Microsoft

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

KEY FINDINGS SUMMARY

Microsoft Security Intelligence Report Key Findings Summary

Microsoft Security Intelligence Report, Volume 14

Volume 14 of the *Microsoft® Security Intelligence Report* (*SIRv14*) provides in-depth perspectives on software vulnerabilities in Microsoft and third-party software, exploits, malicious code threats, and potentially unwanted software. Microsoft developed these perspectives based on detailed trend analyses over the past several years, with a focus on the second half of 2012.

This document summarizes the key findings of the report. *SIRv14* includes a featured article that illustrates how running real-time security software from a reputable vendor and keeping it up to date is one of the most important steps to reduce exposure to malware.

The *SIR* website also includes deep analysis of trends found in more than 100 countries/regions around the world and offers suggestions to help manage risks to your organization, software, and people.

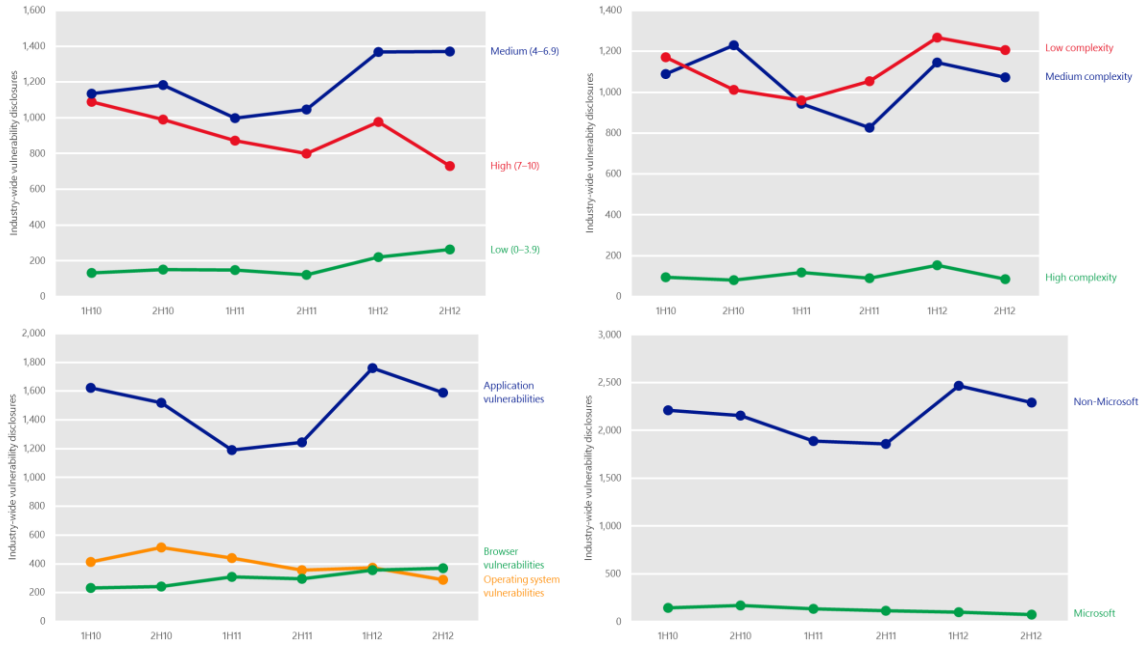
You can download *SIRv14* from www.microsoft.com/sir.

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.

Figure 1. Trends for vulnerability (CVE) severity, vulnerability complexity, disclosures by type, and disclosures for Microsoft and non-Microsoft products, across the entire software industry, 1H10-2H12[1]



- Vulnerability disclosures across the industry were down 7.8 percent from 1H12, primarily because of a decrease in application vulnerability disclosures. Despite this decline, vulnerability disclosures were up 20.0 percent in 2H12 compared to 2H11, a year prior.
- The overall decrease in industry-wide vulnerability disclosures was caused entirely by a decrease in high-severity vulnerabilities, which declined 25.1

[1] Throughout the report, half-yearly and quarterly time periods are referenced using the *n*H*yy* or *n*Q*yy* formats, where *yy* indicates the calendar year and *n* indicates the half or quarter. For example, 2H12 represents the second half of 2012 (July 1 through December 31), and 4Q12 represents the fourth quarter of 2012 (October 1 through December 31).

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.

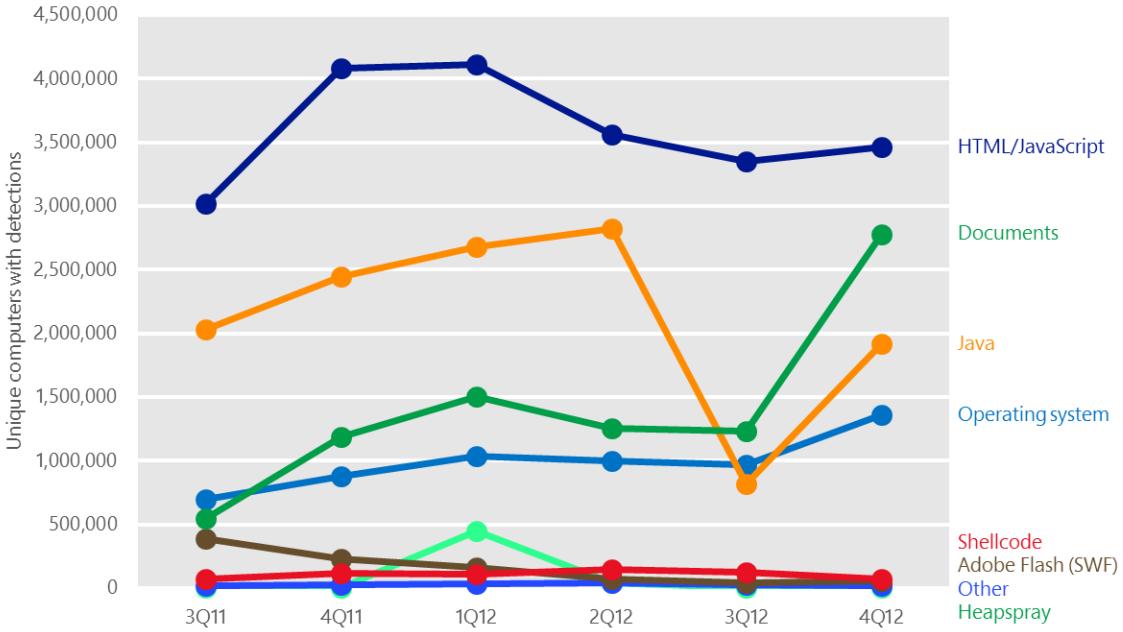
- An increase in application vulnerability disclosures in 1H12 interrupted a trend of consistent period-over-period decreases dating to 2H09.

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 the user's knowledge. Exploits target vulnerabilities in operating systems, web browsers, applications, or software components that are installed on the computer. For more information, download *SIRv14* at www.microsoft.com/sir.

Figure 2 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.

Figure 2. Unique computers reporting different types of exploits, 3Q11-4Q12



- 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.

- Exploits that target vulnerabilities in document readers and editors rose sharply in 4Q12, driven by increased detections of Win32/Pdfjsc.
- Detections of Java exploits fell in 3Q12 to less than a third of their 2Q12 total, but then made up about half of the difference in 4Q12 to become the third most commonly detected type of exploit during the second half of the year.

Exploit families

Figure 3 lists the exploit related families detected most often during the second half of 2012.

Figure 3. 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	1,187,265	2,757,703
Blacole	HTML/JavaScript	3,154,826	2,793,451	2,464,172	2,381,275
CVE-2012-1723*	Java	—	—	110,529	1,430,501
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	270,894	220,780
CVE-2011-3402 (MS11-087)	Operating system	42	24	66	199,648
CVE-2011-3544*	Java	1,358,266	803,053	149,487	116,441
ShellCode*	Shell code	105,479	145,352	120,862	73,615
JS/Phoex	Java	274,811	232,773	201,423	25,546

* 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.
- 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.

Malware and potentially unwanted software

Except where specified, the information in this section was compiled from telemetry data that was generated from more than 600 million computers worldwide and some of the busiest online services on the Internet. Infection rates are given in computers cleaned per mille (CCM), or thousand, and represent the number of reported computers cleaned in a quarter for every 1,000 executions of the Windows® Malicious Software Removal Tool, which is available through Microsoft Update and the Microsoft Safety & Security Center website.

For a perspective on infection patterns worldwide, Figure 4 shows the infection rates in locations around the world using CCM. Detections and removals in individual countries/regions can vary significantly from quarter to quarter.

Figure 4. Infection rates by country/region in 4Q12, by CCM

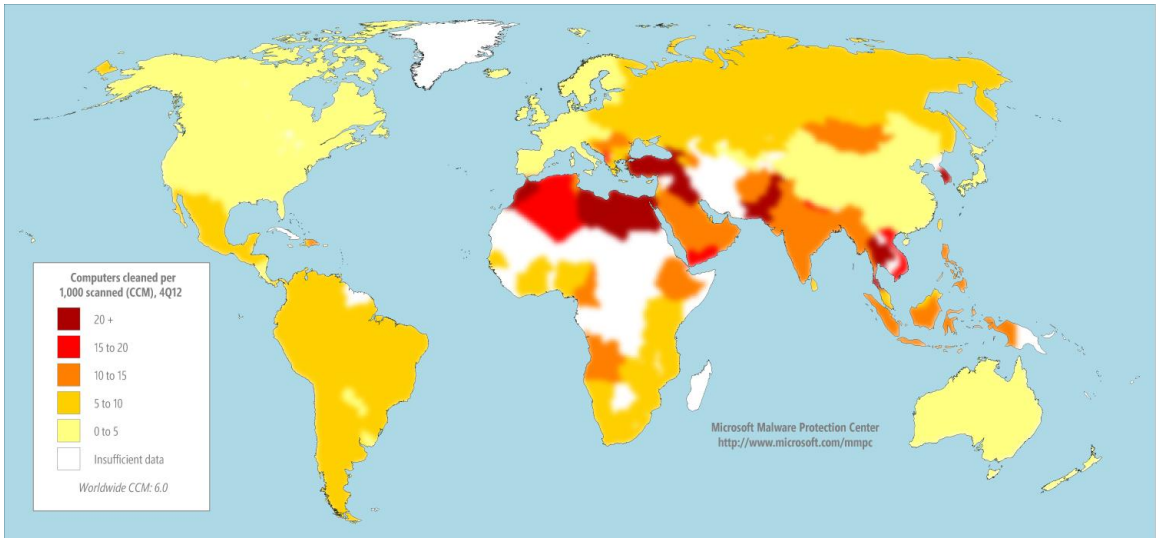
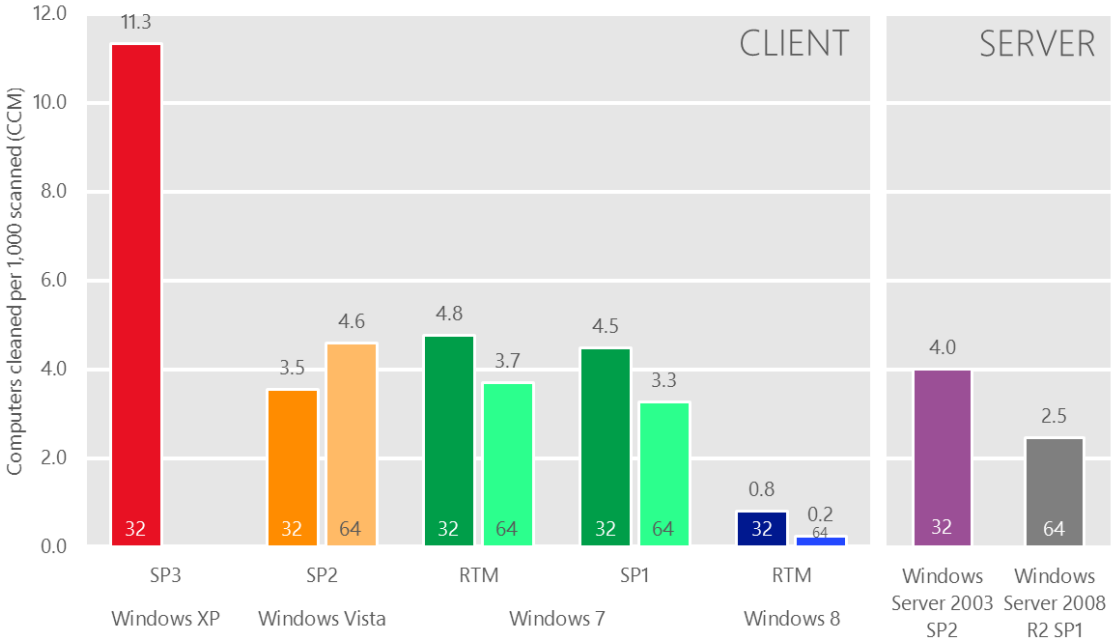


Figure 5. Infection rate (CCM) by operating system and service pack in 4Q12

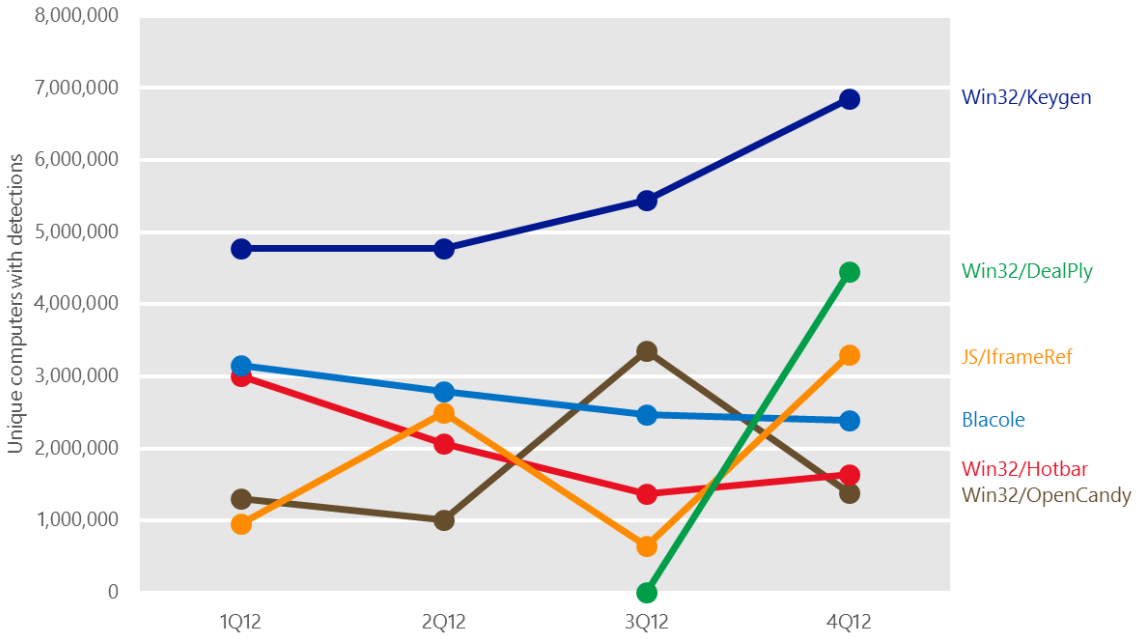


"32" = 32-bit edition; "64" = 64-bit edition. SP = Service Pack. RTM = release to manufacturing. Operating systems with at least 0.1 percent of total MSRT executions in 4Q12 shown.

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).

Threat families

Figure 1. Detection trends for a number of notable families in 2012



- Detections of Win32/Keygen, the most common detection 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.)

Home and enterprise threats

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 also which threats are more likely to succeed in each environment.

- Six families are common to both lists, notably the generic families Win32/Keygen and INF/Autorun 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 adware are typically much more common on non-domain computers than on domain-joined computers. The adware family Win32/DealPly was the second most commonly detected threat family on non-domain computers in 4Q, with another adware family, Win32/Hotbar, ranking 10th. By contrast, none of the top 10 families detected on domain-joined computers were adware families.

Figure 7. Quarterly trends for the top 10 families detected on domain-joined computers in 2H12, by percentage of domain-joined computers reporting detections

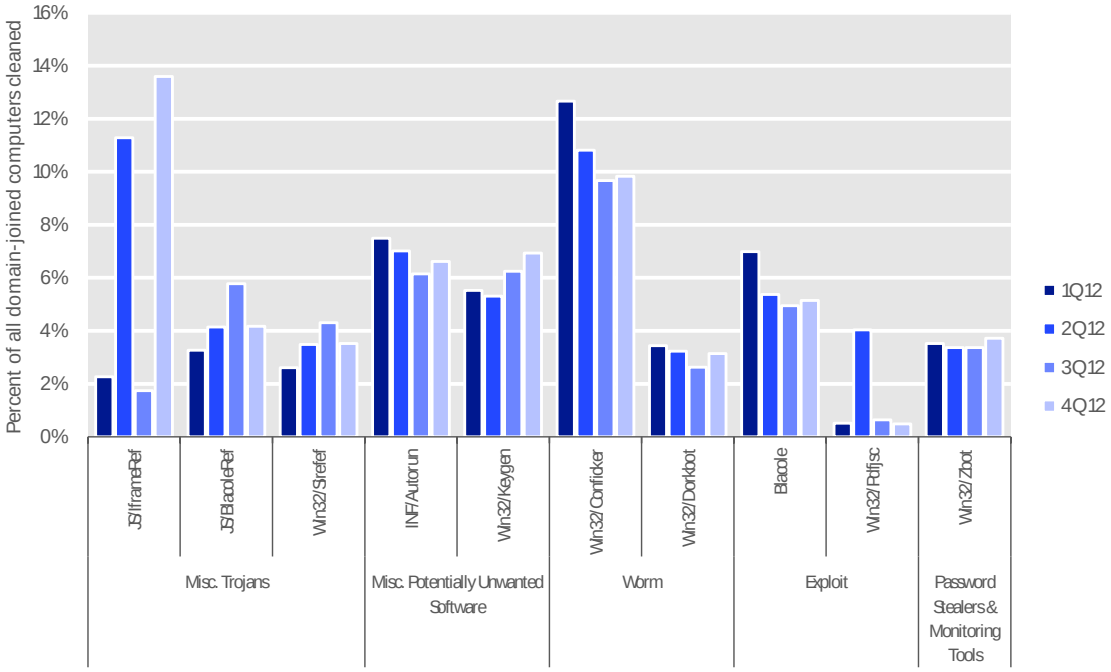
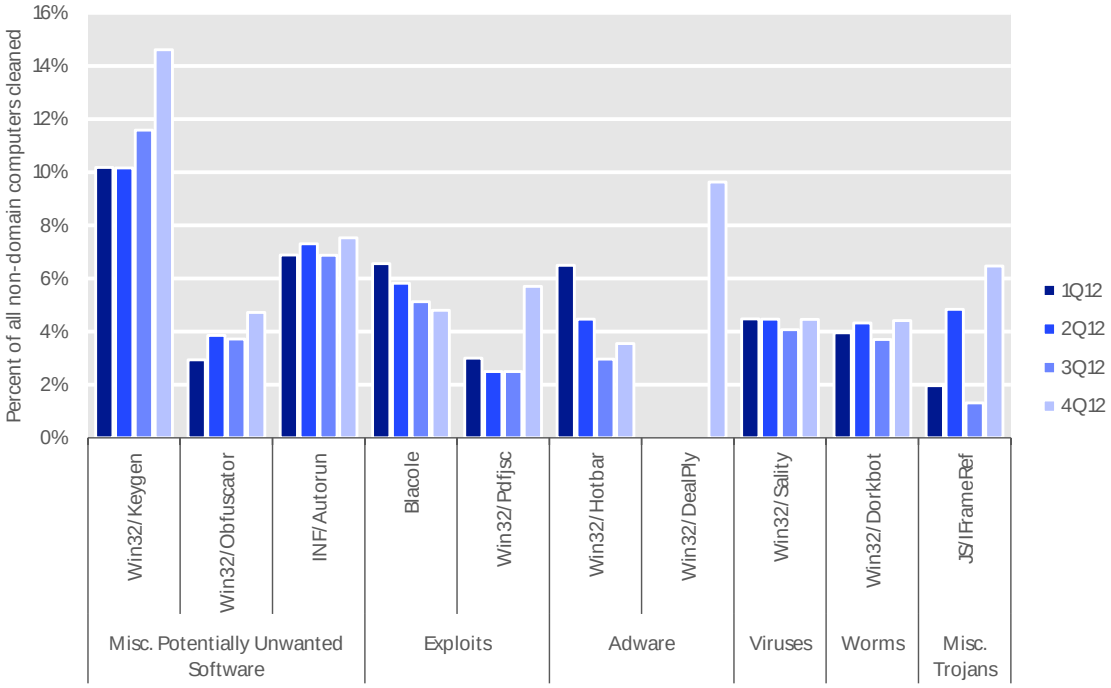


Figure 8. Quarterly trends for the top 10 families detected on non-domain computers in 2H12, by percentage of non-domain computers reporting detections

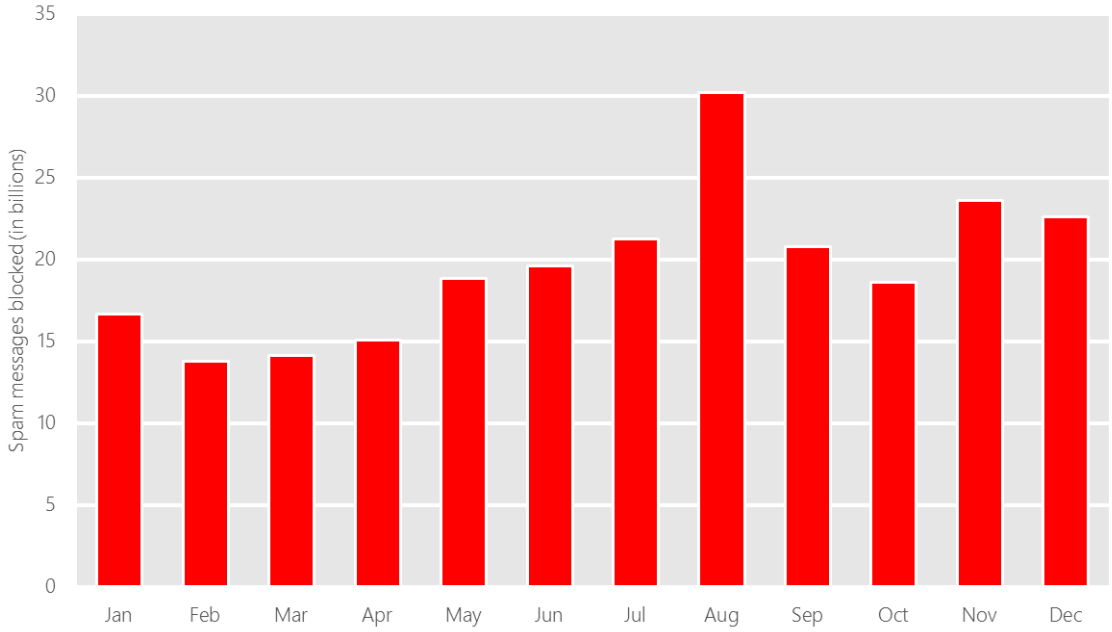


Email threats

Spam messages blocked

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

Figure 9. 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. 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 botnets, notably Cutwail (August 2010) and Rustock (March 2011).[2] 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.

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

Figure 10. Messages blocked by Exchange Online Protection each half-year period, 1H09–2H12

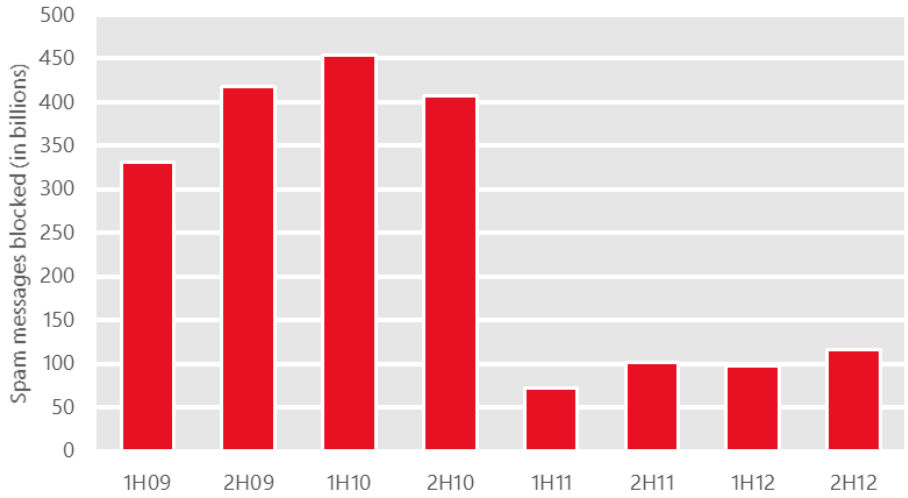
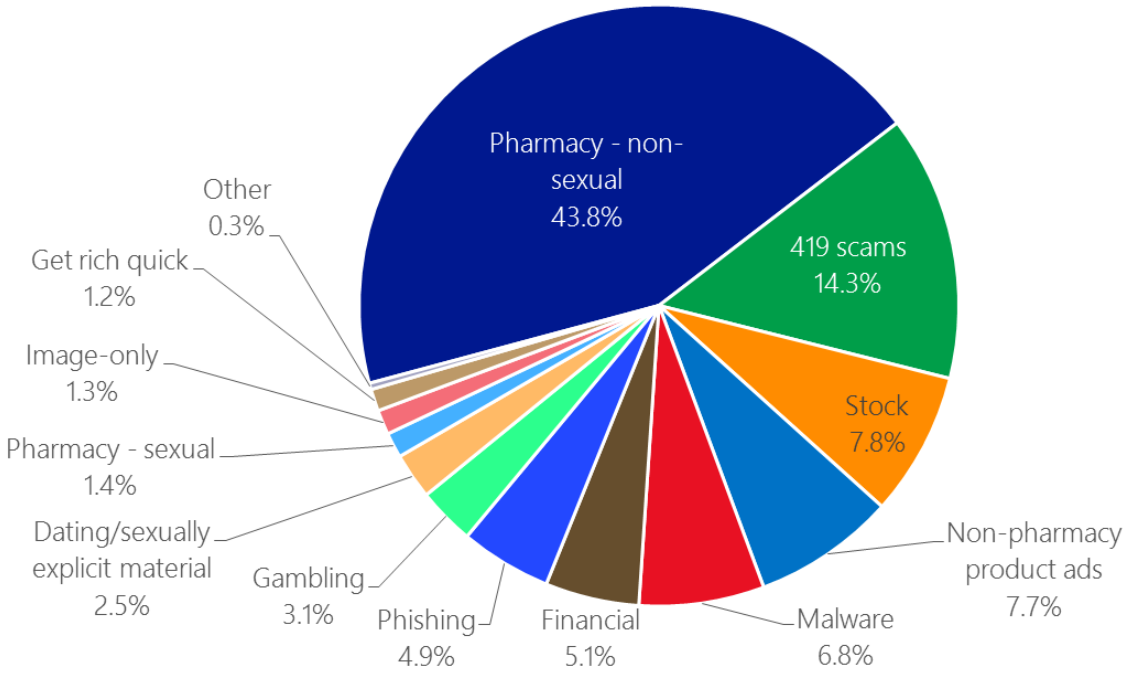


Figure 11.Inbound messages blocked by Exchange Online Protection filters in 2H12, by category



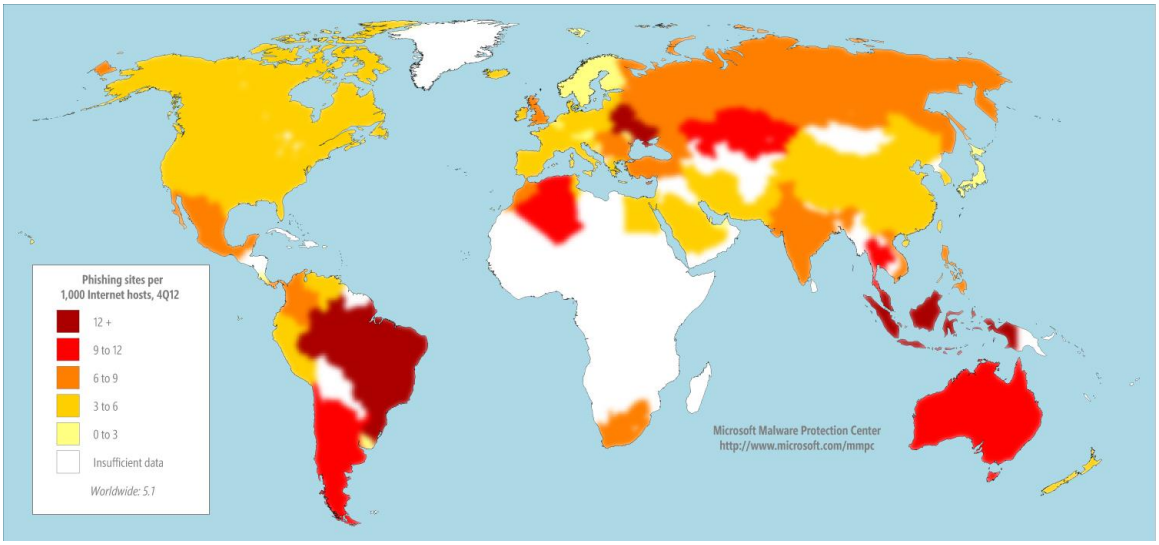
The Exchange Online Protection content filters recognize several different common types of spam messages. Figure 11 shows the relative prevalence of the spam types that were detected in 2H12.

Malicious websites

Phishing sites

Phishing sites are hosted all over the world on free hosting sites, on compromised web servers, and in numerous other contexts.

Figure 12. Phishing sites per 1,000 Internet hosts for locations around the world in 4Q12

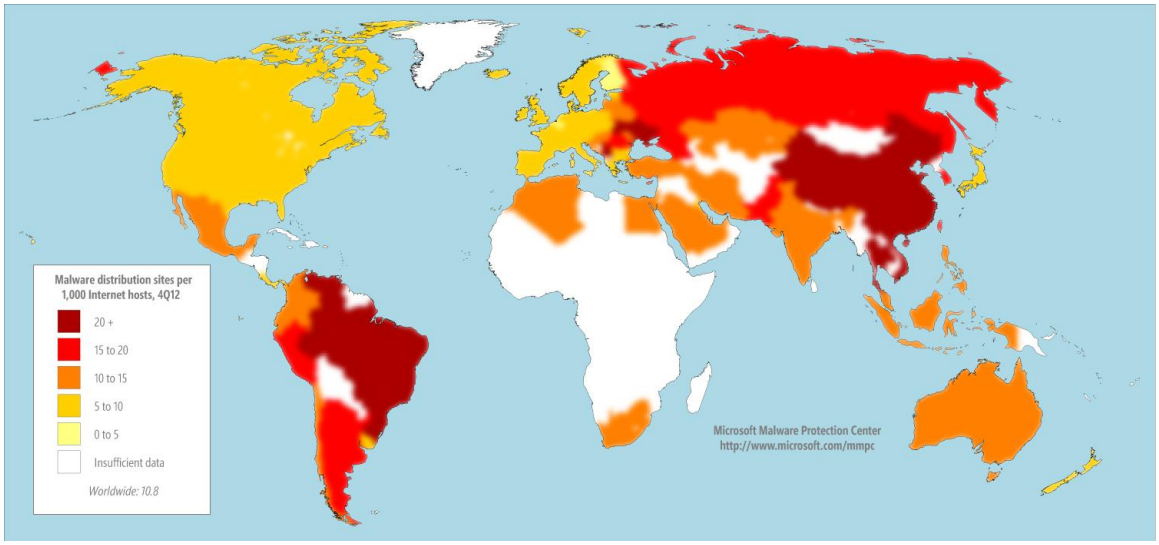


- SmartScreen Filter detected 5.1 phishing sites per 1000 Internet hosts worldwide in 4Q12.
- Locations with higher than average concentrations of phishing sites include Brazil (12.6 per 1000 Internet hosts in 4Q12), Australia (9.1), and Russia (8.3). Locations with low concentrations of phishing sites include Japan (1.8), Finland (1.9), and Sweden (2.8).

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 23. Malware distribution sites per 1,000 Internet hosts for locations around the world in 4Q12



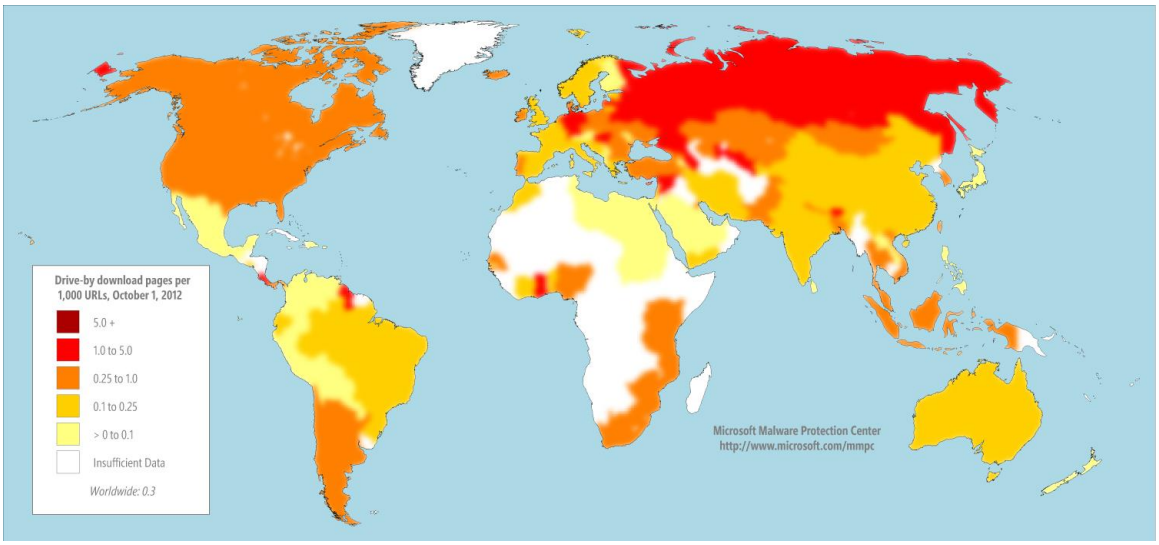
- SmartScreen Filter detected [3]10.8 malware hosting sites per 1,000 Internet hosts worldwide in 4Q12.
- China, which had a lower than average concentration of phishing sites (3.4 phishing sites per 1000 Internet hosts in 4Q12), also had a very high concentration of malware hosting sites (25.1 malware hosting sites per 1,000 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).

[3] 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.

Drive-by download sites

A drive-by download site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything.

Figure 14. Drive-by download pages indexed by Bing at the end of 4Q12, per 1,000 URLs in each country/region



This document summarizes the key findings of the report. The *SIR* website also includes deep analysis of trends found in more than 100 countries/regions around the world and offers suggestions to help manage risks to your organization, software, and people.

You can download *SIRv14* from www.microsoft.com/sir.

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