Microsoft

Microsoft Security Intelligence Report

Volume 16 | July through December, 2013

Worldwide Threat Assessment

Authors

Dennis Batchelder
Microsoft Malware Protection Center

Joe Blackbird
Microsoft Malware Protection Center

David Felstead
Bing

Paul Henry
Wadeware LLC

Jeff Jones
Microsoft Trustworthy Computing

Aneesh Kulkarni
Windows Services Safety Platform

John Lambert
Microsoft Trustworthy Computing

Marc Lauricella
Microsoft Trustworthy Computing

Ken Malcolmson
Microsoft Trustworthy Computing

Matt Miller
Microsoft Trustworthy Computing

Nam Ng
Microsoft Trustworthy Computing

Daryl Pecelj
Microsoft IT Information Security and Risk Management

Tim Rains
Microsoft Trustworthy Computing

Vidya Sekhar
Microsoft Malware Protection Center

Holly Stewart
Microsoft Malware Protection Center

Todd Thompson
Microsoft IT Information Security and Risk Management

David Weston
Microsoft Operating Systems Group

Terry Zink
Exchange Online Protection

Contributors

Hyun Choi
Joe Faulhaber
Tanmay Ganacharya
Ben Hope
Aaron Hulett
Hong Jia
Marianne Mallen
Geoff McDonald
Scott Molenkamp
Dolcita Montemayor
Hamish O'Dea
Bill Pfeifer
Dmitriy Pletnev
Hilda Larina Ragragio
Shawn Wang
Iaan Wiltshire
Dan Wolff
Microsoft Malware Protection Center

Joe Gura
Microsoft Trustworthy Computing

Chris Hale
Microsoft Trustworthy Computing

Satomi Hayakawa
CSS Japan Security Response Team

Yurika Kakiuchi
CSS Japan Security Response Team

Jimmy Kuo
Wadeware LLC

Greg Lenti
Microsoft Trustworthy Computing

Chad Mills
Windows Services Safety Platform

Daric Morton
Microsoft Services

Takumi Onodera
Microsoft Premier Field Engineering, Japan

Anthony Penta
Windows Services Safety Platform

Cynthia Sandvick
Microsoft Trustworthy Computing

Richard Saunders
Microsoft Trustworthy Computing

Frank Simorjay
Microsoft Trustworthy Computing

Norie Tamura
CSS Japan Security Response Team

Henk van Roest
CSS Security EMEA

Steve Wacker
Wadeware LLC

Table of contents

About this report v

Trustworthy Computing: Security engineering at Microsoft vi

Worldwide threat assessment 17

Vulnerabilities 19

Industry-wide vulnerability disclosures 19

Vulnerability severity 20

Vulnerability complexity 22

Operating system, browser, and application vulnerabilities 23

Microsoft vulnerability disclosures 25

Guidance: Developing secure software 26

Exploits 27

Exploit families 29

HTML and JavaScript exploits 31

Java exploits 32

Operating system exploits 33

Document exploits 36

Adobe Flash Player exploits 38

Enhanced Mitigation Experience Toolkit (EMET) effectiveness 38

Malware 41

A trio of threats makes waves in 4Q13 42

Malware prevalence worldwide 46

Infection rates by operating system 56

Threat categories 58

Threat families 61

Rogue security software 65

Ransomware 67

Home and enterprise threats 71

Guidance: Defending against malware 75

Email threats 76

Spam messages blocked 76

Spam types 78
Guidance: Defending against threats in email 81
Malicious websites 82
Phishing sites 83
Malware hosting sites 92
Drive-by download sites 98
Guidance: Protecting users from unsafe websites 100

About this report

The *Microsoft Security Intelligence Report (SIR)* focuses on software vulnerabilities, software vulnerability exploits, and malicious 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 2013, 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, 1H13 represents the first half of 2013 (January 1 through June 30), and 4Q12 represents the fourth quarter of 2012 (October 1 through December 31). To avoid confusion, please note the reporting period or periods being referenced when considering the statistics in this report.

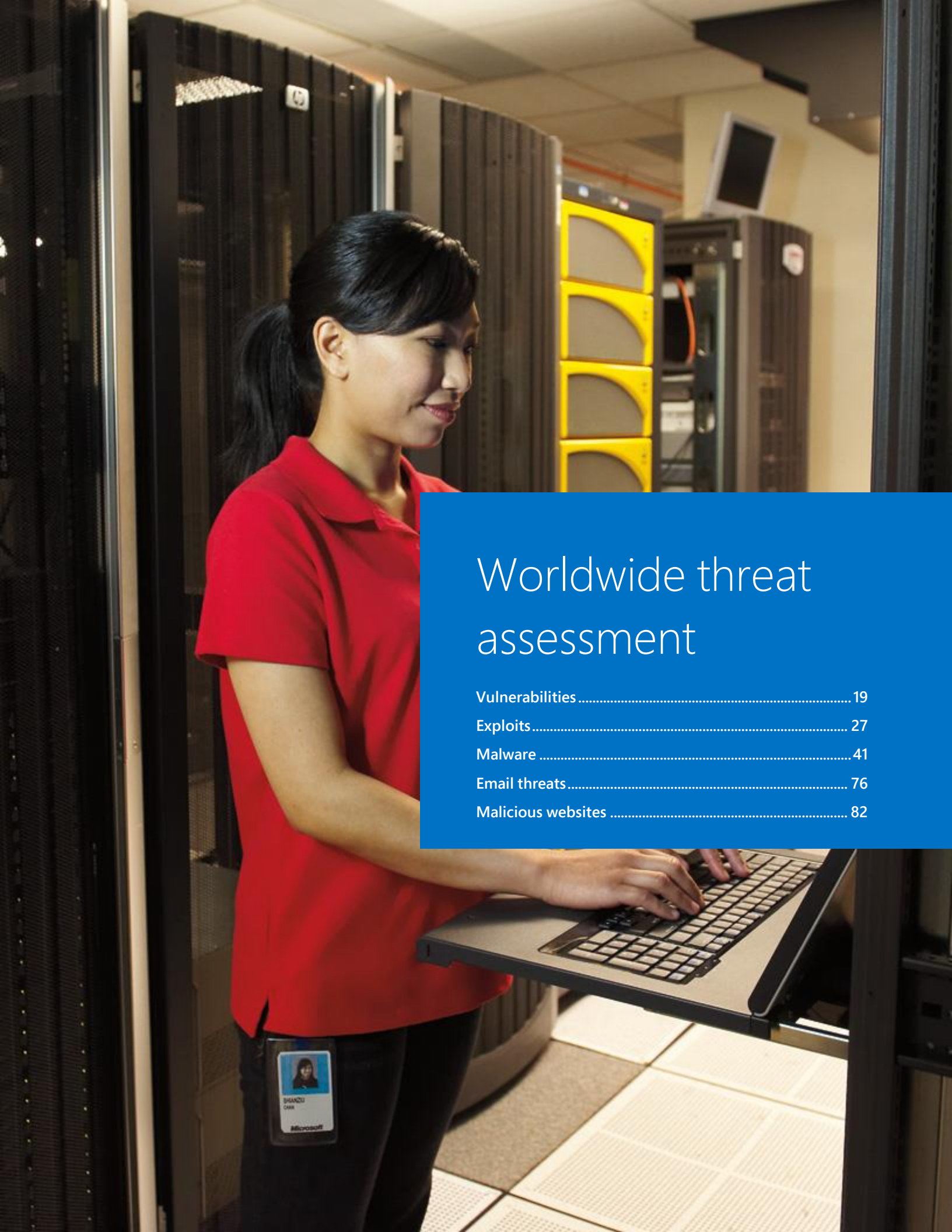
Conventions

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" in the full report. 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 family or variant that is detected by the Microsoft Malware Protection Engine.

Trustworthy Computing:
Security engineering at Microsoft

Amid the increasing complexity of today's computing threat landscape and the growing sophistication of criminal attacks, enterprise organizations and governments are more focused than ever on protecting their computing environments so that they and their constituents are safer online. With more than a billion systems using its products and services worldwide, Microsoft collaborates with partners, industry, and governments to help create a safer, more trusted Internet.

The Microsoft Trustworthy Computing organization focuses on creating and delivering secure, private, and reliable computing experiences based on sound business practices. Most of the intelligence provided in this report comes from Trustworthy Computing security centers—the Microsoft Malware Protection Center (MMPC), Microsoft Security Response Center (MSRC), and Microsoft Security Engineering Center (MSEC)—which deliver in-depth threat intelligence, threat response, and security science. Additional information comes from product groups across Microsoft and from Microsoft IT, the group that manages global IT services for Microsoft. The report is designed to give Microsoft customers, partners, and the software industry a well-rounded understanding of the threat landscape so that they will be in a better position to protect themselves and their assets from criminal activity.



Worldwide threat assessment

Vulnerabilities 19
Exploits 27
Malware 41
Email threats 76
Malicious websites 82

Vulnerabilities

Vulnerabilities are weaknesses in software that enable an attacker to compromise the integrity, availability, or confidentiality of the software or the data that it processes. 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

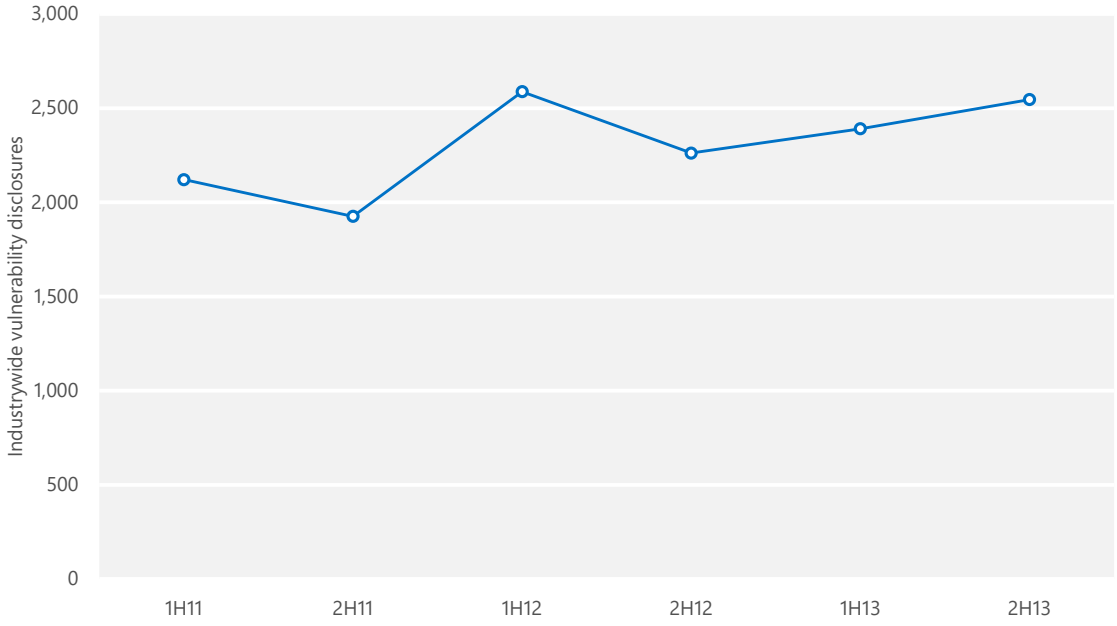
A *disclosure*, as the term is used in the *Microsoft Security Intelligence Report*, is the revelation of a software vulnerability to the public at large. Disclosures can come from a variety of sources, including publishers of the affected software, security software vendors, independent security researchers, 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.[1]

Figure 1 illustrates the number of vulnerability disclosures across the software industry for each half-year period since 1H11. (See "About this report" on page v for an explanation of the reporting period nomenclature used in this report.)

[1] 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 1. Industrywide vulnerability disclosures, 1H11–2H13



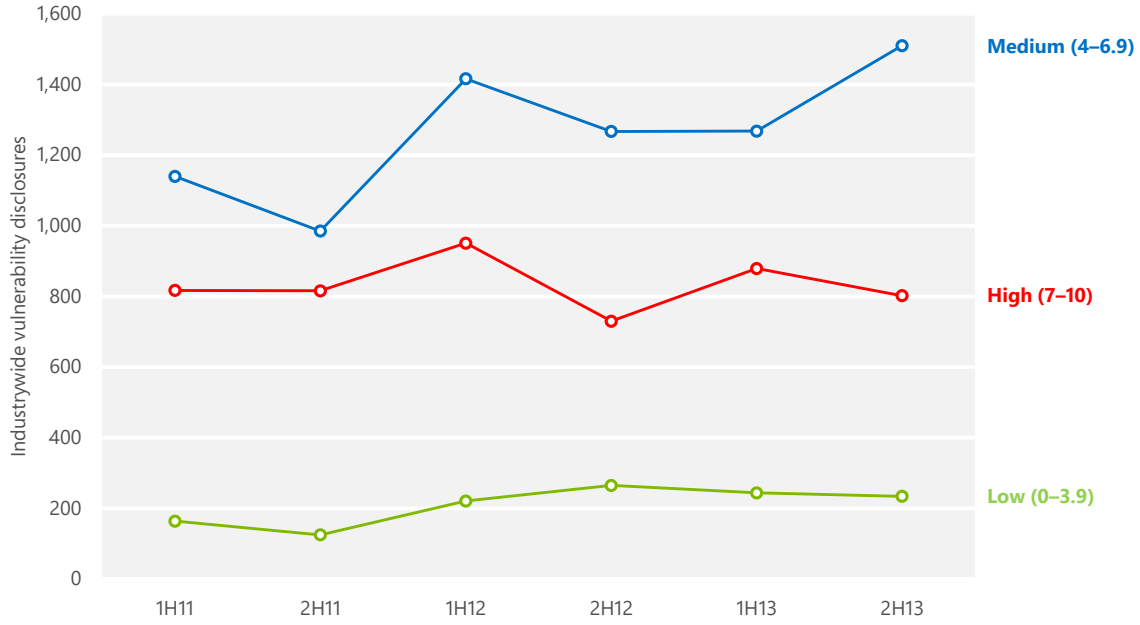
- Vulnerability disclosures across the industry in 2H13 were up 6.5 percent from 1H13, and 12.6 percent from 2H12. Increased disclosures of application vulnerabilities were responsible for much of the increase. (See "Operating system, browser, and application vulnerabilities" on page 23 for more information.)
- Despite increasing during each of the last two half-year periods, industrywide vulnerability disclosures in 2H13 remained below their recent peak level in 1H12, and well below levels seen prior to 2009, when totals of 3,500 disclosures or more per half-year period were not uncommon. For a historical view of the industry vulnerability disclosure trend, see the entry "Trustworthy Computing: Learning About Threats for Over 10 Years–Part 4" (March 15, 2012) at the Microsoft Security Blog at blogs.technet.com/security.

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 Vulnerability

Severity at the *Microsoft Security Intelligence Report* website (www.microsoft.com/sir) for more information.)

Figure 2. Industrywide vulnerability disclosures by severity, 1H11–2H13

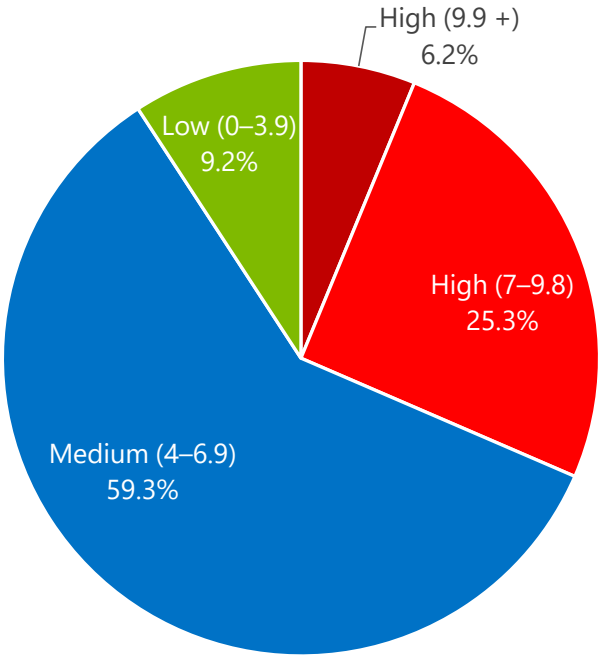


- High-severity vulnerability disclosures decreased 8.8 percent industrywide in 2H13, after increasing by 20.4 percent from 2H12 to 1H13. High-severity vulnerabilities accounted for 31.5 percent of total disclosures in 2H13, compared to 31.6 percent in the previous period.
- Medium-severity vulnerability disclosures increased 19.1 percent from 1H13, and accounted for 59.3 percent of total disclosures in 2H13.
- Low-severity vulnerability disclosures decreased 4.1 percent from 1H13. They remained low in relative terms in 2H13, and accounted for 9.2 percent of total disclosures.
- In general, mitigating the most severe vulnerabilities first is a security best practice. Vulnerabilities that scored 9.9 or greater represent 6.2 percent of all vulnerabilities disclosed in 2H13, as Figure 3 illustrates. This percentage represents a significant decrease from 1H13, when vulnerabilities that scored 9.9 or greater accounted for 12.4 percent of all vulnerabilities. Vulnerabilities that

> Industrywide vulnerability disclosures increased in 2H13, but high-severity vulnerabilities went down.

scored between 7.0 and 9.8 increased to 25.3 percent in 2H13 from 24.4 percent in 1H13.

Figure 3. Industrywide vulnerability disclosures in 2H13, by severity

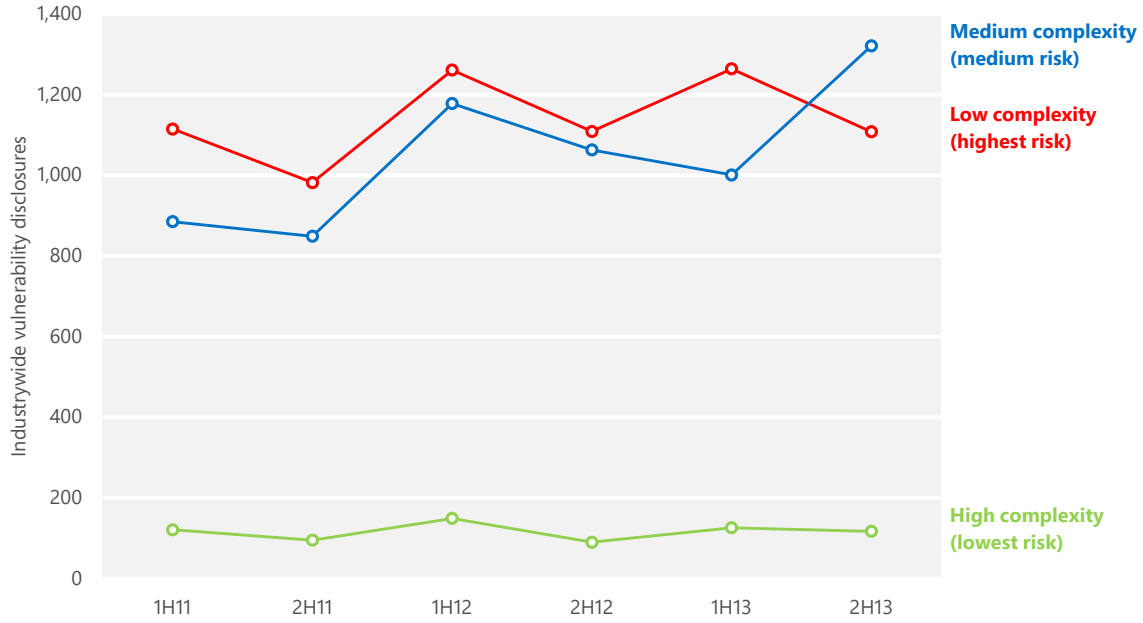


Vulnerability complexity

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 Vulnerability Complexity on the *Microsoft Security Intelligence Report* website for more information about the CVSS complexity ranking system.) Figure 4 shows complexity trends for vulnerabilities disclosed since 1H11. Note that Low complexity in Figure 4 indicates greater risk, just as High severity indicates greater risk in Figure 2.

Figure 4. Industrywide vulnerability disclosures by access complexity, 1H11–2H13



- Disclosures of Low-complexity vulnerabilities—those that are the easiest to exploit—accounted for 43.5 percent of all disclosures in 2H13, a decrease from 52.9 percent in 1H13.
- Disclosures of Medium-complexity vulnerabilities accounted for 51.9 percent of all disclosures in 2H13, an increase from 41.9 percent in 1H13.
- Disclosures of High-complexity vulnerabilities decreased to 4.6 percent of all disclosures in 2H13, down from 5.3 percent in 1H13.

Operating system, browser, and application vulnerabilities

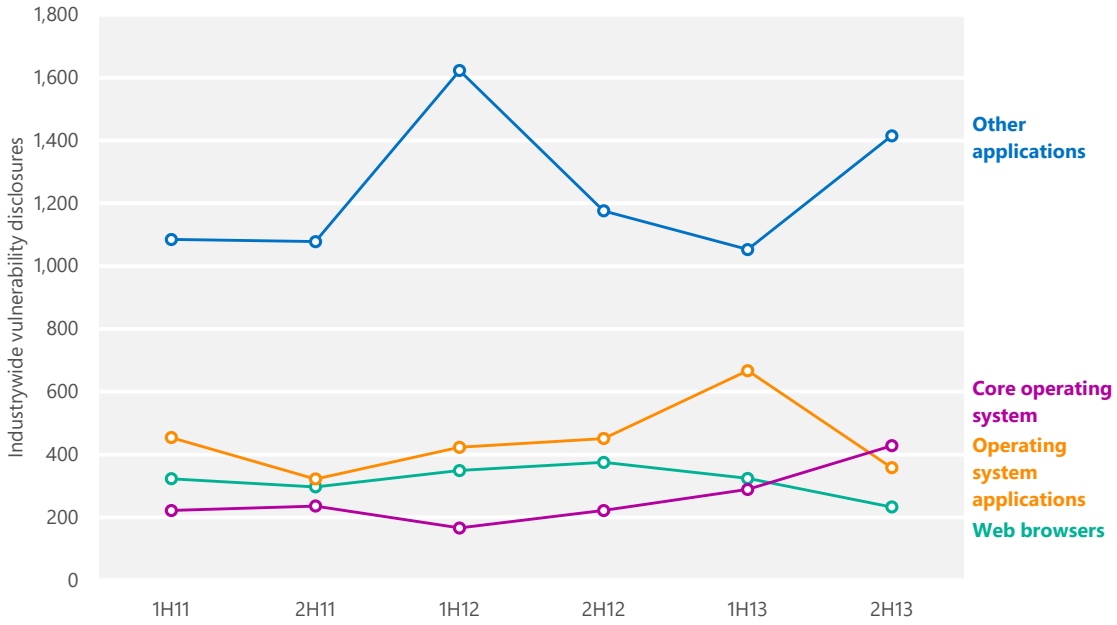
Comparing operating system vulnerabilities to non-operating system vulnerabilities that affect other components requires determining whether a particular program or component should be considered part of an operating system. This determination is not always simple and straightforward, given the componentized 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 product enumeration ("/o") in the NVD that do not also have any application product enumerations ("/a").
- *Operating system application vulnerabilities* are those with at least one /o product enumeration and at least one /a product 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 product enumeration in the NVD that do not have any /o product enumerations, except as described in the previous bullet point.

Figure 5 shows industrywide vulnerabilities for operating systems, browsers, and applications since 1H11.

Figure 5. Industrywide operating system, browser, and application vulnerabilities, 1H11–2H13



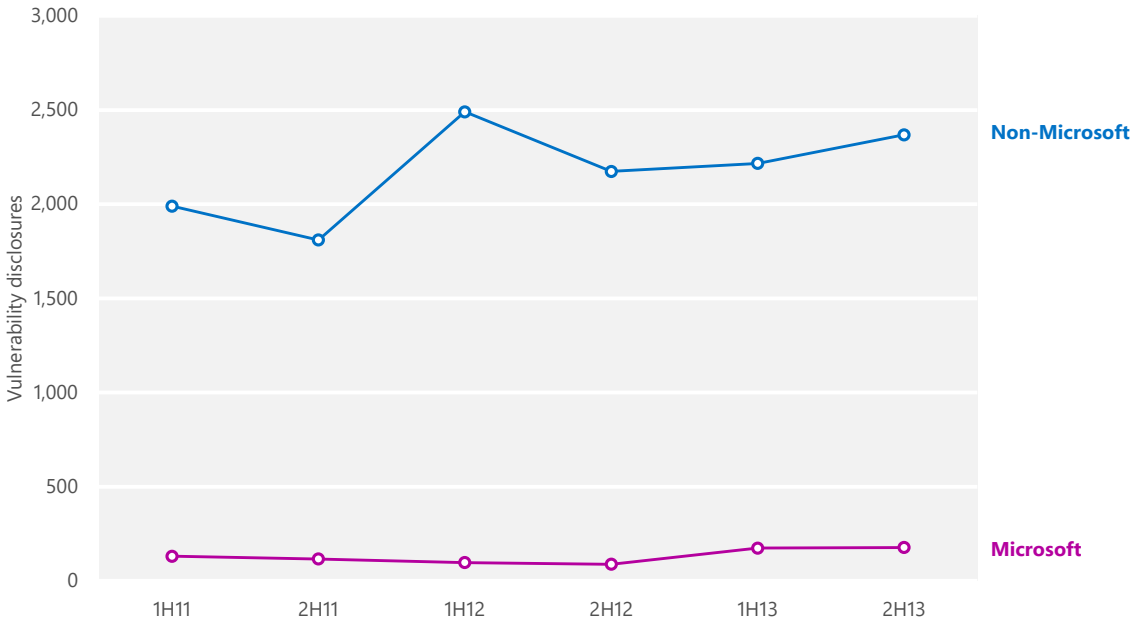
- Vulnerabilities in applications other than web browsers and operating system applications increased 34.4 percent in 2H13 and accounted for 58.1 percent of total disclosures for the period.
- Operating system vulnerabilities increased 48.1 percent in 2H13, going from last place to second. Overall, operating system vulnerabilities accounted for 17.6 percent of total disclosures for the period.
- After reaching a high point in 1H13, operating system application vulnerabilities decreased 46.3 percent in 2H13, and accounted for 14.7 percent of total disclosures for the period.
- Browser vulnerability disclosures decreased 28.1 percent in 2H13 and accounted for 9.6 percent of total disclosures for the period.

> Vulnerabilities in non-OS applications increased 34 percent.

Microsoft vulnerability disclosures

Figure 6 shows vulnerability disclosures for Microsoft and non-Microsoft products since 1H11.

Figure 6. Vulnerability disclosures for Microsoft and non-Microsoft products, 1H11–2H13



- Microsoft vulnerability disclosures remained mostly stable, increasing from 174 disclosures in 1H13 to 177 in 2H13, an increase of 1.7 percent.

- The Microsoft percentage of all disclosures across the industry fell slightly over the same period, from 7.3 percent of all industrywide disclosures in 1H13 to 7.0 in 2H13, because of a larger increase in disclosures from other software publishers.

Guidance: Developing secure 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. 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 companies 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).

For more in-depth information about the SDL and other techniques developers can use to secure their software, see Protecting Your Software in the "Managing Risk" section of the *Microsoft Security Intelligence Report* website.

Exploits

An *exploit* is malicious code that takes advantage of software vulnerabilities to infect, disrupt, or take control of a computer without the user's consent and typically without their knowledge. 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 are 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.[2]

Also see "Exploitation trends" on page 1 for an in-depth, multi-year examination of how attackers exploit vulnerabilities, and how exploitation tactics have changed over time.

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.[3]

Microsoft 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

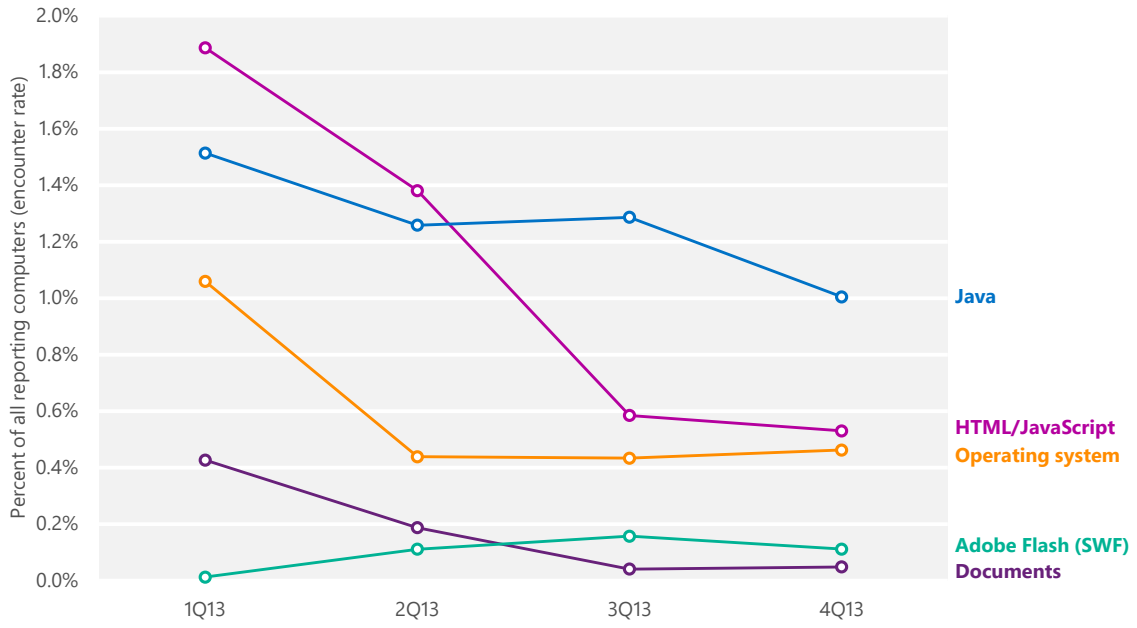
[2] See the Microsoft Security Update Guide at www.microsoft.com/security/msrc/whatwedo/securityguide.aspx for guidance to help protect your IT infrastructure while creating a safer, more secure computing and Internet environment.

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

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. 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 7 shows the prevalence of different types of exploits detected by Microsoft antimalware products in each quarter in 2013, 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 4Q13 was 1.0 percent, meaning that 1 percent of computers running Microsoft real-time security software in 4Q13 encountered Java exploit attempts, and 99 percent did not. In other words, a computer selected at random would have had about a 1 percent chance of encountering a Java exploit attempt in 4Q13. (Only computers whose users have opted in to provide data to Microsoft are considered when calculating encounter rates.[4]) See page 41 for more information about the encounter rate metric.

Figure 7. Encounter rates for different types of exploit attempts in 2013



[4] For privacy statements and other information about the products and services that provide data for this report, see "Appendix B: Data sources" in the full report.

- Computers that report more than one type of exploit are counted for each type detected.
- Detections of individual exploits often increase and decrease significantly from quarter to quarter as exploit kit distributors add and remove different exploits from their kits. This variation can also have an effect on the relative prevalence of different exploit types, as shown in Figure 7.
- Despite decreasing each quarter, Java exploits were the most commonly encountered type of exploits in 2H13.
- Encounters with web-based (HTML/JavaScript) threats decreased by more than half in 2H13 to become the second most commonly encountered type of exploits.
- Detections of operating system, Adobe Flash, and document exploits remained mostly stable during the second half of the year.

> Java exploits were the most commonly encountered type of exploits in 2H13.

Exploit families

Figure 8 lists the exploit-related families that were detected most often during the second half of 2013.

Figure 8. Quarterly encounter rate trends for the top exploit families detected and blocked by Microsoft real-time antimalware products in 2H13, shaded according to relative prevalence

Exploit	Platform or technology	1Q13	2Q13	3Q13	4Q13
CVE-2012-1723	Java	0.72%	0.47%	0.55%	0.32%
CVE-2010-2568 (CplLnk)	Operating system	0.31%	0.33%	0.35%	0.37%
CVE-2013-1493	Java	0.01%	0.20%	0.43%	0.24%
HTML/IframeRef*	HTML/JavaScript	0.82%	0.92%	0.35%	0.30%
CVE-2013-0422	Java	0.35%	0.27%	0.29%	0.18%
CVE-2012-0507	Java	0.39%	0.25%	0.18%	0.17%
Blacole	HTML/JavaScript	0.88%	0.35%	0.17%	0.17%
CVE-2010-0840	Java	0.12%	0.19%	0.14%	0.20%
CVE-2013-2423	Java	—	0.10%	0.15%	0.10%
CVE-2011-3544	Java	0.16%	0.13%	0.11%	0.10%

Totals for individual vulnerabilities do not include exploits that were detected as part of exploit kits.
*Totals include only IframeRef variants categorized as exploits.

- Overall, exploit encounter rates decreased significantly in 2H13, primarily because of HTML/IframeRef. See page 32 for more information.
- CVE-2012-1723, a vulnerability in the Java Runtime Environment (JRE), was the most commonly targeted vulnerability in 2H13, although it declined significantly from its peak in 1Q13. Exploits that target CVE-2012-1723 can use the vulnerability to download and run programs of the attacker's choice on the computer. CVE-2012-1723 is often exploited through drive-by downloads. (See page 98 for more information about drive-by download sites.)
- CVE-2010-2568, the second most commonly targeted vulnerability in 2H13, 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 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.

Overall, exploit encounter rates decreased significantly in 2H13.

- 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 signatures may be changed frequently. The encounter rate for IframeRef peaked in 2Q13 after detection signatures for the variant Trojan:JS/IframeRef.K were added to Microsoft antimalware products in response to the so-called "Darkleech" attacks, which add malicious inline frames to webpages hosted on compromised Apache web servers.
- Blacole is the Microsoft detection name for components of the so-called "Blackhole" exploit kit, which delivers malicious software through infected webpages. Prospective attackers buy or rent the Blacole kit on hacker forums and through other illegitimate outlets. It consists of a collection of malicious webpages that contain exploits for vulnerabilities in versions of Adobe Flash Player, Adobe Reader, Microsoft Data Access Components

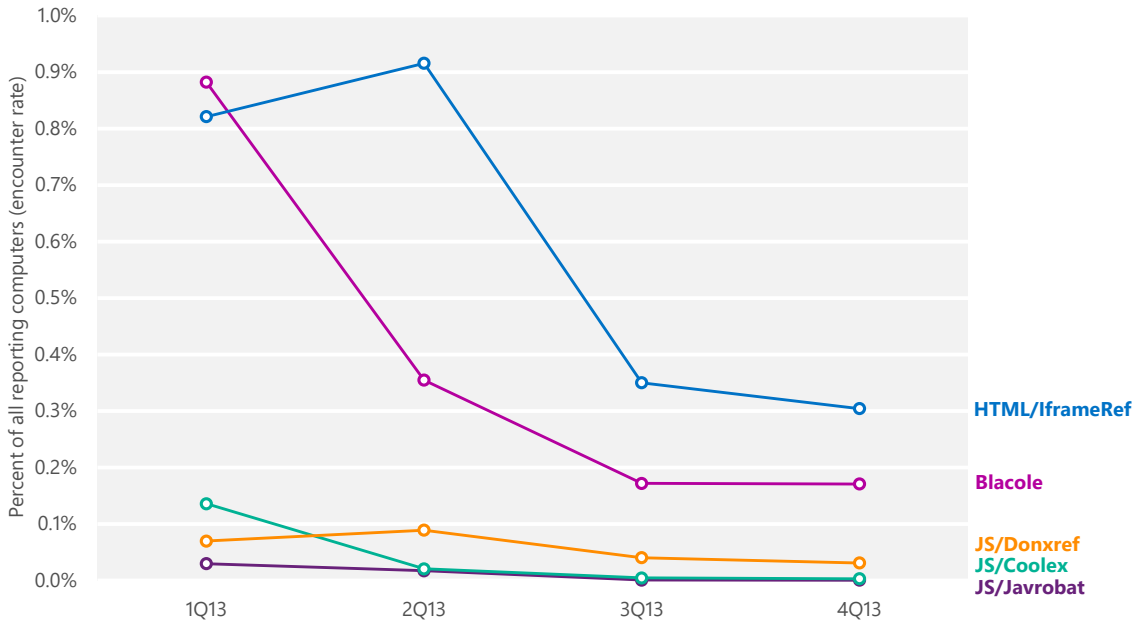
(MDAC), the Oracle Java Runtime Environment (JRE), and other popular products and components. When the attacker loads the Blacole kit on a malicious or compromised web server, visitors who don't have the appropriate security updates installed are at risk of infection through a drive-by download attack. (See the full report for more information about Blacole and other exploit kits.)

Blacole was encountered by 0.88 percent of all reporting computers in 1Q13 but declined steeply after that, with encounter rates of just 0.17 percent in both 3Q13 and 4Q13. The Blacole kit's author, called "Paunch," was known for frequently updating the kit with new exploits and techniques, but development of the kit halted abruptly in October 2013 following the arrest by Russian authorities of a man alleged to be Paunch.[5]

HTML and JavaScript exploits

Figure 9 shows the prevalence of different types of HTML and JavaScript exploits during each of the four most recent quarters.

Figure 9. Trends for the top HTML and JavaScript exploits detected and blocked by Microsoft real-time antimalware products in 2H13



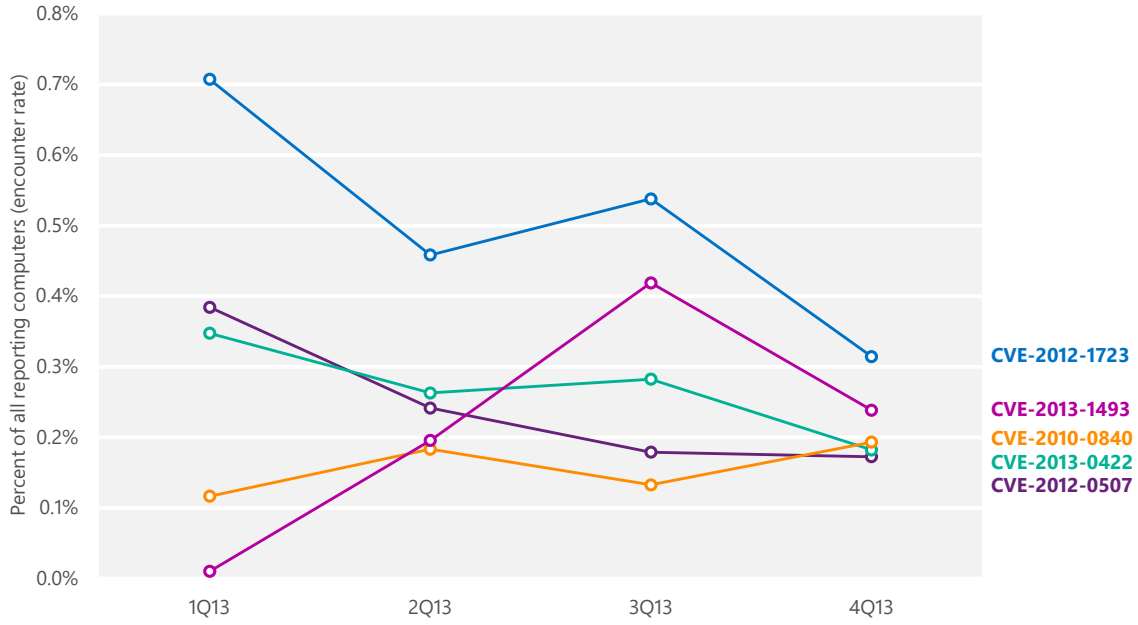
[5] "Blackhole malware exploit kit suspect arrested, *bbc.com*, October 9, 2013, http://www.bbc.com/news/technology-24456988.

- Encounters involving HTML/IframeRef declined considerably in the second half of the year, with the encounter rate in 4Q13 less than a third of that in 2Q13. Increased detections of IframeRef often correspond with apparent malware campaigns that target vulnerabilities in popular web frameworks, often involving exploit kits. Conversely, an absence of large numbers of unpatched web frameworks in 2H13 may be responsible for the decline.
- JS/Donxref is a generic detection for threats that attempt to exploit certain vulnerabilities in Java, Adobe Flash Player, and Windows.
- JS/Coolex is the Microsoft detection name for the so-called "Cool" exploit kit, which first appeared in October 2012 and is often used in ransomware schemes in which an attacker locks a victim's computer or encrypts the user's data and demands money to make it available again. See the "Ransomware" section on page 67 for more information about these threats.

Java exploits

Figure 10 shows the prevalence of different Java exploits by quarter.

Figure 10. Trends for the top Java exploits detected and blocked by Microsoft real-time antimalware products in 2H13



- CVE-2012-1723 accounted for most of the Java exploits detected and blocked in 4Q13. CVE-2012-1723 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 exploits for the vulnerability were added to the Blacole exploit kit shortly thereafter. CVE-2012-1723 exploits were removed from the Blacole kit in 1H13, contributing to the decline in its encounter rate.

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

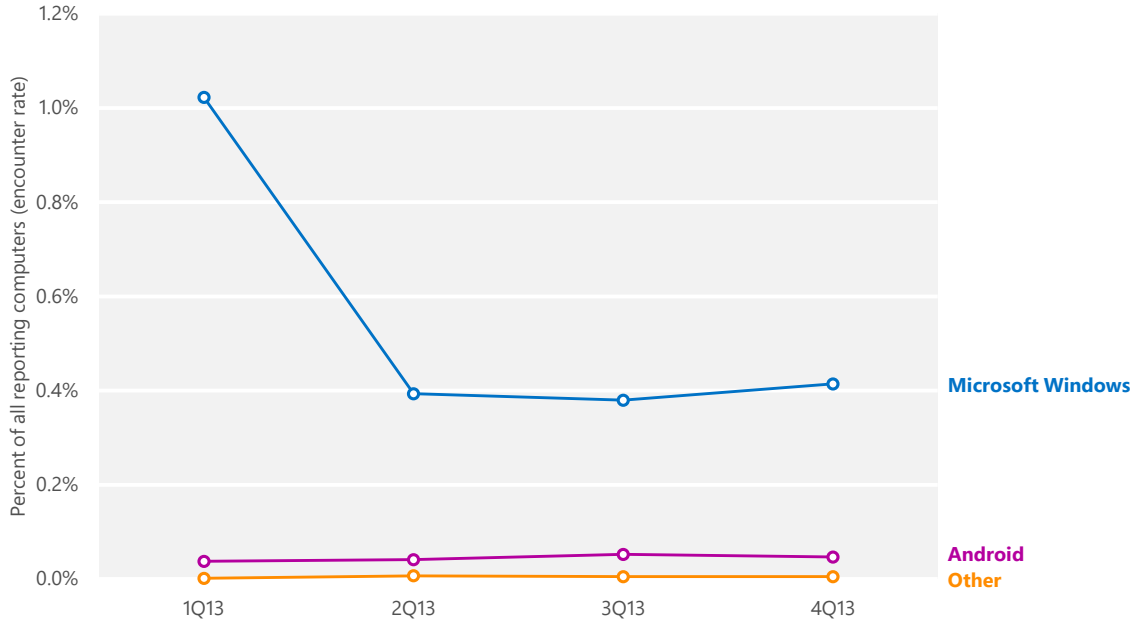
- CVE-2013-1493, a cross-platform vulnerability in the JRE's color management code, was first disclosed and exploited in the wild in 1Q13. Initial exploits targeting the vulnerability used heap-spraying techniques and leaked memory information to locate the accurate memory base location for exploitation. More recently, exploits have used methods such as obfuscated string and code structures in an effort to evade detection. Oracle issued Security Alert CVE-2013-1493 in March 2013 to address the vulnerability.
- CVE-2013-0422, the 3rd most commonly encountered exploit in 2H13, 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 11 shows the prevalence of different exploits against operating system vulnerabilities that were detected and removed by Microsoft real-time antimalware products during each of the past six quarters.

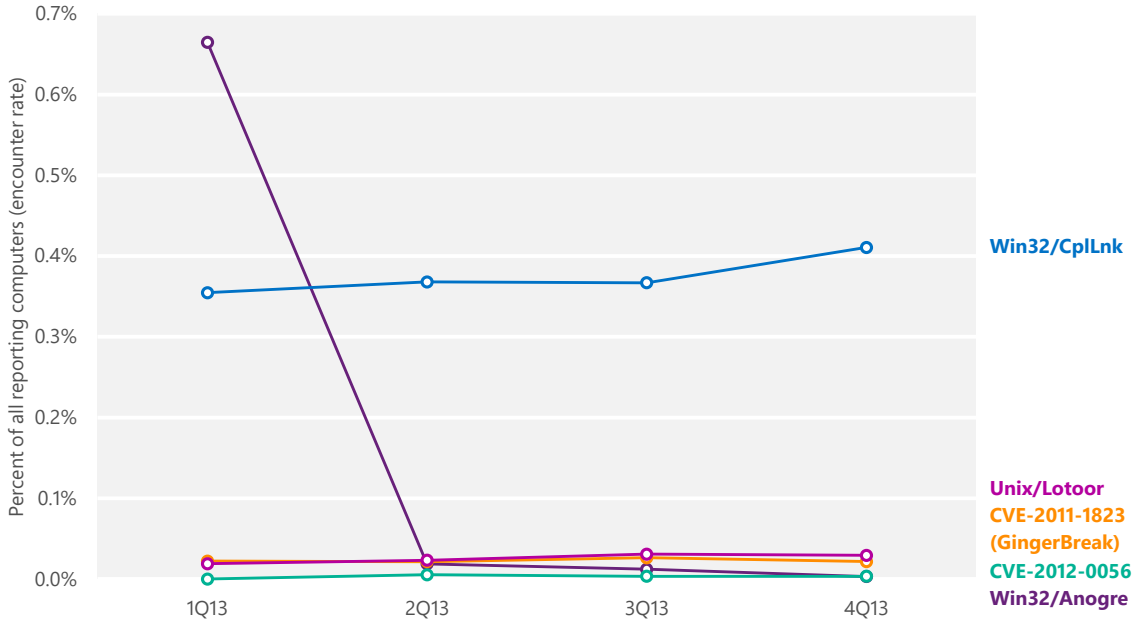
Figure 11. Exploits against operating system vulnerabilities detected and blocked by Microsoft real-time antimalware products in 2013



- Detections of exploit attempts that affect Windows-based computers remained stable in 2H13 after declining significantly in 2Q13 due to fewer detections of Win32/Anogre. (See page 35 for more information about Anogre.)
- Detections of exploits that affect the Android mobile operating system published by Google and the Open Handset Alliance accounted for a small share of operating system exploit detections in 2H13. (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. For these reasons, the information presented here should not be considered a comprehensive analysis of malware in the Android ecosystem.)

For another perspective on these exploits and others, Figure 12 shows trends for the individual exploits most commonly detected and blocked or removed during each of the past four quarters.

Figure 12. Individual operating system exploits detected and blocked by Microsoft real-time antimalware products in 2013



- Win32/CplLnk, an exploit that targets a vulnerability in Windows Shell, remained the most commonly encountered operating system exploit in 2H13. 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.
- Encounters with Win32/Anogre, which briefly accounted for the largest share of operating system exploit encounters in 1Q13, subsequently fell to much lower levels, and were negligible by 4Q13. Anogre targets CVE-2011-3402, a vulnerability in the way the Windows kernel processes TrueType font files. Microsoft released Security Bulletin MS11-087 in December 2011 to address the issue. The steep decline in detections suggests that the exploit ceased being useful to attackers after security software vendors updated their signature databases to detect the attack method it uses.

> The CplLnk exploit remained the most common operating system exploit in 2H13.

- Most detections that affected Android involve a pair of 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.

- 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.
- 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.

Document exploits

Document exploits are exploits that target vulnerabilities in the way a document editing or viewing application processes a particular file format. Figure 13 shows the prevalence of different types of document exploits during each of the four most recent quarters, and Figure 14 shows encounter rates for individual exploits.

Figure 13. Types of document exploits detected and blocked by Microsoft real-time antimalware products in 2013

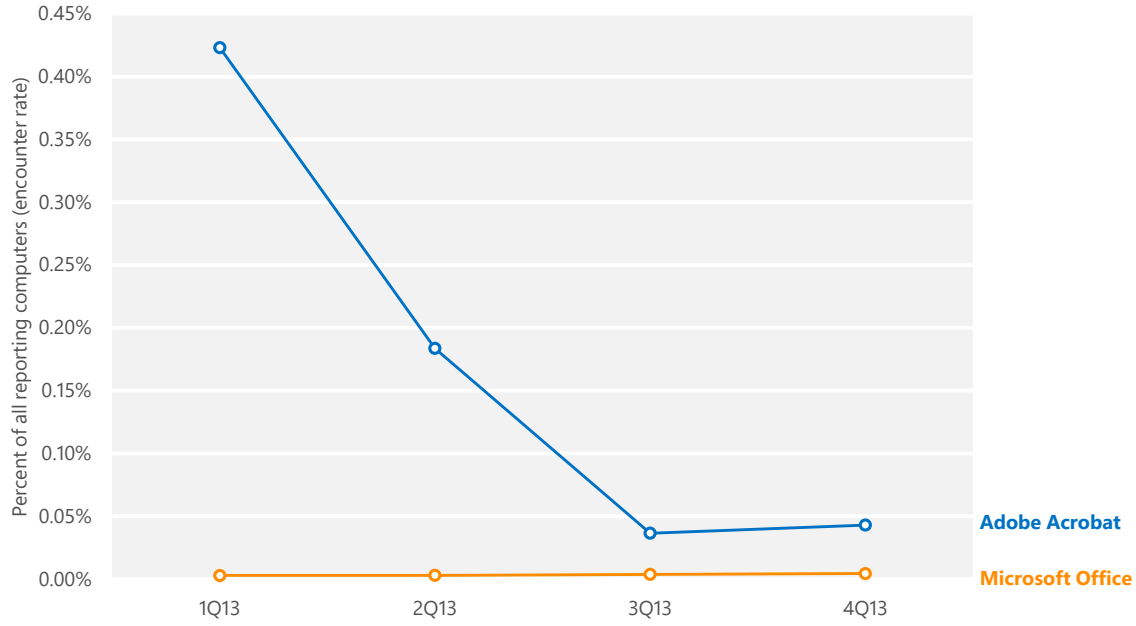
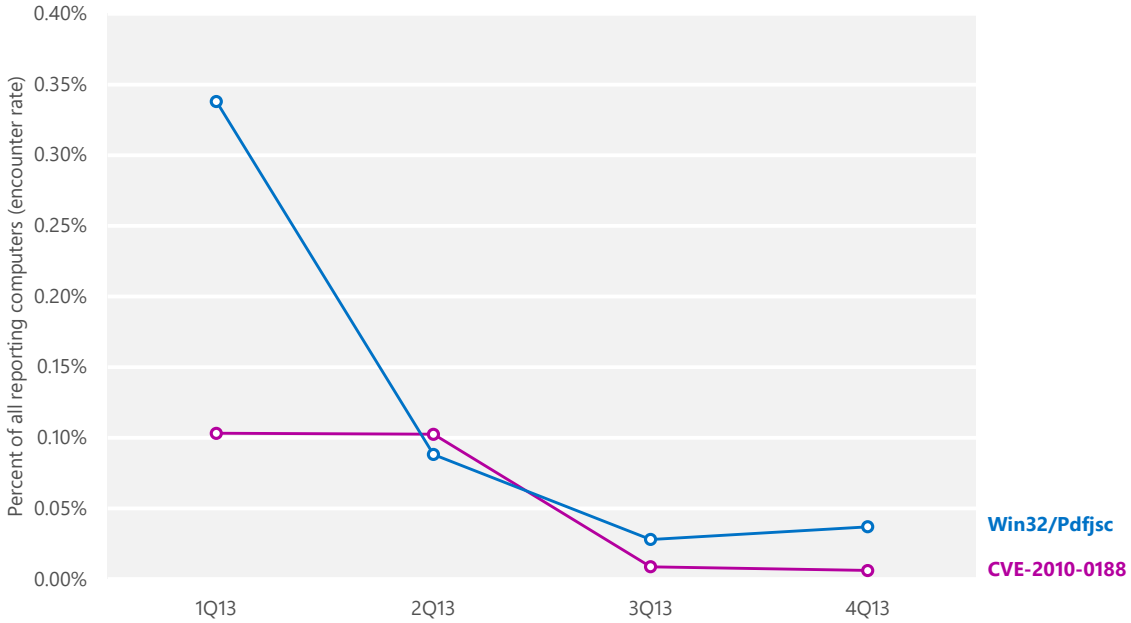


Figure 14. Individual document exploits detected and blocked by Microsoft real-time antimalware products in 2013

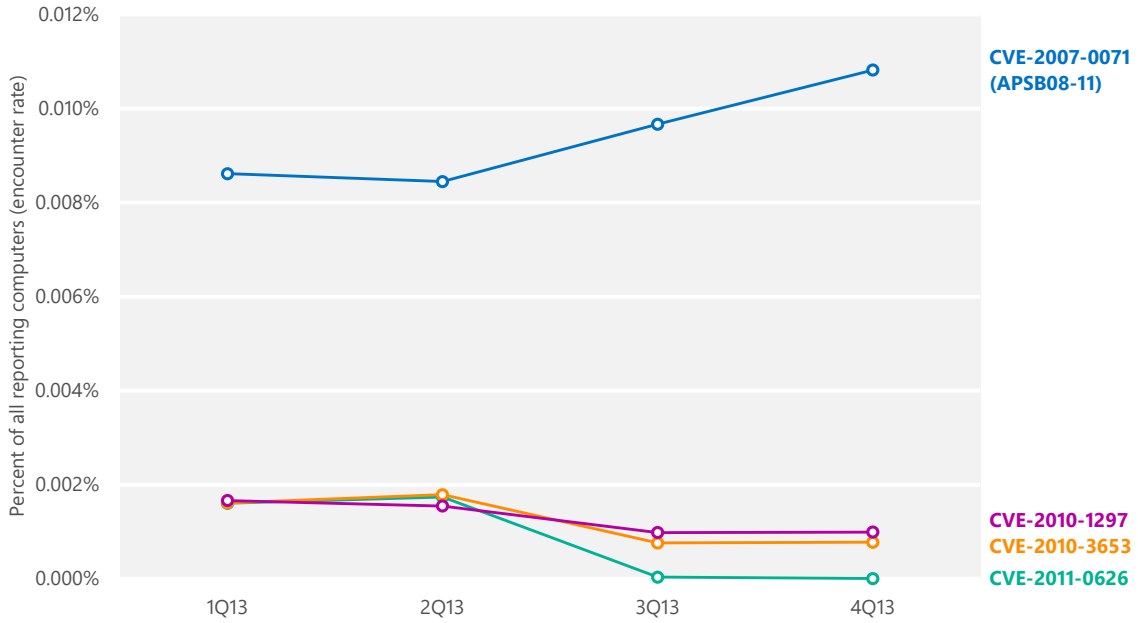


- Detections of exploits that affect Adobe Reader and Adobe Acrobat declined considerably from the first half of the year, in part due to the decreased prevalence of the Blacole exploit kit. Most of these detections were associated with the exploit family Win32/Pdfjsc.

Adobe Flash Player exploits

Figure 15 shows the prevalence of different Adobe Flash Player exploits by quarter.

Figure 15. Adobe Flash Player exploits detected and blocked by Microsoft real-time antimalware products in 2013



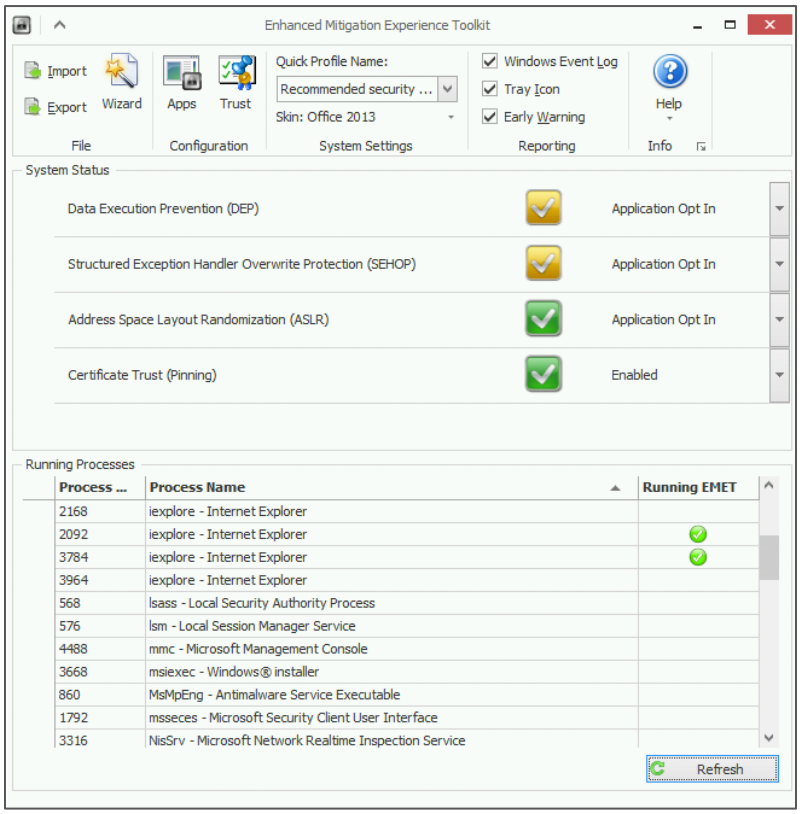
- CVE-2007-0071, the most commonly exploited Adobe Flash Player vulnerability in 2H13, is an invalid pointer vulnerability in some releases of Adobe Flash Player versions 8 and 9. Adobe released Security Bulletin APSB08-11 on April 8, 2008 to address the issue.
- CVE-2010-1297, the second most commonly exploited Adobe Flash Player vulnerability in 2H13, 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.

Enhanced Mitigation Experience Toolkit (EMET) effectiveness

The Enhanced Mitigation Experience Toolkit (EMET) is a utility that helps prevent vulnerabilities in software from being successfully exploited. EMET provides system administrators with the ability to deploy security mitigation technologies such as Address Space Layout Randomization (ASLR), Data Execution Prevention (DEP), Structured Exception Handler Overwrite Protection (SEHOP), and others to selected installed applications. These technologies function as special protections and obstacles that an exploit author must defeat to exploit

software vulnerabilities. These security mitigation technologies do not guarantee that vulnerabilities cannot be exploited, but they work to make exploitation as difficult as possible to perform.

Figure 16. The Enhanced Mitigation Experience Toolkit (EMET), version 4.1



The most recently released version of EMET is version 4.1, released on November 12, 2013 and available from the Microsoft Download Center. It adds support for shared remote desktop environments on servers with EMET installed; improved logging for more accurate reporting in multi-user scenarios; updated default protection profiles, Certificate Trust rules, and Group Policy Object templates; and several other improvements.

> EMET mitigations have directly affected the risk organizations have faced from targeted attacks.

As Figure 17 shows, the mitigations available through EMET have directly affected the level of risk that organizations have faced from targeted attacks by determined adversaries. See the EMET 4 user guide for explanations of the listed mitigations.

Figure 17. Vulnerabilities exploited in targeted attacks during 2013 that were mitigated by EMET 4

Vulnerability	Affected software/component	Security Bulletin	EMET mitigations effective
CVE-2013-0640	Adobe Reader	APSB13-07	ROP, EAF, HeapSpray
CVE-2013-1331	Microsoft Office (PNG)	MS13-051	EAF
CVE-2013-3163	Internet Explorer	MS13-055	EAF, DeepHooks ROP
CVE-2013-3893	Internet Explorer	MS13-080	MandatoryASLR, ROP, EAF, HeapSpray
CVE-2013-3897	Internet Explorer	MS13-080	MandatoryASLR, ROP, EAF, HeapSpray
CVE-2013-3906	Microsoft Office (OGL)	MS13-096	MandatoryASLR, ROP, EAF, HeapSpray
CVE-2013-3918	Internet Explorer (ICARDIE)	MS13-090	ROP
CVE-2013-5065	Adobe Reader (sandbox escape)	MS14-002	NullPage
CVE-2013-5330	Adobe Flash	APSB13-26	DeepHooks ROP

Malware

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 computer and network traffic for threats and blocks them before they can infect the computer, if possible. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed.

For this reason, Microsoft uses two different metrics to measure malware prevalence:[6]

- *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 Win32/Sefnit in Germany in 3Q13 was 1.73 percent. This data means that, of the computers in Germany that were running Microsoft real-time security software in 3Q13, 1.73 percent reported encountering the Sefnit family, and 98.27 percent did not. (Only computers whose users have opted in to provide data to Microsoft are considered when calculating encounter rates.[7])
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers. Because it is not a real-time tool, the MSRT only detects and removes threats that are already

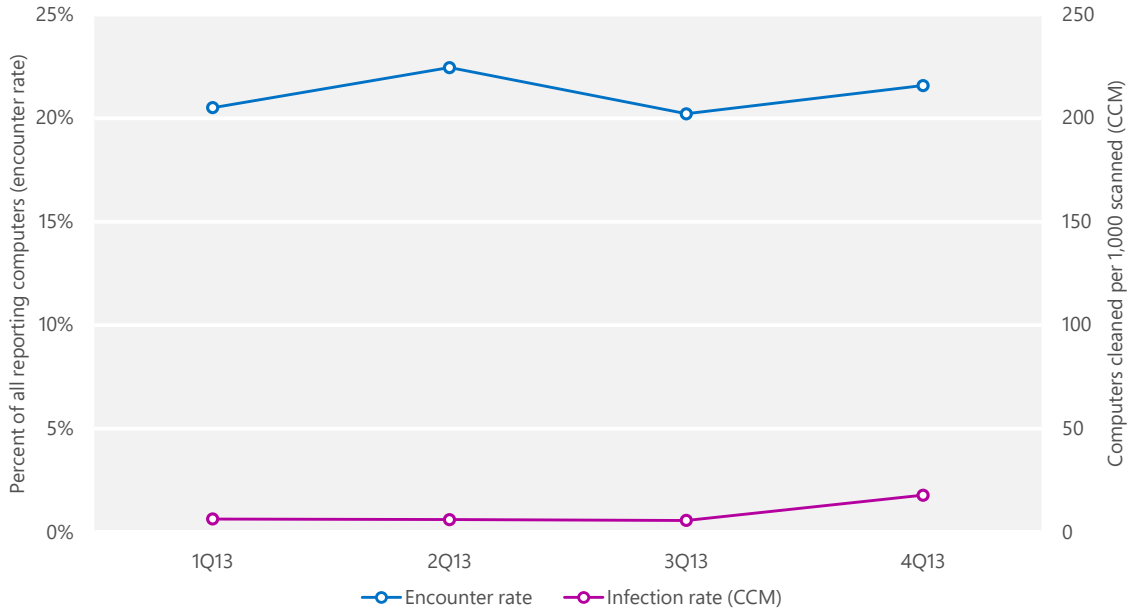
[6] Microsoft regularly reviews and refines its data collection methodology to improve its scope and accuracy. For this reason, the statistics presented in this volume of the *Microsoft Security Intelligence Report* may differ slightly from comparable statistics in previous volumes.

[7] For privacy statements and other information about the products and services that provide data for this report, see "Appendix B: Data sources" in the full report.

present on the computer; it does not block infection attempts as they happen.

Figure 18 illustrates the difference between these two metrics.

Figure 18. Worldwide encounter and infection rates in 2013, by quarter



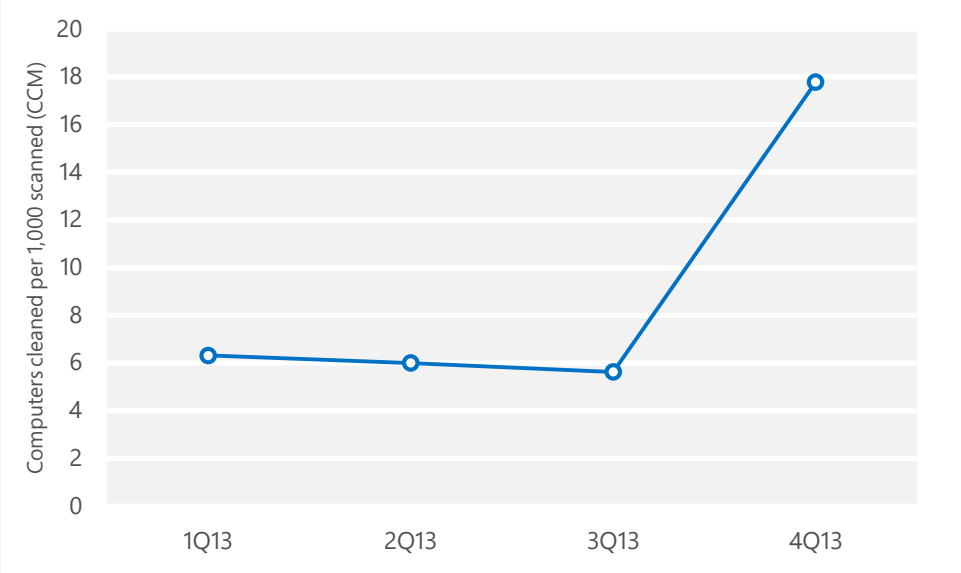
As Figure 18 shows, and as one would expect, malware encounters are much more common than malware infections. On average, about 21.2 percent of reporting computers worldwide encountered malware each quarter in 2013. At the same time, the MSRT removed malware from about 11.7 out of every 1,000 computers, or 1.17 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.

A trio of threats makes waves in 4Q13

Both the worldwide infection rate and encounter rate increased from 3Q13 to 4Q13, but the magnitudes of the two increases were radically different. The rise in the encounter rate was in line with the trend seen in previous quarters, but the infection rate increased from a CCM of 5.6 in 3Q13 to 17.8 in 4Q13—a threefold increase, and the largest quarter-to-quarter infection rate increase ever measured by the MSRT. The discrepancy between these two metrics is the result

of actions taken by the MMPC to combat an old threat using a new distribution method.

Figure 19. Worldwide infection rates in 2013, by quarter



Sefnit: click fraud reloaded

Win32/Sefnit is a bot that allows a remote attacker to use the computer to perform various activities. It has been distributed through peer-to-peer (P2P) file sharing networks disguised as a legitimate program, and by being bundled with other software. Researchers have observed Sefnit being used to perform a number of tasks that are designed to make money for the attacker, including click fraud, performing Bitcoin mining, and redirecting search results. Early versions of Sefnit, from 2010 and 2011, used click hijacking to redirect users' web browsers through advertising networks for some search results, earning money for the attackers through affiliate programs. This behavior made it easier for security software vendors to neutralize Sefnit botnets, because users who noticed that their searches had been redirected often submitted samples to antimalware researchers to help them create improved detection signatures. The click hijacking component was removed from newer versions of Sefnit in 2011, and Sefnit was believed to no longer be very active in the wild. Detection signatures for Sefnit were first added to the MSRT in January 2012.

In mid-2013, Microsoft researchers discovered a new version of Sefnit that uses a different mechanism to commit click fraud. The new click fraud component is structured as a proxy service, allowing attackers to use a botnet of Sefnit-hosted proxies to relay HTTP traffic that issues illegitimate "clicks" for online

advertisements. Because the new component operates in the background and involves no user interaction, new Sefnit variants that used the component managed to evade detection by antimalware researchers for a time. Microsoft added detection signatures for the new variants, and Sefnit became the 3rd most commonly encountered malware family worldwide in 3Q13, and the 8th most commonly encountered family in 4Q13.

For more in-depth information about Sefnit, see the entry "Mevade and Sefnit: Stealthy click fraud" (September 25, 2013) on the MMPC blog at blogs.technet.com/mmpc.

Rotbrow and Brantall: dealing with a backlog

The new campaign of Sefnit distribution that began in 2013 relies heavily on a pair of families, Win32/Rotbrow and Win32/Brantall. Rotbrow is a program that claims to protect the computer from browser add-ons, but actually installs more browser add-ons. Brantall acts as an installer for various legitimate programs, installs itself as a service in some cases, and installs both the advertised legitimate program and additional bundled applications. Both families have been observed directly installing Sefnit.

Rotbrow presents itself as a browser add-on called "Browser Protector" (or alternately "Browser Defender"). Microsoft has been aware of this program since 2011, but it had never displayed malicious behavior until its association with Sefnit was discovered in 2013. Researchers discovered that some versions of the Browser Protector process, called BitGuard.exe, drop an installer for a harmless program called File Scout, and also secretly install Sefnit at the same time. Other versions of Browser Protector do not contain Sefnit, but are capable of being modified to include it. Therefore, to help combat the spread of Sefnit, the MMPC added detection signatures (labeled "Rotbrow") for susceptible versions of Browser Protector to Microsoft real-time security products. In December 2013, these signatures were added to the MSRT.

It was the addition of Rotbrow to the MSRT in December that was most responsible for the dramatic increase in the CCM metric in 4Q13. Because the Browser Protector software had existed since at least 2011 without exhibiting malicious behavior, many security software vendors had not configured their products to block or remove it. The December release of the MSRT therefore detected and removed it from a large number of computers on which it may have been installed for several months or even years. (See page 40 of *Microsoft Security Intelligence Report, Volume 14 (July–December 2012)* for details of a

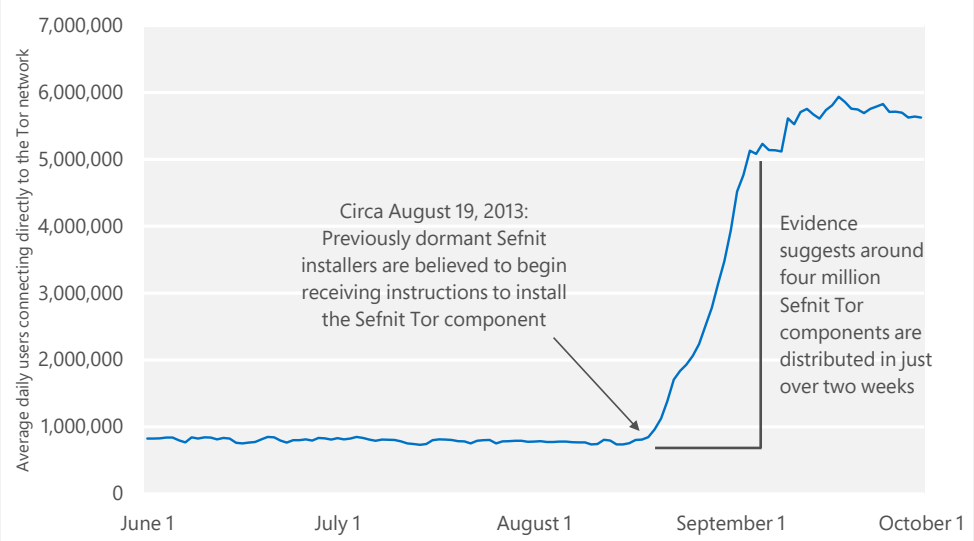
similar incident that primarily affected computers in Korea.) Detections of Rotbrow decreased considerably after December, and the MMPC expects the CCM infection rate to return to more typical levels in subsequent quarters as the MSRT and other security products resolve the remaining backlog of old Rotbrow infections. Microsoft has also contacted other antimalware vendors and provided them with relevant samples so that they can more effectively protect their own customers from these threats.

For more information about Rotbrow and its inclusion in the MSRT, see the entry "Rotbrow: The Sefnit distributor" (December 10, 2013) on the MMPC blog at blogs.technet.com/mmpc.

Sefnit and the Tor network

Sefnit uses the Tor network as one mechanism for administering the botnet. Tor is 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. It has a number of legitimate uses, but it can also be used by an attacker with malicious intent, as with the Sefnit botnet. In 3Q13, the Sefnit authors commanded millions of infected clients to download and install a Tor client and begin using the Tor network for command and control (C&C). Based on usage estimates provided by the Tor Project, this action apparently added more than four million new clients to the Tor network in just over two weeks, as shown in Figure 20.

Figure 20. The effect of Win32/Sefnit on the user base of the Tor network



Data courtesy of the Tor Project (metrics.torproject.org)

When antimalware software removes Sefnit from a computer on which it is installed, the Tor client is left behind and remains connected to the Tor network, unless it is specifically removed. In addition to the increased workload this places on the Tor network infrastructure, it creates a security problem for the formerly infected computers: the Tor client installed by the Sefnit authors does not self-update, which puts these computers at risk of exploitation if significant vulnerabilities are discovered in the (now several months out of date) Tor client version used by Sefnit. After consulting with Tor project developers, the MMPC created detection signatures for the Tor service added by Sefnit and deployed them to Microsoft security products beginning in October, and to the November release of the MSRT. This protection removes the service started by the Sefnit malware, but does not uninstall Tor, remove any Tor binaries, or prevent users from using Tor.

For more information about Sefnit and Tor, see the entry "Tackling the Sefnit botnet Tor hazard" (January 9, 2014) on the MMPC blog at blogs.technet.com/mmpc.

Malware prevalence 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.[8]

[8] For more information about this process, see the entry "Determining the Geolocation of Systems Infected with Malware" (November 15, 2011) in the Microsoft Security Blog (blogs.technet.com/security).

Figure 21. Encounter rate trends for the locations with the most computers reporting malware detections in 2H13, by number of computers reporting

	Country/Region	1Q13	2Q13	3Q13	4Q13
1	United States	15.2%	15.2%	13.2%	12.0%
2	Brazil	26.5%	32.9%	32.3%	38.1%
3	Germany	16.9%	15.3%	13.9%	15.1%
4	Japan	7.3%	8.4%	7.6%	8.0%
5	United Kingdom	15.1%	15.1%	13.9%	16.2%
6	France	16.2%	19.2%	16.8%	25.9%
7	Russia	35.6%	38.4%	30.1%	25.8%
8	Canada	16.5%	15.3%	13.0%	13.6%
9	Italy	23.4%	25.3%	21.1%	26.2%
10	China	28.8%	32.4%	25.4%	20.3%

- Locations in Figure 21 are ordered by the number of computers reporting detections in 2H13.
- The new threats Win32/Rotbrow and Win32/Brantall were among the top 10 families in 4Q13 in all of these locations except China, and the newly active family Win32/Sefnit was in the top 10 in all of these locations except Brazil, Russia, and China. See "A trio of threats makes waves in 4Q13" on page 42 for more information about these families.
- Of these locations, Brazil and France were the only ones that experienced encounter rate increases between 1H13 and 2H13. Brantall (encountered by 11.47 percent of reporting computers in Brazil in 4Q13) and Rotbrow (9.82 percent) were particularly prevalent in Brazil in 4Q13. Other threats that were unusually common in Brazil in 2H13 include the worm family JS/Proslikefan (the 3rd most commonly encountered family in Brazil in 2H13, but only 36th worldwide), and the trojan family Win32/Banload (8th in Brazil, 62nd worldwide), which is often used to target customers of Brazilian banks.

> Rotbrow, Brantall, and Sefnit were among the most common threats in most of the top locations.

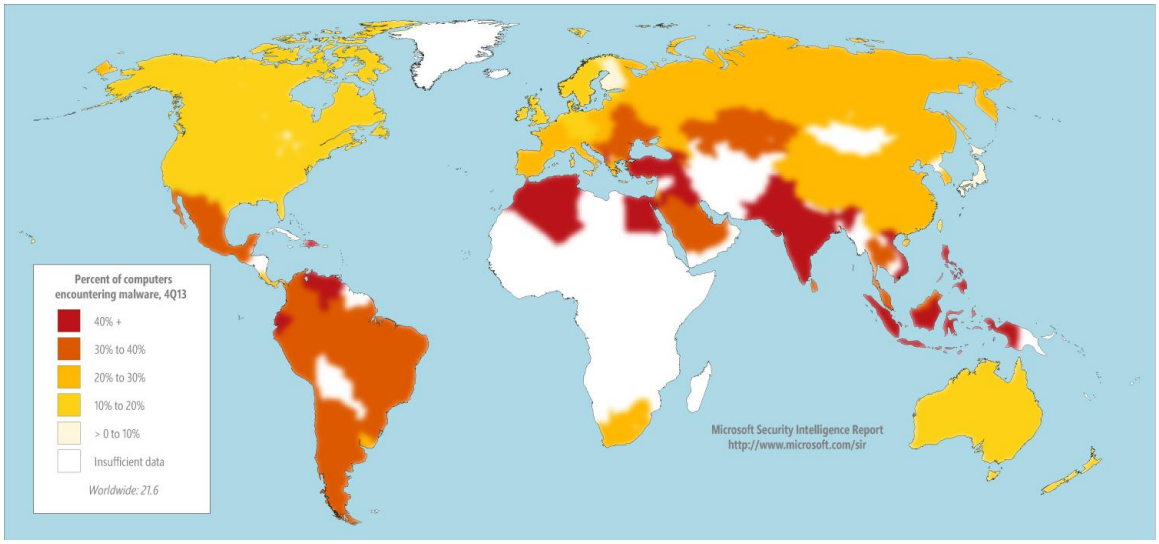
- The trojan family VBS/Miposa was unusually prevalent in Japan (8th in Japan, 254th worldwide). Miposa is a trojan that attempts to download and run Windows Scripting Host (.wsh) files. When used legitimately, .wsh files

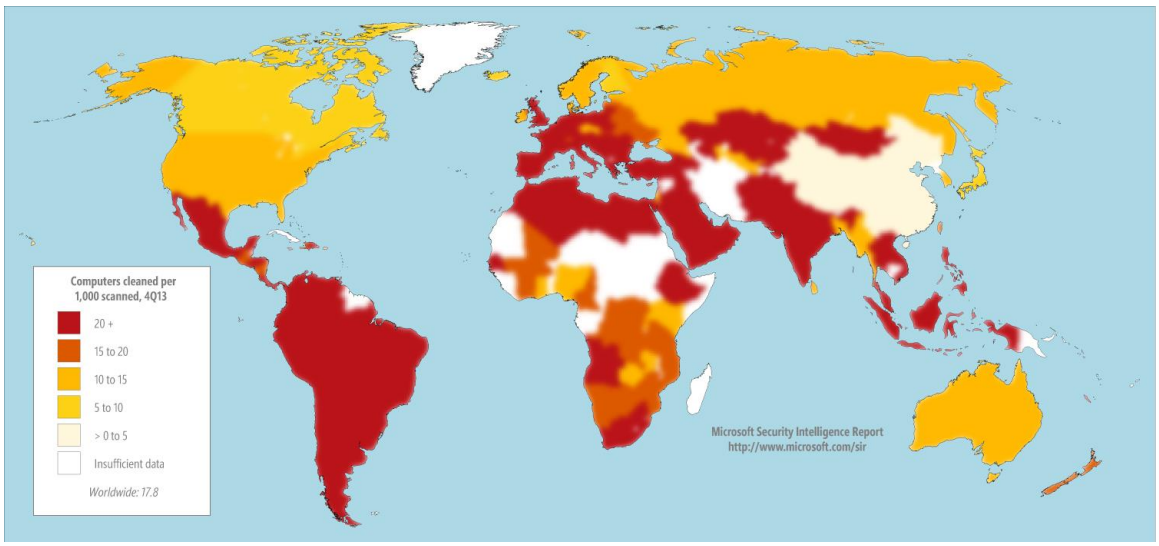
are used to automate tasks. When used maliciously, however, they may be used to run or download other files, including malware.

- The generic detection Win32/Obfuscator was the most commonly encountered family in Russia and China in 2H13. It was encountered more than twice as often as the next most common threat family in both locations. Obfuscator is a generic detection for threats that have been modified by malware obfuscation tools in an attempt to avoid detection by security software.
- Families that were unusually prevalent in Russia in 2H13 include BAT/Qhost (2nd in Russia, 58th worldwide), which attempts to block access to certain websites by modifying the computer's Hosts file; Win32/Deminnix (7th in Russia, 73rd worldwide), which is used in Bitcoin mining schemes; and the generic detection JS/Redirector (8th in Russia, 51st worldwide).
- Families that were unusually prevalent in China in 2H13 include the generic detections Redirector and Win32/Orsam (5th in China, 40th worldwide) and the trojan family Win32/Nitol (9th in China, 102nd worldwide), which allows backdoor access to an infected computer and is used to perform distributed denial-of-service (DDoS) attacks.

For a different perspective on threat patterns worldwide, Figure 22 shows the infection and encounter rates in locations around the world in 4Q13.

Figure 22. Encounter rates (top) and infection rates (bottom) by country/region in 4Q13





The next several figures illustrate trends for specific locations around the world with particularly high or low incidences of threat detection. Figure 23 and Figure 24 show trends for the locations with the highest rates of detection as determined by encounter rate and CCM, respectively.

Figure 23. Trends for the five locations with the highest malware encounter rates in 2H13 (100,000 reporting computers minimum)

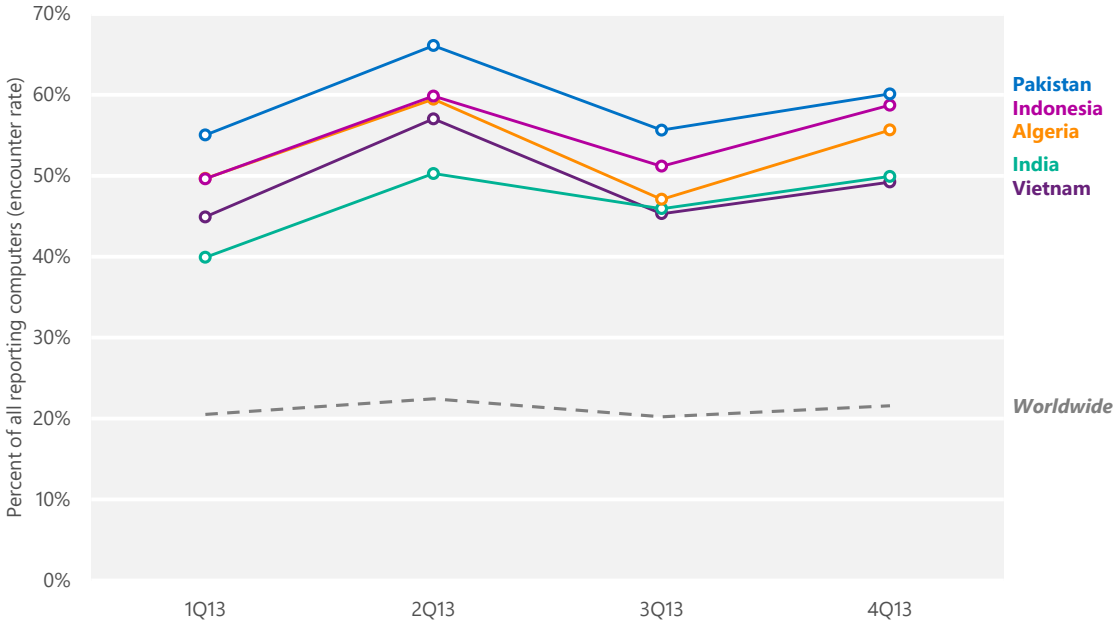
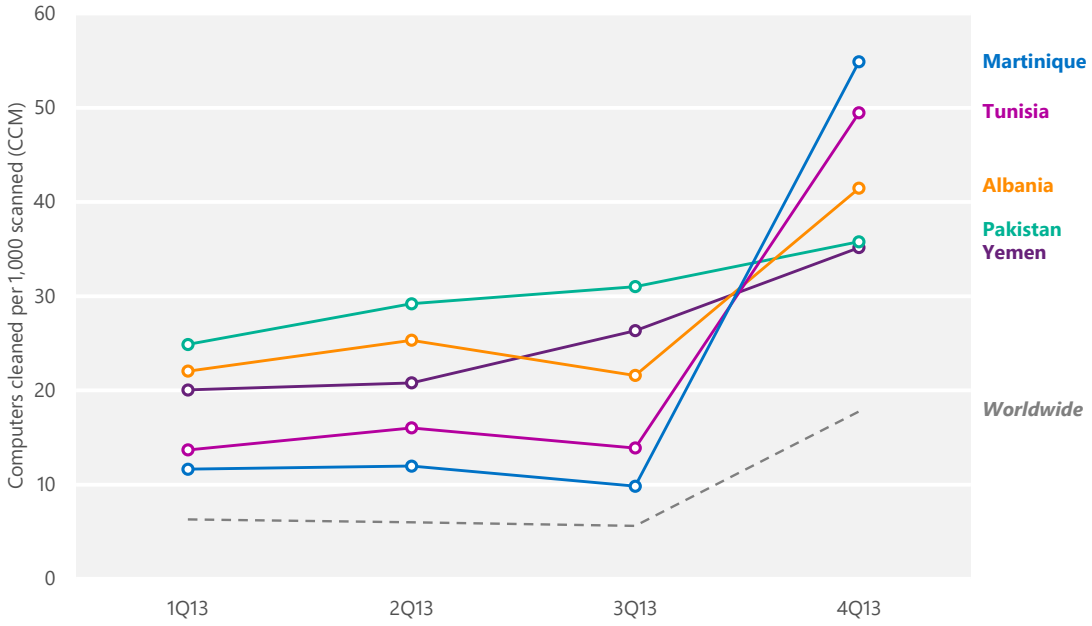


Figure 24. Trends for the five locations with the highest malware infection rates in 2H13, by CCM (100,000 MSRT executions minimum)



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

- Win32/Rotbrow and Win32/Brantall were highly prevalent in all of these locations in 4Q13, contributing to the encounter rate increases seen that quarter. Other threat families that were commonly encountered in multiple locations include INF/Autorun, the 4th most commonly encountered family worldwide in 2H13, and Win32/Gamarue, the 5th most commonly encountered family.
- Pakistan had the highest encounter rate of any significant location in 2H13, with more than half of the computers in Pakistan encountering malware in each of the last two quarters. Autorun, Gamarue, and VBS/Jenxcus were the most commonly encountered families in Pakistan in 4Q13.
- The trojan family Win32/Ramnit and the exploit family Win32/CplLnk were the most commonly encountered threat families in Indonesia in 4Q13.
- The encounter rate in India increased significantly over the course of the year, from 39.9 percent in 1Q13 to 49.9 percent in 4Q13. Rotbrow, Brantall, and Gamarue were the most commonly encountered families in India in 4Q13.

> Infection rates in 4Q13 were heavily influenced by Rotbrow and Brantall.

- Infection rates in 4Q13 were heavily influenced by detections of Rotbrow and Brantall. See "A trio of threats makes waves in 4Q13" on page 42 for more information about these families and their impact on infection rates.

- Martinique experienced the highest CCM of any location in 4Q13, with an infection rate of 54.9, driven by the Rotbrow family's significantly high CCM at 44.3. Win32/Sefnit had the 2nd highest with a CCM of 8.0, followed by the worm families Win32/Brontok and Win32/Vobfus.
- Tunisia has the 2nd highest CCM in 4Q13, at 49.5. Rotbrow was the top family in 4Q13, with an infection rate of 36.1, followed by Sefnit at 6.2.
- The CCM for Albania increased considerably in 2H13, averaging 31.5, with the greatest contributor being Rotbrow at 25.5, followed by Sefnit with an infection rate of 5.6 in 4Q13. Gamarue and the virus family Win32/Sality were also prevalent in Albania.
- Pakistan saw a CCM of 35.8 in 4Q13, driven by Rotbrow at 14.0, followed by Sality and Gamarue.

- Yemen saw a CCM of 35.2 in 4Q13, mostly influenced by Rotbrow and Gamarue. The Ramnit and Sefnit families also influenced Yemen's infection rate.

Figure 25. Trends for locations with low malware encounter rates in 2H13 (100,000 reporting computers minimum)

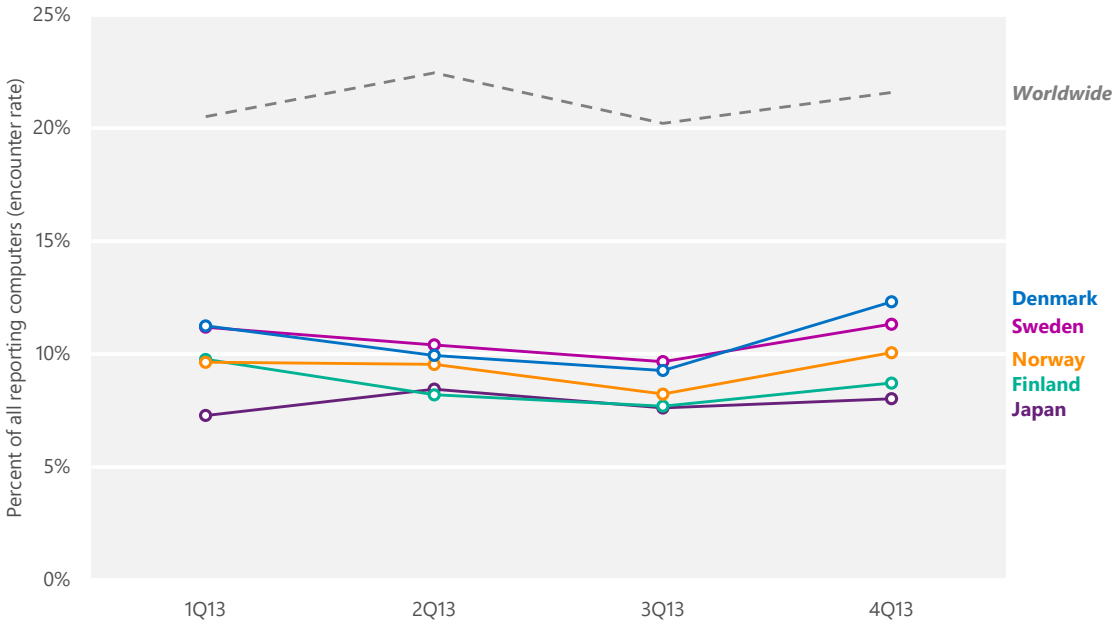
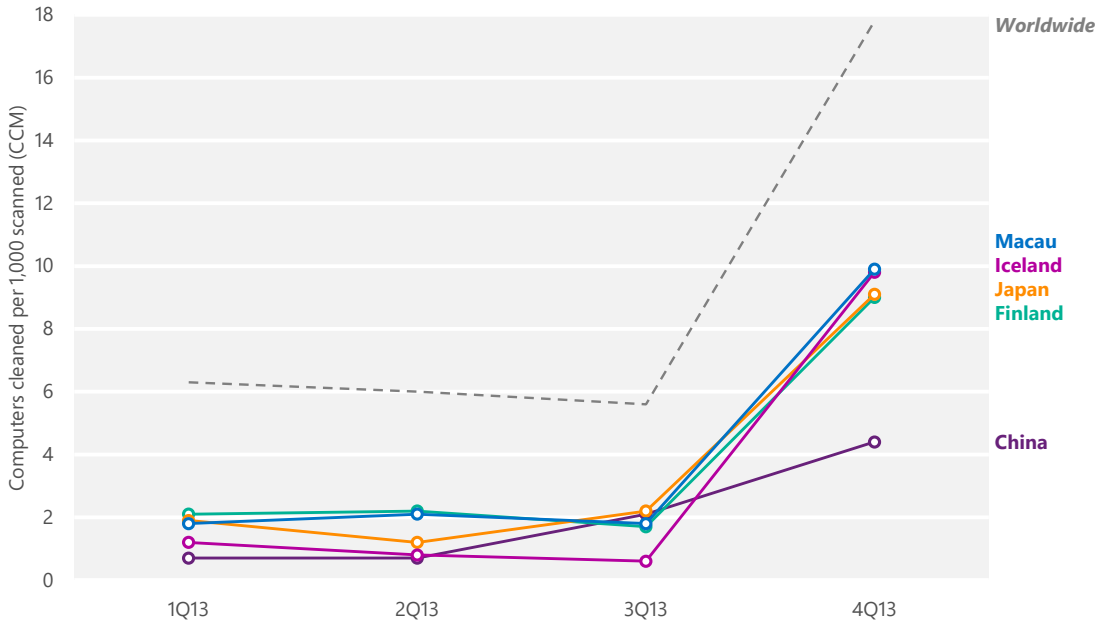


Figure 26. Trends for locations with low malware infection rates in 2H13, by CCM (100,000 reporting computers minimum)



- 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 2H13, these locations typically had encounter and infection rates between about one-third and one-half of the worldwide average. Nevertheless, most of these locations saw significant increases in 4Q13, due to the influence of Win32/Rotbrow and Win32/Brantall.
- The encounter rate in Japan remained stable throughout the year, totaling between about 7 and 8 percent in each quarter. After Rotbrow and Brantall, the most commonly encountered family in Japan in 4Q13 was JS/Urntone, a detection for a web page from an exploit kit called Neutrino that includes a redirector, a traffic distribution system, a domain rotator, a landing page, and a collection of browser exploits.[9]
- Rotbrow, Brantall, and the generic detection Win32/Obfuscator were the most commonly detected threat families in Denmark, Finland, Norway, and Sweden in 4Q13.
- China was affected less by Rotbrow and Brantall than many other locations were, but the infection rate in China still increased in 2H13, from 2.1 in 3Q13 to 4.4 in 4Q13, in part because of the password stealer Win32/Frethog. Frethog is a large family of password-stealing trojans that target confidential data such as account information from multiplayer online games, including World of Warcraft, Hao Fang Battle Net, Lineage, and A Chinese Odyssey.

> The Nordic countries and Japan perennially have some of the lowest infection rates in the world.

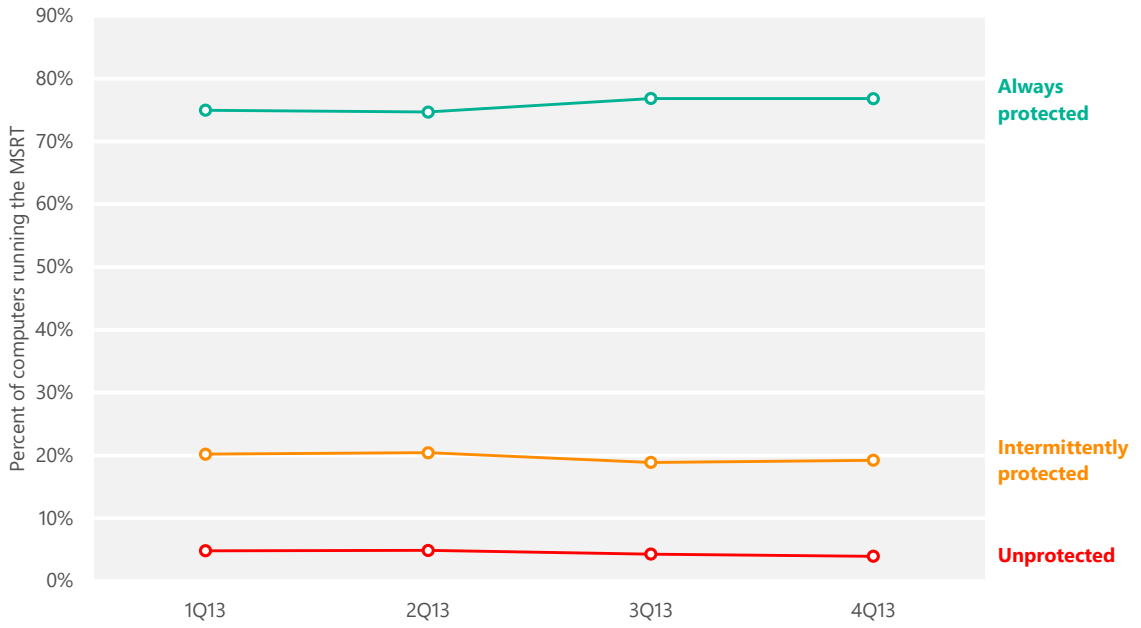
Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on the computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry makes it possible to analyze security software usage patterns around the world and correlate them with infection rates. Figure 27 shows the percentage of computers worldwide that the MSRT found to be protected or unprotected by real-time security software each quarter in 2013.

---

[9] For information and insights about fighting malware in Japan, see the entry "Microsoft Security Intelligence Report volume 14 on the Road: Japan" (May 6, 2013) at the MMPC blog at blogs.technet.com/mmpc.

Figure 27. Percentage of computers worldwide protected by real-time security software in 2013

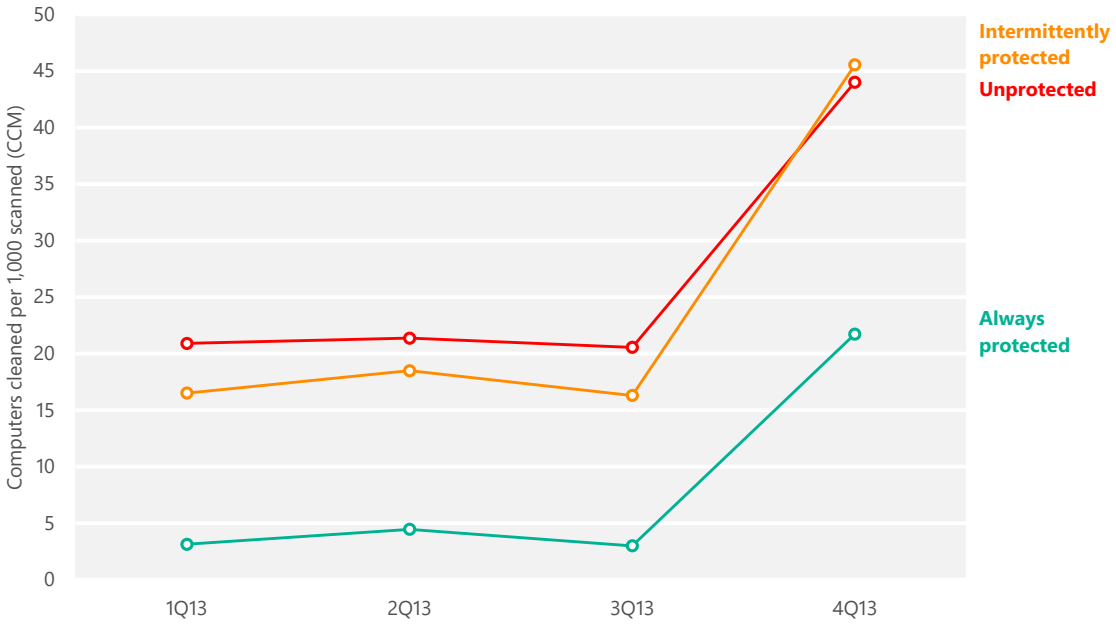


About three-quarters of computers world-wide consistently run real-time security software.

- A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In Figure 27, "Always 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. The trend increased slightly over the four quarters, from 75.0 percent in 1Q13 to 76.8 percent in 4Q13.
- Of the computers that did not always have active protection, most were found to be running real-time security software during at least one of their three monthly MSRT executions. Intermittently protected computers accounted for between 18.9 and 20.4 percent of computers worldwide each quarter, and computers that never reported running security software accounted for between 3.9 and 4.9 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 28 compares infection rates with protection levels worldwide for each of the last four quarters.

Figure 28. Infection rates for protected and unprotected computers in 2013



- The MSRT reported that computers that were never found to be running real-time security software during 3Q13 were 6.7 times as likely to be infected with malware as computers that were always found to be protected.
- The infection rate increased significantly for both protected and unprotected computers in 4Q13 following the emergence of malicious behavior in the trojan dropper family Win32/Rotbrow, which led to the removal of a backlog of files that had not previously been considered malware. (See "A trio of threats makes waves in 4Q13" on page 42 for more information about Rotbrow and the 4Q13 infection rate increase.) Nevertheless, unprotected computers were still twice as likely to be infected with malware in 4Q13 as computers that were always found to be protected.
- Computers that were intermittently protected were 5.4 times as likely to be infected with malware in 3Q13 as computers that were always protected—a ratio nearly as

> Computers that didn't run real-time security software were 6.7 times as likely to be infected as computers that did.

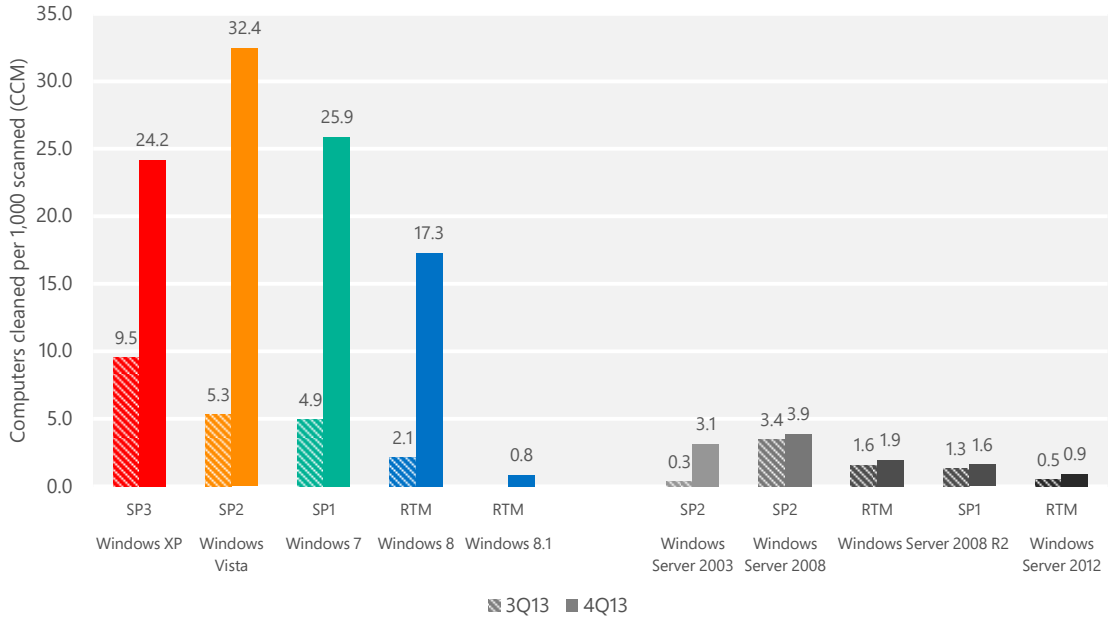
great as that for computers that were never found to be protected. Like unprotected computers, intermittently protected computers were about twice as likely to be infected in 4Q13 as computers that were always protected.

- 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. 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 28 illustrates.

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 29 shows the infection rate for each currently supported Windows operating system/service pack combination.

Figure 29. Infection rate (CCM) by operating system and service pack in 3Q13 and 4Q13



SP = Service Pack. RTM = Release to manufacturing. Support for Windows XP ended April 8, 2014, after the end of 4Q13. CCM figures are expected to return to more typical levels in 2014.

- 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 XP SP3 computers to 1,000 Windows 8 RTM computers).
- Infection rates in 4Q13 were many times higher on all supported Windows client platforms than they were in 3Q13, because of the influence of Win32/Rotbrow. CCM figures are expected to return to more typical levels in 2014. See "A trio of threats makes waves in 4Q13" on page 42 for more information about Rotbrow and its effect on 4Q13 encounter rates.
- 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. In 3Q13, this pattern is clearly visible, with Windows XP displaying an infection rate significantly higher than any other supported Windows client platform, and Windows 8 RTM—at the time the most recently released platform—displaying the lowest. In 4Q13, the typical pattern is affected by the elevated infection rates caused by Rotbrow, as Windows Vista SP2 displayed a slightly higher infection rate than Windows XP SP3.

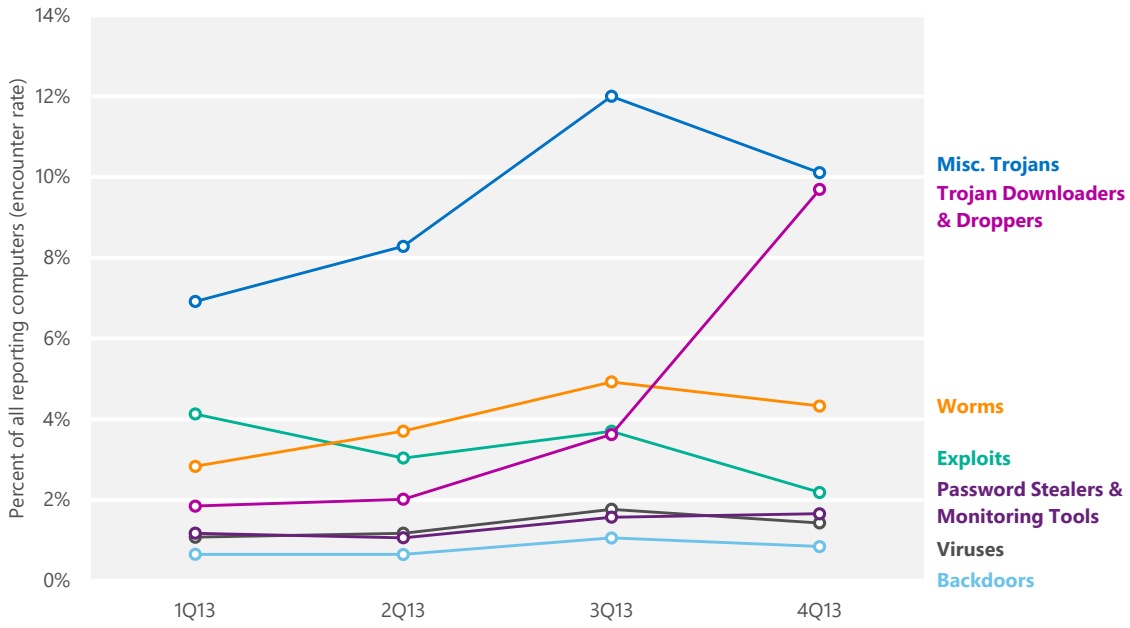
> Infection rates on all platforms were many times higher in 4Q13 due to Rotbrow.

- As in previous periods, infection rates tend to be significantly 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.

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 seven categories based on similarities in function and purpose.

Figure 30. Encounter rates by threat category in 2013



- Totals for each time period may exceed 100 percent because some computers report more than one category of threat in each time period.
- The Miscellaneous Trojans category remained the most commonly encountered threat category in 2H13; its encounter rate peaked at 12.0 percent of reporting computers in 3Q13, more than double that of any other category. The generic detection Win32/Obfuscator was the most commonly encountered threat in this category, with an encounter rate of 2.37 percent in 3Q13 and 1.94 percent in 4Q13. Win32/Sefnit and the trojan variants of

the Autorun family were the 2nd and 3rd most commonly detected threats in the category in 2H13; as with Obfuscator, detections of both families declined in 4Q13.

- The Trojan Downloaders & Droppers category increased significantly in 4Q13 to become the 2nd most commonly encountered category in 4Q13, led by Win32/Rotbrow (5.90 percent in 4Q13) and Win32/Brantall (3.55 percent). See "A trio of threats makes waves in 4Q13" on page 42 for more information about these families.
- The encounter rate for worms trended up to 4.93 percent in 3Q , then fell slightly to 4.33 percent in 4Q, influenced by declines in Win32/Gamarue, Autorun, and Win32/Dorkbot.
- The encounter rate for the Exploits category decreased in 4Q13 after increasing slightly in 3Q13. Exploit families HTML/IframeRef, Java/CVE-2012-1723, and Blacole all declined in 4Q13, which influenced the overall decrease.

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 and its effectiveness are highly dependent on language and cultural 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 31 shows the relative prevalence of different categories of malware in several locations around the world in 4Q13.

Figure 31. Threat category prevalence worldwide and in the 10 locations with the most computers reporting detections in 4Q13

Category	Worldwide	United States	Brazil	Germany	Japan	United Kingdom	France	Russia	Canada	Italy	China
Misc. Trojans	10.1%	5.4%	16.8%	7.2%	2.5%	6.4%	11.2%	18.3%	6.2%	12.9%	11.5%
Trojan Downloaders & Droppers	9.7%	5.1%	21.5%	8.5%	4.4%	9.8%	17.5%	5.6%	6.2%	14.3%	2.2%
Worms	4.3%	0.6%	9.3%	1.0%	0.6%	0.9%	1.9%	4.2%	0.5%	3.1%	3.5%
Exploits	2.2%	2.2%	1.5%	1.8%	1.1%	1.8%	2.4%	1.9%	2.4%	2.4%	1.4%
Password Stealers & Monitoring Tools	1.7%	1.0%	4.1%	1.0%	0.6%	1.2%	1.0%	1.4%	1.1%	1.9%	0.7%
Viruses	1.4%	0.4%	2.1%	0.3%	0.1%	0.3%	0.4%	1.3%	0.3%	0.8%	3.7%
Backdoors	0.8%	0.3%	1.0%	0.3%	0.2%	0.7%	0.6%	0.9%	0.4%	1.0%	1.8%

- Within each row of Figure 31, 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 21 on page 47, the locations in the table are ordered by number of computers reporting detections in 2H13.
- Brazil, Russia, and France saw higher encounter rates across most threat categories than the other locations in Figure 31.
- Russia had the highest Miscellaneous Trojans encounter rate in Figure 31, at 18.3 percent. Brazil was second, with an encounter rate of 16.8 percent, followed by Italy at 12.9 percent.
- Brazil had the highest encounter rates in the Trojan Downloaders category at 21.5 percent, followed by France at 17.5 percent and Italy at 14.3 percent
- Worms continued to be a strong category in some locations, led by Brazil at 9.3 percent. Worm encounters were also prevalent in Russia at 4.2 percent and China at 3.5 percent.

See "Appendix C: Worldwide infection rates" in the full report for more information about malware around the world.

Threat families

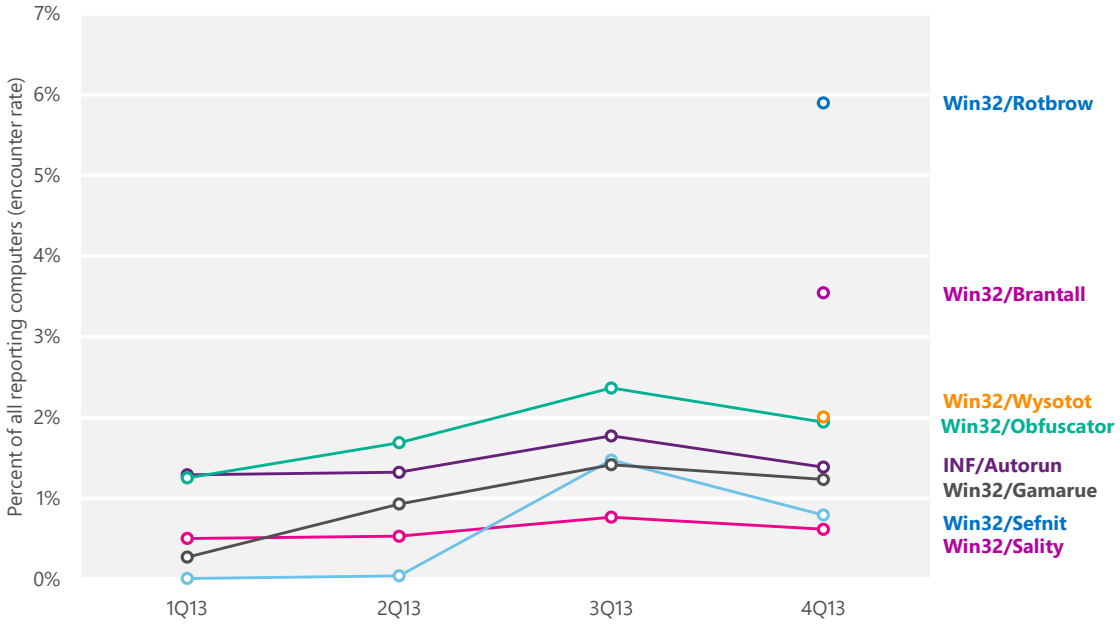
Figure 32 lists the top 10 malware families that were detected on computers by Microsoft real-time antimalware products worldwide in 2H13, with other quarters included for comparison.

Figure 32. Quarterly trends for the top 10 malware families encountered by Microsoft real-time antimalware products in 2H13, shaded according to relative encounter rate

	Family	Most significant category	1Q13	2Q13	3Q13	4Q13
1	Win32/Rotbrow	Trojan Downloaders & Droppers	—	—	—	5.90%
2	Win32/Obfuscator	Miscellaneous Trojans	1.25%	1.91%	2.37%	1.94%
3	Win32/Brantall	Trojan Downloaders & Droppers	—	—	—	3.55%
4	INF/Autorun	Worms	1.29%	1.49%	1.77%	1.39%
5	Win32/Gamarue	Worms	0.27%	1.05%	1.42%	1.23%
6	Win32/Sefnit	Miscellaneous Trojans	0.01%	0.05%	1.47%	0.79%
7	Win32/Wysotot	Miscellaneous Trojans	—	—	—	2.01%
8	Win32/Sirefef	Miscellaneous Trojans	1.10%	0.96%	1.06%	0.54%
9	Win32/Sality	Viruses	0.50%	0.60%	0.77%	0.62%
10	Win32/Ramnit	Miscellaneous Trojans	0.45%	0.56%	0.73%	0.60%

For a different perspective on some of the changes that have occurred throughout the year, Figure 33 shows the detection trends for a number of families that increased or decreased significantly over the past four quarters.

Figure 33. Detection trends for a number of notable malware families in 2013



- Four of the most commonly encountered families in 2H13—Win32/Rotbrow, Win32/Brantall, Win32/Wysotot, and Win32/Sefnit—were either new or reappeared after a significant period of dormancy. See "A trio of threats makes waves in 4Q13" on page 42 for more information about Rotbrow, Brantall, and Sefnit.
- Wysotot is a family of trojans that change the start page of the user's web browser. It is usually installed by software bundlers that advertise free software or games. Wysotot was first detected in October 2013, and detection signatures were added to the MSRT in March 2014. For more information about Wysotot, see the entry "MSRT March 2014 – Wysotot" (March 11, 2014) in the MMPC blog at blogs.technet.com/mmpc.
- Win32/Obfuscator, the 2nd most commonly encountered threat in 2H13, 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 keeps the same functionality as the original program but with different code, data, and geometry.

- INF/Autorun, the 4th 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. Changes to the feature have made this technique less effective, but attackers continue to distribute malware that attempts to target it and Microsoft antimalware products detect and block these attempts, even when they would not be successful.
- Win32/Gamarue, the 5th most commonly encountered threat in 2H13, 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)

> Four of the top families in 2H13 were new or reappeared after a significant period of dormancy.

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. Figure 34 demonstrates how detections of the most prevalent families in 4Q13 ranked differently on different operating system/service pack combinations.

Figure 34. The malware families most commonly encountered by Microsoft real-time antimalware solutions in 4Q13, and how they ranked in prevalence on different platforms

Rank 4Q13	Family	Most significant category	Rank (Windows 8.1 RTM)	Rank (Windows 8 RTM)	Rank (Windows 7 SP1)	Rank (Windows Vista SP2)	Rank (Windows XP SP3)
1	Win32/Rotbrow	Trojan Downloaders & Droppers	2	1	1	1	1
2	Win32/Brantall	Trojan Downloaders & Droppers	3	2	2	2	2
3	Win32/Wysotot	Misc. Trojans	4	4	4	3	4
4	Win32/Obfuscator	Misc. Trojans	1	3	3	7	8
5	INF/Autorun	Worms	5	5	5	16	3
6	Win32/Gamarue	Worms	7	6	6	21	5
7	VBS/Jenxcus	Worms	9	7	7	29	10
8	Win32/Sefnit	Misc. Trojans	24	9	8	8	9
9	Win32/Detplock	Misc. Trojans	23	10	9	5	11
10	JS/Urntone	Exploits	35	11	10	4	13

- The list of most commonly encountered families was largely consistent from platform to platform. Win32/Rotbrow, Win32/Brantall, and Win32/Wysotot, the top three families encountered worldwide in 4Q13, were all within the top four families encountered on each platform.
- Microsoft real-time antimalware products detect and block threats that attempt to infect computers even if those attempts would not otherwise succeed. The generic family INF/Autorun, which propagates using a technique that is ineffective on Windows 7, Windows 8, and Windows 8.1, was nevertheless the 5th most commonly encountered threat family on all three platforms in 4Q13.[10]
- Autorun, the virus family Win32/Sality, and the worm family Win32/Conficker were all encountered more frequently on Windows XP than on any other platform.

[10] Recent changes to Windows XP and Windows Vista, which have been available as automatic updates on Microsoft update services since 2011, make the technique ineffective on those platforms as well. See support.microsoft.com/kb/971029 for more information.

- The trojan family JS/Faceliker and the generic detection Win32/Malagent were ranked higher on Windows 8 and on Windows 8.1 than on other platforms.

Rogue security software

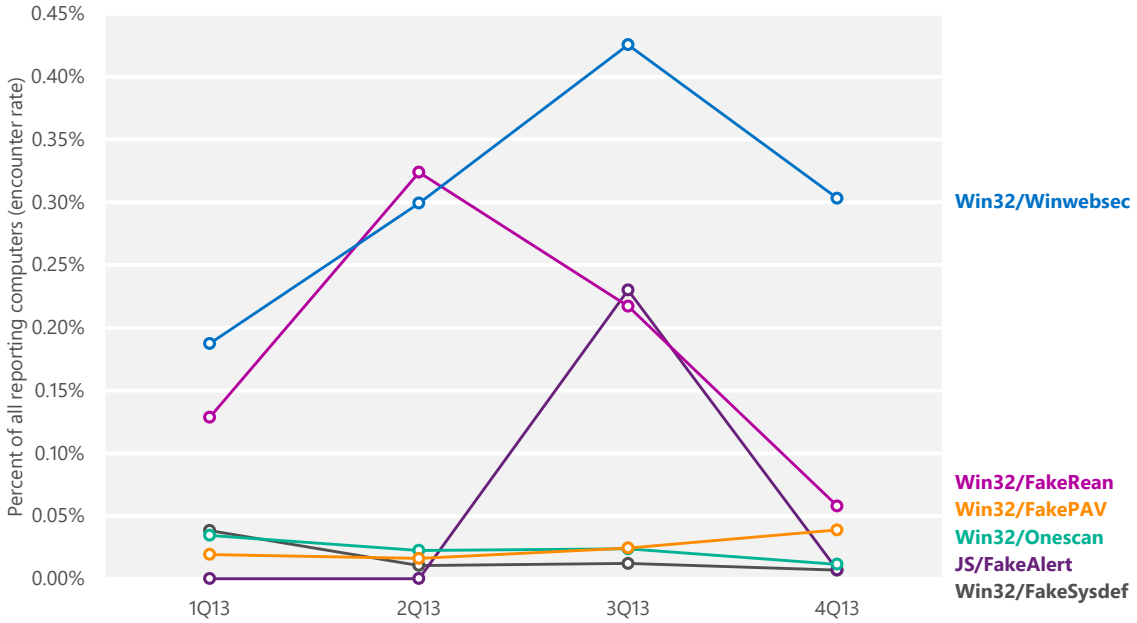
Rogue security software has become one of the most common methods that attackers use to swindle money from victims. Rogue security software, also known as *scareware*, is software that appears to be beneficial from a security perspective but provides limited or no security, generates erroneous or misleading alerts, or attempts to lure users into participating in fraudulent transactions. These programs typically mimic the general look and feel of legitimate security software programs and claim to detect a large number of nonexistent threats while urging users to pay for the so-called "full version" of the software to remove the nonexistent threats.

Attackers typically install rogue security software programs through exploits or other malware, or use social engineering to trick users into believing the programs are legitimate and useful. Some versions emulate the appearance of the Windows Security Center or unlawfully use trademarks and icons to misrepresent themselves. (See www.microsoft.com/security/resources/videos.aspx for an informative series of videos designed to educate general audiences about rogue security software.)

Figure 35. False branding used by a number of commonly detected rogue security software programs

Figure 36 shows detection trends for the most common rogue security software families detected in 2H13.

Figure 36. Trends for the most commonly encountered rogue security software families in 2H13, by quarter



- Win32/Winwebsec, the most commonly encountered rogue security software family in 2H13, has been distributed under a variety of names, with the user interface and other details changing to reflect each variant's individual branding; currently prevalent names include Antiviral Factory 2013, Attentive Antivirus, System Doctor 2014, Win 8 Security System, and several others. These different distributions of the trojan use various installation methods, with file names and system modifications that can differ from one variant to the next.

Rogue security software generates false or misleading alerts to lure users into paying.

- Win32/FakeRean, the 2nd most commonly encountered rogue security software program in 2H13, has been distributed since 2008 under several different names, which are often generated at random based upon the operating system of the affected computer. Its distributors tend to concentrate their efforts into short-term campaigns during which they propagate FakeRean at high volumes, followed by periods of inactivity.
- Win32/Onescan is a Korean-language rogue security software programs. Onescan was a significant threat in Korea for a number of years, but encounters have declined in 2013 to much lower levels. In recent months, the authors of Onescan have shifted their focus from rogue security software to computer optimization software; at the time this report was

prepared, the computer optimization software has not been observed to be associated with malware.

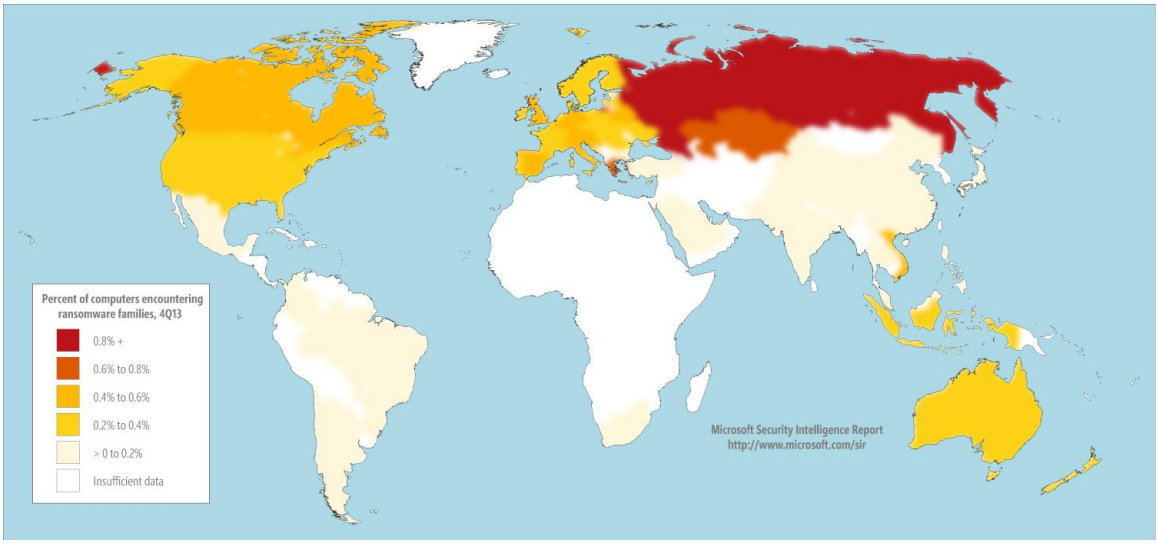
Ransomware

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

Ransomware affects different parts of the world unequally. Figure 38 shows encounter rates for ransomware families by country and region in 4Q13.

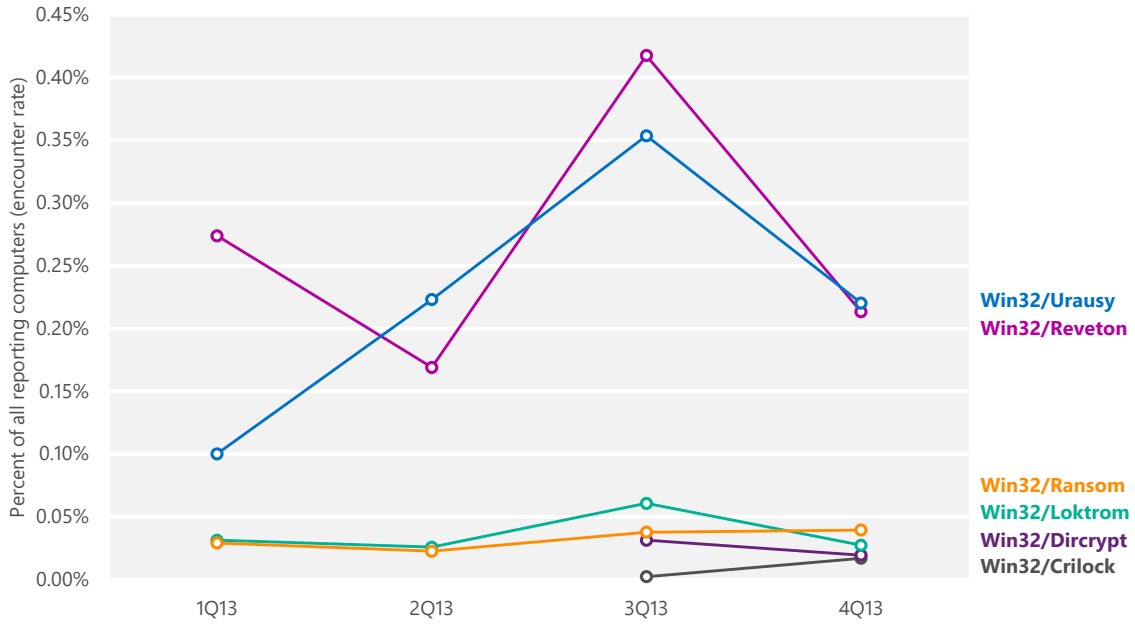
Figure 38. Encounter rates for ransomware families by country/region in 4Q13



- The location with the highest ransomware encounter rate in 4Q13 was Russia (1.62 percent), followed by Kazakhstan (0.73 percent) and Greece (0.63 percent).
- Unlike with most other types of malware, the distribution of ransomware has been very concentrated geographically, with almost all ransomware encounters taking place in Europe, western Asia, and the wealthy English-speaking regions of North America and Oceania. Ransomware encounters were virtually unknown in Latin America, Africa, the Middle East, and eastern and southern Asia.

Figure 39 displays encounter rate trends for several of the most commonly encountered ransomware families worldwide.

Figure 39. Trends for several commonly encountered ransomware families in 2H13, by quarter



- Win32/Reveton was the most commonly encountered ransomware family worldwide in 2H13. 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.

Encounter rates for Reveton were highest in Italy (0.71 percent in 4Q12), Belgium (0.66 percent), and Spain (0.64 percent).

For additional information about Reveton, see the entry "Revenge of the Reveton" (April 18, 2012) in the MMPC blog at blogs.technet.com/mmpc.

Ransomware often masquerades as an official warning from a law enforcement agency.

- Win32/Urausy, the 2nd most prevalent ransomware family worldwide in 2H13, was also most prevalent in Europe. The encounter rate for Urausy peaked in 3Q13 at 0.35 percent, then dropped to 0.22 percent in 4Q13.
- Win32/Crilock, also known as Cryptolocker, received significant media attention in 2013, but was only the 7th most commonly encountered ransomware family in 2H13, with an encounter rate of 0.02 percent in 4Q13. First detected in September 2013, Crilock is often distributed as an email attachment and can spread to other computers via removable drives. After it is installed, Crilock encrypts files of certain popular types, such as photos and Microsoft Office documents, with a unique public key. It then displays a screen demanding that the computer user pay a ransom by a certain date to receive the private key that will supposedly decode the user's files. If the user does not pay by the deadline, the screen says, the attacker will delete the private key permanently.

  Because removing the Crilock 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 Crilock or a similar threat family. For more information, see the entry "Backup the best defense against (Cri)locked files" (November 19, 2013) on the MMPC blog at blogs.technet.com/mmpc.

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.

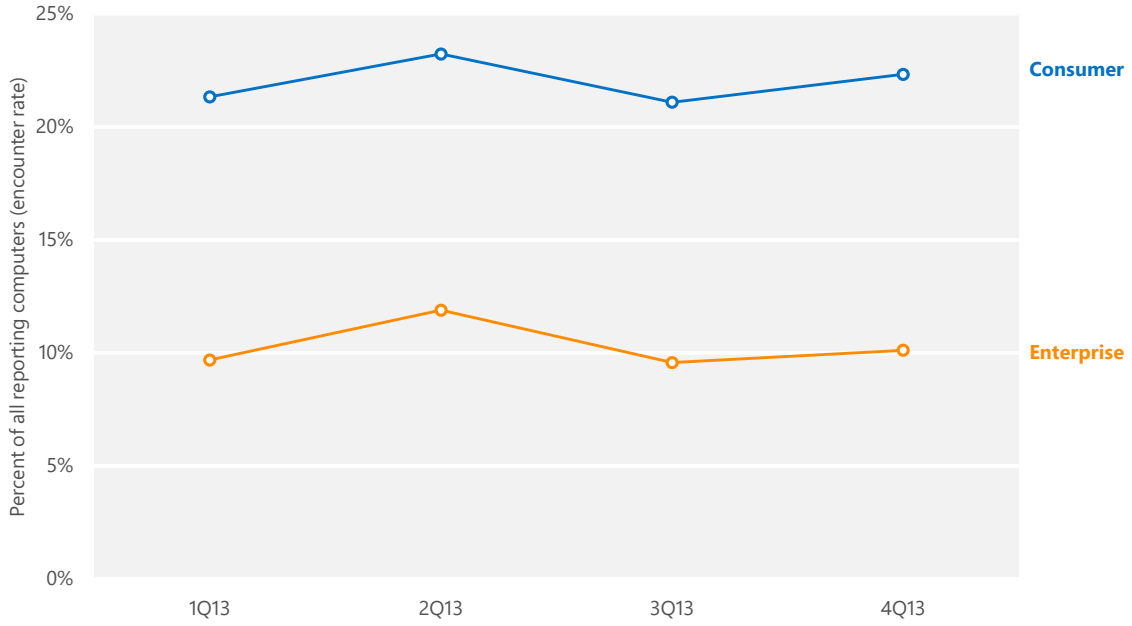
Visit www.microsoft.com/security/portal/mmpc/shared/ransomware.aspx for more information about ransomware and how computer users can avoid being taken advantage of by these threats.

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 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 40. Malware encounter rates for consumer and enterprise computers in 2013



- 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 40 shows, the encounter rate for consumer computers was about 2.2 times as high as the rate for enterprise computers in both 3Q13 and 4Q13.

Figure 41 and Figure 42 list the top 10 families detected on domain-joined and non-domain computers, respectively, in 2H13.

Figure 41. Quarterly trends for the top 10 families detected on domain-joined computers in 2H13, by percentage of computers encountering each family

Family	Most significant category	3Q13	4Q13
Win32/Conficker	Worms	0.85%	0.87%
INF/Autorun	Worms	0.75%	0.73%
Win32/Rotbrow	Trojan Downloaders & Droppers	—	1.43%
Win32/Sirefef	Miscellaneous Trojans	0.73%	0.45%
Win32/Gamarue	Worms	0.49%	0.51%
Win32/Zbot	Password Stealers & Monitoring Tools	0.47%	0.45%
Win32/Brantall	Trojan Downloaders & Droppers	—	0.91%
HTML/IframeRef	Miscellaneous Trojans	0.61%	0.22%
Win32/Obfuscator	Miscellaneous Trojans	0.36%	0.36%
Java/CVE-2012-1723	Exploits	0.47%	0.24%

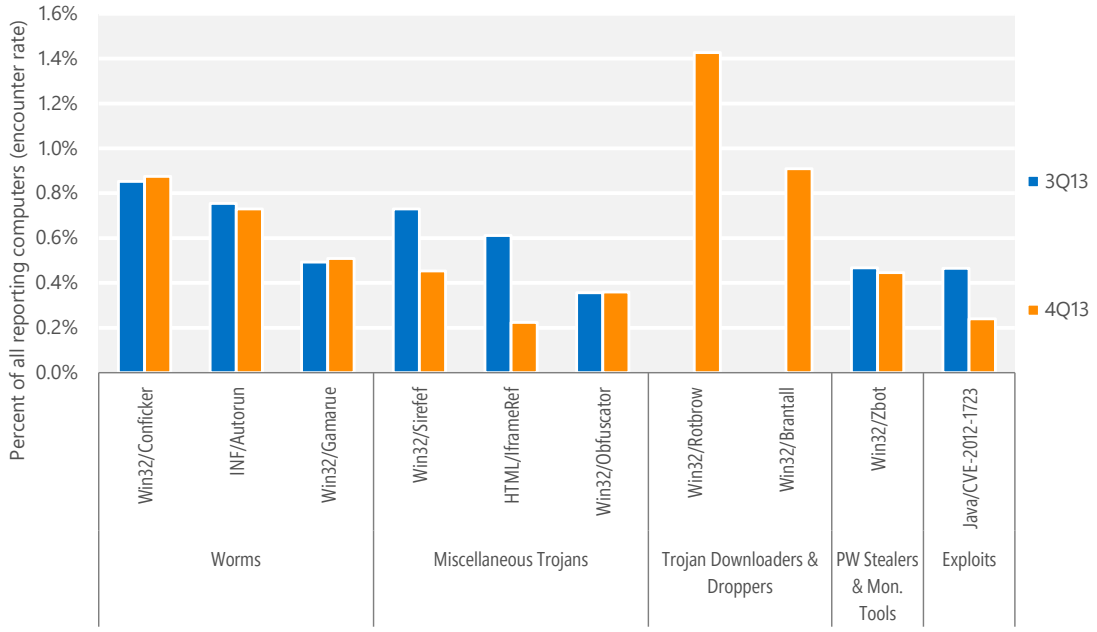
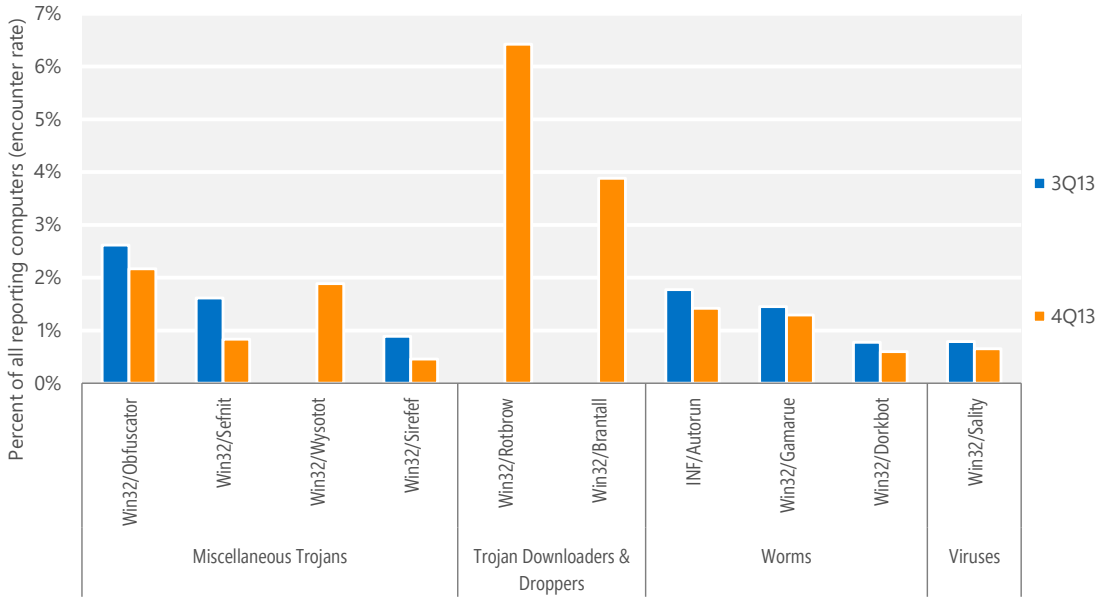


Figure 42. Quarterly trends for the top 10 families detected on non-domain computers in 2H13, by percentage of computers encountering each family

Family	Most significant category	3Q13	4Q13
Win32/Rotbrow	Trojan Downloaders & Droppers	—	6.42%
Win32/Obfuscator	Miscellaneous Trojans	2.62%	2.17%
Win32/Brantall	Trojan Downloaders & Droppers	—	3.88%
INF/Autorun	Worms	1.77%	1.42%
Win32/Gamarue	Worms	1.45%	1.29%
Win32/Sefnit	Miscellaneous Trojans	1.62%	0.84%
Win32/Wysotot	Miscellaneous Trojans	—	1.89%
Win32/Sality	Viruses	0.79%	0.65%
Win32/Dorkbot	Worms	0.78%	0.60%
Win32/Sirefef	Miscellaneous Trojans	0.89%	0.46%



- Five threats—INF/Autorun, Win32/Brantall, Win32/Gamarue, Win32/Obfuscator, and Win32/Rotbrow—were common to both lists. All were more frequently encountered on non-domain computers than on domain-joined computers. See "Threat families" on page 61 for more information about these families.

- Win32/Conficker, the most commonly encountered family on domain-joined computers in 2H13, is a worm that spreads by exploiting a vulnerability addressed by Security Bulletin MS08-067. It can also spread via network shares and removable drives, which are commonly used in domain environments.
- Win32/Zbot, the 6th most commonly encountered family on domain-joined computers in 2H13, is a family of password stealing trojans that also contains backdoor functionality. Zbot is installed on computers via spam email messages and hacked websites, or packaged with other malware families. Zbot has been observed downloading variants of Win32/Crilock, a ransomware family that encrypts files and demand money to unlock them. See "Ransomware" on page 67 for more information.
- Win32/Sefnit, the 6th most commonly encountered famiy on non-domain computers in 2H13, became significantly more active in 3Q13 after a long period of dormancy. Sefnit is a bot that allows a remote attacker to use the computer to perform various activities, using the Tor anonymity network to issue commands to the botnet. See "A trio of threats makes waves in 4Q13" on page 42 for more information about Sefnit and its relationship to Rotbrow and Brantall, two other major threats in 2H13.

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

See "Malware at Microsoft: Dealing with threats in the Microsoft environment" in the full report 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.

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 Protecting Against Malicious and Potentially Unwanted Software in the "Mitigating Risk" section of the *Microsoft Security Intelligence Report* website.

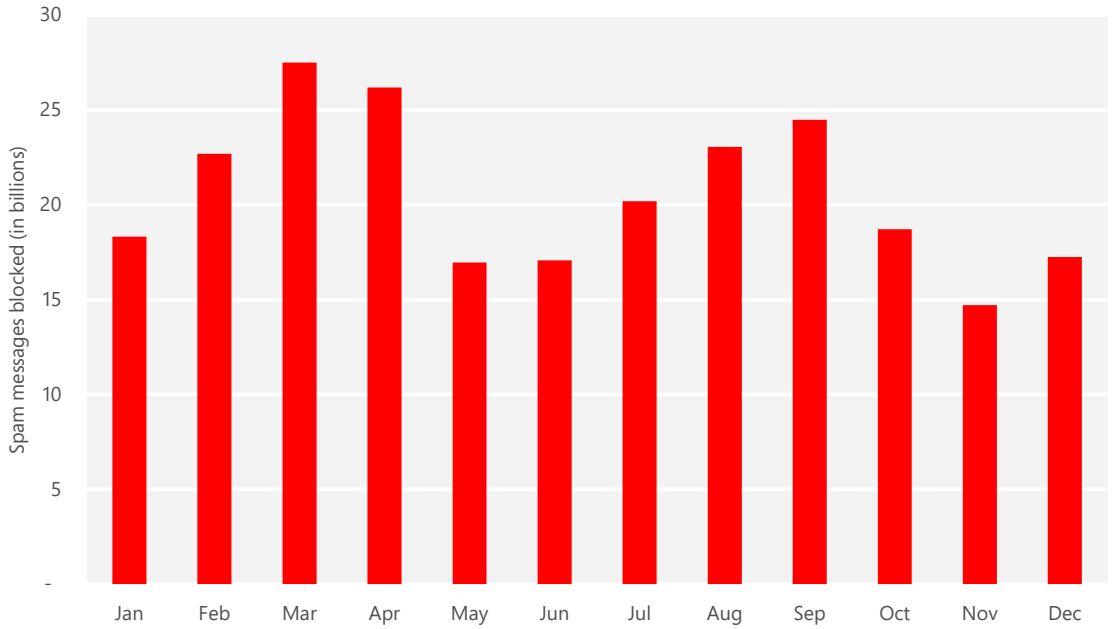
Email threats

More than 75 percent of the email messages sent over the Internet are unwanted. Not only does all this unwanted email tax recipients' inboxes and the resources of email providers, but it also creates an environment in which emailed malware attacks and phishing attempts can proliferate. Email providers, social networks, and other online communities have made blocking spam, phishing, and other email threats a top priority.

Spam messages blocked

The information in this section of the *Microsoft Security Intelligence Report* is compiled from telemetry data provided by Exchange Online Protection, which provides spam, phishing, and malware filtering services. Exchange Online Protection is used by tens of thousands of Microsoft enterprise customers that process tens of billions of messages each month.

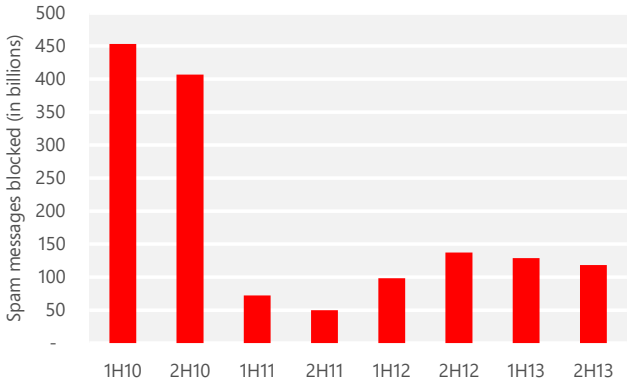
Figure 43. Messages blocked by Exchange Online Protection in 2013, by month



- Blocked mail volumes in 2H13 were consistent with 1H13, and remain well below levels seen prior to the end of 2010, as shown in Figure 44. The

dramatic decline in spam observed since 2010 has occurred in the wake of successful takedowns of a number of large spam-sending botnets, notably Cutwail (August 2010) and Rustock (March 2011).[11] In 2H13, Exchange Online Protection determined that about 1 in 4 email messages did not require blocking or filtering, compared to just 1 in 33 messages in 2010.

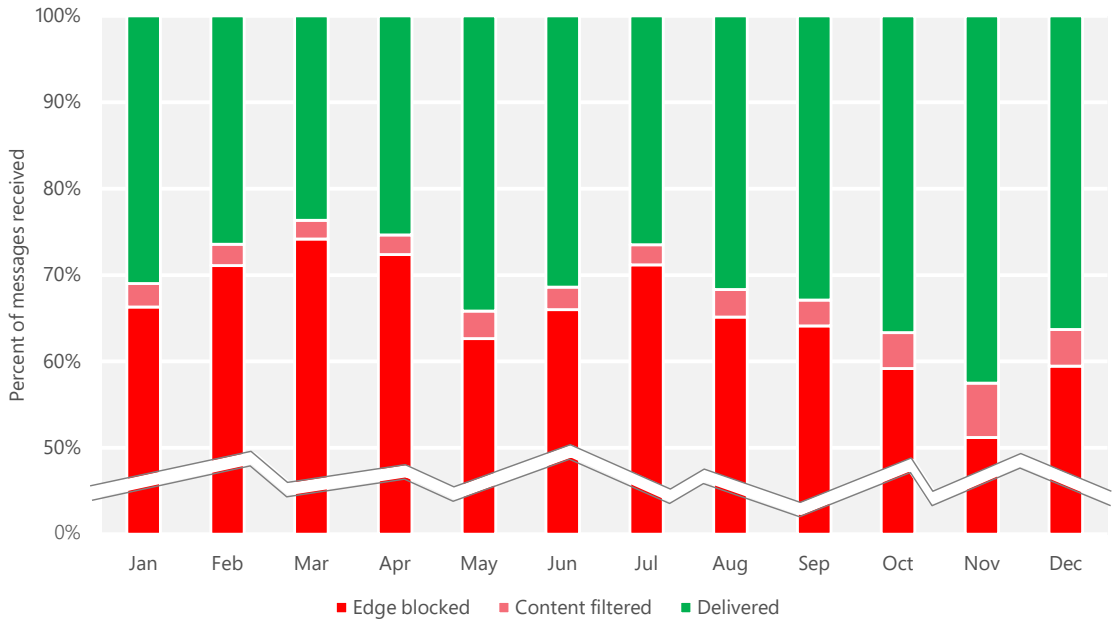
Figure 44. Messages blocked by Exchange Online Protection each half-year period, 1H10–2H13



Exchange Online Protection performs spam filtering in two stages. Most spam is blocked by servers at the network edge, which use reputation filtering and other non-content-based rules to block spam or other unwanted messages. Messages that are not blocked at the first stage are scanned using content-based rules, which detect and filter many additional email threats, including attachments that contain malware.

[11] For more information about the Cutwail takedown, see Microsoft Security Intelligence Report, Volume 10 (July-December 2010). For more information about the Rustock takedown, see "Battling the Rustock Threat," available from the Microsoft Download Center.

Figure 45. Percentages of incoming messages blocked, categorized as bulk email, and delivered, each month in 2013



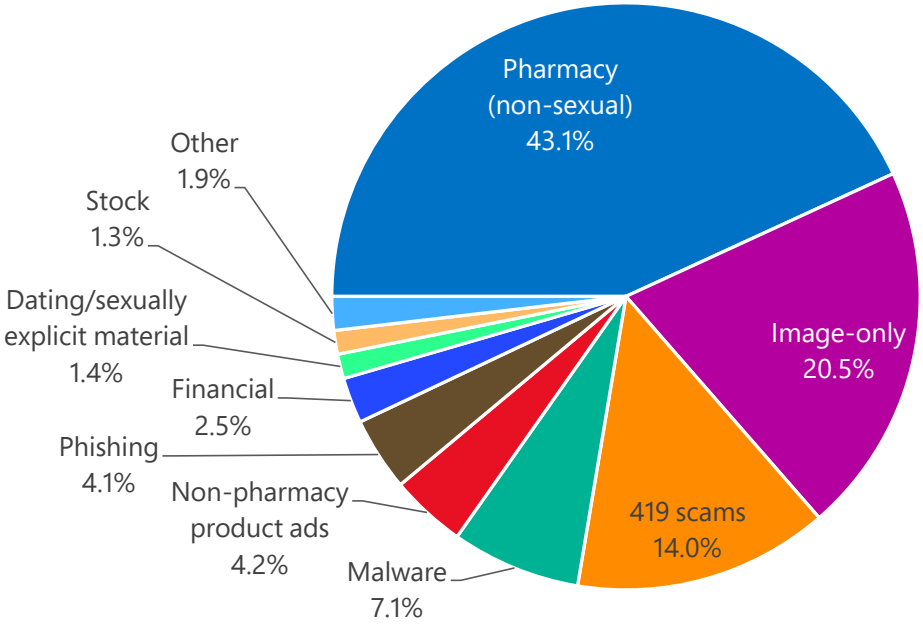
- Between 51.2 and 71.2 percent of incoming messages were blocked at the network edge each month in 2H13, which means that only 28.8 to 48.8 percent of incoming messages had to be subjected to the more resource-intensive content filtering process. Between 8.1 and 12.9 percent of the remaining messages (2.3 to 6.3 percent of all incoming messages) were filtered as spam each month.

Most incoming spam is blocked at the network edge.

Spam types

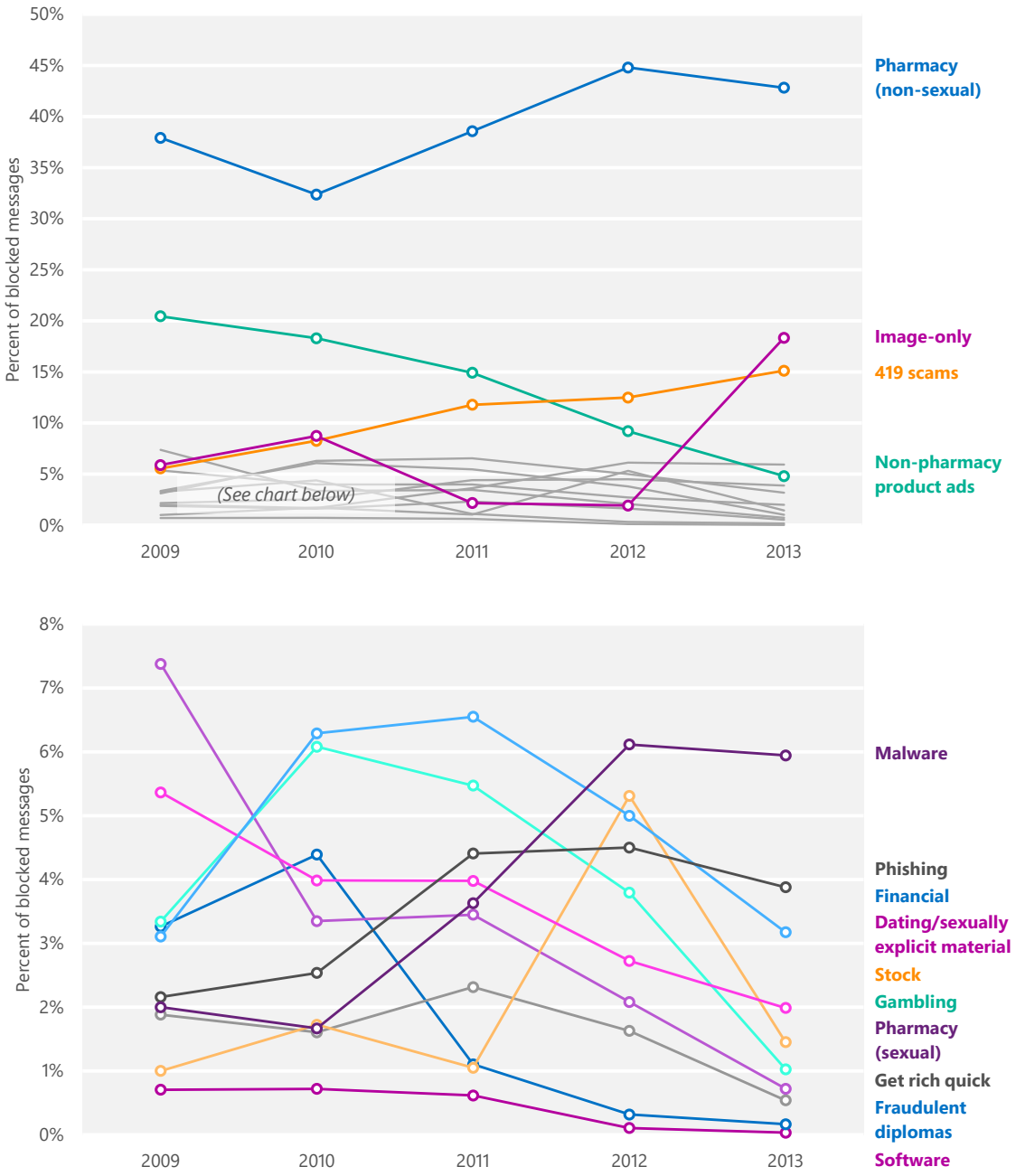
The Exchange Online Protection content filters recognize several different common types of spam messages. Figure 46 shows the relative prevalence of the spam types that were detected from July to October 2013.

Figure 46. Inbound messages blocked by Exchange Online Protection filters, July–October 2013, by category



- Advertisements for non-sexual pharmaceutical products accounted for 43.1 percent of the messages blocked by Exchange Online Protection content filters in 2H13, a slight increase from 42.7 percent in 1H13.
- Spam messages that include images and no text, which spammers sometimes send in an effort to evade detection by antispam software, increased to 20.5 percent of messages blocked in 2H13, up from 17.6 percent in 1H13.
- Spam messages associated with advance-fee fraud (known as *419 scams*) accounted for 14 percent of messages blocked, down slightly from 15.5 percent in 1H13. An advance-fee fraud is a common confidence trick in which the sender of a message purports to have a claim on a large sum of money but is unable to access it directly for some reason that typically involves bureaucratic red tape or political corruption. The sender asks the prospective victim for a temporary loan to be used for bribing officials or paying fees to get the full sum released. In exchange, the sender promises the target a share of the fortune, typically a much larger sum than the original loan, but does not deliver.

Figure 47. Inbound messages blocked by Exchange Online Protection content filters, 2009–2013, by category



- Advertisements for non-sexual pharmaceutical products have accounted for the largest share of spam for the past several years, and increase from about one-third of all spam in 2010 to almost one-half in 2012 and 2013.
- The volume of image-only spam increased significantly in 2013, accounting for the 2nd largest share of spam after two years below 3 percent. The

increase is due to large numbers of spam messages containing two images and a single line of text that began appearing in 2013, which are believed to be the work of a small number of prolific spammers.

- Most categories of spam decreased in 2H13, with 419 scams and image-only spam being the only categories that increased as a percentage of the total.
- Non-pharmacy product ads, sexually related pharmaceutical ads, fraudulent diploma ads, gambling-related ads, and ads for sexually explicit material or dating services all continued multi-year periods of declining percentages in 2013.

Guidance: Defending against threats in email

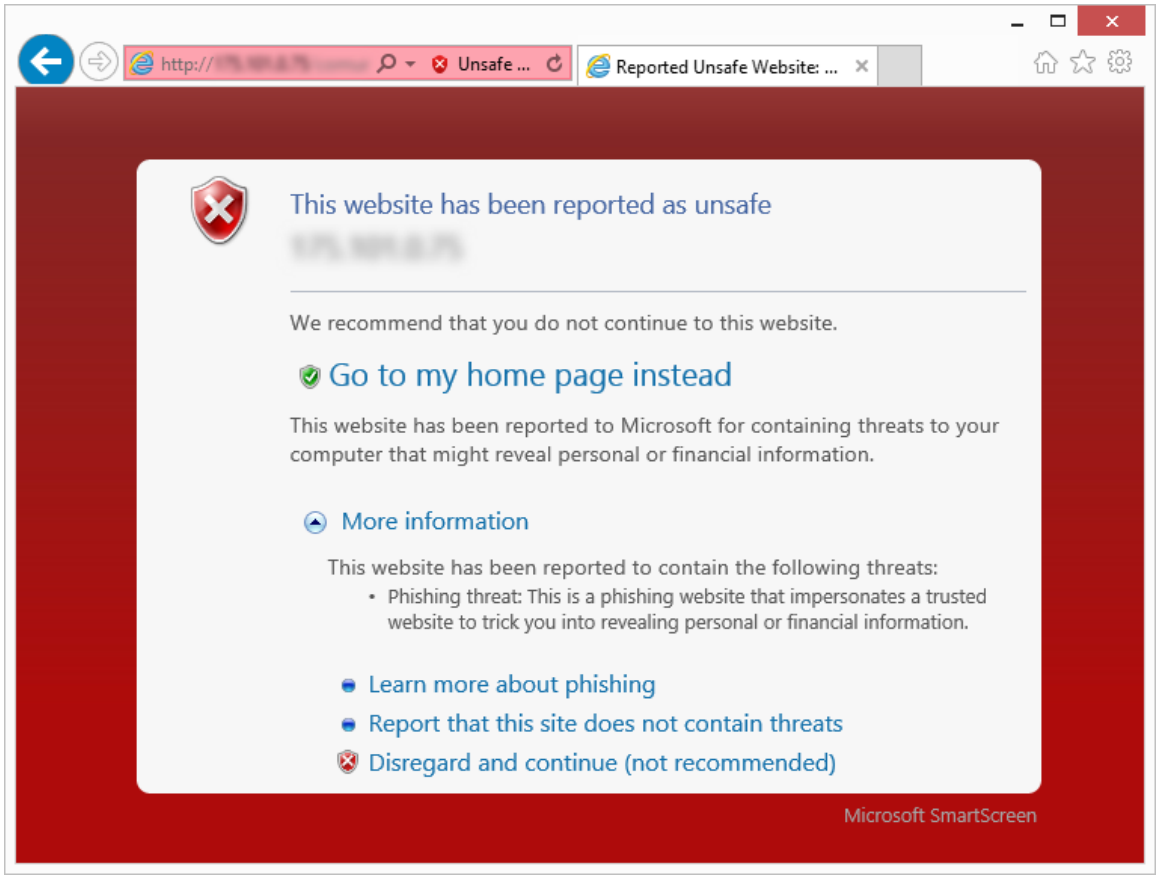
In addition to using a filtering service such as Exchange Online Protection, organizations can take a number of steps to reduce the risks and inconvenience of unwanted email. Such steps include implementing email authentication techniques and observing best practices for sending and receiving email. For in-depth guidance, see Guarding Against Email Threats in the "Managing Risk" section of the *Microsoft Security Intelligence Report* website at www.microsoft.com/sir.

Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear to be completely legitimate, and provide no outward indicators of their malicious nature even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques in efforts by attackers to take advantage of the trust users have invested in such sites. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information in this section is compiled from a variety of internal and external sources, including telemetry data produced by SmartScreen Filter (in Windows Internet Explorer versions 8 through 11) and the Phishing Filter (in Internet Explorer 7), from a database of known active phishing and malware hosting sites reported by users of Internet Explorer and other Microsoft products and services, and from malware data provided by Microsoft antimalware technologies. (See "Appendix B: Data sources" in the full report for more information about the products and services that provided data for this report.)

Figure 48. SmartScreen Filter in Internet Explorer blocks reported phishing and malware distribution sites to protect users



Phishing sites

Microsoft gathers information about phishing sites and impressions from *phishing impressions* that are generated by users who choose to enable the Phishing Filter or SmartScreen Filter in Internet Explorer. A phishing impression is a single instance of a user attempting to visit a known phishing site with Internet Explorer and being blocked, as illustrated in Figure 49.

Figure 49. How Microsoft tracks phishing impressions

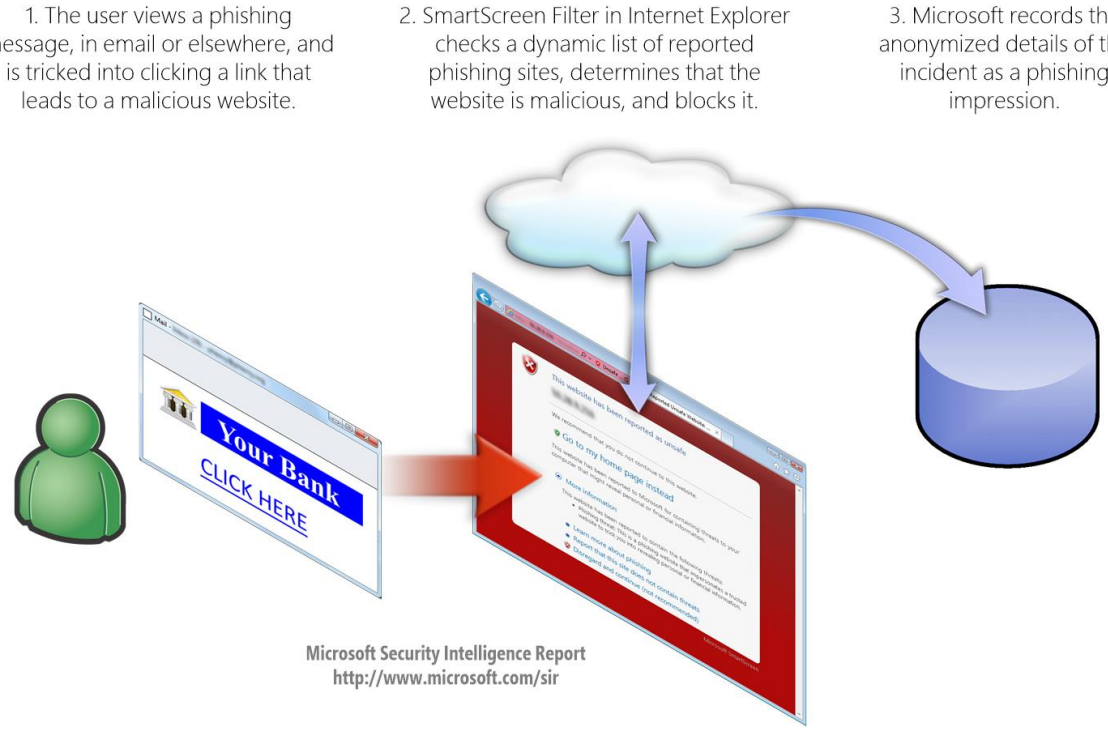
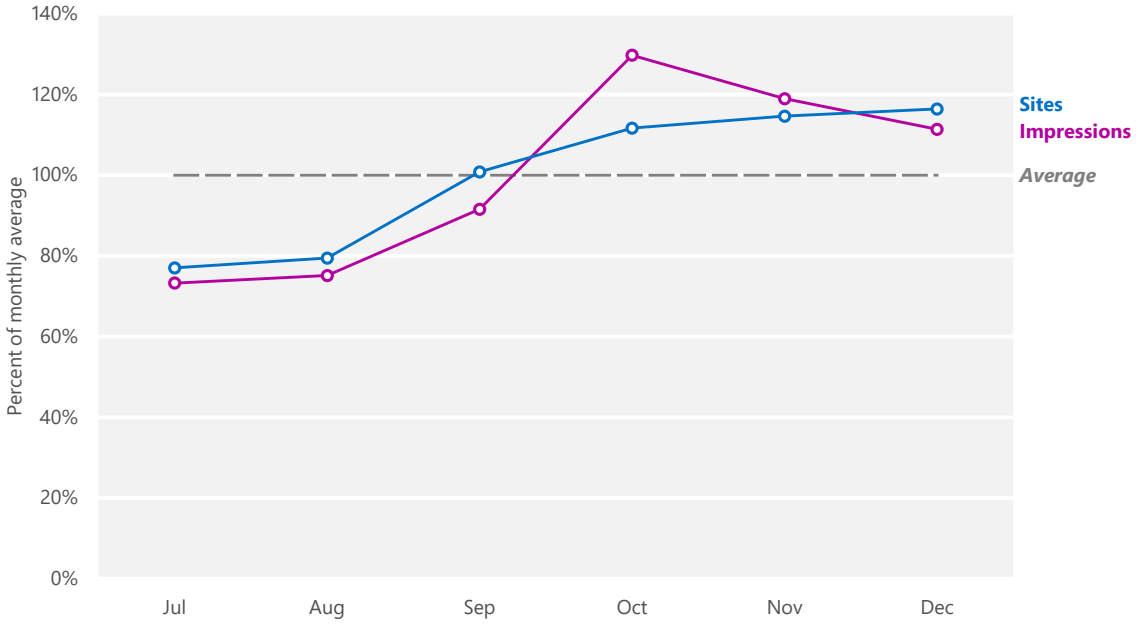


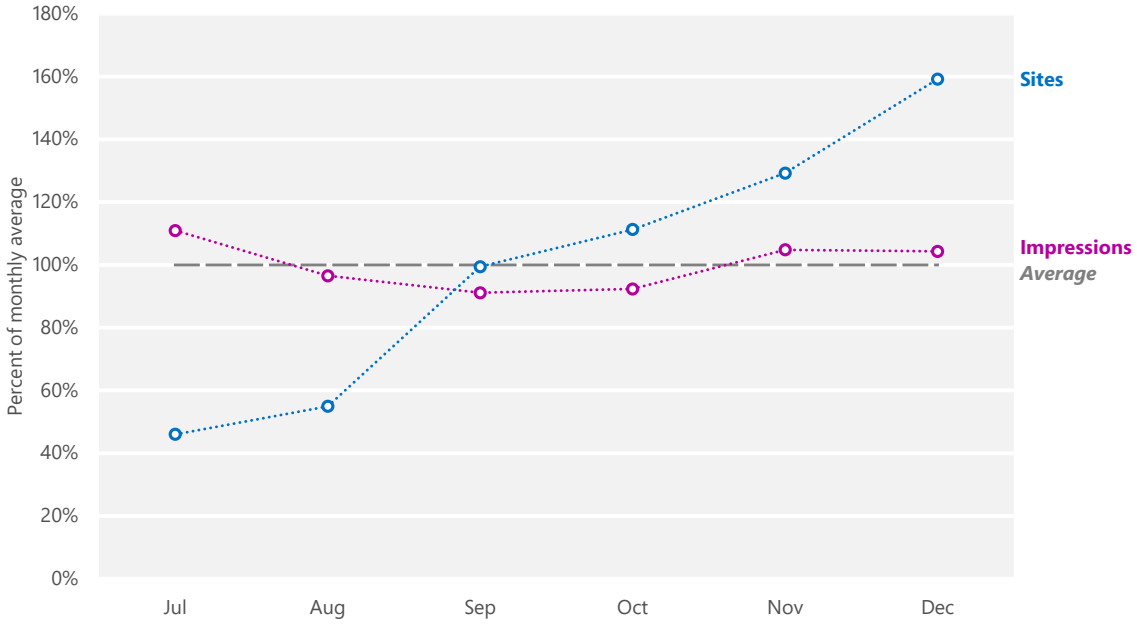
Figure 50 and Figure 51 illustrate the volume of phishing impressions tracked by SmartScreen Filter each month in 2H13 across all devices and on mobile devices running Windows Phone 8, compared to the volume of distinct phishing URLs visited.

Figure 50. Phishing sites and impressions reported by SmartScreen Filter across all devices, July–December 2013, relative to the monthly average for each



- The numbers of active phishing sites and impressions rarely correlate strongly with each other. Phishers sometimes engage in campaigns that temporarily drive more traffic to each phishing page without necessarily increasing the total number of active phishing pages they maintain at the same time. Sites and impressions both rose gradually throughout 3Q13, but total impressions peaked in October and declined through the end of the year, while the number of active sites continued to rise slowly.

Figure 51. Phishing sites and impressions reported by SmartScreen Filter on Windows Phone 8, July–December 2013, relative to the monthly average for each



- As mobile Internet usage grows, so does the volume of phishing impressions from mobile devices. Impressions reported by Internet Explorer running on Windows Phone 8 were stable month to month in 2H13, although they were spread over a larger number of active phishing sites each month than the one before.

Target institutions

Some types of sites tend to consistently draw many more impressions per site than others. The next four figures show the percentage of phishing impressions and unique phishing URLs visited each month from July to December 2013 for the most frequently targeted types of institutions.

Figure 52. Impressions across all devices for each type of phishing site, July–December 2013, as reported by SmartScreen Filter

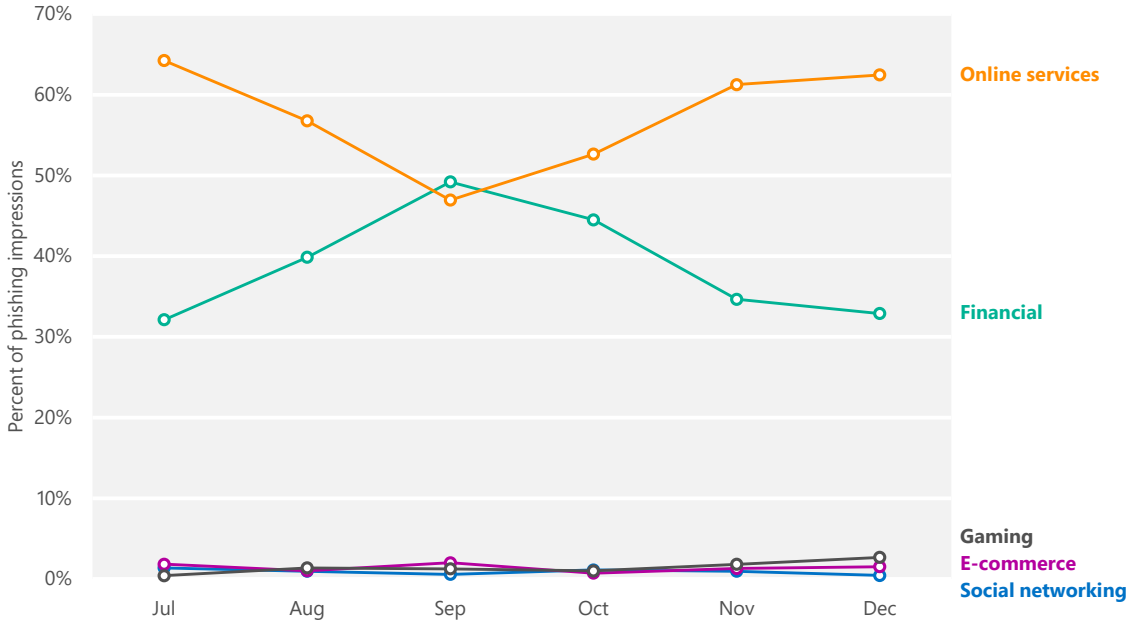
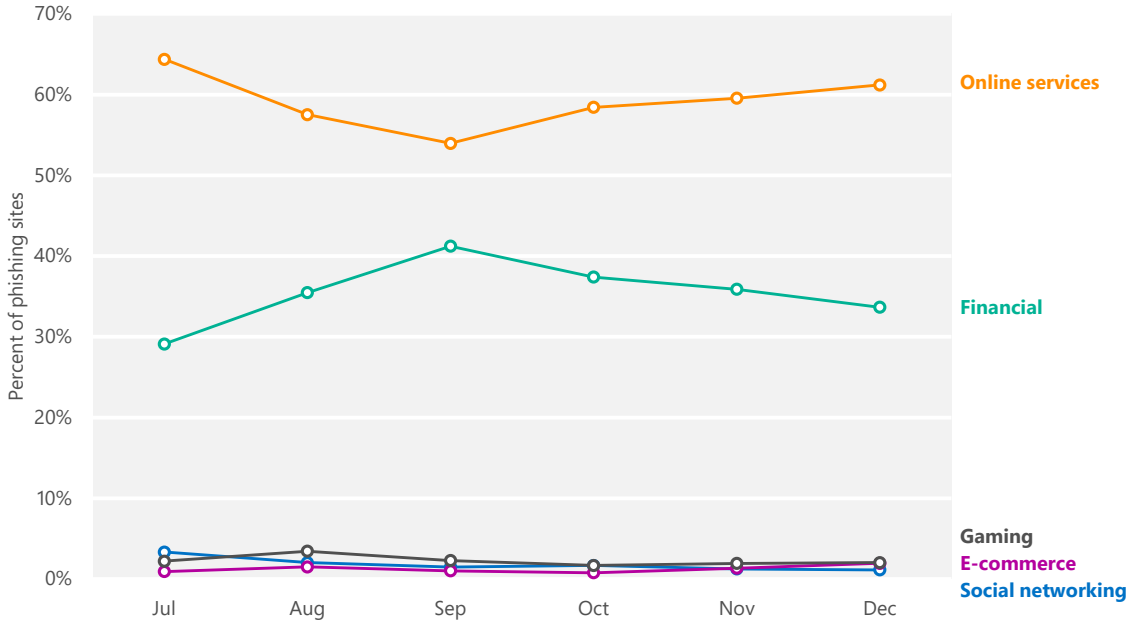


Figure 53. Unique phishing URLs visited by Internet Explorer running on all devices for each type of phishing site, July–December 2013



- Phishing sites that targeted online services accounted for the largest number of active phishing URLs each month in 2H13, and also received the largest share of impressions each month.

- Financial institutions have always been popular phishing targets because of their potential for providing direct illicit access to victims' bank accounts. Sites that targeted financial institutions accounted for the 2nd largest number of active phishing sites each month in 2H13, as well as the 2nd largest number of impressions.
- The other three categories each accounted for a very small percentage of both sites and impressions each month.
- The breakdown of phishing impressions and sites visited on mobile phones running Windows Phone 8 were similar to those observed on all devices, as shown in Figure 54 and Figure 55.

Figure 54. Impressions reported by SmartScreen Filter on Windows Phone 8 for each type of phishing site, July–December 2013

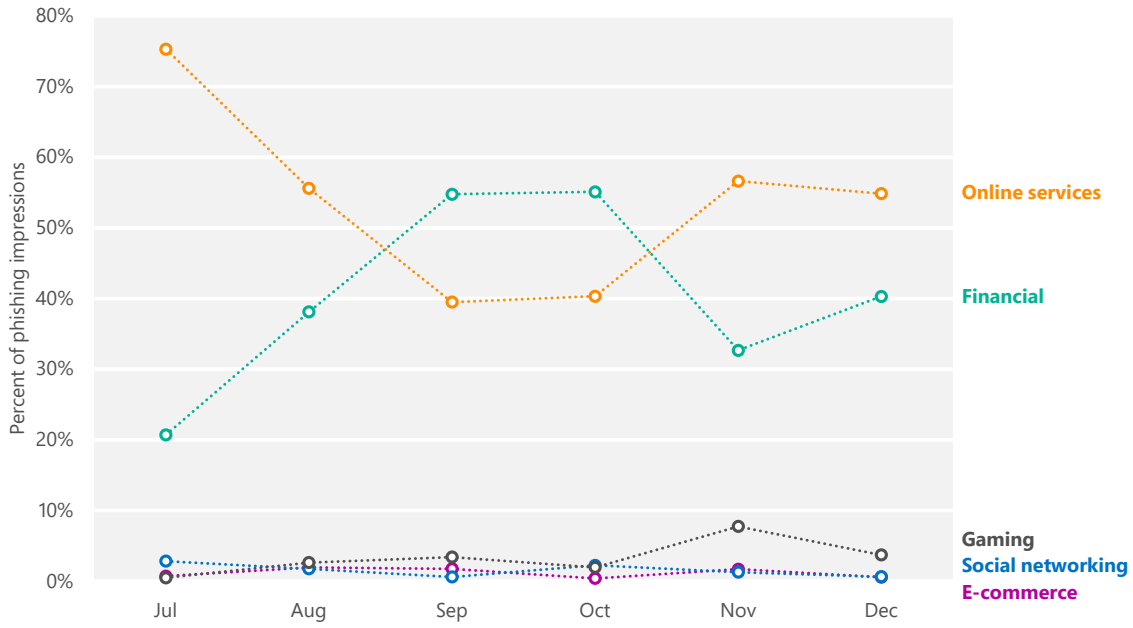
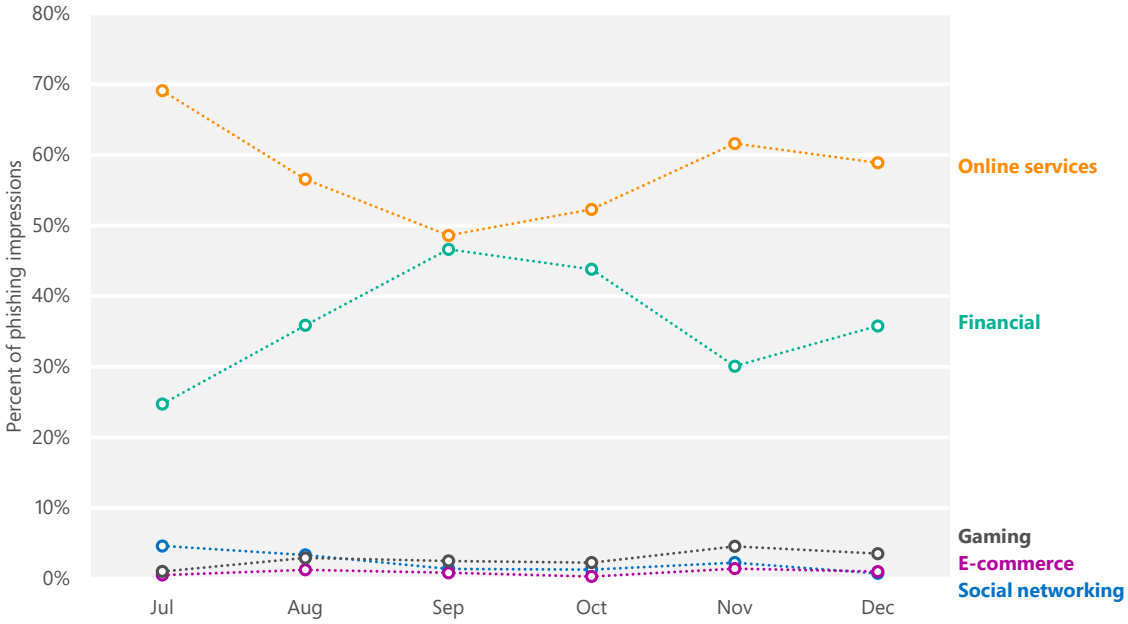


Figure 55. Unique phishing URLs visited by Internet Explorer on Windows Phone 8 for each type of phishing site, July–December 2013, by type of target



Global distribution of phishing sites

Phishing sites are hosted all over the world on free hosting sites, on compromised web servers, and in numerous other contexts. Performing geographic lookups of IP addresses in the database of reported phishing sites makes it possible to create maps that show the geographic distribution of sites and to analyze patterns.

Figure 56. Phishing sites per 1,000 Internet hosts for locations around the world in 3Q13 (top) and 4Q13 (bottom)

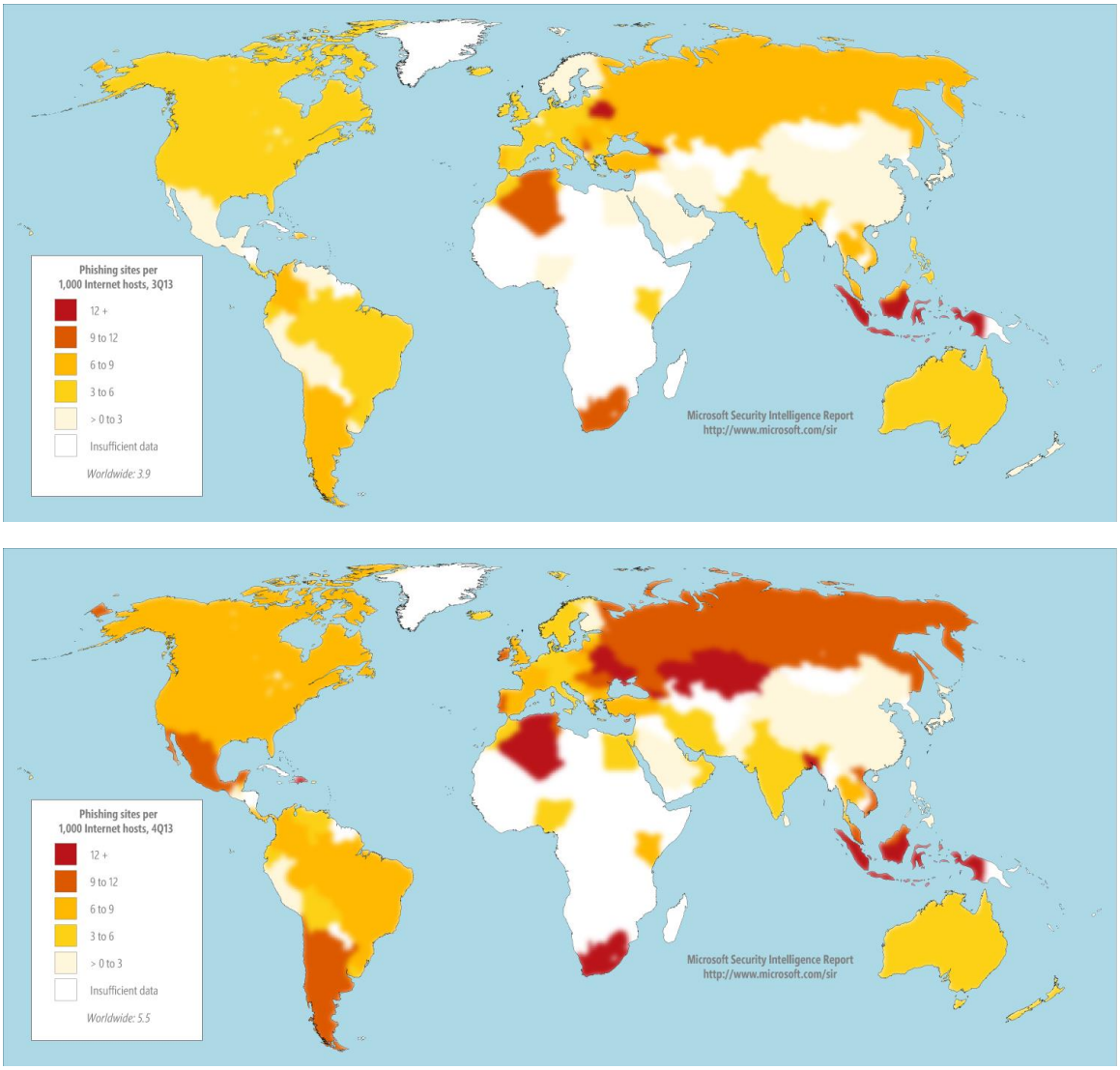
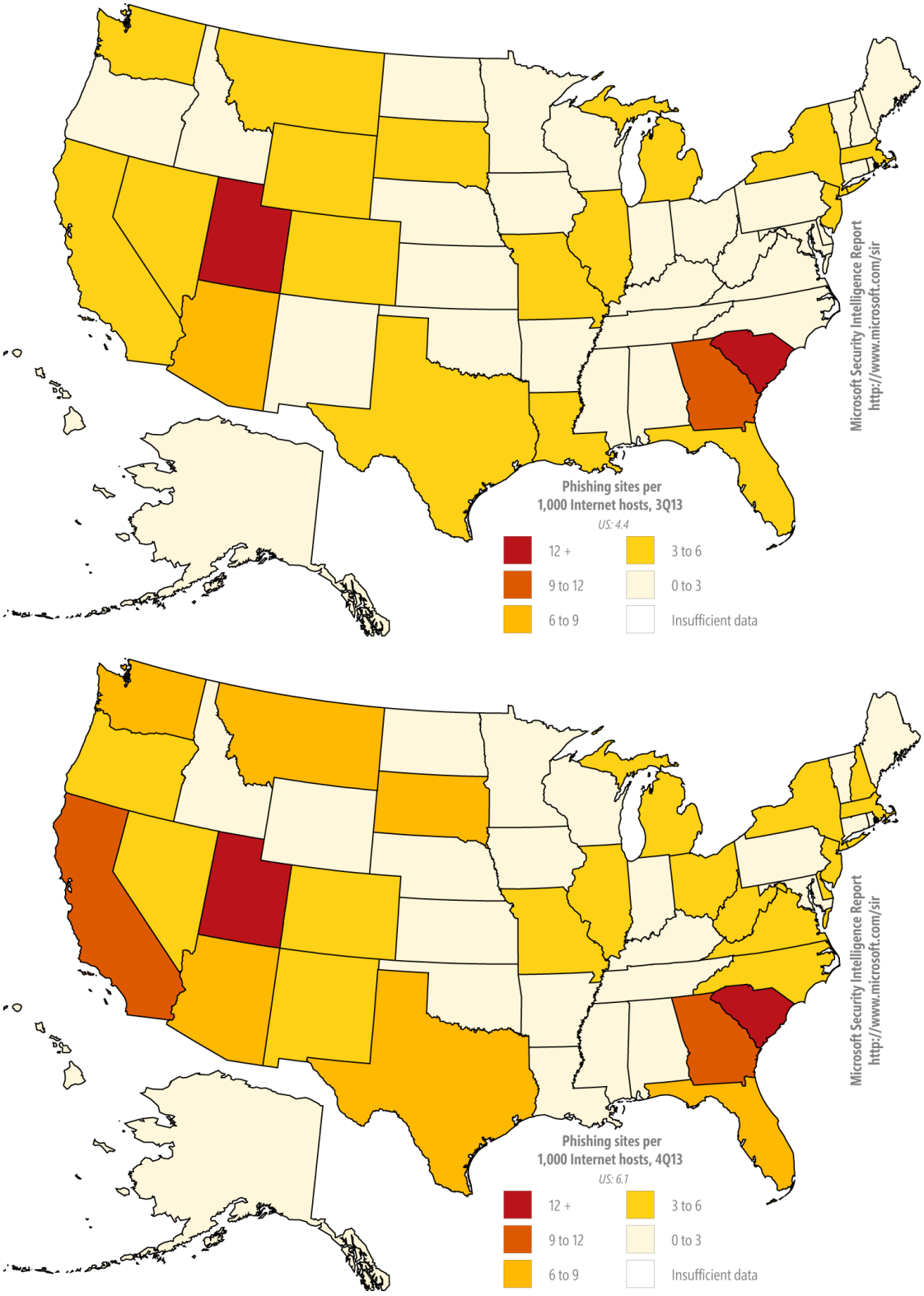


Figure 57. Phishing sites per 1,000 Internet hosts for US states in 3Q13 (top) and 4Q13 (bottom)



- SmartScreen Filter detected 3.9 phishing sites per 1,000 Internet hosts worldwide in 3Q13, and 5.5 per 1,000 in 4Q13.
- Locations with higher than average concentrations of phishing sites include Ukraine (14.2 per 1,000 Internet hosts in 4Q13), Indonesia (12.8), and South Africa (12.5). Locations with low concentrations of phishing sites include Taiwan (1.4), Japan (1.4), and Korea (1.6).
- Those US states with the highest concentrations of phishing sites include South Carolina (13.4 per 1,000 Internet hosts in 4Q12), Utah (12.5), and Georgia (9.2). States with low concentrations of phishing sites include Idaho (0.3), Nebraska (0.7), and Wisconsin (0.8).

Malware hosting sites

SmartScreen Filter in Internet Explorer helps provide protection against sites that are known to host malware, in addition to phishing sites. SmartScreen Filter uses file and URL reputation data and Microsoft antimalware technologies to determine whether sites distribute unsafe content. As with phishing sites, Microsoft collects anonymized data regarding how many people visit each malware hosting site and uses the information to improve SmartScreen Filter and to better combat malware distribution.

Figure 58. SmartScreen Filter in Internet Explorer displays a warning when a user attempts to download an unsafe file

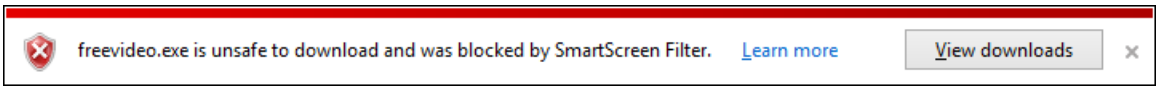
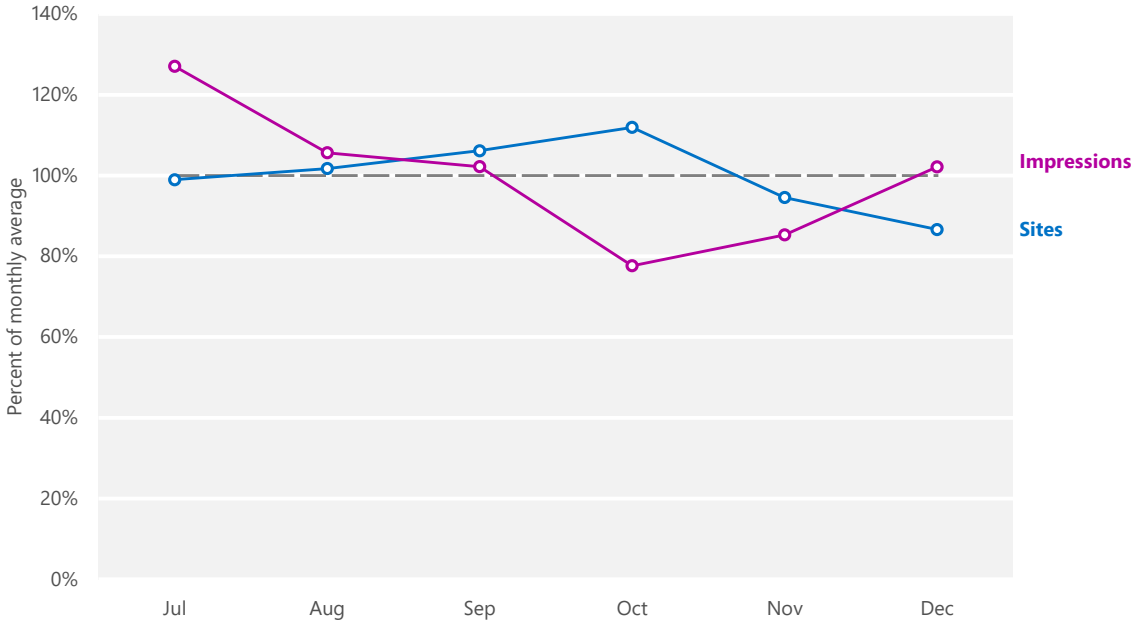


Figure 59 compares the volume of active malware hosting sites in the Microsoft database each month with the volume of malware impressions tracked by Internet Explorer.

Figure 59. Malware hosting sites and impressions tracked each month in 2H13, relative to the monthly average for each



- Malware sites and impressions were mostly stable from month to month in 2H13, never varying by more than 27 percent from the overall monthly average.

Malware categories and families

Figure 60 and Figure 61 show the types of threats hosted at URLs that were blocked by SmartScreen Filter in 2H13.

Figure 60. Categories of malware found at sites blocked by SmartScreen Filter in 2H13, by percent of all impressions

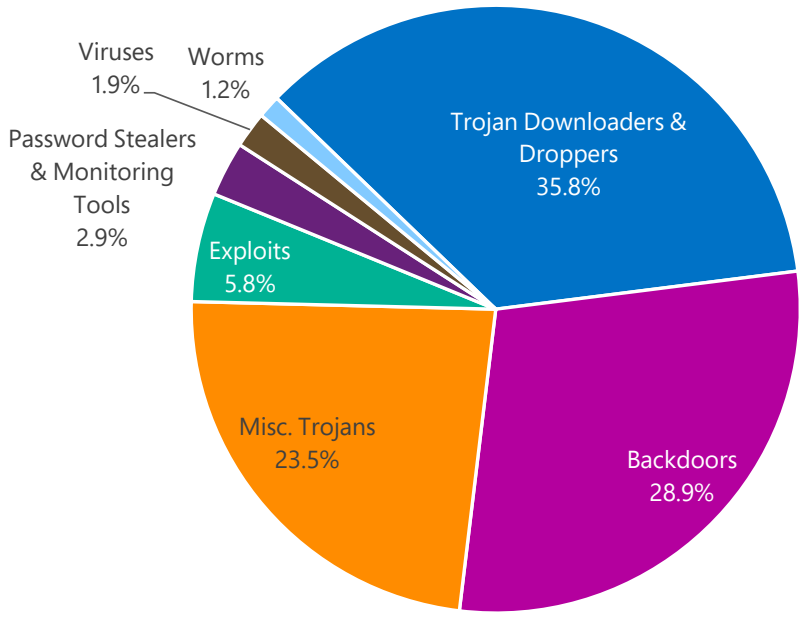


Figure 61. Top families found at sites blocked by SmartScreen Filter in 2H13, by percent of all malware impressions

	Family	Most significant category	% of malware impressions
1	Win32/Bdaejec	Backdoors	27.83%
2	Win32/Delf	Trojan Downloaders & Droppers	9.15%
3	Win32/Microjoin	Trojan Downloaders & Droppers	8.25%
4	Win32/Oceanmug	Trojan Downloaders & Droppers	5.37%
5	Win32/Obfuscator	Miscellaneous Trojans	5.07%
6	Win32/Dynamer	Miscellaneous Trojans	3.29%
7	Win32/Comame	Miscellaneous Trojans	2.80%
8	AndroidOS/CVE-2011-3874	Exploits	2.42%
9	VBS/Psyme	Trojan Downloaders & Droppers	1.93%
10	Win32/Malagent	Miscellaneous Trojans	1.88%
11	Win32/Banload	Trojan Downloaders & Droppers	1.72%
12	Win32/DelfInject	Miscellaneous Trojans	1.45%
13	Win32/Meredrop	Miscellaneous Trojans	1.24%
14	MSIL/Truado	Trojan Downloaders & Droppers	1.24%
15	AndroidOS/CVE-2011-1823	Exploits	1.15%

- Many of the families on the list are generic detections for a variety of threats that share certain identifiable characteristics.
- Win32/Bdaejec, the family responsible for the most malware impressions in 2H13, is a trojan that allows unauthorized access and control of an affected computer, and that may download and install other programs without consent. Bdaejec was found at 27.83 percent of malware hosting sites in 2H13, up from 4.63 percent in 1H13.
- Win32/Delf, the family responsible for the most malware impressions in 1H13, fell to 2nd place in 2H13. Delf is a generic detection for various threats written in the Delphi programming language. It was found at 9.15 percent of malware hosting sites in 2H13, down from 20.41 percent in 1H13.
- Win32/Oceanmug, in 4th place at 5.07 percent, was not among the top 15 families found at malware hosting sites in 1H13. Oceanmug is a trojan that silently downloads and installs other programs without consent.
- Other families that are new to the 2H13 list include Win32/Comame, VBS/Psyme, and Win32/Banload.
- Families that were on the 1H13 list but not the 2H13 list include Win32/Swisyn (responsible for the 3rd largest number of malware impressions in 1H13), Win32/Orsam, and Win32/Rongvhin.
- Two threats that target the Android operating system were among the top 15 families found at sites blocked by SmartScreen Filter in 2H13. AndroidOS/CVE-2011-1823 and AndroidOS/CVE-2011-3874 are both detections for exploits that target vulnerabilities in the operating system in an attempt to gain root privilege. See "Operating system exploits" on page 33 for more information about such threats.

> Two threats targeting Android were among the top families found at sites blocked by SmartScreen Filter.

Global distribution of malware hosting sites

Figure 62 and Figure 63 show the geographic distribution of malware hosting sites reported to Microsoft in 2H13.

Figure 62. Malware distribution sites per 1,000 Internet hosts for locations around the world in 3Q13 (top) and 4Q13 (bottom)

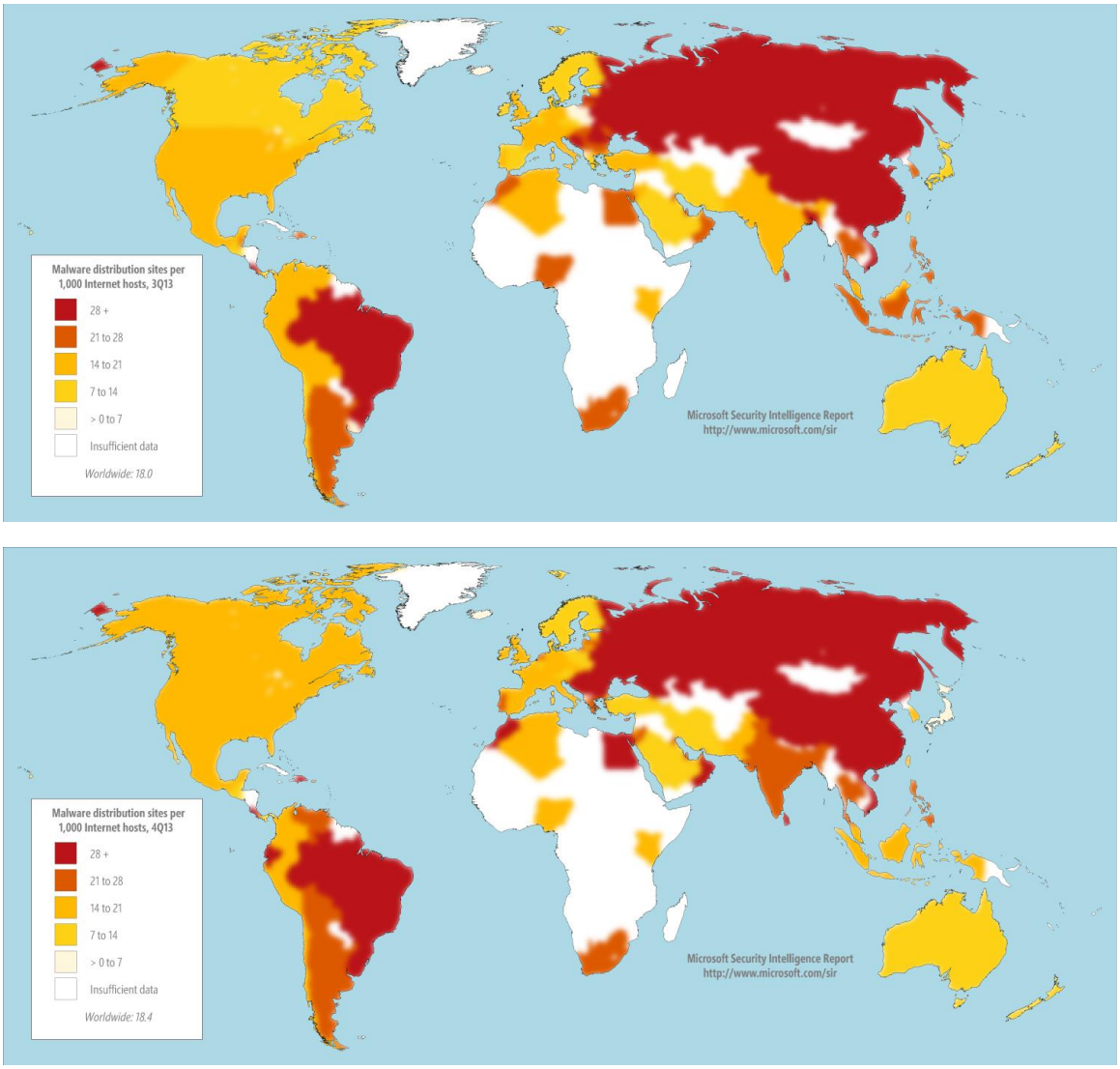
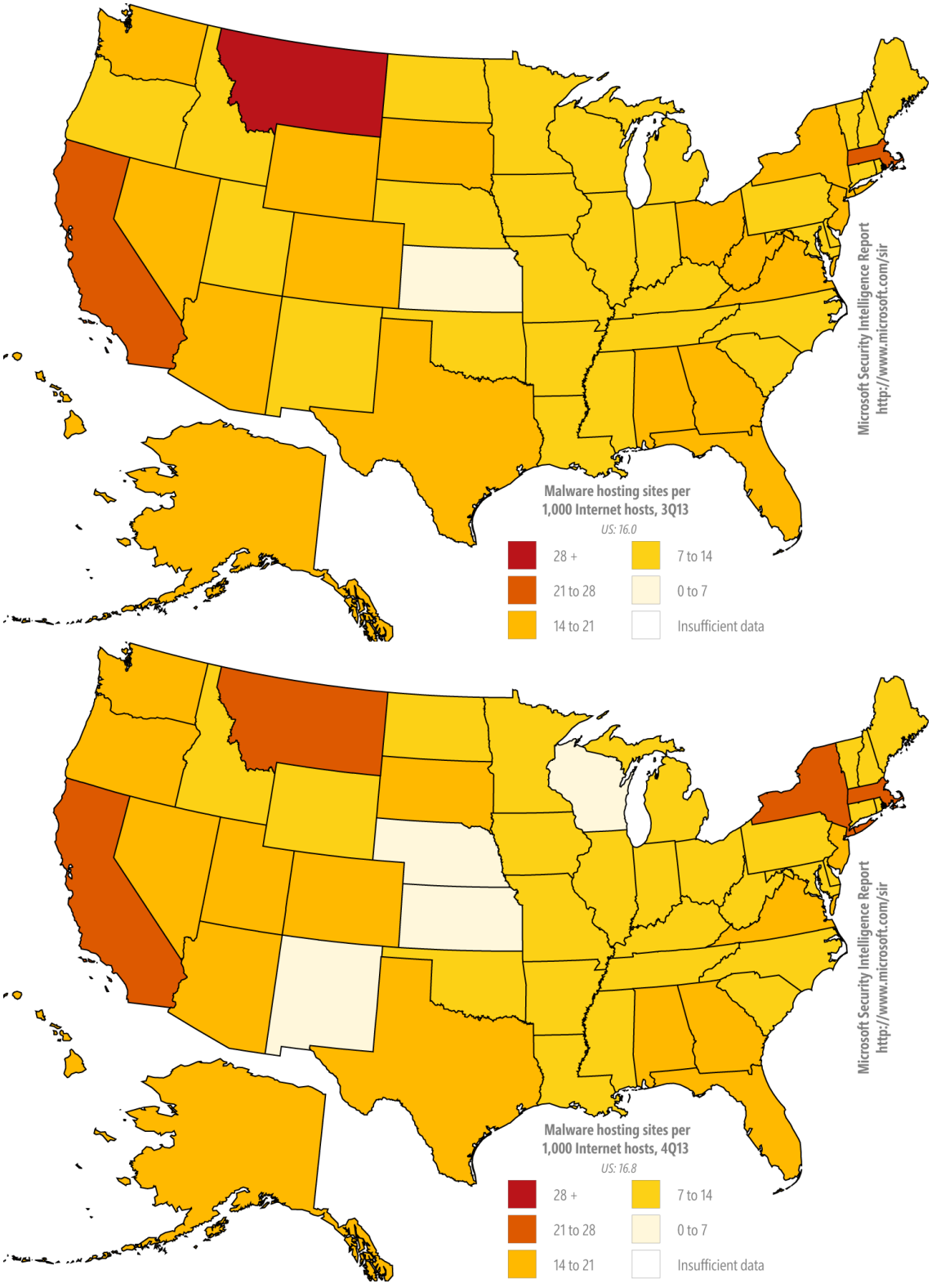


Figure 63. Malware distribution sites per 1,000 Internet hosts for US states in 3Q13 (top) and 4Q13 (bottom)



- Sites that host malware were significantly more common than phishing sites in 2H13. SmartScreen Filter detected 18.0 malware hosting sites per 1,000 Internet hosts worldwide in 3Q13, and 18.4 per 1,000 in 4Q13.
- China, which had a lower than average concentration of phishing sites (2.3 phishing sites per 1,000 Internet hosts in 4Q13), also had a very high concentration of malware hosting sites (35.8 malware hosting sites per 1,000 hosts in 4Q13). Other locations with large concentrations of malware hosting sites included Ukraine (59.2), Romania (57.8), and Russia (41.0). Locations with low concentrations of malware hosting sites included Japan (6.7), New Zealand (7.6), and Finland (8.8).
- US states with high concentrations of malware hosting sites include California (24.2 per 1,000 Internet hosts in 4Q13), Massachusetts (24.1), and Montana (23.9). States with low concentrations of malware hosting sites include Nebraska (5.8), Kansas (5.9), and Wisconsin (6.7).

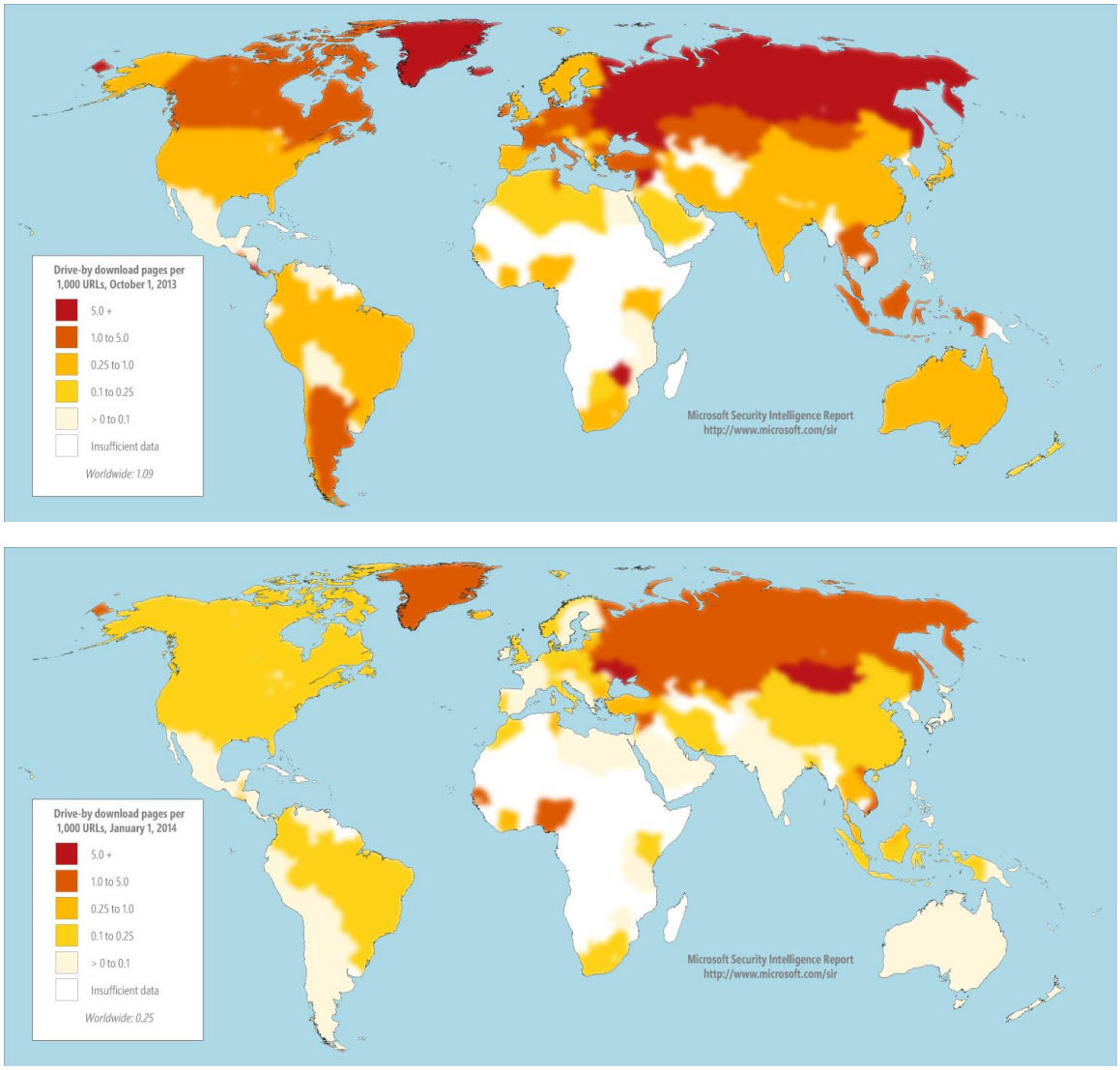
Drive-by download sites

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.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. Bing analyzes websites for exploits as they are indexed and displays warning messages when listings for drive-by download pages appear in the list of search results. (See Drive-By Download Sites at the *Microsoft Security Intelligence Report* website for more information about how drive-by downloads work and the steps Bing takes to protect users from them.)

Figure 64 shows the concentration of drive-by download pages in countries and regions throughout the world at the end of 3Q13 and 4Q13, respectively.

Figure 64. Drive-by download pages indexed by Bing at the end of 3Q13 (top) and 4Q13 (bottom), per 1,000 URLs in each country/region



- 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.
- A number of populous locations displayed significant apparent improvements between 3Q13 and 4Q13. These "improvements" are mostly due to an increase in the number of pages being indexed by Bing, rather than to a decline in the number of active drive-by download pages in absolute terms.

- Significant locations with high concentrations of drive-by download URLs in both quarters include Ukraine, with 9.1 drive-by URLs for every 1,000 URLs tracked by Bing at the end of 4Q13; Vietnam, with 1.6; and Russia, with 1.1.

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 the following resources in the "Managing Risk" section of the *Microsoft Security Intelligence Report* website:

- Promoting Safe Browsing
- Protecting Your People

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