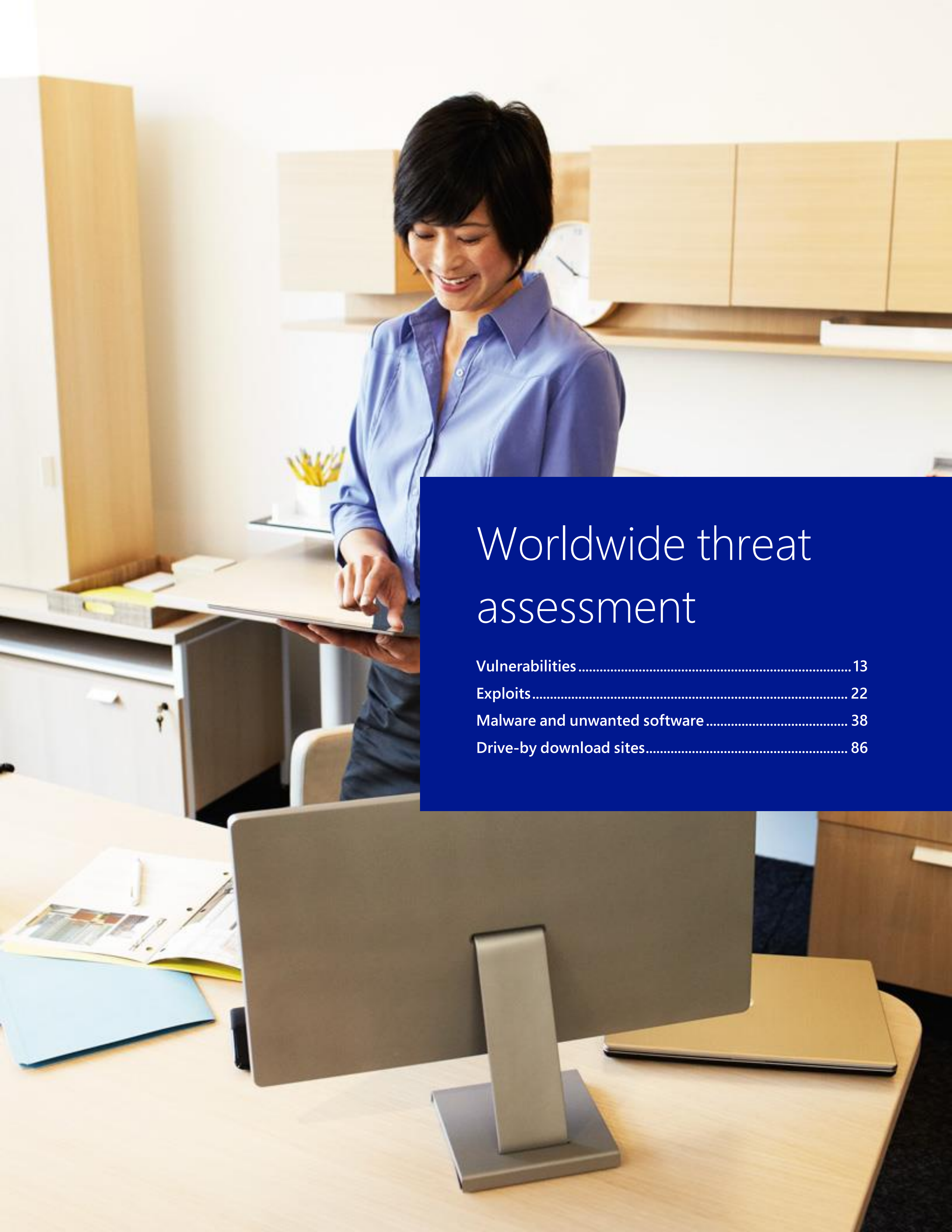
Additional steps users can take to reduce their risk from CVE-2014-6332 exploits and others include the following:

- System warnings. Pay close attention to security messages provided by Internet Explorer and Windows. Research has suggested that most successful attacks, such as the one described above, require some user interaction to be successful.
- Antimalware. Most popular antimalware products, including Microsoft Security Essentials, Windows Defender, and System Center Endpoint Protection (SCEP), have updated their signature files to detect and block the exploitation techniques described here. Running real-time security software

[4] Dan Goodin, "Pwned in 7 seconds: Hackers use Flash and IE to target Forbes visitors," *Ars Technica*, February 11, 2015, http://arstechnica.com/security/2015/02/11/pwned-in-7-seconds-hackers-use-flash-and-ie-to-target-forbes-visitors/.

from a reputable vendor and ensuring that its signature files are updated regularly is one of the best ways to defend against exploits and other types of malware.

- Browser. Users should keep their browser updated for the best security protection, and upgrade to the latest version of Internet Explorer to ensure that they will continue receiving security updates. Enabling Enhanced Protected Mode can help prevent exploits and malicious scripts from gaining unauthorized access to other parts of the computer, such as modifying system settings or writing to the Documents folder. Users running 64-bit editions of Windows can also enable 64-bit processes for Enhanced Protected Mode to apply an additional level of security.
- Applications. Whenever possible, use the newest available versions of applications to take advantage of the latest security fixes and improvements.



Worldwide threat assessment

Vulnerabilities

Vulnerabilities, in the context of computer security, are weaknesses in software that could allow an attacker to compromise the integrity, availability, or confidentiality of the software. Some of the worst vulnerabilities allow attackers to exploit the compromised system by causing it to run malicious code without the user's knowledge.

Industry-wide vulnerability disclosures

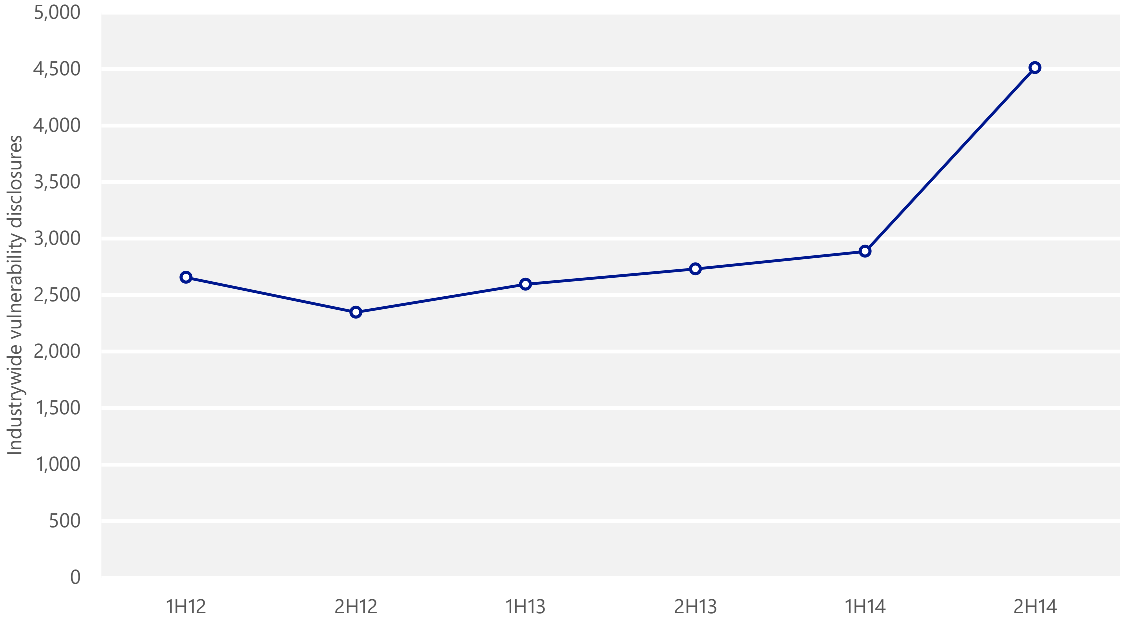
A *disclosure*, as the term is used in the *Microsoft Security Intelligence Report*, is the revelation of a software vulnerability to the public at large. Disclosures can come from a variety of sources, including publishers of the affected software, security software vendors, independent security researchers, and even malware creators.

The information in this section is compiled from vulnerability disclosure data that is published in the National Vulnerability Database (NVD), the US government's repository of standards-based vulnerability management data at nvd.nist.gov. The NVD represents all disclosures that have a published CVE (Common Vulnerabilities and Exposures) identifier.[5]

Figure 6 illustrates the number of vulnerability disclosures across the software industry for each half-year period since 1H12. (See "About this report" on page v for an explanation of the reporting period nomenclature used in this report.)

[5] CVE entries are subject to ongoing revision as software vendors and security researchers publish more information about vulnerabilities. For this reason, the statistics presented here may differ slightly from comparable statistics published in previous volumes of the *Microsoft Security Intelligence Report*.

Figure 6. Industrywide vulnerability disclosures, 1H12–2H14



- After several periods of small changes, vulnerability disclosures across the industry in 2H14 increased 56.3 percent from 1H14. The 4,512 vulnerabilities disclosed during 2H14 is the largest number of vulnerabilities disclosed in any half-year period since the Common Vulnerabilities and Exposures system was launched in 1999.
- This large increase in disclosures is predominantly the result of work performed by the Computer Emergency Response Team (CERT) Coordination Center (CERT/CC) in September and October 2014 to scan Android applications in the Google Play Store for man-in-the-middle vulnerabilities using an automated tool called CERT Tapioca.[6] CERT/CC determined that thousands of Android apps fail to properly validate SSL certificates provided by HTTPS connections, which could allow an attacker on the same network as an Android device to perform a man-in-the-middle attack on the device.[7] This project resulted in the creation of almost 1400 individual CVEs affecting thousands of different publishers of Android apps and code libraries.

Thousands of Android apps fail to properly validate SSL certificates provided by HTTP connections.

[6] Will Dormann, "Finding Android SSL Vulnerabilities with CERT Tapioca," *Cert/CC Blog*, September 3, 2014, http://www.cert.org/blogs/certcc/post.cfm?EntryID=204.

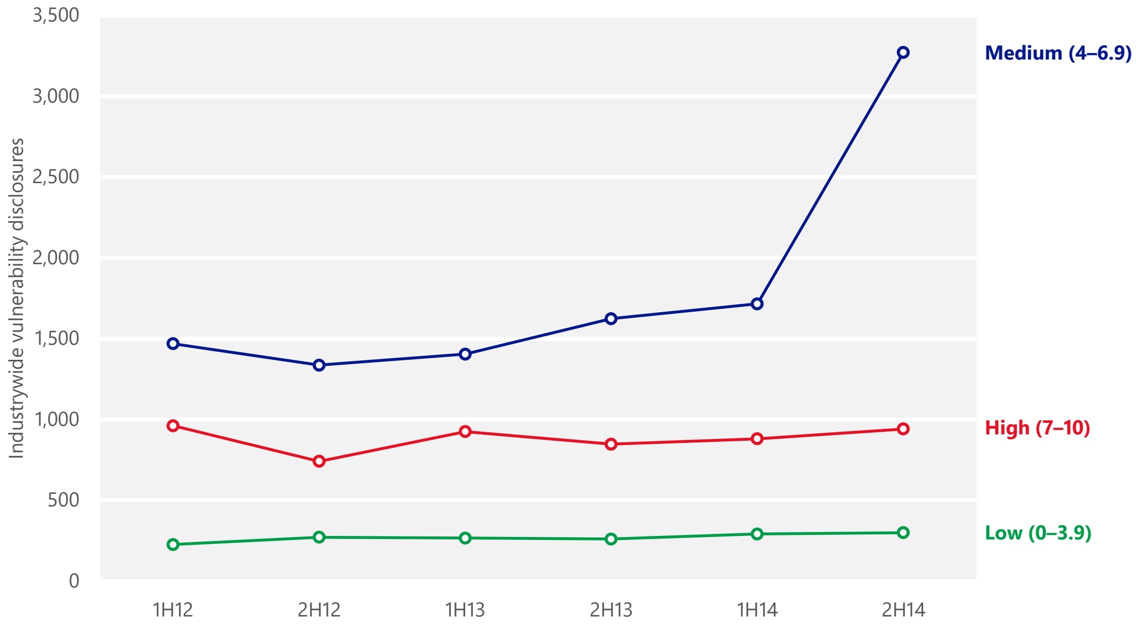
[7] CERT Coordination Center, "Vulnerability Note VU#582497: Multiple Android applications fail to properly validate SSL certificates," *Vulnerability Notes Database*, http://www.kb.cert.org/vuls/id/582497.

- All of the Android SSL vulnerabilities discovered by CERT/CC are medium-severity, medium-complexity vulnerabilities that affect non-operating-system applications.
- Without the Android vulnerabilities discovered by CERT/CC, disclosures in 2H14 would have only increased about 8 percent, which would be more in line with the increases observed over the past several half-year periods.

Vulnerability severity

The Common Vulnerability Scoring System (CVSS) is a standardized, platform-independent scoring system for rating IT vulnerabilities. The CVSS base metric assigns a numeric value between 0 and 10 to vulnerabilities according to severity, with higher scores representing greater severity. (See A Complete Guide to the Common Vulnerability Scoring System Version 2.0 at first.org for more information.)

Figure 7. Industrywide vulnerability disclosures by severity, 1H12–2H14

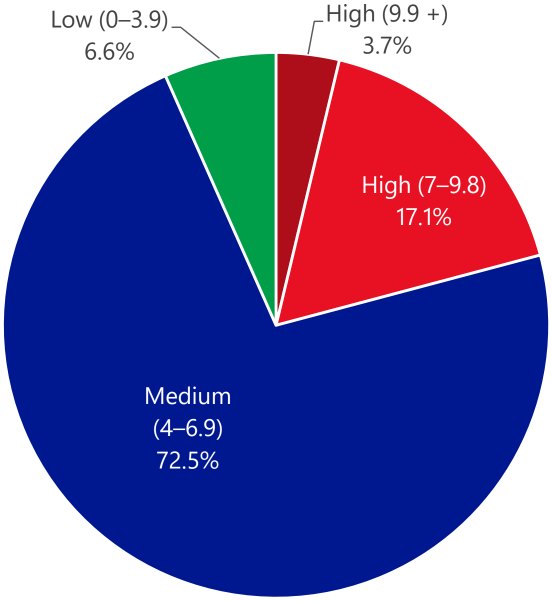


- Medium-severity vulnerabilities—those with CVSS scores from 4 to 7.9—accounted for almost the entire increase in disclosures seen in 2H14, increasing from 59.4 percent of all vulnerabilities in the first half of the year to 72.5 percent in the second. This increase is the result of a research project that uncovered SSL vulnerabilities in a large number of Android apps in the Google Play Store. (See page 14 for more information about this project.)

- By contrast, disclosures of high-severity and low-severity vulnerabilities remained mostly stable, with both categories increasing by less than 10 percent from 1H14 to 2H14. High-severity vulnerabilities accounted for the second-highest share of vulnerability disclosures in 2H14, at 20.9 percent (down from 30.5 percent in 1H14), and low-severity vulnerabilities accounted for the smallest share, at 6.6 percent (down from 10.1 percent in 1H14).
- As shown in Figure 8, the highest-severity vulnerabilities—those scoring 9.9 or higher on the CVSS scale—accounted for 3.7 percent of all vulnerabilities.

Disclosures of high-severity and low-severity vulnerabilities remained mostly stable.

Figure 8. Industrywide vulnerability disclosures in 2H14, by severity

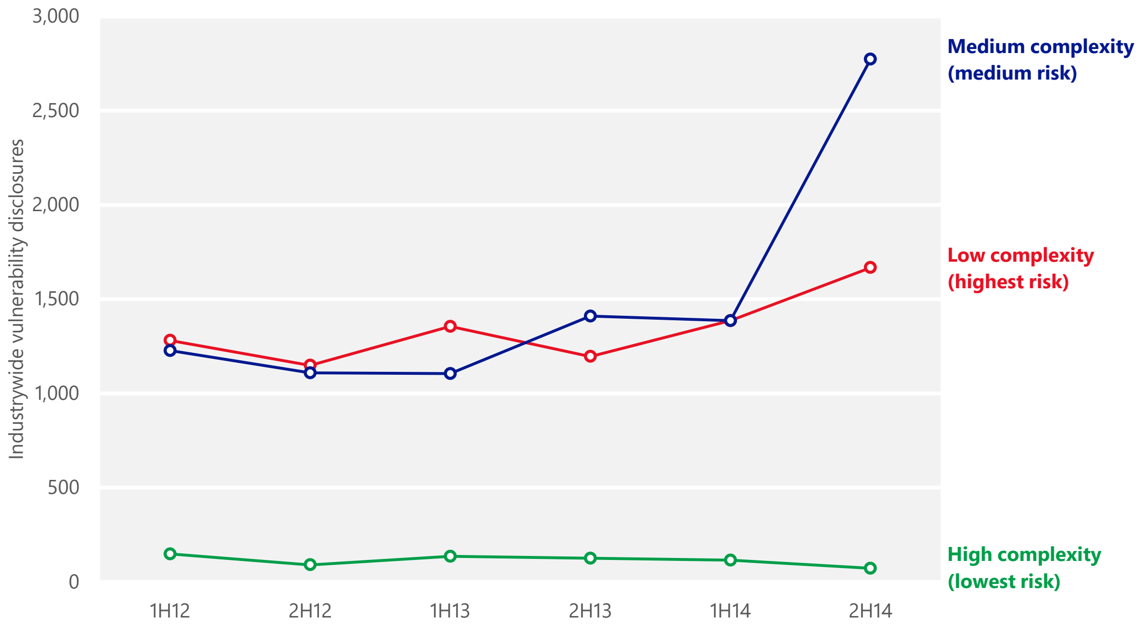


Vulnerability complexity

Some vulnerabilities are easier to exploit than others, and vulnerability complexity is an important factor to consider in determining the magnitude of the threat that a vulnerability poses. A high-severity vulnerability that can only be exploited under very specific and rare circumstances might require less immediate attention than a lower-severity vulnerability that can be exploited more easily.

The CVSS assigns each vulnerability a complexity ranking of Low, Medium, or High. (See A Complete Guide to the Common Vulnerability Scoring System Version 2.0 at first.org for more information about the CVSS complexity ranking system.) Figure 9 shows complexity trends for vulnerabilities disclosed since 1H12. Note that Low complexity in Figure 9 indicates greater risk, just as High severity indicates greater risk in Figure 7.

Figure 9. Industrywide vulnerability disclosures by access complexity, 1H12–2H14



- Medium-complexity vulnerabilities accounted for the largest category of disclosures in 2H14 as well as the bulk of the significant increase in total disclosures observed during the period. Medium-complexity vulnerability disclosures doubled from 1H14 to 2H14, increasing from 48.0 percent of all disclosures in the first half of the year to 61.5 percent in the second. The increase is the result of a research project that uncovered SSL vulnerabilities in a large number of Android apps in the Google Play Store. (See page 14 for more information about this project.)
- Disclosures of Low-complexity vulnerabilities—those that are the easiest to exploit—also increased significantly in 2H14. Low-complexity vulnerability disclosures increased 20.3 percent from 1H14 to 2H14, although their share of all vulnerabilities declined from 48.0 percent to 36.9 percent.
- Disclosures of High-complexity vulnerabilities decreased to 1.6 percent of all disclosures in 2H14, down from 4.0 percent in 1H14.

Disclosures of Low-complexity vulnerabilities—those that are the easiest to exploit—increased significantly in 2H14.

Operating system, browser, and application vulnerabilities

Comparing operating system vulnerabilities to non-operating system vulnerabilities that affect other components requires determining whether a particular program or component should be considered part of an operating system. This determination is not always simple and straightforward, given the componentized nature of modern operating systems. Some programs (media players, for example) ship by default with some operating system software but can also be downloaded from the software vendor's website and installed individually. Linux distributions, in particular, are often assembled from components developed by different teams, many of which provide crucial operating functions such as a graphical user interface (GUI) or Internet browsing.

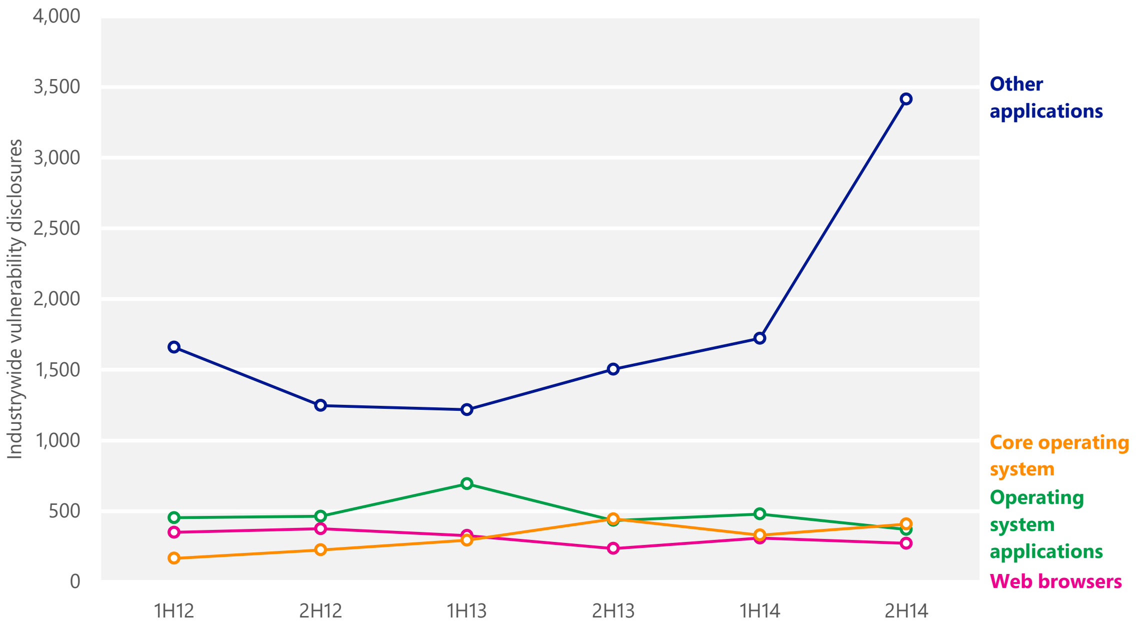
To facilitate analysis of operating system and browser vulnerabilities, the *Microsoft Security Intelligence Report* distinguishes among four different kinds of vulnerabilities:

- *Core operating system vulnerabilities* are those with at least one operating system platform enumeration ("/o") in the NVD that do not also have any application platform enumerations ("/a").[8]
- *Operating system application vulnerabilities* are those with at least one /o platform enumeration and at least one /a platform enumeration listed in the NVD, except as described in the next bullet point.
- *Browser vulnerabilities* are those that affect components defined as part of a web browser, including web browsers such as Internet Explorer and Apple's Safari that ship with operating systems, along with third-party browsers such as Mozilla Firefox and Google Chrome.
- *Other application vulnerabilities* are those with at least one /a platform enumeration in the NVD that do not have any /o platform enumerations, except as described in the previous bullet point.

Figure 10 shows industrywide vulnerabilities for operating systems, browsers, and applications since 1H12.

[8] See nvd.nist.gov/cpe.cfm for information about the Common Platform Enumeration (CPE) standard for naming information technology systems, software, and packages.

Figure 10. Industrywide operating system, browser, and application vulnerabilities, 1H12–2H14



- Disclosures of vulnerabilities in applications other than web browsers and operating system applications increased 98.3 percent in 2H14 and accounted for 76.5 percent of total disclosures for the period. The increase is the result of a research project that uncovered SSL vulnerabilities in a large number of Android apps in the Google Play Store. (See page 14 for more information about this project.)

- Core operating system vulnerability disclosures increased 23.6 percent in 2H14, although their share of all disclosures decreased from 11.6 percent in 1H14 to 9.1 percent in 2H14.

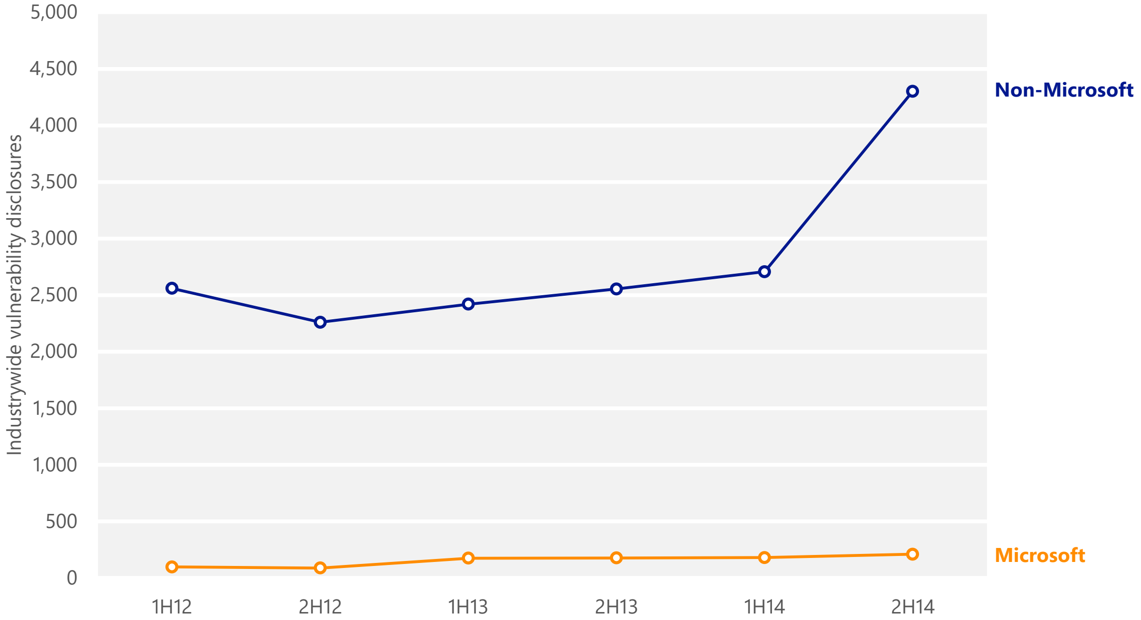
- Operating system application vulnerability disclosures decreased 22.8 percent in 2H14, and accounted for 8.3 percent of total disclosures for the period.

- Browser vulnerability disclosures decreased by 12.0 percent in 2H14, and accounted for 6.1 percent of total disclosures for the period.

Microsoft vulnerability disclosures

Figure 11 shows trends for vulnerability disclosures affecting Microsoft products compared to the rest of the industry.

Figure 11. Vulnerability disclosures for Microsoft and non-Microsoft products, 1H12–2H14



- Microsoft vulnerability disclosures increased from 180 disclosures in 1H14 to 210 in 2H14, an increase of 16.7 percent.
- At the same time, disclosures affecting non-Microsoft software increased 93.8 percent. This increase is the result of a research project that uncovered SSL vulnerabilities in a large number of Android apps in the Google Play Store. (See page 14 for more information about this project.)

Guidance: Developing secure software

Using a methodology like the SDL can help reduce the number and severity of vulnerabilities in software.

The Security Development Lifecycle (SDL) (www.microsoft.com/sdl) is a free software development methodology that incorporates security and privacy best practices throughout all phases of the development process, with the goal of protecting software users. Using such a methodology can help reduce the number and severity of vulnerabilities in software and help manage vulnerabilities that might be discovered after deployment.

"Life in the Digital Crosshairs," at sdlstory.com, is a multimedia presentation that explores the genesis and development of the SDL from its origins in the Windows team's well-documented all-hands security push in the early 2000s. It includes interviews with several of the pivotal figures in the history of the SDL and Microsoft's focus on secure software. Security professionals and anyone else with an interest in secure development are likely to find the site invaluable for putting the SDL into historical context and understanding what the future holds.

To learn more about how the SDL is applied in the present day, see "State of Application Security: Immature Practices Fuel Inefficiencies, but Positive ROI Is Attainable - A Forrester Consulting Thought Leadership Paper Commissioned by Microsoft" to learn how organizations are putting SDL techniques to work for them, and "Secure Software Development Trends in the Oil & Gas Sectors" for an example of how the SDL has helped one critical industry. Both papers are available from the Microsoft Download Center (www.microsoft.com/download).

Exploits

An *exploit* is a piece of code that uses software vulnerabilities to access information on a computer or install malware. Exploits target vulnerabilities in operating systems, web browsers, applications, or software components that are installed on a computer.

In some scenarios, targeted components are add-ons that may be pre-installed by the computer manufacturer before the computer is sold. A user may not even use the vulnerable add-on or be aware that it is installed. In addition, some software has no facility for updating itself, so even if the software vendor publishes an update that fixes the vulnerability, the user may not know that the update is available or how to obtain it and therefore remains vulnerable to attack.[9]

Software vulnerabilities are enumerated and documented in the Common Vulnerabilities and Exposures (CVE) list (cve.mitre.org), a standardized repository of vulnerability information. Here and throughout this report, exploits are labeled with the CVE identifier that pertains to the affected vulnerability, if applicable. In addition, exploits that affect vulnerabilities in Microsoft software are labeled with the Microsoft Security Bulletin number that pertains to the vulnerability, if applicable.[10]

Microsoft real-time security products can detect and block attempts to exploit known vulnerabilities whether the computer is affected by the vulnerabilities or not. For example, the CVE-2010-2568 CplLnk vulnerability has never affected Windows 8, but if a Windows 8 user receives a malicious file that attempts to exploit that vulnerability, Windows Defender is designed to detect and block it anyway. Encounter data provides important information about which products and vulnerabilities are being targeted by attackers, and by what means.

[9] See the Microsoft Security Update Guide, Second Edition at the Microsoft Download Center (www.microsoft.com/download) for guidance to help protect your IT infrastructure while creating a safer, more secure computing and Internet environment.

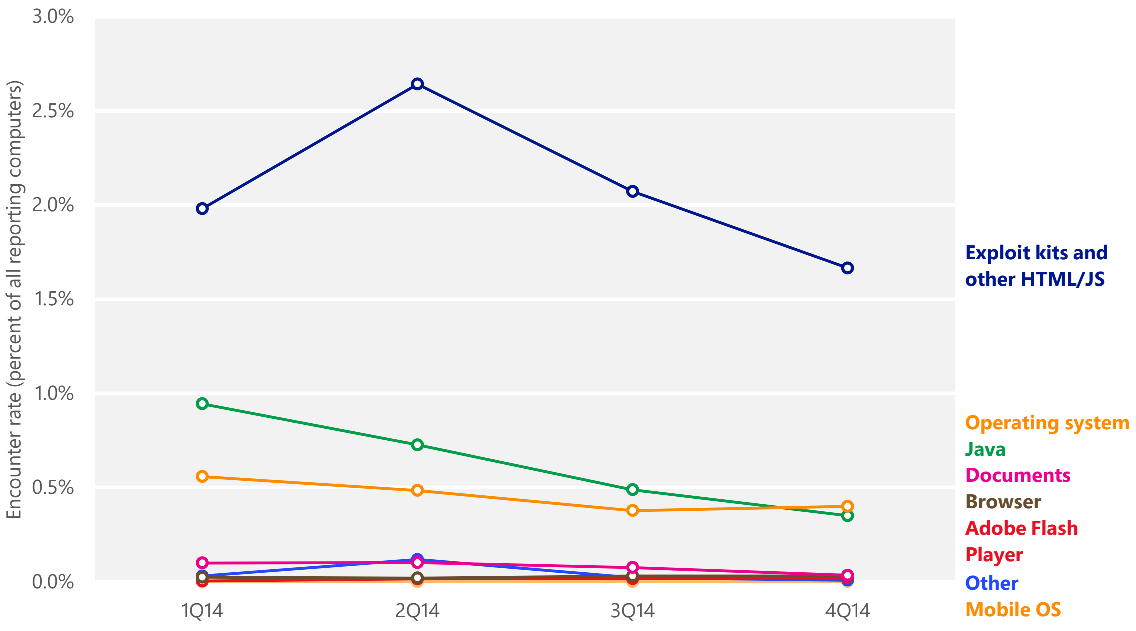
[10] See technet.microsoft.com/security/bulletin to search and read Microsoft Security Bulletins.

However, the statistics presented in this report should not be interpreted as evidence of successful exploit attempts, or of the relative vulnerability of computers to different exploits.

Figure 12 shows the prevalence of different types of exploits detected by Microsoft antimalware products in each quarter in 2014, by encounter rate. *Encounter rate* is the percentage of computers running Microsoft real-time security products that report a malware encounter. For example, the encounter rate for Java exploit attempts in 4Q14 was 0.35 percent, meaning that 0.35 percent of computers running Microsoft real-time security software in 4Q14 encountered Java exploit attempts, and 99.65 percent did not. In other words, a computer selected at random would have had about a 0.35 percent chance of encountering a Java exploit attempt in 4Q14. Only computers whose users have opted in to provide data to Microsoft are considered when calculating encounter rates.[11] See page 38 for more information about the encounter rate metric.

> Microsoft security products can detect and block attempts to exploit known vulnerabilities whether the computer is affected by the vulnerability or not.

Figure 12. Encounter rates for different types of exploit attempts in 2014



[11] For information about the products and services that provide data for this report, see "Appendix B: Data sources" on page 107.

- Computers that report more than one type of exploit are counted for each type detected.
- Encounters with exploit kits and other HTML and JavaScript (JS) threats decreased by nearly a third between 2Q14 and 4Q14, but remained the most commonly encountered type of exploit in the second half of the year, with an encounter rate more than four times as high as the next most common type of exploit. See "Exploit kits and other HTML/JavaScript exploits" on page 25 for more information about these exploits.
- Encounters with Java exploits decreased each quarter, becoming the third-most commonly encountered type of exploit by the fourth quarter, while remaining the second-most commonly encountered type of exploit in 2H14. See "Java exploits" on page 28 for more information.
- Encounters with exploits that target operating systems increased slightly to become the second-most commonly encountered type of exploits in 4Q14.
- Encounters with document, Adobe Flash Player, and browser exploits remained mostly stable during the second half of the year, and each accounted for a small percentage of total exploits.

Exploit families

Figure 13 lists the exploit-related malware families that were detected most often during the second half of 2014.

Figure 13. Quarterly encounter rate trends for the exploit families most commonly detected and blocked by Microsoft real-time antimalware products in 2H14, shaded according to relative prevalence

Exploit	Type	1Q14	2Q14	3Q14	4Q14
JS/Axpergle	Exploit kit	0.55%	1.04%	0.87%	0.86%
JS/Anogre	Exploit kit	0.04%	0.15%	0.60%	0.43%
CVE-2010-2568 (CplLnk)	Operating system	0.50%	0.44%	0.35%	0.35%
JS/Fiexp	Exploit kit	0.18%	0.31%	0.31%	0.30%
HTML/Meadgive	Exploit kit	0.03%	0.17%	0.15%	0.08%
HTML/IframeRef	Generic	0.34%	0.18%	0.10%	0.09%
JS/Neclu	Exploit kit	0.44%	0.65%	0.11%	0.06%
CVE-2012-1723	Java	0.24%	0.16%	0.10%	0.06%
CVE-2012-0507	Java	0.16%	0.09%	0.07%	0.05%
Java/Obfuscator	Java	0.00%	0.07%	0.05%	0.05%

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

- Exploit kits accounted for 5 of the 10 most commonly encountered exploits during the second half of the year. See page 25 for more information about exploit kits.
- CVE-2010-2568, the most commonly targeted individual vulnerability in 2H14, 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.
- 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 may be changed frequently.

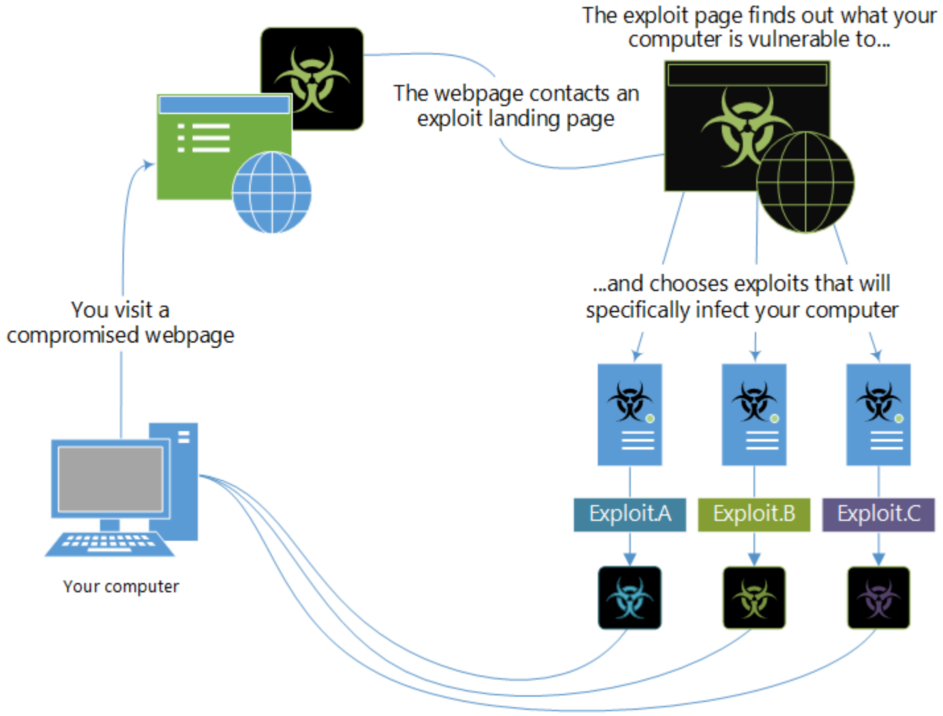
> HTML/IframeRef is a generic detection for HTML inline frames that redirect to remote websites that contain malicious content.

- Obfuscator is a generic detection for programs that have been modified by malware obfuscation tools. See page 61 for more information.
- Three of the top 10 exploits encountered in 2H14 are Java exploits. See page 28 for more information about these exploits.

Exploit kits and other HTML/JavaScript exploits

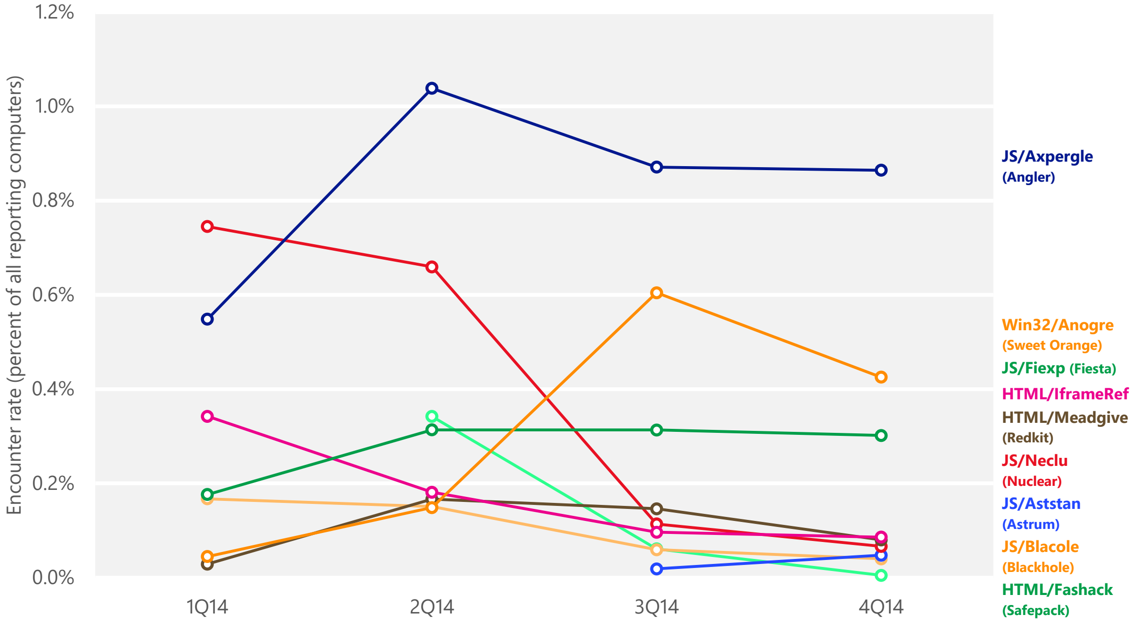
Exploit kits are collections of exploits bundled together and sold as commercial software or as a service. Prospective attackers buy or rent exploit kits on malicious hacker forums and through other illegitimate outlets. A typical kit comprises a collection of webpages that contain exploits for several vulnerabilities in popular web browsers and browser add-ons. When the attacker installs the kit on a malicious or compromised web server, visitors who don't have the appropriate security updates installed are at risk of having their computers compromised through drive-by download attacks.

Figure 14. How a typical exploit kit works


The exploit page finds out what your computer is vulnerable to...
The webpage contacts an exploit landing page
You visit a compromised webpage
...and chooses exploits that will specifically infect your computer
Exploit.A
Exploit.B
Exploit.C
Your computer

Microsoft security products detect and block the characteristic techniques that a number of common exploit kits use to infect computers, along with several generic HTML and JavaScript exploit techniques. Figure 15 shows the prevalence of several top web-based exploit kits and techniques during each of the four most recent quarters.

Figure 15. Trends for the top exploit kits and generic HTML/JavaScript threats detected and blocked by Microsoft real-time antimalware products in 2H14



- JS/Axpergle, a detection for the so-called Angler exploit kit, was the most commonly encountered exploit kit family in 2H14. The Angler kit first appeared in 3Q14 and rapidly increased in prominence during the second quarter. It is known to target a number of vulnerabilities in Silverlight (CVE-2013-0074), Internet Explorer (CVE-2013-2551), Adobe Flash Player (CVE-2013-0634 and CVE-2013-5329), and Java (CVE-2013-2460), although exploit kit authors frequently change the exploits included in their kits in an effort to stay ahead of software publishers and security software vendors.
- Win32/Anogre is a detection for the Sweet Orange exploit kit, which targets vulnerabilities in Java (CVE-2013-0422), Adobe Flash Player (CVE-2014-0497 and CVE-2014-0515), and the TrueType font rendering engine in Windows (CVE-2011-3402), among others.
- The Fiesta exploit kit (detected as JS/Fiexp) was responsible for the third-largest number of exploit kit encounters in 2H14. It targets vulnerabilities in Silverlight (CVE-2013-0074), Internet Explorer (CVE-2014-0322), and Java (CVE-2012-0507, CVE-2013-1493, and CVE-2013-2463), among others.

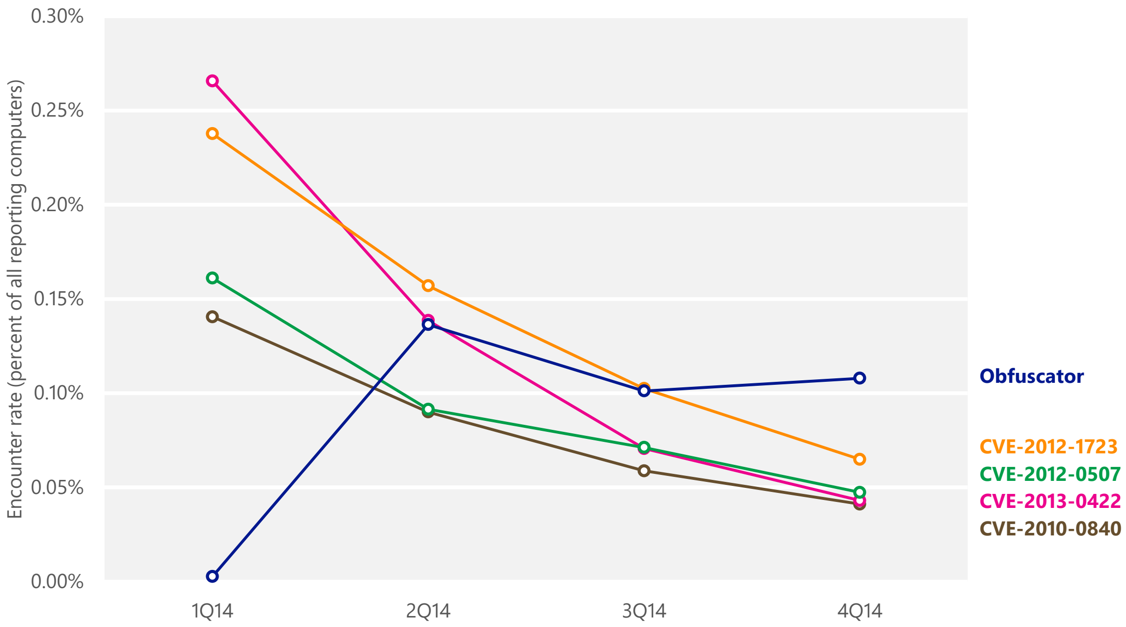
A typical exploit kit comprises a collection of webpages that contain exploits for several vulnerabilities in popular web browsers and browser add-ons.

- Detections of the Nuclear exploit kit (detected as JS/Neclu) decreased significantly in 3Q14, making it the fourth-most commonly encountered exploit kit during the second half of the year.

Java exploits

Figure 16 shows the prevalence of different Java exploits by quarter.

Figure 16. Trends for the top Java exploits detected and blocked by Microsoft real-time antimalware products in 2H14



- Overall, encounters with Java exploits continued to decrease significantly in 2H14. This decrease is likely caused by several important changes in the way web browsers evaluate and execute Java applets:
  - The IExtensionValidation interface in Internet Explorer 11, released in late 2013, provides a mechanism for security software to validate that a webpage is safe before allowing instantiation of ActiveX controls, such as the control that hosts embedded Java applets. If a webpage is determined to be malicious, the ActiveX controls are blocked from loading, and the actual Java exploit itself is therefore never encountered. (See “Exploit detection with Internet Explorer and IExtensionValidation” on page 33 for more information.) Subsequent Internet Explorer security updates released in June and July added an isolated heap mechanism

and a deferred-free method to mitigate use-after-free bugs, which further hardened Internet Explorer against Java exploitation.

  - Beginning with Java 7 update 51, released in January 2014, the Java Runtime Environment (JRE) requires Java applets running in web browsers to be digitally signed by default.

- Obfuscator is a generic detection for programs that have been modified by malware obfuscation, often in an attempt to avoid detection by security software. Files identified as Java/Obfuscator can represent exploits that target many different Java vulnerabilities. The increase in Java/Obfuscator encounters beginning in 2Q14 is primarily caused by detection changes and improvements.

> Beginning in January 2014, the JRE requires Java applet running in web browsers to be digitally signed by default.

- CVE-2012-1723, the most commonly encountered individual Java exploit in 4Q14, is a type-confusion vulnerability in the Java Runtime Environment (JRE), which is exploited by tricking the JRE into treating one type of variable like another type. Oracle confirmed the existence of the vulnerability in June 2012, and addressed it the same month with its June 2012 Critical Patch Update. The vulnerability was observed being exploited in the wild beginning in early July 2012, and has been used in a number of exploit kits.

  For more information about this exploit, see the entry "The rise of a new Java vulnerability - CVE-2012-1723" (August 1, 2012) in the Microsoft Malware Protection Center (MMPC) blog at blogs.technet.com/mmpc.

- CVE-2012-0507, the second-most commonly encountered individual Java exploit in 2H14, allows an unsigned Java applet to gain elevated permissions and potentially have unrestricted access to a host system outside its sandbox environment. The vulnerability is a logic error that allows attackers to run code with the privileges of the current user, which means that an attacker can use it to perform reliable exploitation on other platforms that support the JRE, including Apple Mac OS X, Linux, VMWare, and others. Oracle released a security update in February 2012 to address the issue.

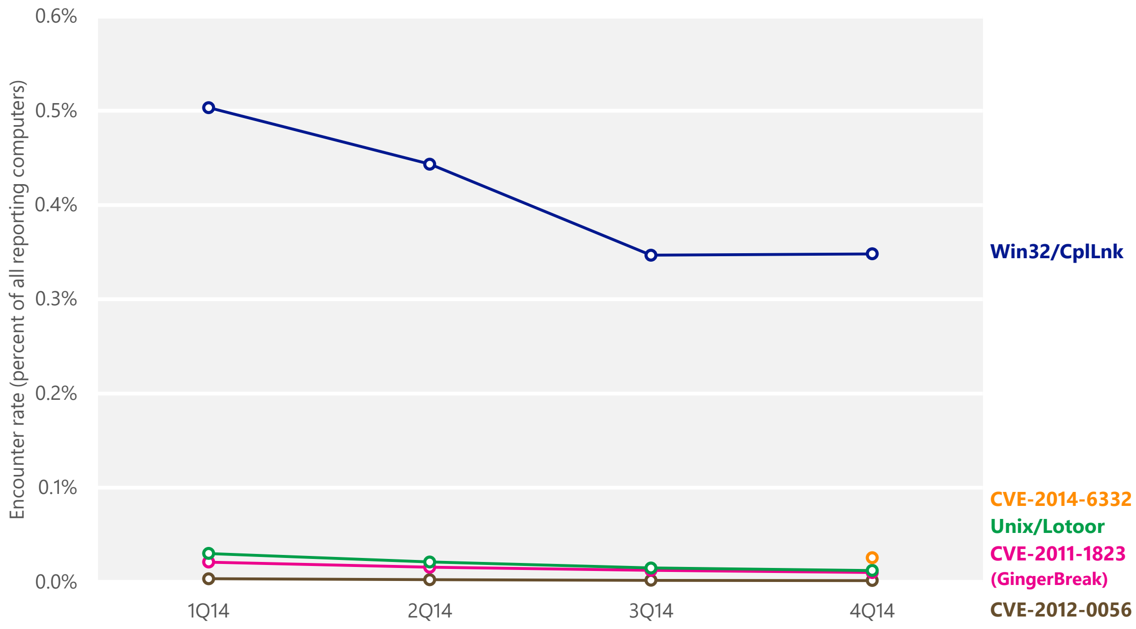
- CVE-2013-0422, the third-most commonly encountered individual Java exploit in 2H14, first appeared in January 2013 as a zero-day vulnerability. CVE-2013-0422 is a package access check vulnerability that allows an untrusted Java applet to access code in a trusted class, which then loads the attacker's own class with elevated privileges. Oracle published a security update to address the vulnerability on January 13, 2013.

For more information about CVE-2013-0422, see the entry "A technical analysis of a new Java vulnerability (CVE-2013-0422)" (January 20, 2013) in the MMPC blog at blogs.technet.com/mmpc.

Operating system exploits

Although most operating system exploits detected by Microsoft security products are designed to affect the platforms on which the security products run, malicious or infected files that affect other operating systems are sometimes downloaded. Figure 17 shows trends for the individual exploits most commonly detected and blocked or removed during each of the past four quarters.

Figure 17. Individual operating system exploits detected and blocked by Microsoft real-time antimalware products in 2014



- Win32/CplLnk, an exploit that targets a vulnerability in Windows Shell, remained the most commonly encountered operating system exploit in 2H14. An attacker exploits the vulnerability (CVE-2010-2568) by creating a malformed shortcut file that forces a vulnerable computer to load a malicious file when the shortcut icon is displayed in Windows Explorer. Microsoft released Security Bulletin MS10-046 in August 2010 to address this issue.

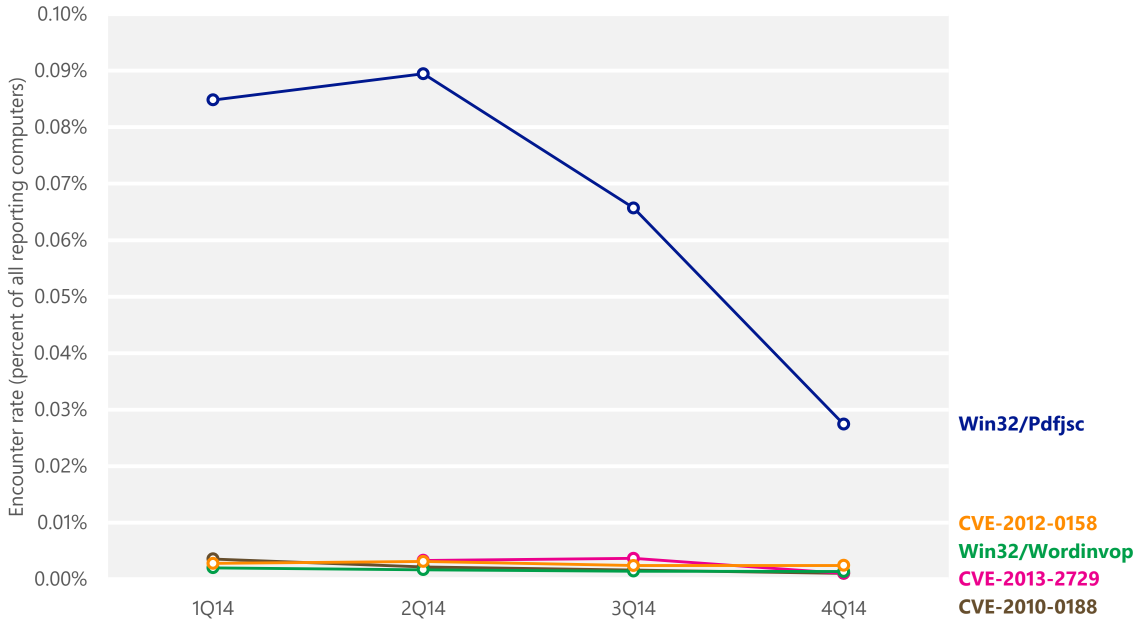
- CVE-2014-6332 is a vulnerability in Windows Object Linking and Embedding (OLE) that can be used to perform remote attacks on a computer through Internet Explorer in some circumstances. Microsoft released Security Bulletin MS14-064 in November 2014 to address this issue. See "The life and times of an exploit" on page 3 for more information about this vulnerability and what Microsoft has done to mitigate it.
- Two of the five most commonly encountered operating system exploits on Windows computers in 2H14 actually target the Android mobile operating system published by Google and the Open Handset Alliance. Microsoft security products detect these threats when Android devices or storage cards are connected to computers running Windows, or when Android users knowingly or unknowingly download infected or malicious programs to their computers before transferring the software to their devices. Most detections that affect Android involve exploits that enable an attacker or other user to obtain root privileges on vulnerable Android devices. Device owners sometimes use such exploits intentionally to gain access to additional functionality (a practice often called *rooting* or *jailbreaking*), but these exploits can also be used by attackers to infect devices with malware that bypasses many typical security systems.
    - Unix/Lotoor is an exploit family that exploits vulnerabilities in the Android operating system to gain root privileges on a mobile device. Google published a source code update in March 2011 that addressed the vulnerability.
    - CVE-2011-1823 is sometimes called the GingerBreak vulnerability because of its use by a popular rooting application of that name. It is also used by AndroidOS/GingerMaster, a malicious program that can allow a remote attacker to gain access to the mobile device. GingerMaster may be bundled with clean applications, and includes an exploit for the CVE-2011-1823 vulnerability disguised as an image file. Google published a source code update in May 2011 that addressed the vulnerability.

> Two of the five most commonly encountered system exploits on Windows computers in 2H14 actually target the Android mobile operating system.

Document exploits

Document exploits are exploits that target vulnerabilities in the way a document editing or viewing application processes a particular file format. Figure 18 shows encounter rates for individual exploits.

Figure 18. Individual document exploits detected and blocked by Microsoft real-time antimalware products in 2014

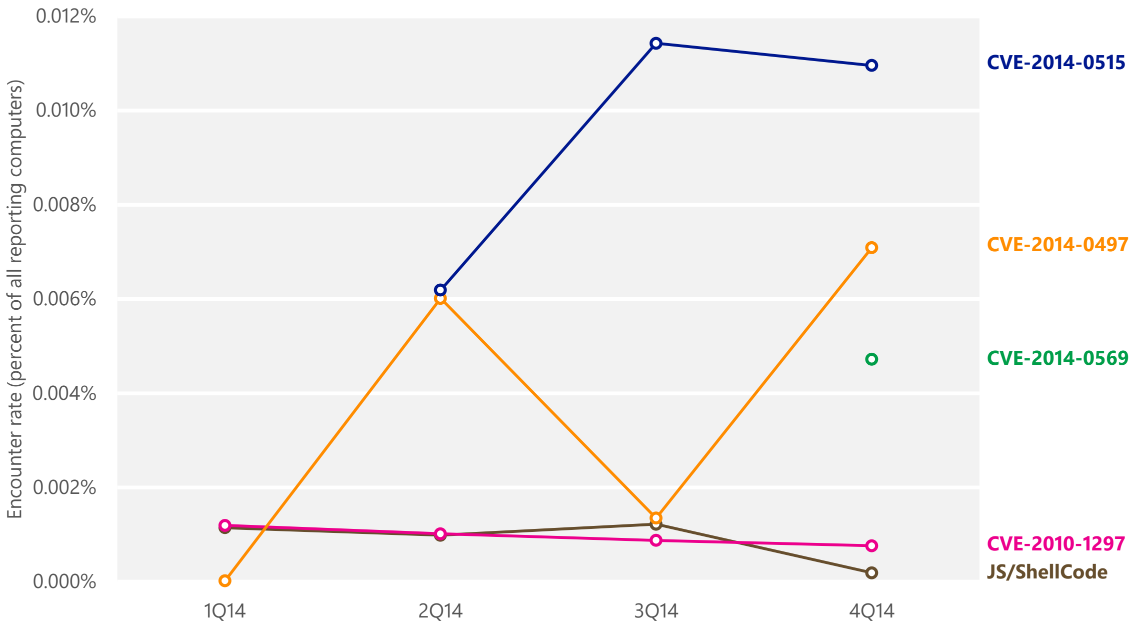


- Most detections of exploits that affect Adobe Reader and Adobe Acrobat were associated with the exploit family Win32/Pdfjsc, a detection for PDF files containing malicious JavaScript that targets CVE-2010-0188 and other vulnerabilities. Adobe released Security Bulletin APSB10-07 in February 2010 to address CVE-2010-0188. Pdfjsc and related exploits were particularly prevalent in Russian-speaking regions. Pdfjsc mostly targets older Java vulnerabilities, so attackers may find it less useful as more computers are updated to newer versions of Java, which could explain the decrease in encounters in the second half of the year.

Adobe Flash Player exploits

Figure 19 shows the prevalence of different Adobe Flash Player exploits by quarter.

Figure 19. Adobe Flash Player exploits detected and blocked by Microsoft real-time antimalware products in 2014

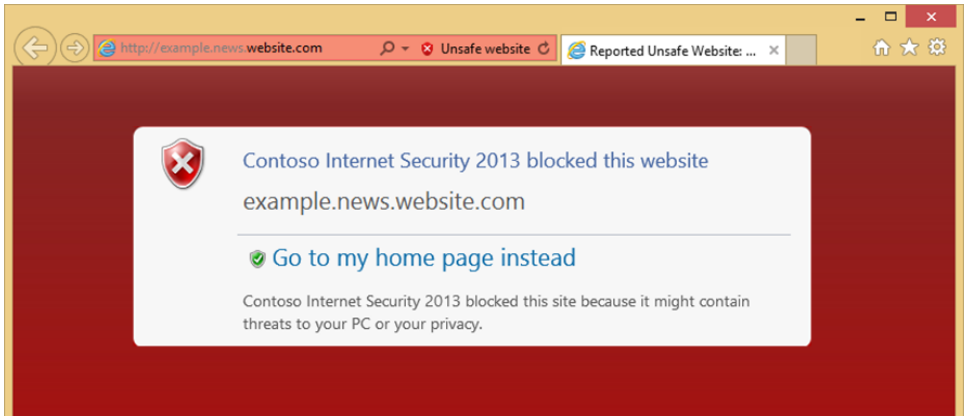


- CVE-2014-0515, the most commonly exploited Adobe Flash Player vulnerability in 2H14, is a buffer overflow vulnerability. Adobe released Security Bulletin APSB14-13 on April 28, 2014 to address the issue.
- CVE-2014-0497, the second-most commonly exploited Adobe Flash Player vulnerability in 2H14, is an integer underflow vulnerability. Adobe released Security Bulletin APSB14-04 on February 4, 2014 to address the issue.
- CVE-2010-1297, the third-most commonly exploited Adobe Flash Player vulnerability in 2H14, is a memory corruption vulnerability in some releases of Adobe Flash Player versions 9 and 10 and earlier versions. Adobe released Security Bulletin APSB10-14 on June 10, 2010 to address the issue.

Exploit detection with Internet Explorer and IExtensionValidation

IExtensionValidation is an interface introduced in Internet Explorer 11 that real-time security software can implement to block ActiveX controls from loading on malicious pages. When Internet Explorer loads a webpage that includes ActiveX controls, if the security software has implemented IExtensionValidation, the browser calls the security software to scan the HTML and script content on the page before loading the controls themselves. If the security software determines that the page is malicious (for example, if it identifies the page as an exploit kit landing page), it can direct Internet Explorer to prevent individual controls or the entire page from loading.

Figure 20. Internet Explorer 11 can block pages that contain ActiveX controls if security software determines that the page is malicious



Contoso Internet Security 2013 blocked this website

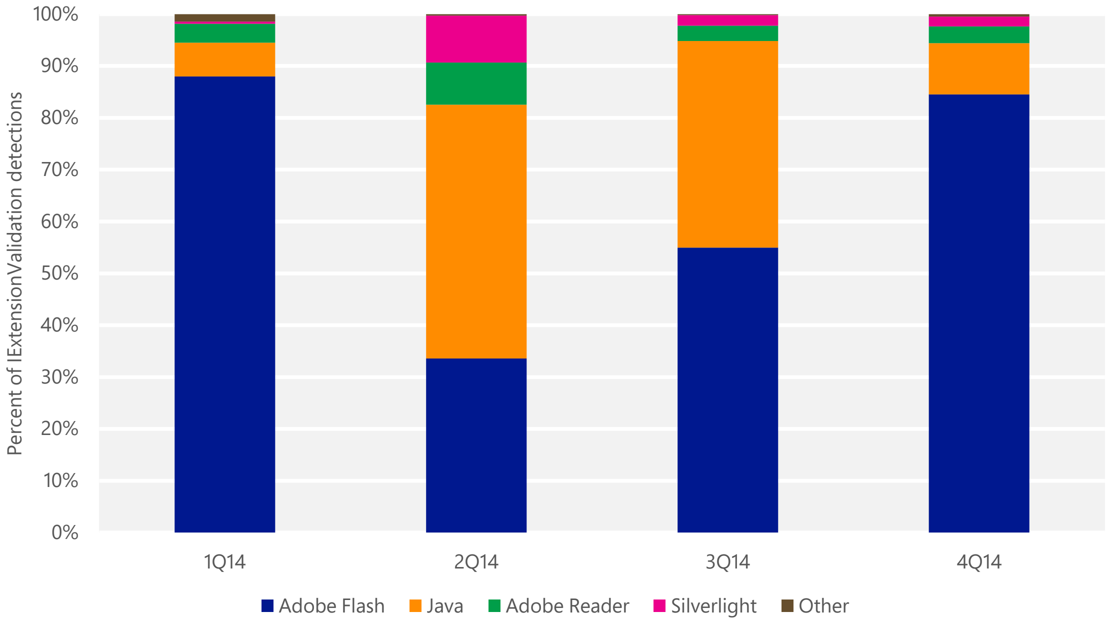
example.news.website.com

Go to my home page instead

Contoso Internet Security 2013 blocked this site because it might contain threats to your PC or your privacy.

Figure 21 shows the types of ActiveX controls identified on malicious webpages in Internet Explorer 11 for each quarter in 2014.

Figure 21. ActiveX controls detected on malicious webpages through IExtensionValidation in 2014, by control type



- Adobe Flash objects were the most commonly detected type of object hosted on malicious pages in every quarter except 2Q14.
- After accounting for a high of 48.9 percent of object detections in 2Q14, detections of Java applets on malicious pages decreased to 39.8 percent of

detections in 3Q14, then decreased again to 9.9 percent of detections in 4Q14. This decline may be related to new security requirements in recent versions of Java that require applets in web pages to be digitally signed by default. (See "Java exploits" on page 28 for more information.) If so, the decreases observed here may be expected to continue.

Exploits used in targeted attacks

A *targeted attack* is a malware attack against a specific group of companies or individuals. This type of attack usually attempts to gain access to the computer or network before trying to steal information or disrupt the infected computers. The following paragraphs describe some of the exploits Microsoft has observed being used in targeted attacks in 2H14.

CVE-2014-6332: Remote code execution vulnerability in Windows OLE (MS14-064)

CVE-2014-6332, a vulnerability in Windows Object Linking and Embedding (OLE), was disclosed in November 2014 and quickly began to be used in targeted attacks. See "The life and times of an exploit" on page 3 for in-depth information about this vulnerability and how it has been exploited.

CVE-2014-4114 and CVE-2014-6352: Remote code execution vulnerabilities in Windows OLE (MS14-060, MS14-064)

CVE-2014-4114, a vulnerability in Windows OLE, was addressed by Security Bulletin MS14-060 in October 2014; a closely related vulnerability, CVE-2014-6352, was addressed by Security Bulletin MS14-064 the following month. CVE-2014-4114 and CVE-2014-6352 are non-memory-corruption vulnerabilities in Windows Packager, a component of OLE, that can be exploited via a malicious PowerPoint presentation sent as an email attachment or downloaded from a malicious or compromised website. The vulnerabilities can be reliably exploited to launch a remote executable hosted on the attacker's server.

> CVE-2014-4114 has been used to target SCADA industrial control systems.

CVE-2014-4114 was originally discovered by iSIGHT Partners, which observed a known targeted attack group using it against western European governments.[12] Later, Trend Micro and iSIGHT found evidence that the vulnerability has been

[12] Stephen Ward, "iSIGHT discovers zero-day vulnerability CVE-2014-4114 used in Russian cyber-espionage campaign," iSIGHT Partners, October 14, 2014, www.isightpartners.com/2014/10/cve-2014-4114/.

used to target supervisory control and data acquisition (SCADA) industrial control systems and install a variant of the "BlackEnergy" malware family (detected as Win32/Phdet by Microsoft security products).[13] CVE-2014-6352 was reported by McAfee and Google after Security Bulletin MS14-060 was released to address the earlier vulnerability. Like CVE-2014-4114, this vulnerability can be exploited via a malicious PowerPoint presentation, among other methods.

CVE-2014-6324: Elevation of privilege vulnerabilities in Windows Kerberos (MS14-068)

CVE-2014-6324, a vulnerability in Windows Kerberos, was addressed by Security Bulletin MS14-068 in November 2014. CVE-2014-6324 allows remote elevation of privilege in domains running Windows domain controllers. An attacker with the credentials of any domain user can elevate their privileges to that of any other account on the domain, including domain administrator accounts. It is typically exploited against the domain controller from a compromised workstation computer in the domain. CVE-2014-6324 can be very reliably exploited on computers that have not been updated with Security Bulletin MS14-068. Exploits are hard to detect, and a successful attacker can use the vulnerability to easily move from computer to computer within a domain.

Exploits of CVE-2014-6234 are hard to detect, and a successful attacker can use the vulnerability to easily move from computer to computer within a domain.

The exploit was initially discovered in the wild by the Qualcomm Information Security & Risk Management team, which observed it being used in a sophisticated limited targeted attack. Following the release of Security Bulletin MS14-068, several security researchers have developed public and commercial exploits that target the vulnerability.

For more information about this vulnerability, see the entry "Additional information about CVE-2014-6324" (November 18, 2014) on the Microsoft Security Research and Defense Blog at blogs.technet.com/srd.

[13] "Sandworm and SCADA," *Simply Security*, Trend Micro, October 16, 2014, blog.trendmicro.com/sandworm-and-scada/; John Hultquist, "Sandworm Team – Targeting SCADA Systems," iSIGHT Partners, October 21, 2014, www.isightpartners.com/2014/10/sandworm-team-targeting-scada-systems/.

CVE-2014-4148: Remote code execution vulnerability in Windows TrueType engine (MS14-058)

CVE-2014-4148, a vulnerability in the Windows TrueType font parsing engine, was addressed by Security Bulletin MS14-058 in October 2014. CVE-2014-4148 is a memory corruption vulnerability that can be exploited using a specially crafted TrueType font. Because the font parser executes in kernel mode, successful exploitation of the vulnerability allows the attacker to execute code in kernel mode as well.

FireEye Labs discovered CVE-2014-4148 in use as a zero-day vulnerability exploited through a limited targeted attack.[14] The attack involved a malicious Word document sent as an email attachment. The document contains a malicious embedded TrueType font that infects a vulnerable computer when it is opened in Word. The exploit itself is fairly advanced; it injects a payload directly from kernel mode into a user-mode process (winlogon.exe or lsass.exe), and executes further actions from there. It is written to succeed on several different Windows platforms, includes a mechanism to avoid executing the exploit multiple times, and has a built-in deactivation date of October 31, 2014.

CVE-2014-4113: Elevation of privilege vulnerability in Win32k.sys (MS14-058)

CVE-2014-4113, a vulnerability in the Windows kernel, was addressed by Security Bulletin MS14-058 in October 2014. When successfully exploited, it enables the attacker to gain elevated privileges on the computer. As with CVE-2014-4148, CVE-2014-4113 was discovered as a zero-day vulnerability by FireEye Labs, which observed it being used in targeted attacks against enterprises to gain additional privileges after an initial compromise. CrowdStrike has connected exploits of CVE-2014-4113 to a Chinese targeted attack group dubbed "Hurricane Panda."[15] Following the release of Security Bulletin MS14-058, exploits targeting CVE-2014-4113 began to appear in a number of exploit kits, including Angler and Nuclear (SHA1: fdeda30dea2c5e972a245b3b7601540d3c4b3f1c).

[14] Dan Caselden, "Two Limited, Targeted Attacks; Two New Zero-Days," *Threat Research Blog*, FireEye Labs, October 14, 2014, https://www.fireeye.com/blog/threat-research/2014/10/two-targeted-attacks-two-new-zero-days.html.

[15] Dmitri Alperovitch, "CrowdStrike Discovers Use of 64-bit Zero-Day Privilege Escalation Exploit (CVE-2014-4113) by Hurricane Panda," *The Adversary Manifesto* (blog), CrowdStrike, October 14, 2014, blog.crowdstrike.com/crowdstrike-discovers-use-64-bit-zero-day-privilege-escalation-exploit-cve-2014-4113-hurricane-panda/.

Malware and unwanted software

Most attempts by malware to infect computers are unsuccessful. More than three-quarters of Internet-connected personal computers worldwide are protected by real-time security software that constantly monitors the computers and network traffic for threats and blocks them before they can infect the computers, if possible. Therefore, a comprehensive understanding of the malware landscape requires consideration of infection attempts that are blocked as well as infections that are removed.

Microsoft uses two different metrics to measure malware and unwanted software prevalence:[16]

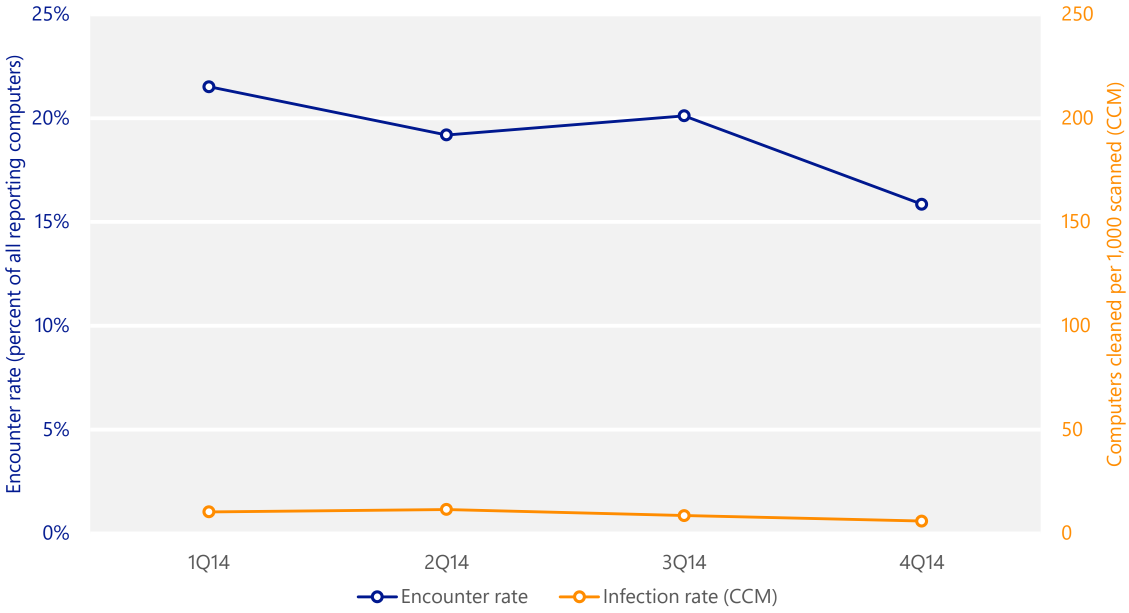
- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter. For example, the encounter rate for the malware family JS/Axpergle in France in 4Q14 was 0.6 percent. This data means that, of the computers in France that were running Microsoft real-time security software in 4Q14, 0.6 percent reported encountering the Axpergle family, and 99.4 percent did not. Encountering a threat does not mean the computer has been infected. Only computers whose users have opted in to provide data to Microsoft are considered when calculating encounter rates.[17]
- *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

[16] Microsoft regularly reviews and refines its data collection methodology to improve its scope and accuracy. For this reason, the statistics presented in this volume of the *Microsoft Security Intelligence Report* may differ slightly from comparable statistics in previous volumes.
[17] For information about the products and services that provide data for this report, see “Appendix B: Data sources” on page 107.

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 22 illustrates the difference between these two metrics.

Figure 22. Worldwide encounter and infection rates, 1Q14–4Q14, by quarter



Figures do not include Brantall, Rotbrow, and Filcout. See "Brantall, Rotbrow, and Filcout" on page 40 for more information.

As Figure 22 shows, and as one would expect, malware encounters are much more common than malware infections. On average, about 19.2 percent of reporting computers worldwide encountered malware over the past four quarters. At the same time, the MSRT removed malware from about 9.1 out of every 1,000 computers, or 0.91 percent. Together, encounter and infection rate information can help provide a broader picture of the malware landscape by offering different perspectives on how malware propagates and how computers get infected.

> Malware encounters are much more common than malware infections.

Brantall, Rotbrow, and Filcout

Where noted, the figures in this report omit detections of Win32/Brantall, Win32/Rotbrow, and Win32/Filcout. These three families were involved in an incident in which a rogue developer with access to commercial source code modified the source code to serve as a stealth distribution method for malware without being detected by major security software vendors. When the modification was discovered, it resulted in a significant installed base of commercial software being reclassified as malicious, which had an outsized effect on infection rates. Microsoft believes that the unmodified infection and encounter figures do not create an accurate picture of the worldwide threat landscape over the past year and a half. As a result, totals for the Brantall, Filcout, and Rotbrow families have been removed from the infection and encounter figures presented here where appropriate, as noted.

See "The Sefnit saga: a timeline" on pages 57–64 of *Microsoft Security Intelligence Report, Volume 17 (January–June 2014)*, available from the Microsoft Download Center, for a more in-depth explanation of the incident, along with detection statistics and a timeline of events.

Malware and unwanted software worldwide

The telemetry data generated by Microsoft security products from computers whose administrators or users choose to opt in to provide data to Microsoft includes information about the location of the computer, as determined by IP geolocation. This data makes it possible to compare infection and encounter rates, patterns, and trends in different locations around the world.[18]

[18] For more information about this process, see the entry "Determining the Geolocation of Systems Infected with Malware" (November 15, 2011) in the Microsoft Cyber Trust Blog (blogs.microsoft.com/cybertrust).

Figure 23. Encounter rate trends for the locations with the most computers reporting malware and unwanted software encounters in 2H14, by number of computers reporting

Country/region	1Q14	2Q14	3Q14	4Q14
United States	13.0%	12.3%	15.4%	11.5%
Brazil	34.1%	30.8%	32.9%	21.7%
Russia	28.8%	26.4%	27.3%	24.2%
France	20.4%	16.9%	22.8%	13.0%
India	51.1%	41.9%	38.2%	32.1%
Turkey	45.7%	40.4%	35.1%	28.0%
United Kingdom	13.4%	13.3%	17.2%	11.5%
Italy	25.9%	20.7%	25.0%	16.5%
Germany	13.8%	13.6%	14.5%	9.3%
Mexico	38.9%	32.3%	30.0%	21.9%

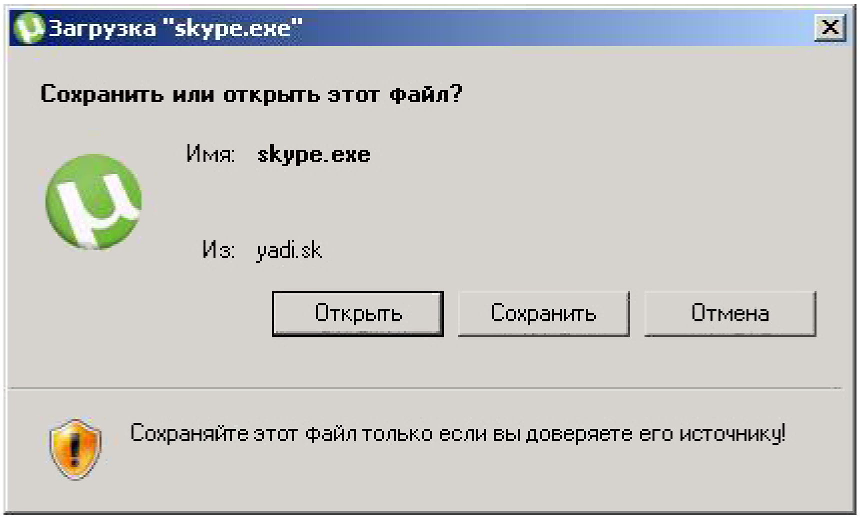
Figures do not include Brantall, Rotbrow, and Filcout. See "Brantall, Rotbrow, and Filcout" on page 40 for more information.

- Locations in Figure 23 are ordered by the number of computers reporting detections in 2H14.
- As shown in Figure 22 on page 39, encounter rates generally trended down in 2014, except for a slight increase in 3Q14 that was primarily caused by the appearance of two associated threats, the downloader family Win32/Tugspay and the adware family Win32/CostMin. See "Threat families" beginning on page 59 for more information about these and other malware and unwanted software families.
- Encounter rates fell worldwide in 4Q14 as detections of Tugspay and CostMin decreased. Of the 95 countries and regions with valid sample sizes tracked in this volume, all but 10 saw encounter rates decrease from 3Q14 to 4Q14.
- Tugspay and CostMin mostly targeted wealthy countries and regions in Europe and the Americas. Of the locations that saw more than a 20 percent encounter rate increase from 2Q14 to 3Q14, all except Sweden and the Netherlands are individual members of the Group of Twenty (G20) group of major world economies. Meanwhile, all locations in Africa, the Middle East, and Asia outside the G20 saw encounter rates fall from 2Q14 to 3Q14.
- France and Italy were hit particularly hard by Tugspay in 3Q14, with both locations seeing encounter rates above 8 percent for Tugspay alone that

quarter. Consequently, both experienced large overall encounter rate declines in 4Q when Tugspay encounters decreased.

- The worm family VBS/Jenxcus, the third-most commonly encountered threat family overall in 2H14, was also highly concentrated geographically. It ranked first in Brazil and Mexico and second in India, but ranked 89th in the United States, 49th in Germany, 57th in the United Kingdom, and 53rd in Russia. See page 61 for information about a recent successful takedown action against the Jenxcus network that is likely to affect encounter rates in the future.
- In addition to Jenxcus and Tugspay, malware families that were unusually prevalent in Brazil include the worm family JS/Proslikefan (the sixth-most commonly encountered family in Brazil in 2H14, but only 53th worldwide), the downloader family Win32/Banload (eighth in Brazil, 74th worldwide), and the password stealer Win32/Mujormel (15th in Brazil, 125th worldwide).
- Encounters in Russia were dominated by Win32/Ogimant, a downloader family that masquerades as a utility that helps users download items such as pictures and movies, usually from peer-to-peer or torrent services. The encounter rate for Ogimant in Russia in 3Q14 was 10.5 percent, more than three times as high as that of the next most prevalent family in Russia, the generic detection Win32/Obfuscator. Ogimant was highly prevalent in Russia and several other former Soviet republics, but was virtually unknown elsewhere.

Figure 24. An example of the user interface for Win32/Ogimant, which masquerades as a download helper



Загрузка "skype.exe"

Сохранить или открыть этот файл?

Имя: skype.exe

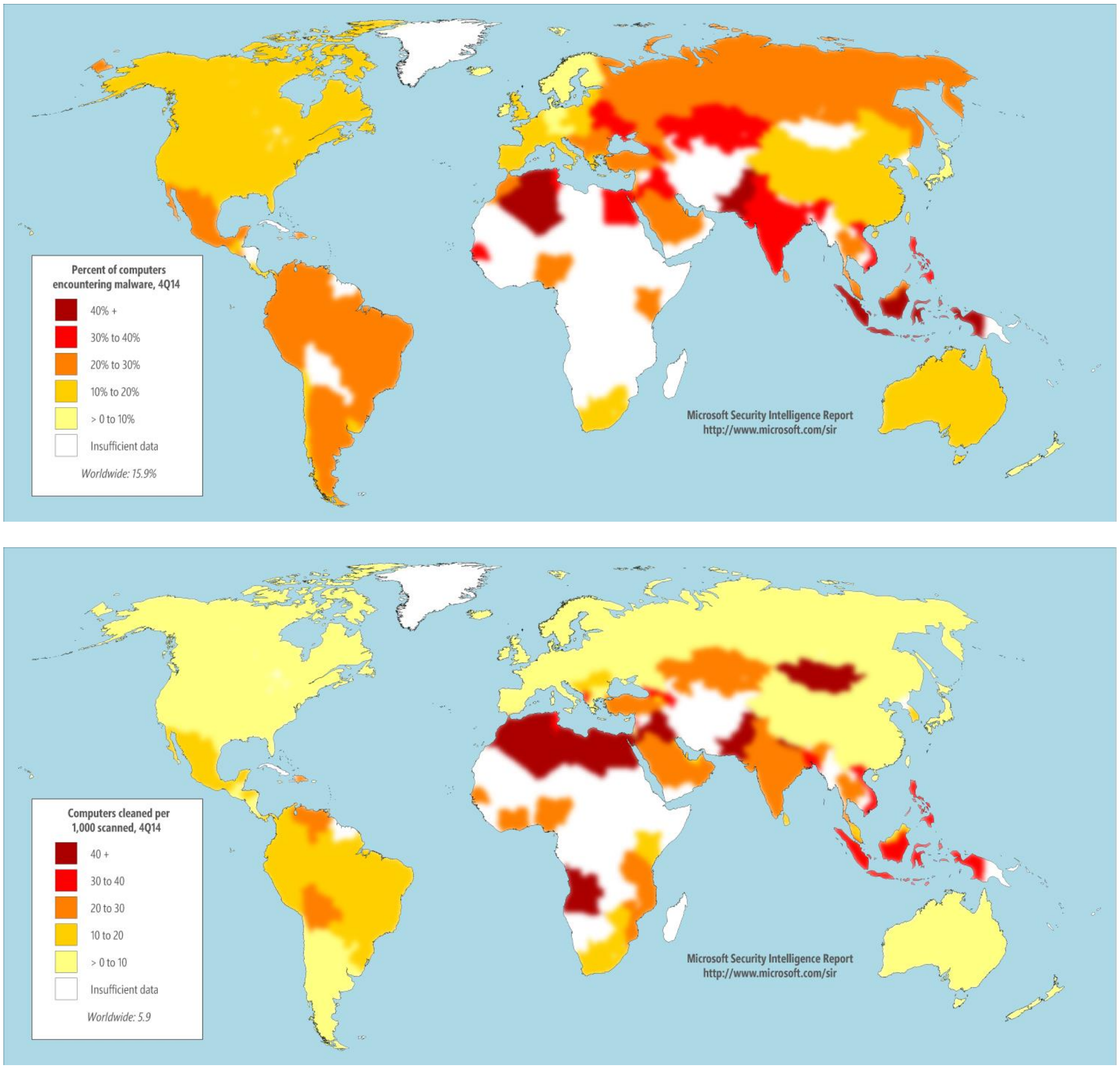
Из: yadi.sk

Сохраняйте этот файл только если вы доверяете его источнику!

- Encounter rates in India and Turkey improved considerably in 2014, but remained significantly higher than those of the other locations on the list. Families that were unusually prevalent in India included Win32/Vercuser (eighth in India, 91st worldwide) and MSIL/Mofin (ninth in India, 130th worldwide), both worms. Families that were unusually prevalent in Turkey included Win32/Rimod (fifth in Turkey, 88th worldwide), Win32/BeeVry (ninth in Turkey, 139th worldwide), and MSIL/Balamid (14th in Turkey, 169th worldwide), all trojans.
- The downloader family Win64/Bregent was unusually common in Germany (ranked 11th in Germany, 259th worldwide).
- Threat families that were unusually common in Mexico included the trojan family Win32/Crastic (ranked ninth in Mexico, 194th worldwide) and the worm family JS/Bondat (tenth in Mexico, 82nd worldwide).

For a different perspective on threat patterns worldwide, Figure 25 shows the infection and encounter rates in locations around the world in 4Q14.

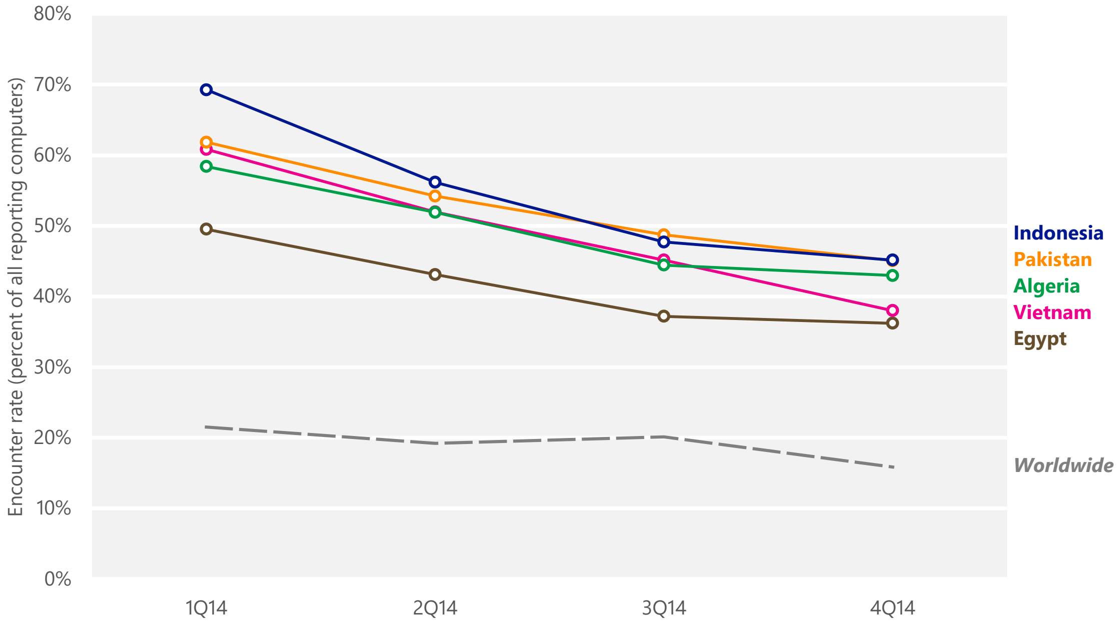
Figure 25. Encounter rates (top) and infection rates (bottom) by country/region in 4Q14


Percent of computers encountering malware, 4Q14
40% +
30% to 40%
20% to 30%
10% to 20%
> 0 to 10%
Insufficient data
Worldwide: 15.9%
Microsoft Security Intelligence Report
http://www.microsoft.com/sir
Computers cleaned per 1,000 scanned, 4Q14
40 +
30 to 40
20 to 30
10 to 20
> 0 to 10
Insufficient data
Worldwide: 5.9
Microsoft Security Intelligence Report
http://www.microsoft.com/sir

Figures do not include Brantall, Rotbrow, and Filcout. See "Brantall, Rotbrow, and Filcout" on page 40 for more information.

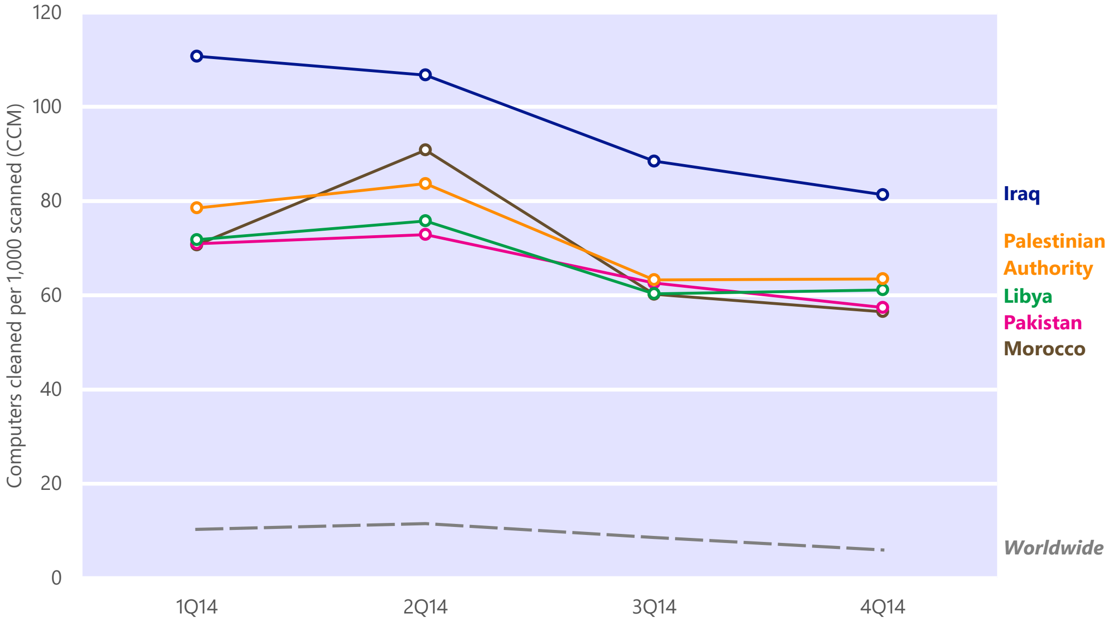
The next several figures illustrate trends for specific locations around the world with particularly high or low incidences of threat detection. Figure 26 and Figure 27 show trends for the locations with the highest rates of detection as determined by encounter rate and CCM, respectively.

Figure 26. Trends for the five locations with the highest encounter rates in 2H14 (100,000 reporting computers minimum)



Figures do not include Brantall, Rotbrow, and Filcout. See "Brantall, Rotbrow, and Filcout" on page 40 for more information.

Figure 27. Trends for the five locations with the highest infection rates in 2H14, by CCM (100,000 MSRT computers minimum)



Figures do not include Brantall, Rotbrow, and Filcout. See "Brantall, Rotbrow, and Filcout" on page 40 for more information.

- The locations with the highest encounter rates were Indonesia, Pakistan, Algeria, Vietnam, and Egypt.

- All of these locations were also among the five locations with the highest encounter rates in 1H14 except for Egypt, which moved up from ninth to fifth in 2H14.
- Notably, no exploit kits were among the most commonly encountered families in 2H14 in any of these locations, despite the prevalence of exploit kits such as JS/Axpergle and Win32/Anogre worldwide.
- Viruses and worms accounted for six of the top 10 malware families in Indonesia in the second half of 2014, including Win32/Slugin, a virus family that was only detected in seven other countries and regions, all at much lower encounter rates than Indonesia. The most commonly detected families in Indonesia in 2H14 were the trojan family Win32/Ramnit (ranked 14th worldwide) and the worm family Win32/Gamarue (ranked 6th worldwide).
- The list of top threats encountered in Pakistan was also dominated by viruses and worms, including the worm families VBS/Jenxcus and Gamarue, and the virus family Win32/Sality. The worm family Win32/Chir was disproportionately prevalent there, with computers in Pakistan accounting for more than half of all Chir encounters worldwide. Chir is a worm that can spread via email, shared drives, and also has a virus component that infects other files. In Pakistan, it often arrives with a file name that includes "Jinsi Maloomat" (or "Gensi Maloomat"), a reference to an Urdu-language book. Other threats that were unusually common in Pakistan included the backdoor family Win32/Bifrose (ranked ninth in Pakistan, 131st worldwide) and the worm family Win32/Tupym (tenth in Pakistan, 120th worldwide).

Despite their prevalence worldwide, no exploit kits were among the most commonly encountered families in 2H14 in any of these locations.

- Although the encounter rate for Jenxcus in Algeria was down significantly from 1H14, the worm still accounted for nearly twice as many encounters as any other family there in 2H14. Unusually prevalent families in Algeria include the worm family Win32/Ippedo (third in Algeria, 68th worldwide) and the backdoor family MSIL/Bladabindi (eighth in Algeria, 35th worldwide).
- Seven of the most commonly detected threats in Vietnam were not among the 10 most commonly detected families worldwide, including the trojan family JS/Faceliker, ranked first in Vietnam but only 25th worldwide, and the virus DOS/Sigru (tenth in Vietnam, 230th

worldwide). The well-known worm Win32/Conficker was the ninth-most commonly encountered family in 2H14 in Vietnam, the only location listed in Figure 26 to have Conficker in the top 10.

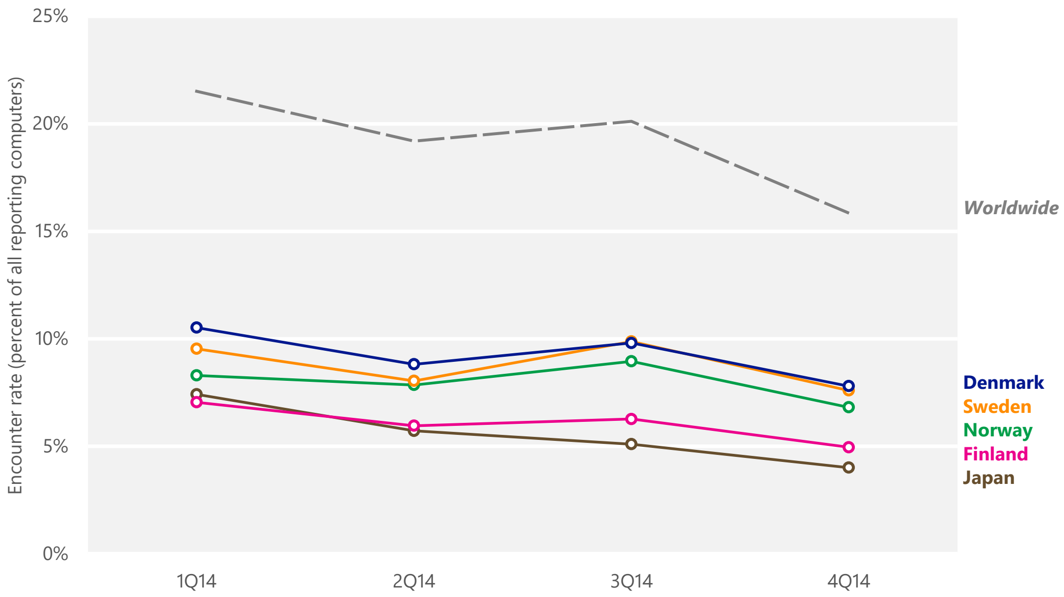
    - Jenxcus was also the most commonly detected malware family in Egypt, being encountered by nearly twice as many computers as any other family. Unusually prevalent families in Egypt include the virus family Win32/Virut (fourth in Egypt, 30th worldwide) and Win32/Nitol (seventh in Egypt, 83rd worldwide), which is used to conduct distributed denial-of-service (DDoS) attacks.

- The locations with the highest infection rates were Iraq, the Palestinian territories, Libya, Pakistan, and Morocco.
    - Jenxcus, Sality, and Bladabindi were the most common malware families infecting computers in Iraq in 2H14. In fourth place was the worm family Win32/Wecykler, which had its highest infection rate there (a CCM of 10.9 in Iraq in 4Q14, compared to 0.9 in Nepal, the next highest location). 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.
    - Jenxcus and Sality were the most common infecting malware families in the Palestinian territories. Each family had an infection rate more than four times as large as the third place family, Bladabindi.
    - Bladabindi, Jenxcus, and Sality were the most common infecting malware families in Libya; Sality, Jenxcus, and Gamarue were the most common in Pakistan.
    - In Morocco, the most common infecting malware family was the worm family Win32/Yeltminky, which had its highest infection rate there (a CCM of 21.2 in Morocco in 4Q14, compared to 3.4 in Algeria, the next highest location). Yeltminky is a family of worms that spreads by making copies of itself on all available drives and creating an autorun.inf file to execute the copies.

- For more information about malware in many of these countries/regions, see "The Threat Landscape in the Middle East and Southwest Asia," a five-part series on the Microsoft Cyber Trust blog (blogs.microsoft.com/cybertrust):
    - Part 1: Relatively High Malware Infection Rates (March 12, 2014)

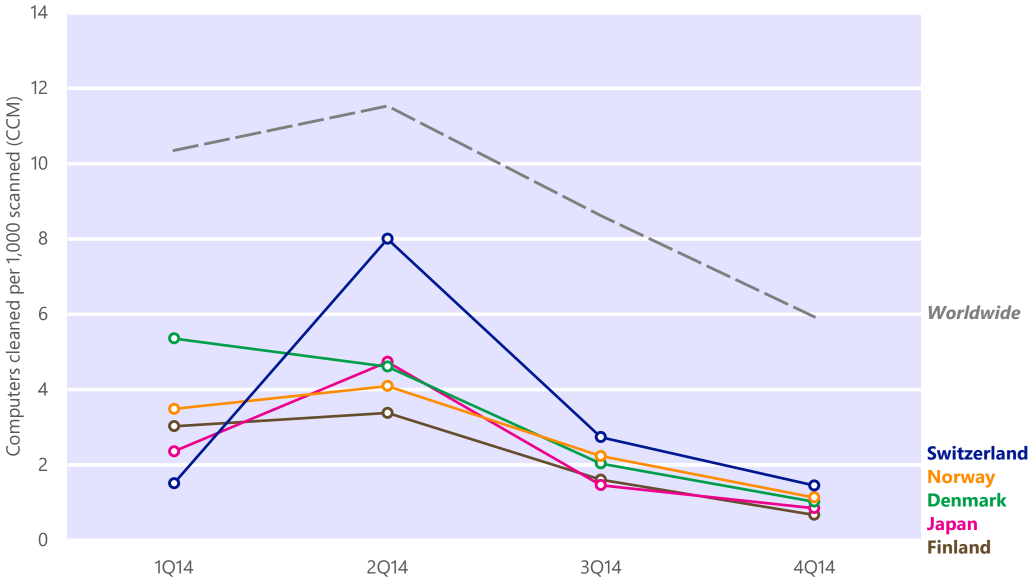
- Part 2: Relatively High Malware Encounter Rates (March 13, 2014)
- Part 3: Regional Anti-virus Software Usage (March 17, 2014)
- Part 4: Regional Windows XP Market Share (March 18, 2014)
- Part 5: Socio-economic Factors and Regional Malware Infection Rates (March 19, 2014)

Figure 28. Trends for locations with low encounter rates in 2H14 (100,000 reporting computers minimum)



Figures do not include Brantall, Rotbrow, and Filcout. See “Brantall, Rotbrow, and Filcout” on page 40 for more information.

Figure 29. Trends for locations with low infection rates in 2H14, by CCM (100,000 reporting computers minimum)



Figures do not include Brantall, Rotbrow, and Filcout. See “Brantall, Rotbrow, and Filcout” on page 40 for more information.

- The Nordic countries, including Denmark, Finland, Iceland, Norway, and Sweden, have perennially been among the healthiest locations in the world with regard to malware exposure, as has Japan. In 2H14, these locations typically had encounter and infection rates between about one-third and one-half of the worldwide average. (See the blog entry series "Lessons from Least Infected Countries" at blogs.technet.com/b/security/p/series-lessons-from-least-infected-countries.aspx for more information about locations that typically have low infection and encounter rates.)
- The unwanted software families Win32/CostMin and Win32/CouponRuc, the exploit family JS/Axpergle, and the generic detection Win32/Obfuscator were all among the five most commonly encountered or infecting threat families in all of these locations.
- Despite its physical and cultural distance from the other locations, the threat mix in Japan was fairly similar, with exploit kit families such as Axpergle and unwanted software families such as CostMin and CouponRuc leading the detections. Threats that were unusually common in Japan included JS/Neclu (ranked sixth in Japan and 64th worldwide), a detection for the Nuclear exploit kit, and the adware family Win32/AddLyrics. Win32/Tugspay, the most commonly detected malware family worldwide in 2H14, was not among the most commonly encountered families in Japan.

> The Nordic countries have perennially been among the healthiest locations in the world with regard to malware exposure, as has Japan.

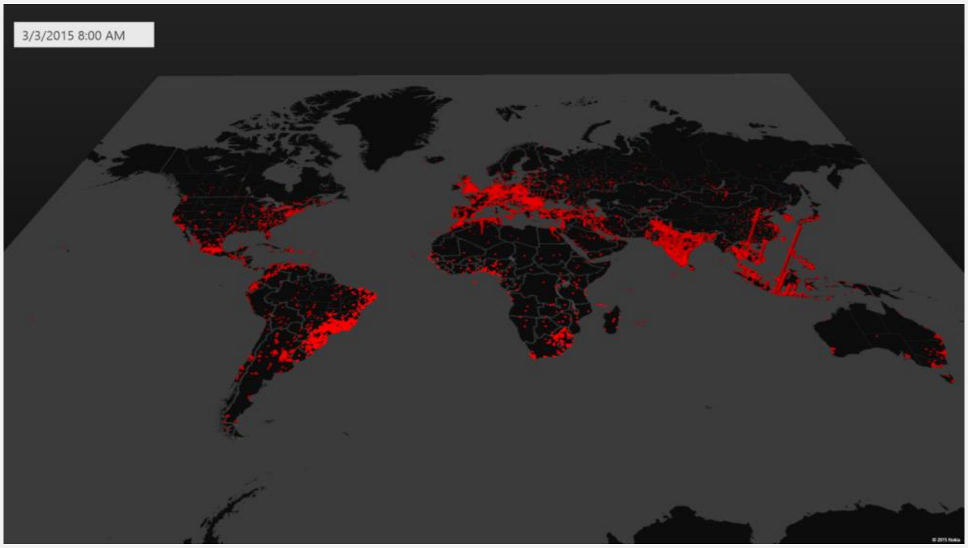
- Win32/Lecpetex was the malware family with the highest infection rate in Norway in 2H14, with a CCM of 0.5 in 3Q14, though it dropped to 0.03 in the fourth quarter. Lecpetex is a trojan that uses the infected computer's resources to "mine" for Litecoins, a type of digital currency similar to Bitcoin. Threats with unusually high encounter rates in Norway included Java/CVE-2013-1488 (15th in Norway, 121st worldwide), a detection for an exploit affecting the Java Runtime Environment (JRE).
- The generic detection Win32/Comame, which was the 27th-most commonly encountered threat worldwide in 2H14, ranked ninth in Finland. Comame encounters in Finland typically involve malicious files with Finnish language filenames such as "Maijan laulut.exe" or "Potilassiirtojen Ergonomiakortti tehtävä 1."

- The sharp rise in the infection rate in Switzerland in 2Q14 and subsequent decline can be attributed mostly to detections of the trojan family Win32/Sefnit. See "The Sefnit saga: a timeline" on pages 57–64 of *Microsoft Security Intelligence Report, Volume 17 (January–June 2014)*, available from the Microsoft Download Center, for more information about Sefnit.

Microsoft and partners disrupt the Ramnit botnet

In February 2015, the Microsoft Digital Crimes Unit (DCU), in cooperation with Symantec, the Financial Information Sharing and Analysis Center (FS-ISAC), and a number of internal Microsoft groups including the Microsoft Malware Protection Center team (MMPC), referred a large global botnet case involving the malware family Win32/Ramnit to Europol's European Cybercrime Centre (EC3) and other law enforcement authorities in the UK, Germany, Italy, and the Netherlands. Law enforcement focused on taking action against the cybercriminals where their primary command and control (C&C) infrastructure was located, while Microsoft focused on the cyberforensics and a scanning/cleaning solution to enable Ramnit victims worldwide to regain control of their computing devices.

Figure 30. Ramnit-infected computers connecting to the DCU sinkhole during the first week of the takedown in February 2015



About Ramnit

Ramnit is a module-based threat that concentrates on stealing credential information from banking websites—mostly involving bank accounts based in the UK, but with branches all over the world. Ramnit is configured to hide itself, disable security defenses, and establish a connection with the Ramnit C&C

server. The criminal operation behind the Ramnit botnet was fairly sophisticated—for example, it implemented a feature that sent SMS messages to the end user to help defeat dual-factor authentication by the banks.

Components of Ramnit include:

- A module that monitors the user's web browser and injects its own HTML into the page when certain websites are visited. This capability enables Ramnit to collect sensitive information, such as credit card details.
- A module that disables certain Windows components and most popular antimalware products.
- Modules that steal browser cookies and FTP login credentials.

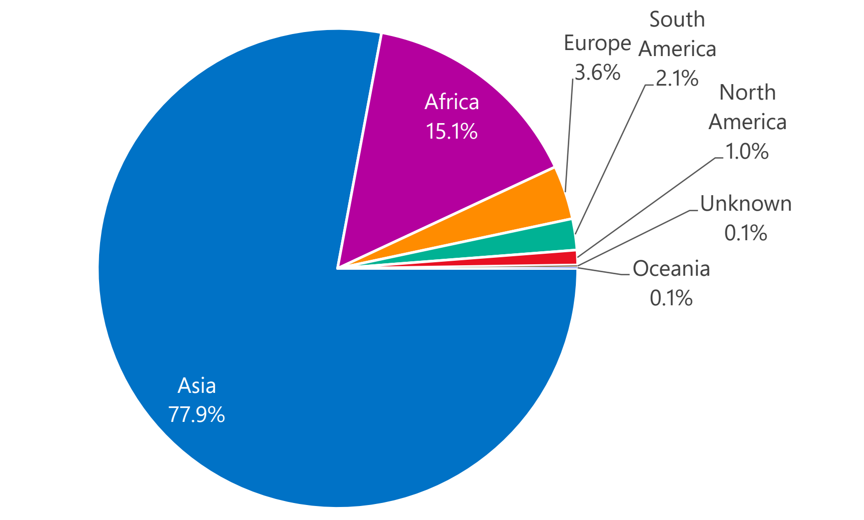
For more information about the Ramnit malware, see the following entries in the MMPC blog at blogs.technet.com/mmpc:

- Little Red Ramnit: My, what big eyes you have, Grandma! (May 10, 2011)
- Ramnit - The renewed bot in town (March 14, 2013)
- Microsoft Malware Protection Center assists in disrupting Ramnit (February 25, 2015)

Botnet scope and scale

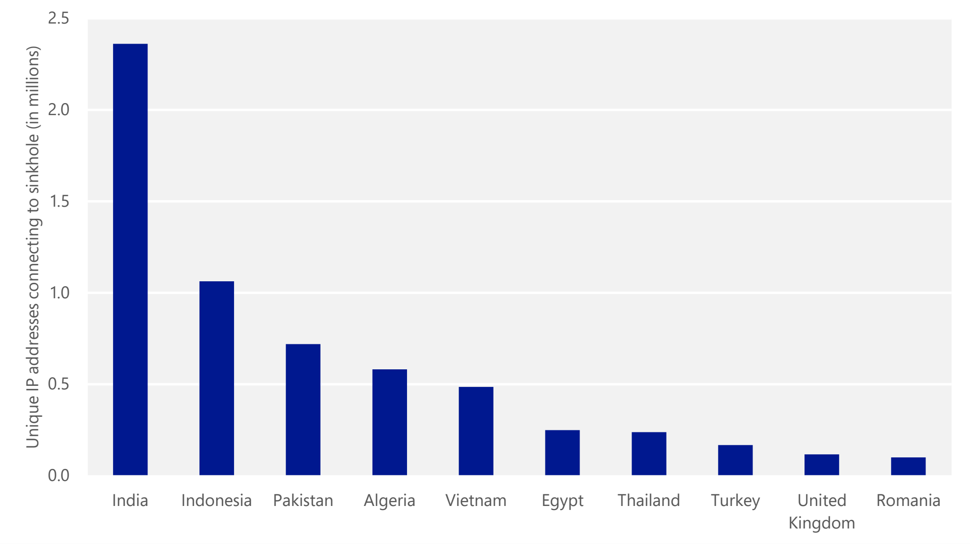
Microsoft estimates that as of April 2015, more than 1,000,000 computing devices are currently infected by Ramnit worldwide. Because the malware can disable real-time security software, most of its victims may not be aware they have been compromised.

Figure 31. Unique IP addresses connecting to the Ramnit sinkhole, by location



As the Ramnit C&C infrastructure was taken offline, Microsoft replaced it with a sinkhole to monitor the botnet's scope and the progress of remediation efforts. Since the takedown, Microsoft has observed nearly 10 million different IP addresses from 197 countries and regions connecting to the sinkhole, accounting for nearly 1 billion connections overall. More than three-quarters of the IP addresses connecting to the sinkhole were located in Asia, with India alone accounting for nearly one-third of the addresses worldwide.

Figure 32. Countries and regions with the most IP addresses connecting to the Ramnit sinkhole

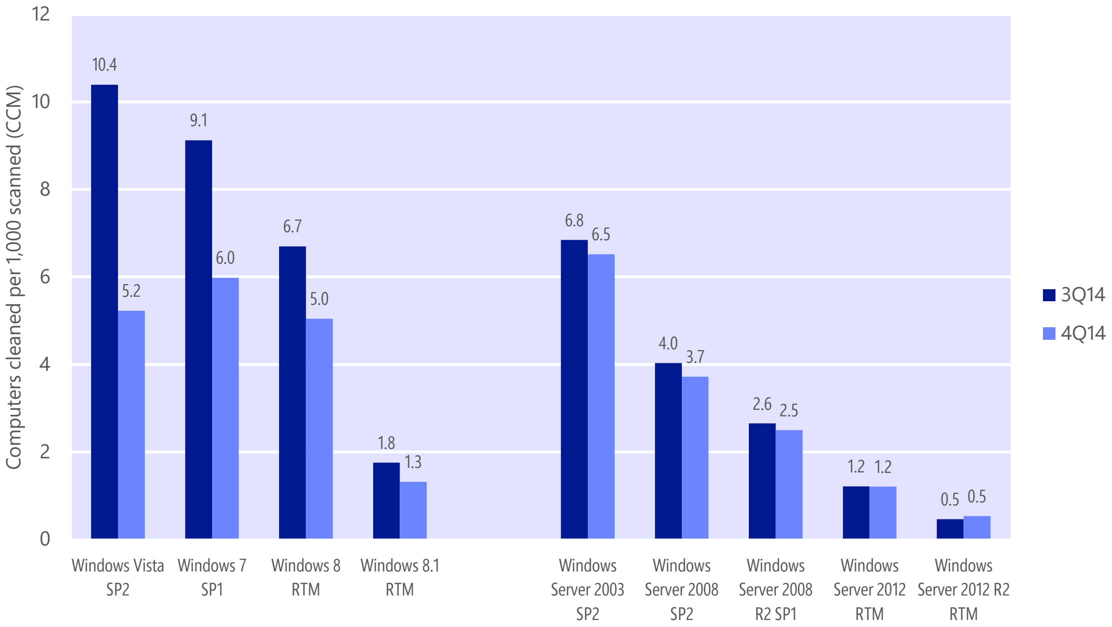


The MMPC and the DCU are working with security software vendors, CERTs, and ISPs globally to notify victims and remediate their devices.

Infection rates by operating system

The features and updates that are available with different versions of the Windows operating system and the differences in the way people and organizations use each version affect the infection rates for the different versions and service packs. Figure 33 shows the infection rate for each currently supported Windows operating system/service pack combination.

Figure 33. Infection rate by client and server operating system in 3Q14 and 4Q14



Figures do not include Brantall, Rotbrow, and Filcout. See "Brantall, Rotbrow, and Filcout" on page 40 for more information.

- This data is normalized; that is, the infection rate for each version of Windows is calculated by comparing an equal number of computers per version (for example, 1,000 Windows Vista SP2 computers to 1,000 Windows 8 RTM computers).
- Infection rates decreased from 3Q14 to 4Q14 on every supported client and server platform except Windows Server 2012 R2, which remained stable and low.
- In general, infection rates for more recently released operating systems and service packs tend to be lower than infection rates for earlier releases, for both client and server platforms. This pattern can be seen clearly in Figure 33, with the oldest supported operating system release (Windows Vista SP2) having the highest CCM for the half-year period, and the newest supported release (Windows 8.1 RTM) having the lowest. The pattern holds true for server platforms as well, with each supported release having a lower infection rate than its most recent predecessor.

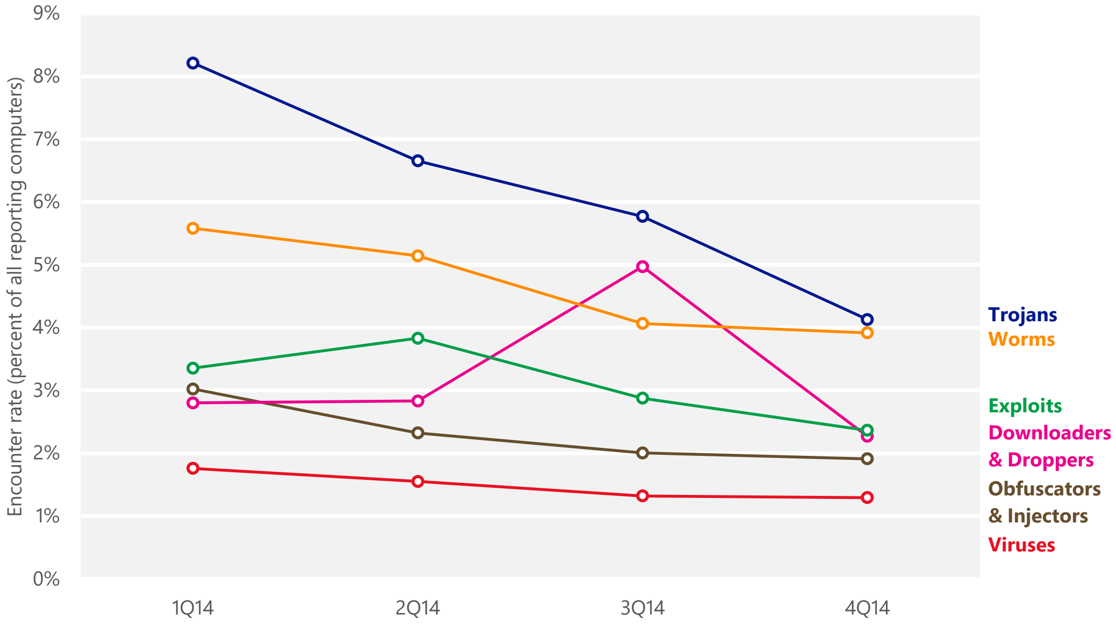
> Infection rates decreased on every supported platform except Windows Server 2012 R2, which remained stable and low.

- Infection rates also tend to be lower on server platforms than on client platforms. Servers are not typically used to browse the web nearly as frequently as client computers, and web browser features such as Enhanced Security Configuration in Internet Explorer discourage using servers to visit untrusted websites. The pattern is particularly apparent when comparing client and server platforms that are built on the same code base. For example, Windows Vista SP2, with a 4Q14 CCM of 5.2, shares a code base with Windows Server 2008 SP2, with a 4Q14 CCM of 3.7; likewise, Windows 8, with a CCM of 5.0 in the fourth quarter, shares a code base with Windows Server 2012, with a CCM of 1.2.

Threat categories

The MMPC classifies individual threats into types based on a number of factors, including how the threat spreads and what it is designed to do. To simplify the presentation of this information and make it easier to understand, the *Microsoft Security Intelligence Report* groups these types into categories based on similarities in function and purpose.

Figure 34. Encounter rates for significant malware categories in 2014



Figures do not include Brantall, Rotbrow, and Filcout. See "Brantall, Rotbrow, and Filcout" on page 40 for more information.

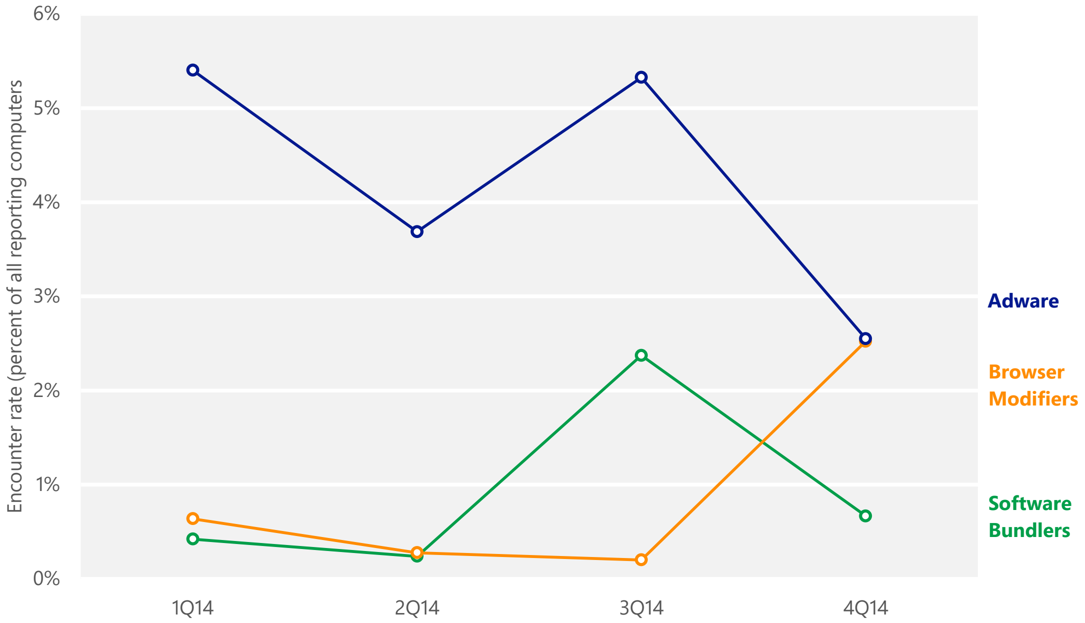
- Totals for each time period may exceed 100 percent because some computers report more than one category of threat in each time period.

- Encounters with most categories of malware remained stable or decreased throughout the second half of 2014, in keeping with the general worldwide decline in malware encounters.
- The encounter rate for the Downloaders & Droppers category of malware spiked in 3Q14 because of detections of Win32/Tugspay. See "Threat families" on page 59 for more information about this and other malware and unwanted software families.
- Encounters with malware families in the Trojans category declined by nearly half between 1Q14 and 4Q14 because of decreased detections of a number of formerly prevalent threats, including Win32/Wysotot, JS/Faceliker, and MSIL/Spacekito. Despite this decline, Trojans remained the most commonly detected category of malware throughout 2H14.

> Encounters with most categories of malware remained stable or decreased throughout the second half of 2014.

- Though not shown in Figure 37, encounters involving the Ransomware category increased from a low of 0.25 percent in 2Q14 to a high of 0.55 percent in 4Q14 because of increased detections of JS/Krypterade and Win32/Crowti. See "Ransomware" on page 67 for more information about these and other prevalent ransomware families.
- Along with Ransomware, the Backdoors, Password Stealers & Monitoring Tools, and Other Malware categories each had encounter rates of less than 1 percent each quarter and are not shown in Figure 37.

Figure 35. Encounter rates for unwanted software categories in 2014



Figures do not include Brantall, Rotbrow, and Filcout. See "Brantall, Rotbrow, and Filcout" on page 40 for more information.

- Unwanted software encounter rates are often dominated by small numbers of individual families that increase and decrease relatively quickly. During the first half of the year, almost all of the unwanted software encounters reported to Microsoft involved adware, with encounter rates for browser modifiers and software bundlers amounting to less than 1 percent each in 1Q14 and 2Q14. In the second half of the year, while adware encounters remained high, their dominance was challenged by spikes in encounters with software bundlers in the third quarter and browser modifiers in the fourth.
- The increase in Adware encounters in 3Q14 and subsequent decrease in 4Q14 is primarily caused by the rise and fall of Win32/CostMin, the most commonly encountered adware family in 2H14. See "Threat families" beginning on page 59 for more information about CostMin and other unwanted software families.
- Encounters that involve the Software Bundlers category spiked in 3Q14 because of a number of new bundlers, notably Win32/Softpulse and Win32/SquareNet. Most of the prevalent software bundlers in 3Q14 subsequently decreased in 4Q14, causing the overall decrease in detections for the category.

- The increase in encounters involving the Browser Modifiers category in 4Q14 occurred after the MMPC changed its unwanted software detection criteria to include software that bypasses consent dialogs for installing browser extensions, or prevents the user from viewing or modifying browser features or settings. Two new families that were created as a result of this change in detection criteria, BrowserModifer:Win32/CouponRuc and BrowserModifier:Win32/DefaultTab, were subsequently responsible for almost all of the browser modifier encounters in 4Q14.

  For more information about the new unwanted software detection criteria, see the following entries in the MMPC blog at blogs.technet.com/mmpc:

  - Close means close: New adware detection criteria (October 16, 2014)
  - Staying in control of your browser: New detection changes (October 17, 2014)

Threat categories by location

Significant differences exist in the types of threats that affect users in different parts of the world. The spread of malware can be highly dependent on language and socioeconomic factors as well as on the methods used for distribution. Some threats are spread using techniques that target people who speak a particular language or who use online services that are local to a specific geographic region. Other threats target vulnerabilities or operating system configurations and applications that are unequally distributed around the world.

Figure 36 shows the relative prevalence of different categories of malware in several locations around the world in 4Q14.

Figure 36. Threat category prevalence worldwide and in the 10 locations with the most computers reporting encounters in 4Q14

Category	Worldwide	United States	Brazil	Russia	France	India	Turkey	United Kingdom	Italy	Germany	Mexico
Trojans	4.1%	2.7%	5.4%	9.4%	2.2%	8.1%	11.4%	2.1%	3.4%	2.0%	4.0%
Worms	3.9%	0.4%	6.7%	3.4%	1.3%	19.2%	11.4%	0.6%	2.9%	0.7%	12.6%
Adware	2.6%	2.4%	5.6%	3.3%	3.7%	3.1%	4.3%	2.3%	3.3%	1.8%	2.6%
Browser Modifiers	2.5%	2.4%	1.8%	1.5%	2.5%	4.5%	3.0%	1.5%	2.4%	1.3%	3.0%
Exploits	2.4%	3.2%	1.3%	1.2%	1.6%	2.6%	1.7%	3.1%	2.7%	2.3%	1.5%
Downloaders & Droppers	2.3%	1.5%	3.8%	9.1%	2.3%	3.0%	2.0%	2.2%	2.9%	1.5%	2.1%
Obfuscators & Injectors	1.9%	0.7%	2.6%	4.3%	1.2%	4.9%	3.7%	0.9%	1.7%	1.1%	2.2%
Viruses	1.3%	0.3%	1.4%	1.0%	0.3%	5.0%	3.8%	0.3%	0.6%	0.3%	0.9%
Backdoors	0.8%	0.4%	0.7%	1.3%	0.6%	1.9%	1.4%	0.5%	0.6%	0.3%	0.7%
Software Bundlers	0.7%	0.7%	0.7%	0.2%	0.7%	1.4%	0.7%	0.9%	0.8%	0.4%	0.8%
Ransomware	0.5%	1.2%	0.4%	0.2%	0.8%	0.0%	0.2%	0.6%	0.7%	0.6%	0.2%
Password Stealers & Monitoring Tools	0.5%	0.5%	0.9%	0.5%	0.2%	0.6%	0.6%	0.4%	0.7%	0.3%	0.4%
Other Malware	0.4%	0.7%	0.1%	0.1%	0.2%	0.3%	0.3%	0.3%	0.3%	0.2%	0.2%

Figures do not include Brantall, Rotbrow, and Filcout. See "Brantall, Rotbrow, and Filcout" on page 40 for more information.

- Within each row of Figure 36, a darker color indicates that the category is more prevalent in the specified location than in the others and a lighter color indicates that the category is less prevalent. As in Figure 23 on page 41, the locations in the table are ordered by number of computers reporting detections in 2H14.
- India experienced higher encounter rates for Backdoors, Browser Modifiers, Obfuscators & Injectors, Software Bundlers, Viruses, and Worms than the other locations in Figure 36.

- The United States and United Kingdom had the highest encounter rates for Exploits, led by Win32/Anogre (a detection for the Sweet Orange exploit kit) and JS/Axpergle (a detection for the Angler exploit kit). See "Exploit kits and other HTML/JavaScript exploits" on page 25 for more information about these families.
- The United States also had particularly high encounter rates for Ransomware, led by JS/Krypterade, and Other Malware, led by the generic detection Win32/MpTamperSrp and the rogue security software families Win32/FakeRean and Win32/FakePAV. See "Ransomware" on page 67 for more information about Krypterade and other ransomware families.

> The United States and United Kingdom had high encounter rates for Exploits.

- Brazil had the highest encounter rate for Adware, led by Win32/PennyBee and Win32/CostMin, and Password Stealers & Monitoring Tools, led by Win32/Mujormel.
- Russia had the highest encounter rate for Downloaders & Droppers, led by Win32/Ogimant.
- Turkey had a particularly high rate of encounters involving the Trojans category, led by JS/Kilim (for which Turkey accounted for about two-thirds of all encounters in 3Q14), and Win32/Rimod.

See "Appendix C: Worldwide infection rates" on page 109 for more information about malware around the world.

Threat families

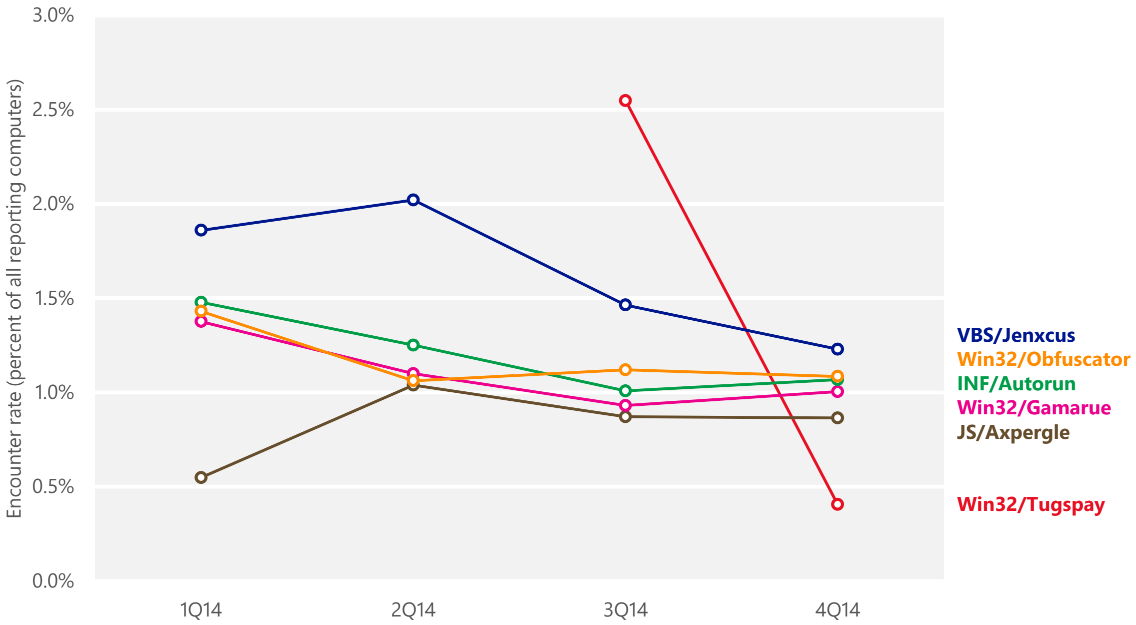
Figure 37 and Figure 38 show trends for the top malware families that were detected on computers by Microsoft real-time antimalware products worldwide in 2H14.

Figure 37. Quarterly trends for the top 10 malware families encountered by Microsoft real-time antimalware products in 2H14, shaded according to relative encounter rate

Rank	Family	Most significant category	1Q14	2Q14	3Q14	4Q14
1	Win32/Tugspay	Downloaders & Droppers	—	—	2.55%	0.41%
2	VBS/Jenxcus	Worms	1.86%	2.02%	1.46%	1.23%
3	Win32/Obfuscator	Obfuscators & Injectors	1.43%	1.06%	1.12%	1.09%
4	INF/Autorun	Obfuscators & Injectors	1.48%	1.25%	1.01%	1.07%
5	Win32/Gamarue	Worms	1.38%	1.10%	0.93%	1.00%
6	JS/Axpergle	Exploits	0.55%	1.04%	0.87%	0.86%
7	Win32/Ogimant	Downloaders & Droppers	0.00%	0.36%	0.65%	0.54%
8	Win32/Anogre	Exploits	0.04%	0.15%	0.60%	0.43%
9	Win32/Sality	Viruses	0.71%	0.59%	0.48%	0.47%
10	Win32/Ramnit	Trojans	0.62%	0.54%	0.47%	0.47%

Figures do not include Brantall, Rotbrow, and Filcout. See "Brantall, Rotbrow, and Filcout" on page 40 for more information.

Figure 38. Encounter rate trends for a number of notable malware families in 2H14



Win32/Tugspay, the most commonly encountered malware family in 2H14, is a downloader that spreads by posing as an installer for legitimate software, such as a Java update, or through other malware. When installed, it downloads unwanted software to the computer, including Win32/CostMin and Win32/Adpeak. Tugspay was first detected in July of 2014 and became the most commonly encountered malware family in 3Q14 by a large margin.

In coordination with Microsoft, the commercial software vendor that produced the Tugspay downloader subsequently modified the behavior of its software so that it no longer meets the definition of malware, which explains the large encounter rate decrease in 4Q14.[19]

- VBS/Jenxcus, the most commonly encountered malware family in 4Q14 and the second-most commonly encountered family in 2H14 overall, is a worm coded in VBScript that opens a backdoor on an infected computer, enabling an attacker to control it remotely. In addition to spreading via removable drives, Jenxcus was often transmitted via a fake Adobe Flash Player update from spoofed YouTube web pages. 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. The original owners of the botnet subsequently left the project, but the Jenxcus code is now being used by other criminal organizations.

  See "The Microsoft DCU and the legal side of fighting malware" on pages 29–32 of *Microsoft Security Intelligence Report, Volume 17 (January–June 2014)*, available from the Microsoft Download Center, for more information about the Microsoft takedown of the Jenxcus botnet. For additional technical information about Jenxcus, see the following entries in the MMPC blog (blogs.technet.com/mmpc):

  - MSRT February 2014 – Jenxcus (February 11, 2014)
  - Microsoft Digital Crimes Unit disrupts Jenxcus and Bladabindi malware families (June 30, 2014)

> The original owners of the Jenxcus botnet left the project following the takedown, but the code is now being used by other criminal organizations.

- Win32/Obfuscator, the third-most commonly encountered threat in 2H14, is a generic detection for programs that have been modified by malware obfuscation tools. These tools typically use a combination of methods, including encryption, compression, and anti-debugging or anti-emulation techniques, to alter malware programs in an effort to hinder analysis or detection by security products. The output is usually another program that

[19] Microsoft has published the criteria that the company uses to classify programs as unwanted software at www.microsoft.com/security/portal/mmpc/shared/objectivecriteria.aspx. For programs that have been classified as unwanted software, Microsoft provides a dispute resolution process to allow for reporting of potential false positives and to provide software vendors with the opportunity to request investigation of a rating with which they do not agree.

keeps the same functionality as the original program but with different code, data, and geometry.

- INF/Autorun, the fourth-most commonly encountered threat worldwide during the period, is a generic detection for worms that spread between mounted volumes using the AutoRun feature in some versions of Windows. The Autorun detection uses a technique that is mostly ineffective against versions of Windows released or updated within the last several years, but detections remain high because of several prevalent families' use of malicious .INF files as a vector for attempting to spread malware via removable drives. Microsoft antimalware products detect these malicious .INF files as Autorun variants, and block these attempts even when they would not be successful.
- Win32/Gamarue, the fifth-most commonly encountered threat in 2H14, is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers. For more information about Gamarue, see the following entries in the MMPC blog at blogs.technet.com/mmpc:
    - Get gamed and rue the day… (October 25, 2011)
    - The strange case of Gamarue propagation (February 27, 2013)
- JS/Axpergle is a detection for the Angler exploit kit, which exploits vulnerabilities in some versions of Internet Explorer, Microsoft Silverlight, Adobe Flash Player, and the Java Runtime Environment (JRE). It has been observed downloading Win32/Reveton, a ransomware family. See "Exploit kits and other HTML/JavaScript exploits" on page 25 for more information about Axpergle and other exploit kits.

The Angler exploit kit has been observed downloading Win32/Reveton, a ransomware family.

- The downloader family Win32/Ogimant and the exploit family Win32/Anogre are new to the top 10 list in 2H14. First detected in August 2014, Ogimant uses social engineering techniques to appear legitimate, and has been observed to use falsified or stolen digital certificates. Anogre is the Microsoft detection name for the Sweet Orange exploit kit. See "Exploit kits and other HTML/JavaScript exploits" on page 25 for more information about Anogre and other exploit kits.

- The virus family Win32/Sality and the trojan family Win32/Ramnit both returned to the list in 2H14 after an absence. Sality is a file infector that was first detected in 2008; it also attempts to tamper with the installed antimalware solution and to make it harder for Windows to boot in safe mode.

  Ramnit, first detected in 2010, is a multi-component family of trojans and viruses that attempt to steal banking information and allow the attacker unauthorized access to the computer. In February 2015, the MMPC and the Microsoft Digital Crimes Unit (DCU) participated in an international effort to disrupt the Ramnit botnet; encounters involving Ramnit are likely to decrease in 2015 as a result. For more information about the takedown effort, see "Microsoft and partners disrupt the Ramnit botnet" on page 50.

- The trojan families Win32/Wysotot and JS/Faceliker, which were among the top 10 malware families encountered worldwide in 1H14, ranked 11th and 17th in 2H14, respectively.

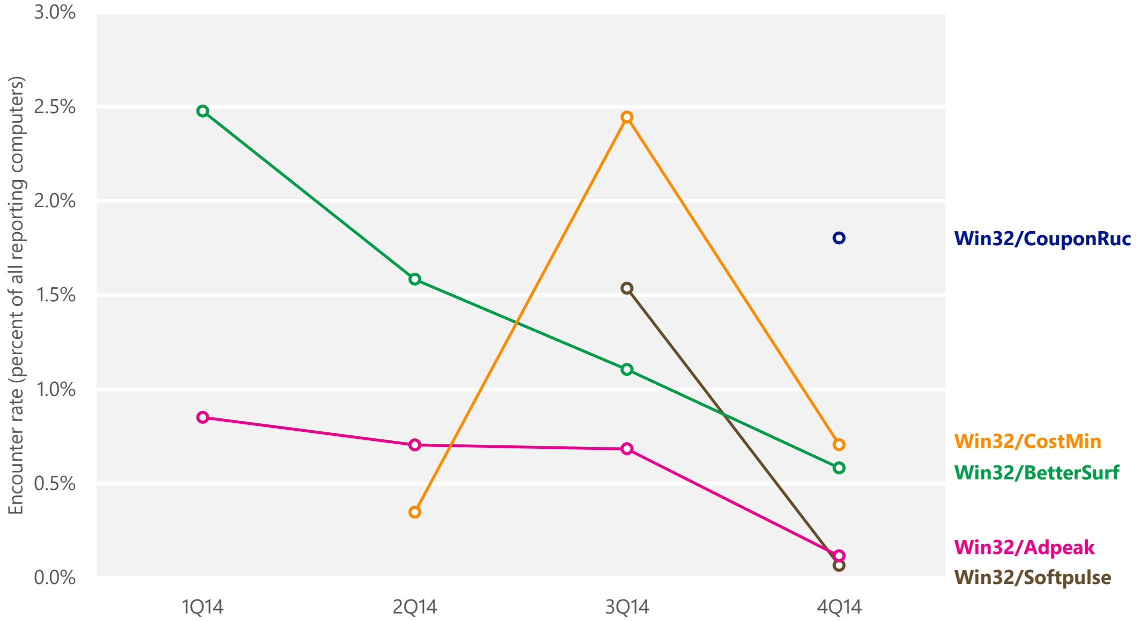
> In February 2015, the MMPC and the DCU participated in an international effort to disrupt the Ramnit botnet.

Figure 39 and Figure 40 show trends for the top unwanted software families that were detected on computers by Microsoft real-time antimalware products worldwide in 2H14.

Figure 39. Quarterly trends for the top five unwanted software families encountered by Microsoft real-time antimalware products in 2H14, shaded according to relative encounter rate

Rank	Family	Most significant category	1Q14	2Q14	3Q14	4Q14
1	Win32/CostMin	Adware	—	0.35%	2.44%	0.71%
2	Win32/CouponRuc	Browser Modifiers	—	—	—	1.80%
3	Win32/BetterSurf	Adware	2.48%	1.58%	1.10%	0.58%
4	Win32/Softpulse	Software Bundlers	—	—	1.54%	0.07%
5	Win32/Adpeak	Adware	0.85%	0.70%	0.68%	0.12%

Figure 40. Encounter rate trends for the top unwanted software families in 2H14



- Win32/CostMin, the most commonly encountered unwanted software family in 2H14 overall and in 3Q14, is an adware family that installs itself as a browser extension for Internet Explorer, Mozilla Firefox, and Google Chrome, and displays advertisements as the user browses the Internet. First detected in 2Q14, CostMin encounters peaked in August of 2014 and declined significantly thereafter.
- Win32/CouponRuc, the most commonly encountered unwanted software family in 4Q14 and the second-most commonly detected unwanted software family in 2H14 overall, is a browser modifier that changes browser settings and may also modify some computer and Internet settings. The MMPC added detections for CouponRuc in December of 2014, and it was detected at high levels thereafter.
- Win32/BetterSurf, the most commonly encountered unwanted software family in 1H14, fell to third place in 2H14. BetterSurf is an adware family that displays advertisements within websites and search engine results. It first appeared in 4Q13, peaked the following quarter, and declined significantly in each quarter thereafter.
- Win32/Softpulse, the fourth-most commonly detected unwanted software family in 2H14, is a software bundler that no longer meets Microsoft detection criteria for unwanted software following a program update in

September of 2014. A small number of Softpulse encounters continued into 4Q14, mostly involving older versions of the program or computers that had not yet updated to the latest detection signatures.

- Win32/Adpeak is an adware program that displays unwanted advertisements in various contexts. Adpeak is often called ScorpionSaver; it injects ads into webpages and does not mention where the ads came from.

Threat families by platform

Malware does not affect all platforms equally. Some threats are spread by exploits that are ineffective against one or more operating system versions. Some threats are more common in parts of the world where specific platforms are more or less popular than elsewhere. In other cases, differences between platforms may be caused by simple random variation.

As Figure 41 demonstrates, the threats encountered by client and server platforms tend to be quite different.

Figure 41. The malware and unwanted software families most commonly encountered on supported Windows client and server platforms in 4Q14

	Client family	Most significant category	4Q14	Server family	Most significant category	4Q14
1	Win32/CouponRuc	Browser Modifiers	1.91%	Win32/Conficker	Worms	0.37%
2	VBS/Jenxcus	Worms	1.15%	Win32/Sality	Viruses	0.29%
3	Win32/Obfuscator	Obfuscators & Injectors	1.13%	INF/Autorun	Obfuscators & Injectors	0.28%
4	INF/Autorun	Obfuscators & Injectors	1.00%	Win32/Gamarue	Worms	0.23%
5	Win32/Gamarue	Worms	0.97%	PHP/SimpleShell	Backdoors	0.21%
6	JS/Axpergle	Exploits	0.95%	Win32/Dynamer	Trojans	0.20%
7	Win32/DefaultTab	Browser Modifiers	0.73%	Win32/Obfuscator	Obfuscators & Injectors	0.20%
8	Win32/CostMin	Adware	0.73%	VBS/Jenxcus	Worms	0.16%
9	Win32/BetterSurf	Adware	0.59%	Win32/Ramnit	Trojans	0.15%
10	Win32/Ogimant	Downloaders & Droppers	0.57%	Win32/Small	Backdoors	0.14%

Figures do not include Brantall, Rotbrow, and Filcout. See "Brantall, Rotbrow, and Filcout" on page 40 for more information.

- Four of the top ten families encountered by client versions of Windows in 4Q14—Win32/CouponRuc, Win32/DefaultTab, Win32/CostMin, and Win32/BetterSurf—were unwanted software families. By contrast, unwanted software families are entirely absent from the list of families most often detected on server computers, reflecting the very different ways that servers are used to access the Internet, enforced by features such as Enhanced Security Configuration in Internet Explorer.

Figure 42 and Figure 43 demonstrate how detections of the most prevalent malware and unwanted software families in 4Q14 ranked differently on different operating system/service pack combinations.

Figure 42. The malware families most commonly encountered by Microsoft real-time antimalware solutions in 4Q14, and how they ranked in prevalence on different platforms

Rank 4Q14	Family	Most significant category	Rank (Windows Vista SP2)	Rank (Windows 7 SP1)	Rank (Windows 8 RTM)	Rank (Windows 8.1 RTM)
1	VBS/Jenxcus	Worms	12	2	1	2
2	Win32/Obfuscator	Obfuscators & Injectors	1	4	4	1
3	INF/Autorun	Obfuscators & Injectors	7	3	3	3
4	Win32/Gamarue	Worms	10	5	2	4
5	JS/Axpergle	Exploits	39	1	176	19
6	Win32/Ogimant	Downloaders & Droppers	49	7	5	5
7	Win32/Sality	Viruses	64	9	7	10
8	Win32/Ramnit	Trojans	45	10	6	6
9	Win32/Anogre	Exploits	8	6	71	74
10	Win32/Tugspay	Downloaders & Droppers	2	17	8	7
15	JS/Krypterade	Ransomware	3	16	10	9

Figures do not include Brantall, Rotbrow, and Filcout. See "Brantall, Rotbrow, and Filcout" on page 40 for more information.

- The top of the list of most commonly encountered malware families was largely consistent from platform to platform. VBS/Jenxcus, Win32/Obfuscator, INF/Autorun, and Win32/Gamarue were all among the five most commonly encountered malware platform on each supported client platform except the oldest, Windows Vista.
- The two exploit kits on the list, JS/Axpergle and Win32/Anogre, showed the most difference between platforms of all the families on the list: Axpergle was the most commonly encountered family on Windows 7 but much lower on the other platforms, and Anogre was commonly encountered on Windows Vista and Windows 7 but rarely encountered on Windows 8 and Windows 8.1. The malicious web pages that exploit kits use to spread malware often include scripts that detect the operating system the client is

running and only present their exploits to certain platforms as designated by the attacker.

Figure 43. The unwanted software families most commonly encountered by Microsoft real-time antimalware solutions in 4Q14, and how they ranked in prevalence on different platforms

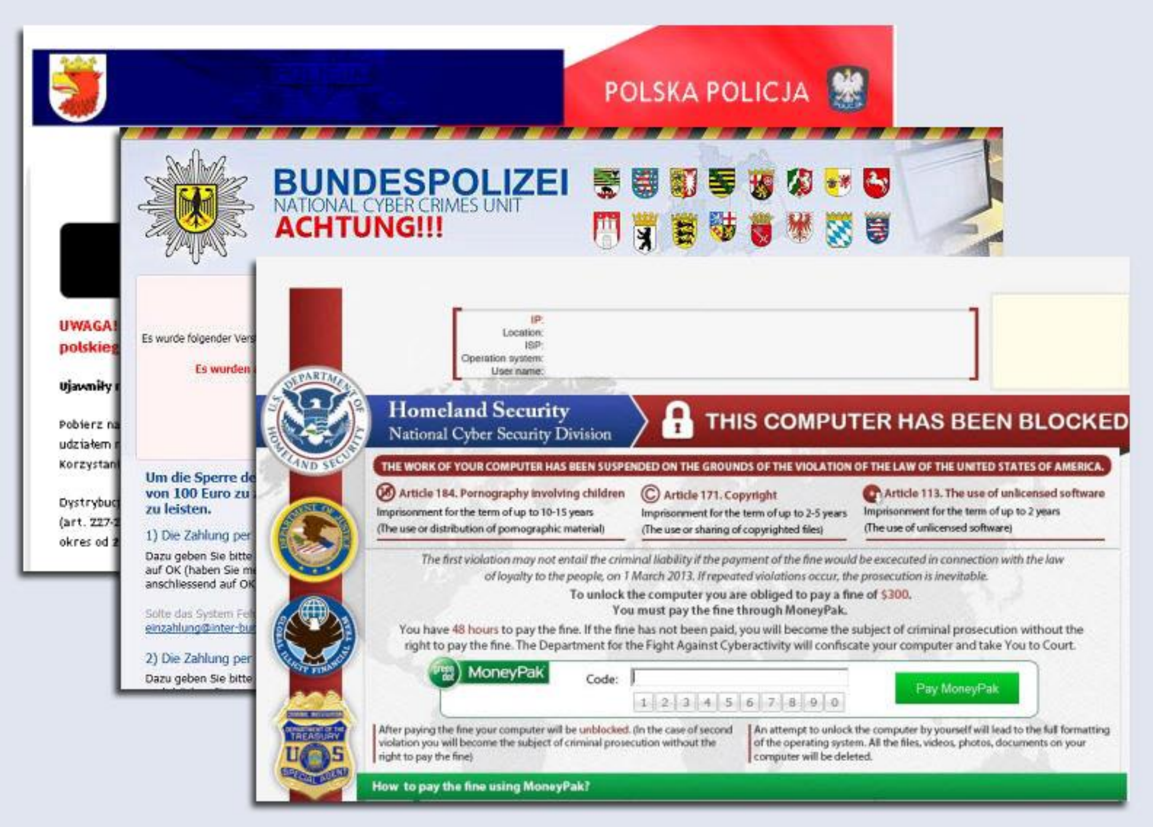
Rank 4Q14	Family	Most significant category	Rank (Windows Vista SP2)	Rank (Windows 7 SP1)	Rank (Windows 8 RTM)	Rank (Windows 8.1 RTM)
1	Win32/CouponRuc	Browser Modifiers	1	1	1	1
2	Win32/CostMin	Adware	3	3	2	2
3	Win32/DefaultTab	Browser Modifiers	2	2	5	4
4	Win32/BetterSurf	Adware	4	4	3	5
5	Win32/PennyBee	Adware	5	5	4	3

- Unlike malware, unwanted software delivery mechanisms typically make little effort to distinguish between different platforms, and as a result the list of the most commonly encountered unwanted software families is nearly identical on each supported platform.

Ransomware

Ransomware is a type of malware that is designed to render a computer or its files unusable until the computer user pays a certain amount of money to the attacker or takes other actions. It often pretends to be an official-looking warning from a well-known law enforcement agency, such as the US Federal Bureau of Investigation (FBI) or the Metropolitan Police Service of London (also known as Scotland Yard). Typically, it accuses the computer user of committing a computer-related crime and demands that the user pay a fine via electronic money transfer or a virtual currency such as Bitcoin to regain control of the computer. Some recent ransomware threats are also known as FBI Moneypak or the FBI virus for their common use of law enforcement logos and requests for payment using Green Dot MoneyPak, a brand of reloadable debit card. A ransomware infection does not mean that any illegal activities have actually been performed on the infected computer.

Figure 44. Examples of the lock screens used by different ransomware families, masquerading as warnings from various national or regional police forces



IP:
Location:
ISP:
Operation system:
User name:

Homeland Security
National Cyber Security Division

THIS COMPUTER HAS BEEN BLOCKED

THE WORK OF YOUR COMPUTER HAS BEEN SUSPENDED ON THE GROUNDS OF THE VIOLATION OF THE LAW OF THE UNITED STATES OF AMERICA.

Article 184. Pornography involving children
Imprisonment for the term of up to 10-15 years
(The use or distribution of pornographic material)

Article 171. Copyright
Imprisonment for the term of up to 2-5 years
(The use or sharing of copyrighted files)

Article 113. The use of unlicensed software
Imprisonment for the term of up to 2 years
(The use of unlicensed software)

The first violation may not entail the criminal liability if the payment of the fine would be excecuted in connection with the law of loyalty to the people, on 1 March 2013. If repeated violations occur, the prosecution is inevitable.

To unlock the computer you are obliged to pay a fine of $300.
You must pay the fine through MoneyPak.

You have 48 hours to pay the fine. If the fine has not been paid, you will become the subject of criminal prosecution without the right to pay the fine. The Department for the Fight Against Cyberactivity will confiscate your computer and take You to Court.

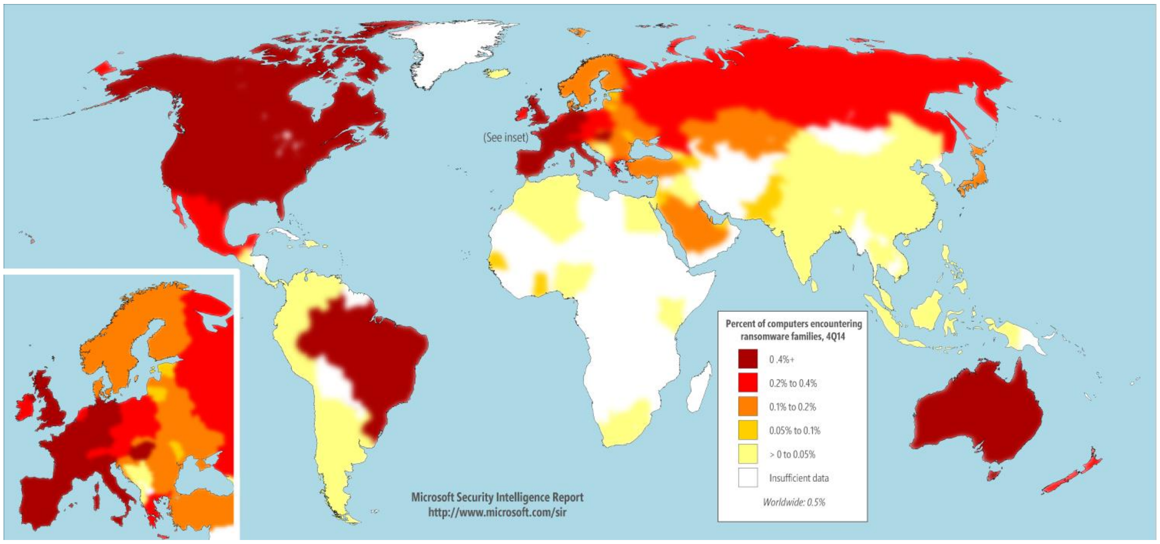
After paying the fine your computer will be unblocked. (In the case of second violation you will become the subject of criminal prosecution without the right to pay the fine)

An attempt to unlock the computer by yourself will lead to the full formatting of the operating system. All the files, videos, photos, documents on your computer will be deleted.

How to pay the fine using MoneyPak?

Ransomware affects different parts of the world unequally. Figure 45 shows encounter rates for ransomware families by country and region in 4Q14.

Figure 45. Encounter rates for ransomware families by country/region in 4Q14



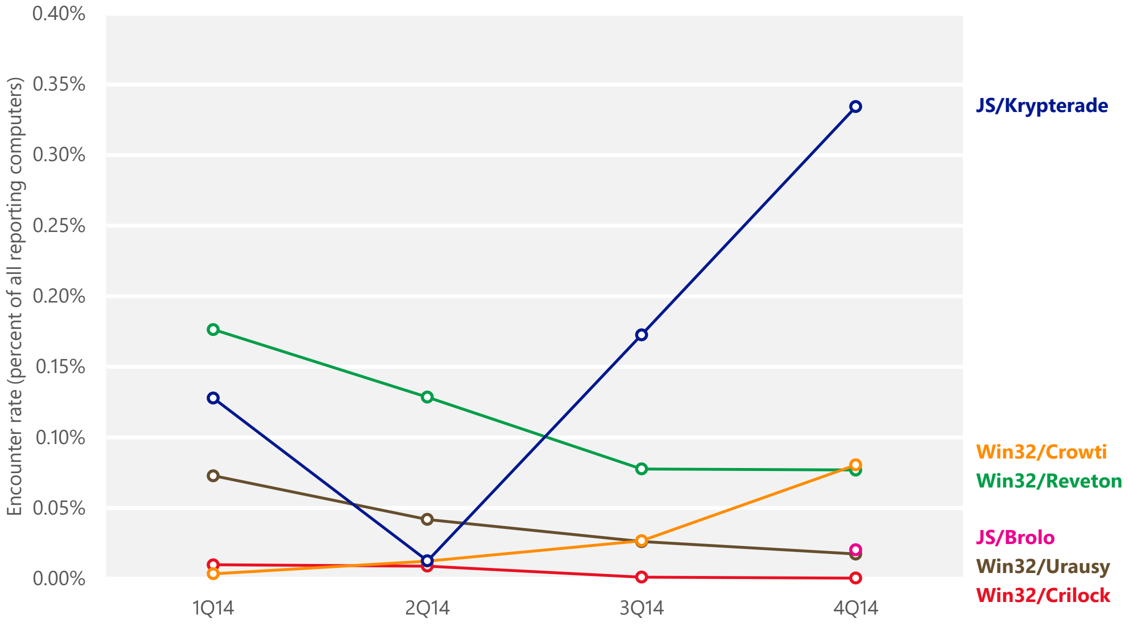
(See inset)
Percent of computers encountering ransomware families, 4Q14
0.4%+
0.2% to 0.4%
0.1% to 0.2%
0.05% to 0.1%
> 0 to 0.05%
Insufficient data
Worldwide: 0.5%
Microsoft Security Intelligence Report
http://www.microsoft.com/sir

- The location with the highest ransomware encounter rate in 4Q14 was the United States (1.18 percent), followed by Canada (1.06 percent) and Portugal (0.84 percent).
- Unlike with many other types of malware, the distribution of ransomware has been highly concentrated geographically. Ransomware encounters in 4Q14 were concentrated in Europe, North America, Brazil, and Oceania, and were much lower elsewhere.

> Unlike many other types of malware, ransomware has been highly concentrated geographically.

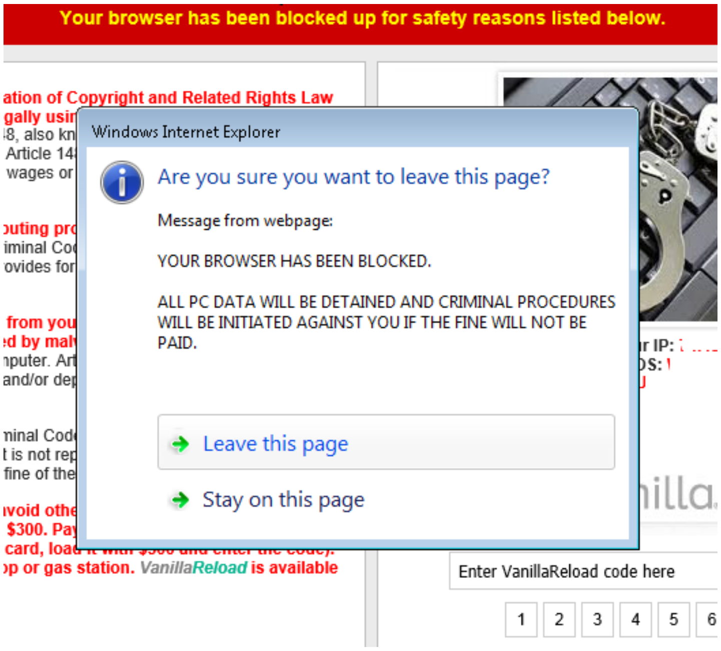
Figure 46 displays encounter rate trends for several of the most commonly encountered ransomware families worldwide.

Figure 46. Trends for several commonly encountered ransomware families in 2H14, by quarter



- Two browser lockers, JS/Krypterade and JS/Brolo, were among the most commonly encountered ransomware families in 2H14. Instead of locking the entire computer, browser lockers only affect the active browser; they use malicious JavaScript to disable any action that can close the browser or navigate to another page, and display warning messages like the one in Figure 47.

Figure 47. An example of a warning message from JS/Brolo



Your browser has been blocked up for safety reasons listed below.

Windows Internet Explorer

Are you sure you want to leave this page?

Message from webpage:

YOUR BROWSER HAS BEEN BLOCKED.

ALL PC DATA WILL BE DETAINED AND CRIMINAL PROCEDURES WILL BE INITIATED AGAINST YOU IF THE FINE WILL NOT BE PAID.

ation of Copyright and Related Rights Law
Leave this page
Stay on this page
Enter VanillaReload code here
1
2
3
4
5
6
op or gas station. VanillaReload is available

Unlike traditional ransomware attacks, which attempt to use exploits and social engineering to launch malicious binary files on targeted computers, browser lockers affect anyone who navigates to the malicious or compromised web page with a conventional browser. Fortunately, browser lockers can also be defeated much more easily than binary ransomware (for example, by using Task Manager to terminate the browser process, or by restarting the computer).

Instead of locking the entire computer, browser lockers only affect the active browser.

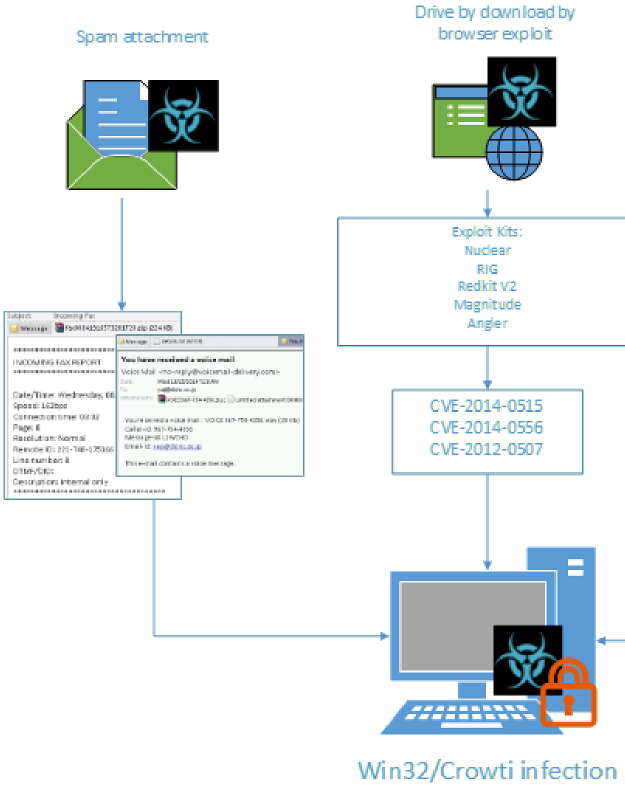
For more information about these threats, see the entry "Your Browser is (not) Locked" (December 17, 2014) in the MMPC blog at blogs.technet.com/mmpc.

- Krypterade was the most commonly encountered ransomware family in 2H14 by a significant margin, being encountered more than four times as frequently as any other ransomware family in the fourth quarter. In addition to displaying fake government warnings like other ransomware threats, Krypterade also sometimes masquerades as the official Java website, disabling attempts to leave the page unless the user downloads a supposed "security update," which may contain more malware. The highest Krypterade encounter rates in 4Q14 were in the United States (0.76 percent), Canada (0.73 percent), and France (0.63 percent).

    - Brolo first appeared in 4Q14. It masquerades as an official government warning page, and can be region-specific. The location with the highest Brolo encounter rate in 4Q14 was the United Kingdom (0.09 percent), followed by Canada (0.07 percent) and the United States (0.05 percent).

- Win32/Crowti (known as “CryptoWall” and “CryptoDefense”), the second-most commonly encountered ransomware family worldwide in 4Q14 and the third in 2H14, typically spreads through spam or is installed by downloader malware and exploits. First detected in late 2013, Crowti is a file encrypting ransomware family that uses a public key to encrypt files on the computer, and then displays a screen demanding that the computer user pay a ransom to receive the private key that will supposedly decode the user’s files. Encounter rates for Crowti were highest in the United States (0.29 percent in 4Q14), Canada (0.10 percent), and Australia (0.04 percent).

Figure 48. Some of the methods attackers use to spread Win32/Crowti



Subject: Incoming Fax

INCOMING FAX REPORT

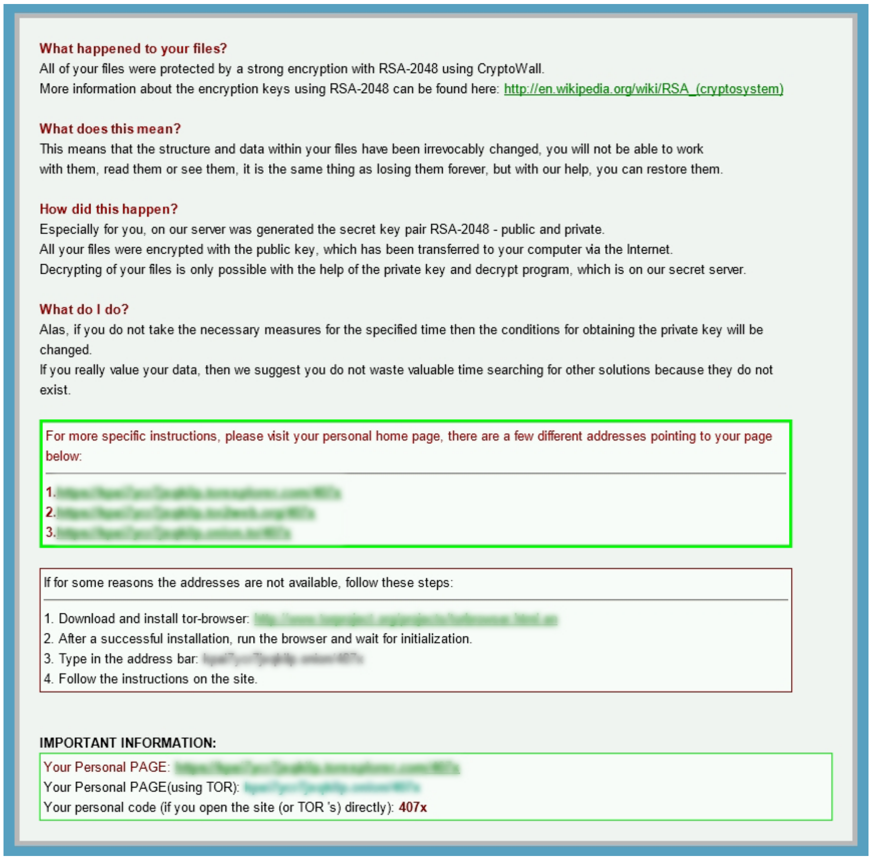
Date/Time: Wednesday, 08
Speed: 1628bps
Connection time: 03:02
Page: 8
Resolution: Normal
Remote ID: 221-168-175166
Line number: 8
DTMF/DID:
Description: Internal only

You have received a voice mail
Voice Mail <no-reply@voicemail-delivery.com>

This e-mail contains a voice message.

After being installed, Crowti encrypts files in important folders such as the user’s Documents, Desktop, and AppData folders, disables a number of services, and displays a ransom note demanding that the user pay several hundred US dollars in exchange for the key that the attacker claims will unlock the files. Crowti makes use of anonymizing services and technologies in an effort to protect the attackers from law enforcement efforts: the victim is instructed to pay the ransom using the Bitcoin virtual currency, and the URLs it provides for paying the ransom are anonymized via the Tor network.

Figure 49. An example of a ransom screen displayed by Win32/Crowti



What happened to your files?
All of your files were protected by a strong encryption with RSA-2048 using CryptoWall.
More information about the encryption keys using RSA-2048 can be found here: http://en.wikipedia.org/wiki/RSA_(cryptosystem)

What does this mean?
This means that the structure and data within your files have been irrevocably changed, you will not be able to work with them, read them or see them, it is the same thing as losing them forever, but with our help, you can restore them.

How did this happen?
Especially for you, on our server was generated the secret key pair RSA-2048 - public and private.
All your files were encrypted with the public key, which has been transferred to your computer via the Internet.
Decrypting of your files is only possible with the help of the private key and decrypt program, which is on our secret server.

What do I do?
Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed.
If you really value your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:

1.[redacted]
2.[redacted]
3.[redacted]

If for some reasons the addresses are not available, follow these steps:

1. Download and install tor-browser: [redacted]
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: [redacted]
4. Follow the instructions on the site.

IMPORTANT INFORMATION:
Your Personal PAGE: [redacted]
Your Personal PAGE(using TOR): [redacted]
Your personal code (if you open the site (or TOR 's) directly): **407x**

Because removing the Crowti infection from the computer does not decrypt the encrypted files, regular backups are the best way to avoid losing access to important files in the event of an infection from Crowti or a similar threat family. For more information about Crowti, see the following entries in the MMPC blog:

- The dangers of opening suspicious emails: Crowti ransomware (October 28, 2014)
- Crowti update - CryptoWall 3.0 (January 13, 2015)

- Win32/Reveton was the third-most commonly encountered ransomware family worldwide in 4Q14 and the second in 2H14. Reveton displays behavior that is typical of many ransomware families: it locks computers, displays a webpage that covers the entire desktop of the infected computer, and demands that the user pay a fine for the supposed possession of illicit material. The webpage that is displayed and the identity of the law enforcement agency that is allegedly responsible for it are often customized, based on the user's current location. Some variants also steal passwords and transmit them to the attacker. Encounter rates for Reveton were highest in Italy (0.23 percent in 4Q14), Portugal (0.22 percent), and Belgium (0.20 percent).

For additional information about Reveton, see the following entries in the MMPC blog (blogs.technet.com/mmpc):

- Revenge of the Reveton (April 18, 2012)
- No paysafecard needed, your passwords will pay off (May 16, 2013)

> Microsoft recommends that victims of malware encounters not pay the so-called fine.

Microsoft recommends that victims of ransomware infections not pay the so-called fine. Ransomware is distributed by malicious attackers, not legitimate authorities, and paying the ransom is no guarantee that the attacker will restore the affected computer to a usable state. Microsoft provides free tools and utilities, such as the Microsoft Safety Scanner and Windows Defender Offline, that can help remove a variety of malware infections even if the computer's normal operation is being blocked.

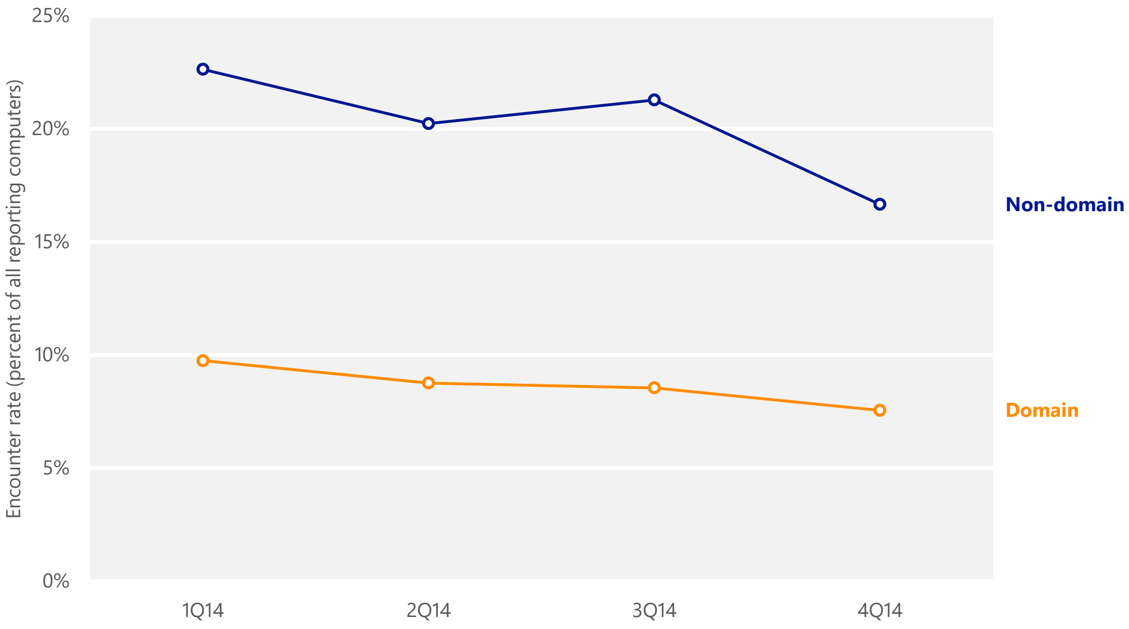
Visit www.microsoft.com/security/portal/mmpc/shared/ransomware.aspx for more information about ransomware and how computer users can avoid being taken advantage of by this type of threat.

Home and enterprise threats

The usage patterns of home users and enterprise users tend to be very different. Enterprise users typically use computers to perform business functions while connected to a network, and may have limitations placed on their Internet and email usage. Home users are more likely to connect to the Internet directly or through a home router and to use their computers for entertainment purposes, such as playing games, watching videos, shopping, and communicating with friends. These different usage patterns mean that home users tend to be exposed to a different mix of computer threats than enterprise users.

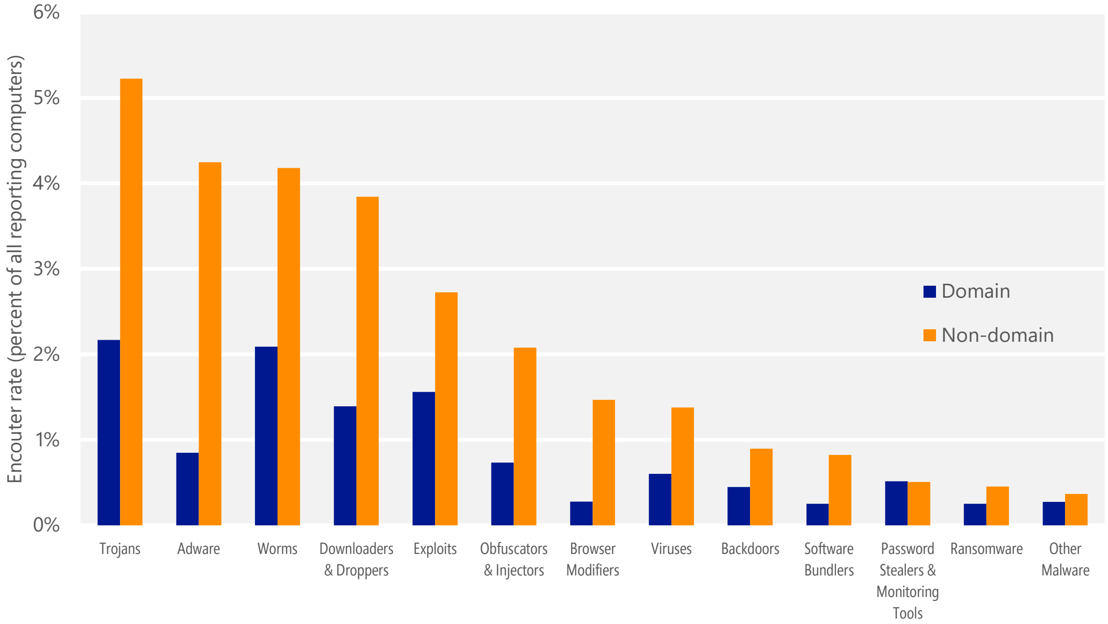
The infection telemetry data produced by Microsoft antimalware products and tools includes information about whether the infected computer belongs to an Active Directory Domain Services (AD DS) domain. Such domains are used almost exclusively in enterprise environments, and computers that do not belong to a domain are more likely to be used at home or in other non-enterprise contexts. Comparing the threats encountered by domain-joined computers and non-domain computers 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 50. Malware encounter rates for domain-based and non-domain computers in 2014



Figures do not include Brantall, Rotbrow, and Filcout. See “Brantall, Rotbrow, and Filcout” on page 40 for more information.

Figure 51. Malware and unwanted software encounter rates for domain-based and non-domain computers, 2H14, by category



Figures do not include Brantall, Rotbrow, and Filcout. See "Brantall, Rotbrow, and Filcout" on page 40 for more information.

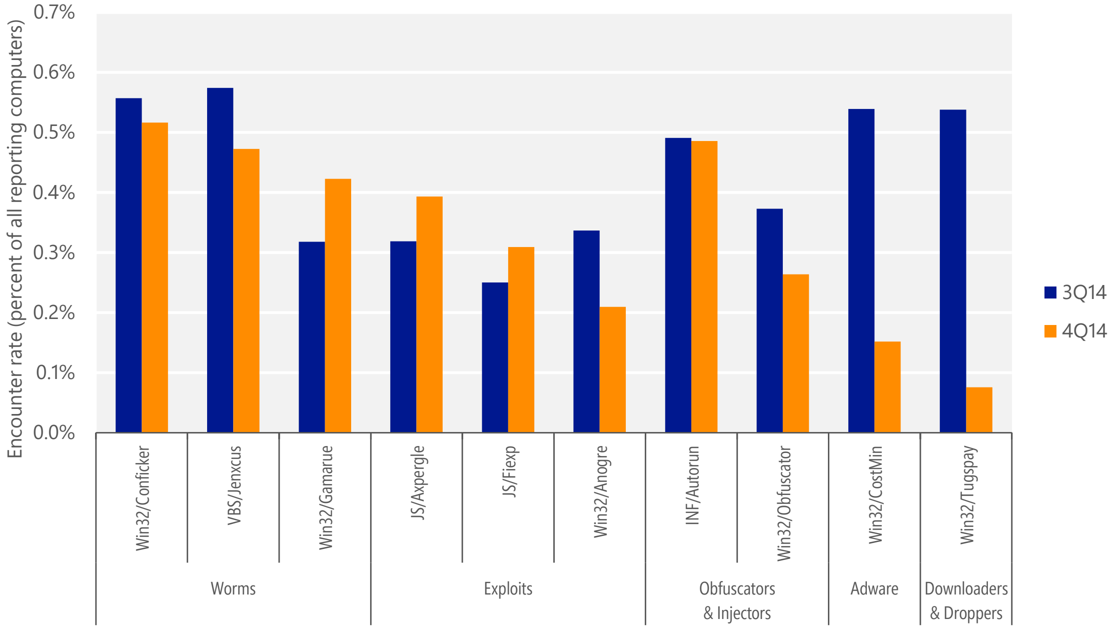
- Enterprise environments typically implement defense-in-depth measures, such as enterprise firewalls, that prevent a certain amount of malware from reaching users' computers. Consequently, enterprise computers tend to encounter malware at a lower rate than consumer computers. As Figure 50 shows, the encounter rate for consumer computers was about 2.3 times as high as the rate for enterprise computers in 2H14.
- In addition to encountering less malware in general, computers in enterprise environments tend to encounter different kinds of threats than consumer computers, as shown in Figure 51. Non-domain computers encountered disproportionate amounts of unwanted software compared to domain-based computers, with Adware, Browser Modifiers, and Software Bundlers each appearing between three and six times as often on non-domain computers. Meanwhile, despite encountering less than half as much malware as non-domain computers overall, domain-based computers actually encountered slightly more Password Stealers & Monitoring Tools malware than their non-domain counterparts.

> The usage patterns of home and enterprise users tend to be very different.

Figure 52 and Figure 53 list the top 10 malware families detected on domain-joined and non-domain computers, respectively, in 2H14.

Figure 52. Quarterly trends for the top 10 malware and unwanted software families detected on domain-joined computers in 2H14, by percentage of computers encountering each family

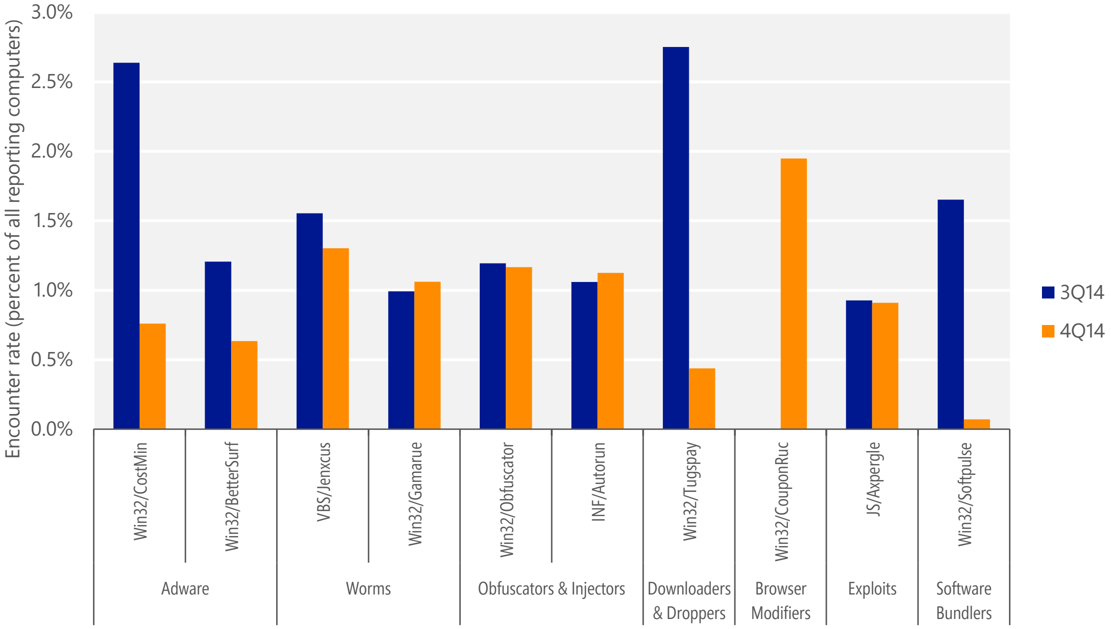
Family	Most significant category	3Q14	4Q14
Win32/Conficker	Worms	0.56%	0.52%
VBS/Jenxcus	Worms	0.57%	0.47%
INF/Autorun	Obfuscators & Injectors	0.49%	0.49%
Win32/Gamarue	Worms	0.32%	0.42%
JS/Axpergle	Exploits	0.32%	0.39%
Win32/CostMin	Adware	0.54%	0.15%
Win32/Obfuscator	Obfuscators & Injectors	0.37%	0.26%
Win32/Tugspay	Downloaders & Droppers	0.54%	0.08%
JS/Fiexp	Exploits	0.25%	0.31%
Win32/Anogre	Exploits	0.34%	0.21%



Figures do not include Brantall, Rotbrow, and Filcout. See "Brantall, Rotbrow, and Filcout" on page 40 for more information.

Figure 53. Quarterly trends for the top 10 malware and unwanted software families detected on non-domain computers in 2H14, by percentage of computers encountering each family

Family	Most significant category	3Q14	4Q14
Win32/CostMin	Adware	2.64%	0.76%
Win32/Tugspay	Downloaders & Droppers	2.75%	0.44%
VBS/Jenxcus	Worms	1.55%	1.30%
Win32/Obfuscator	Obfuscators & Injectors	1.19%	1.17%
INF/Autorun	Obfuscators & Injectors	1.06%	1.13%
Win32/Gamarue	Worms	0.99%	1.06%
Win32/CouponRuc	Browser Modifiers	—	1.95%
Win32/BetterSurf	Adware	1.21%	0.63%
JS/Axpergle	Exploits	0.93%	0.91%
Win32/Softpulse	Software Bundlers	1.65%	0.07%



Figures do not include Brantall, Rotbrow, and Filcout. See "Brantall, Rotbrow, and Filcout" on page 40 for more information.

- Seven threats—Win32/Tugspay, VBS/Jenxcus, Win32/Obfuscator, INF/Autorun, Win32/Gamarue, JS/Axpergle, and Win32/CostMin—were common to both lists. All were more frequently encountered on non-domain computers than on domain-joined computers. See "Threat families" on page 59 for more information about these families.

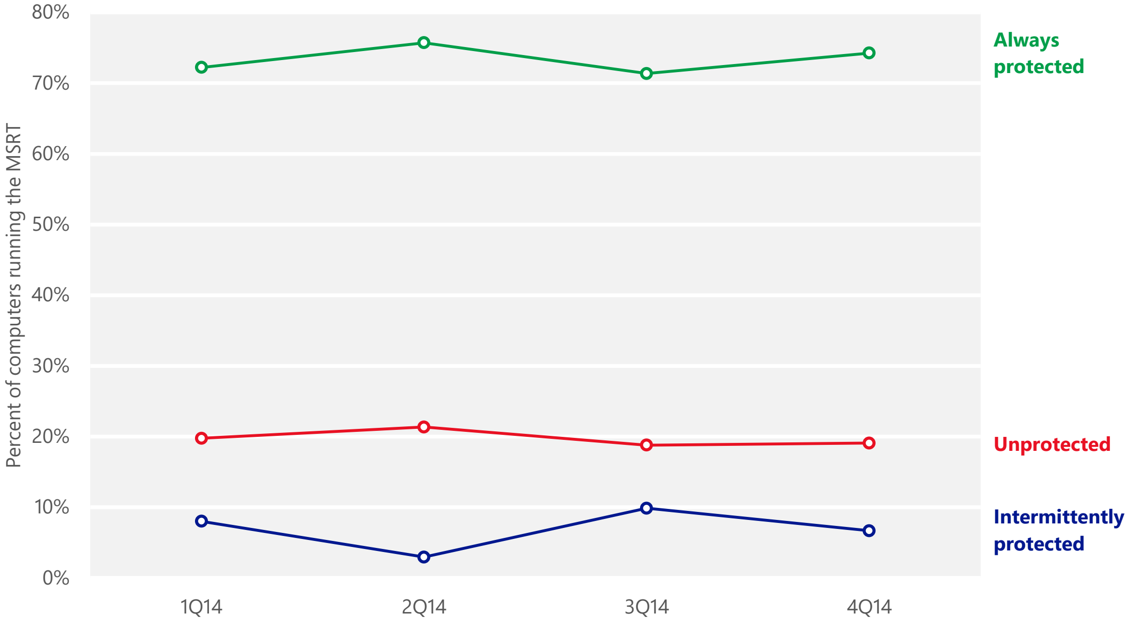
- Four of the top 10 malware families on domain-joined computers are worms that can spread via removable drives, which are commonly used in domain environments. (Although classified with Obfuscators & Injectors here, INF/Autorun is also considered a worm, because it uses automatic propagation techniques to spread.) Autorun and Win32/Conficker also spread via mapped network drives.
- The three families that are unique to the top 10 list for domain-joined computers but not for non-domain computers are Conficker and the exploit kit families JS/Fiexp and Win32/Anogre. Fiexp and Anogre were actually encountered at slightly higher rates on non-domain computers than on domain-joined computers, but did not make the list because other families were encountered more often on non-domain computers. 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.

See "Malware at Microsoft: Dealing with threats in the Microsoft environment" on page 93 for information about the threat landscape on computers at Microsoft and to learn about the actions Microsoft IT takes to protect users, data, and resources.

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. Figure 54 shows the percentage of computers worldwide that the MSRT found to be protected or unprotected by real-time security software each quarter in 2014.

Figure 54. Percentage of computers worldwide protected by real-time security software in 2014



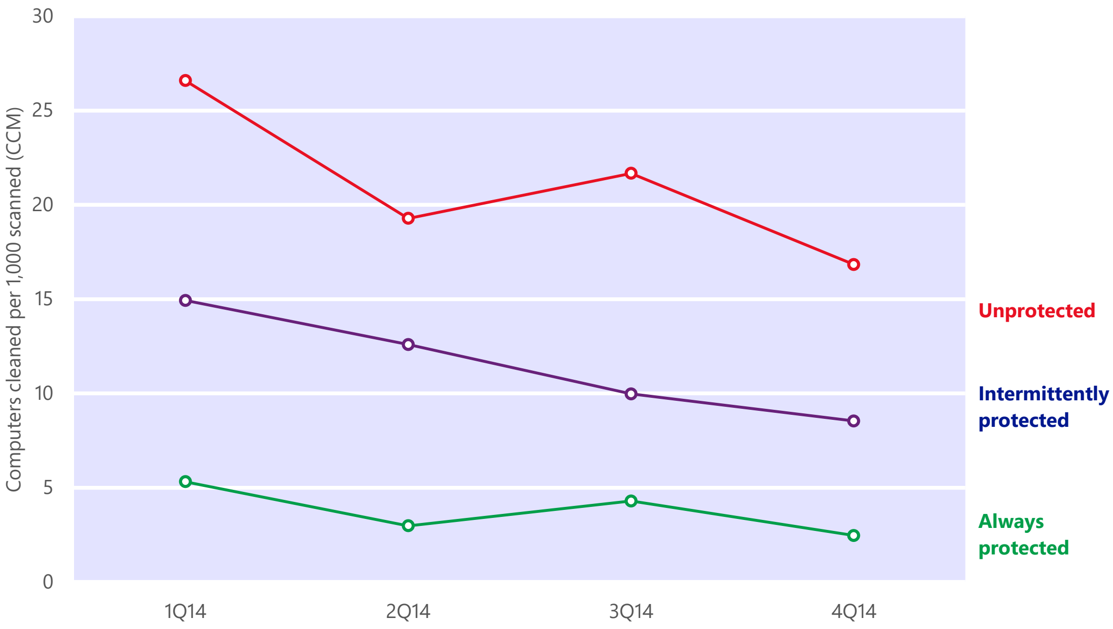
- A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In Figure 54, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" 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.
- 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 75.7 percent.

> About three-fourths of computers worldwide were found to be protected by real-time security software at every monthly MSRT execution.

- Computers that never reported running security software accounted for between 18.8 and 21.3 percent of computers worldwide each quarter. Intermittently protected computers—those that were found to be running real-time security software during at least one MSRT execution in a quarter, but not all of them—accounted for between 2.9 and 9.8 percent of computers each quarter.

Computers that do not run real-time security software are at significantly greater risk of malware infection than computers that do. Figure 55 compares infection rates with protection levels worldwide for each of the last four quarters.

Figure 55. Infection rates for protected and unprotected computers in 2014



Figures do not include Brantall, Rotbrow, and Filcout. See "Brantall, Rotbrow, and Filcout" on page 40 for more information.

- The MSRT reported that computers that were never found to be running real-time security software during 2H14 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 as likely to be infected with malware in 2H14 as computers that were always protected.

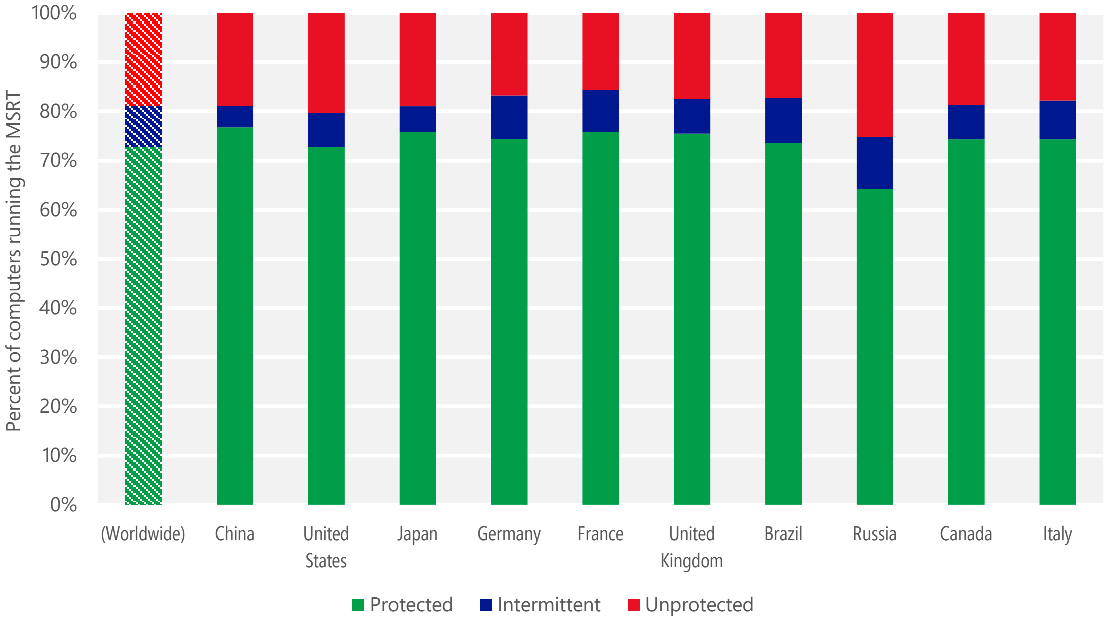
Computers that do not run real-time security software are at significantly greater risk of malware infection than computers that do.

- Users who don't run real-time security software aren't always unprotected by choice: a number of prevalent malware families are capable of disabling some security products, potentially without the user even knowing. Other users may disable or uninstall security software intentionally because of perceived performance issues, a belief that protection is not necessary, or a desire to run programs that would be quarantined or removed by security software. In other cases, users lose up-to-date real-time protection when they don't renew paid subscriptions for their antimalware software, which may come pre-installed with their computers as limited-time trial software. (See "The challenge of expired security software" on pages 21–28 of *Microsoft Security Intelligence Report, Volume 17 (January–June 2014)*, available from the Microsoft Download Center, for more information about the causes and consequences of expired security software.) Whatever the reason, users who don't have functioning real-time antimalware protection face significantly greater risk from malware infection than users who do, as Figure 55 illustrates.

Security software use worldwide

Just as infection and encounter rates differ from one country or region to another, so do security software usage rates, as shown in Figure 56.

Figure 56. Average quarterly security software protection state for the locations with the most computers executing the MSRT in 2H14



- Computers that reported being fully protected in these locations ranged between 64.3 percent and 76.7 percent, with all locations except the United States and Russia exceeding the worldwide rate of 72.8 percent of computers reporting as fully protected.
- Computers that reported being fully unprotected in these locations ranged between 15.6 percent and 25.2 percent, with Russia, the United States,

Japan, and China reporting larger percentages of fully unprotected computers than the world overall.

- Computers that were protected in some months but not in others accounted for between 4.3 percent and 10.5 percent in these locations.

The rate of security software usage in a country or region often correlates with its infection rate. Figure 57 and Figure 58 show the percentage of computers in different countries and regions that reported being fully protected and fully unprotected, respectively, in 4Q14.

Figure 57. Percent of computers reporting as Protected during every MSRT execution in 4Q14, by country/region

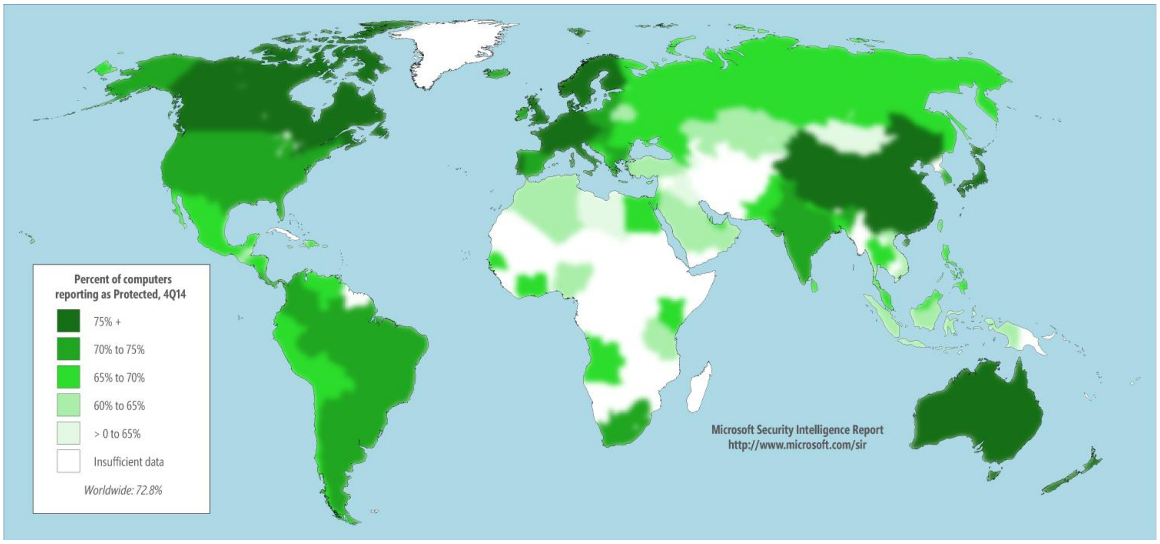
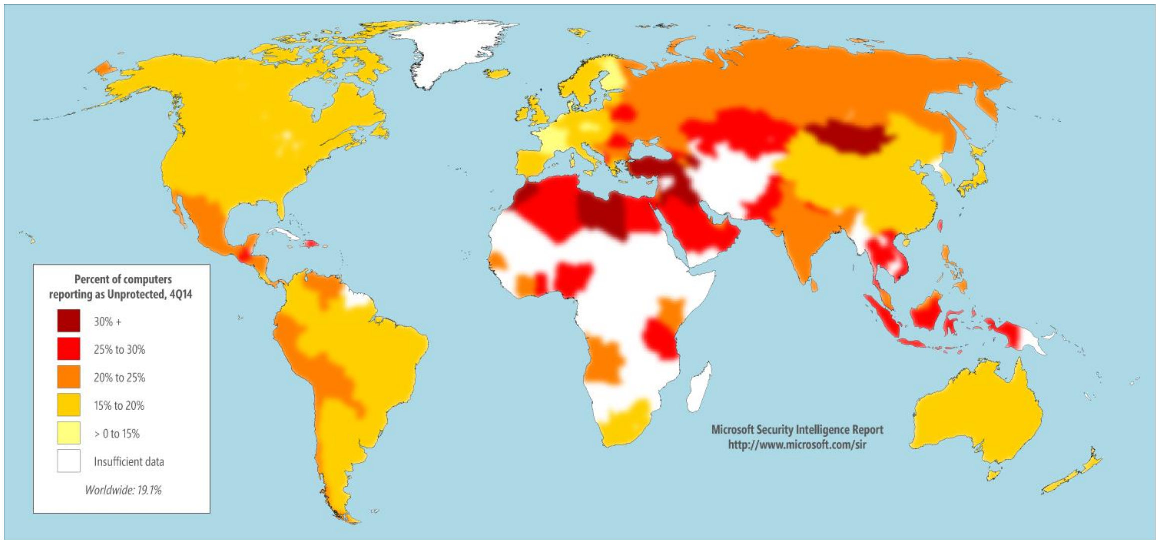

Percent of computers reporting as Protected, 4Q14
75% +
70% to 75%
65% to 70%
60% to 65%
> 0 to 65%
Insufficient data
Worldwide: 72.8%
Microsoft Security Intelligence Report
http://www.microsoft.com/sir

Figure 58. Percent of computers reporting as Unprotected during every MSRT execution in 4Q14, by country/region


Percent of computers reporting as Unprotected, 4Q14
30% +
25% to 30%
20% to 25%
15% to 20%
> 0 to 15%
Insufficient data
Worldwide: 19.1%
Microsoft Security Intelligence Report
http://www.microsoft.com/sir

- The locations with the most computers reporting as fully protected by real-time security software include Finland, with 84.2 percent of computers reporting as fully protected in 4Q14; Denmark, at 79.8 percent; and Norway and the Czech Republic, both at 79.1 percent. Locations with the fewest computers reporting as fully protected include Libya, at 47.3 percent; Iraq, at 53.5 percent; and Azerbaijan, at 58.1 percent.
- The ranking of countries and regions by unprotected rate is largely an inverse of their ranking according to protected rate. The locations with the fewest computers reporting as fully unprotected include Finland, at 10.4 percent; Denmark, at 14.1 percent; and the Czech Republic, at 14.3 percent. Locations with the most computers reporting as fully unprotected include Libya, at 41.6 percent; Iraq, at 39.5 percent; and Azerbaijan, at 32.5 percent.

Countries and regions with high percentages of computers reporting as fully unprotected also tend to have high infection rates, as Figure 59 shows.

Figure 59. Infection rates for the locations with the highest percentage of computers reporting as fully unprotected in 2H14

Country/Region	2H14 Average Unprotected %	CCM 3Q14	CCM 4Q14	Unprotected CCM 3Q14	Unprotected CCM 4Q14
Libya	40.7%	60.3	61.2	111.8	113.5
Iraq	39.3%	88.5	81.3	192.5	172.9
Azerbaijan	32.1%	35.5	31.0	81.8	69.2
Palestinian Authority	32.1%	63.3	63.5	144.5	156.9
Morocco	32.1%	60.2	56.5	145.1	146.8
Mongolia	32.1%	—	66.3	—	167.7
Jordan	31.0%	42.4	40.4	107.4	99.7
Turkey	30.2%	40.7	24.9	86.4	59.8
Lebanon	30.2%	33.3	31.7	79.5	80.2
Vietnam	29.7%	39.9	35.7	93.0	79.6
Worldwide	*18.9%*	*8.6*	*5.9*	*21.7*	*16.8*

Figures do not include Brantall, Rotbrow, and Filcout. See "Brantall, Rotbrow, and Filcout" on page 40 for more information.

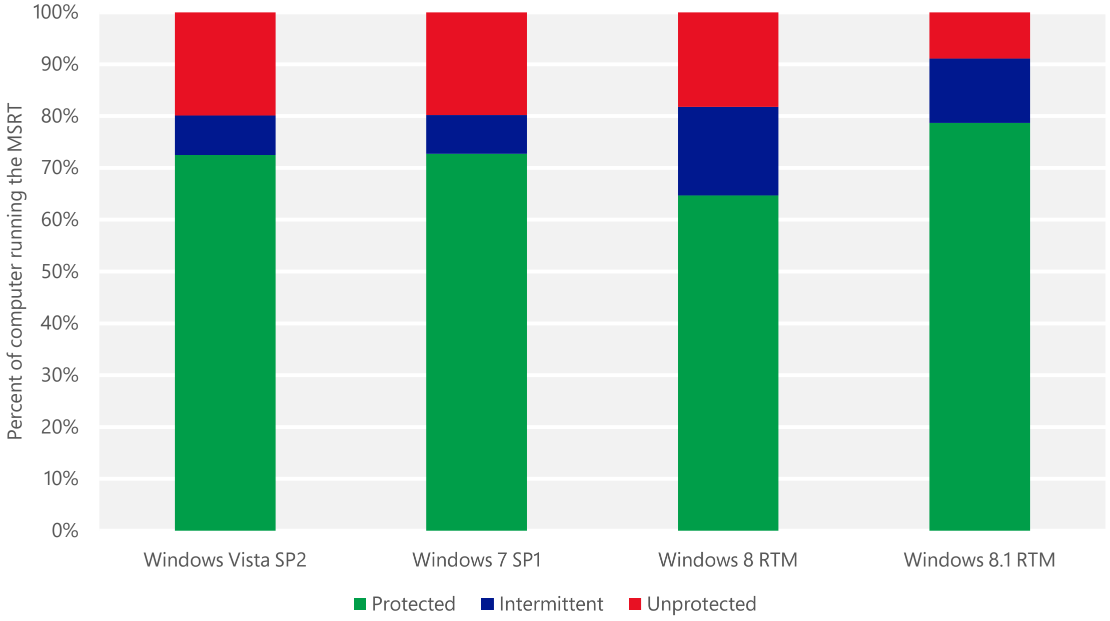
- The locations in the table all had overall infection rates ranging between 3.9 and 13.8 times as high as the worldwide average each quarter.
- The infection rates for fully unprotected computers in these locations ranged between 3.6 and 10.3 times as high as the infection rates for fully unprotected computers worldwide, and between 9.2 and 29.3 times as

high as the infection rates for all computers worldwide. In Iraq, the location with the highest infection rates in Figure 59, the MSRT detected and removed malware on 19.3 percent of the fully unprotected computers that executed it at least once in 3Q14 (a CCM of 192.5).

Security software use by platform

Protection rates can also vary by operating system, as shown in Figure 60.

Figure 60. Average quarterly security software protection state for supported client versions of Windows in 2H14



- Only 8.9 percent of computers running Windows 8.1 reported being unprotected during every MSRT execution each quarter on average, which is less than half of the rate reported by computers running any other supported client version of Windows. As Figure 61 shows, this factor contributed directly to the Windows 8.1 low infection rate overall, with just 0.8 out of every 1,000 fully protected computers running Windows 8.1 reporting an infection (a CCM of 0.8), and a CCM of 1.5 for Windows 8.1 computers overall.

Figure 61. Infection rate (CCM) for supported client versions of Windows in 2H14, by average quarterly security software protection state

Platform	Overall	Protected	Intermittent	Unprotected
Windows Vista SP2	7.8	4.3	9.8	15.8
Windows 7 SP1	7.6	3.2	11.2	18.4
Windows 8 RTM	5.9	2.1	7.8	15.3
Windows 8.1 RTM	1.5	0.8	3.1	5.7

Guidance: Defending against malware

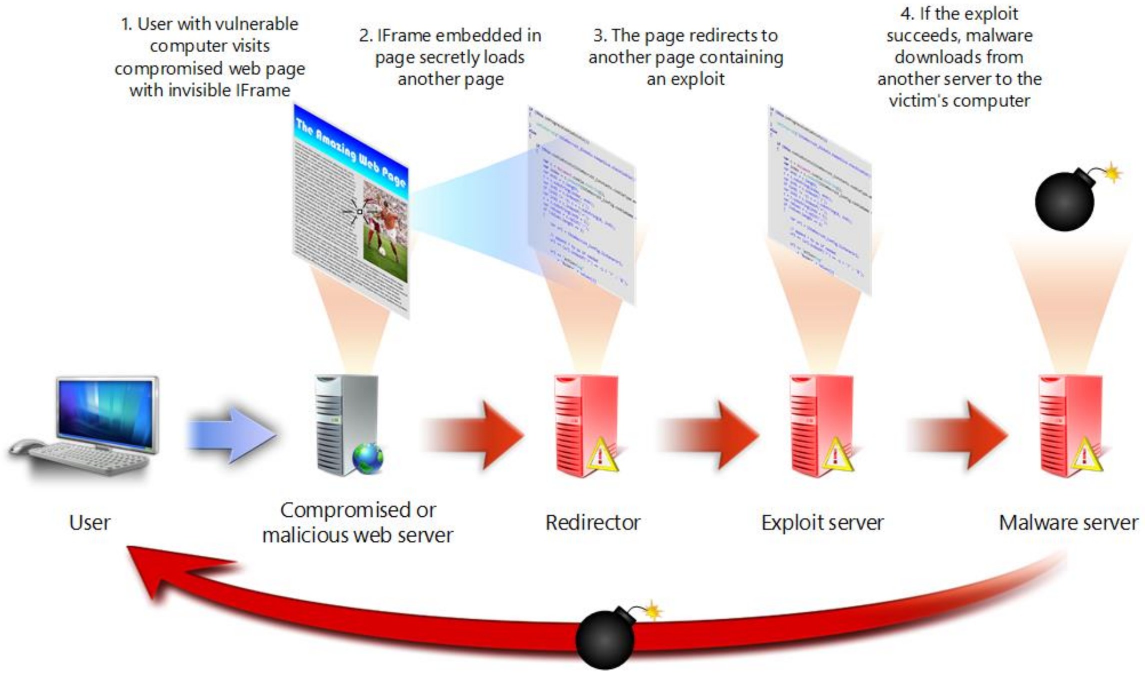
Effectively protecting users from malware requires an active effort on the part of organizations and individuals. For in-depth guidance, see Help prevent malware infection on your PC at the Microsoft Malware Protection Center website at www.microsoft.com/mmpc.

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.

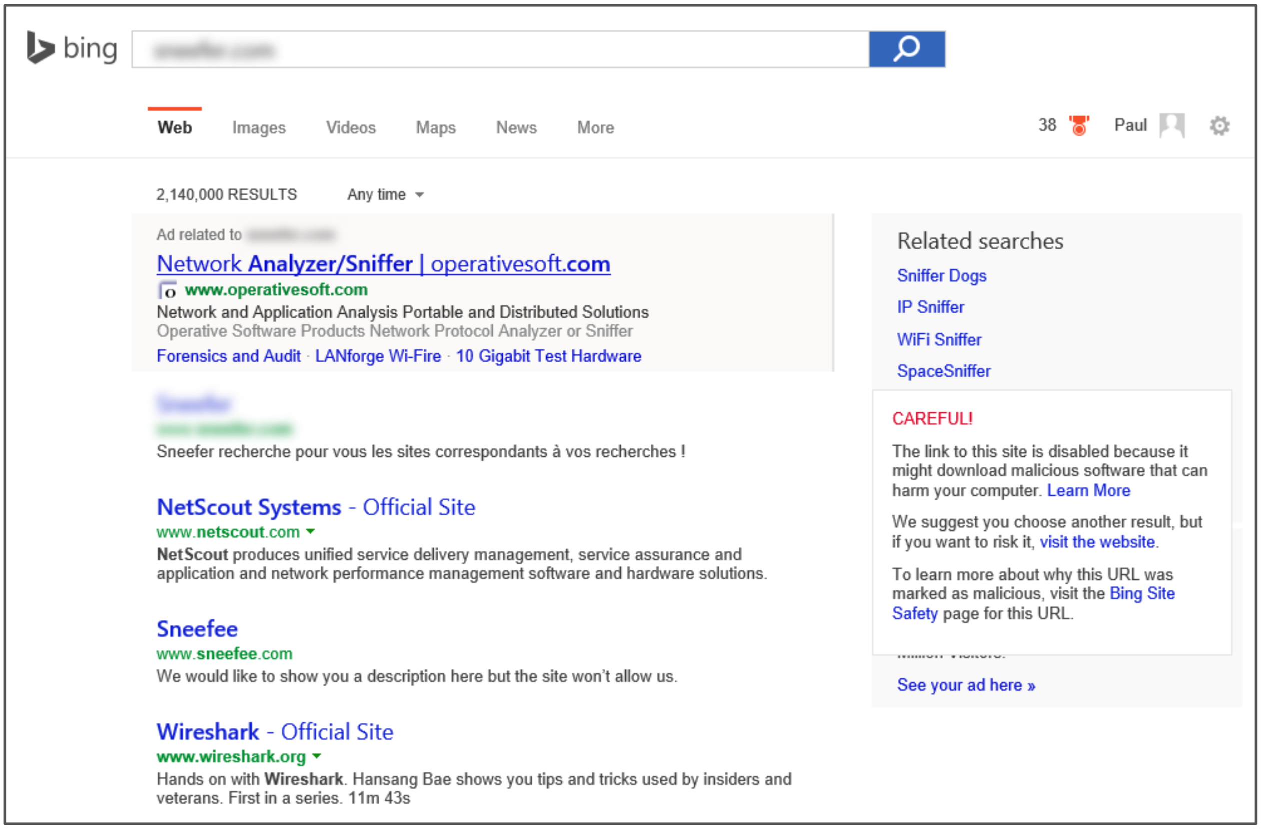
Drive-by download pages are usually hosted on legitimate websites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Figure 62. One example of a drive-by download attack


1. User with vulnerable computer visits compromised web page with invisible IFrame
2. IFrame embedded in page secretly loads another page
3. The page redirects to another page containing an exploit
4. If the exploit succeeds, malware downloads from another server to the victim's computer
The Amazing Web Page
User
Compromised or malicious web server
Redirector
Exploit server
Malware server

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes webpages, they are assessed for malicious elements or malicious behavior. Because the owners of compromised sites are usually victims themselves, the sites are not removed from the Bing index. Instead, clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software, as shown in Figure 63.

Figure 63. A drive-by download warning from Bing



2,140,000 RESULTS Any time

Ad related to [redacted]

Network Analyzer/Sniffer | operativesoft.com
www.operativesoft.com
Network and Application Analysis Portable and Distributed Solutions
Operative Software Products Network Protocol Analyzer or Sniffer
Forensics and Audit · LANforge Wi-Fire · 10 Gigabit Test Hardware

[redacted]
Sneefer recherche pour vous les sites correspondants à vos recherches !

NetScout Systems - Official Site
www.netscout.com
NetScout produces unified service delivery management, service assurance and application and network performance management software and hardware solutions.

Sneefee
www.sneefee.com
We would like to show you a description here but the site won't allow us.

Wireshark - Official Site
www.wireshark.org
Hands on with Wireshark. Hansang Bae shows you tips and tricks used by insiders and veterans. First in a series. 11m 43s

Related searches
Sniffer Dogs
IP Sniffer
WiFi Sniffer
SpaceSniffer

CAREFUL!

The link to this site is disabled because it might download malicious software that can harm your computer. Learn More

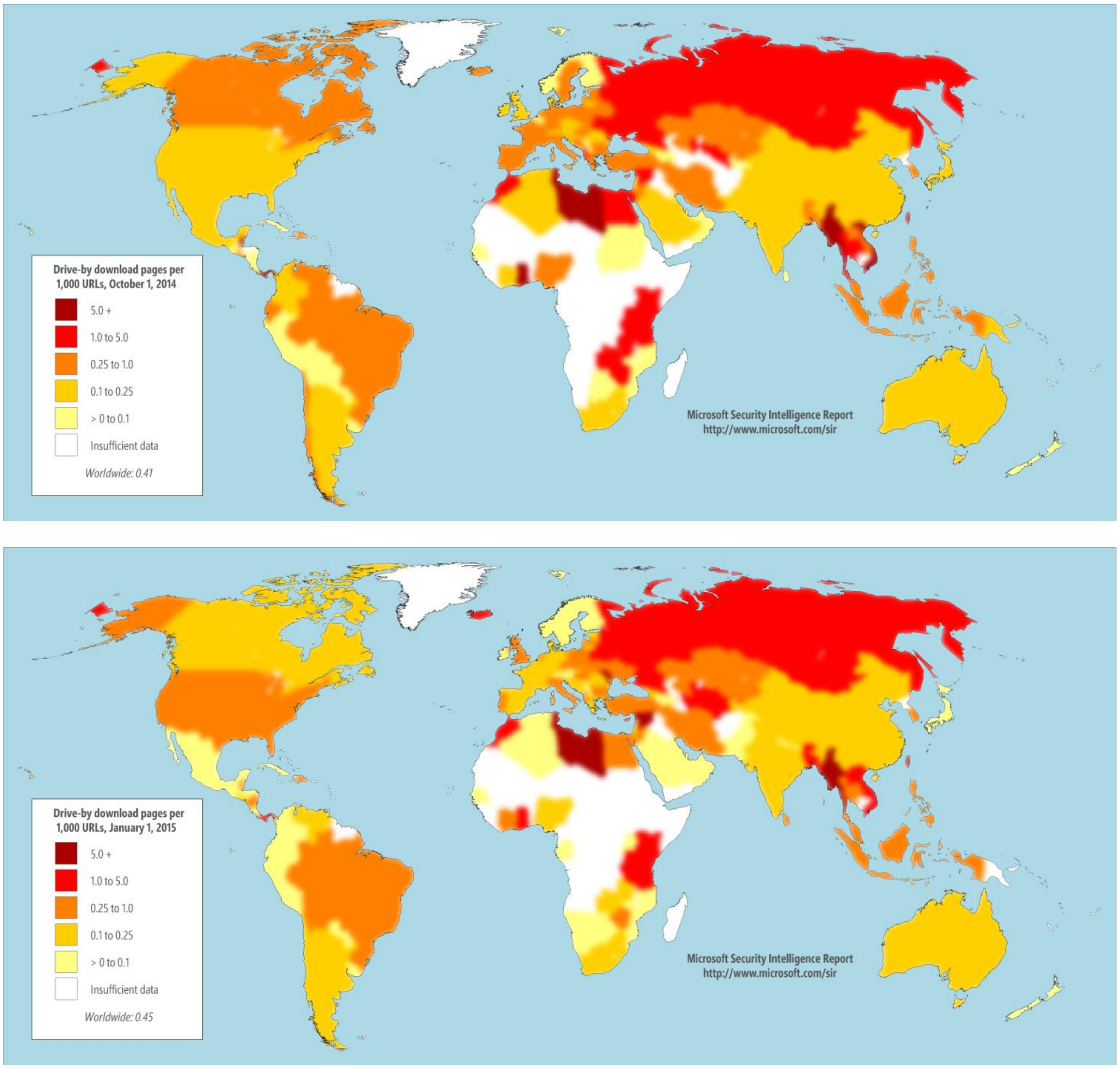
We suggest you choose another result, but if you want to risk it, visit the website.

To learn more about why this URL was marked as malicious, visit the Bing Site Safety page for this URL.

See your ad here »

Figure 64 shows the concentration of drive-by download pages in countries and regions throughout the world at the end of 3Q14 and 4Q14, respectively.

Figure 64. Drive-by download pages indexed by Bing at the end of 3Q14 (top) and 4Q14 (bottom), per 1,000 URLs in each country/region


Drive-by download pages per 1,000 URLs, October 1, 2014
5.0 +
1.0 to 5.0
0.25 to 1.0
0.1 to 0.25
> 0 to 0.1
Insufficient data
Worldwide: 0.41
Microsoft Security Intelligence Report
http://www.microsoft.com/sir
Drive-by download pages per 1,000 URLs, January 1, 2015
5.0 +
1.0 to 5.0
0.25 to 1.0
0.1 to 0.25
> 0 to 0.1
Insufficient data
Worldwide: 0.45
Microsoft Security Intelligence Report
http://www.microsoft.com/sir

- Each map shows the concentration of drive-by download URLs tracked by Bing in each country or region on a reference date at the end of the associated quarter, expressed as the number of drive-by download URLs per every 1,000 URLs hosted in the country/region.
- Significant locations with high concentrations of drive-by download URLs in both quarters include Taiwan, with 12.1 drive-by URLs for every 1,000 URLs tracked by Bing at the end of 4Q14; Vietnam, with 4.1; and Russia, with 2.4.

Guidance: Protecting users from unsafe websites

One of the best ways organizations can protect their users from malicious and compromised websites is by mandating the use of web browsers with appropriate protection features built in and by promoting safe browsing practices. For in-depth guidance, see "Top security solutions" at www.microsoft.com/security/pc-security/solutions.aspx.

Mitigating risk

Malware at Microsoft: Dealing with threats in the Microsoft environment

Microsoft IT

Microsoft IT provides information technology services internally for Microsoft employees and resources. Microsoft IT manages more than 600,000 devices for more than 150,000 users across more than 100 countries and regions worldwide. Safeguarding a computing infrastructure of this size requires implementation of strong security policies, technology to help keep malware off the network and away from mission-critical resources, and dealing with malware outbreaks swiftly and comprehensively when they occur.

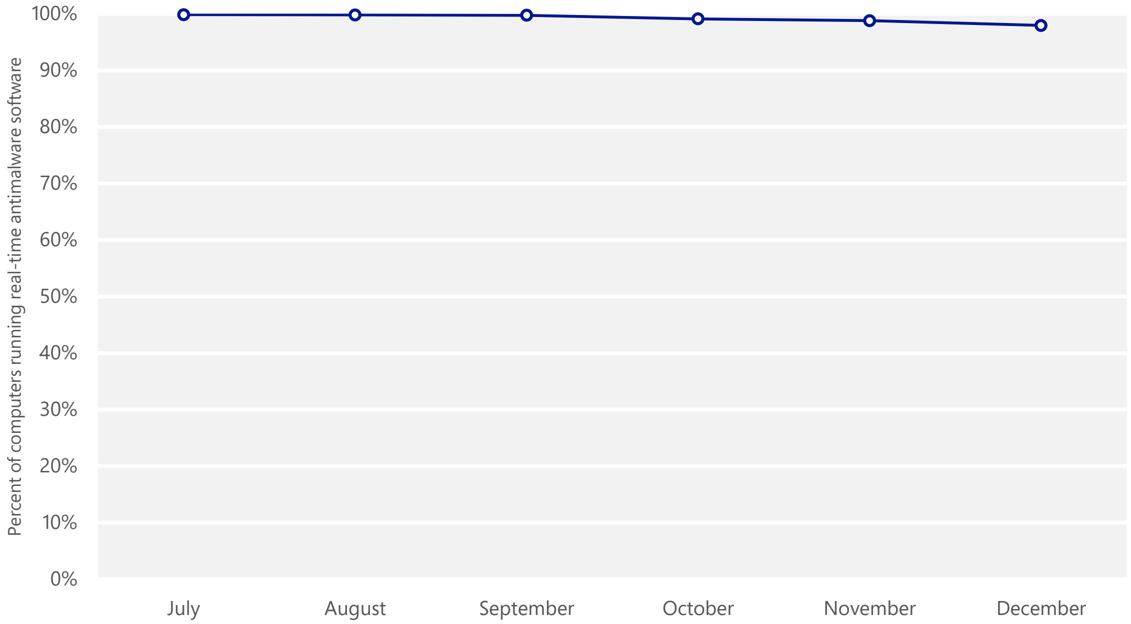
This section of the report compares the potential impact of malware to the levels of antimalware compliance from more than 500,000 workstation computers and servers managed by Microsoft IT between July and December 2014. This data is compiled from multiple sources, including System Center Endpoint Protection (SCEP), Windows Defender, Network Access Protection, DirectAccess, and manual submission of suspicious files. Comparing the nature and volume of the malware detected on these computers to the level of protection they receive can illustrate significant trends and provide insights as to the effectiveness of antimalware software and security best practices.

Antimalware usage

Real-time antimalware software is required on all user devices that connect to the Microsoft corporate network. System Center Endpoint Protection 2012 (SCEP) is the antimalware solution that Microsoft IT deploys to its users. To be considered compliant with antimalware policies and standards, user computers must be running the latest version of the SCEP client, antimalware signatures must be no more than six days old, and real-time protection must be enabled.

Figure 65 shows the level of antimalware noncompliance in the Microsoft user workstation environment for each month in 2H14.

Figure 65. Percentage of computers at Microsoft running real-time antimalware software in 2H14



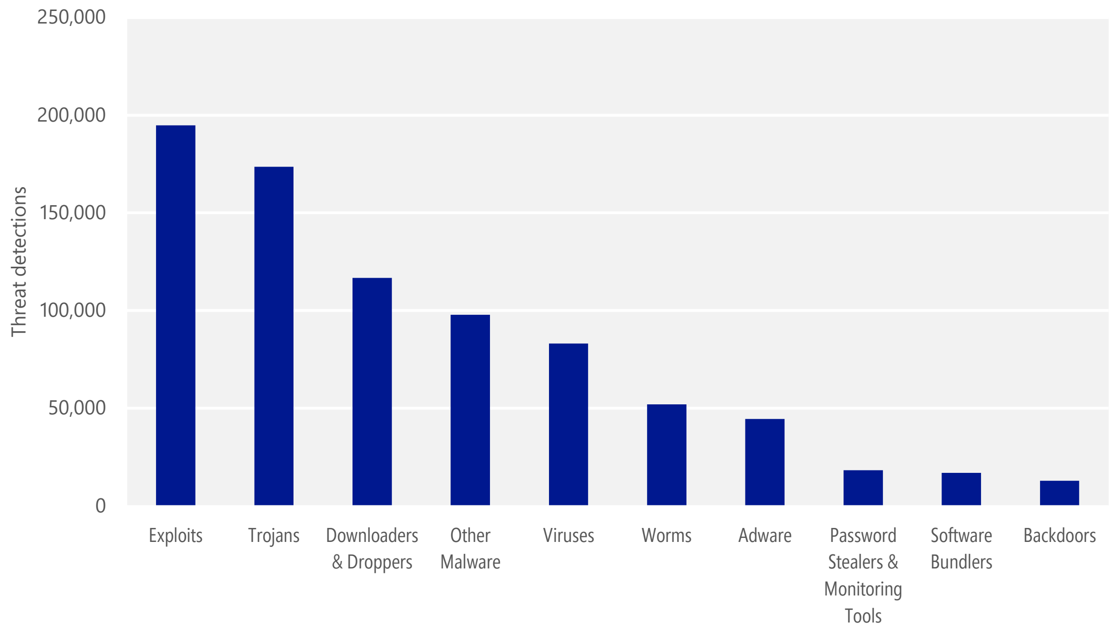
The average monthly compliance rate at Microsoft exceeded 99 percent during the second half of the year, despite a small drop in compliance toward the end of the year that was mostly related to internal testing of current and future versions of Windows. In any network of this size, it is almost inevitable that a small number of computers will be in a noncompliant state at any given time. In most cases, these are computers that are being rebuilt or are otherwise in a state of change when online, rather than computers that have had their antimalware software intentionally disabled.

Microsoft IT believes that a compliance rate in excess of 99 percent among approximately half a million computers is an acceptable level of compliance. In most cases, attempting to boost a large organization’s compliance rate the rest of the way to 100 percent will likely be a costly endeavor, and the end result—100 percent compliance—will be unsustainable over time.

Malware detections

Figure 66 shows the categories of malware and unwanted software that were most frequently detected at Microsoft in 2H14.

Figure 66. Top categories of malware and unwanted software detected by System Center Endpoint Protection at Microsoft in 2H14

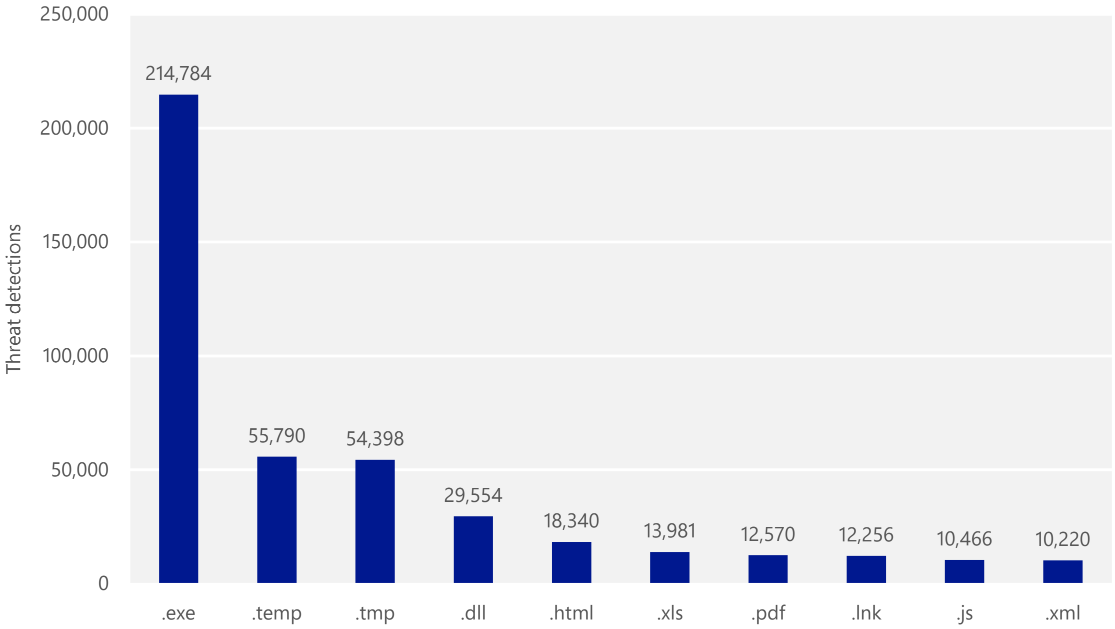


In this section, malware detections are defined as files and processes flagged by SCEP, regardless of the success or failure of automated containment or remediation. Malware detections are a measure of attempted malware activity, and do not necessarily indicate that a computer has been successfully infected. (Note that the methodology for assessing encounters used elsewhere in this report counts unique computers with detections, an approach that differs from the methodology used in this section, in which individual detections are counted. For example, if a computer encountered one malware family in August and another one in November, it would only be counted once for the purposes of figures such as Figure 34 on page 54. In the preceding Figure 66, it would be counted twice, once for each detection.)

Exploits was the most prevalent category. Trojans had the second-most number of detections, followed by Downloaders & Droppers and Other Malware.

Figure 67 shows the top 10 file types among threat detections at Microsoft in 2H14.

Figure 67. Threat detections at Microsoft in 2H14, by file type



Executable program files with the .exe extension were the most commonly detected type of malicious file at Microsoft, accounting for about half of all file detections. Files with the .temp and .tmp extensions, typically used for temporary files, were the next most common types of threats, followed by malicious .dll files. Malicious JavaScript files with the .js extension, which had been the second-most common type of threat in 1H14, fell to ninth in 2H14, being detected at less than a tenth of the volume at which they were detected from January to June. The decrease in malicious JavaScript detections is generally in line with the worldwide decrease in JavaScript-based exploit kit detections, as shown in Figure 12 on page 23.

Transmission vectors

Examining the processes targeted by malware can help illustrate the methods that attackers use to propagate it. Figure 68 lists the top five transmission vectors used by the malware encountered at Microsoft in 2H14.

Figure 68. The top five transmission vectors used by malware encountered at Microsoft in 2H14

Rank	Description
1	File transfers in the operating system
2	Web browsing
3	File transfer applications
4	Operating system tasks
5	Email

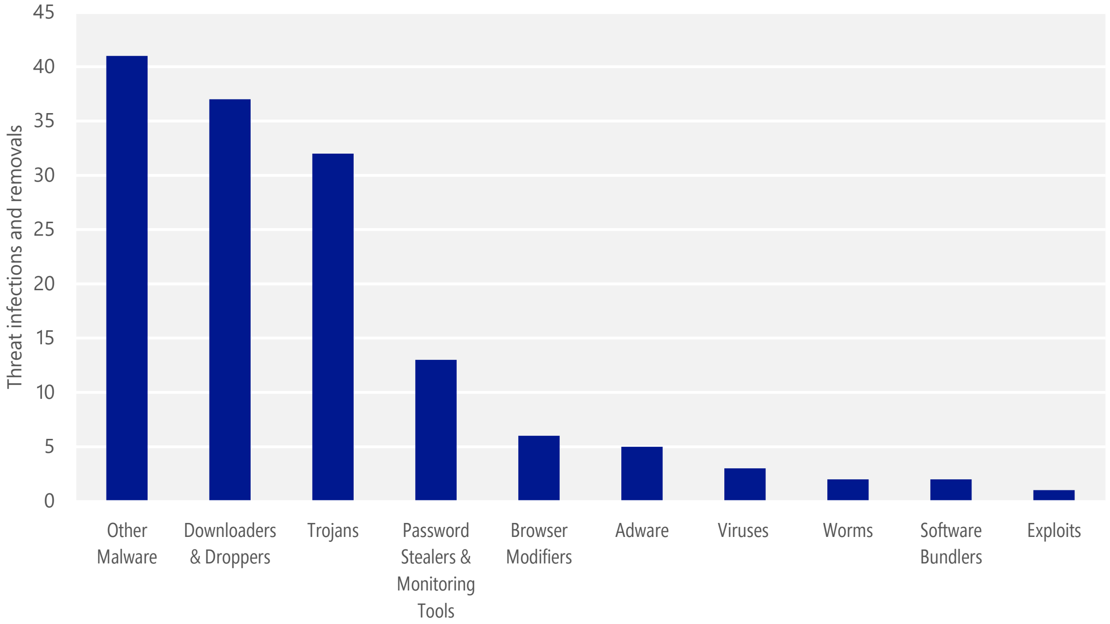
The transmission vector most commonly used by infection attempts detected on Microsoft computers in 2H14 involved file transfers made through Windows Explorer, followed by web browsing and file transfer applications, including peer-to-peer (P2P) applications. Scheduled operating system tasks and email were fourth and fifth.

Malware infections

Because almost all of the computers at Microsoft run real-time security software at all times, most infection attempts are detected and blocked before they are able to infect the target computer. When SCEP does disinfect a computer, it is usually because its signature database has been updated to enable it to detect a threat that it did not recognize when the computer first encountered the threat. This lack of recognition may be because the threat is a new malware family, a new variant of a known family, a known variant that has been encrypted or otherwise repackaged to avoid detection, or because of some other reason. The MMPC constantly analyzes malware samples submitted to it, develops appropriate detection signatures, and deploys them to customers who use SCEP, Microsoft Security Essentials, and Windows Defender.

Figure 69 shows the most commonly detected categories of malware and unwanted software that SCEP removed from computers at Microsoft between July and December of 2014.

Figure 69. Top categories of malware and unwanted software detected on computers at Microsoft in 2H14



As this chart shows, detection and infection statistics were significantly different in 2H14. Exploits, which were the most commonly detected category of malware at Microsoft between July and December, only accounted for a single infection and removal in the MSIT environment during the period. Most of the other categories also show clear differences between Figure 66 and Figure 69, although the ordering in the latter chart is significantly influenced by the low volumes involved.

Figure 70 shows the top 10 file types used by malware to infect computers at Microsoft in 2H14.

Figure 70. Infections and removals at Microsoft in 2H14, by file type

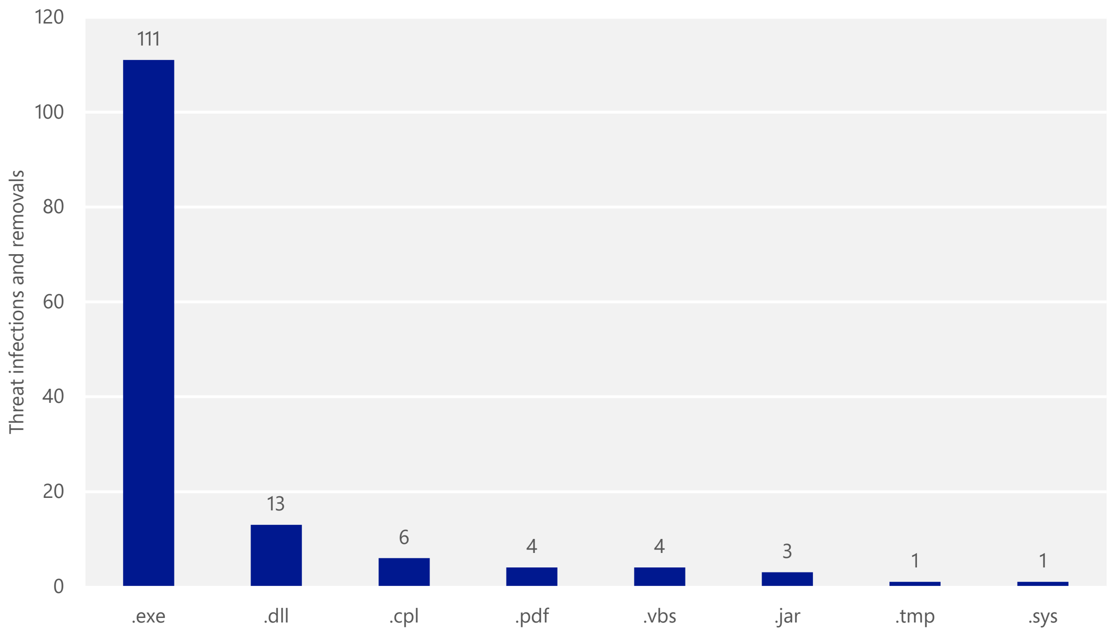


Figure 70 is important because it provides information about threats that SCEP did not detect when they were first encountered—and therefore provides a clue about the areas in which malware authors have been focusing their efforts in recent months. More than three-quarters of the malicious files removed from computers at Microsoft by SCEP in 2H14 had the extension .exe, used by executable program files, with seven extensions accounting for the remaining files. The .dll extension, which denotes dynamic-link library files, was a distant second, with other file types accounting for a handful of infections and removals each.

What IT departments can do to minimize these trends

- Evaluate commercially available management tools, develop a plan, and implement a third-party update mechanism to disseminate non-Microsoft updates.
- Ensure that all software deployed on computers in the environment is updated regularly. If the software provider offers an automatic update utility similar to Microsoft Update, ensure that it is enabled by default. See "Turn automatic updating on or off" at windows.microsoft.com for instructions on enabling automatic updates of Microsoft software.

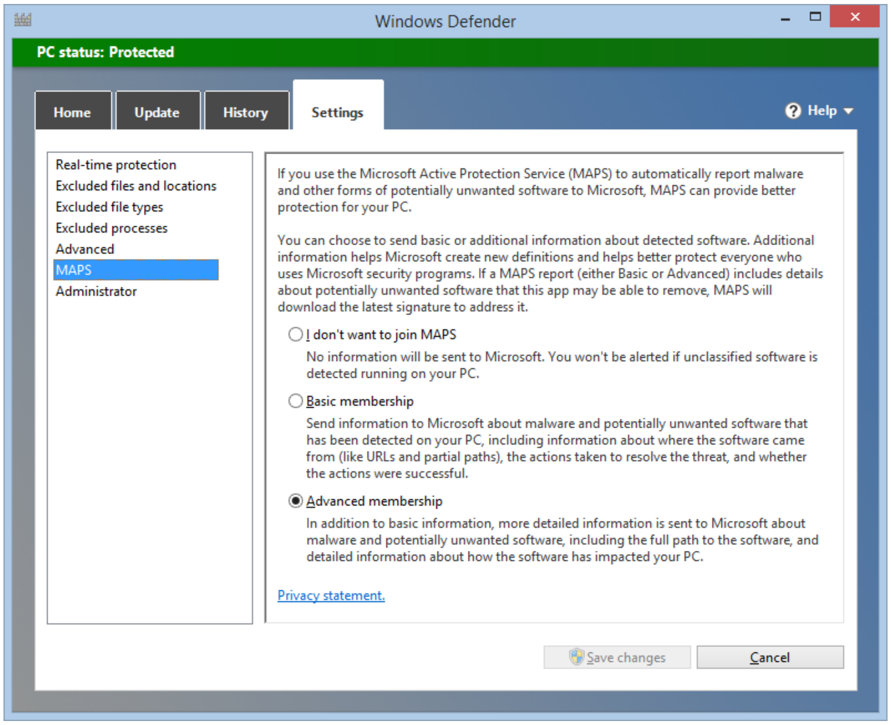
- Ensure that SmartScreen Filter is enabled in Internet Explorer. See "SmartScreen Filter: frequently asked questions" at windows.microsoft.com for more information.

- Use Group Policy to enforce configurations for Windows Update and SmartScreen Filter. See Knowledge Base article KB328010 at support.microsoft.com and "Manage Privacy: SmartScreen Filter and Resulting Internet Communication" at technet.microsoft.com for instructions.

- Set the default configuration for antimalware to enable real-time protection across all drives, including removable devices.

- Enable Microsoft Active Protection Service (MAPS) advanced membership in Windows Defender and Microsoft Security Essentials in your organization to protect your enterprise software security infrastructure in the cloud.

Figure 71. Enabling MAPS advanced membership in Windows Defender



If you use the Microsoft Active Protection Service (MAPS) to automatically report malware and other forms of potentially unwanted software to Microsoft, MAPS can provide better protection for your PC.

You can choose to send basic or additional information about detected software. Additional information helps Microsoft create new definitions and helps better protect everyone who uses Microsoft security programs. If a MAPS report (either Basic or Advanced) includes details about potentially unwanted software that this app may be able to remove, MAPS will download the latest signature to address it.

○ I don't want to join MAPS

No information will be sent to Microsoft. You won't be alerted if unclassified software is detected running on your PC.

○ Basic membership

Send information to Microsoft about malware and potentially unwanted software that has been detected on your PC, including information about where the software came from (like URLs and partial paths), the actions taken to resolve the threat, and whether the actions were successful.

● Advanced membership

In addition to basic information, more detailed information is sent to Microsoft about malware and potentially unwanted software, including the full path to the software, and detailed information about how the software has impacted your PC.

Privacy statement.

- Identify business dependencies on Java and develop a plan to minimize its use where it is not needed.

- Use AppLocker to block the installation and use of unwanted software such as Java or peer-to-peer (P2P) applications. See "AppLocker: Frequently Asked Questions" at technet.microsoft.com for more information.

- Implement the Enhanced Mitigation Experience Toolkit (EMET) to minimize exploitation of vulnerabilities in all software in your environment. See technet.microsoft.com/security/jj653751 for more information.
- Implement strong password policies, and require employees to change their passwords periodically.
- Strengthen authentication by using smart cards. See "Smart Cards" at technet.microsoft.com for more information.
- Use Network Access Protection (NAP) and DirectAccess (DA) to enforce compliance policies for firewall, antimalware, and patch management on remote systems that connect to a corporate network. See "Network Access Protection" at msdn.microsoft.com and "Windows 7 DirectAccess Explained" at technet.microsoft.com for more information.

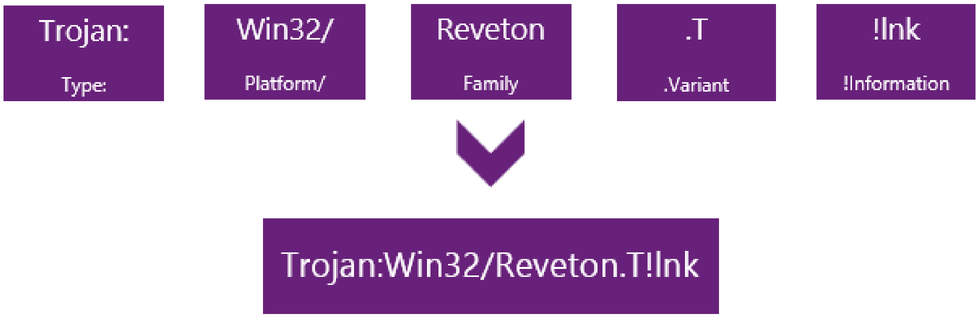
Appendixes

Appendix A: Threat naming conventions

Microsoft names the malware and unwanted software that it detects according to the Computer Antivirus Research Organization (CARO) Malware naming scheme.

This scheme uses the following format:

Figure 72. The Microsoft malware naming convention



When Microsoft analysts research a particular threat, they will determine what each of the components of the name will be.

Type

The type describes what the threat does on a computer. Worms, trojans, and viruses are some of the most common types of threats Microsoft detects.

Platform

The platform refers to the operating system (such as Windows, Mac OS X, and Android) that the threat is designed to work on. Platforms can also include programming languages and file formats.

Family

A group of threats with the same name is known as a family. Sometimes different security software companies use different names.

Variant letters

Variant letters are used sequentially for each different version or member of a family. For example, the detection for the variant ".AF" would have been created after the detection for the variant ".AE."

Additional information

Additional information is sometimes used to describe a specific file or component that is used by another threat in relation to the identified threat. In the preceding example, the !lnk indicates that the threat is a shortcut file used by the Trojan:Win32/Reveton.T variant, as shortcut files usually use the extension .lnk.

Appendix B: Data sources

Data included in the *Microsoft Security Intelligence Report* is gathered from a wide range of Microsoft products and services whose users have opted in to provide usage data. The scale and scope of this telemetry data allows the report to deliver the most comprehensive and detailed perspective on the threat landscape that is available in the software industry:

- Bing, the search and decision engine from Microsoft, contains technology that performs billions of webpage scans per year to seek out malicious content. After such content is detected, Bing displays warnings to users about it to help prevent infection.
- The Malicious Software Removal Tool (MSRT) is a free tool that Microsoft designed to help identify and remove specific prevalent malware families from customer computers. The MSRT is primarily released as an important update through Windows Update, Microsoft Update, and Automatic Updates. A version of the tool is also available from the Microsoft Download Center. The MSRT was downloaded and executed more than 600 million times each month on average in 2H14. The MSRT is not a replacement for an up-to-date real-time antivirus solution.
- The Microsoft Safety Scanner is a free downloadable security tool that provides on-demand scanning and helps remove malware and other malicious software. The Microsoft Safety Scanner is not a replacement for an up-to-date antivirus solution, because it does not offer real-time protection and cannot prevent a computer from becoming infected.
- Microsoft Security Essentials is a free, easy-to-download real-time protection product that provides basic, effective antivirus and antispyware protection.
- Microsoft System Center Endpoint Protection (formerly Forefront Client Security and Forefront Endpoint Protection) is a unified product that provides protection from malware and unwanted software for enterprise desktops, laptops, and server operating systems. It uses the Microsoft Malware Protection Engine and the Microsoft antivirus signature database to provide real-time, scheduled, and on-demand protection.

- Windows Defender in Windows 8 and Windows 8.1 provides real-time scanning and removal of malware and unwanted software.
- Windows Defender Offline is a downloadable tool that can be used to create a bootable CD, DVD, or USB flash drive to scan a computer for malware and other threats. It does not offer real-time protection and is not a substitute for an up-to-date antimalware solution.

Figure 73. US privacy statements for the Microsoft products and services used in this report

Product or service	Privacy statement URL
Bing	www.microsoft.com/privacystatement/en-us/bingandmsn/default.aspx
Malicious Software Removal Tool	www.microsoft.com/security/pc-security/msrt-privacy.aspx
Microsoft Security Essentials	windows.microsoft.com/en-us/windows/security-essentials-privacy
Microsoft Safety Scanner	www.microsoft.com/security/scanner/en-us/privacy.aspx
System Center Endpoint Protection	https://www.microsoft.com/privacystatement/en-us/SystemCenter2012R2/Default.aspx#tilepspSystemCenter2012R2EndpointProtectionModule
Windows Defender in Windows 8.1	windows.microsoft.com/en-us/windows-8/windows-8-1-privacy-statement#T1=supplement&section_43
Windows Defender Offline	windows.microsoft.com/en-us/windows/windows-defender-offline-privacy

Appendix C: Worldwide infection rates

"Malware and unwanted software worldwide," on page 40, explains how threat patterns differ significantly in different parts of the world. Figure 74 shows the infection and encounter rates for 1Q14 and 2Q14 for locations around the world.[20] See page 38 for information about how infection and encounter rates are calculated.

Figure 74. Encounter and infection rates for locations around the world, 3Q14–4Q14, by quarter (100,000 computers reporting minimum)

Country/region	Encounter rate 3Q14	Encounter rate 4Q14	CCM 3Q14	CCM 4Q14
Worldwide	*20.1%*	*15.9%*	*8.6*	*5.9*
Albania	30.3%	26.5%	39.7	33.0
Algeria	44.4%	43.0%	60.5	55.7
Angola	—	—	57.6	44.8
Argentina	27.7%	20.2%	16.2	9.7
Armenia	32.5%	32.1%	18.1	12.5
Australia	14.1%	10.1%	4.6	2.5
Austria	10.6%	9.5%	3.1	1.9
Azerbaijan	—	29.5%	35.5	31.0
Bahamas, The	—	—	14.3	10.5
Bahrain	—	—	23.2	20.7
Bangladesh	—	—	37.1	32.1
Barbados	—	—	6.6	4.6
Belarus	32.1%	30.6%	9.7	9.0
Belgium	16.1%	12.0%	4.8	2.6
Bolivia	—	—	26.4	21.8
Bosnia and Herzegovina	26.2%	25.6%	20.3	19.4

[20] Encounter rate and CCM are shown for locations with at least 100,000 computers running Microsoft real-time security products and the Malicious Software Removal Tool, respectively, during a quarter. Only computers whose users have opted in to provide data to Microsoft are considered when calculating encounter and infection rates.

Country/region	Encounter rate 3Q14	Encounter rate 4Q14	CCM 3Q14	CCM 4Q14
Brazil	32.9%	21.7%	18.4	11.2
Bulgaria	26.0%	23.1%	10.8	8.5
Cambodia	—	—	25.3	21.0
Canada	18.1%	12.6%	4.6	2.4
Chile	23.4%	18.8%	13.1	8.9
China	18.1%	15.3%	3.9	4.0
Colombia	29.9%	21.4%	18.9	10.8
Costa Rica	19.0%	15.2%	10.3	6.2
Côte d'Ivoire	—	—	26.9	20.5
Croatia	18.2%	20.4%	7.1	6.7
Cyprus	18.8%	17.9%	11.3	7.4
Czech Republic	16.1%	14.5%	4.3	3.5
Denmark	9.8%	7.8%	2.0	1.0
Dominican Republic	31.0%	25.9%	32.8	27.1
Ecuador	29.0%	23.5%	21.6	13.3
Egypt	37.2%	36.2%	57.6	51.8
El Salvador	—	20.9%	13.5	9.8
Estonia	13.6%	13.4%	3.4	2.0
Finland	6.3%	5.0%	1.6	0.7
France	22.8%	13.0%	6.8	3.2
Georgia	36.9%	30.2%	37.7	31.3
Germany	14.5%	9.3%	3.1	1.8
Ghana	—	—	33.1	23.4
Greece	18.6%	17.0%	9.5	5.5
Guadeloupe	—	—	11.1	6.0
Guatemala	24.3%	17.8%	13.5	9.8
Honduras	—	—	17.8	14.3
Hong Kong SAR	11.2%	10.0%	3.6	2.8
Hungary	17.8%	15.5%	7.3	5.1
Iceland	8.5%	7.5%	3.6	1.5
India	38.2%	32.1%	33.3	25.7
Indonesia	47.7%	45.1%	36.2	32.8

Country/region	Encounter rate 3Q14	Encounter rate 4Q14	CCM 3Q14	CCM 4Q14
Iraq	35.7%	35.6%	88.5	81.3
Ireland	12.8%	9.3%	3.7	2.3
Israel	16.9%	16.3%	11.5	8.6
Italy	25.0%	16.5%	7.8	4.3
Jamaica	—	20.4%	15.8	12.1
Japan	5.1%	4.0%	1.5	0.8
Jordan	31.9%	31.9%	42.4	40.4
Kazakhstan	35.6%	34.2%	21.8	21.0
Kenya	—	26.7%	24.4	19.9
Korea	17.5%	14.5%	24.2	12.9
Kuwait	24.9%	24.4%	19.1	17.7
Latvia	19.3%	19.0%	4.5	3.3
Lebanon	28.9%	27.2%	33.3	31.7
Libya	—	—	60.3	61.2
Lithuania	19.6%	18.4%	8.5	5.7
Luxembourg	—	—	3.7	2.3
Macao SAR	—	—	5.1	4.9
Macedonia, FYRO	27.2%	26.6%	22.0	21.0
Malaysia	27.2%	24.1%	22.2	18.4
Malta	—	—	7.9	4.4
Martinique	—	—	7.7	3.6
Mauritius	—	—	22.5	15.2
Mexico	30.0%	21.9%	21.1	15.1
Moldova	28.0%	27.8%	13.3	11.4
Mongolia	—	—	—	66.3
Morocco	33.0%	29.0%	60.2	56.5
Mozambique	—	—	—	22.8
Nepal	—	—	47.1	40.5
Netherlands	13.8%	10.1%	3.4	1.9
New Zealand	10.8%	9.4%	4.2	2.8
Nicaragua	—	—	12.5	7.5
Nigeria	33.6%	29.1%	30.9	27.2

Country/region	Encounter rate 3Q14	Encounter rate 4Q14	CCM 3Q14	CCM 4Q14
Norway	9.0%	6.8%	2.2	1.1
Oman	—	—	28.8	29.2
Pakistan	48.7%	45.1%	62.6	57.4
Palestinian Authority	—	—	63.3	63.5
Panama	26.7%	19.5%	20.1	12.7
Paraguay	—	—	14.9	12.7
Peru	32.3%	27.4%	24.8	17.1
Philippines	36.8%	32.9%	38.0	30.8
Poland	16.8%	13.8%	11.3	6.8
Portugal	19.7%	18.6%	9.4	4.3
Puerto Rico	17.7%	14.0%	10.6	8.4
Qatar	25.9%	23.7%	17.0	13.7
Réunion	—	10.3%	9.5	4.4
Romania	23.5%	20.8%	20.2	16.6
Russia	27.3%	24.2%	6.6	5.0
Saudi Arabia	31.6%	29.7%	31.3	29.3
Senegal	—	33.2%	34.1	23.1
Serbia	25.5%	23.1%	16.2	15.3
Singapore	11.8%	11.1%	5.5	4.0
Slovakia	16.7%	14.1%	5.9	4.9
Slovenia	14.6%	14.9%	5.1	3.3
South Africa	21.5%	17.8%	13.7	10.7
Spain	20.8%	16.9%	9.7	5.3
Sri Lanka	32.8%	28.9%	21.2	17.8
Sweden	9.9%	7.6%	2.8	1.5
Switzerland	11.0%	8.8%	2.7	1.5
Taiwan	14.6%	12.7%	7.2	5.7
Tanzania	—	—	27.5	24.2
Thailand	29.8%	25.9%	26.8	22.9
Trinidad and Tobago	—	18.4%	16.2	11.0
Tunisia	35.7%	34.1%	44.5	39.7
Turkey	35.1%	28.0%	40.7	24.9

Country/region	Encounter rate 3Q14	Encounter rate 4Q14	CCM 3Q14	CCM 4Q14
Ukraine	32.2%	31.2%	9.7	9.0
United Arab Emirates	26.4%	24.7%	20.4	16.0
United Kingdom	17.2%	11.5%	5.5	2.6
United States	15.4%	11.5%	8.0	3.8
Uruguay	20.1%	17.2%	9.1	5.4
Venezuela	36.6%	28.5%	33.4	20.8
Vietnam	45.1%	38.0%	39.9	35.7
Zimbabwe	—	—	—	17.0
Worldwide	*20.1%*	*15.9%*	*8.6*	*5.9*

Glossary

For additional information about these and other terms, visit the MMPC glossary at www.microsoft.com/security/portal/Threat/Encyclopedia/Glossary.aspx.

account credentials
Information presented to a service provider to verify that the holder of the credentials is authorized to access an account. Account credentials typically take the form of user names paired with passwords, but other forms of identification are possible.

ActiveX control
A software component of Microsoft Windows that can be used to create and distribute small applications through Internet Explorer. ActiveX controls can be developed and used by software to perform functions that would otherwise not be available using typical Internet Explorer capabilities. Because ActiveX controls can be used to perform a wide variety of functions, including downloading and running programs, vulnerabilities discovered in them may be exploited by malware. In addition, cybercriminals may also develop their own ActiveX controls, which can do damage to a computer if a user visits a webpage that contains the malicious ActiveX control.

adware
A program that displays advertisements. Although some adware can be beneficial by subsidizing a program or service, other adware programs may display advertisements without adequate consent.

backdoor trojan
A type of trojan that provides attackers with remote unauthorized access to and control of infected computers. Bots are a subcategory of backdoor trojans. Also see *botnet*.

Bitcoin mining
The use of computing resources to create new bitcoins, a type of digital currency. Bitcoin mining software needs a lot of computer processing power and may slow down the computer that's running it.

botnet
A set of computers controlled by a “command-and-control” (C&C) computer to execute commands as directed. The C&C computer can issue commands

directly (often through Internet Relay Chat [IRC]) or by using a decentralized mechanism, such as peer-to-peer (P2P) networking. Computers in a botnet are often called bots, nodes, or zombies.

browser modifier
A program that changes browser settings, such as the home page, without adequate consent. This also includes browser hijackers.

buffer overflow
An error in an application in which the data written into a buffer exceeds the current capacity of that buffer, thus overwriting adjacent memory. Because memory is overwritten, unreliable program behavior may result and, in certain cases, allow arbitrary code to run.

C&C
Short for *command and control*. See *botnet*.

CCM
Short for *computers cleaned per mille* (thousand). The number of computers cleaned for every 1,000 executions of the Microsoft Malicious Software Removal Tool (MSRT). For example, if the MSRT has 50,000 executions in a particular location in the first quarter of the year and removes infections from 200 computers, the CCM for that location in the first quarter of the year is 4.0 (200 ÷ 50,000 × 1,000). Also see *encounter rate*.

clean
To remove malware or potentially unwanted software from an infected computer. A single cleaning can involve multiple disinfections.

command and control
See *botnet*.

credentials
See *account credentials*.

detection
The discovery of malware or potentially unwanted software on a computer by antimalware software. Disinfections and blocked infection attempts are both considered detections.

detection signature
A set of characteristics that can identify a malware family or variant. Signatures are used by antimalware products to determine whether a file is malicious or not. Also see *definition*.

disclosure
Revelation of the existence of a vulnerability to a third party.

disinfect
To remove a malware or potentially unwanted software component from a computer or to restore functionality to an infected program. Compare with clean.

downloader
See *downloader/dropper*.

downloader/dropper
A form of trojan that installs other malicious files to a computer that it has infected, either by downloading them from a remote computer or by obtaining them directly from a copy contained in its own code.

encounter
An instance of security software detecting a threat and blocking, quarantining, or removing it from the computer.

encounter rate
The percentage of computers running Microsoft real-time security software that report detecting malware or potentially unwanted software, or report detecting a specific threat or family, during a period. Also see *infection rate*.

exploit
Malicious code that takes advantage of software vulnerabilities to infect a computer or perform other harmful actions.

exploit kit
A collection of exploits bundled together and sold as commercial software. A typical kit contains a collection of web pages that contain exploits for vulnerabilities in popular web browsers and add-ons, along with tools for managing and updating the kit

firewall
A program or device that monitors and regulates traffic between two points, such as a single computer and the network server, or one server to another.

generic
A type of signature that is capable of detecting a variety of malware samples from a specific family, or of a specific type.

IFrame
Short for *inline frame*. An IFrame is an HTML document that is embedded in another HTML document. Because the IFrame loads another webpage, it can be used by criminals to place malicious HTML content, such as a script that downloads and installs spyware, into non-malicious HTML pages that are hosted by trusted websites.

in the wild
Said of malware that is currently detected on active computers connected to the Internet, as compared to those confined to internal test networks, malware research laboratories, or malware sample lists.

infection
The presence of malware on a computer, or the act of delivering or installing malware on a computer. Also see *encounter*.

infection rate
See *CCM*.

jailbreaking
See *rooting*.

Litecoin
See *Bitcoin mining*.

malware
Short for *malicious software*. The general name for programs that perform unwanted actions on a computer, such as stealing personal information. Some malware can steal banking details, lock a computer until the user pays a ransom, or use the computer to send spam. Viruses, worms and trojans are all types of malware.

man-in-the-middle attack
A form of eavesdropping in which a malicious hacker gets in the middle of network communications. The malicious hacker can then manipulate messages or gather information without the people doing the communication knowing.

monitoring tool
Software that monitors activity, usually by capturing keystrokes or screen images. It may also include network sniffing software. Also see *password stealer (PWS)*.

P2P
See *peer-to-peer (P2P)*.

password stealer (PWS)
Malware that is specifically used to transmit personal information, such as user names and passwords. A PWS often works in conjunction with a keylogger. Also see *monitoring tool*.

payload
The actions conducted by a piece of malware for which it was created. Payloads can include, but are not limited to, downloading files, changing system settings, displaying messages, and logging keystrokes.

peer-to-peer (P2P)
A system of network communication in which individual nodes are able to communicate with each other without the use of a central server.

ransomware
A type of malware that prevents use of a computer or access to the data that it contains until the user pays a certain amount to a remote attacker (the "ransom"). Computers that have ransomware installed usually display a screen containing information on how to pay the "ransom." A user cannot usually access anything on the computer beyond the screen.

return-oriented programming (ROP)
An exploit technique that involves gaining control of a program's control flow and calling a chain of instructions that already exist in memory, each of which ends in a return command.

rogue security software
Software that appears to be beneficial from a security perspective but that provides limited or no security capabilities, generates a significant number of erroneous or misleading alerts, or attempts to socially engineer the user into participating in a fraudulent transaction.

rooting
Obtaining administrative user rights on a mobile device through the use of exploits. Device owners sometimes use such exploits intentionally to gain access to additional functionality, but these exploits can also be used by attackers to infect devices with malware that bypasses many typical security systems. The term "rooting" is typically used in the context of Android devices; the comparable process on iOS devices is more commonly referred to as jailbreaking.

ROP
See *return-oriented programming (ROP)*.

sandbox
A specially constructed portion of a computing environment in which potentially dangerous programs or processes may run without causing harm to resources outside the sandbox.

Short Message Service (SMS)
The standardized text messaging service implemented by most mobile phone operators.

signature
See *detection signature*.

sinkhole
A server or set of servers designed to absorb and analyze malware traffic.

SMS
See *Short Message Service (SMS)*.

social engineering
A technique that defeats security precautions by exploiting human vulnerabilities. Social engineering scams can be both online (such as receiving email messages that ask the recipient to click the attachment, which is actually malware) and offline (such as receiving a phone call from someone posing as a representative from one's credit card company). Regardless of the method selected, the purpose of a social engineering attack remains the same—to get the targeted user to perform an action of the attacker's choice.

software bundler
A program that installs unwanted software on your PC at the same time as the software you are trying to install, without adequate consent.

spam
Bulk unsolicited email. Malware authors may use spam to distribute malware, either by attaching the malware to email messages or by sending a message containing a link to the malware. Malware may also harvest email addresses for spamming from compromised machines or may use compromised machines to send spam.

targeted attack
A malware attack against a specific group of companies or individuals. This type of attack usually aims to get access to the PC or network, before trying to steal information or disrupt the infected machines.

tool
In the context of malware, a software program that may have legitimate purposes but may also be used by malware authors or attackers.

Tor
An open source project that provides users with a way to access Internet resources anonymously by relaying traffic through the computers of other Tor users.

trojan
A generally self-contained program that does not self-replicate but takes malicious action on the computer.

unwanted software
A program with potentially unwanted functionality that is brought to the user's attention for review. This functionality may affect the user's privacy, security, or computing experience.

virus
Malware that replicates, typically by infecting other files in the computer, to allow the execution of the malware code and its propagation when those files are activated.

vulnerability
A weakness, error, or poor coding technique in a program that may allow an attacker to exploit it for a malicious purpose.

watering hole attack
A type of targeted attack that involves planting malware at websites visited by people in specific industries or with specific interests.

weaponized
Said of an exploit that is capable of being used by an attacker in the wild.

wild
See *in the wild*.

worm
Malware that spreads by spontaneously sending copies of itself through email or by using other communication mechanisms, such as instant messaging (IM) or peer-to-peer (P2P) applications.

Threat families referenced in this report

The definitions for the threat families referenced in this report are adapted from the Microsoft Malware Protection Center encyclopedia (www.microsoft.com/security/portal), which contains detailed information about a large number of malware and unwanted software families. See the encyclopedia for more in-depth information and guidance for the families listed here and throughout the report.

Win32/Adpeak. Adware that displays extra ads as the user browses the Internet, without revealing where the ads are coming from. It may be bundled with some third-party software installation programs.

Win32/Anogre. A threat that exploits a vulnerability addressed by Microsoft Security Bulletin MS11-087. This vulnerability can allow a hacker to install programs, view, change, or delete data or create new accounts with full administrative privileges.

Win32/Archost. A downloader that installs other programs on the computer without the user's consent, including other malware.

INF/Autorun. 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.

JS/Axpergle. A detection for the Angler exploit kit, which exploits vulnerabilities in recent versions of Internet Explorer, Silverlight, Adobe Flash Player, and Java to install malware.

MSIL/Balamid. A trojan that can use the computer to click on online advertisements without the user's permission or knowledge. This can earn money for a malicious hacker by making a website or application appear more popular than it is.

Win32/Banload. A family of trojans that download other malware. Banload usually downloads Win32/Banker, which steals banking credentials and other sensitive data and sends it back to a remote attacker.

Win32/BeeVry. A trojan that modifies a number of settings to prevent the computer from accessing security-related websites, and lower the computer's security.

Win32/BetterSurf. Adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.

Win32/Bifrose. A backdoor trojan that allows a remote attacker to access the compromised computer, and injects its processes into the Windows shell and Internet Explorer.

JS/Blacole. An exploit pack, also known as Blackhole, that is installed on a compromised web server by an attacker and includes a number of exploits that target browser software. If a vulnerable computer browses a compromised website that contains the exploit pack, various malware may be downloaded and run.

MSIL/Bladabindi. 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.

JS/Bondat. A family of threats that collects information about the computer, infects removable drives, and tries to stop the user from accessing files. It spreads by infecting removable drives, such as USB thumb drives and flash drives.

Win32/Brantall. A family of trojans that download and install other programs, including Win32/Sefnit and Win32/Rotbrow. Brantall often pretends to be an installer for other, legitimate programs.

Win64/Bregent. A downloader that injects malicious code into legitimate processes such as explorer.exe and svchost.exe, and downloads other malware onto the computer.

JS/Brolo. A ransomware family that locks the web browser and displays a message, often pretending to be from a law enforcement agency, demanding money to unlock the browser.

Win32/Chir. A family with a worm component and a virus component. The worm component spreads by email and by exploiting a vulnerability addressed by Microsoft Security Bulletin MS01-020. The virus component may infect .exe, .scr, and HTML files.

Win32/Comame. A generic detection for a variety of threats.

Win32/CostMin. An adware family that installs itself as a browser extension for Internet Explorer, Mozilla Firefox, and Google Chrome, and displays advertisements as the user browses the Internet.

Win32/CouponRuc. A browser modifier that changes browser settings and may also modify some computer and Internet settings.

Win32/CplLnk. A generic detection for specially-crafted malicious shortcut files that attempt to exploit the vulnerability addressed by Microsoft Security Bulletin MS10-046.

Win32/Crastic. A trojan that sends sensitive information to a remote attacker, such as user names, passwords and information about the computer. It can also delete System Restore points, making it harder to recover the computer to a pre-infected state.

Win32/Crilock. A ransomware family that encrypts the computer's files and displays a webpage that demands a fee to unlock them.

Win32/Crowti. A ransomware family that encrypts files on the computer and demands that the user pay a fee to decrypt them, using Bitcoins.

Java/CVE-2013-1488. A detection for threats that use a Java vulnerability to download and run files on your PC, including other malware. Oracle addressed the vulnerability with a security update in April 2013.

Win32/DefaultTab. A browser modifier that redirects web browser searches and prevents the user from changing browser settings.

JS/DonxRef. A generic detection for malicious JavaScript objects that construct shellcode. The scripts may try to exploit vulnerabilities in Java, Adobe Flash Player, and Windows.

Win32/Dynamer. A generic detection for a variety of threats.

JS/Faceliker. A malicious script that “likes” content on Facebook without the user's knowledge or consent.

Win32/FakePAV. A rogue security software family that often masquerades as Microsoft Security Essentials or other legitimate antimalware products.

Win32/FakeRean. A rogue security software family distributed under a variety of randomly generated names, including Privacy Protection, Security Protection, Antivirus Protection 2012, XP Security Protection 2012, and many others.

HTML/Fashack. A detection for the Safehack exploit kit, also known as Flashpack. It uses vulnerabilities in Adobe Flash Player, Java, and Silverlight to install malware on the computer.

JS/Fiexp. A detection for the Fiesta exploit kit, which attempts to exploit Java, Adobe Flash Player, Adobe Reader, Silverlight, and Internet Explorer to install malware.

Win32/Gamarue. A worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.

HTML/IframeRef. A generic detection for specially formed IFrame tags that point to remote websites that contain malicious content.

Win32/Ippedo. A worm that can send sensitive information to a malicious hacker. It spreads through infected removable drives, such as USB flash drives.

VBS/Jenxcus. 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.

JS/Kilim. A trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.

JS/Krypterade. Ransomware that fraudulently claims the computer has been used for unlawful activity, locks it, and demands that the user pay to unlock it.

Win32/Lecpetex. A family of trojans that steal sensitive information, such as user names and passwords. It can also use the computer for Litecoin mining, install other malware, and post malicious content via the user's Facebook account.

Unix/Lotoor. A detection for specially crafted Android programs that attempt to exploit vulnerabilities in the Android operating system to gain root privilege.

HTML/Meadgive. A detection for the Redkit exploit kit, also known as Infinity and Goon. It attempts to exploit vulnerabilities in programs such as Java and Silverlight to install other malware.

MSIL/Mofin. A worm that can steal files from your PC and send them to a malicious hacker. It spreads via infected removable drives, such as USB flash drives.

Win32/MpTamperSrp. A generic detection for an attempt to add software restriction policies to restrict Microsoft antimalware products, such as Microsoft Security Essentials and Windows Defender, from functioning properly.

Win32/Mujormel. A password stealer that can steal personal information, such as user names and passwords, and send the stolen information to a malicious hacker.

JS/Neclu. A detection for the Nuclear exploit kit, which attempts to exploit vulnerabilities in programs such as Java and Adobe Reader to install other malware.

Win32/Nitol. A family of trojans that perform DDoS (distributed denial of service) attacks, allow backdoor access and control, download and run files, and perform a number of other malicious activities on the computer.

Win32/Obfuscator. A generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.

Win32/Ogimant. A threat that claims to help download items from the Internet, but actually downloads and runs files that are specified by a remote attacker.

Win32/Pdfjsc. A family of specially crafted PDF files that exploit Adobe Acrobat and Adobe Reader vulnerabilities. Such files contain malicious JavaScript that executes when the file is opened.

Win32/PennyBee. Adware that shows ads as the user browses the web. It can be installed from the program's website or bundled with some third-party software installation programs.

Win32/Phdet. A family of backdoor trojans that is used to perform distributed denial-of service (DDoS) attacks against specified targets.

JS/Proslikefan. A worm that spreads through removable drives, network shares, and P2P programs. It can lower the computer's security settings and disable antivirus products.

Win32/Ramnit. A family of multi-component malware that infects executable files, Microsoft Office files, and HTML files. Win32/Ramnit spreads to removable drives and steals sensitive information such as saved FTP credentials and browser cookies. It may also open a backdoor to await instructions from a remote attacker.

Win32/Reveton. A ransomware family that targets users from certain countries or regions. It locks the computer and displays a location-specific webpage that covers the desktop and demands that the user pay a fine for the supposed possession of illicit material.

Win32/Rimod. A generic detection for files that change various security settings in the computer

Win32/Rotbrow. A trojan that installs browser add-ons that claim to offer protection from other add-ons. Rotbrow can change the browser's home page, and can install the trojan Win32/Sefnit. It is commonly installed by Win32/Brantall.

Win32/Sality. 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.

Win32/Sefnit. A family of trojans that can allow backdoor access, download files, and use the computer and Internet connection for click fraud. Some variants can monitor web browsers and hijack search results.

JS/ShellCode. A generic detection for script objects that contain malicious shell code and may exhibit suspicious behavior. Malicious websites and malformed PDF documents may contain JavaScript that attempts to execute code without the affected user's consent.

DOS/Sigru. A virus that can stop some files from working correctly in Windows XP and earlier operating systems. It spreads by infecting the master boot record (MBR) on connected hard disks and floppy disks.

PHP/SimpleShell. A backdoor that can give a malicious hacker unauthorized access to and control of the computer.

Win32/Slugin. A file infector that infects .exe and .dll files. It may also perform backdoor actions.

Win32/Small. A generic detection for a variety of threats.

Win32/Softpulse. A software bundler that no longer meets Microsoft detection criteria for unwanted software following a program update in September of 2014.

MSIL/Spacekito. A threat that steals information about the computer and installs browser add-ons that display ads.

Win32/SquareNet. A software bundler that installs other unwanted software, including adware and click-fraud malware.

Win32/Tugspay. A downloader that spreads by posing as an installer for legitimate software, such as a Java update, or through other malware. When installed, it downloads unwanted software to the computer.

Win32/Tupym. A worm that copies itself to the system folder of the affected computer, and attempts to contact remote hosts.

Win32/Urausy. A family of ransomware trojans that lock the computer and display a localized message, supposedly from police authorities, demanding the payment of a fine for supposed criminal activity.

Win32/Vercuser. A worm that typically spreads via drive-by download. It also receives commands from a remote server, and has been observed dropping other malware on the infected computer.

Win32/Virut. A family of file-infecting viruses that target and infect .exe and .scr files accessed on infected systems. Win32/Virut also opens a backdoor by connecting to an IRC server.

Win32/Wecykler. 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.

Win32/Wordinvop. A detection for a specially-crafted Microsoft Word file that attempts to exploit the vulnerability CVE-2006-6456, addressed by Microsoft Security Bulletin MS07-014.

Win32/Wysotot. A threat that can change the start page of the user's web browser, and may download and install other files to the computer. It is installed by software bundlers that advertise free software or games.

Win32/Yeltminky. A family of worms that spreads by making copies of itself on all available drives and creating an autorun.inf file to execute that copy.

Index

Microsoft

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