# Microsoft Security Intelligence Report

*Volume 11*

*An in-depth perspective on software vulnerabilities and exploits, malicious code threats, and potentially unwanted software in the first half of 2011*

# WORLDWIDE THREAT ASSESSMENT

Microsoft

# Microsoft Security Intelligence Report

## Authors


**Joe Faulhaber**
*Microsoft Malware Protection Center*

**David Felstead**
*Bing*

**Paul Henry**
*Wadeware LLC*

**Jeff Jones**
*Microsoft Trustworthy Computing*

**Ellen Cram Kowalczyk**
*Microsoft Trustworthy Computing*

**Jimmy Kuo**
*Microsoft Malware Protection Center*

**John Lambert**
*Microsoft Security Engineering Center*

**Marc Lauricella**
*Microsoft Trustworthy Computing*

**Aaron Margosis**
*Microsoft Public Sector Services*

**Michelle Meyer**
*Microsoft Trustworthy Computing*

**Anurag Pandit**
*Windows Live Safety Platform*

**Anthony Penta**
*Windows Live Safety Platform*

**Dave Probert**
*Microsoft Security Engineering Center*

**Tim Rains**
*Microsoft Trustworthy Computing*

**Mark E. Russinovich**
*Microsoft Technical Fellow*

**Weijuan Shi**
*Windows Business Group*

**Adam Shostack**
*Microsoft Trustworthy Computing*

**Frank Simorjay**
*Microsoft Trustworthy Computing*

**Hemanth Srinivasan**
*Microsoft Malware Protection Center*

**Holly Stewart**
*Microsoft Malware Protection Center*

**Matt Thomlinson**
*Microsoft Security Response Center*

**Jeff Williams**
*Microsoft Malware Protection Center*

**Scott Wu**
*Microsoft Malware Protection Center*

***Terry Zink***
*Microsoft Forefront Online Protection for Exchange*


## Contributors


**Roger Capriotti**
*Windows Live Safety Platform*

**Doug Cavit**
*Microsoft Trustworthy Computing*

**CSS Japan Security Response Team**
*Microsoft Japan*

**Dave Forstrom**
*Microsoft Trustworthy Computing*

**Eric Foster**
*Windows Live Safety Platform*

**Enrique Gonzalez**
*Microsoft Malware Protection Center*

**Heather Goudey**
*Microsoft Malware Protection Center*

**Vinny Gullotto**
*Microsoft Trustworthy Computing*

**Satomi Hayakawa**
*CSS Japan Security Response Team*

**Forbes Higman**
*Windows Live Safety Platform*

**Yuhui Huang**
*Microsoft Malware Protection Center*

**Aaron Hulett**
*Microsoft Malware Protection Center*

**Hilda Larina Ragragio**
*Microsoft Malware Protection Center*

**Eric Lawrence**
*Windows Live Safety Platform*

**Ken Malcolmson**
*Microsoft Trustworthy Computing*

**Takumi Onodera**
*Microsoft Premier Field Engineering, Japan*

**Daryl Pecelj**
*Microsoft IT Information Security and Risk Management*

**Kathy Phillips**
*Microsoft Legal and Corporate Affairs*

**Tareq Saade**
*Microsoft Malware Protection Center*

**Richard Saunders**
*Microsoft Trustworthy Computing*

**Jasmine Sesso**
*Microsoft Malware Protection Center*

**Norie Tamura**
*CSS Japan Security Response Team*

**Matt Thomlinson**
*Microsoft Trustworthy Computing*

**Patrik Vicol**
*Microsoft Malware Protection Center*

**Steve Wacker**
*Wadeware LLC*

# Table of Contents

# Microsoft Security Intelligence Report, Volume 11

Volume 11 of the *Microsoft® Security Intelligence Report* (*SIRv11*) provides in-depth perspectives on software vulnerabilities and exploits, malicious code threats, and potentially unwanted software in Microsoft and third-party software. Microsoft developed these perspectives based on detailed trend analyses over the past several years, with a focus on the first half of 2011.

This document contains statistics and trends related to the state of computer security and threats around the world in a range of different areas. The full report also includes deep analysis of trends found in more than 100 countries/regions around the world and offers ways to manage risks to your organization, software, and people.

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

# 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 exploit the compromised system by causing it to run arbitrary code without the user's knowledge.

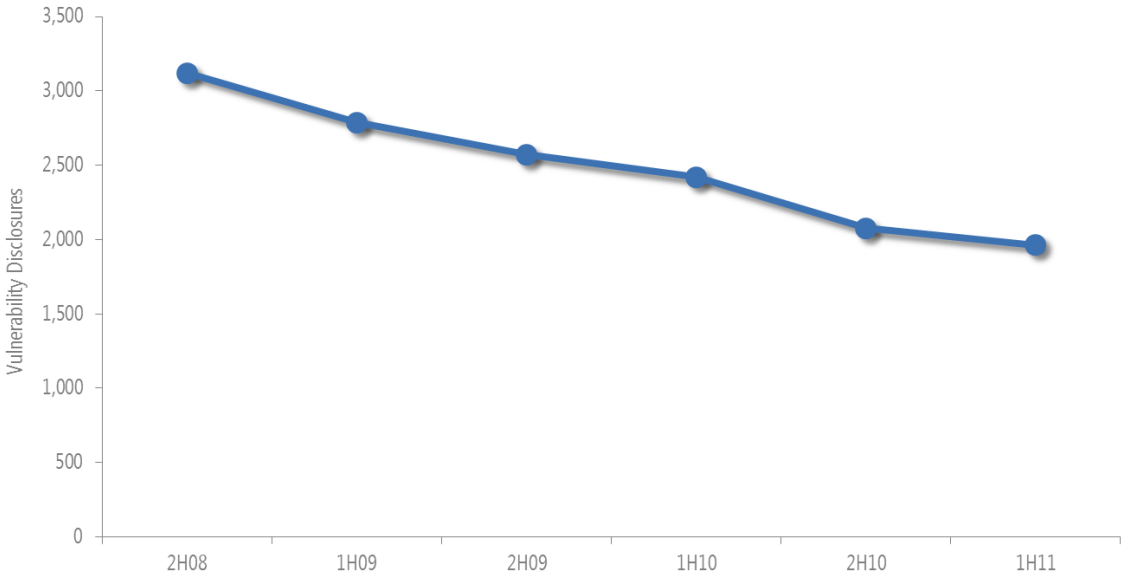
## Industry-Wide Vulnerability Disclosures

A *disclosure*, as the term is used in the *Microsoft Security Intelligence Report*, is the revelation of a software vulnerability to the public at large. It does not refer to any type of private disclosure or disclosure to a limited number of people. Disclosures can come from a variety of sources, including the software vendor, 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. It represents all disclosures that have a CVE (Common Vulnerabilities and Exposures) number.

Figure 1 illustrates the number of vulnerability disclosures across the software industry for each half-year period since 2H08. (See "About This Report" in the full report for an explanation of the reporting period nomenclature used in this report.)

Figure 1. Industry-widevulnerability disclosures, 2H08–1H11



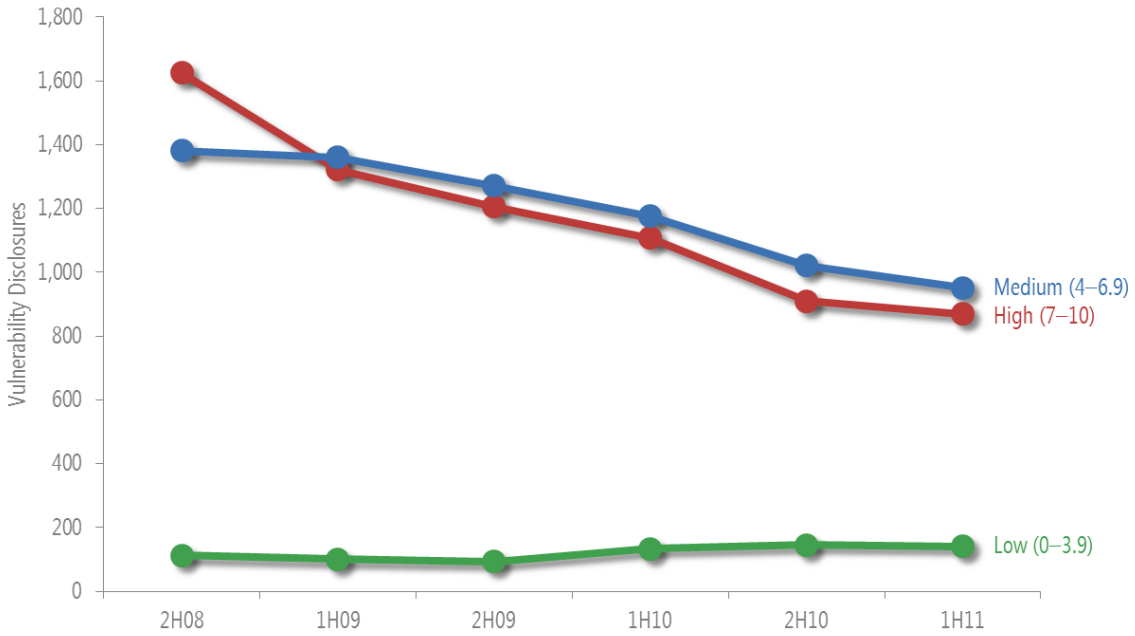

- Vulnerability disclosures across the industry in 1H11 were down 5.5 percent from 2H10, and down 37.1 percent from 2H08.

- 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 results in more secure software and fewer vulnerabilities. (See Protecting Your Software in the "Managing Risk" section of the *Microsoft Security Intelligence Report* website for additional details and guidance about secure development practices.)

## Vulnerability Severity

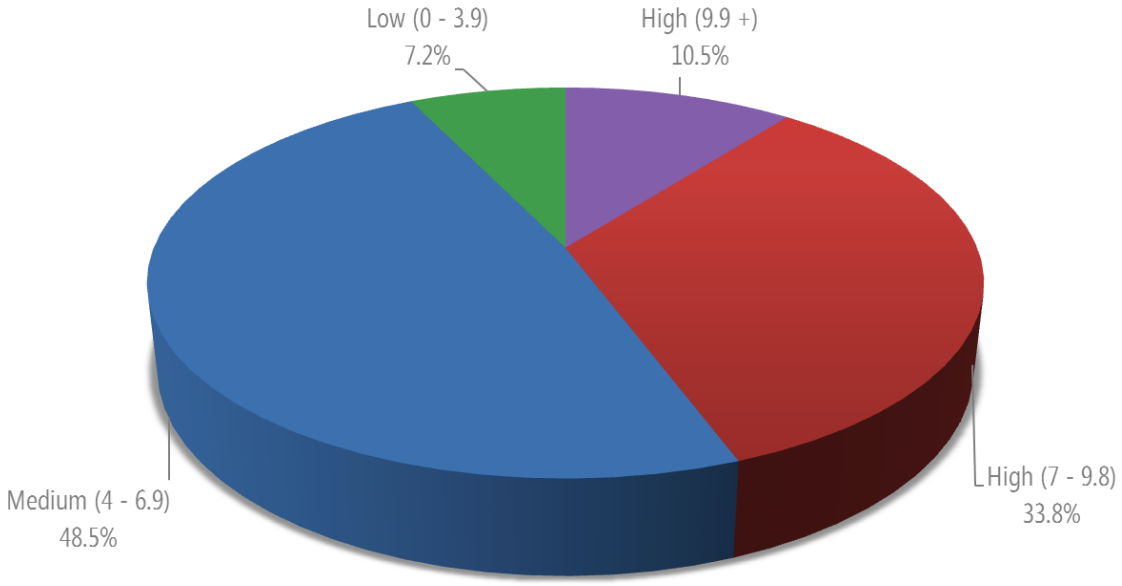
The Common Vulnerability Scoring System (CVSS) is a standardized, platform-independent scoring system for rating IT vulnerabilities. The CVSS assigns a numeric value between 0 and 10 to vulnerabilities according to severity, with higher scores representing greater severity. (See Vulnerability Severity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

Figure 2. Industry-wide vulnerability disclosures by severity, 2H08–1H11




- The overall vulnerability severity trend has been a positive one. Medium and High severity vulnerabilities disclosed in 1H11 were down 6.8 percent and 4.4 percent from 2H10, respectively.
- Even as fewer vulnerabilities are being disclosed overall, the number of Low severity vulnerabilities being disclosed has increased slightly. Low severity vulnerabilities accounted for 7.2 percent of all vulnerabilities disclosed in 1H11.
- Mitigating the most severe vulnerabilities first is a security best practice. High severity vulnerabilities that scored 9.9 or greater represent 10.5 percent of all vulnerabilities disclosed in 1H11, as Figure 3 illustrates.

Figure 3. Industry-wide vulnerability disclosures in 1H11, by severity

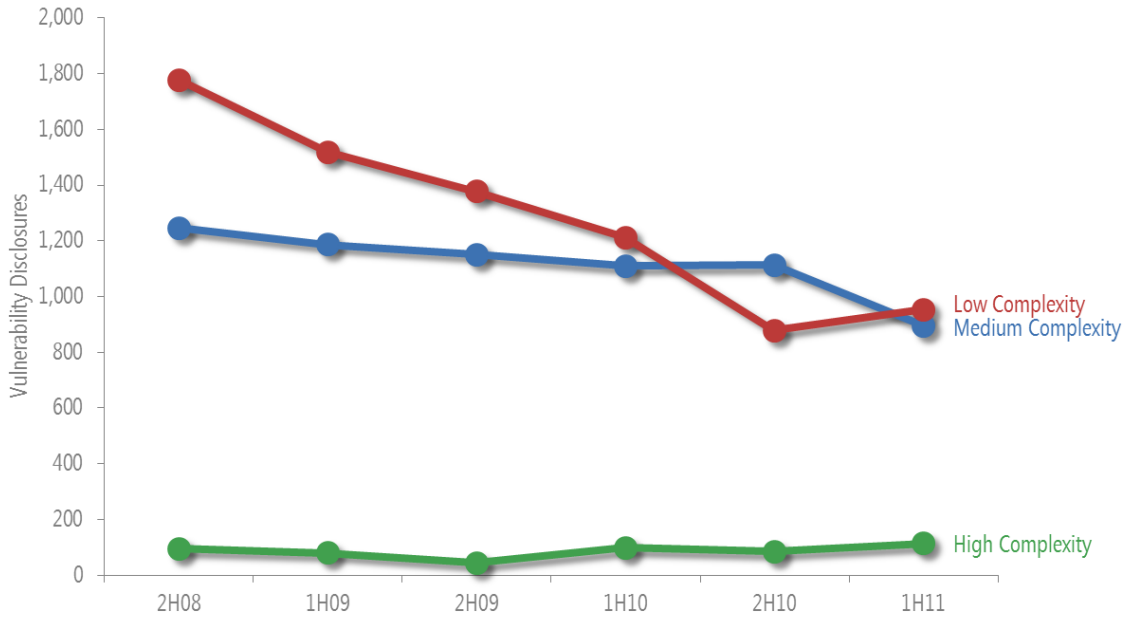



## Vulnerability Complexity

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 at the *Microsoft Security Intelligence Report* website for more information about the CVSS complexity ranking system.) Figure 4 shows complexity trends for vulnerabilities disclosed since July 2006. Note that Low complexity indicates greater danger, just as High severity indicates greater danger in Figure 2.

Figure 4. Industry-wide vulnerability disclosures by access complexity, 2H08–1H11

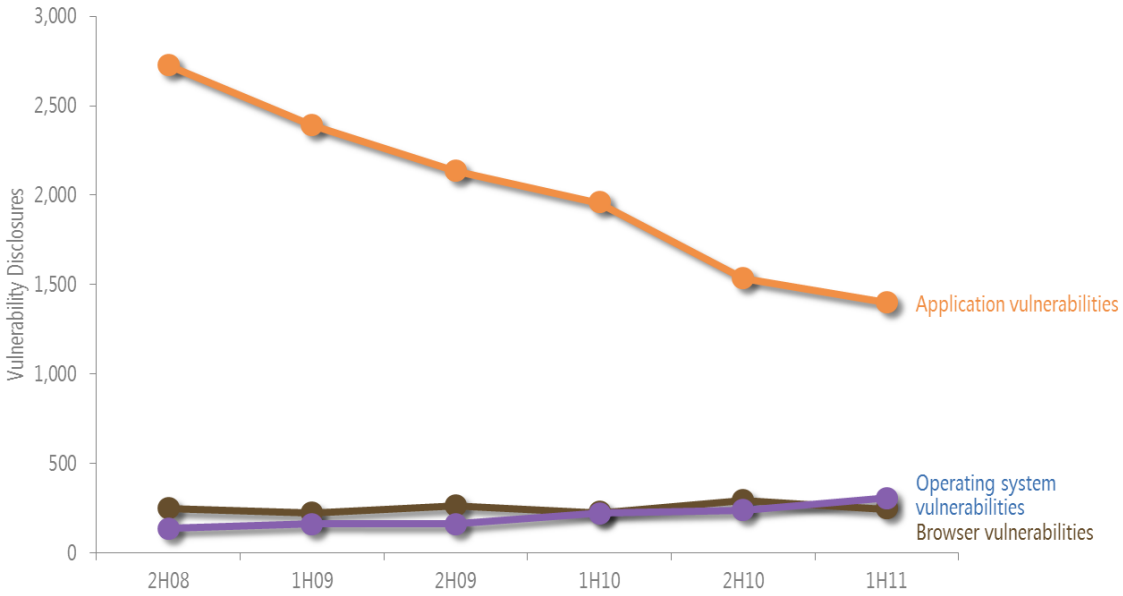



- As with vulnerability severity, the trend here is a positive one, with Low complexity vulnerabilities—the easiest ones to exploit—down 41.2 percent from the prior 12-month period.
- High complexity vulnerability disclosures, meanwhile, have increased slightly. They accounted for 4.9 percent of all vulnerabilities disclosed between July 2010 and June 2011, up from 2.8 percent in the prior 12-month period.

## Operating System, Browser, and Application Vulnerabilities

Figure 5 shows industry-wide vulnerabilities for operating systems, browsers, and applications since July 2006. (See Operating System, Browser, and Application Vulnerabilities at the *Microsoft Security Intelligence Report* website for an explanation of how operating system, browser, and application vulnerabilities are distinguished.)

Figure 5. Industry-wide operating system, browser, and application vulnerabilities, 2H08–1H11

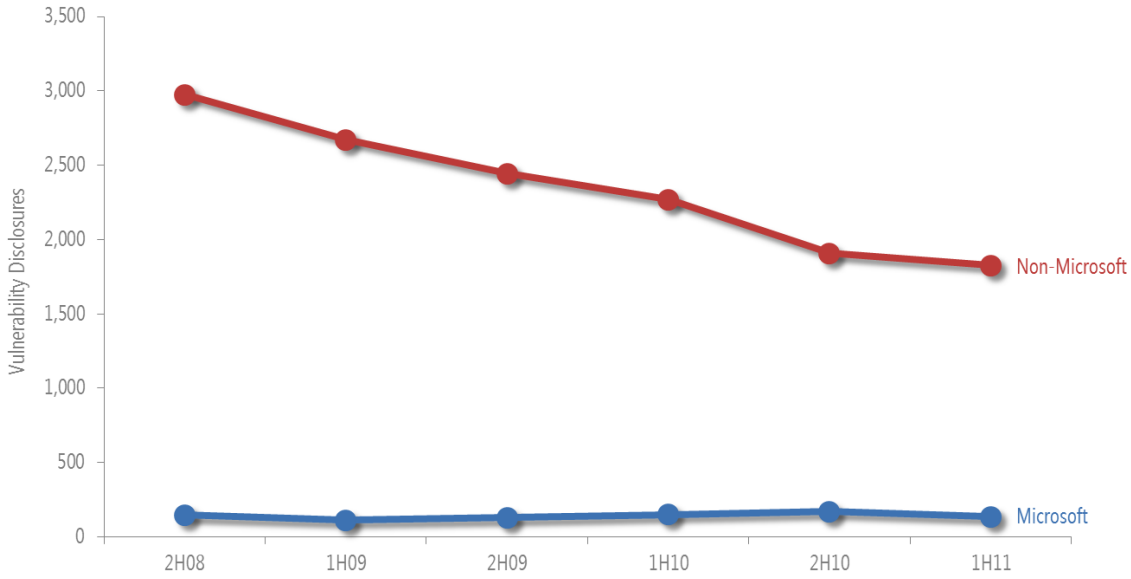



- As Figure 5 shows, most of the industry-wide decline in vulnerability disclosures over the past several years has been caused by a decrease in application vulnerabilities, which were down 8.8 percent from 1H11.
- Despite this decline, application vulnerabilities still accounted for 71.5 percent of all vulnerabilities disclosed in 1H11.
- Operating system and browser vulnerability disclosures have been mostly stable for several years, accounting for 12.7 percent and 15.7 percent of all vulnerabilities disclosed in 1H11, respectively.

## Microsoft Vulnerability Disclosures

Figure 6 charts vulnerability disclosures for Microsoft and non-Microsoft products since 2H08.

Figure 6. Vulnerability disclosures for Microsoft and non-Microsoft products, 2H08–1H11




- Vulnerabilities in Microsoft products accounted for 6.9 percent of all vulnerabilities disclosed in 1H11, down from 8.2 percent in 2H10.
- Vulnerability disclosures for Microsoft products have generally remained stable over the past several periods, though the percentage of all disclosures industry-wide that affect Microsoft products has increased slightly, primarily because of the overall decline in vulnerability disclosures across the industry.

## Guidance: Developing Secure Software

The Security Development Lifecycle (www.microsoft.com/sdl) is a software development methodology that embeds security and privacy throughout all phases of the development process with the goal of protecting software users. Using such a methodology can help reduce vulnerabilities in the software and help manage vulnerabilities that might be found after deployment. (For more in-depth information about the SDL and other techniques developers can use to secure their software, see Protecting Your Software in the "Managing Risk" section of the *Microsoft Security Intelligence Report* website.)

# Exploits

An *exploit* is malicious code that takes advantage of software vulnerabilities to infect, disrupt, or take control of a computer without the user's consent and usually without the user's knowledge. Exploits target vulnerabilities in operating systems, web browsers, applications, or software components that are installed on the computer. In some scenarios, targeted components are add-ons that are pre-installed by the computer manufacturer before the computer is sold. A user may not even use the vulnerable add-on or be aware that it is installed. 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.

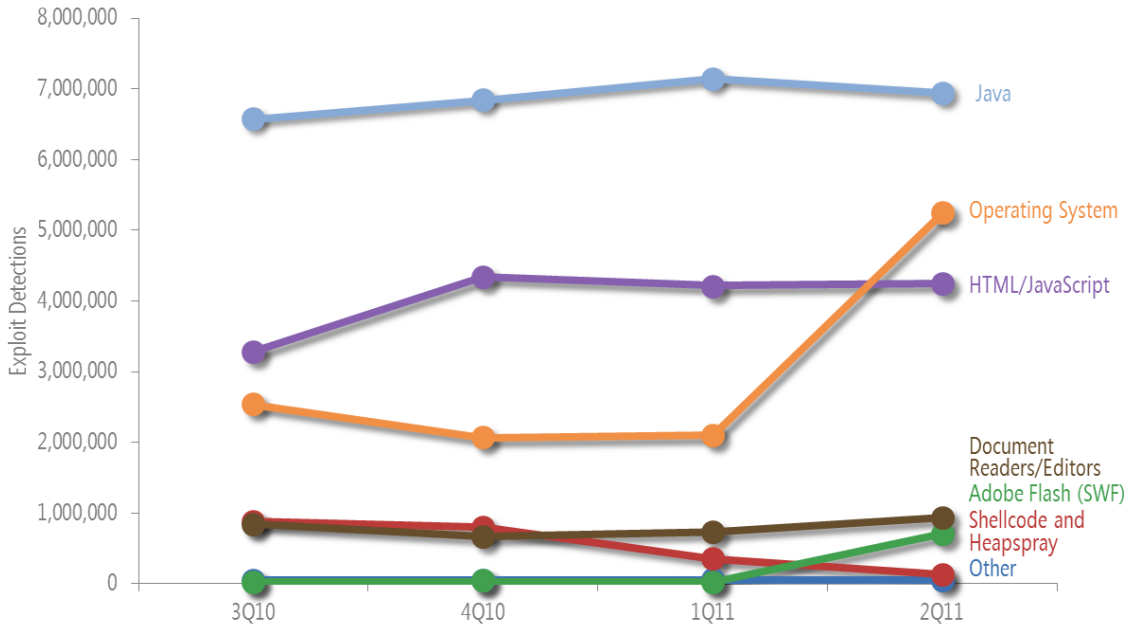
Software vulnerabilities are enumerated and documented in the Common Vulnerabilities and Exposures list (CVE) (http://cve.mitre.org), a standardized repository of vulnerability information. Here and throughout this report, exploits are labeled with the CVE identifier that pertains to the affected vulnerability, 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]

Note that most of the charts in the "Exploits" section, with the exception of Figure 15 on page 25, show individual attack counts rather than unique computers affected.

Figure 7 shows the prevalence of different types of exploits for each quarter between 3Q10 and 2Q11.

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

Figure 7. Exploits detected and blocked by Microsoft antimalware products, 3Q10–2Q11, by targeted platform or technology

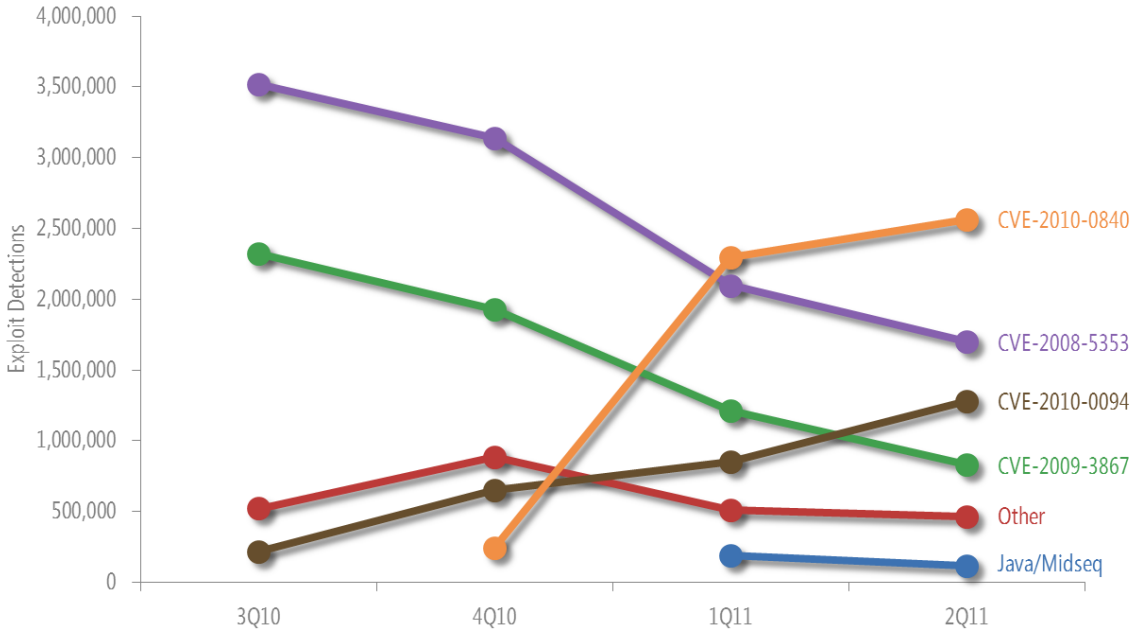



- The most commonly observed type of exploits in 1H11 were those targeting vulnerabilities in the Oracle (formerly Sun) Java Runtime Environment (JRE), Java Virtual Machine (JVM), and Java SE in the Java Development Kit (JDK). Java exploits were responsible for between one-third and one-half of all exploits observed in each of the four most recent quarters.
- Detections of operating system exploits increased dramatically in 2Q11 because of increased exploitation of vulnerability CVE-2010-2568. (See "Operating System Exploits" on page 23 for more information.)
- Detections of exploits targeting Adobe Flash, although uncommon in comparison to some other types of exploits, increased in 2Q11 to more than 40 times the volume seen in 1Q11 because of exploitation of a pair of newly-discovered vulnerabilities. (See "Adobe Flash Player Exploits" on page 25 for more information about these vulnerabilities.)
- The web is the most common vector by which exploits are delivered. Java and HTML/JavaScript exploits are usually delivered through the web, as are large percentages of other types of exploits. Malicious documents that contain exploits are sometimes delivered over the web, but are also often sent directly to prospective victims as files attached to email messages. Similarly, Flash exploits are often delivered over the web, but are sometimes embedded in malicious documents sent through email.

## Java Exploits

Figure 8 shows the prevalence of different Java exploits by quarter.

Figure 8. Java exploits detected and blocked by Microsoft antimalware products, 3Q10–2Q11




- As in previous periods, many of the more commonly exploited Java vulnerabilities are several years old, as are the security updates that have been released to address them.
- The most commonly exploited Java vulnerability in 1Q11 and 2Q11 was CVE-2010-0840, a Java Runtime Environment (JRE) vulnerability first disclosed in March 2010 and addressed with an Oracle security update the same month. Exploitation of the vulnerability was first detected at a low level in 4Q10 before increasing tenfold in 1Q11.
- CVE-2008-5353, the second most commonly exploited Java vulnerability in 1Q11 and 2Q11, was first disclosed in December 2008. This vulnerability affects JVM version 5 up to and including update 22, and JVM version 6 up to and including update 10. It allows an unsigned Java applet to gain elevated privileges and potentially have unrestricted access to a host system, outside its "sandbox" environment. Sun Microsystems released a security update that addressed the vulnerability on December 3, 2008.
- CVE-2010-0094, the fourth most commonly exploited Java vulnerability in 1Q11 and the third in 2Q11, was first disclosed in December 2009. The

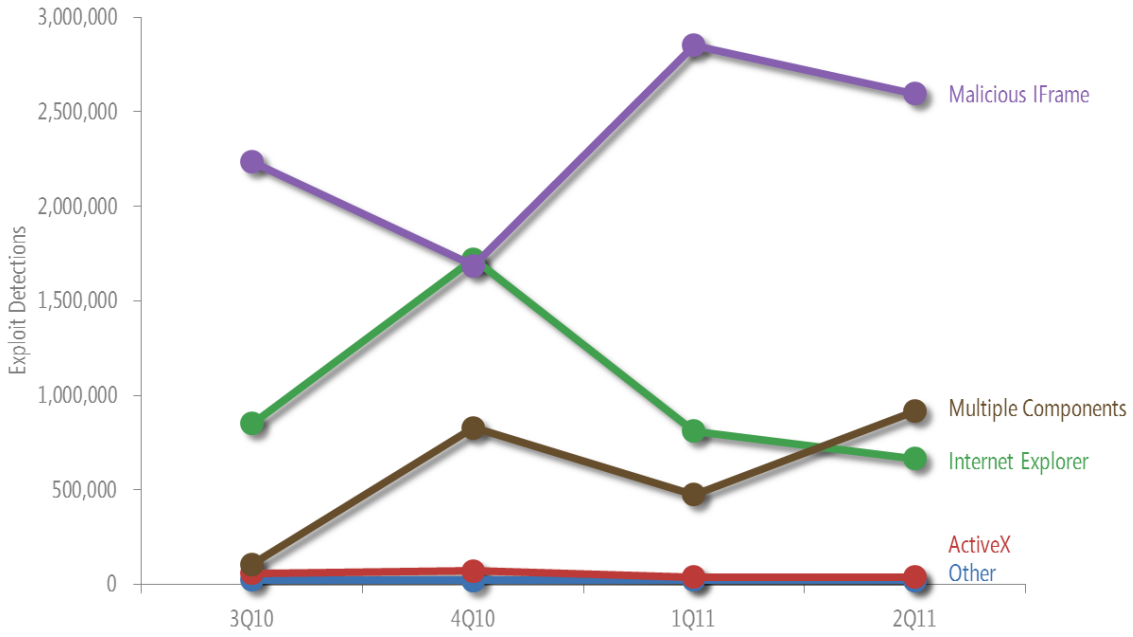
vulnerability affects JRE versions up to and including update 18 of version 6. It allows an unsigned Java applet to gain elevated privileges and potentially have unrestricted access to a host system, outside its sandbox environment. Oracle released a security update that addressed the vulnerability in March 2010.

- CVE-2009-3867, the third most commonly exploited Java vulnerability in 1Q11 and the fourth in 2Q11, was first disclosed in November 2009. The vulnerability affects JVM version 5 up to and including update 21, and JVM version 6 up to and including update 16. When an applet that exploits the vulnerability is loaded by a computer with a vulnerable version of Java, security checks may be bypassed, allowing the execution of arbitrary code. Sun Microsystems released a security update that addressed the vulnerability on November 3, 2009.

## HTML and JavaScript Exploits

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

Figure 9. Types of HTML and JavaScript exploits detected and blocked by Microsoft antimalware products, 3Q10–2Q11




- Most of the exploits observed involved malicious HTML inline frames (IFrames). These exploits are typically generic detections of inline frames that

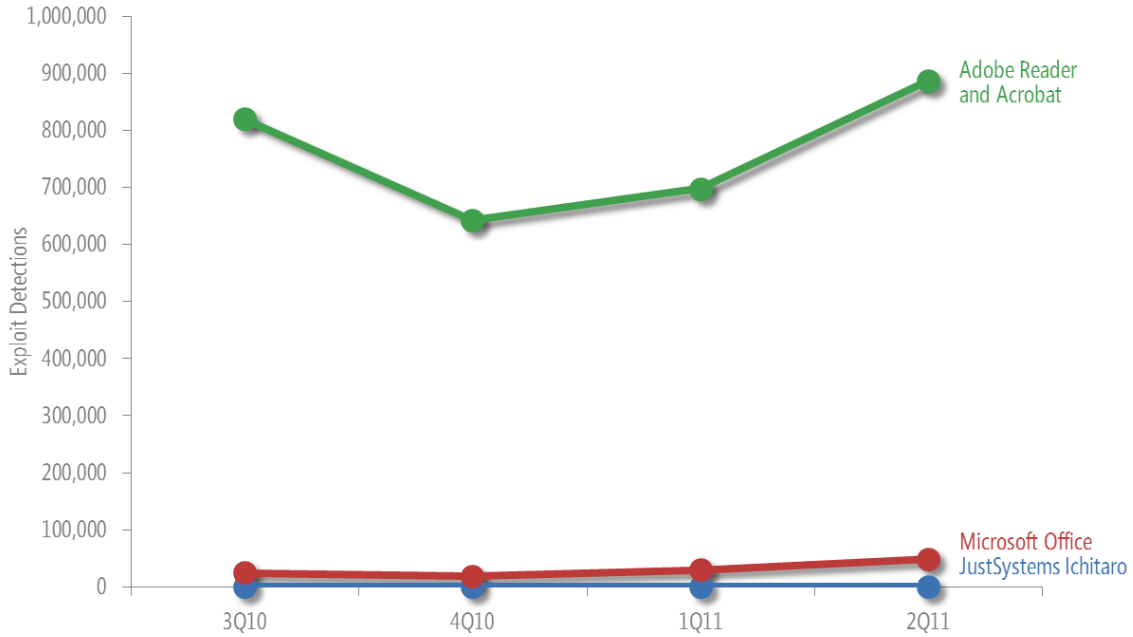
are embedded in web pages and link to other pages that host malicious web content. These malicious pages use a variety of techniques to exploit vulnerabilities in browsers and plugins, with the only commonality being that the exploit can be delivered through an inline frame. The exact exploit delivered and detected by one of these signatures may be changed frequently.

- After peaking in 4Q10, exploits that target Windows Internet Explorer® returned to a more typical level in 1Q11 and stayed at the lower level in 2Q11. The 4Q10 peak largely involved exploits targeting CVE-2010-0806, a vulnerability in versions 6 and 7 of Internet Explorer. Microsoft released security bulletin MS10-018 in March 2010 to address the vulnerability.

## Document Parser Exploits

*Document parser exploits* are those that target vulnerabilities in the way a document editing or viewing application processes, or parses, a particular file format. Figure 10 shows the prevalence of different types of document parser exploits during each of the four most recent quarters.

Figure 10. Types of document parser exploits detected and blocked by Microsoft antimalware products, 3Q10–2Q11




- Exploits that affect Adobe Acrobat and Adobe Reader accounted for most document format exploits detected throughout the last four quarters. Most of

these exploits were detected as variants of the generic exploit family Win32/Pdfjsc.

- Exploits that affect Microsoft Office and Ichitaro, a Japanese-language word processing application published by JustSystems, accounted for a small percentage of exploits detected during the period. (See the following section for more information about Office exploits.)

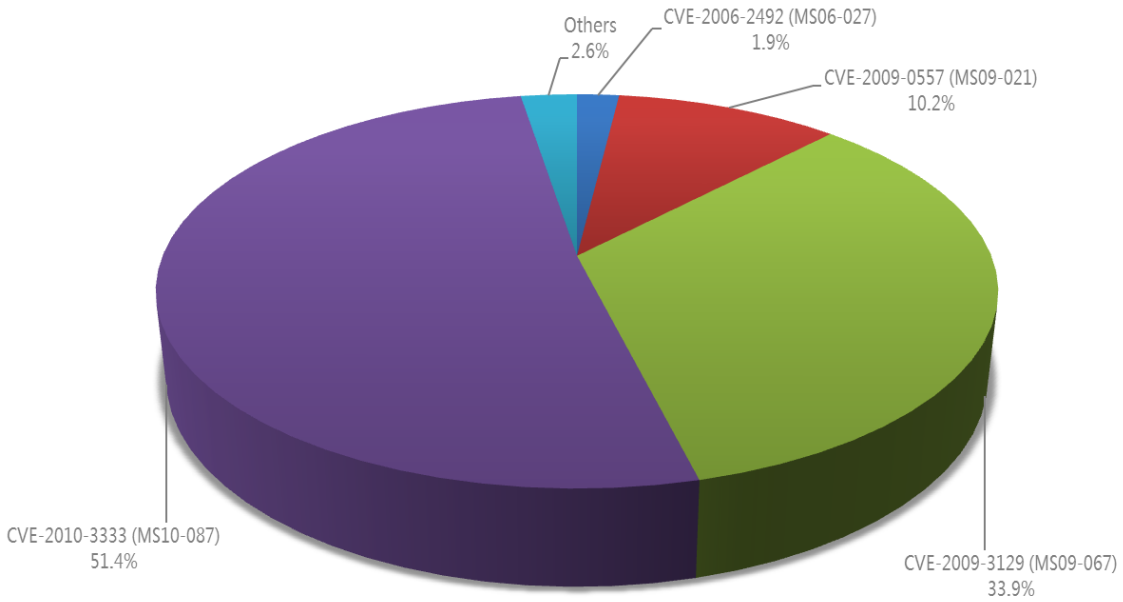
## Microsoft Office File Format Exploits

To assess the use of Microsoft Office system file formats as an attack vector, Microsoft analyzed a sample set of several hundred files that were used for successful attacks in 1H11. The data set was taken from submissions of malicious code sent to Microsoft from customers worldwide.

Figure 11. Vulnerabilities exploited in Microsoft Office file formats in 1H11

| CVE | Vulnerability | Bulletin | Release Date |
|---|---|---|---|
| CVE-2006-2492 | Word Malformed Object Pointer Vulnerability | MS06-027 | June 2006 |
| CVE-2006-0022 | PowerPoint® Remote Execution Via a Malformed Record Vulnerability | MS06-028 | June 2006 |
| CVE-2006-6456 | Word Remote Execution Vulnerability | MS07-014 | February 2007 |
| CVE-2007-0671 | Excel® Malformed Record Vulnerability | MS07-015 | February 2007 |
| CVE-2008-0081 | Macro Validation Vulnerability | MS08-014 | March 2008 |
| CVE-2009-0238 | Excel Memory Corruption Vulnerability | MS09-009 | April 2009 |
| CVE-2009-0557 | Excel Object Record Corruption Vulnerability | MS09-021 | June 2009 |
| CVE-2009-3129 | Excel Record Memory Corruption | MS09-067 | November 2009 |
| CVE-2010-3333 | Word RTF File Parsing Stack Buffer Overflow Vulnerability | MS10-087 | November 2010 |
| CVE-2011-0979 | Excel Parsing Vulnerability allows Remote Code Execution | MS11-021 | April 2011 |

Figure 12. Microsoft Office file format exploits encountered in 1H11, by percentage

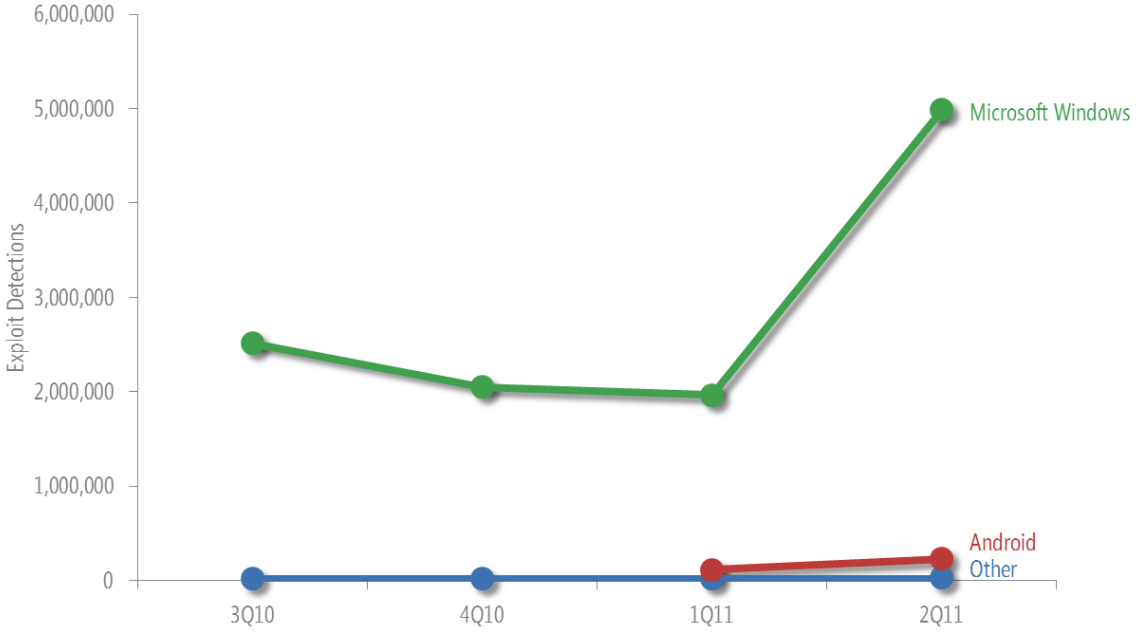



- In total, exploits for 10 vulnerabilities were identified in the sample set, as shown in Figure 11. All 10 of these vulnerabilities had security updates available at the time of the attack. The affected users were exposed because they had not applied the updates.
- More than half of the exploits involved CVE-2010-3333, a vulnerability in the Rich Text Format (RTF) parser in versions of Microsoft Word that was addressed by Security Bulletin MS10-087 in November 2010.
- Most of the other exploits in the sample involved CVE-2009-3129, a vulnerability in Microsoft Excel that was addressed by Security Bulletin MS09-067 in November 2009. Installing these two security updates would have protected users from 85.3 percent of the attacks in the sample set.
- None of the encountered exploits are effective in Office 2010 applications running in their default configurations on Windows Vista or Windows 7. All of the exploits take advantage of techniques that are blocked by address space layout randomization (ASLR) or Data Execution Prevention (DEP), two security-related technologies included in recent versions of Windows. ASLR and DEP are both enabled by default in Office 2010. DEP is available in Windows XP SP3, Windows Vista, and Windows 7; ASLR is available in Windows Vista and Windows 7. (See Appendix D in the full report for a table of Office versions and their level of exposure to the exploits encountered in 1H11.)

## Operating System Exploits

Although most operating system exploits detected by Microsoft security products are designed to affect the platforms on which the security products run, computer users sometimes download malicious or infected files that affect other operating systems. Figure 13 shows the prevalence of different operating system exploits detected and removed by Microsoft security products during each of the past four quarters.

Figure 13. Types of operating system exploits detected and blocked by Microsoft antimalware products, 3Q10–2Q11

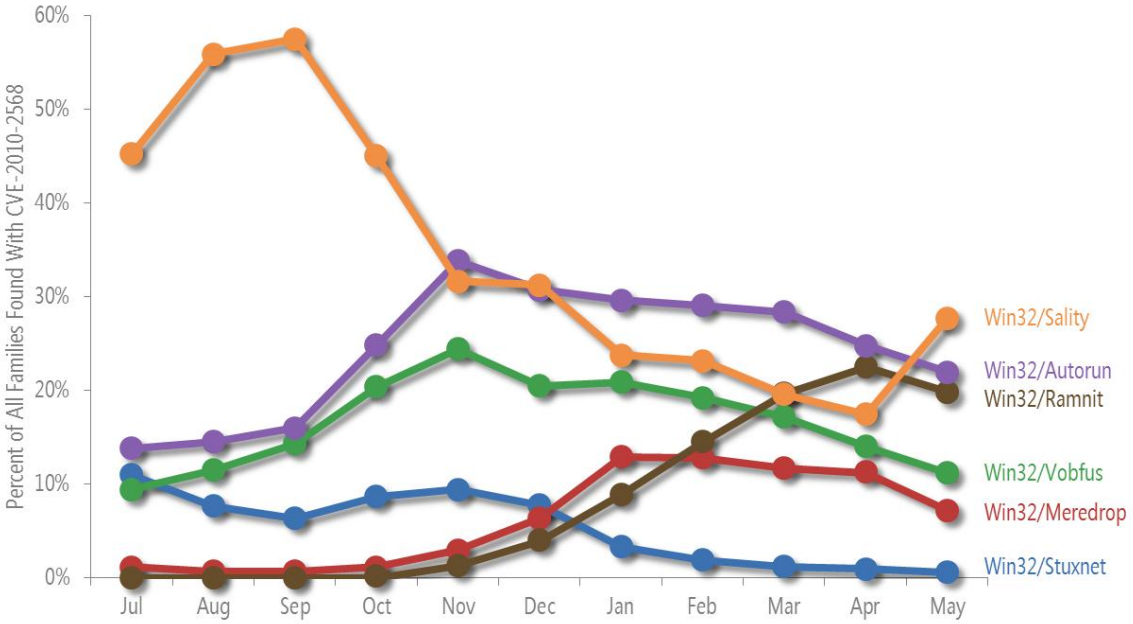



- Detection totals for Windows are inflated by detections of CVE-2010-2568, which is often detected repeatedly on the same computer because of the mechanism it uses to spread. (See page 25 for more information.)
- Exploits that target CVE-2010-2568, a vulnerability in Windows Shell, increased significantly in 2Q11, and were responsible for the entire 2Q11 increase in Windows exploits shown in Figure 13. Microsoft issued Security Bulletin MS10-046 in August 2010 to address the vulnerability.

  An attacker exploits CVE-2010-2568 by creating a malformed shortcut file that forces a vulnerable computer to load a malicious file when the shortcut icon is displayed in Windows Explorer. The vulnerability was first discovered being used by the malware family Win32/Stuxnet in mid-2010, and it has since been exploited by a number of pre-existing families, many of which had

been designed to spread using malicious shortcut files or by abusing the AutoRun feature in Windows. The CVE-2010-2568 attack mechanism is similar to the techniques already in use by these families, which may explain why their authors chose to incorporate the exploit into new variants.

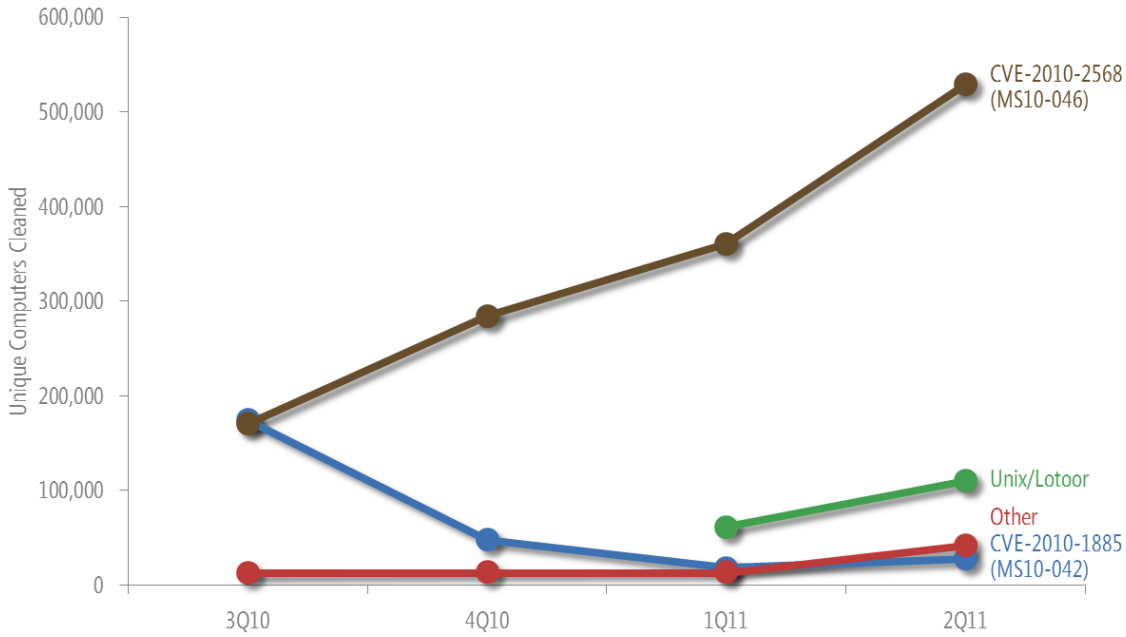
Figure 14. Families commonly found with CVE-2010-2568, July 2010–June 2011




- Exploits that affect the Android mobile operating system published by Google and the Open Handset Alliance have been detected in significant volume beginning in 1H11. Microsoft security products detect these threats when Android users download infected or malicious programs to their computers before transferring the software to their devices. The increase in Android-based threats has been driven primarily by the exploit family Unix/Lotoor, the second most commonly detected operating system exploit in 1Q11 and 2Q11. Lotoor is used to attack vulnerable devices by the trojan family AndroidOS/DroidDream, which often masquerades as a legitimate Android application, and can allow a remote attacker to gain access to the mobile device. Google published a security update in March 2011 that addressed the vulnerability.

For another perspective on these exploits and others, Figure 15 shows trends for the individual exploits most commonly detected and blocked or removed in 1H11.

Figure 15. Individual operating system exploits detected and blocked by Microsoft antimalware products, 3Q10–2Q11, by number of unique computers exposed to the exploit

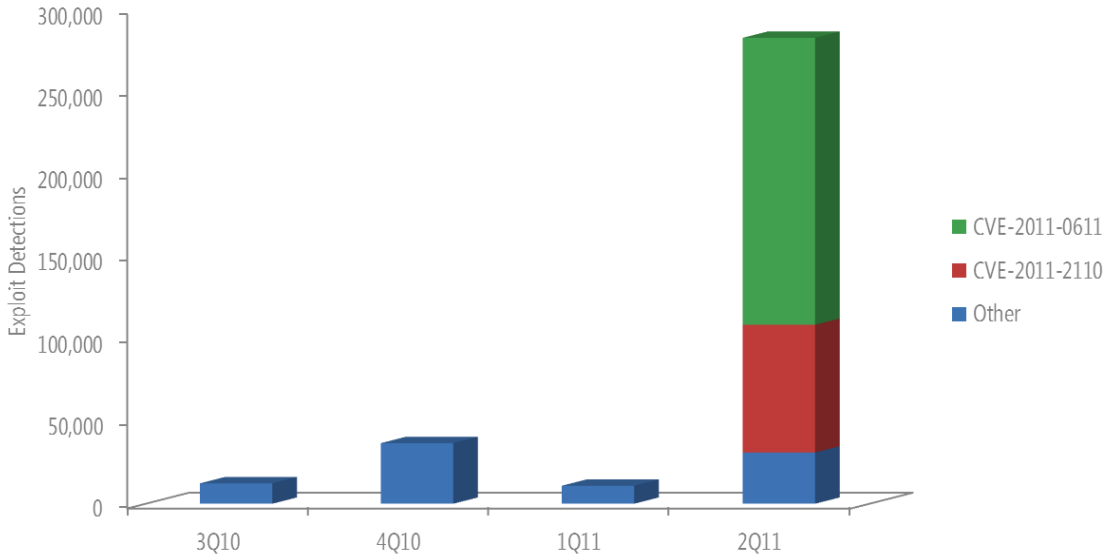



- Unlike the other charts in this section, Figure 15 shows the number of unique computers affected by each exploit, rather than the number of individual attacks detected. CVE-2010-2568 exploits have a tendency to be reported by the same computer many times (eight on average, although some computers report thousands of attack attempts), because of the way the exploit technique works, which could give a misleading impression of the exploit's impact.
- CVE-2010-1885, a vulnerability that affects the Windows Help and Support Center in Windows XP and Windows Server 2003, was a dominant exploit in 2010, but declined significantly in 1H11. Microsoft issued Security Bulletin MS10-042 in July 2010 to address the issue.

## Adobe Flash Player Exploits

Figure 16 shows the prevalence of different Adobe Flash exploits by quarter.

Figure 16. Adobe Flash Player exploits detected and blocked by Microsoft antimalware products, 3Q10–2Q11




- Exploitation of Adobe Flash Player increased dramatically in 2Q11 with the disclosure of two new vulnerabilities, CVE-2011-0611 and CVE-2011-2110.
- CVE-2011-0611 was discovered in April 2011 when it was observed being exploited in the wild, typically in the form of malicious .zip files attached to spam email messages that purported to contain information about the Fukushima Daiichi nuclear disaster in Japan. Adobe Systems released Security Bulletin APSB11-07 on April 15 and Security Bulletin APSB11-08 on April 21 to address the issue. On the same day the security update was released, attacks that targeted the vulnerability skyrocketed and remained high for several days, most of which were detected on computers in Korea. About a month later, a second increase in attacks was observed, affecting multiple locations.
- CVE-2011-2110 was discovered in June 2011, and Adobe released Security Bulletin APSB11-18 on June 15 to address the issue. As with CVE-2011-0611, attacks that targeted the vulnerability spiked just after the security update was released, again with most of the targeted computers located in Korea.
- See the full report for more information about these two vulnerabilities, as well as the following posts on the MMPC blog (blogs.technet.com/mmpc):
  - Analysis of the CVE-2011-0611 Adobe Flash Player vulnerability exploitation (April 12, 2011)
  - Exploits for CVE-2011-2110 focus on Korea (June 21, 2011)

# 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 in the full report for more information about the telemetry used in this report.)

## CCM Calculation Changes

This volume of the *Microsoft Security Intelligence Report (SIR)* introduces a significant change in the way location is determined for computers whose administrators have opted into providing telemetry data to Microsoft. In previous volumes of the report, Windows-based computers reporting information were classified by countries and regions according to the administrator-specified setting under the Location tab or menu in Region and Language in Control Panel. Beginning with this volume of the report, location is determined by geolocation of the IP address used by the computer submitting the telemetry data. (For more information about how location data is collected and used, see Appendix B in the full report.)[2]

Using IP addresses to determine the location of systems sharing telemetry instead of using the administrator-specified Location setting of the computer creates slight differences in the trends observed in most countries/regions reported in the SIR. In a few cases, the reported infection rate has changed significantly. Figure 17 and Figure 18 show trends for the locations with the largest CCM decreases and increases caused by the switch to IP geolocation. (CCM stands for *computers cleaned per mille*, or thousand, and represents the number of reported computers cleaned in a quarter for every 1,000 executions of the Malicious Software Removal Tool (MSRT). For example, if the MSRT has 50,000 executions in a particular location in the first quarter of the year and removes infections from 200

[2] In addition to the geographic changes described here, Microsoft has corrected an error in data tabulation that had caused the worldwide CCM to be reported inaccurately in previous volumes of this report. See the *Microsoft Security Intelligence Report* website for more information about this change.

computers, the CCM for that location in the first quarter is 4.0, or 200 ÷ 50,000 × 1,000.)

Figure 17. The five locations with the largest CCM decreases caused by the switch to IP geolocation

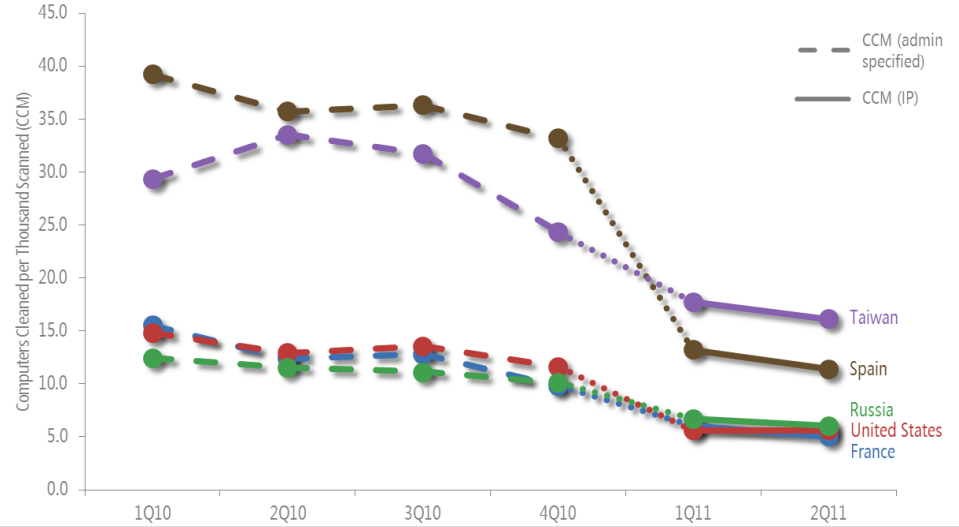
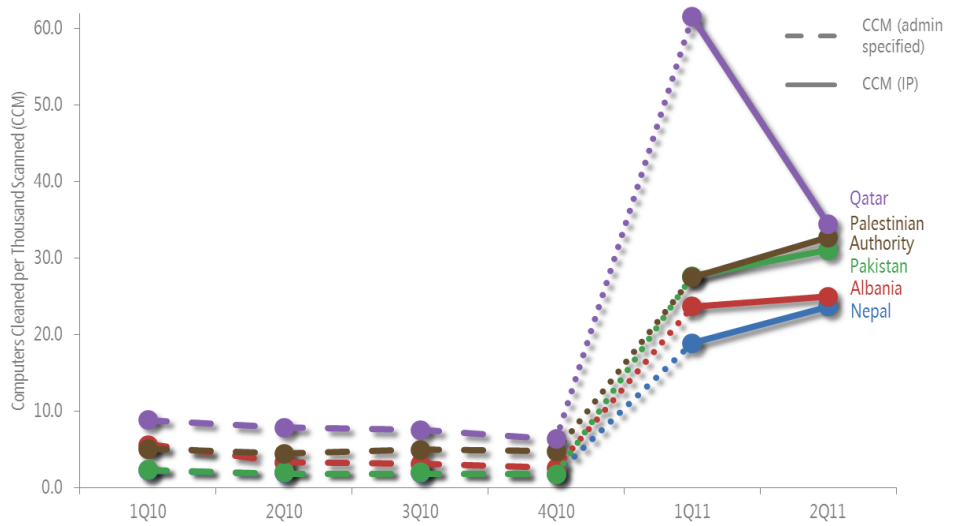



Figure 18. The five locations with the largest CCM increases caused by the switch to IP geolocation




In addition to providing what Microsoft believes will be a more accurate gauge of regional infection rates, this change provides an interesting perspective on computer usage habits around the world.

Very few locations saw their infection rates fall as a result of the switch to IP geolocation—in fact, among locations with at least 100,000 MSRT executions in 1Q11, the five shown in Figure 17 were the only locations that underwent a CCM decrease greater than 1.0 point.

By contrast, there were more than 100 locations whose CCMs rose after applying IP geolocation, with 35 of them moving 10 points or more, and four rising more than 20 points, as shown in Figure 18. In general, most of the locations with significant increases have smaller populations and relatively few reporting computers. The 61.5 CCM for Qatar in 1Q11 is the largest CCM figure ever reported in the *Microsoft Security Intelligence Report*, and is 55.1 points higher than the figure reported for Qatar for 4Q10 using the administrator-configured locale setting to determine location.

Notably, the five locations in which the CCM decreased significantly represent the largest populations using five of the most widely used languages on the Internet: France and French, Spain and Spanish, Russia and Russian, Taiwan and Chinese (Traditional), and the United States and English. This finding suggests that, rather than using the locale settings designated for their country or region, many computer administrators in smaller locations might be using locale settings for larger ones, particularly larger locations in which the dominant language is one spoken by the computer's user. As a result, the reported infection rates were being skewed for some locations. For example, if a Spanish-speaking computer administrator outside Spain configured a computer with the locale settings for Spain, any malware detections on the computer would have been reported for Spain using the previous method for determining location. This factor would have the effect of overreporting malware detections for Spain, and underreporting malware detections for the country or region in which the computer was actually located. Switching to IP address-based geolocation corrects this anomaly and provides more accurate regional infection statistics.

Computer security and response professionals in the more affected locations should consider these findings carefully when developing plans for safeguarding their populations' computers. (See Managing Risk at the *Microsoft Security Intelligence Report* website for guidance about protecting computers, software, and people from threats.)

## Global Infection Rates

The telemetry data generated by Microsoft security products from administrators or users who choose to opt in to data collection includes information about the

location of the computer, as determined by IP geolocation. This data makes it possible to compare infection rates, patterns, and trends in different locations around the world.

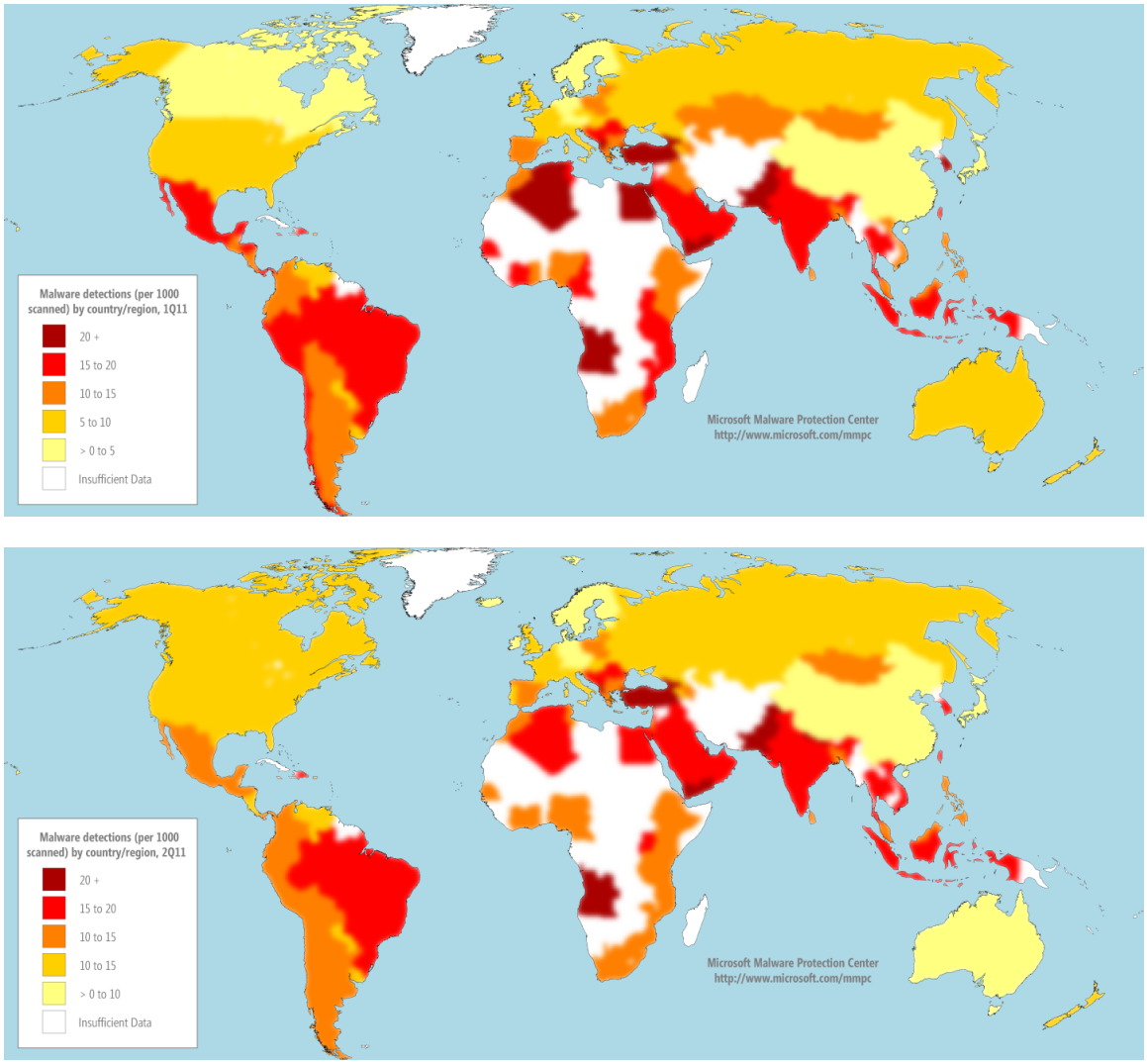
Figure 19. The locations with the most computers reporting detections and removals by Microsoft desktop antimalware products in 1H11

| | Country/Region | 1Q11 | 2Q11 | Chg. 1Q to 2Q |
|---|---|---|---|---|
| 1 | United States | 10,727,964 | 10,471,335 | -2.4% ▼ |
| 2 | Brazil | 3,463,973 | 3,724,844 | 7.5% ▲ |
| 3 | France | 2,351,941 | 2,674,775 | 13.7% ▲ |
| 4 | United Kingdom | 2,175,201 | 2,089,883 | -3.9% ▼ |
| 5 | China | 2,017,682 | 1,883,578 | -6.6% ▼ |
| 6 | Germany | 1,622,081 | 1,530,551 | -5.6% ▼ |
| 7 | Russia | 1,296,208 | 1,583,857 | 22.2% ▲ |
| 8 | Italy | 1,358,166 | 1,509,148 | 11.1% ▲ |
| 9 | Canada | 1,377,173 | 1,353,164 | -1.7% ▼ |
| 10 | Turkey | 1,248,978 | 1,359,181 | 8.8% ▲ |

- In absolute terms, the locations with the most computers reporting detections tend to be ones with large populations and large numbers of computers.
- Detections in Russia increased 22.2 percent from 1Q11 to 2Q11, mostly because of increased detections of Win32/Pameseg, a potentially unwanted software program with a Russian language user interface.
- Detections in France and Italy both increased significantly in 2Q11 because of increased detections of a number of Adware families, including Win32/ClickPotato, Win32/Hotbar, and Win32/OfferBox.
- Detections in China decreased 6.6 percent, primarily because of steep drops in detections of a pair of malware families, JS/ShellCode and Win32/Sogou, that have historically been much more common in China than elsewhere.

For a different perspective on infection patterns worldwide, Figure 20 shows the infection rates in locations around the world using CCM.

Figure 20. Infection rates by country/region in 1Q11 (top) and 2Q11 (bottom), by CCM




Detections and removals in individual countries/regions can vary significantly from quarter to quarter. Increases in the number of computers with detections can be caused not only by increased prevalence of malware in that 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 1H11.

Figure 21. Trends for the five locations with the highest infection rates in 2Q11, by CCM (100,000 MSRT executions minimum per quarter in 2011)

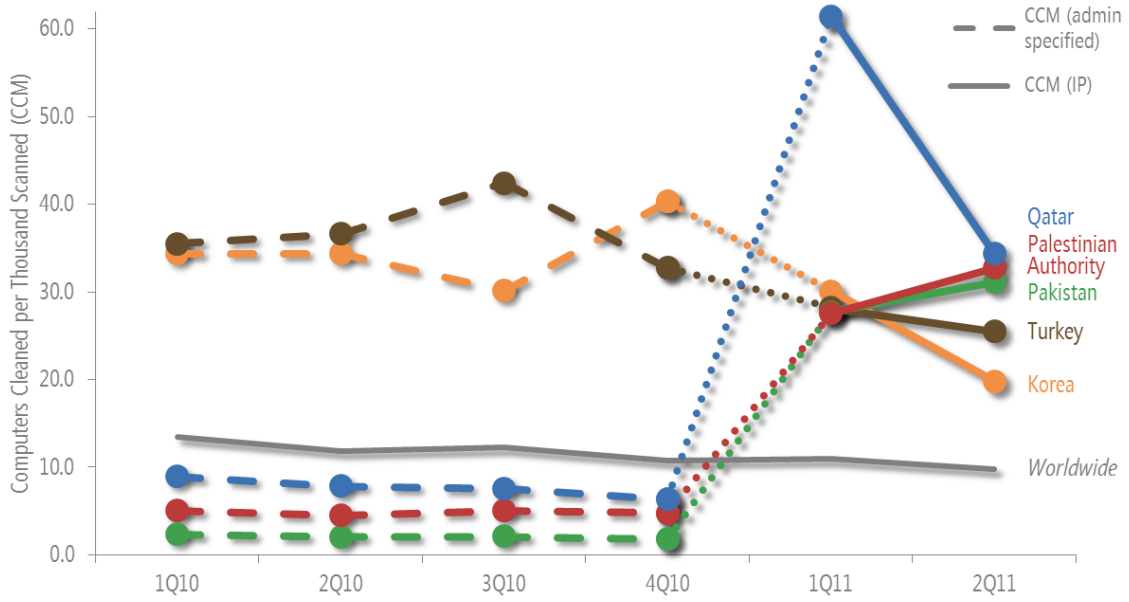
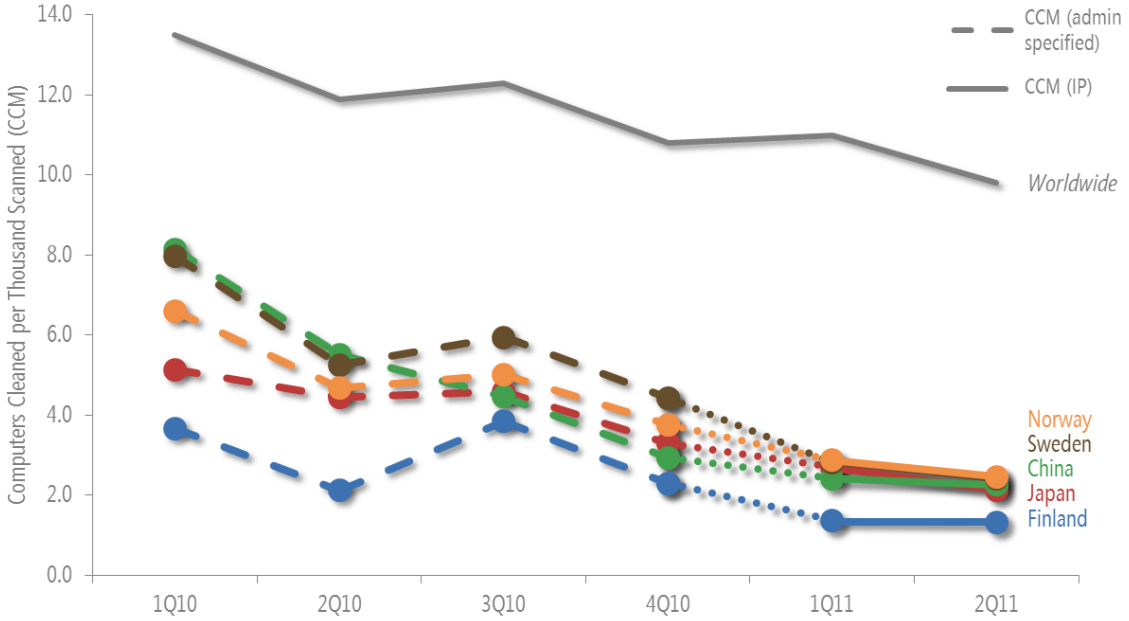


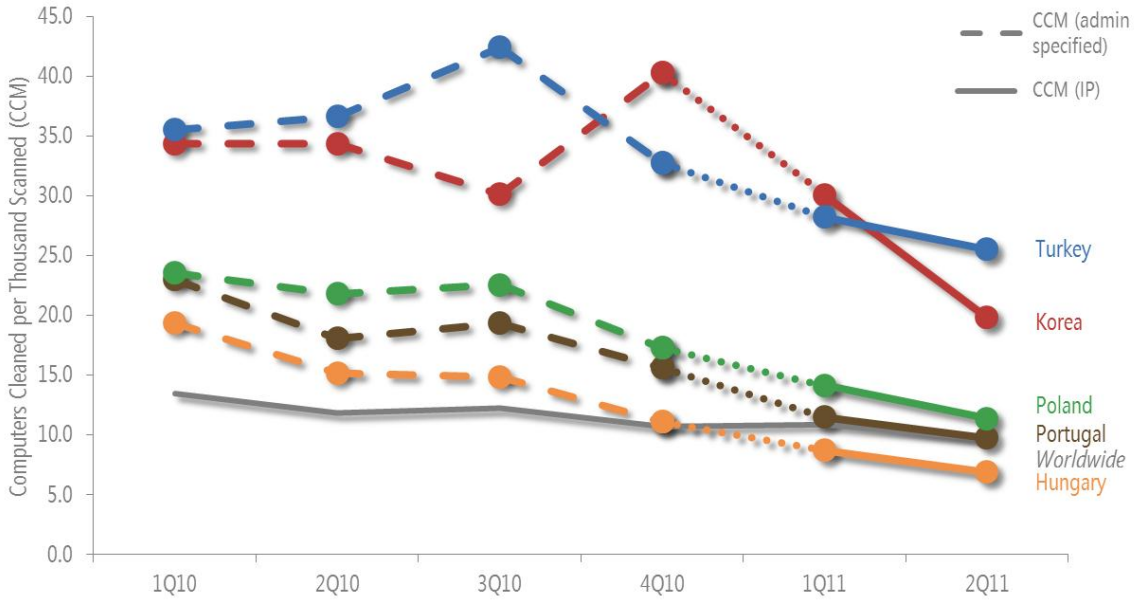

Figure 22. Trends for the five locations with the lowest infection rates in 2Q11, by CCM (100,000 MSRT executions minimum per quarter in 2011)



- The switch from using the administrator-configured location setting to IP address geolocation for classifying computers by country and region (see page 27) is responsible for the significant shifts in Figure 21 between 4Q10 and 1Q11.
- Of the five locations with the highest infection rates in 4Q10—Korea, Spain, Turkey, Taiwan, and Brazil—only Turkey and Korea are on the list for 2Q11. Spain and Taiwan underwent significant decreases with the shift to IP geolocation, and Brazil continued a trend of significant improvement over the last two years.
- Several Nordic countries were among the locations with the lowest infection rates, including Norway, Sweden, and Finland, as shown in Figure 22. Denmark, another Nordic country, had the sixth lowest infection rate in 2Q11.
- Although China is 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 the MSRT, which tends to target malware families that are prevalent globally. As a result, many of the more prevalent threats in China are not represented in the data used to calculate CCM. For a more in-depth perspective on the threat landscape in China, see the "Regional Threat Assessment" section of the *Microsoft Security Intelligence Report* website.

As explained in "CCM Calculation Changes" on page 27, the shift from using administrator-configured location settings to IP address-based geolocation has resulted in significant CCM changes for some countries or regions. To help illustrate which locations improved the most in the first half of 2011, Figure 23 focuses on locations that were not significantly affected by the change. All of the locations shown in Figure 23 are ones in which the 1Q11 infection rate as determined by IP address geolocation differed by less than one percentage point from the 1Q11 infection rate as determined by administrator-configured settings.

Figure 23. Trends for five locations with significant infection rate improvements in 1H11, by CCM (100,000 MSRT executions minimum per quarter in 2011)




## Regional Effective Practices

Computer emergency response teams (CERTs) and computer security incident response teams (CSIRTs) around the world work to protect technology users in their regions. Over time, effective practices that help reduce regional malware infections have emerged. Microsoft asked representatives from some of these teams to share insights into their practices:

- In Korea, the Korea Information Security Agency (KISA) has instituted a two-part remediation effort. The first part is a joint malware notification program developed in cooperation with major ISPs in Korea. KISA provides the participating ISPs with information about computers that are determined to be infected with malware families that are widespread within Korea. When the user of an infected computer logs in, a pop-up window displays with a link to a web page that contains instructions for removing the infection.

  The second part of the remediation effort consists of a program to develop and distribute free "vaccine" software that targets specific malware families that are widespread in Korea. Responding to a series of serious distributed denial-of-service (DDoS) attacks that have affected Korea recently, KISA contracted with major domestic antivirus (AV) vendors to develop the vaccine, which is available for download from www.boho.or.kr.

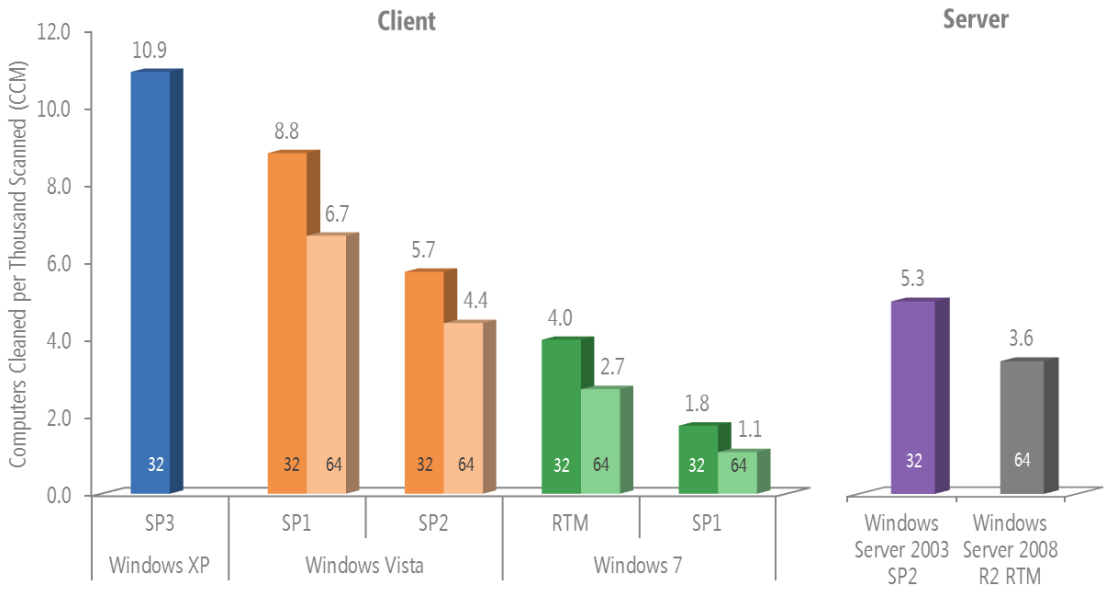
- In Poland, CERT Polska (www.cert.pl) attributes much of the improvement to filtering of port 25, used for Simple Mail Transfer Protocol (SMTP) traffic, by Telekomunikacja Polska, Poland's largest telecommunications provider. SMTP is often abused by malware to send spam and spread infection. Cable Internet providers in Poland have also become more effective at stopping malware and distributing antivirus software to their users. CERT Polska published its annual security report for 2010 at www.cert.pl/PDF/Raport_CP_2010.pdf, and an English-language summary at www.cert.pl/news/3410/langswitch_lang/en.
- In Portugal, infections have decreased significantly since the creation of the National Network of CSIRTs. The Serviço de Resposta a Incidentes de Segurança Informática (CERT.PT) launched the network in 2008 in cooperation with technology companies, telecom providers, and government agencies to address the need for a national response capability for computer security incidents affecting Portugal. As the network has grown and achieved wider recognition, new CSIRTs have been created within ISPs, financial institutions, the Portuguese armed forces, and other companies and agencies.

  In 2011, CERT.PT began sending network members a weekly digest of infected systems within their networks, using data from a range of sources including honeynets, the Shadowserver Foundation, and telemetry provided by Microsoft related to the Rustock botnet. (See *Battling the Rustock Threat*, available from the Microsoft Download Center, for more information about Rustock and Microsoft efforts to fight the botnet.)

## 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 24 shows the infection rate for each currently supported Windows operating system/service pack combination that accounted for at least 0.1 percent of total MSRT executions in 2Q11.

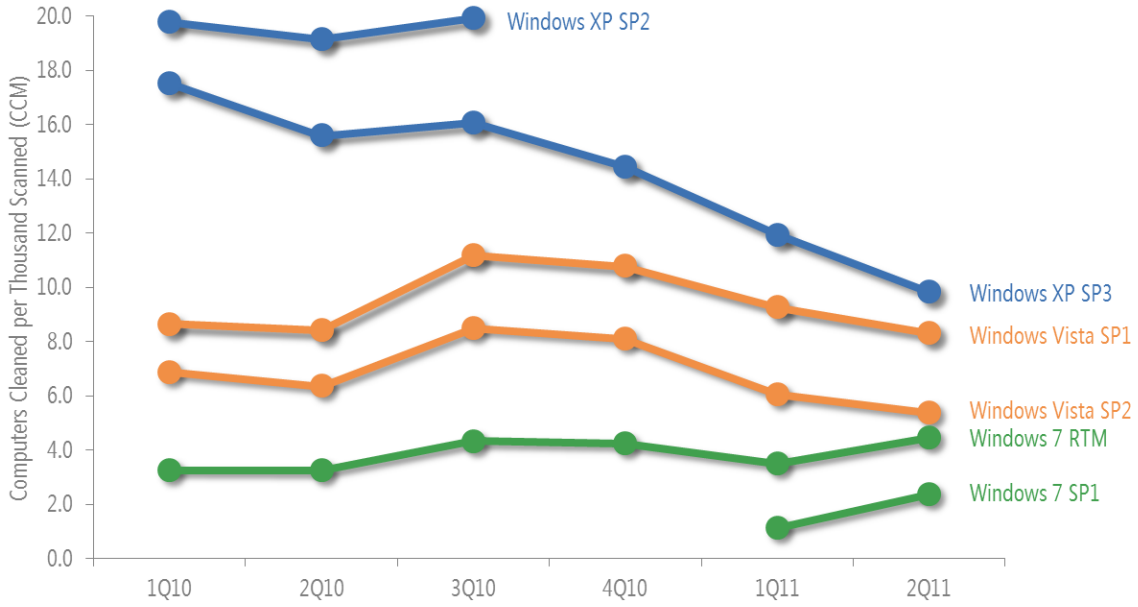
Figure 24. Infection rate (CCM) by operating system and service pack in 2Q11




"32" = 32-bit edition; "64" = 64-bit edition. SP = Service Pack. Supported operating systems with at least 0.1 percent of total executions in 2Q11 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 SP3 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 might 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, might also contribute to the discrepancy by preventing certain types of malware from functioning.

Figure 25. CCM trends for currently and recently supported 32-bit versions of Windows XP, Windows Vista, and Windows 7, 1Q10–2Q11




- Newer operating systems and service packs consistently have lower infection rates than their older counterparts, with Windows 7 having the lowest infection rates of any client version of Windows.
- Infection rates for Windows XP SP3 and Windows Vista declined following the February 2011 release of a security update that changed the way the AutoRun feature works on those platforms to match its functionality in Windows 7. (See the full report for more information about this change.) The impact of this change can be seen in the infection statistics for Win32/Rimecud, the ninth most commonly detected family worldwide in 1H11 and one of the top abusers of the AutoPlay feature.

Figure 26. Increase or decrease of Win32/Rimecud detections with different operating system/service pack combinations

| Platform | CCM Change |
|---|---|
| Windows XP SP3 | -2.7 ▼ |
| Windows Vista SP1 | -1.3 ▼ |
| Windows Vista SP2 | -2.2 ▼ |
| Windows 7 | -0.1 ▼ |

Windows XP SP3 and the two supported Windows Vista service packs received the AutoRun update, and detections of Rimecud on those platforms

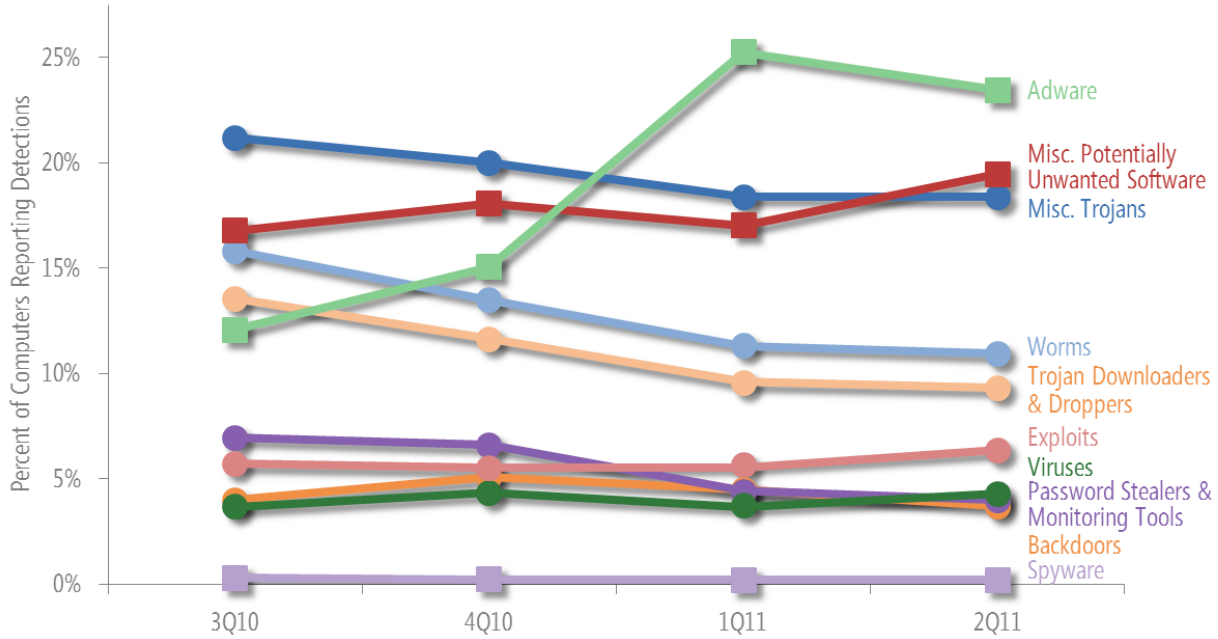
went down by an average of 2.1 computers cleaned per 1000 scanned by the MSRT. Windows 7 already included the more secure AutoPlay functionality; consequently, detections of Rimecud were nearly unchanged.

- Infection rates for Windows 7 RTM and SP1 were higher in 2Q11, primarily because of increased detections of a number of virus and worm families, notably Win32/Sality, Win32/Ramnit, Win32/Brontok, and Win32/Nuqel. Detections of most of these families also increased on Windows XP and Windows Vista, although the infection rates for those platforms decreased overall because of the AutoPlay change discussed earlier.

## 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 *Microsoft Security Intelligence Report* groups these types into 10 categories based on similarities in function and purpose.

Figure 27. Detections by threat category 3Q10–2Q11, by percentage of all computers reporting detections




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

- Totals for each time period may exceed 100 percent because some computers report more than one category of threat in each time period.
- Adware rose to become the most commonly detected category in 1Q11 and 2Q11, primarily because of a pair of new families, Win32/OpenCandy and Win32/ShopperReports, and large increases in detections of a number of older families. See “Threat Families” on page 41 for more information.
- A small increase in detections of Miscellaneous Potentially Unwanted Software families, notably Win32/Keygen, made it the second most commonly detected category in 2Q11, just ahead of Miscellaneous Trojans.
- Worms and Trojan Downloaders & Droppers were two of the more significant categories in 2010, but declined to 10.9 percent and 9.3 percent of detections by 2Q11, respectively. A change in the functionality of the AutoRun feature in older versions of Windows implemented in February 2011 was followed by drops in detections of a number of worm families, contributing to the decline seen here. (See the full report for more information about the AutoRun change.)

## Threat Categories By Location

There are significant differences in the types of threats that affect users in different parts of the world. The spread of malware and its effectiveness are highly dependent on language and cultural factors, 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 online services that are local to a specific geographic region. Other threats target vulnerabilities or operating system configurations and applications that are unequally distributed around the globe.

Figure 28 shows the relative prevalence of different categories of malware and potentially unwanted software in several locations around the world in 2Q11.

Figure 28. Threat category prevalence worldwide and in 10 individual locations, 2Q11

| Category | World | US | Brazil | Fr. | UK | China | Ger. | Russ. | Italy | Can. | Tur. |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Adware | 37.0% | 39.7% | 26.1% | 72.4% | 49.1% | 5.3% | 44.1% | 9.7% | 60.0% | 45.8% | 37.7% |
| Misc. Potentially Unwanted Software | 30.6% | 22.1% | 35.2% | 27.7% | 27.9% | 48.8% | 26.5% | 60.3% | 26.1% | 26.7% | 34.7% |
| Misc. Trojans | 28.9% | 38.9% | 22.6% | 12.1% | 31.9% | 36.6% | 25.4% | 34.1% | 15.5% | 36.2% | 41.9% |
| Worms | 17.2% | 6.3% | 24.2% | 7.3% | 5.9% | 14.0% | 8.6% | 19.9% | 11.9% | 5.0% | 31.3% |
| Trojan Downloaders & Droppers | 14.7% | 17.8% | 21.0% | 7.0% | 13.8% | 20.4% | 13.4% | 9.7% | 9.1% | 17.4% | 13.5% |
| Exploits | 10.0% | 14.4% | 16.3% | 2.7% | 10.5% | 15.0% | 7.9% | 7.1% | 4.0% | 13.1% | 3.4% |
| Viruses | 6.7% | 2.0% | 10.1% | 1.2% | 3.4% | 8.0% | 2.9% | 8.4% | 1.7% | 2.0% | 17.7% |
| Password Stealers & Monitoring Tools | 6.3% | 2.9% | 18.9% | 2.4% | 3.9% | 4.8% | 6.8% | 5.1% | 4.2% | 2.8% | 7.8% |
| Backdoors | 5.8% | 4.8% | 7.7% | 3.3% | 3.9% | 8.4% | 5.8% | 6.3% | 7.1% | 4.6% | 5.4% |
| Spyware | 0.3% | 0.4% | 0.1% | 0.1% | 0.2% | 1.8% | 0.2% | 0.3% | 0.1% | 0.3% | 0.1% |

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

- Within each row of Figure 28, 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.
- Although France had lower than average detection rates in most categories, adware was found on 72.4 percent of computers reporting detections, a rate nearly twice as high as the worldwide average. The top 6 families detected in France in 2Q11 were adware families, with all other categories far behind. (See the *Microsoft Security Intelligence Report* website for additional details.)
- Italy experienced a rise in Adware detections similar to that of France, because of increased detections of many of the same families. A new family, Adware:Win32/OfferBox, was the top family in both France and Italy in 2Q11.
- Brazil has long had higher-than-average detections of Password Stealers & Monitoring Tools because of the prevalence of Win32/Bancos, which targets customers of Brazilian banks. Detections of Password Stealers & Monitoring Tools are still high, but a number of other categories have also increased to significantly above average because of increased detections of families such as JS/Pornpop, HTML/IframeRef, and Win32/OpenCandy.

- China has a relatively high concentration of Miscellaneous Potentially Unwanted Software, Backdoors, and Spyware, and a relatively low concentration of Adware. China routinely exhibits a threat mix that is much different than those of other large countries and regions, featuring a number of Chinese-language families like Win32/BaiduSobar that are uncommon elsewhere. The most commonly detected families in China also include an exploit, JS/CVE-2010-0806, that is less prevalent elsewhere.

See the full report for more information about malware around the world.

## Threat Families

Figure 29 lists the top 10 malware and potentially unwanted software families that were detected on computers by Microsoft antimalware desktop products in the first half of 2011.

Figure 29. Quarterly trends for the top 10 malware and potentially unwanted software families detected by Microsoft antimalware desktop products in 1Q11 and 2Q11, shaded according to relative prevalence

| Family | Category | 3Q10 | 4Q10 | 1Q11 | 2Q11 |
|---|---|---|---|---|---|
| Win32/Hotbar | Adware | 997,111 | 1,661,747 | 3,149,677 | 4,411,501 |
| JS/Pornpop | Adware | 2,659,054 | 3,666,856 | 4,706,968 | 4,330,510 |
| Win32/Autorun | Worms | 2,454,708 | 2,624,241 | 3,718,690 | 3,677,588 |
| Win32/OpenCandy | Adware | — | — | 6,797,012 | 3,652,658 |
| Win32/ShopperReports | Adware | — | — | 3,348,949 | 2,902,430 |
| Win32/Keygen | Misc. Potentially Unwanted Software | 981,051 | 1,402,417 | 2,299,870 | 2,680,354 |
| Win32/ClickPotato | Adware | 451,407 | 2,074,751 | 4,694,442 | 2,592,125 |
| Win32/Zwangi | Misc. Potentially Unwanted Software | 1,637,316 | 2,236,990 | 2,785,111 | 2,586,630 |
| Win32/Rimecud | Misc. Trojans | 1,673,312 | 1,872,449 | 2,123,298 | 1,818,530 |
| Win32/Conficker | Worm | 1,648,481 | 1,636,201 | 1,859,498 | 1,790,035 |

- Win32/OpenCandy was the most commonly detected family in 1H11 overall. OpenCandy is an adware program that may be bundled with certain third-party software installation programs, for which detection was first added in February 2011. Some versions of the OpenCandy program send user-specific information without obtaining adequate user consent, and these versions are detected by Microsoft antimalware products.
- JS/Pornpop, the second most commonly detected family in 1H11 overall, is a detection for specially crafted JavaScript-enabled objects that attempt to

display pop-under advertisements in users' web browsers. Initially, JS/Pornpop appeared exclusively on websites that contained adult content; however, it has since been observed to appear on websites that may contain no adult content whatsoever. First detected in August 2010, it grew quickly to become one of the most prevalent families in the world.

- Win32/Hotbar, the most commonly detected family in 2Q11 and the third most commonly detected family in 1H11, is adware that installs a browser toolbar that displays targeted pop-up ads based on its monitoring of web browsing activities. Hotbar has existed for several years, but has increased significantly in prevalence beginning in 1Q11.
- Win32/Autorun, the fourth most commonly detected family in 1H11, is a generic detection for worms that spread between mounted volumes using the AutoRun feature of Windows. AutoRun detections had been increasing steadily for several quarters before declining slightly in 2Q11, following the February release of a security update that changed the way the AutoPlay feature works in Windows XP and Windows Vista. (See the full report for more information about this change.)
- The adware family Win32/ClickPotato, the fifth most commonly detected family in 1H11, was first detected in August 2010 and rose quickly to occupy the third spot in 1Q11 before rapidly declining in 2Q11. ClickPotato is a program that displays pop-up and notification-style advertisements based on the user's browsing habits.

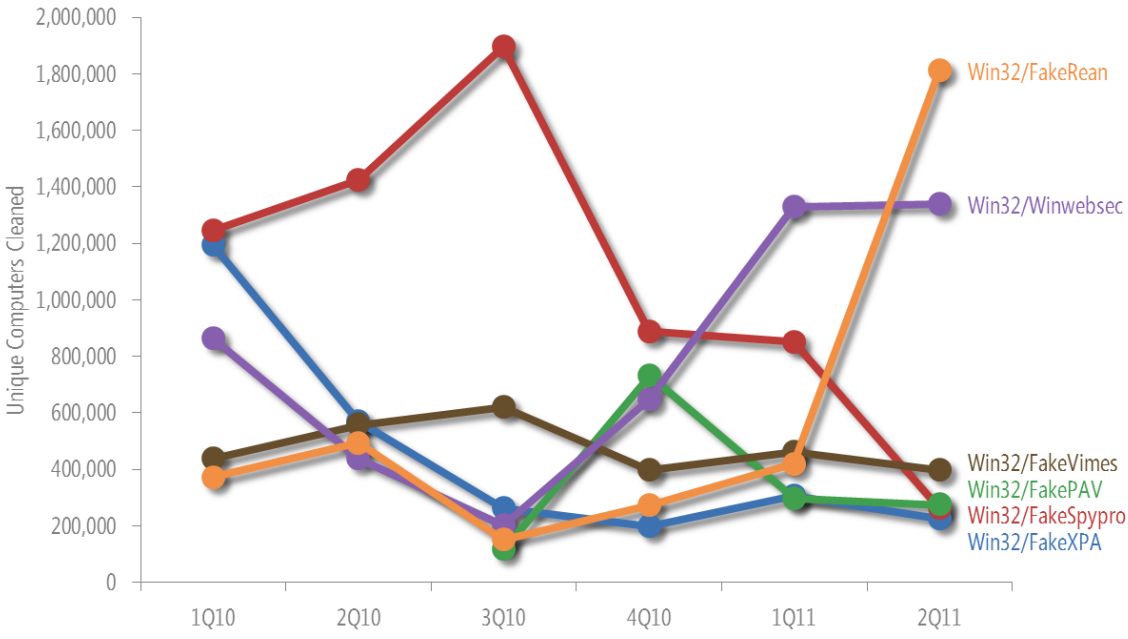
## Rogue Security Software

*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 www.microsoft.com/security/antivirus/rogue.aspx for an informative series of videos designed to educate a general audience about rogue security software.)

Figure 30. "Brands" used by a number of commonly detected rogue security software programs


Figure 31 shows detection trends for the most common rogue security software families detected in 1H11.

Figure 31. Trends for the most common rogue security software families detected in 1H11, by quarter




- Detections of Win32/FakeRean increased more than 300 percent from 1Q11 to 2Q11 to become the most commonly detected rogue security software family of the second quarter. As with a number of other rogue security software families, FakeRean distributors sometimes concentrate their

distribution efforts into discrete "campaigns," which can lead to sudden spikes in detections like the one observed in 2Q11.

FakeRean has been distributed with several different names. The user interface and some other details vary to reflect each variant's individual branding. Current variants of FakeRean choose a name at random, from a number of possibilities determined by the operating system of the affected computer. Detections for FakeRean were added to the MSRT in August 2009.

For more information about FakeRean, see the following entries in the MMPC blog (blogs.technet.com/mmpc):

- Win32/FakeRean and MSRT (August 11, 2009)
- Win32/FakeRean is 33 rogues in 1 (March 9, 2010)

- As with FakeRean, detections of Win32/Winwebsec increased significantly in 2011, making it the second most commonly detected rogue security software family of 2Q11. Winwebsec has also been distributed under many names, with the user interface and other details varying to reflect each variant's individual branding. These different distributions of the trojan use various installation methods, with filenames and system modifications that can differ from one variant to the next. The attackers behind Winwebsec are also believed to be responsible for MacOS_X/FakeMacdef, the highly publicized "Mac Defender" rogue security software program for Apple Mac OS X that first appeared in May 2011. Detections for Winwebsec were added to the MSRT in May 2009.

  For more information about the connection between Winwebsec and FakeMacdef, see the entry "Winwebsec gang responsible for Fakemacdef?" (May 17, 2011) in the MMPC blog.

- Win32/FakeSpypro, the most commonly detected rogue security software family in 2010 by a wide margin, declined steeply beginning in 4Q10 to become only the fifth most prevalent rogue security software family in 2Q11. 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.

## Home and Enterprise Threats

The usage patterns of home users and enterprise users tend to be very different. Enterprise users typically use computers to perform business functions while connected to a network, and may have limitations placed on their Internet and

email usage. Home users are more likely to connect to the Internet directly or through a home router and to use their computers for entertainment purposes, such as playing games, watching videos, shopping, and communicating with friends. These different usage patterns mean that home users tend to be exposed to a different mix of computer threats than enterprise users.

The infection telemetry data produced by Microsoft desktop antimalware products and tools includes information about whether the infected computer belongs to an Active Directory® Domain Services domain. Such domains are used almost exclusively in enterprise environments, and computers that do not belong to a domain are more likely to be used at home or in other non-enterprise contexts. Comparing the threats encountered by domain-joined computers and non-domain computers can provide insights into the different ways attackers target enterprise and home users and which threats are more likely to succeed in each environment.

Figure 32 and Figure 33 list the top 10 families detected on domain-joined and non-domain computers, respectively, in 2Q11.

Figure 32. Top 10 families detected on domain-joined computers, 3Q10–2Q11, by percentage of domain-joined computers reporting detections

| | Family | Most Significant Category | 3Q10 | 4Q10 | 1Q11 | 2Q11 |
|---|---|---|---|---|---|---|
| 1 | Win32/Conficker | Worm | 19.6% | 18.9% | 17.8% | 15.8% |
| 2 | Win32/Autorun | Worm | 10.0% | 10.0% | 11.7% | 11.1% |
| 3 | Win32/Rimecud | Worm | 8.0% | 8.3% | 8.1% | 5.8% |
| 4 | Win32/OpenCandy | Adware | — | — | 8.5% | 4.9% |
| 5 | Win32/RealVNC | Misc. Potentially Unwanted Software | 4.9% | 4.3% | 4.5% | 4.4% |
| 6 | JS/Pornpop | Adware | 3.4% | 4.5% | 4.4% | 3.9% |
| 7 | Win32/Obfuscator | Misc. Trojans | 1.9% | 1.4% | 3.4% | 4.4% |
| 8 | Win32/Keygen | Misc. Potentially Unwanted Software | 1.5% | 2.2% | 2.9% | 3.5% |
| 9 | Java/CVE-2010-0840 | Exploits | — | — | 3.3% | 3.1% |
| 10 | Win32/Sality | Viruses | 2.5% | 2.7% | 2.7% | 2.8% |

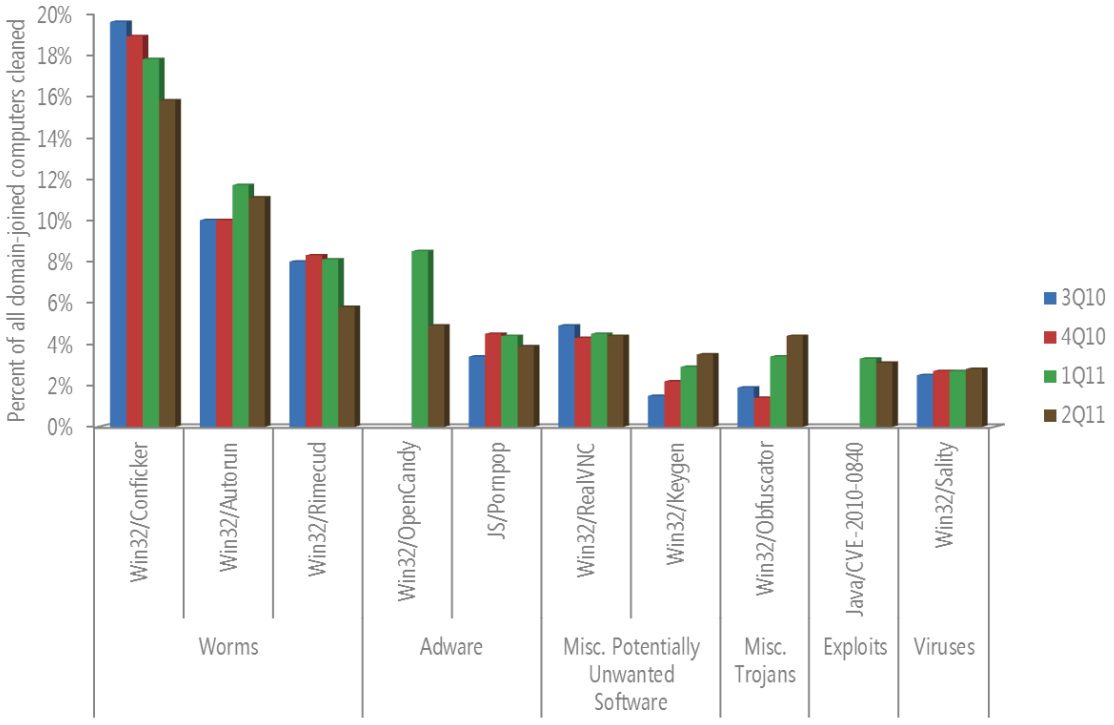
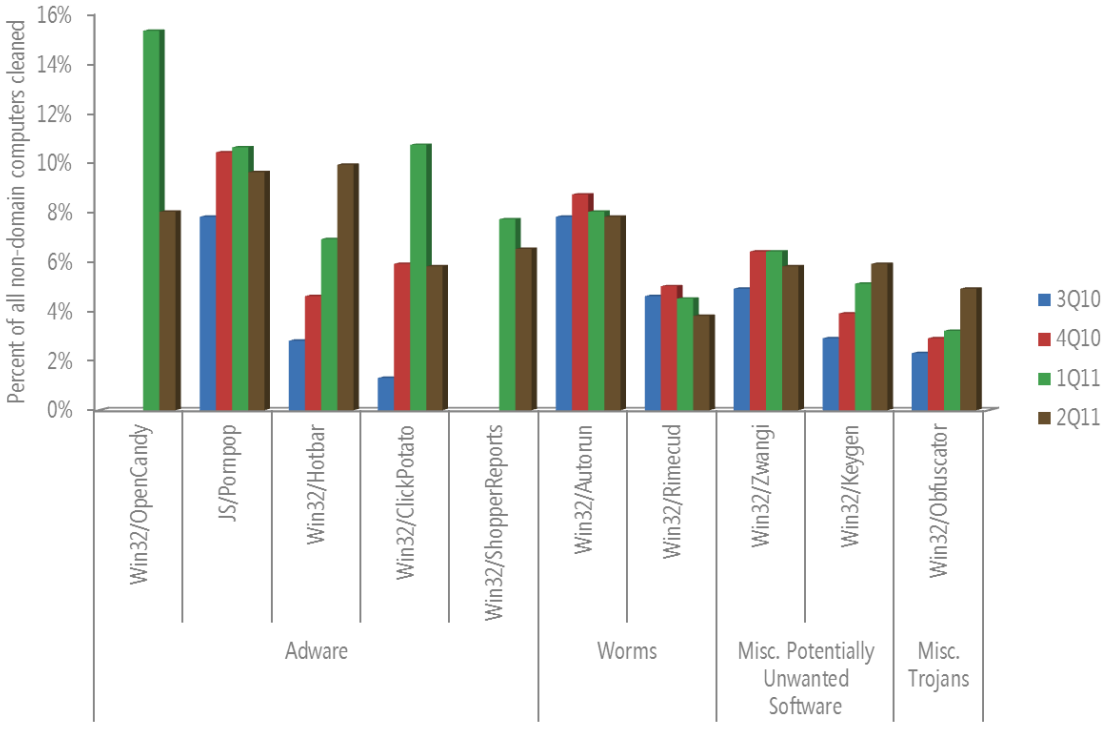


Figure 33. Top 10 families detected on non-domain computers, 3Q10–2Q11, by percentage of non-domain computers reporting detections

| | Family | Most Significant Category | 3Q10 | 4Q10 | 1Q11 | 2Q11 |
|---|---|---|---|---|---|---|
| 1 | Win32/OpenCandy | Adware | — | — | 15.3% | 8.0% |
| 2 | JS/Pornpop | Adware | 7.8% | 10.4% | 10.6% | 9.6% |
| 3 | Win32/Hotbar | Adware | 2.8% | 4.6% | 6.9% | 9.9% |
| 4 | Win32/ClickPotato | Adware | 1.3% | 5.9% | 10.7% | 5.8% |
| 5 | Win32/Autorun | Worm | 7.8% | 8.7% | 8.0% | 7.8% |
| 6 | Win32/ShopperReports | Adware | — | — | 7.7% | 6.5% |
| 7 | Win32/Zwangi | Misc. Potentially Unwanted Software | 4.9% | 6.4% | 6.4% | 5.8% |
| 8 | Win32/Keygen | Misc. Potentially Unwanted Software | 2.9% | 3.9% | 5.1% | 5.9% |
| 9 | Win32/Rimecud | Worms | 4.6% | 5.0% | 4.5% | 3.8% |
| 10 | Win32/Obfuscator | Misc. Trojans | 2.3% | 2.9% | 3.2% | 4.9% |




- Six families are common to both lists, although they are ordered differently and in different proportions. The generic detection Win32/Autorun and the adware family Win32/OpenCandy are high on both lists.

- Worms accounted for the top three families detected on domain-joined computers. Win32/Conficker and Win32/Rimecud, the first and third families on the list, are both designed to propagate via network shares, which are common in domain environments. Conficker has declined slowly over the past four quarters, and dropped 2 percentage points between 1Q11 and 2Q11.
- Adware and potentially unwanted software account for 7 of the top 10 families detected on non-domain computers.
- Families that are significantly more prevalent on domain-joined computers include Conficker and the potentially unwanted software program Win32/RealVNC. RealVNC is a program that enables a computer to be controlled remotely, similar to Remote Desktop Services. It has a number of legitimate uses, but attackers have also used it to gain control of users' computers for malicious purposes.
- Java/CVE-2010-0840, an exploit that targets a vulnerability in older versions of Oracle Java SE and Java for Business, was the ninth most commonly detected threat on domain-joined computers. It is the only exploit to appear on either list. See "Java Exploits" on page 18 for more information about this exploit.
- The virus family Win32/Sality, which was not among the top 10 families detected on domain-joined computers in 2010, ranks tenth in the latest chart. Detections of Sality have not significantly increased over the past four quarters, but significant declines in detections of formerly prevalent families such as Win32/Taterf, Win32/Hamweq, and Win32/Renos have enabled less common families like Sality to make the list.
- Families that are significantly more prevalent on non-domain computers include the adware families Win32/Hotbar, JS/Pornpop, and Win32/ClickPotato, all of which display pop-up or pop-under advertisements in various contexts that may not be desired.
- As with domain-joined computers, a number of formerly prevalent families no longer appear on the list of the top threats detected on non-domain computers. Among these are the worm families Taterf and Conficker, and the rogue security software family Win32/FakeSpypro.

## Guidance: Defending Against Malware

Effectively protecting users from malware requires an active effort on the part of organizations and individuals. For in-depth guidance, see Protecting Against Malicious and Potentially Unwanted Software in the "Mitigating Risk" section of the *Microsoft Security Intelligence Report* website.

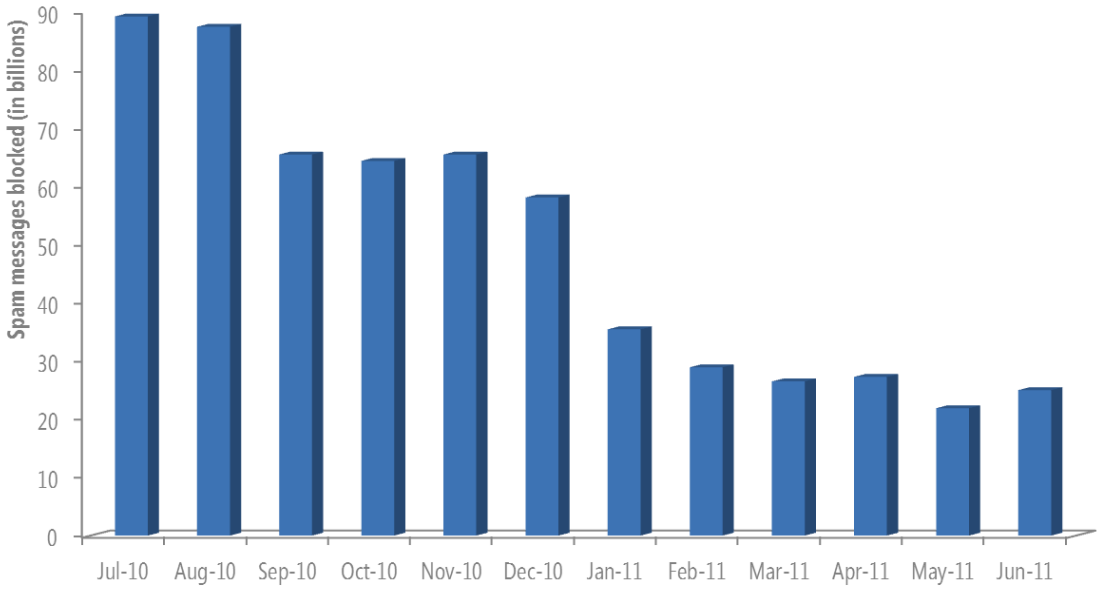
# Email Threats

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 of the *Microsoft Security Intelligence Report* 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 Microsoft enterprise customers that process tens of billions of messages each month.

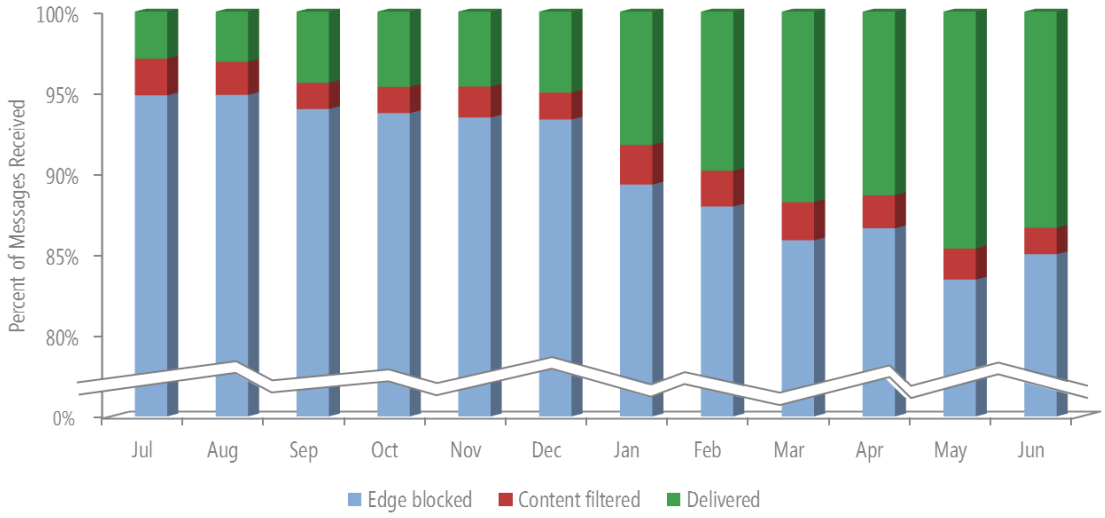
Figure 34. Messages blocked by FOPE each month from July 2010 to June 2011



- The volume of spam blocked by FOPE decreased dramatically over the past 12 months, from a high of 89.2 billion messages in July 2010 to a low of 21.9 billion in May 2011, primarily because of takedowns of two major botnets: Cutwail, which was shut down in August 2010, and Rustock, which was shut down in March 2011 following a period of dormancy that began in January. [3]
- The magnitude of this decrease suggests that coordinated takedown efforts such as the ones directed at Cutwail and Rustock can have a positive effect on improving the health of the email ecosystem.

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 35. Percentage of incoming messages blocked by FOPE using edge-blocking and content filtering from July 2010 to June 2011




- Between 85 and 95 percent of incoming messages were blocked at the network edge each month, which means that only 5 to 15 percent of incoming messages had to be subjected to the more resource-intensive content filtering process.

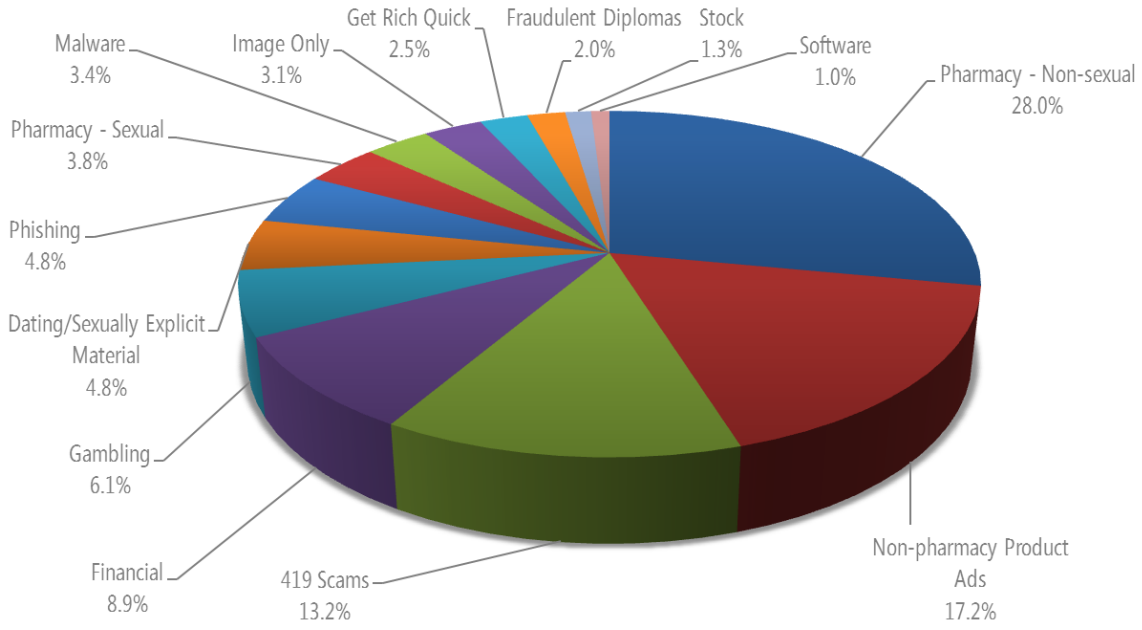
[3] For more information about the Cutwail takedown, see *Microsoft Security Intelligence Report, Volume 10 (July-December 2010)*. For more information about the Rustock takedown, see "Battling the Rustock Threat," available from the Microsoft Download Center.

- The decline in the percentage of messages blocked at the network edge beginning in January was caused by the overall decline in the volume of spam that occurred following the inactivation of the Rustock botnet.

## Spam Types

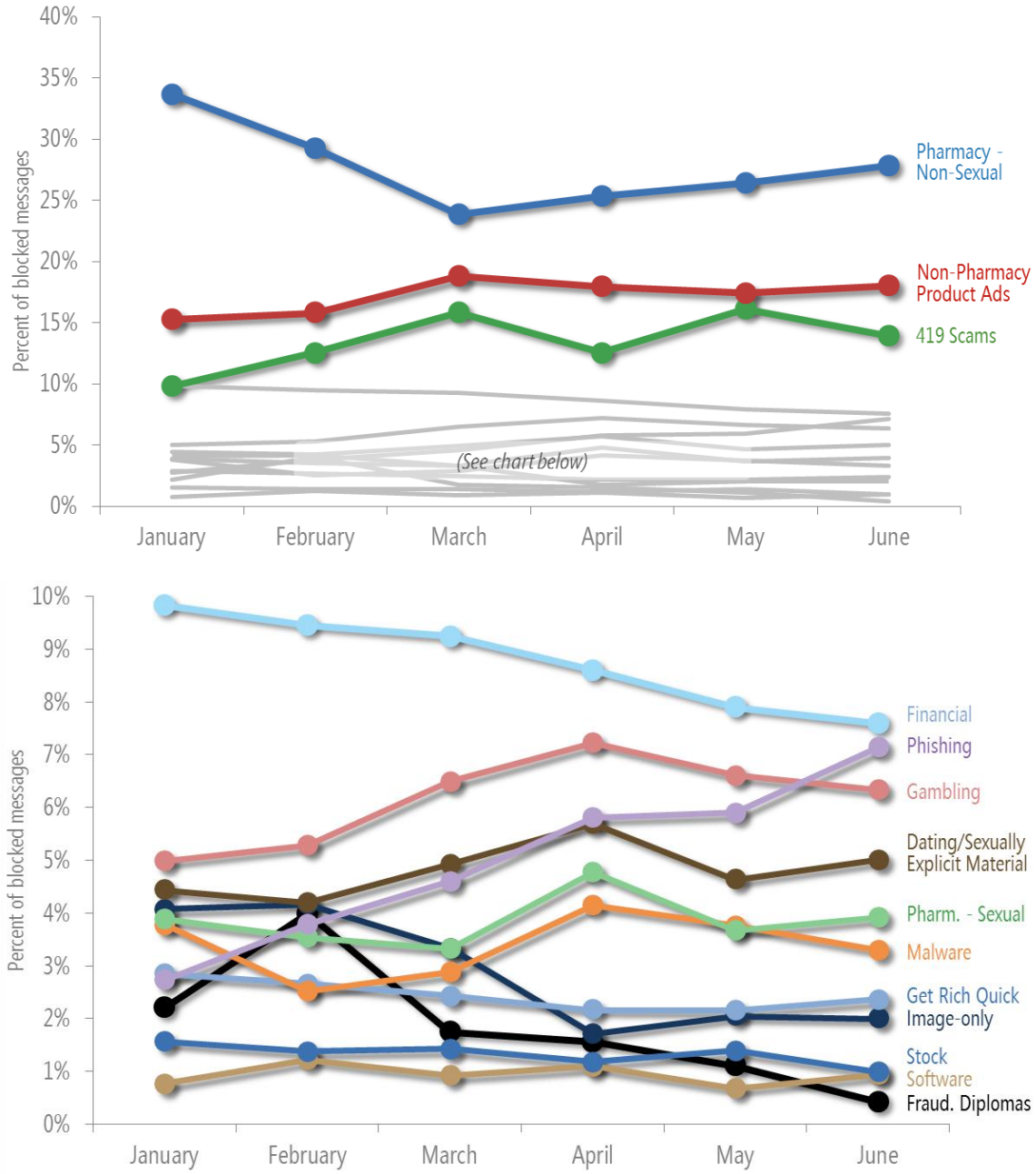
The FOPE content filters recognize several different common types of spam messages. Figure 36 shows the relative prevalence of these spam types in 1H11.

Figure 36. Inbound messages blocked by FOPE filters in 1H11, by category




- As in previous periods, advertisements for nonsexual pharmaceutical products (28.0 percent of the total) and nonpharmaceutical product advertisements (17.2 percent) accounted for the majority of the spam messages blocked by FOPE content filters in 1H11. Together with so-called "419" advance-fee loan scams (13.2 percent), these categories accounted for most of the spam messages that were blocked during the period. (See the *Microsoft Security Intelligence Report* website for more information about these scams.)
- In an effort to evade content filters, spammers sometimes send messages that consist only of one or more images, with no text in the body of the message. Image-only spam messages declined to 3.1 percent of the total in 1H11, down from 8.7 percent in 2010.

Figure 37. Inbound messages blocked by FOPE content filters each month in 1H11, by category




- Unlike in some recent periods, which showed evidence of individual spam "campaigns" featuring large volumes of certain types of spam for short periods of time, the increases and decreases of the spam categories tracked by FOPE were much more gradual from month to month. A possible exception involves

spam that advertises fraudulent university diplomas. Typically a low-volume category, fraudulent diploma spam increased to 4.0 percent of the total in February, following a much larger spike in volume that occurred around the same time in 2010.

- Phishing messages increased significantly over the period, going from 2.8 percent of the total in January to 7.2 percent in June. (See "Phishing Sites" on page 55 for more phishing-related statistics.)

## Guidance: Defending Against Threats in Email

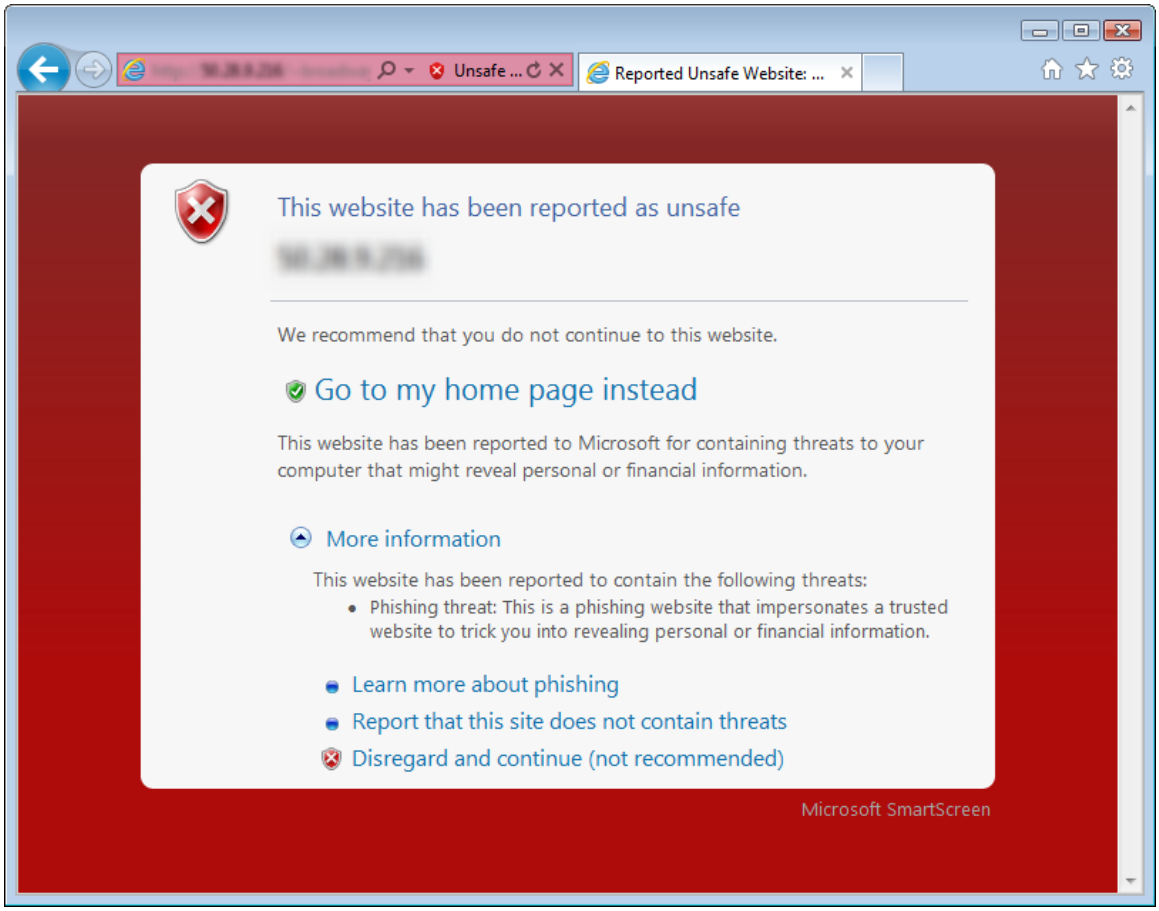
In addition to using a filtering service such as FOPE, organizations can take a number of steps to reduce the risks and inconvenience of unwanted email. Such steps include implementing email authentication techniques and observing best practices for sending and receiving email. For in-depth guidance,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

# Malicious Websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear 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 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 Appendix B in the full report for more information about the products and services that provided data for this report.)

Figure 38. SmartScreen Filter in Internet Explorer 8 and 9 blocks reported phishing and malware distribution sites to protect the user




## Phishing Sites

Microsoft gathers information about phishing sites and impressions from *phishing impressions* generated by users who choose to enable the Phishing Filter or SmartScreen Filter in Internet Explorer. A phishing impression is a single instance of a user attempting to visit a known phishing site with Internet Explorer and being blocked, as illustrated in Figure 39.

Figure 39. How Microsoft tracks phishing impressions

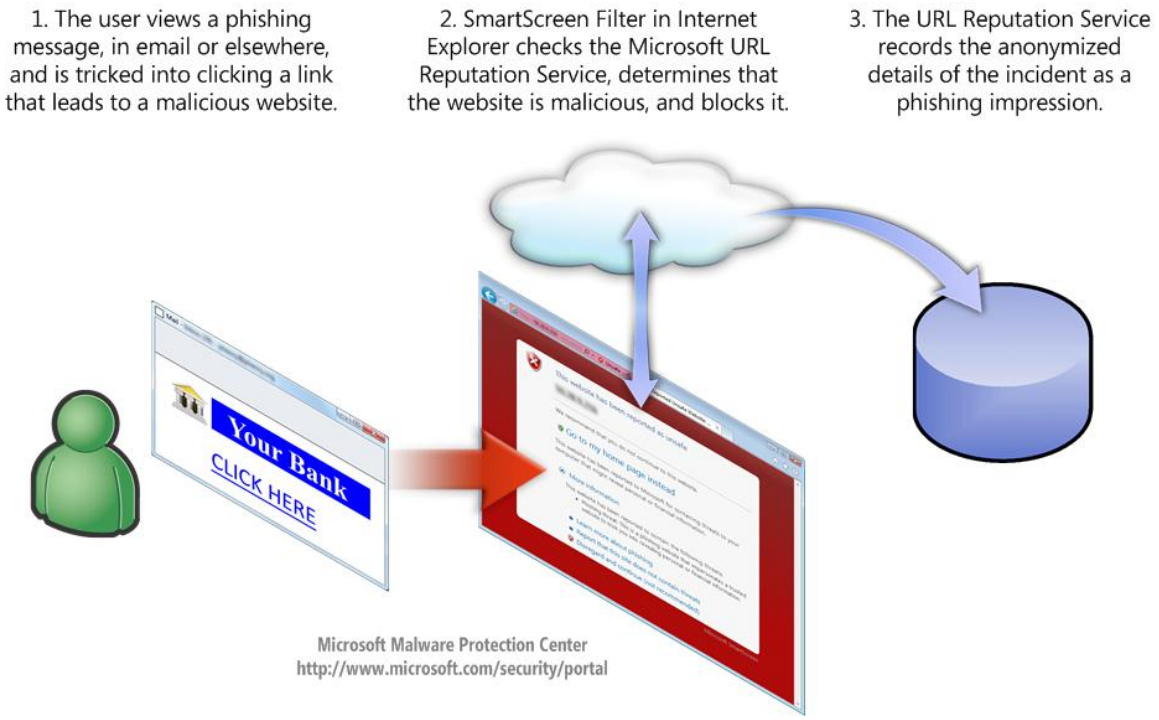
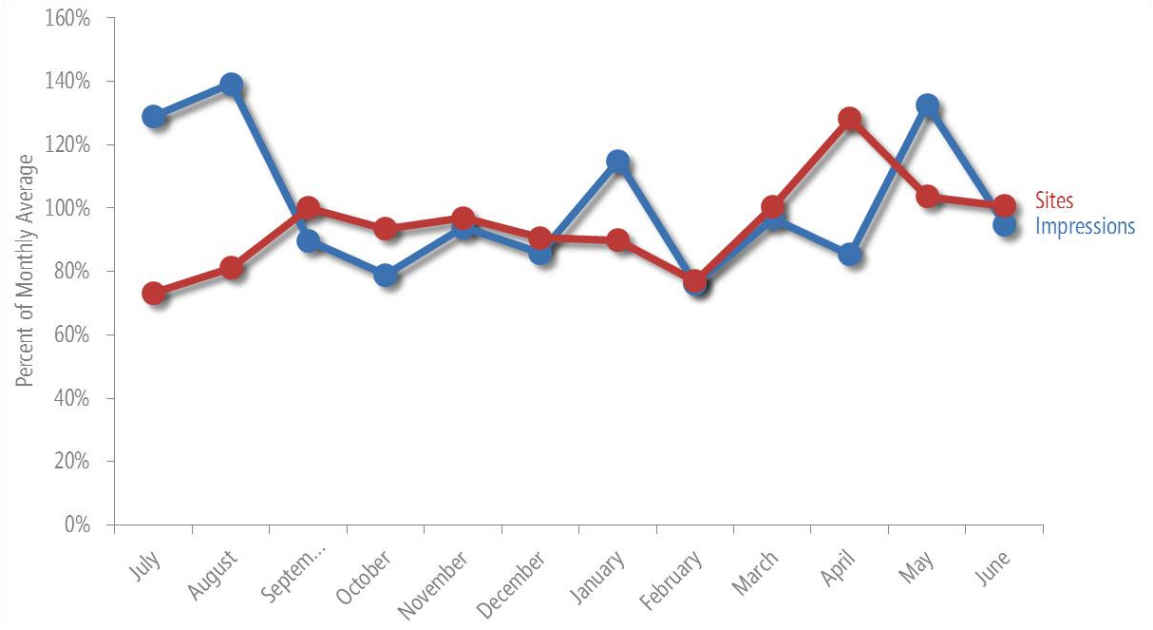



Figure 40 compares the volume of active phishing sites in the Microsoft URL Reputation Service database each month with the volume of phishing impressions tracked by Internet Explorer.

Figure 40. Phishing sites and impressions tracked each month from July 2010 to June 2011 relative to the monthly average for each




- Following a large spike in impressions in June 2010, the figures for both sites and impressions have been mostly stable over the past 12 months. Most phishing sites only last a few days, and attackers create new ones to replace older ones as they are taken offline, so the list of known phishing sites is prone to constant change without significantly affecting overall volume.
- Phishing impressions and active phishing pages rarely correlate strongly with each other. Phishers often engage in discrete campaigns intended to drive more traffic to each phishing page, without necessarily increasing the total number of active phishing pages they maintain at the same time. In August 2010, the month with the highest number of impressions over the past year, the number of active phishing sites tracked was actually near its lowest level for the period.

## Target Institutions

Figure 41 and Figure 42 show the percentage of phishing impressions and active phishing sites, respectively, recorded by Microsoft during each month in 1H11 for the most frequently targeted types of institutions.

Figure 41. Impressions for each type of phishing site each month in 1H11, as reported by SmartScreen Filter

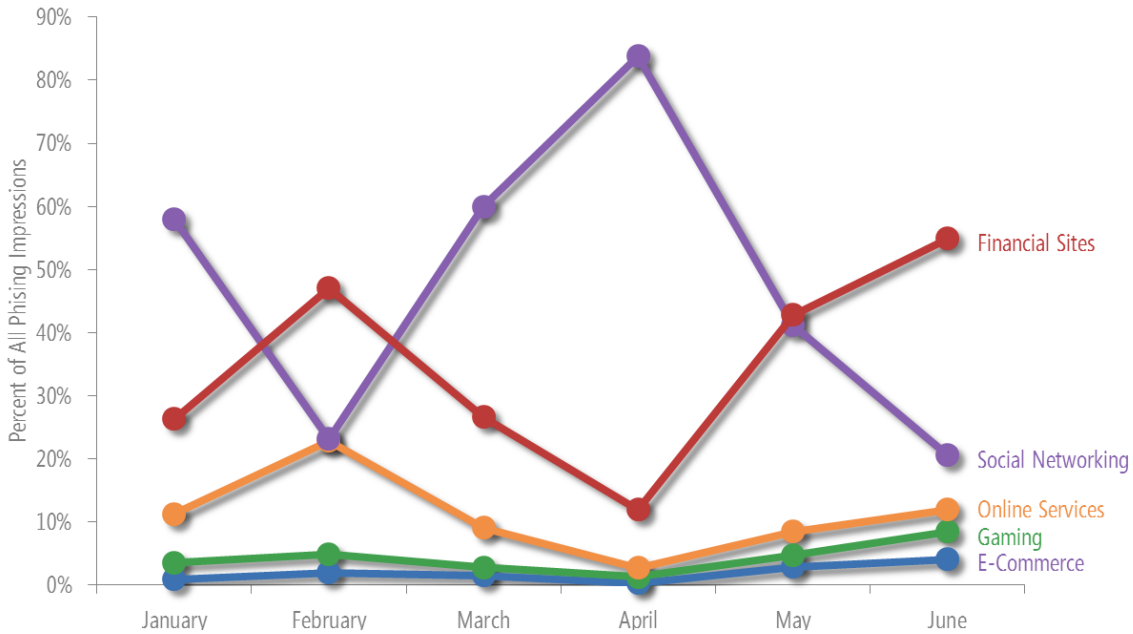
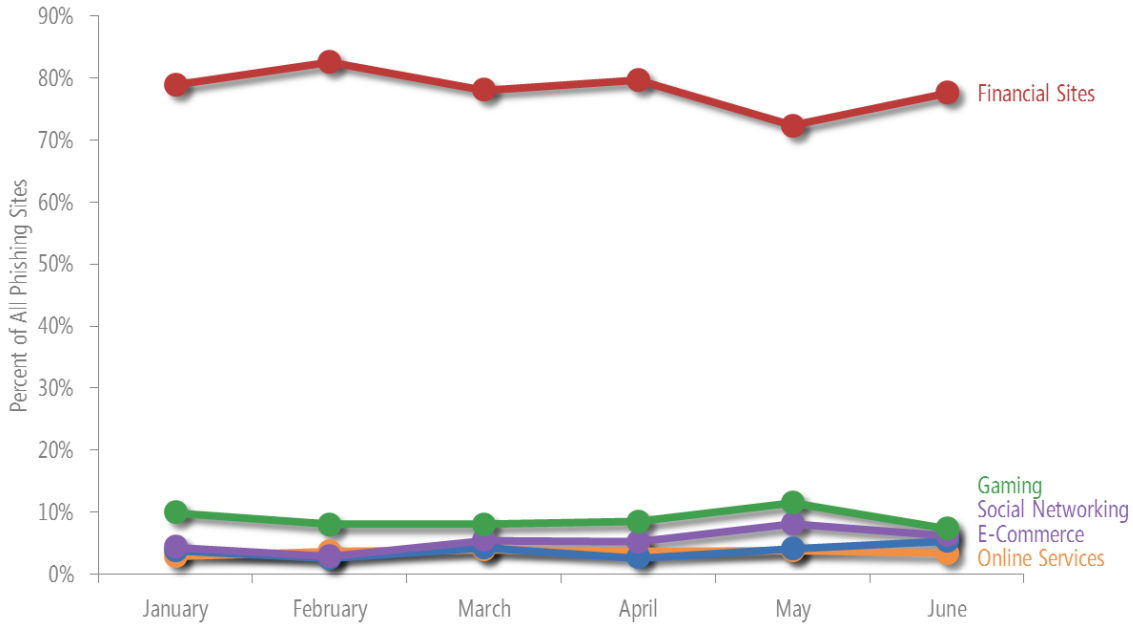



Figure 42. Active phishing sites tracked each month in 1H11, by type of target




- Phishers have traditionally targeted financial sites more than other types of sites, but the largest share of phishing impressions in 1H11 was for sites that

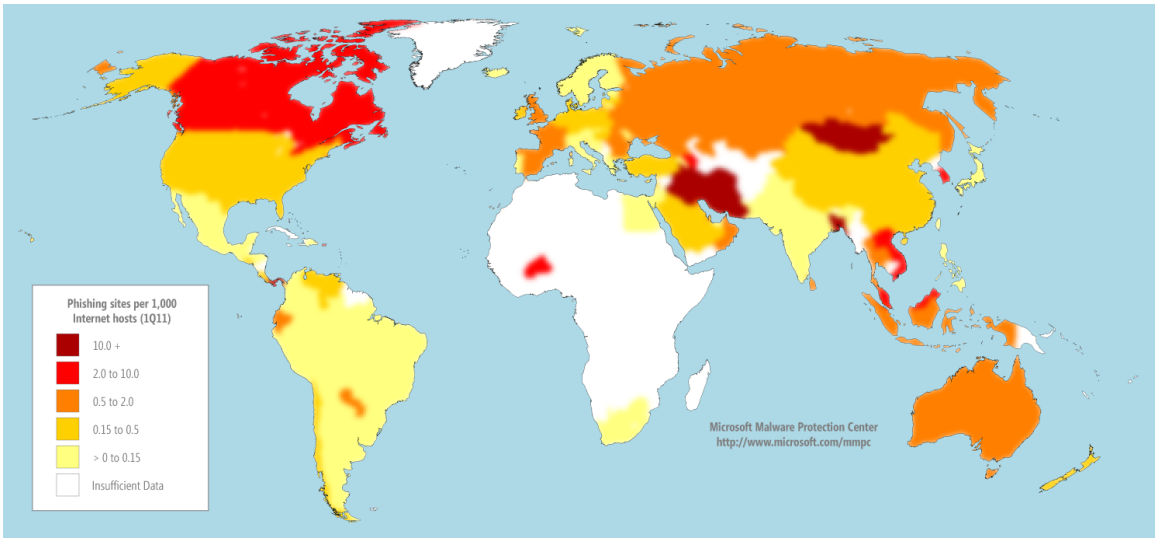
targeted social networks, reaching a high of 83.8 percent of impressions in April. Overall, impressions that targeted social networks accounted for 47.8 percent of all impressions in 1H11, followed by those that targeted financial institutions at 35.0 percent.

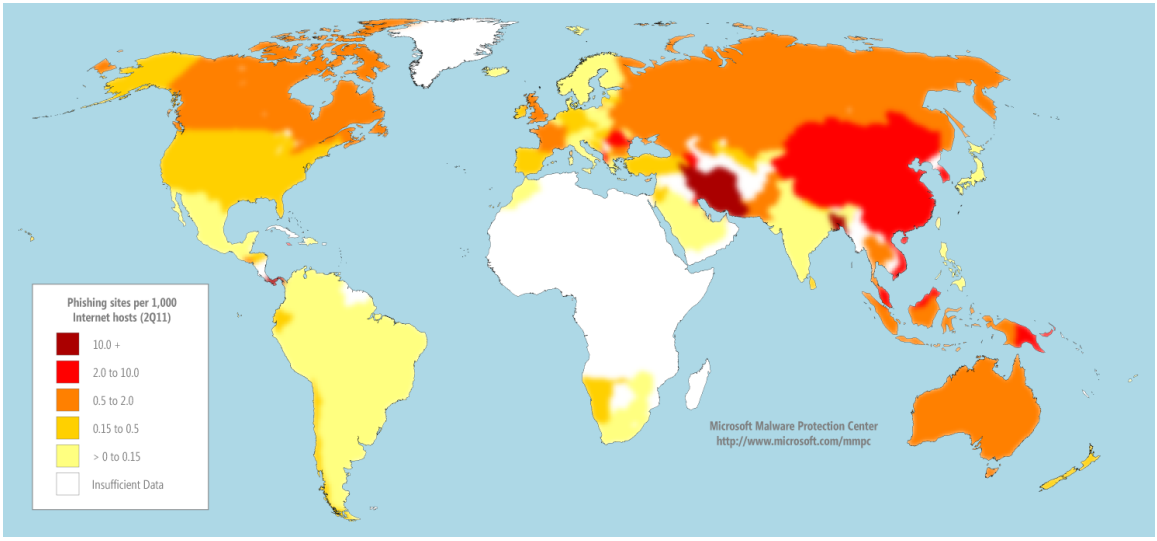
- By contrast, phishing sites that targeted financial institutions accounted for an average of 78.3 percent of active phishing sites tracked each month in 1H11, compared to just 5.4 percent for social networks. Financial institutions targeted by phishers can number in the hundreds, and customized phishing approaches are required for each one. The number of popular social networking sites is much smaller, so phishers who target social networks 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.
- This phenomenon also occurs on a smaller scale with online services and gaming sites. A small number of online services account for the majority of traffic to such sites, so phishing sites that targeted online services garnered 11.0 percent of impressions with just 3.6 percent of sites. Online gaming traffic tends to be spread out among a larger number of sites, so phishing sites that targeted online gaming destinations accounted for 8.9 percent of active sites but gained just 4.3 percent of impressions.
- Phishing sites that targeted e-commerce were responsible for just 3.8 percent of active sites and 1.9 percent of impressions, suggesting that phishers have not found e-commerce sites to be especially profitable targets.

## 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 43. Phishing sites per 1,000 Internet hosts for locations around the world in 1Q11 (top) and 2Q11 (bottom)




- Locations with smaller populations and fewer Internet hosts tend to have higher concentrations of phishing sites, although in absolute terms most phishing sites are located in large, industrialized countries/regions with large numbers of Internet hosts.
- The worldwide distribution of phishing sites remained largely consistent between the first and second quarters. Exceptions include China, which increased from 0.35 phishing sites per 1000 hosts in 1Q11 to 2.54 in 2Q11; Canada, which decreased from 2.05 to 1.02; and France, which decreased from 1.34 to 0.81.

## Malware Hosting Sites

SmartScreen Filter in Internet Explorer 8 and 9 helps provide protection against sites that are known to host malware, in addition to phishing sites. SmartScreen Filter uses URL reputation data and Microsoft antimalware technologies to determine whether 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 SmartScreen Filter and to better combat malware distribution.

Figure 44. SmartScreen Filter in Internet Explorer 8 (top) and Internet Explorer 9 (bottom) displays a warning when a user attempts to download an unsafe file

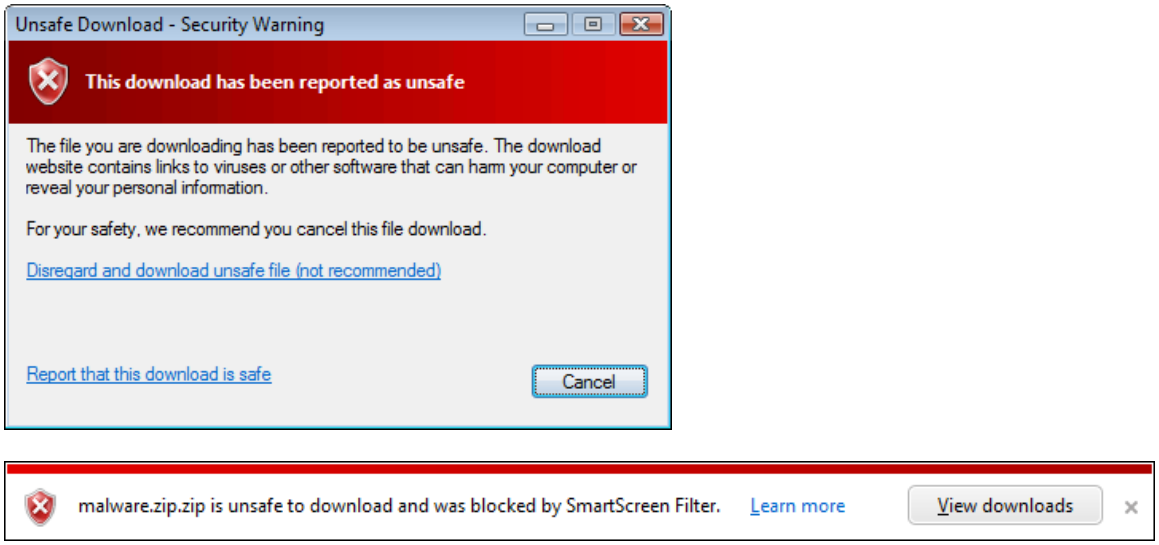
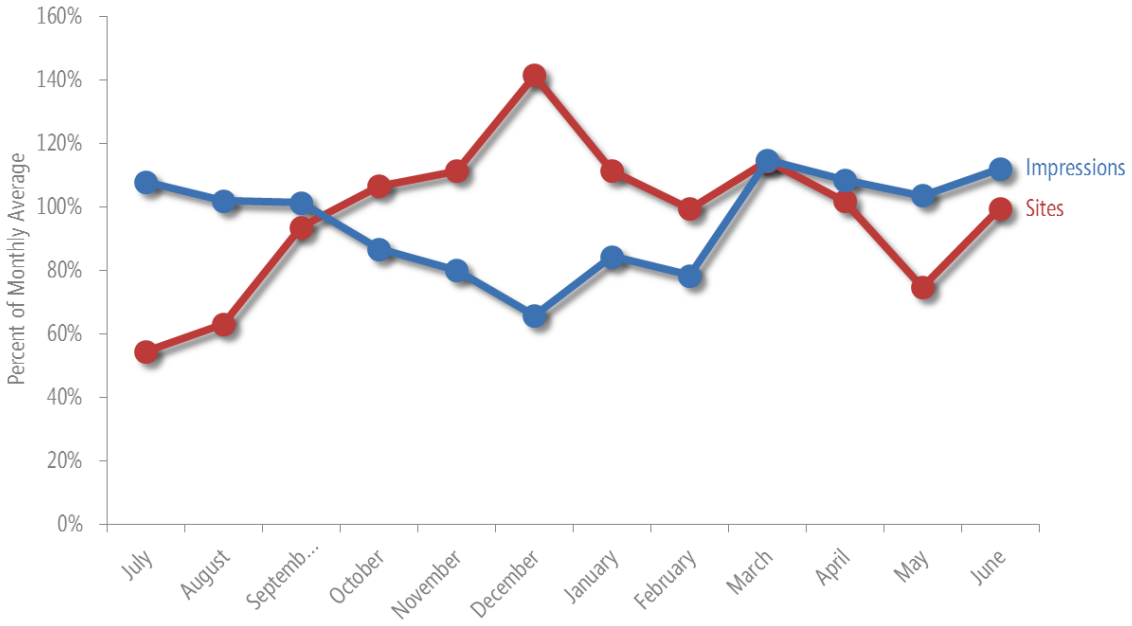



Figure 45 compares the volume of active malware hosting sites in the Microsoft URL Reputation Service database each month with the volume of malware impressions tracked by Internet Explorer.

Figure 45. Malware hosting sites and impressions tracked each month from July 2010 to June 2011, relative to the monthly average for each




- As with phishing, malware hosting impressions and active sites rarely correlate strongly with each other, and months with high numbers of sites and low numbers of impressions (or vice versa) are not uncommon.

## Malware Categories

Figure 46 and Figure 47 show the types of threats hosted at URLs that were blocked by SmartScreen Filter in 1H11.

Figure 46. Threats hosted at URLs blocked by SmartScreen Filter in 1Q11 and 2Q11, by category

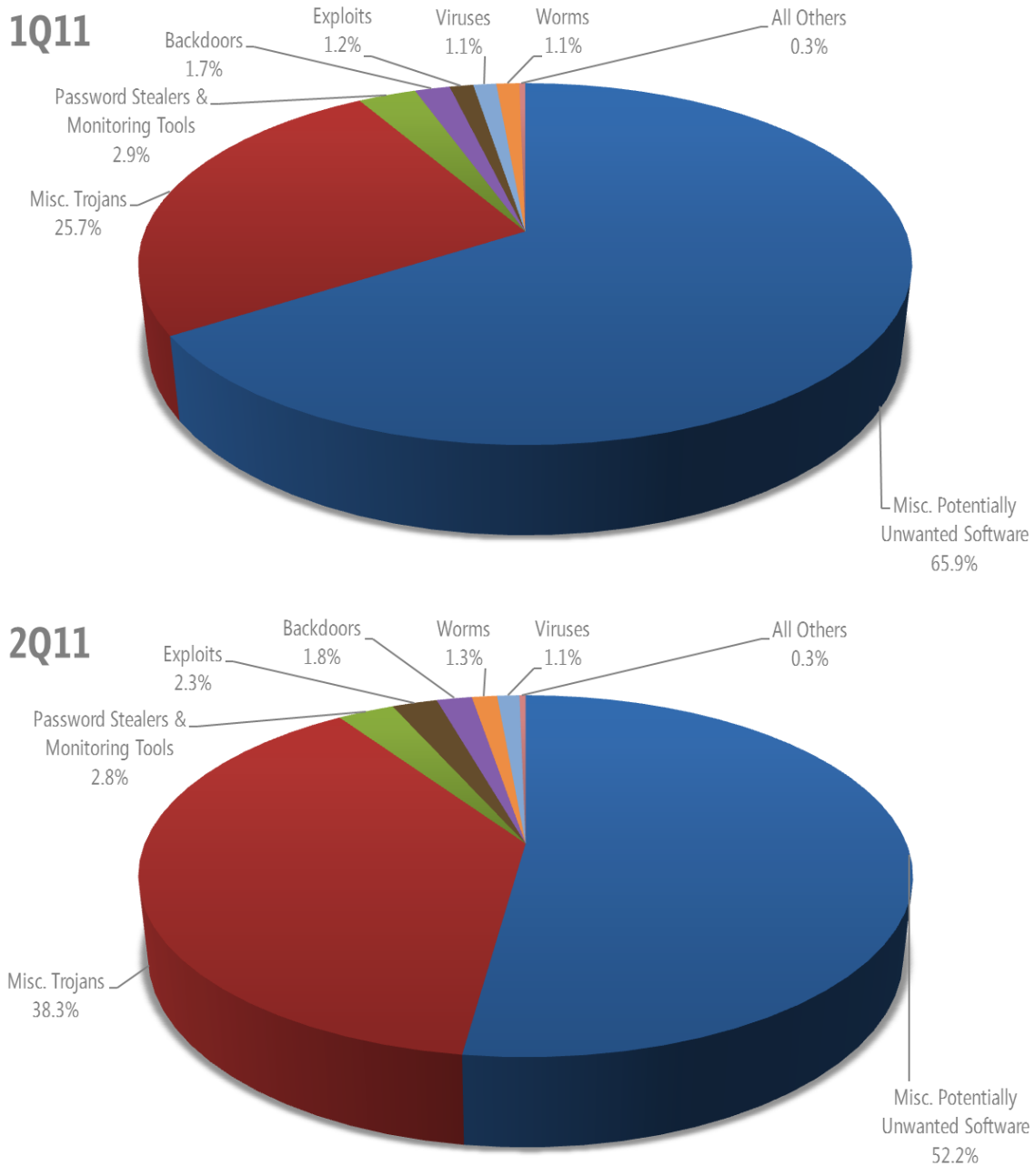


Figure 47. The top 10 malware families hosted on sites blocked by SmartScreen Filter in 1Q11 and 2Q11, by percent of all such sites

| 1Q11 Rank | Threat Name | Category | Percent |
|---|---|---|---|
| 1 | Win32/MoneyTree | Misc. Potentially Unwanted Software | 45.8% |
| 2 | Win32/Obfuscator | Misc. Potentially Unwanted Software | 6.3% |
| 3 | Win32/Begseabug | Trojan Downloaders & Droppers | 4.7% |
| 4 | VBS/Startpage | Misc. Trojans | 4.7% |
| 5 | Win32/Delf | Trojan Downloaders & Droppers | 2.6% |
| 6 | Win32/Bancos | Password Stealers & Monitoring Tools | 1.8% |
| 7 | Win32/VB | Worms | 1.7% |
| 8 | Win32/Banload | Trojan Downloaders & Droppers | 1.7% |
| 9 | Win32/Microjoin | Trojan Downloaders & Droppers | 1.3% |
| 10 | Win32/GameHack | Misc. Trojans | 1.0% |

| 2Q11 Rank | Threat Name | Category | Percent |
|---|---|---|---|
| 1 | Win32/MoneyTree | Misc. Potentially Unwanted Software | 38.8% |
| 2 | VBS/Startpage | Misc. Trojans | 15.7% |
| 3 | Win32/Obfuscator | Misc. Potentially Unwanted Software | 5.2% |
| 4 | Win32/Bancos | Password Stealers & Monitoring Tools | 2.3% |
| 5 | Win32/Small | Trojan Downloaders & Droppers | 2.3% |
| 6 | Win32/Meredrop | Misc. Trojans | 2.2% |
| 7 | Win32/VB | Worms | 1.9% |
| 8 | Win32/Microjoin | Trojan Downloaders & Droppers | 1.7% |
| 9 | Win32/Dynamer | Misc. Trojans | 1.3% |
| 10 | Win32/FakeRean | Misc. Trojans | 1.0% |

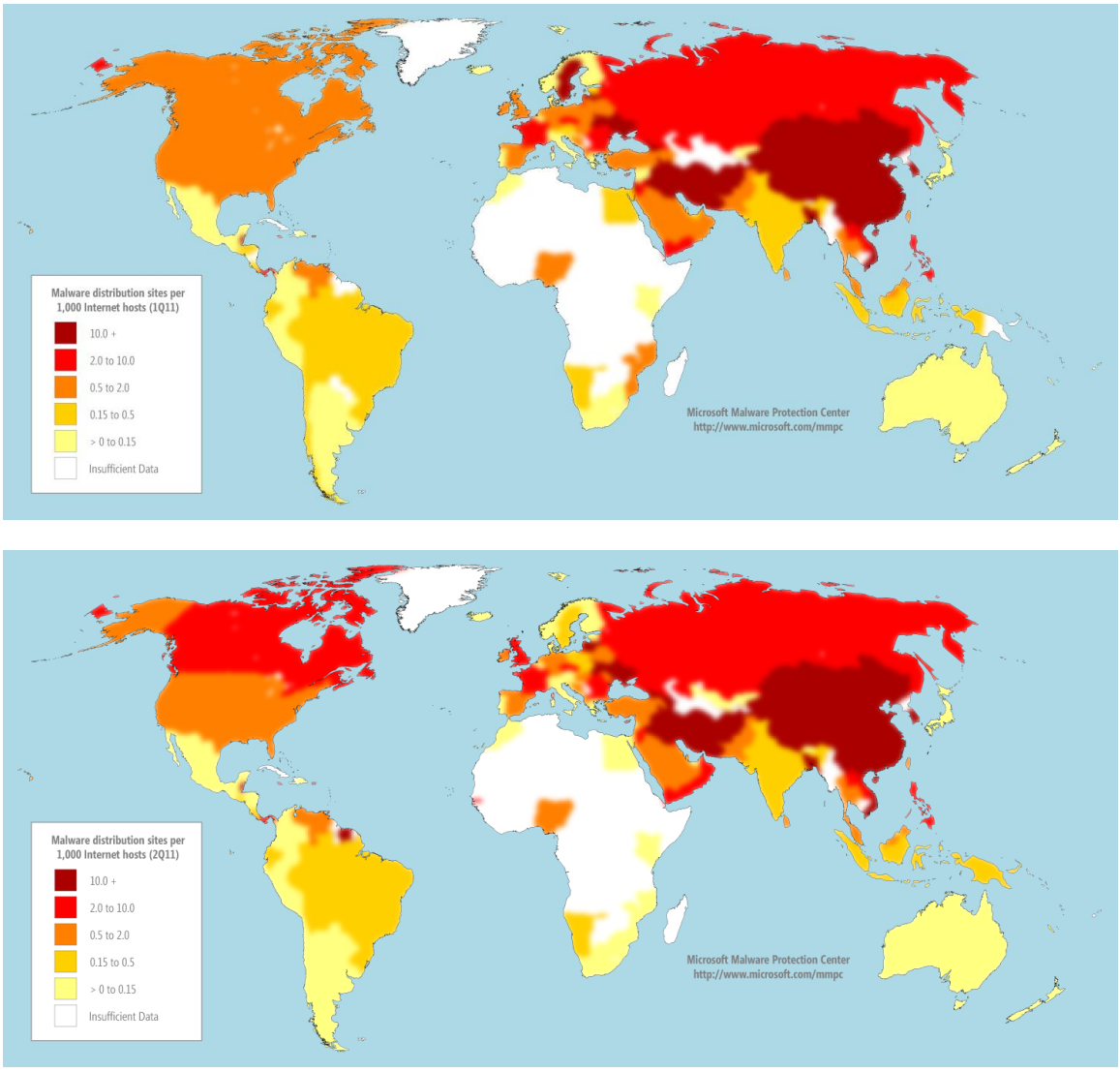
- Overall, sites that hosted the top 10 families constituted 71.6 percent of all impressions in the first quarter of 2011 and 72.3 percent in the second quarter.
- Miscellaneous Potentially Unwanted Software accounted for most impressions in both quarters, primarily because of Win32/MoneyTree. MoneyTree has consistently been the family responsible for the greatest number of impressions since 2009.

- Miscellaneous Trojans increased from 25.7 percent of impressions in 1Q11 to 38.3 percent in 2Q11, primarily because of increased impressions for VBS/Startpage, a generic detection for a range of threats that attempt to change the user's Internet Explorer home page.
- Win32/Begseabug, the third most prevalent family in 1Q11, is a trojan that downloads and executes arbitrary files on an affected computer.
- Win32/Bancos and Win32/Banload are related families that target users' online banking credentials, usually involving Brazilian banks.
- Win32/Obfuscator, Win32/Delf, Win32/Small, Win32/VB, Win32/Meredrop, Win32/Microjoin, and Win32/Dynamer are all generic detections for collections of unrelated threats that share certain identifiable characteristics.

## Global Distribution of Malware Hosting Sites

Figure 48 shows the geographic distribution of malware hosting sites reported to Microsoft in 1H11.

Figure 48. Malware distribution sites per 1,000 Internet hosts for locations around the world in 1Q11 (top) and 2Q11 (bottom)




- As with phishing sites, the worldwide distribution of malware hosting sites was largely stable between the first and second quarters. Exceptions include Sweden, which decreased from 22.48 malware hosting sites per 1000 hosts in 1Q11 to 0.15 in 2Q11; Israel, which decreased from 23.84 to 0.63; and China, which decreased from 34. 64 to 23.70.

## Drive-By Download Sites

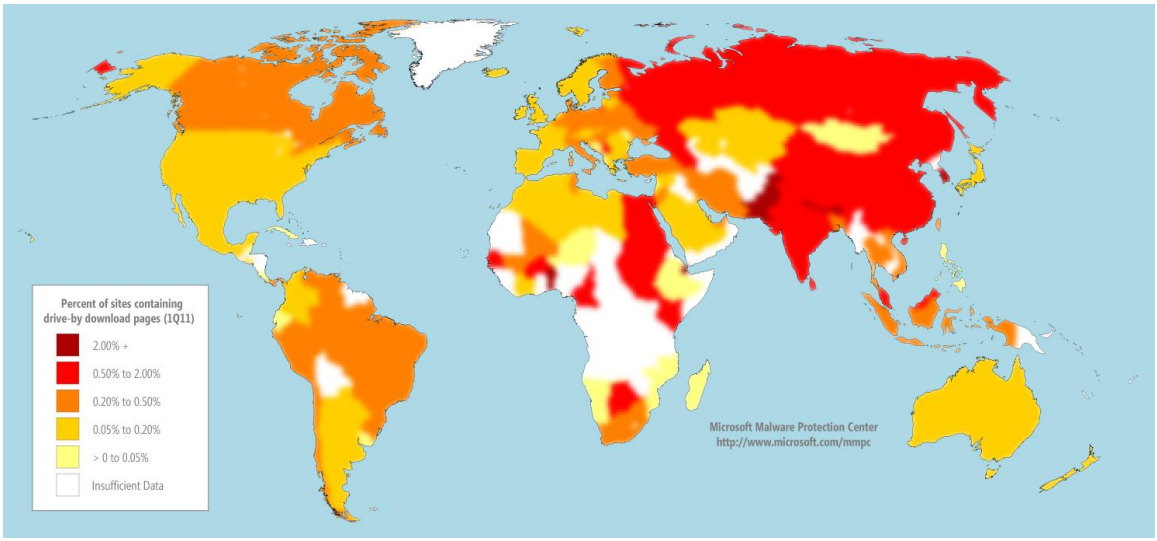
A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything.

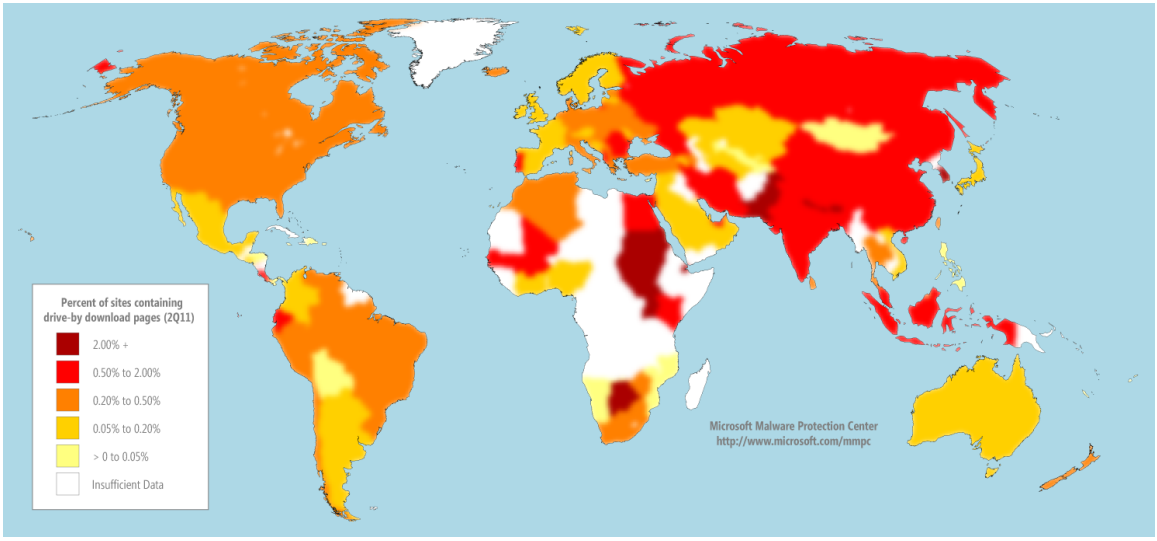
Search engines such as Microsoft Bing® have taken a number of measures to help protect users from drive-by downloads. Bing analyzes websites for exploits as they are indexed and displays warning messages when listings for drive-by download pages appear in the list of search results. (See Drive-By Download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

The information in this section was generated from an analysis of the drive-by download URLs in the Bing index in 1H11.

In previous volumes of the *Microsoft Security Intelligence Report*, drive-by statistics were presented as the percentage of websites in each country-code top-level domain (ccTLD) that host drive-by download pages. To provide a more accurate perspective on the drive-by download landscape, the current volume presents these statistics as the number of individual drive-by pages in each country or region, determined by IP geolocation, as a percentage of the total number of URLs in each. This perspective incorporates two significant changes: individual URLs are used instead of domains, and IP address is used to determine country or region instead of ccTLD. For these reasons, the statistics presented here should not be directly compared to findings in previous volumes of the *Microsoft Security Intelligence Report*.

Figure 49. Drive-by download pages in 1Q11 (top) and 2Q11 (bottom), by percentage of all URLs in each country/region




- In 1H11, about 0.25 percent of the URLs in the Bing index were compromised by drive-by download exploit code.
- Among the locations with large numbers of URLs in the index, the locations with the most pages hosting drive-by download exploit code included Korea (2.77 percent of all pages in 2Q11), China (0.8 percent), and Romania (0.66 percent).
- The locations with the greatest increases from 1Q11 to 2Q11 included Romania, which increased from 0.18 percent of pages infected to 0.66

percent; Ireland, which increased from 0.08 percent to 0.19 percent; and the United States, which increased from 0.14 percent to 0.22 percent.

- The locations with the lowest percentage of malicious or compromised pages included Japan (0.06 percent of all pages in 2Q11), Austria (0.1 percent), and Australia (0.1 percent).
- The locations with the greatest decreases from 1Q11 to 2Q11 included Sweden, which decreased from 0.12 percent of pages infected to 0.07 percent; Denmark, which decreased from 0.35 percent to 0.24 percent; Vietnam, which decreased from 0.21 percent to 0.19 percent.

## Guidance: Protecting Users from Unsafe Websites

Organizations can best protect their users from malicious and compromised websites by mandating the use of web browsers with appropriate protection features built in and by promoting safe browsing practices. For in-depth guidance, see the following resources in the "Managing Risk" section of the *Microsoft Security Intelligence Report* website:

- Promoting Safe Browsing
- Protecting Your People

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