Microsoft Security Intelligence Report

Volume 10

An in-depth perspective on software vulnerabilities and exploits, malicious code threats, and potentially unwanted software in 2010. With new data covering July through December

Microsoft

Microsoft Security Intelligence Report

Authors

Doug Cavit
Microsoft Trustworthy Computing

Joe Faulhaber
Microsoft Malware Protection Center

Vinny Gullotto
Microsoft Malware Protection Center

Jeff Jones
Microsoft Trustworthy Computing

Jimmy Kuo
Microsoft Malware Protection Center

Michelle Meyer
Microsoft Trustworthy Computing

Daryl Pecelj
Microsoft IT Information Security and Risk Management

Anthony Penta
Microsoft Windows Safety Platform

Tim Rains
Microsoft Trustworthy Computing

Javier Salido
Microsoft Trustworthy Computing

Christian Seifert
Bing

Frank Simorjay
Microsoft Trustworthy Computing

Holly Stewart
Microsoft Malware Protection Center

Matt Thomlinson
Microsoft Security Response Center

Jossie Tirado Arroyo
Microsoft IT Information Security and Risk Management

Scott Wu
Microsoft Malware Protection Center

Jeff Williams
Microsoft Malware Protection Center

Terry Zink
Microsoft Forefront Online Protection for Exchange

Contributors

Lawren Ahuna
Microsoft IT Information Security and Risk Management

Eva Chow
Microsoft IT Information Security and Risk Management

Enrique Gonzalez
Microsoft Malware Protection Center

Cristin Goodwin
Microsoft Legal and Corporate Affairs

Satomi Hayakawa
CSS Japan Security Response Team

Yuhui Huang
Microsoft Malware Protection Center

CSS Japan Security Response Team
Microsoft Japan

John Lambert
Microsoft Security Engineering Center

Eric Leonard
Microsoft IT Information Security and Risk Management

Laura Lemire
Microsoft Legal and Corporate Affairs

Ken Malcolmson
Microsoft Trustworthy Computing

Charles McColgan
Microsoft ISD

Don Nguyen
Microsoft IT Information Security and Risk Management

Price Oden
Microsoft IT Information Security and Risk Management

Kathy Phillips
Microsoft Legal and Corporate Affairs

Hilda Larina Ragragio
Microsoft Malware Protection Center

Tareq Saade
Microsoft Malware Protection Center

Richard Saunders
Microsoft Trustworthy Computing

Marc Seinfeld
Microsoft Malware Protection Center

Jasmine Sesso
Microsoft Malware Protection Center

Norie Tamura (GOMI)
CSS Japan Security Response Team

Gilou Tenebro
Microsoft Malware Protection Center

Table of Contents

About This Report

Scope

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

Reporting Period

In this volume of the *Microsoft Security Intelligence Report*, statistics about malware families and infections are reported on a quarterly basis and other statistics continue to be reported on a half-yearly basis, with a focus on 2010.

Throughout the report, half-yearly and quarterly time periods are referenced using the *n*H*yy* or *n*Q*yy* formats, respectively, where *yy* indicates the calendar year and n indicates the half or quarter. For example, 1H10 represents the first half of 2010 (January 1 through June 30), and 2Q10 represents the second quarter of 2010 (April 1 through June 30). To avoid confusion, please pay attention to 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.

Key Findings Summary

Volume 10 of the *Microsoft® Security Intelligence Report* (*SIRv10*) provides in-depth perspectives on software vulnerabilities, software vulnerability exploits, malicious and potentially unwanted software, and security breaches in both Microsoft and third party software. Microsoft developed these perspectives based on detailed trend analysis over the past several years, with a focus on 2010.

This document summarizes the key findings of the report. The full *SIRv10* also includes deep analysis of trends found in 117 countries/regions around the world and offers ways to manage risks to your organization, software, and people.

The full *SIRv10*, as well as previous volumes of the report and related videos, can be downloaded from www.microsoft.com/sir.

Vulnerability Disclosures

- Vulnerabilities in applications versus operating systems or web browsers continued to account for a large majority of all vulnerabilities in 2010, although the total number of application vulnerabilities declined 22.2 percent from 2009.
- Industry vulnerability disclosure trends continue an overall trend of moderate declines since 2006. This trend is likely because of better development practices and quality control throughout the industry, which result in more secure software and fewer vulnerabilities.
- Vulnerability disclosures for Microsoft products increased slightly in 2010 but have generally remained stable over the past several periods.

Exploits

- The exploitation of Java vulnerabilities sharply increased in the third quarter of 2010 and surpassed every other exploitation category that the

MMPC tracks, including generic HTML/scripting exploits, operating system exploits, and document exploits.

- Exploits that use HTML and JavaScript steadily increased throughout the year and continue to represent a large portion of exploits. The most prevalent type of attack in this category involved malicious IFrames.
- The number of Adobe Acrobat and Adobe Reader exploits dropped by more than half after the first quarter and remained near this reduced level throughout the remainder of the year.

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.

Operating System Infection Rates

- As in previous periods, infection rates for more recently released Microsoft operating systems and service packs are consistently lower than older ones, for both client and server platforms. Windows 7 and Windows Server 2008 R2, the most recently released Windows client and server versions, respectively, have the lowest infection rates.

- Infection rates for the 64-bit versions of Windows Vista® and Windows 7 are lower than for the corresponding 32-bit versions of those operating systems. One reason may be that 64-bit versions of Windows still appeal to a more technically savvy audience than their 32-bit counterparts, despite increasing sales of 64-bit Windows versions among the general computing population. Kernel Patch Protection (KPP), a feature of 64-bit versions of Windows that protects the kernel from unauthorized modification, may also contribute to the difference by preventing certain types of malware from operating.

Threat Families

- JS/Pornpop, the most commonly detected family in 4Q10, is a detection for specially crafted JavaScript-enabled objects that attempt to display

pop-under advertisements in users' web browsers, usually with adult content.

- Detections and removals of Win32/Autorun, a generic detection for worms that spread between mounted volumes using the Autorun feature of Windows, increased significantly in 4Q10, although Autorun dropped to second place because of the spread of Pornpop.

- Win32/Taterf, the most prevalent threat in 2Q10, dropped to third by 4Q10. Taterf belongs to a category of threats that are designed to steal passwords for popular online computer games and transmit them to the attackers. See "Online Gaming-Related Families" on page 62 of *Microsoft Security Intelligence Report, Volume 5 (January through June 2008)* for more information about these threats.

Home and Enterprise Threats

- Seven malware families are common to home and enterprise network environments, although they are ordered differently and in different proportions. The worm family Win32/Conficker, which uses several methods of propagation that work more effectively within a typical enterprise network environment than they do over the public Internet, leads the domain-joined list by a significant margin, but ranks ninth on the non-domain list.

- On non-domain computers, JS/Pornpop was the most commonly detected family in 4Q10 and the fourth most commonly detected family in 2010 overall. By contrast, this family was detected much less often on domain-joined computers. Pornpop is often found on websites that host illegal or illicit content, which users in domain environments are often restricted from accessing by organizational policy or blocking software.

Email Threats

- After increasing gradually and then reaching a plateau through the first eight months of 2010, the number of spam messages received and blocked by Microsoft Forefront® Online Protection for Exchange (FOPE) dropped abruptly in September, and again in December. These

drops can be correlated with events involving two of the world's most significant spam-sending botnets:

- During the last week of August 2010, researchers affiliated with the security firm LastLine spearheaded a coordinated takedown of command-and-control (C&C) servers associated with the Win32/Cutwail spambot. In the days following the takedown, FOPE recorded a significant drop in the average daily volume of messages blocked.

- On or about December 25, 2010, spam researchers around the world recorded an almost complete cessation of spam originating from the large Rustock botnet, with some spam trackers reporting a drop in the global spam rate as high as 50 percent or more. During the final week of December, the number of messages blocked by FOPE was almost 30 percent less than in the prior week, compared to a drop of less than two percent between the final two weeks of 2009. The Rustock botnet subsequently began sending spam again in mid-January, and the number of messages blocked by FOPE has risen accordingly. The reasons for this hiatus are still being investigated.

Spam Types

- Advertisements for nonsexual pharmaceutical products accounted for 32.4 percent of the spam messages blocked by FOPE content filters in 2010.

- Together with nonpharmaceutical product ads (18.3 percent of the total) and advertisements for sexual performance products (3.3 percent), product advertisements accounted for 54.0 percent of spam in 2010, which is down from 69.2 percent a year ago.

Malicious Websites

- In the first half of 2010, phishers showed signs of targeting online gaming sites with increasing frequency, although this push appeared to have dwindled as social networks came under increased attack. Impressions that targeted gaming sites reached a high of 16.7 percent of

all impressions in June before dropping to a more typical 2.1 percent in December.

- Phishing sites that target social networks routinely receive the highest number of impressions per active phishing site. The percentage of active phishing sites that targeted social networks increased during the final months of the year, but still only accounted for 4.2 percent of active sites in December, despite receiving 84.5 percent of impressions that month. Nevertheless, the number of active sites targeting gaming sites remained relatively high during the second half of the year, which suggests that more campaigns may be coming.

Trustworthy Computing: Security Engineering at Microsoft

Amid the increasing complexity of today's computing threat landscape and the growing sophistication of criminal attacks, enterprises and governments are more focused than ever on protecting their computing environments so that they and their constituents can feel 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.

Trustworthy Computing (TwC), formed in 2002, is Microsoft's commitment to creating and delivering secure, private, and reliable computing experiences based on sound business practices. The intelligence provided in this report comes from Trustworthy Computing security centers that deliver in-depth threat intelligence, threat response, and security science, as well as information from product groups across Microsoft. The report is designed to give our customers, partners, and the industry a better understanding of the threat landscape so that they will be in a better position to protect themselves and their assets from criminal activity.

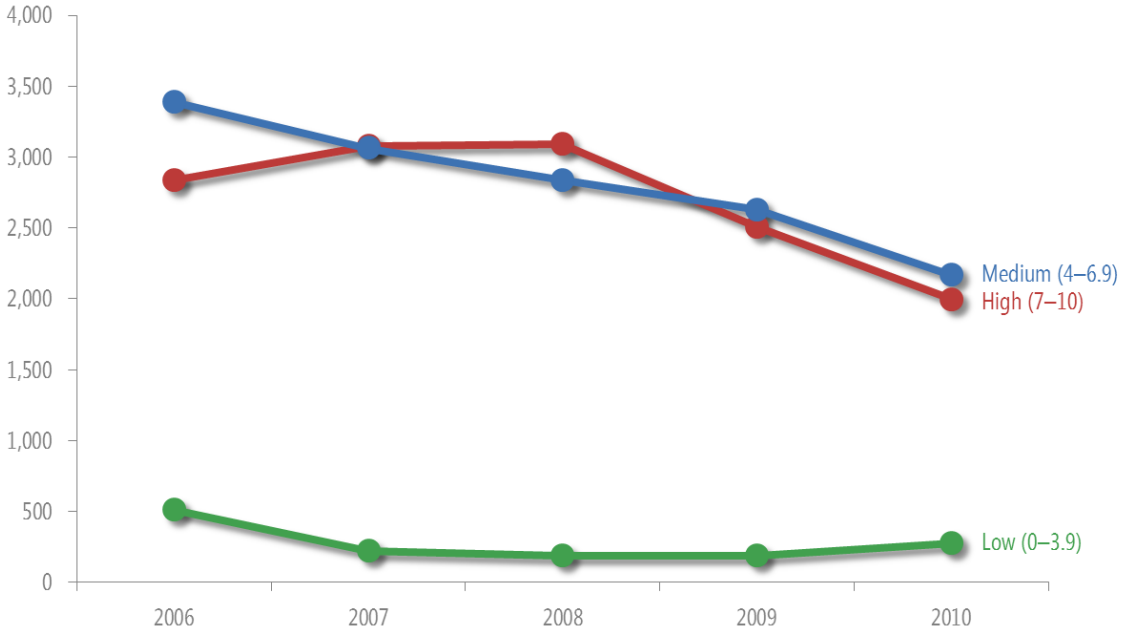
Vulnerabilities

Vulnerabilities are weaknesses in software that enable an attacker to compromise the integrity, availability, or confidentiality of that software or the data it processes. Some of the worst vulnerabilities allow attackers to run arbitrary code, called *exploits*, on the compromised system. See Industry-Wide Vulnerability Reports in the "Reference Guide" section of the *Security Intelligence Report* website for more information about vulnerabilities.

Vulnerability Severity

The Common Vulnerability Scoring System (CVSS) is a standardized, platform-independent scoring system for rating IT vulnerabilities. The CVSS assigns a numeric value between 0 and 10 to vulnerabilities according to severity, with higher scores representing greater severity. (See Vulnerability Severity in the "Reference Guide" section of the *Security Intelligence Report* website for more information.)

Figure 1. Industry-wide vulnerability disclosures by severity, 2006–2010

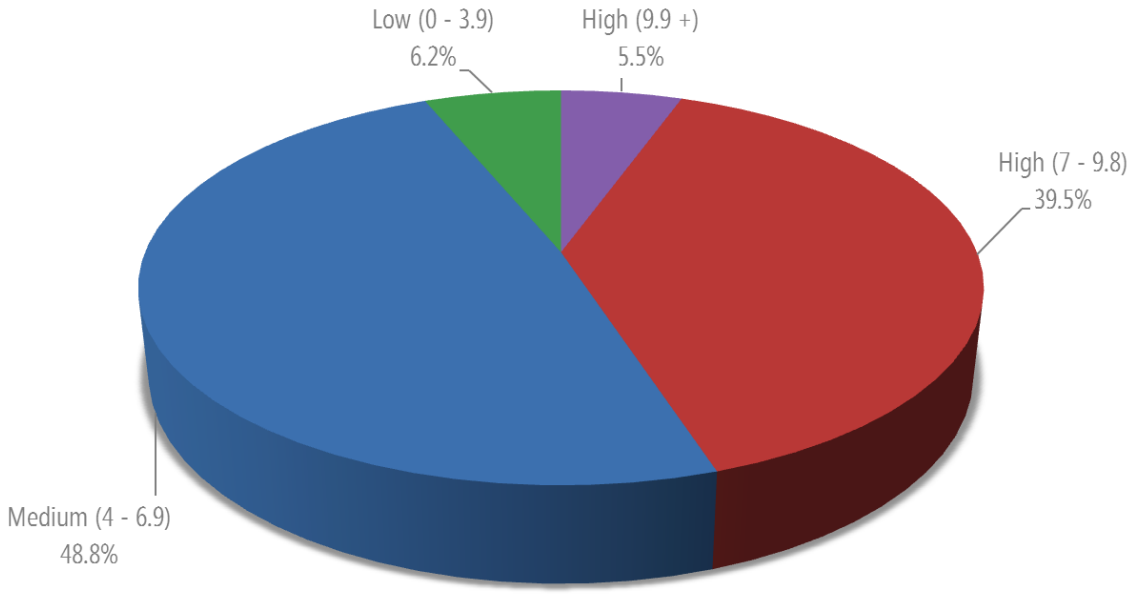


- Although the number of Medium and High severity vulnerabilities disclosed is routinely much greater than the number of Low severity vulnerability disclosures, the trend in 2010 is a positive one, with Medium and High disclosures declining by 17.5 percent and 20.2 percent from 2009, respectively.

- Low severity vulnerability disclosures increased 45.8 percent, from 190 in 2009 to 277 in 2010.

- Mitigating the most severe vulnerabilities first is a security best practice. High severity vulnerabilities that scored 9.9 or greater represent 5.5 percent of all vulnerabilities disclosed in 2010, as Figure 2 illustrates. This percentage is down from 6.7 percent in 2009.

Figure 2. Industry-wide vulnerability disclosures in 2010, by severity

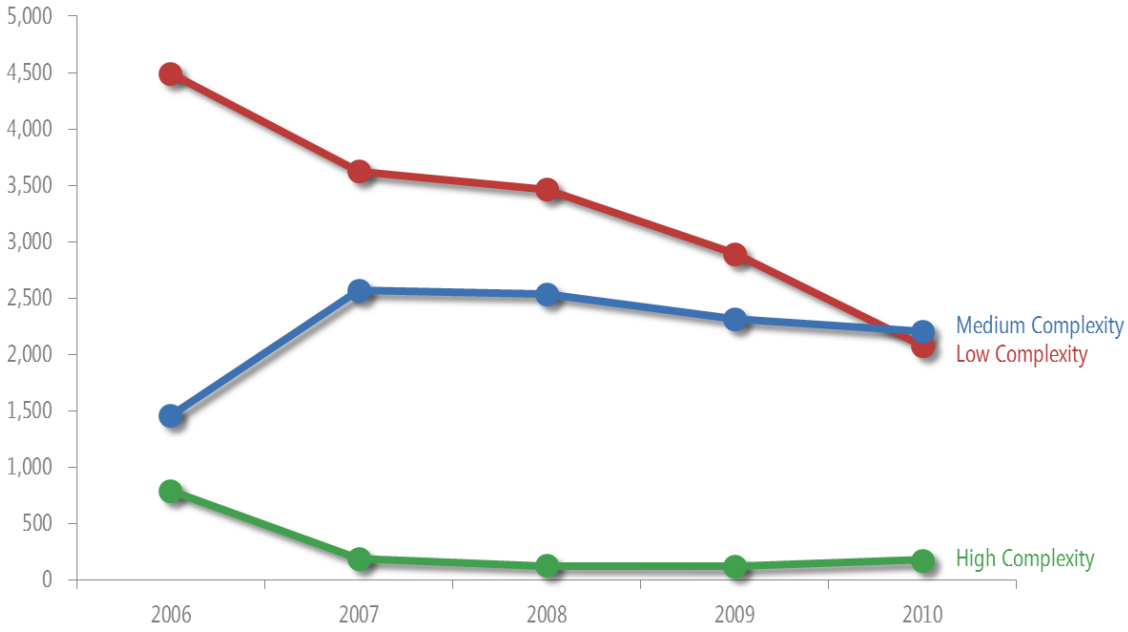


Vulnerability Complexity

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 gives each vulnerability a complexity ranking of Low, Medium, or High. (See Vulnerability Complexity in the "Reference Guide" section of the *Security Intelligence Report* website for more information about the CVSS complexity ranking system.) Figure 3 shows the complexity mix for vulnerabilities disclosed each year since 2006. Note that Low complexity indicates greater danger, just as High severity indicates greater danger in Figure 2.

Figure 3. Industry-wide vulnerabilities by access complexity, 2006–2010



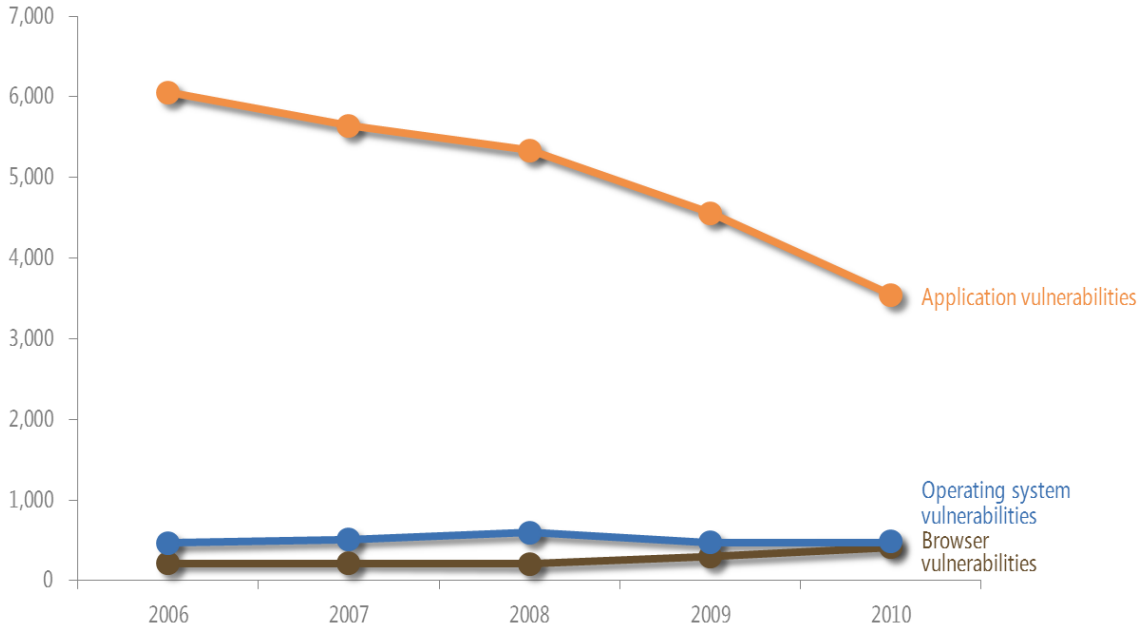
- As with vulnerability severity, the trend here is a positive one, with Low and Medium complexity vulnerability disclosures declining 28.3 percent and 5.0 percent from 2009, respectively.

- High complexity vulnerability disclosures increased 43.3 percent, from 120 in 2009 to 172 in 2010.

Operating System, Browser, and Application Vulnerabilities

Figure 4 shows industry-wide vulnerabilities for operating systems, browsers, and applications since 2006. (See Operating System, Browser, and Application Vulnerabilities in the "Reference Guide" section of the *Security Intelligence Report* website for an explanation of how operating system, browser, and application vulnerabilities are distinguished.)

Figure 4. Industry-wide operating system, browser, and application vulnerabilities, 2006–2010



- Application vulnerabilities continued to account for a large majority of all vulnerabilities in 2010, although the total number of application vulnerabilities declined 22.2 percent from 2009.

- Operating system and browser vulnerabilities remained relatively stable by comparison, with each type accounting for a small fraction of the total.

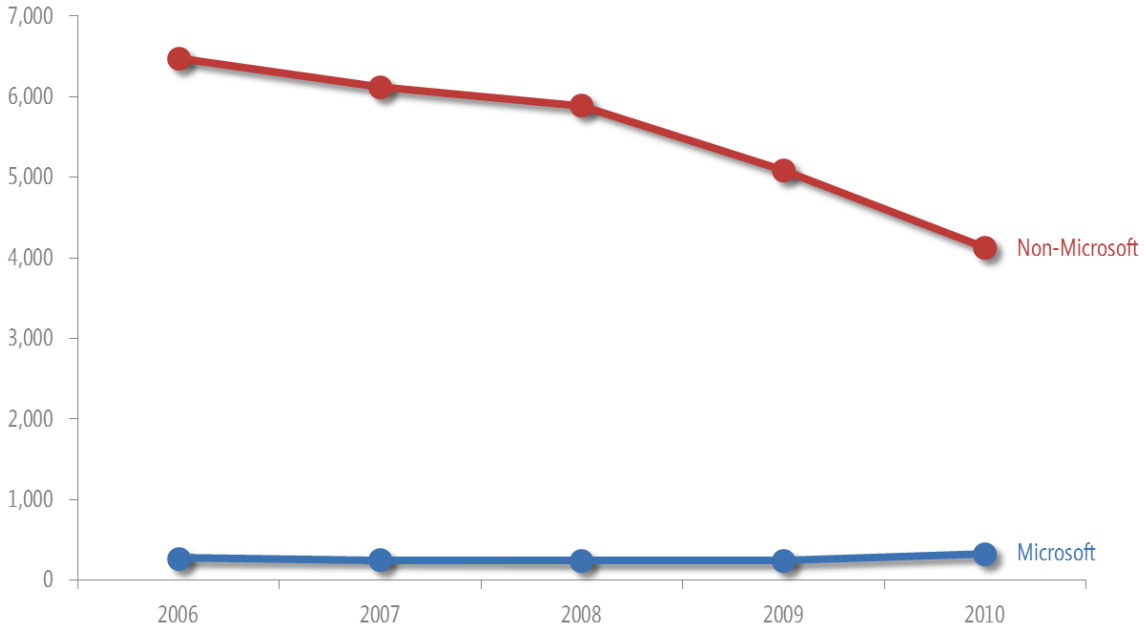
Vulnerability Disclosures

A *disclosure*, as the term is used in the *SIR*, is the revelation of a software vulnerability to the public at large. It does not refer to any sort of private disclosure or disclosure to a limited number of people. Disclosures can come from a variety of sources, including the software vendor itself, 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 (http://nvd.nist.gov), the U.S. government repository of standards-based vulnerability management.

Figure 5 charts vulnerability disclosures for Microsoft and non-Microsoft products since 2006.

Figure 5. Vulnerability disclosures for Microsoft and non-Microsoft products, 2006–2010



- Vulnerability disclosures across the industry were down 16.5 percent in 2010 from 2009.
- This decline continues an overall trend of moderate declines since 2006. This trend is likely because of better development practices and quality control throughout the industry, which result in more secure software and fewer vulnerabilities. (See Protecting Your Software in the "Managing Risk" section of the *Security Intelligence Report* website for additional details and guidance about secure development practices.)
- Vulnerability disclosures for Microsoft products increased slightly in 2010 but have generally remained stable over the past several periods.
- Vulnerabilities in Microsoft products accounted for 7.2 percent of all vulnerabilities disclosed in 2010. This percentage is up from 4.5 percent in 2009, primarily because of the overall decline in vulnerability disclosures across the industry during that time.

Exploits

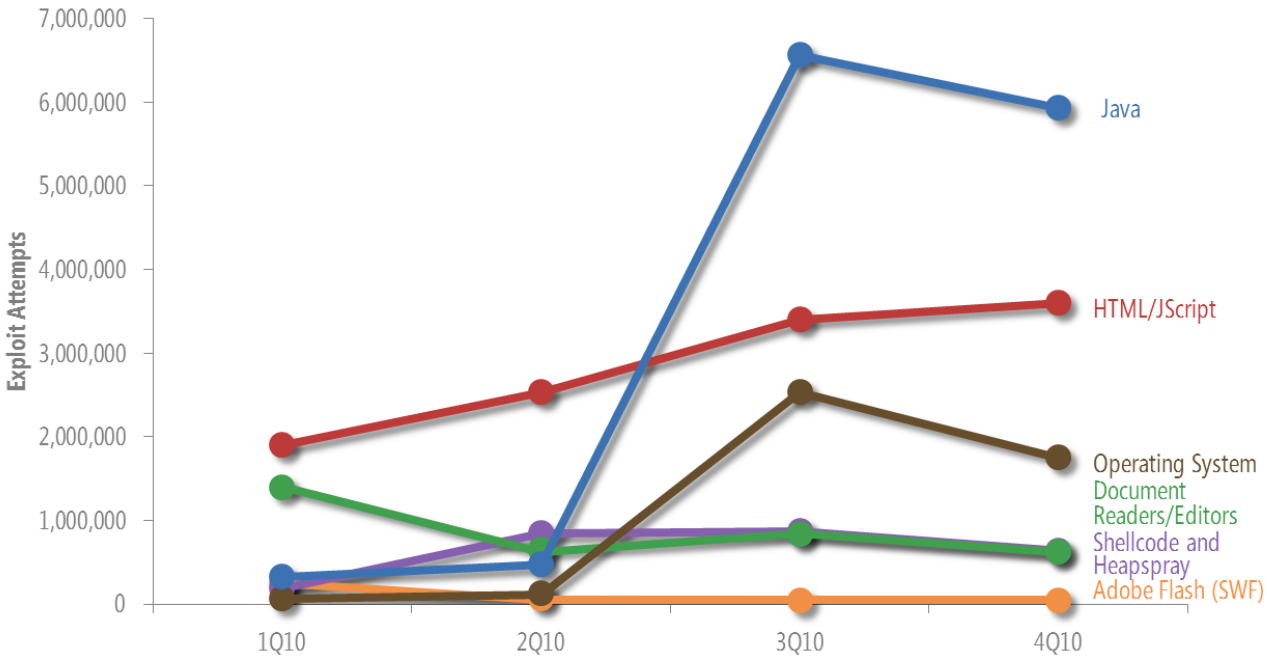
An *exploit* is malicious code that takes advantage of software vulnerabilities to infect a computer, without the user's consent and usually without the user's knowledge. Exploits target vulnerabilities in the operating system, web browsers, applications, or software components that are installed on 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. 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.

Software vulnerabilities are enumerated and documented in the Common Vulnerabilities and Exposures list (CVE) (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.[1]

Figure 6 shows the prevalence of different types of exploits for each quarter in 2010.

[1] See www.microsoft.com/technet/security/Current.aspx to search and read Microsoft Security Bulletins.

Figure 6. Exploits detected by Microsoft desktop antimalware products in 2010, by targeted platform or technology



- Malware written in Java has existed for many years, but attackers had not focused significant attention on exploiting Java vulnerabilities until somewhat recently. In 3Q10, the number of Java attacks increased to fourteen times the number of attacks recorded in 2Q10, driven mostly by the exploitation of a pair of vulnerabilities in versions of the Sun (now Oracle) JVM, CVE-2008-5353 and CVE-2009-3867. Together, these two vulnerabilities accounted for 85 percent of the Java exploits detected in the second half of 2010.

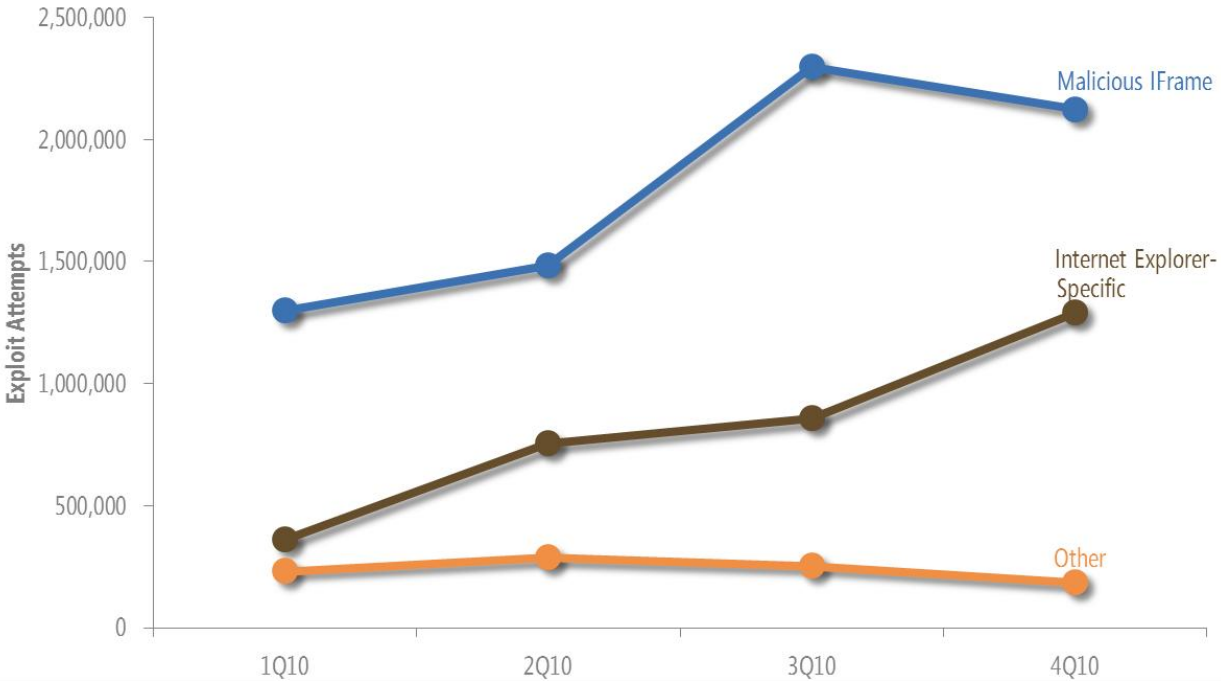
- Exploits that target document editors and readers, such as Microsoft® Word and Adobe Reader, declined in 2Q10 and remained at a lower level thereafter.

- Operating system exploits, which have been less prevalent than other types of exploits for several years, increased significantly in 3Q10, primarily because of exploitation of two Windows® vulnerabilities.

HTML and JScript/JavaScript Exploits

Figure 7 shows the prevalence of different types of HTML and Jscript®/JavaScript exploits each quarter in 2010.

Figure 7. Types of HTML and JScript/JavaScript exploits detected by Microsoft desktop antimalware products in 2010



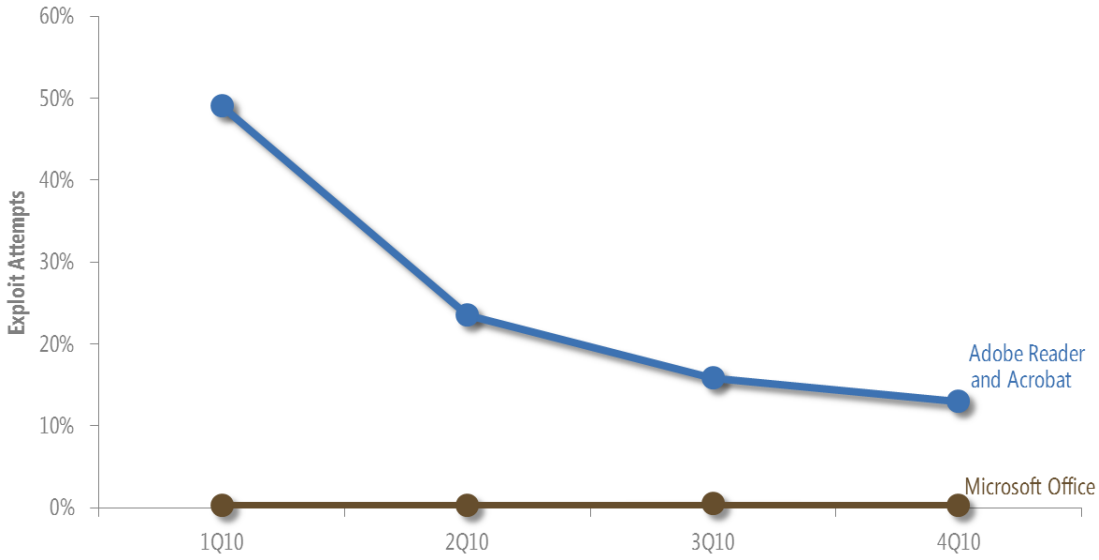
- Most of the exploits observed involved malicious HTML inline frames (IFrames) that surreptitiously open pages hosting malicious code in users' web browsers.

- Exploits that target Windows Internet Explorer® vulnerabilities accounted for between 19 and 36 percent of HTML-related exploits each quarter. Most of these exploits targeted CVE-2010-0806, a vulnerability that affects Internet Explorer versions 6 and 7 running on versions of Windows earlier than Windows 7 and Windows Server 2008 R2. Microsoft has issued Security Bulletin MS10-018 to address this vulnerability. For more information, see the post "Active Exploitation of CVE-2010-0806" (March 30, 2010) on the MMPC blog (http://blogs.technet.com/mmpc).

Document Exploits

Figure 8 shows the prevalence of different types of document format exploits by quarter in 2010.[2]

Figure 8. Types of document exploits detected by Microsoft desktop antimalware products in 2010



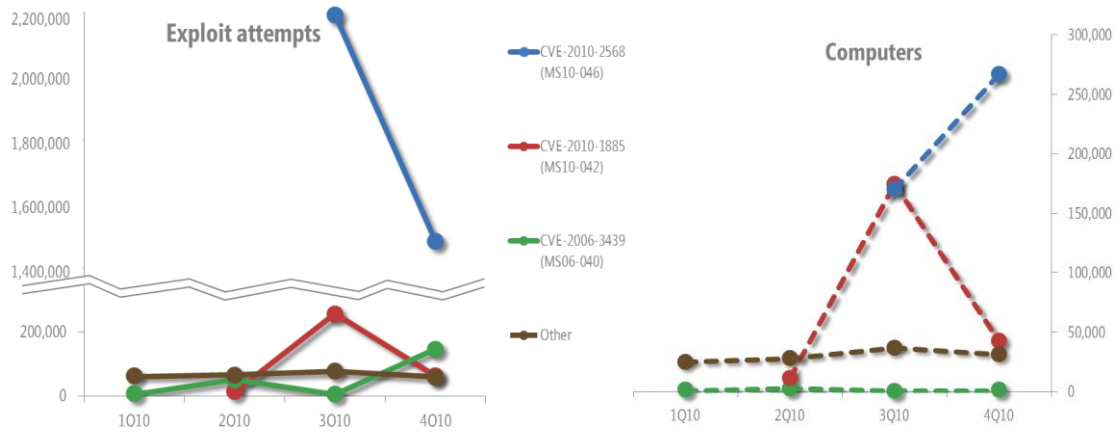
- Exploits that affected Adobe Acrobat and Adobe Reader accounted for most document format exploits detected throughout 2010. Almost all of these exploits involved the generic exploit family Win32/Pdfjsc.
- Adobe Acrobat and Adobe Reader exploits dropped by more than half after the first quarter and remained near this reduced level throughout the remainder of the year.
- Microsoft Office file format exploits accounted for between 0.5 and 2.8 percent of the document format exploits that were detected each quarter in 2010.

[2] Microsoft also detected a very small number of exploits that affect JustSystems Ichitaro, a Japanese-language word processing program. These exploits affected fewer than 200 computers each quarter and are not shown in the figure.

Operating System Exploits

Figure 9 shows the prevalence of different operating system exploits by quarter in 2010.

Figure 9. Operating system exploits detected by Microsoft desktop antimalware products in 2010



- Several of the operating system exploits with the most detections in 2010 were caused by worms that spread in ways that result in large numbers of detections on each computer they try to infect. Figure 9 provides another perspective on these statistics, and shows the number of individual computers that reported exploit attempts for several of these exploits, in addition to the total number of detections.

- Operating system exploits had been declining for several years prior to 2010, and detections numbered less than 200,000 in each of the first two quarters of the year. This decline changed in 3Q10 with the discovery and publication of two *zero-day exploits* (exploits that take advantage of undisclosed or newly disclosed vulnerabilities before the vendor releases security updates for them) for two vulnerabilities that affect Windows, CVE-2010-1885 and CVE-2010-2568.

- CVE-2010-1885 is a vulnerability that affects the Windows Help and Support Center in Windows XP and Windows Server® 2003. Details of the vulnerability were made public on June 10, 2010, about three weeks before the end of the second quarter, and Microsoft issued an "out-of-band" Security Bulletin, MS10-042, to address the vulnerability on July 13.

Microsoft detected a relatively small number of exploits targeting CVE-2010-1885 (fewer than 14,000 worldwide) in 2Q10, followed by a steep rise to more than 250,000 detections in the third quarter. By the end of the year, exploitation had declined significantly, with fewer than 65,000 detections in 4Q10.

For additional information, see the post Attacks on the Windows Help and Support Center Vulnerability (CVE-2010-1885) (June 30, 2010) on the MMPC blog, http://blogs.technet.com/mmpc.

- CVE-2010-2568 is a vulnerability that involves the way Windows Shell handles shortcut files. This vulnerability was first discovered in mid-July 2010 following analysis of the Win32/Stuxnet worm, which uses the vulnerability as a means of propagation. Microsoft issued an out-of-band Security Bulletin, MS10-046, to address the vulnerability on August 2. Initially, Stuxnet was the only family found to be making significant use of CVE-2010-2568 exploits, but detections and removals rose as authors of other malware families, including Win32/Vobfus and Win32/Sality, began releasing new variants that exploited the vulnerability. For additional information, see the post Stuxnet, malicious .LNKs, ...and then there was Sality (July 30, 2010) on the MMPC blog, http://blogs.technet.com/mmpc.

  CVE-2010-2568 exploits affected about as many computers in 3Q10 as CVE-2010-1885 exploits, but the number of detections per infected computer was much higher (12.9 detections per infected computer, compared to 1.5 for CVE-2010-1885). The Stuxnet worm uses USB storage devices as its primary transmission vector, and the nature of the shortcut vulnerability caused some computers to log large numbers of detections as the Windows Shell repeatedly attempted to process the same malicious shortcut file.

- CVE-2006-3439 is a vulnerability that affects the Server service in Windows 2000, pre-Service Pack 3 versions of Windows XP, and pre-Service Pack 2 versions of Windows Server 2003. Microsoft issued Security Bulletin MS06-040 to address the vulnerability in August 2006.

  In this case, although Microsoft detected significant numbers of infection attempts targeting CVE-2006-3439, the actual number of computers involved was quite small (fewer than 3,000 worldwide each quarter). Exploits targeting network services, such as the Server service, can generate large numbers of detections by real-time antimalware products:

a worm traversing a network may make repeated attempts to infect an individual computer using the exploit, with each unsuccessful attempt logged as a separate detection.

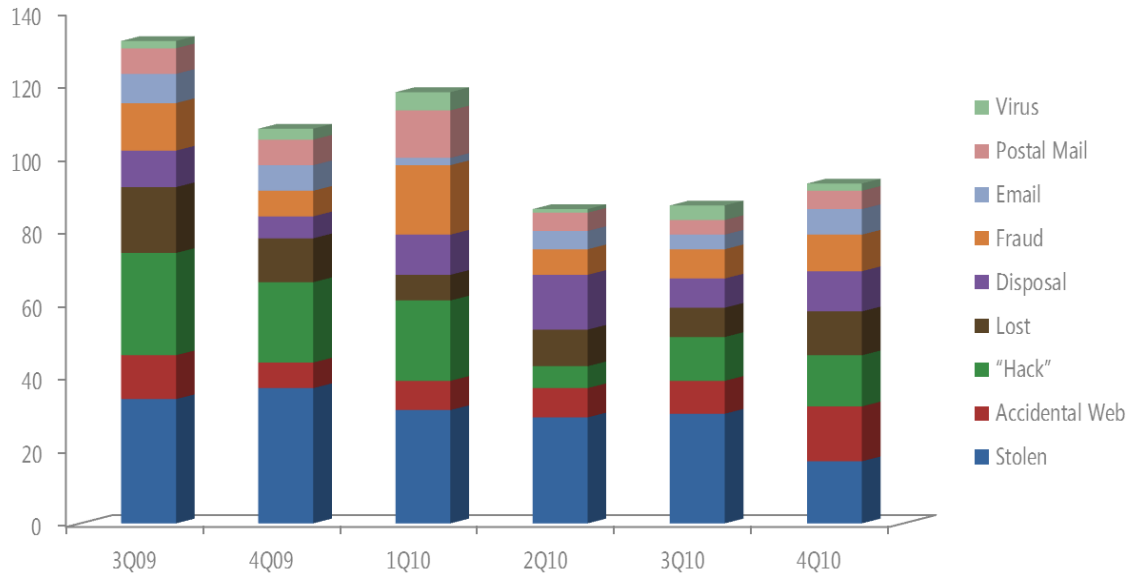
In general, successful exploitation of operating system vulnerabilities as old as CVE-2006-3439 should be rare, as most of the Windows installations that were initially affected have since been updated with the appropriate security updates or service packs or replaced by newer versions of Windows that are not affected by the vulnerability. In 2010, detections of CVE-2006-3439 exploits were strongly correlated with detections of the uncommon Trojan family Win32/ServStart, suggesting a possible connection between the two.

Security Breach Trends

In recent years, laws have been passed in a number of jurisdictions around the world that require affected individuals to be notified when an organization loses control of personally identifiable information (PII) with which it has been entrusted. These mandatory notifications offer unique insights into how information security efforts need to address issues of negligence as well as technology.

The information in this section was generated from worldwide data security breach reports from news media outlets and other information sources that volunteers have recorded in the Data Loss Database (DataLossDB) at http://datalossdb.org. (See Security Breach Trends in the "Reference Guide" section of the *Security Intelligence Report* website for more information about the DataLossDB and the breach types referenced here.)

Figure 10. Security breach incidents by incident type, 3Q09–4Q10

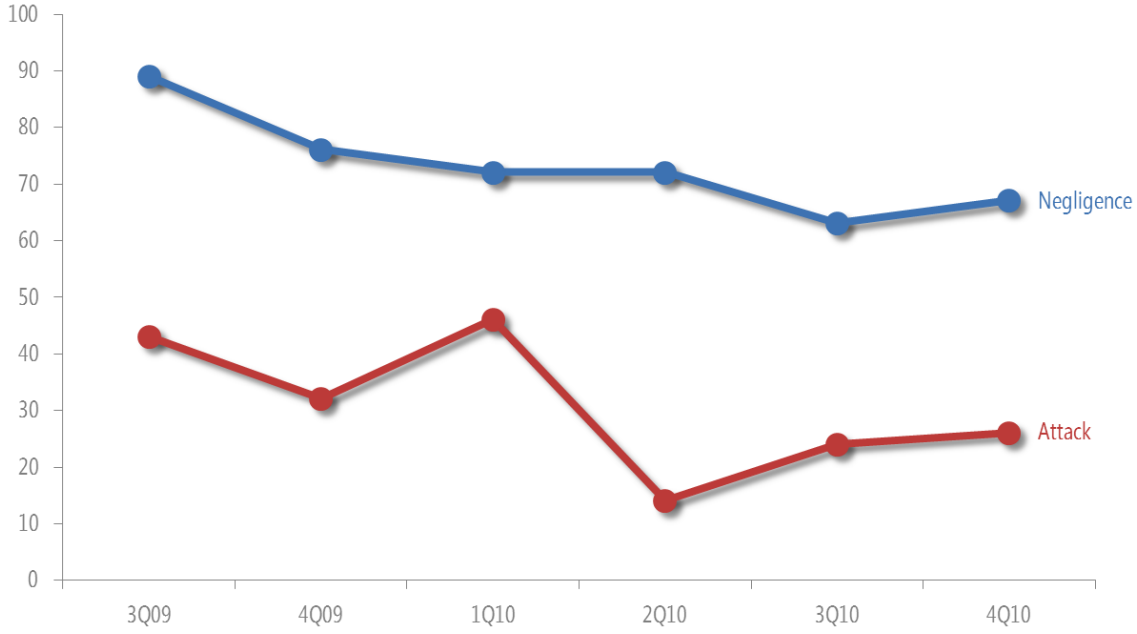


- The largest single category of incidents in each of the past six quarters involved stolen equipment, ranging from a high of 34.5 percent of the total in 3Q09 to a low of 18.6 percent of the total in 4Q10.

- Malicious incidents (those involving "hacking" incidents, malware, and fraud) routinely account for less than half as many incidents as negligence (involving lost, stolen, or missing equipment; accidental disclosure; or improper disposal), as Figure 11 illustrates.

- Improper disposal of business records accounts for a significant portion of incidents and is relatively easy for organizations to address by developing and enforcing effective policies regarding the destruction of paper and electronic records that contain sensitive information.

Figure 11. Breach incidents resulting from attacks and negligence, 3Q09–4Q10



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 Internet online services. (See "Appendix B: Data Sources" on page 71 for more information about the telemetry used in this report.)

Global Infection Rates

The telemetry data generated by Microsoft® security products from users who choose to opt in to data collection includes information about the location of the computer, as determined by the setting of the **Location** tab or menu in **Regional and Language Options** in Control Panel. This data makes it possible to compare infection rates, patterns, and trends in different locations around the world.

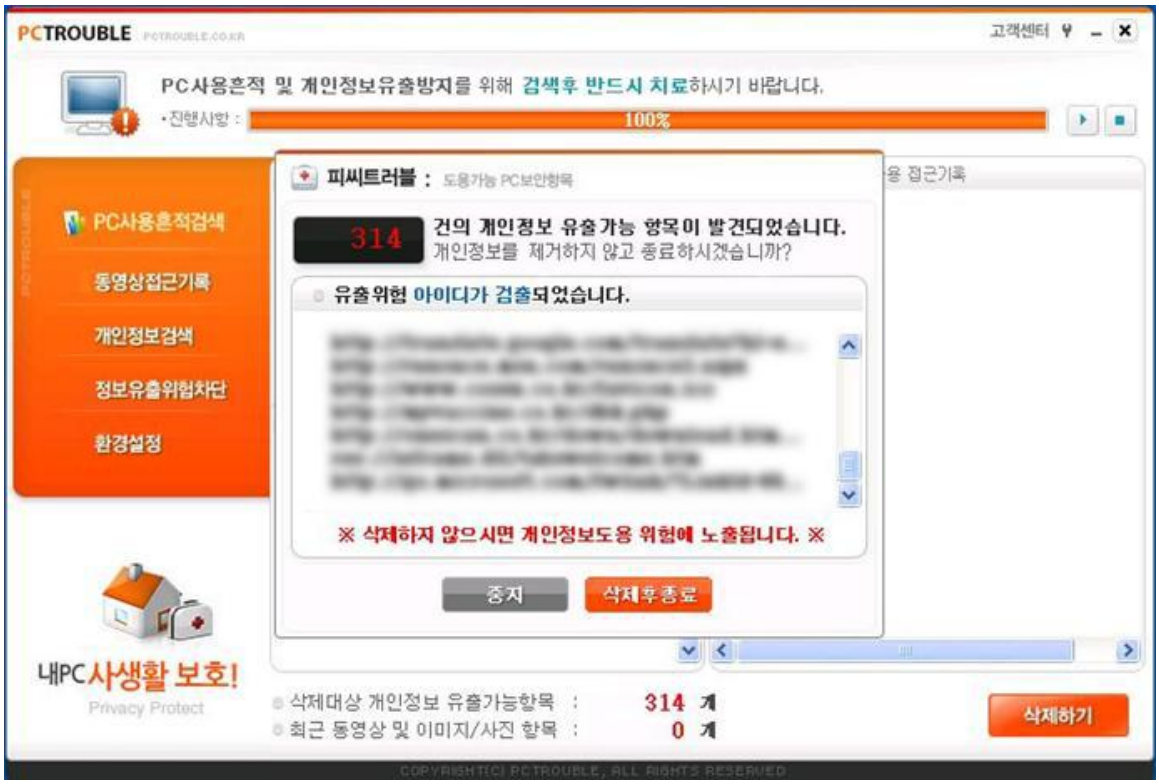
Figure 12. The locations with the most computers reporting detections and removals by Microsoft desktop antimalware products in 2010

	Country/Region	1Q10	2Q10	3Q10	4Q10	Chg. 3Q to 4Q
1	United States	11,025,811	9,609,215	11,340,751	11,817,437	4.2% ▲
2	Brazil	2,026,578	2,354,709	2,985,999	2,922,695	-2.1% ▼
3	China	2,168,810	1,943,154	2,059,052	1,882,460	-8.6% ▼
5	United Kingdom	1,490,594	1,285,570	1,563,102	1,857,905	18.9% ▲
4	France	1,943,841	1,510,857	1,601,786	1,794,953	12.1% ▲
7	Korea	962,624	1,015,173	1,070,163	1,678,368	56.8% ▲
6	Spain	1,358,584	1,348,683	1,588,712	1,526,491	-3.9% ▼

	Country/Region	1Q10	2Q10	3Q10	4Q10	Chg. 3Q to 4Q
9	Russia	700,685	783,210	928,066	1,311,665	41.3% ▲
8	Germany	949,625	925,332	1,177,414	1,302,406	10.6% ▲
10	Italy	836,593	794,099	900,964	998,458	10.8% ▲

- Detections in Korea rose 56.8 percent from 3Q10 to 4Q10, with three families—Win32/Onescan, Win32/Parite, and Win32/Nbar—representing 77 percent of the 3Q–4Q increase. Onescan, a Korean-language rogue security software family first detected in 4Q10, was itself responsible for about 32 percent of all detections in Korea. (For more information, see "Rogue Security Software" on page 41.)

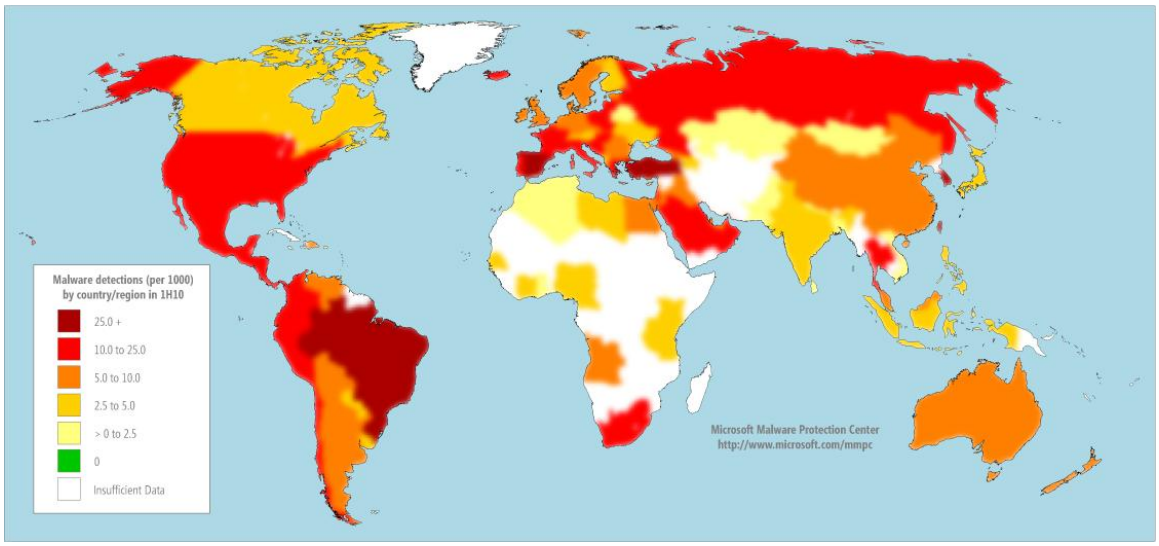
Figure 13. False malware detections by Win32/Onescan, a Korean-language rogue security software family



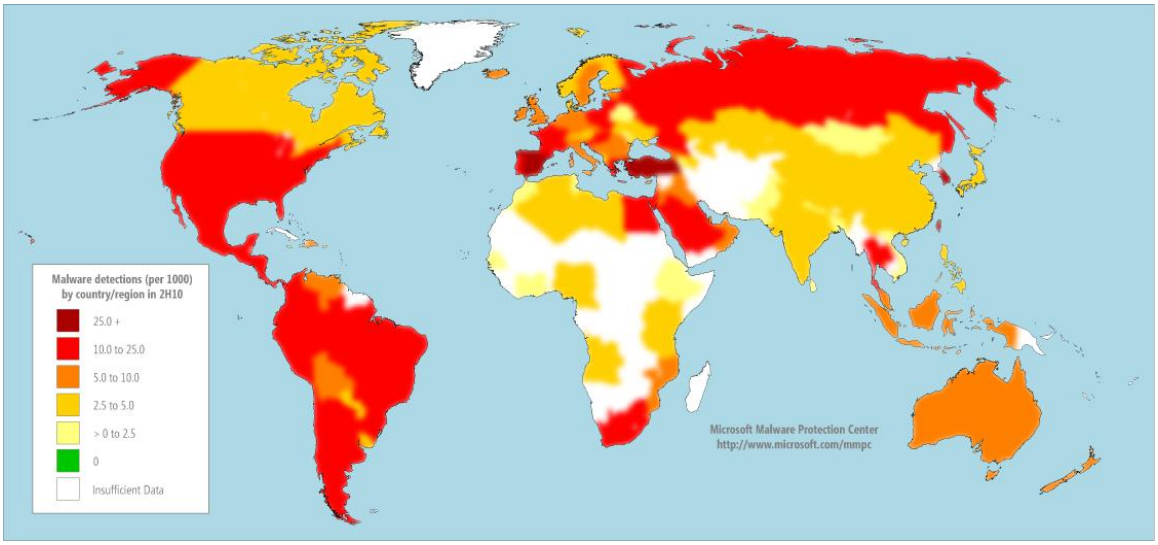
- Detections in Russia rose 41.3 percent from 3Q to 4Q, primarily because of a significant increase in the number of computers running Microsoft Security Essentials there.

In absolute terms, the locations with the most computers reporting detections tend to be ones with large populations and large numbers of computers. To control for this effect, Figure 14 shows the infection rates in locations around the world using a metric called *computers cleaned per mille* (thousand), or *CCM*, which represents the number of reported computers cleaned in a quarter for every 1,000 executions of the Microsoft Windows® Malicious Software Removal Tool (MSRT).[3] (See the *Security Intelligence Report* website for more information about the CCM metric.)

Figure 14. Infection rates by country/region in 1H10 (top) and 2H10 (bottom), by CCM



[3] For the maps in Figure 14, the CCM totals are averaged for the first two and last two quarters of 2010, respectively, to produce CCM totals for 1H10 and 2H10.



- Among locations with at least 100,000 executions of MSRT in 4Q10, Korea had the highest infection rate, with 40.3 computers cleaned for every 1,000 MSRT executions (CCM 40.3). Following Korea were Spain (33.2), Turkey (32.8), Taiwan (24.3), and Brazil (20.8).

- For the entire year, Turkey had the highest average quarterly CCM at 36.8, followed by Spain (36.1), Korea (34.8), Taiwan (29.7), and Brazil (24.7). These five locations have consistently had the highest infection rates among large countries and regions for most of the past six quarters, as shown in Figure 15 on page 31.

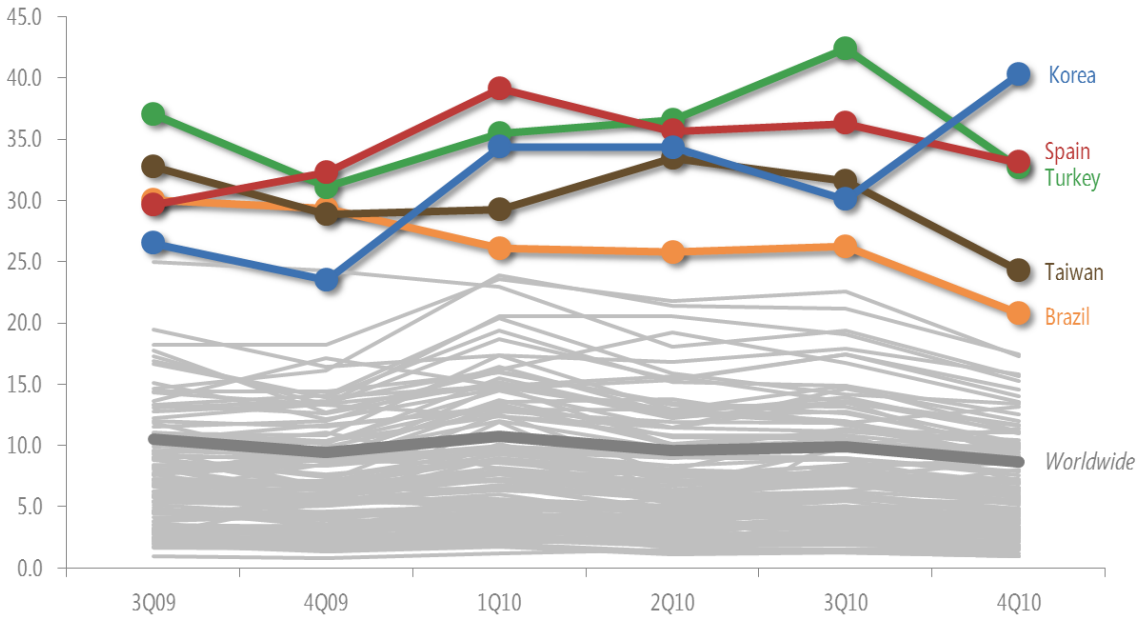
- Locations with low infection rates include Mongolia (1.3 average CCM for 2010), Bangladesh (1.4), and Belarus (1.6). Large countries and regions with low infection rates include the Philippines (3.1), Austria (3.4), India (3.8), and Japan (4.4).

Detections and removals in individual countries/regions can vary significantly from period to period. Increases in the number of computers with detections can be caused not only by increased prevalence of malware in that country but also by improvements in the ability of Microsoft antimalware solutions to detect malware. Large numbers of new antimalware installations in a location also typically increase the number of computers cleaned in that location.

The next two 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 2010. (See Infection Trends Worldwide in the "Key

Findings" section of the *Security Intelligence Report* website for additional details about this information.)

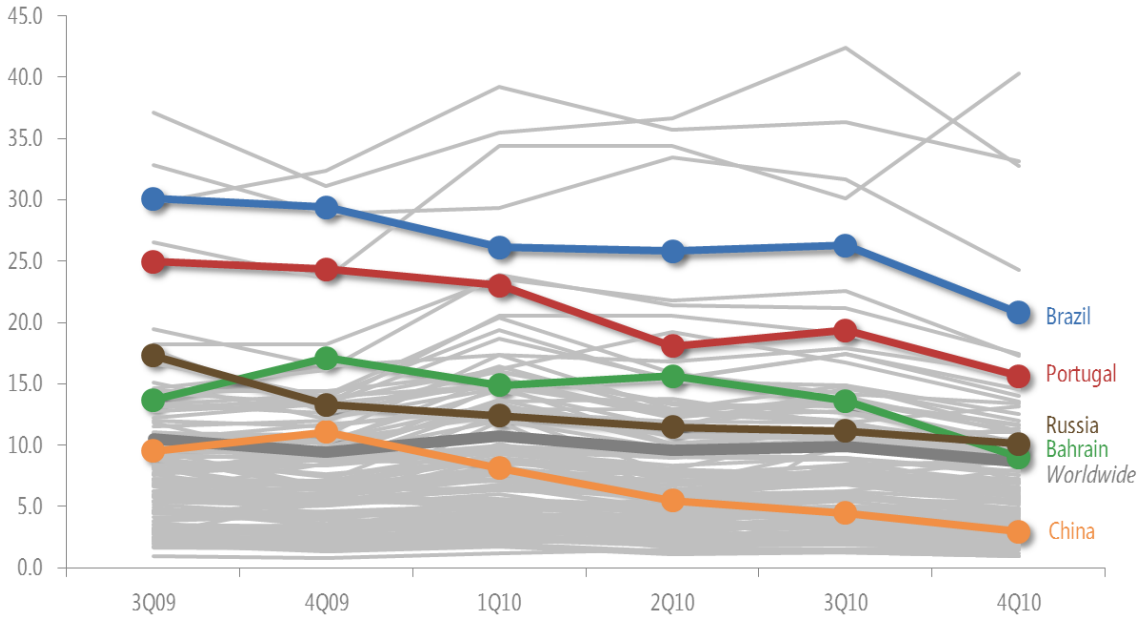
Figure 15. Trends for the five locations with the highest infection rates in 4Q10, by CCM (100,000 MSRT executions minimum per quarter in 2010)



- Korea has come under sustained attack in recent quarters, resulting in a dramatic rise from 4th place in 3Q10 to 1st place in 4Q10. The CCM in Korea rose from 23.6 in 4Q09 to 40.3 a year later, an increase of 16.7 points, or 71.1 percent—the largest such increase over the past year. (See the "Global Threat Assessment" section of the *Security Intelligence Report* website for more information about threats in Korea.)

- Korea, Spain, Turkey, Taiwan, and Brazil have occupied the top five spots among large countries and regions with the highest infection rates in all but one of the last six quarters (the sole exception being 4Q09, when Portugal edged Korea for 5th place).

Figure 16. Infection rate trends for the five most improved locations between 4Q09 and 4Q10, by CCM (100,000 MSRT executions minimum in 4Q10)



- The most improved locations are those that showed the greatest decline in CCM between 4Q09 and 4Q10.

- Brazil, though still one of the locations with the highest infection rates, has improved significantly over the past six quarters, dropping from 30.1 CCM in 3Q09 to 20.8 in 4Q10. Declines in Win32/Frethog and Win32/Hamweq were chiefly responsible for this improvement, followed by declines in Win32/Conficker and Win32/Rimecud. (See "Threat Families" on page 39 for more information about these and other malware families.)

- Although the total number of detections and removals in Russia increased through 2010, as explained on page 28, the actual infection rate declined significantly, from 17.3 CCM in 3Q09 to 10.1 in 4Q10. This decrease was primarily because of decreases in Conficker, Hamweq, and Win32/Taterf.

- Infection rates in Portugal and Bahrain fluctuated over the past six quarters, but both locations ended 4Q10 showing significant improvements over 3Q09. Portugal went from 25.0 CCM to 15.6, a 37.6

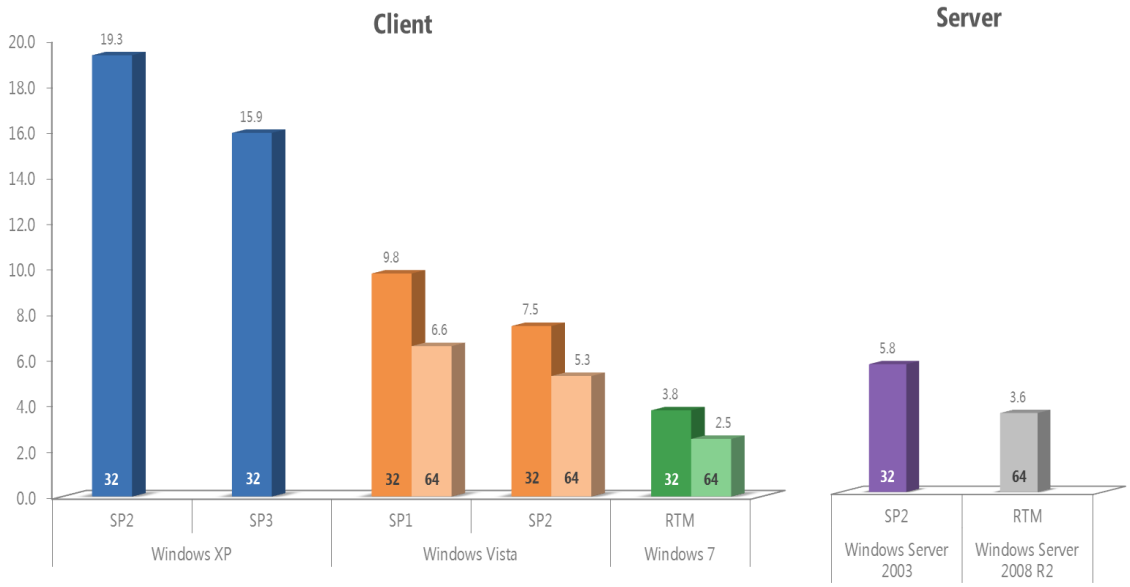
percent decrease. Bahrain dropped from 13.6 to 9.0, a decline of 33.8 percent.

- The CCM in China decreased from 9.5 in 3Q09 to 2.9 in 4Q10. Although this makes China one of the locations with the lowest infection rates worldwide as measured by CCM, a number of factors that are unique to China are important to consider when assessing the state of computer security there. The malware ecosystem in China is dominated by a number of Chinese- language threats that are not prevalent anywhere else. The CCM figures are calculated based on telemetry from MSRT, which targets global malware families. To date, we have not targeted families specific to China with. In 2010, for example, 92 to 94 percent of the threats reported by computers running Microsoft Security Essentials in China would not have been detected by MSRT. For a more in-depth perspective on the threat landscape in China, see the "Global Threat Assessment" section of the *Security Intelligence Report* website.

Operating System Infection Rates

The features and updates that are available with different versions of the Windows operating system, along with the differences in the way people and organizations use each version, affect the infection rates for the different versions and service packs. Figure 17 shows the infection rate for each Windows operating system/service pack combination that accounted for at least 0.1 percent of total MSRT executions in 2010.

Figure 17. Average quarterly infection rate (CCM) by operating system and service pack in 2010



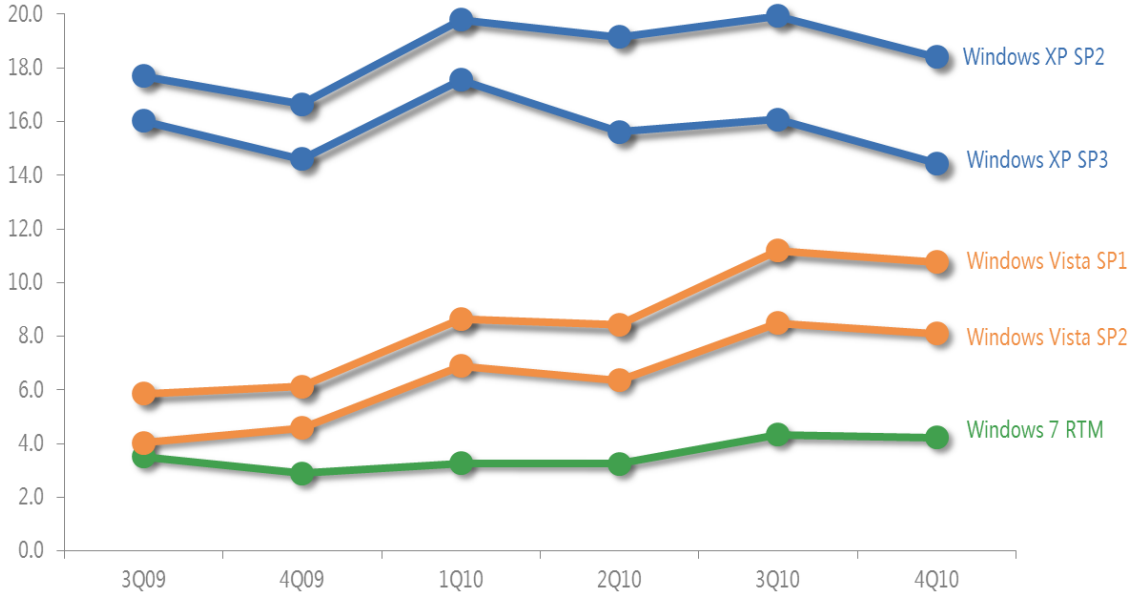
"32" = 32-bit; "64" = 64-bit. Supported systems with at least 0.1 percent of total executions shown.

- This data is normalized: 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 SP2 computers to 1,000 Windows 7 RTM computers).

- As in previous periods, infection rates for more recently released operating systems and service packs are consistently lower than earlier ones, for both client and server platforms. Windows 7 and Windows Server® 2008 R2, the most recently released Windows client and server versions, respectively, have the lowest infection rates on the chart.

- Infection rates for the 64-bit versions of Windows Vista® and Windows 7 are lower than for the corresponding 32-bit versions of those operating systems. One reason may be that 64-bit versions of Windows still appeal to a more technically savvy audience than their 32-bit counterparts, despite increasing sales of 64-bit Windows versions among the general computing population. Kernel Patch Protection (KPP), a feature of 64-bit versions of Windows that protects the kernel from unauthorized modification, may also contribute to the discrepancy by preventing certain types of malware from operating.

Figure 18. CCM trends for supported 32-bit versions of Windows XP, Windows Vista, and Windows 7, 3Q09-4Q10

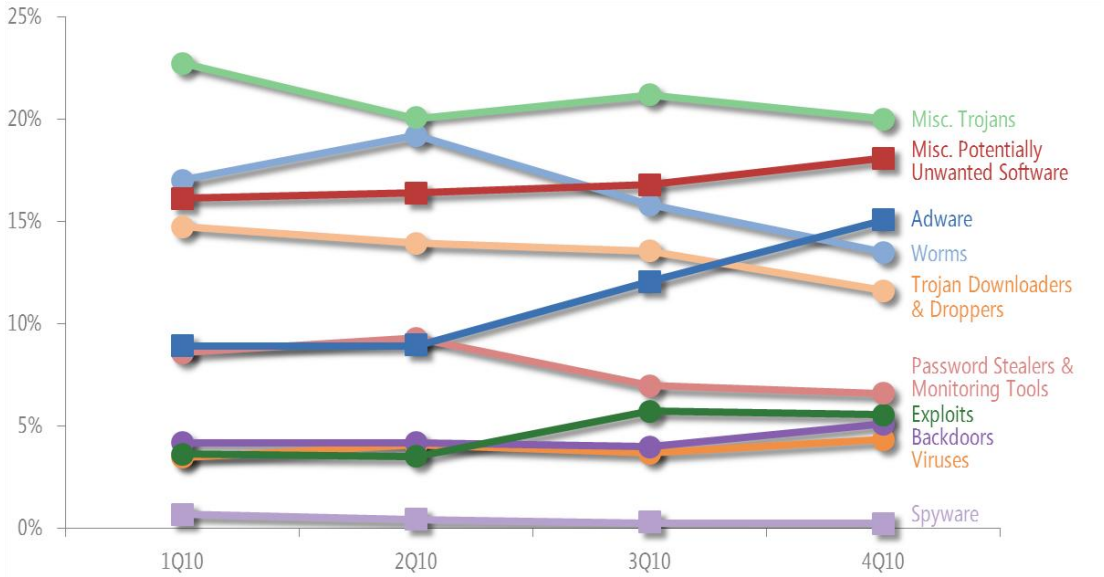


- As Figure 18 shows, Windows 7 has consistently had the lowest infection rate of any 32-bit client operating system/service pack combination over the past six quarters.

Threat Categories

The Microsoft Malware Protection Center (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 *SIR* groups these types into 10 categories based on similarities in function and purpose.

Figure 19. Detections by threat category each quarter in 2010, 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 have more than one category of threat detected and removed from them in each time period.

- The miscellaneous trojans category, which consists of all trojans that are not categorized as trojan downloaders & droppers, was the most prevalent category each quarter in 2010, with detections on 20.0 percent of all infected computers in 4Q10, down from 22.7 percent in 1Q10.

- Detections of adware increased significantly during the second half of the year, rising from 8.9 percent of infected computers in 2Q10 to 15.1 percent in 4Q10. This increase was almost completely caused by the appearance of a pair of new adware families, JS/Pornpop and

Win32/ClickPotato, in the third quarter. (See "Threat Families" on page 39 for more information about these and other families.)

- After increasing from 1Q10 to 2Q10, worms declined significantly through the end of the year, from a second-quarter high of 19.2 percent of infected computers to 13.5 percent in 4Q10. A 61.3 percent decrease in detections and removals of the worm family Win32/Hamweq between 1Q10 and 4Q10 is partially responsible for this relative decline, combined with increases in other categories. (Hamweq was added to MSRT in December 2009, and was detected by the tool on more than 1 million computers by the end of 1Q10. By the end of the year, Hamweq detections had declined significantly, with MSRT removing it from fewer than 300,000 computers in 4Q10.)

- The miscellaneous potentially unwanted software and trojan downloaders & droppers categories began the year at similar levels of prevalence, and then diverged. miscellaneous potentially unwanted software rose from 16.1 percent of infected computers to 18.1 percent, with increased detections of the potentially unwanted software families Win32/Zwangi and Win32/Keygen accounting for much of the increase (the increase in detections of the latter family was caused more by improved detection than by increased prevalence). trojan downloaders & droppers declined from 14.7 percent to 11.6 percent, in part because of a decline in detections of Win32/Renos, a perennially common family.

- Each of the other categories was detected on fewer than 10 percent of infected computers. Password Stealers & Monitoring Tools declined to 6.6 percent of infected computers in 4Q10 following a decrease in detections of Win32/Frethog, which targets passwords for online games. Spyware, which has never been very common, declined even more in 2010 to just 0.2 percent of infected computers in the fourth quarter.

Threat Categories by Location

There are significant differences in the types of threats that affect users in different parts of the world. The spread and effectiveness of malware are highly dependent on language and cultural factors, in addition to the methods used for distribution. Some threats are spread using techniques that target people who speak a particular language or who use services that are local to a particular geographic region. Other threats target vulnerabilities or operating system configurations and applications that are unequally distributed around the globe.

Figure 20 shows the relative prevalence of different categories of malware and potentially unwanted software in several locations around the world in 2010.

Figure 20. Threat category prevalence worldwide and in nine individual locations in 2010

Category	World	US	Brazil	China	UK	Fr.	Spain	Russia	Ger.	Korea
Misc. Trojans	31.6%	43.4%	23.2%	28.0%	36.5%	21.6%	20.1%	40.3%	28.4%	17.3%
Misc. Potentially Unwanted Software	25.5%	22.6%	31.2%	52.1%	23.6%	24.3%	22.6%	33.8%	24.5%	10.3%
Worms	24.4%	16.6%	35.6%	13.5%	11.8%	21.0%	40.2%	32.8%	14.4%	40.1%
Trojan Downloaders & Droppers	20.1%	20.2%	26.2%	18.8%	20.3%	19.7%	16.9%	17.0%	28.9%	8.0%
Adware	17.4%	21.4%	9.4%	3.4%	29.3%	33.0%	10.7%	8.2%	16.3%	12.1%
Password Stealers & Monitoring Tools	11.7%	6.1%	27.9%	10.7%	7.5%	9.2%	20.5%	10.3%	9.3%	14.7%
Exploits	7.1%	9.6%	10.5%	13.5%	7.3%	2.7%	3.0%	8.0%	5.7%	3.3%
Backdoors	6.6%	5.3%	5.7%	10.3%	4.2%	4.4%	8.4%	8.2%	5.1%	7.1%
Viruses	5.9%	5.1%	10.3%	6.1%	3.4%	3.3%	3.7%	12.1%	3.2%	13.8%
Spyware	0.6%	0.7%	0.2%	2.3%	0.4%	0.3%	0.2%	0.5%	0.7%	0.5%

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

- Within each row of Figure 20, 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.

- The United States and the United Kingdom, two predominantly English-speaking locations that also share a number of other cultural similarities, have similar threat mixes in most categories. Exceptions include Adware, which is more common in the UK, and Worms, which are more common in the US.

- Brazil has an unusually high concentration of Password Stealers & Monitoring Tools, primarily because of the prevalence of Win32/Bancos, which targets customers of Brazilian banks.

- China has a relatively high concentration of Miscellaneous Potentially Unwanted Software, Exploits, Backdoors, and Spyware, and a relatively low concentration of Worms and Adware. China routinely exhibits a threat mix that is much different than those of other large countries and regions. Two of the most common threats in China, Win32/BaiduSobar and Win32/Sogou, are Chinese-language potentially unwanted software families that are uncommon elsewhere. The most common families in China also include a pair of exploits, JS/CVE-2010-0806 and JS/ShellCode, that were less prevalent elsewhere.

- Adware dominates in France, led by Win32/ClickPotato.

- Worms and Backdoors are unusually common in Spain. The top six families detected in Spain in 2010 were worms.

- The threat mix in Russia resembles that of the world as a whole, with the exception of an unusually low concentration of Adware, perhaps because of the highly language-dependent nature of online advertising.

- In Germany, Trojan Downloaders & Droppers are nearly twice as common as in the rest of the world, led by Win32/Renos.

- Korea has a large concentration of viruses, led by Win32/Parite, and worms. Viruses and worms have long been unusually common in Korea, perhaps because of the popularity of public Internet gaming centers there where viruses are easily transmitted between computers and removable volumes.

See "Appendix C: Worldwide Infection Rates" on page 73 for more information about malware around the world.

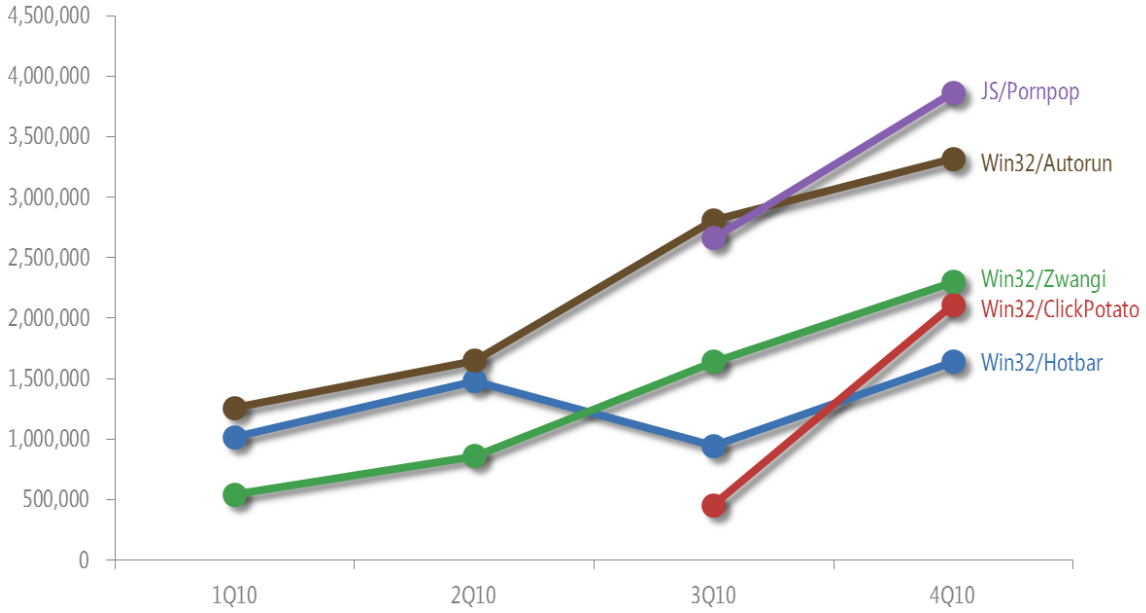
Threat Families

Figure 21 lists the top 10 malware and potentially unwanted software families that were detected on computers by Microsoft desktop security products in the second half of 2010.

Figure 21. Quarterly trends for the top 10 malware and potentially unwanted software families detected by Microsoft desktop security products in 2H10

	Family	Most Significant Category	1Q10	2Q10	3Q10	4Q10
1	JS/Pornpop	Adware	–	–	2,660,061	3,860,365
2	Win32/Autorun	Worms	1,256,649	1,646,532	2,805,585	3,314,092
3	Win32/Taterf	Worms	1,496,780	2,323,750	2,338,517	1,615,649
4	Win32/Zwangi	Misc. Potentially Unwanted Software	542,534	860,747	1,638,398	2,299,210
5	Win32/Renos	Trojan Downloaders & Droppers	2,693,093	1,889,680	2,109,631	1,655,865
6	Win32/Rimecud	Worms	1,809,231	1,749,708	1,674,975	1,892,919
7	Win32/Conficker	Worms	1,498,256	1,664,941	1,649,934	1,744,986
8	Win32/FakeSpypro	Miscellaneous Trojans	1,244,903	1,424,152	1,897,420	889,277
9	Win32/Hotbar	Adware	1,015,659	1,483,289	942,281	1,640,238
10	Win32/ClickPotato	Adware	–	–	451,660	2,110,117

Figure 22. The families that increased the most in prevalence in 2010



- JS/Pornpop, the most commonly detected family in 4Q10, is a detection for specially crafted JavaScript-enabled objects that attempt to display pop-under advertisements in users' web browsers, usually with adult content.

Pornpop is one of the fastest spreading malware families seen in several years. First detected in August 2010, it quickly grew to become the second most prevalent family in 3Q10, and the most prevalent family in 4Q10 and in the second half of the year as a whole.

- Detections and removals of Win32/Autorun, a generic detection for worms that spread between mounted volumes using the Autorun feature of Windows, increased significantly in 4Q10, although Autorun dropped to second place because of the spread of Pornpop.

- Win32/Taterf, the most prevalent threat in 2Q10, dropped to third by 4Q10. Taterf belongs to a category of threats that are designed to steal passwords for popular online computer games and transmit them to the attackers. See "Online Gaming-Related Families" on page 62 of *Microsoft Security Intelligence Report, Volume 5 (January through June 2008)* for more information about these threats.

- Win32/Renos, the most prevalent threat in 1Q10, dropped to fifth by 4Q10. Renos is a family of Trojan downloaders that is often used to install rogue security software. Since 2006, it has consistently been one of the threats most commonly detected and removed by Microsoft antimalware desktop products and services.

- The potentially unwanted software family Win32/Zwangi rose from tenth in 2Q10 to fourth in 4Q10. Zwangi is a program that runs as a service in the background and modifies web browser settings to visit a particular website.

- The adware family Win32/ClickPotato, first detected in August 2010, rose quickly to become the tenth most prevalent family in 4Q10. ClickPotato is a program that displays pop-up and notification-style advertisements based on the user's browsing habits.

Rogue Security Software

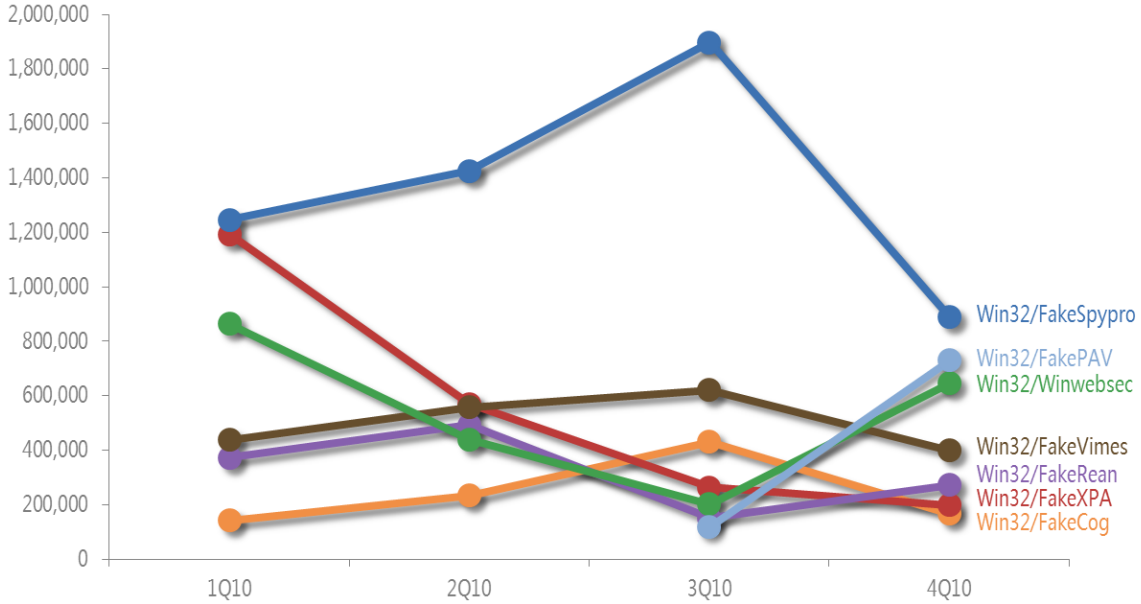
Rogue security software has become one of the most common methods that attackers use to swindle money from victims. Rogue security software, also known as *scareware*, is software that appears to be beneficial from a security perspective but provides limited or no security, generates erroneous or misleading 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 "full version" of the software to remove the 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 Rogue Security Software in the "Reference Guide" section of the *Security Intelligence Report* website for more information about this kind of threat. Also see www.microsoft.com/security/antivirus/rogue.aspx for an informative series of videos about rogue security software aimed at a general audience.)

Figure 23. Some of the "brands" used by different versions of the rogue security software family Win32/FakeXPA

Figure 24 shows detection trends for the most common rogue security software families detected in 2010.

Figure 24. Trends for the most commonly detected rogue security software families in 2010, by quarter



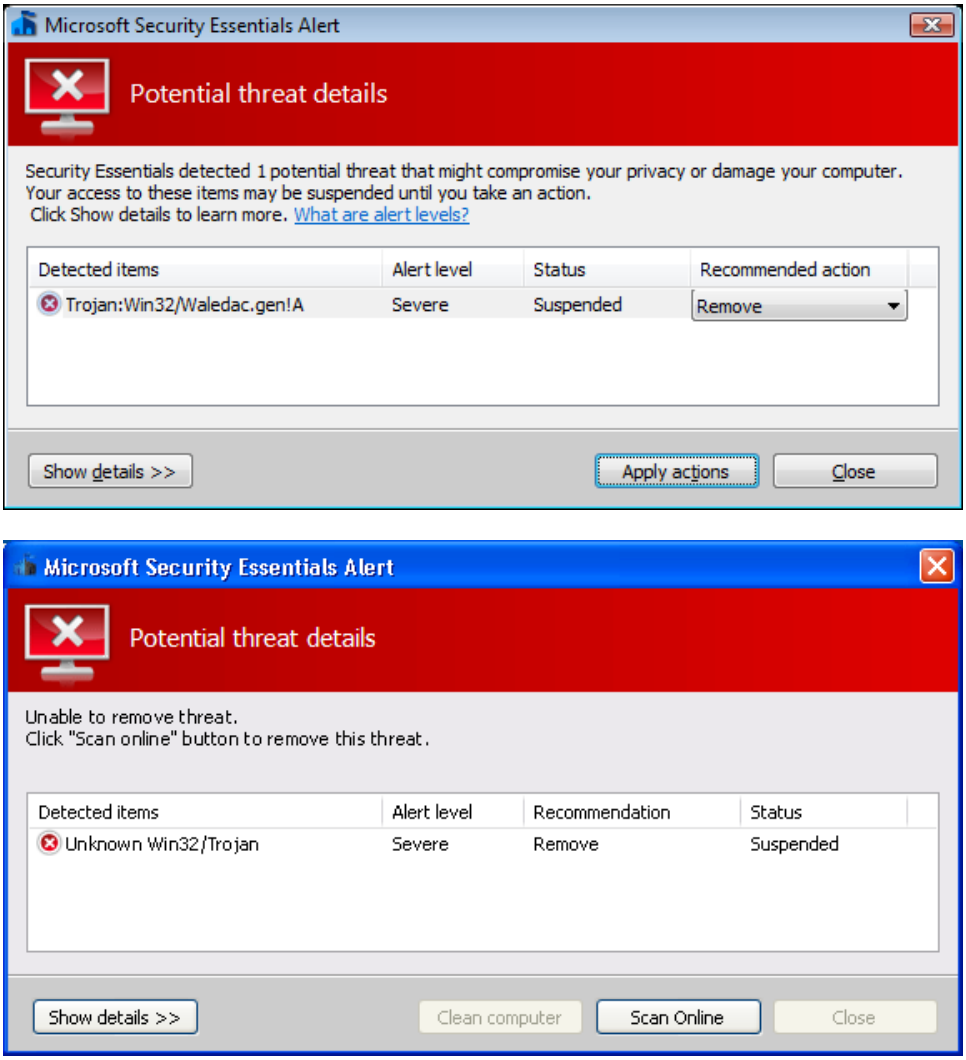
- Win32/FakeSpypro was the most commonly detected rogue security software family in each quarter of 2010, with more than twice as many detections and removals overall as the next most prevalent family. Names under which FakeSpypro is distributed include AntispywareSoft, Spyware Protect 2009, and Antivirus System PRO. Detections for FakeSpypro were added to MSRT in July 2009.

- Win32/FakeXPA, the second most commonly detected rogue security software family overall in 2010, fell from a near tie with FakeSpypro in 1Q10 to sixth place in 4Q10. FakeXPA is a persistent, frequently updated threat that uses a variety of techniques to evade detection and removal by legitimate security products. It is distributed under a large number of names, some of which are shown in Figure 23. Detections for FakeXPA were added to MSRT in December 2008.

- Win32/FakePAV was first detected in 3Q10 and rose quickly to become the second most commonly detected rogue security software family in the fourth quarter. FakePAV is one of several rogue security software families that masquerade as Microsoft Security Essentials. It presents a dialog box that is similar in appearance to a Security Essentials alert, listing one or more nonexistent infections that it claims it cannot remove. It then offers to "install" a trial version of a different security program

(actually another part of FakePAV itself), after which it proceeds in a manner similar to other rogue security software programs.

Figure 25. A genuine Microsoft Security Essentials alert (top) and a fake alert generated by Win32/FakePAV (bottom)



Names under which FakePAV is distributed include Red Cross Antivirus, Peak Protection 2010, AntiSpy Safeguard, Major Defense Kit, Pest Detector, ThinkPoint, Privacy Guard 2010, Palladium Pro, and others. Detections for FakePAV were added to MSRT in November 2010. For additional information, see the post MSRT Tackles Fake Microsoft Security Essentials (November 9, 2010) on the MMPC blog, http://blogs.technet.com/mmpc.

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, 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 produced by Microsoft desktop antimalware products and tools includes information about whether the infected computer belongs to an Active Directory® Domain Services domain. 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 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 26 and Figure 27 list the top 10 families detected on domain-joined and non-domain computers in 4Q10.

Figure 26. Top 10 families detected on domain-joined computers in 2010, by percentage of domain-joined computers reporting detections

	Family	Most Significant Category	1Q10	2Q10	3Q10	4Q10
1	Win32/Conficker	Worms	21.3%	22.0%	19.6%	18.9%
2	Win32/Autorun	Worms	7.3%	8.3%	10.0%	10.0%
3	Win32/Rimecud	Worms	9.0%	9.8%	8.0%	8.3%
4	Win32/Taterf	Worms	4.1%	6.9%	5.9%	4.1%
5	Win32/RealVNC	Miscellaneous Potentially Unwanted Software	5.6%	5.4%	4.9%	4.3%
6	Win32/Hamweq	Worms	7.0%	5.3%	3.2%	2.4%
7	Win32/Frethog	Password Stealers & Monitoring Tools	6.5%	6.0%	2.8%	2.4%
8	Win32/Renos	Trojan Downloaders & Droppers	5.2%	3.4%	4.0%	2.8%
9	Win32/Alureon	Miscellaneous Trojans	2.7%	2.4%	2.8%	1.8%
10	Win32/FakeSpypro	Miscellaneous Trojans	2.3%	3.0%	2.8%	0.9%

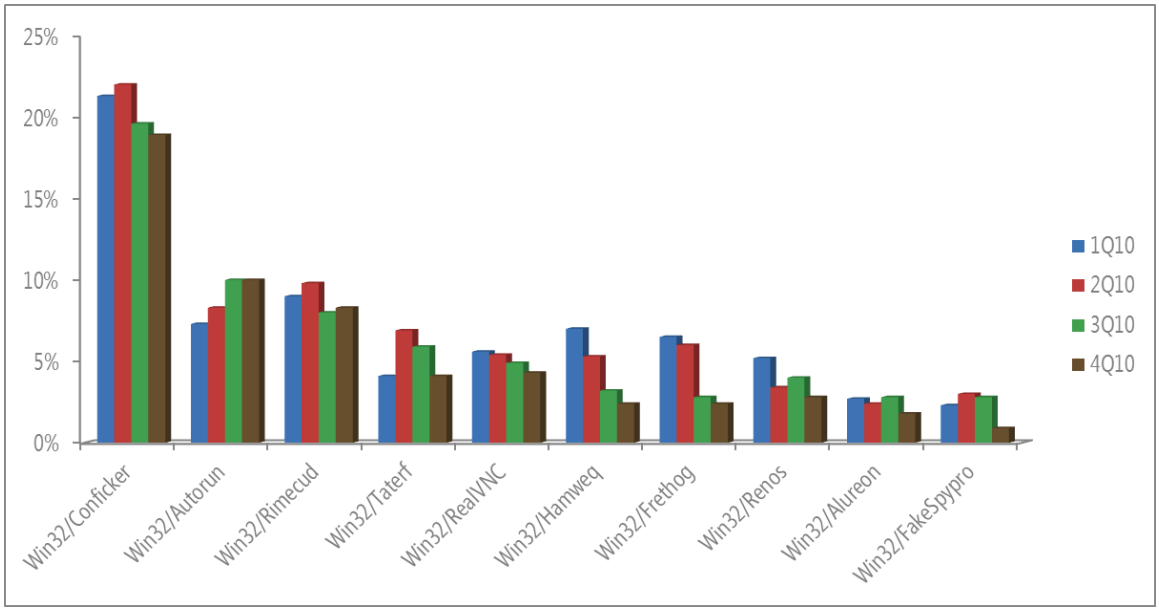
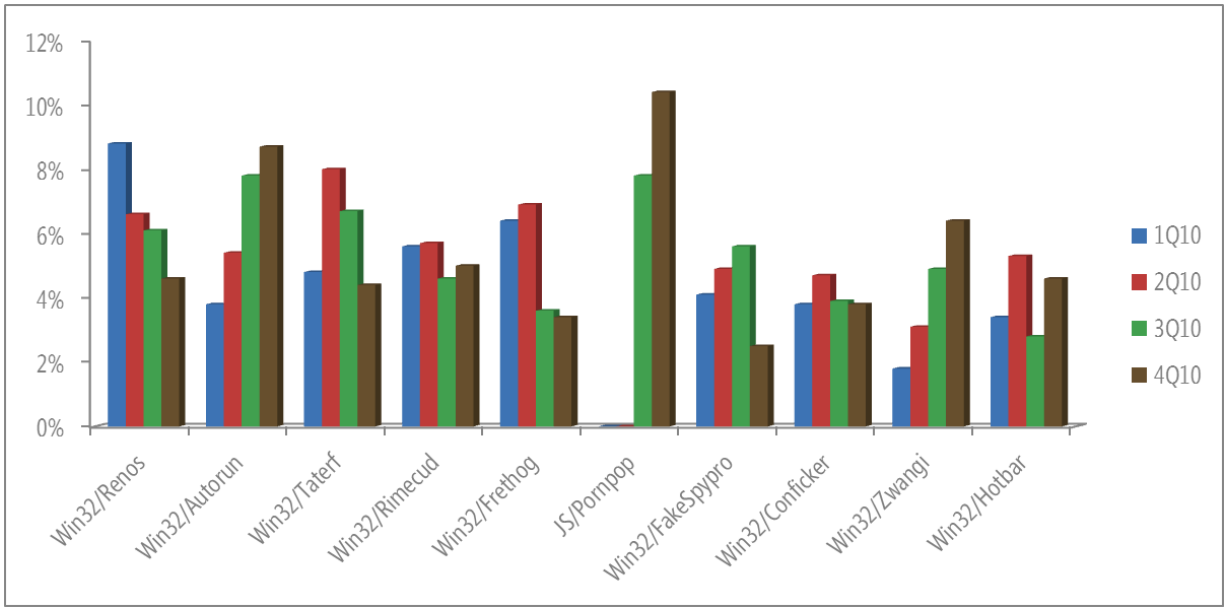


Figure 27. Top 10 families detected on non-domain computers in 2010, by percentage of all infected non-domain computers reporting detections

	Family	Category	Q1	Q2	Q3	Q4
1	Win32/Renos	Trojan Downloaders & Droppers	8.8%	6.6%	6.1%	4.6%
2	Win32/Autorun	Worms	3.8%	5.4%	7.8%	8.7%
3	Win32/Taterf	Worms	4.8%	8.0%	6.7%	4.4%
4	Win32/Rimecud	Worms	5.6%	5.7%	4.6%	5.0%
5	Win32/Frethog	Password Stealers & Monitoring Tools	6.4%	6.9%	3.6%	3.4%
6	JS/Pornpop	Adware	—	—	7.8%	10.4%
7	Win32/FakeSpypro	Miscellaneous Trojans	4.1%	4.9%	5.6%	2.5%
8	Win32/Conficker	Worms	3.8%	4.7%	3.9%	3.8%
9	Win32/Zwangi	Miscellaneous Potentially Unwanted Software	1.8%	3.1%	4.9%	6.4%
10	Win32/Hotbar	Adware	3.4%	5.3%	2.8%	4.6%



- Seven families are common to both lists, although they are ordered differently and in different proportions. The worm family Win32/Conficker, which uses several methods of propagation that work more effectively within a typical enterprise network environment than they do over the public Internet, leads the domain-joined list by a significant margin, but ranks ninth on the non-domain list.

- Worms accounted for five of the top 10 families detected on domain-joined computers. Several of these worms, including Conficker, Win32/Autorun, and Win32/Taterf, are designed to propagate via network shares, which are common in domain environments.

- On non-domain computers, JS/Pornpop was the most commonly detected family in 4Q10 and the fourth most commonly detected family in 2010 overall. By contrast, this family was detected much less often on domain-joined computers. Pornpop is an adware family that attempts to display pop-under advertisements that usually contain adult content in users' web browsers. It is often found on websites that host illegal or illicit content, which users in domain environments are often restricted from accessing by organizational policy or blocking software.

- Taterf and Win32/Frethog are two related families that are designed to steal the passwords of users who play massively multiplayer online role-playing games (MMORPGs). Such games are not common in the workplace, yet both families were detected with similar frequency on both domain-joined and non-domain computers. Taterf and Frethog both rely heavily on removable drives to propagate—a technique that was probably developed to help spread them in Internet cafés and public gaming centers, but one that has had the effect of spreading them efficiently in enterprise environments as well, which was perhaps unexpected.

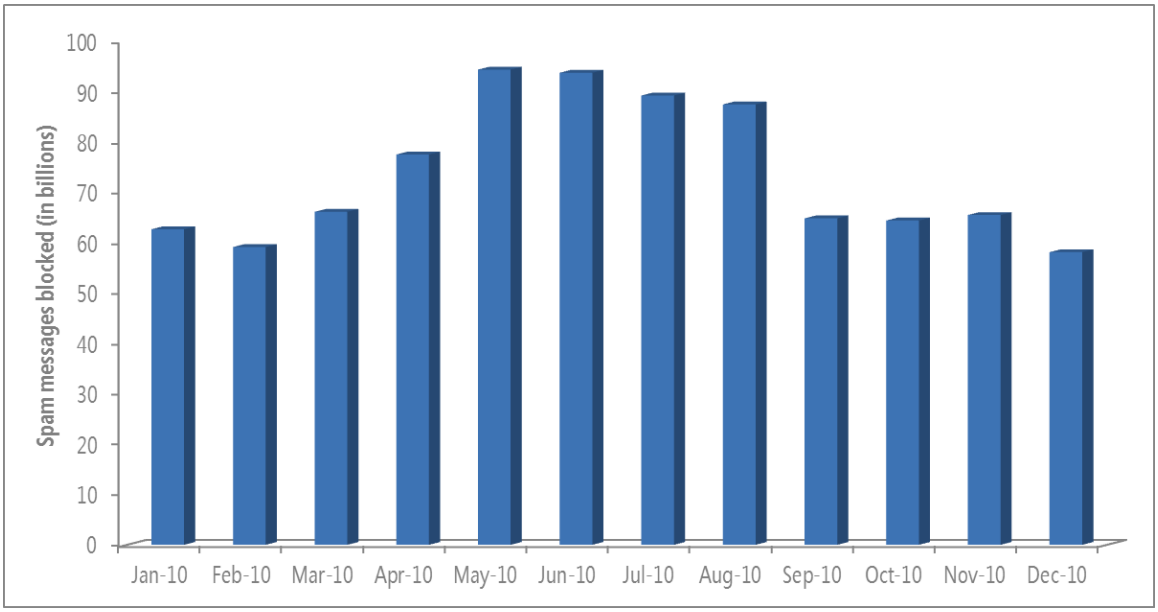
Email Threats

Most 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 is compiled from telemetry data provided by Microsoft Forefront® Online Protection for Exchange (FOPE), which provides spam, phishing, and malware filtering services for thousands of enterprise customers and tens of billions of messages per month. (See Spam Trends in the "Reference Guide" section of the *Security Intelligence Report* website for more information.)

Figure 28. Messages blocked by FOPE each month in 2010



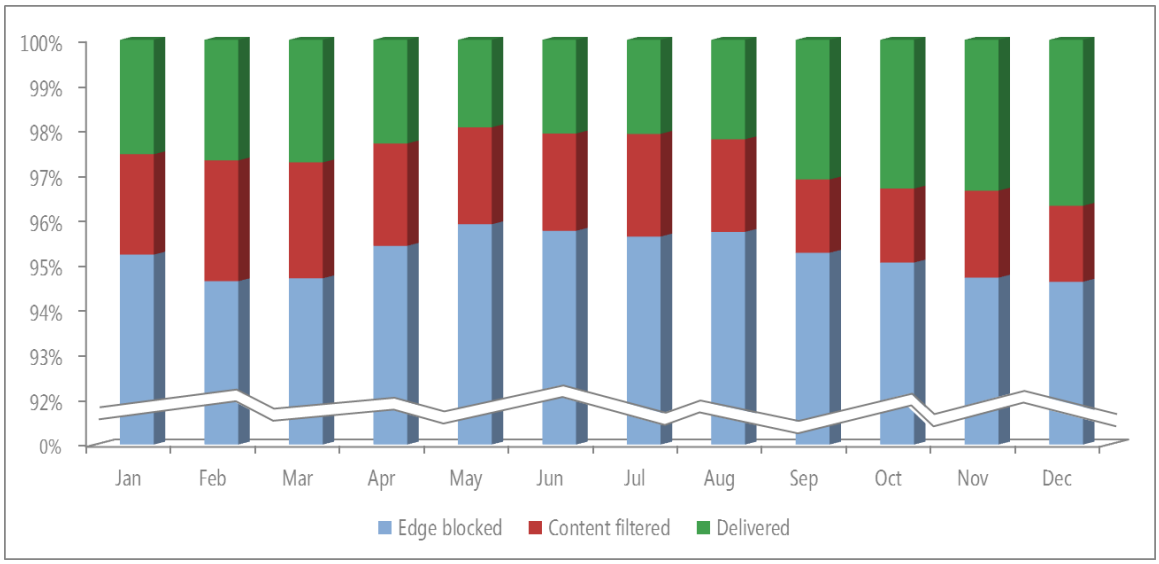
- After increasing gradually and then reaching a plateau through the first eight months of 2010, the number of spam messages received and blocked by FOPE dropped abruptly in September, and again in December. These drops can be correlated with events involving two of the world's most significant spam-sending botnets:

    - During the last week of August, researchers affiliated with the security firm LastLine spearheaded a coordinated takedown of command-and-control (C&C) servers associated with the Win32/Cutwail spambot. In the days following the takedown, FOPE recorded a significant drop in the average daily volume of messages blocked.

    - Around December 25, spam researchers around the world recorded an almost complete cessation of spam originating from the large Rustock botnet, with some spam trackers reporting a drop in the global spam rate as high as 50 percent or more. During the final week of December, the number of messages blocked by FOPE was almost 30 percent less than in the prior week, compared to a drop of less than two percent between the final two weeks of 2009. The Rustock botnet subsequently began sending spam again in mid-January, and the number of messages blocked by FOPE has risen accordingly. The reasons for this hiatus are still being investigated.

FOPE 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 29. Percentage of incoming messages blocked by FOPE using edge-blocking and content filtering in 2010



- In 2010 overall, only about one out of every 38.5 incoming messages made it to recipients' inboxes. The rest were blocked at the network edge or through content filtering.

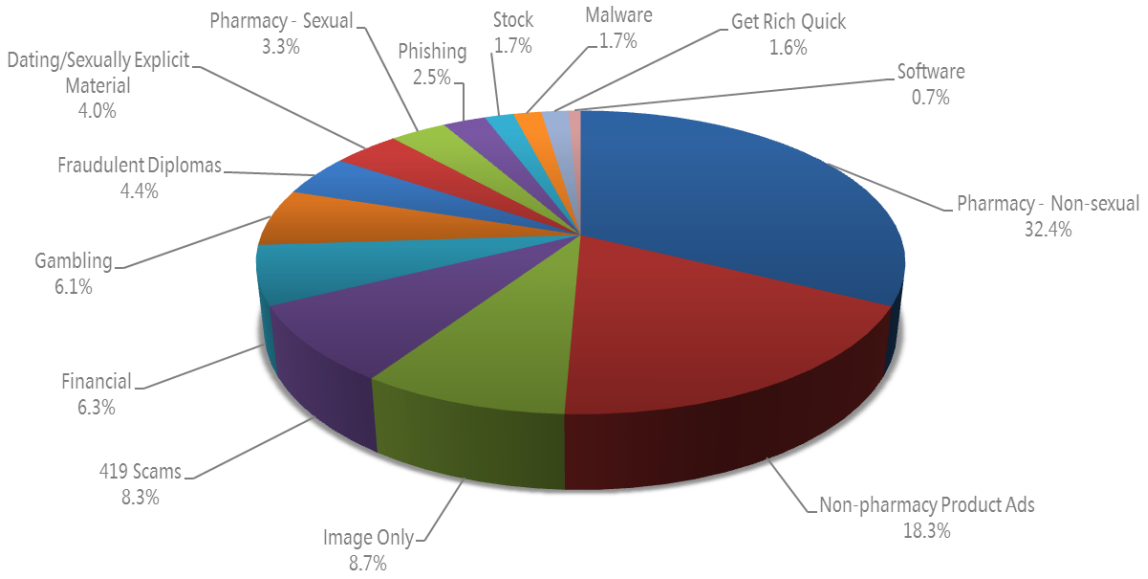
- Approximately 95.3 percent of all incoming messages were blocked at the network edge, which means that only 4.7 percent of incoming messages had to be subjected to the more resource-intensive content filtering process.

- The effectiveness of edge-filtering techniques such as IP address reputation checking, SMTP connection analysis, and recipient validation have increased dramatically over the past several years, which enables mail-filtering services to provide better protection to users even as the total amount of unwanted message traffic on the Internet remains very high.

Spam Types

The FOPE content filters recognize several different common types of spam messages. Figure 30 shows the relative prevalence of these spam types in 2010.

Figure 30. Inbound messages blocked by FOPE filters in 2010, by category

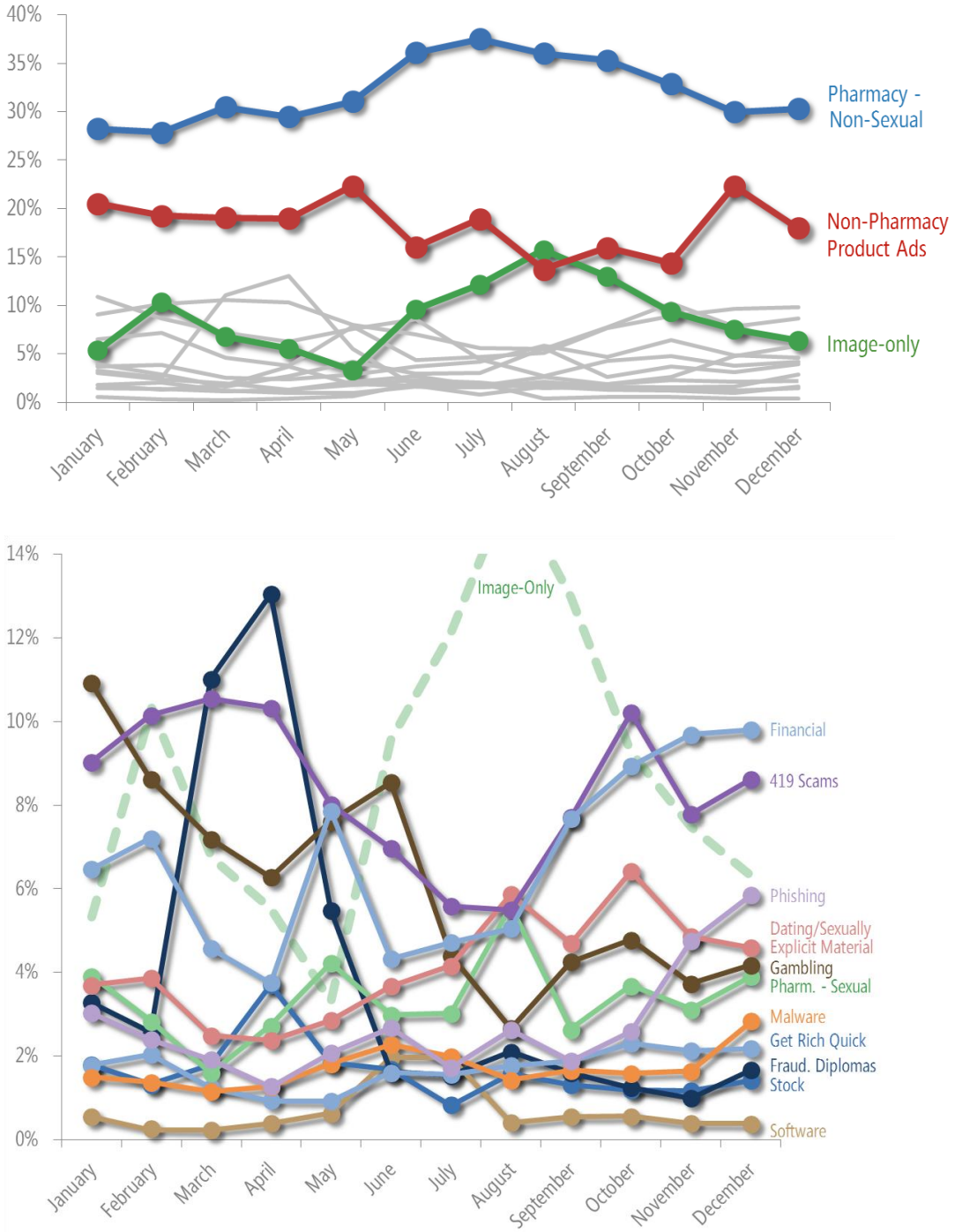


- Advertisements for nonsexual pharmaceutical products accounted for 32.4 percent of the spam messages blocked by FOPE content filters in 2010.

- Together with nonpharmaceutical product ads (18.3 percent of the total) and advertisements for sexual performance products (3.3 percent), product advertisements accounted for 54.0 percent of spam in 2010, which is down from 69.2 percent a year ago.

- In an effort to evade content filters, spammers often send messages that consist only of one or more images, with no text in the body of the message. Image-only spam messages accounted for 8.7 percent of the total in 2010, up from 6.3 percent in 2009.

Figure 31. Inbound messages blocked by FOPE content filters each month in 2010, by category



- Nonsexual pharmaceutical ads and nonpharmaceutical product ads were the most highly ranked categories by a significant margin throughout most of 2010.

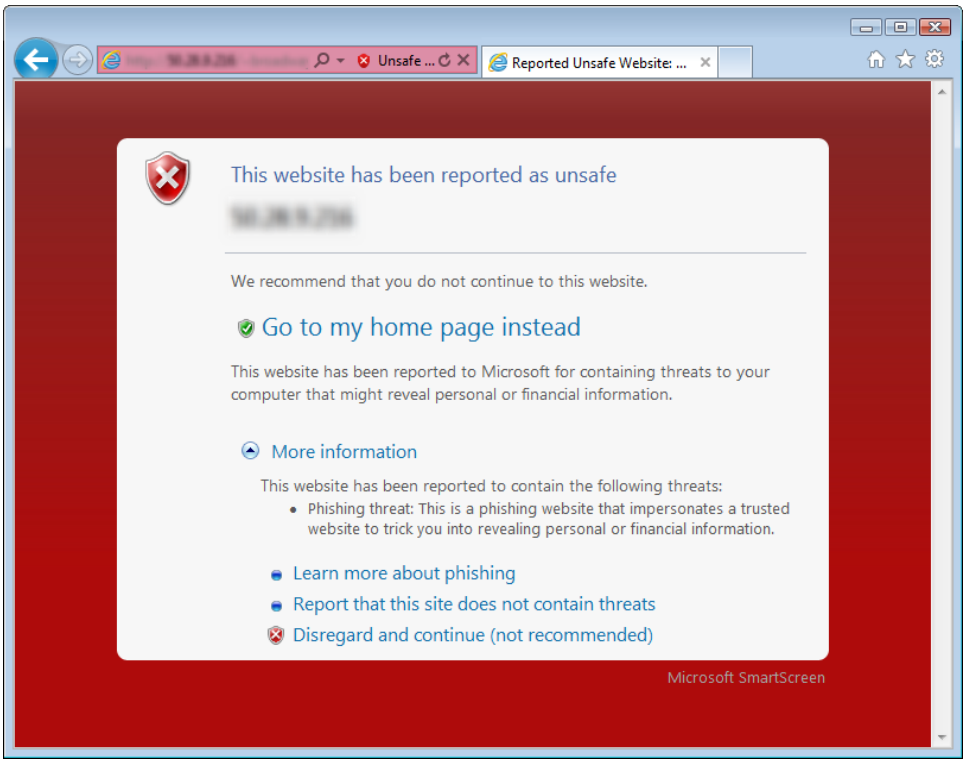
- As Figure 31 illustrates, spam categories can vary considerably from month to month as spammers conduct time-based campaigns, much like legitimate advertisers do. Spam that advertises fraudulent university diplomas, typically a low-volume category, increased nearly six fold between February and March and was actually the third most prevalent category in March and April before declining to last place in June. Similarly, image-only ads, which accounted for a small and declining percentage of spam through May, suddenly began rising in prominence in June, briefly eclipsed nonpharmaceutical product ads in August, and then returned to more typical levels through the end of the year.

Malicious Websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. 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 the SmartScreen® filter (in Windows® Internet Explorer® 8 and 9), 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 Phishing and Malware Hosts in the "Reference Guide" section of the *Security Intelligence Report* website for more information.)

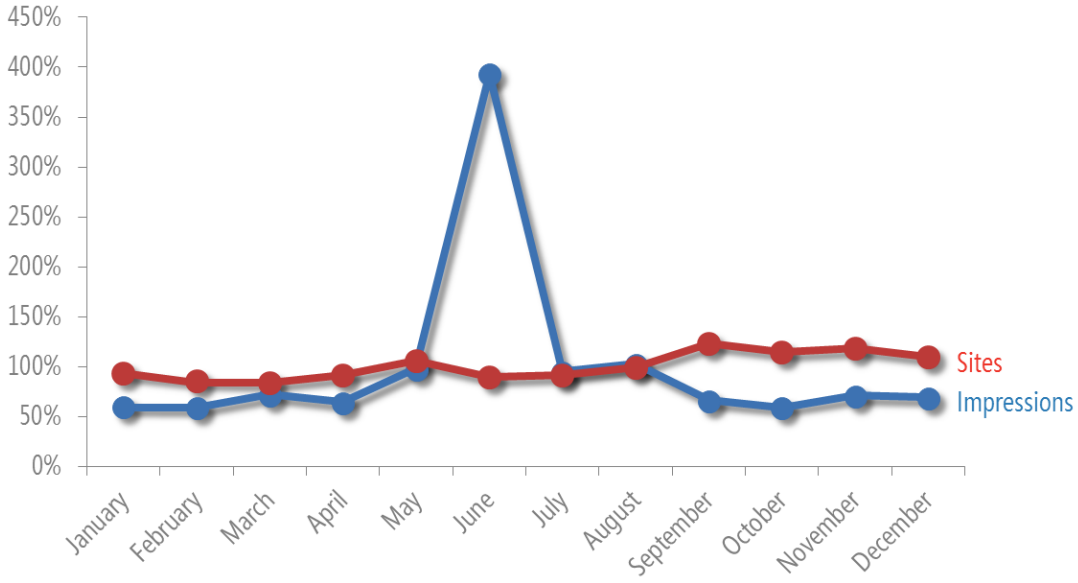
Figure 32. The SmartScreen filter in Internet Explorer 8 and 9 blocks reported phishing and malware distribution sites



Phishing Sites

Figure 33 compares the volume of active phishing sites in the SmartScreen database each month with the volume of *phishing impressions* tracked by 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.

Figure 33. Phishing sites and impressions tracked each month in 2010, relative to the monthly average for each



- Sudden sharp spikes in impressions like the one shown in June are not unusual. Phishers often engage in discrete campaigns that are intended to drive more traffic to each phishing page, without necessarily increasing the total number of active phishing pages they are maintaining at the same time. In this case, the June increase is not strongly correlated with increases in any particular type of target institution.

- Phishing impressions and active phishing pages rarely correlate strongly with each other. The total number of active phishing pages tracked by Microsoft remained very stable from month to month, with no month deviating by more than about 15 percent from the six-month average.

Target Institutions

Figure 34 and Figure 35 show the percentage of phishing impressions and active phishing sites, respectively, recorded by Microsoft during each month in 2010 for the most frequently targeted types of institutions.

Figure 34. Impressions for each type of phishing site each month in 2010

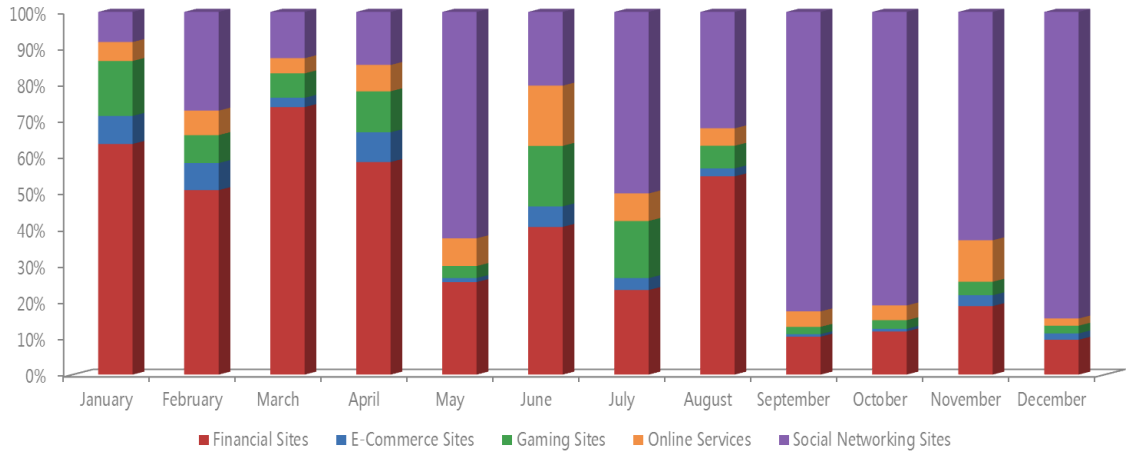
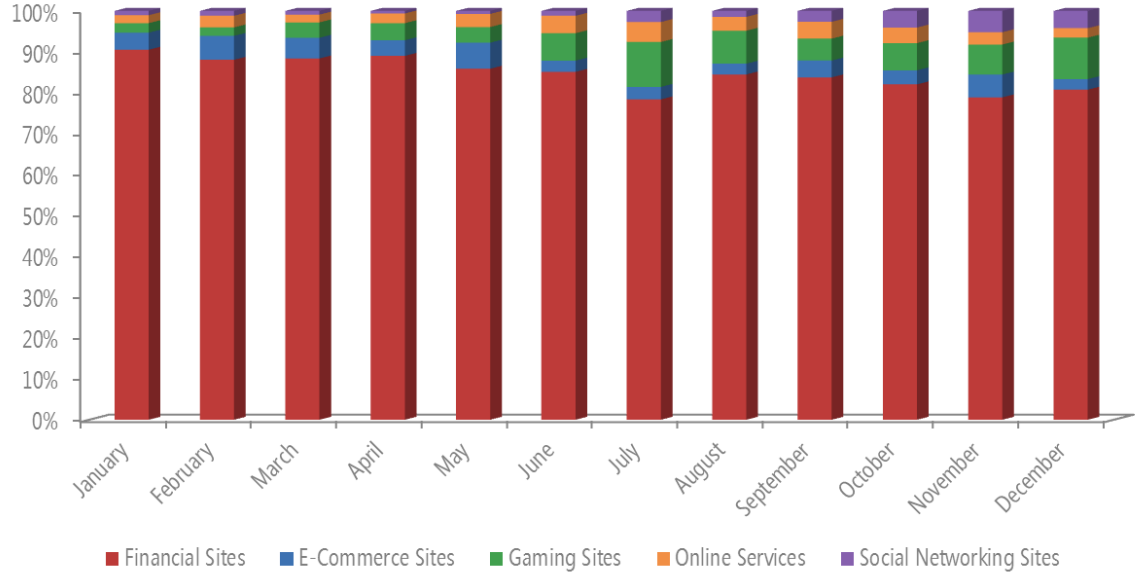


Figure 35. Active phishing sites tracked each month in 2010, by type of target



- Phishers have traditionally targeted financial sites more than other types of sites, but 2010 showed evidence of a shift to social networks. Phishing impressions that targeted social networks increased from a low of 8.3 percent of all impressions in January to a high of 84.5 percent of impressions in December. In particular, the final four months of the year

show signs of a strong and sustained phishing campaign or campaigns against social networks.

- Early in 2010, phishers showed signs of targeting online gaming sites with increased frequency, although this push appears to have dwindled as social networks came under increased attack. Impressions that targeted gaming sites reached a high of 16.7 percent of all impressions in June before dropping to a more typical 2.1 percent in December.

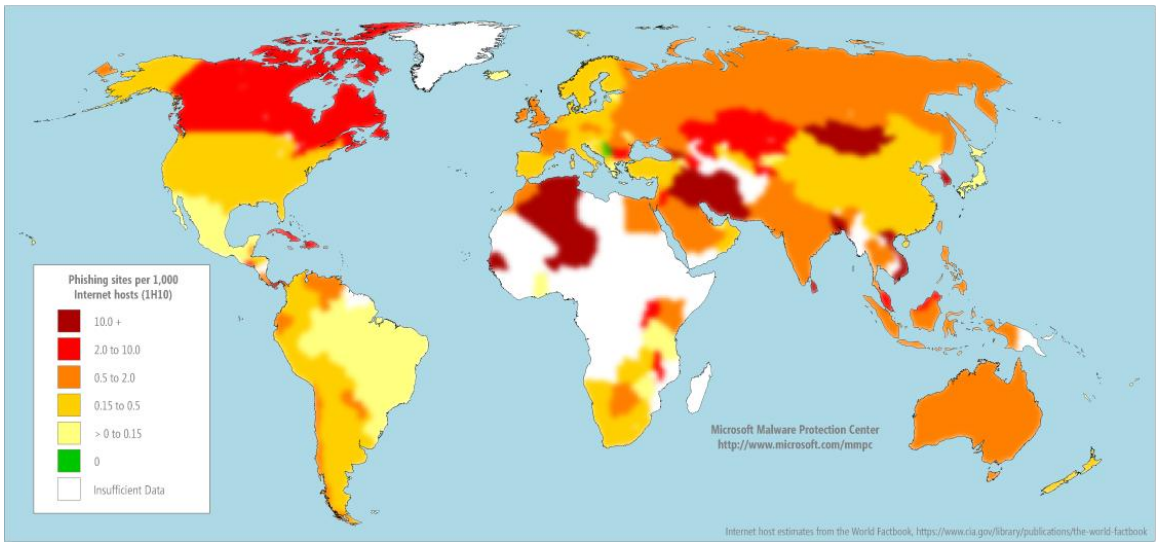
- Phishing sites that target social networks routinely receive the highest number of impressions per active phishing site. The percentage of active phishing sites that targeted social networks increased during the final months of the year, but still only accounted for 4.2 percent of active sites in December, despite receiving 84.5 percent of impressions that month. Nevertheless, the number of active sites targeting gaming sites remained relatively high during the second half of the year, which suggests that more campaigns may be coming.

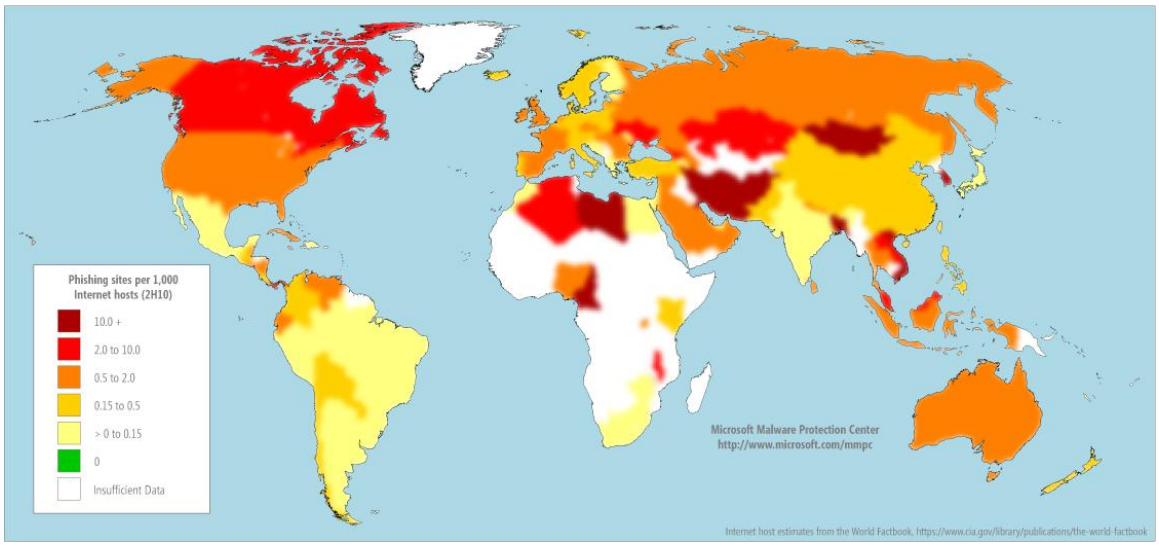
- As in previous periods, phishing sites that targeted financial institutions accounted for the majority of active phishing sites, ranging from 78 to 91 percent of sites each month. Financial institutions targeted by phishers can number in the hundreds, and customized phishing approaches are required for each one. By contrast, just a handful of popular sites account for the bulk of the social network and online service usage on the Internet, so phishers can effectively target many more people per site. Still, the potential for direct illicit access to victims' bank accounts means that financial institutions remain perennially popular phishing targets, and they continue to receive the largest or second-largest number of impressions each month.

Global Distribution of Phishing Sites

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

Figure 36. Phishing sites per 1,000 Internet hosts for locations around the world in 1H10 (top) and 2H10 (bottom)





- The worldwide distribution of phishing sites remained largely consistent between the first and second halves of the year.
- Phishing sites are concentrated in a few locations but have been detected on every inhabited continent.
- Locations with smaller populations and fewer Internet hosts tend to have higher concentrations of phishing pages, although in absolute terms most

phishing pages are located in large, industrialized countries/regions with large numbers of Internet hosts.

Malware Hosting Sites

The SmartScreen filter in Internet Explorer 8 and 9 helps provide protection against sites that are known to host malware, in addition to phishing sites. The SmartScreen antimalware feature uses URL reputation data and Microsoft antimalware technologies to determine whether those servers 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 the SmartScreen filter and to better combat malware distribution. (See Malware Hosts in the "Reference Guide" section of the *Security Intelligence Report* website for more information.)

Figure 37. The SmartScreen filter in Internet Explorer 8 (top) and Internet Explorer 9 (bottom) displays a warning when a user attempts to download an unsafe file

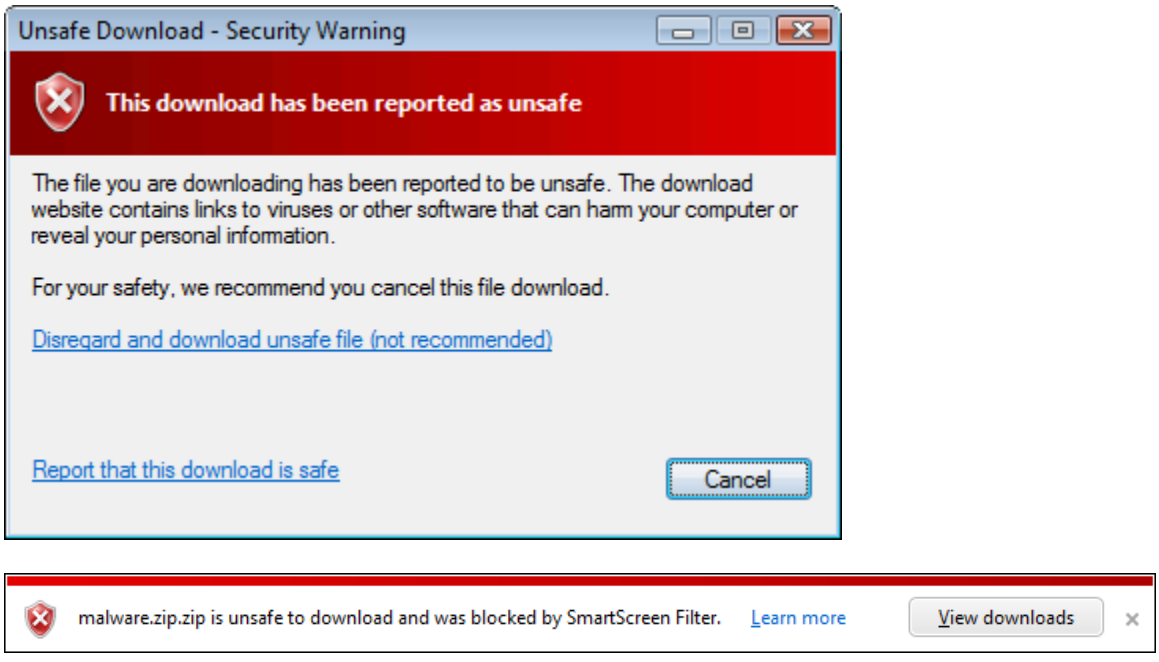
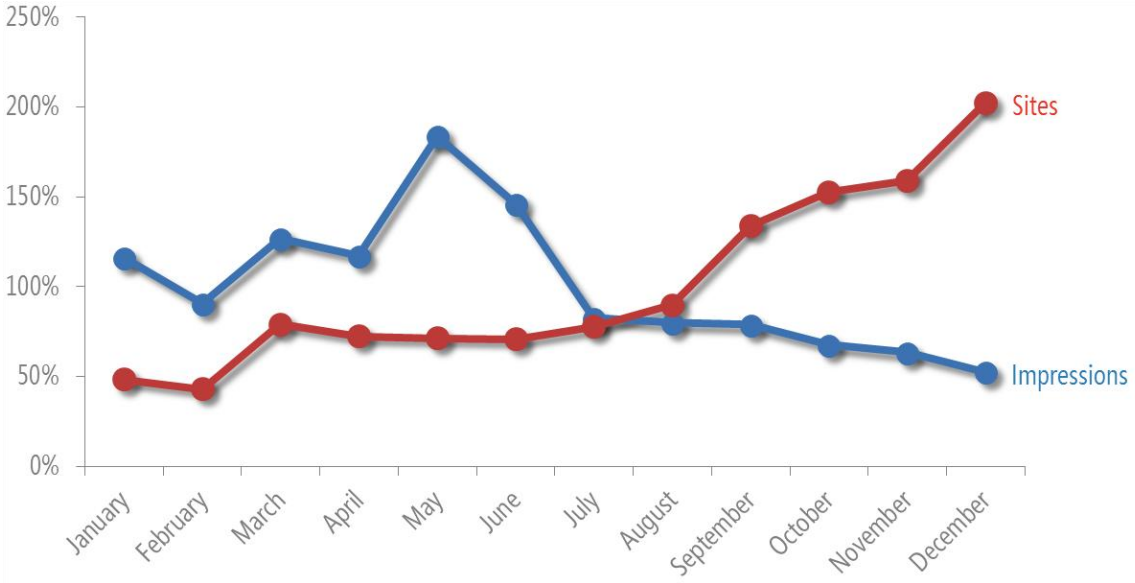


Figure 38 compares the volume of active malware hosting sites in the SmartScreen database each month with the volume of malware impressions tracked by Internet Explorer.

Figure 38. Malware hosting sites and impressions tracked each month in 2010, relative to the monthly average for each



- The number of active malware hosting sites tracked each month increased gradually through the year, mostly because of improved detection.

- After a rising trend during the first five months, the number of malware hosting impressions decreased each month for the rest of the year. Malware host protection in browsers is a relatively new development compared to phishing protection, and it is possible that attackers are reacting by moving away from this method of distribution to other techniques.

Malware Categories

Figure 39 and Figure 40 show the types of threats hosted at URLs that were blocked by the SmartScreen filter in 2H10.

Figure 39. Threats hosted at URLs blocked by the SmartScreen filter in 2010, by category

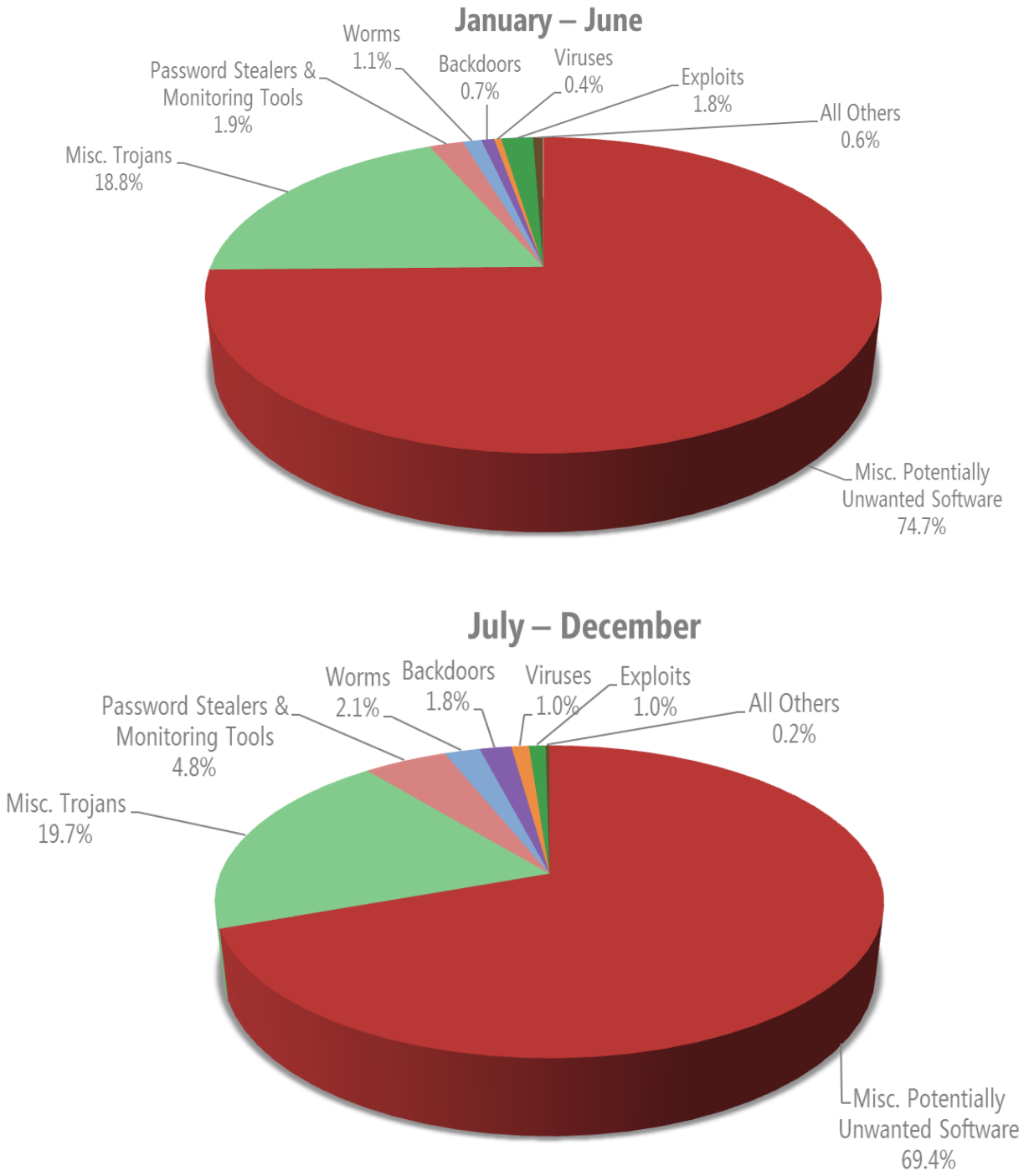


Figure 40. The top 10 malware families hosted on sites blocked by the SmartScreen filter in 1H10 and 2H10, by percent of all such sites

1H10 Rank	Threat Name	Most Significant Category	Percent
1	Win32/MoneyTree	Misc. Potentially Unwanted Software	61.1
2	Win32/FakeXPA	Miscellaneous Trojans	3.3
3	Win32/VBInject	Misc. Potentially Unwanted Software	2.3
4	Win32/Winwebsec	Miscellaneous Trojans	2.0
5	Win32/Obfuscator	Misc. Potentially Unwanted Software	1.9
6	Win32/Pdfjsc	Exploits	1.4
7	Win32/Small	Trojan Downloaders & Droppers	1.3
8	Win32/Bancos	Password Stealers & Monitoring Tools	1.3
9	Win32/Swif	Miscellaneous Trojans	1.2
10	WinNT/Citeary	Misc. Potentially Unwanted Software	1.1

2H10 Rank	Threat Name	Most Significant Category	Percent
1	Win32/MoneyTree	Misc. Potentially Unwanted Software	47.3
2	Win32/Small	Trojan Downloaders & Droppers	5.8
3	Win32/Delf	Trojan Downloaders & Droppers	5.1
4	Win32/Startpage	Miscellaneous Trojans	4.2
5	Win32/Obfuscator	Misc. Potentially Unwanted Software	3.2
6	Win32/Banload	Trojan Downloaders & Droppers	2.8
7	Win32/Bancos	Password Stealers & Monitoring Tools	2.0
8	Win32/Agent	Miscellaneous Trojans	1.1
9	Win32/Microjoin	Trojan Downloaders & Droppers	1.1
10	Win32/Ciucio	Trojan Downloaders & Droppers	1.0

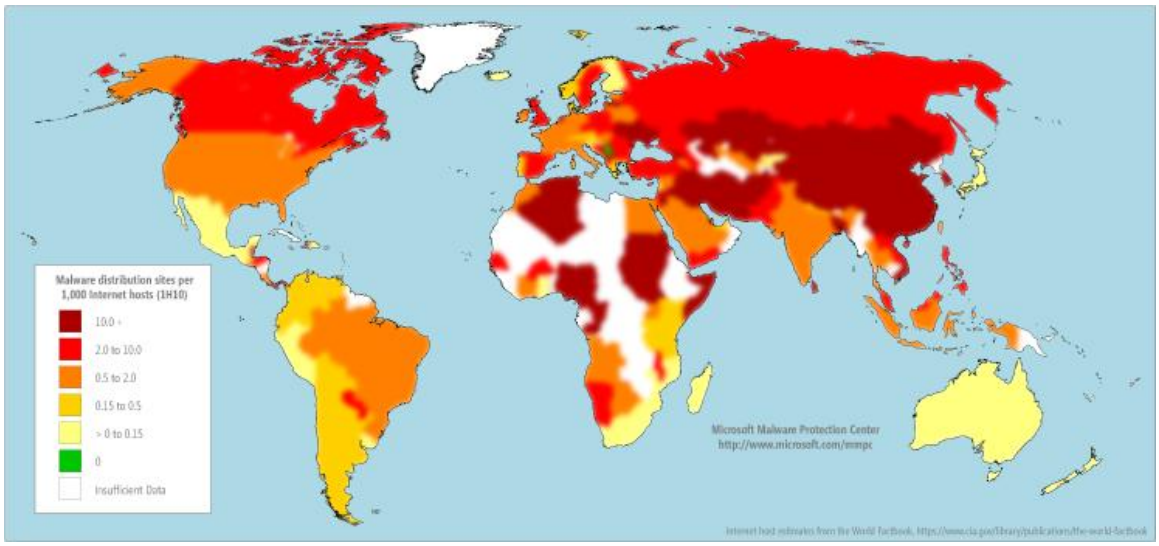
- Overall, sites that hosted the top 10 families constituted 76.9 percent of all malware impressions in the first half of the year and 71.6 percent in the second half.
- Miscellaneous Potentially Unwanted Software consistently accounts for between two-thirds and three-fourths of all malware impressions in most periods, primarily because of Win32/MoneyTree. MoneyTree has been the malware family responsible for the largest number of malware impressions during every six-month period since 1H09.
- Document exploit downloads blocked by the SmartScreen filter decreased from 1.9 percent of the total in 1H10 to 0.96 percent in 2H10. This decrease correlates with the decline in document exploit detections in favor of Java exploits, as shown in Figure 6 on page 19.
- Win32/VBInject, Win32/Obfuscator, Win32/Pdfjsc, Win32/Small, Win32/Startpage, and Win32/Swif are all generic detections for

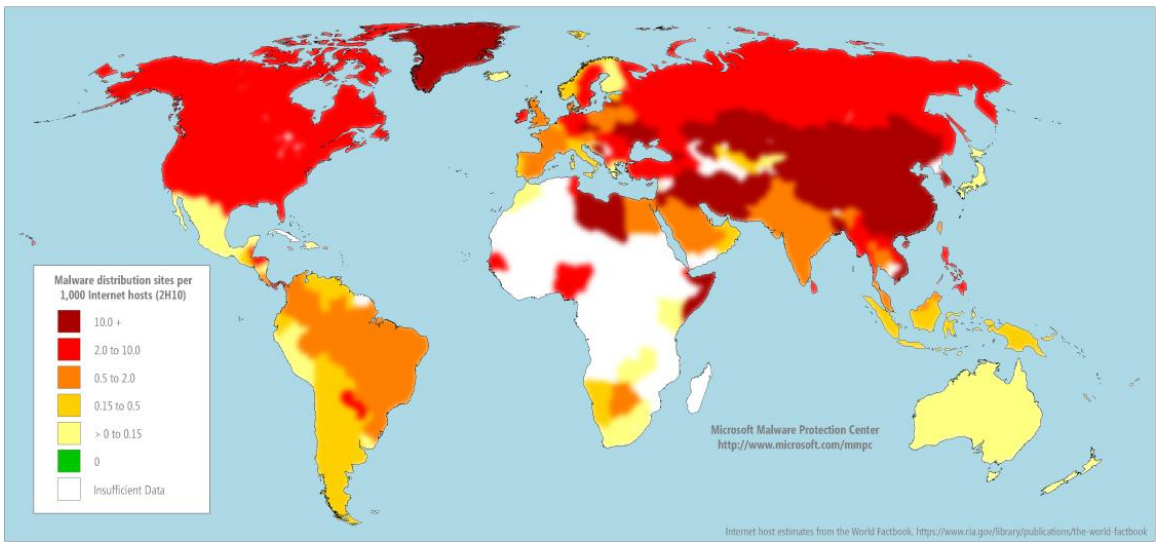
collections of unrelated threats that share certain identifiable characteristics.

Global Distribution of Malware Hosting Sites

Figure 41 shows the geographic distribution of malware hosting sites reported to Microsoft in 2010.

Figure 41. Malware distribution sites per 1,000 Internet hosts for locations around the world in 1H10 (top) and 2H10 (bottom)





- As with phishing sites, the worldwide distribution of sites that host malware remained largely consistent between periods.

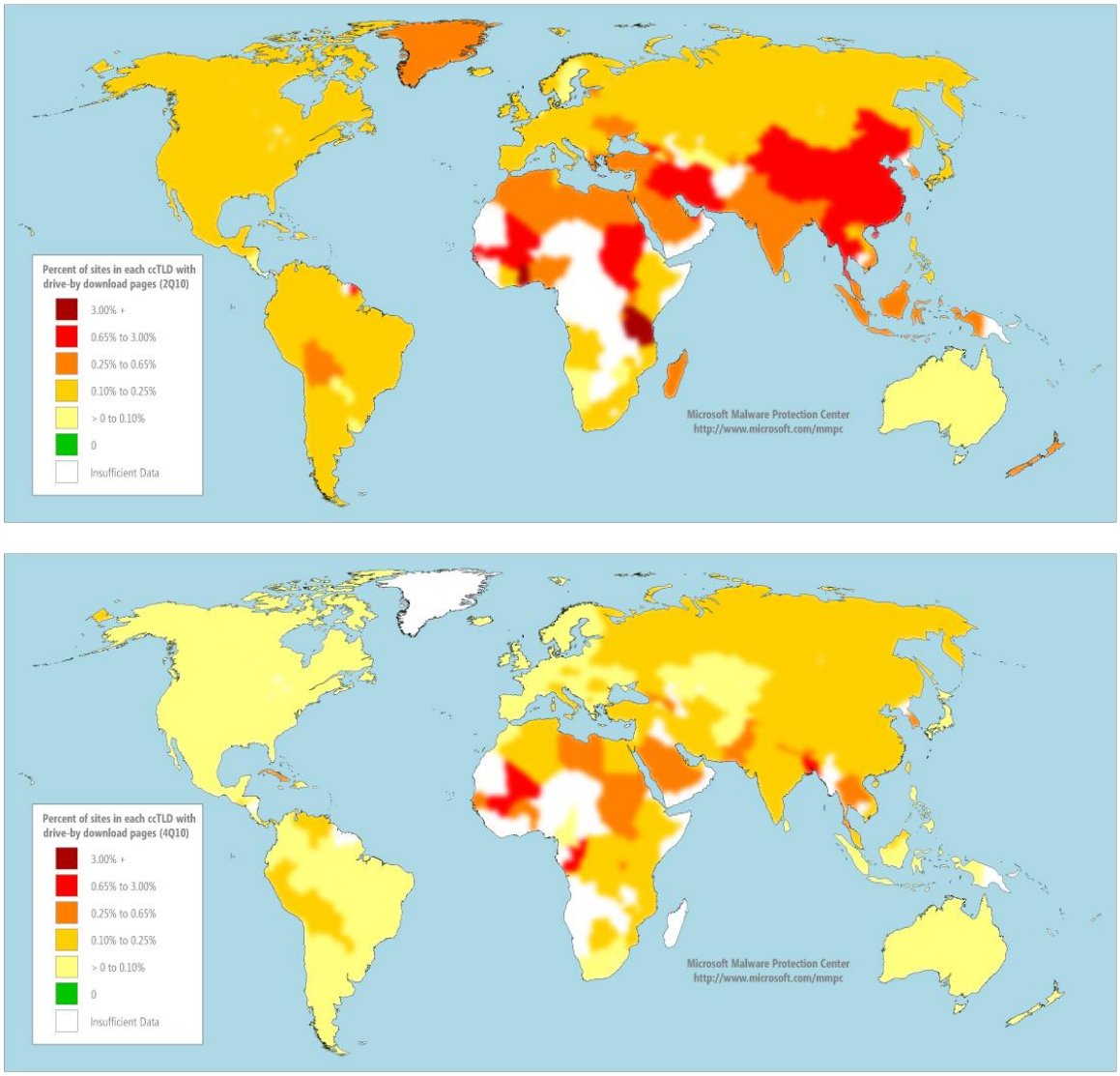
Drive-By Download Sites

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 Microsoft 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 in the "Reference Guide" section of the *Security Intelligence Report* website for more information about how drive-by downloads work and the steps Bing takes to protect users from them.)

The information in this section was generated from an analysis of the country code top-level domains (ccTLDs) of the websites in the Bing index that hosted drive-by download pages in 2010.

Figure 42. Percentage of websites in each country-code top-level domain (ccTLD) that hosted drive-by pages in 2Q10 (top) and 4Q10 (bottom)



- In 2H10, drive-by download pages appeared on about 2.4 of every 1,000 search results pages displayed to users during that time.

- Overall, the most heavily infected ccTLDs were small ones. Small TLDs are susceptible to large swings in infection rates because of their size. For example, if a major ISP in a small country or region were to become compromised by an attacker, a large percentage of the domains in the associated ccTLD could be affected.

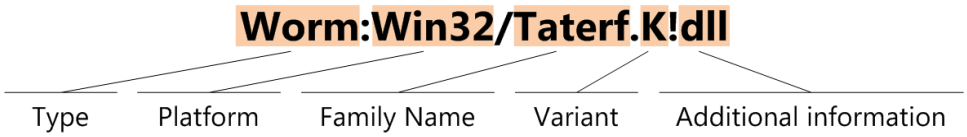
- Figure 42 does not reflect the physical locations of hosted sites; not all ccTLD sites are hosted in the locations to which the ccTLDs themselves are assigned. However, most ccTLD sites are targeted at Internet users in a particular country/region and are typically written in an appropriate language, so Figure 42 can be considered a reasonable indicator of how users in different parts of the world are more or less at risk of encountering drive-by download pages.

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 43.

Figure 43. 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 *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.

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) 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 PWS:Win32/Frethog.C and TrojanDownloader:Win32/Frethog.C, among others. In the *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 *Security Intelligence Report,* a threat name consisting 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 is referred to simply as "Taterf" on subsequent mention in some places, and Worm:Win32/Taterf.K simply as "Taterf.K."

Appendix B: Data Sources

Microsoft Products and Services

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 allows the *Security Intelligence 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. Once detected, Bing displays warnings to users about the malicious content to help prevent infection.

- Windows Live® Hotmail® has hundreds of millions of active email users in more than 30 countries/regions around the world.

- Forefront Online Protection for Exchange (FOPE) protects the networks of thousands of enterprise customers worldwide by helping to prevent malware from spreading through email. FOPE scans billions of email messages every year to identify and block spam and malware.

- Windows Defender is a program that is available at no cost to licensed users of Windows that provides real-time protection against pop-ups, slow performance, and security threats caused by spyware and other potentially unwanted software. Windows Defender runs on more than 100 million computers worldwide.

- The Malicious Software Removal Tool (MSRT) is a free tool that Microsoft designed to help identify and remove prevalent malware families from customer computers. 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. MSRT was downloaded and executed 3.2 billion times in 1H10, or nearly 600 million times each month on average. 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.

- Microsoft Forefront Endpoint Protection (formerly Forefront Client Security) is a unified product that provides protection from malware and potentially unwanted software for enterprise desktops, laptops, and server operating systems. Like Windows Live OneCare, it uses the Microsoft Malware Protection Engine and the Microsoft antivirus signature database to provide real-time, scheduled, and on-demand protection.

- Microsoft Security Essentials is a real-time protection product that combines an antivirus and antispyware scanner with phishing and firewall protection.

- The Windows Live OneCare safety scanner (http://safety.live.com) is a free online tool that uses the same definition database as the Microsoft desktop anti-malware products to detect and remove malware and potentially unwanted software. The Windows Live OneCare 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 user's computer from becoming infected.

- Microsoft Security Essentials is a basic, consumer-oriented anti-malware product, offered at no charge to licensed users of Windows, which provides real-time protection against viruses, spyware, and other harmful software.

- The SmartScreen filter in Internet Explorer 8 and 9 offers Internet Explorer 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.

Appendix C: Worldwide Infection Rates

"Global Infection Rates," on page 27, explains how threat patterns differ significantly in different parts of the world. Figure 44 shows the infection rates in locations with at least 100,000 quarterly MSRT executions in 2010. (CCM is the number of computers cleaned for every 1,000 executions of MSRT. See the *Security Intelligence Report* website for more information about the CCM metric.)

Figure 44. Infection rates (CCM) for locations around the world in 2010, by quarter

Country/Region	1Q10	2Q10	3Q10	4Q10
Albania	5.6	3.3	3.1	2.6
Algeria	2.2	2.1	2.4	2.7
Angola	5.4	4.6	5.5	3.9
Argentina	9.3	9.7	11.4	9.2
Armenia	–	–	–	2.4
Australia	7.2	5.9	6.2	5.5
Austria	3.8	3.0	3.5	3.3
Azerbaijan	2.9	2.6	4.2	2.8
Bahamas, The	7.3	7.2	6.9	5.4
Bahrain	14.9	15.6	13.6	9.0
Bangladesh	1.2	1.5	1.5	1.5
Barbados	2.6	2.2	2.3	1.5
Belarus	2.0	1.3	1.5	1.5
Belgium	10.1	7.0	7.5	6.1
Bolivia	7.7	7.8	7.1	5.7
Bosnia and Herzegovina	13.7	10.7	10.6	8.3
Brazil	26.1	25.8	26.3	20.8
Brunei	7.7	7.0	8.0	6.6
Bulgaria	10.0	9.0	10.1	9.9
Cambodia	–	–	–	1.5

Country/Region	1Q10	2Q10	3Q10	4Q10
Cameroon	3.9	3.2	3.3	2.8
Canada	5.2	4.5	4.9	4.2
Chile	12.9	12.9	14.9	12.5
China	8.1	5.5	4.5	2.9
Colombia	16.0	13.5	12.6	10.0
Costa Rica	16.4	12.6	11.9	13.2
Côte d'Ivoire	3.9	2.3	2.4	1.8
Croatia	20.4	15.8	14.1	13.4
Cyprus	9.9	9.3	9.0	7.9
Czech Republic	7.1	5.5	6.2	8.0
Denmark	6.0	4.1	4.9	3.9
Dominican Republic	8.9	7.4	7.9	6.9
Ecuador	17.3	12.9	12.0	8.9
Egypt	9.7	9.0	10.0	11.4
El Salvador	20.6	20.5	19.1	15.2
Estonia	11.9	6.0	8.1	5.9
Ethiopia	—	—	1.3	1.0
Finland	3.7	2.1	3.8	2.3
France	15.5	12.4	12.8	9.8
Georgia	7.9	7.1	7.7	7.3
Germany	5.5	4.6	5.6	5.3
Ghana	2.9	1.6	1.5	1.2
Greece	18.7	15.4	17.5	14.0
Guadeloupe	3.5	3.0	3.6	2.8
Guatemala	16.1	13.3	13.2	10.2
Honduras	14.8	12.6	13.9	11.0
Hong Kong S.A.R.	9.4	9.1	8.8	6.3
Hungary	19.4	15.2	14.9	11.1
Iceland	12.5	7.7	7.1	5.9
India	4.6	3.4	4.1	3.2
Indonesia	3.2	2.7	10.8	7.1
Iraq	7.2	6.7	9.8	10.0
Ireland	7.6	6.4	7.3	6.2
Israel	15.2	12.2	13.6	11.0

Country/Region	1Q10	2Q10	3Q10	4Q10
Italy	12.0	9.7	10.3	8.9
Jamaica	5.4	3.7	3.6	2.5
Japan	5.1	4.4	4.6	3.3
Jordan	8.6	7.4	8.4	8.7
Kazakhstan	2.5	2.2	2.5	2.8
Kenya	3.4	2.7	2.9	2.5
Korea	34.4	34.4	30.1	40.3
Kuwait	13.2	11.5	14.6	12.0
Latvia	12.4	10.8	10.8	9.4
Lebanon	6.5	5.6	6.0	4.8
Libya	4.4	4.1	4.7	4.4
Lithuania	13.4	10.1	11.2	10.5
Luxembourg	8.2	7.1	7.9	6.9
Macao S.A.R.	3.2	2.8	2.7	2.1
Macedonia, F.Y.R.O.	9.6	8.0	7.7	6.6
Malaysia	7.6	6.2	6.8	5.1
Malta	6.3	5.9	5.8	4.3
Martinique	3.9	3.7	5.0	3.7
Mauritius	4.7	4.8	5.0	4.9
Mexico	23.9	21.4	21.1	17.4
Moldova	3.3	2.0	2.1	1.6
Mongolia	1.7	1.1	1.3	1.0
Montenegro	7.7	5.3	5.7	4.6
Morocco	2.7	1.9	1.9	1.6
Mozambique	–	–	8.4	6.9
Nepal	2.3	2.0	2.0	1.8
Netherlands	9.0	6.1	7.3	5.8
Netherlands Antilles	3.0	2.5	2.5	2.2
New Zealand	6.6	4.9	5.7	4.9
Nicaragua	13.5	13.8	11.7	9.1
Nigeria	3.5	3.2	3.7	2.8
Norway	6.6	4.7	5.0	3.8
Oman	13.2	10.0	10.3	9.0
Pakistan	2.4	2.1	2.1	1.8

Country/Region	1Q10	2Q10	3Q10	4Q10
Palestinian Authority	5.1	4.5	5.0	4.8
Panama	14.5	11.5	13.6	11.7
Paraguay	4.9	5.1	4.9	3.4
Peru	16.2	19.2	16.7	13.5
Philippines	3.0	3.3	3.5	2.8
Poland	23.6	21.8	22.6	17.3
Portugal	23.0	18.1	19.3	15.6
Puerto Rico	5.0	4.0	4.4	3.6
Qatar	8.9	7.9	7.6	6.4
Réunion	2.8	2.7	4.0	3.0
Romania	6.8	5.7	7.0	5.4
Russia	12.4	11.5	11.1	10.1
Saudi Arabia	17.3	16.8	17.9	15.8
Senegal	3.4	2.6	2.4	1.9
Serbia	7.7	5.3	5.7	4.6
Singapore	9.2	8.0	11.1	11.0
Slovakia	8.8	7.6	8.3	8.5
Slovenia	14.8	10.0	9.8	9.1
South Africa	12.8	11.9	11.8	9.8
Spain	39.2	35.7	36.3	33.2
Sri Lanka	2.3	1.8	2.0	1.7
Sweden	8.0	5.2	5.9	4.4
Switzerland	5.0	4.0	4.7	4.1
Taiwan	29.3	33.5	31.7	24.3
Tanzania	4.3	3.9	4.3	3.1
Thailand	14.6	15.3	17.4	14.5
Trinidad and Tobago	5.6	5.1	6.1	4.6
Tunisia	2.5	1.8	1.9	1.6
Turkey	35.5	36.6	42.4	32.8
Uganda	—	—	4.4	2.8
Ukraine	4.0	3.6	3.3	3.1
United Arab Emirates	9.5	8.4	9.0	7.5
United Kingdom	7.9	6.7	7.4	8.7
United States	14.8	12.9	13.5	11.6

Country/Region	1Q10	2Q10	3Q10	4Q10
Uruguay	3.7	4.4	5.1	3.1
Venezuela	9.9	9.5	9.8	9.7
Vietnam	2.2	2.1	2.1	1.6
Worldwide	**10.8**	**9.6**	**9.9**	**8.7**

Glossary

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 access to infected computers. Bots are a sub- category 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 nodes or zombies.

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

CCM
Short for *computers cleaned per mille* (thousand). The number of computers cleaned for every 1,000 executions of 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 ÷ 50,000 × 1,000).

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

command and control
See *botnet*.

definition
A set of *signatures* that can be used to identify malware by using antivirus or antispyware products. Other vendors may refer to definitions as DAT files, pattern files, identity files, or antivirus databases.

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

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

downloader/dropper
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.

Internet Relay Chat (IRC)
A distributed real-time Internet chat protocol that is designed for group communication. Many botnets use the IRC protocol for C&C.

keylogger
A program that sends keystrokes or screen shots to an attacker. Also see *password stealer (PWS)*.

Malicious Software Removal Tool
The Microsoft Windows Malicious Software Removal Tool (MSRT) is designed to help identify and remove specifically targeted, prevalent malware from customer computers and is available at no charge to licensed Windows users. The main release mechanism of MSRT is through Windows Update (WU), Microsoft Update (MU), or Automatic Updates (AU). A version of the tool is also available for download from the Microsoft Download Center. MSRT is not a replacement for an up-to-date antivirus solution, because it specifically targets only a small subset of malware families that are determined to be especially prevalent. In addition, MSRT includes no real-time protection and cannot be used to prevent malware from initially infecting a computer. More details about MSRT are available at www.microsoft.com/security/malwareremove/default.mspx.

malware
Malware is any software that's been designed specifically to cause damage to a user's computer, server, or network. Viruses, worms, trojans, and spyware are all types of malware.

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)*.

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

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

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 7, 8, or 9, and being blocked by the Phishing Filter or SmartScreen filter. Also see *malware impression*.

pop-under
A webpage that opens in a separate window that appears beneath the active browser window. Pop-under windows are commonly used to display advertisements.

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.

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.

rootkit
A program whose main purpose is to perform certain functions that cannot be easily detected or undone by a system administrator, such as hiding itself or other malware.

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

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.

tool
Software 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.

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

Threat Families Referenced in This Report

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

Win32/Agent. A generic detection for a number of trojans that may perform different malicious functions. The functionality exhibited by this family is highly variable.

Win32/Alureon. A data-stealing trojan that gathers confidential information such as user names, passwords, and credit card data from incoming and outgoing Internet traffic. It may also download malicious data and modify DNS settings.

Win32/Autorun. A family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.

Win32/BaiduSobar. A Chinese-language Web browser toolbar that delivers pop-up and contextual advertisements, blocks certain other advertisements, and changes the Internet Explorer search page.

Win32/Bancos. A data-stealing trojan that captures online banking credentials and relays them to the attacker. Most variants target customers of Brazilian banks.

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

Win32/Ciucio. A family of trojans that connect to certain websites in order to download arbitrary files.

WinNT/Citeary. A kernel mode driver installed by Win32/Citeary, a worm that spreads to all available drives including the local drive, installs device drivers and attempts to download other malware from a predefined website.

Win32/ClickPotato. A program that displays popup and notification-style advertisements based on the user's browsing habits.

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/Cutwail. A trojan that downloads and executes arbitrary files, usually to send spam. Win32/Cutwail has also been observed to download the attacker tool Win32/Newacc.

JS/CVE-2010-0806. A detection for malicious JavaScript that attempts to exploit the vulnerability addressed by Microsoft Security Bulletin MS10-018.

Win32/Delf. A detection for various threats written in the Delphi programming language. The behaviors displayed by this malware family are highly variable.

Win32/FakeCog. A rogue security software family distributed under the names Defense Center, AntiMalware, and many others.

Win32/FakePAV. A rogue security software family that masquerades as Microsoft Security Essentials.

Win32/FakeRean. A rogue security software family distributed under a variety of randomly generated names, including Win 7 Internet Security 2010, Vista Antivirus Pro, XP Guardian, and many others.

Win32/FakeSpypro. A rogue security software family distributed under the names Antivirus System PRO, Spyware Protect 2009, and others.

Win32/FakeVimes. A rogue security software family distributed under the names Ultra Antivir 2009, Extra Antivirus, Virus Melt, and many others.

Win32/FakeXPA. A rogue security software family distributed under the names Antivirus 7, Personal Security, AntiVir2010, Antivirus BEST, Green AV, MaCatte, and many others.

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

Win32/Hamweq. A worm that spreads through removable drives, such as USB memory sticks. It may contain an IRC-based backdoor that enables the computer to be controlled remotely by an attacker.

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

Win32/Keygen. A generic detection for tools that generate product keys for illegally obtained versions of various software products.

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/MoneyTree. A family of software that provides the ability to search for adult content on local disks. It may also install other potentially unwanted software, such as programs that display pop-up ads.

Win32/Nbar. A program that may display advertisements and redirect user searches to a certain website. It may also download malicious or unwanted content into the system without user consent.

Win32/Obfuscator. A generic detection for programs that have had their purpose disguised to hinder analysis or detection by anti-virus 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, My Vaccine, and others.

Win32/Parite. A family of viruses that infect .exe and .scr executable files on the local file system and on writeable network shares.

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/Pornpop. A generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.

Win32/RealVNC. A management tool that allows a computer to be controlled remotely. It can be installed for legitimate purposes but can also be installed from a remote location by an attacker.

Win32/Renos. A family of trojan downloaders that install rogue security software.

Win32/Rimecud. A family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.

Win32/Rustock. A multi-component family of rootkit-enabled backdoor trojans that were first developed around 2006 to aid in the distribution of spam email.

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.

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

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

Win32/Sogou. A Chinese-language browser toolbar that may display popup advertisements and may download and install additional components without user consent.

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/Swif. A generic detection for maliciously-crafted SWF (Small Web Format) files. SWF files are commonly used for graphics and video online and are developed for the Adobe Flash platform.

Win32/Taterf. A family of worms that spread through mapped drives to steal login and account details for popular online games.

Win32/VBInject. A generic detection for obfuscated malware. The loader is written in Microsoft Visual Basic® and the malicious code, which may have virtually any purpose, is encrypted.

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, System Security, and others.

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

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