

An in-depth perspective on software vulnerabilities and exploits, malware, potentially unwanted software, and malicious websites

# Microsoft Security Intelligence Report

Volume 14

July through December, 2012



## Microsoft Security Intelligence Report

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it.

Copyright © 2013 Microsoft Corporation. All rights reserved.

Microsoft, the Microsoft logo, Active Directory, ActiveX, Bing, Forefront, Hotmail, Internet Explorer, MSDN, Outlook, the Security Shield logo, SmartScreen, System Center, Visual Basic, Win32, Windows, Windows Server, and Windows Vista are trademarks of the Microsoft group of companies. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

## Authors

**Danielle Alyias**

*Microsoft Trustworthy Computing*

**Dennis Batchelder**

*Microsoft Protection Technologies*

**Joe Blackbird**

*Microsoft Malware Protection Center*

**Joe Faulhaber**

*Microsoft Malware Protection Center*

**David Felstead**

*Bing*

**Paul Henry**

*Wadeware LLC*

**Jeff Jones**

*Microsoft Trustworthy Computing*

**Jimmy Kuo**

*Microsoft Malware Protection Center*

**Marc Lauricella**

*Microsoft Trustworthy Computing*

**Le Li**

*Microsoft Windows Safety Platform*

**Nam Ng**

*Microsoft Trustworthy Computing*

**Tim Rains**

*Microsoft Trustworthy Computing*

**Vidya Sekhar**

*Microsoft Malware Protection Center*

**Holly Stewart**

*Microsoft Malware Protection Center*

**Matt Thomlinson**

*Microsoft Trustworthy Computing*

**Terry Zink**

*Microsoft Forefront Online Protection for Exchange*

## Contributors

**Horea Coroiu**

*Microsoft Malware Protection Center*

**Methusela Cebrian Ferrer**

*Microsoft Malware Protection Center*

**Tanmay Ganacharya**

*Microsoft Malware Protection Center*

**Enrique Gonzalez**

*Microsoft Malware Protection Center*

**Heather Goudey**

*Microsoft Malware Protection Center*

**Angela Gunn**

*Microsoft Trustworthy Computing*

**Satomi Hayakawa**

*CSS Japan Security Response Team*

**Ben Hope**

*Microsoft Malware Protection Center*

**Aaron Hulett**

*Microsoft Malware Protection Center*

**Michael Johnson**

*Microsoft Malware Protection Center*

**Lesley Kipling**

*Microsoft EMEA Security Incident Response Team*

**Aneesh Kulkarni**

*Microsoft Windows Safety Platform*

**Jenn LeMond**

*Microsoft IT Information Security and Risk Management*

**Greg Lenti**

*CSS Security Readiness & Response Team*

**Wei Li**

*Microsoft Malware Protection Center*

**Marianne Mallen**

*Microsoft Malware Protection Center*

**Daric Morton**

*Microsoft Services*

**Yurika Muraki**

*CSS Japan Security Response Team*

**Jeong Wook Oh**

*Microsoft Malware Protection Center*

**Takumi Onodera**

*Microsoft Premier Field Engineering, Japan*

**Daryl Pecelj**

*Microsoft IT Information Security and Risk Management*

**Anthony Penta**

*Microsoft Windows Safety Platform*

**Hilda Larina Rraggio**

*Microsoft Malware Protection Center*

**Tim Reckmeyer**

*Microsoft Services*

**Laura A. Robinson**

*Microsoft Information Security & Risk Management*

**Cynthia Sandvick**

*Microsoft Trustworthy Computing*

**Richard Saunders**

*Microsoft Trustworthy Computing*

**Jasmine Sesso**

*Microsoft Malware Protection Center*

**Frank Simorjay**

*Microsoft Trustworthy Computing*

**Chris Stubbs**

*Microsoft Malware Protection Center*

**Norie Tamura**

*CSS Japan Security Response Team*

**Vincent Tiu**

*Microsoft Malware Protection Center*

**Henk van Roest**

*CSS Security EMEA*

**Steve Wacker**

*Wadeware LLC*

**Shawn Wang**

*Microsoft Malware Protection Center*

**Iaan Wiltshire**

*Microsoft Malware Protection Center*

**Dan Wolff**

*Microsoft Malware Protection Center*

# Table of Contents

About this report .....	v
Executive Foreword .....	vi
Trustworthy Computing: Security engineering at Microsoft .....	vii
Running unprotected: Measuring the benefits of real-time security software.....	1
Why go without real-time antimalware protection? .....	3
Real-time protection statistics .....	4
Operating system statistics .....	6
Geographic statistics .....	11
Guidance: Fighting infection with real-time protection.....	13
Worldwide threat assessment.....	15
Vulnerabilities .....	17
Industry-wide vulnerability disclosures .....	17
Vulnerability severity .....	18
Vulnerability complexity .....	20
Operating system, browser, and application vulnerabilities .....	21
Microsoft vulnerability disclosures.....	23
Guidance: Developing secure software .....	24
Exploits .....	25
Exploit families.....	27
Java exploits .....	28
HTML and JavaScript exploits .....	29
Document exploits.....	31
Operating system exploits .....	32
Adobe Flash Player exploits.....	35
Malware and potentially unwanted software .....	37
Global infection rates .....	37
Operating system infection rates.....	43
Threat categories .....	45
Threat categories by location .....	46
Threat families .....	48
Threat families by platform.....	50
Rogue security software .....	52

Home and enterprise threats.....	55
Guidance: Defending against malware.....	58
Email threats.....	59
Spam messages blocked.....	59
Spam types.....	61
Guidance: Defending against threats in email.....	64
Malicious websites.....	65
Phishing sites.....	66
Target institutions.....	68
Global distribution of phishing sites.....	69
Malware hosting sites.....	72
Malware categories.....	73
Global distribution of malware hosting sites.....	75
Drive-by download sites.....	78
Guidance: Protecting users from unsafe websites.....	81
Appendixes.....	83
Appendix A: Threat naming conventions.....	85
Appendix B: Data sources.....	87
Appendix C: Worldwide infection rates.....	89
Glossary.....	94
Threat families referenced in this report.....	100
Index.....	106

# About this report

The *Microsoft Security Intelligence Report (SIR)* focuses on software vulnerabilities, software vulnerability exploits, and malicious and potentially unwanted software. Past reports and related resources are available for download at [www.microsoft.com/sir](http://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 2012, with trend data for the last several years 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 *nHyy* or *nQyy* formats, where *yy* indicates the calendar year and *n* indicates the half or quarter. For example, 1H12 represents the first half of 2012 (January 1 through June 30), and 4Q11 represents the fourth quarter of 2011 (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 and potentially unwanted software. For information about this standard, see "[Microsoft Malware Protection Center Naming Standard](#)" on the MMPC website. In this report, any threat or group of threats sharing a common unique base name is considered a family for the sake of presentation. This includes threats that may not otherwise be considered families according to common industry practices, such as adware programs and generic detections.

Infection rates are given using a metric called *computers cleaned per mille* (CCM), which represents the number of computers cleaned for every 1,000 executions of the MSRT. For example, if the MSRT has 50,000 executions in a particular location in the first quarter of the year and removes infections from 200 computers, the CCM for that location in the first quarter of the year is 4.0 ( $200 \div 50,000 \times 1,000$ ). For periods longer than a quarter, the CCM is averaged for all quarters contained in the period.

# Executive Foreword

Welcome to Volume 14 of the *Microsoft Security Intelligence Report*. Over the past six and a half years we've published literally thousands of pages of threat intelligence in this report. Categories of focus continue to include trends and insights on security vulnerabilities, exploit activity, malware and potentially unwanted software, spam, phishing, malicious websites, and security trends from 105+ locations around the world.

Volume 14 contains the latest intelligence with analysis completed, focused on the second half of 2012 and inclusive of trend data going back a year or more. To summarize across the findings of hundreds of pages of new data: industry-wide vulnerability disclosures are down, exploit activity has increased in many parts of the world, several locations with historically high malware infection rates saw improvements but the worldwide malware infection rate increased slightly, Windows 8 has the lowest malware infection rate of any Windows-based operating system observed to date, Trojans continue to top the list of malware threats, spam volumes went up slightly, and phishing levels remained consistent.

We've also included some new, previously unpublished data in this volume of the report that helps quantify the value of using antimalware software. Characterizing the value of security software in a way that resonates relative to other IT investments persists as a challenge for many organizations; especially those who have successfully avoided a security crisis for a long period of time. And, the efficacy of antimalware software is often the source of discussion by Security professionals. Based on telemetry from hundreds of millions of systems around the world, Volume 14 returns the data on malware infection rates for unprotected systems versus systems that run antimalware software. The verdict is in: systems that run antimalware software have significantly lower malware infection rates, even in locations with the highest malware infection rates in the world. This data will likely help many people understand the value of using antimalware software – which we continue to consider a best practice and strongly recommend to all of our customers.

I hope you find this volume of the *Microsoft Security Intelligence Report* useful and enlightening. I also encourage people to visit [microsoft.com/sir](http://microsoft.com/sir) which includes a variety of additional information.

Adrienne Hall  
General Manager, Trustworthy Computing  
Microsoft



# 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.

Microsoft's 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 (MSIT), 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.



# Running unprotected: Measuring the benefits of real-time security software



Practicing safe browsing habits, such as using a web browser with built-in safety features and paying attention to alerts and warnings encountered while browsing, is one of the most important steps Internet users can take to protect themselves from malicious software (malware).<sup>1</sup> Nevertheless, it can sometimes be difficult for even experienced Internet users to avoid coming into contact with malware. The cybercriminals who publish and distribute malware devote significant effort to convincing or tricking Internet users into clicking links that lead to malware, or that download malicious attachments or applications. Even familiar and trusted websites can sometimes be exploited by attackers to distribute malware using tactics such as drive-by downloads. (See page 78 for more information about drive-by downloads.)

An antivirus or antimalware product that offers real-time protection is one of the most crucial defenses a computer user has against these and other malware distribution tactics. Unfortunately, many computers are not protected by real-time antimalware software, either because no such software has been installed, because it has expired, or because it has been disabled intentionally by the user or secretly by malware. New data analyzed by Microsoft reveals the magnitude of the additional risk that such computers and their users face: in the second half of 2012, computers that did not have real-time antimalware protection were more than 5 times as likely to be infected with malware and potentially unwanted software as computers that did have protection.

This section of the *Microsoft Security Intelligence Report* provides additional details about these findings, including statistics that pertain to different countries and regions and to different operating systems and service pack levels. Although the figures may vary slightly between different regions and platforms, the overall message is very clear: using real-time antimalware software from a reputable vendor and keeping it up to date is one of the most effective steps individuals and organizations can take to reduce their exposure to malware.

## Why go without real-time antimalware protection?

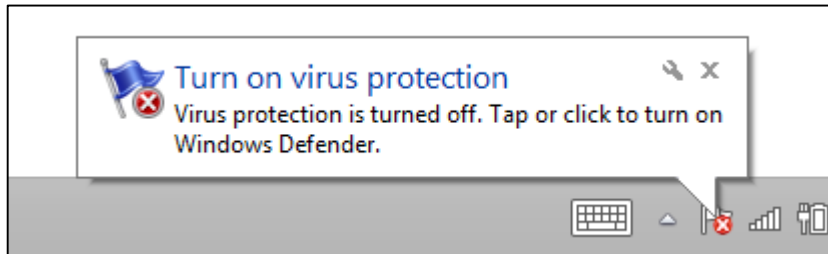
Windows users have many options for effective real-time antimalware protection. Enterprise IT departments typically use Group Policy to install security software on client computers and keep it updated. For home users and others, a number of vendors offer basic real-time products that can be

---

<sup>1</sup> See [www.microsoft.com/security](http://www.microsoft.com/security) for informative tips and advice about staying safe online.

downloaded or installed inexpensively or at no charge. In addition, all currently supported versions of Windows include mechanisms for monitoring the state of security software running on the computer and displaying alerts and other visual cues to inform the computer user when security software is not installed, not running, or out of date.

Figure 1. Windows alerts the user if antimalware software is disabled or not installed



With so many options and reminders, why would users choose to go unprotected? For some users, it may not be a choice. A number of prevalent malware and potentially unwanted software 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 the following pages will reveal.

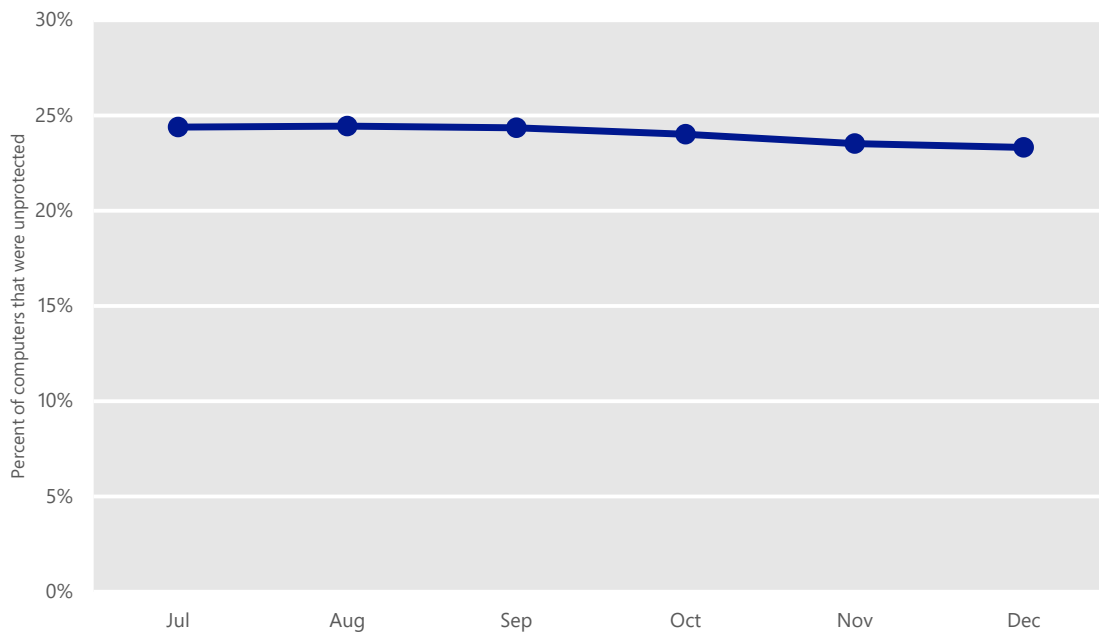
## Real-time protection statistics

The *Microsoft Security Intelligence Report* measures computer infection rates with a metric called *computers cleaned per mille* (CCM), which indicates the number of computers cleaned by the Microsoft Malicious Software Removal Tool (MSRT) for every 1,000 computers scanned by the tool. (See page v for more information about the CCM metric.)

Most computers that run the MSRT obtain each monthly release of the tool automatically through a Microsoft update service such as Windows Update. It executes in the background and automatically removes selected prevalent

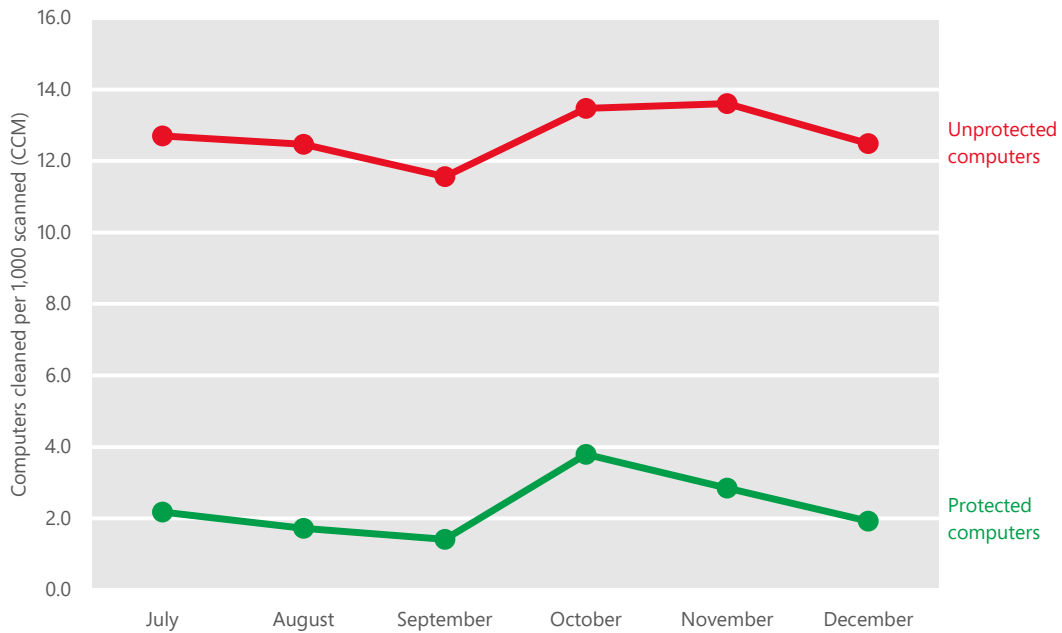
malware families from the computer. Recent releases of the MSRT collect and report details about the state of real-time antimalware software on the computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

Figure 2. Unprotected computers each month in 2H12



On average, about 24 percent of computers scanned by the MSRT each month in 2H12 were not running real-time antimalware software or were running out-of-date antimalware software at the time they were scanned (referred to as "unprotected computers" in this section). As Figure 3 shows, these computers were significantly more likely to be infected with malware than computers with up-to-date real-time protection ("protected computers").

Figure 3. Infection rates for protected and unprotected computers each month in 2H12



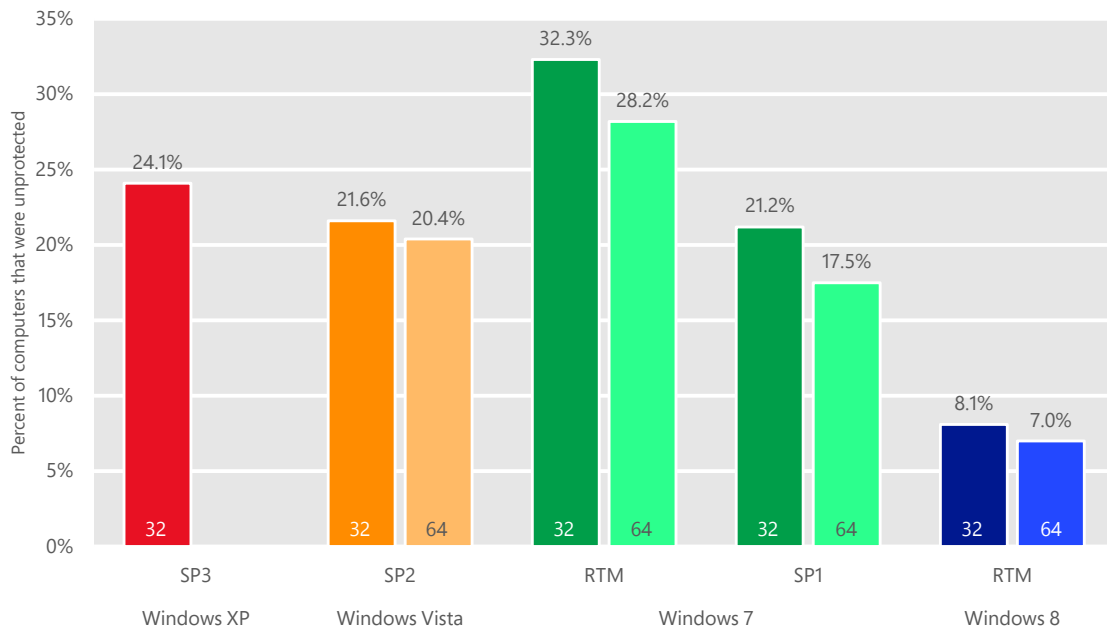
Computers that did not have up-to-date real-time antimalware protection were 5.5 times more likely on average to report malware infections each month than computers that did have protection. The CCM for unprotected computers ranged from 11.6 to 13.6, and the CCM for protected computers ranged from 1.4 to 3.8.

### Operating system statistics

Computers running newer Windows versions and service pack levels were generally more likely to run up-to-date real-time antimalware software, as shown in Figure 4.



Figure 4. Unprotected computers in 2H12, by operating system version and service pack level



32 = 32-bit edition; 64 = 64-bit edition. SP = Service Pack. RTM = release to manufacturing. Operating systems with at least 0.05 percent of total MSRT executions in 2Q12 shown.

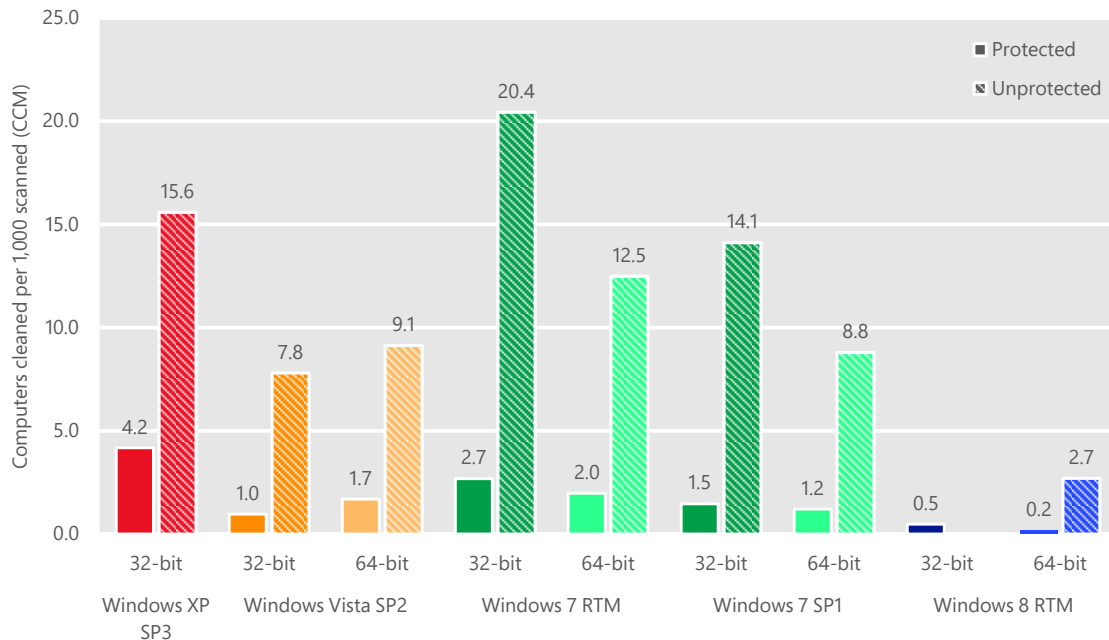
Computers running Windows 8 had the highest rate of protection, with just 8.1 percent of computers running the 32-bit edition and 7.0 percent of computers running the 64-bit edition lacking up-to-date real-time protection. Windows 8 includes real-time antimalware and antispysware protection by default,<sup>2</sup> which is likely a significant factor in the reduced number of Windows 8 computers not running security software; previous releases of Windows did not include real-time antimalware software by default. In addition, Windows 8 was only generally available for slightly more than two months of the half-year period, which provided less of an opportunity for real-time protection to expire or to be disabled by computer users or by malware.

Among supported releases of Windows, the lowest rate of protection was observed on computers running the RTM version of Windows 7, of which 32.3 percent of computers running the 32-bit edition and 28.2 percent of computers running the 64-bit edition lacked up-to-date real-time protection. Computers running Windows 7 SP1, the most recent service pack available for Windows 7, were significantly less likely to lack real-time protection than computers running the RTM version.

<sup>2</sup> See [windows.microsoft.com/en-US/windows-8/windows-defender](http://windows.microsoft.com/en-US/windows-8/windows-defender) for more information about antimalware protection in Windows 8.

Although infection rates for unprotected computers were significantly higher than those for protected computers, regardless of operating system version or service pack level, platforms with greater usage of up-to-date security software also tended to have lower infection rates in general, as shown in Figure 5.

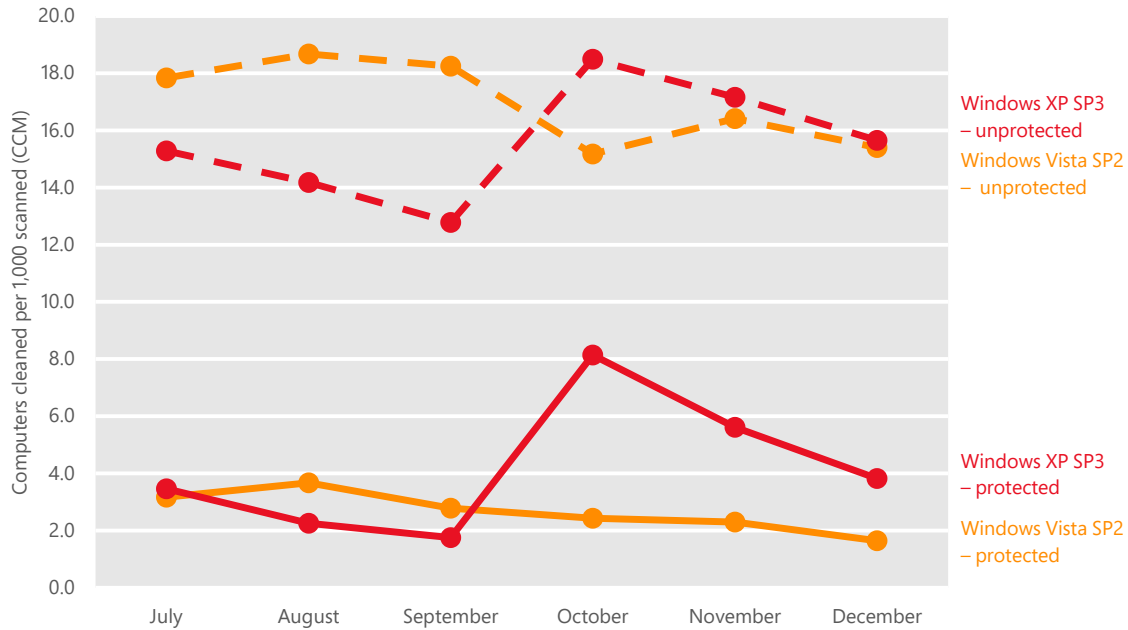
Figure 5. Infection rates for computers with and without up-to-date real-time antimalware protection in 2H12, by operating system version and service pack level



32 = 32-bit edition; 64 = 64-bit edition. SP = Service Pack. RTM = release to manufacturing. Operating systems with at least 0.05 percent of total MSRT executions in 2Q12 shown.

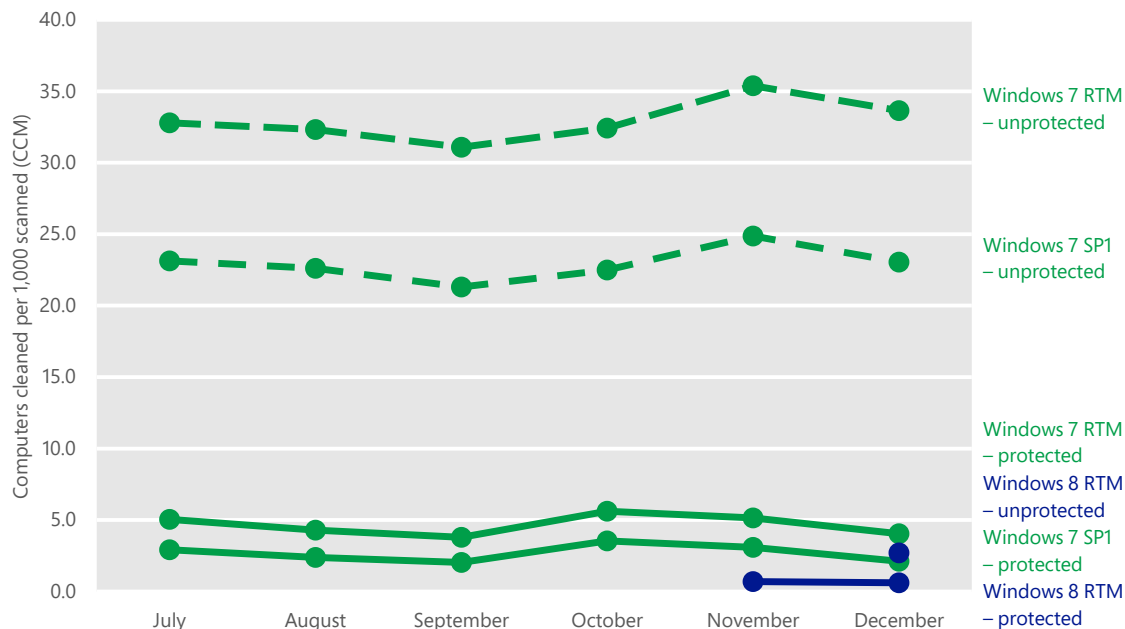
Of all the currently supported Windows client operating system and service pack combinations, Windows XP SP3 had the smallest relative difference between the infection rates of protected and unprotected computers, with protected computers reporting an infection rate 3.7 times greater than unprotected computers. More recently released versions of Windows feature a number of security improvements that are not included in Windows XP, which means that even protected computers running Windows XP face risks from exploitation and malware infection that don't apply to more recent versions of Windows.

Figure 6. Infection rates for computers running Windows XP and Windows Vista with and without up-to-date real-time antimalware protection in 2H12, by month



The RTM version of Windows 7, which had the highest percentage of unprotected computers of any platform (shown in Figure 4), also displayed the highest infection rates for unprotected computers, with a CCM of 20.4 for the 32-bit edition and 12.5 for the 64-bit edition. This correlation suggests that a larger population of unprotected users within a platform creates an attractive target for attackers.

Figure 7. Infection rates for computers running Windows 7 and Windows 8 with and without up-to-date real-time antimalware protection in 2H12, by month



On Windows 8, which had the lowest infection rate overall, unprotected computers have an infection rate (CCM) that is 16.2 times greater than the infection rate for protected users. This difference is much higher than average, and suggests that protected users benefit far more from their protection than protected users on other platforms. Because Windows 8 includes real-time antimalware protection by default,<sup>3</sup> many or most unprotected Windows 8 computers may lack protection because their users have chosen to disable it.<sup>4</sup>

The threat family most commonly detected by Microsoft security products on Windows 8 computers in 2H12 was [Win32/Keygen](#), a detection for tools that generate keys for various software products that are often distributed by software pirates to enable users to run software illegally. Such tools are typically detected as malware or potentially unwanted software by most antimalware scanners, so some users may choose to disable their security software to use the tools.<sup>5</sup> As the analysis presented here demonstrates, such users face significantly

<sup>3</sup> See [blogs.msdn.com/b/b8/archive/2011/09/15/protecting-you-from-malware.aspx](http://blogs.msdn.com/b/b8/archive/2011/09/15/protecting-you-from-malware.aspx) for more information about this change and other security improvements in Windows 8.

<sup>4</sup> As with other Windows releases, many computer vendors ship Windows 8 with a preinstalled trial version of a different antivirus product. The MMPC will continue to monitor MSRT telemetry to determine whether Windows 8 computers tend to become unprotected due to license expiration or for other reasons.

<sup>5</sup> Microsoft classifies Win32/Keygen as potentially unwanted software rather than malware, and therefore does not include detection signatures for the family in the MSRT.

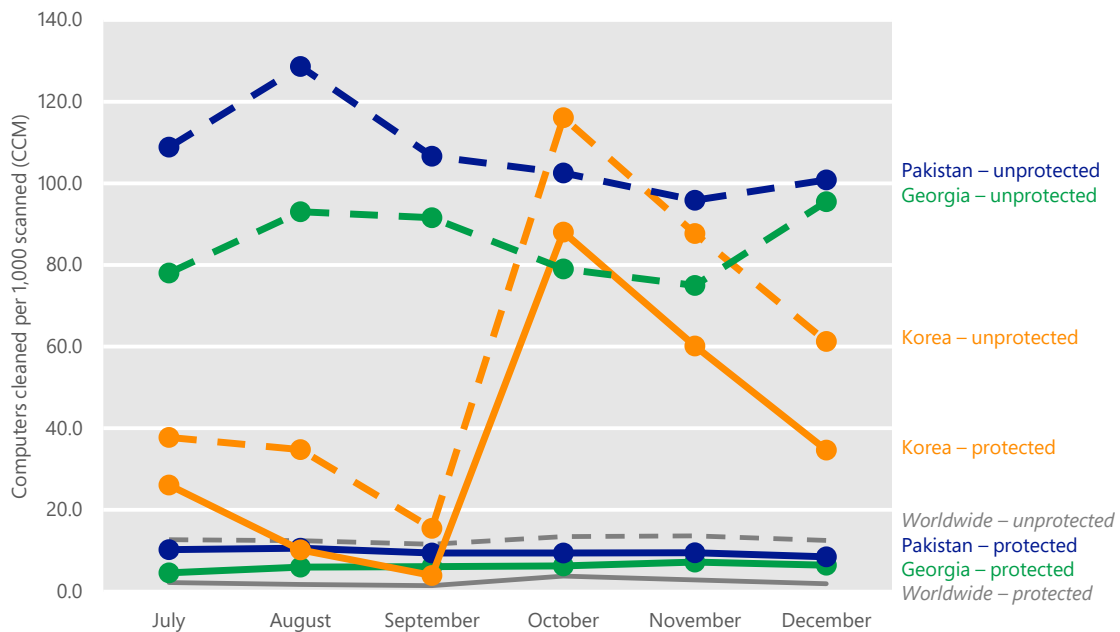
greater risk from malware than do users who leave real-time protection enabled.<sup>6</sup>

See “Operating system infection rates” on page 43 for more information and statistics about infection rates by operating system.

### Geographic statistics

Figure 8 and Figure 9 show the infection rate differences for protected and unprotected computers in locations around the world with particularly high and low infection rates overall.

Figure 8. Infection rates for protected and unprotected computers in three locations with high CCM



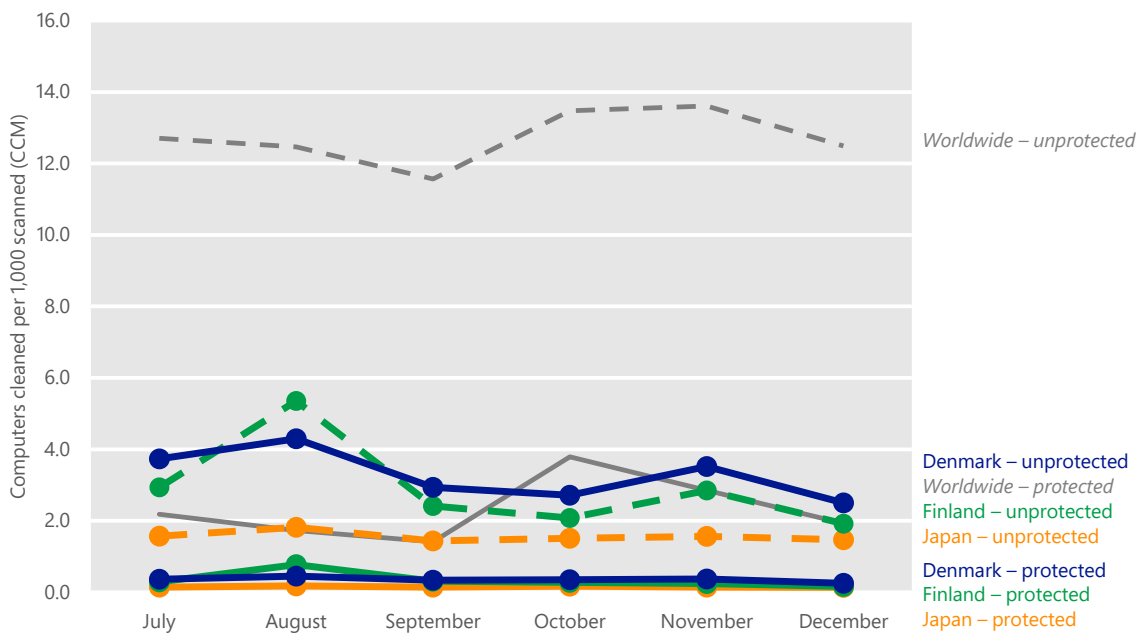
Pakistan and Georgia, which both had significantly more computers without up-to-date real-time protection than the world as a whole (38.6 percent in Pakistan, 33.5 percent in Georgia) also displayed a larger infection rate gap between protected and unprotected computers than the world overall. In Pakistan, unprotected computers were 11.7 times more likely to be infected than protected computers, which translates to a CCM over 100.0 in 5 out of the 6 months in 2H12—in other words, the MSRT found that more than 1 of every 10 unprotected computers in Pakistan was infected with malware. In Georgia,

<sup>6</sup> See “Deceptive downloads: Software, music, and movies” on page 1 of *Microsoft Security Intelligence Report, Volume 13 (January–June 2012)* for more information about Keygen and the threats users face from insecure software distribution channels.

unprotected computers were 14.0 times more likely to be infected than protected computers, with CCM figures between 75.0 and 95.5 each month, compared to a range of 4.6 to 6.4 for protected computers in Georgia.

In Korea, infection rates for both protected and unprotected computers were heavily influenced by a steep increase in detections of the rogue security software family [Win32/Onescan](#) and the Trojan downloader family [Win32/Pluzoks](#), which affected both protected and unprotected computers in similar proportions. Overall, the infection rate for unprotected computers in Korea in 2H12 was 1.6 times higher than the infection rate for protected computers there. See “Rogue security software” on page 52 for more information.

Figure 9. Infection rates for protected and unprotected computers in three locations with low CCM



Unprotected computers in Japan have an infection rate that is 10.4 times higher than the infection rate for protected computers. The overall infection rate in Japan for protected users is very low, at 0.2 on average. Unprotected users make up 23.2 percent of computers in Japan, which is slightly lower than the worldwide average.

The infection rate for unprotected computers in Finland is 8.6 times higher than the infection rate for protected computers there. Finland also has a significantly higher adoption rate for real-time security software than the world as a whole,

with only 14.6 percent of computers in Finland lacking up-to-date real-time protection.

In Denmark, unprotected computers have an infection rate that is 9.3 times higher than that of protected computers. The adoption rate for real-time security software in Denmark is slightly higher than for the world as a whole, with 19.8 percent of computers lacking up-to-date real-time protection, about 4 percentage points lower than the global average.

## Guidance: Fighting infection with real-time protection

Although there is no such thing as a perfect security product, the findings in this section clearly show that using real-time security software from a reputable vendor and keeping it up to date are two of the most important steps individuals and organizations can take to reduce the risk they face from malware and potentially unwanted software. With attackers becoming ever more proficient at exploiting software vulnerabilities and trusted relationships to spread malware in unexpected ways, it is dangerous for even expert users to assume that they will be able to detect threats on their own without the help of real-time protection before being affected by them. Simply installing and using real-time antimalware software can help individuals and organizations reduce malware infection by more than 80 percent. See [www.microsoft.com/windows/antivirus-partners](http://www.microsoft.com/windows/antivirus-partners) for a list of vendors that provide consumer security software solutions for Windows.

Users who believe their security software may have been disabled by malware should take advantage of a tool like the Microsoft Safety Scanner ([www.microsoft.com/security/scanner/](http://www.microsoft.com/security/scanner/)) or Windows Defender Offline ([windows.microsoft.com/en-US/windows/what-is-windows-defender-offline](http://windows.microsoft.com/en-US/windows/what-is-windows-defender-offline)) to scan their computers for malware and remove any threats that are found.





# Worldwide threat assessment



# 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.

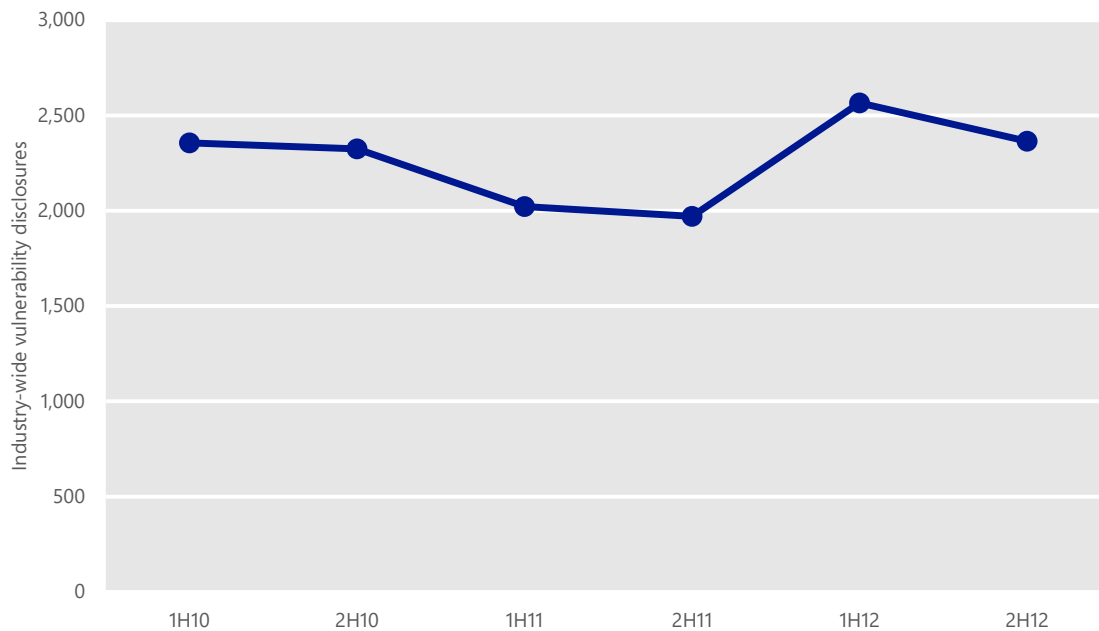
The information in this section is compiled from vulnerability disclosure data that is published in the National Vulnerability Database (NVD), the US government repository of standards-based vulnerability management data at [nvd.nist.gov](http://nvd.nist.gov). The NVD represents all disclosures that have a published CVE (Common Vulnerabilities and Exposures) identifier.<sup>7</sup>

Figure 10 illustrates the number of vulnerability disclosures across the software industry for each half-year period since 1H10. (See "About this report" on page v for an explanation of the reporting period nomenclature used in this report.)

---

<sup>7</sup> 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. Industry-wide vulnerability disclosures, 1H10–2H12



- Vulnerability disclosures across the industry were down 7.8 percent from 1H12, primarily because of a decrease in application vulnerability disclosures. (See “Operating system, browser, and application vulnerabilities” on page 21 for more information.) Despite this decline, vulnerability disclosures were up 20.0 percent in 2H12 compared to 2H11, a year prior.
- An increase in application vulnerability disclosures in 1H12 interrupted a trend of consistent period-over-period decreases dating back to 2H09. It remains to be seen whether the decrease in 2H12 marks a return to this trend. Overall, however, vulnerability disclosures remain significantly lower than they were prior to 2009, when totals of 3,500 disclosures or more per half-year period were not uncommon.

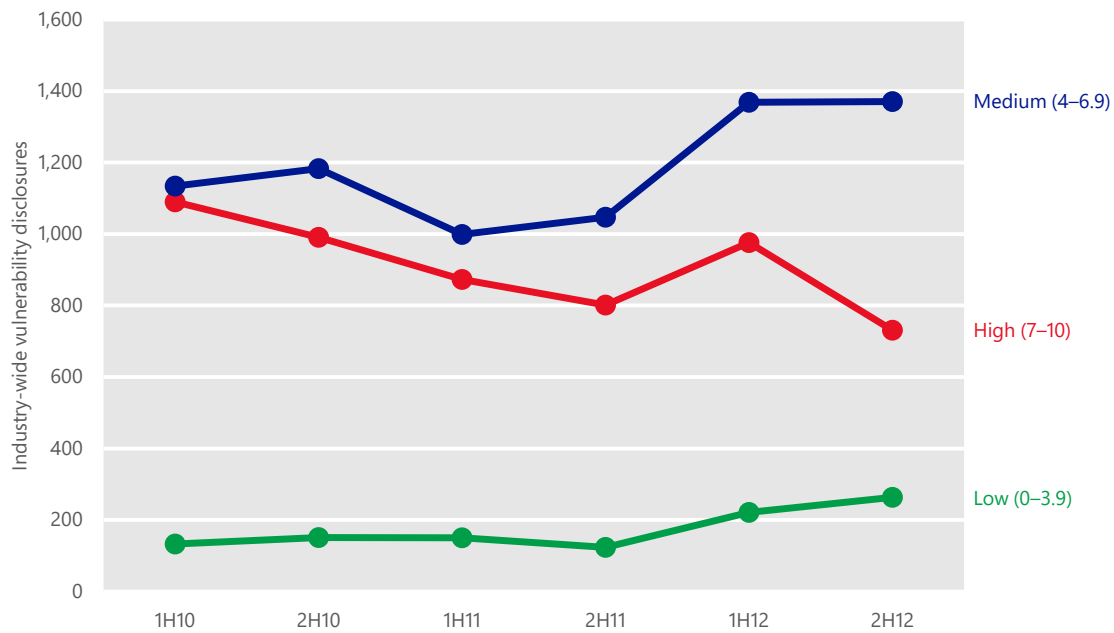
For a ten-year view of the industry vulnerability disclosure trend, see the entry “[Trustworthy Computing: Learning About Threats for Over 10 Years—Part 4](#)” (March 15, 2012) at the Microsoft Security Blog at [blogs.technet.com/security](http://blogs.technet.com/security).

## 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 for more information.)

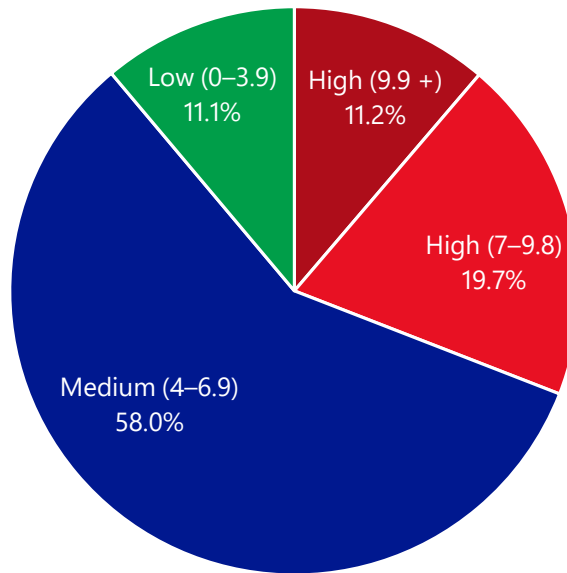
Figure 11. Industry-wide vulnerability disclosures by severity, 1H10–2H12



- The overall decrease in industry-wide vulnerability disclosures shown in Figure 10 was caused entirely by a decrease in high-severity vulnerabilities, shown in Figure 11, which declined 25.1 percent from 1H12. High-severity vulnerabilities accounted for 30.9 percent of total disclosures in 2H12, compared to 38.0 percent in the previous period.
- Medium-severity vulnerability disclosures remained stable, increasing 0.1 percent from 1H12. Medium-severity vulnerabilities accounted for 58.0 percent of total disclosures in 2H12.
- Low-severity vulnerability disclosures increased 19.0 percent from 1H12 but remained relatively low, accounting for 11.1 percent of total disclosures in 2H12.
- Mitigating the most severe vulnerabilities first is a security best practice. Vulnerabilities that scored 9.9 or greater represent 11.2 percent of all vulnerabilities disclosed in 2H12, as Figure 12 illustrates. These figures are a slight increase from 1H12, when vulnerabilities that scored 9.9 or greater accounted for 9.7 percent of all vulnerabilities. Vulnerabilities that scored

between 7.0 and 9.8 decreased to 19.7 percent in 2H12, down from 29.0 percent in 1H12.

Figure 12. Industry-wide vulnerability disclosures in 2H12, by severity



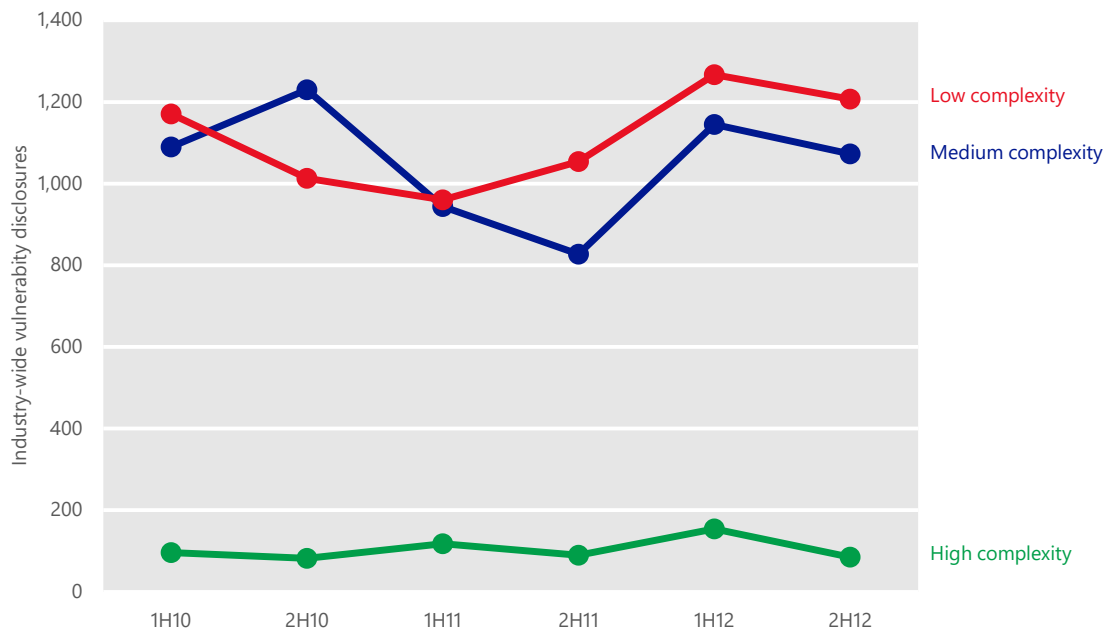
## Vulnerability complexity

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](#) at the *Microsoft Security Intelligence Report* website for more information about the CVSS complexity ranking system.)

Figure 13 shows complexity trends for vulnerabilities disclosed since 1H10. Note that Low complexity in Figure 13 indicates greater risk, just as High severity indicates greater risk in Figure 11.

Figure 13. Industry-wide vulnerability disclosures by access complexity, 1H10–2H12



Low complexity indicates the greatest risk; High complexity indicates the least risk.

- Vulnerability disclosures in each of the three complexity classifications decreased by a roughly similar amount, as shown in Figure 13.
- Disclosures of Low-complexity vulnerabilities—those that are the easiest to exploit—accounted for 51.0 percent of all disclosures in 2H12, a slight increase from 49.4 percent in 1H12.
- Disclosures of Medium-complexity vulnerabilities accounted for 45.4 percent of all disclosures in 2H12, compared to 44.6 percent in 1H12.
- Disclosures of High-complexity vulnerabilities fell to 3.6 percent of all disclosures in 2H12, down from 6.0 percent in 1H12.

## 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 GUI or Internet browsing.

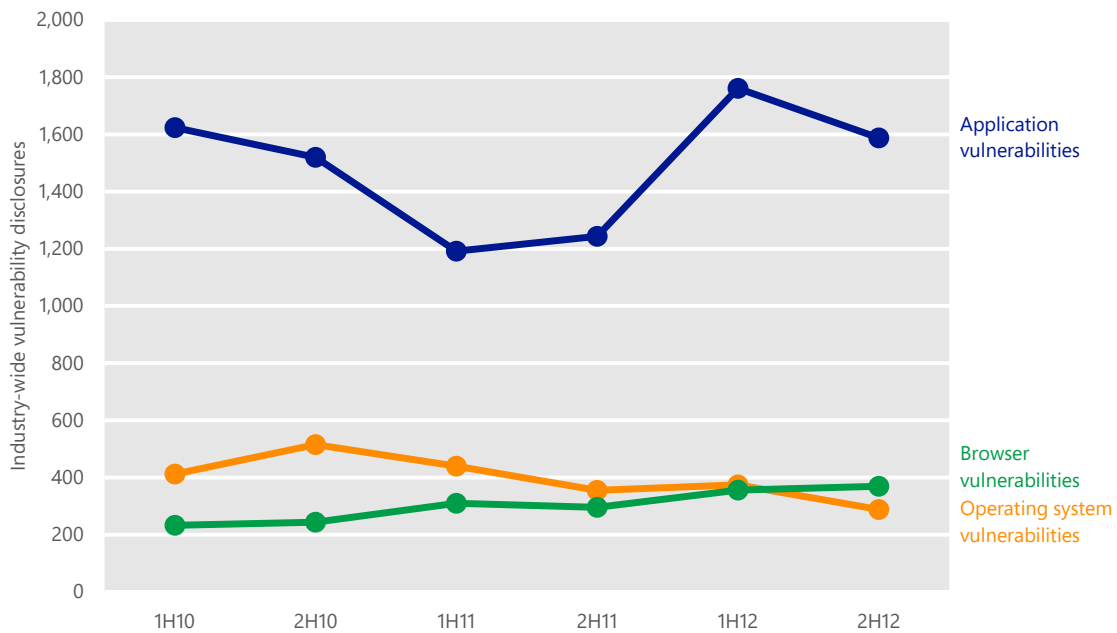
To facilitate analysis of operating system and browser vulnerabilities, the *Microsoft Security Intelligence Report* distinguishes among three different kinds of vulnerabilities:

- *Operating system vulnerabilities* are those that affect the Linux kernel, or that affect components that ship with an operating system produced by Microsoft, Apple, or a proprietary Unix vendor, and are defined as part of the operating system by the vendor, except as described in the next paragraph.
- *Browser vulnerabilities* are those that affect components defined as part of a web browser, including web browsers that ship with operating systems such as Internet Explorer and Apple's Safari, along with third-party browsers such as Mozilla Firefox and Google Chrome.
- *Application vulnerabilities* are those that affect all other components, including executable files, services, and other components published by operating system vendors and other vendors. Vulnerabilities in open source components that may ship with Linux distributions (such as the X Window System, the GNOME desktop environment, GIMP, and others) are considered application vulnerabilities.

Figure 14 shows industry-wide vulnerabilities for operating systems, browsers, and applications since 1H10.



Figure 14. Industry-wide operating system, browser, and application vulnerabilities, 1H10–2H12

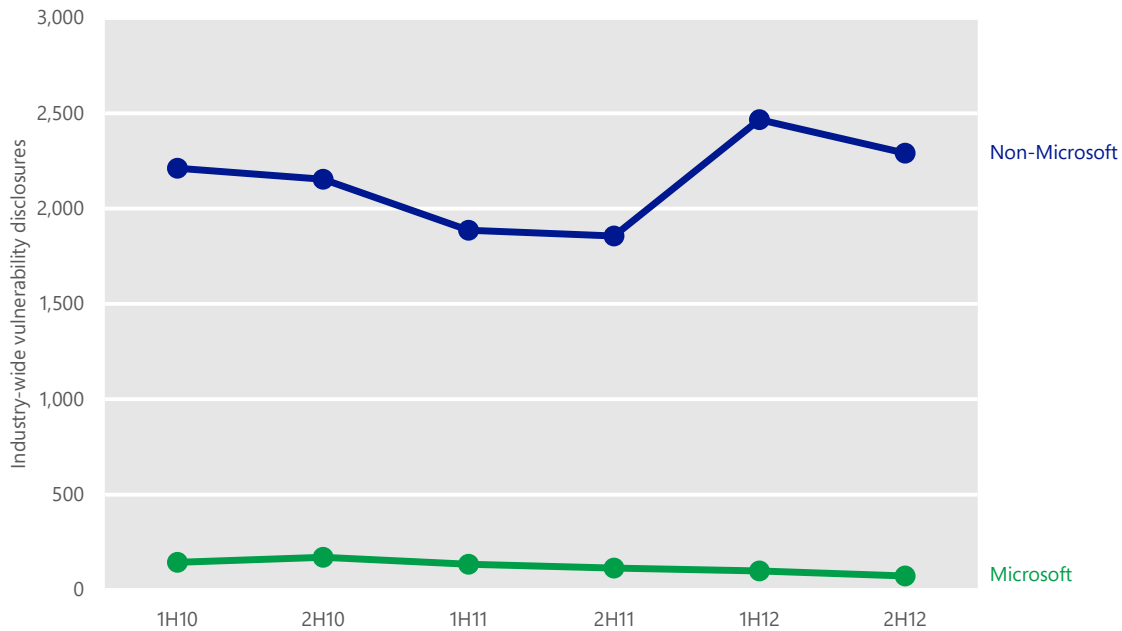


- After increasing significantly in 1H12, application vulnerability disclosures decreased 23.0 percent in 2H12, which accounted for nearly the entire decline in industry-wide vulnerability disclosures observed for the period. Application vulnerability disclosures accounted for 70.7 percent of total disclosures for the period.
- Operating system vulnerability disclosures dropped to their lowest level since 2003, although vulnerabilities in web browsers continued a multi-year trend upwards. In previous periods, disclosures of operating system vulnerabilities routinely outnumbered those of browser vulnerabilities; however, in 2H12 browser vulnerability disclosures accounted for 16.4 percent of total disclosures, compared to just 12.8 percent for operating system vulnerability disclosures.

## Microsoft vulnerability disclosures

Figure 15 shows vulnerability disclosures for Microsoft and non-Microsoft products since 1H10.

Figure 15. Vulnerability disclosures for Microsoft and non-Microsoft products, 1H10–2H12



- Disclosures of vulnerabilities in Microsoft products in 2H12 fell 26.3 percent to their lowest level since 2005.
- Overall, disclosures of vulnerabilities in Microsoft products accounted for 3.1 percent of all disclosures across the industry, down from 3.9 percent in 1H12.

## Guidance: Developing secure software

The Security Development Lifecycle ([www.microsoft.com/sdl](http://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 the software and help manage vulnerabilities that might be found after deployment. (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 the 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.<sup>8</sup>

Software vulnerabilities are enumerated and documented in the Common Vulnerabilities and Exposures (CVE) list ([cve.mitre.org](http://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.<sup>9</sup>

Microsoft security products can detect and block exploit attempts whether the affected computer is vulnerable to them or not. (For example, the [CVE-2010-2568](#) vulnerability has never affected Windows 8, but if a Windows 8 user receives a malicious file that attempts to exploit that vulnerability, Windows Defender should detect and block it anyway.) Therefore, the statistics presented here should not be interpreted as evidence of successful exploit attempts, or of the relative vulnerability of computers to different exploits.

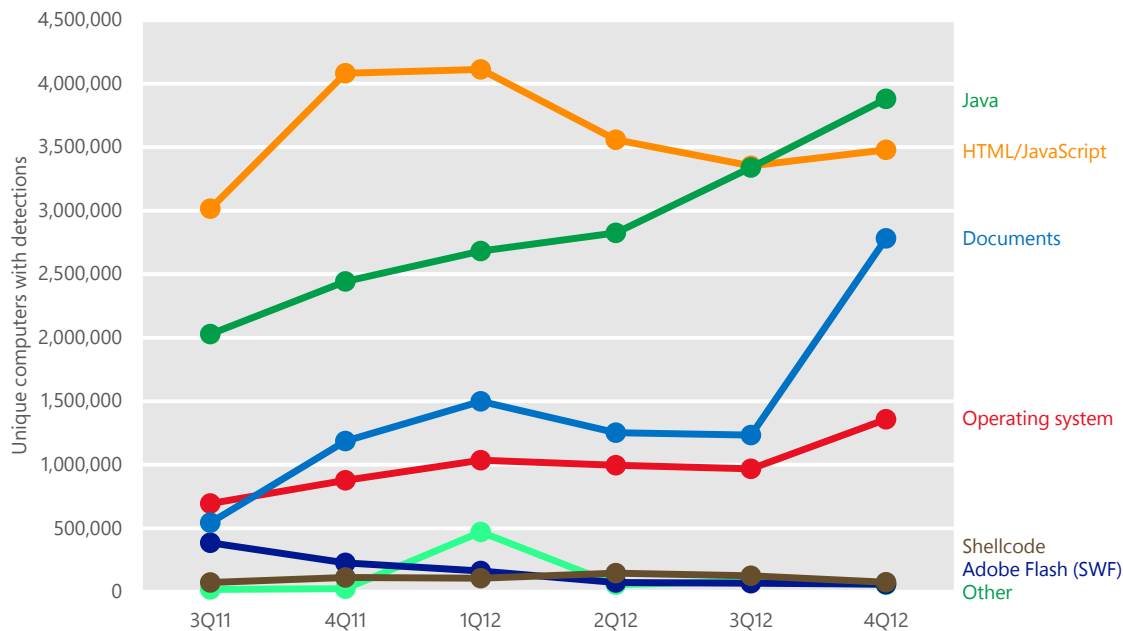
Figure 16 shows the prevalence of different types of exploits detected by Microsoft antimalware products each quarter from 3Q11 to 4Q12, by number of unique computers affected. (See "Appendix B: Data sources" on page 87 for more information about the products and services that provided data for this report.)

---

<sup>8</sup> See the Microsoft Security Update Guide at [www.microsoft.com/security/msrc/whatwedo/securityguide.aspx](http://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.

<sup>9</sup> See [technet.microsoft.com/security/bulletin](http://technet.microsoft.com/security/bulletin) to search and read Microsoft Security Bulletins.

Figure 16. Unique computers reporting different types of exploits, 3Q11–4Q12



- Computers that report more than one type of exploit are counted for each type detected.
- Detections of individual exploits often rise and fall significantly from quarter to quarter as exploit kit distributors add and remove different ones from their kits. This can also have an effect on the relative prevalence of different exploit types, as shown in Figure 16.
- Detections of Java exploits grew steadily throughout the year, surpassing HTML/JavaScript exploits in 2H12. See “Java exploits” on page 28 for more information.
- The number of computers reporting exploits delivered through HTML or JavaScript remained high during the second half of 2012, primarily driven by the continued prevalence of the multiplatform exploit family [Blacole](#). (More information about Blacole is provided in the next section.)
- Exploits that target vulnerabilities in document readers and editors rose sharply in 4Q12, driven by increased detections of [Win32/Pdfjsc](#). See “Document exploits” on page 31 for more information about these exploits.
- After falling slightly for two quarters, detections of operating system exploits increased by more than a third from 3Q12 to 4Q12, led by [CVE-2010-2568](#)

(MS10-046), CVE-2010-1885 (MS10-042), and Unix/Lotoor. See “Operating system exploits” on page 32 for more information.

## Exploit families

Figure 17 lists the exploit-related families that were detected most often during the second half of 2012.

Figure 17. Quarterly trends for the top exploit families detected by Microsoft antimalware products in 2H12, by number of unique computers with detections, shaded according to relative prevalence

Exploit	Platform or technology	1Q12	2Q12	3Q12	4Q12
Win32/Pdfjsc	Documents	1,430,448	1,217,348	1,190,116	2,760,390
CVE-2012-1723*	Java	—	—	1,300,554	2,392,818
Blacole	HTML/JavaScript	3,154,826	2,793,451	2,465,810	2,381,505
Malicious Iframe	HTML/JavaScript	950,347	812,470	567,014	1,017,351
CVE-2010-2568 (MS10-046)	Operating system	726,797	783,013	791,520	1,001,053
CVE-2012-0507*	Java	205,613	1,494,074	1,417,804	940,989
CVE-2012-4681	Java	—	—	323,981	660,291
CVE-2011-3544	Java	1,358,266	803,053	521,879	443,475
CVE-2012-5076	Java	—	—	—	311,811
CVE-2011-3402 (MS11-087)	Operating system	42	24	66	199,648

\* This vulnerability is also used by the Blacole kit; the totals given here for this vulnerability exclude Blacole detections.

- Detections of [Win32/Pdfjsc](#), a detection for specially crafted PDF files that exploit vulnerabilities in Adobe Reader and Adobe Acrobat, more than doubled from 3Q12 to 4Q12. It was the most commonly detected exploit during the last quarter of the year and the second most common for the half-year period overall. See page 31 for more information about Pdfjsc.
- Blacole is Microsoft’s detection name for components of the so-called “Blackhole” exploit kit, which delivers malicious software through infected webpages. Blacole was the most commonly detected exploit family in the second half of 2012. 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

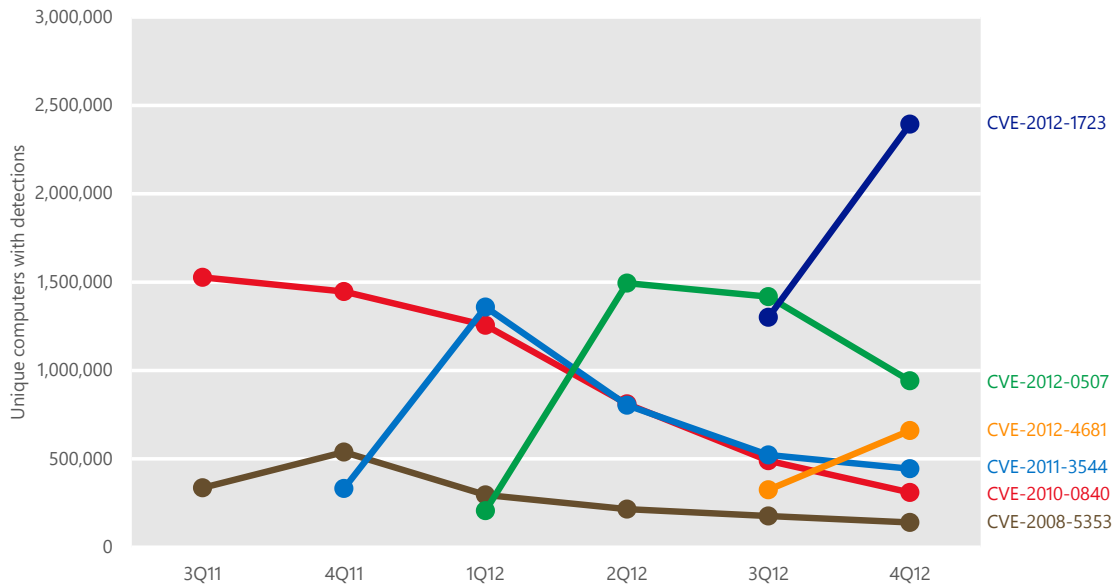
have the appropriate security updates installed are at risk of infection through a drive-by download attack. (See page 78 for more information about drive-by download attacks.)

- Detections of exploits that target [CVE-2011-3402](#), a vulnerability in the way the Windows kernel processes TrueType font files, increased in 4Q12 when they were added to the so-called Cool exploit kit. See page 34 for more information.

## Java exploits

Figure 18 shows the prevalence of different Java exploits by quarter.

Figure 18. Trends for the top Java exploits detected and blocked by Microsoft antimalware products in 2H12



- [CVE-2012-1723](#) accounted for most of the Java exploits detected and blocked in 4Q12. Like [CVE-2012-0507](#), which was exploited heavily in 2Q12, 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 published a [security update](#) to address it the same month. 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.

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

- CVE-2012-0507, which accounted for the largest number of Java exploits detected and blocked in 3Q12, was detected in much greater numbers during 2Q12; exploits of this vulnerability then declined significantly, apparently in favor of the more recently discovered CVE-2012-1723, which was added to the Blacole kit in 2H12. Detections of CVE-2012-0507 exploits continued to decline in 4Q12.

CVE-2012-0507 allows an unsigned Java applet to gain elevated permissions and potentially have unrestricted access to a host system outside its sandbox environment. Oracle released a [security update](#) in February 2012 to address the issue. The CVE-2012-0507 vulnerability is a logic error that allows attackers to run code with the privileges of the current user, which means that an attacker can use it to perform reliable exploitation on other platforms that support the JRE, including Apple Mac OS X, Linux, VMWare, and others. On Mac OS X, CVE-2012-0507 exploits have been observed to install [MacOS\\_X/Flashback](#), a trojan that gained notoriety in early 2012.

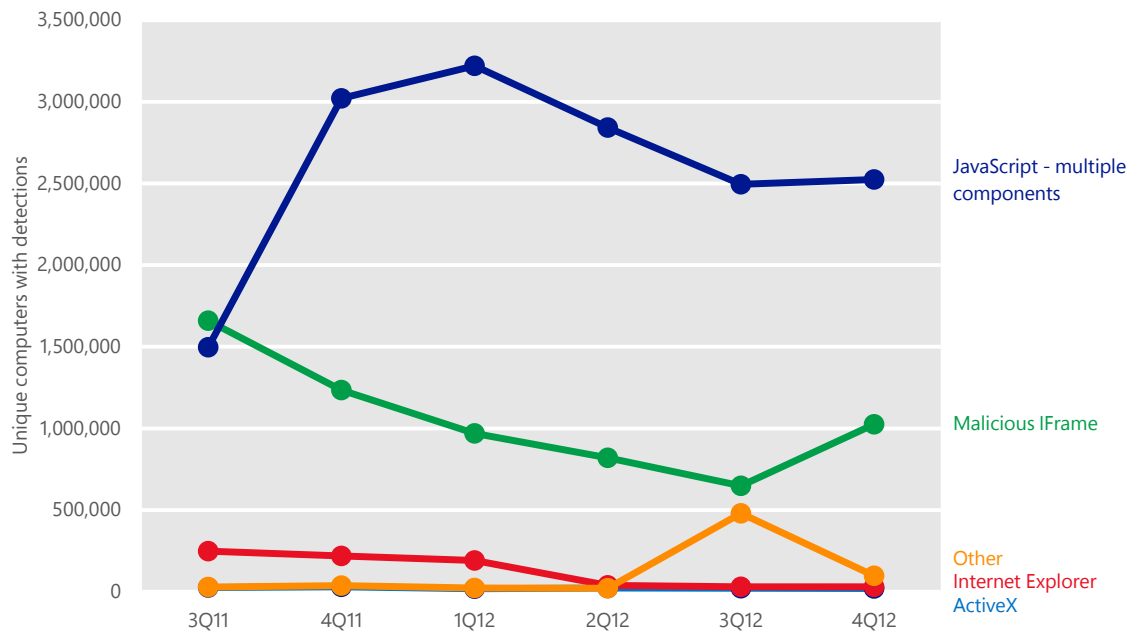
For more information about this vulnerability, see the entry "[An interesting case of JRE sandbox breach \(CVE-2012-0507\)](#)" (March 20, 2012) at the MMPC blog.

- Detections of exploits targeting [CVE 2011-3544](#) and [CVE-2010-0840](#), two vulnerabilities with significant exploitation in the first half of the year, declined in 2H12. Both are cross-platform vulnerabilities that were formerly targeted by the Blacole kit but have been removed from more recent versions of the kit.

## HTML and JavaScript exploits

Figure 19 shows the prevalence of different types of HTML and JavaScript exploits during each of the six most recent quarters.

Figure 19. Types of HTML and JavaScript exploits detected and blocked by Microsoft antimalware products, 3Q11–4Q12



- The use of malicious JavaScript code designed to exploit one or more web-enabled technologies declined in 2H12. However, these exploits continued to account for most of the HTML and JavaScript exploits detected during the period, primarily because of the Blacole exploit kit. (See page 27 for more information about Blacole.)
- Detections of exploits that involve malicious HTML inline frames (IFrames) continued their multi-quarter decline in 3Q12, then nearly doubled from 3Q12 to 4Q12. These exploits are typically generic detections of inline frames that are embedded in webpages and link to other pages that host malicious web content. 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 increase in detections in 4Q12 may have been caused in part by spam campaigns that distributed HTML attachments containing malicious IFrames to recipients in email messages that purported to come from well-known organizations, in a manner similar to phishing.
- Detections of exploits that target ActiveX, Internet Explorer, and other browser vulnerabilities remained comparatively low.

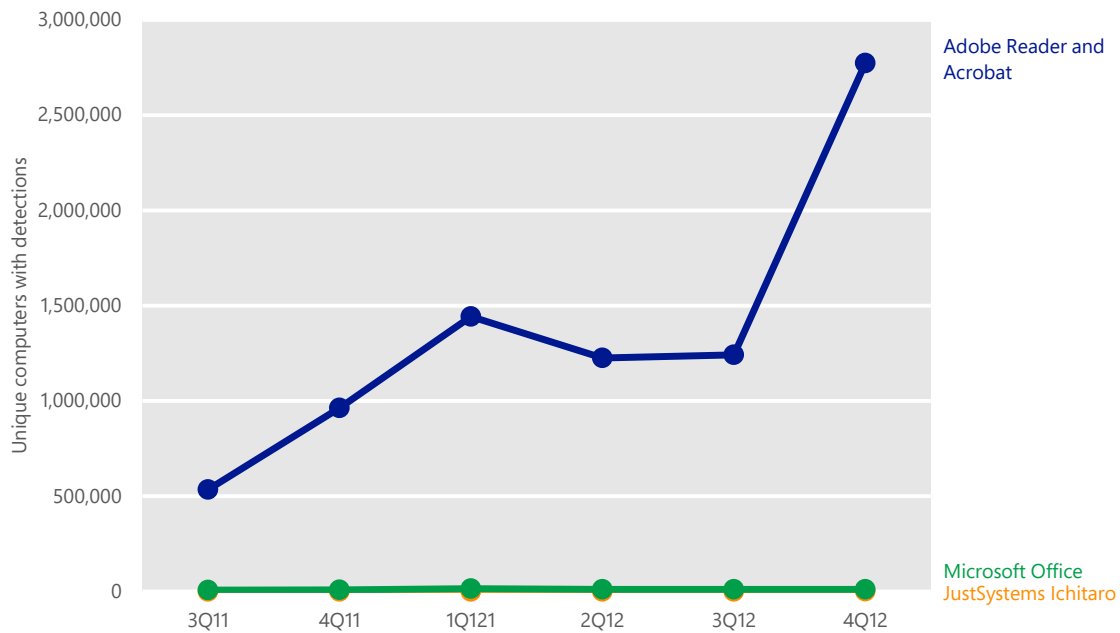


## Document exploits

*Document exploits* are exploits that target vulnerabilities in the way a document editing or viewing application processes, or parses, a particular file format.

Figure 20 shows the prevalence of different types of document exploits during each of the six most recent quarters.

Figure 20. Types of document exploits detected and blocked by Microsoft antimalware products, 3Q11–4Q12



- Detections of exploits that affect Adobe Reader and Adobe Acrobat more than doubled from 3Q12 to 4Q12. Almost all of these exploits were detected as variants of the generic exploit family [Win32/Pdfjsc](#), as shown in Figure 21.

Figure 21. Top document exploit families detected by Microsoft antimalware products in 4Q12, by number of unique computers with detections

	Exploit	Delivery	Affected component	Computers with detections
1	Win32/Pdfjsc	PDF	Adobe Acrobat	2,760,390
2	CVE-2010-0188	PDF	Adobe Acrobat	5,813
3	CVE-2011-0097	Office document	Microsoft Office	3,917
4	Win32/Pidief	PDF	Adobe Acrobat	3,719
5	Win32/Wordinvop	Office document	Microsoft Word	3,632

Pdfjsc is a generic detection for PDF files that contain malicious JavaScript designed to exploit vulnerabilities in different versions of Adobe Reader and

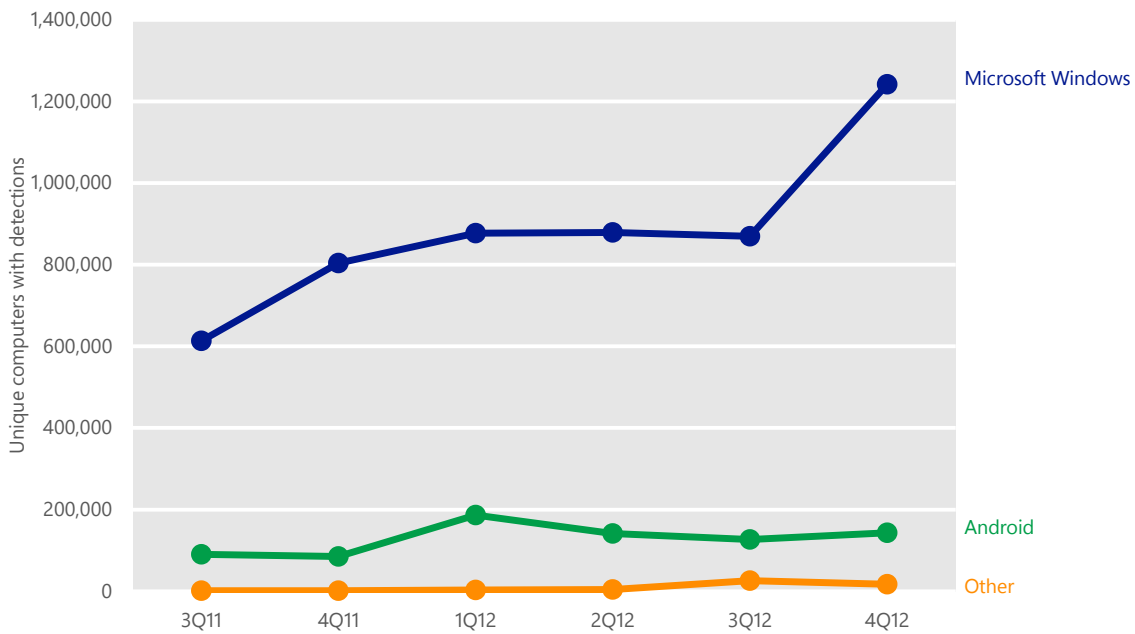
Adobe Acrobat. The rise in detections observed in 4Q12 may be caused by increased use of this technique by a number of exploit kits, including Blacole.

- Exploits that affect Microsoft Office and Ichitaro, a Japanese-language word processing application published by JustSystems, accounted for a small percentage of exploits detected during the period.

## 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, computer users sometimes download malicious or infected files that affect other operating systems. Figure 22 shows the prevalence of different exploits against operating system vulnerabilities that were detected and removed by Microsoft antimalware products during each of the past six quarters.

Figure 22. Exploits against operating system vulnerabilities detected and blocked by Microsoft antimalware products, 3Q11–4Q12

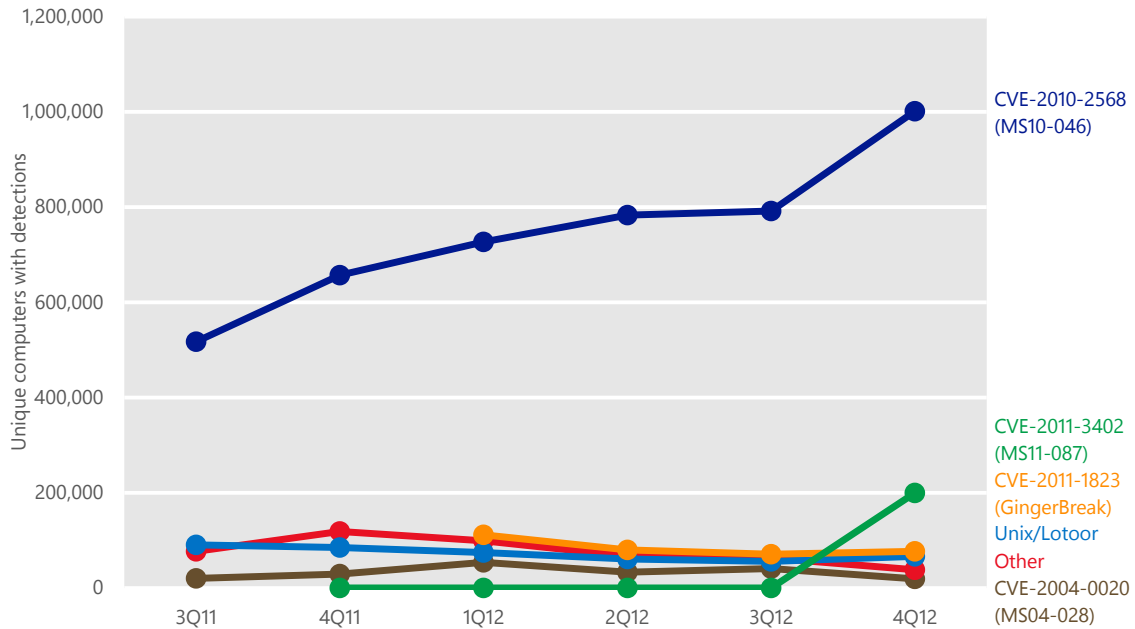


- Detections of exploits that affect Microsoft Windows increased 42 percent from 3Q12 to 4Q12, because of increased detections of exploits that target a pair of vulnerabilities, [CVE-2010-2568](#) and [CVE-2011-3402](#). See Figure 23 for more information about these exploits.
- Detections of exploits that affect the Android mobile operating system published by Google and the Open Handset Alliance accounted for about

15 percent of operating system exploit detections in 4Q12. Microsoft security products detect these threats when Android devices or storage cards are connected to computers running Windows, or when Android users unknowingly download infected or malicious programs to their computers before transferring the software to their devices. See page 34 for more information about these exploits.

For another perspective on these exploits and others, Figure 23 shows trends for the individual exploits most commonly detected and blocked or removed during each of the past six quarters.

Figure 23. Individual operating system exploits detected and blocked by Microsoft antimalware products, 3Q11–4Q12, by number of unique computers exposed to the exploit



- Detections of exploits that target CVE-2010-2568, a vulnerability in Windows Shell, increased by 26.5 percent from 3Q12 to 4Q12, and accounted for more than 85 percent of Windows exploit detections in the second half of the year. 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. Microsoft released Security Bulletin [MS10-046](#) in August 2010 to address this issue.

The vulnerability was first discovered being used by the malware family [Win32/Stuxnet](#) in mid-2010. It has since been exploited by a number of other malware families, many of which predated the disclosure of the

vulnerability and were subsequently adapted to attempt to exploit it. The 4Q12 increase suggests that attackers have begun to target CVE-2010-2568 more aggressively, particularly on computers in Asia, as Figure 24 shows.

Figure 24. Countries and regions with the most detections of exploits targeting CVE-2010-2568 in 4Q12

Rank	Country or region	Computers	Rank	Country or region	Computers
1	India	166,567	11	Algeria	18,103
2	Indonesia	120,937	12	Ukraine	18,050
3	Vietnam	115,664	13	Egypt	17,030
4	Pakistan	64,447	14	Russia	16,080
5	Mexico	44,613	15	Colombia	15,704
6	Philippines	35,058	16	Bangladesh	15,049
7	Turkey	32,852	17	United States	11,157
8	Saudi Arabia	23,953	18	Morocco	9,224
9	Thailand	23,164	19	Tunisia	9,160
10	Brazil	18,627	19	Iraq	9,160

- Detections of exploits that target CVE-2011-3402, which had numbered less than 100 in each quarter since the vulnerability was discovered, increased to nearly 200,000 in 4Q12. CVE-2011-3402 is a vulnerability in the way the Windows kernel processes TrueType font files. An attacker exploits the vulnerability by encouraging a user to open a specially crafted document or visit a malicious webpage that embeds TrueType font files, which enables the attacker to run arbitrary code in kernel mode. Microsoft released Security Bulletin [MS11-087](#) in December 2011 to address this issue.

CVE-2011-3402 is targeted by exploits in 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. Recent versions of the Blacole kit may also include exploits that target the vulnerability. Together, the Cool and Blacole kits are likely responsible for most or all of the increase in CVE-2011-3402 detections.

- Most detections that affect Android involve a pair of exploits that enable an attacker or other user to obtain root privileges on vulnerable Android devices. Device owners sometimes use such exploits intentionally to gain access to additional functionality (a practice often called *rooting* or

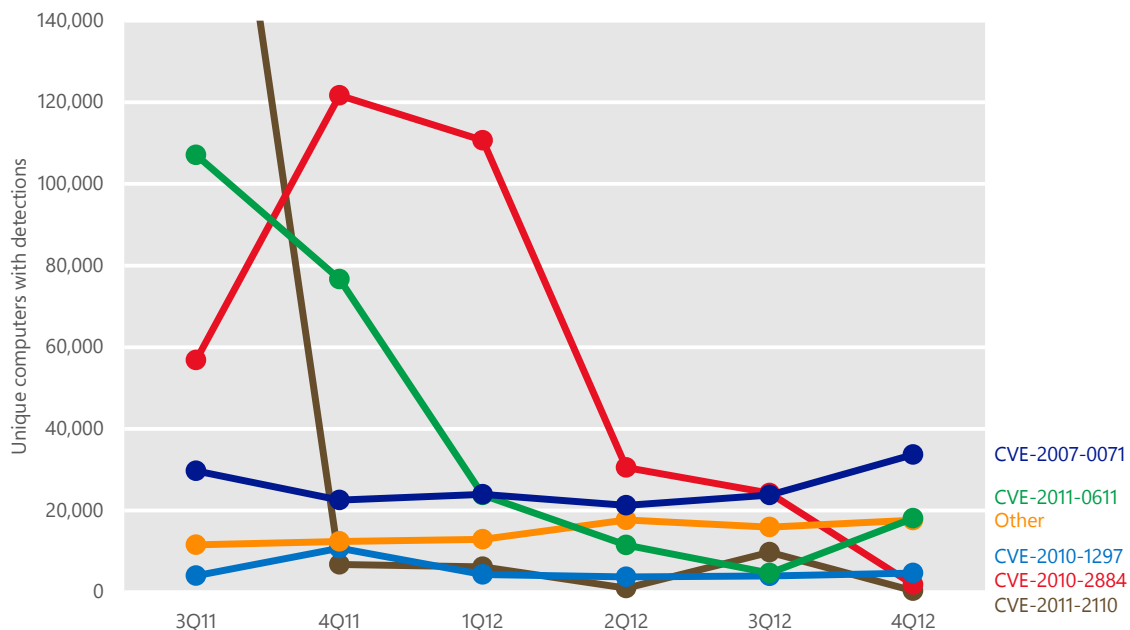
jailbreaking), but these exploits can also be used by attackers to infect devices with malware that bypasses many typical security systems.

- [CVE-2011-1823](#) is sometimes called the GingerBreak vulnerability because of its use by a popular rooting application of that name (detected separately as [Exploit:AndroidOS/GingerBreak](#)). 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 dropped by [TrojanSpy:AndroidOS/DroidDream.A](#), a malicious program that often masquerades as a legitimate Android application and can allow a remote attacker to gain access to the device. Google published a source code update in March 2011 that addressed the vulnerability.

## Adobe Flash Player exploits

Figure 25 shows the prevalence of different Adobe Flash Player exploits by quarter.

Figure 25. Adobe Flash Player exploits detected and blocked by Microsoft antimalware products, 3Q11–4Q12, by number of unique computers exposed to the exploit



- Detections of exploits that target Adobe Flash Player remained at a relatively low level throughout the second half of 2012. No one vulnerability accounted for most of the exploits, unlike in previous quarters.
- [CVE-2007-0071](#), an invalid pointer vulnerability in some releases of Adobe Flash Player versions 8 and 9, accounted for the largest number of Adobe Flash Player exploitation attempts detected in 3Q12 and 4Q12. Adobe released Security Bulletin [APSB08-11](#) on April 8, 2008 to address the issue. Detections increased 58.5 percent between 2Q12 and 4Q12, probably because of the popularity of exploits for the vulnerability in exploit kits.
- [CVE-2011-0611](#) accounted for the second largest number of Adobe Flash Player exploitation attempts detected in 2H12. CVE-2011-0611 was discovered in April 2011 when it was observed being exploited in the wild; Adobe released Security Bulletin [APSB11-07](#) on April 15 and Security Bulletin [APSB11-08](#) on April 21 to address the issue. Detections of CVE-2011-0611 exploits nearly tripled between 3Q12 and 4Q12, but remained well below levels observed in earlier quarters.
- Detections of exploits that target [CVE-2010-2884](#), the most commonly targeted vulnerability in 1H12, declined to very low levels in the second half of the year. CVE-2010-2884 was discovered in the wild in September 2010 as a zero-day vulnerability, and Adobe released Security Bulletin [APSB10-22](#) the same month to address the issue. The decline is likely caused by more computers receiving the security update combined with an overall saturation of exploitable targets.

# Malware and potentially unwanted software

Except where specified, the information in this section was compiled from telemetry data that was generated from more than 1 billion computers worldwide and some of the busiest services on the Internet. (See “Appendix B: Data sources” on page 87 for more information about the telemetry used in this report.)

## Global infection rates

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 rates, patterns, and trends in different locations around the world.<sup>10</sup>

Figure 26. Trends for the locations with the most computers reporting detections and removals by Microsoft desktop antimalware products in 2H12

	Country or region	1Q12	2Q12	3Q12	4Q12	Chg. 1H–2H
1	United States	9,407,423	12,474,127	9,647,906	8,959,660	-15.0% ▼
2	Brazil	3,715,163	3,333,429	3,528,282	4,458,573	13.3% ▲
3	Korea	2,137,136	2,820,641	2,019,828	3,259,183	6.5% ▲
4	Russia	2,580,673	2,510,591	2,294,438	2,505,561	-5.7% ▼
5	Turkey	1,924,387	1,911,837	1,925,421	1,900,570	-0.3% ▼
6	China	1,889,392	2,000,576	1,917,106	1,770,264	-5.2% ▼
7	France	1,677,242	1,555,522	1,530,048	1,951,247	7.7% ▲
8	Germany	1,544,774	1,486,309	1,561,074	1,586,739	3.9% ▲
9	India	1,254,378	1,287,945	1,519,086	1,544,008	20.5% ▲
10	United Kingdom	1,648,801	1,509,488	1,460,015	1,516,078	-5.8% ▼

<sup>10</sup> For more information about this process, see the entry “[Determining the Geolocation of Systems Infected with Malware](http://blogs.technet.com/security)” (November 15, 2011) on the Microsoft Security Blog (blogs.technet.com/security).

- In absolute terms, the locations with the most computers reporting detections tend to be ones with large populations and large numbers of computers.
- Detections in the United States fell 7.1 percent in the fourth quarter, and ended the year down 4.8 percent from 1Q12. Fewer detections of the trojan families [Win32/Tracur](#) and [Win32/Sirefef](#) and the exploit family [Blacole](#) were the largest contributors to the decline.
- Detections in Brazil were up 20.0 percent over 1Q12, primarily because of detections of the adware family [Win32/DealPly](#) in the fourth quarter. Detections of the potentially unwanted software families [Win32/Keygen](#) and [Win32/Protlerdob](#) also increased significantly through the end of the year. Protlerdob is a software installer with a Portuguese-language user interface. It presents itself as a free movie download but bundles with it a number of potentially unwanted software programs, including DealPly.

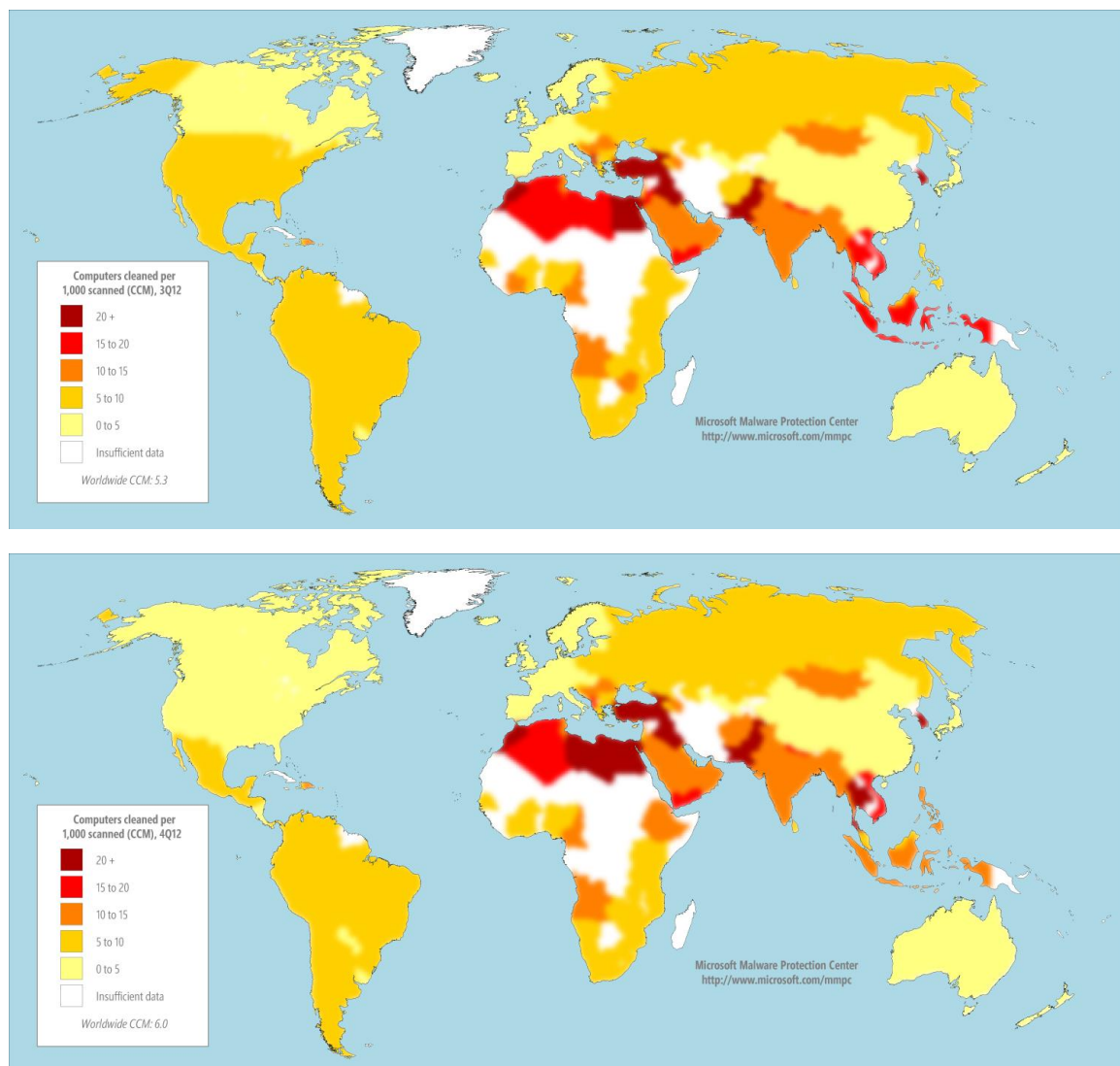
Keygen is a detection for tools that generate keys for various software products. Such tools are often distributed by software pirates to enable users to run software illegally. Attackers often package Keygen tools into bundles with malware alongside or instead of pirated software or media. (See “Deceptive downloads: Software, music, and movies” on page 1 of [Microsoft Security Intelligence Report, Volume 13 \(January–June 2012\)](#) for more information about Keygen and the threats users face from unsecured software distribution channels.)

- Detections in Korea rose 52.5 percent between 1Q12 and 4Q12 because of increased detections of the rogue security software family [Win32/Onescan](#). See page 40 for more information about the infection rate in Korea.
- Detections in Russia were down 2.9 percent from 1Q12, after a trend of declining detections reversed in the fourth quarter because of increased detections of Keygen and the exploit family [Win32/Pdfjsc](#).
- A number of adware families including DealPly and [Win32/Hotbar](#) along with the potentially unwanted software family [Win32/Zwangi](#) contributed to a 16.3 percent rise in detections in France from 1Q12 to 4Q12.
- Detections increased significantly in India beginning in the third quarter, which contributed to a 23.1 percent increase from 1Q12 to 4Q12. Growth in detections of Keygen, the generic family [INF/Autorun](#), and the virus family [Win32/Sality](#) all contributed to the increase.



For a different perspective on infection patterns worldwide, Figure 27 shows the infection rates in locations around the world in *computers cleaned per mille* (CCM), which represents the number of reported computers cleaned for every 1,000 executions of the Microsoft Malicious Software Removal Tool (MSRT). Normalizing the data this way makes it possible to compare malware infection rates of different locations without skewing the data because of differences in populations and install bases. See the [Microsoft Security Intelligence Report website](#) for more information about the CCM metric.

Figure 27. Infection rates by country/region in 3Q12 (top) and 4Q12 (bottom), by CCM

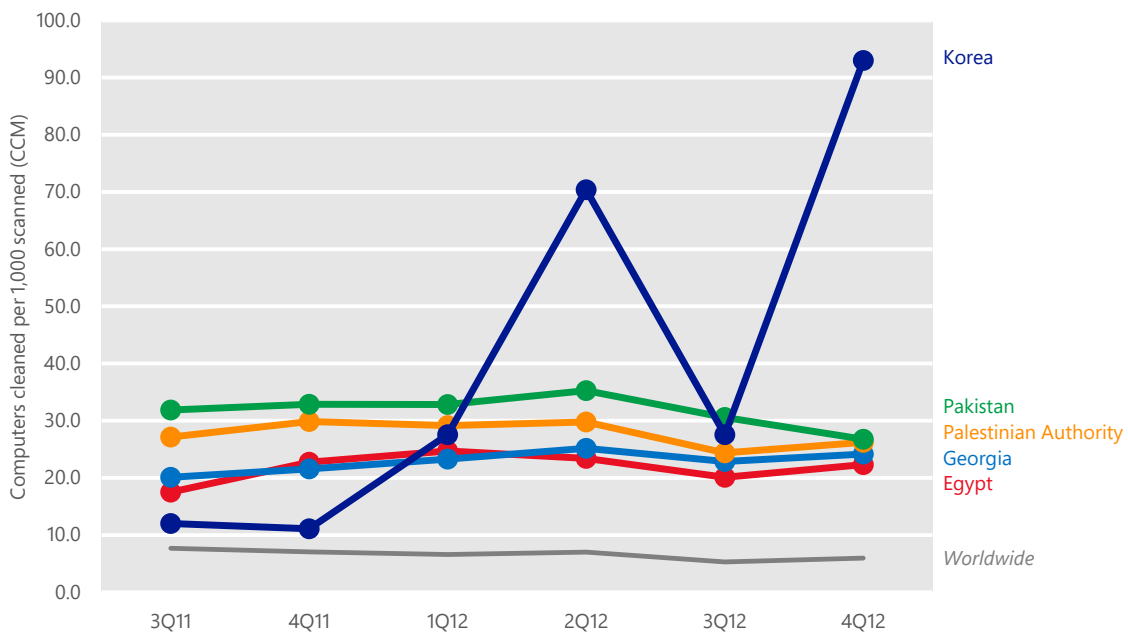


Detections and removals in individual countries/regions can vary significantly from quarter to quarter. Increases in the number of computers with detections

can be caused not only by increased prevalence of malware in that location, but also by improvements in the ability of Microsoft antimalware solutions to detect malware. Large numbers of new antimalware product or tool installations in a location also typically increase the number of computers cleaned in that location.

The next three figures illustrate infection rate trends for specific locations around the world, relative to the trends for all locations with at least 100,000 MSRT executions each quarter in 2H12.

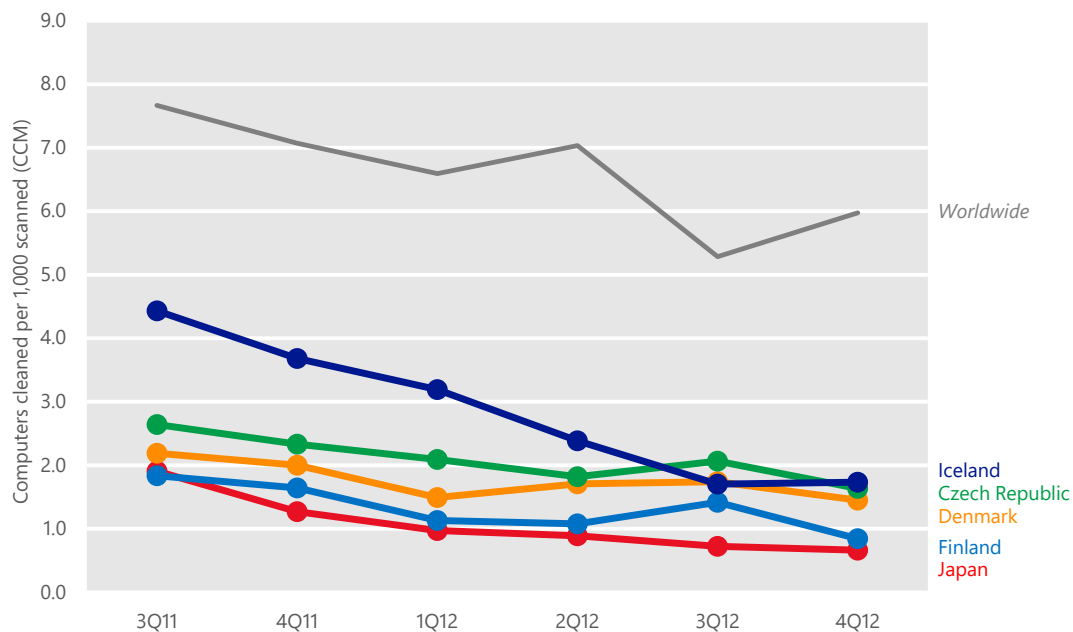
Figure 28. Trends for the five locations with the highest malware infection rates in 2H12, by CCM (100,000 MSRT executions minimum)



- After decreasing from 70.4 in the second quarter to 27.5 in the third quarter, the CCM in Korea ended the year with an infection rate of 93.0, nearly three and a half times that of the next highest location. These spikes are mostly artifacts caused by the addition to the MSRT of detections for two families that have been highly prevalent in Korea, [Win32/Pluzoks](#) in March 2012 and [Win32/Onescan](#) in October. In both cases, detections increased significantly but temporarily as the MSRT detected and removed infections that may have been resident on some computers for several months or even years. (See “Rogue security software” on page 52 for more information about Onescan in Korea.)

- Pakistan, the location with the second highest infection rate in 1H12, remained in second place during the second half of the year. However, its CCM decreased from 35.3 in 2Q12 to 26.8 in 4Q12, which made it one of the locations showing the most improvement in 2H12. (See page 42 for more information.)
- Infection rates in the Palestinian territories, Georgia, and Egypt all increased slightly in 4Q12 after small decreases from 2Q12 to 3Q12. The virus family [Win32/Sality](#) was the most commonly detected family in all three locations.

Figure 29. Trends for locations with low malware infection rates in 2H12, by CCM (100,000 MSRT executions minimum)<sup>11</sup>

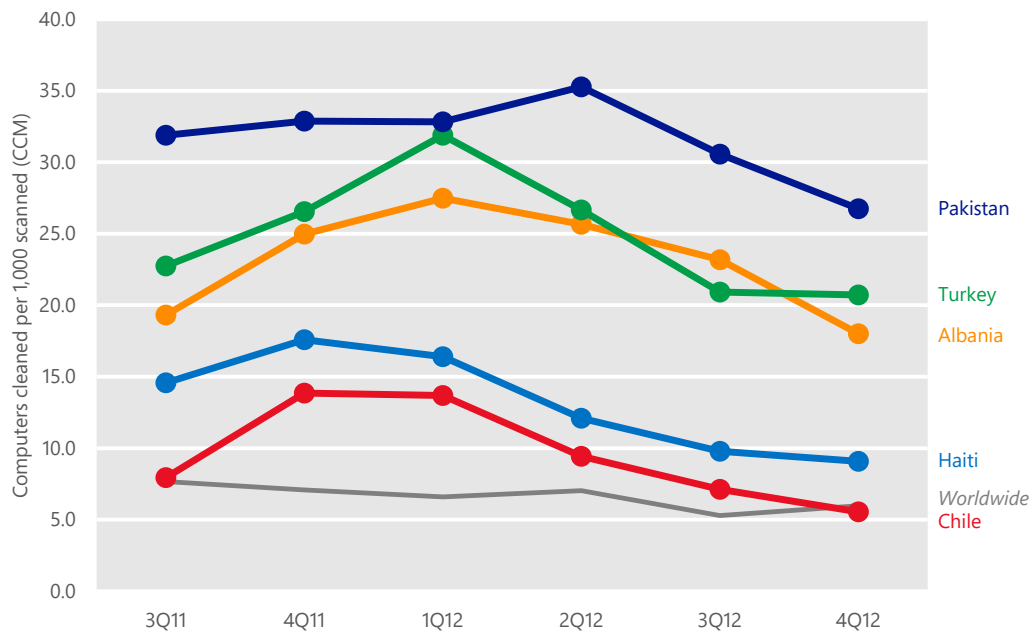


- Trends for the locations with the lowest infection rates in the second half of the year were consistent with previous periods. Denmark, Finland, and Japan (which had the lowest infection rates in 2H12) were also on the list in 1H12, and Iceland had the fourth lowest infection rate of the period following a long period of improvement. The worm family [Win32/Conficker](#), the password stealing trojan [Win32/Zbot](#), and the virus family [Win32/Sality](#) were among the families with the largest detection decreases in Iceland in 2H12.

<sup>11</sup> Figure 29 excludes China, which would otherwise rank among the locations with the lowest infection rates. Microsoft considers the MSRT telemetry from China unreliable for a number of reasons, including the relatively low prevalence of many of the global threats the MSRT monitors compared to the more localized threats that dominate the malware landscape in China. See the entry "[The Threat Landscape in China: A Paradox](#)" (March 11, 2013) on the Microsoft Security Blog at [blogs.technet.com/security](http://blogs.technet.com/security) for more information, and see the "[Regional Threat Assessment](#)" section of the *Microsoft Security Intelligence Report* website for a more in-depth perspective on the threat landscape in China.

- Historically, Nordic countries such as Norway, Finland, and Iceland have had some of the lowest malware infection rates in the world. Japan also typically experiences a low infection rate.
- The CCM in Finland increased from 1.1 in 2Q12 to 1.4 in 3Q12, mostly because of a rise in [Win32/Keygen](#) detections, but declined to 0.8 in 4Q12.<sup>12</sup>

Figure 30. Trends for the five locations with the most significant infection rate improvements from 1H12 to 2H12, by CCM (100,000 MSRT executions minimum per quarter)



- Fewer detections of the virus family [Win32/Sality](#), the sixth most commonly detected threat family worldwide in 4Q12, played a part in most of the declining trends shown in Figure 30.
- The infection rate in Pakistan declined to 26.8 in 4Q12 after peaking at 35.3 in 2Q12. Fewer detections of the virus families Sality and [Win32/Chir](#) and the trojan family [Win32/Ramnit](#) accounted for part of the decline.
- Fewer detections of Sality also improved the infection rates in Albania, as did a reduction in detections of the backdoor family [Win32/IRCbot](#) in 4Q12.
- The infection rate in Turkey improved significantly because of fewer detections of Sality and the worm family [Win32/Helompy](#), which tends to be more prevalent on computers in Turkey than elsewhere.

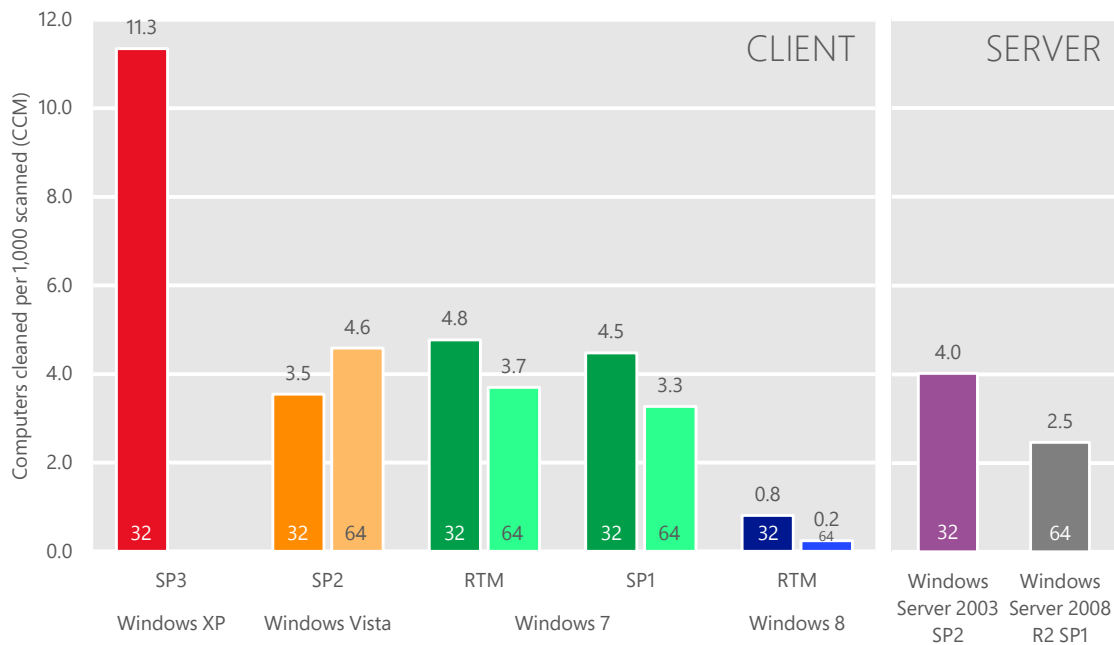
<sup>12</sup> See [www.microsoft.com/download/details.aspx?id=28968](http://www.microsoft.com/download/details.aspx?id=28968) for a case study of one Finnish telecom provider's use of Microsoft security data to remove botnet devices from its network.

- Steady reductions in detections of Sality, the worm families [Win32/Vobfus](#) and [Win32/Dorkbot](#), and the password stealer [Win32/Zbot](#) helped Haiti improve its infection rate from 16.4 at the beginning of the year to 9.1 in the 4th quarter.
- Chile, which began the year with a CCM of 13.7, improved each quarter to close out the year with a CCM of 5.6. A drastic decline in Zbot detections throughout the year was responsible for much of the improvement.

## Operating system infection rates

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 31 shows the infection rate for each currently supported Windows operating system/service pack combination that accounted for at least 0.1 percent of total MSRT executions in 4Q12.

Figure 31. Infection rate (CCM) by operating system and service pack in 4Q12



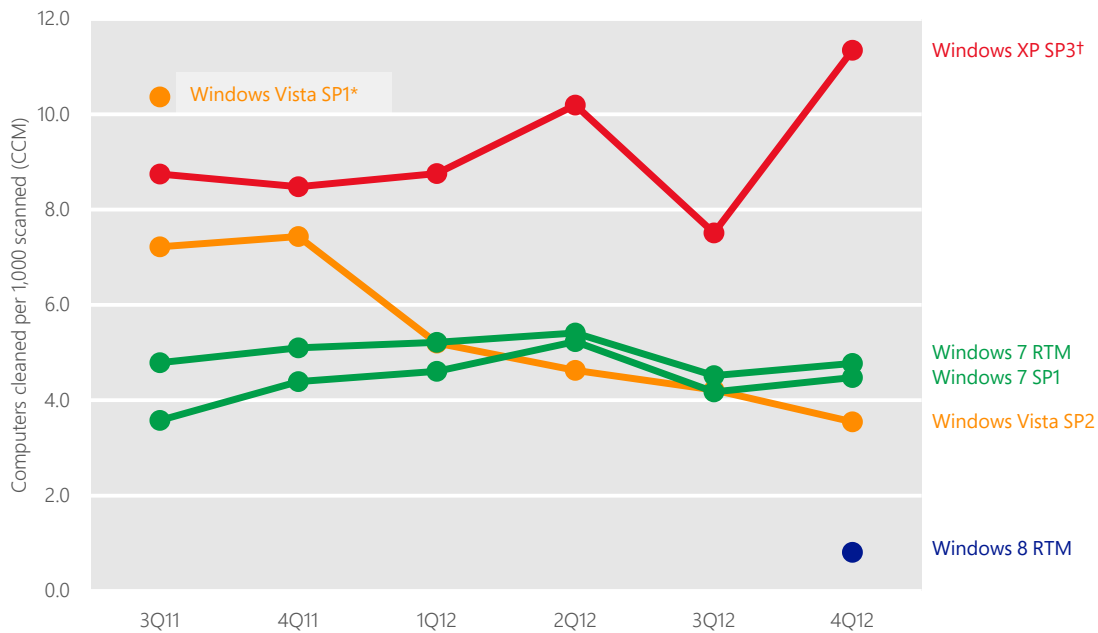
"32" = 32-bit edition; "64" = 64-bit edition. SP = Service Pack. RTM = release to manufacturing. Operating systems with at least 0.1 percent of total MSRT executions in 4Q12 shown.

- 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).

- As in previous periods, 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.
- RTM and Windows Server 2008 R2 SP1 have the lowest infection rates on the chart, and the infection rate for Windows XP SP3 is the highest by a significant margin. (The volume of MSRT executions on Windows Server 2012 wasn't sufficient for reliable measurement by the end of 4Q12.)
- Windows 8, which was released to the general public in 4Q12, had the lowest infection rate of any platform by a significant margin, with a CCM of 0.8 for the 32-bit edition and 0.2 for the 64-bit edition. Windows 8 includes a new version of Windows Defender that provides real-time antimalware protection out of the box, which is probably a significant contributor to this difference. (See "Running unprotected: Measuring the benefits of real-time security software" on page 1 for an analysis of the infection rate differences between computers with and without up-to-date real-time antimalware protection.)

Figure 32. Infection rate (CCM) trends for supported 32-bit client versions of Windows, 3Q11–4Q12



\* Support ended July 12, 2011.

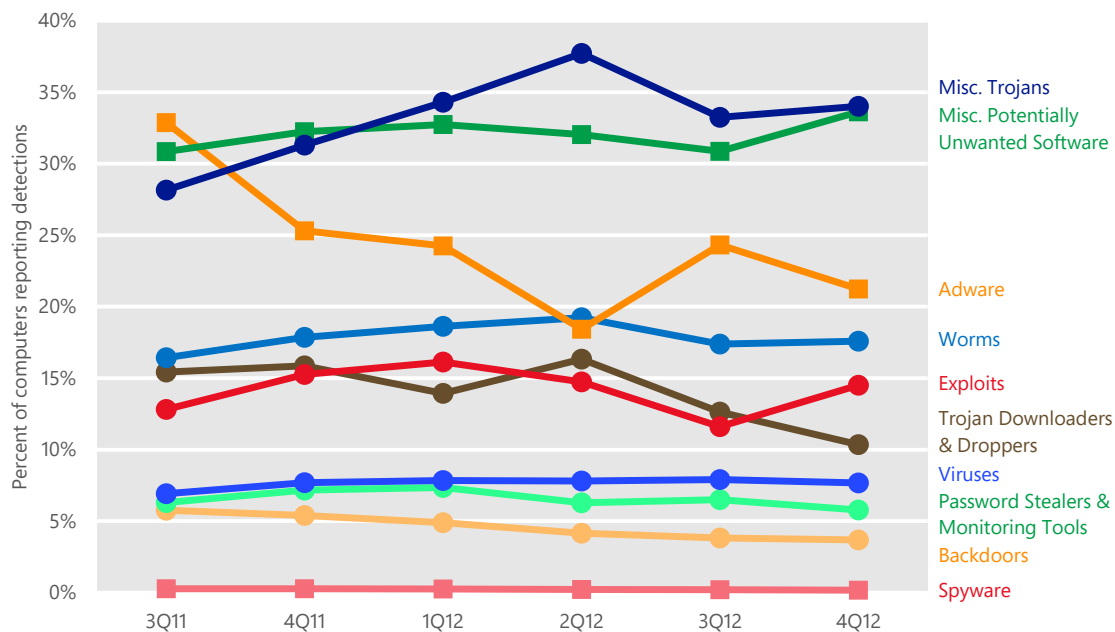
†Extended support for Windows XP ends April 8, 2014.

- The infection rate for Windows XP SP3 increased significantly in 4Q12 primarily because of increased detection of the rogue security software family [Win32/Onescan](#) in Korea, where Windows XP retains a larger market share than in most other large countries and regions. (See “Rogue security software” on page 52 for more information about Onescan in Korea.)
- The infection rate for Windows Vista has declined moderately over the past several periods, which may be because attackers have shifted their efforts to Windows 7 as the newer operating system release has gained market share.

## 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 10 categories based on similarities in function and purpose.

Figure 33. Detections by threat category, 3Q11–4Q12, by percentage of all computers reporting detections



Round markers indicate malware categories; square markers indicate potentially unwanted software categories.

- 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 detected threat category in 4Q12, led by [Win32/Sirefef](#), the rogue security software family [Win32/Onescan](#), and the generic detection [JS/IframeRef](#).
- Detections of Miscellaneous Potentially Unwanted Software increased in 4Q12 to nearly equal Miscellaneous Trojans, which was caused primarily by increased reports of product key generators detected as [Win32/Keygen](#). The generic detections [Win32/Obfuscator](#) and [INF/Autorun](#) were also prevalent threats in this category.

Autorun is a generic detection for worms that spread between mounted volumes using the AutoRun feature of Windows. Recent changes to the feature in Windows XP and Windows Vista 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.

- Adware returned to third place in 2H12 because of increased detections of [Win32/Hotbar](#) and a new family, [Win32/DealPly](#), in the 4th quarter.
- Detections in the Exploits category increased in 4Q12 after two quarters of small declines because of increased detections of [Blacole](#), [Win32/Pdfjsc](#), and [Win32/CplLnk](#).

### 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 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 globe.

Figure 34 shows the relative prevalence of different categories of malware and potentially unwanted software in several locations around the world in 4Q12.



Figure 34. Threat category prevalence worldwide and in the 10 locations with the most detections in 4Q12

Category	Worldwide	US	Brazil	Russia	Korea	France	Turkey	China	Germany	India	UK
Adware	21.2%	20.8%	40.8%	9.3%	32.6%	41.1%	11.1%	3.8%	18.8%	14.6%	23.9%
Misc. Potentially Unwanted Software	33.6%	20.0%	38.0%	50.0%	9.7%	34.1%	38.7%	49.0%	29.2%	38.6%	30.5%
Misc. Trojans	34.0%	43.9%	17.1%	37.1%	75.6%	20.0%	34.7%	32.1%	27.2%	34.7%	29.8%
Worms	17.6%	5.6%	15.7%	17.5%	3.1%	9.4%	34.7%	12.5%	9.2%	39.9%	6.8%
Trojan Downloaders & Droppers	10.4%	9.6%	16.7%	12.6%	9.1%	9.2%	10.0%	14.5%	7.1%	5.5%	9.5%
Exploits	14.5%	23.0%	4.8%	14.2%	4.2%	11.7%	9.0%	6.4%	27.0%	14.6%	23.8%
Viruses	7.7%	2.0%	6.6%	5.5%	1.4%	1.8%	16.5%	15.2%	2.8%	23.8%	3.1%
Password Stealers & Monitoring Tools	5.8%	5.2%	10.5%	5.0%	2.7%	3.5%	4.8%	3.5%	8.8%	7.6%	6.2%
Backdoors	3.7%	2.7%	2.5%	2.9%	1.4%	2.4%	5.0%	6.3%	2.5%	6.4%	3.0%
Spyware	0.2%	0.3%	0.0%	0.2%	0.0%	0.1%	0.0%	1.2%	0.2%	0.1%	0.1%

Totals for each location may exceed 100% because some computers reported threats from more than one category.

- Within each row of Figure 34, 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 26 on page 37, the locations in the table are ordered by number of computers reporting detections in 2H12.
- Exploits were unusually common in the United States, the United Kingdom, and Germany, with [Blacole](#) and [Win32/Pdfjsc](#) among the most common exploit families detected. Detections of Pdfjsc increased 141 percent in Germany between 3Q12 and 4Q12, and detections of Blacole went up 9.4 percent in the UK.
- Adware was unusually common in Brazil and France, with adware detected on more than 40 percent of computers reporting detections in each location. The most commonly detected family in France in 3Q12 was [Win32/EoRezo](#), an adware program that delivers French-language advertisements. The Miscellaneous Potentially Unwanted Software category

was also unusually prevalent in Brazil, with [Win32/Keygen](#) the most commonly detected threat in the category in 4Q12.

- Families in the Miscellaneous Trojans category were detected on 75.6 percent of all computers that reported detections in Korea, mostly because of [Win32/Onescan](#). (See “Rogue security software” on page 52 for more information about Onescan in Korea.)
- As in 1H12, the Miscellaneous Potentially Unwanted Software category was especially prevalent in Russia, led by Keygen and [Win32/Pameseg](#). Pameseg is a family of installers that require the user to send a text message to a premium number to successfully install certain programs, some of which are otherwise available for free. Currently, most variants target Russian speakers.
- Keygen was detected on almost half of the computers reporting detections in China, making the Miscellaneous Potentially Unwanted Software category especially prevalent there. Spyware was also unusually prevalent in China, led by [Win32/CnsMin](#). Although Spyware was the least prevalent category in China, it was more than six times as prevalent there as in the world overall.
- Worms were unusually prevalent in Turkey and India, led by [INF/Autorun](#).

See “Appendix C: Worldwide infection rates” on page 89 for more information about malware around the world.

## Threat families

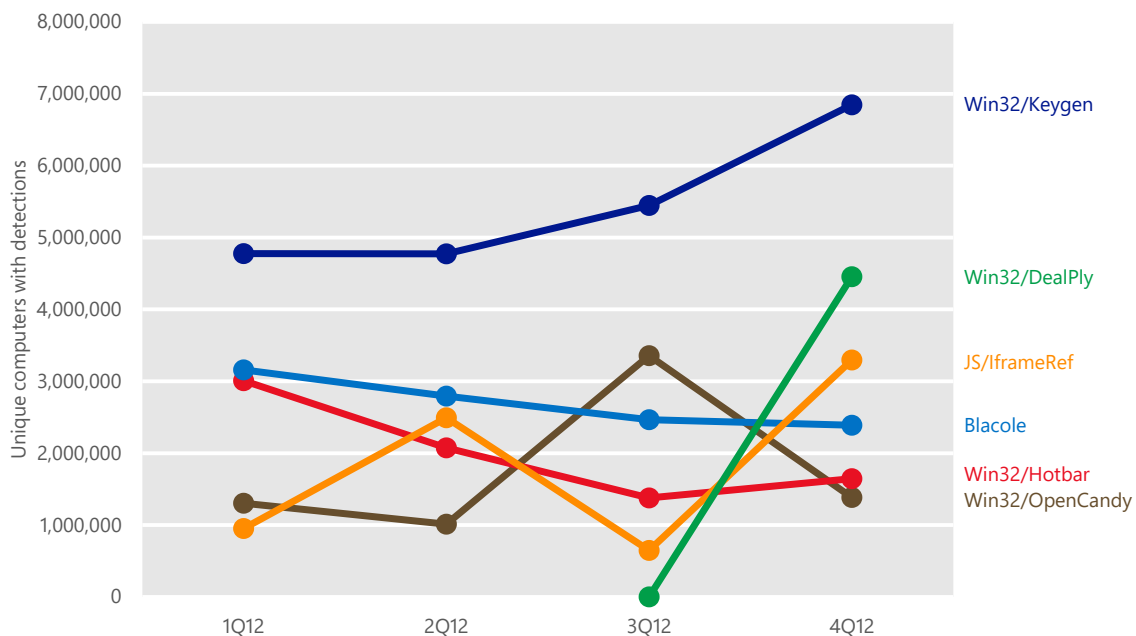
Figure 35 lists the top 10 malware and potentially unwanted software families that were detected on computers by Microsoft antimalware products in the fourth quarter of 2012, with other quarters included for comparison.

Figure 35. Quarterly trends for the top 10 malware and potentially unwanted software families detected by Microsoft antimalware products in 2H12, shaded according to relative prevalence

	Family	Most significant category	1Q12	2Q12	3Q12	4Q12
1	Win32/Keygen	Misc. Potentially Unwanted Software	4,775,464	4,775,243	5,448,253	6,845,681
2	INF/Autorun	Misc. Potentially Unwanted Software	3,316,107	3,510,816	3,293,134	3,604,651
3	Blacole	Exploits	3,157,580	2,794,300	2,464,753	2,387,852
4	Win32/OpenCandy	Adware	1,304,390	1,011,980	3,358,270	1,382,133
5	Win32/DealPly	Adware	—	—	—	4,454,344
6	Win32/Sality	Viruses	2,101,968	2,097,663	1,911,592	2,093,211
7	Win32/Obfuscator	Misc. Potentially Unwanted Software	1,393,148	1,851,304	1,762,317	2,221,140
8	Win32/Pdfjsc	Exploits	1,431,288	1,217,813	1,187,797	2,760,030
9	JS/IframeRef	Misc. Trojans	952,111	2,493,830	646,607	3,296,531
10	Win32/Dorkbot	Worms	1,883,642	2,055,244	1,758,243	2,095,793

For a different perspective on some of the changes that have occurred throughout the year, Figure 36 shows the detection trends for a number of families that increased or decreased significantly over the past four quarters.

Figure 36. Detection trends for a number of notable malware and potentially unwanted software families in 2012



- Detections of [Win32/Keygen](#), the most commonly detected family overall in 2H12, increased each quarter, from 4.8 million computers in 2Q12 to 6.8

million in 4Q12. Keygen is a detection for tools that generate keys for various software products, which may allow users to run the products illegally.

- The adware detection [Win32/DealPly](#), which first appeared in 4Q12, quickly became the second most common detection of the quarter. DealPly is an adware program that displays offers that are related to the user's web browsing habits. It has been observed being bundled with certain third-party software installation programs, including [Win32/Protlerdob](#).
- Detections of the generic family [JS/IframeRef](#) increased fivefold in 4Q12 after falling off significantly between 2Q12 and 3Q12. IFrameRef is a generic detection for specially formed HTML inline frame (IFrame) tags that redirect to remote websites that contain malicious content. The increased IFrameRef detections in 2Q12 and 4Q12 resulted from the discovery of a pair of widely used new variants in April and November 2012. (In January 2013, these variants were reclassified as [Trojan:JS/Seedabutor.A](#) and [Trojan:JS/Seedabutor.B](#), respectively.)

### **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 37 demonstrates how detections of the most prevalent families in 4Q12 ranked differently on different operating system/service pack combinations.

Figure 37. The malware and potentially unwanted software families most commonly detected by Microsoft antimalware solutions in 4Q12, and how they ranked in prevalence on different platforms

Rank 4Q12	Family	Most significant category	Rank (Windows 8 RTM)	Rank (Windows 7 SP1)	Rank (Windows Vista SP2)	Rank (Windows XP SP3)
1	Win32/Keygen	Misc. Potentially Unwanted Software	1	1	10	5
2	Win32/DealPly	Adware	15	2	1	9
3	INF/Autorun	Misc. Potentially Unwanted Software	3	3	14	3
4	JS/IframeRef	Misc. Trojans	2	7	8	2
5	Win32/Pdfjsc	Exploits	20	4	3	7
6	Blacole	Exploits	17	5	6	6
7	Win32/Onescan	Misc. Trojans	84	16	24	1
8	Win32/Obfuscator	Misc. Potentially Unwanted Software	5	6	12	12
9	Win32/Dorkbot	Worms	13	8	23	10
10	Win32/Sality	Viruses	11	12	41	4
14	Win32/Zwangi	Misc. Potentially Unwanted Software	54	17	2	35

- Windows 7 is the most widely used consumer operating system worldwide, and the most prevalent families on Windows 7 SP1 tended to be the same families that were prevalent overall.
- The rogue security software family [Win32/Onescan](#) was the most commonly detected family on Windows XP SP3 in 4Q12 but ranked much lower on other platforms. Detections of Onescan were highly concentrated in Korea, where use of Windows XP remains relatively higher than in the rest of the world.
- Microsoft real-time antimalware products detect and block threats that attempt to infect computers even if those attempts would not have succeeded otherwise. The generic family [INF/Autorun](#), which propagates by using a technique that is ineffective on Windows 7 and Windows 8, was

nevertheless the 3rd most commonly detected threat family on those platforms in 4Q12.<sup>13</sup>

## 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](http://www.microsoft.com/security/resources/videos.aspx) for an informative series of videos designed to educate general audiences about rogue security software.)

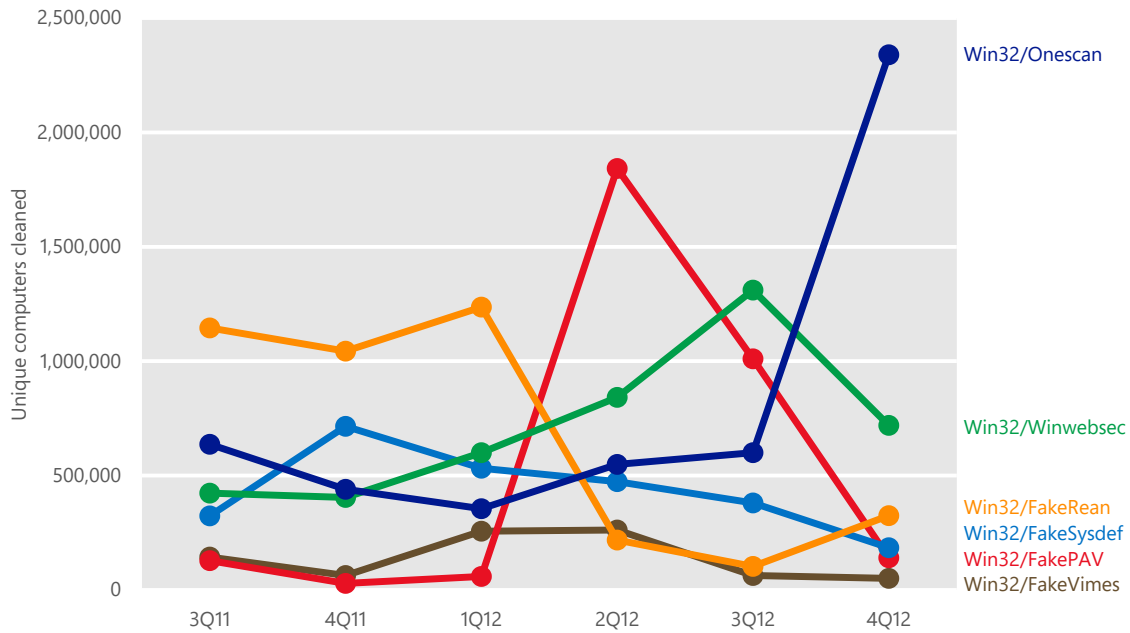
Figure 38. False branding used by a number of commonly detected rogue security software programs



Figure 39 shows detection trends for the most common rogue security software families detected in 2H12.

<sup>13</sup> 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](http://support.microsoft.com/kb/971029) for more information.

Figure 39. Trends for the most common rogue security software families detected in 2H12, by quarter



- Detections of [Win32/Onescan](#) nearly quadrupled in 4Q12 after Microsoft added detection signatures for the family to the MSRT in October 2012. Onescan is a Korean-language rogue security software distributed under a variety of names, brands, and logos. The installer selects the branding randomly from a defined set, apparently without regard to the operating system version.

Figure 40. A variant of Win32/Onescan, a Korean-language rogue security program



As shown in Figure 41, the overwhelming majority of Onescan detections occurred in Korea, where Onescan was the most commonly detected family by a considerable margin. In 4Q12, when detection signatures for the family were added to the MSRT, more than 98 percent of Onescan detections were in Korea.

Figure 41. The 5 locations with the most Win32/Onescan detections in 3Q12 (left) and 4Q12 (right)

Country or region	Computers (3Q12)	Country or region	Computers (4Q12)
Korea	573,763	Korea	2,299,917
China	9,180	United States	11,071
United States	6,036	China	5,665
Canada	1,523	Japan	3,978
Japan	1,402	Australia	2,811

- [Win32/Winwebsec](#) was the second most commonly detected rogue security software family in the second half of the year despite detections decreasing by nearly half from 3Q12 to 4Q12. Winwebsec has been distributed under a variety of names, with the user interface and other details varying to reflect



each variant's individual branding; currently prevalent names include AVASoft Professional Antivirus, Smart Fortress 2012, 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. The attackers behind Winwebsec are also believed to be responsible for [MacOS\\_X/FakeMacdef](#), the "Mac Defender" rogue security software program for Apple Mac OS X that first appeared in May 2011.

- Detections of [Win32/FakePAV](#), which peaked at 1.8 million infected computers in 2Q12, declined to fewer than 200,000 computers by 4Q12. FakePAV has also been distributed under many names, including Windows Threats Destroyer, Windows Firewall Constructor, Windows Attacks Preventor, and Windows Basic Antivirus. FakePAV frequently spreads by masquerading as Microsoft Security Essentials on malicious and compromised webpages; it presents a graphic that resembles a genuine Microsoft Security Essentials window and claims to have discovered several infections on the target computer. Recent variants have included large amounts of irrelevant text, such as excerpts from William Shakespeare's *Romeo and Juliet*, in the installation package in an apparent effort to obfuscate the files and avoid detection by antimalware software.

## 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 42 and Figure 43 list the top 10 families detected on domain-joined and non-domain computers, respectively, in 2H12.

Figure 42. Quarterly trends for the top 10 families detected on domain-joined computers in 2H12, by percentage of domain-joined computers reporting detections

	Family	Category	1Q12	2Q12	3Q12	4Q12
1	JS/IframeRef*	Misc. Trojans	2.3%	11.3%	1.7%	13.6%
2	Win32/Conficker	Worms	12.7%	10.8%	9.7%	9.8%
3	Win32/Keygen	Misc. Potentially Unwanted Software	5.5%	5.3%	6.2%	6.9%
4	INF/Autorun	Misc. Potentially Unwanted Software	7.5%	7.0%	6.2%	6.6%
5	Blacole*	Exploits	7.0%	5.4%	5.0%	5.1%
6	JS/BlacoleRef*	Misc. Trojans	3.3%	4.1%	5.8%	4.2%
7	Win32/Zbot*	Password Stealers & Monitoring Tools	3.5%	3.4%	3.4%	3.7%
8	Win32/Sirefef*	Misc. Trojans	2.6%	3.5%	4.3%	3.5%
9	Win32/Dorkbot*	Worms	3.4%	3.2%	2.6%	3.1%
10	Win32/Pdfjsc*	Exploits	0.5%	4.0%	0.6%	0.5%

\* In the second half of 2012, 7 out of the top 10 threats affecting enterprises were delivered through websites.

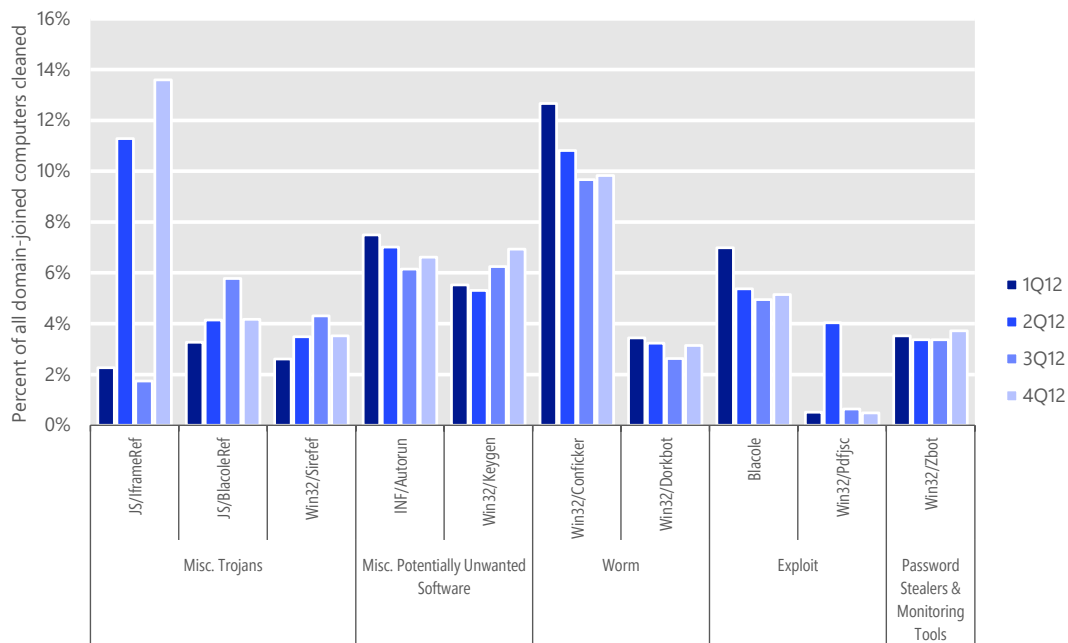
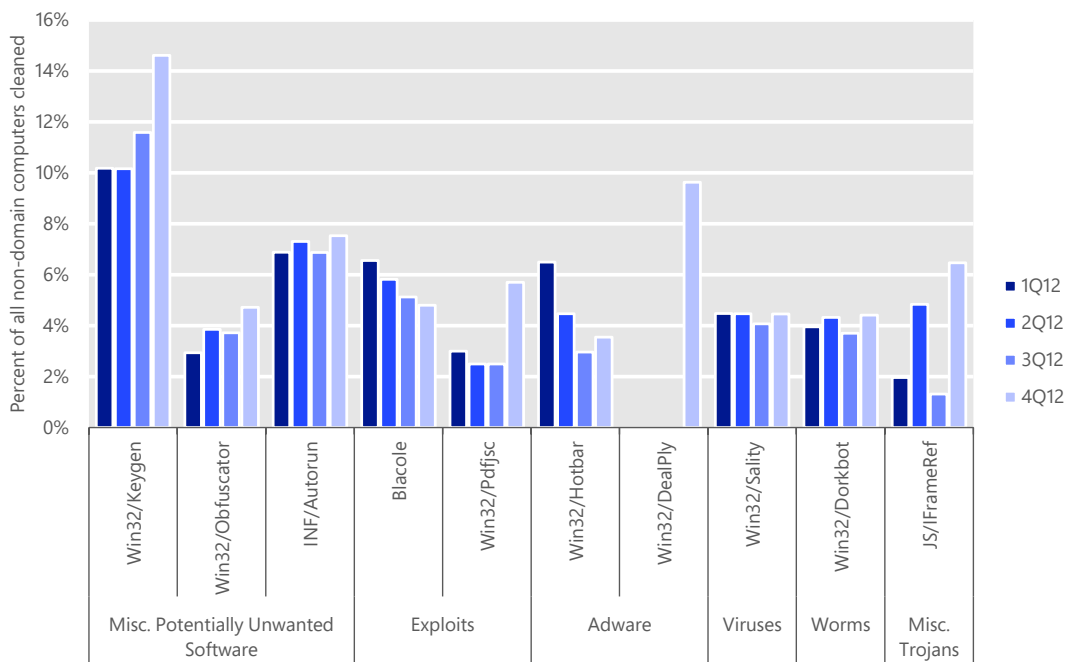


Figure 43. Quarterly trends for the top 10 families detected on non-domain computers in 2H12, by percentage of non-domain computers reporting detections

	Family	Category	1Q12	2Q12	3Q12	4Q12
1	Win32/Keygen	Misc. Potentially Unwanted Software	10.2%	10.2%	11.6%	14.6%
2	Win32/DealPly	Adware	—	—	—	9.6%
3	INF/Autorun	Misc. Potentially Unwanted Software	6.9%	7.3%	6.9%	7.5%
4	JS/IframeRef	Misc. Trojans	2.0%	4.8%	1.3%	6.5%
5	Win32/Pdfjsc	Exploits	3.0%	2.5%	2.5%	5.7%
6	Blacole	Exploits	6.6%	5.8%	5.1%	4.8%
7	Win32/Obfuscator	Misc. Potentially Unwanted Software	2.9%	3.9%	3.7%	4.7%
8	Win32/Sality	Viruses	4.5%	4.5%	4.1%	4.5%
9	Win32/Dorkbot	Worms	4.0%	4.3%	3.7%	4.4%
10	Win32/Hotbar	Adware	6.5%	4.5%	3.0%	3.6%



- Six families are common to both lists, notably the generic families [Win32/Keygen](#) and [INF/Autorun](#) and the exploit family [Blacole](#). Keygen, the most commonly detected family on non-domain computers in 2H12, was detected on about twice as many non-domain computers as domain-joined computers, although it was prevalent enough on the latter to rank third on the domain-joined list in both quarters.

- Detections in the Worms category remained high for domain-joined computers, led by [Win32/Conficker](#), which declined slightly over the course of the year but remained the second most commonly detected family on domain-joined computers. See “How Conficker continues to propagate” in [Microsoft Security Intelligence Report, Volume 12 \(July–December 2011\)](#) for more information.
- Detections of the exploit family [Win32/Pdfjsc](#), which targets a vulnerability in some versions of Adobe Acrobat and Adobe Reader, increased significantly on domain-joined computers in 4Q12. The use of the PDF format to store and transfer documents is common in many enterprise environments, although in this case the prevalence of the exploit may have more to do with its use by the Blacole exploit kit and others. (See page 27 for more information about Blacole.)
- Detections of adware are typically much more common on non-domain computers than on domain-joined computers. The adware program [Win32/DealPly](#) was the second most commonly detected threat family on non-domain computers in 4Q, with another adware program, [Win32/Hotbar](#), ranking 10th. By contrast, none of the top 10 families detected on domain-joined computers were adware families.

## 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.

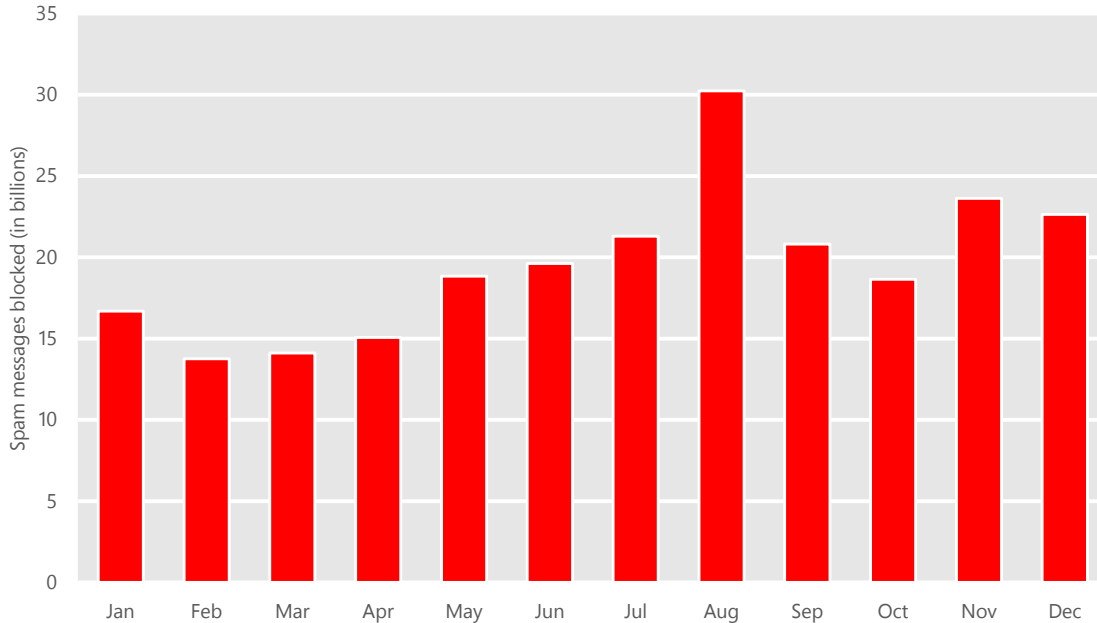
# Email threats

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

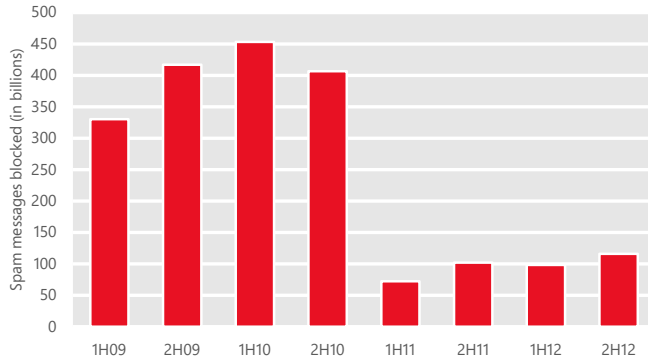
The information in this section of the *Microsoft Security Intelligence Report* is compiled from telemetry data provided by Exchange Online Protection, which provides spam, phishing, and malware filtering services for thousands of Microsoft enterprise customers that process tens of billions of messages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

Figure 44. Messages blocked by Exchange Online Protection each month in 2012



- Blocked mail volumes in 2H12 were up slightly from 1H12, but remain well below levels seen prior to the end of 2010, as shown in Figure 45. The dramatic decline in spam observed over the past two years has occurred in the wake of successful takedowns of a number of large spam-sending

Figure 45. Messages blocked by Exchange Online Protection each half-year period, 1H09–2H12



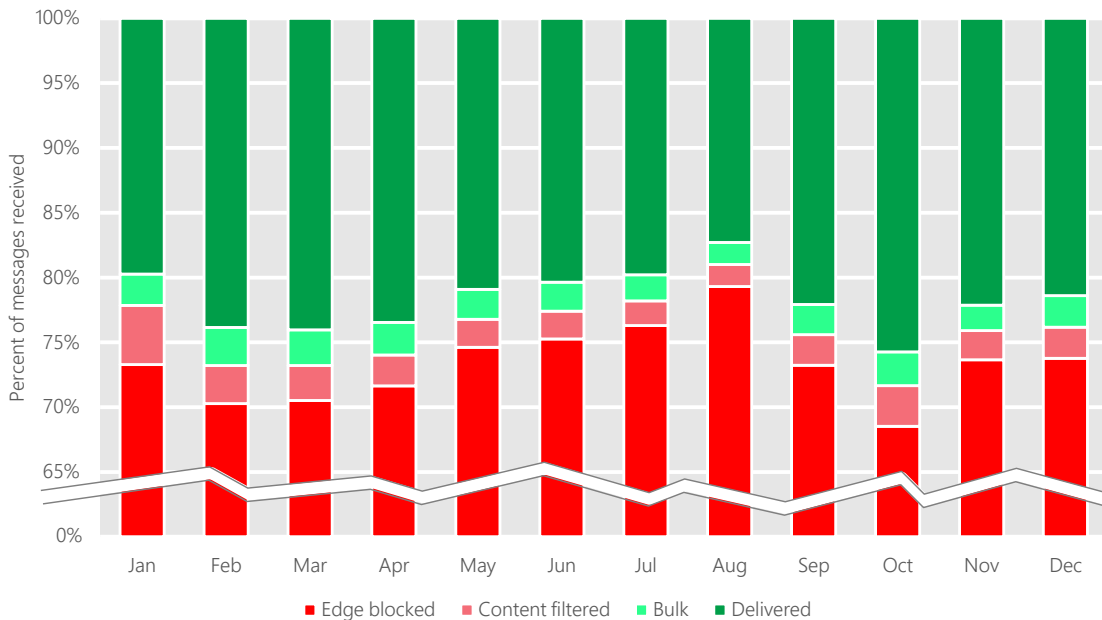
botnets, notably Cutwail (August 2010) and Rustock (March 2011).<sup>14</sup>

In 2H12, about 1 in 4 email messages were delivered to recipients' inboxes without being blocked or filtered, compared to just 1 in 33 messages in 2010.

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.

Figure 46. Percentage of incoming messages blocked, categorized as bulk email, and delivered, January–December 2012



- Between 68.5 and 79.3 percent of incoming messages were blocked at the network edge each month in 2H12, which means that only 20.7 to 31.5

<sup>14</sup> 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.

percent of incoming messages had to be subjected to the more resource-intensive content filtering process. Between 8 and 10 percent of the remaining messages (1.7 to 3.1 percent of all incoming messages) were filtered as spam each month.

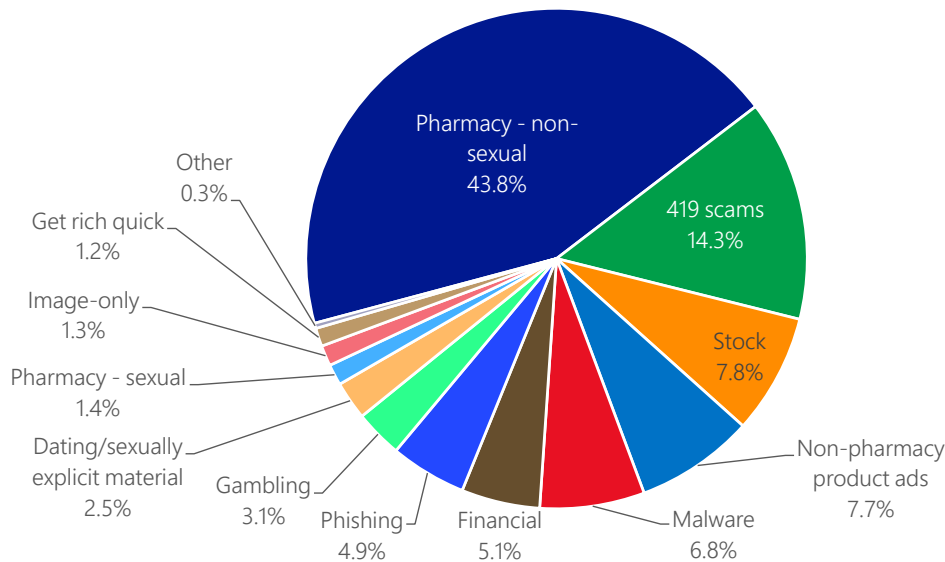
- Exchange Online Protection identifies bulk email messages that some users consider unwanted but that aren't categorized as spam by edge blocks or content filters. These messages typically include email newsletters, advertisements, and marketing messages that users claim they never asked for, or don't remember subscribing to. Exchange Online Protection flags these messages as bulk in an incoming header so customers and individual users can use rules in Microsoft Outlook or Exchange to filter, move, or deliver them as desired.

Bulk email volumes did not vary significantly from month to month in 2H12. Between 8 and 11 percent of all delivered messages were categorized as bulk each month.

## Spam types

The Exchange Online Protection content filters recognize several different common types of spam messages. Figure 47 shows the relative prevalence of the spam types that were detected in 2H12.

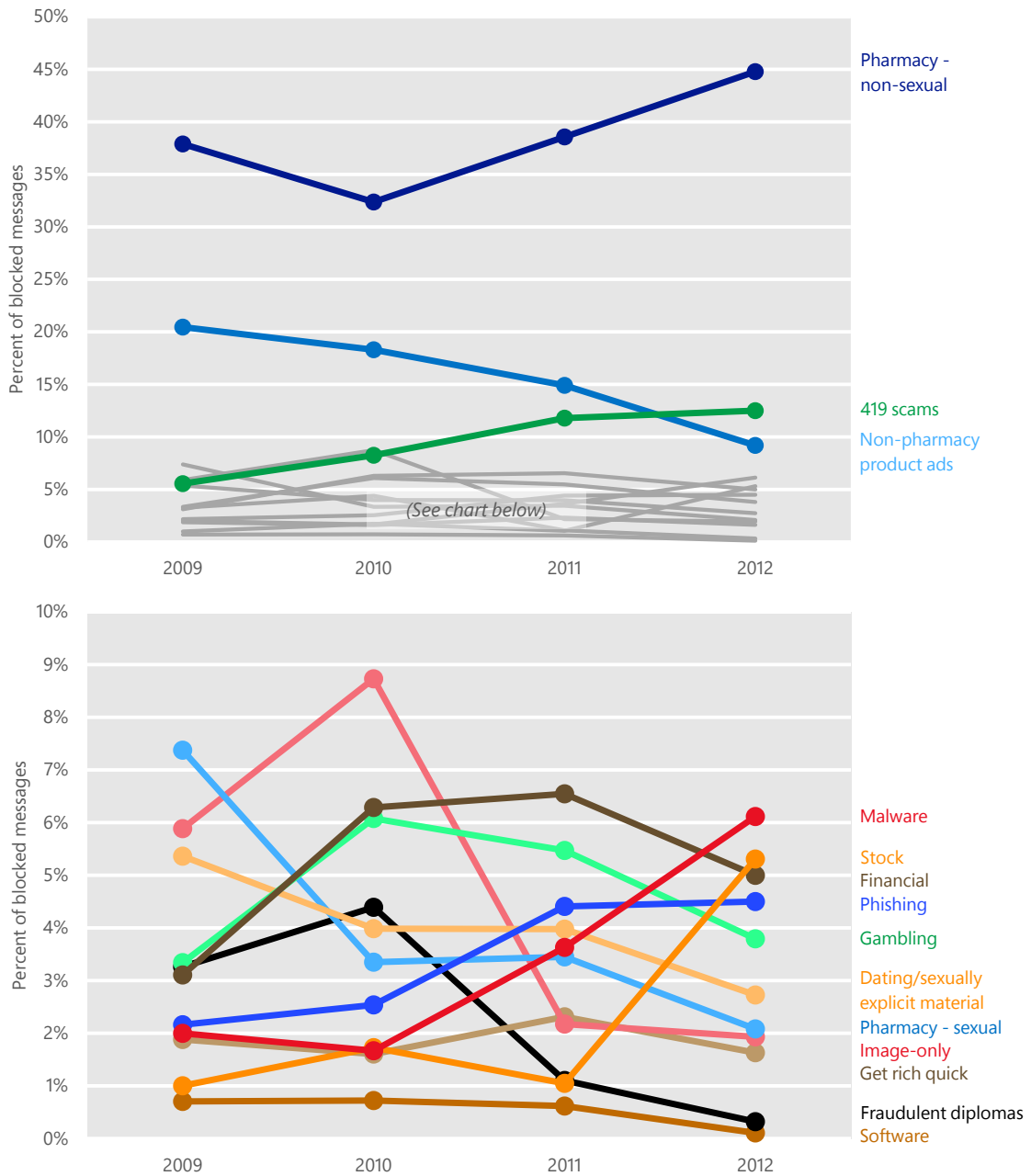
Figure 47. Inbound messages blocked by Exchange Online Protection filters in 2H12, by category



- Advertisements for non-sexual pharmaceutical products accounted for 43.8 percent of the messages blocked by Exchange Online Protection content filters in 2H12, a slight decrease from 46.7 percent in 1H12.
- Spam messages associated with advance-fee fraud (so-called 419 scams) accounted for 14.3 percent of messages blocked, an increase from 9.1 percent in 1H12. 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, 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 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.
- Stock-related spam, which accounted for less than 1 percent of the total in 1H12, rose to 7.8 percent in 2H12 because of a large increase beginning in September. Such messages are typically used in so-called pump-and-dump schemes designed to temporarily increase the share price of a low-priced stock issue in which the spammer owns shares.



Figure 48. Inbound messages blocked by Exchange Online Protection content filters, 2009–2012, by category



- Advertisements for non-sexual pharmaceutical products have accounted for the largest share of spam for the past several years, increasing from about one-third of all spam in 2010 to almost one-half in 2012.
- Other categories that have been trending up include 419 scams, which have more than doubled as a percentage of the whole since 2009; spam that

contains malicious attachments; and phishing messages. (See “Malicious websites” beginning on page 65 for more information about phishing.)

- Spam messages that included images and no text, which spammers sometimes send in an effort to evade detection by antispam software, have decreased significantly since 2009. Other categories that have been trending down include non-pharmacy product ads, sexually related pharmaceutical ads, and ads for sexually explicit material or dating services.

## Guidance: Defending against threats in email

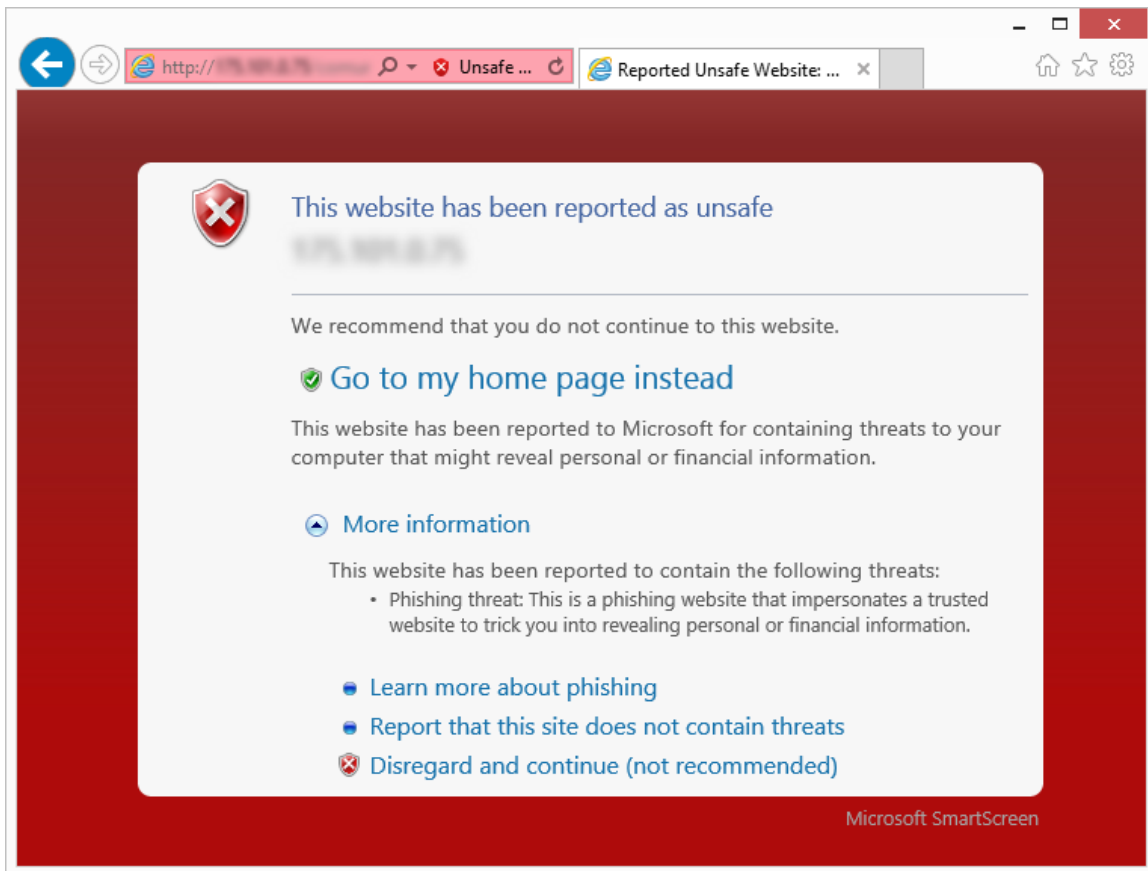
In addition to using a filtering service such as Exchange Online Protection, organizations can take a number of steps to reduce the risks and inconvenience of unwanted email. Such steps include implementing email authentication techniques and observing best practices for sending and receiving email.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

## Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear to be completely legitimate and often 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 an effort by attackers to take advantage of the trust users have invested in them. 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 10) 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 87 for more information about the products and services that provided data for this report.)

Figure 49. 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 50.

Figure 50. How Microsoft tracks phishing impressions

1. The user views a phishing message, in email or elsewhere, and is tricked into clicking a link that leads to a malicious website.
2. SmartScreen Filter in Internet Explorer checks Microsoft Reputation Services, determines that the website is malicious, and blocks it.
3. Microsoft Reputation Services records the anonymized details of the incident as a phishing impression.

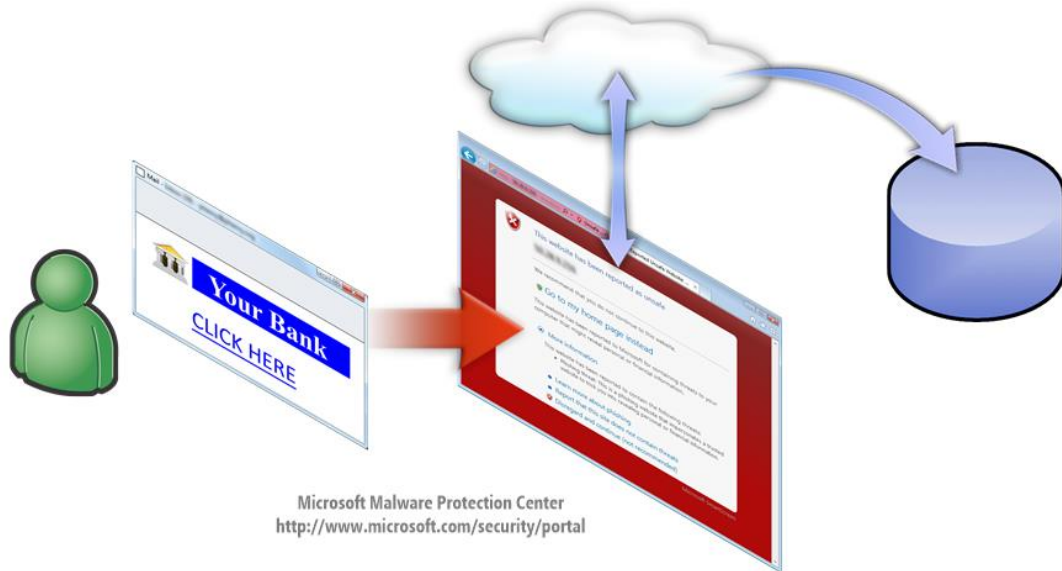
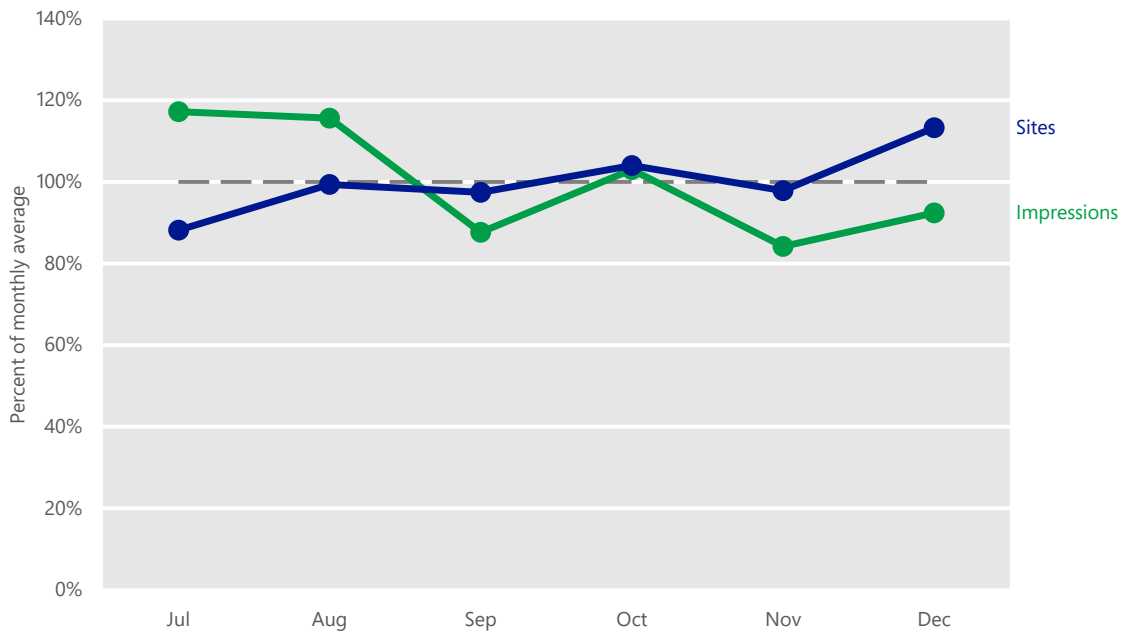


Figure 51 compares the volume of active phishing sites in the Microsoft Reputation Services database each month with the volume of phishing impressions tracked by Internet Explorer.

Figure 51. Phishing sites and impressions tracked each month, July–December 2012, relative to the monthly average for each



- The numbers of active phishing sites and impressions rarely correlate strongly with each other; some types of sites tend to draw many more impressions per site than others, as shown in Figure 52 and Figure 53, and 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. Nevertheless, both sites and impressions were mostly stable throughout 2H12, with both remaining between 80 and 120 percent of their 2H12 average each month.

### Target institutions

Figure 52 and Figure 53 show the percentage of phishing impressions and active phishing sites, respectively, recorded by Microsoft during each month from July to December 2012 for the most frequently targeted types of institutions.

Figure 52. Impressions for each type of phishing site each month, July–December 2012, as reported by SmartScreen Filter

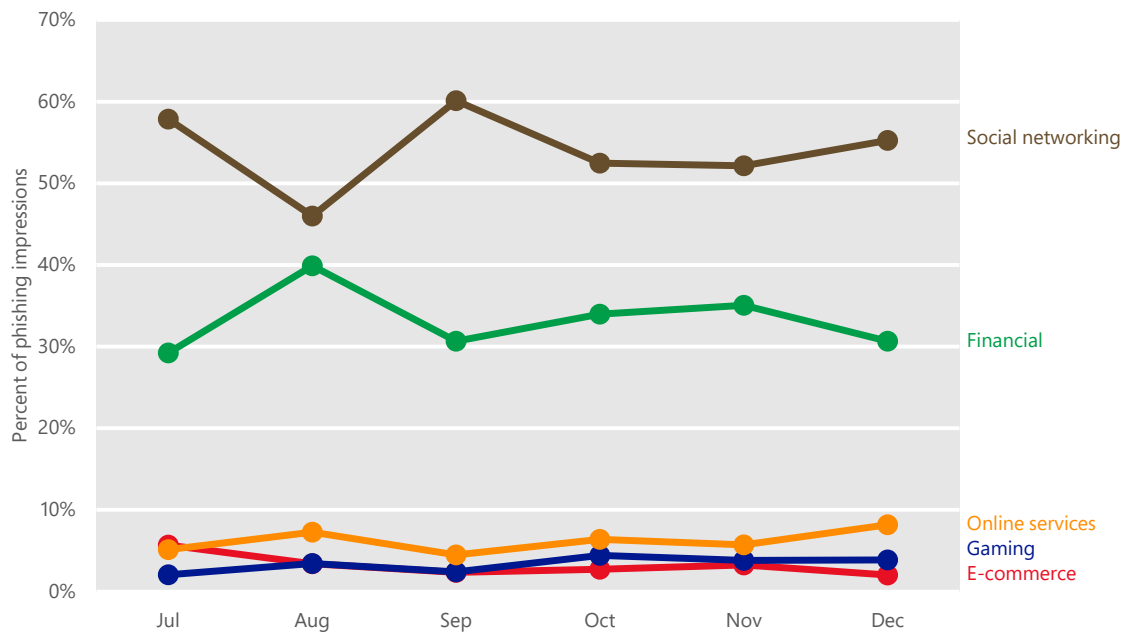
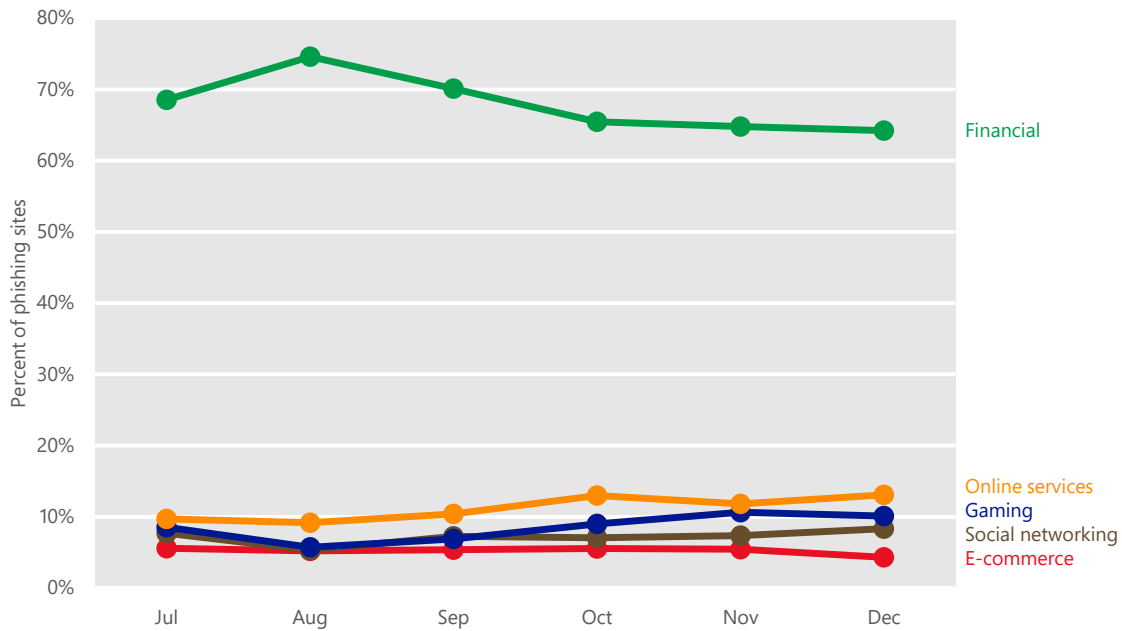


Figure 53. Active phishing sites tracked each month, July–December 2012, by type of target



- Phishing sites that targeted social networks received the largest number of impressions each month in 2H12, and accounted for most of the impressions recorded each month except August. Despite the number of impressions, sites that targeted social networks only accounted for between 5.3 and 8.3 percent of active phishing sites each month. Most social networking activity involves a small number of very popular websites, so phishers can target large numbers of victims without having to maintain many different phishing sites.
- Sites that targeted financial institutions accounted for between 64.2 and 74.6 percent of active phishing sites each month in 2H12. Unlike social networks, financial institutions targeted by phishers can number in the hundreds and customized phishing approaches are required for each one. Still, the potential for direct illicit access to victims’ bank accounts means that financial institutions remain perennially popular phishing targets, and they received the second-largest number of impressions each month during the period.

### 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.

To provide a more accurate perspective on the phishing and malware hosting landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Figure 54. Phishing sites per 1,000 Internet hosts for locations around the world in 3Q12 (top) and 4Q12 (bottom)

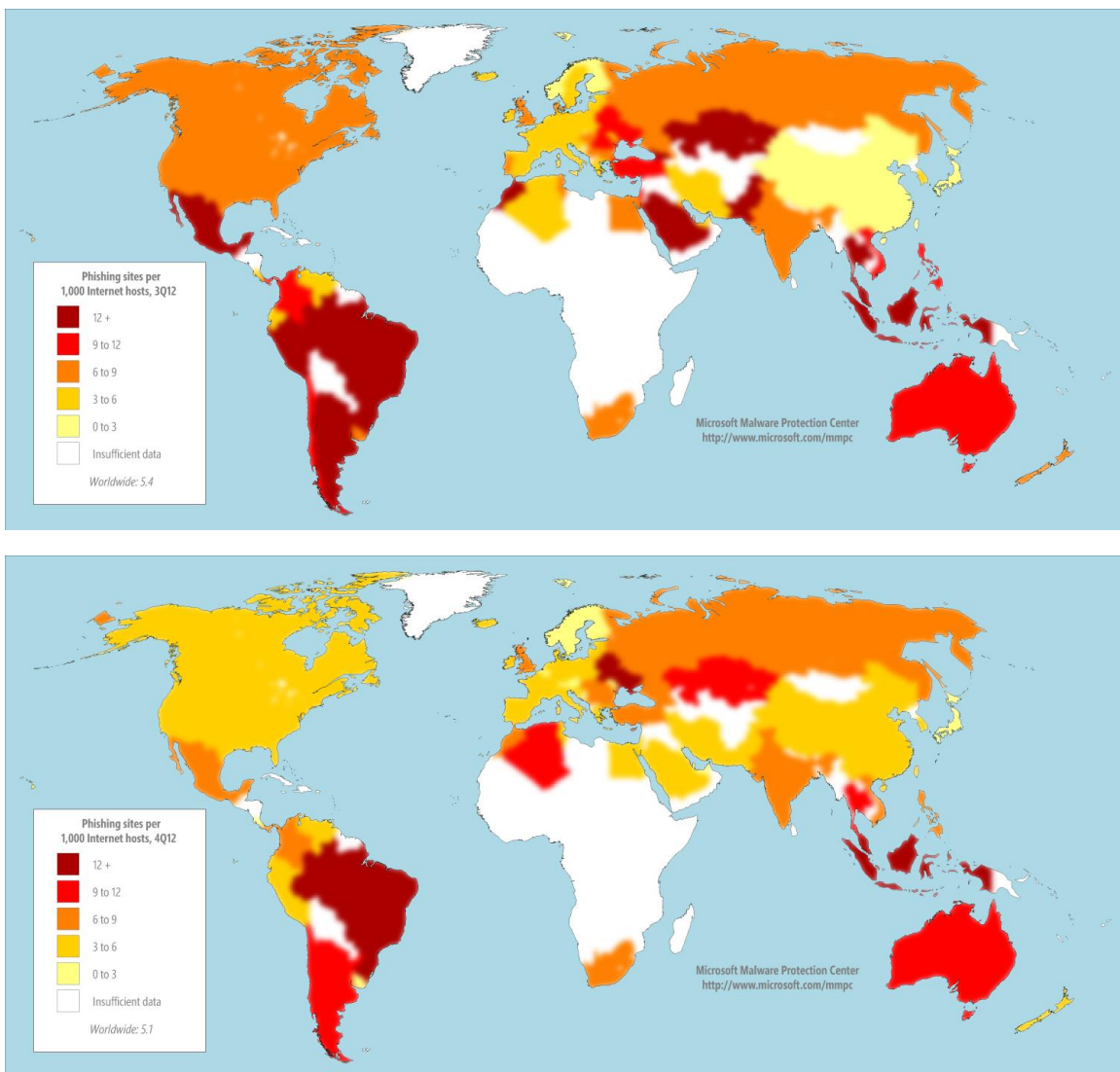
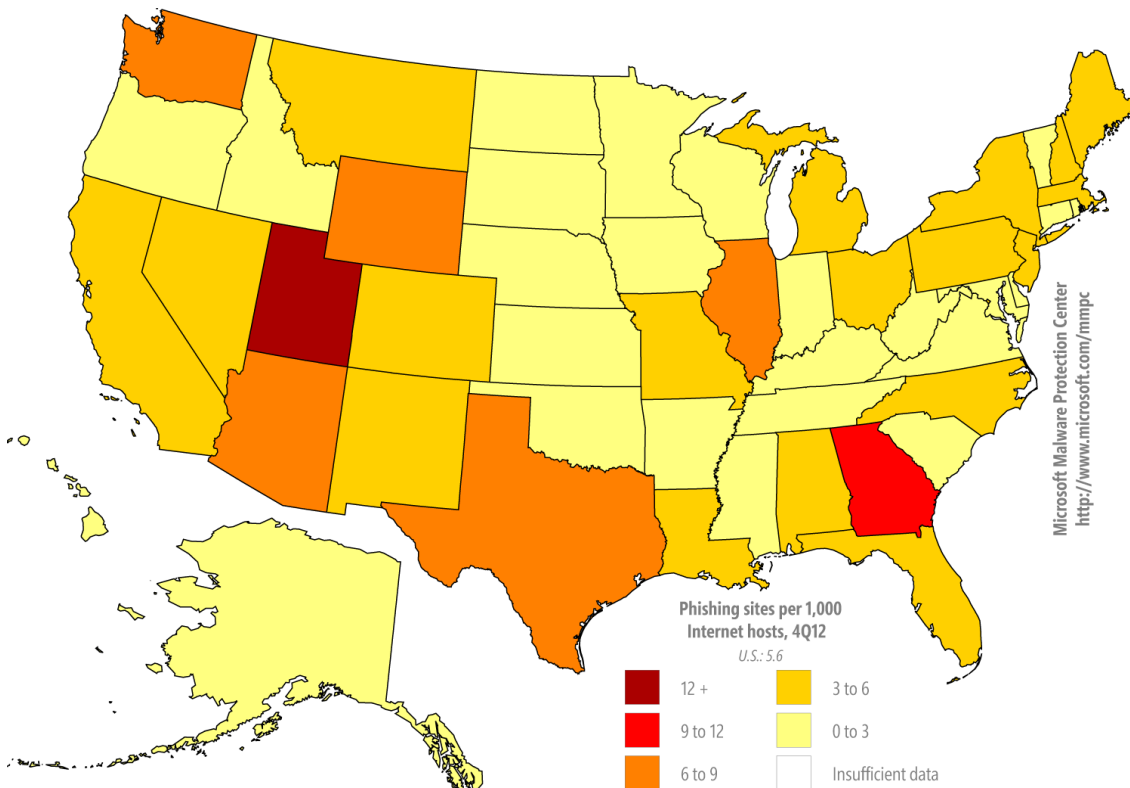
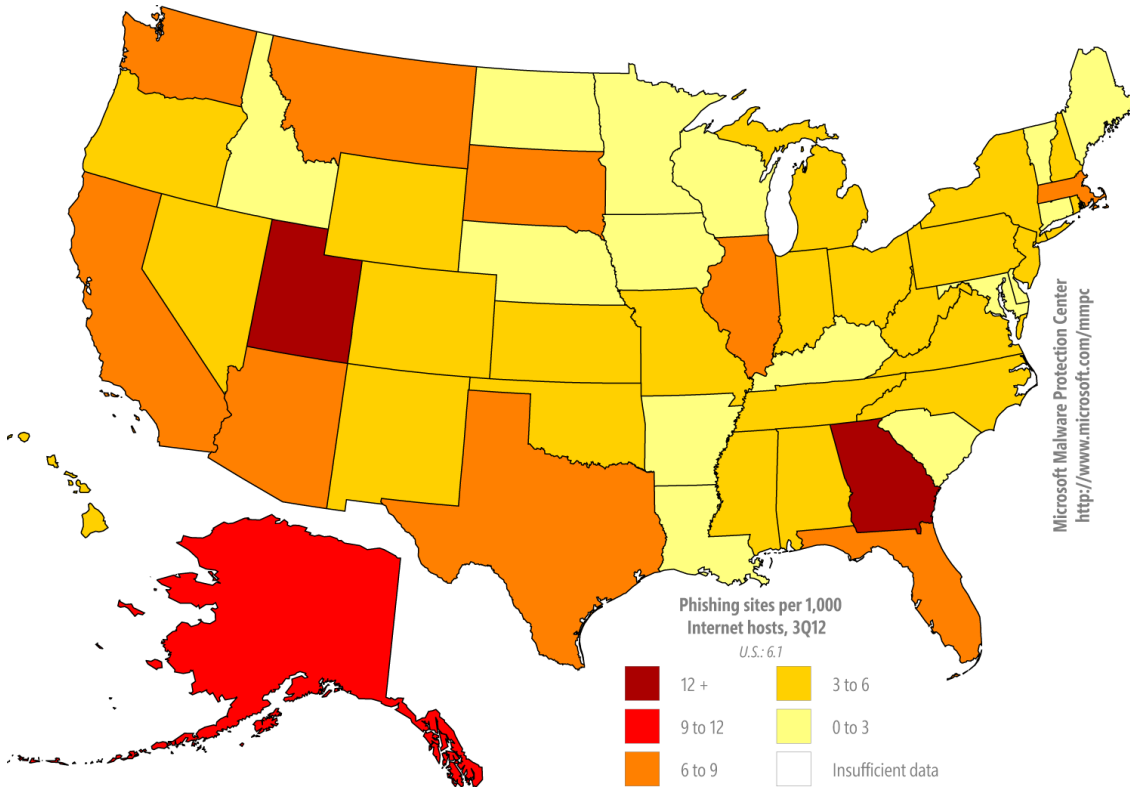




Figure 55. Phishing sites per 1,000 Internet hosts for US states in 3Q12 (top) and 4Q12 (bottom)



- SmartScreen Filter detected 5.4 phishing sites per 1,000 Internet hosts worldwide in 3Q12, and 5.1 per 1,000 in 4Q12.
- Locations with higher than average concentrations of phishing sites include Brazil (12.6 per 1,000 Internet hosts in 4Q12), Australia (9.1), and Russia (8.3). Locations with low concentrations of phishing sites include Japan (1.8), Finland (1.9), and Sweden (2.8).
- In the United States, as a general rule, states with more Internet hosts tend to have higher concentrations of phishing sites as well, although there are plenty of exceptions.
- Those US states with the highest concentrations of phishing sites include Utah (17.4 per 1,000 Internet hosts in 4Q12), Georgia (11.0), and Arizona (8.6). States with low concentrations of phishing sites include Vermont (0.7), Nebraska (0.9), and Rhode Island (1.0).

## 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 URL reputation data and Microsoft antimalware technologies to determine whether sites distribute unsafe content. As with phishing sites, Microsoft keeps track of how many people visit each malware hosting site and uses the information to improve SmartScreen Filter and to better combat malware distribution.

Figure 56. SmartScreen Filter in Internet Explorer displays a warning when a user attempts to download an unsafe file

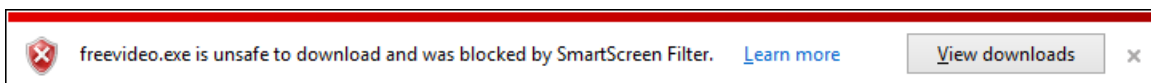
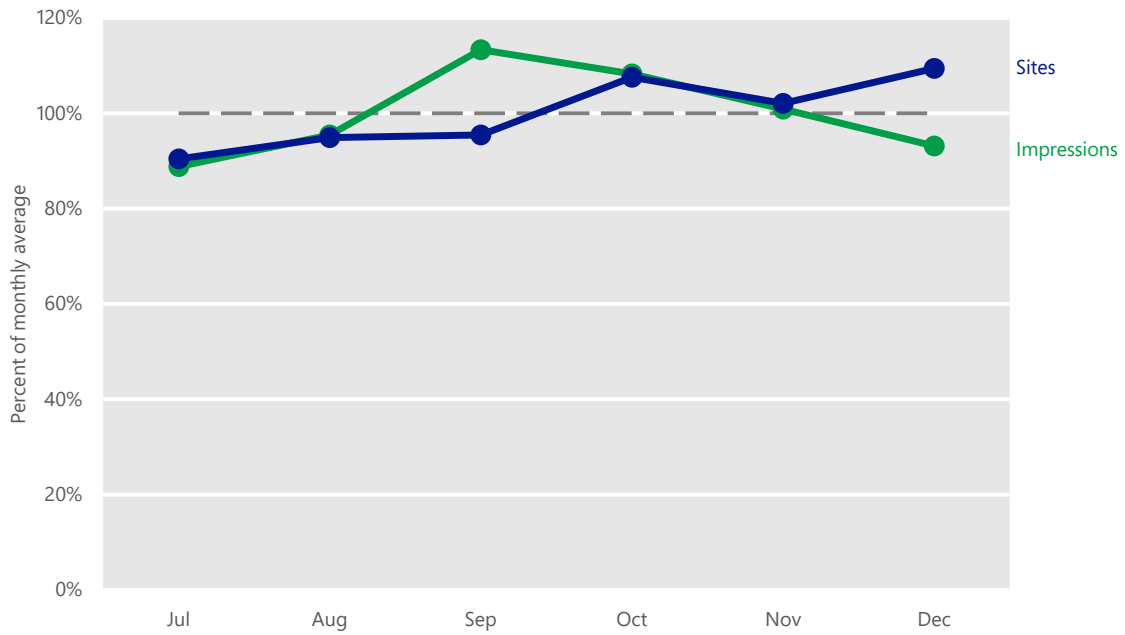


Figure 57 compares the volume of active malware hosting sites in the Microsoft Reputation Services database each month with the volume of malware impressions tracked by Internet Explorer.

Figure 57. Malware hosting sites and impressions tracked each month in 2H12, relative to the monthly average for each



- As with phishing, malware hosting sites and impressions were stable throughout the period, with both remaining between 88 and 113 percent of their 2H12 average each month.

### Malware categories

Figure 58 and Figure 59 show the types of threats hosted at URLs that were blocked by SmartScreen Filter in 2H12.

Figure 58. Categories of malware found at sites blocked by SmartScreen Filter in 2H12, by percent of all malware impressions

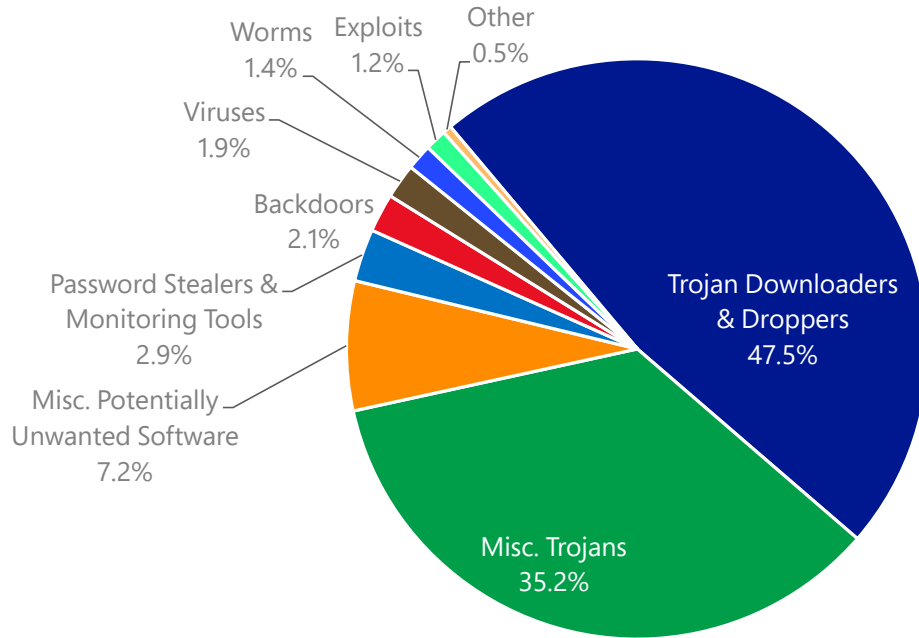


Figure 59. Top families found at sites blocked by SmartScreen Filter in 2H12, by percent of all malware impressions

	Family	Category	Percent of malware impressions
1	Win32/Swisyn	Trojan Downloaders & Droppers	20.8%
2	Win32/Meredrop	Misc. Trojans	10.7%
3	Win32/Microjoin	Trojan Downloaders & Droppers	7.1%
4	Win32/Rimod	Misc. Trojans	5.3%
5	Win32/Dynamer	Misc. Trojans	4.7%
6	Win32/Obfuscator	Misc. Potentially Unwanted Software	4.4%
7	Win32/Dowque	Trojan Downloaders & Droppers	3.9%
8	Win32/Malagent	Misc. Trojans	2.1%
9	Win32/QBundle	Trojan Downloaders & Droppers	2.1%
10	Java/SMSer	Misc. Trojans	1.8%
11	Win32/Kuluoz	Trojan Downloaders & Droppers	1.7%
12	Win32/VB	Worms	1.6%
13	Win32/Xolondox	Trojan Downloaders & Droppers	1.6%
14	Win32/Small	Trojan Downloaders & Droppers	1.5%
15	VBS/Startpage	Misc. Trojans	1.4%

- Most of the families on the list are generic detections for a variety of threats that share certain identifiable characteristics. Eight of the families on the list were also among the top 15 families found at sites blocked by SmartScreen Filter in 1H12, including 4 of the top 5.
- [Win32/Swisyn](#), the family responsible for the most malware impressions in 2H12, is a family of trojans that drops and executes malware on infected computers. These files may be embedded as resource files, and are often bundled with legitimate files in an effort to evade detection. Sites that hosted Swisyn accounted for 20.8 percent of malware impressions in 2H12, a decrease from 24.1 percent in 1H12.
- [Win32/Meredrop](#), in second place, is a generic detection for trojans that drop and execute multiple forms of malware on local computers. 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. Sites that host Meredrop accounted for 10.7 percent of malware impressions in 1H12, an increase from 9.0 percent in 2H11.
- [Win32/Rimod](#), which was not among the top 15 families found at sites blocked by SmartScreen Filter in 1H12, ranked fourth in 2H12. Rimod is a generic detection for certain files that change various security settings in the computer. It is dropped by some variants of Swisyn.
- The generic detection [Win32/Bumat](#), which was third on the 1H11 list, was not among the top 15 families found at sites blocked by SmartScreen Filter in 2H12.

### **Global distribution of malware hosting sites**

As with phishing sites, Figure 60 and Figure 61 show the geographic distribution of malware hosting sites reported to Microsoft in 2H12.

Figure 60. Malware distribution sites per 1,000 Internet hosts for locations around the world in 3Q12 (top) and 4Q12 (bottom)

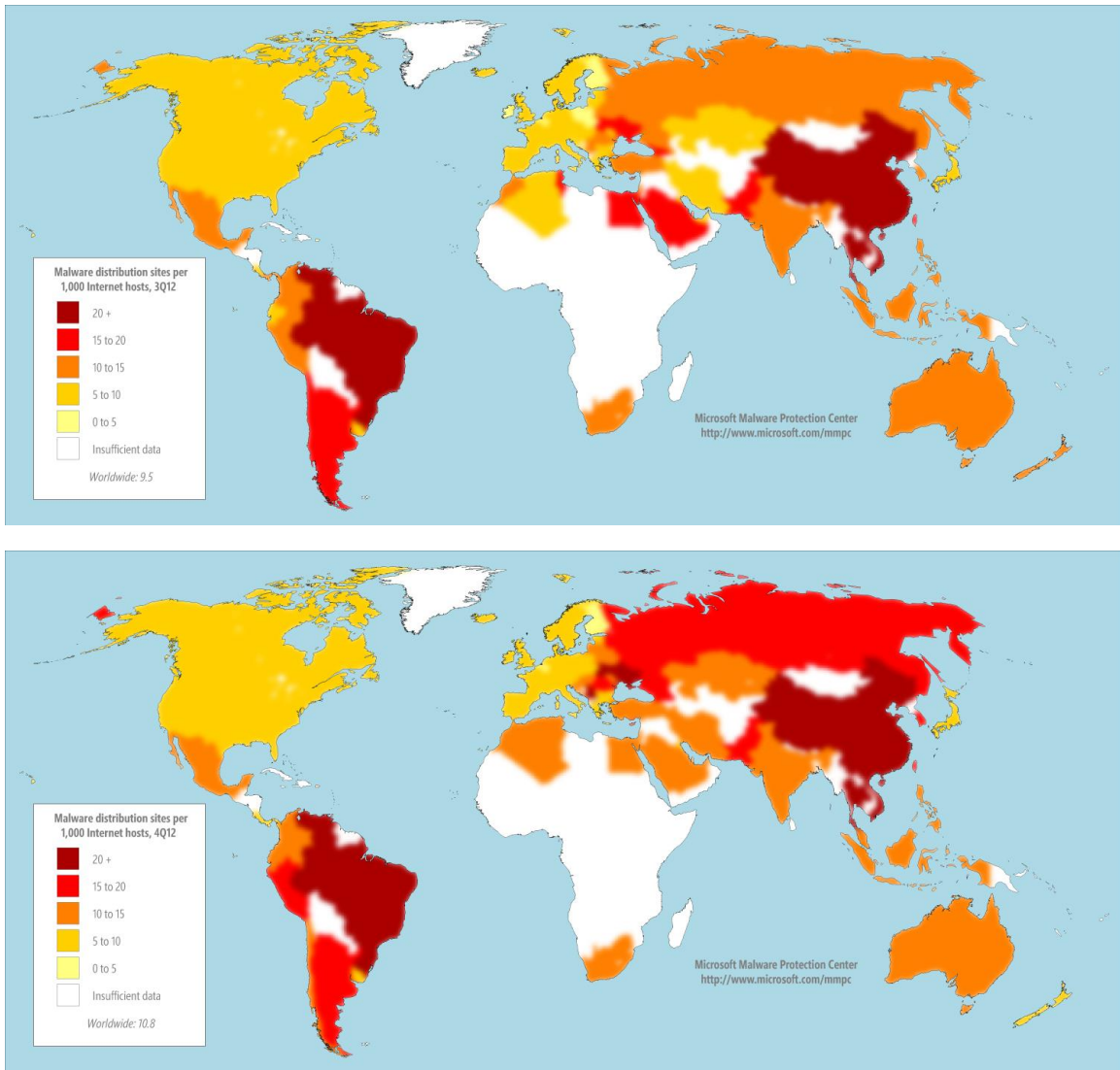
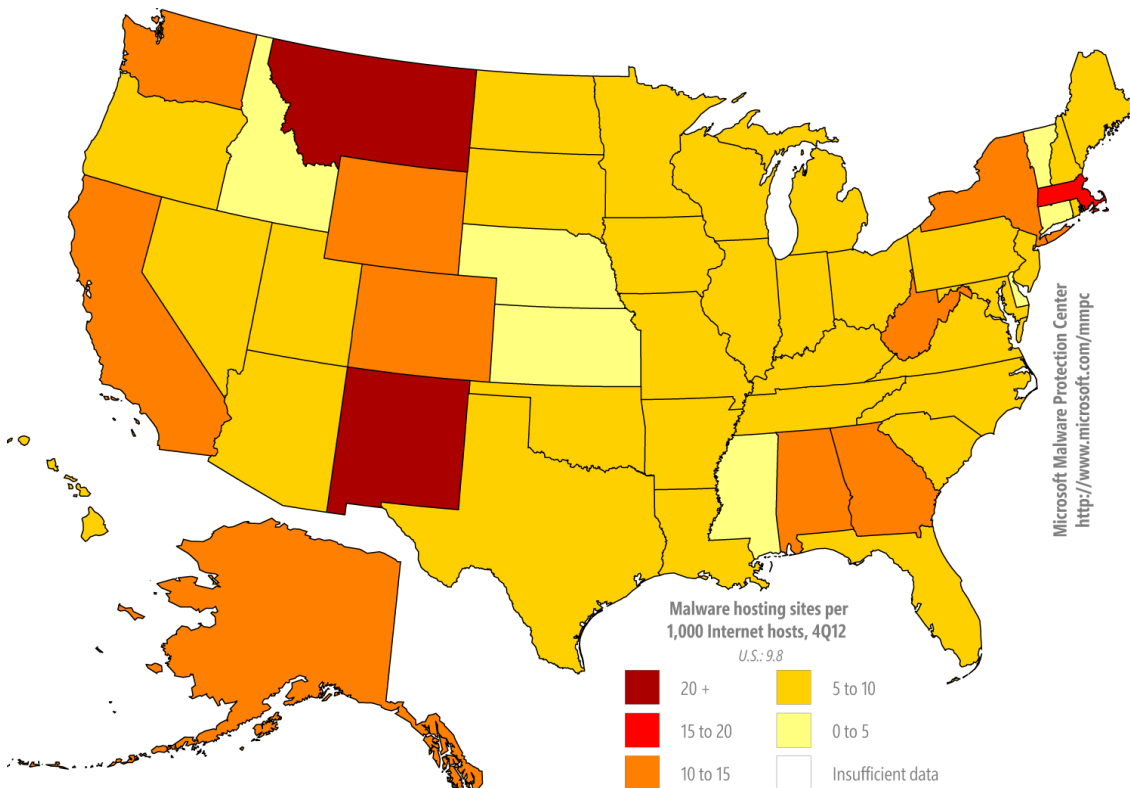
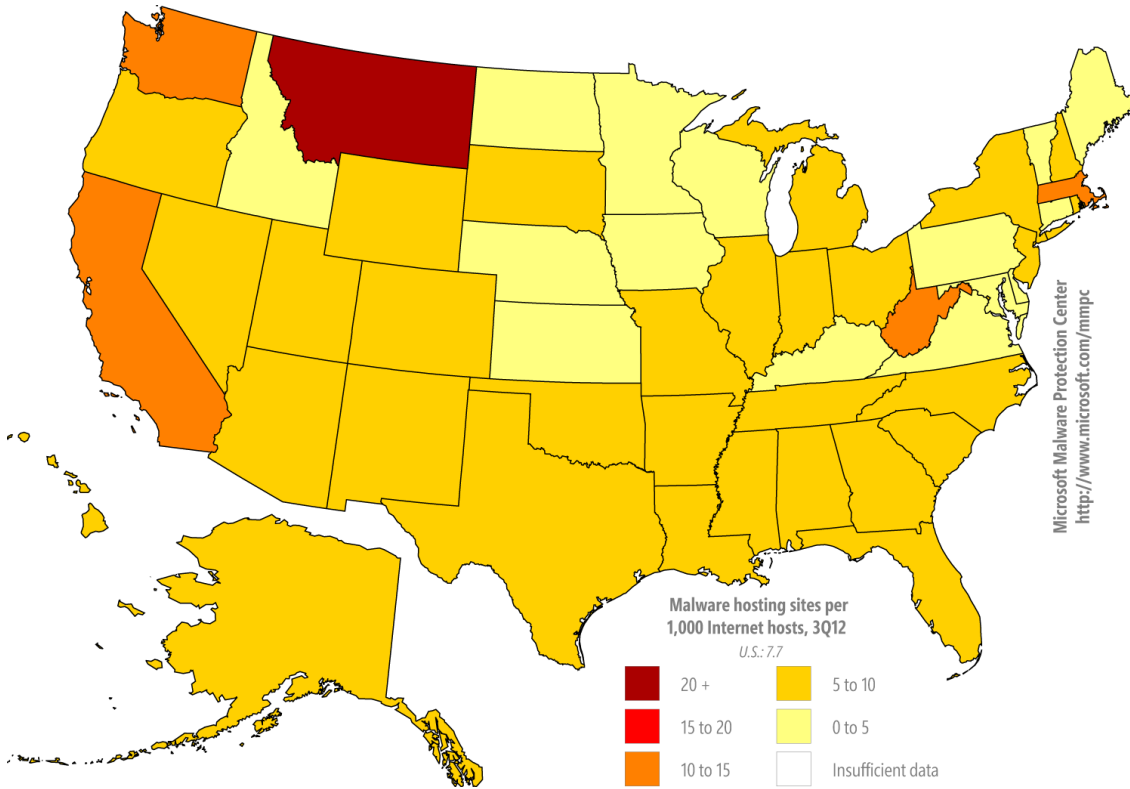
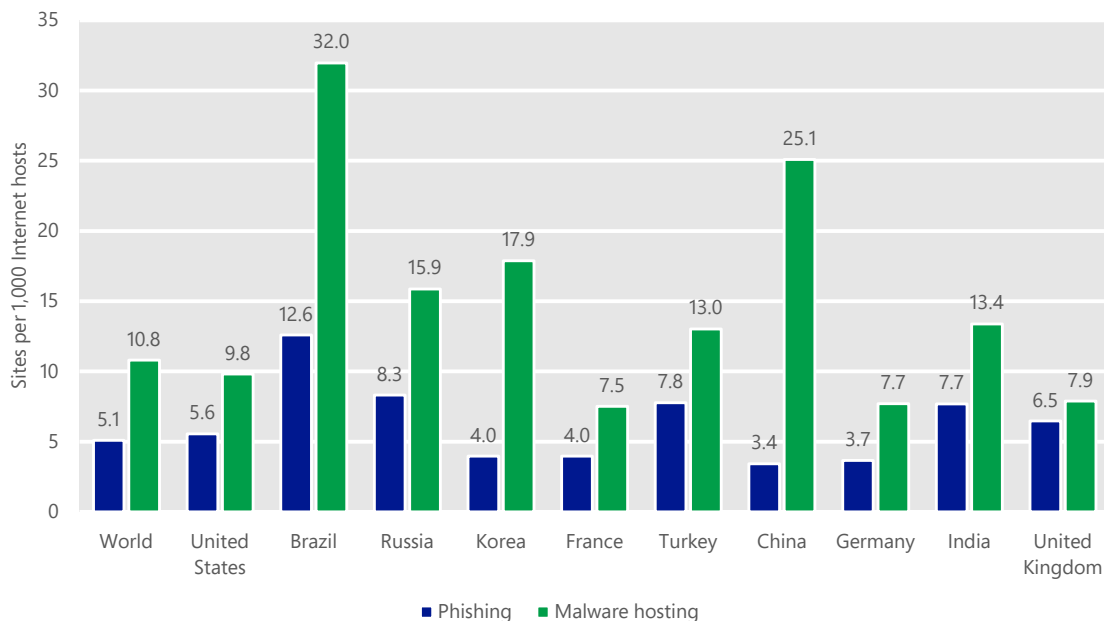


Figure 61. Malware distribution sites per 1,000 Internet hosts for US states in 3Q12 (top) and 4Q12 (bottom)



- Sites that host malware were significantly more common than phishing sites in 2H12. SmartScreen Filter detected 9.5 malware hosting sites per 1000 Internet hosts worldwide in 3Q12, and 10.8 per 1000 in 4Q12.
- China, which had a lower than average concentration of phishing sites (3.4 phishing sites per 1000 Internet hosts in 4Q12), also had a very high concentration of malware hosting sites (25.1 malware hosting sites per 1000 hosts in 4Q12). Other locations with large concentrations of malware hosting sites included Brazil (32.0), Korea (17.9), and Russia (15.9). Locations with low concentrations of malware hosting sites included Japan (5.3), Sweden (5.4), and Poland (6.1).
- Unlike with phishing sites, no significant correlation was observed among US states between number of hosts and malware hosting site concentration.
- US states with high concentrations of malware hosting sites include New Mexico (34.6 per 1000 Internet hosts in 2Q12), Montana (22.0), and Massachusetts (15.1). States with low concentrations of malware hosting sites include Idaho (3.2), Delaware (3.3), and Kansas (3.3).

Figure 62. Phishing and malware hosting sites worldwide and for 10 prominent locations, 4Q12



## 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

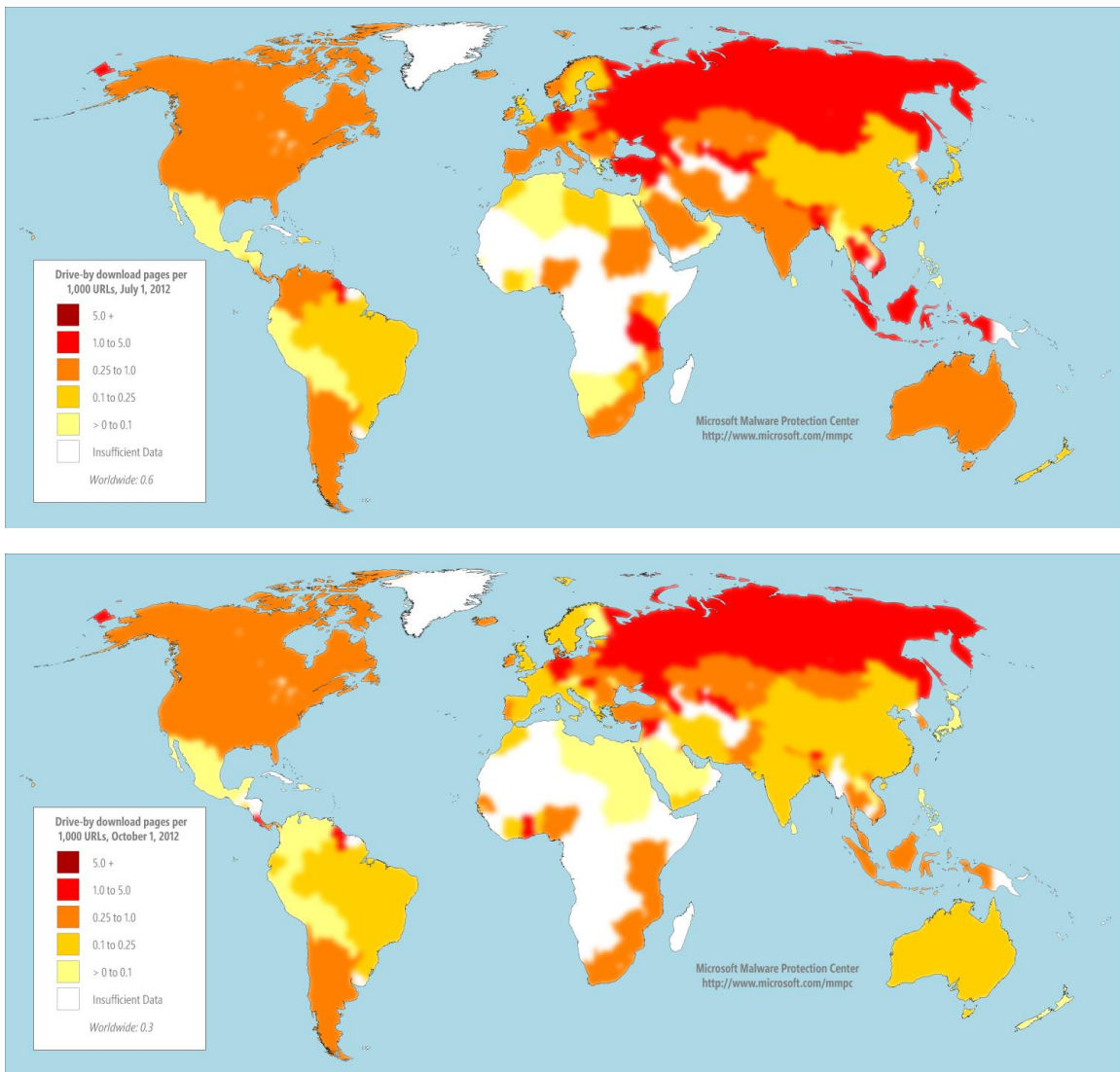


computers can be infected with malware simply by visiting such a website, even without attempting to download anything.

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 63 shows the concentration of drive-by download pages in countries and regions throughout the world at the end of 3Q12 and 4Q12, respectively.

Figure 63. Drive-by download pages indexed by Bing at the end of 3Q12 (top) and 4Q12 (bottom), per 1000 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.
- Significant locations with high concentrations of drive-by download URLs in both quarters include Azerbaijan, with 3.9 drive-by URLs for every 1,000 URLs tracked by Bing at the end of 4Q12; Syria, with 3.8; and Uzbekistan, with 3.2.

## 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](#)



# Appendixes

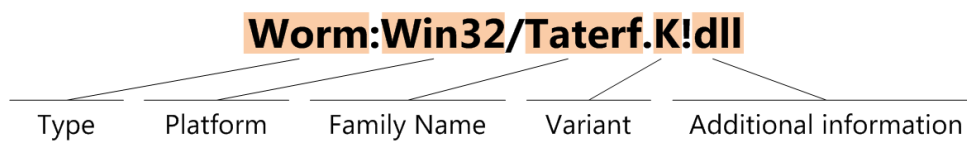


## Appendix A: Threat naming conventions

The MMPC malware naming standard is derived from the Computer Antivirus Research Organization (CARO) Malware Naming Scheme, originally published in 1991 and revised in 2002. Most security vendors use naming conventions that are based on the CARO scheme, with minor variations, although family and variant names for the same threat can differ between vendors.

A threat name can contain some or all of the components seen in Figure 64.

Figure 64. The Microsoft malware naming convention



The *type* indicates the primary function or intent of the threat. The MMPC assigns each individual threat to one of a few dozen different 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 10 categories. For example, the TrojanDownloader and TrojanDropper types are combined into a single category, called Trojan Downloaders & Droppers.

The *platform* indicates the operating environment in which the threat is designed to run and spread. For most of the threats described in this report, the platform is listed as "Win32," for the Win32 API used by 32-bit and 64-bit versions of Windows desktop and server operating systems. (Not all Win32 threats can run on every version of Windows, however.) Platforms can include programming languages and file formats, in addition to operating systems. For example, threats in the ASX/Wimad family are designed for programs that parse the Advanced Stream Redirector (ASX) file format, regardless of operating system. Some families have components that run on multiple platforms, in which case the most significant platform is usually the one given. In some contexts, a different platform might be listed for a family than one given elsewhere, when appropriate. In some rare cases, some predominantly multiplatform families may be listed without a platform, as with the exploit family Blacole.

Groups of closely related threats are organized into *families*, which are given unique names to distinguish them from others. The family name is usually not related to anything the malware author has chosen to call the threat. Researchers use a variety of techniques to name new families, such as excerpting and modifying strings of alphabetic characters found in the malware file. Security vendors usually try to adopt the name used by the first vendor to positively identify a new family, although sometimes different vendors use completely different names for the same threat, which can happen when two or more vendors discover a new family independently. The MMPC Encyclopedia ([www.microsoft.com/mmpc](http://www.microsoft.com/mmpc)) lists the names used by other major security vendors to identify each threat, when known.

Some malware families include multiple components that perform different tasks and are assigned different types. For example, the Win32/Frethog family includes variants designated TrojanDownloader:Win32/Frethog.C and PWS:Win32/Frethog.C, among others. In the *Microsoft Security Intelligence Report*, the category listed for a particular family is the one that Microsoft security analysts have determined to be the most significant category for the family (which, in the case of Frethog, is Password Stealers & Monitoring Tools).

Malware creators often release multiple *variants* for a family, typically in an effort to avoid being detected by security software. Variants are designated by letters, which are assigned in order of discovery—A through Z, then AA through AZ, then BA through BZ, and so on. A variant designation of “gen” indicates that the threat was detected by a generic signature for the family rather than as a specific variant. Any additional characters that appear after the variant provide comments or additional information.

In the *Microsoft Security Intelligence Report*, a threat name that consists of a platform and family name (for example, “Win32/Taterf”) is a reference to a family. When a longer threat name is given (for example, “Worm:Win32/Taterf.K!dll”), it is a reference to a more specific signature or to an individual variant. To make the report easier to read, family and variant names have occasionally been abbreviated in contexts where confusion is unlikely. Thus, Win32/Taterf would be referred to simply as “Taterf” on subsequent mention in some places, and Worm:Win32/Taterf.K simply as “Taterf.K.”



## 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 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.
- [Exchange Online Protection](#) protects the networks 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.
- [Hotmail](#) has hundreds of millions of active email users in more than 30 countries/regions around the world.
- The [Malicious Software Removal Tool](#) (MSRT) is a free tool that Microsoft designed to help identify and remove 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 2H12. The MSRT is not a replacement for an up-to-date antivirus solution because of its lack of real-time protection and because it uses only the portion of the Microsoft antivirus signature database that enables it to target specifically selected, prevalent malicious software.
- 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 real-time protection product that combines an antivirus and antispyware scanner with phishing and firewall 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.
- [SmartScreen Filter](#), a feature in Internet Explorer 8, 9, and 10, 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](#) is a program that is available at no cost to licensed users of Windows that provides real-time protection against spyware and other potentially unwanted software. Windows Defender runs on more than 100 million computers worldwide. Windows 8 includes a new version of Windows Defender that provides real-time antimalware protection as well.
- [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 65. US privacy statements for the Microsoft products and services used in this report

Product or Service	Privacy Statement URL
Bing	<a href="http://www.microsoft.com/privacystatement/en-us/bing/default.aspx">www.microsoft.com/privacystatement/en-us/bing/default.aspx</a>
Exchange Online Protection	<a href="https://admin.messaging.microsoft.com/legal/privacy/en-us.htm">https://admin.messaging.microsoft.com/legal/privacy/en-us.htm</a>
Hotmail	<a href="http://privacy.microsoft.com/en-us/fullnotice.mspix">privacy.microsoft.com/en-us/fullnotice.mspix</a>
Internet Explorer 10	<a href="http://windows.microsoft.com/en-US/internet-explorer/ie10-win8-privacy-statement">windows.microsoft.com/en-US/internet-explorer/ie10-win8-privacy-statement</a>
Malicious Software Removal Tool	<a href="http://www.microsoft.com/security/pc-security/msrt-privacy.aspx">www.microsoft.com/security/pc-security/msrt-privacy.aspx</a>
Microsoft Security Essentials	<a href="http://windows.microsoft.com/en-us/windows/security-essentials-privacy">windows.microsoft.com/en-us/windows/security-essentials-privacy</a>
Microsoft Safety Scanner	<a href="http://www.microsoft.com/security/scanner/en-us/Privacy.aspx">www.microsoft.com/security/scanner/en-us/Privacy.aspx</a>
System Center Endpoint Protection	<a href="http://technet.microsoft.com/en-us/library/hh508835.aspx">technet.microsoft.com/en-us/library/hh508835.aspx</a>
Windows Defender in Windows 8	<a href="http://windows.microsoft.com/en-US/windows-8/windows-8-privacy-statement?T1=supplement#section_36">windows.microsoft.com/en-US/windows-8/windows-8-privacy-statement?T1=supplement#section_36</a>
Windows Defender Offline	<a href="http://windows.microsoft.com/en-us/windows/windows-defender-offline-privacy">windows.microsoft.com/en-us/windows/windows-defender-offline-privacy</a>

## Appendix C: Worldwide infection rates

“Global infection rates,” on page 37, explains how threat patterns differ significantly in different parts of the world. Figure 66 shows the infection rates in locations with at least 100,000 quarterly MSRT executions in 2H12, as determined by geolocation of the IP address of the reporting computer.<sup>15</sup> CCM is the number of computers cleaned for every 1,000 executions of MSRT. See “About this report” on page v for more information about the CCM metric and how it is 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 66. Infection rates (CCM) for locations around the world in 2012, by quarter

Country/Region	1Q12	2Q12	3Q12	4Q12
<b>Worldwide</b>	<b>6.6</b>	<b>7.0</b>	<b>5.3</b>	<b>6.0</b>
Afghanistan	10.3	10.6	9.8	12.2
Albania	27.5	25.7	23.2	18.0
Algeria	20.1	19.0	16.4	17.9
Angola	15.0	14.8	12.9	10.6
Argentina	8.7	7.2	6.5	5.7
Armenia	6.7	6.5	5.9	7.2
Australia	4.0	2.9	3.8	3.2
Austria	2.8	2.8	2.3	2.0
Azerbaijan	12.8	12.0	11.0	11.2
Bahamas, The	11.6	10.4	8.6	9.2
Bahrain	15.4	14.7	12.3	12.6
Bangladesh	15.6	15.1	14.4	12.9
Barbados	5.3	3.8	3.7	3.1
Belarus	5.4	7.2	6.5	5.2

<sup>15</sup> For more information about this process, see the entry “[Determining the Geolocation of Systems Infected with Malware](#)” (November 15, 2011) on the Microsoft Security Blog ([blogs.technet.com/security](http://blogs.technet.com/security)).

Country/Region	1Q12	2Q12	3Q12	4Q12
Belgium	3.7	4.1	3.0	2.1
Bolivia	11.7	10.7	9.4	9.4
Bosnia and Herzegovina	16.6	14.9	13.5	14.0
Brazil	13.3	10.1	9.0	7.3
Brunei	8.0	7.9	6.6	7.2
Bulgaria	9.0	8.0	6.9	7.6
Burkina Faso	—	10.1	8.5	7.4
Cambodia	11.8	11.6	10.5	9.8
Cameroon	14.6	13.6	12.4	12.9
Canada	3.8	2.7	2.7	2.2
Chile	13.7	9.4	7.1	5.6
China	0.8	0.6	0.6	0.7
Colombia	8.3	7.2	7.1	5.8
Costa Rica	5.8	4.3	4.0	3.7
Côte d'Ivoire	15.2	12.6	10.8	8.8
Croatia	9.3	8.0	7.4	7.3
Cyprus	7.3	6.3	5.3	5.4
Czech Republic	2.1	1.8	2.1	1.6
Denmark	1.5	1.7	1.7	1.5
Dominican Republic	15.2	13.8	13.1	12.4
Ecuador	11.3	11.1	9.8	8.7
Egypt	24.7	23.4	20.1	22.3
El Salvador	6.8	6.1	5.9	5.4
Estonia	3.6	3.0	2.4	2.3
Ethiopia	9.7	10.5	9.1	11.3
Finland	1.1	1.1	1.4	0.8
France	3.2	2.9	2.2	1.9
Georgia	23.3	25.2	22.9	24.2
Germany	3.5	3.0	2.6	2.1
Ghana	11.9	11.1	8.8	8.2
Greece	7.3	6.3	5.3	5.7

Country/Region	1Q12	2Q12	3Q12	4Q12
Guadeloupe	9.6	9.6	8.2	7.4
Guatemala	8.0	6.9	6.8	6.1
Haiti	16.4	12.1	9.8	9.1
Honduras	9.1	8.5	7.9	7.1
Hong Kong SAR	3.5	2.6	2.3	2.2
Hungary	5.3	5.2	4.5	4.7
Iceland	3.2	2.4	1.7	1.7
India	13.2	12.5	11.3	10.0
Indonesia	17.0	16.6	15.7	14.2
Iran	10.8	12.4	11.1	11.0
Iraq	23.7	25.3	20.7	20.6
Ireland	4.0	2.9	2.3	2.0
Israel	9.7	8.6	6.9	6.9
Italy	6.5	4.5	3.7	3.2
Jamaica	8.8	8.2	6.8	6.0
Japan	1.0	0.9	0.7	0.7
Jordan	15.8	18.0	16.0	12.6
Kazakhstan	8.8	8.5	7.1	6.9
Kenya	9.5	9.0	7.3	6.8
Korea	27.5	70.4	27.5	93.0
Kuwait	11.8	11.6	10.0	9.7
Latvia	5.1	4.5	3.8	4.1
Lebanon	13.3	13.9	10.4	13.0
Libya	25.4	23.0	19.3	20.9
Lithuania	7.4	6.4	5.8	6.4
Luxembourg	2.8	2.0	2.2	2.2
Macao SAR	3.0	2.2	1.9	1.9
Macedonia, FYRO	16.5	14.3	13.1	14.8
Malaysia	9.3	8.7	8.1	7.9
Malta	4.1	3.6	2.5	2.3
Martinique	8.0	8.6	6.8	6.2

Country/Region	1Q12	2Q12	3Q12	4Q12
Mauritius	9.2	8.2	7.2	7.0
Mexico	11.2	10.0	9.3	7.8
Moldova	5.9	6.7	6.1	7.8
Mongolia	12.0	13.8	11.3	13.1
Morocco	15.6	20.1	21.1	20.1
Mozambique	11.9	11.3	9.2	8.1
Myanmar	—	—	12.0	13.9
Namibia	10.5	9.7	9.2	9.5
Nepal	20.0	19.3	18.2	16.5
Netherlands	6.3	4.8	5.6	2.6
New Zealand	3.5	3.1	3.3	3.2
Nicaragua	6.2	6.3	6.2	4.7
Nigeria	8.1	8.1	7.2	7.0
Norway	1.6	1.9	3.0	2.2
Oman	14.9	16.2	12.2	13.4
Pakistan	32.8	35.3	30.6	26.8
Palestinian Authority	29.1	29.8	24.4	26.2
Panama	9.9	7.6	6.4	5.7
Paraguay	6.1	4.9	5.8	4.9
Peru	10.7	10.3	9.6	8.4
Philippines	10.2	9.8	9.9	10.7
Poland	9.0	8.0	7.8	7.2
Portugal	6.4	5.1	3.8	3.3
Puerto Rico	6.7	5.9	4.9	4.7
Qatar	12.1	11.6	9.0	8.6
Réunion	7.1	7.3	6.2	5.2
Romania	14.9	15.0	12.9	12.4
Russia	6.2	6.7	5.5	5.0
Saudi Arabia	14.0	13.4	10.7	11.4
Senegal	11.5	9.7	8.5	9.2
Serbia	15.1	13.5	11.7	11.6

Country/Region	1Q12	2Q12	3Q12	4Q12
Singapore	5.6	4.4	3.9	3.7
Slovakia	3.4	3.0	2.8	2.6
Slovenia	4.2	4.0	4.3	3.4
South Africa	7.9	6.9	6.4	6.5
Spain	7.3	5.4	4.0	3.6
Sri Lanka	10.5	10.0	9.9	8.2
Sudan	16.5	17.5	15.8	14.9
Sweden	1.8	2.1	2.8	1.6
Switzerland	1.8	1.7	2.3	1.6
Syria	16.2	19.8	19.1	23.1
Taiwan	6.9	5.3	4.8	5.2
Tanzania	10.1	9.8	7.8	7.3
Thailand	18.9	17.3	18.0	21.0
Trinidad and Tobago	8.5	7.2	5.8	5.0
Tunisia	15.3	14.3	10.9	12.9
Turkey	31.9	26.7	20.9	20.7
Uganda	11.4	11.1	8.2	8.2
Ukraine	6.6	7.0	7.9	7.2
United Arab Emirates	16.1	14.6	11.9	11.0
United Kingdom	3.9	3.2	3.0	2.3
United States	5.0	6.0	5.0	3.3
Uruguay	4.3	4.0	3.9	3.1
Uzbekistan	4.3	4.5	3.6	3.4
Venezuela	7.0	6.0	5.8	5.3
Vietnam	17.0	18.1	16.9	16.9
Yemen	21.8	21.9	18.8	18.7
Zambia	12.4	11.7	8.5	7.6
Zimbabwe	12.7	13.4	10.7	9.7
<b>Worldwide</b>	<b>6.6</b>	<b>7.0</b>	<b>5.3</b>	<b>6.0</b>

# Glossary

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

## **419 scam**

See *advance-fee fraud*.

## **ActiveX control**

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

## **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.

## **adware**

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

## **backdoor trojan**

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



**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*.

**CCM**

Short for *computers cleaned per mille* (thousand). The number of computers cleaned for every 1,000 executions of MSRT. For example, if MSRT has 50,000 executions in a particular location in the first quarter of the year and removes infections from 200 computers, the CCM for that location in the first quarter of the year is 4.0 ( $200 \div 50,000 \times 1,000$ ).

**clean**

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

**definition**

A set of signatures that antivirus, antispymware, or antimalware products can use to identify malware. Other vendors may refer to definitions as DAT files, pattern files, identity files, or antivirus databases.

**DEP**

See *Data Execution Prevention (DEP)*.

**detection**

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

**detection signature**

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

**disclosure**

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

**downloader**

See *trojan downloader/dropper*.

**exploit**

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

**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.

**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.

**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 10. 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)*.

**packed**

Said of malware that has been prepared for distribution using a packaging program called a packer, typically in an effort to evade detection by security software.

**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*.

**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 10, and being blocked by the Phishing Filter or SmartScreen Filter. Also see *malware impression*.

**potentially unwanted software**

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

**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.

**remote control software**

A program that provides access to a computer from a remote location. Such programs are often installed by the computer owner or administrator and are only a risk if unexpected.

**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.

### **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.

### **spyware**

A program that collects information, such as the websites a user visits, without adequate consent. Installation may be without prominent notice or without the user’s knowledge.

**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.

**tool**

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

**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](http://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.

**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.

**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.

**JS/BlacoleRef.** An obfuscated script, often found inserted into compromised websites, that uses a hidden inline frame to redirect the browser to a Blacole exploit server.

**Win32/Bumat.** A generic detection for a variety of threats.

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

**Win32/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.

**Win32/CnsMin.** Spyware that installs a browser helper object (BHO) that redirects Internet Explorer searches to a Chinese search portal. It may be

installed without adequate user consent, and may prevent its files from being removed.

**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/DealPly.** Adware that displays offers related to the user's web browsing habits. It may be bundled with certain third-party software installation programs.

**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/Dowque.** A generic detection for malicious files that are capable of installing other malware.

**AndroidOS/DroidDream.** A malicious program that affects mobile devices running the Android operating system. It may be bundled with clean applications, and is capable of allowing a remote attacker to gain access to the mobile device.

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

**Win32/EoRezo.** Adware that displays predominantly French-language targeted advertising to affected users while browsing the Internet, based on downloaded pre-configured information.

**MacOS\_X/FakeMacdef.** A rogue security software family that affects Apple Mac OS X. It has been distributed under the names MacDefender, MacSecurity, MacProtector, and possibly others.

**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, Win 7 Internet Security 2010, Vista Antivirus Pro, XP Guardian, 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/FakeVimes.** A rogue security software family distributed under the names Internet Security Guard, Extra Antivirus, Virus Melt, and many others.

**MacOS\_X/Flashback.** A trojan that targets Java JRE vulnerability CVE-2012-0507 on Mac OS X to enroll the infected computer in a botnet.

**AndroidOS/GingerBreak.** A program that affects mobile devices running the Android operating system. It drops and executes an exploit that, if run successfully, gains administrator privileges on the device.

**AndroidOS/GingerMaster.** A malicious program that affects mobile devices running the Android operating system. It may be bundled with clean applications, and is capable of allowing a remote attacker to gain access to the mobile device.

**Win32/Helompy.** A worm that spreads via removable drives and attempts to capture and steal authentication details for a number of different websites or online services.

**Win32/Hotbar.** Adware that displays a dynamic toolbar and targeted pop-up ads based on its monitoring of web-browsing activity.

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

**Win32/IRCbot.** A large family of backdoor trojans that drops other malicious software and connects to IRC servers to receive commands from attackers.

**Win32/Keygen.** A detection for tools that generate product keys for various software products.

**Win32/Kuluoz.** A trojan that tries to steal passwords and sensitive files from the affected computer. It may also download other malware, including rogue security software.

**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.

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

**Win32/OpenCandy.** An adware program that may be bundled with certain third-party software installation programs. Some versions may send user-specific information, including a unique machine code, operating system information, locale, and certain other information to a remote server without obtaining adequate user consent. These versions are detected by Microsoft's antimalware products.

**Win32/Pameseg.** A fake program installer that requires the user to send SMS messages to a premium number to successfully install certain programs.

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

**JS/Phoex.** A malicious script that exploits the Java Runtime Environment (JRE) vulnerability discussed in CVE-2010-4452. If run in a computer running a vulnerable version of Java, it downloads and executes arbitrary files.

**Win32/Pidief.** An exploit that targets vulnerability CVE-2010-0188 in Adobe Acrobat and Adobe Reader. Adobe released security bulletin APSB10-07 in February 2010 to address the vulnerability.

**Win32/Pluzoks.** A trojan that silently downloads and installs other programs without consent. This could include the installation of additional malware or malware components.

**Win32/Protlerdob.** A software installer with a Portuguese language user interface. It presents itself as a free movie download but bundles with it a number of programs that may charge for services.

**Win32/QBundle.** A multi-component family that connects to a remote server to receive commands, and downloads files (possibly including malware) to the computer.

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

**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/Seedabutor.** A JavaScript trojan that attempts to redirect the browser to another website.

**Win32/Sirefef.** A rogue security software family distributed under the name Antivirus 2010 and others.

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

**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/Startpage.** A detection for various threats that change the configured start page of the affected user's web browser and may also perform other malicious actions.

**Win32/Stuxnet.** A multi-component family that spreads via removable volumes by exploiting the vulnerability addressed by Microsoft Security Bulletin MS10-046.

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

**Win32/Tracur.** A trojan that downloads and executes arbitrary files, redirects web search queries to a malicious URL, and may also install other malware.

**Win32/VB.** A detection for various threats written in the Visual Basic programming language.

**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 Winweb Security, Win 8 Security System, System Security, and others.

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

**Win32/Xolondox.** A trojan downloader that uses fake filenames to masquerade as a legitimate program.

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

**Win32/Zwangi.** A program that runs as a service in the background and modifies web browser settings to visit a particular website.

# Index

- 419 scams. *See* advance-fee fraud
- Active Directory Domain Services, 55
- Adobe Acrobat, 27, 31, 32, 58, 103, 104
- Adobe Flash Player, 27, 35, 36
- Adobe Reader, 27, 31, 58, 103, 104
- Adobe Systems
  - security updates, 36, 104
- advance-fee fraud, 62, 63
- adware, 38, 46, 47, 49, 50, 51, 57, 58
- Albania, 42
- Algeria, 34
- Android, 32, 34, 35, 101, 102
  - security updates, 35
- Apple, Inc., 22, 29, 55
- Arizona, 72
- Autorun (threat family), 38, 46, 48, 49, 51, 56, 57, 100
- AutoRun (Windows feature), 46
- Azerbaijan, 80
- Bangladesh, 34
- Bing, 79, 80, 87, 88
- Blackhole exploit kit. *See* Blacole
- Blacole, 26, 27, 28, 29, 30, 32, 34, 38, 46, 47, 49, 51, 56, 57, 58, 100
- BlacoleRef, 56, 100
- Brazil, 34, 37, 38, 47, 72, 78
- Bumat, 75, 100
- Canada, 54
- CCM. *See* computers cleaned per mille
- Chile, 43
- China, 37, 41, 48, 54, 78
- Chir, 42, 100
- CnsMin, 48, 100
- Colombia, 34
- Common Vulnerabilities and Exposures. *See* CVE identifier
- Common Vulnerability Scoring System, 18, 20
- computers cleaned per mille, v, 4, 6, 8, 9, 10, 11, 12, 13, 38, 39, 40, 41, 42, 43, 44, 45
- Conficker, 41, 56, 58, 100
- Cool exploit kit, 28, 34
- CpLnk. *See* CVE-2010-2568
- Cutwail botnet, 60
- CVE identifier, 17, 25
- CVE-2006-6456, 105
- CVE-2007-0071, 36
- CVE-2010-0188, 31, 104
- CVE-2010-0840, 29
- CVE-2010-1885, 27
- CVE-2010-2568, 25, 26, 32, 33, 34, 46
  - detections by country or region, 34
- CVE-2010-2884, 36
- CVE-2010-4452, 103
- CVE-2011-0097, 31
- CVE-2011-0611, 36
- CVE-2011-1823, 35
- CVE-2011-3402, 28, 32, 34
- CVE-2011-3544, 29
- CVE-2012-0507, 28, 29, 102
- CVE-2012-1723, 28, 29
- CVSS. *See* Common Vulnerability Scoring System
- DealPly, 38, 46, 49, 50, 51, 57, 58, 101
- Delaware, 78
- Denmark, 13, 41
- Dorkbot, 43, 49, 51, 56, 57, 101
- Dowque, 74, 101
- drive-by downloads, 28, **78–80**
- DroidDream, 35, 101
- Dynamer, 74, 101
- Egypt, 34, 41
- email threats, **59–64**
- EoRezo, 47, 101
- Exchange Online Protection, 59, 60, 61, 62, 63, 64, 87, 88
- exploits, **25–36**, 38, 46, 47, 49, 51, 56, 57, 58
  - Adobe Acrobat, 31–32
  - Adobe Flash Player, 35–36
  - Adobe Reader, 31–32

- Android, 32–35
- document parser, 26, 31–32
- families, 27–28
- HTML, 26, 29–30
- Java, 26, 28–29
- JavaScript, 26, 29–30
- JustSystems Ichitaro, 31–32
- Microsoft Office, 31–32
- Microsoft Windows, 32–35
- operating system, 26, 32–35
- FakeMacdef, 55, 101
- FakePAV, 55, 101
- FakeRean, 101
- FakeSysdef, 102
- FakeVimes, 102
- Finland, 12, 41, 42, 72
- Flashback, 29, 102
- Forefront Client Security. *See* Microsoft System Center Endpoint Protection
- Forefront Endpoint Protection. *See* Microsoft System Center Endpoint Protection
- Forefront Online Protection for Exchange. *See* Exchange Online Protection
- France, 37, 38, 47
- French language, 47, 101
- FTP, 104
- generic detections, 30, 31, 38, 46, 50, 51, 57, 75
- Georgia (country), 11, 41
- Georgia (US state), 72
- Germany, 37, 47
- GingerBreak, 35, 102
- GingerMaster, 35, 102
- Google, 22, 32, 35
- Group Policy, 3
- Haiti, 43
- Helompy, 42, 102
- Hotbar, 38, 46, 57, 58, 102
- Hotmail, 87, 88
- HTML, 104
- HTML exploits, 29–30
- Iceland, 41, 42
- Idaho, 78
- IframeRef, 46, 49, 50, 51, 56, 57, 102
- IFrames. *See* inline frames, malicious
- India, 34, 37, 38, 48
- Indonesia, 34
- infection rate. *See* computers cleaned per mille
- inline frames, malicious, 30, 50, 102
- Internet Explorer, 22, 30, 65, 66, 67, 72, 88, 100
- Iraq, 34
- IRCbot, 42, 102
- jailbreaking, 35
- Japan, 12, 41, 42, 54, 72, 78
- Japanese language, 32
- Java Runtime Environment, 27, 28, 29, 102, 103
  - exploits, 28–29
  - security updates, 28, 29
- JavaScript
  - exploits, 29–30
- JRE. *See* Java Runtime Environment
- JustSystems Ichitaro, 32
- Kansas, 78
- Keygen, 10, 11, 38, 42, 46, 48, 49, 51, 56, 57, 102
- Korea, 12, 37, 38, 40, 45, 48, 51, 54, 78
- Korean language, 53, 54, 103
- Kuluoz, 74, 102
- Linux, 22, 29
- Lotoor, 27, 35, 102
- Mac Defender. *See* Fakemacdef
- Mac OS X, 29, 55
- Malagent, 74, 103
- Malicious Software Removal Tool, v, 4, 5, 7, 8, 10, 11, 39, 40, 41, 42, 43, 44, 53, 54, 87, 88
- malware and potentially unwanted software, **37–58**
  - by country or region, 37–43
  - by operating system, 43–45
  - categories, 45–48
    - by location, 46–48
  - families, 48–52
    - by operating system, 50–52

global, 37–43  
 on home and enterprise computers, 55–58  
 rogue security software, 52–55  
 malware hosting sites, 72–78  
   by country or region, 75–78  
   categories of malware hosted, 73–75  
 malware impressions, 72, 73, 74, 75  
 Massachusetts, 78  
 Meredrop, 74, 75, 103  
 Mexico, 34  
 Microjoin, 74, 103  
 Microsoft Download Center, 60, 87  
 Microsoft IT, vii  
 Microsoft Malware Protection Center, v, vii, 29, 45  
   blog, 29  
 Microsoft Office, 31, 32, 104  
 Microsoft Reputation Services, 67, 72  
 Microsoft Safety Scanner, 13, 87, 88  
 Microsoft Security Blog, 18, 37, 41, 89  
 Microsoft Security Bulletins, 25, 33, 34  
 Microsoft Security Engineering Center, vii  
 Microsoft Security Essentials, 55, 87, 88  
 Microsoft Security Response Center, vii  
 Microsoft System Center Endpoint Protection, 88  
 Microsoft Update, 4, 52, 87  
 Microsoft Windows, 3, 4, 6, 7, 8, 9, 10, 13, 25, 28, 32, 33, 34, 43, 44, 45, 46, 51, 52, 65, 88  
   Windows 7, 7, 10, 44, 45, 51  
     RTM, 7, 9  
     SP1, 7, 51  
   Windows 8, vi, 7, 10, 25, 44, 51, 88  
   Windows Server 2003, 43  
   Windows Server 2008 R2, 44  
   Windows Server 2012, 44  
   Windows Vista, 9, 45, 46, 51, 52  
   Windows XP, 8, 9, 44, 45, 46, 51, 52  
 Microsoft Word, 31, 105  
 Miscellaneous Potentially Unwanted Software, 4, 38, 46, 47, 48, 49, 51, 56, 57, 74  
 Miscellaneous Trojans, 46, 48, 49, 51, 56, 57, 74  
 MMPC. *See* Microsoft Malware Protection Center  
 Montana, 78  
 Morocco, 34  
 MS01-020, 100  
 MS07-014, 105  
 MS08-067, 100  
 MS10-042, 27  
 MS10-046, 27, 33, 101, 105  
 MS11-087, 34  
 MSEC. *See* Microsoft Security Engineering Center  
 MSIT. *See* Microsoft IT  
 MSRC. *See* Microsoft Security Response Center  
 MSRT. *See* Malicious Software Removal Tool  
 National Vulnerability Database, 17  
 Nebraska, 72  
 New Mexico, 78  
 Norway, 42  
 NVD. *See* National Vulnerability Database  
 Obfuscator, 46, 49, 51, 57, 74, 103  
 Onescan, 12, 38, 40, 45, 46, 48, 51, 53, 54, 103  
 OpenCandy, 49, 103  
 Oracle Corporation, 28  
 Pakistan, 11, 34, 41, 42  
 Palestinian Authority, 41  
 Pameseg, 48, 103  
 Password Stealers & Monitoring Tools, 43, 56  
 PDF, 27, 31, 58, 101, 103  
 Pdfjsc, 26, 27, 31, 38, 46, 47, 49, 51, 56, 57, 58, 103  
 Philippines, 34  
 phishing impressions, 66, 67, 68, 69  
 phishing sites, 66–72  
   by country or region, 69–72, 78  
   target institutions, 68–69  
 Phoex, 103  
 Pidief, 31, 104  
 Pluzoks, 12, 40, 104

Poland, 78  
 Portuguese language, 38, 104  
 potentially unwanted software. *See* malware  
     and potentially unwanted software  
 Protlerdob, 38, 50, 104  
 QBundle, 74, 104  
 Ramnit, 42, 104  
 ransomware, 34, 104  
 Rhode Island, 72  
 Rimod, 74, 75, 104  
 rogue security software, 12, 38, 40, 45, 46,  
     51, 53, 54, 52–55, 101, 102, 103, 104, 105  
 rooting, 34, 35  
 Russia, 34, 37, 38, 48, 72, 78  
 Rustock botnet, 60  
 Sality, 38, 41, 42, 43, 49, 51, 57, 104  
 Saudi Arabia, 34  
 scareware. *See* rogue security software  
 SDL. *See* Security Development Lifecycle  
 Security Development Lifecycle, 24  
 Seedabutor, 50, 104  
 Sirefef, 38, 46, 56, 104  
 Small, 74, 104  
 SmartScreen Filter, 65, 66, 68, 72, 73, 74, 75,  
     78, 88  
 SMS. *See* text messaging  
 SMSer, 74, 104  
 social engineering, 52  
 spam  
     image-only, 64  
     messages blocked, 59–61  
     stock-related, 62  
     types, 61–64  
 spyware, 48  
 Startpage, 74, 105  
 Stuxnet, 33, 105  
 Sweden, 72, 78  
 Swisyn, 74, 75, 105  
 Syria, 80  
 text messaging, 48, 103, 104  
 Thailand, 34  
 Tracur, 38, 105  
 Trojan Downloaders & Droppers, 74  
 trojans, 29, 38, 41, 42, 55  
 Trustworthy Computing, vi, vii, 18  
 Tunisia, 34  
 Turkey, 34, 37, 42, 48  
 TwC. *See* Trustworthy Computing  
 Ukraine, 34  
 United Kingdom, 37, 47  
 United States, 34, 37, 38, 47, 54, 72  
 Unix, 22, 27, 35  
 Utah, 72  
 Uzbekistan, 80  
 VB, 74, 105  
 Vermont, 72  
 Vietnam, 34  
 viruses, 38, 41, 42, 49, 51, 57  
 Vobfus, 43, 105  
 vulnerabilities, **17–24**  
     application, 21–23  
     browser, 21–23  
     complexity, 20–21  
     in Microsoft products, 23–24  
     industry-wide disclosures, 17–18  
     operating system, 21–23  
     severity, 18–20  
 Windows. *See* Microsoft Windows  
 Windows 8, 88  
 Windows Defender, 25, 44, 88  
 Windows Defender Offline, 13, 88  
 Windows Explorer, 33  
 Windows Update, 4, 87  
 Winwebsec, 54, 105  
 Wordinvop, 31, 105  
 worms, 41, 42, 43, 46, 48, 49, 51, 56, 57, 58,  
     74, 75  
 Xolondox, 74, 105  
 Zbot, 41, 43, 56, 105  
 Zwangi, 38, 51, 105



One Microsoft Way  
Redmond, WA 98052-6399  
[microsoft.com/security](https://microsoft.com/security)