Microsoft

# Microsoft Security Intelligence Report

Volume 16 | July through December, 2013

## 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

## Exploitation trends 1

**From potential risk to actual risk** ..... 3

Putting exploits into perspective ..... 3

When vulnerabilities are exploited ..... 4

How vulnerabilities are exploited ..... 6

Who exploits vulnerabilities ..... 8

**The rise of exploit kits** ..... 11

**Guidance: Staying ahead of exploits** ..... 16

## 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

## Mitigating risk 101

**Malware at Microsoft: Dealing with threats in the Microsoft environment ..... 103**
Antimalware usage ..... 103
Malware detections ..... 104
Malware infections ..... 107
What IT departments can do to minimize these trends ..... 108

## Appendixes 111

**Appendix A: Threat naming conventions ..... 113**
**Appendix B: Data sources ..... 115**
**Appendix C: Worldwide infection and encounter rates ..... 117**
**Glossary ..... 123**
**Threat families referenced in this report ..... 131**
**Index ..... 138**

# 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" on page 113. 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.

# Exploitation trends

From potential risk to actual risk ..... 3
The rise of exploit kits ..... 11
Guidance: Staying ahead of exploits ..... 16

# From potential risk to actual risk

Effective risk management requires having enough information about potential threats to accurately assess both their likelihood and consequences. Microsoft is committed to helping customers assess the risk they face from vulnerabilities.

The Microsoft Security Bulletins and Microsoft Security Advisories that are issued each month give IT professionals the latest information about vulnerabilities, the products they affect, and any security updates or actions they can implement to mitigate related risks. For the past several years, Microsoft Security Bulletins have also included Exploitability Index ratings designed to help customers assess not only the severity of vulnerabilities, but the likelihood that a given vulnerability will be exploited in the wild within the first 30 days of a bulletin's release. For example, a critical vulnerability that would be difficult and costly for an attacker to exploit may be less likely to be exploited than a less severe vulnerability that is easier to exploit. Microsoft believes that providing customers with comprehensive and relevant information about vulnerabilities can help make the entire computing ecosystem safer, by reducing the return on investment that attackers expect to gain from exploiting vulnerabilities.

Although forward-looking mechanisms such as Security Bulletins and the Exploitability Index can help customers assess the potential risk they face from software vulnerabilities, reviewing past vulnerabilities that have actually been exploited can help put that risk into perspective. To that end, Microsoft researchers have studied some of the exploits that have been discovered over the past several years and the vulnerabilities they targeted. Understanding which vulnerabilities get exploited, who exploits them, how they do it, and when vulnerabilities are exploited is key to accurately assessing the risk that they pose.

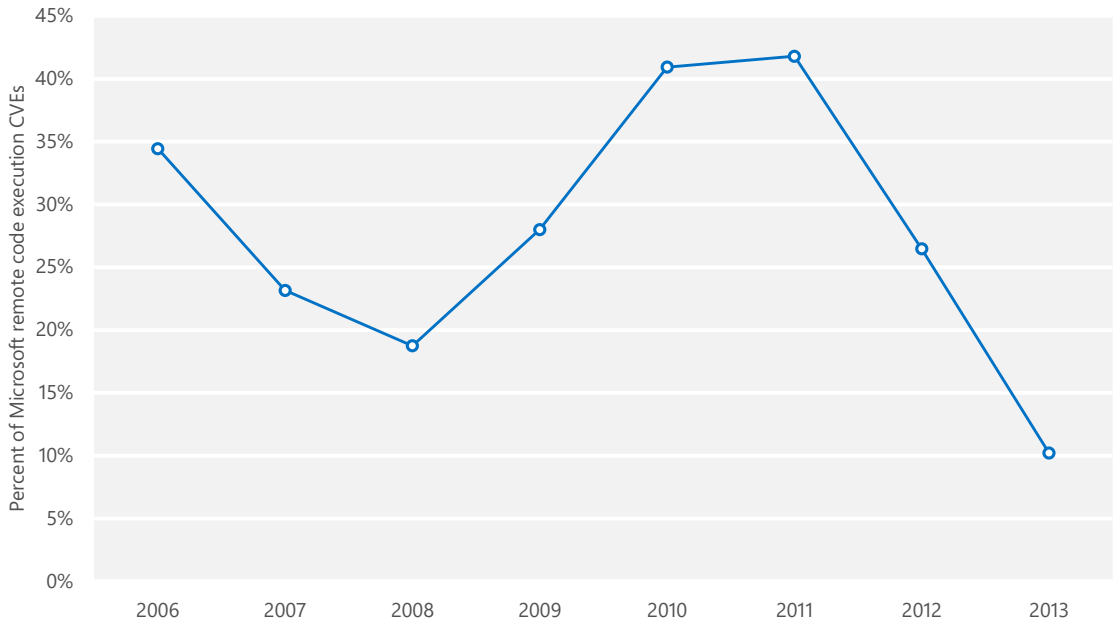
> In the modern era, the profit motive underlies most malicious exploitation activity.

### Putting exploits into perspective

In the modern era, the profit motive underlies most malicious exploitation activity. "Black hat" researchers and exploit developers sell access to vulnerability

information and exploit code, and attackers use exploits to deliver malware to victims' computers for use in illegitimate endeavors such as sending spam, credential theft, and many other profit-making schemes. For this reason, vulnerabilities often go unexploited if they would cost more to successfully exploit than an attacker is likely to make from doing it. For example, some vulnerabilities can only be exploited under very limited and uncommon conditions; others do not provide an attacker with access to enough of the computer's functionality to be worthwhile. As Figure 1 shows, even some of the most dangerous vulnerabilities—those that allow an attacker to remotely execute arbitrary code on the victim's computer—only get exploited in a minority of cases.

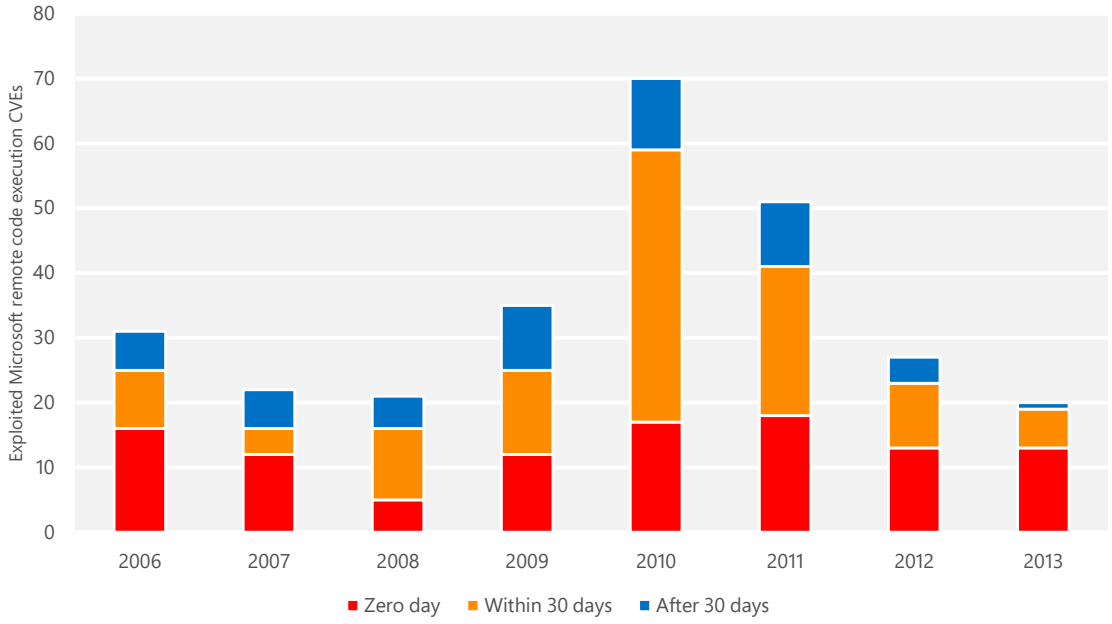
Figure 1. Percent of Microsoft remote code execution CVEs with known exploits, by year of security bulletin




## When vulnerabilities are exploited

Of those vulnerabilities that do get exploited, the greatest potential risk comes from *zero-day* exploits, which are discovered in the wild before the publisher of the affected software is able to release a security update to address the vulnerability.

Figure 2. Microsoft remote code execution CVEs, 2006–2013, by timing of first known exploit




As Figure 2 shows, the number of zero-day exploits detected each year has decreased since 2011 in absolute terms; subsequently, zero-day exploits have accounted for a larger share of the total in each of the last three years, and now account for the bulk of all exploited Microsoft remote code execution CVEs. With new remote code execution vulnerabilities becoming harder to find and exploit as secure coding practices improve across the software industry, the value of previously undisclosed exploits in the underground economy has increased, and developing new exploits has become more expensive. This reality provides "black hat" security researchers and exploit developers with a powerful incentive to maximize their own profits by selling exclusive access to a vulnerability and exploit to an attacker before the affected publisher can issue a security update, and before security software vendors can update their detection signatures. Such a scenario could explain the relative rise in zero-day vulnerabilities seen in recent years.

> Exploits that first appear more than 30 days after a security update are rare.

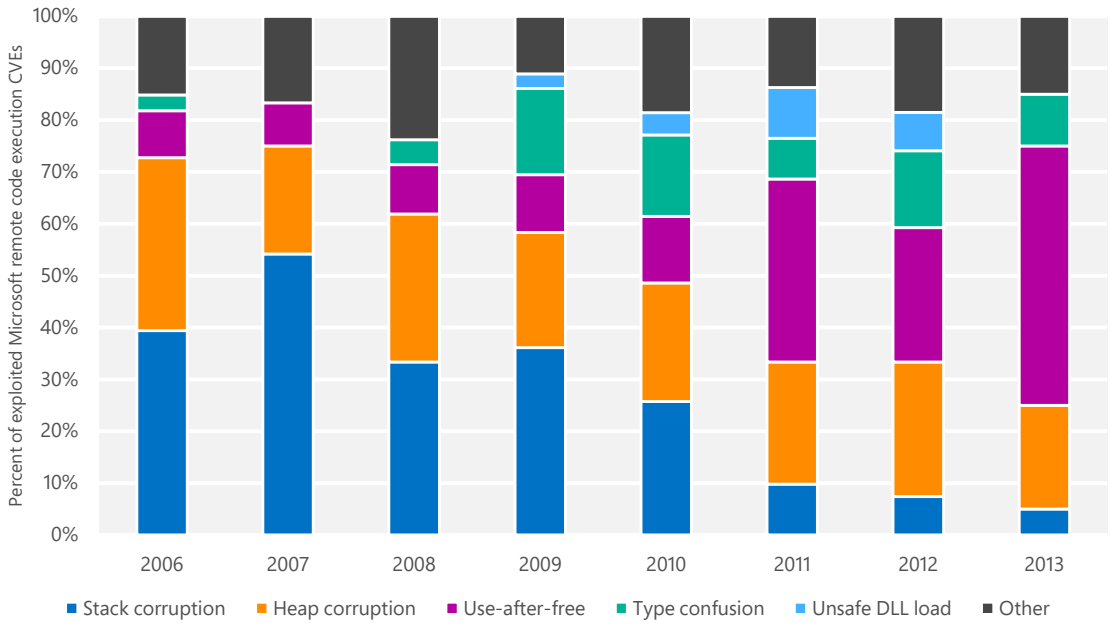
By contrast, exploits that first appear more than 30 days after security update publication have become rare, with only one such instance in 2013. Microsoft has worked with customers to make it easier for them to test and deploy updates quickly after release, even in large organizations. As the share of

computers receiving updates with the first month of release continues to increase, exploiting older vulnerabilities becomes less profitable for attackers, which provides an incentive for them to focus their attentions elsewhere.

## How vulnerabilities are exploited

The root cause of a vulnerability plays a key role in defining the set of exploitation techniques that an attacker can use when developing an exploit. As a result, the level of difficulty in developing an exploit is heavily dependent on the type of vulnerability that is being exploited. In terms of risk management, the root cause of a vulnerability can be an important factor in influencing the likelihood that an exploit will be developed. As Figure 3 illustrates, there have been some noteworthy shifts in the classes of vulnerabilities that are known to have been exploited.

Figure 3. The root causes of exploited Microsoft remote code execution CVEs, by year of security bulletin




The first clear shift can be seen in the declining percentage of exploits for stack corruption vulnerabilities, such as stack-based buffer overflows, which accounted for 54.2 percent of known exploited Microsoft remote code execution CVEs in 2007 but accounted for just 5.0 percent in 2013. This vulnerability class has historically been the most likely to be exploited, but has declined considerably since its 2007 peak. Two factors that could be contributing to this decline are the increasing prevalence of exploit mitigations

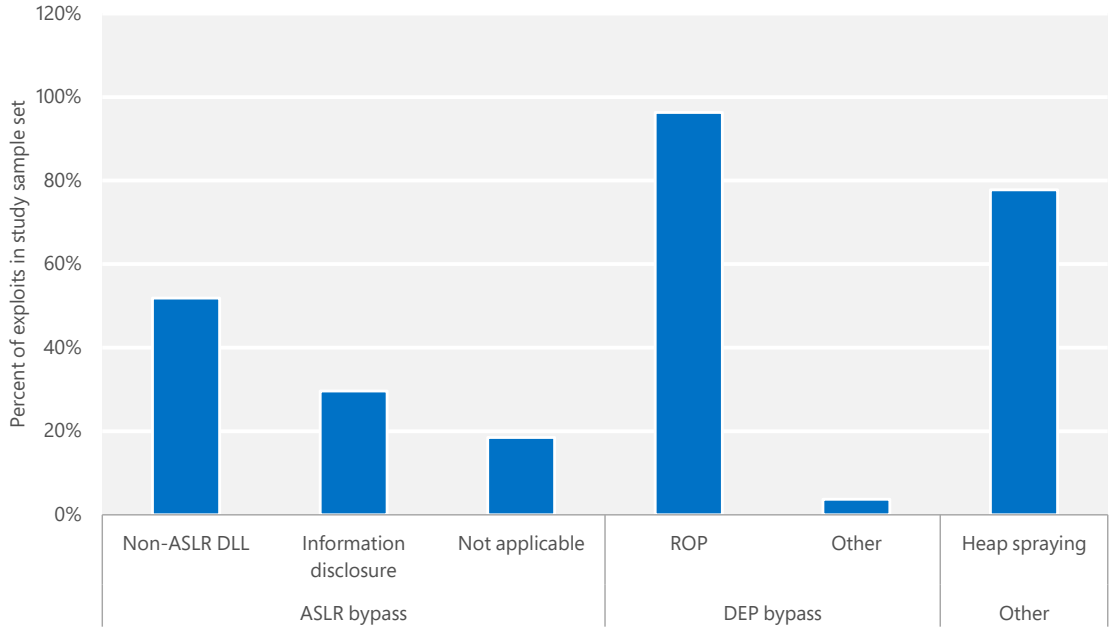
for stack corruption issues (such as /GS and SafeSEH) and the increasing effectiveness of static analysis tools designed to detect such vulnerabilities.[1]

A second shift can be seen in the increasing number of use-after-free vulnerabilities that have been exploited. This vulnerability class includes issues that arise because of incorrect management of object lifetimes. One reason for this increase is that client-side vulnerabilities have become a prime focus for attackers, and object lifetime issues are a common vulnerability class encountered in applications. Exploits that involve unsafe dynamic-link libraries (DLLs) were seen in a small percentage of cases from 2009 to 2012, but not in 2013.

> Stack corruption exploits have declined, and use-after-free exploits have increased.

The introduction of technologies such as Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR) has also affected the way attackers attempt to exploit vulnerabilities. Figure 4 shows the techniques used in exploits targeting vulnerabilities in Microsoft products that were discovered over the past two years.

Figure 4. Techniques used by exploits targeting Microsoft products, January 2012–February 2014




[1] See www.microsoft.com/sdl for information and guidance about using the Security Development Lifecycle to develop secure software.

As this data suggests, the increasing prevalence of DEP and ASLR has forced attackers to identify new techniques that can be used to exploit vulnerabilities even when these features are enabled. An increasing number of exploits attempt to bypass ASLR by relying on images that have not opted into ASLR or by taking advantage of a vulnerability to disclose information about the layout of an application's address space. (Customers can reduce the risk they face from these bypass techniques by deploying the latest version of the Enhanced Mitigation Experience Toolkit (EMET), which can be used to block exploits that use the ROP technique.)

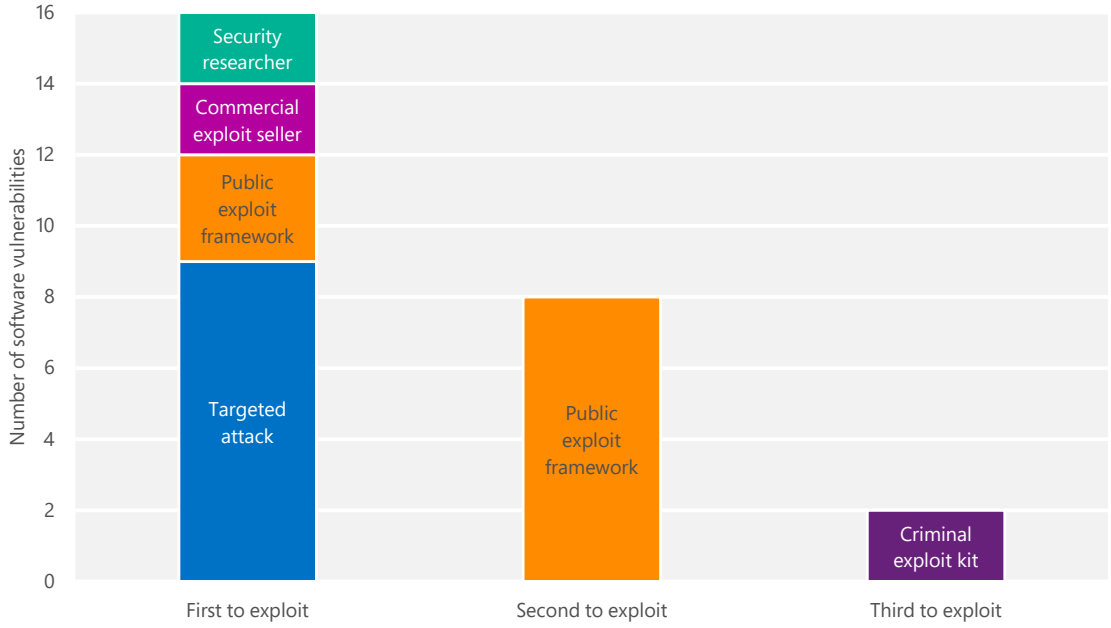
DEP and ASLR have forced attackers to find new techniques.

Having to bypass DEP and ASLR makes developing exploits more difficult and expensive, which has likely been a major factor in the declining trend of new exploits discovered over the past several years. Increased adoption of recent versions of Internet Explorer and EMET should help contribute to this trend, as developing effective exploits becomes even more difficult.

### Who exploits vulnerabilities

The parties that initially disclose vulnerabilities are not always the same parties that go on to develop and use exploits that take advantage of them. Vulnerability disclosures originate from a variety of sources, from the dangerous (such as malicious exploit developers and vulnerability sellers) to the beneficial (such as the affected software vendors themselves and security researchers who are committed to coordinated vulnerability disclosure). To explore how exploits make their way into criminal hands, Microsoft analyzed exploits targeting the 16 vulnerabilities in various software products that had known exploits discovered between January 2012 and February 2014.

Figure 5. The first, second, and third parties responsible for known exploits of the 16 software vulnerabilities studied, discovered between January 2012 and February 2014




Of these 16 vulnerabilities, nine were initially exploited in *targeted attacks* against specific targets. In these attacks, often called *advanced persistent threats* or *targeted attacks by determined adversaries*, the attacker concentrates on compromising a single designated target by using a variety of technical and social engineering techniques as necessary. Such attackers are often able to draw upon considerable technological and financial resources, which can include obtaining exclusive access to information about previously undisclosed vulnerabilities that the target is unlikely to have mitigated.[2] Of the remaining exploits, three were first released via public exploit framework, two were released through commercial sellers, and two were released by security researchers.

> Most exploits were first used in targeted attacks that affected relatively few people.

Eight of the exploits subsequently showed up in public exploit frameworks. A public exploit framework is a tool designed to help test computer systems for vulnerability to a variety of exploits. Two of these exploits then appeared in criminal exploit kits.

[2] For more information about targeted attacks, see the paper "Determined Adversaries and Targeted Attacks," available from the Microsoft Download Center, and the post "Targeted Attacks Video Series" (June 13, 2013) on the Microsoft Security Blog at blogs.technet.com/security.

Although the small sample size makes generalization difficult, these findings may be considered to lend additional support to the proposition that installing security updates quickly is one of the best ways to mitigate the risk from exploits. Most of the analyzed exploits were first used in targeted attacks that affected relatively few people. Criminal exploit kits affect a much larger number of people, but the only two exploits to be used in exploit kits were added to the kits several months after security updates that addressed the vulnerabilities were published and widely distributed.

# The rise of exploit kits

## In addition to one-on-one transactions in which buyers purchase exclusive access to exploits, exploits are also monetized through *exploit kits*—collections of exploits bundled together and sold as commercial software or as a service.

Prospective attackers buy or rent exploit kits on malicious hacker forums and through other illegitimate outlets. A typical kit contains a collection of web pages that contain exploits for several vulnerabilities in popular web browsers and browser add-ons, as shown in Figure 6. When the attacker installs the kit on a malicious or compromised web server, visitors who don't have the appropriate security updates installed are at risk of infection through drive-by download attacks. (See page 98 for more information about drive-by download attacks.)

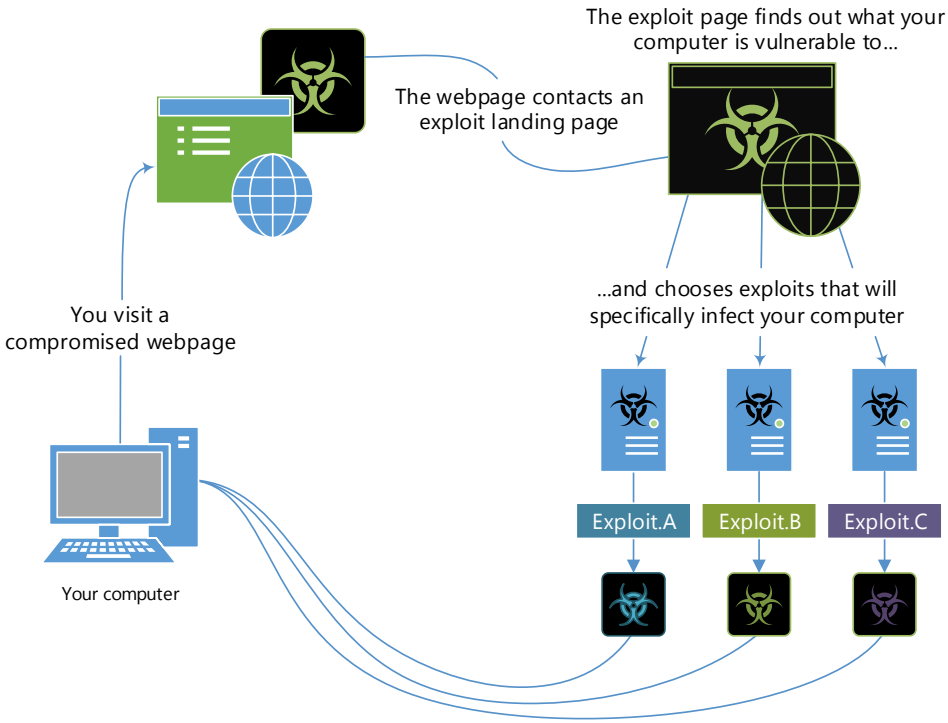
> The potential for illegitimate profit from exploit kits can be considerable.

Commercial exploit kits have existed since at least 2006 in various forms, but early versions required a considerable amount of technical expertise to use, which limited their appeal among prospective attackers. This requirement changed in 2010 with the initial release of the Blackhole exploit kit, which was designed to be usable by novice attackers with limited technical skills—in short, anyone who wanted to be a cybercriminal and could afford to pay for the kit. The potential profits that can be gained by using exploit kits to distribute malware can be considerable: the criminal group behind the malware family Win32/Reveton was reportedly making $50,000 USD per day in 2012 through Reveton installations delivered by exploit kits.[3] (See the "Ransomware" section beginning on page 67 for more information about Reveton and similar threats.)

---

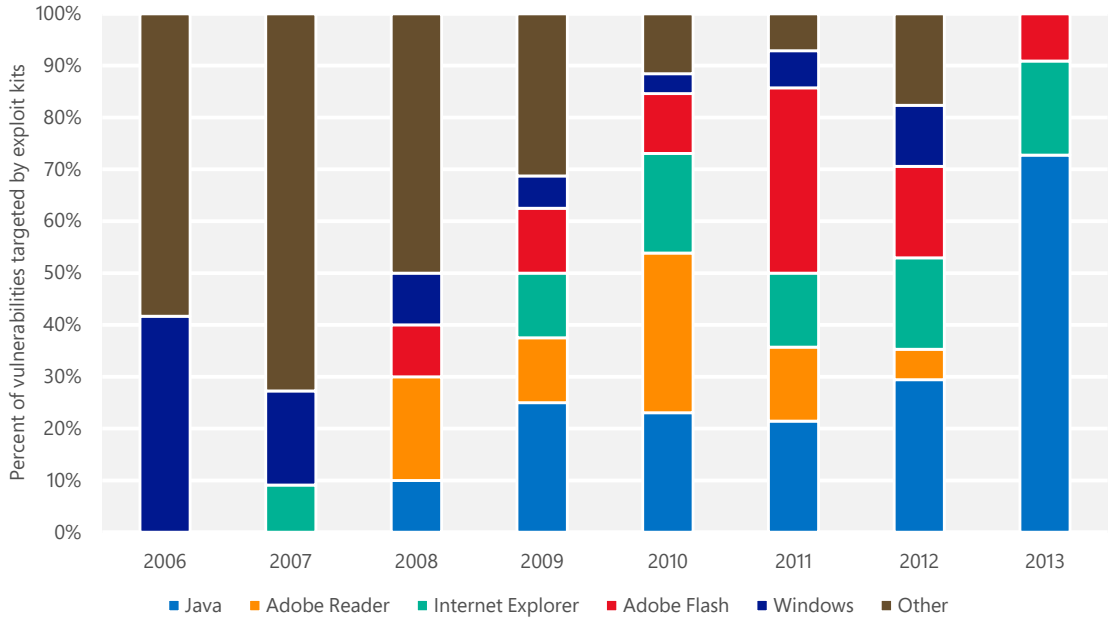
[3] Brian Krebs, "Inside a 'Reveton' Ransomware Operation," *Krebs on Security*, August 13, 2012, http://krebsonsecurity.com/2012/08/inside-a-reveton-ransomware-operation/.

Figure 6. How the Blackhole exploit kit works




Exploit kits are commercial products, if illegitimate ones, and many kits offer highly polished user interfaces and advanced feature sets. Several well-known kits provide attackers with in-depth analytics that can help them plan more effective attacks. The administration screen for the Blackhole kit is similar to a web analytics package, showing where the kit's victims came from, the browsers and operating systems they were using, how many were successfully infected, and how they were infected. Like legitimate commercial software, exploit kits often include license agreements and may come with support contracts.

Figure 7. Exploit kit exploits targeting vulnerabilities in different products, 2006–2013



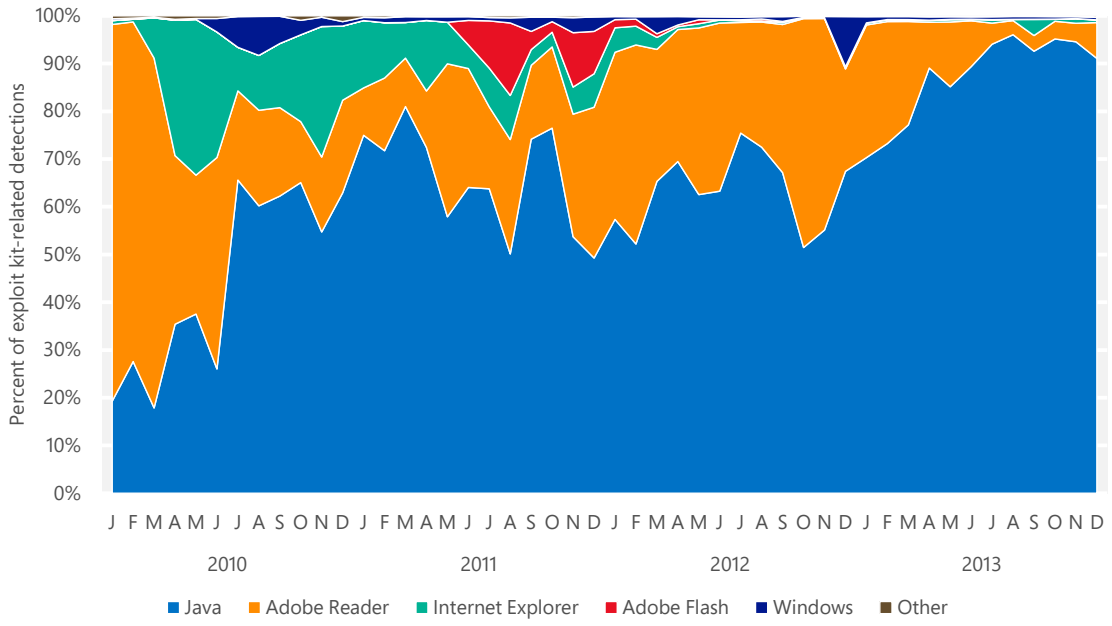

Data taken from the Contagio Exploit Pack Table, http://contagiodump.blogspot.com/2010/06/overview-of-exploit-packs-update.html.

Exploit kit makers continually update the set of exploits included in their kits, adding new exploits as they are discovered and discarding old exploits that are no longer effective or are considered too likely to be detected by security software. Early exploit kits targeted vulnerabilities in a diverse set of products from several different vendors. Over the years, kit makers have gradually narrowed down the list of products they target to a handful of widely deployed products and components, notably Adobe Flash and Reader, Microsoft Windows and Internet Explorer, and Oracle Java. Recently, kit makers have increasingly focused on vulnerabilities in out-of-date versions of the Java Runtime Environment (JRE), which is often installed on desktop and laptop computers as a browser add-on. In 2013, nearly three-quarters of the exploits used by exploit kits targeted JRE vulnerabilities.

As Figure 8 shows, the trend toward JRE vulnerabilities becomes even more pronounced when actual exploit detections are considered.[4]

[4] Figure 8 and Figure 9 examine computers with detections of exploits that are known to be targeted by exploit kits. Detections for CVEs that are not known to be exploited by exploit kits are not included in these charts, nor are detections that cannot be associated with a specific CVE. Computer totals are expressed as percentages of

Figure 8. Exploit kit-related malware detections, 2010–2013, by product or component targeted




Although exploit kit makers continue to include exploits for a variety of programs and components, not all of the exploits get exposed to every computer that visits a malicious web page. To reduce their chances of detection by security software, many exploit kits include code that allows them to expose only a subset of the vulnerabilities in the kit based on the characteristics of the visiting computer, or on which exploits have been the most successful in the past. Over the past few years, exploit kit-related detections have become increasingly dominated by JRE exploits. In 2013, JRE exploits accounted for between 84.6 and 98.5 percent of exploit kit-related detections each month, with Adobe Reader exploits a distant second. Exploits targeting all other products, including Internet Explorer, accounted for just 1.1 percent of detections each month in 2013 on average.

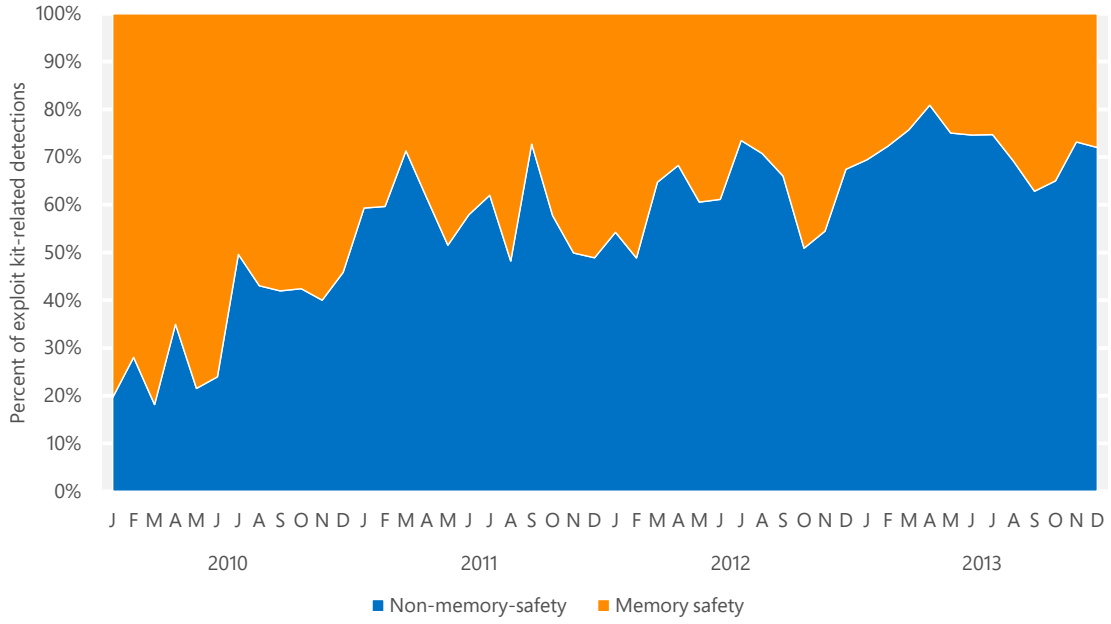
> Memory safety issues have become harder to exploit because of mitigations like ASLR and DEP.

Technologies such as DEP and ASLR are a likely factor in exploit kit authors' increasing preference for exploits that don't involve memory safety, as shown in Figure 9.

---

computers that encountered the aforementioned exploits, not as percentages of all reporting computers. See "Exploits" on page 27 for a more comprehensive look at exploits and related threats.

Figure 9. Exploit kit-related malware detections, 2010–2013, by type of vulnerability




Memory safety issues, which as recently as 2010 accounted for a clear majority of malware detections from exploit kits, have become harder to reliably exploit because of mitigations such as ASLR and DEP. Consequently, memory safety exploits have become less popular among kit authors than other exploit techniques.

# Guidance: Staying ahead of exploits

The likelihood that a vulnerability will be successfully exploited depends on many factors, including the type of vulnerability being exploited, the product versions being targeted, an attacker's ability to make use of the necessary exploitation techniques, and the amount of time required to build a reliable exploit. The following actions can help organizations and individuals significantly reduce the risk they face from exploits.

## Stay current on security updates

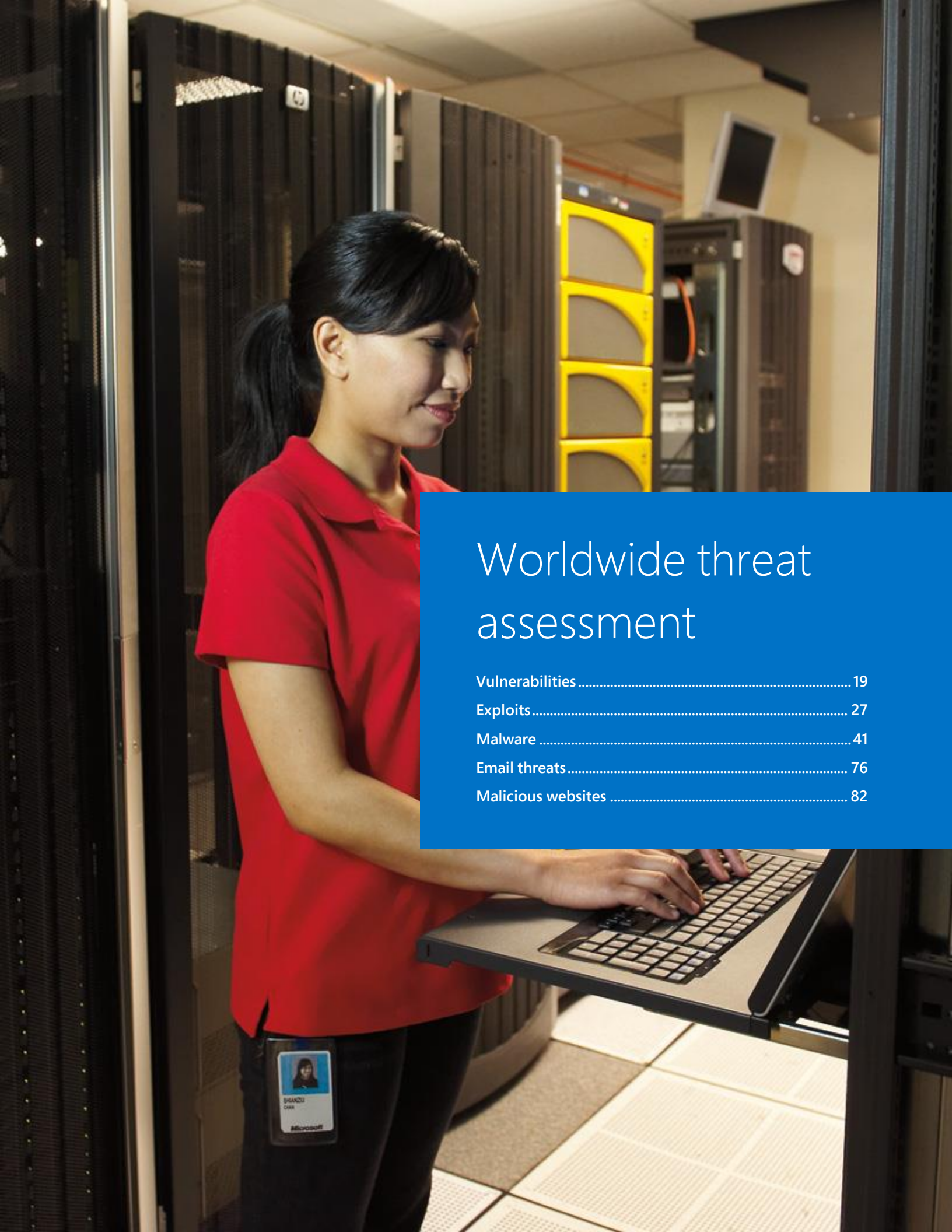
Most of the examined vulnerabilities only showed signs of being exploited after a security update had been made available. Exploit kits, in particular, tended to target vulnerabilities for which security updates had already been available for a significant amount of time. Installing security updates as soon as they are available can help minimize risk.

## Use the newest versions of applications

Windows 8.1, Internet Explorer 11, and Office 2013 all take advantage of improved security features that more effectively mitigate techniques that are currently being used to exploit vulnerabilities. Deploying these product versions widely can mitigate the risk an organization faces from several of the most commonly detected exploits. Using the 64-bit edition of Internet Explorer 11 with Enhanced Protected Mode enabled can also help protect users from a range of Internet-borne threats.

## Use the Enhanced Mitigation Experience Toolkit (EMET)

EMET can be used to protect applications that run on all supported versions of Windows. The features included in EMET are specifically designed to break exploitation techniques that are currently used by attackers. See "Enhanced Mitigation Experience Toolkit (EMET) effectiveness" on page 38 for more information about EMET and how it can be used to reduce risk.



# 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

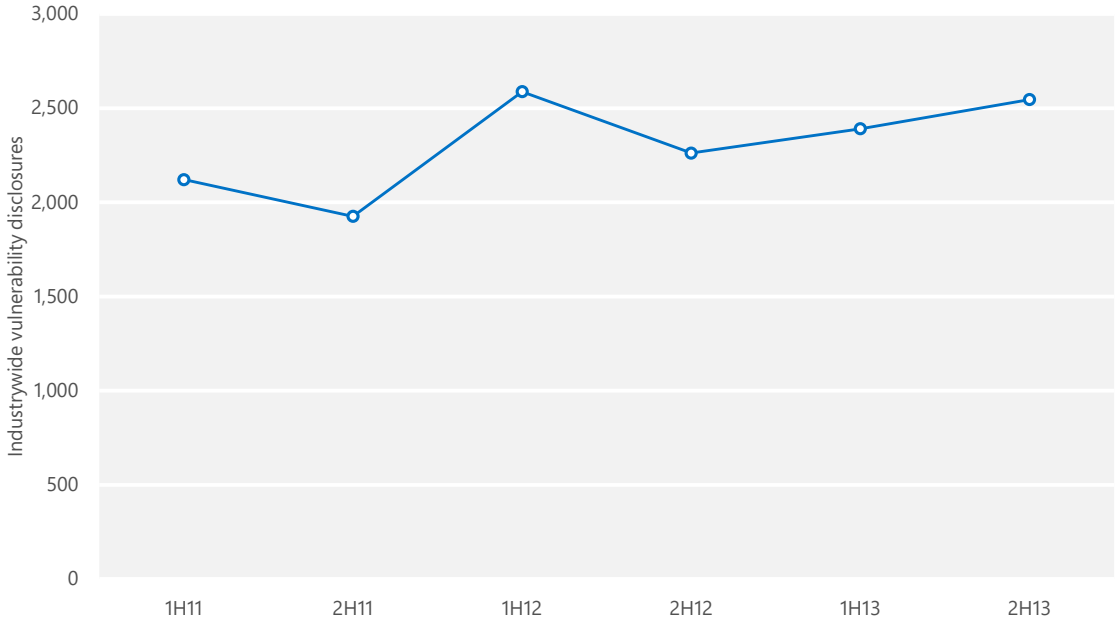
A *disclosure*, as the term is used in the *Microsoft Security Intelligence Report*, is the revelation of a software vulnerability to the public at large. Disclosures can come from a variety of sources, including publishers of the affected software, security software vendors, independent security researchers, 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.[5]

Figure 10 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.)

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

Figure 10. Industrywide vulnerability disclosures, 1H11–2H13



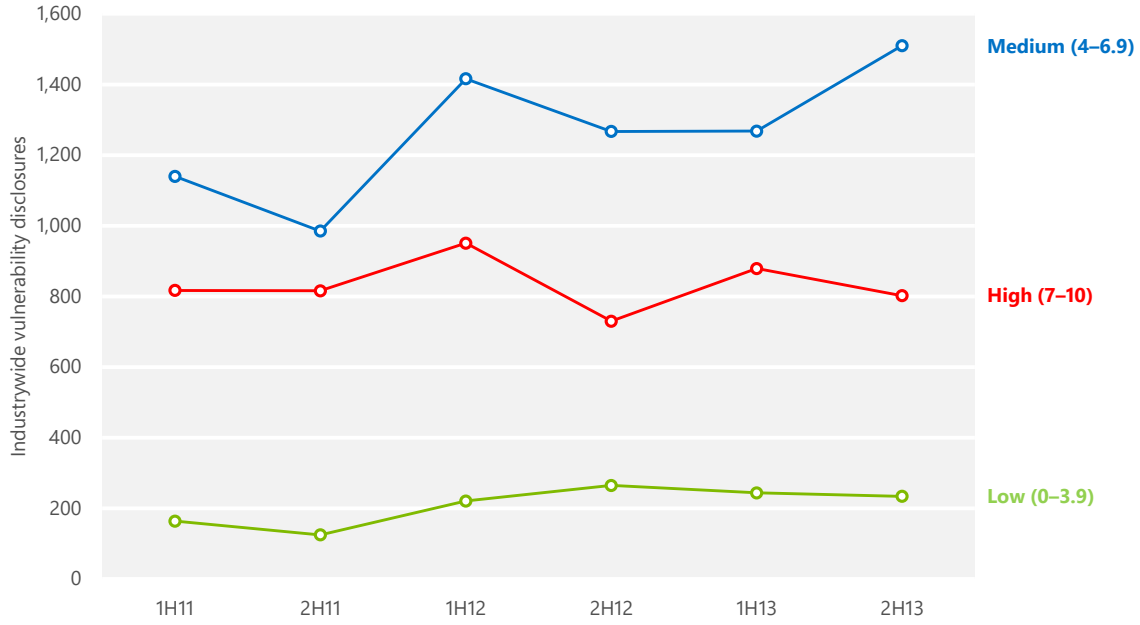

- Vulnerability disclosures across the industry in 2H13 were up 6.5 percent from 1H13, and 12.6 percent from 2H12. Increased disclosures of application vulnerabilities were responsible for much of the increase. (See "Operating system, browser, and application vulnerabilities" on page 23 for more information.)
- 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 11. Industrywide vulnerability disclosures by severity, 1H11–2H13

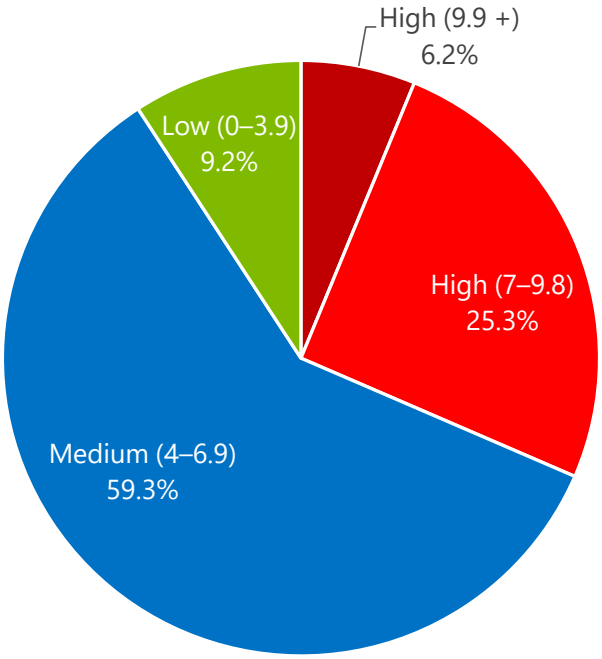



- High-severity vulnerability disclosures decreased 8.8 percent industrywide in 2H13, after increasing by 20.4 percent from 2H12 to 1H13. High-severity vulnerabilities accounted for 31.5 percent of total disclosures in 2H13, compared to 31.6 percent in the previous period.
- Medium-severity vulnerability 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 12 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 12. Industrywide vulnerability disclosures in 2H13, by severity

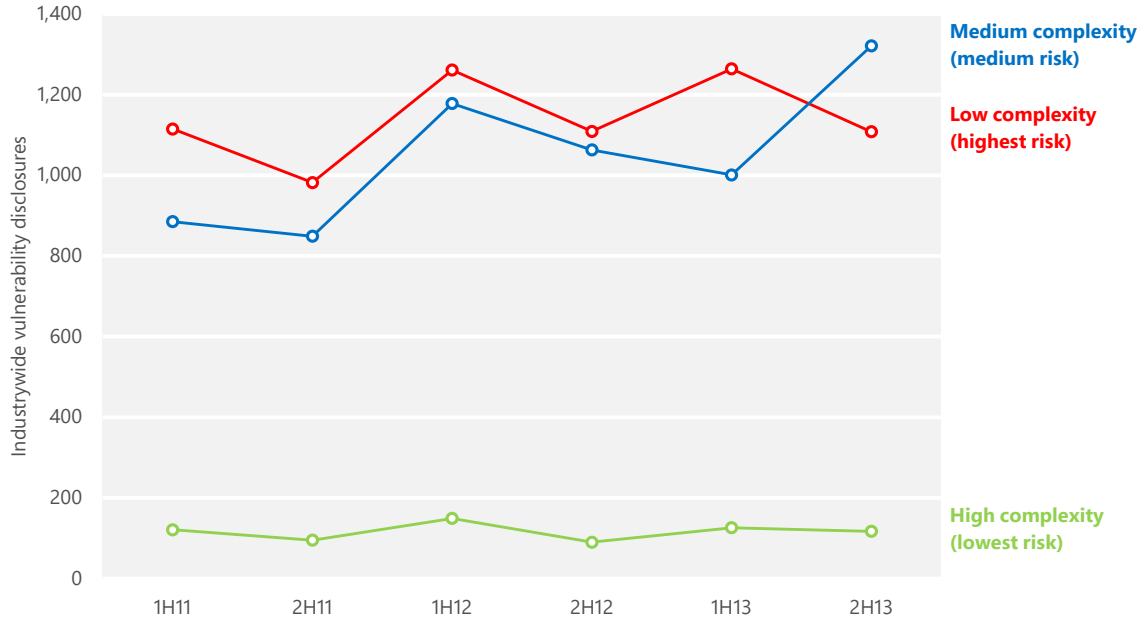



## Vulnerability complexity

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 13 shows complexity trends for vulnerabilities disclosed since 1H11. Note that Low complexity in Figure 13 indicates greater risk, just as High severity indicates greater risk in Figure 11.

Figure 13. 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

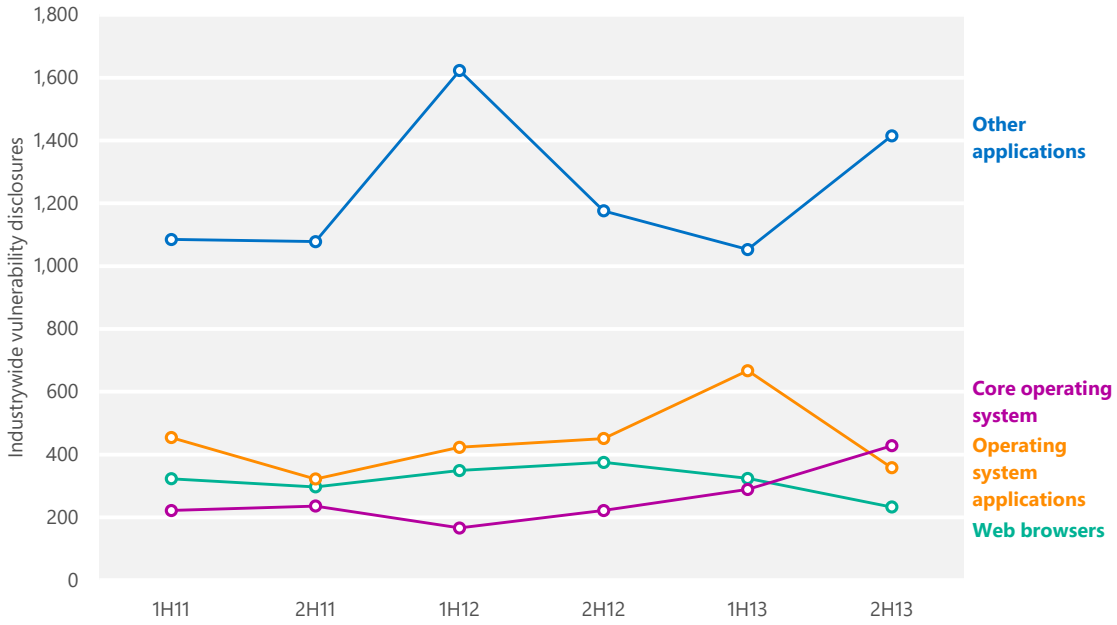
Comparing operating system vulnerabilities to non-operating system vulnerabilities that affect other components requires determining whether a particular program or component should be considered part of an operating system. This determination is not always simple and straightforward, given the componentized 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 14 shows industrywide vulnerabilities for operating systems, browsers, and applications since 1H11.

Figure 14. Industrywide operating system, browser, and application vulnerabilities, 1H11–2H13



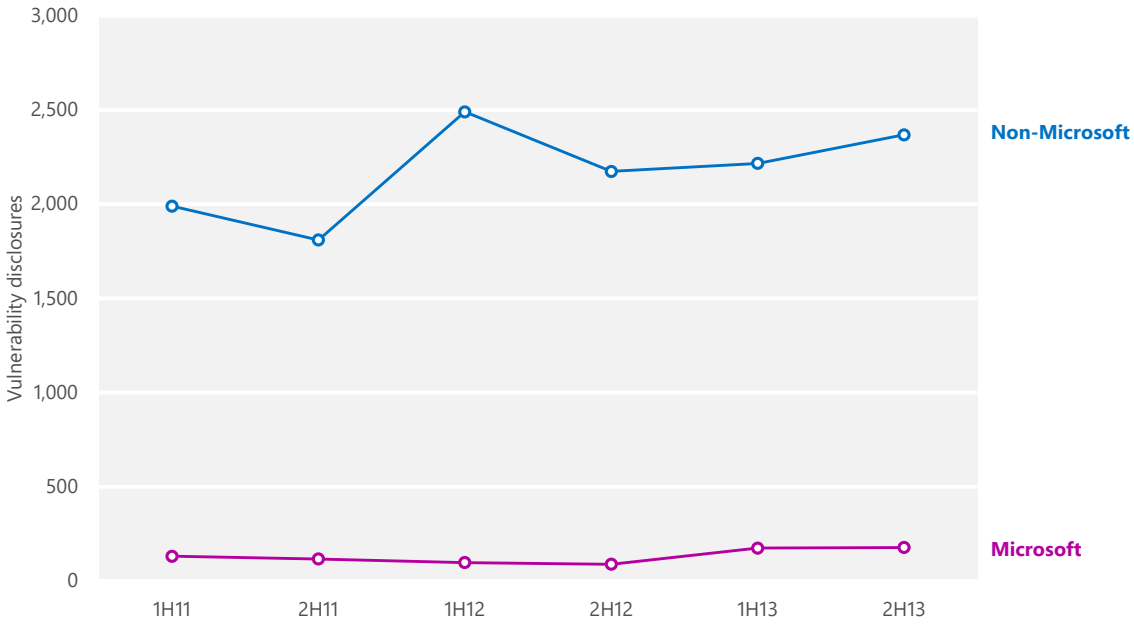
- Vulnerabilities in applications other than web browsers and operating system applications increased 34.4 percent in 2H13 and accounted for 58.1 percent of total disclosures for the period.
- Operating system vulnerabilities increased 48.1 percent in 2H13, going from last place to second. Overall, operating 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 15 shows vulnerability disclosures for Microsoft and non-Microsoft products since 1H11.

Figure 15. 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.[6]

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.[7]

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

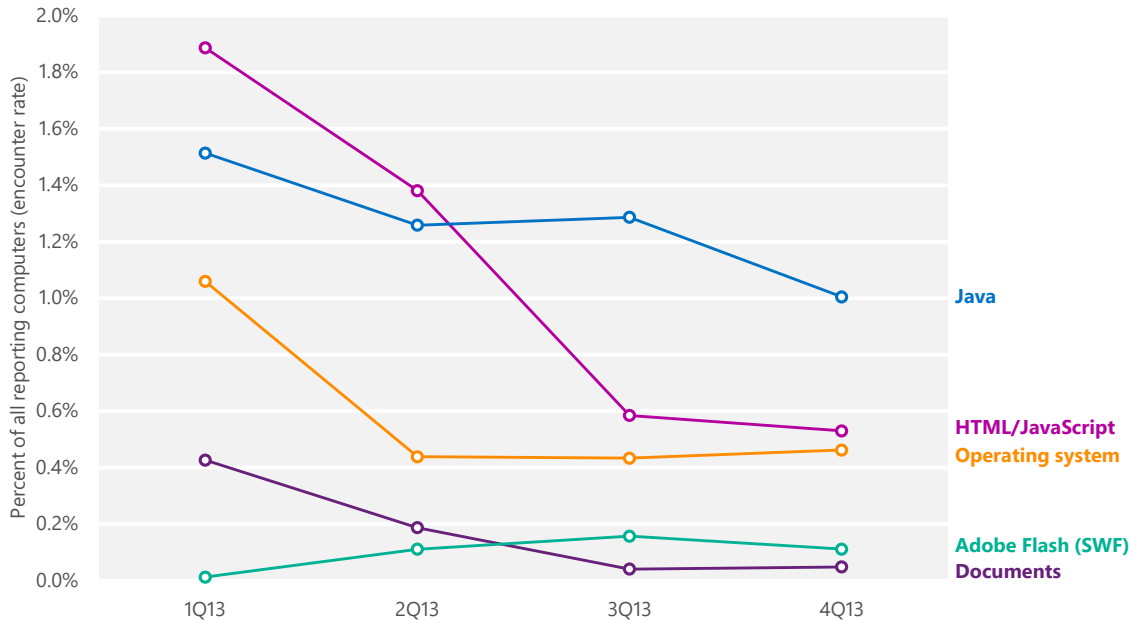
[6] See the Microsoft Security Update Guide at www.microsoft.com/security/msrc/whatwedo/securityguide.aspx for guidance to help protect your IT infrastructure while creating a safer, more secure computing and Internet environment.

[7] 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 16 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.[8]) See page 41 for more information about the encounter rate metric.

Figure 16. Encounter rates for different types of exploit attempts in 2013




[8] For privacy statements and other information about the products and services that provide data for this report, see "Appendix B: Data sources" on page 115.

- 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 16.
- 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 17 lists the exploit-related families that were detected most often during the second half of 2013.

Figure 17. 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

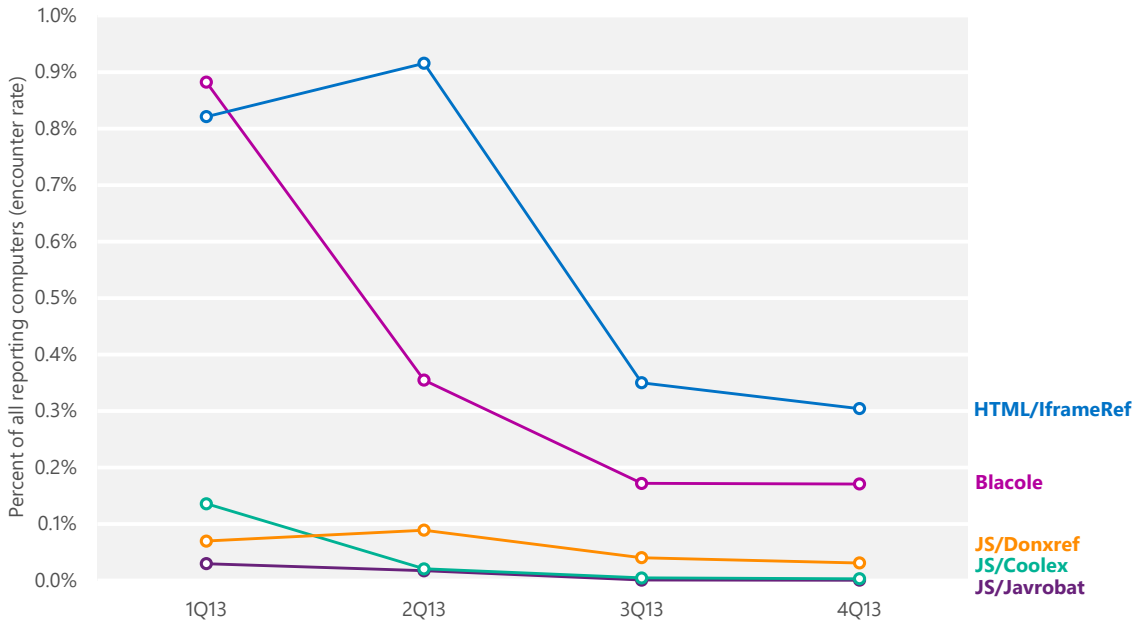
(MDAC), the Oracle Java Runtime Environment (JRE), and other popular products and components. When the attacker loads the Blacole kit on a malicious or compromised web server, visitors who don't have the appropriate security updates installed are at risk of infection through a drive-by download attack. (See page 11 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.[9]

## HTML and JavaScript exploits

Figure 18 shows the prevalence of different types of HTML and JavaScript exploits during each of the four most recent quarters.

Figure 18. Trends for the top HTML and JavaScript exploits detected and blocked by Microsoft real-time antimalware products in 2H13



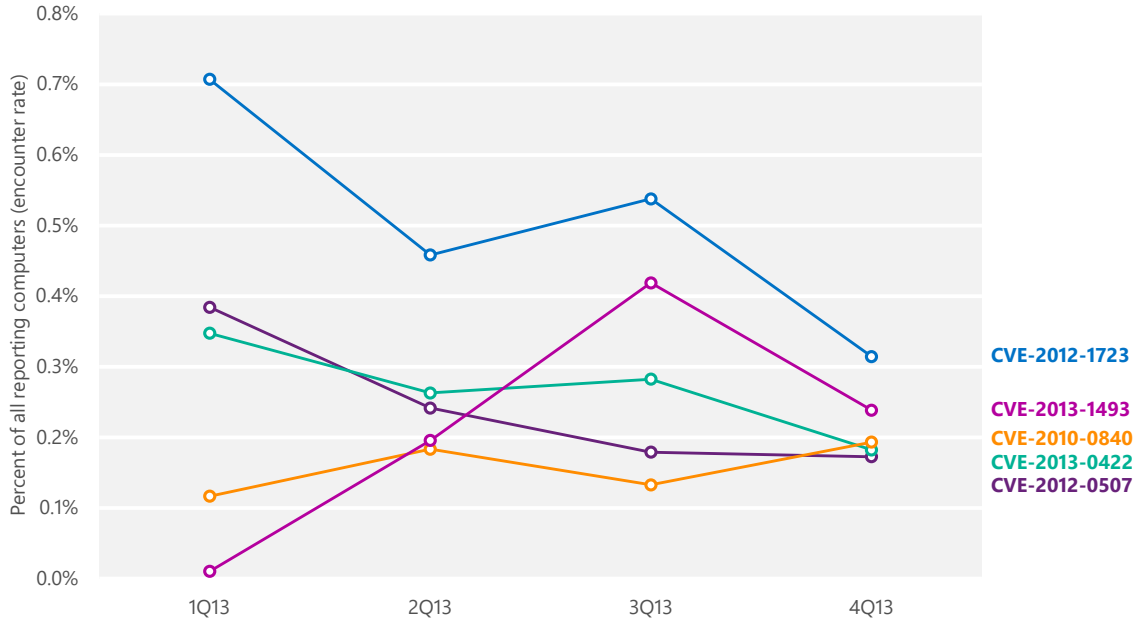

[9] "Blackhole malware exploit kit suspect arrested, *bbc.com*, October 9, 2013, http://www.bbc.com/news/technology-24456988.

- 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 19 shows the prevalence of different Java exploits by quarter.

Figure 19. 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.

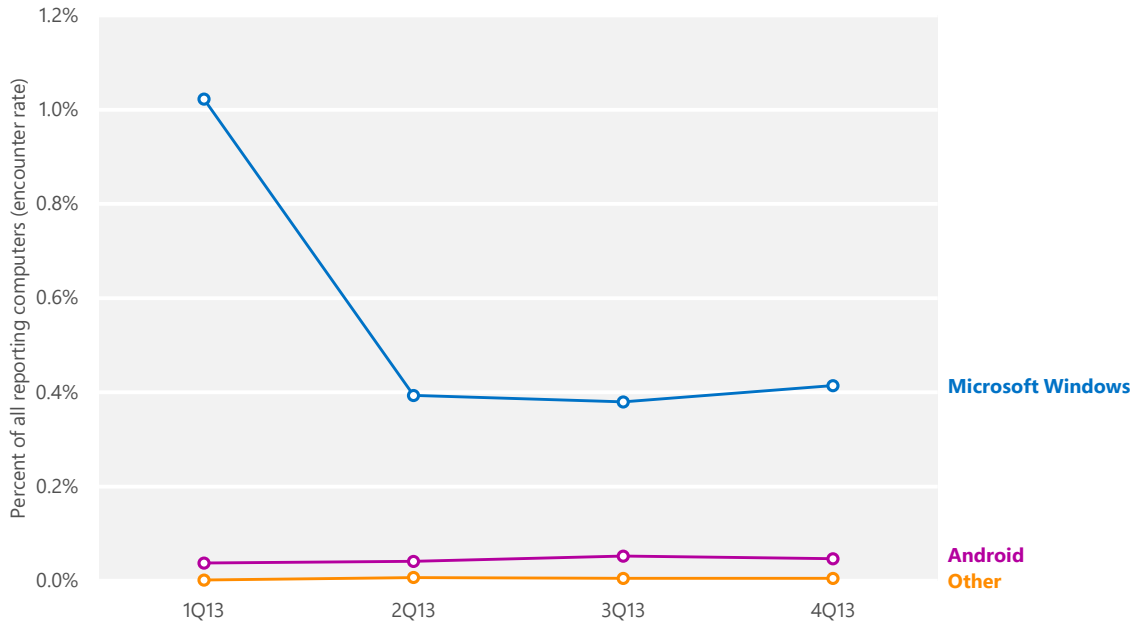
- CVE-2013-1493, a cross-platform vulnerability in the JRE's color management code, was first disclosed and exploited in the wild in 1Q13. Initial exploits targeting the vulnerability used heap-spraying techniques and leaked memory information to locate the accurate memory base location for exploitation. 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 20 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.

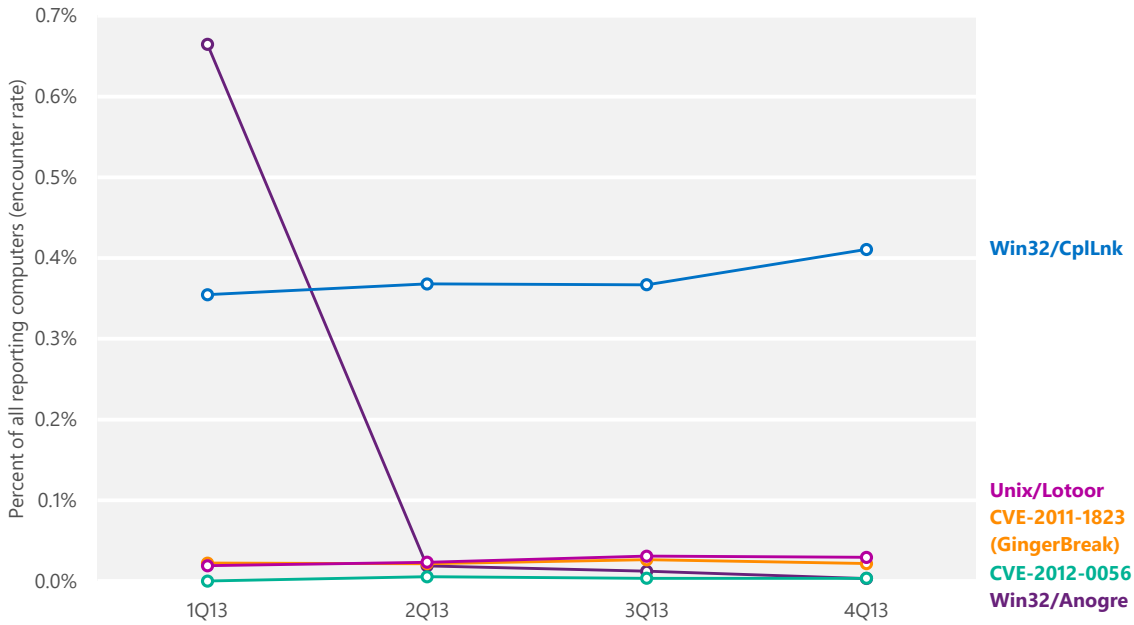
Figure 20. Exploits against operating system vulnerabilities detected and blocked by Microsoft real-time antimalware products in 2013




- 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 21 shows trends for the individual exploits most commonly detected and blocked or removed during each of the past four quarters.

Figure 21. 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.
- 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

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

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 22 shows the prevalence of different types of document exploits during each of the four most recent quarters, and Figure 23 shows encounter rates for individual exploits.

Figure 22. Types of document exploits detected and blocked by Microsoft real-time antimalware products in 2013

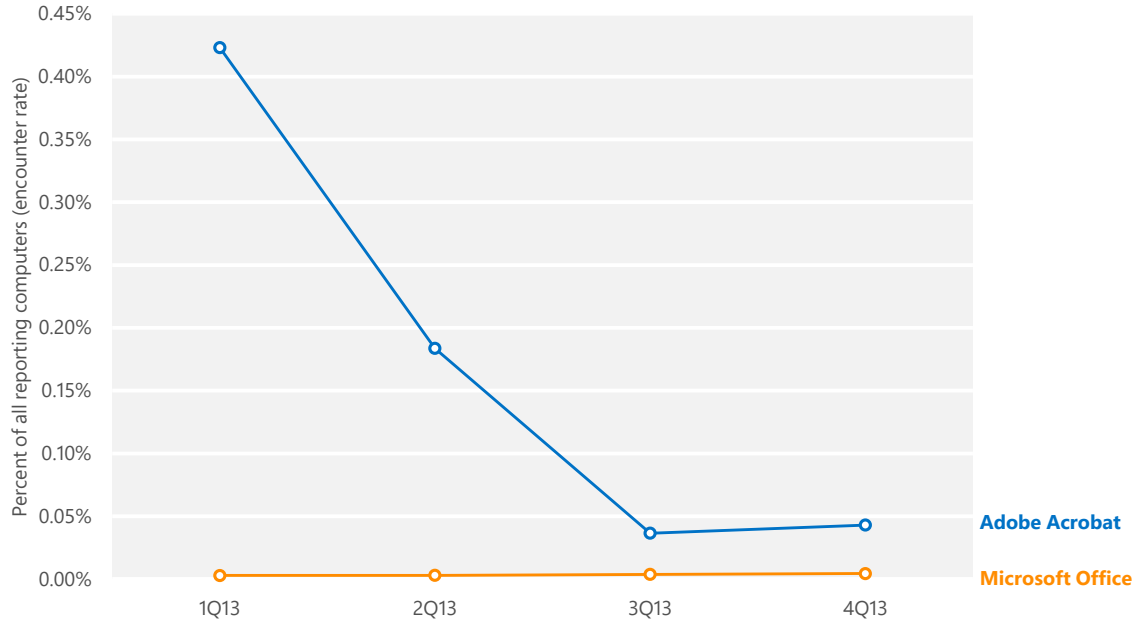
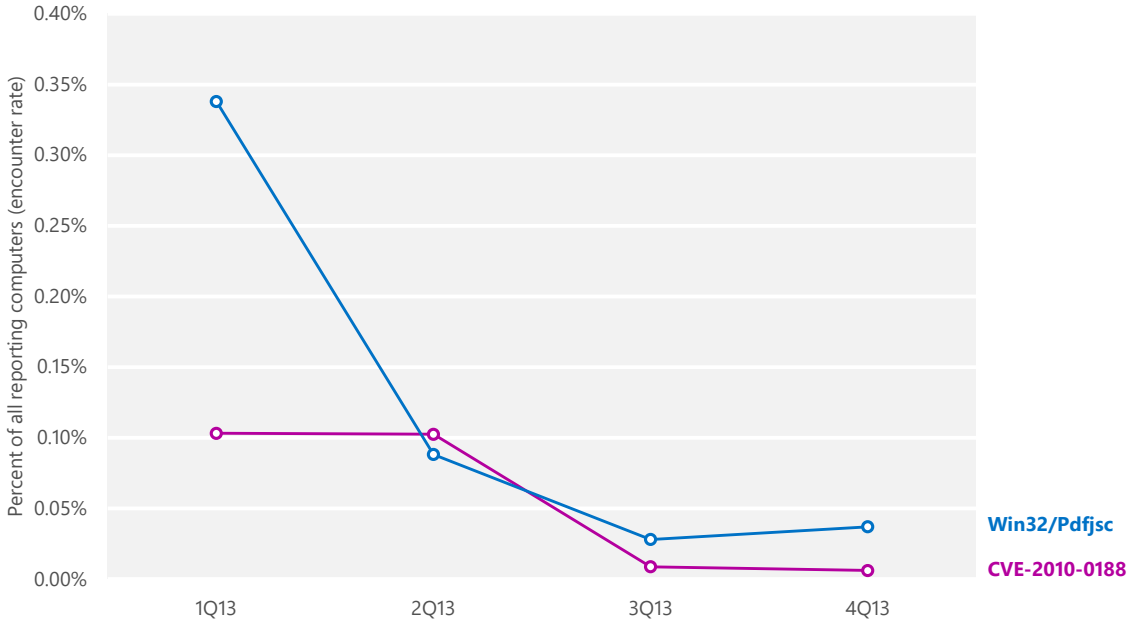



Figure 23. Individual document exploits detected and blocked by Microsoft real-time antimalware products in 2013

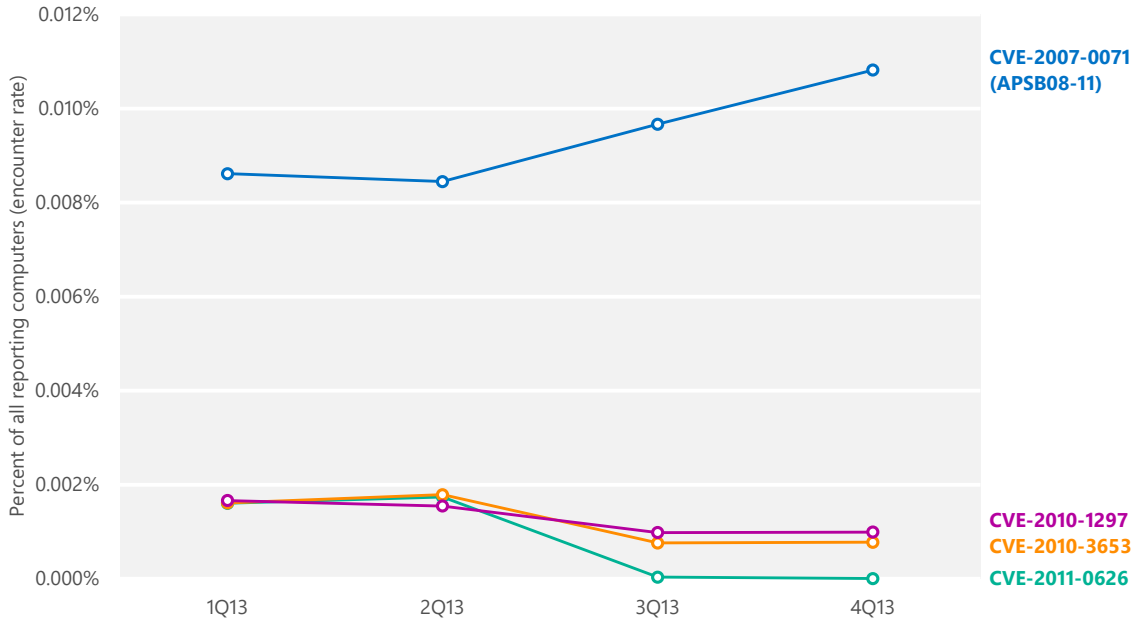



- Detections of exploits that affect Adobe Reader and Adobe Acrobat declined considerably from the first half of the year, in part due to the decreased prevalence of the Blacole exploit kit. Most of these detections were associated with the exploit family Win32/Pdfjsc.

## Adobe Flash Player exploits

Figure 24 shows the prevalence of different Adobe Flash Player exploits by quarter.

Figure 24. Adobe Flash Player exploits detected and blocked by Microsoft real-time antimalware products in 2013



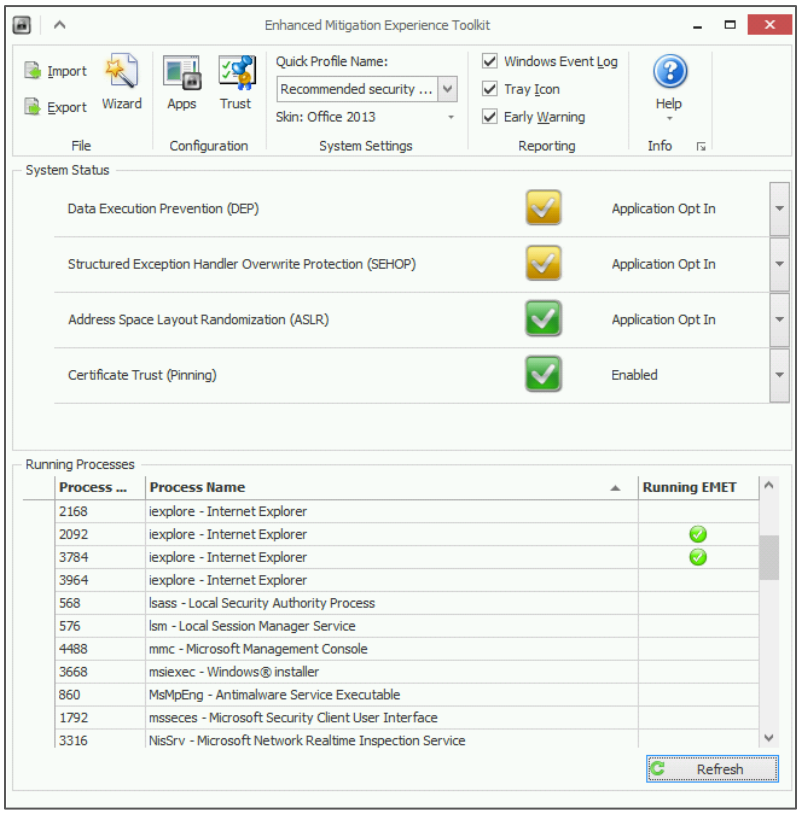

- CVE-2007-0071, the most commonly exploited Adobe Flash Player vulnerability in 2H13, is an invalid pointer vulnerability in some releases of Adobe Flash Player versions 8 and 9. Adobe released Security Bulletin APSB08-11 on April 8, 2008 to address the issue.
- CVE-2010-1297, the second most commonly 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 25. 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 26 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 26. 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:[10]

- *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.[11])
- *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

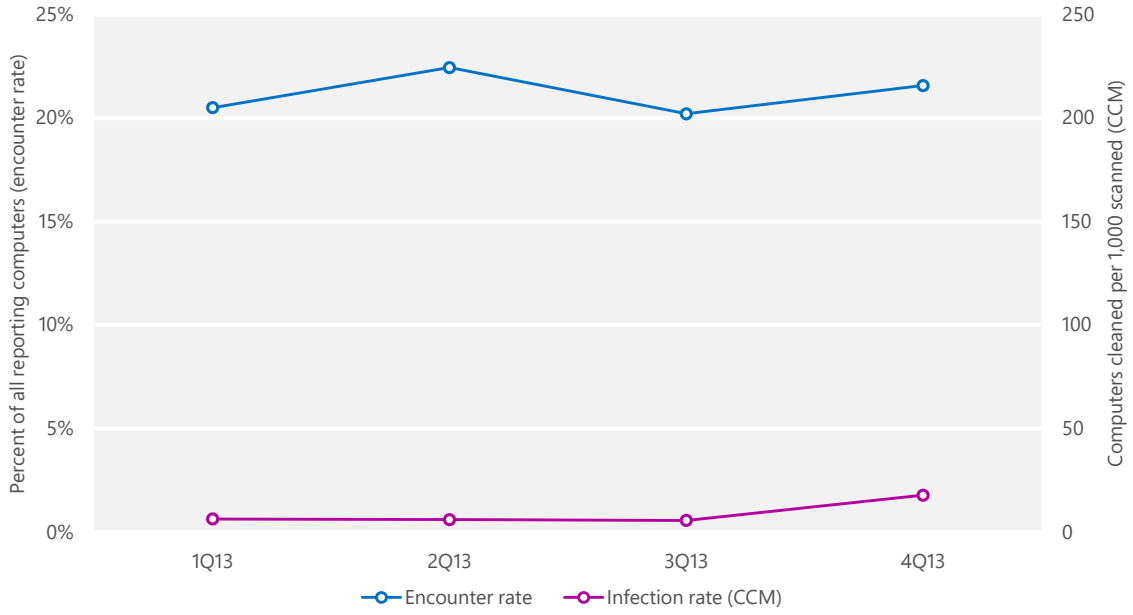
[10] Microsoft regularly reviews and refines its data collection methodology to improve its scope and accuracy. For this reason, the statistics presented in this volume of the *Microsoft Security Intelligence Report* may differ slightly from comparable statistics in previous volumes.

[11] For privacy statements and other information about the products and services that provide data for this report, see "Appendix B: Data sources" on page 115.

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

Figure 27 illustrates the difference between these two metrics.

Figure 27. Worldwide encounter and infection rates in 2013, by quarter



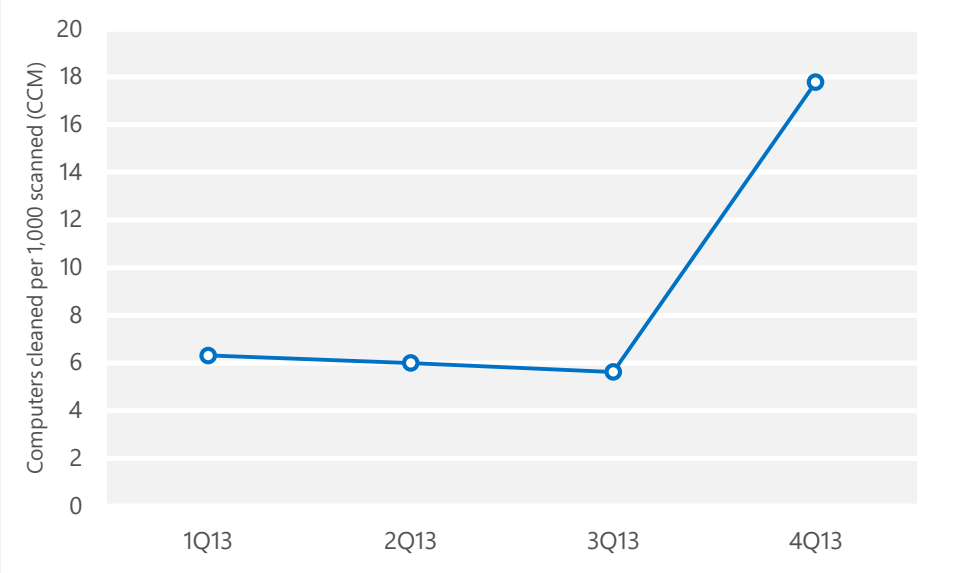

As Figure 27 shows, and as one would expect, malware encounters are much more common than malware infections. On average, about 21.2 percent of reporting computers worldwide encountered malware each quarter in 2013. At the same time, the MSRT removed malware from about 11.7 out of every 1,000 computers, 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 28. 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

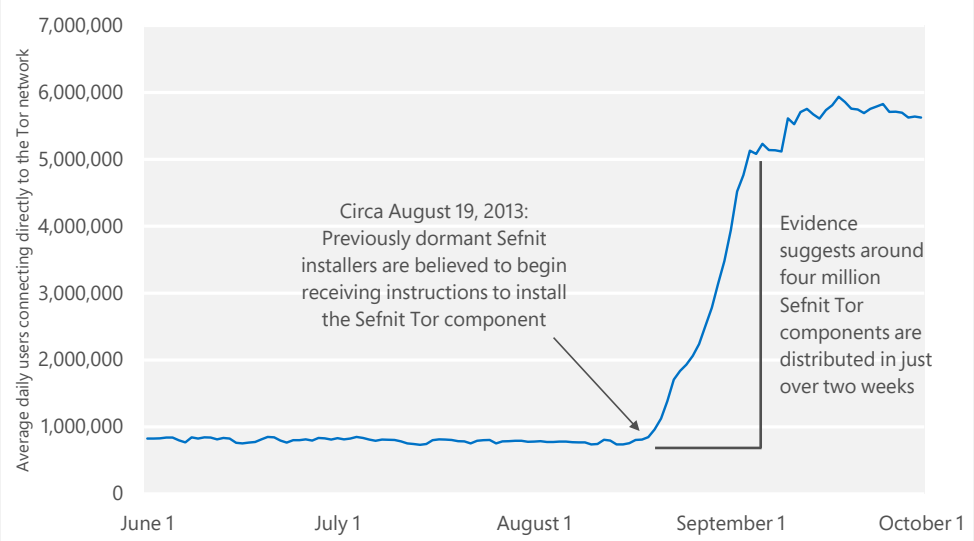
similar incident that primarily affected computers in Korea.) Detections of Rotbrow decreased considerably after December, and the MMPC expects the CCM infection rate to return to more typical levels in subsequent quarters as the MSRT and other security products resolve the remaining backlog of old Rotbrow 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 29.

Figure 29. 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.[12]

[12] 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 30. 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 30 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.

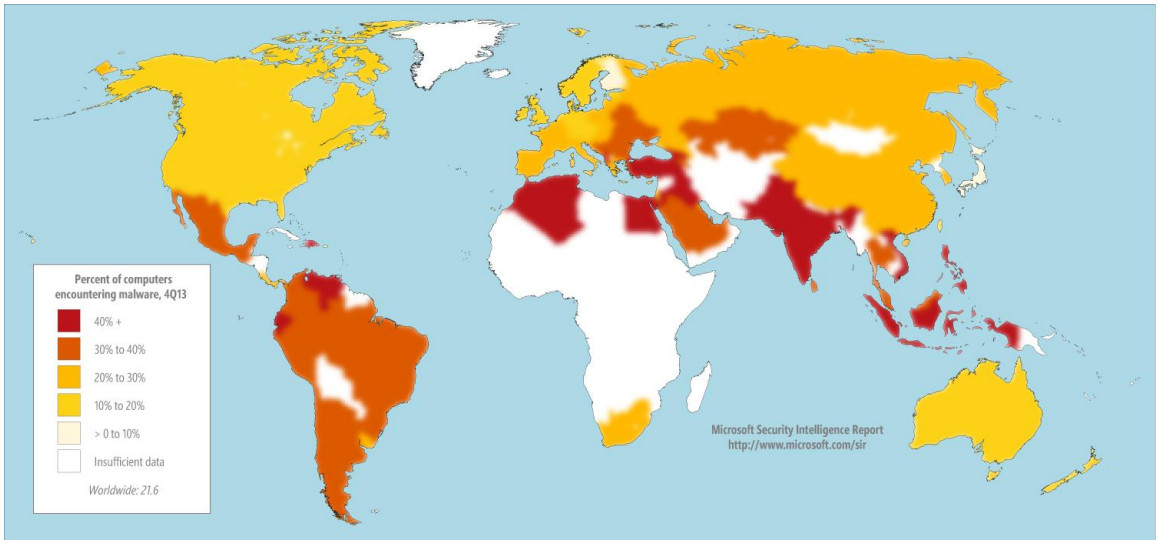
- The trojan family VBS/Miposa was unusually prevalent in Japan (8th in Japan, 254th worldwide). Miposa is a trojan that attempts to download and run Windows Scripting Host (.wsh) files. When used legitimately, .wsh files

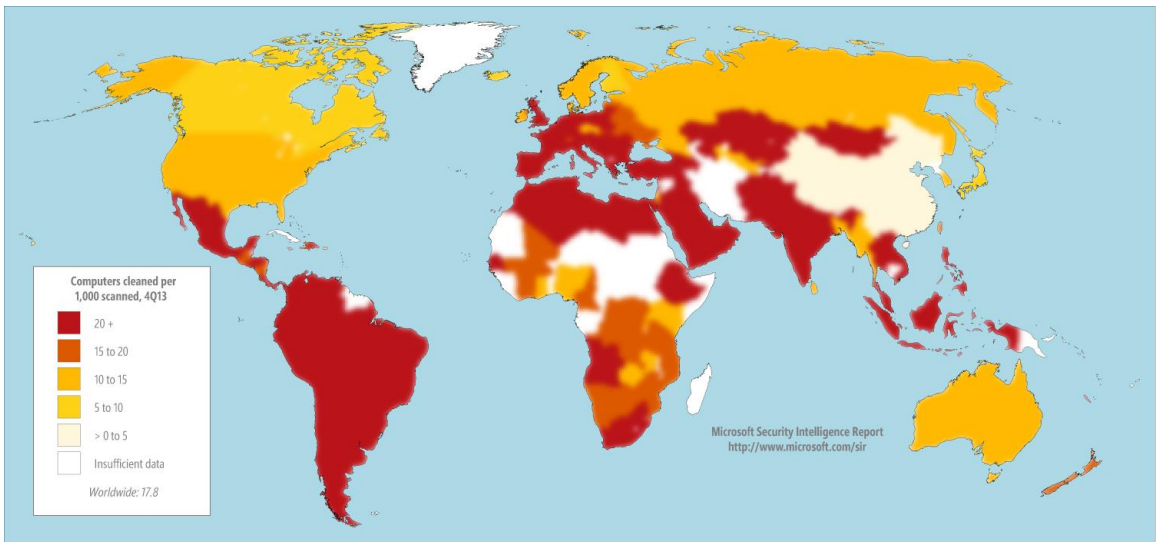
are used to automate tasks. When used maliciously, however, they may be used to run or download other files, including malware.

- 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 31 shows the infection and encounter rates in locations around the world in 4Q13.

Figure 31. 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 32 and Figure 33 show trends for the locations with the highest rates of detection as determined by encounter rate and CCM, respectively.

Figure 32. Trends for the five locations with the highest malware encounter rates in 2H13 (100,000 reporting computers minimum)

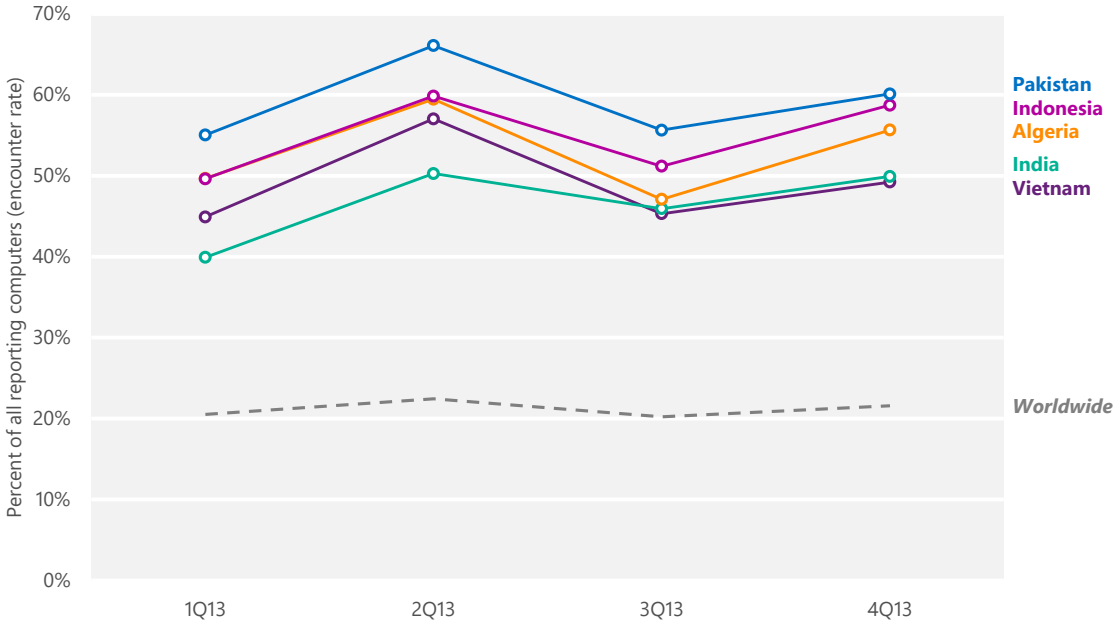
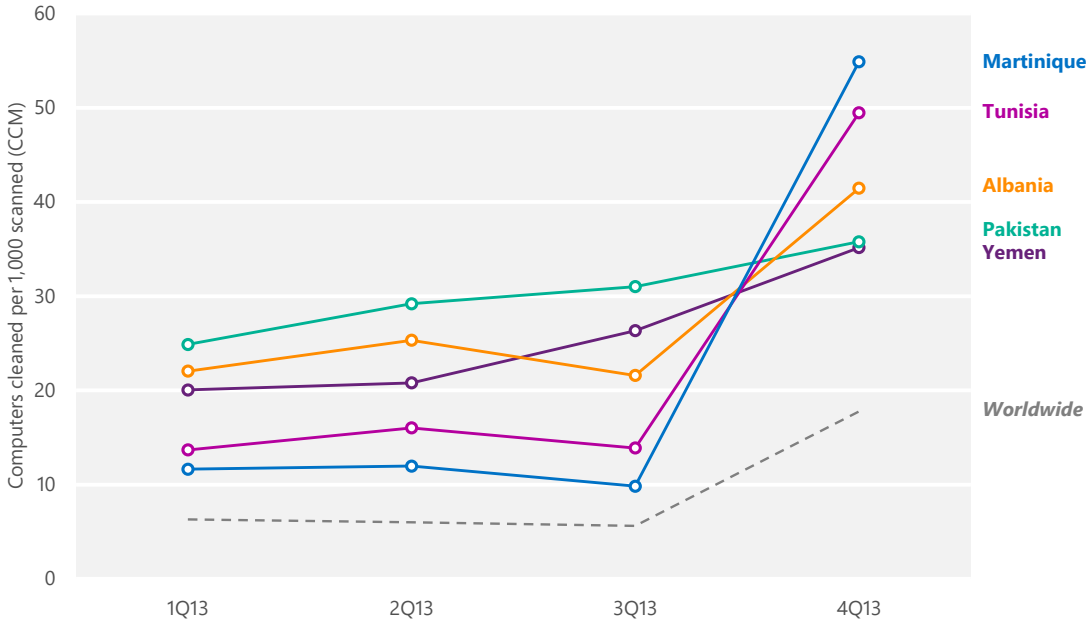



Figure 33. Trends for the five locations with the highest malware infection rates in 2H13, by CCM (100,000 MSRT executions minimum)




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

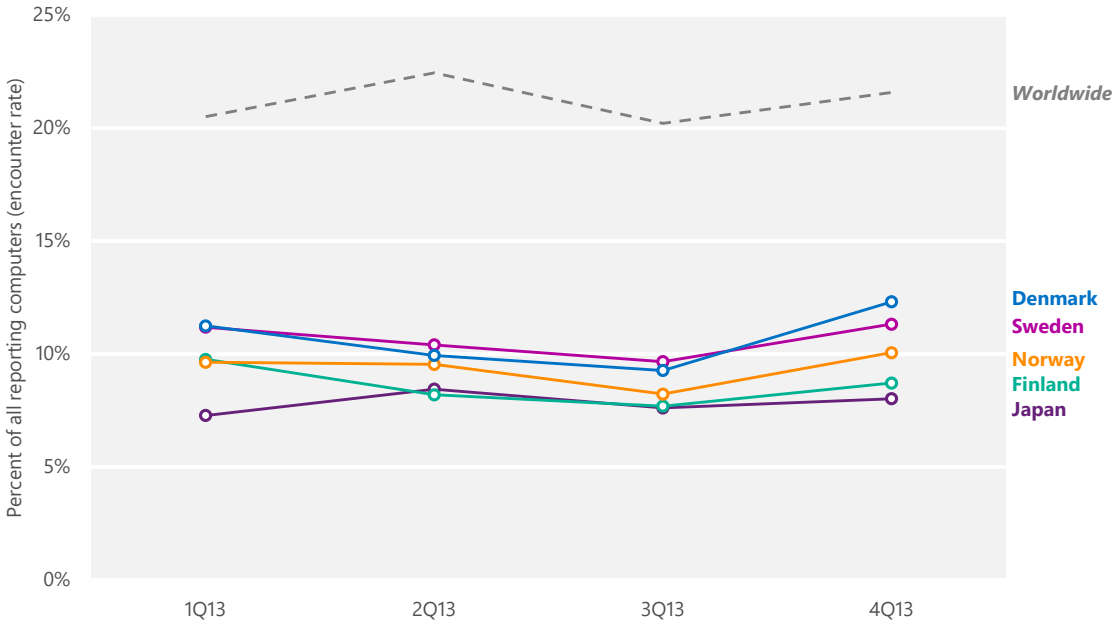
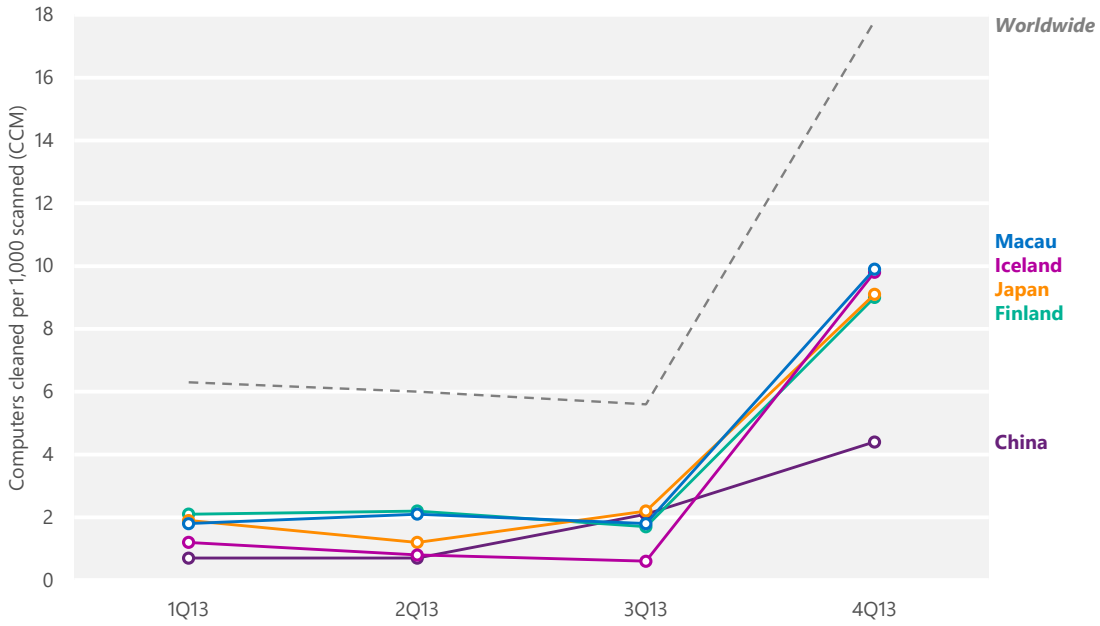



Figure 35. Trends for locations with low malware infection rates in 2H13, by CCM (100,000 reporting computers minimum)



- 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.[13]
- 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.

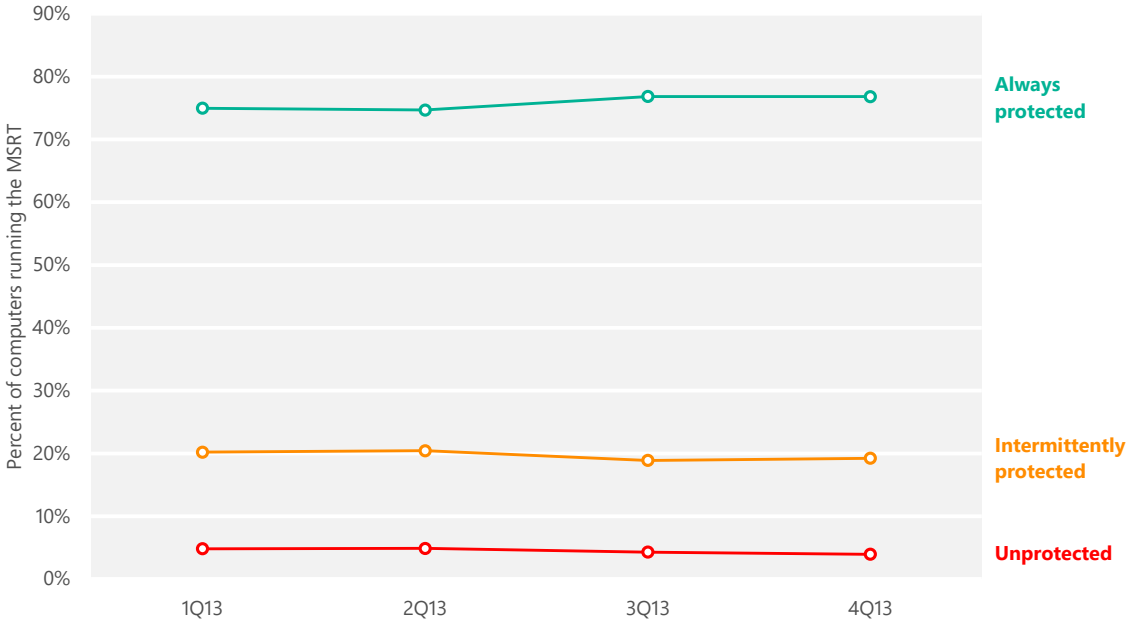
## Security software use

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 36 shows the percentage of computers worldwide that the MSRT found to be protected or unprotected by real-time security software each quarter in 2013.

---

[13] 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 36. Percentage of computers worldwide protected by real-time security software in 2013

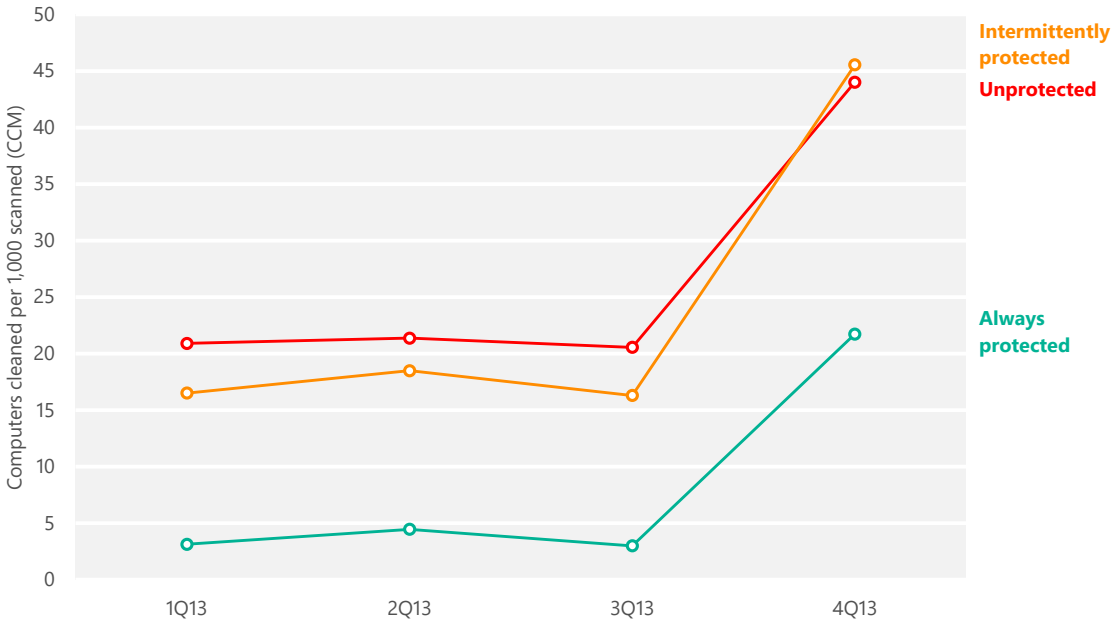



About three-quarters of computers world-wide consistently run real-time security software.

- A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In Figure 36, "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 37 compares infection rates with protection levels worldwide for each of the last four quarters.

Figure 37. 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.

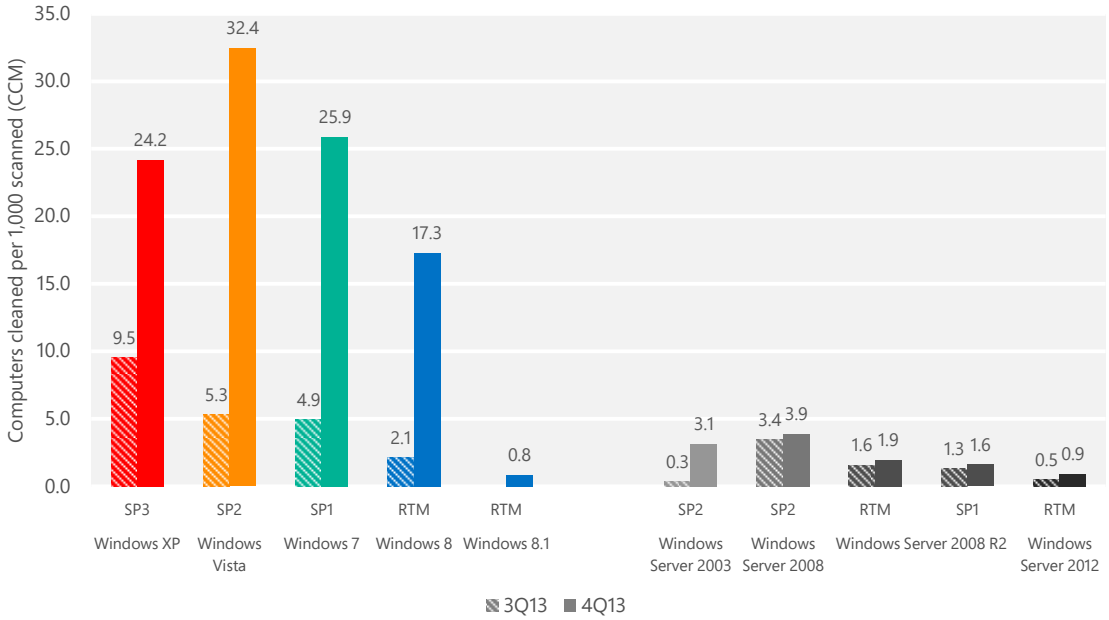
great as that for computers that were never found to be protected. Like unprotected computers, intermittently protected computers were about twice as likely to be infected in 4Q13 as computers that were always protected.

- 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 37 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 38 shows the infection rate for each currently supported Windows operating system/service pack combination.

Figure 38. 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.

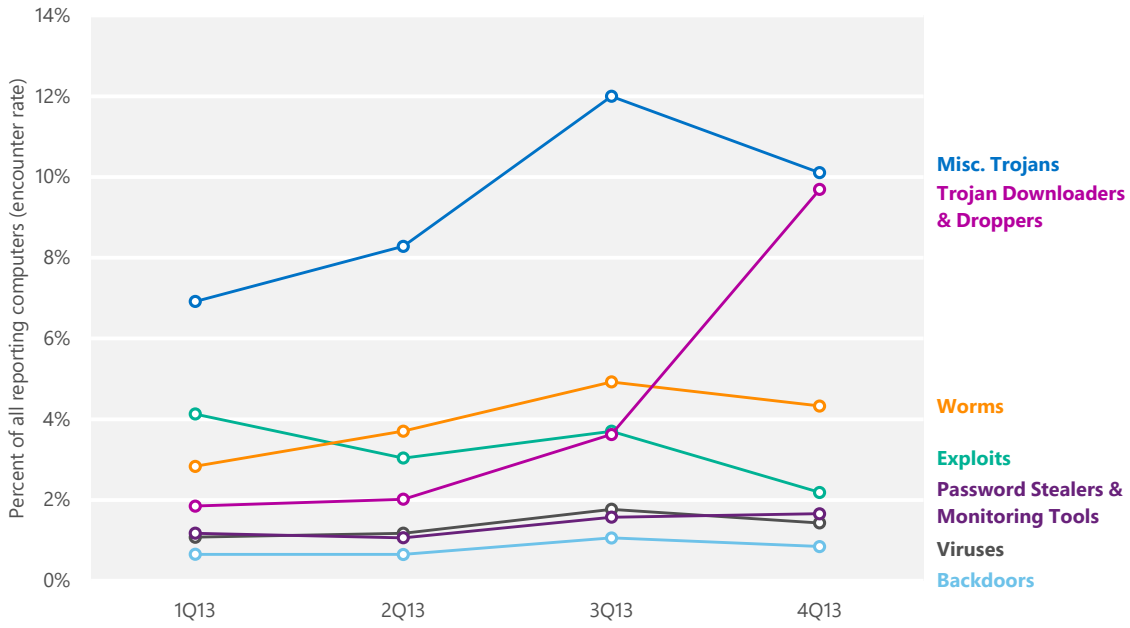
> Infection rates on all platforms were many times higher in 4Q13 due to Rotbrow.

- 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 39. 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 40 shows the relative prevalence of different categories of malware in several locations around the world in 4Q13.

Figure 40. 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 40, 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 30 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 40.
- Russia had the highest Miscellaneous Trojans encounter rate in Figure 40, 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 and encounter rates" on page 117 for more information about malware around the world.

## Threat families

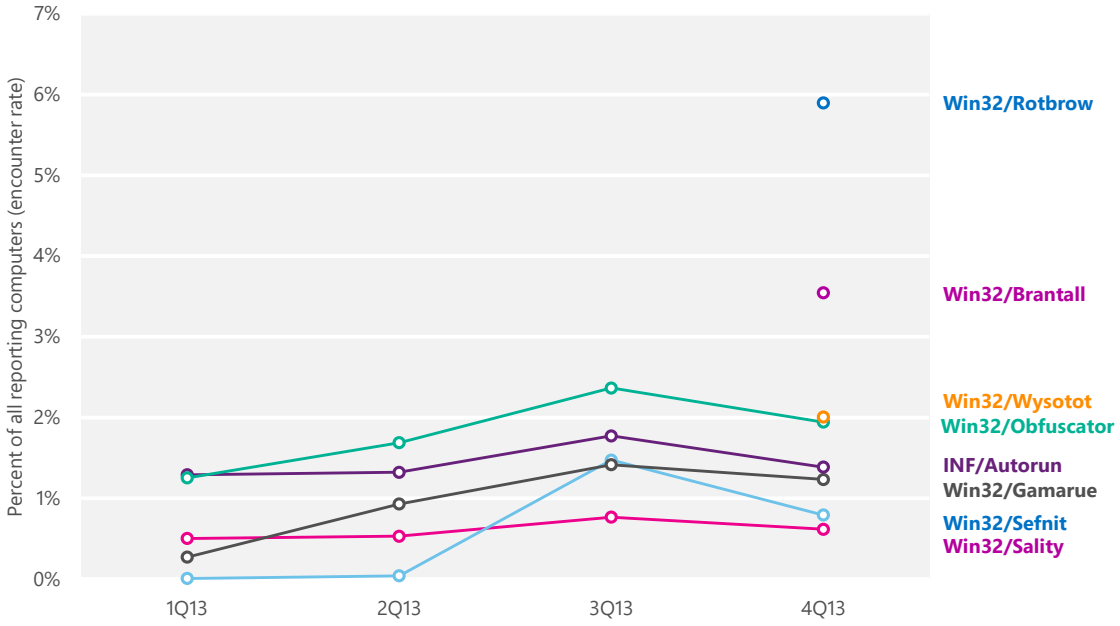
Figure 41 lists the top 10 malware families that were detected on computers by Microsoft real-time antimalware products worldwide in 2H13, with other quarters included for comparison.

Figure 41. 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 42 shows the detection trends for a number of families that increased or decreased significantly over the past four quarters.

Figure 42. 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 43 demonstrates how detections of the most prevalent families in 4Q13 ranked differently on different operating system/service pack combinations.

Figure 43. 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.[14]
- 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.

[14] 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

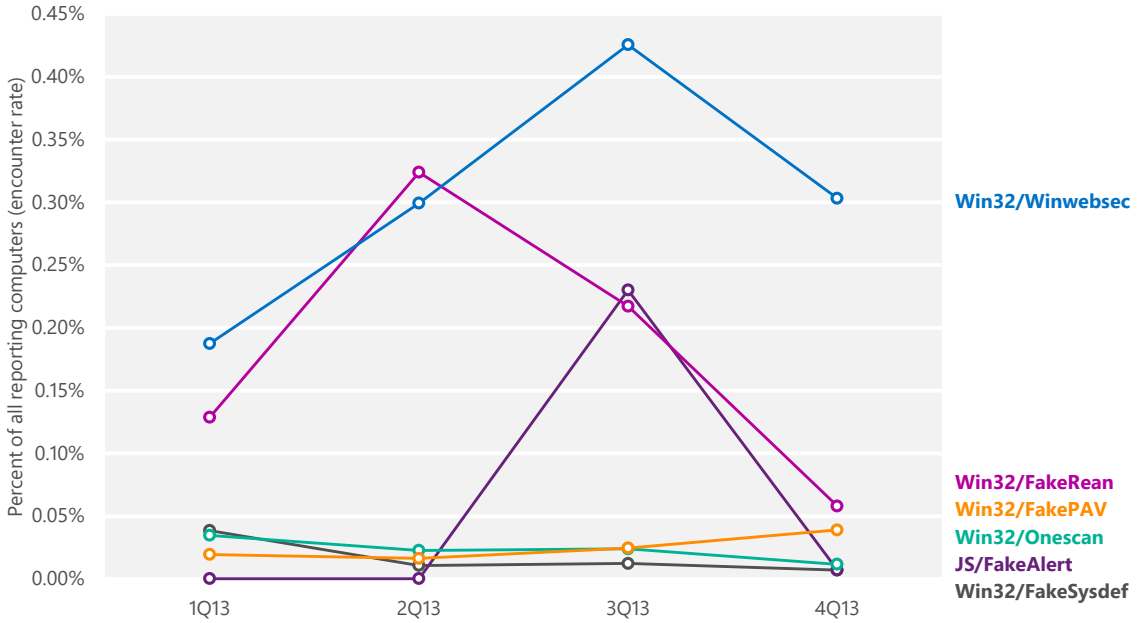
*Rogue security software* has become one of the most common methods that attackers use to swindle money from victims. Rogue security software, also known as *scareware*, is software that appears to be beneficial from a security perspective but provides limited or no security, generates erroneous or misleading 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 44. False branding used by a number of commonly detected rogue security software programs


Figure 45 shows detection trends for the most common rogue security software families detected in 2H13.

Figure 45. 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.

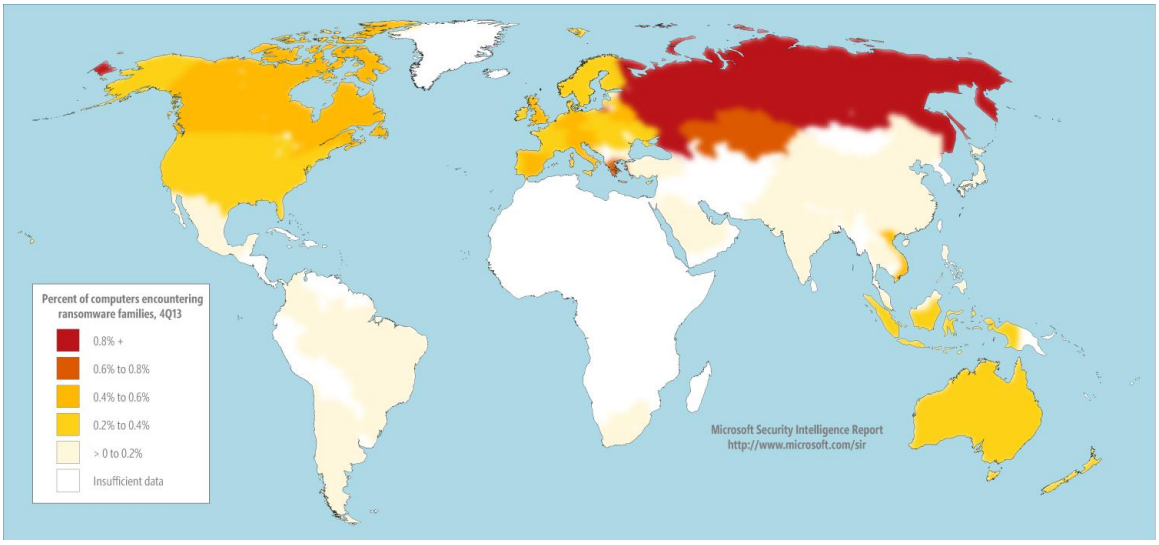
## Ransomware

*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 46. 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 47 shows encounter rates for ransomware families by country and region in 4Q13.

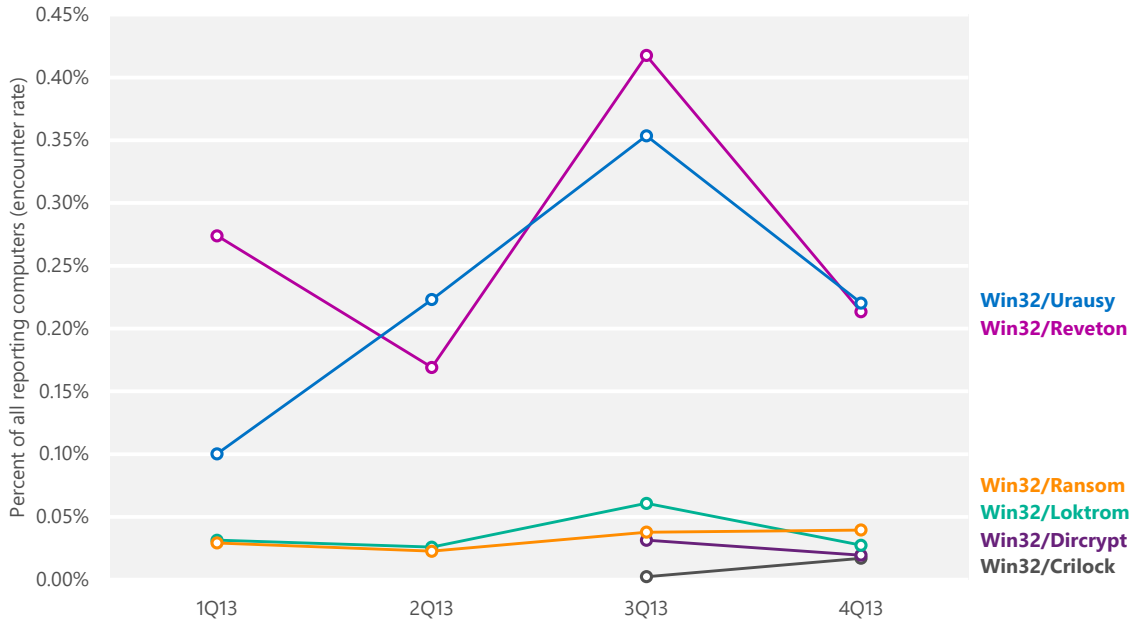
Figure 47. Encounter rates for ransomware families by country/region in 4Q13



- 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 48 displays encounter rate trends for several of the most commonly encountered ransomware families worldwide.

Figure 48. 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.

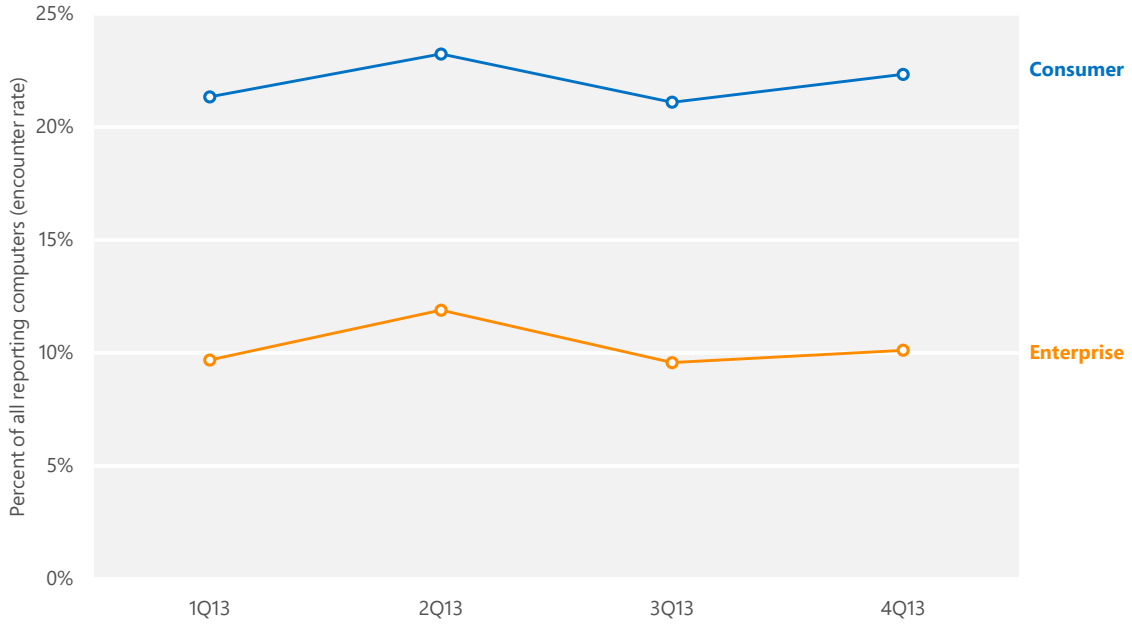
Visit www.microsoft.com/security/portal/mmpc/shared/ransomware.aspx for more information about ransomware and how computer users can avoid being taken advantage of by these threats.

## 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 49. 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 49 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 50 and Figure 51 list the top 10 families detected on domain-joined and non-domain computers, respectively, in 2H13.

Figure 50. 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% |

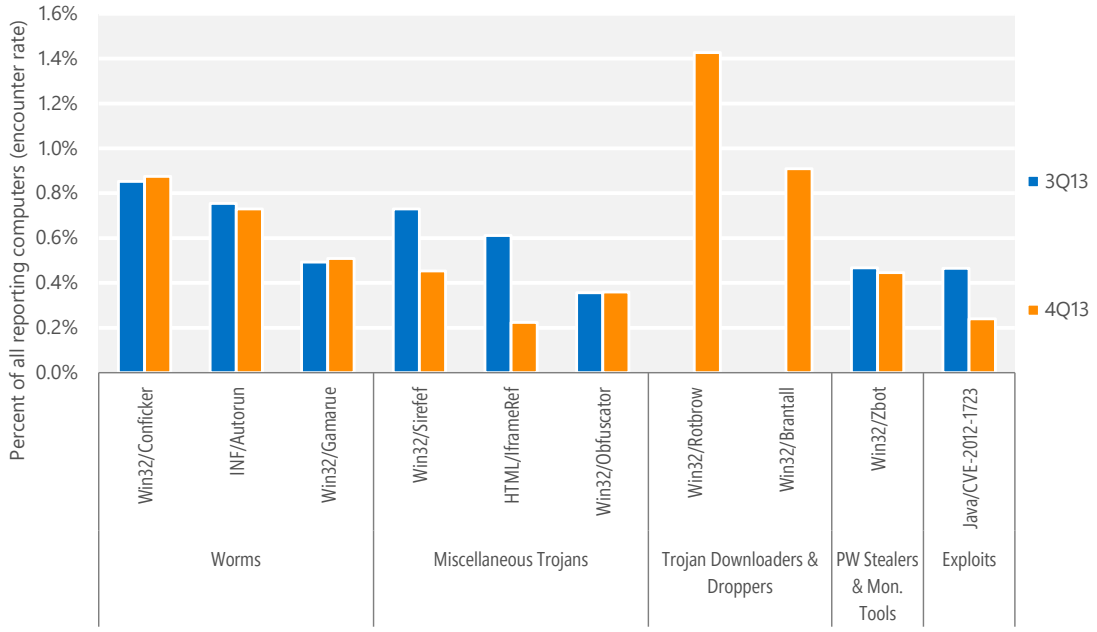
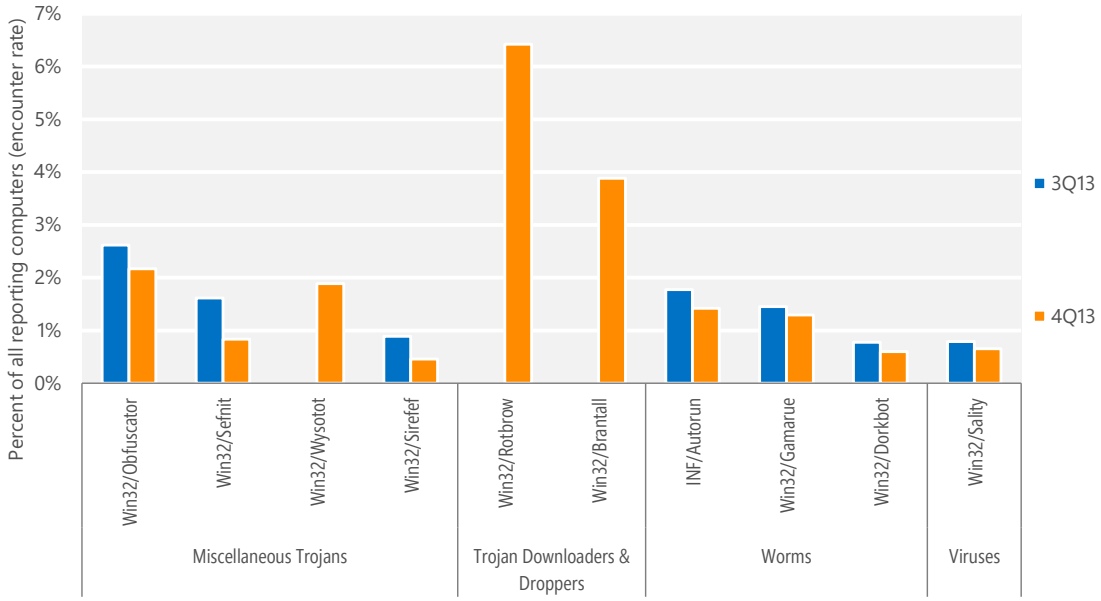


Figure 51. Quarterly trends for the top 10 families detected on non-domain computers in 2H13, by percentage of computers encountering each family

| 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" on page 103 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.

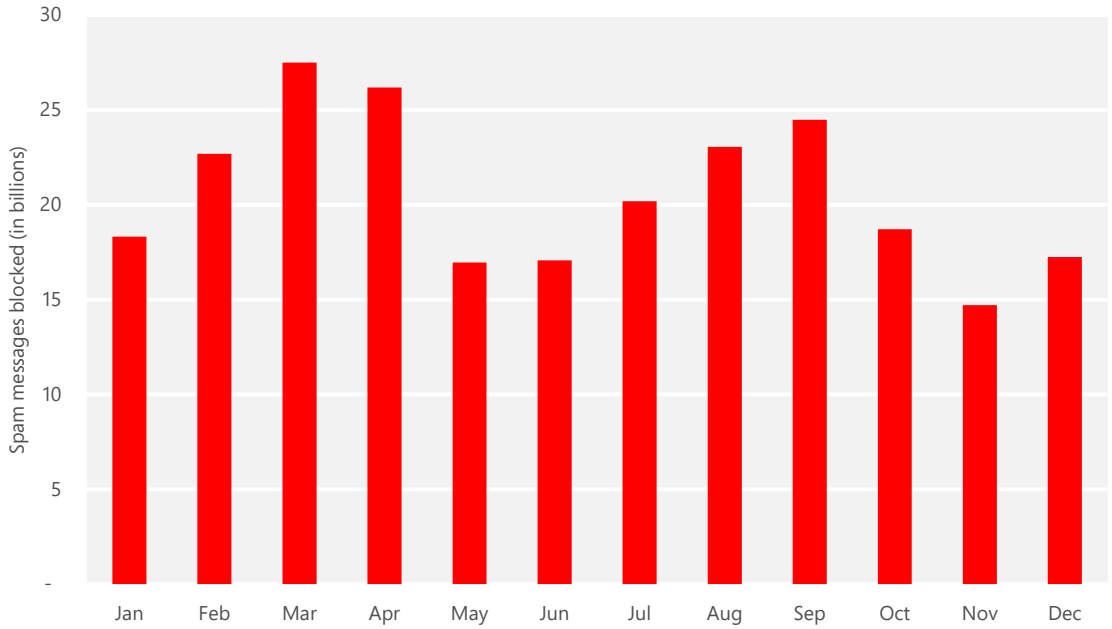
# Email threats

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.

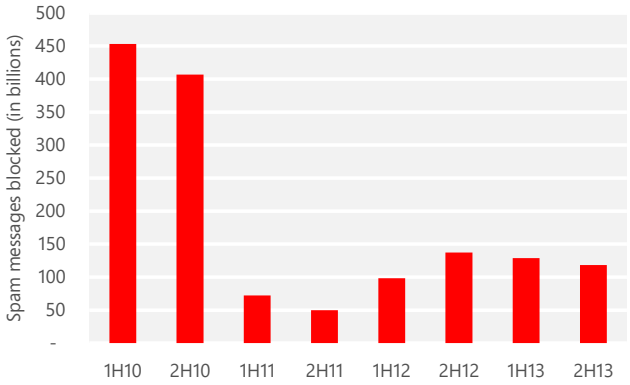
Figure 52. Messages blocked by Exchange Online Protection in 2013, by month




- 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 55. 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).[15] 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.

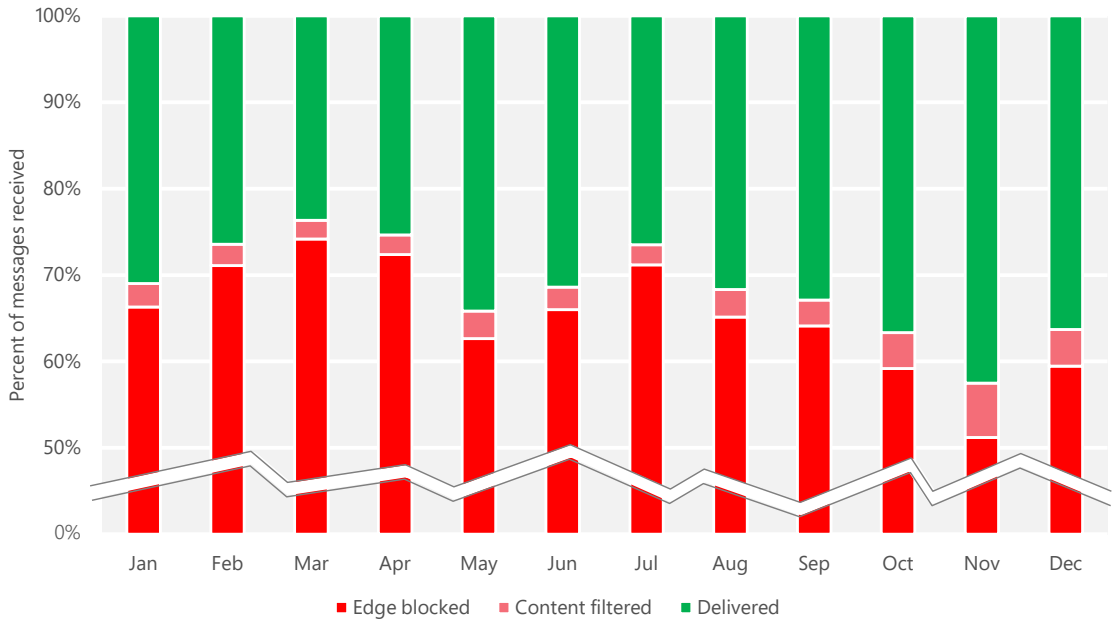
Figure 53. Messages blocked by Exchange Online Protection each half-year period, 1H10–2H13




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.

[15] 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 54. Percentages of incoming messages blocked, categorized as bulk email, and delivered, each month in 2013



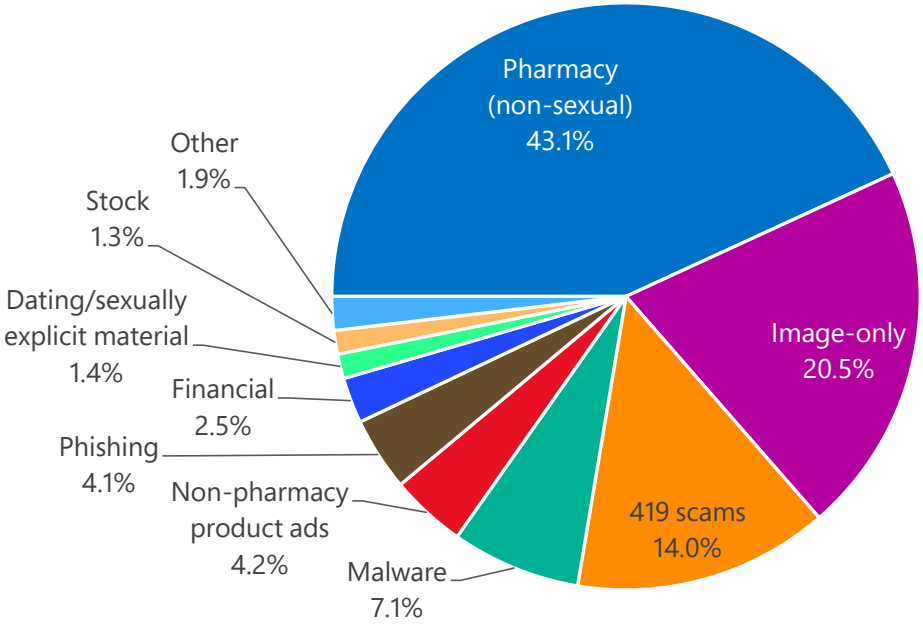

- Between 51.2 and 71.2 percent of incoming messages were blocked at the network edge each month in 2H13, which means that only 28.8 to 48.8 percent of incoming messages had to be subjected to the more resource-intensive content filtering process. Between 8.1 and 12.9 percent of the remaining messages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

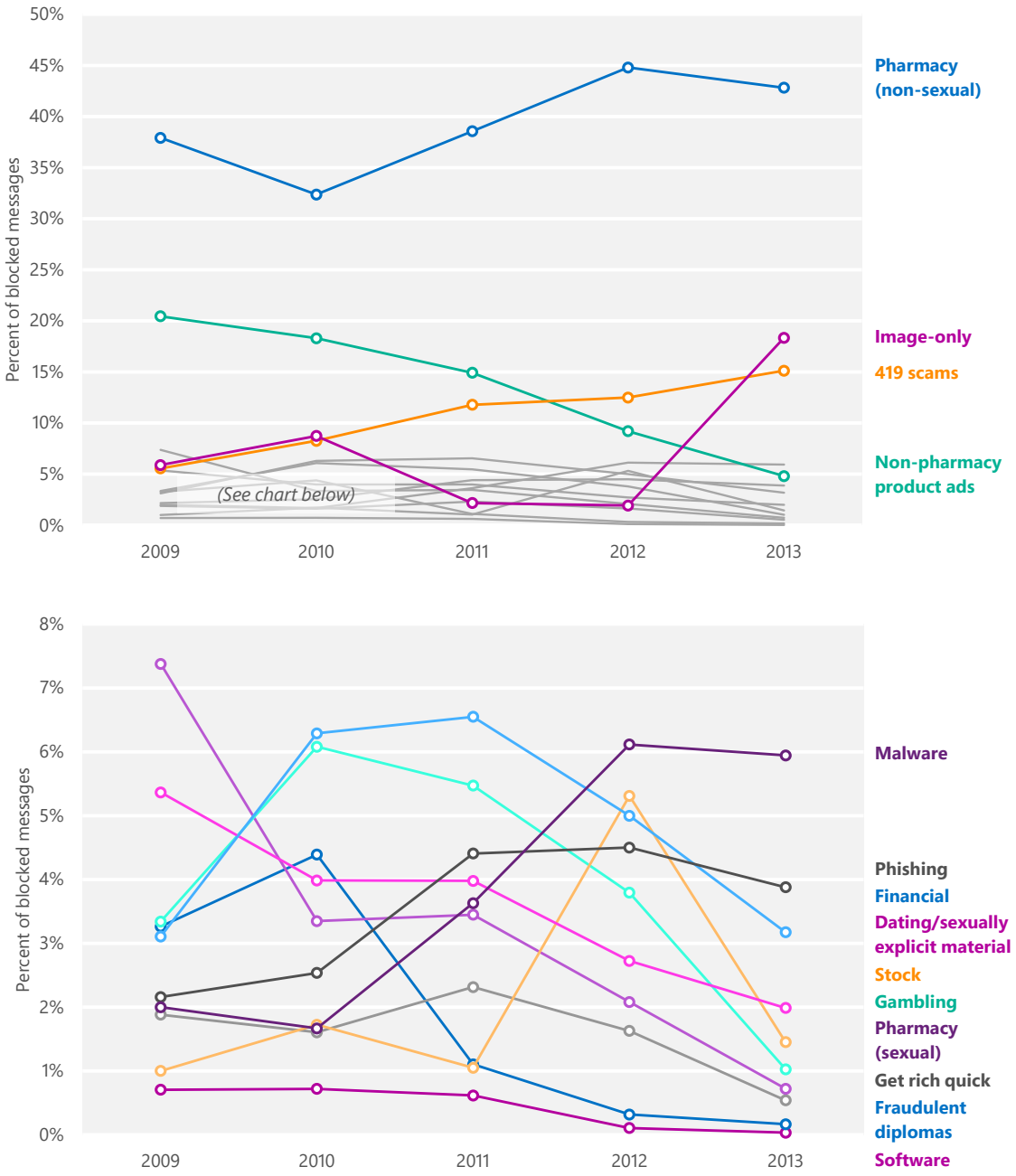
The Exchange Online Protection content filters recognize several different common types of spam messages. Figure 55 shows the relative prevalence of the spam types that were detected from July to October 2013.

Figure 55. 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 56. 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

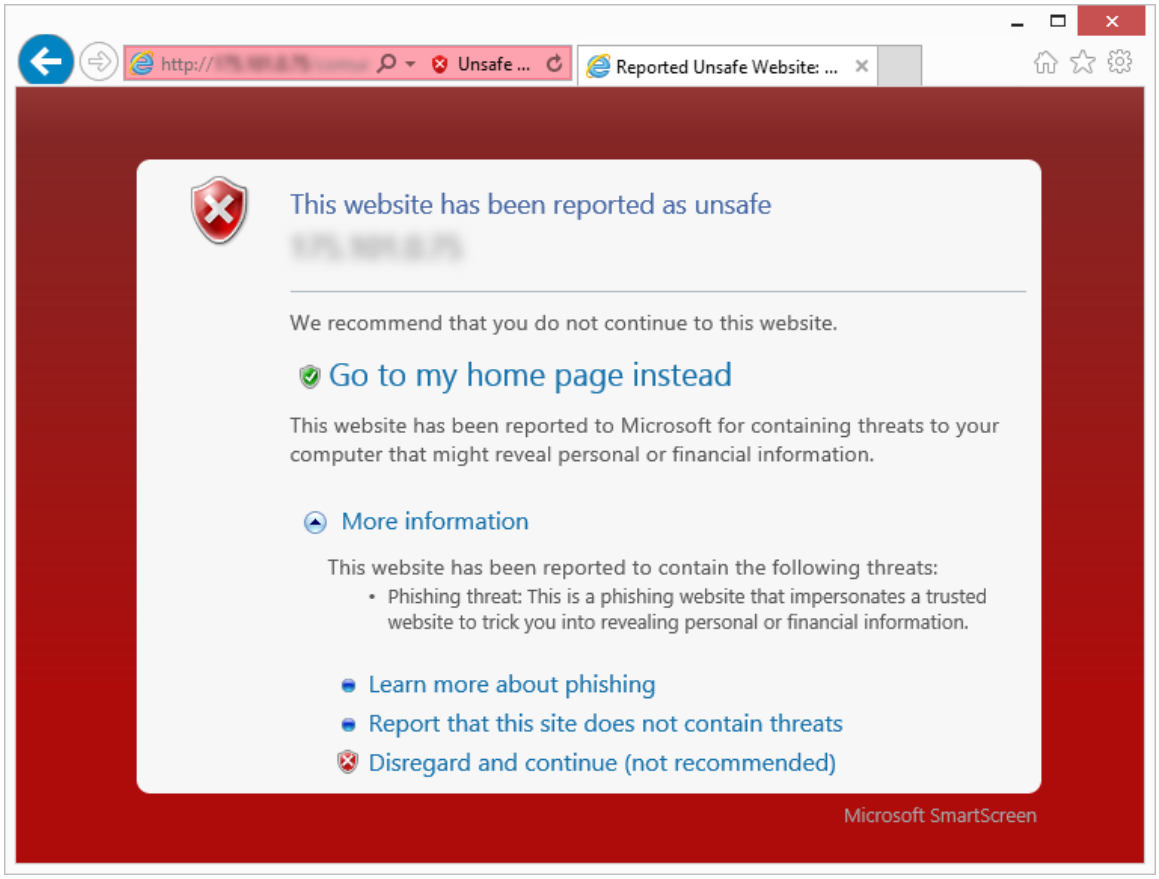
In addition to using a filtering service such as Exchange Online Protection, organizations can take a number of steps to reduce the risks and inconvenience of unwanted email. Such steps include implementing email authentication techniques and observing best practices for sending and receiving email. 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" on page 115 for more information about the products and services that provided data for this report.)

Figure 57. 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 58.

Figure 58. How Microsoft tracks phishing impressions

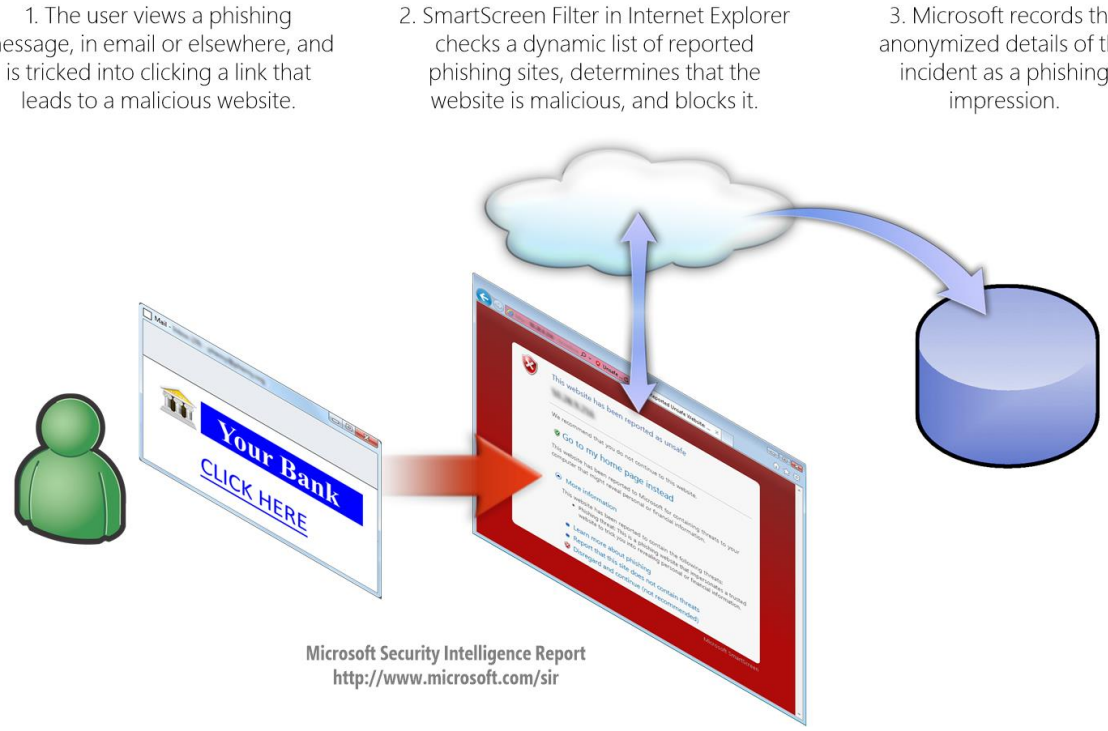
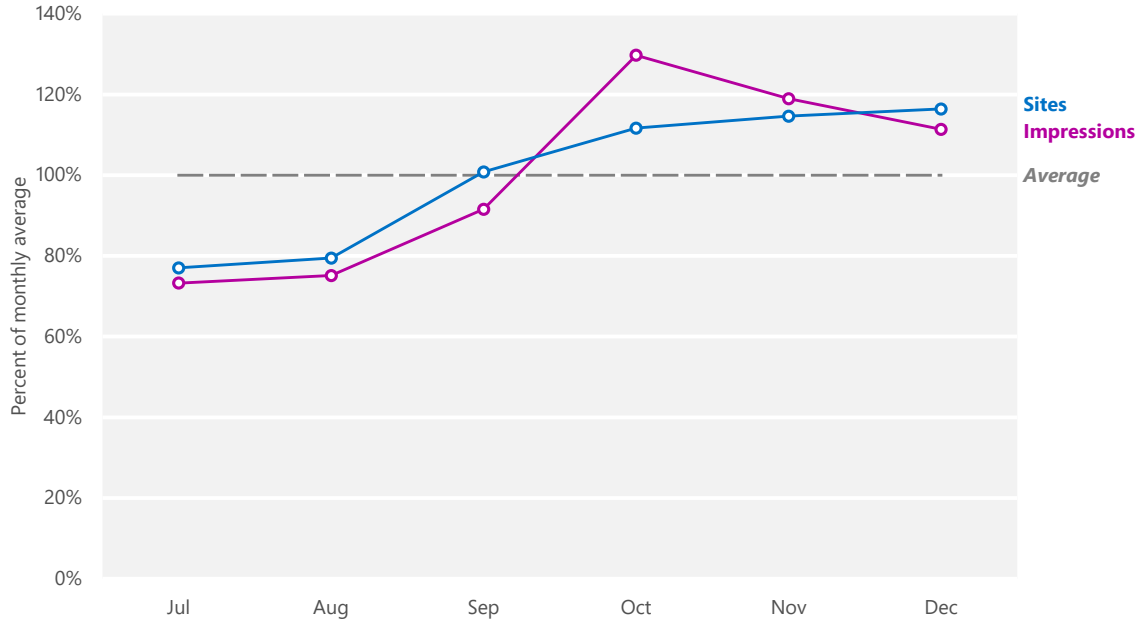


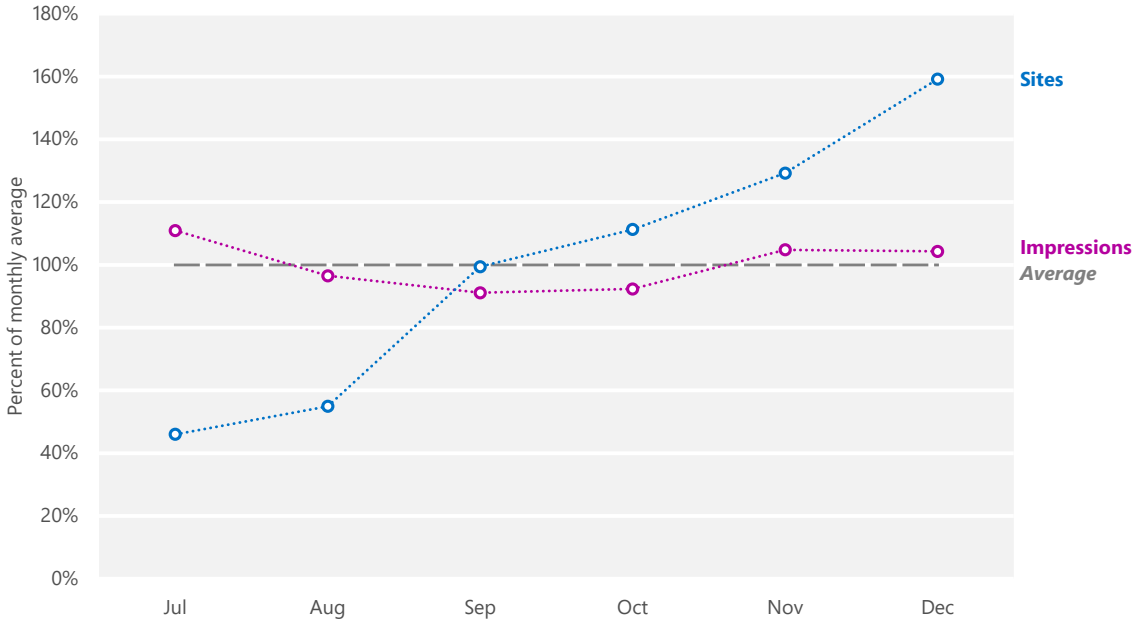

Figure 59 and Figure 60 illustrate the volume of phishing impressions tracked by SmartScreen Filter each month in 2H13 across all devices and on mobile devices running Windows Phone 8, compared to the volume of distinct phishing URLs visited.

Figure 59. 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 60. 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 61. Impressions across all devices for each type of phishing site, July–December 2013, as reported by SmartScreen Filter

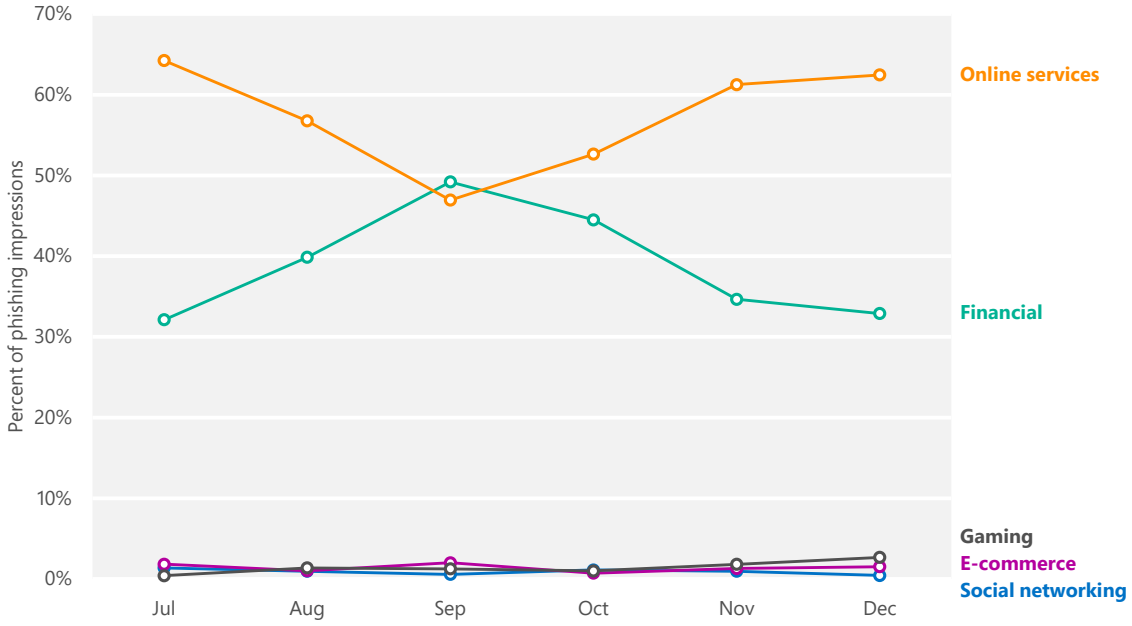
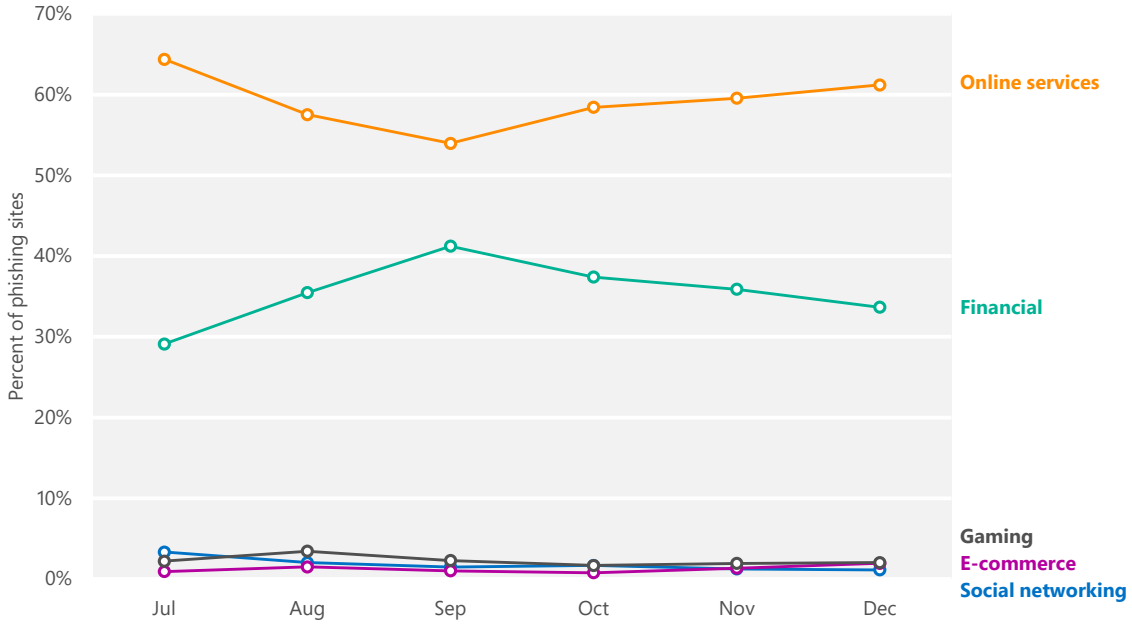



Figure 62. Unique phishing URLs visited by Internet Explorer running on all devices for each type of phishing site, July–December 2013




- 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 63 and Figure 64.

Figure 63. Impressions reported by SmartScreen Filter on Windows Phone 8 for each type of phishing site, July–December 2013

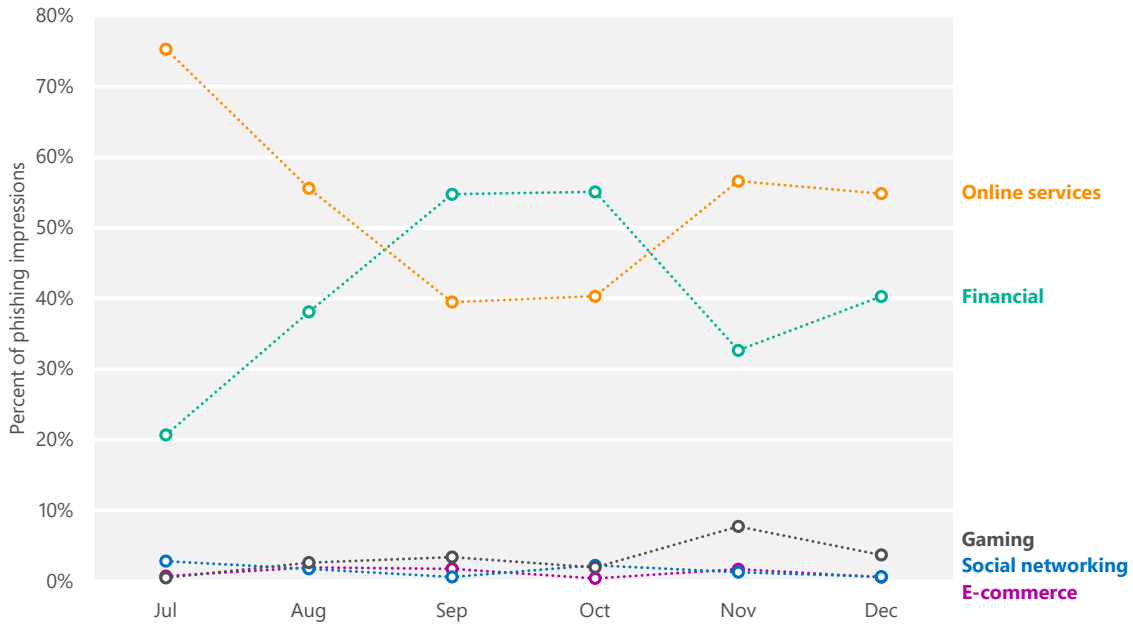
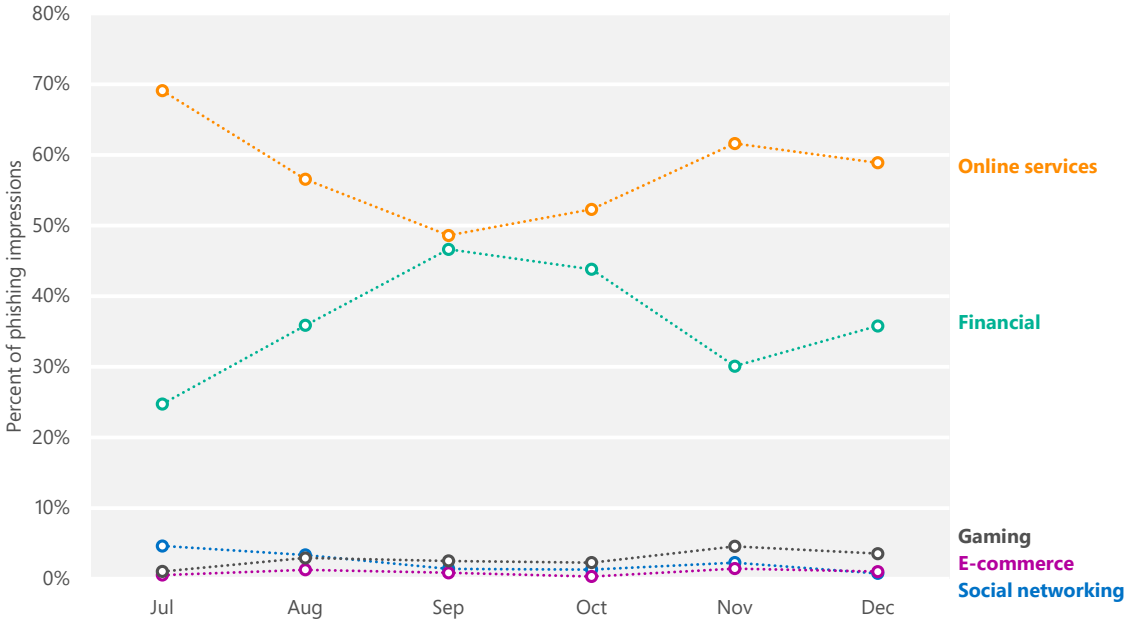


Figure 64. Unique phishing URLs visited by Internet Explorer on Windows Phone 8 for each type of phishing site, July–December 2013, by type of target




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

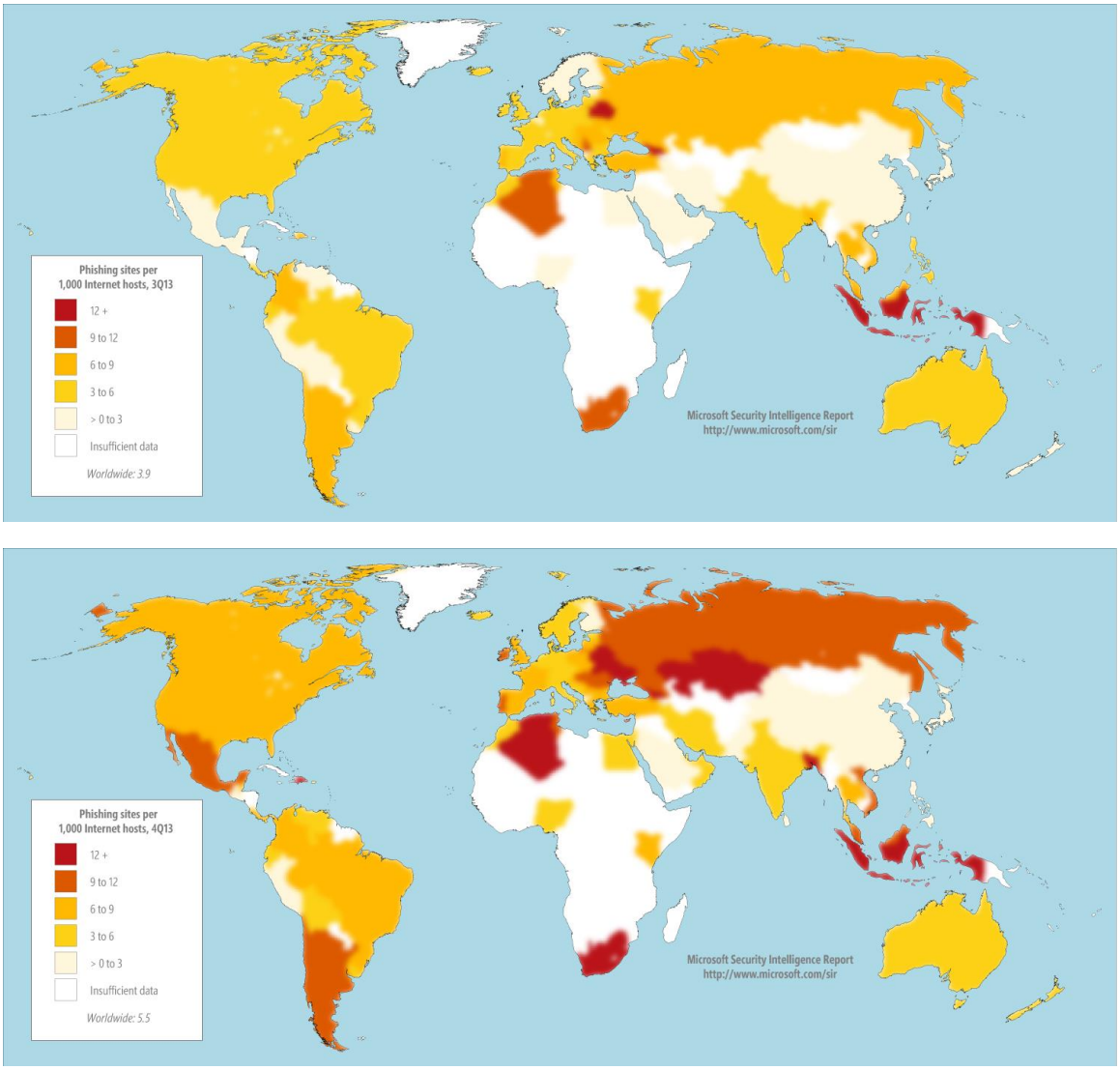
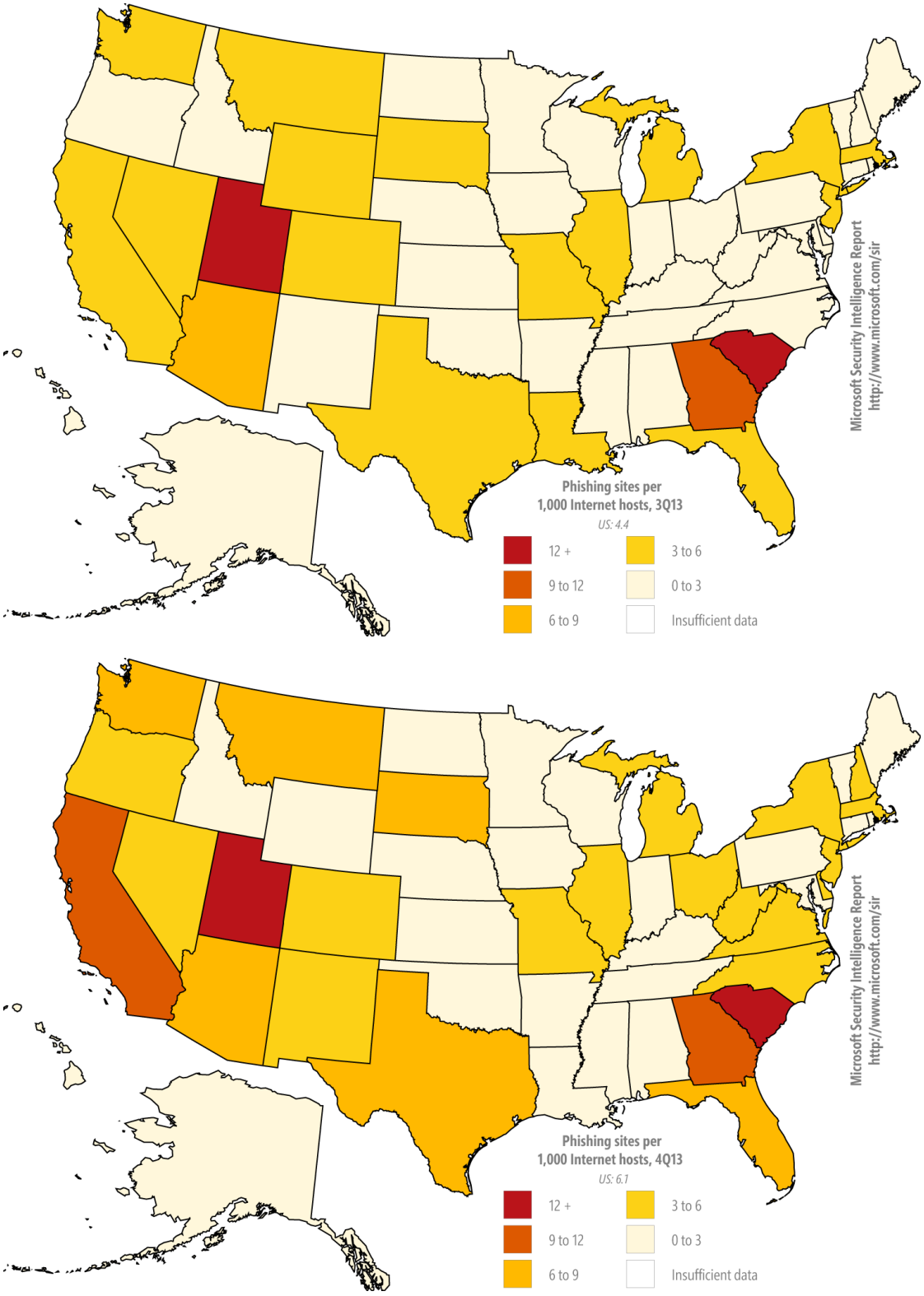


Figure 66. Phishing sites per 1,000 Internet hosts for US states in 3Q13 (top) and 4Q13 (bottom)



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

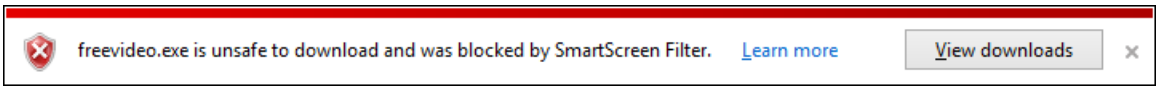
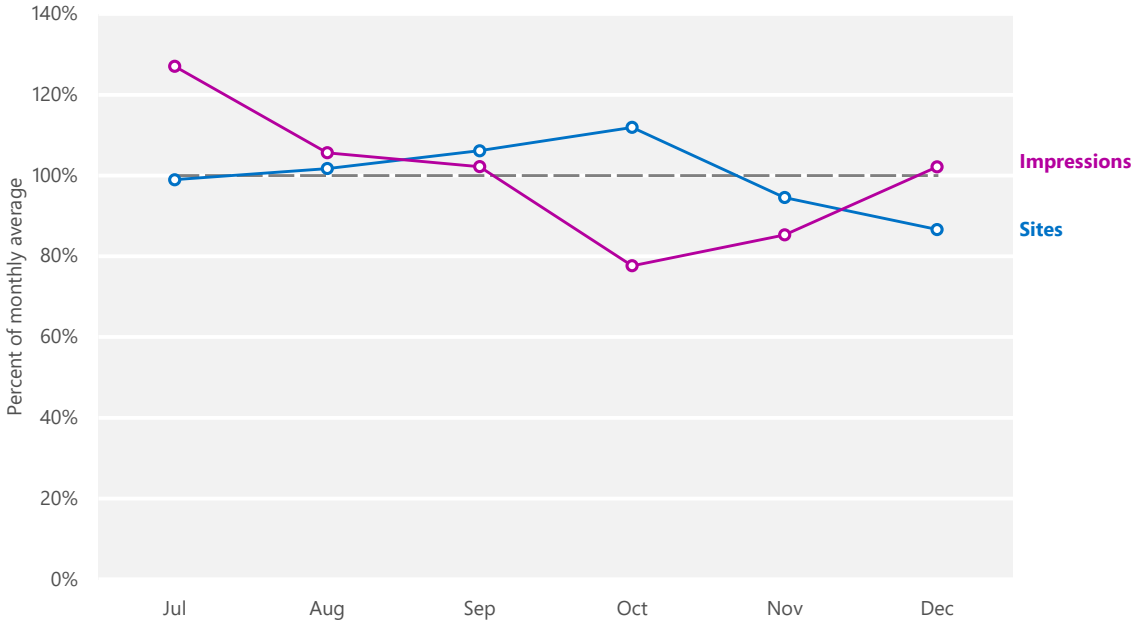



Figure 68 compares the volume of active malware hosting sites in the Microsoft database each month with the volume of malware impressions tracked by Internet Explorer.

Figure 68. 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 69 and Figure 70 show the types of threats hosted at URLs that were blocked by SmartScreen Filter in 2H13.

Figure 69. Categories of malware found at sites blocked by SmartScreen Filter in 2H13, by percent of all impressions

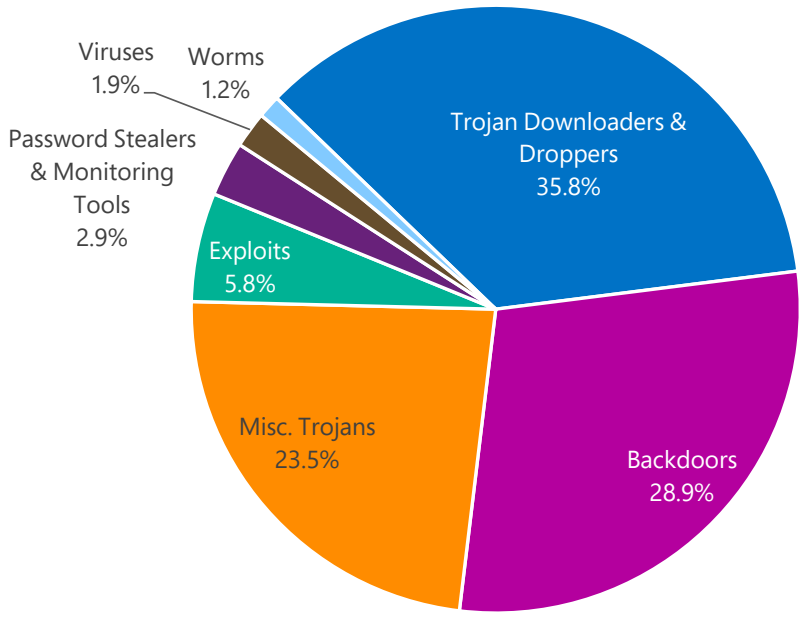



Figure 70. Top families found at sites blocked by SmartScreen Filter in 2H13, by percent of all malware impressions

| | 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 71 and Figure 72 show the geographic distribution of malware hosting sites reported to Microsoft in 2H13.

Figure 71. Malware distribution sites per 1,000 Internet hosts for locations around the world in 3Q13 (top) and 4Q13 (bottom)

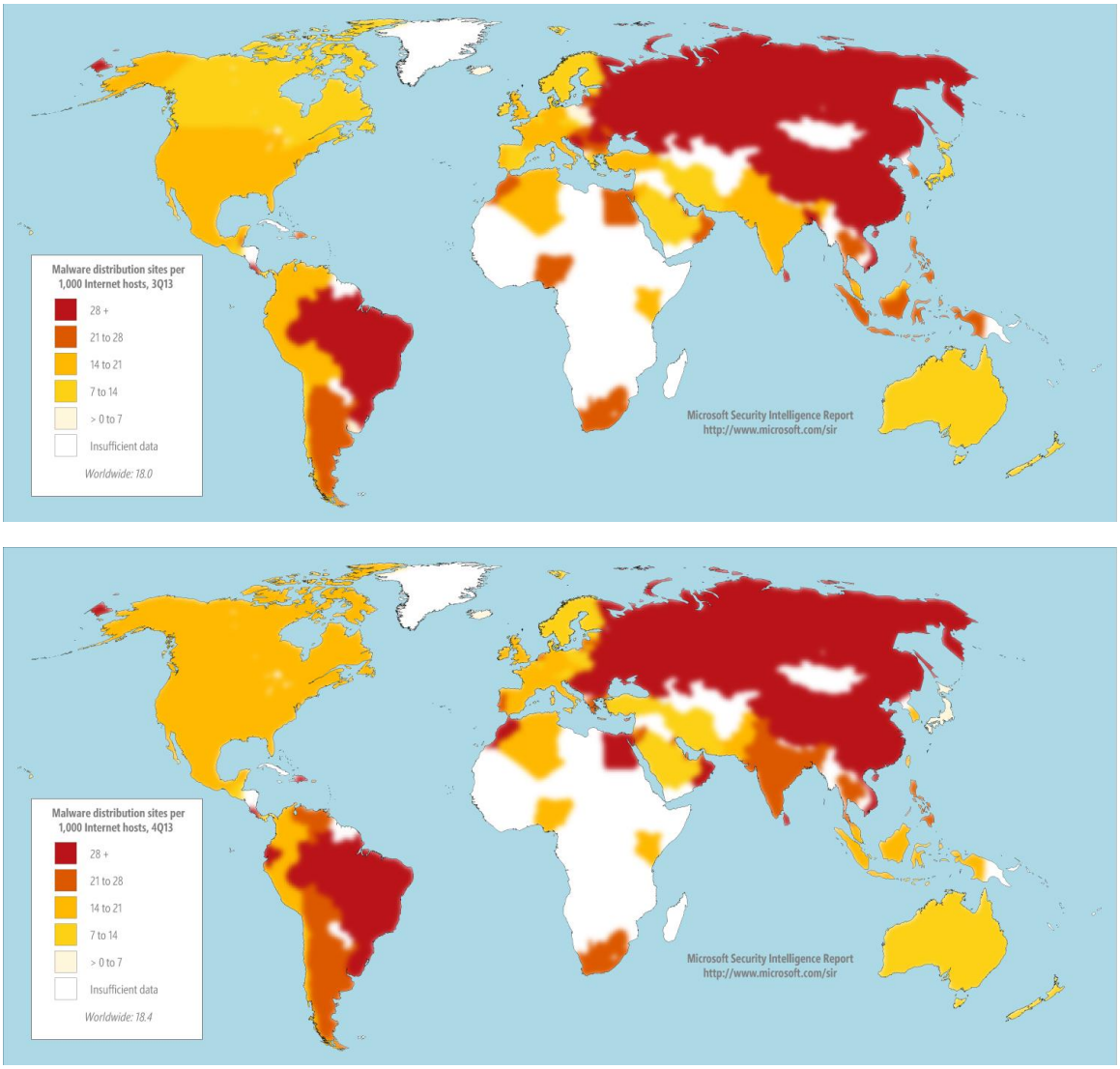
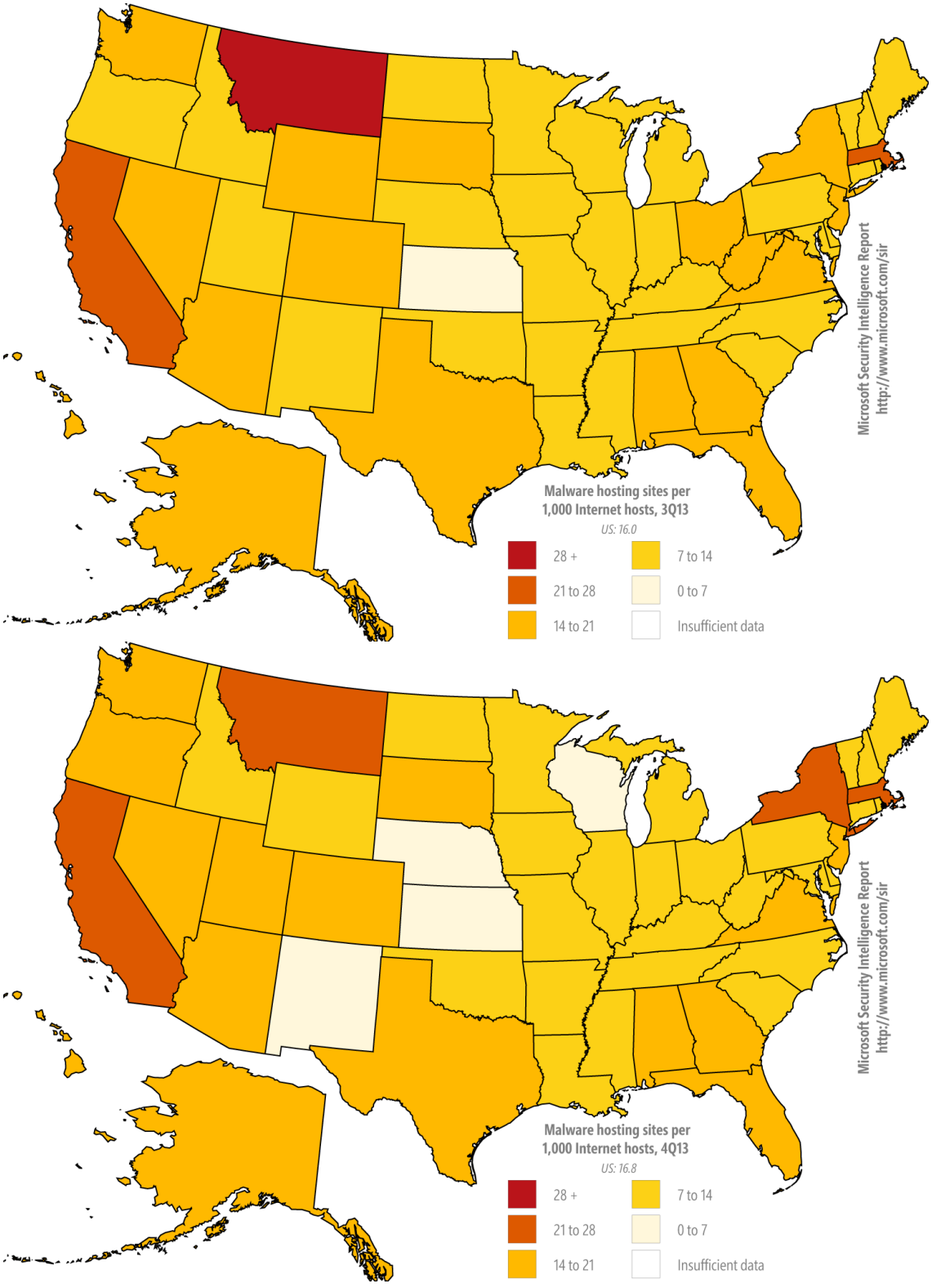


Figure 72. Malware distribution sites per 1,000 Internet hosts for US states in 3Q13 (top) and 4Q13 (bottom)



- 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).

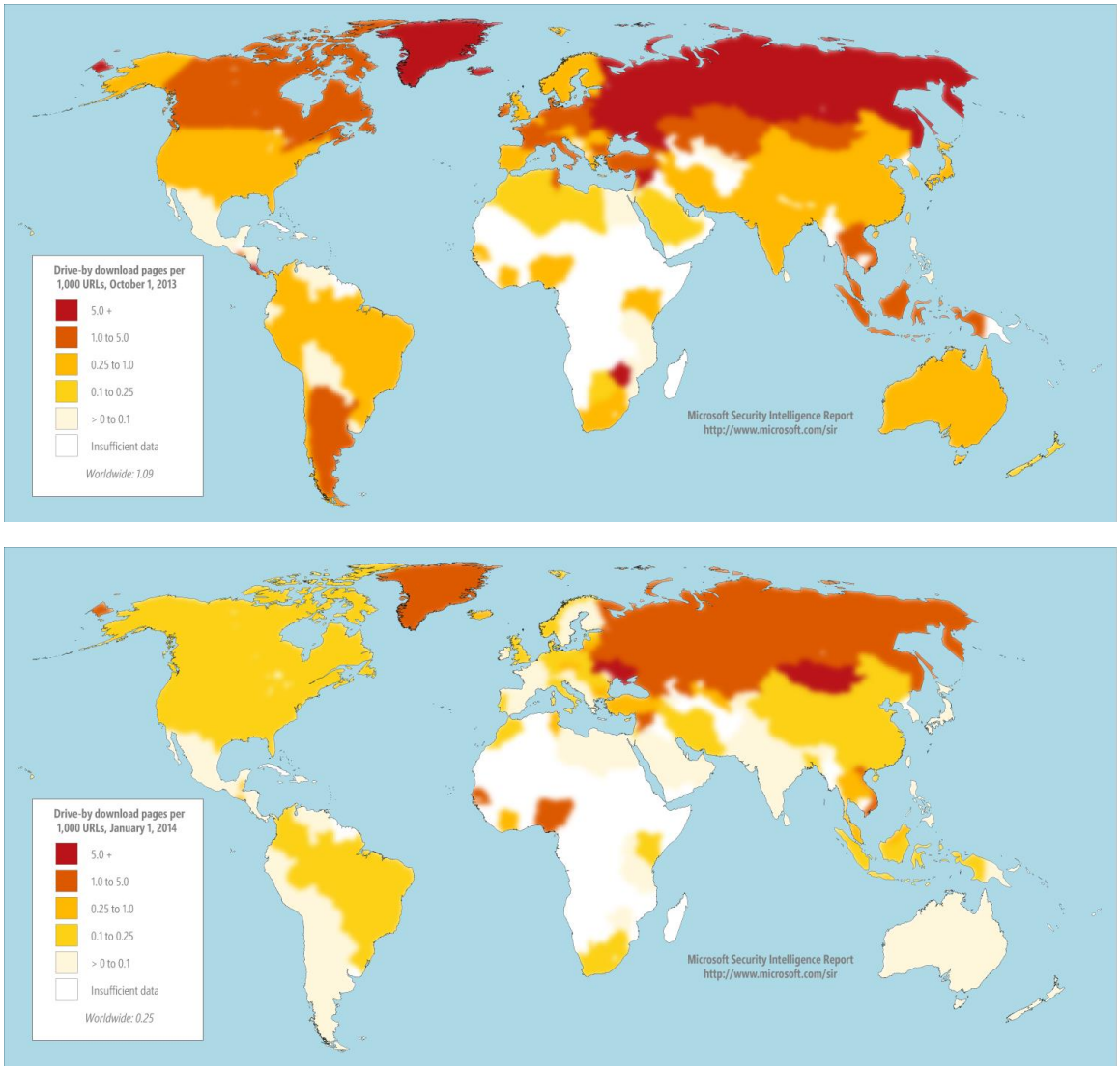
### Drive-by download sites

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

Figure 73. 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

# Mitigating risk

**Malware at Microsoft: Dealing with threats in the Microsoft environment.....103**

# Malware at Microsoft: Dealing with threats in the Microsoft environment

***Microsoft IT***

*Microsoft IT provides information technology services internally for Microsoft employees and resources. Microsoft IT manages 600,000 devices for 180,000 users across more than 100 countries and regions worldwide, with approximately 2 million remote connections per month. Safeguarding a computing infrastructure of this size requires implementation of strong security policies, technology to help keep malware off the network and away from mission-critical resources, and dealing with malware outbreaks swiftly and comprehensively when they occur.*

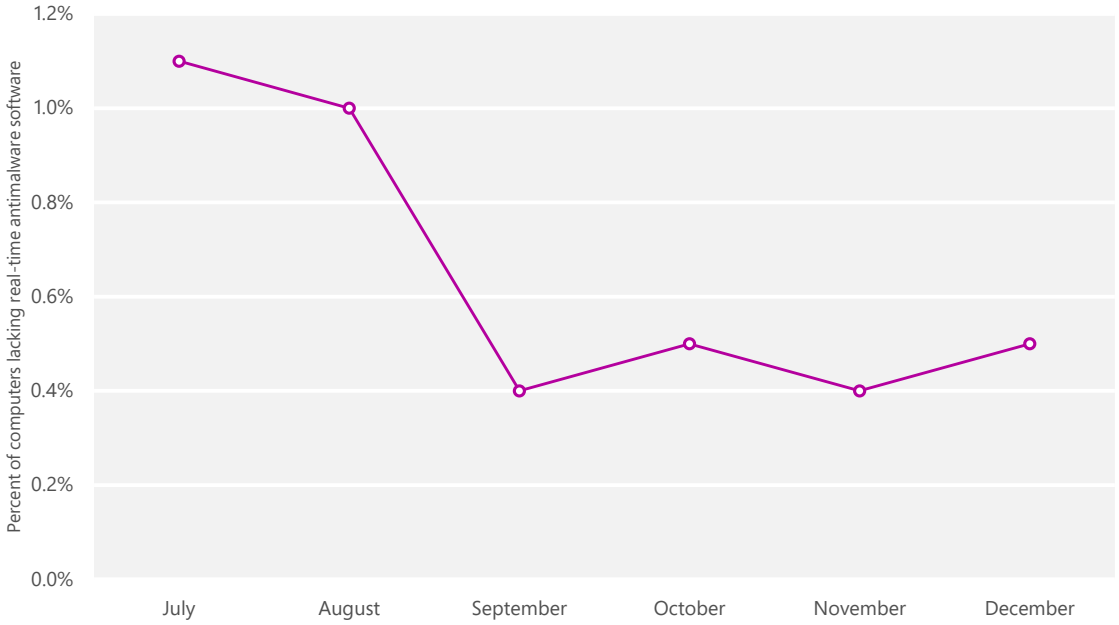
This section of the report compares the potential impact of malware to the levels of antimalware compliance from approximately 350,000 workstation computers managed by Microsoft IT between July and December 2013. This data is compiled from multiple sources, including System Center Endpoint Protection (SCEP), Network Access Protection, DirectAccess, and manual submission of suspicious files. Comparing the nature and volume of the malware detected on these computers to the level of protection they receive can illustrate significant trends and provide insights as to the effectiveness of antimalware software and security best practices.

## Antimalware usage

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

Figure 74 shows the level of antimalware noncompliance in the Microsoft user workstation environment for each month in 2H13.

Figure 74. Percentage of computers at Microsoft not running real-time antimalware software in 2H13

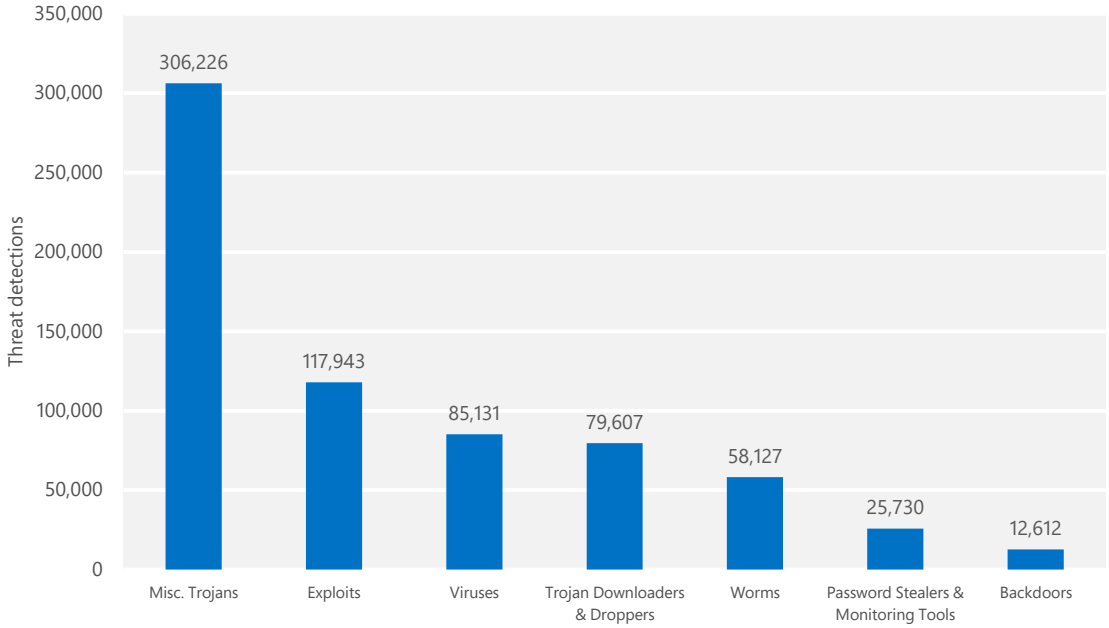



At an average of less than 1 percent noncompliance during the six-month period, the antimalware compliance rate at Microsoft is very high. In any network of this size, it is almost inevitable that a small number of computers will be in a noncompliant state at any given time. In most cases, these are computers that are being rebuilt or are otherwise in a state of change when online, rather than computers that have had their antimalware software intentionally disabled. Microsoft IT believes that a compliance rate in excess of 99 percent among 350,000 computers is an acceptable level of compliance. In most cases, attempting to boost a large organization's compliance rate the rest of the way to 100 percent will likely be a costly endeavor, and the end result—100 percent compliance—will be unsustainable over time.

## Malware detections

Figure 75 shows detections of categories of malware at Microsoft in 2H13.

Figure 75. Malware detected by System Center Endpoint Protection at Microsoft in 2H13, by category

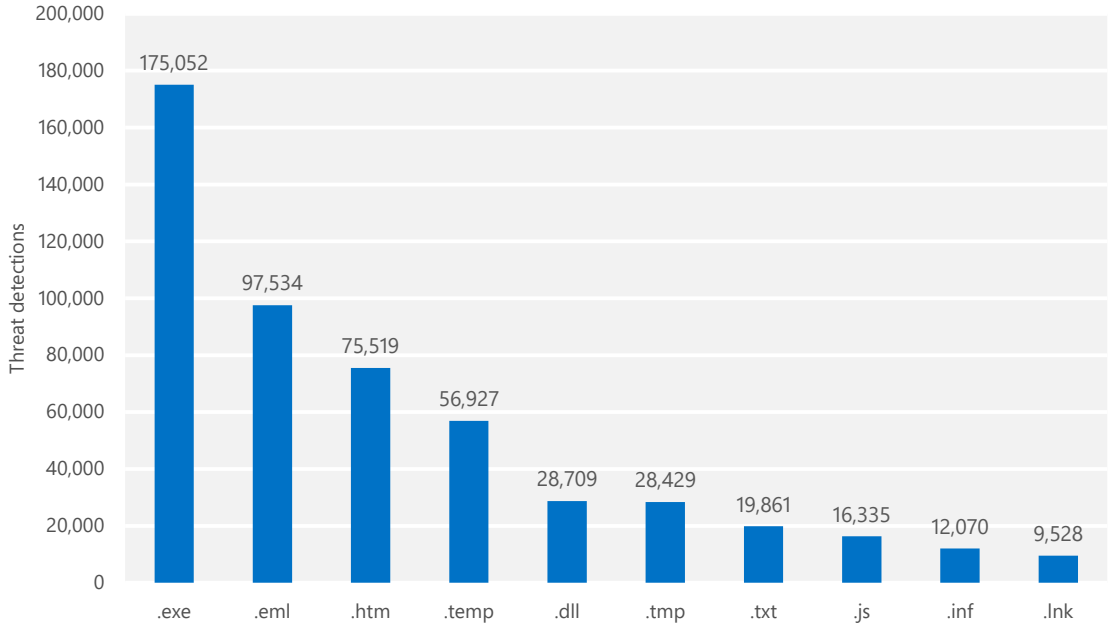



In this section, malware detections are defined as files and processes flagged by SCEP, regardless of the success or failure of automated containment or remediation. Malware detections are a measure of attempted malware activity, and do not necessarily indicate that a computer has been successfully infected. (Note that the methodology for assessing encounters used elsewhere in this report counts unique computers with detections, an approach that differs from the methodology used here in which individual detections are counted. For example, if a computer encountered one malware family in April and another one in June, it would only be counted once for the purposes of figures such as Figure 39 on page 58. In the preceding Figure 75, it would be counted twice, once for each detection.)

Miscellaneous Trojans was the most prevalent category. Exploits had the 2nd most number of detections, followed by Viruses and Trojan Downloaders & Droppers.

Figure 76 shows the top 10 file types among threat detections at Microsoft in 2H13.

Figure 76. Threat detections at Microsoft in 2H13, by file type




Executable program files with the .exe extension were the most commonly detected type of malicious file at Microsoft, accounting for about one-third of all file detections. Files with the .eml extension used by some email programs were the next most common type of threat, followed by HTML files.

## Transmission vectors

Examining the processes targeted by malware can help illustrate the methods that attackers use to propagate it. Figure 77 lists the top 5 transmission vectors used by the malware encountered at Microsoft in 2H13.

Figure 77. The top 5 transmission vectors used by malware encountered at Microsoft in 2H13

| Rank | Description |
|---|---|
| 1 | File transfers in the operating system |
| 2 | Web browsing |
| 3 | File transfer applications |
| 4 | Email |
| 5 | Non-Microsoft software |

The transmission vector most commonly used by infection attempts detected on Microsoft computers in 2H13 involved file transfers made through Windows Explorer, followed by attempts to deliver malware through the user's web

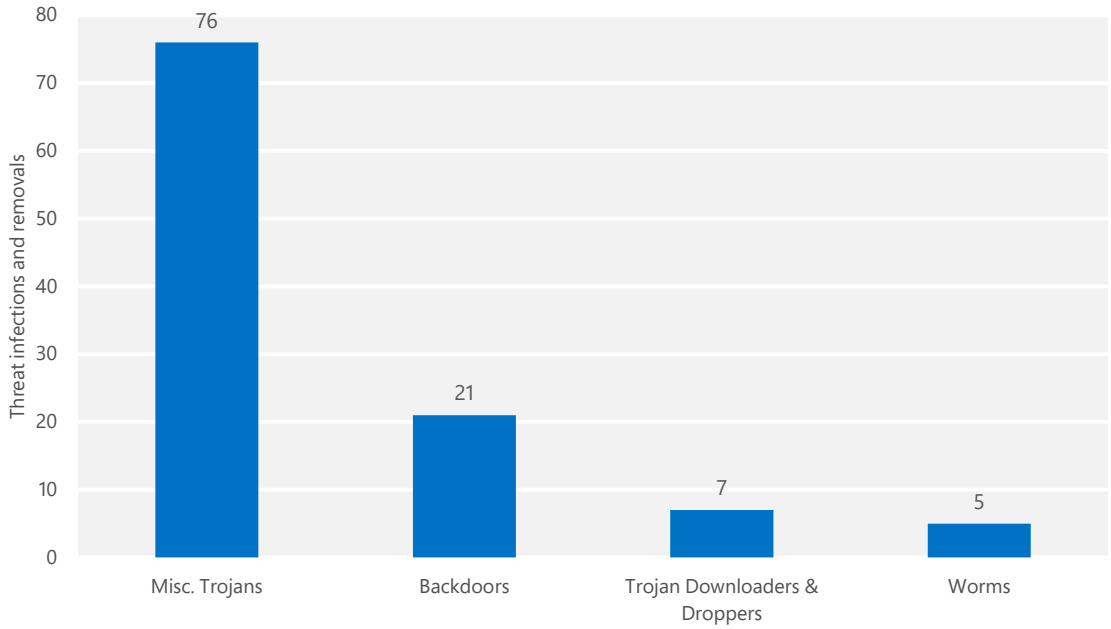
browser. File transfer applications, such as Microsoft OneDrive, Microsoft SharePoint, and peer-to-peer (P2P) applications, made up the 3rd most common transmission vector, followed by email and non-Microsoft software.

## Malware infections

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

Figure 78 summarizes the threats that SCEP detected on and removed from computers at Microsoft between July and December of 2013.

Figure 78. Computers at Microsoft cleaned of malware in 2H13, by category

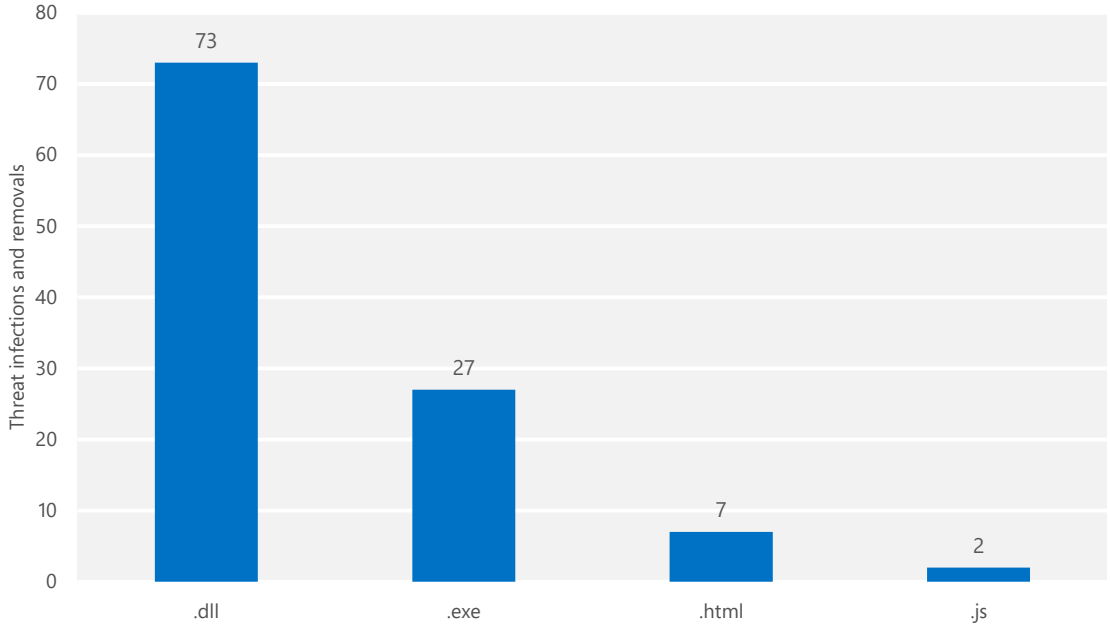



As with detections, Miscellaneous Trojans was the most common threat category to infect computers at Microsoft in 2H13, but the rest of the list shows

significant differences. Despite Exploits being the 2nd most commonly detected malware category at Microsoft in 2H13, no exploit infections were removed from computers at Microsoft during the period. Meanwhile, Backdoors were responsible for the smallest number of detections, but the 2nd largest number of infections.

Figure 79 shows the top 10 file types used by malware to infect computers at Microsoft in 2H13.

Figure 79. Infections and removals at Microsoft in 2H13, by file type




Of the four malware charts presented in this section, Figure 79 is potentially the most important because it provides information about threats that SCEP did not detect when they were first encountered—and therefore provides a clue about the areas in which malware authors have been focusing their efforts in recent months. The .dll extension, which denotes dynamic-link library files, was the most commonly used file type among successful infections, followed by .exe, used for executable program files. Malicious HTML and JavaScript files were each responsible for a small number of infections.

### What IT departments can do to minimize these trends

- Evaluate commercially available management tools, develop a plan, and implement a third-party update mechanism to disseminate non-Microsoft updates.

- Ensure that all software deployed on computers in the environment is updated regularly. If the software provider offers an automatic update utility similar to Microsoft Update, ensure that it is enabled by default. See "Turn automatic updating on or off" at windows.microsoft.com for instructions on enabling automatic updates of Microsoft software.
- Ensure that SmartScreen Filter is enabled in Internet Explorer. See "SmartScreen Filter: frequently asked questions" at windows.microsoft.com for more information.
- Use Group Policy to enforce configurations for Windows Update and SmartScreen Filter. See Knowledge Base article KB328010 at support.microsoft.com and "Manage Privacy: SmartScreen Filter and Resulting Internet Communication" at technet.microsoft.com for instructions.
- Set the default configuration for antimalware to enable real-time protection across all drives, including removable devices.
- Move to a 64-bit hardware architecture.
- Identify business dependencies on Java and develop a plan to minimize its use where it is not needed.
- Use AppLocker to block the installation and use of potentially unwanted software such as Java or peer-to-peer (P2P) applications. See "AppLocker: Frequently Asked Questions" at technet.microsoft.com for more information.
- Implement the Enhanced Mitigation Experience Toolkit (EMET) to minimize exploitation of vulnerabilities in all manufactured software. See Knowledge Base article KB2458544 at support.microsoft.com for more information.
- Strengthen authentication by using smart cards. See "Smart Cards" at technet.microsoft.com for more information.
- Use Network Access Protection (NAP) and DirectAccess (DA) to enforce compliance policies for firewall, antimalware, and patch management on remote systems that connect to a corporate network. See "Network Access Protection" at msdn.microsoft.com and "Windows 7 DirectAccess Explained" at technet.microsoft.com for more information.

# Appendixes

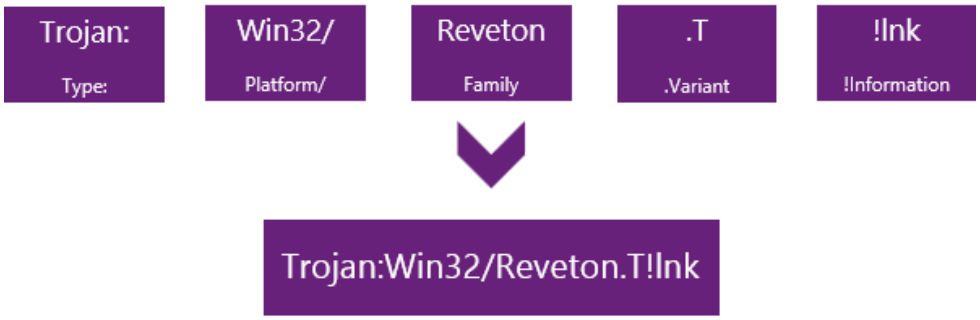
Appendix A: Threat naming conventions ..... 113
Appendix B: Data sources..... 115
Appendix C: Worldwide infection and encounter rates..... 117
Glossary.....123
Threat families referenced in this report..... 131

# Appendix A: Threat naming conventions

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

This scheme uses the following format:

Figure 80. The Microsoft malware naming convention




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

### Type

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

### Platform

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

### Family

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

### Variant letters

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

### Additional information

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

# Appendix B: Data sources

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

- Bing, the search and decision engine from Microsoft, contains technology that performs billions of webpage scans per year to seek out malicious content. After such content is detected, Bing displays warnings to users about it to help prevent infection.
- The 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 to selected installed applications.
- Exchange Online Protection protects the networks of tens of thousands of enterprise customers worldwide by helping to prevent malware from spreading through email. Exchange Online Protection scans billions of email messages every year to identify and block spam and malware.
- The Malicious Software Removal Tool (MSRT) is a free tool that Microsoft designed to help identify and remove specific prevalent malware families from customer computers. The MSRT is primarily released as an important update through Windows Update, Microsoft Update, and Automatic Updates. A version of the tool is also available from the Microsoft Download Center. The MSRT was downloaded and executed more than 600 million times each month on average in 2H13. The MSRT is not a replacement for an up-to-date real-time antivirus solution.
- The Microsoft Safety Scanner is a free downloadable security tool that provides on-demand scanning and helps remove malware and other malicious software. The Microsoft Safety Scanner is not a replacement for an up-to-date antivirus solution, because it does not offer real-time protection and cannot prevent a computer from becoming infected.
- Microsoft Security Essentials is a free, easy-to-download real-time protection product that provides basic, effective antivirus and antispyware protection.

- Microsoft System Center Endpoint Protection (formerly Forefront Client Security and Forefront Endpoint Protection) is a unified product that provides protection from malware and potentially unwanted software for enterprise desktops, laptops, and server operating systems. It uses the Microsoft Malware Protection Engine and the Microsoft antivirus signature database to provide real-time, scheduled, and on-demand protection.
- Outlook.com has more than 400 million active email users in more than 30 countries/regions around the world.
- SmartScreen Filter, a feature of Internet Explorer, offers users protection against phishing sites and sites that host malware. Microsoft maintains a database of phishing and malware sites reported by users of Internet Explorer and other Microsoft products and services. When a user attempts to visit a site in the database with the filter enabled, Internet Explorer displays a warning and blocks navigation to the page.
- Windows Defender in Windows 8 and Windows 8.1 provides real-time scanning and removal of malware and potentially unwanted software.
- Windows Defender Offline is a downloadable tool that can be used to create a bootable CD, DVD, or USB flash drive to scan a computer for malware and other threats. It does not offer real-time protection and is not a substitute for an up-to-date antimalware solution.

Figure 81. US privacy statements for the Microsoft products and services used in this report

| Product or service | Privacy statement URL |
|---|---|
| Bing | www.microsoft.com/privacystatement/en-us/bing/default.aspx |
| Exchange Online (Office 365) | www.microsoft.com/online/legal/v2/?docid=22&langid=en-us |
| EMET | technet.microsoft.com/en-US/security/dn133615 |
| Internet Explorer 11 | windows.microsoft.com/en-US/internet-explorer/ie11-win8-privacy-statement |
| Malicious Software Removal Tool | www.microsoft.com/security/pc-security/msrt-privacy.aspx |
| Microsoft Security Essentials | windows.microsoft.com/en-us/windows/security-essentials-privacy |
| Microsoft Safety Scanner | www.microsoft.com/security/scanner/en-us/privacy.aspx |
| Outlook.com | privacy.microsoft.com/en-us/fullnotice.mspx |
| System Center Endpoint Protection | technet.microsoft.com/en-us/library/hh508835.aspx |
| Windows Defender in Windows 8.1 | windows.microsoft.com/en-us/windows-8/windows-8-1-privacy-statement#T1=supplement&section_43 |
| Windows Defender Offline | windows.microsoft.com/en-us/windows/windows-defender-offline-privacy |

# Appendix C: Worldwide infection and encounter rates

"Malware prevalence worldwide" on page 46, explains how threat patterns differ significantly in different parts of the world. Figure 82 shows the infection and encounter rates for 3Q13 and 4Q13 for locations around the world.[16] See page 41 for information about how infection and encounter rates are calculated.

For a more in-depth perspective on the threat landscape in any of these locations, see the "Regional Threat Assessment" section of the *Microsoft Security Intelligence Report* website.

Figure 82. Encounter and infection rates for locations around the world, 3Q13–4Q13, by quarter (100,000 computers reporting minimum)

| Country/Region | Encounter rate 3Q13 | Encounter rate 4Q13 | CCM 3Q13 | CCM 4Q13 |
|---|---|---|---|---|
| *Worldwide* | *20.21%* | *21.58%* | *5.6* | *17.8* |
| Afghanistan | — | — | 26.5 | 27.3 |
| Albania | 32.39% | 45.13% | 21.6 | 41.5 |
| Algeria | 47.09% | 55.66% | 18.5 | 40.3 |
| Angola | — | — | 14.9 | 24.5 |
| Argentina | 26.66% | 33.41% | 5.0 | 42.3 |
| Armenia | — | 33.98% | 8.0 | 21.5 |
| Australia | 13.34% | 12.95% | 3.4 | 11.8 |
| Austria | 13.27% | 14.44% | 2.1 | 20.1 |
| Azerbaijan | — | — | 12.9 | 27.6 |
| Bahamas, The | — | — | 7.7 | 31.1 |
| Bahrain | — | — | 15.1 | 31.0 |
| Bangladesh | — | — | 13.1 | 14.4 |
| Barbados | — | — | 4.0 | 24.4 |

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

| Country/Region | Encounter rate 3Q13 | Encounter rate 4Q13 | CCM 3Q13 | CCM 4Q13 |
|---|---|---|---|---|
| Belarus | 36.46% | 33.34% | 7.4 | 16.6 |
| Belgium | 17.06% | 20.12% | 2.1 | 28.6 |
| Bolivia | — | — | 13.4 | 21.4 |
| Bosnia and Herzegovina | — | 37.50% | 14.3 | 44.6 |
| Botswana | — | — | 10.2 | 17.8 |
| Brazil | 32.28% | 38.08% | 6.6 | 26.0 |
| Brunei | — | — | 8.8 | 24.9 |
| Bulgaria | 25.03% | 34.01% | 6.6 | 32.7 |
| Burkina Faso | — | — | 6.2 | 16.4 |
| Cambodia | — | — | 13.5 | 15.7 |
| Cameroon | — | — | 9.9 | 17.3 |
| Canada | 12.95% | 13.60% | 3.3 | 9.9 |
| Chile | 24.13% | 33.18% | 5.1 | 34.3 |
| China | 25.37% | 20.33% | 2.1 | 4.4 |
| Colombia | 33.58% | 34.35% | 6.5 | 24.3 |
| Costa Rica | — | — | 9.9 | 16.4 |
| Côte d'Ivoire | 17.79% | 24.97% | 2.4 | 24.9 |
| Croatia | — | — | 8.7 | 19.4 |
| Cyprus | 20.08% | 26.17% | 4.5 | 26.7 |
| Czech Republic | 21.25% | 27.75% | 6.6 | 36.3 |
| Congo (DRC) | 16.11% | 16.60% | 1.7 | 11.4 |
| Denmark | 9.27% | 12.31% | 1.3 | 14.0 |
| Dominican Republic | 33.66% | 42.01% | 16.1 | 39.1 |
| Ecuador | 40.77% | 40.56% | 16.5 | 35.6 |
| Egypt | 45.08% | 47.08% | 25.3 | 27.6 |
| El Salvador | — | — | 5.2 | 24.0 |
| Estonia | 13.30% | 16.12% | 1.8 | 13.1 |
| Ethiopia | — | — | 24.8 | 28.9 |
| Finland | 7.69% | 8.71% | 0.6 | 9.8 |
| France | 16.82% | 25.89% | 1.9 | 37.5 |
| Georgia | 45.63% | 44.83% | 24.4 | 35.5 |

| Country/Region | Encounter rate 3Q13 | Encounter rate 4Q13 | CCM 3Q13 | CCM 4Q13 |
|---|---|---|---|---|
| Germany | 13.86% | 15.13% | 2.7 | 21.9 |
| Ghana | — | — | 7.1 | 10.8 |
| Greece | 23.37% | 28.98% | 4.7 | 36.7 |
| Guadeloupe | — | — | 9.1 | 50.8 |
| Guam | — | — | 0.0 | 12.0 |
| Guatemala | 32.10% | 31.09% | 5.5 | 15.3 |
| Haiti | — | — | 7.5 | 18.9 |
| Honduras | — | — | 8.9 | 21.7 |
| Hong Kong SAR | 13.87% | 13.03% | 2.0 | 11.4 |
| Hungary | 19.75% | 23.62% | 4.3 | 24.1 |
| Iceland | — | — | 1.7 | 9.0 |
| India | 45.94% | 49.92% | 14.3 | 26.4 |
| Indonesia | 51.18% | 58.71% | 13.3 | 22.2 |
| Iraq | 47.19% | 47.13% | 31.3 | 31.3 |
| Ireland | 12.07% | 14.85% | 1.8 | 13.3 |
| Israel | 16.52% | 19.13% | 5.8 | 6.2 |
| Italy | 21.13% | 26.20% | 3.2 | 27.5 |
| Jamaica | — | — | 6.9 | 28.3 |
| Japan | 7.62% | 8.02% | 2.2 | 9.1 |
| Jordan | 31.78% | 44.00% | 16.8 | 32.6 |
| Kazakhstan | 40.83% | 38.56% | 12.4 | 25.9 |
| Kenya | — | — | 7.7 | 14.9 |
| Korea | 34.10% | 22.98% | 17.9 | 11.1 |
| Kuwait | — | 29.39% | 11.4 | 25.7 |
| Kyrgyzstan | — | — | 14.4 | 21.3 |
| Laos | — | — | 16.1 | 20.3 |
| Latvia | 19.26% | 21.04% | 3.6 | 16.3 |
| Lebanon | — | — | 15.8 | 33.6 |
| Libya | — | — | 21.8 | 36.0 |
| Lithuania | 23.08% | 26.27% | 5.6 | 22.5 |
| Luxembourg | — | — | 2.1 | 18.5 |

| Country/Region | Encounter rate 3Q13 | Encounter rate 4Q13 | CCM 3Q13 | CCM 4Q13 |
|---|---|---|---|---|
| Macao SAR | — | — | 1.8 | 9.9 |
| Macedonia, FYRO | — | 38.63% | 12.4 | 33.9 |
| Malaysia | 29.85% | 34.29% | 9.3 | 31.0 |
| Mali | — | — | 7.0 | 17.1 |
| Malta | — | — | 2.7 | 25.1 |
| Martinique | — | — | 9.8 | 54.9 |
| Mauritius | — | — | 7.4 | 36.8 |
| Mexico | 33.29% | 35.38% | 10.2 | 30.5 |
| Moldova | 30.77% | 32.39% | 9.0 | 21.9 |
| Mongolia | — | — | 17.7 | 31.0 |
| Morocco | 35.51% | 44.86% | 19.7 | 39.8 |
| Mozambique | — | — | 8.6 | 17.4 |
| Myanmar | — | — | 9.4 | 12.5 |
| Namibia | — | — | 7.7 | 18.2 |
| Nepal | — | — | 20.0 | 27.3 |
| Netherlands | 15.58% | 16.69% | 2.5 | 20.3 |
| New Caledonia | — | — | 0.0 | 44.4 |
| New Zealand | 12.20% | 14.56% | 3.8 | 17.3 |
| Nicaragua | — | — | 4.0 | 19.4 |
| Nigeria | — | — | 6.3 | 12.8 |
| Norway | 8.23% | 10.06% | 1.3 | 11.6 |
| Oman | — | — | 11.5 | 28.7 |
| Pakistan | 55.63% | 60.11% | 31.0 | 35.8 |
| Palestinian Authority | — | — | 25.3 | 29.3 |
| Panama | — | 30.00% | 5.9 | 24.0 |
| Paraguay | — | — | 5.2 | 25.8 |
| Peru | 44.59% | 39.19% | 20.1 | 27.3 |
| Philippines | 43.92% | 46.28% | 17.3 | 32.1 |
| Poland | 21.71% | 26.65% | 5.4 | 44.0 |
| Portugal | 22.32% | 27.58% | 2.8 | 27.4 |
| Puerto Rico | 14.70% | 19.78% | 4.7 | 18.2 |

| Country/Region | Encounter rate 3Q13 | Encounter rate 4Q13 | CCM 3Q13 | CCM 4Q13 |
|---|---|---|---|---|
| Qatar | 27.98% | 33.12% | 9.2 | 27.7 |
| Réunion | — | — | 3.3 | 28.7 |
| Romania | 27.50% | 30.79% | 13.5 | 25.7 |
| Russia | 30.11% | 25.81% | 4.7 | 12.3 |
| Rwanda | — | — | 7.0 | 13.1 |
| Saudi Arabia | 29.39% | 34.91% | 11.4 | 23.7 |
| Senegal | — | — | 8.2 | 29.2 |
| Serbia | 27.27% | 34.32% | 11.4 | 36.7 |
| Singapore | 10.64% | 12.31% | 3.7 | 9.0 |
| Slovakia | 15.95% | 20.13% | 2.4 | 19.7 |
| Slovenia | 16.90% | 19.27% | 2.9 | 17.3 |
| South Africa | 23.10% | 28.28% | 6.5 | 20.5 |
| Spain | 21.20% | 27.60% | 3.0 | 44.4 |
| Sri Lanka | — | 39.16% | 8.2 | 14.8 |
| Sweden | 9.66% | 11.32% | 1.5 | 14.1 |
| Switzerland | 12.97% | 14.22% | 2.1 | 19.4 |
| Taiwan | 18.98% | 18.60% | 4.7 | 15.9 |
| Tanzania | — | — | 9.4 | 15.3 |
| Thailand | 36.93% | 33.74% | 18.3 | 25.5 |
| Trinidad and Tobago | — | — | 6.2 | 32.7 |
| Tunisia | 37.77% | 52.26% | 13.9 | 49.5 |
| Turkey | 38.83% | 44.86% | 21.6 | 25.2 |
| Uganda | — | — | 6.5 | 10.7 |
| Ukraine | 34.97% | 32.43% | 6.9 | 15.5 |
| United Arab Emirates | 27.89% | 34.10% | 12.2 | 34.0 |
| United Kingdom | 13.91% | 16.17% | 2.6 | 22.8 |
| United States | 13.19% | 11.97% | 6.9 | 11.9 |
| Uruguay | — | 29.98% | 3.4 | 35.3 |
| Uzbekistan | — | — | 8.3 | 12.9 |
| Venezuela | 33.90% | 42.31% | 7.9 | 37.3 |
| Vietnam | 45.31% | 49.22% | 18.3 | 24.1 |

| Country/Region | Encounter rate 3Q13 | Encounter rate 4Q13 | CCM 3Q13 | CCM 4Q13 |
|---|---|---|---|---|
| Yemen | — | — | 26.3 | 35.2 |
| Zambia | — | — | 6.7 | 14.2 |
| Zimbabwe | — | — | 7.9 | 15.4 |
| *Worldwide* | *20.21%* | *21.58%* | *5.6* | *17.8* |

# Glossary

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

**419 scam**
See *advance-fee fraud*.

**Address Space Layout Randomization (ASLR)**
A security feature in recent versions of Windows that randomizes the memory locations used by system files and other programs, which makes it harder for an attacker to exploit the system by targeting specific memory locations.

**advance-fee fraud**
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, typically involving bureaucratic red tape or political corruption. The sender asks the prospective victim for a temporary loan to be used for bribing officials or for paying fees to get the full sum released. In exchange, the sender promises the target a share of the fortune amounting to a much larger sum than the original loan, but does not deliver. Advance-fee frauds are often called *419 scams*, in reference to the article of the Nigerian Criminal Code that addresses fraud.

**ASLR**
See *Address Space Layout Randomization (ASLR)*.

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

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

**"black hat"**
A term used to characterize software developers and security researchers who act criminally, maliciously, or unethically, as opposed to those who work to protect computers from attack.

**bot**
A malware program that joins an infected computer to a botnet.

**botnet**
A set of computers controlled by a "command-and-control" (C&C) computer to execute commands as directed. The C&C computer can issue commands directly (often through Internet Relay Chat [IRC]) or by using a decentralized mechanism, such as peer-to-peer (P2P) networking. Computers in a botnet are often called bots, nodes, or zombies.

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

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

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

**clean**
To remove malware from an infected computer. A single cleaning can involve multiple disinfections.

**command and control**
See *botnet*.

**coordinated disclosure**
The practice of disclosing vulnerabilities privately to an affected vendor so it can develop a comprehensive security update to address the vulnerability before it becomes public knowledge.

**Data Execution Prevention (DEP)**
A security technique designed to prevent buffer overflow attacks. DEP enables the system to mark areas of memory as non-executable, which prevents code in those memory locations from running.

**denial of service (DoS)**
A condition that occurs when the resources of a target computer are deliberately exhausted, which effectively overwhelms the computer and causes it to fail to respond or function for its intended users. There are a number of different types of attack that may be used to result in a denial of service condition using different types of flooding, or malformed network traffic. Also see *distributed denial of service (DDoS)*.

**DEP**
See *Data Execution Prevention (DEP)*.

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

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

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

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

**distributed denial of service (DDoS)**
A form of denial of service (DoS) that uses multiple computers to attack the target. Considerable resources may be required to exhaust a target computer and cause it to fail to respond. Often multiple computers are used to perform these types of malicious attack and increase the attack's chances of success. This can occur, for example, when a number of compromised computers, such as those that comprise a botnet, are commandeered and ordered to access a target network or server over and over again within a small period of time.

**downloader**
See *trojan downloader/dropper*.

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

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

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

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

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

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

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

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

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

**infection rate**
See *CCM*.

**jailbreaking**
See *rooting*.

**malware**
Any software that is designed specifically to cause damage to a user's computer, server, or network. Viruses, worms, and trojans are all types of malware. By default, Microsoft security products automatically block, quarantine, or remove malware that is determined to have a high negative impact on affected computers.

**malware impression**
A single instance of a user attempting to visit a page known to host malware and being blocked by SmartScreen Filter in Internet Explorer versions 8 through 11. Also see *phishing impression*.

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

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

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

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

**phishing**
A method of credential theft that tricks Internet users into revealing personal or financial information online. Phishers use phony websites or deceptive email messages that mimic trusted businesses and brands to steal personally

identifiable information (PII), such as user names, passwords, credit card numbers, and identification numbers.

**phishing impression**
A single instance of a user attempting to visit a known phishing page with Internet Explorer versions 7 through 11, and being blocked by the Phishing Filter or SmartScreen Filter. Also see *malware impression*.

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

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

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

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

**SEHOP**
*See Structured Exception Handler Overwrite Protection (SEHOP).*

**signature**
See *detection signature*.

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

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

**SQL injection**
A technique in which an attacker enters a specially crafted Structured Query Language (SQL) statement into an ordinary web form. If form input is not filtered and validated before being submitted to a database, the malicious SQL statement may be executed, which could cause significant damage or data loss.

**Structured Exception Handler Overwrite Protection (SEHOP)**
A security technique designed to prevent exploits from overwriting exception handlers to gain code execution. SEHOP verifies that a thread's exception handler list is intact before allowing any of the registered exception handlers to be called.

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

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

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

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

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

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

**wild**
See *in the wild*.

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

# Threat families referenced in this report

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

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

INF/Autorun. A family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.

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

Win32/Bdaejec. A trojan that allows unauthorized access and control of an affected computer, and may download and install other programs without consent.

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

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

Win32/Brontok. A mass-mailing email worm that spreads by sending copies of itself as email attachments to addresses gathered from files on the infected computer, and by copying itself to removable volumes. Brontok can disable security software, and may conduct DoS attacks against certain websites.

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

Win32/Conficker. A worm that spreads by exploiting a vulnerability addressed by Security Bulletin MS08-067. Some variants also spread via removable drives and by exploiting weak passwords. It disables several important system services and security products, and downloads arbitrary files.

JS/Coolex. A detection for scripts from an exploit pack known as the "Cool Exploit Kit." These scripts are often used in ransomwhere schemes in which an attacker locks a victim's computer or encrypts the user's data and demands money to make it available again.

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

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

AndroidOS/CVE-2011-1823. A detection for specially-crafted Android programs that attempt to exploit a vulnerability in the Android operating system to gain root privilege.

AndroidOS/CVE-2011-3874. A threat that attempts to exploit a vulnerability in the Android operating system to gain access to and control of the device

Java/CVE-2012-1723. A family of malicious Java applets that attempt to exploit vulnerability CVE-2012-1723 in the Java Runtime Environment (JRE) in order to download and install files of an attacker's choice onto the computer.

Win32/Delf. A detection for various threats written in the Delphi programming language.

Win32/DelfInject. A detection for various threats that inject themselves into running processes.

Win32/Deminnix. A trojan that uses the computer for Bitcoin mining and changes the home page of the web browser. It can accidentally be downloaded along with other files from torrent sites.

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

Win32/Dircrypt. Ransomware that encrypts the user's files and demands payment to release them. It is distributed through spam email messages and can be downloaded by other malware.

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

Win32/Dorkbot. A worm that spreads via instant messaging and removable drives. It also contains backdoor functionality that allows unauthorized access and control of the affected computer. Win32/Dorkbot may be distributed from compromised or malicious websites using PDF or browser exploits.

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

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

JS/FakeAlert. A malicious script that falsely claims that the computer is infected with viruses and that additional software is needed to disinfect it.

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

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

Win32/FakeSysdef. A rogue security software family that claims to discover nonexistent hardware defects related to system memory, hard drives, and overall system performance, and charges a fee to fix the supposed problems.

Win32/Frethog. A large family of password-stealing trojans that targets confidential data, such as account information, from massively multiplayer online games.

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

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

JS/Javrobat. An exploit that tries to check whether certain versions of Adobe Acrobat or Adobe Reader are installed on the computer. If so, it tries to install malware.

VBS/Jenxcus. A worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.

Win32/Loktrom. Ransomware that locks the computer and displays a full-screen message pretending to be from a national police force, demanding payment to unlock the computer.

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

Win32/Malagent. A generic detection for malware that exhibit explicit forms of malicious behavior.

Win32/Meredrop. A generic detection for trojans that drop and execute multiple forms of malware on a local computer. These trojans are usually packed, and may contain multiple trojans, backdoors, or worms. Dropped malware may connect to remote websites and download additional malicious programs.

Win32/Microjoin. A generic detection for tools that bundle malware files with clean files in an effort to deploy malware without being detected by security software.

VBS/Miposa. A trojan that downloads and runs malicious Windows Scripting Host (.wsh) files.

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

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

Win32/Oceanmug. A trojan that silently downloads and installs other programs without consent.

Win32/Onescan. A Korean-language rogue security software family distributed under the names One Scan, Siren114, EnPrivacy, PC Trouble, Smart Vaccine, and many others.

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

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

VBS/Psyme. A VBScript trojan that exploits a vulnerability addressed by Microsoft Security Bulletin MS06-014. The trojan is encountered when a user visits a malicious Web page containing the script, and it attempts to download and execute arbitrary files on the affected system.

BAT/Qhost. A generic detection for trojans that modify the HOSTS file on the computer to redirect or limit Internet traffic to certain sites.

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

Win32/Ransom. A detection for malicious programs that seize control of the computer on which they are installed. This trojan usually locks the screen and prevents the user from using the computer. It usually displays an alert message.

JS/Redirector. A detection for a class of JavaScript trojans that redirect users to unexpected websites, which may contain drive-by downloads.

Win32/Reveton. A ransomware family that targets users from certain countries or regions. It locks the computer and displays a location-specific webpage that

covers the desktop and demands that the user pay a fine for the supposed possession of illicit material.

Win32/Rongvhin. A family of malware that perpetrates click fraud. It might be delivered to the computer via hack tools for the game CrossFire.

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

Win32/Sality. A family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.

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

Win32/Sirefef. A malware platform that receives and runs modules that perform different malicious activities.

Java/SMSer. A ransomware trojan that locks an affected user's computer and requests that the user send a text message to a premium-charge number to unlock it.

Win32/Swisyn. A trojan that drops and executes arbitrary files on an infected computer. The dropped files may be potentially unwanted or malicious programs.

MSIL/Truado. A trojan that poses as an update for certain Adobe software.

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

JS/Urntone. A webpage component of the Neutrino exploit kit. It checks the version numbers of popular applications installed on the computer, and attempts to install malware that targets vulnerabilities in the software.

Win32/Vobfus. A family of worms that spreads via network drives and removable drives and download/executes arbitrary files. Downloaded files may include additional malware.

Win32/Winwebsec. A rogue security software family distributed under the names AVASoft Professional Antivirus, Smart Fortress 2012, Win 8 Security System, and others.

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

Win32/Zbot. A family of password stealing trojans that also contains backdoor functionality allowing unauthorized access and control of an affected computer.

# Index


419 scams. *See* advance-fee fraud
Active Directory, 71
Address Space Layout Randomization, 7, 8, 14, 15, 38, 40, 123
Adobe Acrobat, 37, 134
Adobe Flash Player, 13, 29, 30, 32, 38, 40, 133
Adobe Reader, 13, 14, 30, 37, 40, 134
Adobe Systems, 13, 14, 29, 30, 32, 37, 38, 40, 133, 134, 136
  security updates, 38, 40
advanced persistent threats. *See* targeted attacks
advance-fee fraud, 79, 80, 81, 123
Afghanistan, 117
Africa, 69, 92
Albania, 51, 117
Algeria, 50, 117
Android, 34, 35, 36, 95, 113, 128, 132, 134
  security updates, 36
Angola, 117
Anogre, 34, 35, 131
antimalware software. *See* real-time security software
antivirus software. *See* real-time security software
Apache HTTP Server, 30
AppLocker, 109
Argentina, 117
Armenia, 117
Asia, 69
ASLR. *See* Address Space Layout Randomization
Australia, 117
Austria, 117
Automatic Updates, 115
AutoRun (feature), 63
Autorun (malware family), 51, 59, 61, 63, 64, 73, 74, 131
Azerbaijan, 117
backdoors, 60, 94, 105, 107, 108, 137
Bahamas, 117
Bahrain, 117
Bangladesh, 117
Banload, 47, 94, 95, 131
Barbados, 117
Bdaejec, 94, 95, 131
Belarus, 118
Belgium, 70, 118
Bing, ii, 98–100, 115, 116
Bitcoin, 43, 48, 67, 123, 133
"black hat" security researchers, 3, 5, 123
Blackhole exploit kit. *See* Blacole
Blacole, 11, 12, 29, 30, 31, 33, 37, 59, 131
Bolivia, 118
Bosnia and Herzegovina, 118
botnets, 43, 45, 46, 75, 123, 124, 125
Botswana, 118
Brantall, **44**–**45**, 47, 51, 53, 59, 61, 62, 64, 73, 74, 75, 131, 136
Brazil, 47, 60, 118
Brontok, 51, 132
Browser Defender. *See* Rotbrow
Browser Protector. *See* Rotbrow
Brunei, 118
Bulgaria, 118
Burkina Faso, 118
California, 98
Cambodia, 118
Cameroon, 118
Canada, 47, 60, 118
Chile, 118
China, 47, 48, 53, 60, 98, 118
click fraud, 43, 44, 136
Colombia, 118
Comame, 94, 95, 132
Common Vulnerabilities and Exposures. *See* CVE identifier
Common Vulnerability Scoring System, 20, 22

computers cleaned per mille, 41–**42**, 44, 45, 49, 50, 51, 52, 57, 117–22, 124, 127
Conficker, 64, 73, 75, 132
Congo (DRC), 118
Cool exploit kit. *See* Coolex
Coolex, 32, 132
coordinated disclosure, 8, 124
Costa Rica, 118
Côte d'Ivoire, 118
CplLnk. *See* CVE-2010-2568
credential theft, 4, 53, 75, 127, 131, 133, 135, 137
Crilock, 69, 70, 75, 132
Croatia, 118
Cryptolocker. *See* Crilock
Cutwail, 77
CVE identifier, 19, 27
CVE-2007-0071, 38
CVE-2010-0188, 37
CVE-2010-0840, 29, 32
CVE-2010-1297, 38
CVE-2010-2568, 27, 29, 30, 35, 51, 132
CVE-2010-3653, 38
CVE-2011-0626, 38
CVE-2011-1823, 35, 36, 94, 95, 132
CVE-2011-3402, 35
CVE-2011-3544, 29
CVE-2011-3874, 94, 95, 132
CVE-2012-0056, 35
CVE-2012-0507, 29, 32
CVE-2012-1723, 29, 30, 32, 33, 59, 73, 132
CVE-2013-0422, 29, 32, 33
CVE-2013-0640, 40
CVE-2013-1331, 40
CVE-2013-1493, 29, 32, 33
CVE-2013-2423, 29
CVE-2013-3163, 40
CVE-2013-3893, 40
CVE-2013-3897, 40
CVE-2013-3906, 40
CVE-2013-3918, 40
CVE-2013-5065, 40
CVE-2013-5330, 40
CVSS. *See* Common Vulnerability Scoring System
Cyprus, 118
Czech Republic, 118
Darkleech, 30
Data Execution Prevention, 7, 8, 14, 15, 38, 125
DDoS. *See* distributed denial of service
Delf, 94, 95, 132
DelfInject, 94, 132
Deminnix, 48, 133
Denmark, 53, 118
DEP. *See* Data Execution Prevention
determined adversaries. *See* targeted attacks
Dircrypt, 69, 133
DirectAccess, 103, 109
distributed denial of service, 48, 125, 134
Dominican Republic, 118
Donxref, 32
Dorkbot, 59, 74, 133
drive-by downloads, 11, 30, 31, **98–100**, 135
Dynamer, 94, 133
Ecuador, 118
Egypt, 118
El Salvador, 118
email threats, 76–81
EMET. *See* Enhanced Mitigation Experience Toolkit
encounter rate, 28, 29, 30, 33, **41**, 42, 47, 49, 51, 53, 58, 59, 61, 69, 70, 72, 117–22, 126
Enhanced Mitigation Experience Toolkit, 8, 16, **38–40**, 109, 115, 116
Estonia, 118
Ethiopia, 118
Exchange Online Protection, ii, 76, 77, 78, 79, 80, 81, 115, 116
exploit kits, 9, 10, **11–15**, 16, 29, 31, 32, 63, 126, 134
Exploitability Index, 3
exploits, 1–16, **27–40**, 59, 60, 73, 94, 95, 105, 108, 126
  Adobe Flash Player, 38
  document, 36–37

families, 29–31
HTML, 29, 31–32
Java, 13, 14, 28, 29, 30, 31, 32–33, 59, 73, 109, 132, 133
JavaScript, 29, 31–32
operating system, 33–36
Facebook, 133
Faceliker, 65, 133
FakeAlert, 66, 133
FakePAV, 66, 133
FakeRean, 66, 133
FakeSysdef, 66, 133
FBI. *See* Federal Bureau of Investigation
Federal Bureau of Investigation, 67
Finland, 53, 98, 118
firewalls, 72, 109, 126
France, 47, 60, 118
Frethog, 53, 133
Gamarue, 51, 52, 59, 61, 63, 64, 73, 74, 134
generic detections, v, 30, 32, 48, 53, 58, 62, 63, 65, 95, 126, 132, 133, 134, 135
Georgia (country), 118
Georgia (US state), 92
Germany, 41, 47, 60, 119
Ghana, 119
GingerBreak, 36
GingerMaster, 36
Google Chrome, 24
Greece, 69, 119
Group Policy, 39, 109
Guadeloupe, 119
Guam, 119
Guatemala, 119
Haiti, 119
Honduras, 119
Hong Kong SAR, 119
HTML, 106, 108, 126, 135
Hungary, 119
Iceland, 53, 119
Idaho, 92
IframeRef, 29, 30, 32, 59, 73, 134
India, 50, 51, 119
Indonesia, 50, 51, 92, 119
infection rate. *See* computers cleaned per mille
Internet Explorer, 8, 13, 14, 16, 24, 40, 58, 82, 83, 86, 87, 89, 92, 109, 116, 127, 128
Internet Explorer Enhanced Protected Mode, 16
Internet Explorer Enhanced Security Configuration, 58
Iraq, 119
Ireland, 119
Israel, 119
Italy, 47, 60, 70, 119
jailbreaking, 128
Jamaica, 119
Japan, ii, 47, 53, 60, 92, 98, 119
Java Runtime Environment, 13, 14, 30, 31, 32, 33, 132
security updates, 33
JavaScript, 31–32, 108, 135
Javrobat, 134
Jenxcus, 51, 64, 134
Jordan, 119
JRE. *See* Java Runtime Environment
Kansas, 98
Kazakhstan, 69, 119
Kenya, 119
Korea, 45, 66, 92, 119
Kuwait, 119
Kyrgyzstan, 119
Laos, 119
Latin America, 69
Latvia, 119
Lebanon, 119
Libya, 119
Linux, 23
Lithuania, 119
Loktrom, 69, 134
Lotoor, 36, 134
Luxembourg, 119
Macao SAR, 120
Macedonia, FYRO, 120
Malagent, 65, 94, 134
Malaysia, 120
Mali, 120

Malicious Software Removal Tool, 41, 42, 43, 44, 45, 46, 50, 53, 54, 55, 62, 115, 116, 117, 124
Malta, 120
malware, **41–75**
by country or region, 46–53
by operating system, 46–53
categories, 58–60, 105
by location, 59–60
families, 61–65
by operating system, 63–65
file types, 106
on home and enterprise computers, 71–75
malware hosting sites, 92–98
by country or region, 96–98
categories of malware hosted, 93–95
malware impressions, 92, 93, 94, 95, 127
Martinique, 51, 120
Massachusetts, 98
Mauritius, 120
Meredrop, 94, 134
Mexico, 120
Microjoin, 94, 134
Microsoft IT, ii, vi, 75, **103–9**
Microsoft Malware Protection Center, ii, v, vi, 33, 43, 44, 45, 46, 53, 58, 62, 63, 70, 107, 123, 131
Microsoft Malware Protection Engine, v, 116
Microsoft Office, 16, 40, 70, 135
Microsoft OneDrive, 107
Microsoft Safety Scanner, 70, 115, 116
Microsoft Security Advisories, 3
Microsoft Security Bulletin MS08-067, 75, 132
Microsoft Security Bulletin MS10-046, 30, 35, 132
Microsoft Security Bulletin MS11-087, 35
Microsoft Security Bulletin MS13-051, 40
Microsoft Security Bulletin MS13-055, 40
Microsoft Security Bulletin MS13-080, 40
Microsoft Security Bulletin MS13-090, 40
Microsoft Security Bulletin MS13-096, 40
Microsoft Security Bulletin MS14-002, 40
Microsoft Security Bulletins, 3, 4, 6, 27, 30, 35, 40, 75, 131, 132, 135
Microsoft Security Engineering Center, vi
Microsoft Security Essentials, 107, 115, 116, 133
Microsoft Security Response Center, vi
Microsoft SharePoint, 107
Microsoft Update, 109, 115
Middle East, 69
Miposa, 47, 134
Miscellaneous Trojans, 58, 60, 61, 64, 73, 74, 94, 105, 107
MMPC. *See* Microsoft Malware Protection Center
Moldova, 120
Mongolia, 120
Montana, 98
Morocco, 120
Mozambique, 120
Mozilla Firefox, 24
MSEC. *See* Microsoft Security Engineering Center
MSRC. *See* Microsoft Security Response Center
MSRT. *See* Malicious Software Removal Tool
Myanmar, 120
Namibia, 120
National Vulnerability Database, 19, 24
Nebraska, 92, 98
Nepal, 120
Netherlands, 120
Network Access Protection, 103, 109
Neutrino exploit kit, 53, 136
New Caledonia, 120
New Zealand, 98, 120
Nicaragua, 120
Nigeria, 120
Nitol, 48, 134
North America, 69
Norway, 53, 120
NVD. *See* National Vulnerability Database
Obfuscator, 48, 53, 58, 61, 62, 64, 73, 74, 94, 135
Oceania, 69

Oceanmug, 94, 95, 135
Oman, 120
Onescan, 66, 135
Oracle Corporation, 13, 31, 33
Orsam, 48, 95, 135
Outlook.com, 116
Pakistan, 50, 51, 120
Palestinian Authority, 120
Panama, 120
Paraguay, 120
Password Stealers & Monitoring Tools, 60, 73, 94, 105
password theft. *See* credential theft
Paunch, 31
Pdfjsc, 37
Peru, 120
Philippines, 120
phishing, **83–92**, 127
  by country or region, 89–92
  target institutions, 86–89
Phishing Filter. *See* SmartScreen Filter
phishing impressions, 83, 84, 85, 86, 88, 128
Poland, 120
Portugal, 120
privacy statements, 116
Proslikefan, 47, 135
Psyme, 94, 95, 135
public exploit frameworks, 9
Puerto Rico, 120
Qatar, 121
Qhost, 48, 135
Ramnit, 51, 52, 61, 135
Ransom (malware family), 69
ransomware, 11, 32, **67–71**, 75, 128, 132, 135, 136
Ransomware, 134
real-time security software, **53–56**
Redirector, 48, 135
return-oriented programming, 40
Réunion, 121
Reveton, 11, 69, 70, 135
rogue security software, **65–67**, 128, 133, 135, 137
Romania, 98, 121
rooting, 36, 95, 127, 128
Rotbrow, **44–45**, 47, 51, 52, 53, 55, 57, 59, 61, 62, 64, 73, 74, 75, 131, 136
Russia, 47, 48, 60, 69, 98, 100, 121
Rustock, 77
Rwanda, 121
Safari, 24
Sality, 51, 61, 64, 74, 136
Saudi Arabia, 121
scareware. *See* rogue security software
SCEP. *See* System Center Endpoint Protection
Scotland Yard, 67
SDL. *See* Security Development Lifecycle
Security Development Lifecycle, 7, 26
Sefnit, 41, **43–44**, 45–46, 47, 51, 52, 58, 61, 62, 64, 74, 75, 131, 136
SEHOP. *See* Structured Exception Handler Overwrite Protection
Senegal, 121
Serbia, 121
Singapore, 121
Sirefef, 61, 73, 74, 136
Slovakia, 121
Slovenia, 121
smart cards, 109
SmartScreen Filter, **82–98**, 109, 116, 127, 128
social engineering, 129
South Africa, 121
South Carolina, 92
Spain, 70, 121
spam, 4, 75, **76–81**, 115, 129
  image-only, 79, 80
  malware in, 79, 80
  messages blocked, 76–78
  types, 78–81
SQL injection, 82, 129
Sri Lanka, 121
Structured Exception Handler Overwrite Protection, 38, 129
Stuxnet, 30
Sweden, 53, 121
Switzerland, 121

System Center Endpoint Protection, 103, 105, 107, 108, 116
Taiwan, 92, 121
Tanzania, 121
targeted attacks, 9, 10, 39, 40
Thailand, 121
Tor network, 45–46, 129
Trinidad and Tobago, 121
Trojan Downloaders & Droppers, 59, 60, 61, 64, 73, 74, 94, 105, 107
trojans, 47, 48, 51, 55, 58, 65, 66, 95, 113, 123, 127, 129, 130, 131, 133, 134, 135, 136, 137
Truado, 94, 136
Tunisia, 51, 121
Turkey, 121
Uganda, 121
Ukraine, 92, 98, 100, 121
United Arab Emirates, 121
United Kingdom, 47, 60, 121
United States, 47, 60, 121
Urausy, 69, 70, 136
Urntone, 53, 64, 136
Uruguay, 121
Utah, 92
Uzbekistan, 121
Venezuela, 121
Vietnam, 100, 121
viruses, 60, 61, 74, 94, 105, 113, 127, 130
Vobfus, 51, 137
vulnerabilities, 1–16, **19–26**, 27–40, 46, 59, 75, 95, 98, 109, 115, 124, 125, 126, 129, 130, 131, 132, 133, 134, 135, 136
  application, 23–25
  browser, 23–25
  buffer overflow, 6, 124
  complexity, 22–23
  heap corruption, 6
  in Microsoft products, 25–26
  industry-wide disclosures, 19–20
  memory safety, 14, 15
  operating system, 23–25
  severity, 20–22
  stack corruption, 6, 7
  type confusion, 6
  unsafe DLL, 6, 7
  use-after-free, 6, 7
vulnerability
  buffer overflow, 125
websites, malicious, 82–100
Windows 7, 64, 109
Windows 8, 16, 27, 57, 64, 65, 116
Windows 8.1, 16, 64, 65, 116
Windows Defender, 28, 70, 107, 116
Windows Defender Offline, 116
Windows Phone 8, 84, 86, 88, 89
Windows Scripting Host, 47, 134
Windows Update, 109, 115
Windows Vista, 57, 64
Windows XP, 57, 64
Winwebsec, 66, 137
Wisconsin, 92, 98
World of Warcraft, 53
worms, 60, 61, 64, 73, 74, 94, 105, 107, 113, 127, 130, 134, 135, 137
Wysotot, 61, 62, 64, 74, 137
Yemen, 52, 122
Zambia, 122
Zbot, 73, 75, 137
zero-day exploits, 4, 5, 33
Zimbabwe, 122

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