Microsoft Security Intelligence Report

Volume 8

July through December 2009

An in-depth perspective on software vulnerabilities and exploits, malicious code threats, and potentially unwanted software, focusing on the second half of 2009

Microsoft

Microsoft Security Intelligence Report

Authors

Bret Arsenault
Microsoft Information Security

Darren Canavor
Microsoft Security Engineering Center

Eva Chow
Microsoft Information Security

Joe Faulhaber
Microsoft Malware Protection Center

Vinny Gullotto
Microsoft Malware Protection Center

Paul Henry
Wadeware LLC

Robert Hensing
Microsoft Security Response Center

Yuhui Huang
Microsoft Malware Protection Center

Jeff Jones
Microsoft Trustworthy Computing

Jimmy Kuo
Microsoft Malware Protection Center

John Lambert
Microsoft Security Engineering Center

Ken Malcolmson
Microsoft Trustworthy Computing

Bala Neerumalla
Microsoft Secure SQL Initiative Team

Anthony Penta
Microsoft Windows Safety Platform

Paul Pottorff
Windows Consumer Product Management

Tim Rains
Microsoft Trustworthy Computing

Christian Seifert
Bing

Javier Salido
Microsoft Trustworthy Computing

Frank Simorjay
Microsoft Trustworthy Computing

Holly Stewart
Microsoft Malware Protection Center

Adrian Stone
Microsoft Security Response 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

Theresa Burch
Microsoft Security Essentials

Doug Cavit
Microsoft Trustworthy Computing

Enrique Gonzalez
Microsoft Malware Protection Center

Cristin Goodwin
Microsoft Legal and Corporate Affairs

Roger Grimes
Microsoft Information Security

Karl Hanmore
Microsoft Security Response Center

Satomi Hayakawa
Microsoft Japan Security Response Team

Japan Security Response Team
Microsoft Japan

Hilda Larina Ragragio
Microsoft Malware Protection Center

Laura Lemire
Microsoft Legal and Corporate Affairs

Nishanth Lingamneni
Microsoft Security Essentials

Ziv Mador
Microsoft Client, Management and Protection

Charles McColgan
Microsoft ISD

Ritesh Mordani
Microsoft Forefront Online Protection for Exchange

Price Oden
Microsoft Information Security

Sasi Parthasarathy
Bing

Daryl Pecelj
Microsoft Information Security

Kathy Phillips
Microsoft Legal and Corporate Affairs

Tareq Saade
Microsoft Malware Protection Center

Jireh Sanico
Microsoft Malware Protection Center

Table of Contents

Microsoft Malware Protection Center

Malware Patterns Around the World

About This Report

Scope

The *Microsoft® Security Intelligence Report (SIR)* is published twice per year. These reports focus on data and trends observed in the first and second halves of each calendar year. Past reports and related resources are available for download at http://www.microsoft.com/sir. We continue to focus on malware data, software vulnerability disclosure data, vulnerability exploit data, and related trends in this eighth installment of the *Security Intelligence Report*. We hope that readers find the data, insights, and guidance provided in this report useful in helping them protect their networks and users.

Reporting Period

This volume of the *Security Intelligence Report* focuses on the second half of 2009 (2H09), though it also contains data and trends observed over the past several years. The nomenclature used throughout the report to refer to different reporting periods is *n*H*yy*, where *n*H refers to either the first (1) or second (2) half of the year, and *yy* denotes the year. For example, 2H08 represents the period covering the second half of 2008 (July 1 through December 31), and 1H09 represents the period covering the first half of 2009 (January 1 through June 30).

Conventions

This report uses the Microsoft Malware Protection Center (MMPC) naming standard for families and variants of malware and potentially unwanted software. For information about this standard, see "Appendix A: Threat Naming Conventions," beginning on page 236.

Data Sources

If you are interested in the products, services, tools, and Web sites used to provide the data for this report, please see "Appendix B: Data Sources," beginning on page 238.

Key Findings

Volume 8 of the *Microsoft Security Intelligence Report* provides in-depth perspectives on malicious and potentially unwanted software, software exploits, security breaches, and software vulnerabilities in both Microsoft and third-party software. Microsoft developed these perspectives based on detailed analysis over the past several years, with a focus on the second half of 2009 (2H09).

Key Findings from the Microsoft Malware Protection Center

Global Malicious and Potentially Unwanted Software Trends

Microsoft security products obtain user consent to gather data from more than 500 million computers worldwide and from some of the Internet's busiest online services. Analysis of this data provides a comprehensive and unique perspective on malware and potentially unwanted software activity around the world.

Geographic Trends

- Two of the largest increases in the number of computers cleaned were experienced by China and Brazil, which increased 19.1 percent and 15.8 percent from 1H09, respectively. Much of this increase was caused by the September 2009 release of Microsoft Security Essentials, an anti-malware solution for home computers that is available at no charge to licensed users of Windows®. China and Brazil have both been significant early adopters of Security Essentials.
- A number of locations experienced significant decreases in infection rates:
  - The largest decline in the number of computers cleaned is the 26.2 percent decrease in Turkey, which can be mainly attributed to the decreased prevalence of Win32/Taterf and Win32/Frethog, two password stealers that target players of online games.
  - The decreased prevalence of Taterf and Frethog is largely responsible for a 19.6 percent decrease for Taiwan.

  - Italy's 20.0 percent decline is mostly the result of a steep decline in detections of the rogue security software family Win32/Wintrim.
- The threat environments in the United States and the United Kingdom are very similar. Both locations have nearly the same proportion of threat categories, and 7 of the top 10 families in each location are the same. Miscellaneous Trojans account for the largest single threat category. Families such as Win32/FakeXPA, Win32/Renos, and Win32/Alureon rank high in both locations.
- In China, many of the most prevalent threats are localized families that don't appear in the list of top threats for any other location. These include some versions of Win32/BaiduSobar, a Chinese-language browser toolbar, and password stealers such as Win32/Lolyda and Win32/Ceekat that target several popular online games in China.
- In Brazil, Password Stealers & Monitoring Tools is the most common category, primarily because of a number of Portuguese-language password stealers that target online users of Brazilian banks. Win32/Bancos is the most common of these password stealers.
- Korea is dominated by worms, primarily Win32/Taterf, which targets players of online games. The prevalence of Taterf in Korea might be caused in part by the worm's propensity to spread easily in Internet cafés and LAN gaming centers, which are popular in Korea.

Operating System Trends

- As in previous periods, infection rates for more recently released operating systems and service packs are consistently lower than previous ones, for both client and server platforms.
- Windows 7, which was released in 2H09, and Windows Vista® with Service Pack 2 (SP2) have the lowest infection rates of any platform.
  - The 64-bit versions of Windows 7 and Windows Vista SP2 had lower infection rates than any other operating system configuration in 2H09, although the 32-bit versions both had infection rates that were less than half of Windows XP with its most up-to-date service pack, SP3.

- For operating systems with service packs, each successive service pack has a lower infection rate than the one before it.
  - The infection rate for Windows XP with SP3 is less than half of that for SP2, and less than a third of that for SP1.
  - Similarly, Windows Vista SP2 has a lower infection rate than SP1, which has a lower infection rate than Windows Vista RTM.
  - For server operating systems, the infection rate for Windows Server® 2008 with SP2 is 20 percent less than that of its predecessor, Windows Server 2008 RTM.

Worldwide Category Trends

- Overall, detections of the top threats are down by a considerable margin from the first half of 2009.
  - In 1H09, seven families were removed from at least 2 million computers each by Microsoft desktop anti-malware tools, compared to just four families in 2H09.
  - Even Win32/Taterf, 2H09's top family, was removed from nearly 1 million fewer computers this period than in 1H09.
  - The 3.9 million computers infected by Taterf in 2H09 is significantly less than 1H08's top family, Win32/Zlob, which was removed from 9.0 million computers during that period.
  - Many attackers use Trojan downloaders and Trojan droppers, such as Win32/Renos and ASX/Wimad (the second- and eleventh-most prevalent families in 2H09, respectively) to distribute other threats, such as botnets, rogues, and password stealers, to computers.
  - In general, the malware landscape in 2H09 is marked by a greater diversity of moderately prevalent families, with fewer single families dominating the top of the list with very large numbers of removals. The rapid adoption of Microsoft Security Essentials may also be partially responsible for the decline in removals, because real-time anti-malware tools can often intercept and remove downloaders and droppers before they are able to install other threats (which therefore would not be present on the computer for desktop security products to detect).

Trends in Sample Proliferation

Malware authors attempt to evade detection by continually releasing new variants in an effort to outpace the release of new signatures by antivirus vendors. One way to determine which families and categories of malware are currently most active is to count unique samples.

- More than 126 million malicious samples were detected in the wild in 2H09.
- The decrease in the Password Stealers & Monitoring Tools category was primarily caused by Win32/Lolyda, which declined from 5.7 million samples in 1H09 to less than 100,000 in 2H09.
- The increase in the Spyware category was primarily caused by Win32/ShopAtHome, which had nearly five times as many unique samples in 2H09 as in the prior period.
- The large number of virus samples is caused by the fact that viruses can infect many different files, each of which is a unique sample. Sample counts for viruses should therefore not be considered an indication of large numbers of true variants for these families.

Rogue Security Software

Rogue security software—software that displays false or misleading alerts about infections or vulnerabilities on the victim's computer and offers to fix the supposed problems for a price—has become one of the most common methods that attackers use to swindle money from victims.

- Microsoft security products cleaned rogue security software–related malware on 7.8 million computers in 2H09, up from 5.3 million computers in 1H09—an increase of 46.5 percent, which suggests that rogue security software provides its distributors with large payoffs relative to some other, less prevalent kinds of threats.
- A rogue security software family, Win32/FakeXPA, was the third-most prevalent threat detected by Microsoft desktop security products worldwide in 2H09. Three others—Win32/Yektel, Win32/FakeSpypro, and Win32/Winwebsec—ranked eleventh, fourteenth, and seventeenth, respectively.
- Three new consumer-oriented videos have been posted on http://www.microsoft.com/protect that are designed to educate consumers about the increasing threat to their security and privacy from rogue security software.

The Threat Landscape at Home Versus the Enterprise

- Domain-joined computers were much more likely to encounter worms than non-domain computers, primarily because of the way worms propagate. Worms typically spread most effectively via unsecured file shares and removable storage volumes, both of which are often plentiful in enterprise environments and less common in homes.
  - Worms accounted for 4 of the top 10 families detected on domain-joined computers.
  - Win32/Conficker, which uses several methods of propagation that work more effectively within a typical enterprise network environment than over the public Internet, leads the list by a wide margin.
  - Similarly, Win32/Autorun, which targets removable drives, was more common in domain environments where such volumes are often used to exchange files.
- In contrast, the Adware and Miscellaneous Trojans categories are much more common on non-domain computers.

E-Mail Threats

The data in this section is based on e-mail filtered by Microsoft Forefront® Online Protection for Exchange (FOPE), which provides spam, phishing, and malware filtering services for thousands of enterprise customers.

Spam messages associated with advance-fee fraud (so-called "419 scams") and gambling increased significantly in 2H09. Most other categories remained relatively stable in percentage terms.

- An advance-fee fraud is a common confidence trick in which the sender of a message purports to have a claim on a large sum of money but is unable to access it directly for some reason. Typically, the specified reason involves bureaucratic red tape or political corruption. The sender asks the prospective victim for a temporary loan that the sender will use to bribe officials or pay fees to get the full sum released. In exchange, the sender promises the target a share of the fortune, which amounts to a much larger sum than the original loan.
- These messages are often associated with Nigeria ("419" refers to the article of the Nigerian Criminal Code that deals with fraud) and other countries in western Africa, including Sierra Leone, the Ivory Coast, and Burkina Faso.

Botnets and spam networks of malware-infected computers that can be controlled remotely by an attacker are responsible for much or most of the spam that is sent today. To measure the impact that botnets have on the spam landscape, FOPE monitors spam messages sent from IP addresses that have been reported to be associated with known botnets. In 2H09, the top 5 botnets were responsible for sending more than 94 percent of all botnet spam.

Malicious Web Sites

As published in previous volumes of the *Security Intelligence Report*, social networking properties suffered the highest total volume of phishing impressions as well as the highest rate of phishing impressions per phishing site. Financial institutions received the lowest volume of phishing impressions per site though they received by far the highest total volume of distinct fraudulent sites.

- The Miscellaneous Potentially Unwanted Software and Miscellaneous Trojans categories dominated the list of threats served by malicious Web sites in both periods.
- The Trojan Downloaders & Droppers category, which was nearly as prevalent as Miscellaneous Trojans in 1H09, fell by nearly 50 percent in the second half of the year, but Exploits more than doubled.

Key Findings from the Microsoft Security Response Center

Industry-Wide Vulnerability Disclosures

- Vulnerability disclosures in 2H09 were down 8.4 percent from the first half of the year, which continues an overall trend of moderate declines since 2006.
- Low severity vulnerabilities accounted for just 3.5 percent of overall vulnerabilities in 2H09, down from 4.1 percent in the first half of the year.
- High severity vulnerabilities disclosed in 2H09 were down 9.0 percent from the first half of the year, and 30.7 percent from 2H08.
  - The continued predominance of High severity and Medium severity vulnerability disclosures is likely caused, at least in part, to the tendency of both attackers and legitimate security researchers to prioritize searching for the most severe vulnerabilities.
- Application vulnerabilities continued to account for most vulnerabilities in 2H09, although the total number of application vulnerabilities was down significantly from 2H08 and 1H09.
- Operating system and browser vulnerabilities were both roughly stable, and each accounted for a small fraction of the total.

Vulnerability Disclosures for Microsoft Products

- Vulnerability disclosures for Microsoft products increased to 127 in 2H09 from 113 in 1H09.
- Generally, trends for Microsoft vulnerability disclosures mirrored those for the entire industry, with peaks in 2H06–1H07 and again in 2H08.
- Over the past four years, Microsoft vulnerability disclosures have consistently accounted for 3 to 5 percent of all disclosures industry wide.
- Responsible disclosure means disclosing vulnerabilities privately to an affected vendor so it can develop a comprehensive security update to address the vulnerabilities before the details become public knowledge. In 2H09, 80.7 percent of Microsoft vulnerability disclosures adhered to responsible disclosure practices, up from 79.5 percent in 1H09 and higher than in any previous tracked period.

- The percentage of disclosures submitted by vulnerability brokers declined slightly to 8.6 percent of all disclosures in 2H09, compared to 10.5 percent in the first half of the year.
- The MSRC releases security bulletins each month that address vulnerabilities in Microsoft software. In 2H09, Microsoft released 47 security bulletins that addressed 104 individual vulnerabilities that were identified on the Common Vulnerabilities and Exposures (CVE) list.
- Although the overall number of bulletins shipped increased from 27 in 1H09, the number of vulnerabilities addressed per bulletin decreased from 3.1 to 2.2.

Microsoft Update adoption has increased significantly over the past several years. The number of computers using the more comprehensive service increased by more than 17 percent since 1H09.

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft anti-malware products and the monthly release of the MSRT.
- **Microsoft Update** (http://update.microsoft.com/microsoftupdate) provides all of the updates offered through Windows Update and provides updates for other Microsoft software. Users can opt in to the service when installing software serviced through Microsoft Update or at the Microsoft Update Web site.

  Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Key Findings from the Microsoft Security Engineering Center

Security Science: Exploit Trends

- An *exploit* is malicious code that takes advantage of software vulnerabilities to infect a computer, without the user's consent and often without the user's knowledge. Exploits are often distributed through Web pages, although attackers also use a number of other distribution methods, such as e-mail and instant messaging (IM) services. Malware distributors use various techniques to attempt to direct Internet users to Web sites that have been compromised or are intentionally hosting hostile code.
  - In the past, exploit kit makers tended to package four to six exploits together per kit to increase the chances of a successful attack. This average dropped to 3.2 exploits per package in the first half of 2009 as attackers took advantage of a number of reliable and prevalent vulnerabilities in third-party components, which rendered large numbers of exploits unnecessary.
  - This trend continued into 2H09; the average number of exploits per package fell to 2.3.
  - However, some attackers still preferred to use large numbers of exploits—the largest exploit kit observed in 2H09 included 23 exploits.
- CVE-2007-0071, a vulnerability in Adobe Flash Player that was the most commonly exploited browser vulnerability in 1H09, fell to twenty-third place in the second half of the year and accounted for just 0.4 percent of exploits.
  - Significant shifts such as these might be related to the tendency of exploit-kit creators to frequently replace older exploits with newer ones.
- Comparing exploits that target Microsoft software to third-party exploits (those that target vulnerabilities in software produced by other vendors) suggests that the vulnerability landscape of Windows Vista and Windows 7 is very different from that of Windows XP.
  - In Windows XP, Microsoft vulnerabilities account for 55.3 percent of all attacks in the studied sample.
  - In Windows Vista and Windows 7, the proportion of Microsoft vulnerabilities is significantly smaller, accounting for just 24.6 percent of attacks in the studied sample.
    - The number of vulnerabilities is greater than the 15.5 percent in 1H09 (includes Windows Vista only) because of increased attacks on CVE-2009-0075/MS09-002, a vulnerability in Internet Explorer® 7 that affects Windows Vista RTM and SP1 but not Windows Vista SP2 or Windows 7. This vulnerability was addressed by a Microsoft security update in January 2009.

Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or when they post malicious code to a poorly secured Web form, like a comment field on a blog.

- An analysis of the specific vulnerabilities targeted by drive-by download sites indicates that most exploits used by such malicious sites target older browsers and are ineffective against newer ones. Exploits that affect Internet Explorer 6 appeared on more than four times as many drive-by sites in 2H09 as did exploits that affect the newer Internet Explorer 7.
- As Bing™ indexes the Web, pages are assessed for malicious elements or malicious behavior.
  - Bing detects a large number of drive-by download pages each month, with several hundred thousand sites that host active drive-by pages being tracked at any given time.
  - Because the owners of compromised sites are usually victims themselves, the sites are not removed from the Bing index. Instead, clicking the link in the list of search results displays a prominent warning, saying that the page might contain malicious software.
    - In 2H09, about 0.3 percent of the search results pages served to users by Bing contained warnings about malicious sites.
  - Overall, the number of affected Web sites tracked by Bing increased in 2H09, with 0.24 percent of all Web sites that host at least one malicious page, up from 0.16 percent in 1H09. This increase is probably due in part to a number of new, improved detection mechanisms that Bing deployed in the second half of 2009.
- Although Bing has detected drive-by download sites all over the world, the risk is not spread equally among Internet users worldwide. Users in some parts of the world are more at risk than in others.
  - Drive-by download pages were discovered on more than 2.1 percent of the sites in the .th ccTLD (associated with Thailand) and almost 1 percent in the .cn ccTLD (China).

- By comparison, generic and sponsored top-level domains that do not serve particular countries/regions do not display the same level of variance that ccTLDs do.
  - The .biz TLD, which is intended for businesses, contains the highest percentage of sites that host drive-by download pages; 0.76 percent of all active .biz sites were found to contain such pages.
- Although drive-by download pages can be found in quantity in most generic, sponsored, and country-code TLDs, exploit servers are concentrated in a much smaller number of TLDs, led by .com (33.2 percent) and .cn (19.0 percent).
  - In 2H08, the most heavily used exploit server in the world had a reach of about 100,000 pages. This increased to more than 450,000 pages in 1H09, and to nearly 750,000 pages in 2H09.
    - Despite this increase, very few of the servers at the top of the list in 1H09 remain there in 2H09.
- Malware distribution networks tend to be moving targets, with servers that constantly appear and disappear in different locations.

Attackers increasingly use common file formats as transmission vectors for exploits (formats like .doc, .pdf, .ppt, and .xls, for example). *Parser vulnerabilities* are a class of vulnerability in which the attacker creates a specially crafted document that takes advantage of an error in how the code processes or parses the file format. Many of these formats are complex and designed for performance, and an attacker can create a file with a malformed section that exploits a vulnerability in the program.

- Most of the exploited vulnerabilities in Microsoft Office file format exploits that Microsoft analyzed in 2H09 were several years old, and all of them had security updates available to help protect against exploitation; a third of them were first identified in 2006.
- 75.8 percent of the attacks exploited a single vulnerability (CVE-2006-2492, the Malformed Object Pointer Vulnerability in Microsoft Office Word) for which a security fix had been available for more than three years by the end of 2009.

- Users who do not keep their Office program installations up to date with service packs and security updates are at increased risk of attack. Most attacks involved computers with severely out-of-date Office program installations.
  - More than half (56.2 percent) of the attacks affected Office program installations that had not been updated since 2003.
  - Most of these attacks involved Office 2003 users who had not applied a single service pack or other security update since the original release of Office 2003 in October 2003.
  - It is not at all uncommon for victims of Office program exploit attacks to have Windows installations that are much more current. Almost two-thirds (62.7 percent) of the Office attacks observed in 2H09 affected computers that run versions of Windows that had been updated within the previous 12 months.
  - The median amount of time since the last operating system update for computers in the sample was about 8.5 months, compared to 6.1 years for the most recent Office program update—almost nine times as long.
    - This data helps illustrate the fact that users can keep Windows rigorously up-to-date and still face increased risk from exploits unless they also update their other programs regularly, including third-party programs..

Security Breach Trends

Security Incidents That Led to Privacy Consequences

- There is a clear downward trend in the absolute number of incidents in every single category except for malware attacks, which remains unchanged.
- Stolen equipment & media and accidental Web loss account for the largest declines.
- Improper disposal of business records accounts for quite a few incidents. Organizations can address this type of data breach relatively easily with effective policies regarding the destruction of paper and electronic records that contain sensitive information.
- Although many people link security breaches with malicious parties who seek and gain unlawful access to sensitive data, incidents that involve attacks (hacking, malware, and fraud) have been significantly outnumbered in recent years by incidents that involve negligence (lost, stolen, or missing equipment; accidental disclosure; or improper disposal).
- Incidents that involve negligence have declined steeply over the past two years, from 110 in 1H08 to just 34 in 2H09.
  - Organizations might be taking more steps to secure sensitive equipment, such as security checks at facility gates or programs to educate employees about secure practices.
  - Adoption of strong encryption solutions such as Windows BitLocker® Drive Encryption might also affect the decline. Disclosure laws in many jurisdictions do not require notification when encrypted data is lost or stolen because it is much more difficult for the thief or finder to extract than unencrypted data.

Executive Foreword

Welcome to Volume 8 of the *Microsoft Security Intelligence Report*. Volume 8 of the *Security Intelligence Report* covers the second half of 2009 (July 1 through December 31) and is based on data that we receive from more than 500 million systems around the world each month and from some of the most widely used services on the Internet.

This report is the most extensive and comprehensive volume we've published to date and includes an expanded "Threat Assessments for Individual Locations" section. These assessments provide detailed information about the differing patterns in malicious and potentially unwanted software infection rates in 26 countries and regions around the world. The regional threat patterns of infection and the trends we see evolving provide actionable intelligence. This data can inform your risk management decisions and help identify potential adjustments to your security posture. Our global insight and analysis makes the *Security Intelligence Report* unique in our industry.

In my 15 years at Microsoft, I have been involved in many of the advances in secure software development that Microsoft has pioneered, including establishing the road map for Windows XP Service Pack 2 (SP2) and leading the Secure Windows Initiative team that played a major role in driving increased security into many products, including Windows Vista and Windows 7. These efforts, along with my team's recent work on evolving the Security Development Lifecycle (SDL) and production of several key security analysis tools, have contributed to making Microsoft software more secure and a harder target for attackers to successfully exploit. We can see the results in this volume of the *Security Intelligence Report*—the most common attacks are deployed against third-party software, and the most prevalent malicious software threats tend to spread by exploiting human error rather than by exploiting software vulnerabilities. More than ever before, the security of computer users' environments—in the enterprise and in the home—is dependent on the whole software industry, not just on Microsoft.

People rely on software providers to build secure software, and they trust them to respond appropriately in the case of an attack. Much of the world's most innovative applications rely on the Microsoft platform. The majority of attacks now target applications. This is why Microsoft continues to work hard to help our industry partners and competitors build more secure software. Over the past couple of years, my team has developed and released a range of tools, processes, and guidance intended to help software developers and architects design, build, test, and deploy software with fewer, less severe vulnerabilities.

Our approach to this challenge can be summarized in three key tactics intended to decrease the return on investment for an attacker when software is the target:

- **Increase attacker investment** required to find usable vulnerabilities (via the SDL).
  - Remove entire classes of vulnerabilities, where possible.
  - Focus on automation to scale human efforts.

- **Increase attacker investment** required to write reliable exploits (via techniques such as Address Space Layout Randomization [ASLR]).
  - Build mitigations that reduce vulnerability reliability.
  - Make writing completely reliable exploits impossible.
- **Decrease attacker opportunity** to recover their investment (via speedier update deployment).
  - Shrink window of vulnerability usage.
  - Execute rapid detection and suppression of exploit usage.

The data in this volume of the *Security Intelligence Report* indicates that this strategy is having a positive effect—the Microsoft share of the software vulnerabilities disclosed each six-month period since the introduction of the SDL remains very low (95 percent of vulnerabilities disclosed in the second half of 2009 were in third-party software); malicious software infection rates for more recent versions of the Windows operating system (and more recent Service Packs, where available) were significantly lower than previous versions; and in attacks against vulnerabilities in browser-based software, attackers favored exploits against third-party software vulnerabilities on more recent versions of Windows.

As I mentioned earlier, Microsoft is sharing the results of our security investment with our industry partners and even competitors in order that our customers can benefit from a more secure ecosystem. In addition to releasing the Security Development Lifecycle for developers to use on any platform (the SDL guidance has been downloaded more than 80,000 times to date, and SDL tools have been downloaded more than 50,000 times), my team has also made available a range of analysis tools and programs which we use within Microsoft to detect and remedy potential software vulnerabilities. I encourage developers to visit the SDL Web page, at www.microsoft.com/sdl, to take advantage of the free framework, tools, and guidance and to subscribe to our Trustworthy Computing blogs, at http://www.microsoft.com/mscorp/twc/blogs/default.mspx, to keep up to date on the latest vulnerability and exploit developments and announcements from my team.

Just want to reduce your risk profile and protect your PC? Then keep all of the software up to date (including third-party software); use the Microsoft Update service in preference to Windows Update; move to the latest version of software, if possible; and run an up-to-date antivirus product from a trusted vendor.

Patterns of threat and infection change constantly. Making security decisions can be a lengthy, complex process, requiring risk-management assessments based on real data and analysis. As a result, we continue to evolve the Security Intelligence Report to provide the information you need to help you make informed decisions about your security posture.

Do you have thoughts or suggestions on this report or what you would like to see in the next volume of the *Security Intelligence Report*? Please let us know what you think by e-mailing sirfb@microsoft.com.

Matt Thomlinson
General Manager, Microsoft Product Security
Microsoft Trustworthy Computing Group

Trustworthy Computing: Security Engineering at Microsoft

The computer threat landscape is constantly changing. As threats continue to evolve from mischievous hackers pursuing notoriety to organized criminals stealing data for monetary gain, public concern is escalating. Trustworthy Computing (TwC), formed in 2002, is Microsoft's commitment to providing more secure, private, and reliable computing experiences for our customers.

TwC Security includes three technology centers that work together to address security issues by working closely together to supply the services, information, and response needed to better understand the evolving threat landscape, help protect customers from online threats, and share knowledge with the broader security ecosystem.

Microsoft Security Engineering Center

The Microsoft Security Engineering Center (MSEC) helps protect Microsoft customers by providing security guidance to our product teams, helping them implement the industry-leading Security Development Lifecycle, and deploying applied security science and technology that help improve product security.

Microsoft Security Response Center

The Microsoft Security Response Center (MSRC) is a leading security risk analysis and management center that helps identify, monitor, resolve, and respond to security incidents and Microsoft software security vulnerabilities 24 hours a day, seven days a week. On constant alert for security issues, the MSRC monitors security newsgroups, responds to e-mail messages sent to secure@microsoft.com, and manages a company-wide security update release process.

Microsoft Malware Protection Center

The Microsoft Malware Protection Center (MMPC) is a global team of experienced malware research and response specialists dedicated to protecting customers from new threats, including viruses, worms, spyware, adware, and other malicious and potentially unwanted software. The MMPC provides malware research and response expertise that supports the range of Microsoft security products and services, including the Forefront suite of products, Windows Live™ OneCare™, Windows Defender, Microsoft Security Essentials, and the Malicious Software Removal Tool. The response arm of the MMPC includes a global network of research and response labs located around the world.

The data and analysis in this report are presented from the perspective of these three centers and their partners in the various Microsoft product groups.

Microsoft Security Engineering Center

The Microsoft Security Engineering Center (MSEC) helps to protect Microsoft customers by delivering more secure products and services. The three MSEC subteams work closely together and with other groups at Microsoft to promote secure software development by focusing on the three traditional pillars of IT management—people, process, and technology.

The *Security Development Lifecycle (SDL)* team manages updating, releasing, and evangelizing the Microsoft Security Development Lifecycle—the industry-leading software security process. The SDL has played a critical role in embedding security and privacy into Microsoft software and culture, leading to measurable security and privacy improvements in flagship products such as Windows 7, Microsoft Office, and Microsoft SQL Server®.

The *Security Assurance* team helps teams ship products that are fundamentally secure by ensuring the requirements of the SDL are met or exceeded. Security Assurance is instrumental in driving security innovations, processes, and technologies into products throughout Microsoft. Security Assurance influences the design and strategy of the SDL to ensure it stays relevant and can be implemented in a practical way.

The *Security Science* team protects customers by improving the security and privacy resiliency of Microsoft products through applied security research. Specifically, the Security Science team develops more effective and scalable ways to find vulnerabilities, researches and applies innovative exploit mitigation techniques to Microsoft products, and focuses on tracking and providing early warning of new exploits.

Exploit Trends

An *exploit* is malicious code that takes advantage of software vulnerabilities to infect a computer, without the user's consent and often without the user's knowledge. Exploits are often distributed through Web pages, although attackers also use a number of other distribution methods, such as e-mail and instant messaging (IM) services. Malware distributors use various techniques to attempt to direct Internet users to Web sites that have been compromised or are intentionally hosting hostile code. The malware server hosts one or more exploits that are designed to use specific vulnerabilities to install themselves secretly on the user's computer, a tactic that is sometimes called a *drive-by download*. (See "Analysis of Drive-By Download Pages," beginning on page 31, for a more in-depth look at this tactic.) The vulnerabilities targeted by these exploits are typically found in Web browsers themselves or in browser add-ons, such as ActiveX® controls that enable users to experience popular types of media content within the browser environment. In some cases, these add-ons are preinstalled by the computer manufacturer before the computer is sold. The user may not even use the vulnerable add-on or be aware that it is installed. Much of this software has no facility for updating itself, so even when 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 remains vulnerable to attack. (See "Update Clients and Services," on page 66, for information about the use of Windows Update and Microsoft Update to distribute kill bits for vulnerable ActiveX controls.)

Most malicious Web sites use *exploit kits* that package together several exploits. Each kit is designed to offer malware distributors optimal levels of applicability, stealth, reliability, and detection evasion. Exploit kit creators continually update their kits, removing poorly performing exploits and replacing them with new ones. The exploits included in a kit typically target vulnerabilities affecting several different platforms, browsers, and add-ons from different software vendors in an effort to ensnare as many potential victims as possible.

In the past, exploit-kit makers tended to package four to six exploits together per kit to increase the chances of a successful attack. This average dropped to 3.2 exploits per package in the first half of 2009 as attackers took advantage of a number of reliable and prevalent vulnerabilities in third-party components, rendering large numbers of exploits unnecessary. This trend continued into 2H09, with the average number of exploits per package dropping to 2.3. Nevertheless, some attackers still preferred to use large numbers of exploits—the largest exploit kit observed in 2H09 included 23 exploits.

The most highly sought-after exploits are *zero-day exploits*, which take advantage of undisclosed or newly disclosed vulnerabilities before the vendor releases a security update for it. Exploits that initially appear in the wild as zero-day exploits often remain active long after the update for the vulnerability is made available because many users install updates only sporadically, or not at all, and remain vulnerable. Even today, exploits for vulnerabilities fixed in 2003 are still being seen in the wild. This underscores the importance of staying up to date on all installed browser add-ons, in addition to installing updates for the browser,

operating system, and other installed programs. To make this process easier, some security companies offer update management products that aggregate and distribute security updates published by different software vendors.

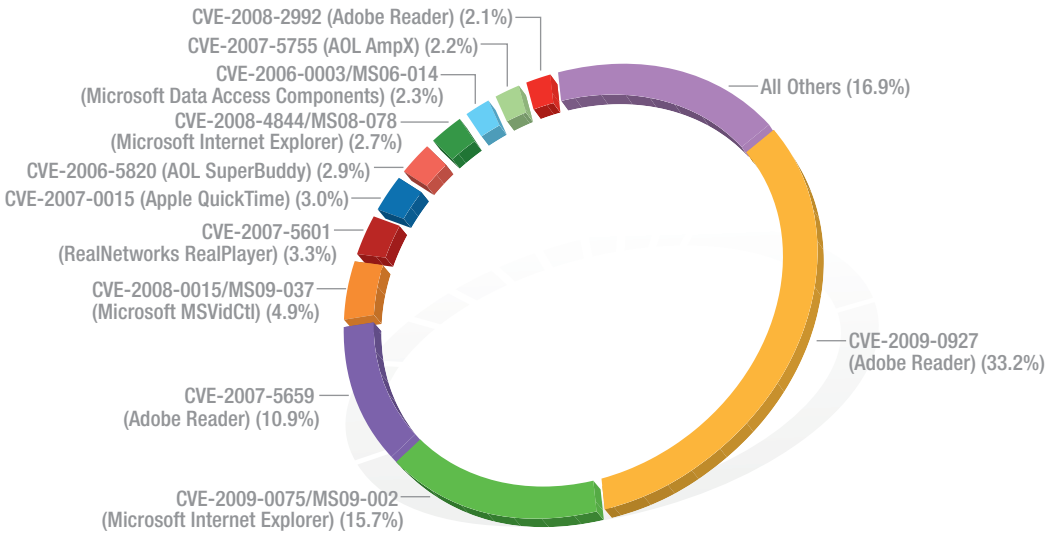
Top Browser-Based Exploits

Information about how attackers are exploiting browsers and add-ons can provide security researchers with a greater understanding of the risk posed by drive-by downloads and other browser-based attacks. To assess the relative prevalence of browser-based exploits in 2H09, Microsoft analyzed a sample of data obtained from customer-reported incidents, submissions of malicious code, and Windows error reports. The data encompasses multiple versions of Windows and Internet Explorer, from Windows XP to Windows 7,[1] and browser add-ons from many different vendors. It also includes data from third-party browsers (such as Maxthon and UUSee Player) that host the Internet Explorer rendering engine, called Trident.

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 pertaining to the affected vulnerability, if applicable. In addition, exploits affecting vulnerabilities in Microsoft software are labeled with the Microsoft Security Bulletin number pertaining to the vulnerability, if applicable.[2]

Figure 1 shows the browser-based exploits encountered by users in 2H09, ordered by percentage.

FIGURE 1. Browser-based exploits encountered, by percentage, in 2H09



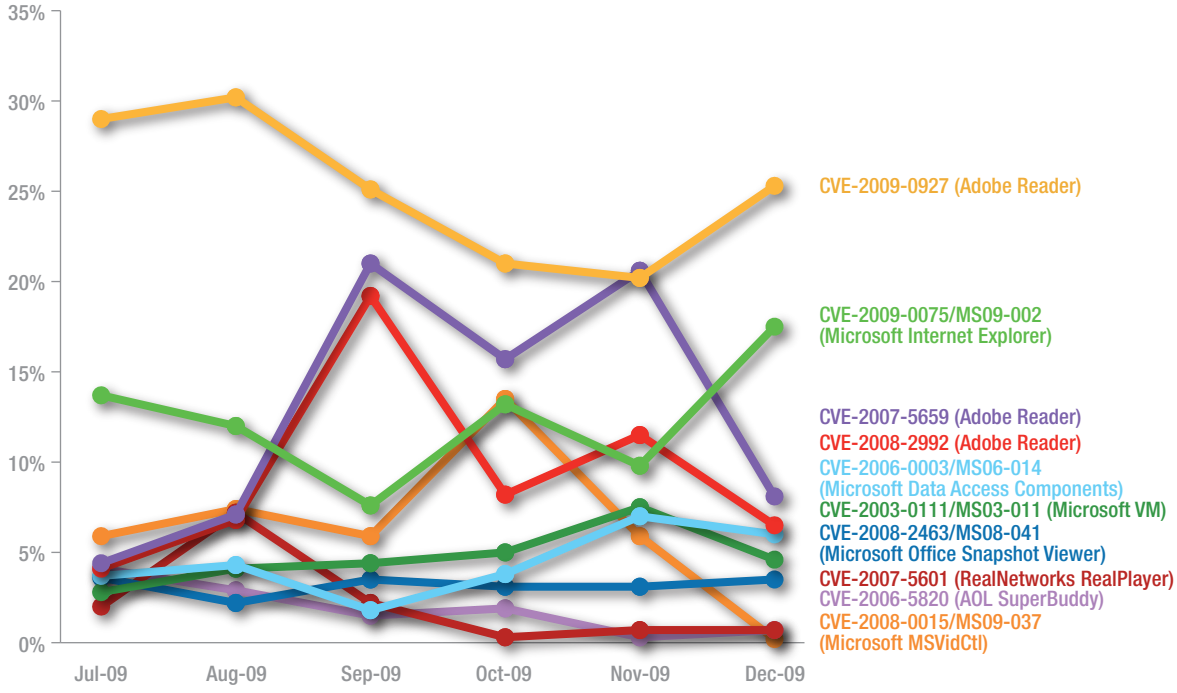
[1] Includes Windows XP release to manufacturing (RTM) version and Windows XP with Service Pack 1 (SP1), SP2, and SP3; Windows Vista RTM, SP1, and SP2; Windows 7 RTM; and versions of Internet Explorer 6, Internet Explorer 7, and Internet Explorer 8.

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

The two most commonly encountered exploits in the data sample targeted vulnerabilities disclosed in 2009. CVE-2009-0927, a vulnerability in Adobe Reader, was first with 33.2 percent of exploits, followed by CVE-2009-0075, a vulnerability in Internet Explorer, with 15.7 percent. Adobe and Microsoft addressed these vulnerabilities with Security Advisory APSB09-04 in March and Security Bulletin MS09-002 in February, respectively. An additional Adobe Reader vulnerability, CVE-2007-5659, occupied the third spot, followed by CVE-2008-0015, a vulnerability in the Microsoft Video ActiveX control. Both exploits are newcomers to the top exploits list, and both have been addressed by security updates.

CVE-2007-0071, a vulnerability in Adobe Flash Player that was the most commonly exploited browser vulnerability in 1H09, fell to twenty-third place in the second half of the year, accounting for just 0.4 percent of exploits. Significant shifts such as these may be related to the tendency of exploit-kit creators to frequently replace older exploits with newer ones, as explained earlier. As Figure 2 shows, the incidence of several of the most prevalent exploits varied significantly from month to month in 2H09.

FIGURE 2. Top 10 browser-based exploits, by percentage of all exploits each month, in 2H09



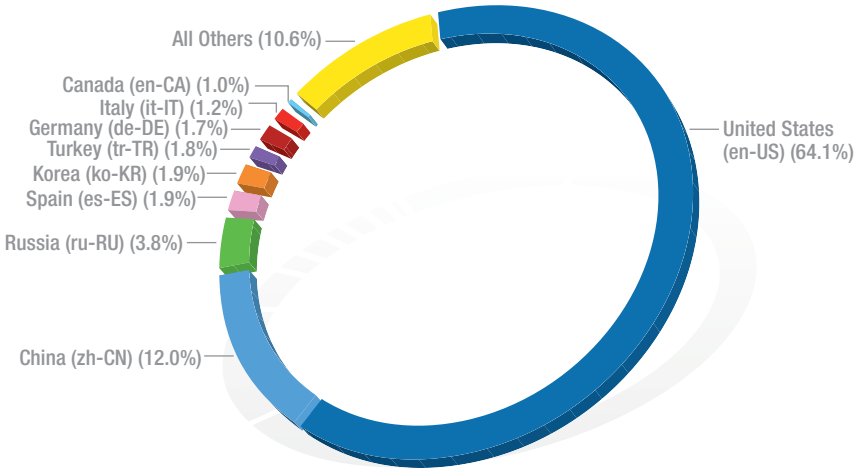
Browser-Based Exploits by System Locale

Malware distributors target different parts of the world unequally. The mechanisms attackers use often depend on language and cultural factors, which by nature tend to target specific segments of the global population. In addition, the spread of malware through exploits is often dependent on the availability of exploitable vulnerabilities in software

used by people in different countries and regions. Analyzing the system locale information included with Windows error reports can help illustrate the relative frequency with which different locations around the world are being targeted.

Figure 3 shows the browser-based exploits encountered by users in 2H09, ordered by the system locale of the victim.

FIGURE 3. Browser-based exploits encountered, by system locale of victim, in 2H09



The most common system locale for victims in 2H09 was en-US (English language, United States), accounting for 64.1 percent of all exploits in the sample, up from 27.5 percent in 1H09. This rise is due in large part to aggressive growth in the exploitation of several Adobe Reader vulnerabilities and the MS09-002 vulnerability in Internet Explorer (see Figure 1 on page 26), the impact of which was disproportionately felt in the United States. The most common locale during the first half of the year, zh-CN (Chinese language, China), fell from 53.6 percent of exploits to just 12.0 percent in 2H09. Common exploits in China often involve vulnerabilities in Chinese-language ActiveX controls, none of which were exploited as aggressively this period as the aforementioned Adobe Reader and Internet Explorer vulnerabilities.

Browser-Based Exploits by Operating System and Software Vendor

Every browser-based exploit can be traced to a vulnerability in a specific piece of software. Comparing exploits that target Microsoft software to third-party exploits (those that target vulnerabilities in software produced by other vendors) suggests that the vulnerability landscape of Windows Vista and Windows 7 is very different from that of Windows XP.

Figure 4 and Figure 5 show the relative percentages of exploits against vulnerabilities in Microsoft and third-party software in 2H09 on computers running Windows XP (Figure 4) and Windows Vista and Windows 7 combined (Figure 5).

FIGURE 4. Browser-based exploits targeting Microsoft and third-party software on computers running Windows XP in 2H09

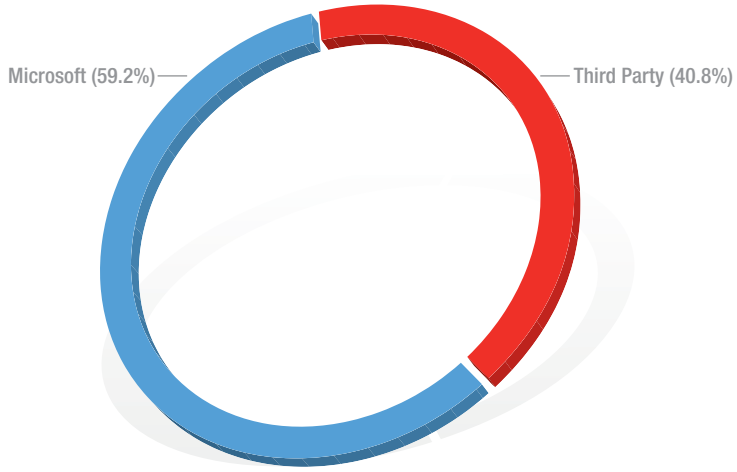
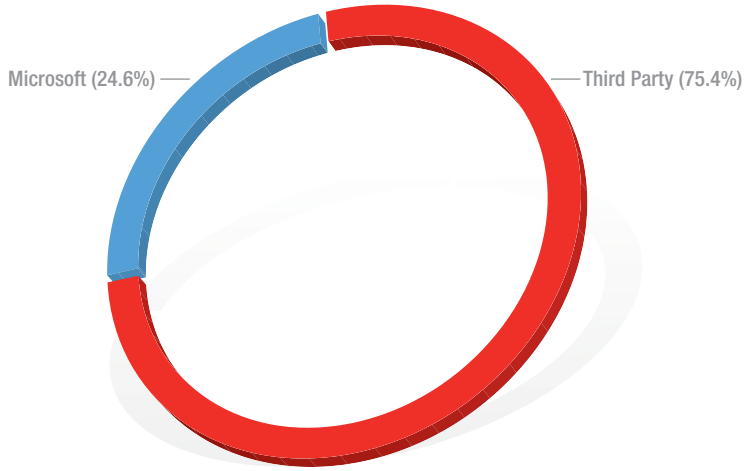


FIGURE 5. Browser-based exploits targeting Microsoft and third-party software on computers running Windows Vista and Windows 7 in 2H09



In Windows XP, Microsoft vulnerabilities account for 59.2 percent of all attacks in the sample. In Windows Vista and Windows 7, the proportion of Microsoft vulnerabilities is significantly smaller, accounting for just 24.6 percent of attacks in the sample. Although lower than the total for Windows XP, this total is up from 15.5 percent in 1H09,[3] due to increased attacks on CVE-2009-0075/MS09-002, a vulnerability in Internet Explorer 7 that affects Windows Vista RTM and SP1 (but not Windows Vista SP2 or Windows 7).

[3] Total for 1H09 is for Windows Vista only.

Figure 6 and Figure 7 show the 10 vulnerabilities exploited most often in Windows XP (Figure 6) and in Windows Vista and Windows 7 (Figure 7).

FIGURE 6. The 10 browser-based vulnerabilities exploited most often on computers running Windows XP, by percentage of all exploits, in 2H09

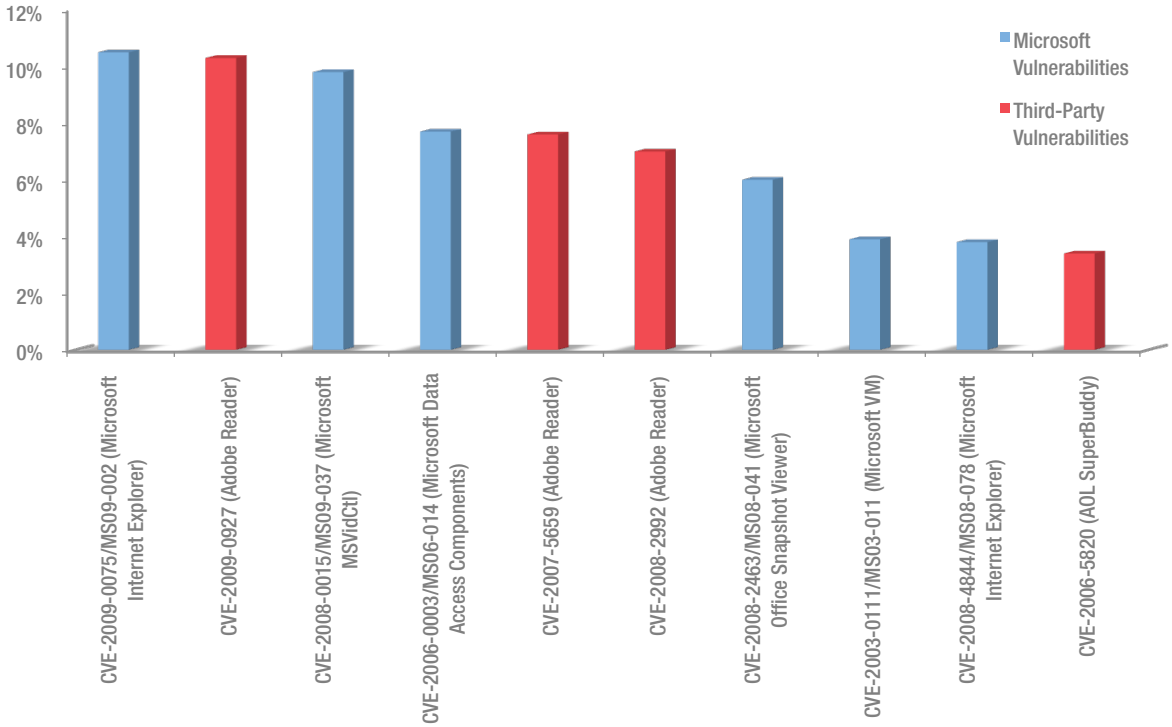
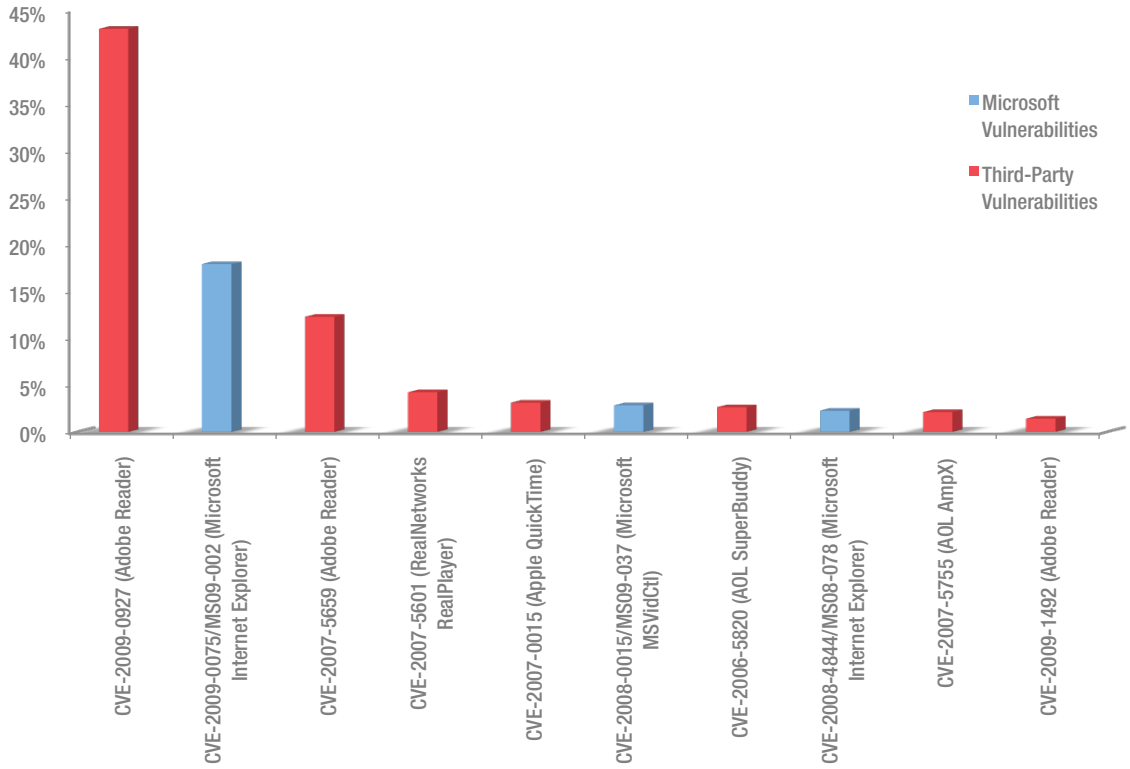


FIGURE 7. The 10 browser-based vulnerabilities exploited most often on computers running Windows Vista and Windows 7, by percentage of all exploits, in 2H09

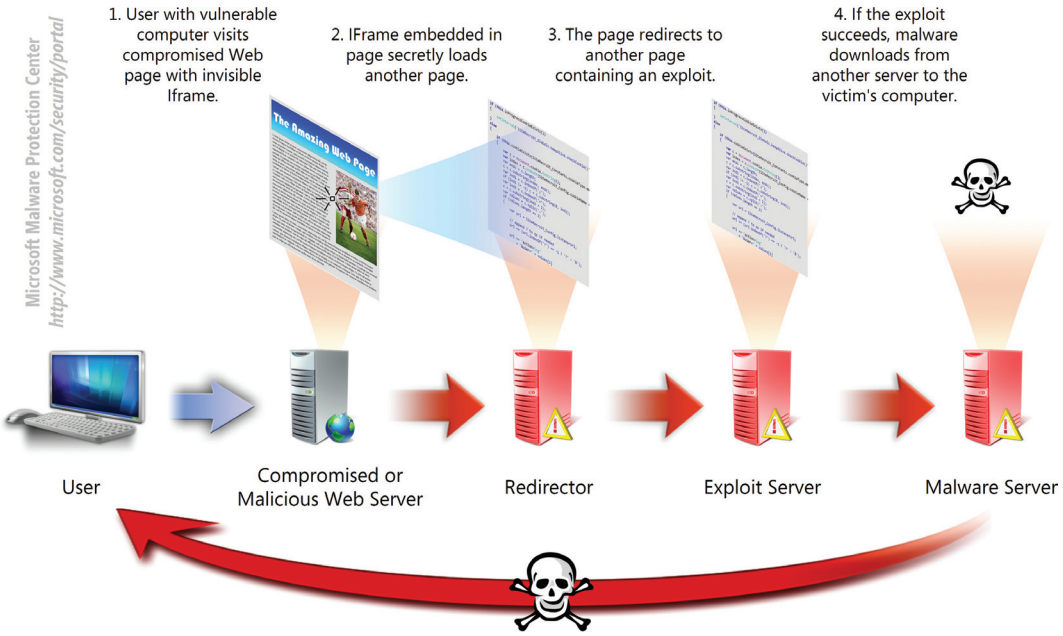


In Windows XP, Microsoft software accounts for 6 of the top 10 vulnerabilities, compared to 3 in Windows Vista and Windows 7.

Analysis of Drive-By Download Pages

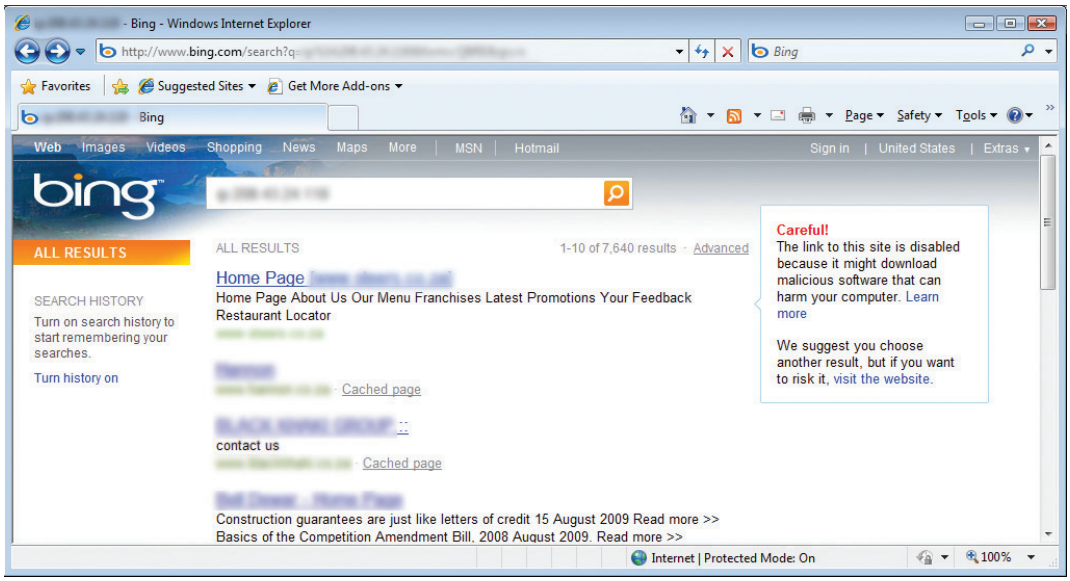
Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured Web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results. Search engines such as Bing have taken a number of measures to protect users from drive-by downloads.

FIGURE 8. One example of a drive-by download attack



As Bing indexes the Web, pages are assessed for malicious elements or malicious behavior. Because the owners of compromised sites are usually victims themselves, the sites are not removed from the Bing index. Instead, clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software, as shown in Figure 9. In 2H09, about 0.3 percent of the search results pages served to users by Bing contained warnings about malicious sites, compared to 0.2 percent in the previous period.

FIGURE 9. A drive-by download warning from Bing



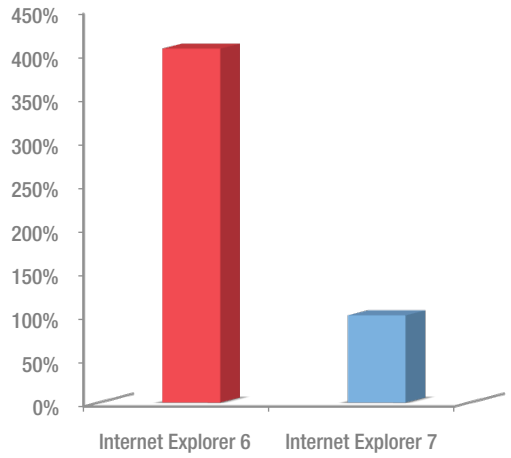
In most cases, the effect of a large drop in traffic originating from search engines (only about 2 percent of Bing users proceed to visit compromised sites after being shown the warning) serves to alert webmasters that something has gone wrong. Bing works with webmasters to inform them about compromised sites through the Bing Webmaster Center (http://webmaster.bing.com) and provides guidance for the removal of malicious code so that pages can be reenabled in the index. Bing reenables many such sites per day following requests from webmasters, indicating that such malware detection efforts can have a positive effect on the safety of Web sites and their customers.

Bing detects a large number of drive-by download pages each month, with several hundred thousand sites hosting active drive-by pages being tracked at any given time. Overall, the number of affected Web sites tracked by Bing has increased in 2H09, with 0.24 percent of all Web sites hosting at least one malicious page, up from 0.16 percent in 1H09. This increase is probably due in part to a number of new, improved detection mechanisms that Bing deployed in the latter half of 2009.

Drive-By Downloads and Targeted Browsers

An analysis of the specific vulnerabilities targeted by drive-by download sites indicates that the majority of the exploits used by such malicious sites target older browsers and are ineffective against newer ones. To assess the prevalence of drive-by download attacks against older browsers, Microsoft researchers examined sites that target Internet Explorer 6 and Internet Explorer 7. As Figure 10 illustrates, exploits affecting Internet Explorer 6 appeared on more than four times as many drive-by sites in 2H09 as did exploits affecting the newer Internet Explorer 7.

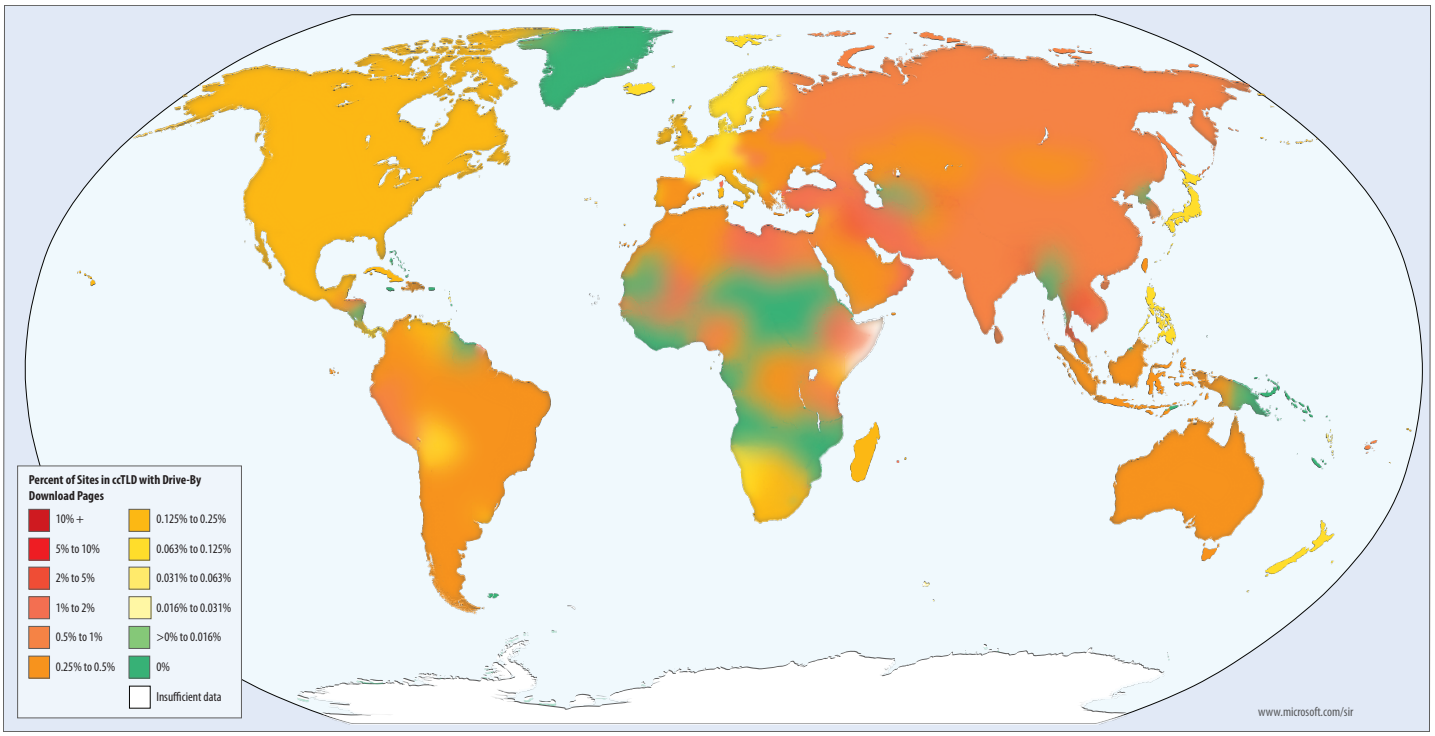
FIGURE 10. Drive-by download sites that targeted Internet Explorer 6 and Internet Explorer 7, indexed to the total for Internet Explorer 7, in 2H09



Geographic Distribution of Drive-By Download Sites

Although Bing has detected drive-by download sites all over the world, the risk is not spread equally among Internet users worldwide. Users in some parts of the world are more at risk than in others. Figure 11 shows the portion of Web sites in each country-code top-level domain (ccTLD) that were found to be hosting drive-by download pages in 2H09.

FIGURE 11. Percentage of Web sites in each country-code top-level domain (ccTLD) that hosted drive-by download pages in 2H09



Among ccTLDs that included at least one site hosting drive-by download pages, percentages varied greatly. Drive-by download pages were discovered on more than 2.1 percent of the sites in the .th ccTLD (associated with Thailand) and nearly 1 percent in the .cn ccTLD (China), but less than 0.1 percent of the sites in some other large ccTLDs, like .fr (associated with France) or .de (associated with Germany), were similarly affected. Note that Figure 11 does not reflect the physical locations of hosted sites; not all ccTLD sites are hosted in the locations to which the ccTLDs themselves are assigned. However, most ccTLD sites are targeted at Internet users in a particular country/region and are typically written in an appropriate language, so Figure 11 can be taken as a reasonable indicator of how users in different parts of the world are more or less at risk of encountering drive-by download pages.

By comparison, generic and sponsored top-level domains, which do not serve particular countries/regions, do not display the same level of variance that ccTLDs do, as illustrated by Figure 12.

FIGURE 12. Percentage of Web sites in the seven most populous generic top-level domains that hosted drive-by download pages in 2H09

TLD	2H09	1H09	% Change
.biz	0.76%	0.30%	60.5% ▲
.info	0.26%	0.39%	-50.0% ▼
.net	0.24%	0.25%	-4.2% ▼
.com	0.23%	0.11%	52.2% ▲
.org	0.21%	0.25%	-19.1% ▼
.edu	0.09%	0.22%	-144.4% ▼
.gov	0.01%	0.03%	-200.0% ▼

The .biz TLD, which is intended for businesses, contains the highest percentage of sites hosting drive-by download pages, with 0.76 percent of all active .biz sites found to contain such pages. Apart from .biz, most of the more heavily used generic and sponsored TLDs are clustered around 0.2 percent. A number of smaller TLDs, including .int and .coop, exhibited significant swings between 1H09 and 2H09, due to the small numbers of sites in these TLDs.

Some network operators (Internet service providers [ISPs], data centers, backbone providers, and similar operators) are particularly prone to providing hosting services to sites containing drive-by download pages, possibly due to poor security practices. Bing works with selected national Computer Emergency Response Teams (CERTs) with which it has partnered to help network operators clean and secure their infrastructures. As Figure 13 shows, 9.3 percent of the sites hosted by one network operator were found to contain drive-by pages, with several others showing site infection rates between 2.4 and 5.3 percent.

FIGURE 13. The 10 network operators providing hosting services to the largest percentage of compromised hosts in 2H09

Rank	ASN	Autonomous System Name	Location	% of Operator's Sites Containing Drive-By Pages
1	AS16557	COLOSOLUTIONS (Colo Solutions Global Services Inc)	United States	9.3%
2	AS48619	SO-AS (Service Online LLC)	Ukraine	5.3%
3	AS17799	CHINATELECOM-LN-AS-AP (asn for Liaoning Provincial Net of CT)	China	4.5%
4	AS23974	MOE-edNET-AS-AP (Ministry of education)	Thailand	4.2%
5	AS10865	ABACOM (Les Services Internet ABACOM inc)	Canada	3.4%
6	AS10135	EASPNET-AS-AP (EASPNET Inc.)	Taiwan	2.6%
7	AS49879	HOSTHANE (ISIK Bilgisayar Internet ve Yayincilik Hizmetleri)	Turkey	2.6%
8	AS45223	WIN-AS-TH-AP (World Internetwork Co.,Ltd , Thailand.)	Thailand	2.6%
9	AS23884	PROENNET-AS (Proimage Engineering and Communication Co.,Ltd.)	Thailand	2.5%
10	AS15755	ISPRONET (ISPRO Autonomous System Izmir,TURKEY)	Turkey	2.4%

Three of the top 10 most infected network operators are based in Thailand, which correlates to the high percentage of malicious Web sites found in the .th ccTLD. Three others are based in Turkey and China; 1.3 percent of sites in the .tr ccTLD and 1.0 percent of sites in .cn were found to be hosting drive-by sites. In all, then, more than half of the top 10 most infected operators are based in countries or regions associated with ccTLDs that had very high incidences of drive-by download sites in 2H09.

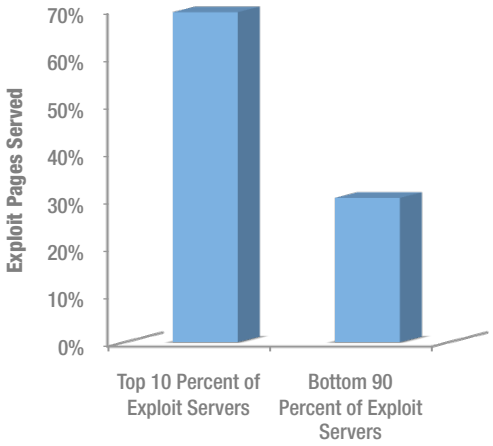
Overall, though, the infection rates of the top 10 most-infected network operators have improved. The site infection rates for the 10 most-infected operators in 2H09 ranged between 2.4 percent and 9.3 percent, down from 4.4 percent and 17.8 percent for the 10 most-infected network operators in 1H09. The top 10 sites accounted for 1.8 percent of all sites identified as hosting drive-by downloads in 2H09, down from 3.8 percent in 1H09. Colo Solutions, Inc., which ranked first on the list, decreased significantly from 17.8 percent to 9.3 percent. Nine of the operators from the 1H09 list have dropped off the list for 2H09. Of particular note is ZeelandNet BV, which ranked seventh on the 1H09 list with drive-by sites detected on 5.5 percent of the sites it hosted, but which appears to have completely eliminated drive-by sites since then—none of the drive-by sites tracked by Bing at the end of 2H09 were hosted by ZeelandNet. It appears that changes in infection rate per network operator are common. As network operators adjust their security policies and enforcement, attackers find it more difficult to infect Web sites hosted by these networks and move elsewhere.

Distribution of Exploit Servers

Most drive-by download attacks use malware distribution networks, similar to the one depicted in Figure 8 on page 32. Rather than being completely self-contained, the exploit code itself is hosted on a different Web server and is exposed through the compromised Web page using a technique like a URL embedded in malicious script code or an *inline frame*. (An inline frame, or *IFrame*, is used to load a separate HTML page into a window on the current page. Inline frames can be as small as a single pixel to avoid detection.) Bing security analysts locate these malicious servers and examine them with the help of other Microsoft groups, such as the CSS Security China Team.

Analyzing the URLs that host the malicious code or inline frames themselves reveals that a small number of exploit servers host the exploits used by the vast majority of drive-by download pages worldwide. Figure 14 shows the percentage of drive-by pages served by the top 10 percent and bottom 90 percent of exploit servers.

FIGURE 14. Drive-by pages served by the top 10 percent and bottom 90 percent of exploit servers, respectively, in 2H09

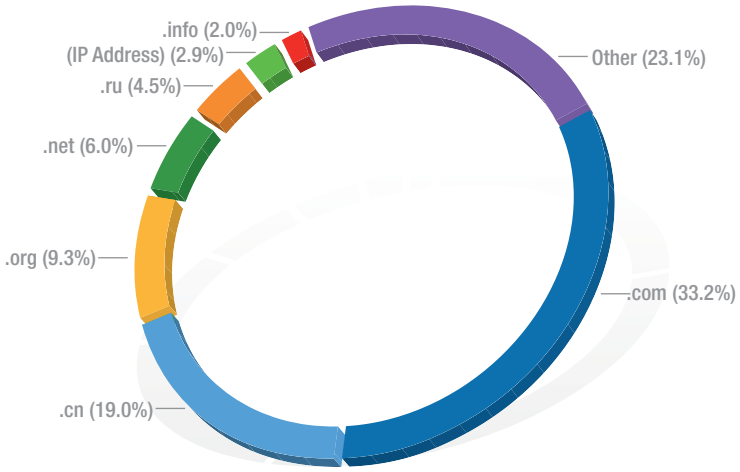


In the second half of 2009, the top 10 percent of exploit servers accounted for 69.6 percent of drive-by download pages. This is mostly unchanged from 1H09, when the top 10 percent of servers accounted for 72.8 percent of drive-by download pages.

One significant trend observed over the past several periods is that the number of drive-by pages served by the exploit servers at the very top of the curve continues to increase exponentially. In 2H08, the most heavily used exploit server in the world had a reach of around 100,000 pages. This increased to more than 450,000 pages in 1H09 and to nearly 750,000 pages in 2H09. Despite this, very few of the servers at the top of the list in 1H09 remain there in 2H09. Malware distribution networks tend to be moving targets, with servers constantly appearing and disappearing in different locations. As malware distribution servers get blocked by services such as Bing, they lose their effectiveness, and attackers move them elsewhere.

The TLD distribution of exploit servers is very different from that of the compromised pages that point to them, as illustrated by Figure 15.

FIGURE 15. Exploit servers used in drive-by download attacks, by TLD, in 2H09



Whereas drive-by download pages can be found in quantity in the majority of generic, sponsored, and country-code TLDs, exploit servers are concentrated in a much smaller number of TLDs, led by .com (33.2 percent) and .cn (19.0 percent). About 2.9 percent of exploit servers did not use the Domain Name System (DNS) and were contacted using only IP addresses. Most of the TLDs hosting significant numbers of exploit servers are among the most heavily used TLDs in the world.

Document File Format Exploits

Increasingly, attackers are using common file formats as transmission vectors for exploits. Most modern e-mail and instant messaging programs are configured to block the transmission of potentially dangerous files by extension, such as .exe, .com, and .scr, which have historically been misused to transmit malware. However, these same programs typically permit the transmission of many popular file formats, like .doc, .pdf, .ppt, and .xls. These formats are used legitimately by many people every day to share information and get work done, so blocking them is often not practical. This has made them an attractive target for exploitation.

This class of vulnerability can be described as *parser vulnerabilities*, wherein the attacker creates a specially crafted document that takes advantage of an error in how the code processes or parses the file format. Many of these formats are complex and designed for performance, and an attacker can create a file with a malformed section that exploits a vulnerability in the program.

There are two common attack scenarios. In one, the user receives an e-mail message with a document attachment. The e-mail message may look legitimate and may appear to come from someone the user knows. In the other common scenario, a user browsing the Web encounters a malicious or compromised Web site. The malicious code forces the browser to navigate to a malicious document, which is opened by the associated program. In both scenarios, when the document is opened, the exploit is activated and it downloads malware or extracts malware buried inside the document. Real-time antivirus scanning can help mitigate the danger from these attacks in some cases.

To assess the use of Microsoft Office system file formats as an attack vector, Microsoft analyzed a sample of several hundred files that were used for successful attacks in 2H09. The data set was taken from submissions of malicious code sent to Microsoft from customers worldwide.

In total, exploits for nine different vulnerabilities were identified in the sample set, as shown in Figure 16.

FIGURE 16. Vulnerabilities exploited in Microsoft Office file formats in 2H09

Bulletin	Date	Vulnerability	CVE
MS06-027	June 2006	Word Malformed Object Pointer Vulnerability	CVE-2006-2492
MS06-028	June 2006	PowerPoint Remote Code Execution Using a Malformed Record Vulnerability	CVE-2006-0022
MS06-060	October 2006	Word Mail Merge Vulnerability	CVE-2006-3651
MS07-015	February 2007	Excel Malformed Record Vulnerability	CVE-2007-0671
MS07-025	May 2007	Drawing Object Vulnerability	CVE-2007-1747
MS08-014	March 2008	Macro Validation Vulnerability	CVE-2008-0081
MS09-009	April 2009	Excel Memory Corruption Vulnerability	CVE-2009-0238
MS09-017	May 2009	PowerPoint Memory Corruption Vulnerability	CVE-2009-0556
MS09-021	June 2009	Excel Object Record Corruption Vulnerability	CVE-2009-0557

All nine of these vulnerabilities had security updates available at the time of attack. The affected users were exposed because they had not applied the updates. Office 2000, Office XP, Office 2003, and the 2007 Microsoft Office system were each affected by at least one of the nine vulnerabilities (see Figure 20 on page 42 for details).

Most of the vulnerabilities exploited in the data sample were several years old, with a third of them first identified in 2006. As Figure 17 illustrates, 75.8 percent of attacks exploited a single vulnerability (CVE-2006-2492, the Malformed Object Pointer Vulnerability in Microsoft Office Word) for which a security fix had been available for more than three years by the end of 2009.

FIGURE 17. Microsoft Office file format exploits encountered, by percentage, in 2H09

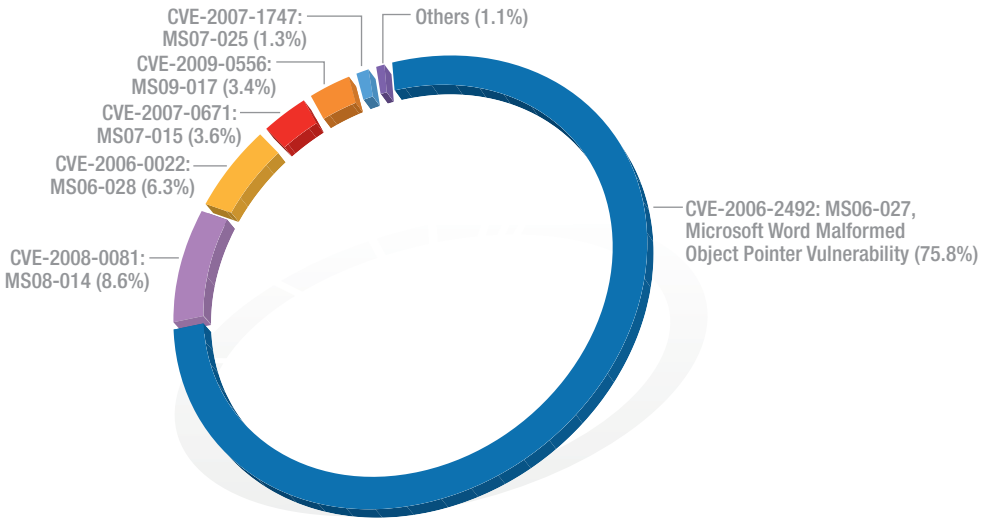
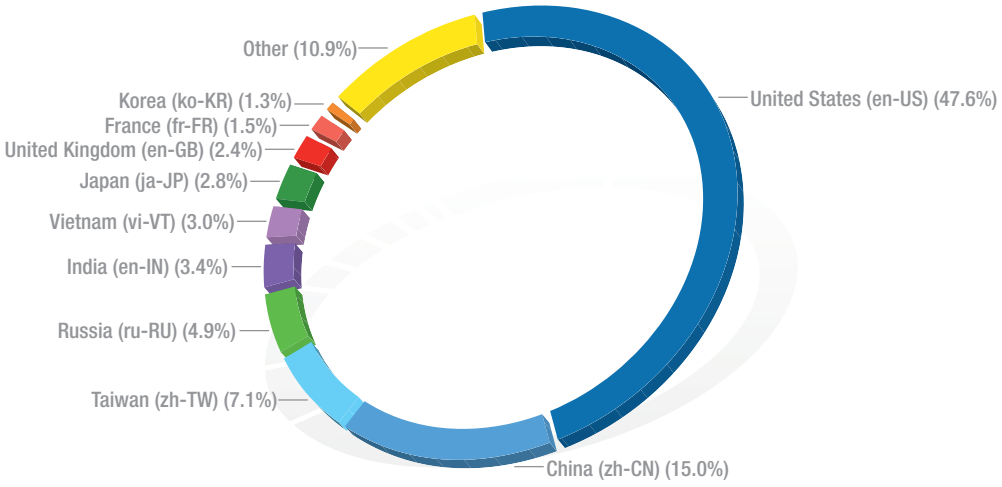


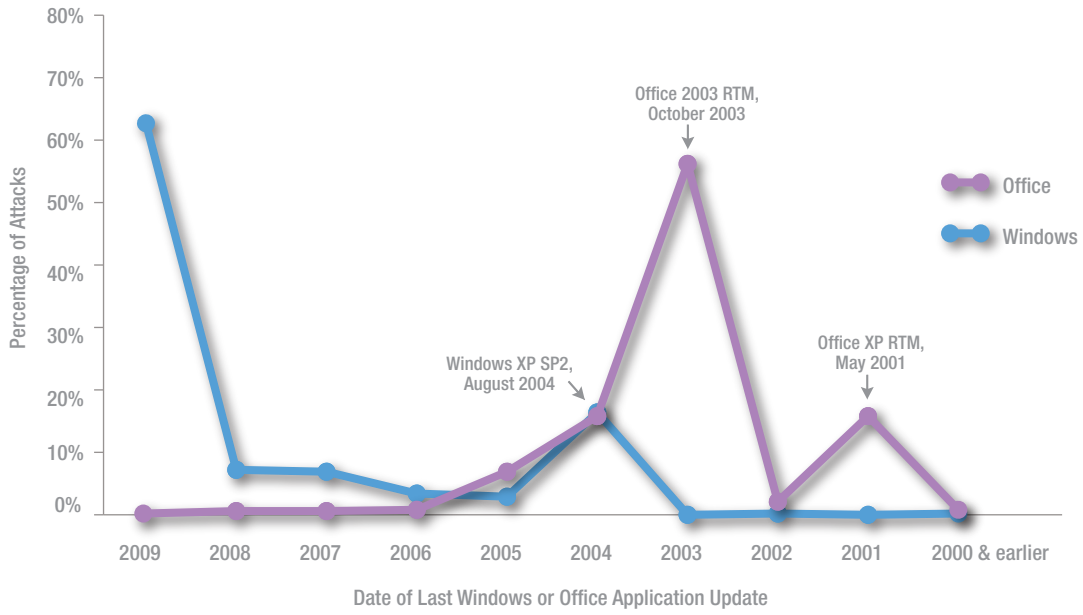
Figure 18 shows Microsoft Office file format exploits ordered by the system locale of the victim. The most common locale for victims was en-US (English language, United States), accounting for 47.6 percent of all incidents, followed by zh-CN (Chinese language, China), with 15.0 percent of incidents.

FIGURE 18. Microsoft Office file format exploits encountered, by system locale of victim, in 2H09



Users who do not keep their Office program installations up to date with service packs and security updates are at increased risk of attack. Figure 19 compares attacks observed in the sample set against Windows and Office during the second half of 2009.

FIGURE 19. Microsoft Office file format exploits encountered, by date of last Windows or Office program update, in 2H09



The horizontal axis shows the last date that the computers in the sample set were updated with security updates for Windows and Office. The vast majority of attacks involved computers with severely out-of-date Office program installations. Just 2.3 percent of attacks involved Office installations that had been updated within four years of December 2009, with more than half (56.2 percent) affecting Office program installations that had last been updated in 2003. Most of these attacks involved Office 2003 users who had not applied a single service pack or other security update since the original release of Office 2003 in October 2003.

As Figure 19 illustrates, it is not at all uncommon for victims of Office program exploit attacks to have Windows installations that are much more current. Almost two-thirds (62.7 percent) of the Office attacks observed in 2H09 affected computers running versions of Windows that had been updated within the previous 12 months. The median amount of time since the last operating system update for computers in the sample was about 8.5 months, compared to 6.1 years for the most recent Office program update—nearly nine times as long. This is not to suggest that users who apply Windows security updates are at greater risk of attack, but it does help illustrate the fact that users can keep Windows rigorously up to date and still face increased risk from exploits unless they also update their other programs regularly. (For information about the online update services Microsoft offers, see "Usage Trends for Windows Update and Microsoft Update," on page 66.)

To further illustrate the importance of applying all service packs and other security updates, Figure 20 and Figure 21 compare the relative levels of vulnerability of different versions of Microsoft Office as originally released and with the most recent service pack for each version installed.

FIGURE 20. Vulnerabilities affecting RTM versions of Office 2000 through Office 2007

Vulnerability	Bulletin	Office 2000 RTM	Office XP RTM	Office 2003 RTM	Office 2007 RTM
CVE-2006-0022	MS06-028	Yes	Yes	Yes	No
CVE-2006-2492	MS06-027	Yes	Yes	Yes	No
CVE-2006-3651	MS06-060	Yes	Yes	Yes	No
CVE-2007-0671	MS07-015	Yes	Yes	Yes	No
CVE-2007-1747	MS07-025	Yes	Yes	Yes	Yes
CVE-2008-0081	MS08-014	Yes	Yes	Yes	Yes
CVE-2009-0238	MS09-009	Yes	Yes	Yes	Yes
CVE-2009-0556	MS09-017	Yes	Yes	Yes	Yes
CVE-2009-0557	MS09-021	Yes	Yes	Yes	Yes

FIGURE 21. Vulnerabilities affecting Office 2000 through Office 2007 with latest service packs installed

Vulnerability	Bulletin	Office 2000 SP3	Office XP SP3	Office 2003 SP3	Office 2007 SP2
CVE-2006-0022	MS06-028	Yes	Yes	No	No
CVE-2006-2492	MS06-027	Yes	Yes	No	No
CVE-2006-3651	MS06-060	Yes	Yes	No	No
CVE-2007-0671	MS07-015	Yes	Yes	No	No
CVE-2007-1747	MS07-025	Yes	Yes	No	No
CVE-2008-0081	MS08-014	Yes	Yes	No	No
CVE-2009-0238	MS09-009	Yes	Yes	Yes	No
CVE-2009-0556	MS09-017	Yes	Yes	Yes	Yes
CVE-2009-0557	MS09-021	Yes	Yes	Yes	Yes

The RTM versions of Office 2000, Office XP, and Office 2003 are each affected by all of the vulnerabilities seen in the sample set, and the RTM version of Office 2007 is affected by five of the nine vulnerabilities. If the Office 2003 RTM users in the sample had installed SP3 and no other security updates, they would have been protected against 96 percent of observed attacks; likewise, Office 2007 RTM users would have been protected from 99 percent of attacks by installing SP2.

However, merely installing service packs is often not enough to provide an adequate level of protection against attacks, especially for older program versions. Office 2000, Office XP, and Office 2003 are each affected by all nine of the vulnerabilities exploited in the sample, even with the latest service pack installed. Users of any of these Office versions who install all service packs and security updates as they are released (for example, by configuring their computers to use Microsoft Update (http://update.microsoft.com) instead of Windows Update) are protected from all nine of these vulnerabilities, as of December 2009.

Mitigating Exploits with Windows Security Improvements

Microsoft Security Response Center (MSRC) Engineering and MSEC Science

Comparing exploit patterns across different systems shows a clear trend: Newer software releases, like Windows 7 and the 2007 Microsoft Office system, are consistently less prone to active exploitation than older releases. To understand why this is so, let's take a look at some of the exploit mitigation technologies that Microsoft has implemented over the past few years, how they work, and how application developers and IT departments can take advantage of them to help create a safer computing experience for everyone.

Exploit Mitigation Technologies in Windows

These are some of the significant exploit mitigation technologies that have been added to Windows over the past few years:

- **Data Execution Prevention (DEP)**: *Buffer overflow* attacks, in which an attacker forces a program or component to store malicious code in an area of memory not intended for it, are some of the most common exploits seen today. DEP is a Windows feature that enables the system to mark one or more pages of memory as non-executable. Marking memory regions as non-executable means that code cannot be run from that region of memory, which makes it harder for exploits involving buffer overruns to succeed.

  DEP was introduced in Windows XP SP2 and has been included in all subsequent releases of Windows desktop and server operating systems. For application compatibility reasons, DEP is "opt-in" in Windows XP, Windows Vista, and Windows 7. DEP protects the operating system and core system files by default, but application developers or IT administrators must specifically configure other programs to take advantage of DEP. (DEP is "opt-out" in Windows Server operating systems, meaning that DEP is enabled for all programs unless specifically disabled for a program.)

Continued on next page…

- **Address Space Layout Randomization (ASLR)**: In older versions of Windows, core processes tended to be loaded into predictable memory locations upon system startup. Some exploits work by targeting memory locations known to be associated with particular processes. ASLR randomizes the memory locations used by system files and other programs, making it much harder for an attacker to correctly guess the location of a given process. The combination of ASLR and DEP creates a fairly formidable barrier for attackers to overcome in order to achieve reliable code execution when exploiting vulnerabilities.

  ASLR was introduced in Windows Vista and has been included in all subsequent releases of Windows. As with DEP, ASLR is only enabled by default for core operating system binaries and applications that are explicitly configured to use it via a new linker switch. You can learn more about ASLR by reading "Inside the Windows Vista Kernel: Part 3" in the April 2007 issue of *TechNet Magazine* (http://technet.microsoft.com/magazine).

- **/SafeSEH and /GS (compiler flags)**: Introduced in the Visual C++® .NET 2002 (also known as VC7) compiler, /SafeSEH and /GS are compile-time flags that developers can use to make their applications harder to exploit in the face of stack-based buffer overruns. For a great overview of /GS and its effectiveness, see the entry "GS cookie protection – effectiveness and limitations" (March 16, 2009) on the Security Research & Defense Blog (http://blogs.technet.com/srd). For more information on how this security feature is being enhanced in Visual Studio® 2010, see the entry "GS" (March 19, 2009) on the Visual C++ Team Blog (http://blogs.msdn.com/vcblog).

- **Structured Exception Handler Overwrite Protection (SEHOP)**: Another common technique used by exploit writers is to overwrite an exception handler to gain code execution. SEHOP stops this entire class of exploits from working by verifying that a thread's exception handler list is intact before allowing any of the registered exception handlers to be called.

  SEHOP was introduced in Windows Server 2008 RTM and Windows Vista SP1, and has been included in all subsequent Windows releases. For application compatibility reasons, SEHOP is disabled by default on Windows Vista and Windows 7 and is only enabled by default on server versions of Windows. See the entry "Preventing the Exploitation of Structured Exception Handler (SEH) Overwrites with SEHOP" (February 2, 2009) on the Security Research & Defense Blog to learn more about SEHOP, including how to turn it on for client SKUs.

- **Windows Heap Manager Security Enhancements**: Two new heap manager checks were introduced in Windows XP SP2 and Windows Server 2003 SP1 that make exploiting heap overruns less reliable. Additional checks have been added to the core in Windows Vista and newer operating systems. See the entry "Preventing the Exploitation of User Mode Heap Corruption Vulnerabilities" (August 4, 2009) on the Security Research & Defense Blog for more information about these new security enhancements.

Continued on next page…

- **Safe Unlinking in the Kernel Pool**: Windows 7 and Windows Server 2008 R2 include code that makes it much harder for attackers to exploit kernel pool overruns. See the entry "Safe Unlinking in the Kernel Pool" (May 26, 2009) on the Security Research & Defense Blog for more information.

FIGURE 22. Exploit mitigation availability by platform

Feature	Windows XP SP2 and Windows Server 2003	Windows Vista SP1 and Windows Server 2008	Windows 7 and Windows Server 2008 R2
DEP	•	•	•
ASLR		•	•
/GS	•	•	•
SEHOP		•	•
Heap Manager Security Enhancements	• *	•	•
Kernel Safe Unlinking			•

* Safe unlinking and heap entry header cookies introduced in Windows XP SP2 and Windows Server 2003 SP1; other enhancements introduced in Windows Vista

Exploit Mitigation in Action

Figure 20 and Figure 21 illustrate the importance of keeping Microsoft Office installations current with the latest service packs and security updates. As guides to the general exploitability of different Office versions, though, they don't tell the whole story. Just because a program is vulnerable to a given exploit doesn't mean the exploit can run successfully in every environment. By taking advantage of the exploit mitigation technologies explained earlier, individuals and organizations can significantly decrease their attack surface and defend themselves against vulnerabilities—even many zero-day vulnerabilities.

As shown in Figure 17, the second-most commonly exploited Office file format vulnerability observed in the second half of 2009 was CVE-2008-0081, a macro validation vulnerability in Microsoft Office Excel®. Microsoft released Security Bulletin MS08-014 in March 2008 to address this vulnerability.

Microsoft researchers analyzed a number of malicious .xls files that exploited the MS08-014 vulnerability and determined that due to the differences in the layout of memory between Excel 2003 running on Windows XP and Excel 2003 running on Windows Vista, the exploits embedded in the malicious files could not work on Windows Vista as written, because of the hard-coded stack addresses the attackers were using to gain reliable code execution.

Continued on next page…

More recently, exploits for CVE-2009-0238, a memory corruption vulnerability in Microsoft Office Excel addressed by Security Bulletin MS09-009, were observed to become the first exploits to successfully target the 2007 Microsoft Office system, more than two years after the suite's release. It's clear that the attackers in this instance were targeting Windows XP users, because the 2007 Microsoft Office system opts in to ASLR (which makes the exploits unreliable) on Windows Vista and Windows 7, but not on Windows XP. Moreover, simply configuring the 2007 Microsoft Office system to opt in to DEP would prevent exploitation on Windows XP as well. For more information and a simple installer that allows Office to opt in to DEP on any platform, see the following entries on the Security Research & Defense Blog (http://blogs.technet.com/srd):

- Understanding DEP as a mitigation technology part 1 (June 12, 2009)
- Understanding DEP as a mitigation technology part 2 (June 12, 2009)

Protecting Yourself

So here are three big action items for computer users and administrators who take these types of attacks very seriously:

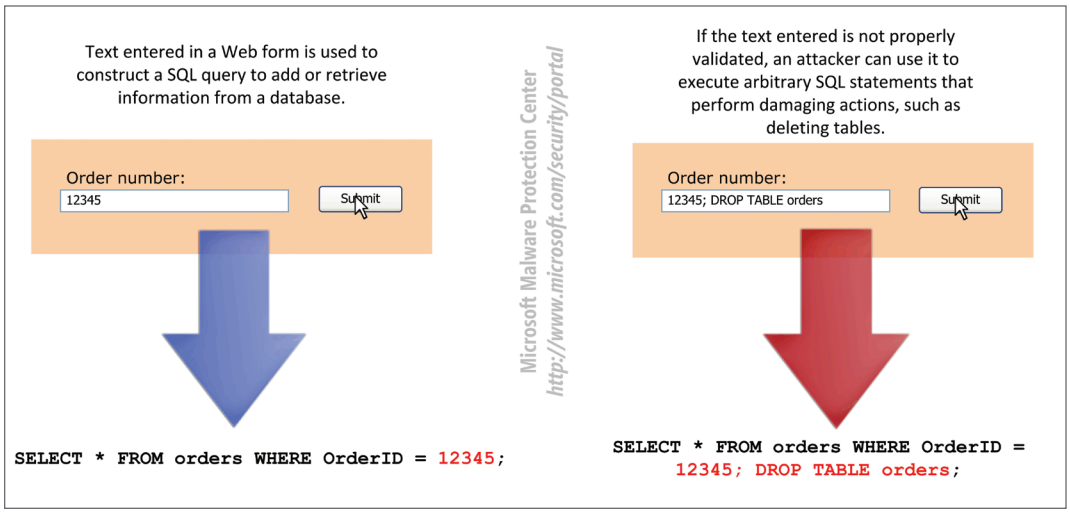
- **Keep your operating system up to date.** This doesn't just mean deploying the latest security updates—it means tracking advances in operating system design and making business decisions to deploy the latest operating system version if its features offer a benefit to your organization.
- **Keep your applications up to date.** Keeping the applications that run on top of the operating system "fresh" is as important as staying up to date on the operating system itself. Again, this doesn't just mean deploying security updates for older versions of the software. Consider how the exploit mitigation features in newer application versions complement and integrate with the features discussed here. This is true for Microsoft and non-Microsoft applications alike (for example, the latest versions of Adobe Flash and Adobe Reader opt in to ASLR and DEP on versions of Windows that support it; older versions of those applications do not).
- **Take advantage of available exploit mitigation technologies.** By default, client versions of Windows are configured with backward compatibility in mind: Features like DEP, SEHOP, and heap corruption detection are disabled by default to minimize disruption for users of older applications. Make the effort to test your applications with these features enabled in a non-production environment with the goal of rolling them out widely if no problems are encountered. If a full rollout turns out to be impractical, consider enabling DEP for specific applications using application compatibility shims (on Windows XP) or the registry (on Windows Vista and Windows 7).

Visit the Security Research & Defense Blog for more information about exploit mitigation technologies, and see "Mitigation Strategies for Protecting Networks, Systems, and People," beginning on page 216, for more guidance related to these and other security-related topics.

Automated SQL Injection Attacks

SQL injection is a technique used by attackers to damage or steal data residing in databases that use Structured Query Language (SQL) syntax to control information storage and retrieval. SQL injection usually involves using a mechanism such as a text field in a Web form to directly pass malicious SQL to a program or script that queries a database. If the program or script does not properly validate the input, the attacker may be able to execute arbitrary database commands, such as deleting tables, altering sensitive records, or accessing other parts of the database or network.[4]

FIGURE 23. Example of a simple SQL injection attack



SQL injection has been around for many years, but until recently it was mostly used in isolated efforts to attack individual servers on the Internet. Beginning in late 2007, however, attackers began to use automated tools to compromise large numbers of Web sites through SQL injection in an attempt to spread malware.

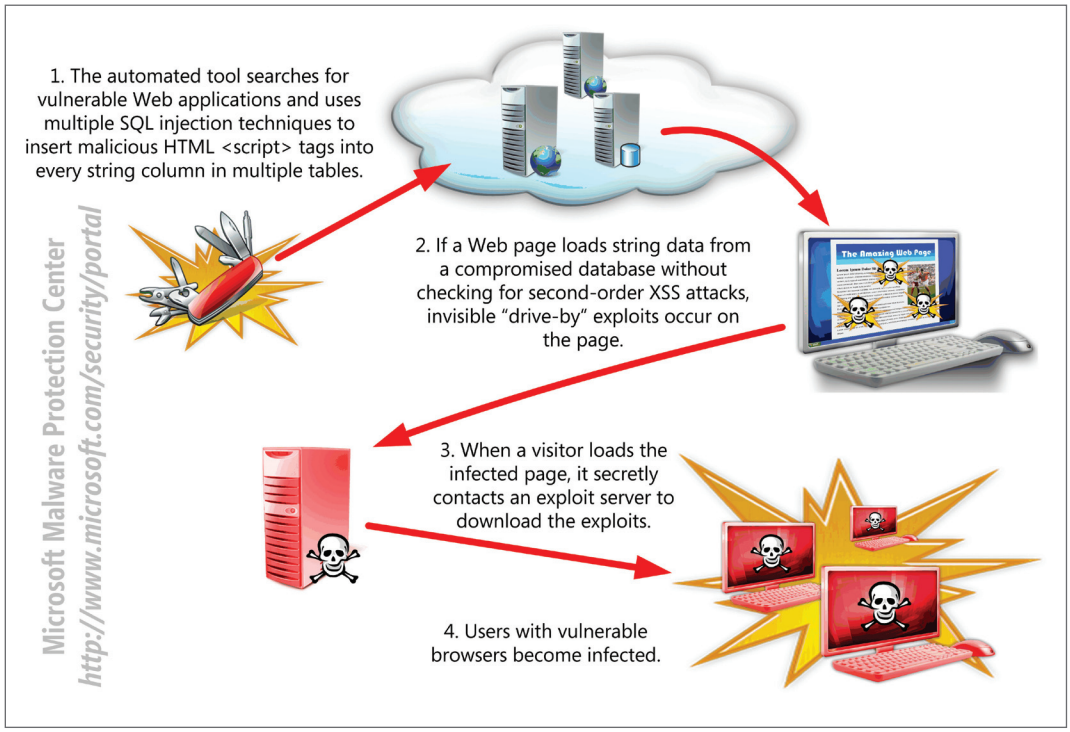
Web applications often construct pages dynamically as they are requested, by retrieving information from a database and using it to populate the page. The goal of the automated mass SQL injection tool is to insert malicious HTML and JavaScript code into the database so that it becomes a part of every page requested by visitors to the site, a technique called *persistent cross-site scripting (XSS)*.

The tool begins its attack by conducting a Web search for URLs that take user input through URI query strings (such as *http://www.example.com/page.aspx?id=12345*, where *id* is a parameter and *12345* is its value). The tool performs some simple tests to determine which of these Web pages may be vulnerable to SQL injection and then tries multiple SQL injection payloads to discover some details about the SQL server and account used by the Web page. It then uses a SQL injection payload to append malicious JavaScript code within

[4] For a more in-depth explanation of SQL injection and how to guard against it, see "SQL Injection," in *Microsoft SQL Server 2008 Books Online*, at http://msdn.microsoft.com/library/ms161953.aspx.

HTML <script> tags to every string column in every table in the database. When a site visitor requests a page that includes some of this compromised string data, unless the page mitigates XSS, the malicious script executes in the visitor's Web browser and attempts to use multiple browser-related exploits to download and install malware.

FIGURE 24. How the mass SQL injection tool works



Microsoft uses a number of methods to detect and track Web sites that have been victimized by automated SQL injection attacks. Figure 25 lists the top-level domains (TLDs) that hosted the most sites affected by SQL injection attacks in 2H09.

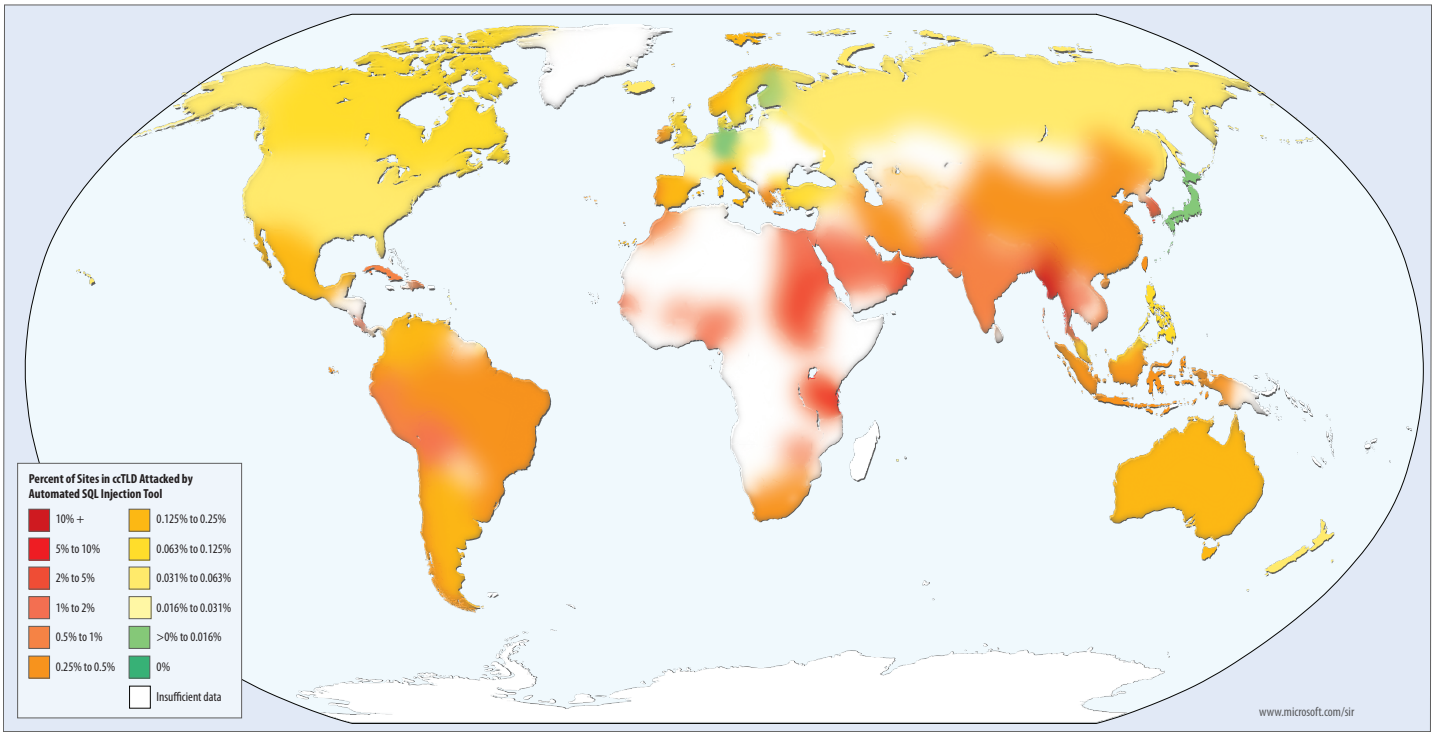
FIGURE 25. Top 10 TLDs affected by SQL injection attacks in 2H09

Rank	TLD	Associated With	Victimized Pages
1	.com	Commercial entities	53,560
2	.cn	China	30,139
3	.net	Network infrastructure	13,163
4	.tw	Taiwan	4,675
5		(IP address only)	3,704
6	.org	Non-profit organizations	3,254
7	.br	Brazil	1,878
8	.ir	Iran	707
9	.th	Thailand	583
10	.fr	France	301

Web sites in and associated with China were heavily affected by automated SQL injection attacks in 2H09. The .cn top-level domain (TLD) was second only to the heavily used .com TLD in the number of victimized Web sites, as shown in Figure 25.

Figure 26 shows the portion of Web sites in each country-code top-level domain (ccTLD) that were found to have been attacked using automated SQL injection tools in 2H09.

FIGURE 26. Web sites victimized by SQL injection, by ccTLD, in 2H09



Microsoft has provided a number of resources that can help server administrators defend against these kinds of attacks.

- Security Advisory 954462 includes an overview of SQL injection attacks and offers guidance for identifying and correcting vulnerable ASP and ASP.NET Web application code that does not follow best practices for secure Web application development.
- The Microsoft SDL team has issued a Quick Security Reference (http://go.microsoft.com/?linkid=9723267) on SQL injection that addresses the vulnerability from the perspective of various business roles, such as business decision maker, architect, developer, and tester/QA.
- The following TechNet blog entries also contain further in-depth information:
  - Anatomy of a SQL Injection Incident (March 14, 2008)
  - Anatomy of a SQL Injection Incident, Part 2: Meat (March 15, 2008)

For additional information about safeguarding computers against compromised Web sites, see "Promote Safe Browsing" on page 223.

Security Breach Trends

Over the last few years, laws have been passed in a number of jurisdictions around the world requiring that affected individuals be notified when an organization loses control of personally identifiable information (PII) with which it has been entrusted. These mandatory notifications offer unique insights into how information security efforts need to address issues of negligence as well as technology. They differ from surveys in that the information offered is not from self-selected respondents, and, for a given set of criteria, participation is mandated by law.

Since 2005, volunteer security researchers have tracked worldwide reports of such data security breaches and recorded them in the Data Loss Database (DataLossDB) at http://datalossdb.org. DataLossDB volunteers collect data by monitoring data breach reports published by news media outlets or other information sources and by filing formal information requests with the governments of several jurisdictions that have mandatory notification laws. Since 2008, the DataLossDB has been maintained by the Open Security Foundation (OSF) (http://www.opensecurityfoundation.org), a nonprofit organization dedicated to compiling community-sourced information about security vulnerabilities and data breaches.

This section of the *Security Intelligence Report* uses the information in the DataLossDB to examine the types of breach incidents from around the world that took place in 2H09 and earlier. The data, despite containing a lot of valuable information, is not perfect. It is not as detailed as might be hoped for, and laws in different jurisdictions contain different trigger clauses for when notice must be given. Nevertheless, the data is of sufficient quality to lend itself to an effective analysis of security failures.

Breach incidents are recorded in the DataLossDB using a common format that can track such details as the date and location of the incident, the companies or organizations involved, the number of records affected, and any arrests or lawsuits connected with the incident. Incidents are classified using a list of 23 individual breach types, which for the purposes of this analysis, have been grouped into 10 categories.[5] The categories are shown in Figure 27.

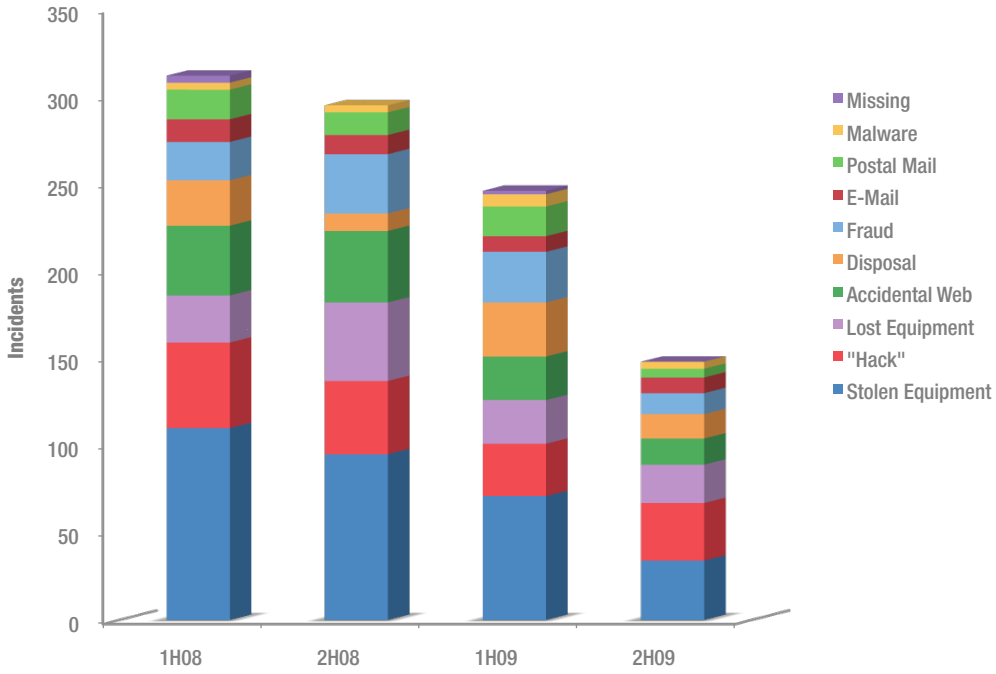
[5] The OSF DataLossDB includes a small number of incidents for which the breach type is listed as "Unknown." These incidents are not included in the data and analysis presented in this report.

FIGURE 27. Security breach incident categories used in this section

SIR Label	Definition	DataLossDB Breach Types
Stolen Equipment	Stolen computers, disks, tapes, or documents	Stolen Computer, Stolen Document, Stolen Drive, Stolen Laptop, Stolen Media, Stolen Tape
"Hack"	Reported as some type of computer intrusion where the data is not available to the public	Hack
Lost Equipment	Reported as lost computers, disks, tapes, or documents	Lost Computer, Lost Document, Lost Drive, Lost Laptop, Lost Media, Lost Tape
Accidental Web	Accidental exposure on a Web site, available to the public with a Web browser	Web
Fraud	Frauds and scams, perpetrated by insiders or outsiders; this includes disputed cases, on which Microsoft takes no position	Fraud Se
Postal Mail	Information exposed by physical mail, either sent to an incorrect recipient or with data visible outside the envelope	Snail Mail
E-Mail	E-mail sent to an unintended or unplanned recipient	E-Mail
Disposal	Improper disposal of any sort	Disposal Computer, Disposal Document, Disposal Drive, Disposal Tape
Malware	Malware was blamed	Virus
Missing	One or more laptop computers gone missing without explanation	Missing Laptop

Figure 28 illustrates the overall distribution of incidents by type since 1H08.[6]

FIGURE 28. Security breach incidents, by incident type, 1H08–2H09



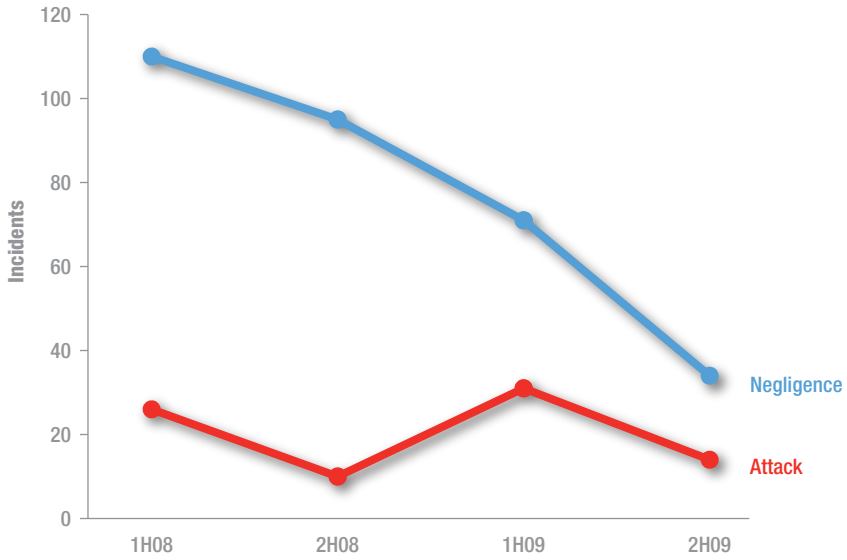
Trends that can be deduced from this data include the following:

- Overall, in this two-year period, there is a clear downward trend in the absolute number of incidents in every single category except for malware attacks, which remains unchanged. Stolen equipment & media and accidental Web loss account for the largest declines. This downward trend may be related to the overall decline in worldwide economic activity over the same time period. It is an open question whether the trend will continue or reverse as the global economy improves.
- Improper disposal of business records accounts for quite a few incidents and is relatively easy for organizations to address by developing and enforcing effective policies regarding the destruction of paper and electronic records containing sensitive information.
- Although security breaches are often linked in the popular consciousness with malicious parties seeking and gaining unlawful access to sensitive data, incidents involving attacks (hacking, malware, and fraud) have been significantly outnumbered in recent years by incidents involving negligence (lost, stolen, or missing equipment; accidental disclosure; or improper disposal), as shown in Figure 29.

[6] Based on DataLossDB statistics as of February 18, 2010. Researchers continually update the database with breach reports from different periods, so the figures presented here are subject to change in the future.

- As Figure 29 also shows, incidents involving negligence have declined steeply over the past two years, from 110 in 1H08 to just 34 in 2H09. Organizations may be taking more steps to secure sensitive equipment, such as security checks at facility gates or programs to educate employees about secure practices. Adoption of strong encryption solutions, like Windows BitLocker Drive Encryption, may also be contributing to the decline. Disclosure laws in many jurisdictions do not require notification when encrypted data is lost or stolen because it is much more difficult for the thief or finder to extract than unencrypted data.

FIGURE 29. Breach incidents resulting from attacks and negligence, 1H08–2H09



Overall, the decline in incident reports is relatively consistent over time, with no obvious anomalies or severe fluctuations. This could be taken to support the reliability of the data and can be used to influence information security decisions.

Microsoft Security Response Center

The **Microsoft Security Response Center (MSRC)** investigates and responds to reports of vulnerabilities in Microsoft products. MSRC staffers constantly monitor a number of communication channels, including Internet-based security forums and e-mail messages sent to secure@microsoft.com by independent security researchers, for information that may indicate the existence of a new vulnerability or exploit. When MSRC researchers verify that a vulnerability exists, they work with the affected product team to develop, test, and deliver a security update in response to the vulnerability. Security updates are made available for download through several different mechanisms, including Windows Update, Microsoft Update, and the Microsoft Download Center.

The MSRC publishes Microsoft Security Bulletins and Microsoft Security Advisories to communicate vulnerability and exploit information to the public. Microsoft Security Bulletins provide information and guidance about updates that are available to address software vulnerabilities that may exist in Microsoft products. With each security bulletin that is released, there is an associated software update available for the affected product. Microsoft Security Advisories are meant to give customers detailed information and guidance on a variety of security-related issues that may not be specifically tied to a software update. For example, an advisory may detail Microsoft software updates that introduce changes to the behavior of the product or may provide late-breaking and timely information that customers can use to help protect themselves from threats or attack. The MSRC also engages with other software vendors to help them identify and resolve vulnerabilities in their software. The MSRC blog, at http://blogs.technet.com/msrc, provides additional information about vulnerabilities, exploits, security bulletins, and security advisories.

Industry-Wide Vulnerability Disclosures

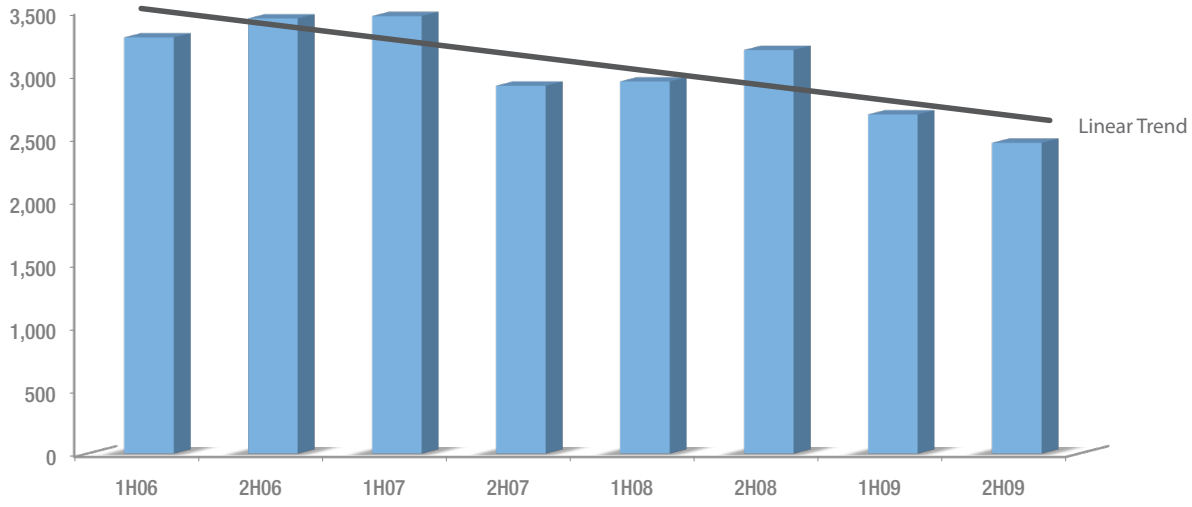
Vulnerabilities are weaknesses in software that allow an attacker to compromise the integrity, availability, or confidentiality of that software. Some of the worst vulnerabilities allow attackers to run arbitrary code on the compromised system.

This section of the *Microsoft Security Intelligence Report* analyzes new vulnerabilities that were disclosed during the second half of 2009 and examines trends in vulnerability disclosures since 2006. A *disclosure*, as the term is used in this report, is the revelation of a software vulnerability to the public at large. It does not refer to any sort of private disclosure or disclosure to a limited number of people. Disclosures can come from a variety of sources, including the software vendor itself, security software vendors, independent security researchers, and even malware creators. This section discusses software vulnerability disclosures for the software industry as a whole. See "Vulnerability Reports for Microsoft Products," beginning on page 61, for Microsoft-specific vulnerability information.

Vulnerability Disclosures

Vulnerability disclosures in 2H09 were down 8.4 percent from the first half of the year, continuing an overall trend of moderate declines since 2006. Figure 30 illustrates the number of vulnerability disclosures across the software industry for each half-year period since 1H06.

FIGURE 30. Industry-wide vulnerability disclosures by half-year, 1H06–2H09



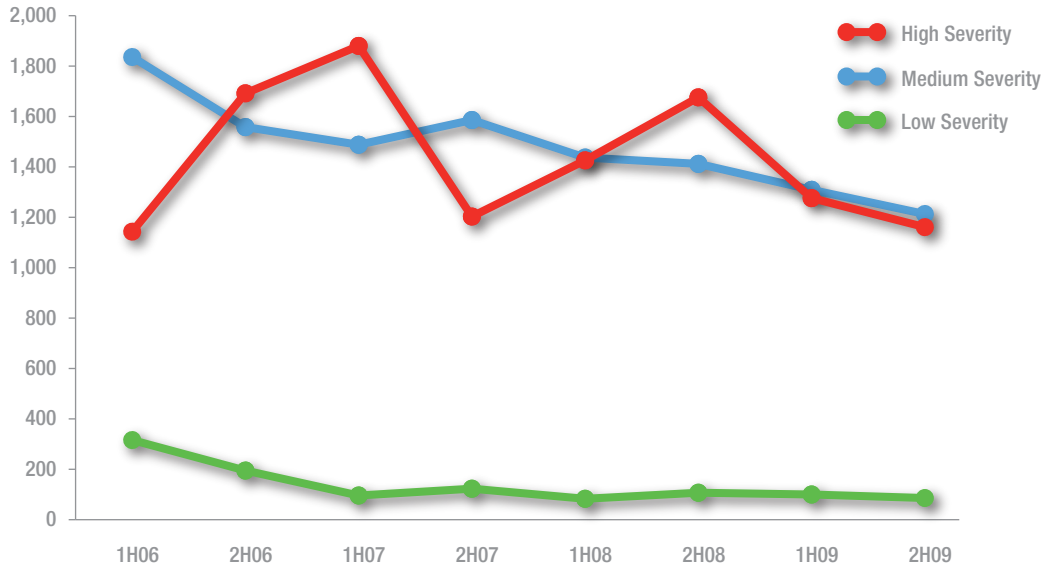
Vulnerability Severity

In general, large numbers of disclosed vulnerabilities create significant challenges for IT security administrators who have deployed the affected products. Not all vulnerabilities are equal, however, and an analysis of vulnerability severity can help IT professionals understand and prioritize the nature and severity of the threats they face from newly disclosed vulnerabilities.

The Common Vulnerability Scoring System (CVSS) is a standardized, platform-independent scoring system for rating IT vulnerabilities, developed by a coalition of security professionals from around the world representing the commercial, non-commercial, and academic sectors. Currently in its second version, the system assigns a numeric value between 0 and 10 to vulnerabilities according to severity, with higher scores representing greater severity.[7]

High severity vulnerabilities disclosed in 2H09 were down 9.0 percent from the first half of the year, and 30.7 percent from 2H08. As Figure 31 illustrates, disclosures for all three classes of vulnerability were down in 2H09, with both High severity and Medium severity vulnerabilities falling by about the same amount.

FIGURE 31. Industry-wide vulnerability disclosures by severity, 1H06–2H09



Low severity vulnerabilities accounted for just 3.5 percent of overall vulnerabilities in 2H09, down from 4.1 percent in the first half of the year. The continuing predominance of High severity and Medium severity vulnerability disclosures is likely due at least in part to the tendency of both attackers and legitimate security researchers to prioritize searching for the most severe vulnerabilities. Attackers seek out severe vulnerabilities so they can

[7] For an explanation of the CVSS scoring methodology, see http://www.first.org/cvss/cvss-guide.html#i3.

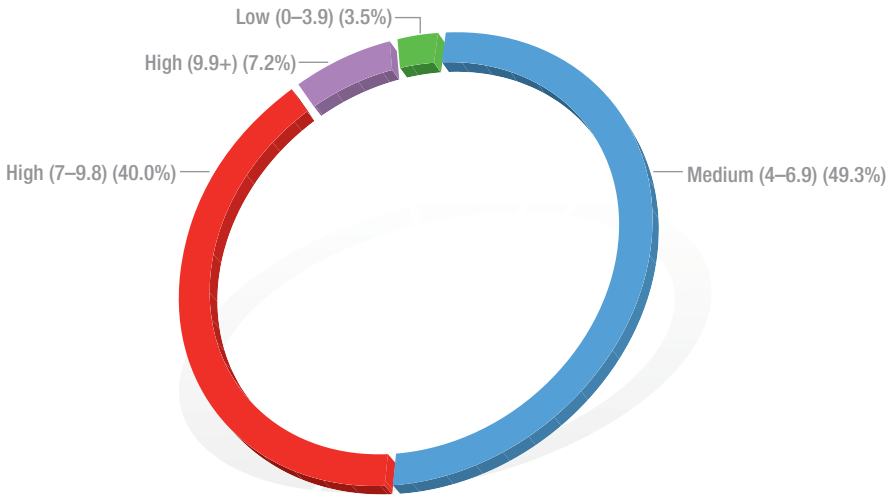
develop more effective attacks, and legitimate researchers focus on finding the vulnerabilities that could cause the most damage if exploited so software vendors can address them quickly.

Focusing on mitigating the most severe vulnerabilities first is a security best practice. Although CVSS, through the National Vulnerability Database (NVD),[8] provides a base score across the set of industry vulnerabilities, security professionals should look first to their software vendors for further security information because they are the people who understand their software best. However, not all vendors provide their own assessment of severity or even provide security advisories for vulnerabilities.

The large number of High severity vulnerabilities underscores the importance of looking beyond the simpler groupings of Low, Medium, and High to leverage the CVSS score behind the rating label, in addition to other information that is available. With High severity vulnerabilities accounting for close to half of all vulnerabilities during each of the last several periods, administrators need more information to effectively set priorities for responding to vulnerabilities.

Along these lines, the chart in Figure 32 illustrates the severity breakdown for 2H09. It shows the percentage distributions of the severity ratings and includes a breakout for the most severe of the High severity vulnerabilities—those with a base CVSS score of 9.9 or higher, which indicates that an attacker could easily exploit the vulnerability to run arbitrary code. High severity vulnerabilities that scored 9.9 or higher represent 7.2 percent of all vulnerabilities disclosed in 2H09.

FIGURE 32. Industry-wide vulnerability disclosures, by severity, in 2H09



[8] The National Vulnerability Database (http://nvd.nist.gov) is the U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP). CVE and CVSS are both components of SCAP.

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 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. Security investigators take both severity and complexity into account when determining the appropriate response to a vulnerability. Access complexity is one of the metrics used to calculate the CVSS base score for a vulnerability. CVSS version 2.0 uses three complexity designations: Low, Medium, and High. Figure 33 gives definitions for these designations.[9]

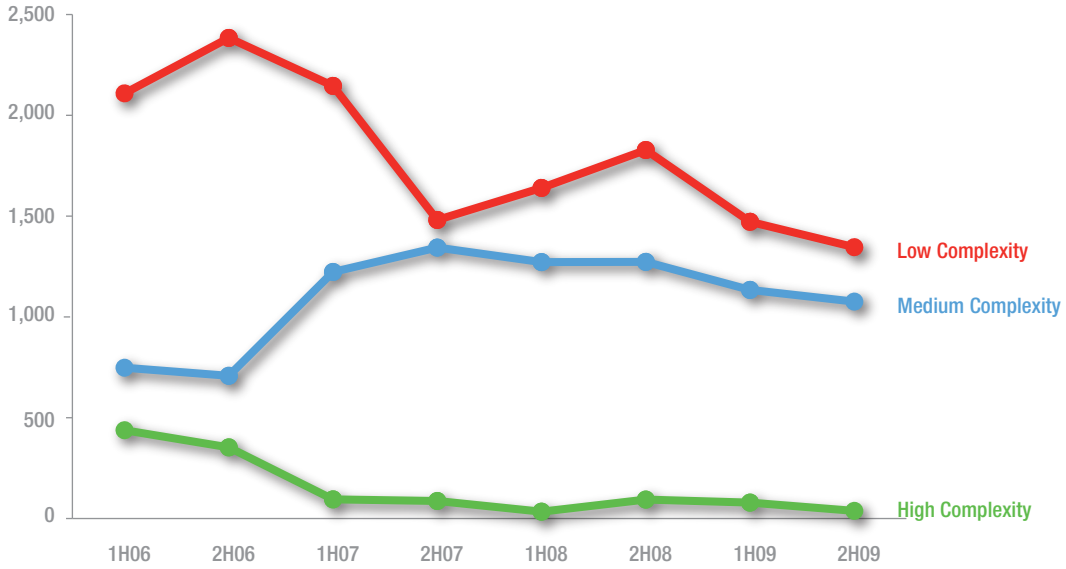
FIGURE 33. NVD complexity rankings and definitions

High	Specialized access conditions exist. For example: • In most configurations, the attacking party must already have elevated privileges or spoof additional systems in addition to the attacking system (for example, DNS hijacking). • The attack depends on social engineering methods that would be easily detected by knowledgeable people. For example, the victim must perform several suspicious or atypical actions. • The vulnerable configuration is seen very rarely in practice. • If a race condition exists, the window is very narrow.
Medium	The access conditions are somewhat specialized. The following are examples: • The attacking party is limited to a group of systems or users at some level of authorization, possibly untrusted. • Some information must be gathered before a successful attack can be launched. • The affected configuration is non-default and is not commonly configured (for example, a vulnerability present when a server performs user account authentication via a specific scheme but not present for another authentication scheme). • The attack requires a small amount of social engineering that might occasionally fool cautious users (for example, phishing attacks that modify a Web browser's status bar to show a false link, having to be on someone's "buddy" list before sending an IM exploit).
Low	Specialized access conditions or extenuating circumstances do not exist. The following are examples: • The affected product typically requires access to a wide range of systems and users, possibly anonymous and untrusted (for example, Internet-facing Web or mail server). • The affected configuration is default or ubiquitous. • The attack can be performed manually and requires little skill or additional information gathering. • The "race condition" is a lazy one (in other words, it is technically a race but easily winnable).

Figure 34 shows the complexity mix for vulnerabilities disclosed in each half-year period since 1H06. Note that Low complexity indicates greater danger, like High severity does in Figure 31.

[9] Definitions from Peter Mell, Karen Scarfone, and Sasha Romanosky, *A Complete Guide to the Common Vulnerability Scoring System Version 2.0*, section 2.1.2. http://www.first.org/cvss/cvss-guide.html

FIGURE 34. Industry-wide vulnerability disclosures by access complexity, 1H06–2H09



The complexity mix has remained roughly constant since 1H08, with High complexity vulnerabilities—those that are generally the most difficult to exploit—remaining a very small portion of the total. As in previous periods, more than half of all vulnerabilities (54.7 percent in 2H09) were Low complexity vulnerabilities, indicating that attackers may have an easy time developing reliable exploits for these vulnerabilities. As with High severity vulnerabilities, both attackers and legitimate security researchers tend to prioritize searching for Low complexity vulnerabilities, for reasons similar to those given earlier.

Operating System and Browser Vulnerabilities

Comparing operating system vulnerabilities to non-operating system vulnerabilities requires determining whether a particular program or component should be considered part of an operating system. This is not always a simple and straightforward question to answer, given the componentized nature of modern operating systems. Some programs (media players, for example) ship by default with operating system software but can also be downloaded from the system software vendor's Web site and installed individually. Linux distributions, in particular, are often assembled from components developed by different teams, many of which provide crucial operating functions, like a graphical user interface (GUI) or Internet browsing.

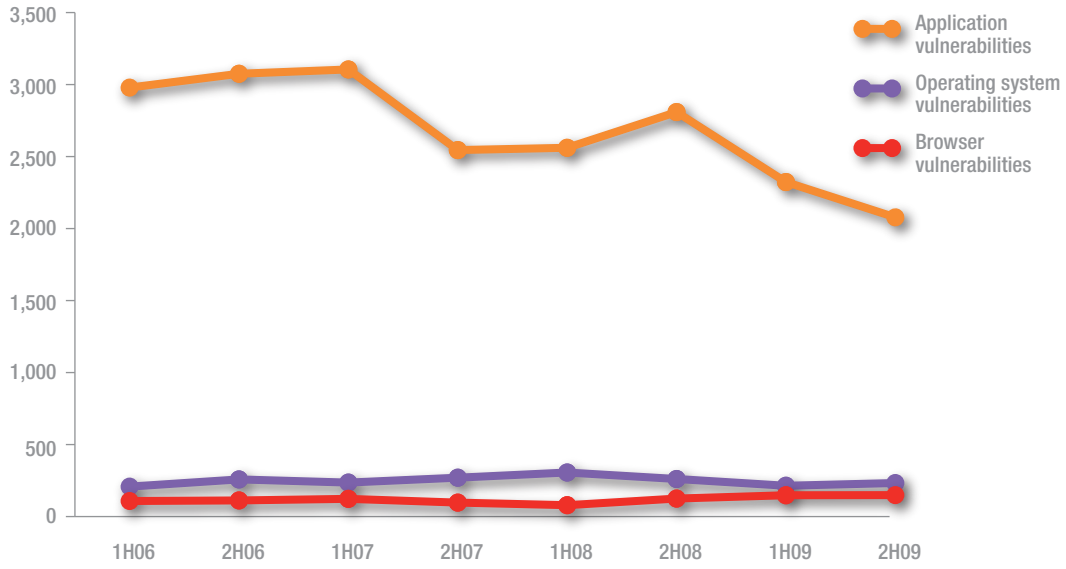
To facilitate analysis of operating system and browser vulnerabilities, this section distinguishes between three different kinds of vulnerabilities:

- *Operating system vulnerabilities* are those affecting the Linux kernel; or components that ship with an operating system produced by Microsoft, Apple, or a proprietary Unix vendor, and defined as part of the operating system by the vendor, except as described in the next paragraph.

- *Browser vulnerabilities* are those affecting components defined as part of a Web browser. This includes Web browsers that ship with operating systems, such as Windows Internet Explorer and Apple's Safari, along with third-party browsers, such as Mozilla Firefox and Google Chrome.
- *Application vulnerabilities* are those affecting all other components, including components published by operating system vendors and other vendors. Vulnerabilities in open source components that may ship with Linux distributions (such as the X Window System, the GNOME desktop environment, GIMP, and others) are considered application vulnerabilities.

Figure 35 shows vulnerabilities for operating systems, browsers, and applications since 1H06, as determined by this simple model.

FIGURE 35. Industry-wide operating system, browser, and application vulnerabilities, 1H06–2H09

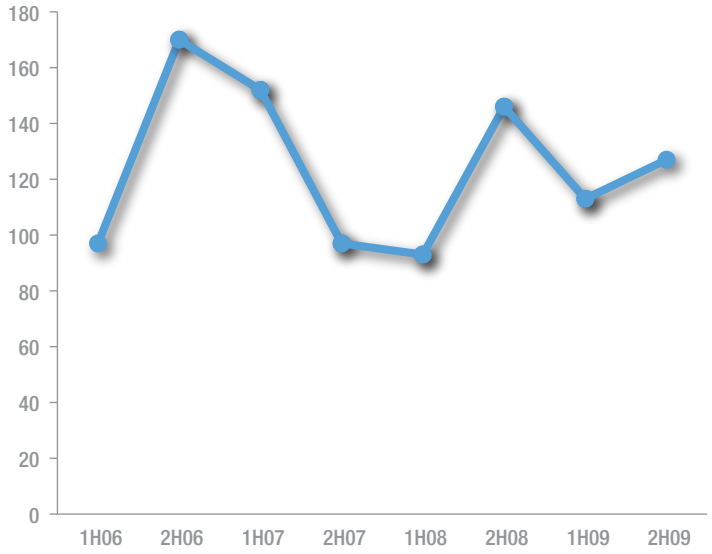


Application vulnerabilities continued to account for a large majority of all vulnerabilities in 2H09, though the total number of application vulnerabilities was down significantly from 2H08 and 1H09. Operating system and browser vulnerabilities were both roughly stable, with each accounting for a small fraction of the total.

Vulnerability Reports for Microsoft Products

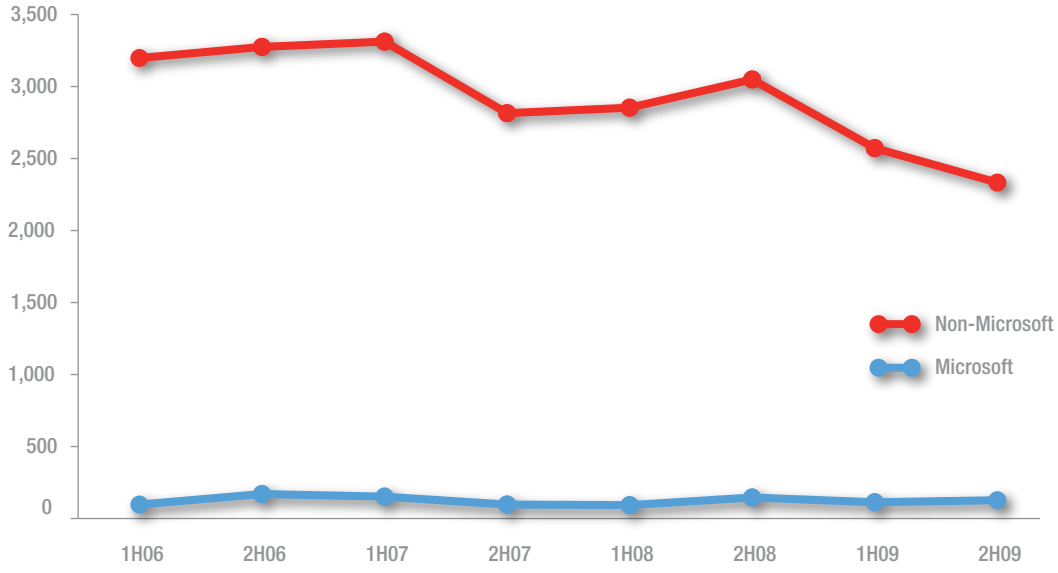
Figure 36 charts vulnerability disclosures for Microsoft products since 1H06.

FIGURE 36. Vulnerability disclosures for Microsoft products, 1H06–2H09



Vulnerability disclosures for Microsoft products increased to 127 in 2H09 from 113 in 1H09. In general, trends for Microsoft vulnerability disclosures have mirrored those for the industry as a whole, with peaks in 2H06–1H07 and again in 2H08, as shown in Figure 37. Over the past four years, Microsoft vulnerability disclosures have consistently accounted for 3 to 5 percent of all disclosures industry wide.

FIGURE 37. Vulnerability disclosures for Microsoft and non-Microsoft products, 1H06–2H09

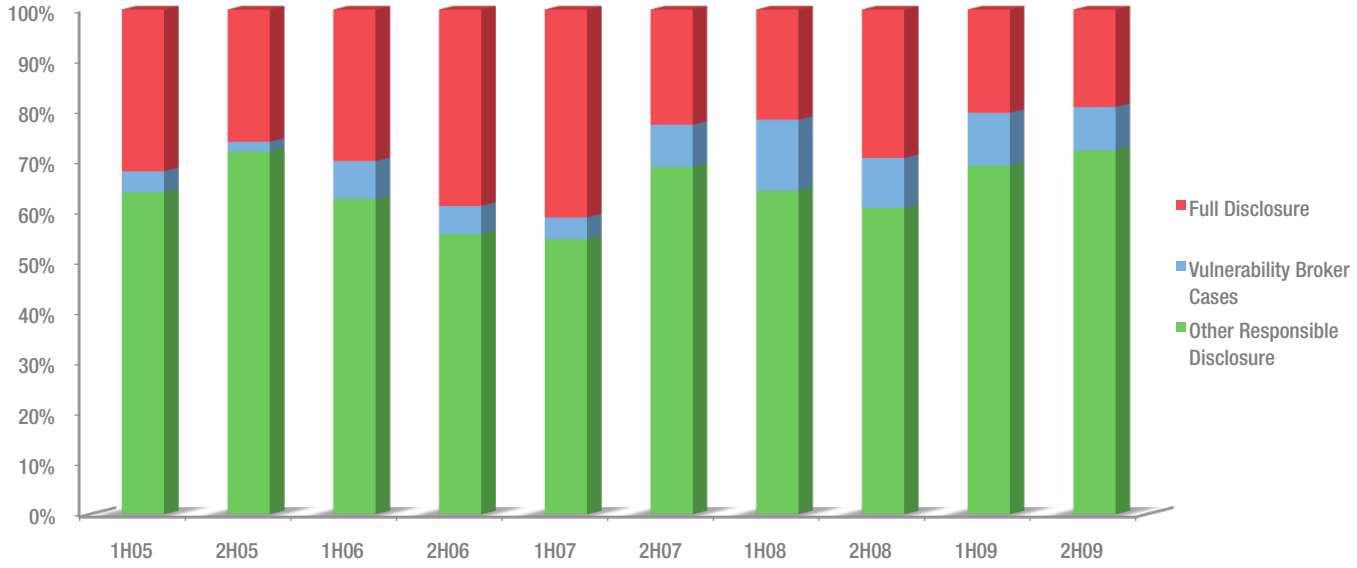


Responsible Disclosures

Responsible disclosure means disclosing vulnerabilities privately to an affected vendor so it can develop a comprehensive security update to address the vulnerability before the details become public knowledge. Ideally, with responsible disclosure, the release of the security update coincides with vulnerability information becoming publicly available. This helps to keep users safer by preventing potential attackers from learning about newly discovered vulnerabilities before security updates are available.

Figure 38 shows responsible disclosures of vulnerabilities in Microsoft software received by the Microsoft Security Response Center in each half-year period since 1H05, as a percentage of all disclosures.

FIGURE 38. Responsible disclosures as a percentage of all disclosures involving Microsoft software, 1H05–2H09



In 2H09, 80.7 percent of Microsoft vulnerability disclosures adhered to responsible disclosure practices, up from 79.5 percent in 1H09 and higher than in any previous tracked period. Responsible disclosure figures include disclosures brought to the MSRC by vulnerability brokers iDefense and ZDI. A *vulnerability broker* is a company or other entity that provides software vendors, such as Microsoft, with vulnerability information provided to it by external security researchers. In exchange for such compensation as the broker may provide, the security researchers agree not to disclose any information about the vulnerability to anyone other than the vulnerability broker and the affected vendor. Microsoft and the MSRC continue to work with vulnerability brokers as a means of providing an avenue for researchers to responsibly disclose security issues to vendors, as an alternative to full public disclosures that place customers and the overall computing ecosystem at risk.

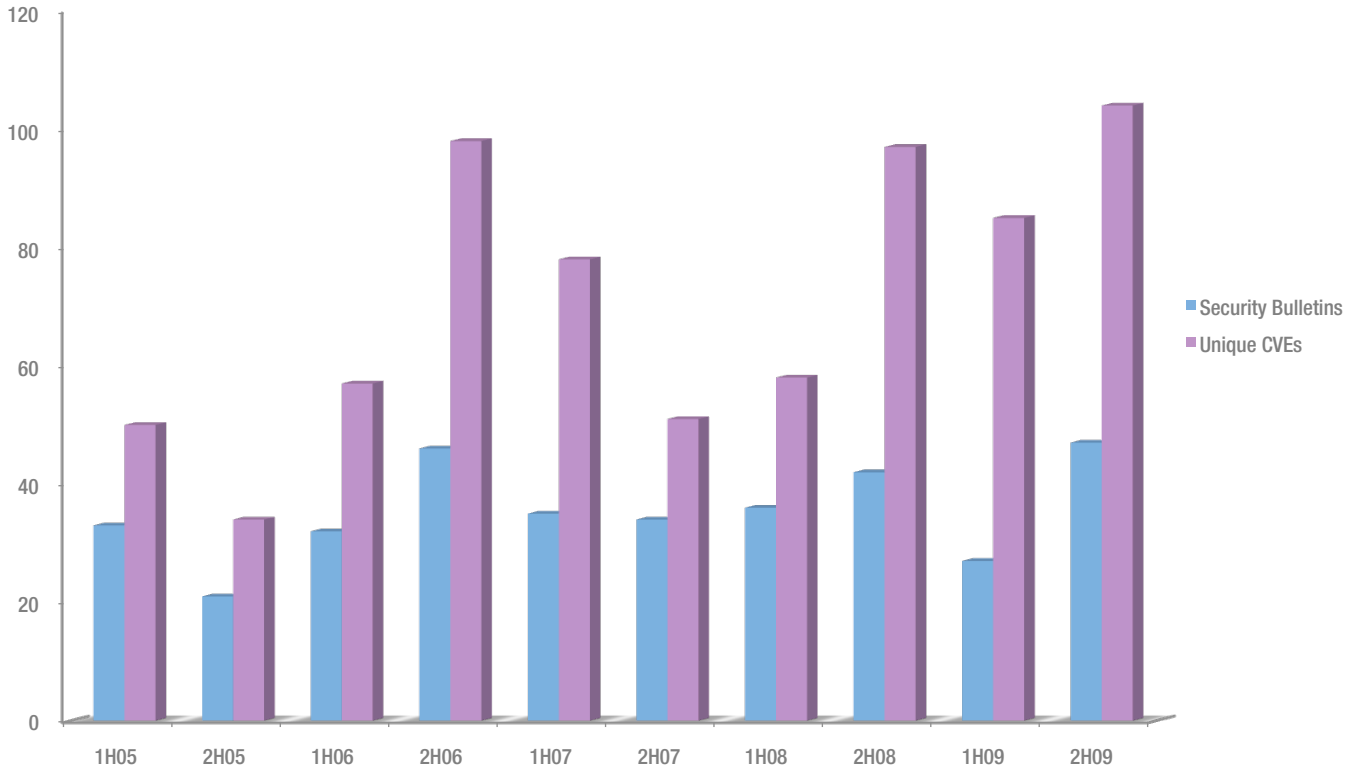
While the overall percentage of reported vulnerabilities that were disclosed responsibly rose about 1 percent, the percentage of disclosures submitted by vulnerability brokers declined slightly to 8.6 percent of all disclosures in 2H09, compared to 10.5 percent in the first half of the year—meaning that the percentage of reported vulnerabilities that were disclosed responsibly through other means rose by about 3 percent, from 69.1 percent to 72.1 percent. Microsoft believes that software vendors can achieve high responsible disclosure rates by engaging with the security community directly and by proactively addressing security issues in a timely manner, while working with the security researcher on the reported vulnerability.

Microsoft Security Bulletins in 2H09

The MSRC is the group at Microsoft that identifies, monitors, resolves, and responds to Microsoft software security vulnerabilities. The MSRC releases security bulletins each month that address vulnerabilities in Microsoft software. Security bulletins are numbered serially within each calendar year. For example, "MS09-012" refers to the twelfth security bulletin released in 2009. Security bulletins are typically released on the second Tuesday of each month, although on rare occasions Microsoft releases a so-called *out-of-band* security update to address an urgent issue.

A single security bulletin often addresses multiple vulnerabilities from the CVE database,[10] each of which is listed in the bulletin, along with any other relevant issues. Figure 39 shows the number of security bulletins released and the number of individual CVE-identified vulnerabilities they have addressed for each half-year period since 1H05. (Note that not all vulnerabilities are addressed in the period in which they are initially disclosed.)

FIGURE 39. Security bulletins released and CVEs addressed by Microsoft by half-year, 1H05–2H09

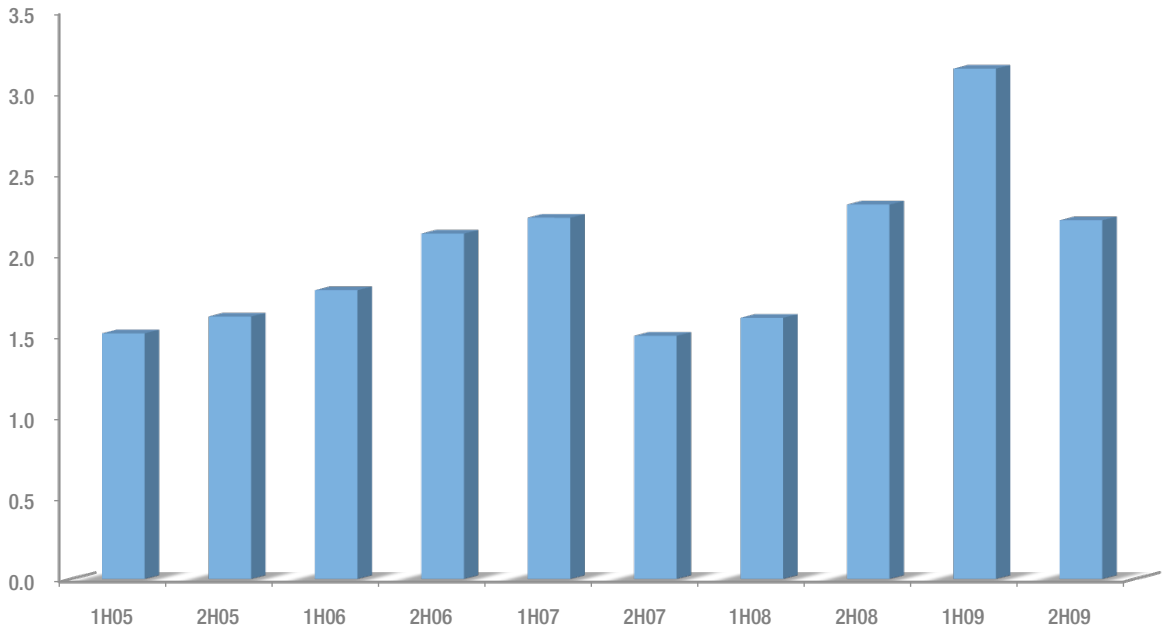


[10] See http://cve.mitre.org to look up vulnerabilities by CVE identifier.

In 2H09, Microsoft released 47 security bulletins that addressed 104 individual vulnerabilities identified on the CVE list. Most of this increase is due to a rise in the number of responsible disclosure reports Microsoft has received, which means that in most cases the MSRC is able to test and release security updates addressing the vulnerabilities before their existence is widely known. (See page 62 for more information about responsible disclosure.)

Although the overall number of bulletins shipped increased from 27 in 1H09, the number of vulnerabilities addressed per bulletin decreased from 3.1 to 2.2, as shown in Figure 40.

FIGURE 40. Average number of CVEs addressed per security bulletin, 1H05–2H09



Whenever possible, the MSRC consolidates multiple vulnerabilities affecting a single binary or component and addresses them with a single security bulletin, to maximize the effectiveness of each update while minimizing the potential disruption that customers face from testing and integrating individual security updates into their computing environments. Consolidation is not always feasible, as when vulnerabilities affect different unrelated components and must be addressed by separate updates. Although the ratio of CVEs to security bulletins in 2H09 is down from the historic high achieved in the first half of the year, it remains high in relation to most previous periods, and the overall trend is a positive one.

Usage Trends for Windows Update and Microsoft Update

The prompt, widespread adoption of security updates and other software upgrades can significantly mitigate the spread and impact of malware. Over the past decade, many software vendors have developed mechanisms for informing users about the availability of new updates and enabling them to obtain and install updates easily and automatically. Security-conscious IT departments have responded by developing practices to quickly test and assess newly issued updates and to deliver them to their users.

Update Clients and Services

Microsoft provides several tools and services that enable users to download and install updates directly from Microsoft or from update servers designated by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in Windows 7, Windows Vista, and Windows Server 2008) connects to an update service for the list of available updates. After the update client has determined which updates are applicable to the user's computer, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

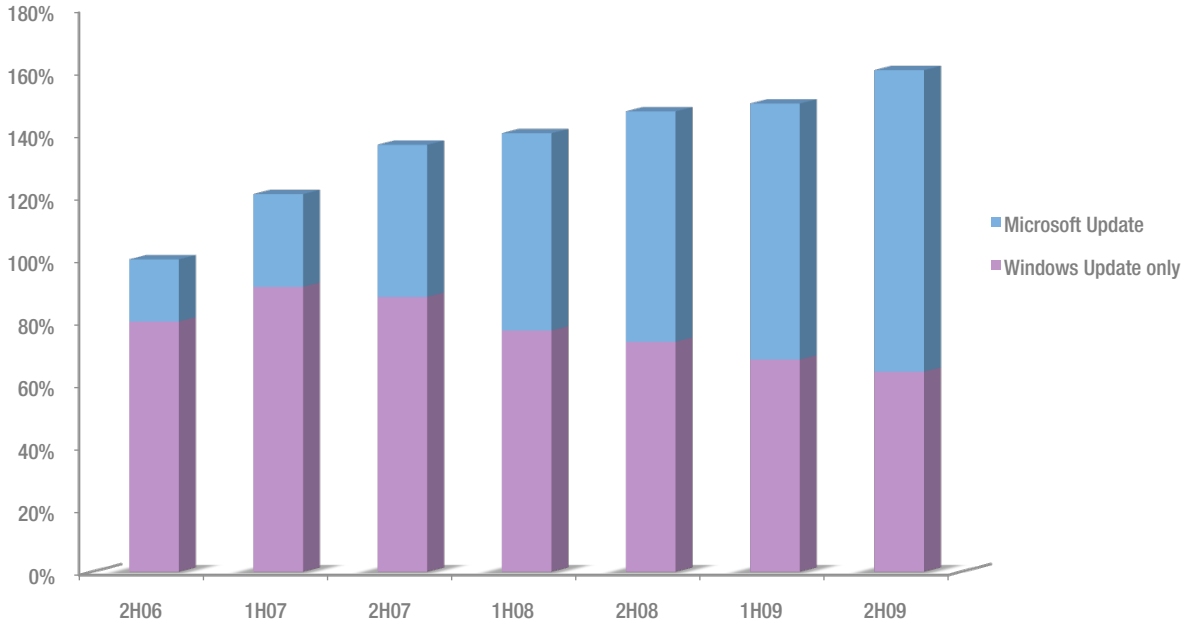
For end users, Microsoft provides two update services that the update clients can use:

- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft anti-malware products and the monthly release of the MSRT. To help secure users against exploitation, Microsoft also uses Windows Update to distribute *kill bits* that prevent certain vulnerable add-ons from running in Internet Explorer.[11] By default, when the user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software serviced through Microsoft Update or at the Microsoft Update Web site (http://update.microsoft.com/microsoftupdate).

[11] See http://support.microsoft.com/kb/240797 for more information about kill bits. While Microsoft does not currently provide third-party non-driver software updates directly through its update services, the Microsoft Vulnerability Research (MSVR) program does notify vendors of potential vulnerabilities in their respective products and assists in the determination of next steps and servicing.

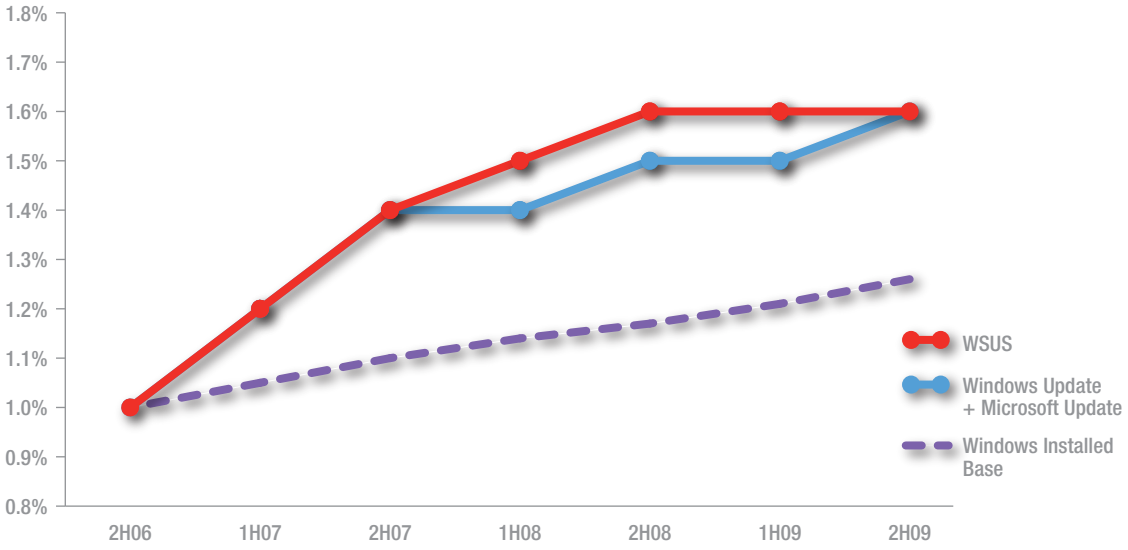
As Figure 41 shows, Microsoft Update adoption has risen significantly over the past several years, with the number of computers using the more comprehensive service increasing by more than 16 percent since 1H09.

FIGURE 41. Usage of Windows Update and Microsoft Update, 2H06–2H09, indexed to 2H06 total usage



Enterprise customers can use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to provide update services for their managed computers. As Figure 42 shows, end-user update service usage and the number of WSUS servers managing updates have both grown faster than the Windows installed base since 2H06, indicating that users are choosing to enable updating on existing Windows installations and on new ones.

FIGURE 42. Relative growth in Microsoft WSUS and end-user update services, 2H06–2H09, indexed to 2H06



Windows Update and Microsoft Update experienced their highest relative rate of increase in 2H09, due in part to the release of Windows 7, which has had relatively high opt-in rates for automatic updating. The overall number of WSUS servers declined during this period as administrators completed migrations to WSUS 3.0, the latest version, and decommissioned their WSUS 2 servers.

Updates and Supportability

The Microsoft Support Lifecycle (MSL) policy defines how Microsoft offers support and updates for business and developer software products, including Windows operating systems and service packs. Originally announced in 2002, the MSL provides predictable and consistent worldwide support timelines for Microsoft products.[12]

The following Microsoft operating systems will be affected by Support Lifecycle milestones in 2010:

- **On April 13, 2010, Windows Vista RTM** reached End of Support. Installation of Windows Vista SP1 (SP2 is recommended) is required to continue receiving support and new updates.
- **On July 13, 2010, Windows XP SP2** will reach End of Support. Installation of Windows XP SP3 is required to continue receiving support and new updates.
- **On July 13, 2010, Windows 2000** will transition from Extended Support to End of Life. Customers will need to migrate to a supported operating system to continue getting new updates and support.
- **On July 13, 2010, Windows Server 2003** will transition from Mainstream Support to Extended Support. Customers will need to pay for incident support and hotfix services or migrate to a supported operating system. Security updates are offered in Extended Support.

Customers impacted by the service pack support milestones should use Windows Update or the Microsoft Update Web site (on Windows XP and Windows Server 2003) to update to the latest service pack level and install other available security updates. Customers affected by operating system end-of-support milestones should migrate to a supported operating system.

[12] See http://support.microsoft.com/gp/lifepolicy for more information about the MSL.

Microsoft Malware Protection Center

The Microsoft Malware Protection Center (MMPC) is the group at Microsoft that researches and responds to malware and potentially unwanted software. The MMPC provides the Microsoft Malware Protection Engine, the technology that underlies most Microsoft anti-malware security products and services. The Microsoft Malware Protection Engine relies on constantly updated definition files containing detection signatures for thousands of different malware and potentially unwanted software families. To develop these definition files and to respond quickly and effectively to new threats, the MMPC maintains research and response labs in the United States, Ireland, and Australia, with additional researchers in other locations.

The MMPC uses a number of different mechanisms to disseminate malware and security information to the public. The center maintains the MMPC Portal (http://www.microsoft.com/security/portal), a central source for malware and security information, definition updates, and malware sample submissions. The MMPC Portal includes an encyclopedia that provides detailed analyses of thousands of current threats, including technical information about the threat, how readers can tell if they are infected, and how to recover from the threat or avoid exposure to it altogether. (The threat descriptions that appear in marginal callouts throughout this report are condensed from the MMPC Portal encyclopedia). MMPC researchers also publish a blog at http://blogs.technet.com/mmpc, which they use to communicate with the public directly about topics such as current malware outbreaks, security conferences, and other security-related issues.

Malware and Potentially Unwanted Software Trends

In general, the malware landscape in 2H09 is marked by a greater diversity of moderately prevalent families than in the past. Earlier periods often had one or two threats dominating the top of the list with very large numbers of removals, with all other families far behind. As more computer users around the world take advantage of anti-malware tools and update or replace older, less secure versions of software, malware authors have been forced to change their tactics in an effort to defeat security measures.

Except where specified, the data in this section has been compiled from telemetry generated from more than 500 million computers worldwide by a number of different Microsoft security tools and services, including the MSRT, Microsoft Security Essentials, Windows Defender, Microsoft Forefront Client Security, Windows Live OneCare, and the Windows Live OneCare safety scanner. See "Appendix B: Data Sources," beginning on page 238, for more information on these tools.

For an explanation of the names used for malware and potentially unwanted software, see "Appendix A: Threat Naming Conventions" on page 236.

Infection Rates and CCM

To produce a consistent measure of infection that can be used to compare different populations of computers to each other, infection rates in this report are expressed using a metric called *computers cleaned per thousand*, or *CCM*, which represents the number of reported computers cleaned for every 1,000 executions of the MSRT. (The *M* in CCM stands for *mille*, the Latin word for *thousand*.) For example, if the MSRT has 50,000 executions in a particular location in July and removes infections from 200 computers, the CCM infection rate for that location in July is 4.0 (200 ÷ 50,000 × 1,000). A new version of the MSRT is released every month, so figures for multiple months, or for 2H09 as a whole, are derived by averaging the CCM for each month in the period. The MSRT data is used to calculate CCM because the tool's global reach, large installed base, and regularly scheduled release facilitate a consistent comparison of relative infection rates between different populations of computers.

Geographic Trends

The telemetric data generated by Microsoft security products includes information about the location of the system, as determined by the setting of the **Location** tab or menu in **Regional and Language Options** in the Control Panel. This data makes it possible to compare infection rates, patterns, and trends in different locations around the world. ("Malware Patterns Around the World," beginning on page 129, includes more in-depth information about the threat landscapes in many of the locations listed here.)

FIGURE 43. The 25 locations with the most computers cleaned by Microsoft desktop anti-malware products in 2H09

Rank	Region	Computers Cleaned (2H09)	Computers Cleaned (1H09)	Change
1	United States	15,383,476	13,971,056	10.1% ▲
2	China	3,333,368	2,799,456	19.1% ▲
3	Brazil	2,496,674	2,156,259	15.8% ▲
4	United Kingdom	2,016,132	2,043,431	-1.3% ▼
5	Spain	1,650,440	1,853,234	-10.9% ▼
6	France	1,538,749	1,703,225	-9.7% ▼
7	Korea	1,367,266	1,619,135	-15.6% ▼
8	Germany	1,130,632	1,086,473	4.1% ▲
9	Canada	967,381	942,826	2.6% ▲
10	Italy	954,617	1,192,867	-20.0% ▼
11	Mexico	915,786	957,697	-4.4% ▼
12	Turkey	857,463	1,161,133	-26.2% ▼
13	Russia	677,601	581,601	16.5% ▲
14	Taiwan	628,202	781,214	-19.6% ▼
15	Japan	609,066	553,417	10.1% ▲
16	Netherlands	565,248	494,997	14.2% ▲
17	Poland	555,242	551,419	0.7% ▲
18	Australia	463,768	416,435	11.4% ▲
19	Portugal	437,707	375,502	16.6% ▲
20	Sweden	239,711	197,242	21.5% ▲
21	Belgium	210,298	208,627	0.8% ▲
22	Saudi Arabia	196,908	205,157	-4.0% ▼
23	Colombia	186,389	183,994	1.3% ▲
24	Denmark	175,734	160,001	9.8% ▲
25	Greece	167,934	161,639	3.9% ▲
Worldwide		**41,024,375**	**39,328,515**	**4.3% ▲**

As Figure 43 shows, the number of computers cleaned in individual countries/regions can vary quite a bit from period to period. Increases in the number of cleaned computers can be caused not only by increased prevalence of malware in that country, but also by new installations of Microsoft anti-malware solutions. Large numbers of new installations are likely to increase the number of computers cleaned. Conversely, using the SmartScreen feature in Internet Explorer 8 can block some malware downloads before they can be installed, reducing the number of detections and cleanings.

Two of the largest increases in this Figure are for China and Brazil, which increased 19.1 percent and 15.8 percent from 1H09, respectively. Much of this increase is due to the September 2009 release of Microsoft Security Essentials, an anti-malware solution for home computers that is available at no charge to licensed users of Windows. China and Brazil have both been strong early adopters of Security Essentials, localized versions of which have been available in both locations since launch day. Data from other Microsoft anti-malware tools for China and Brazil remained roughly consistent from 1H09 to 2H09, suggesting that many new users of Security Essentials in those areas had not been actively using anti-malware software before. (Infection figures for new users of anti-malware software are typically higher than average because the software often detects large amounts of previously undiscovered malware on the formerly unprotected computers.)

A number of other locations saw significant decreases. The largest decline in this Figure is the 26.2 percent decrease in Turkey, which can be mainly attributed to the decreased prevalence of Win32/Taterf and Win32/Frethog, two threats that target players of online games.[13] Local authorities and service providers in Turkey made notable strides in mitigating Taterf infections in 2H09 as part of an ongoing community-based response effort. Likewise, decreases in Taterf and Frethog led to a 19.6 percent decrease for Taiwan. Italy's 20.0 percent decline is mostly due to a steep decline in detections of the Trojan family Win32/Wintrim.

Despite the global nature of the Internet, there are significant differences in the types of threats that affect users in different parts of the world. The spread and effectiveness of malware are highly dependent on language and cultural factors, in addition to the methods used for distribution. Some threats are spread using techniques that target people who speak a particular language or who use services that are local to a particular geographic region. Others target vulnerabilities or operating system configurations and applications that are unequally distributed around the globe. As a result, security researchers face a threat landscape that is much more complex than a simple examination of the biggest threats worldwide would suggest. Figure 44 illustrates the infection rates of locations around the world, expressed in CCM. See page 71 for an explanation of the CCM metric.

Encyclopedia

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

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

Win32/Wintrim: A family of trojans that display pop-up advertisements depending on the user's keywords and browsing history. Its variants can monitor the user's activities, download applications, and send system information back to a remote server.

http://www.microsoft.com/av

[13] For more information about this class of threat, see "Online Gaming-Related Families" on page 62 of *Microsoft Security Intelligence Report, Volume 5 (January through June 2008)*.

FIGURE 44. Infection rates by country/region in 2H09

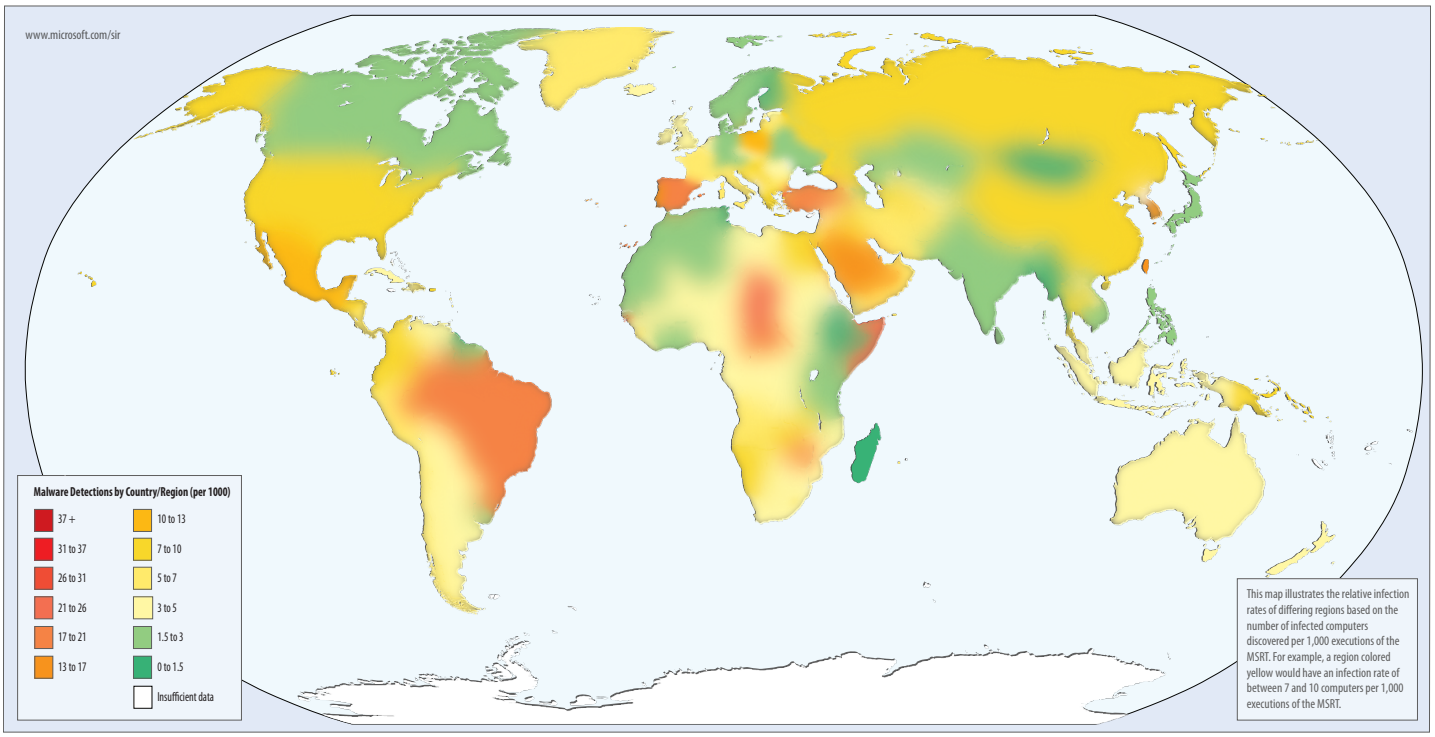


Figure 45 shows the infection rates for the world as a whole, and for locations around the world with at least 1 million average monthly MSRT executions in 2H09, derived by averaging each location's monthly CCM for each of the six months in the period. See "Malware Patterns Around the World" on page 129 for a more comprehensive list with 213 locations, and for an in-depth look at the threat landscapes for 26 locations around the world, encompassing every inhabited continent and multiple languages and computer usage patterns.

FIGURE 45. Infection rates (CCM) for locations around the world with at least 1 million average monthly MSRT executions in 2H09

Country/Region	CCM (2H09)
Argentina	4.7
Australia	3.4
Austria	1.7
Belgium	3.3
Brazil	18.0
Canada	2.5
Chile	6.7
China	7.0
Colombia	9.1
Czech Republic	4.1
Denmark	2.5
Finland	1.4
France	5.6
Germany	2.2
Greece	7.7
Hong Kong S.A.R.	6.0
Hungary	8.9
India	2.6
Ireland	3.5
Israel	7.3
Italy	5.3
Japan	2.3
Korea	16.0
Malaysia	4.0

Country/Region	CCM (2H09)
Mexico	10.0
Netherlands	3.3
New Zealand	3.0
Norway	2.5
Peru	6.4
Philippines	1.7
Poland	11.0
Portugal	13.6
Romania	4.0
Russia	9.8
Saudi Arabia	13.0
Singapore	4.6
Slovakia	4.5
South Africa	4.8
Spain	17.1
Sweden	2.8
Switzerland	2.3
Taiwan	16.7
Thailand	9.8
Turkey	20.0
Ukraine	2.9
United Kingdom	4.1
United States	7.8
Venezuela	4.5
Worldwide	**7.0**

Figure 46 and Figure 47 offer a closer look at these geographic statistics, listing the 25 locations with the lowest infection rates and the 25 locations with the highest infection rates in 2H09, respectively, among locations with at least 100,000 average monthly MSRT executions.

FIGURE 46. Locations with the lowest infection rates, by CCM, in 2H09 (100,000 monthly MSRT executions or more)

Rank	Country/Region	CCM (2H09)
1	Réunion	1.3
2	**Finland**	**1.4**
3	Tunisia	1.4
4	Algeria	1.5
5	Belarus	1.5
6	**Austria**	**1.7**
7	Senegal	1.7
8	**Philippines**	**1.7**
9	Morocco	1.8
10	Vietnam	1.8
11	Kazakhstan	1.8
12	Kenya	1.9
13	Macao S.A.R.	2.0
14	Guadeloupe	2.2
15	Pakistan	2.2
16	**Germany**	**2.2**
17	Jamaica	2.3
18	**Switzerland**	**2.3**
19	**Japan**	**2.3**
20	Puerto Rico	2.4
21	**Norway**	**2.5**
22	**Denmark**	**2.5**
23	**Canada**	**2.5**
24	**India**	**2.6**
25	Uruguay	2.6

(**Bold text** indicates countries and regions with more than one million average monthly MSRT executions.)

FIGURE 47. Locations with the highest infection rates, by CCM, in 2H09 (100,000 monthly MSRT executions or more)

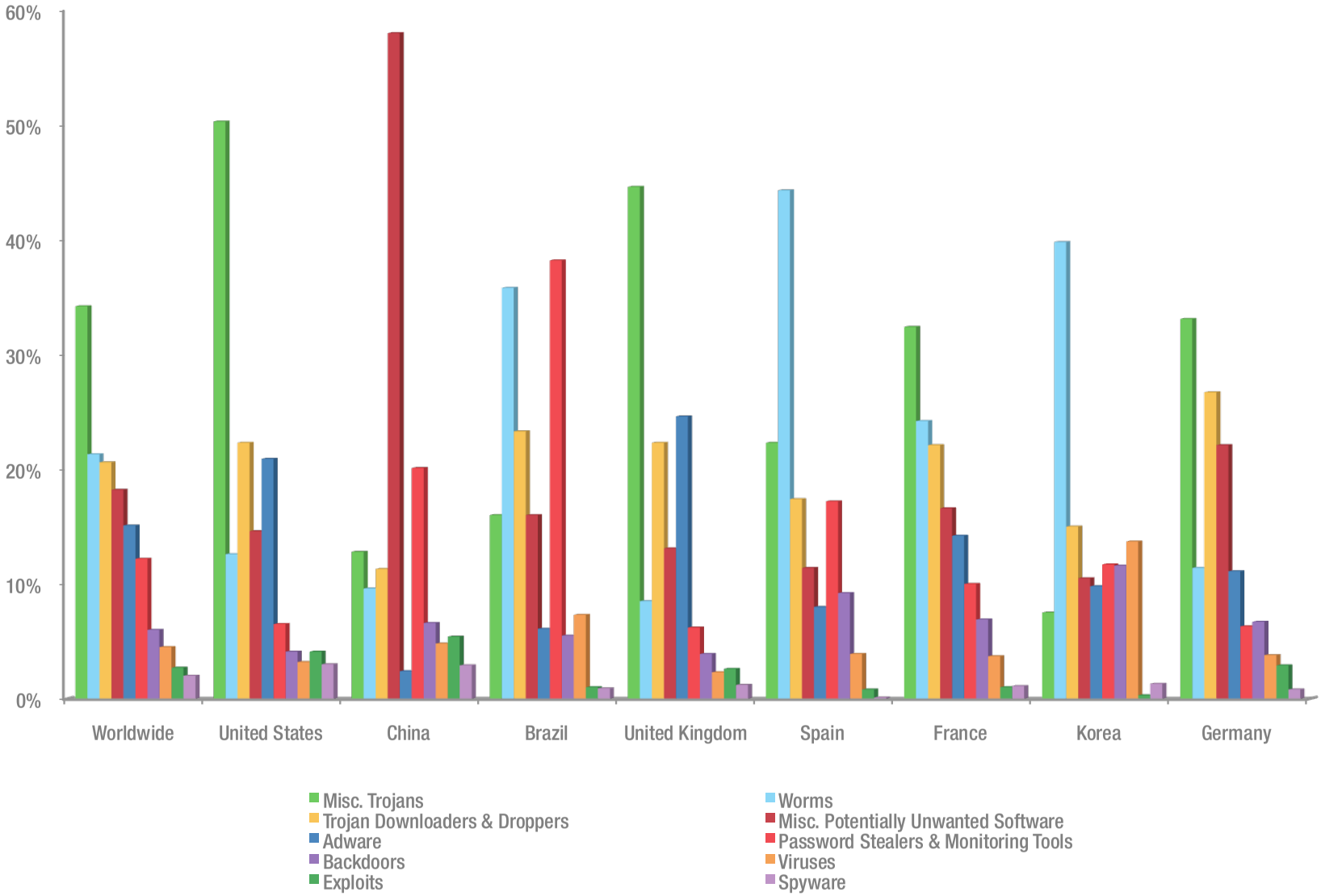
Rank	Country/Region	CCM (2H09)
1	**Turkey**	**20.0**
2	**Brazil**	**18.0**
3	**Spain**	**17.1**
4	**Taiwan**	**16.7**
5	**Korea**	**16.0**
6	**Portugal**	**13.6**
7	**Saudi Arabia**	**13.0**
8	Guatemala	12.5
9	**Poland**	**11.0**
10	**Mexico**	**10.0**
11	**Russia**	**9.8**
12	**Thailand**	**9.8**
13	Kuwait	9.3
14	El Salvador	9.2
15	Honduras	9.1
16	Colombia	9.1
17	**Hungary**	**8.9**
18	Croatia	8.9
19	Egypt	8.6
20	Serbia and Montenegro*	8.1
21	**United States**	**7.8**
22	**Greece**	**7.7**
23	Ecuador	7.6
24	**Israel**	**7.3**
25	**China**	**7.0**

(**Bold text** indicates countries and regions with more than one million average monthly MSRT executions.)

* Figure reflects the combined markets of Montenegro and Serbia for 2H09.

Infection data from several Microsoft security products for some of the more populous locations around the world demonstrates the highly localized nature of malware and potentially unwanted software. Figure 48 shows the relative prevalence of different categories of malware and potentially unwanted software in the eight locations with the most computers cleaned in 2H09, expressed as percentages of the total number of computers cleaned in each location. (The sum of the totals for each location may exceed 100 percent because some computers have more than one category of threat removed from them during each time period.) See page 79 for an explanation of the categories used in this figure.

FIGURE 48. Threat categories worldwide and in the eight locations with the most infected computers, by incidence among all computers cleaned by Microsoft desktop anti-malware products, in 2H09



- The threat environments in the **United States** and the **United Kingdom** are very similar. Both locations have nearly the same proportion of threat categories, and 7 of the top 10 families in each location are the same. Miscellaneous Trojans account for the largest single category of threat, with families such as Win32/FakeXPA, Win32/Renos, and Win32/Alureon ranking high in both locations.
- In **China**, many of the most prevalent threats are localized families that don't appear in the list of top threats for any other location. These include some versions of Win32/BaiduSobar, a Chinese-language browser toolbar, and password stealers like Win32/Lolyda and Win32/Ceekat that target several online games that are popular in China.
- In **Brazil**, Password Stealers & Monitoring Tools is the most common category, due primarily to a number of Portuguese-language password stealers that target online users of Brazilian banks, led by Win32/Bancos.
- **Korea** is dominated by worms, led by Win32/Taterf, which targets players of online games. The prevalence of Taterf in Korea may be due in part to the worm's propensity to spread easily in Internet cafés and LAN gaming centers, which are popular in Korea. See "Online Gaming-Related Families," on page 62 of *Microsoft Security Intelligence Report, Volume 5 (January through June 2008)*, for more information about the methods of propagation used by Win32/Taterf and related families.

Category Trends

As explained in "Appendix A: Threat Naming Conventions" on page 236, the MMPC classifies individual threats into types based on a number of factors, including how the threat spreads and what it is designed to do. To simplify the presentation of this information and make it easier to understand, the *Security Intelligence Report* groups these types into 10 categories based on similarities in function and purpose. For example, the TrojanDownloader and TrojanDropper types are combined into a single category, called Trojan Downloaders & Droppers.

Encyclopedia

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

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

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

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

Win32/Lolyda: A family of trojans that sends account information from popular online games to a remote server. They may also download and execute arbitrary files.

Win32/Ceekat: A collection of trojans that steal information such as passwords for online games, usually by reading information directly from running processes in memory. Different variants target different processes.

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

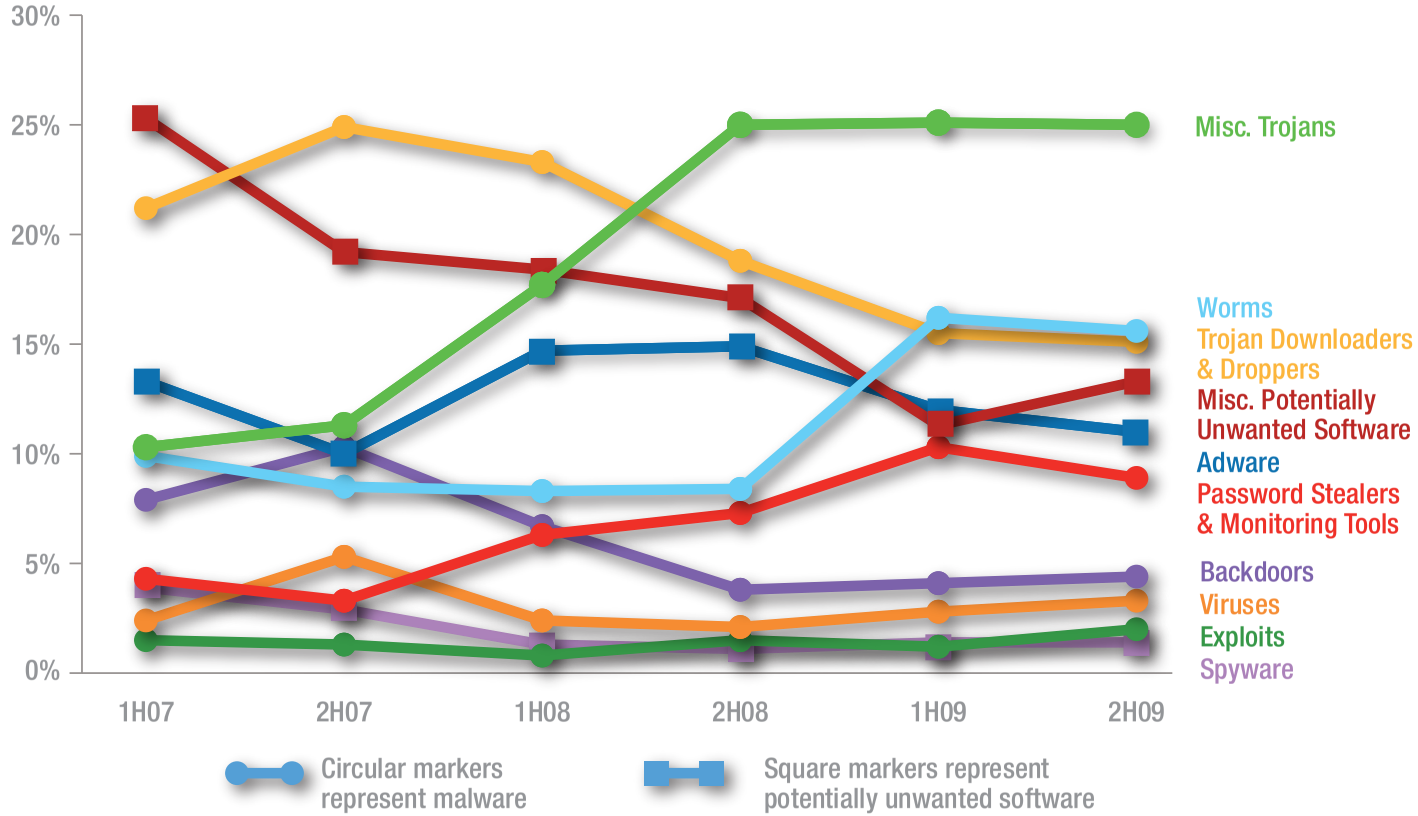
Win32/Taterf: A family of worms that spread through mapped drives to steal login and account details for popular online games.

http://www.microsoft.com/av

Malware categories often overlap, and many threat families exhibit characteristics of multiple categories. To produce the information and figures in this section, each threat has been associated with the single category that Microsoft security analysts determine to be most appropriate for the threat. The Miscellaneous Trojans category consists of all trojans that are not categorized as Trojan Downloaders & Droppers, including some rogue security software families. The Miscellaneous Potentially Unwanted Software category consists of all potentially unwanted software that is not categorized as Adware or Spyware, such as browser modifiers and remote control software. See the Glossary, beginning on page 240, for definitions of the other categories described in this section.

Figure 49 shows the relative prevalence of different categories of malware and potentially unwanted software since 2007, expressed as a percentage of the total number of computers cleaned by all Microsoft security products during each time period. Totals may exceed 100 percent for each time period because some computers are cleaned of more than one category of threat during each time period.

FIGURE 49. Computers cleaned by threat category, by percentage of all infected computers, 1H07–2H09



Encyclopedia

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

Win32/Yektel: A family of trojans that display fake warnings of spyware or malware in an attempt to lure the user into installing or paying money to register rogue security software programs such as Win32/FakeXPA.

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

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

http://www.microsoft.com/av

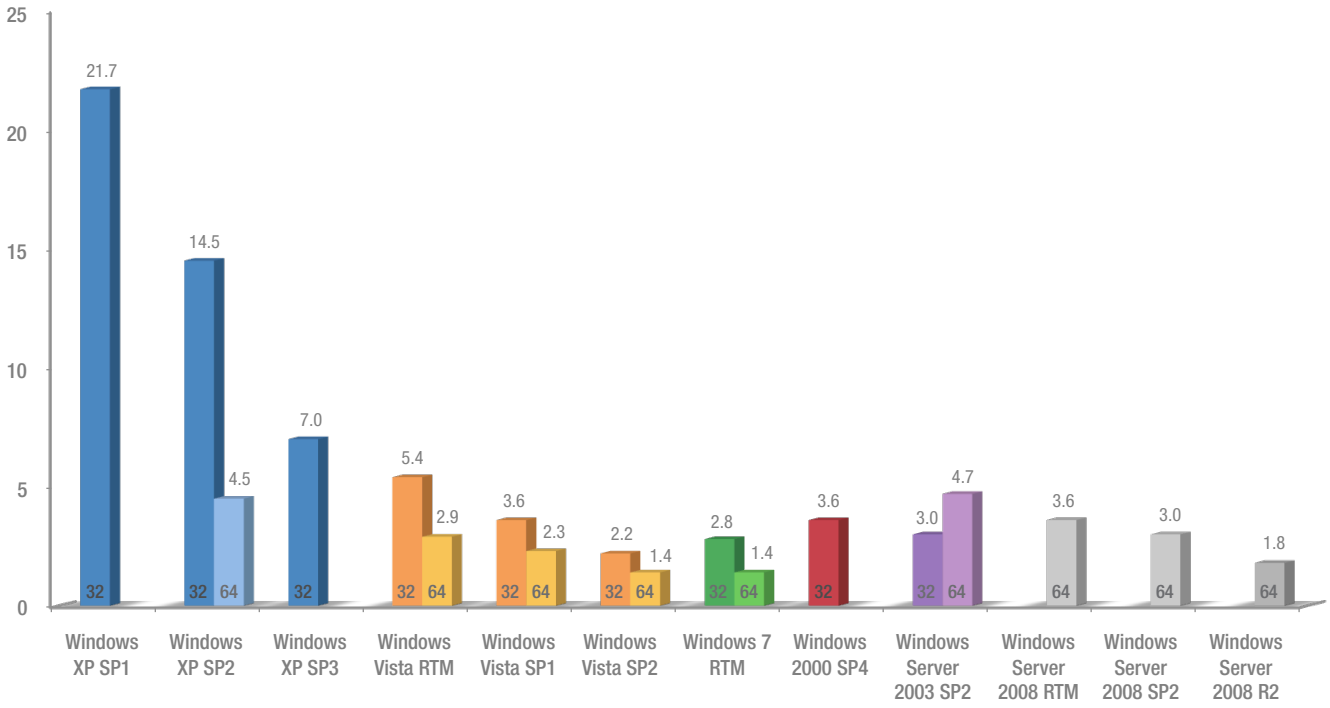
The relative prevalence of each category remained unusually stable in 2H09, with no category varying by more than 2.0 percent from its 1H09 share. Miscellaneous Trojans remained the most prevalent category in 2H09, for the third straight period, due in large part to the persistence of rogue security software families like Win32/FakeXPA and Win32/Yektel. (See "Rogue Security Software" on page 95 for more information). Worms, the second-most prevalent category, fell slightly in relative terms in 2H09, reversing the category's dramatic growth trend observed between 2H08 and 1H09. This reversal is largely due to the diminished prevalence of Win32/Conficker, which was the most common family worldwide in 1H09 but which fell to fifth in the second half of the year.

Miscellaneous Potentially Unwanted Software reversed a multiyear trend of relative declines to show the largest relative increase in 2H09, largely because of the prevalence of the new family Win32/Zwangi. Trojan Downloaders & Droppers, Adware, and Password Stealers & Monitoring Tools all had slight relative declines, and the other categories remained both stable and relatively rare.

Operating System Trends

The features and updates 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 seen with different versions and service packs. Figure 50 shows the infection rate for each Windows operating system/service pack combination that accounted for at least 0.1 percent of total MSRT executions in 2H09. (Note that this data is normalized: The infection rate for each version of Windows is calculated separately, and the infection rate for a version is not affected by the number of computers running it. See page 71 for a definition of the CCM metric used to calculate infection rates.)

FIGURE 50. Number of computers cleaned for every 1,000 MSRT executions, by operating system, in 2H09



("32" = 32-bit; "64" = 64-bit. Systems with at least 0.05 percent of total executions shown.)

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, which was released in 2H09, and Windows Vista with Service Pack 2 have the lowest infection rate of any platform on the chart. The 64-bit versions of Windows 7 and Windows Vista SP2 had lower infection rates (1.4 for both) than any other operating system configuration in 2H09, and the 32-bit versions both had infection rates that were less than half of Windows XP with its most up-to-date service pack, SP3.

For operating systems with service packs, each successive service pack has a lower infection rate than the one before it. The infection rate for Windows XP with SP3 is less than half of that for SP2, and less than a third of that for SP1. Similarly, Windows Vista SP2 has a lower infection rate than SP1, which has a lower infection rate than Windows Vista RTM. On the server side, the infection rate for Windows Server 2008 with SP2 is 3.0, which is 20 percent less than that of its predecessor, Windows Server 2008 RTM. There are two likely reasons for these trends:

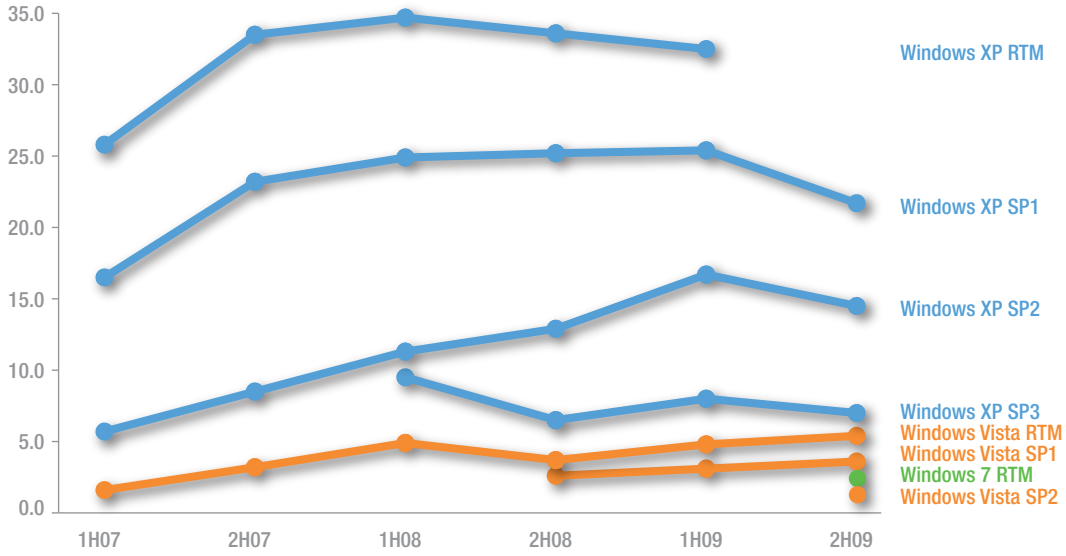
- Service packs include fixes for all security vulnerabilities fixed in security updates at the time of issue. They can also include additional security features, mitigations, or changes to default settings to protect users.
- Users who install service packs may generally maintain their computers better than users who do not install service packs and therefore may also be more cautious in the way they browse the Internet, open attachments, and engage in other activities that can open computers to attack.

Infection rates for the 64-bit versions of Windows XP, Windows Vista, and Windows 7 are lower than for the corresponding 32-bit versions of those platforms. The enhanced security features available in 64-bit versions of Windows, like Kernel Patch Protection ("PatchGuard") and Data Execution Prevention (DEP),[14] may be responsible for part of the difference. Another factor might be a higher level of technical expertise on the part of people who run 64-bit operating systems. This difference may be expected to decrease as 64-bit computing continues to make inroads among mainstream users. Microsoft original equipment manufacturer (OEM) partners are increasingly selling the 64-bit version of Windows Vista with mid-range and high-end desktop and laptop computers, and the infection rate differences between the 32-bit and 64-bit versions of Windows Vista and Windows 7 are correspondingly lower than that of Windows XP SP2. Notably, the infection rate for the 64-bit version of Windows Server 2003 SP2 is actually higher than that of the 32-bit version, which may be a reflection of the increasing dominance of 64-bit computing in the general server population and the accompanying relegation of 32-bit server platforms to specialized situations.

Figure 51 illustrates the consistency of these trends over time, showing infection rates for different configurations of the 32-bit versions of Windows XP and Windows Vista for each six-month period between 1H07 and 2H09.

[14] See http://www.microsoft.com/whdc/driver/kernel/64bitpatch_FAQ.mspx for more information about Kernel Patch Protection. DEP is available in 32-bit and 64-bit versions of Windows but is only enabled by default for 64-bit programs. See http://windows.microsoft.com/en-US/windows7/Data-Execution-Prevention-frequently-asked-questions for more information about DEP.

FIGURE 51. CCM trends for 32-bit versions of Windows XP and Windows Vista, 1H07–2H09



(Systems with at least 0.05 percent of total executions in each period shown.)

Infection rates as measured by the MSRT are greatly influenced by the selection of new families detected by the monthly releases of the tool, so upward or downward trends between periods can be misleading. However, the ratios between Windows XP and Windows Vista in different configurations demonstrate clearly that Windows Vista is significantly less susceptible to infection than Windows XP and has remained so since its introduction. Likewise, the first period of infection data for Windows 7, which shares and builds upon the security improvements introduced with Windows Vista, suggests that it, too, is likely to remain less susceptible to infection than Windows XP, even as larger segments of the computer-using population begin using the new operating system.

Malware and Potentially Unwanted Software Families

Figure 52 lists the top 25 malware and potentially unwanted software families that were detected on computers by Microsoft desktop security products in 2H09.

FIGURE 52. Top 25 malware and potentially unwanted software families detected by Microsoft anti-malware desktop products in 2H09

Rank	Family	Most Significant Category	2H09
1	Win32/Taterf	Worms	3,921,963
2	Win32/Renos†	Trojan Downloaders & Droppers	3,640,697
3	Win32/FakeXPA*	Miscellaneous Trojans	2,939,542
4	Win32/Alureon†	Miscellaneous Trojans	2,694,128
5	Win32/Conficker†	Worms	1,919,333 [15]
6	Win32/Frethog	Password Stealers & Monitoring Tools	1,823,066
7	Win32/Agent	Miscellaneous Trojans	1,621,051
8	Win32/BaiduSobar	Misc. Potentially Unwanted Software	1,602,230
9	Win32/GameVance	Adware	1,553,646
10	Win32/Hotbar	Adware	1,476,838
11	Win32/Yektel*	Miscellaneous Trojans	1,377,123
12	ASX/Wimad	Trojan Downloaders & Droppers	1,306,644
13	Win32/ZangoSearchAssistant	Adware	1,235,666
14	Win32/FakeSpypro*	Miscellaneous Trojans	1,193,737
15	Win32/Hamweq	Worms	967,436
16	Win32/Bancos	Password Stealers & Monitoring Tools	963,221
17	Win32/Winwebsec*	Miscellaneous Trojans	947,781
18	Win32/Vundo†	Miscellaneous Trojans	935,087
19	Win32/Autorun	Worms	754,168
20	Win32/Koobface†	Worms	753,695
21	Win32/PossibleHostsFileHijack	Misc. Potentially Unwanted Software	730,019
22	Win32/Zlob†	Trojan Downloaders & Droppers	670,924
23	Win32/C2Lop†	Miscellaneous Trojans	654,017
24	Win32/Bredolab	Trojan Downloaders & Droppers	635,277
25	Win32/DoubleD	Adware	630,965

(Asterisks [*] indicate rogue security software families. Daggers [†] indicate families that have been observed to download rogue security software.)

[15] The Shadowserver Foundation, which tracks active Win32/Conficker infections, reported that 4.6 million Conficker-infected computers were being tracked by Shadowserver-operated sinkholes on the last day of 2H09, down from 5.2 million on the last day of 1H09. Counting the amount of malware found and cleaned by anti-malware software can sometimes yield figures that are very different from estimates produced through observations of active infected computers, and there is no widespread agreement about which method is preferable.

Overall, detections of the top threats are down by a considerable margin from the first half of the year. In 1H09, seven families were removed from at least 2 million computers by Microsoft desktop anti-malware tools, compared to just four families in 2H09. Even Win32/Taterf, 2H09's top family, was removed from nearly 1 million fewer computers this period than in 1H09, when it ranked second behind Win32/Conficker—and the 3.9 million computers infected by Taterf in 2H09 pales in comparison to 1H08's top family, Win32/Zlob, which was removed from 9.0 million computers during that period.

The rapid adoption of Microsoft Security Essentials may have contributed to the decline in removals. Many attackers use trojan downloaders and trojan droppers, like Win32/Renos and ASX/Wimad (the second- and eleventh-most prevalent families in 2H09, respectively) to distribute other threats, such as botnets, rogues, and password stealers, to computers. Real-time anti-malware tools, including Microsoft Security Essentials, can often intercept and remove downloaders and droppers before they are able to install other threats (which therefore would not be present on the computer for desktop security products to detect). Likewise, browser protection features like the SmartScreen Filter in Internet Explorer 8 may be having a measurable amount of success in preventing users from ever being exposed to some threats at all. (See "Malicious Web Sites" beginning on page 116 for more information about the SmartScreen Filter.)

This list reflects the growing prevalence of families associated with rogue security software—programs that falsely claim to detect malware or other security problems on a victim's computer and offer to "fix" them for a price. Four of the top 25 families—Win32/FakeXPA, Win32/Yektel, Win32/Fakespypro, and Win32/Winwebsec— are rogue security software families. FakeXPA, Yektel, and Winwebsec are returnees from 1H09, when they ranked sixth, seventeenth, and twenty-first respectively; all three rose in the ranking in 2H09. FakeSpypro is a newer family, detections for which were added to the MSRT in July 2009.

User Reaction to Alerts

Software cannot always be classified in binary terms as "good" or "bad." Some software inhabits a gray area wherein the combination of behaviors and value propositions presented by the software is neither universally desired nor universally reviled. This gray area includes a number of programs that do things like display advertisements to the user that may appear outside the context of the Web browser or other application and that may be difficult or impossible to control. Many users consider some behaviors of these programs objectionable, but some may appreciate the advertisements or may wish to use other applications that come bundled with the advertising programs and that will not function if the advertising programs are not present. Microsoft refers to software in this gray area as *potentially unwanted software* and provides products and technologies to give visibility and control to the user.[16]

[16] Microsoft has published the criteria that the company uses to classify programs as potentially unwanted software at http://www.microsoft.com/windows/products/winfamily/defender/analysis.mspx. For programs that have been classified as potentially unwanted software, Microsoft provides a dispute resolution process to allow for reporting of potential false positives and to provide software vendors with the opportunity to request investigation of a rating with which they do not agree.

Encyclopedia

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

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

Win32/Zlob: A family of trojans that often pose as downloadable media codecs. When installed, Win32/Zlob displays frequent pop-up advertisements for rogue security software.

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

ASX/Wimad: A detection for malicious Windows Media files that can be used to encourage users to download and execute arbitrary files on an affected machine.

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

Win32/Yektel: A family of trojans that display fake warnings of spyware or malware in an attempt to lure the user into installing or paying money to register rogue security software programs such as Win32/FakeXPA.

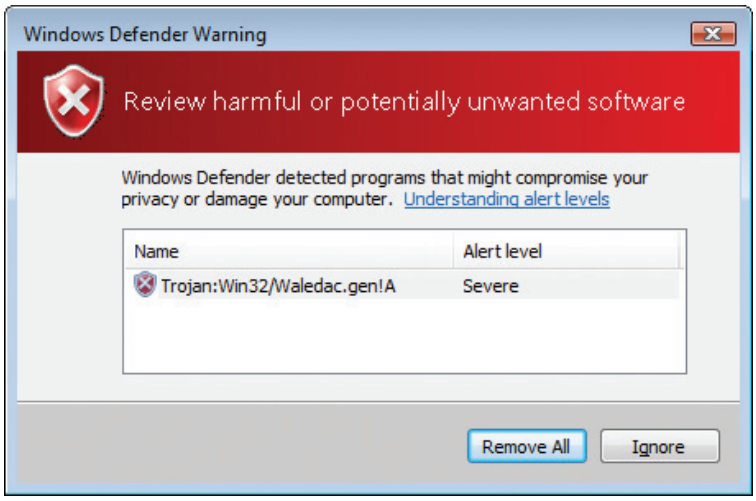
Win32/FakeSpypro: A rogue security software family distributed under the names Antivirus System PRO, Spyware Protect 2009, and others.

Win32/Winwebsec: A rogue security software family distributed under the names Winweb Security, System Security, and others.

http://www.microsoft.com/av

Many of the tools Microsoft provides for dealing with malware and potentially unwanted software are designed to allow users to make informed decisions about removing or retaining specific software, rather than to simply remove it outright. These tools give each of the families they track a severity rating of Low, Medium, High, or Severe, based on an objective analysis of the specific behaviors seen in the software. Threats rated High and Severe are removed automatically during scheduled scans. At other times, when the anti-malware software detects a potential threat, the user is given the opportunity to decide how the threat should be handled. Users can always choose to remove the threat immediately or to ignore it for the moment. Depending on the severity level of the threat and the anti-malware software being used, the software may present the user with additional choices as well.

FIGURE 53. A Windows Defender user action prompt for a threat rated Severe



- The user can remove a threat, eliminating it from the computer. Users can remove threats individually with the **Remove** option, or they can select **Clean computer** (variously, **Remove All**, **Clean System**, or **Clean All**, depending on the product used) to remove all threats that have been detected.
- For viruses, a **Clean** option is offered to remove the virus from the infected files and to leave the files on the computer, if possible.
- The user can quarantine the threat, disabling it in a way that allows it to be restored at a later time.
- If the user considers the detected item harmless or beneficial, he or she can choose the **Allow** option (variously, **Always allow** or **Ignore always**), so the anti-malware software will no longer consider it a threat.

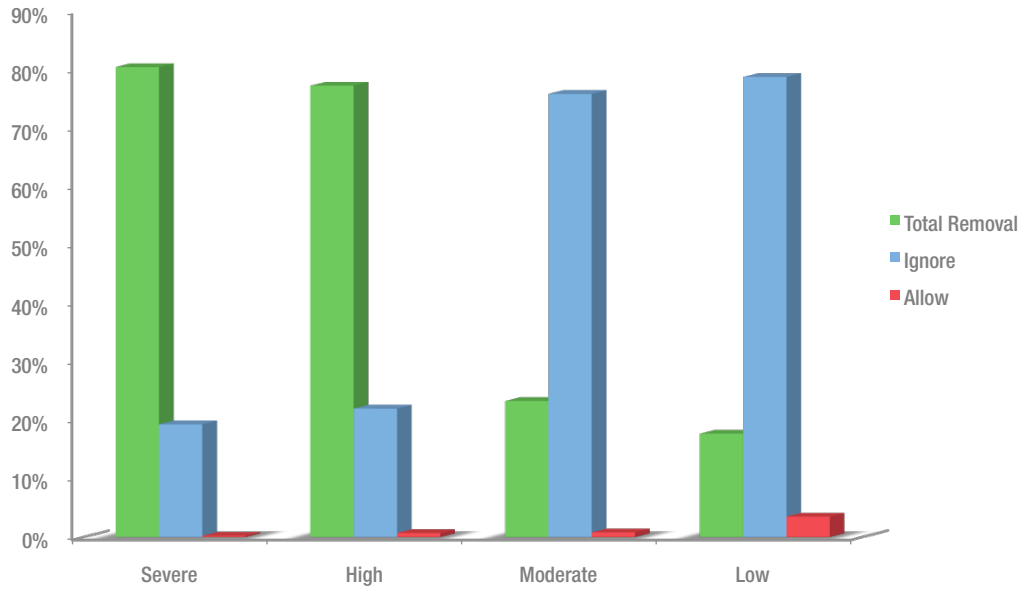
- The user can ignore the threat temporarily, deferring the decision to remove or allow it. Windows Defender provides an explicit **Ignore** option that the user can select. A user can also implicitly ignore a threat by clicking the window's **Close** button when asked to make a decision. Users may choose to ignore an alert multiple times for the same detected item.

For threats ranked Severe or High, the tool recommends the **Remove** option. For threats ranked Medium or Low, no recommendation is given, and the user must select the desired action when dealing with threats individually. (Selecting **Clean computer** or an equivalent action removes all detected items, regardless of any recommendations.)

Users are influenced by a number of factors when dealing with detected threats, such as their level of expertise, how certain they feel about their judgment regarding the software in question, the context in which the software was obtained, societal considerations, and the benefit (if any) being delivered by the software or by other software that is bundled with it. Users make choices about what to do about a piece of potentially unwanted software for different reasons, so it's important not to draw unwarranted conclusions about their intent. For instance, **Remove** and **Quarantine** usually indicate that the user is making an active choice to eliminate the software. **Allow** usually suggests that the user wants to keep the software. However, users choose to ignore threats for a variety of reasons. For example, they might be confused by the choices, they might want to defer the action to a more convenient time, or they might want to spend more time evaluating the software before making a decision.

Figure 54 shows the actions users took in 2H09 in response to threats labeled Severe, High, Moderate, and Low.

FIGURE 54. User action by threat severity in 2H09



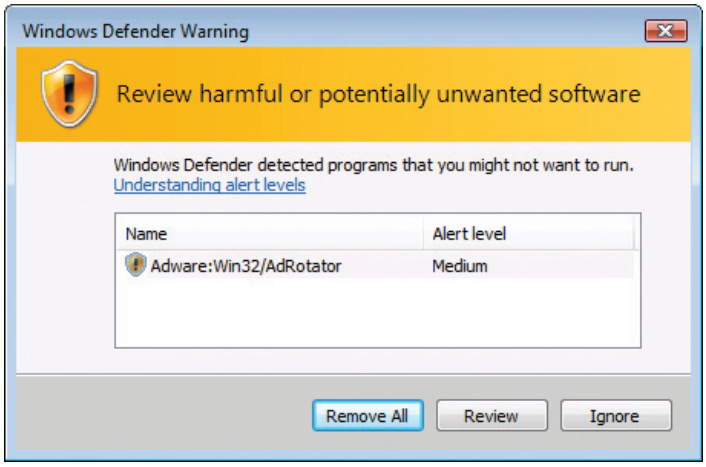
A few important points to keep in mind when interpreting Figure 54 above and Figure 56 on page 91:

- "Total Removal" includes cases in which the user selected **Clean computer** or an equivalent action to remove all detected items together and cases in which the user dealt with threats individually using the **Remove**, **Clean**, and **Quarantine** options.
- By default, threats rated High and Severe are automatically removed after scheduled scans, without the user being asked to make a choice.
- The large number of Ignore events recorded is due in part to the fact that users can choose to repeatedly ignore alerts pertaining to the same detected item, which causes an Ignore event to be recorded each time.

The data shows that users overwhelmingly choose to remove threats labeled Severe and High. As shown in Figure 53, the user interfaces of Microsoft desktop anti-malware utilities present these threats in a negative light. The color red is used prominently to inform users of Severe and High threats, appearing in banners and icons to connote danger. The user is given the opportunity to see detailed information and recommendations about the threat, and an appropriate removal action is preselected as the default choice.

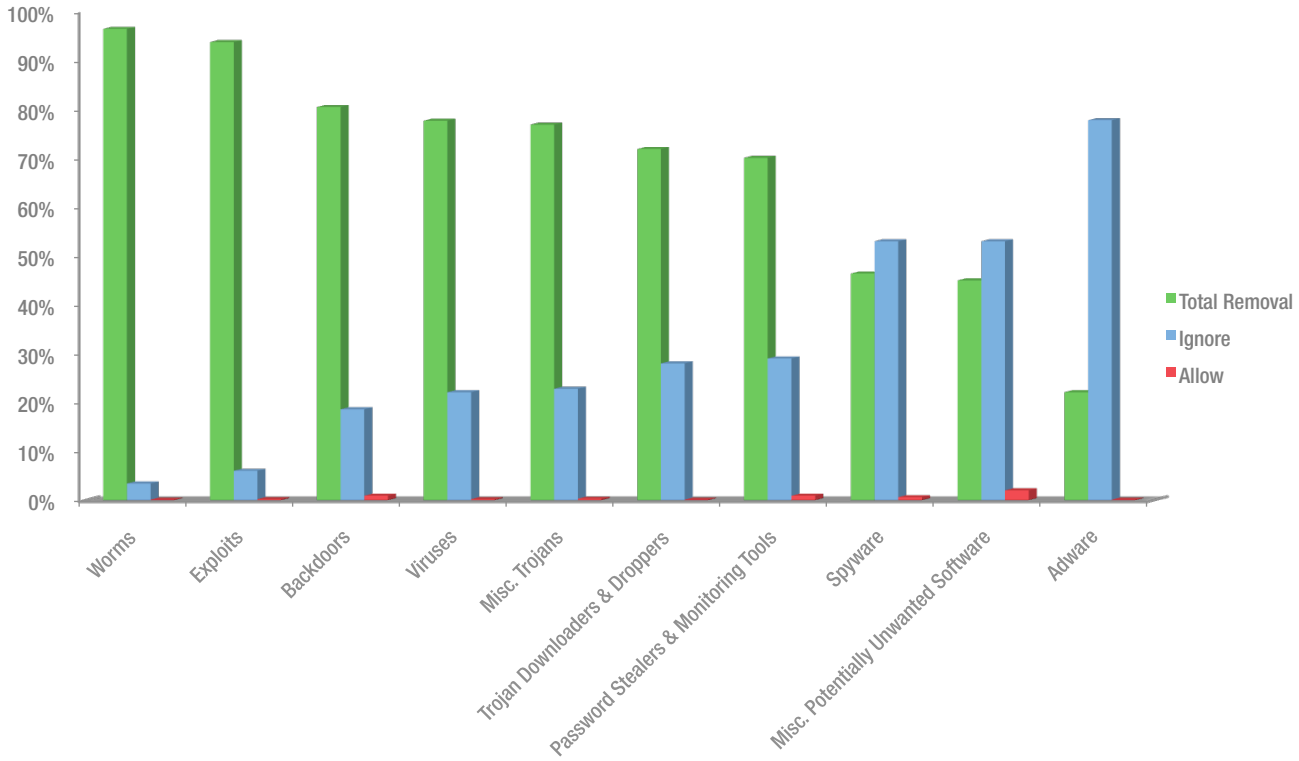
By contrast, users are more likely to ignore threats labeled Medium and Low. The user interface presents these threats with more nuanced graphics and descriptions than Severe and High threats, as seen in Figure 55. Medium and Low threats are associated with the color yellow, connoting caution rather than danger. The text used to identify and describe the nature of the threat is also softer and often places more emphasis on user choice than on clear, identified danger.

FIGURE 55. A Windows Defender user action prompt for a threat rated Medium



The nature of the detected threat also tends to have an effect on user actions, as illustrated by Figure 56.

FIGURE 56. User action by threat category in 2H09



All of the most frequently removed categories are malware categories. Most threats in these categories have alert levels of Severe or High, and the categories used to classify these threats have names that are well-known to large segments of the computing public or have clear negative connotations—virus, worm, backdoor, trojan.

The three potentially unwanted software categories (Spyware, Miscellaneous Potentially Unwanted Software, and Adware) have the fewest removal actions and the most Ignore actions, suggesting that many users accept the value propositions presented by such programs and believe their benefits outweigh any specific behaviors that other people may not want.

Notably, Allow appears very infrequently in the data, accounting for no more than 2 percent of any category. Some users may not understand that an **Allow** option is available for software they want to keep. For example, real-time protection alerts, like the ones shown in Figure 53 and Figure 55, typically offer a simplified set of choices, and the user must request additional information to see the full list of options. Other users may prefer to ignore the alert, in some cases repeatedly, rather than take an action with more perceived finality.

Trends in Sample Proliferation

Malware authors attempt to evade detection by continually releasing new variants in an effort to outpace the release of new signatures by antivirus vendors. Counting unique samples is one way to determine which families and categories of malware are currently most active (in other words, which families and categories are currently being most actively worked on by their developers) and how effective such activity is in helping malware developers reach their goal of infecting large numbers of computers.

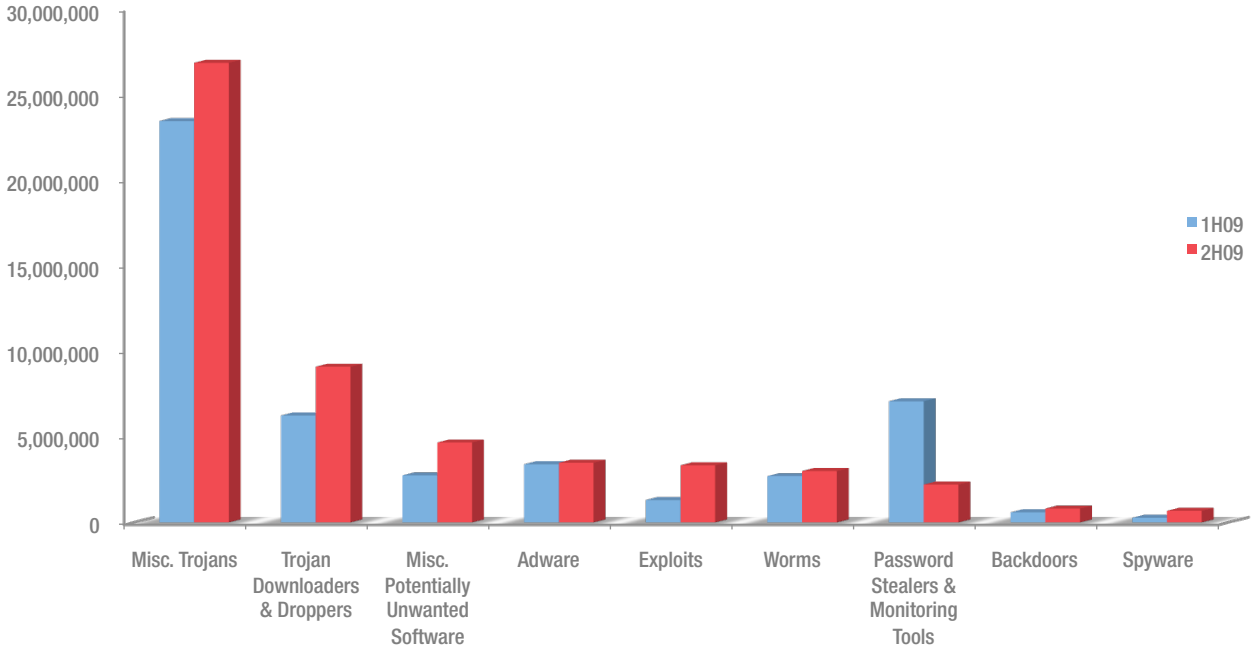
More than 126 million malicious samples were detected in the wild in 2H09. Figure 57 lists the number of unique files detected in each category of threat by Microsoft security products in 2H09, not including damaged or corrupted samples. (Malware often creates corrupted samples when replicating. These samples cannot affect users and are not counted when analyzing samples.)

FIGURE 57. Unique samples by category, 1H09–2H09

Category	2H09	1H09	Difference
Viruses	71,991,221	68,008,496	5.9% ▲
Miscellaneous Trojans	26,881,574	23,474,539	14.5% ▲
Trojan Downloaders & Droppers	9,107,556	6,251,286	45.7% ▲
Misc. Potentially Unwanted Software	4,674,336	2,753,008	69.8% ▲
Adware	3,492,743	3,402,224	2.7% ▲
Exploits	3,341,427	1,311,250	154.8% ▲
Worms	3,006,966	2,707,560	11.1% ▲
Password Stealers & Monitoring Tools	2,217,902	7,087,141	-68.7% ▼
Backdoors	812,256	589,747	37.7% ▲
Spyware	678,273	269,556	151.6% ▲
Total	**126,204,254**	**115,854,807**	**8.9% ▲**

Continued on next page

FIGURE 57. Continued



(Graph excludes virus samples.)

The decrease in the Password Stealers & Monitoring Tools category was primarily due to Win32/Lolyda, which declined from 5.7 million samples in 1H09 to less than 100,000 in 2H09. The increase in the Spyware category was driven by Win32/ShopAtHome, which had nearly five times as many unique samples in 2H09 as in the prior period.

The high number of virus samples is due to the fact that viruses can infect many different files, each of which is a unique sample. Sample counts for viruses should therefore not be taken as an indication of large numbers of true variants for these families.

Another factor that tends to inflate the sample count for certain families is *polymorphism*, which results in the automatic creation of large numbers of unique (but functionally identical) files as part of the malware replication process. There are two general types of polymorphism that affect sample counts:

- **Server-side polymorphism**, in which a server is configured to serve a slightly different version of a file every time it is accessed, typically in an effort to foil detection signatures. This can result in hundreds or thousands of files with different hash values but identical functionality being detected, which inflates the number of samples.
- **Malware polymorphism**, in which the malware itself changes slightly every time it replicates, possibly by changing the file name of a component to a new random value, or by encrypting or compressing it in a slightly different way.

Encyclopedia

Win32/Lolyda: A family of trojans that sends account information from popular online games to a remote server. They may also download and execute arbitrary files.

Win32/ShopAtHome: A browser redirector that monitors Web-browsing behavior and online purchases. It claims to track points for ShopAtHome rebates when the user buys products directly from affiliated merchant Web sites.

http://www.microsoft.com/av

Encyclopedia

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

Win32/Virut: A family of file-infecting viruses that target and infect .exe and .scr files accessed on infected systems. Win32/Virut also opens a backdoor by connecting to an IRC server.

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

ASX/Wimad: A detection for malicious Windows Media files that can be used to encourage users to download and execute arbitrary files on an affected machine.

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

Win32/Yektel: A family of trojans that display fake warnings of spyware or malware in an attempt to lure the user into installing or paying money to register rogue security software programs such as Win32/FakeXPA.

http://www.microsoft.com/av

Figure 58 lists the families with the most unique detected samples in 2H09.

FIGURE 58. Families with more than 1 million unique samples detected in 2H09

Family	Most Significant Category	Total Samples
Win32/Parite	Viruses	33,906,946
Win32/Virut	Viruses	17,376,150
Win32/Sality	Viruses	10,033,778
Win32/Agent	Miscellaneous Trojans	6,901,068
Win32/FakeXPA	Miscellaneous Trojans	5,457,424
Win32/Nimda	Miscellaneous Trojans	4,060,143
ASX/Wimad	Trojan Downloaders & Droppers	3,403,025
Win32/Renos	Trojan Downloaders & Droppers	3,357,867
Win32/Chir	Viruses	3,246,102
Win32/GameVance	Adware	2,786,560
HTML/IframeRef	Exploits	2,773,324
Win32/Yektel	Miscellaneous Trojans	2,378,725
Win32/Jeefo	Viruses	2,086,154
Win32/Mabezat	Viruses	1,397,904
Win32/C2Lop	Miscellaneous Trojans	1,258,892
Win32/Vundo	Miscellaneous Trojans	1,257,988

Three virus families—Win32/Parite, Win32/Virut, and Win32/Sality—were responsible for the most unique samples by a large margin, accounting for almost as many samples as all other families combined. Win32/Agent is actually a generic detection that finds and removes groups of similar threats, so the large number of samples should not be taken as an indication of development activity for any particular family.

ASX/Wimad is a detection for a class of malicious Windows Media® files that contain links to executable files, which can contain malicious payloads. The URLs used can vary widely, resulting in large numbers of unique samples. Win32/FakeXPA and Win32/Yektel are polymorphic rogue security software families (see below for more information). Most of the other families on the list also employ server-side polymorphism to some degree.

The high number of variants seen for some categories and families illustrates why simple hash lists based on specific variants are ineffective in stopping threats and why security software vendors must use more complex heuristics to identify and stop threats.

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, claiming to detect a large number of nonexistent threats and urging the user to pay for the "full version" of the software to remove them. Some families emulate the appearance of the Windows Security Center or unlawfully use trademarks and icons to misrepresent themselves.

FIGURE 59. Fake "security scans" from different variants of Win32/FakeXPA, the most prevalent rogue security software family in 2H09

Microsoft security products detected and removed rogue security software–related malware on 7.8 million computers in 2H09, up from 5.3 million computers in 1H09—an increase of 46.5 percent, suggesting that rogue security software has been providing its distributors with large payoffs relative to some other, less prevalent kinds of threats. A rogue security software family, Win32/FakeXPA, was the third-most prevalent threat detected by Microsoft desktop security products worldwide in 2H09. Three others—Win32/Yektel, Win32/ FakeSpypro, and Win32/Winwebsec—ranked eleventh, fourteenth, and seventeenth, respectively.

Encyclopedia

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

Win32/Yektel: A family of trojans that display fake warnings of spyware or malware in an attempt to lure the user into installing or paying money to register rogue security software programs such as Win32/FakeXPA.

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

Win32/Winwebsec: A rogue security software family distributed under the names Winweb Security, System Security, and others.

http://www.microsoft.com/av

Figure 60 lists the top locations around the world for rogue security software infections in 2H09 and the top rogue families in each.

FIGURE 60. The countries and regions with the most rogue security software infections in 2H09, with the number of computers cleaned in total and the top five rogue families in each location

Worldwide	*7,779,898*
Win32/FakeXPA	*2,940,995*
Win32/Yektel	*1,378,055*
Win32/FakeSpypro	*1,194,527*
Win32/Winwebsec	*948,413*
Win32/FakeRean	*594,070*

United States	4,267,754
Win32/FakeXPA	2,288,896
Win32/Yektel	997,114
Win32/FakeSpypro	981,744
Win32/Winwebsec	660,644
Win32/FakeVimes	413,485

United Kingdom	402,161
Win32/FakeXPA	206,816
Win32/Yektel	120,085
Win32/FakeSpypro	75,260
Win32/Winwebsec	74,954
Win32/FakeVimes	35,976

Canada	242,682
Win32/FakeXPA	133,095
Win32/Yektel	55,771
Win32/FakeSpypro	53,816
Win32/Winwebsec	24,428
Win32/FakeVimes	21,684

France	97,926
Win32/FakeXPA	38,616
Win32/FakeAdpro	32,889
Win32/Yektel	26,421
Win32/Winwebsec	22,547
Win32/FakeCog	19,228

Korea	88,846
Win32/FakeBye	61,788
Win32/FakeRean	24,252
Win32/Winwebsec	2,806
Win32/FakeSpypro	2,268
Win32/InternetAntivirus	2,177

Australia	79,452
Win32/FakeXPA	38,234
Win32/Yektel	20,955
Win32/FakeSpypro	20,263
Win32/Winwebsec	15,329
Win32/FakeRean	8,204

Germany	65,609
Win32/FakeAdpro	33,211
Win32/FakeXPA	17,512
Win32/FakeRean	14,886
Win32/Winwebsec	12,158
Win32/Yektel	11,602

Italy	52,752
Win32/FakeCog	22,042
Win32/Winwebsec	17,027
Win32/FakeXPA	13,683
Win32/Yektel	9,725
Win32/FakeSmoke	9,021

Rogue security software infections tend to be concentrated in certain geographic areas. Most rogue security software is written in English, so the social engineering techniques they use tend to be more effective in English-speaking regions. For example, Canada and Australia, which have large English-speaking populations, rank third and sixth on the list in Figure 60, compared to just ninth and eighteenth in the number of computers cleaned overall in 2H09 (see Figure 43 on page 72). Rogue security software also tends to target wealthier societies and those that are more accustomed to paying for software with credit cards. In Norway, which has one of the highest per-capita GDPs in the world, rogue security software accounts for 6 of the top 25 families, whereas in China, where credit cards are relatively rare, none of the top 25 families are rogue security software families. (For more information about threats around the world, see "Malware Patterns Around the World," beginning on page 130.)

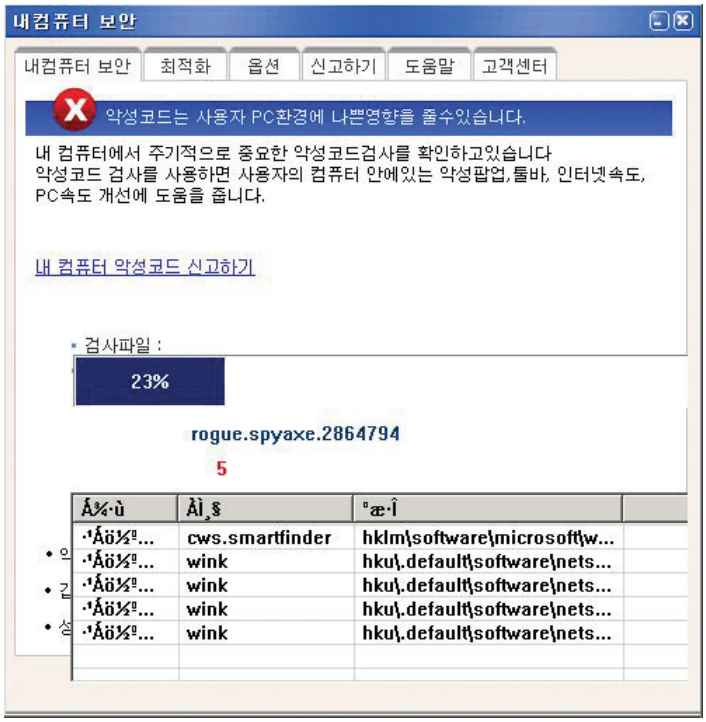
Although rogue security software remains a predominantly English-language problem, attackers sometimes use localized variants to target other populations. Korea had the fifth-largest number of computers infected with rogue security software in 2H09, due mostly to detections of Win32/FakeBye, a family with a Korean-language user interface.

Encyclopedia

Win32/FakeBye: A rogue security software family that uses a Korean-language user interface.

http://www.microsoft.com/av

FIGURE 61. The Korean-language rogue security software family Win32/FakeBye



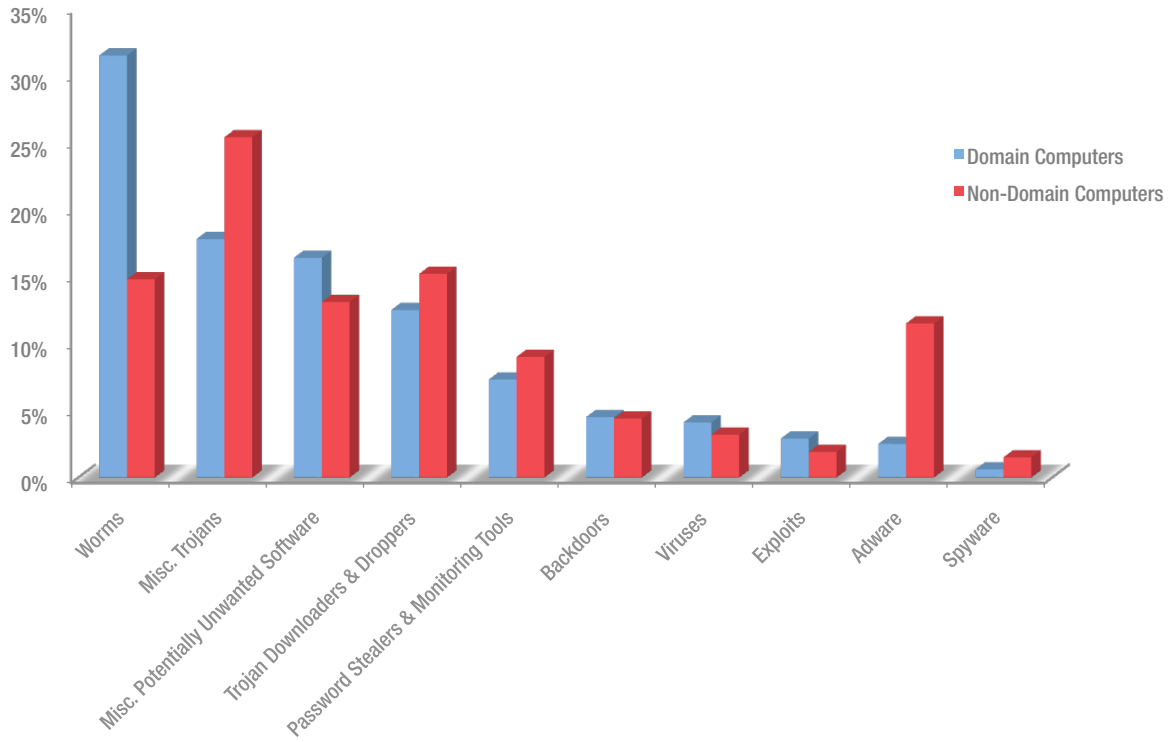
Threats at Home and in the Enterprise

Notwithstanding the "road warrior" scenario, in which an employee takes an enterprise laptop home or to another location, most desktop and laptop computers are predominately or exclusively used either at home or in the workplace. The behavior patterns of home users and enterprise users tend to be very different. Enterprise users typically use computers to perform business functions and may have limitations placed on their Internet and e-mail usage. Home users are more likely to use their computers for entertainment purposes, like playing games, watching videos, and communicating with friends. These different behavior patterns mean that home users tend to be exposed to a different mix of computer threats than do enterprise users.

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

Figure 62 shows the relative prevalence of different categories of malware and potentially unwanted software on infected domain-joined and non-domain computers in 2H09, expressed as a percentage of the total number of computers of each type that were cleaned. Totals exceed 100 percent because some computers were cleaned of more than one category of family.

FIGURE 62. Threat category breakdown for domain-joined and non-domain computers in 2H09



Domain-joined computers were much more likely to encounter worms than non-domain computers, due in large part to the way worms propagate. Worms typically spread most effectively via file shares and removable storage volumes, both of which are often plentiful in enterprise environments and less common in homes. In contrast, the Adware and Miscellaneous Trojans categories are much more common on non-domain computers.

As Figure 63 and Figure 64 show, the top families detected on domain-joined and non-domain computers were also different.

FIGURE 63. Top 10 families detected on domain-joined computers, by percentage of all computers cleaned, in 2H09

Rank	Family	Most Significant Category	Percent
1	Win32/Conficker	Worms	24.4%
2	Win32/Taterf	Worms	9.2%
3	Win32/RealVNC	Miscellaneous Potentially Unwanted Software	6.3%
4	Win32/Autorun	Worms	6.0%
5	Win32/Renos	Miscellaneous Trojans	5.9%
6	Win32/Hamweq	Worms	5.3%
7	Win32/Agent	Miscellaneous Trojans	4.2%
8	Win32/FakeXPA	Miscellaneous Trojans	3.7%
9	Win32/Alureon	Miscellaneous Trojans	3.5%
10	Win32/Frethog	Password Stealers & Monitoring Tools	3.4%

FIGURE 64. Top 10 families detected on non-domain computers, by percentage of all computers cleaned, in 2H09

Rank	Family	Most Significant Category	Percent
1	Win32/Taterf	Worms	9.6%
2	Win32/Renos	Miscellaneous Trojans	9.0%
3	Win32/FakeXPA	Miscellaneous Trojans	7.4%
4	Win32/Alureon	Miscellaneous Trojans	6.7%
5	Win32/Frethog	Password Stealers & Monitoring Tools	4.5%
6	Win32/BaiduSobar	Miscellaneous Potentially Unwanted Software	4.1%
7	Win32/GameVance	Adware	3.9%
8	Win32/Agent	Miscellaneous Trojans	3.9%
9	Win32/Hotbar	Adware	3.8%
10	Win32/Conficker	Worms	3.7%

Encyclopedia

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

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

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

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

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

Win32/GameVance: Software that displays advertisements and tracks anonymous usage information in exchange for a free online gaming experience at the Web address "gamevance.com."

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

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

http://www.microsoft.com/av

Worms accounted for 4 of the top 10 families detected on domain-joined computers. The worm family Win32/Conficker, which employs several methods of propagation that work more effectively within a typical enterprise network environment than they do over the public Internet, leads the list by a wide margin. Similarly, Win32/Autorun, which targets removable drives, was more common in domain environments, where such volumes are often used to exchange files. Other families that are more common in domain environments include Win32/Hamweq, a worm family, and the remote access tool Win32/RealVNC. RealVNC is a program that enables a computer to be controlled remotely, similar to Remote Desktop. It has a number of legitimate uses, but attackers have also used it to gain malicious control of users' computers. Detections of RealVNC and other Virtual Network Computing (VNC) programs, which are often used for remote administration, are partially responsible for the relative prevalence of the Miscellaneous Potentially Unwanted Software category on domain-joined computers, as shown in Figure 62.

The rogue security software-related families Win32/Renos and Win32/FakeXPA appear on both lists, but were more likely to be found on non-domain computers. The social engineering messages used in connection with rogue security software may be less effective in an enterprise environment, where malware protection is typically the responsibility of the IT department, and may appear on Web sites and in other contexts that users are more likely to encounter at home. (For more information, see "Rogue Security Software" on page 95.) The non-domain list also includes the browser modifier Win32/BaiduSobar and the adware families Win32/GameVance and Win32/Hotbar, potentially unwanted software families that target computer users seeking entertainment or assistance.

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

Threat Combinations

When a threat is detected on a computer, it is often not alone. The security products and tools that provide the information for this section frequently find multiple threats present on an infected computer. There are several reasons for this:

- With profit-oriented criminal endeavors now accounting for most malware activity, attackers rarely act alone. Attacks are usually not perpetrated by malware creators themselves. Instead, creators and their customers come together in online black markets where malware kits and botnet access are bought and sold. A bot-herder, for example, may rent out the same collection of infected computers to multiple parties for different purposes, requiring the installation of different types of malware.[17]
- Trojan downloaders and droppers, which were found on 15.1 percent of infected computers in 2H09 (see Figure 49 on page 81), are designed specifically to install other malware on an infected computer, resulting in multiple infections. Other types of malware also download files, in addition to their primary function.
- A single attack event, such as a drive-by download, often results in multiple threats being installed on a computer.
- Users who have not been taught about computer security and staying safe online may be prone to repeatedly engaging in the same unsafe practices, exposing them to multiple threats.

Examining which threats are typically found together on the same infected computer can provide insights into the motives and techniques of attackers and help security researchers develop more effective methods for fighting them.

Malware Distribution Networks

Malware found on the Web often downloads other malware. Some threats simply contact a single URL to check for updates. Other threats make use of elaborate networks involving several interrelated and dependent threat families.

Microsoft collects and analyzes malware from the Web to help researchers identify and prioritize important threats. Automated agents download and analyze malware files from malicious URLs submitted to Microsoft through a number of different mechanisms. Any embedded URLs discovered within these files are themselves submitted to agents for processing. The telemetry data generated through this process helps researchers better understand how malware spreads, by indicating which threat families are likely to download other threats, and how.

Figure 65 and Figure 66 show category breakdowns for parent threats (threats that downloaded others) and child threats (threats that were downloaded by others), respectively.

[17] For more information, see "The Threat Ecosystem," in *Microsoft Security Intelligence Report, Volume 5 (January through June 2008)*, pages 12-23.

FIGURE 65. Parent threats (those that downloaded other threats), by category, in 2H09

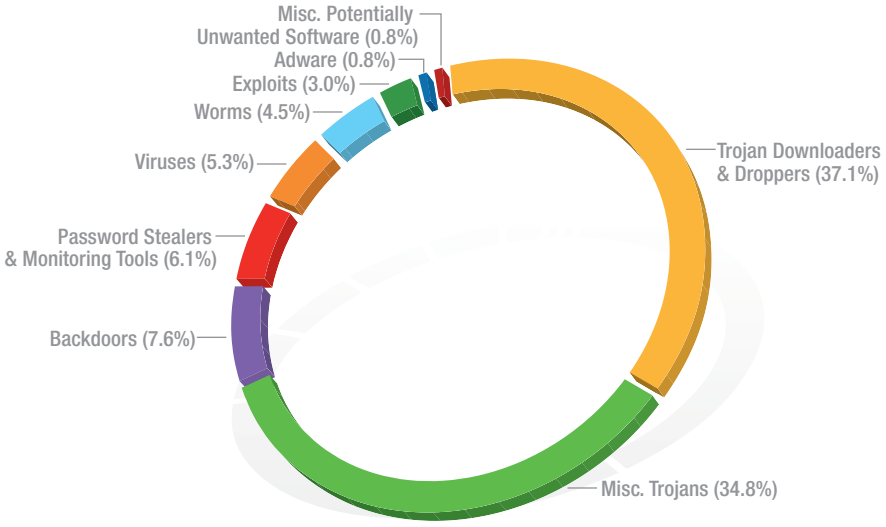
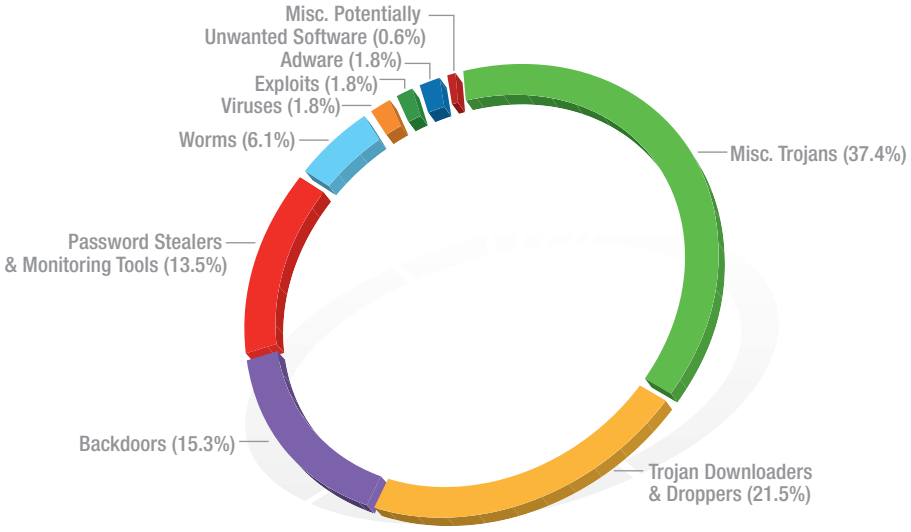


FIGURE 66. Child threats (those that were downloaded by other threats), by category, in 2H09

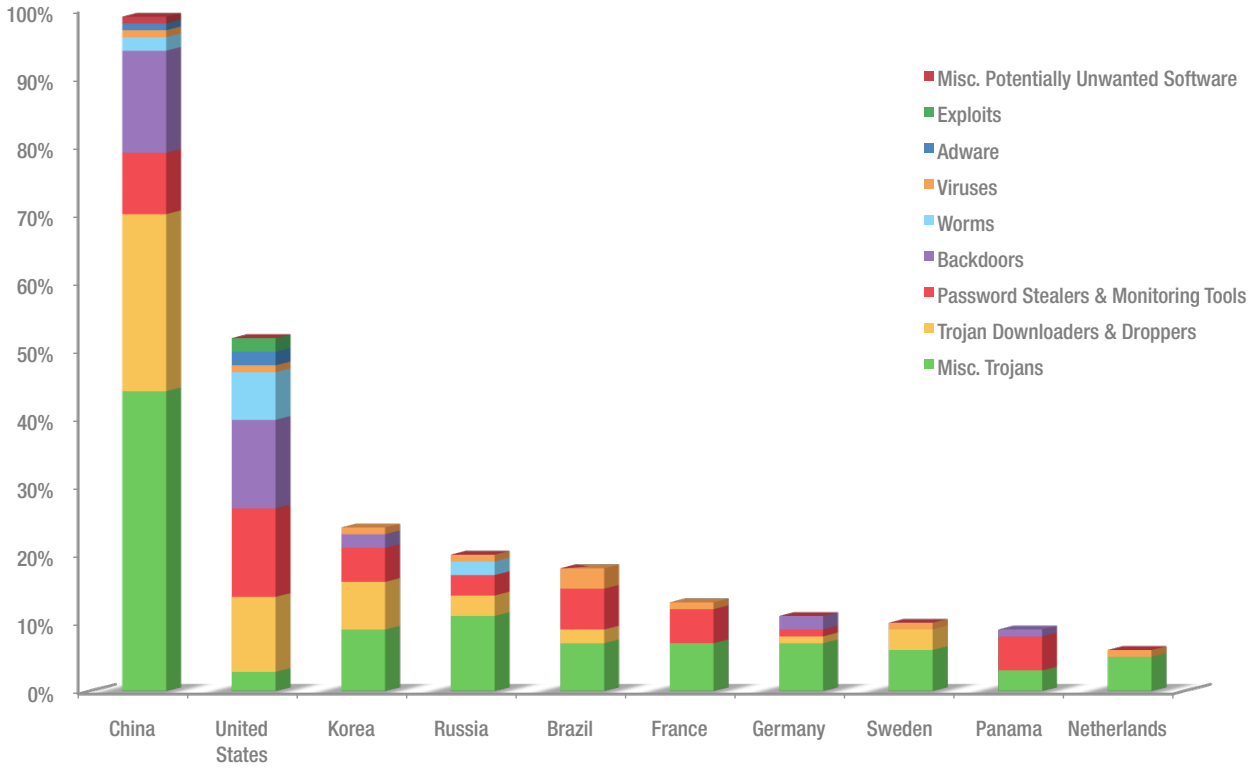


As might be expected, threats in the Trojan Downloaders & Droppers category were observed to download the most threats, followed by Miscellaneous Trojans. Altogether, trojans were responsible for more than two-thirds of parent threats and more than half of child threats. Notably, downloaders and droppers also accounted for a significant percentage of child threats—attackers often use one downloader to download another, to add a layer of indirection or for management purposes (for example, to transfer control of some of the computers in a botnet to a purchaser).

Comparing the percentages in the two figures suggests that some categories tend to be more effectively used as parent threats and others as child threats. Adware, Password Stealers & Monitoring Tools, and Backdoors were each more than twice as likely to be used as child threats than as parent threats. In contrast, Viruses were almost three times as likely to be used as parent threats, with Trojan Downloaders & Droppers and Exploits also used as parent threats significantly more often. Whereas threats such as viruses and exploits are often used as a means of compromising computers for other purposes, attackers are more likely to use adware and password stealers directly in service of a goal, like stealing sensitive information from victims or collecting payments from an adware affiliate program.

Threats hosted at URLs embedded in other malware are called *second-level threats*. China and the United States were found to host the most second-level threats by a wide margin, with Korea, Russia, Brazil, and other locations far behind.

FIGURE 67. Top 10 countries or regions hosting malicious URLs, indexed to the top location, in 2H09



Families Often Found Together

Threats can be detected together on the same computer for a number of reasons. They might have both been installed during the same infection event; one might be a payload downloaded by the other; the user's Internet behavior might simply make him or her especially susceptible to two threats that use similar methods to propagate. Examining some of the more commonly encountered threat combinations can provide insights into the way malware propagates.

The next several tables show the families that are most often found alongside several currently prevalent threats of different types. For each such threat, the corresponding table lists the other families most commonly detected by Microsoft Forefront Client Security, which is usually run in enterprise environments, and Microsoft Security Essentials, which is usually run in home environments. (See "Appendix B: Data Sources," on page 238, for more information about these and other tools.)

Figure 68 lists the other threats most often detected on computers infected with ASX/Wimad, the twelfth-most commonly detected threat in 2H09. Wimad is a detection for a class of malicious Windows Media files that contain links to executable files, which can contain malicious payloads. Whereas many threats are closely controlled by a single attacker or group, Wimad files are constructed by many separate attackers with no connection to each other. Threats found alongside Wimad are therefore likely to be relatively common, with none showing a particularly strong correlation, making Wimad a good baseline for comparison.

FIGURE 68. Other threats found on computers infected with ASX/Wimad in 2H09

Enterprise (Forefront Client Security)		Home (Microsoft Security Essentials)	
Other Family	Percent of ASX/Wimad-Infected Computers	Other Family	Percent of ASX/Wimad-Infected Computers
Win32/Autorun	21.9%	Win32/Renos	11.7%
Win32/Conficker	19.6%	Win32/Agent	10.6%
Win32/Agent	17.5%	Win32/Autorun	8.7%
Win32/Renos	12.4%	Win32/Yabector	7.1%

As expected, the threats most commonly found on computers infected with ASX/Wimad are highly prevalent threats in general. Win32/Renos, Win32/Conficker, and Win32/Agent were all among the top 10 most prevalent families in 2H09; Win32/Autorun is nineteenth. None of the correlations are particularly strong on computers running Security Essentials. Correlations on the computers running Forefront Client Security are a bit stronger at the top, due to Autorun and Conficker employing propagation methods that are well suited to enterprise environments. (See "Threats at Home and in the Enterprise," on page 98, for more information.)

Encyclopedia

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

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

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

Win32/Autorun: A worm that attempts to spread by being copied into all removable drives.

http://www.microsoft.com/av

As an example of a family with much stronger correlations, Figure 69 lists the other threats most often detected on computers infected with the trojan family Win32/Waledac. Waledac is a closely controlled family that was used to create a botnet that was primarily used for sending spam. Waledac variants are also able to download and execute arbitrary files.

FIGURE 69. Other threats found on computers infected with Win32/Waledac in 2H09

Enterprise (Forefront Client Security)		Home (Microsoft Security Essentials)	
Other Family	**Percent of Win32/Waledac-Infected Computers**	**Other Family**	**Percent of Win32/Waledac-Infected Computers**
Win32/Winwebsec	39.6%	Win32/Winwebsec	53.8%
Win32/Bredolab	39.0%	Win32/Obfuscator	30.7%
Win32/Hiloti	28.6%	Win32/Renos	28.1%
Win32/Obfuscator	28.2%	Win32/Alureon	27.1%
Win32/Ursnif	25.1%	Win32/Bredolab	26.8%
Win32/Tikayb	24.6%	Win32/Tikayb	22.9%
Win32/Cutwail	22.4%	ASX/Wimad	20.6%

Some Win32/Waledac variants have been observed to download the rogue security software threat Win32/Winwebsec, and indeed Winwebsec was found very frequently on computers infected with Waledac—on more than a third of those running Forefront Client Security and on more than half of those running Security Essentials. The trojan downloader Win32/Bredolab has been observed to download spambot families such as Waledac, explaining the presence of Bredolab on large percentages of computers infected with Waledac in both home and enterprise environments. Several relatively rare threats, such as Win32/Ursnif and Win32/Tikayb, were also detected on a large percentage of the computers infected with Win32/Waledac, suggesting significant connections to these families.

Some groups of families have a tendency to appear together in clusters. Figure 70, Figure 71, and Figure 72 illustrate the significant amount of overlap between computers infected with the worm families Win32/Taterf, Win32/Rimecud, and Win32/Hamweq, respectively.

Encyclopedia

Win32/Winwebsec: A rogue security software family distributed under the names Winweb Security, System Security, and others.

Win32/Bredolab: A downloader that can access and execute arbitrary files from a remote host. Bredolab has been observed to download several other malware families to infected computers.

Win32/Ursnif: A family of trojans that steals sensitive information from an affected computer.

Win32/Tikayb: A trojan that attempts to establish a secure network connection to various Web sites without the user's consent.

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

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

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

http://www.microsoft.com/av

FIGURE 70. Other threats found on computers infected with Win32/Taterf in 2H09

Enterprise (Forefront Client Security)		Home (Microsoft Security Essentials)	
Other Family	Percent of Win32/Taterf-Infected Computers	Other Family	Percent of Win32/Taterf-Infected Computers
Win32/Autorun	46.1%	Win32/Autorun	36.9%
Win32/Conficker	41.3%	Win32/Frethog	25.0%
Win32/Hamweq	23.2%	Win32/Conficker	24.5%
Win32/Rimecud	20.4%	Win32/Rimecud	17.2%

FIGURE 71. Other threats found on computers infected with Win32/Rimecud in 2H09

Enterprise (Forefront Client Security)		Home (Microsoft Security Essentials)	
Other Family	Percent of Win32/Rimecud-Infected Computers	Other Family	Percent of Win32/Rimecud-Infected Computers
Win32/Autorun	47.6%	Win32/Autorun	38.2%
Win32/Conficker	40.6%	Win32/Taterf	27.1%
Win32/Taterf	28.8%	Win32/Conficker	24.1%
Win32/Hamweq	26.0%	Win32/DelfInject	17.5%

FIGURE 72. Other threats found on computers infected with Win32/Hamweq in 2H09

Enterprise (Forefront Client Security)		Home (Microsoft Security Essentials)	
Other Family	Percent of Win32/Hamweq-Infected Computers	Other Family	Percent of Win32/Hamweq-Infected Computers
Win32/Autorun	46.9%	Win32/Autorun	47.8%
Win32/Conficker	37.8%	Win32/Taterf	31.6%
Win32/Taterf	24.5%	Win32/Conficker	29.9%
Win32/Rimecud	19.6%	Win32/Rimecud	22.8%

Taterf is a password-stealing worm, and Rimecud and Hamweq have backdoor functionality. These three worm families have something significant in common—they are designed to spread via removable volumes, including USB flash drives and network drives. Each family appears in the list of other threats found on computers infected with the other two in home or enterprise environments, or both. In addition, all are frequently found with Win32/Conficker and Win32/Autorun, a generic detection. The frequency with which all of these threats are detected together suggests that users who make frequent use of removable storage volumes and/or network drives face an elevated risk of infection from multiple threats that use the specific propagation method described here.

Encyclopedia

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

Win32/Autorun: A worm that attempts to spread by being copied into all removable drives.

http://www.microsoft.com/av

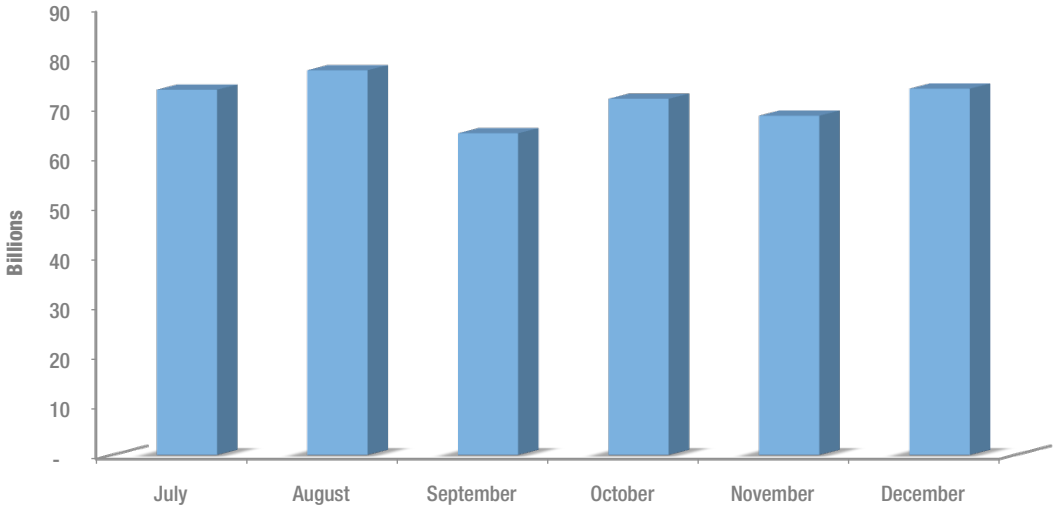
E-Mail Threats

The vast majority of the e-mail messages sent over the Internet are unwanted. Not only does all this unwanted e-mail tax the recipients' inboxes and the resources of e-mail providers, but it also creates an environment in which e-mailed malware attacks and phishing attempts can proliferate. Blocking spam, phishing, and other e-mail threats is a top priority for e-mail providers, social networks, and other online communities. ("Malicious Web Sites," beginning on page 116, includes more information about phishing in particular.)

Spam Trends and Statistics

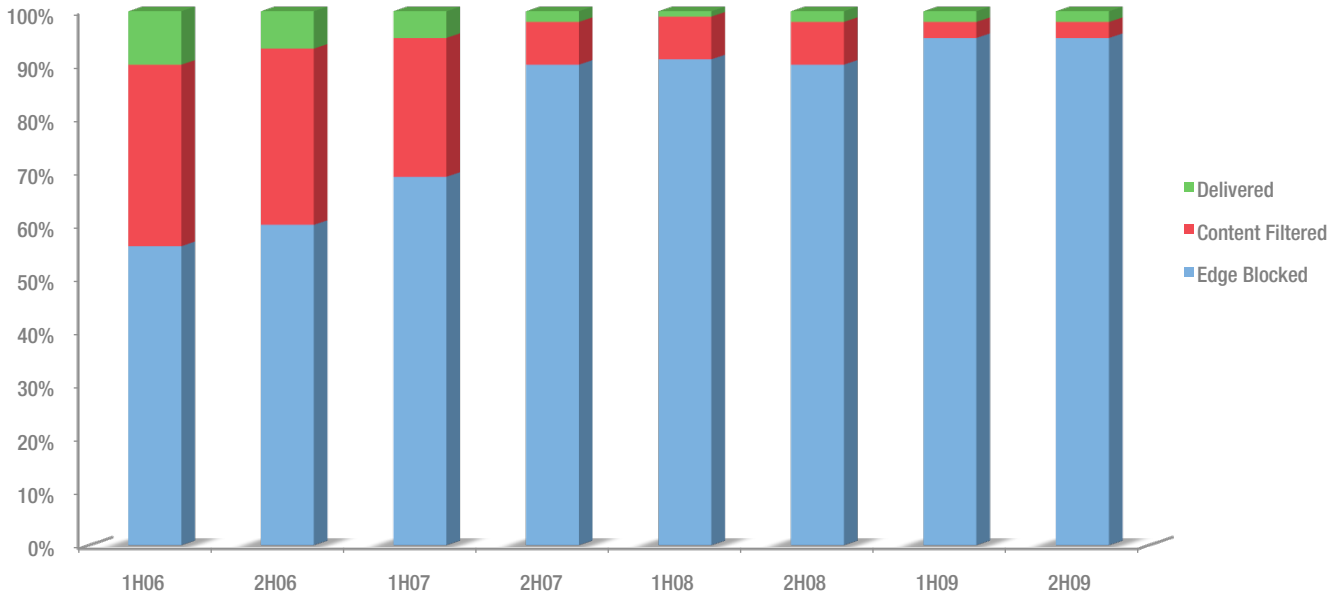
The spam statistics in the *Security Intelligence Report* are provided by Microsoft Forefront Online Protection for Exchange (FOPE), which provides spam, phishing, and malware filtering services for thousands of enterprise customers. FOPE performs spam filtering in two stages. The vast majority of spam 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 e-mail threats, including attachments containing malware.

FIGURE 73. Incoming messages blocked by FOPE each month in 2H09



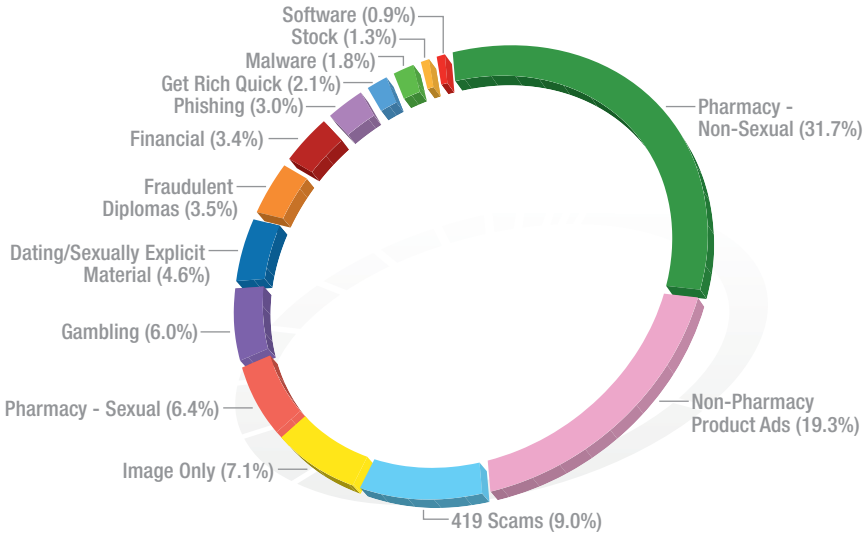
In 2H09 overall, about 97.8 percent of all unwanted messages were blocked at the network edge, which means that only 2.2 percent of unwanted messages had to be subjected to the more resource-intensive content filtering process. As Figure 74 demonstrates, the effectiveness of edge-filtering techniques, such as IP address reputation checking, SMTP connection analysis, and recipient validation, have increased dramatically over the past several years, enabling mail-filtering services to provide better protection to end users even as the total amount of unwanted message traffic on the Internet remains as high as ever.

FIGURE 74. Percentage of incoming messages blocked by FOPE using edge-blocking and content filtering, 1H06–2H09



As in previous periods, spam in 2H09 was dominated by illegal or illicit product advertisements, primarily for pharmaceutical products. Figure 75 shows the subject category breakdown for the messages blocked by the FOPE content filters during 2H09. These figures do not include messages blocked at the network edge, though from past experience Microsoft security analysts believe the category breakdown for edge-blocked spam to be substantially similar to that for content-filtered spam.

FIGURE 75. Inbound messages blocked by FOPE content filters, by category, in 2H09

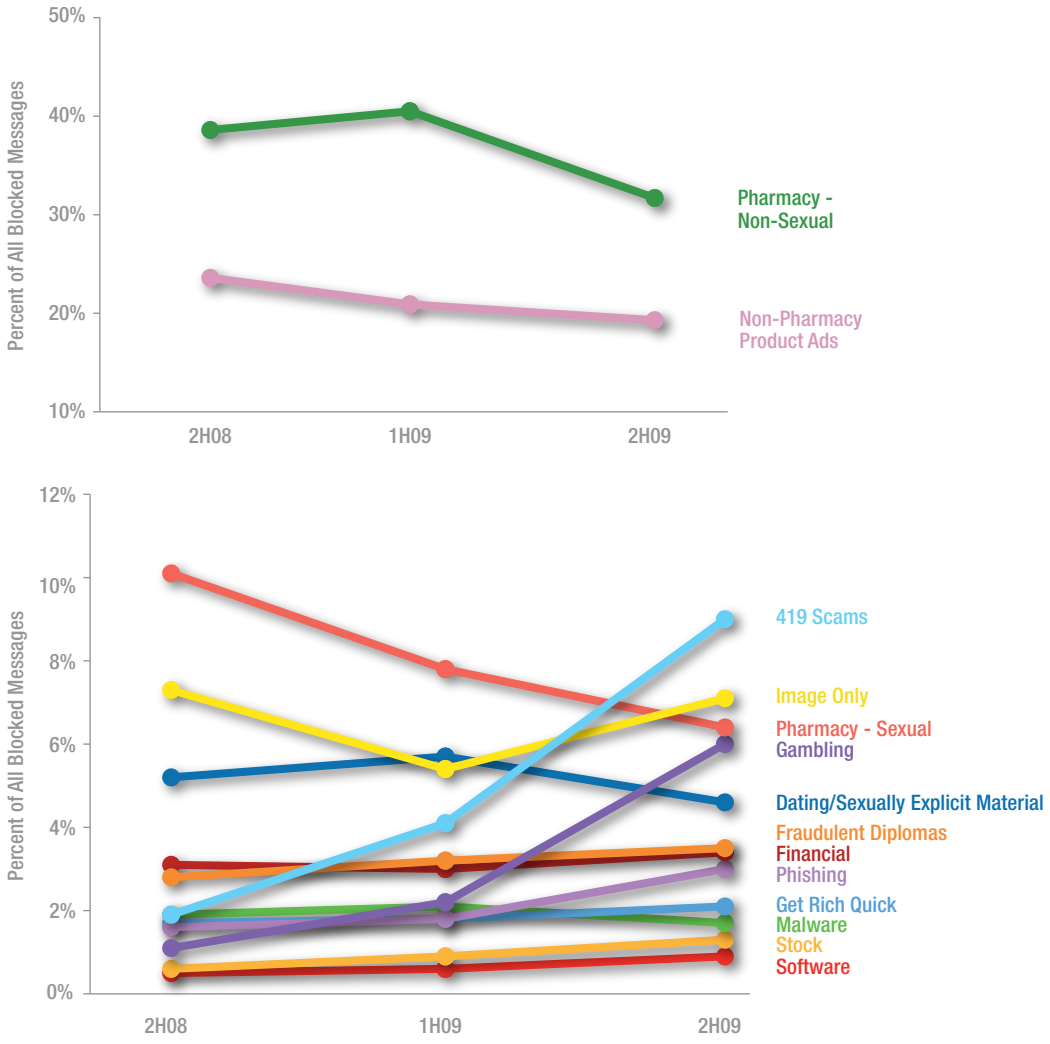


Advertisements for pharmaceutical products accounted for 38.1 percent of the spam messages blocked by FOPE content filters in 2H09, with advertisements for sexual performance products accounting for 6.4 percent of the overall total and non-sexual pharmaceutical products accounting for the remaining 31.7 percent. Together with non-pharmacy product ads (19.3 percent of the total), product advertisements accounted for 57.4 percent of spam in 2H09, down from 69.2 percent in 1H09.

In an effort to evade content filters, spammers often send messages consisting only of one or more images, with no text in the body of the message. Image-only spam messages accounted for 7.1 percent of the total in 2H09, up from 5.4 percent in 1H09.

Figure 76 shows the trend in these statistics over time, from 2H08 to 2H09.

FIGURE 76. Inbound messages blocked by FOPE content filters, by category, 2H08–2H09



Spam messages associated with advance-fee fraud (so-called "419 scams") and gambling increased significantly in 2H09, with most other categories remaining relatively stable in percentage terms. An advance-fee fraud is a common confidence trick in which the sender of a message purports to have a claim on a large sum of money, but is unable to access it directly for some reason, typically involving bureaucratic red tape or political corruption. The sender asks the prospective victim for a temporary loan to be used for bribing officials or for paying fees to get the full sum released. In exchange, the sender promises the target a share of the fortune amounting to a much larger sum than the original loan. These messages are often associated with Nigeria ("419" refers to the article of the Nigerian Criminal Code dealing with fraud) and other countries in western Africa, including Sierra Leone, Ivory Coast, and Burkina Faso. Independent reports indicate that advance-fee fraud activity increased significantly in 2009, explaining the rise in 419 scam messages detected by FOPE. One investigative firm estimated that 419 scammers collectively took in U.S.$9.3 billion in 2009, nearly 50 percent more than in the previous year.[18]

Geographic Origins of Spam Messages

To measure the geographic distribution of spam, FOPE performs geographic lookups on the originating IP addresses of post-edge-blocked spam and maps them to their countries/regions of origin. Most spam today is sent through botnets or other automated tools, so the geographic origin of a spam message typically provides little or no information about the location of the parties that wrote and transmitted the message. However, determining the origins of spam can provide another way to measure the magnitude of security problems affecting different areas of the globe.

Figure 77 shows the countries/regions around the world that sent the most spam, as detected by FOPE from July through December 2009.

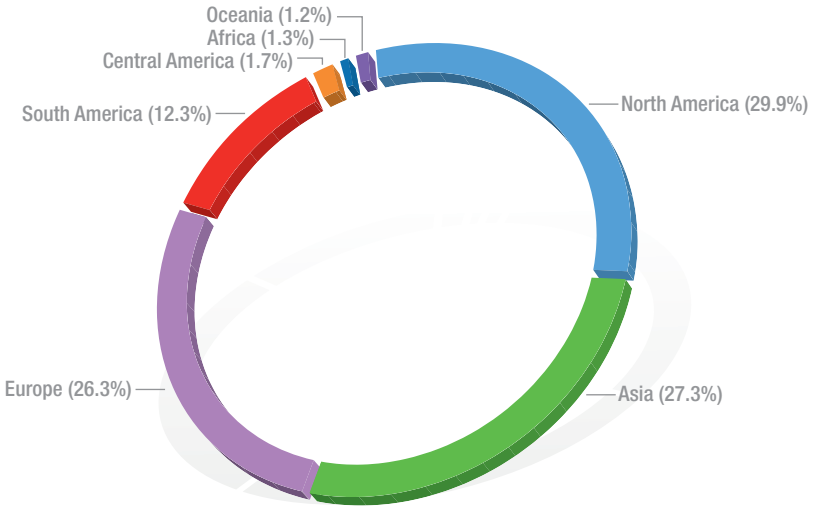
[18] Ultrascan Advanced Global Investigations. "419 Advance Fee Fraud Statistics 2009." Amsterdam: Ultrascan AGI, 2010. (http://www.ultrascan-agi.com/public_html/html/pdf_files/419_Advance_Fee_Fraud_Statistics_2009.pdf)

FIGURE 77. Locations sending the most spam, by percentage of all spam sent, in 2H09

Rank	Country/Region	Percent
1	United States	27.0%
2	Korea	6.9%
3	China	6.1%
4	Brazil	5.8%
5	Russia	2.9%
6	France	2.4%
7	United Kingdom	2.3%
8	India	2.1%
9	Colombia	2.1%
10	Poland	2.0%
11	Argentina	2.0%
12	Spain	2.0%
13	Canada	1.9%
14	Japan	1.9%
15	Romania	1.6%
16	Germany	1.4%
17	Italy	1.4%
18	Czech Republic	1.3%
19	Ukraine	1.2%
20	Vietnam	1.2%
21	Netherlands	1.2%
22	Turkey	1.0%
23	Mexico	1.0%
24	Bulgaria	1.0%
25	Chile	1.0%
	All Other	19.3%

Figure 78 shows this data organized by continent or large region. Overall, the trend is consistent with 1H09, with no one region varying by more than a few percentage points of the total.

FIGURE 78. Geographic origins of spam, by percentage of total spam sent, in 2H09



In general, countries and regions with large numbers of Internet users tend to send large amounts of spam. To compensate for this effect, Figure 79 lists the countries or regions that sent the most spam messages per Internet user in 2H09, among locations that sent at least 1 million spam messages during the period.

FIGURE 79. Locations sending the most spam messages per Internet user in 2H09 (minimum 1 million spam messages sent)

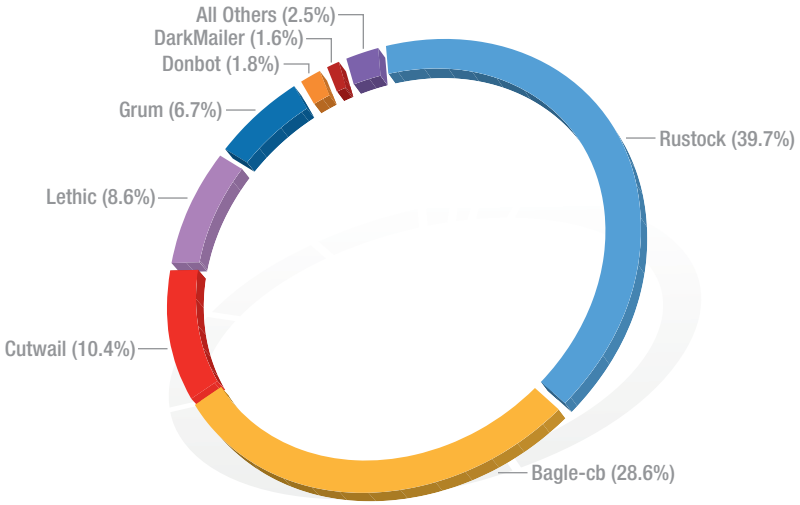
Rank	Country/Region	Spam Messages Sent Per Internet User
1	Guam	52.8
2	Thailand	39.4
3	Cambodia	25.0
4	Albania	21.5
5	Panama	14.0
6	Bulgaria	13.4
7	Trinidad and Tobago	13.3
8	Bahamas	12.9
9	Namibia	11.4
10	Honduras	9.1
11	Nicaragua	8.9
12	Czech Republic	8.4
13	Estonia	8.0
14	Cyprus	7.9
15	Bahrain	7.9
16	Puerto Rico	7.8
17	Lithuania	7.7
18	Romania	7.2
19	Costa Rica	6.8
20	Ireland	6.6
21	Kuwait	6.5
22	Iceland	6.5
23	Korea	6.2
24	Latvia	6.2
25	Ukraine	6.1

Internet usage estimates from Internet World Stats (http://www.internetworldstats.com/stats.htm)

Spam from Botnets

Botnets—networks of malware-infected computers that can be controlled remotely by an attacker—are responsible for much or most of the spam sent today. To measure the impact that botnets have on the spam landscape, FOPE monitors spam messages sent from IP addresses that have been reported to be associated with known botnets. As Figure 80 illustrates, a handful of botnets are responsible for sending almost all of the botnet spam observed in 2H09.

FIGURE 80. Botnets sending spam, by percentage of all botnet spam, in 2H09



The names used to track botnets usually coincide with the names assigned to the dominant malware families associated with each one, but not always. Some botnets are associated with more than one threat family, due to development activity on the part of malware creators and to the existence of generic detections. For example, some Win32/Lethic variants are detected as Win32/IRCbot.gen!T.

The Rustock botnet was responsible for 39.7 percent of botnet spam received by FOPE in 2H09. Win32/Rustock is a multi-component family of rootkit-enabled backdoor trojans. First discovered sometime in early 2006, Rustock has evolved to become a prevalent and pervasive threat. Recent variants appear to be associated with the rogue security programs.

Encyclopedia

Win32/Lethic: A trojan that connects to remote servers, which may lead to unauthorized access to an affected system.

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

http://www.microsoft.com/av

The Rustock botnet appears to be closely controlled by a single individual or group. The operation of the botnet was adversely affected by the November 2008 shutdown of McColo, an Internet service provider that hosted command-and-control servers for Rustock and several other large botnets. Rustock's controllers were later able to move their servers to a different provider.[19] Some researchers have found Rustock being spread through an affiliate-based "pay-per-install" scheme.[20]

The Bagle-cb and Cutwail botnets are responsible for 28.6 percent and 10.4 percent of botnet spam received by FOPE in 2H09, respectively. A family of mass-mailing worms first detected in 2004, Win32/Bagle was one of the first malware families developed with profit in mind. Today, Bagle variants are used as relay proxies to forward spam messages to their destinations.[21] Win32/Cutwail is a multipurpose threat family that employs a rootkit and other defensive techniques to avoid detection and removal.

Encyclopedia

Win32/Bagle: A worm that spreads by e-mailing itself to addresses found on an infected computer. Some variants also spread through P2P networks. Bagle acts as a backdoor trojan and can be used to distribute other malicious software.

http://www.microsoft.com/av

[19] Kirk, Jeremy. "Dodgy ISP McColo briefly comes online, updates botnet." *IT World*, November 17, 2008. (http://www.itworld.com/security/57943/dodgy-isp-mccolo-briefly-comes-online-updates-botnet)

[20] Stevens, Kevin. "The Underground Economy of the Pay-Per-Install (PPI) Business." *SecureWorks*, September 29, 2009. (http://www.secureworks.com/research/threats/ppi/)

[21] Kassner, Michael. "The top 10 spam botnets: New and improved." *TechRepublic.com*, February 25, 2010. (http://blogs.techrepublic.com.com/10things/?p=1373)

Malicious Web Sites

Attackers often use Web sites to host phishing pages or distribute malware. Malicious Web sites typically appear completely legitimate and often give no outward indicators of their malicious nature, even to experienced computer users. In many cases, just visiting a malicious site can be dangerous because attackers often create exploits that can download malware to vulnerable computers silently as soon as the user loads the page. Installing updated versions and security updates for the operating system, the browser, and any installed browser add-ons in a timely manner can greatly reduce users' chances of being victimized, although zero-day exploits (see page 25) pose a risk even to up-to-date computers.

To protect users from malicious Web pages, 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. Analyzing the telemetry produced by these tools can provide valuable information about the nature and spread of malicious Web sites.

Analysis of Phishing Sites

Phishing is a method of identity theft that tricks Internet users into revealing personal or financial information online. Attackers send messages purporting to be from a trusted institution, such as a bank, auction site, or popular Web site, attempting to lure potential victims into unwittingly divulging login credentials or other sensitive information, such as credit card numbers. Although phishers sometimes set up Web servers of their own, most phishing pages are hosted on compromised sites belonging to innocent parties that have been victimized by exploits or other techniques.[22]

Phishing activity spiked severely in two identifiable and apparently unrelated campaigns in July and December of 2009, with comparatively low activity observed at other times. (A *phishing impression* is a single instance of a user attempting to visit a known phishing site with Internet Explorer and being blocked.)

[22] Notably, malware distribution sites are more likely to be hosted by the attackers themselves than are phishing sites, perhaps due to the fact that widespread use of filtering tools for malware distribution sites is still relatively new and attackers have not yet faced the level of take-down pressure that victimized institutions have brought to bear against phishers.

Phishing Sites and Traffic

Microsoft maintains a database of known active phishing sites reported by users of Internet Explorer and other Microsoft products and services. When a user attempts to visit a site in the database with the Phishing Filter (in Internet Explorer 7) or SmartScreen Filter (in Internet Explorer 8) enabled, Internet Explorer checks the URL against the database. If the site has been reported as a phishing site, Internet Explorer blocks navigation to the site and displays a warning, as shown in Figure 81.[23] Microsoft monitors traffic to the reported phishing URLs and uses the information to improve its filtering technology and its efforts to track suspected phishing sites.[24]

FIGURE 81. The SmartScreen Filter in Internet Explorer 8 blocks reported phishing and malware distribution sites.

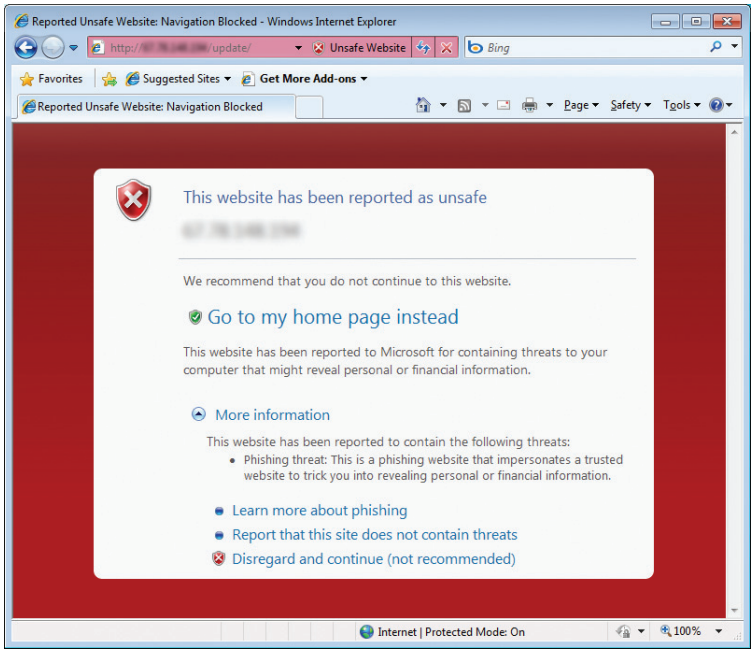
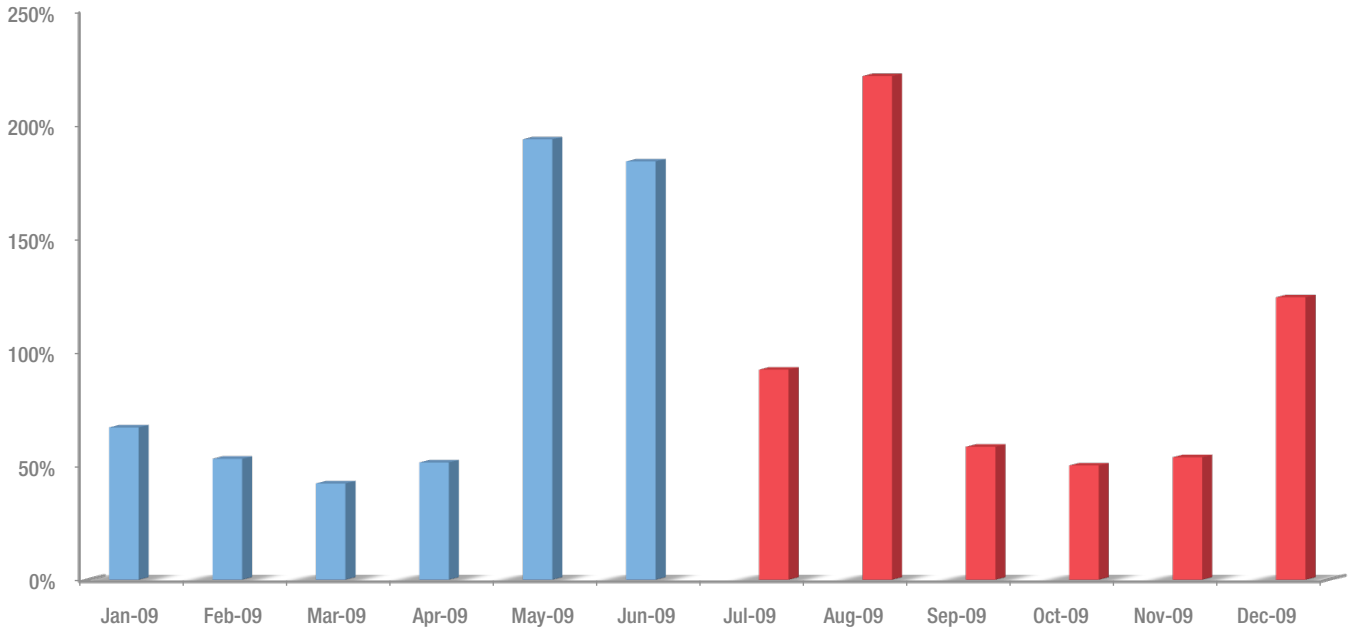


Figure 82 shows the number of phishing impressions recorded by Internet Explorer 8 each month in 2H09.

[23] See http://blogs.msdn.com/ie/archive/2008/07/02/ie8-security-part-iii-smartscreen-filter.aspx for more information about the SmartScreen Filter and how it protects Internet users.

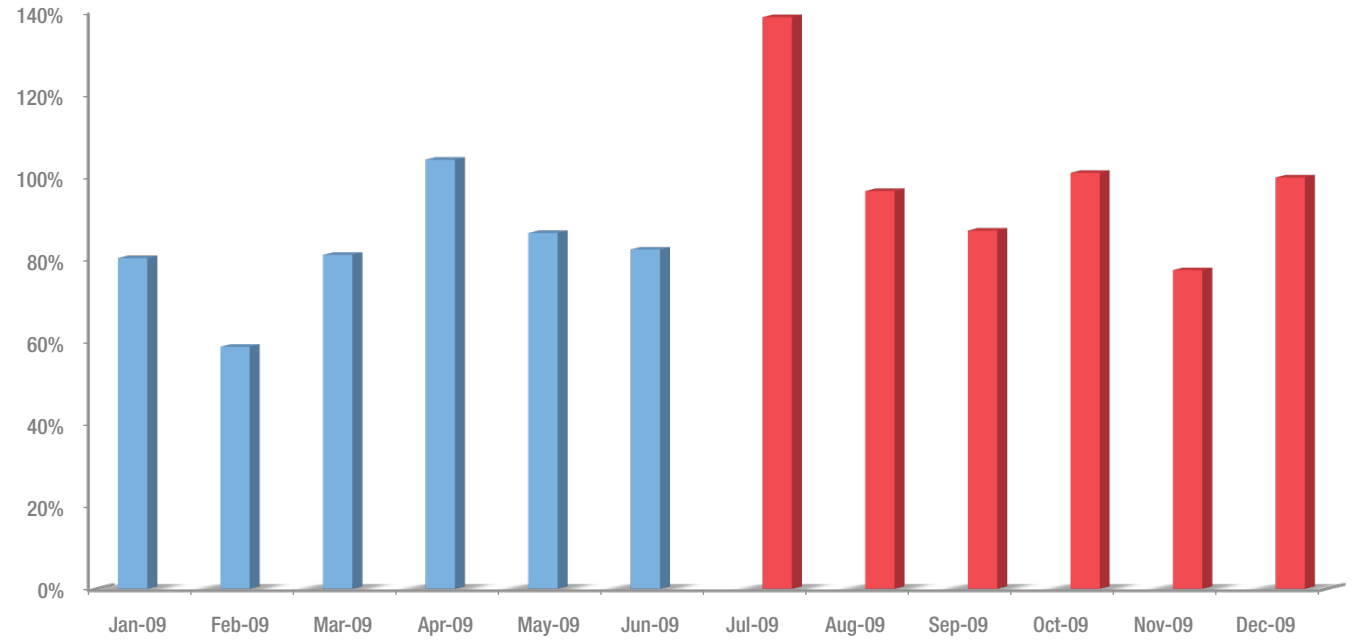
[24] Microsoft is committed to protecting its customers' privacy. See http://www.microsoft.com/windows/internet-explorer/privacy.aspx for the privacy statement for Internet Explorer 8, and see http://www.microsoft.com/windows/ie/ie7/privacy/ieprivacy_7.mspx for the privacy statement for Internet Explorer 7.

FIGURE 82. Phishing impressions tracked by Internet Explorer 8 each month in 2009, indexed to 2H09 average



At the same time, the total number of active phishing pages tracked by Microsoft remained much more stable from month to month, with the average for 2H09 up slightly from the first half of the year.

FIGURE 83. Active phishing sites tracked each month in 2009, indexed to 2H09 average



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 are maintaining at the same time. In this case, the steep spikes in impressions in August and December (see Figure 82 on page 118) correspond to campaigns targeting online services and social networking sites, neither of which typically require large numbers of phishing pages, as explained in the next section.

Target Institutions

As published in previous volumes of the *Security Intelligence Report*, social networking properties suffered the highest total volume of phishing impressions as well as the highest rate of phishing impressions per phishing site. Financial institutions received the lowest volume of phishing impressions per site though by far the highest total volume of distinct fraudulent sites. Figure 84 and Figure 85 show the percentage of phishing impressions and active phishing sites, respectively, recorded by Microsoft each month in 2H09 for each of the most frequently targeted types of institutions.

FIGURE 84. Impressions for each type of phishing site each month in 2H09

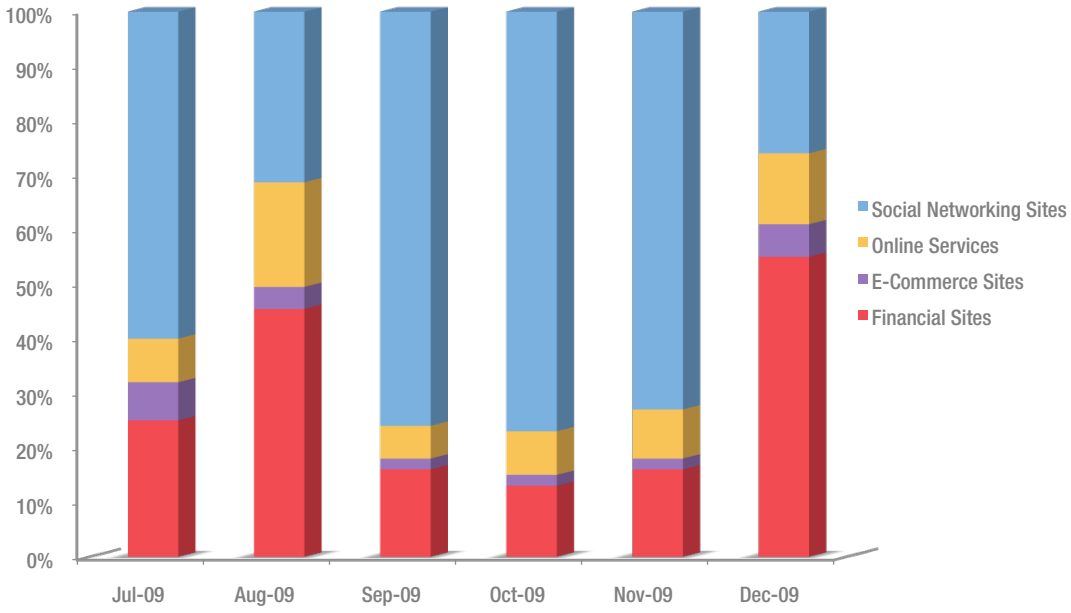
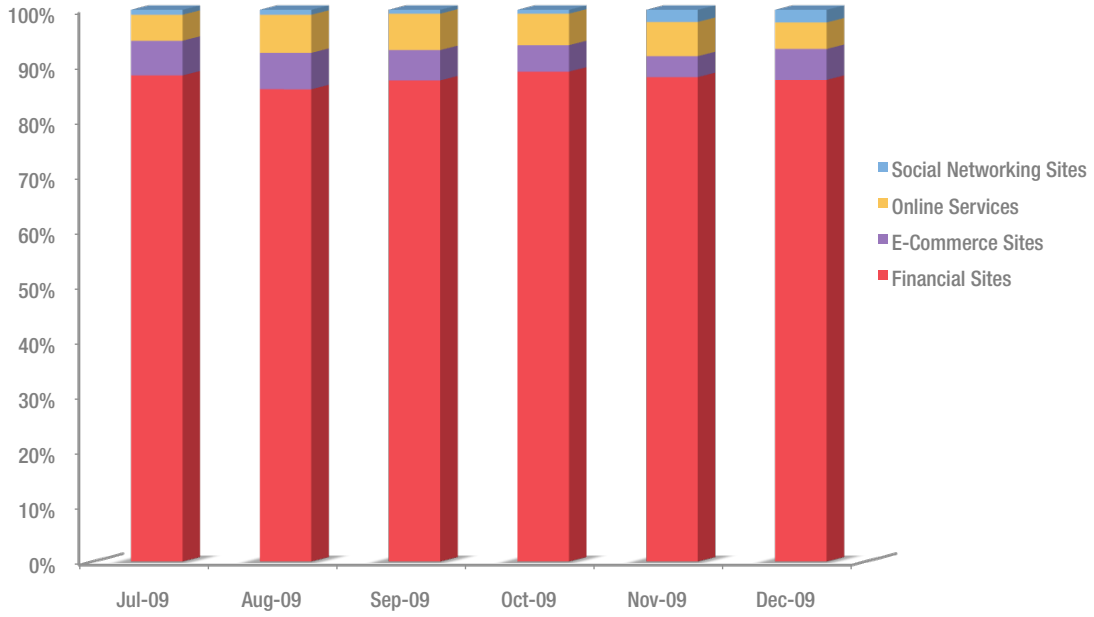


FIGURE 85. Active phishing sites tracked each month, by type of target, in 2H09



As Figure 84 shows, sites targeting social networks accounted for the majority of phishing impressions in four of the six months in 2H09; the spikes in August and December, seen in Figure 82, were due largely to a campaign or campaigns of attacks targeting online services. Even during these periods of increased activity, however, phishing sites targeting social networks and online services each only accounted for a small percentage of active phishing pages, with the majority of pages consistently targeting financial institutions. Financial institutions targeted by phishers can number in the hundreds, requiring customized phishing approaches for each one. By contrast, just a handful of popular sites account for the bulk of the social network and online service usage on the Internet, so phishers can effectively target many more people per site.

The online services category includes sites dedicated to online games, which phishers targeted with increased frequency in 2H09. Gaming sites accounted for less than 1 percent of active phishing sites but more than 2 percent of total phishing impressions.

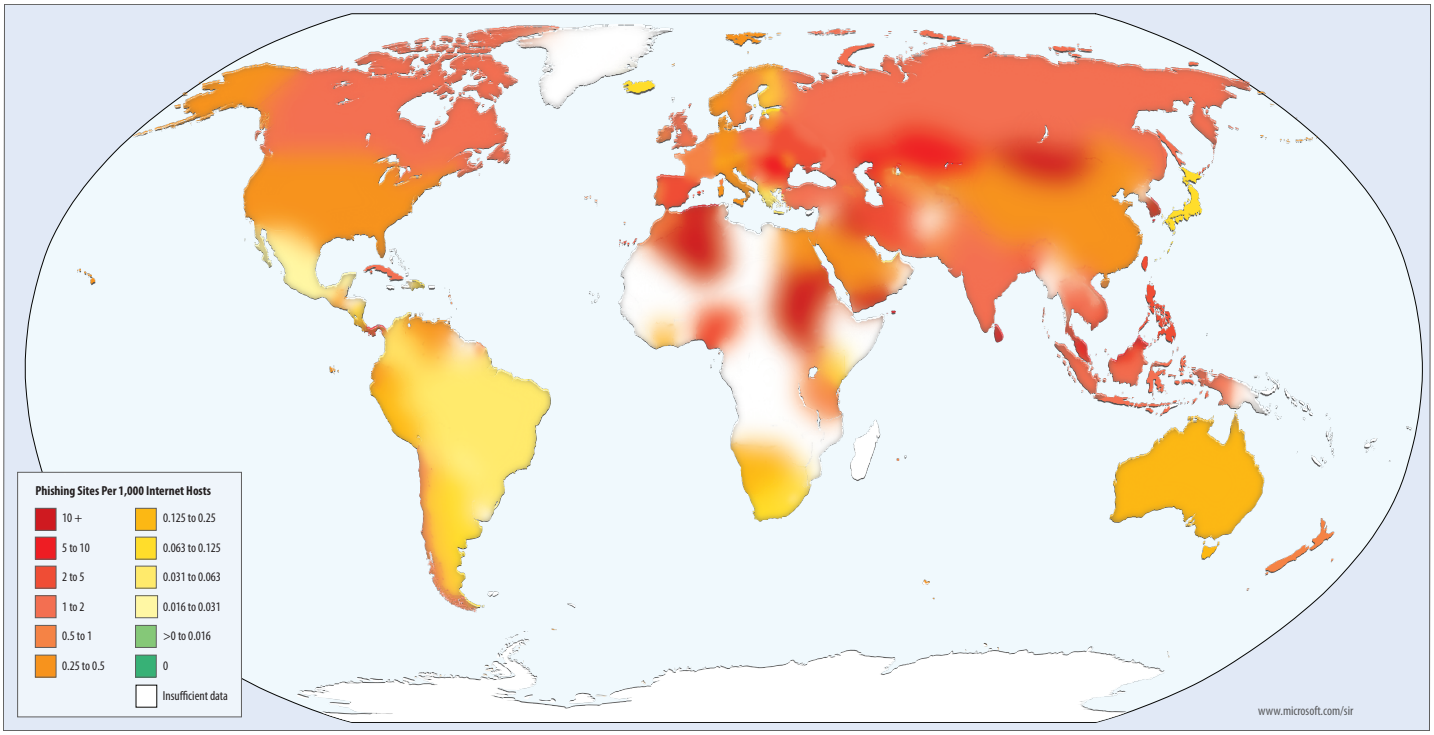
As phishers have widened the scope of their attacks in recent years, online services and social networks have put a great deal of effort into fighting the problem through collaborative efforts like the Anti-Phishing Working Group (http://www.antiphishing.org) and by launching initiatives to educate their own users about phishing and how to avoid being tricked. Despite these efforts, however, the relatively high payoff potential suggests that phishers will continue to target these types of institutions in the future.

Geographic 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 on the IP addresses of the sites in the database of reported phishing sites makes it possible to create maps showing the geographic distribution of sites and to analyze patterns.

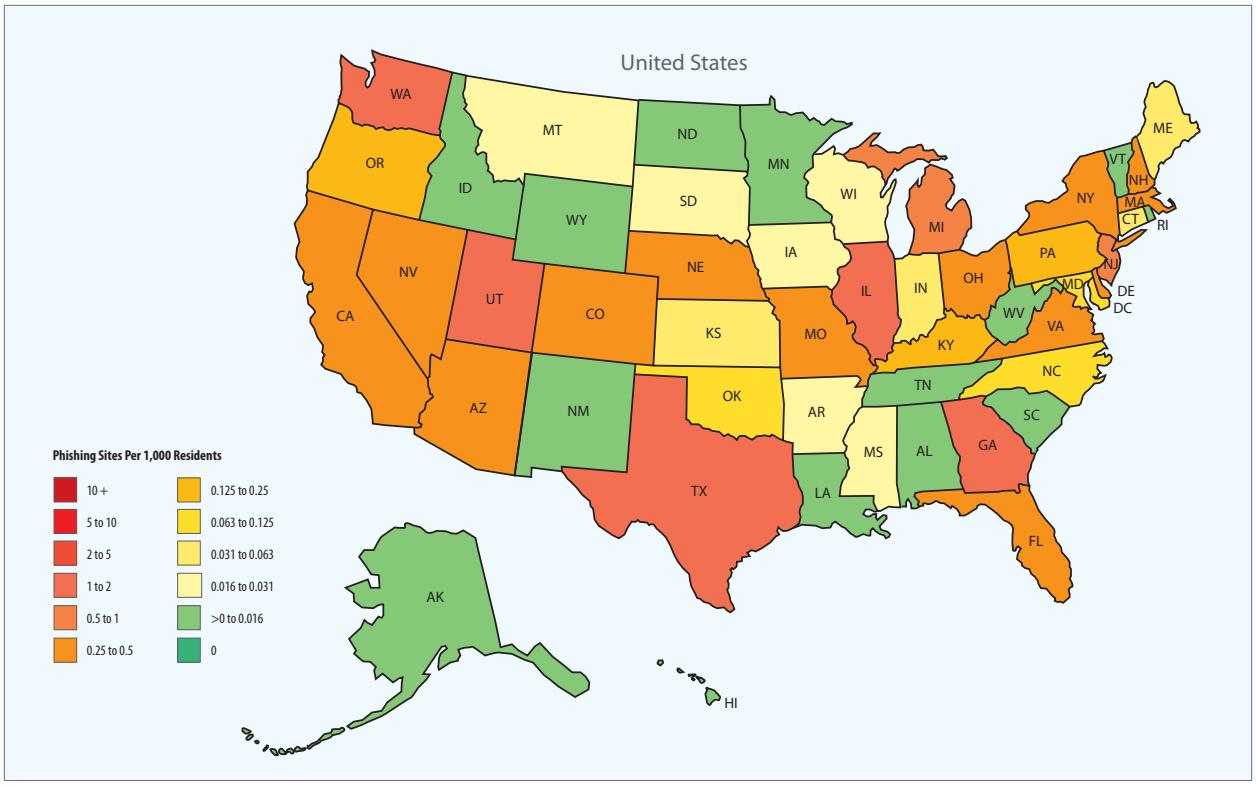
Figure 86 and Figure 87 show the relative concentration of phishing sites in different locations around the world and in U.S. states in 2H09.[25]

FIGURE 86. Phishing sites per 1,000 Internet hosts for locations around the world in 2H09



[25] Internet host estimates are from the World Factbook, at https://www.cia.gov/library/publications/the-world-factbook/. Due to a lack of reliable state-by-state Internet host data, Figure 87 shows the number of phishing pages per 1,000 residents of each state, based on population estimates for 2009 published by the U.S. Census Bureau at http://www.census.gov/popest/states/.

FIGURE 87. Phishing sites per 1,000 residents by U.S. state in 2H09

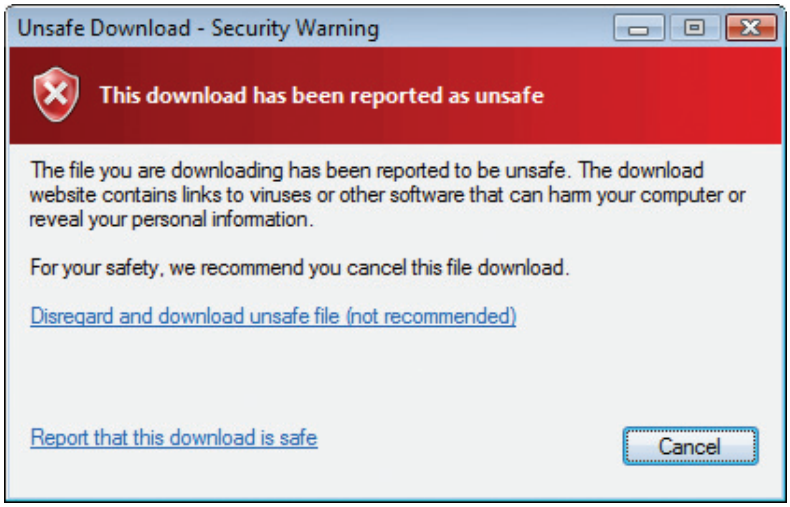


As these maps show, phishing sites are concentrated in a few locations but have been detected in many places around the world. Microsoft has tracked phishing sites on every inhabited continent and in all 50 U.S. states. Locations with smaller populations and fewer Internet hosts tend to have higher concentrations of phishing pages, although in absolute terms most phishing pages are located in large, industrialized countries/regions with large numbers of Internet hosts.

Analysis of Malware Hosts

Internet Explorer 8, released in March 2009, includes the SmartScreen Filter, a successor to the Phishing Filter in Internet Explorer 7. The SmartScreen Filter continues to provide protection against phishing sites, as described in "Analysis of Phishing Sites," beginning on page 116, and also includes anti-malware support. The SmartScreen anti-malware feature is URL reputation–based, which means that it evaluates servers hosting downloads to determine if those servers are distributing unsafe content. If a user visits a site known to distribute malware, Internet Explorer 8 displays the SmartScreen blocking page (see Figure 81 on page 117) and indicates that the server is known to distribute unsafe software. Additionally, if a user attempts to download an unsafe file, Internet Explorer displays a warning message, shown in Figure 88.

FIGURE 88. The SmartScreen Filter in Internet Explorer 8 displays a warning when a user attempts to download an unsafe file.

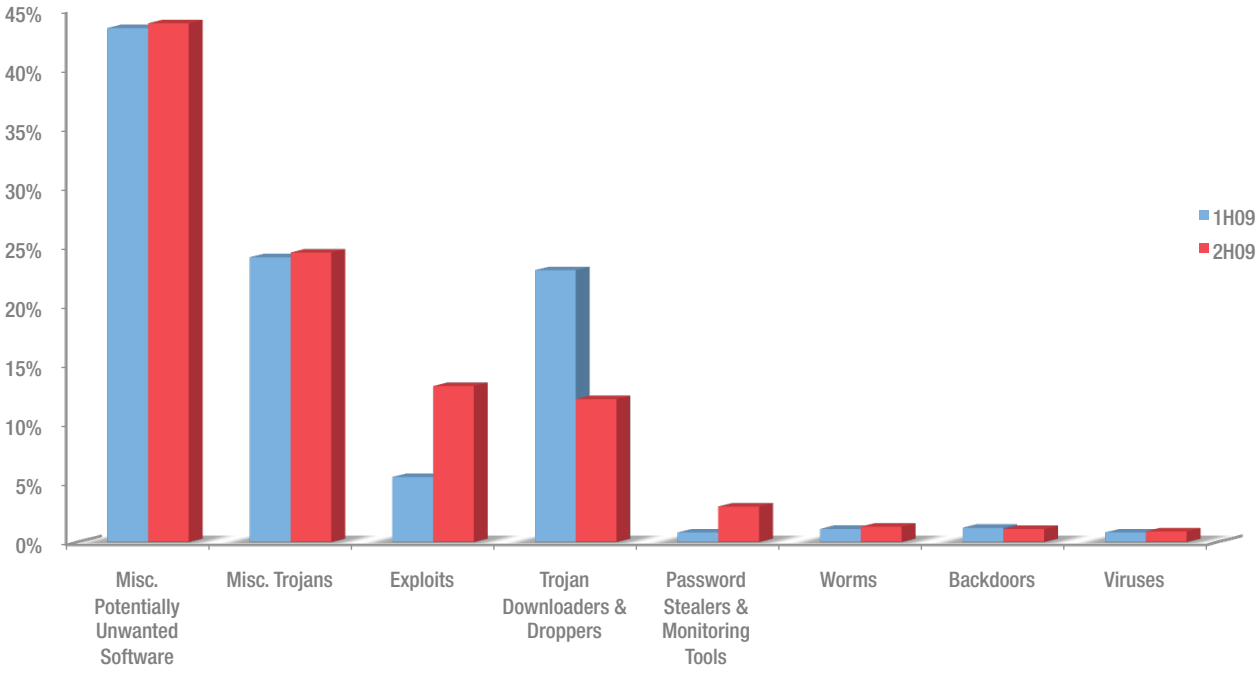


As with phishing sites, Microsoft keeps track of how many people visit each malware hosting site and uses the information to improve the SmartScreen Filter and to better combat malware distribution.

Types of Malware Distributed over the Web

Figure 89 shows the category breakdown for threats hosted at URLs blocked by the SmartScreen Filter in 1H09 and 2H09.

FIGURE 89. Threats hosted at URLs blocked by the SmartScreen Filter, by category, in 1H09 and 2H09



The Miscellaneous Potentially Unwanted Software and Miscellaneous Trojans categories dominated the list in both periods. The Trojan Downloaders & Droppers category, which was nearly as prevalent as Miscellaneous Trojans in 1H09, fell by nearly 50 percent in the second half of the year, but Exploits more than doubled. Comparing this data to Figure 49 on page 81, which shows threat category trends over time as detected by all Microsoft desktop anti-malware products, reveals a number of notable similarities and differences:

- The Miscellaneous Potentially Unwanted Software category accounted for 43.9 percent of malware impressions in 2H09, but the percent of computers cleaned remained much lower, at 13.3 percent. (A *malware impression* is a single instance of an Internet Explorer user attempting to visit a site known to host malware and being blocked.) This suggests that SmartScreen and similar technologies may be having a measurable amount of success in protecting users from being infected by these threats at all, thereby ensuring that they are not present on the computer for desktop security products to detect.

- By contrast, worms are rarely distributed by malicious Web sites, accounting for just 1.3 percent of SmartScreen impressions, compared to 15.6 percent of computers cleaned. Worms are designed to spread by sending copies of themselves to other computers, using mechanisms like e-mail, instant messaging (IM), cross-site scripting, and vulnerabilities in network protocols. They are therefore typically less dependent on distribution methods like malicious Web sites than other types of malware.
- Exploits, which accounted for just 2.0 percent of computers cleaned, increased sharply to 13.1 percent of malware impressions in 2H09.[26] Most of these involved malicious Portable Document Format (PDF) files that exploited a number of vulnerabilities in versions of Adobe Reader. Attackers often use exploits to install other malware on victims' computers by taking advantage of vulnerabilities in Web browsers and other popular software. (See "Exploit Trends," beginning on page 25, for more information.)

Figure 90 lists the top 10 malware and potentially unwanted software families blocked by the SmartScreen Filter in 2H09, by user impression.

FIGURE 90. The top 10 malware families hosted on sites blocked by the Internet Explorer 8 SmartScreen Filter in 2H09

Rank	Family	Most Significant Category	Percent of Malware Impressions
1	Win32/MoneyTree	Misc. Potentially Unwanted Software	31.6%
2	Win32/CeeInject	Misc. Potentially Unwanted Software	9.1%
3	Win32/Pdfjsc	Exploits	8.9%
4	Win32/Winwebsec	Miscellaneous Trojans	8.1%
5	Win32/Banload	Trojan Downloaders & Droppers	3.8%
6	Win32/Bancos	Password Stealers & Monitoring Tools	2.8%
7	Win32/Swif	Miscellaneous Trojans	2.4%
8	Win32/Small	Trojan Downloaders & Droppers	1.8%
9	Win32/Renos	Trojan Downloaders & Droppers	1.4%
10	Win32/PrivacyCenter	Miscellaneous Trojans	1.4%

[26] The SmartScreen filter monitors the distribution of malware in downloadable files. The figures presented here for exploits do not include exploits that target the browser itself or browser add-ons.

Encyclopedia

Win32/MoneyTree: A family of software that provides the ability to search for adult content on the local computer. It may also install other potentially unwanted software, such as programs that display pop-up ads.

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

Win32/Swif: A trojan that exploits a vulnerability in Adobe Flash Player to download malicious files. Adobe has published security bulletin APSB08-11 addressing the vulnerability.

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

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

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

http://www.microsoft.com/av

Overall, sites hosting these 10 families constituted 71.2 percent of all malware impressions. Coincidentally, this is almost exactly the same share accounted for by the top 10 families in 1H09 (71.4 percent) and 2H08 (71.2 percent), though the list of the top families has changed from period to period. Win32/MoneyTree, the family most detected and blocked by the SmartScreen Filter, remained roughly stable (31.6 percent in 2H09, down from 32.8 percent in 1H09), while Win32/CeeInject, which was not among the top 10 families most detected by the filter in 1H09, rose to second place during the latter half of the year. CeeInject is actually a generic detection for a group of programs that malware authors use to inject code into other running applications.

Win32/Pdfjsc and Win32/Swif are generic detections for malicious Portable Document Format (PDF) files and Adobe Flash files, two types of media that are common on the Internet. Among the top 10 families, Pdfjsc and Swif had the most impressions per distribution point in 2H09, while the widespread trojan downloader Win32/Renos had the fewest.

Win32/Banload and Win32/Bancos are two related families that target users of online banking and financial services. These families primarily target customers of Brazilian banks and use Portuguese-language text strings and social engineering tactics.[27]

Geographic Distribution of Malware Hosting Sites

While more malware distribution sites are discovered on a daily basis than phishing sites, malware hosting tends to be more stable and less geographically diverse. This is probably due to the relatively recent use of server takedowns and Web reputation as weapons in the fight against malware distribution, which means that malware distributors have not been forced to diversify their hosting arrangements, as phishers have. As Internet Explorer 8 becomes more widely used, malware distributors may be expected to behave more like phishers, moving their operations more frequently to avoid detection and shutdown.

Figure 91 and Figure 92 show the geographic distribution of malware hosting sites reported to Microsoft in 2H09, around the world and in the United States.

[27] See "Online Banking Malware" on page 23 of *Microsoft Security Intelligence Report, Volume 6 (July through December 2008)* for more information about this type of threat.

FIGURE 91. Malware distribution sites per 1,000 Internet hosts for locations around the world in 2H09

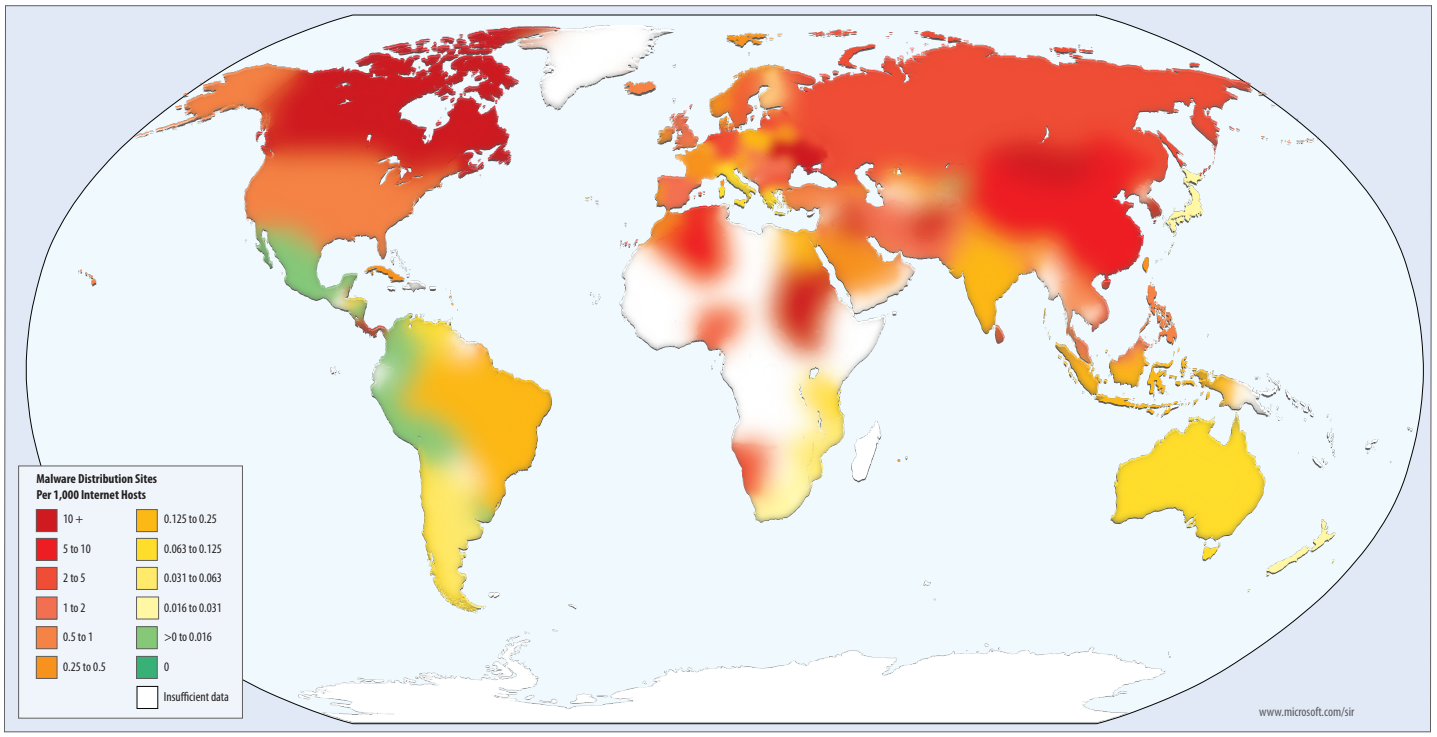
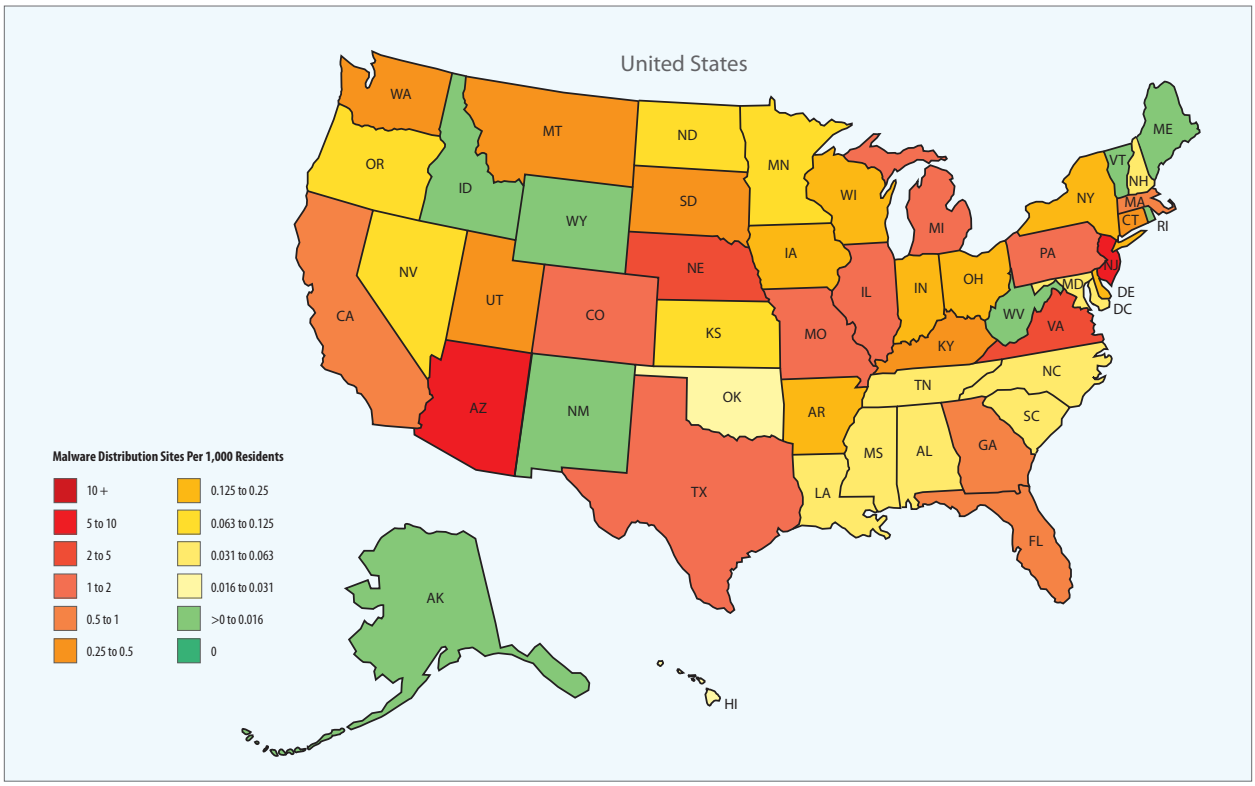


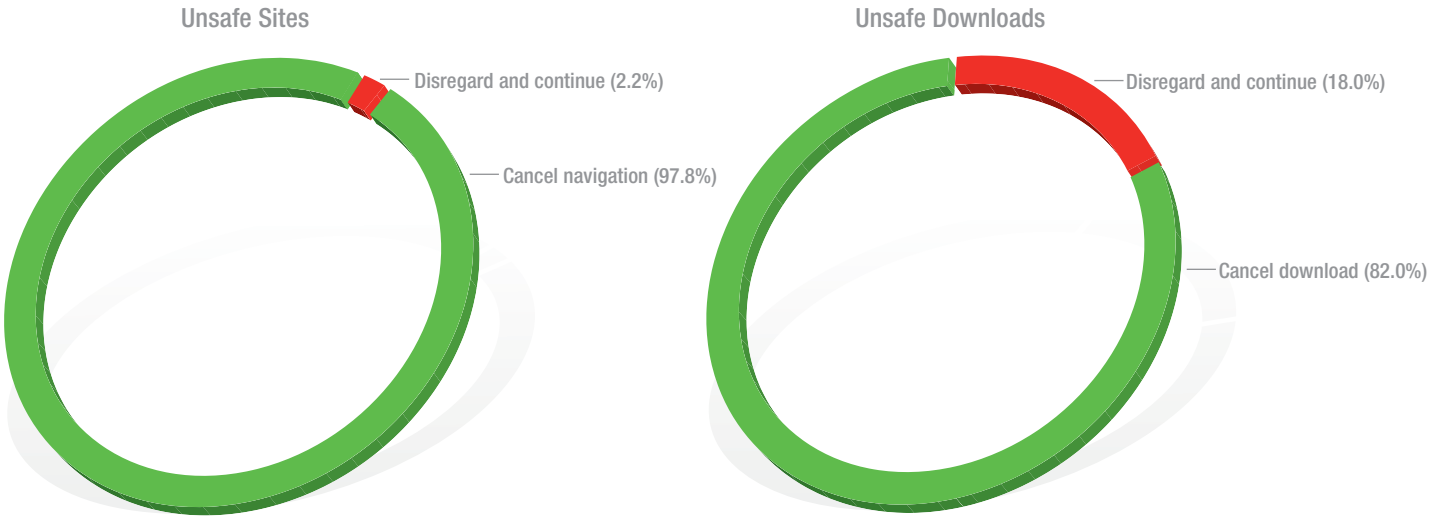
FIGURE 92. Malware distribution sites per 1,000 residents by U.S. state in 2H09



User Reaction to SmartScreen Warnings

When the SmartScreen Filter and Phishing Filter block access to reported malware and phishing sites, they give the user the option of disregarding the warning and continuing to the potentially unsafe content. Likewise, when the SmartScreen Filter in Internet Explorer 8 displays an unsafe download warning, the user may choose to dismiss the warning dialog box and download the unsafe file anyway. By default, the SmartScreen Filter reports aggregate information about how often users choose to disregard these warnings, providing insights into user reactions to Internet-based threats and the efficacy of different kinds of warnings. (See "User Reaction to Alerts," beginning on page 87, for another perspective on user reactions based on telemetry from Microsoft desktop anti-malware products).

FIGURE 93. Percentages of users who disregard SmartScreen unsafe content warnings



In a sample of data collected during the first few weeks of 2010, when blocked from viewing a reported phishing or malware distribution site, users chose to disregard the warning and continue to the unsafe site just 2.2 percent of the time. By contrast, users disregarded the Unsafe Download dialog box much more frequently. Users chose to download the unsafe content 18.0 percent of the time and clicked **Cancel** just 82.0 percent of the time. (See "Promote Safe Browsing," on page 223, for guidance about using Group Policy to enforce SmartScreen Filter warnings throughout your organization.)

Part of this discrepancy may be due to the different nature of the two different warnings. The Unsafe Website screen (see Figure 81 on page 117) requires two clicks to dismiss. The user must first click **More information**, which displays additional information about the threat, and then click **Disregard and continue (not recommended)**. By contrast, when the SmartScreen Filter displays the Unsafe Download dialog box (see Figure 88 on page 123), the user can continue the download by clicking **Disregard and download unsafe file (not recommended)**, requiring just one click instead of two.

Malware Patterns Around the World

Malware is a global problem that affects different parts of the world in different ways. The next several pages feature data collected by the Microsoft Malware Protection Center for countries and regions around the world, including detailed statistics for 26 individual locations.

Full Geographic Data

The "Geographic Trends" section, beginning on page 71, explains how threat patterns differ significantly in different parts of the world. Figure 94 shows the infection rate in 213 different locations around the world, derived from averaging each location's monthly CCM for each of the six months in 2H09. (CCM is the number of computers cleaned for every 1,000 executions of the MSRT. See "Infection Rates and CCM," on page 71, for more information about the CCM metric.)

FIGURE 94. Infection rates for locations around the world, by CCM, in 2H09

Country/Region	CCM	Country/Region	CCM	Country/Region	CCM
Afghanistan	5.0	Burkina Faso	3.7	Faroe Islands	3.2
Albania	3.6	Burundi	5.3	Fiji	2.8
Algeria	1.5	Cambodia	2.3	Finland	1.4
American Samoa	9.3	Cameroon	3.0	France	5.6
Andorra	2.0	Canada	2.5	French Guiana	1.8
Angola	5.2	Cape Verde	11.1	French Polynesia	3.0
Anguilla	2.9	Cayman Islands	1.3	Gabon	4.8
Antigua and Barbuda	0.9	Central African Republic	18.0	Gambia, The	6.2
Argentina	4.7	Chad	24.9	Georgia	5.8
Armenia	3.7	Chile	6.7	Germany	2.2
Aruba	3.2	China	7.0	Ghana	1.5
Australia	3.4	Colombia	9.1	Gibraltar	2.6
Austria	1.7	Comoros	21.7	Greece	7.7
Azerbaijan	2.8	Congo (DRC)	4.0	Greenland	6.1
Bahamas, The	5.8	Congo	3.7	Grenada	1.9
Bahrain	15.5	Costa Rica	6.6	Guadeloupe	2.2
Bangladesh	1.1	Côte d'Ivoire	1.8	Guam	0.7
Barbados	1.7	Croatia	8.9	Guatemala	12.5
Belarus	1.5	Cuba	3.9	Guernsey	0.5
Belgium	3.3	Cyprus	4.7	Guinea	3.8
Belize	3.6	Czech Republic	4.1	Guinea-Bissau	36.2
Benin	3.2	Denmark	2.5	Guyana	1.4
Bermuda	1.7	Dominica	4.2	Haiti	3.5
Bhutan	3.0	Dominican Republic	5.3	Honduras	9.1
Bolivia	4.7	Ecuador	7.6	Hong Kong S.A.R.	6.0
Bosnia and Herzegovina	6.8	Egypt	8.6	Hungary	8.9
Botswana	4.6	El Salvador	9.2	Iceland	3.9
Brazil	18.0	Equatorial Guinea	3.6	India	2.6
British Indian Ocean Territory	15.3	Estonia	3.4	Indonesia	3.5
British Virgin Islands	16.9	Ethiopia	1.1	Iran	5.8
Brunei	4.4	Falkland Islands (Islas Malvinas)	10.7	Iraq	7.5
Bulgaria	5.3			Ireland	3.5

(Continued on next page)

FIGURE 94. Continued

Country/Region	CCM
Israel	7.3
Italy	5.3
Jamaica	2.3
Japan	2.3
Jordan	6.6
Kazakhstan	1.8
Kenya	1.9
Korea	16.0
Kuwait	9.3
Kyrgyzstan	1.8
Laos	4.0
Latvia	6.2
Lebanon	5.7
Lesotho	9.3
Liberia	4.2
Libya	3.5
Liechtenstein	0.9
Lithuania	6.3
Luxembourg	3.7
Macao S.A.R.	2.0
Macedonia, F.Y.R.O.	5.6
Madagascar	1.0
Malawi	3.8
Malaysia	4.0
Maldives	2.5
Mali	3.6
Malta	4.1
Martinique	1.9
Mauritania	2.0
Mauritius	2.8
Mayotte	7.0
Mexico	10.0
Micronesia	16.9
Moldova	2.0
Monaco	0.8
Mongolia	1.3
Morocco	1.8
Mozambique	4.6
Myanmar	1.1
Namibia	7.4

Country/Region	CCM
Nepal	1.8
Netherlands	3.3
Netherlands Antilles	1.8
New Caledonia	1.7
New Zealand	3.0
Nicaragua	6.6
Niger	3.7
Nigeria	3.0
Northern Mariana Islands	0.9
Norway	2.5
Oman	6.1
Pakistan	2.2
Palau	9.2
Palestinian Authority	4.4
Panama	5.9
Papua New Guinea	9.7
Paraguay	3.2
Peru	6.4
Philippines	1.7
Poland	11.0
Portugal	13.6
Puerto Rico	2.4
Qatar	5.4
Réunion	1.3
Romania	4.0
Russia	9.8
Rwanda	1.6
Saint Kitts and Nevis	3.5
Saint Lucia	5.1
Saint Vincent and the Grenadines	1.3
Samoa	6.5
San Marino	1.1
São Tomé and Príncipe	11.5
Saudi Arabia	13.0
Senegal	1.7
Serbia and Montenegro*	8.1
Seychelles	4.7
Sierra Leone	6.3
Singapore	4.6

Country/Region	CCM
Slovakia	4.5
Slovenia	6.0
Solomon Islands	7.9
Somalia	23.9
South Africa	4.8
Spain	17.1
Sri Lanka	1.9
Sudan	4.5
Suriname	2.0
Swaziland	10.0
Sweden	2.8
Switzerland	2.3
Syria	4.8
Taiwan	16.7
Tajikistan	3.9
Tanzania	2.8
Thailand	9.8
Timor-Leste	18.4
Togo	1.6
Tonga	10.7
Trinidad and Tobago	3.4
Tunisia	1.4
Turkey	20.0
Turkmenistan	7.2
Turks and Caicos Islands	3.5
Uganda	2.9
Ukraine	2.9
United Arab Emirates	5.8
United Kingdom	4.1
United States	7.8
Uruguay	2.6
Uzbekistan	4.2
Vanuatu	16.2
Venezuela	4.5
Vietnam	1.8
Virgin Islands	1.6
Yemen	5.1
Zambia	7.2
Zimbabwe	17.8
Worldwide	**7.0**

(* Figure reflects the combined markets of Montenegro and Serbia for 2H09.)

Figure 11, on page 34, illustrates the geographic distribution of drive-by download sites by country-code top-level domain (ccTLD). Figure 95 shows the data for individual ccTLDs.

FIGURE 95. Percentage of Web sites in each ccTLD that hosted drive-by download pages in 2H09

TLD	Associated Country/ Region	Percent of Sites
.ac	Ascension Island	0.25%
.ad	Andorra	0.57%
.ae	United Arab Emirates	0.37%
.af	Afghanistan	0.45%
.ag	Antigua and Barbuda	0.09%
.al	Albania	0.17%
.am	Armenia	0.38%
.an	Netherlands Antilles	0.33%
.ar	Argentina	0.47%
.as	American Samoa	0.07%
.at	Austria	0.11%
.au	Australia	0.26%
.az	Azerbaijan	1.73%
.ba	Bosnia and Herzegovina	0.47%
.bb	Barbados	0.65%
.bd	Bangladesh	2.70%
.be	Belgium	0.17%
.bf	Burkina Faso	0.71%
.bg	Bulgaria	0.27%
.bm	Bermuda	0.14%
.bo	Bolivia	0.12%
.br	Brazil	0.31%
.bt	Bhutan	2.51%
.bw	Botswana	0.16%
.by	Belarus	0.73%
.bz	Belize	0.11%
.ca	Canada	0.17%
.cc	Cocos (Keeling) Islands	0.67%
.cd	Congo (DRC)	0.40%
.ch	Switzerland	0.10%
.cl	Chile	0.36%
.cm	Cameroon	0.30%
.cn	China	0.98%
.co	Colombia	0.27%
.cr	Costa Rica	0.17%
.cu	Cuba	0.15%
.cx	Christmas Island	0.05%
.cy	Cyprus	0.20%
.cz	Czech Republic	0.51%
.de	Germany	0.09%
.dk	Denmark	0.10%
.do	Dominican Republic	0.26%
.dz	Algeria	0.48%
.ec	Ecuador	0.27%
.ee	Estonia	0.22%
.eg	Egypt	0.87%
.es	Spain	0.30%
.et	Ethiopia	1.32%
.eu	European Union	0.21%
.fi	Finland	0.11%
.fj	Fiji	0.95%
.fm	Micronesia	0.11%
.fr	France	0.07%
.gd	Grenada	0.45%
.ge	Georgia	1.43%
.gf	French Guiana	1.35%
.gg	Guernsey	0.05%
.gr	Greece	0.28%
.gs	South Georgia and the South Sandwich Islands	0.09%
.gt	Guatemala	0.33%
.hk	Hong Kong S.A.R.	0.25%
.hn	Honduras	0.56%
.hr	Croatia	0.24%
.ht	Haiti	0.25%
.hu	Hungary	0.51%
.id	Indonesia	0.29%
.ie	Ireland	0.22%
.il	Israel	0.33%

(Continued on next page)

FIGURE 95. Continued

TLD	Associated Country/ Region	Percent of Sites
.im	Isle of Man	0.40%
.in	India	0.95%
.io	British Indian Ocean Territory	0.16%
.iq	Iraq	3.39%
.ir	Iran	1.46%
.is	Iceland	0.09%
.it	Italy	0.20%
.jo	Jordan	0.68%
.jp	Japan	0.11%
.ke	Kenya	0.21%
.kg	Kyrgyzstan	0.45%
.kh	Cambodia	1.00%
.ki	Kiribati	0.12%
.km	Comoros	9.09%
.kr	Korea	0.65%
.kw	Kuwait	0.63%
.ky	Cayman Islands	0.12%
.kz	Kazakhstan	0.35%
.la	Laos	0.62%
.lb	Lebanon	0.21%
.lc	Saint Lucia	0.85%
.li	Liechtenstein	0.09%
.lk	Sri Lanka	0.61%
.lt	Lithuania	0.29%
.lu	Luxembourg	0.04%
.lv	Latvia	0.29%
.ly	Libya	1.02%
.ma	Morocco	0.37%
.mc	Monaco	0.20%
.md	Moldova	0.36%
.me	Montenegro	0.01%
.mg	Madagascar	0.16%
.mk	Macedonia, F.Y.R.O.	0.18%
.ml	Mali	1.47%
.mn	Mongolia	0.43%
.mo	Macao S.A.R.	0.11%
.mq	Martinique	3.85%
.ms	Montserrat	0.04%

TLD	Associated Country/ Region	Percent of Sites
.mt	Malta	0.45%
.mu	Mauritius	0.11%
.mx	Mexico	0.24%
.my	Malaysia	0.45%
.na	Namibia	0.06%
.nf	Norfolk Island	0.11%
.ng	Nigeria	0.51%
.nl	Netherlands	0.13%
.no	Norway	0.10%
.np	Nepal	0.94%
.nr	Nauru	0.25%
.nu	Niue	0.08%
.nz	New Zealand	0.09%
.om	Oman	1.58%
.pa	Panama	0.12%
.pe	Peru	0.66%
.ph	Philippines	0.09%
.pk	Pakistan	0.93%
.pl	Poland	0.39%
.ps	Palestinian Authority	0.82%
.pt	Portugal	0.15%
.py	Paraguay	0.28%
.qa	Qatar	0.29%
.re	Réunion	0.39%
.ro	Romania	0.46%
.rs	Serbia	0.48%
.ru	Russia	0.53%
.sa	Saudi Arabia	0.49%
.sc	Seychelles	0.13%
.se	Sweden	0.12%
.sg	Singapore	0.26%
.sh	Saint Helena	0.08%
.si	Slovenia	0.27%
.sk	Slovakia	0.54%
.sn	Senegal	0.57%
.st	São Tomé and Príncipe	0.06%
.sv	El Salvador	0.23%
.sy	Syria	0.22%

TLD	Associated Country/ Region	Percent of Sites
.sz	Swaziland	0.60%
.tc	Turks and Caicos Islands	0.04%
.tf	French Southern and Antarctic Lands	0.03%
.tg	Togo	0.76%
.th	Thailand	2.16%
.tj	Tajikistan	3.51%
.tk	Tokelau	0.51%
.tn	Tunisia	0.49%
.to	Tonga	0.13%
.tr	Turkey	1.31%
.tt	Trinidad and Tobago	0.09%
.tv	Tuvalu	0.28%
.tw	Taiwan	0.44%
.tz	Tanzania	0.52%
.ua	Ukraine	0.46%
.ug	Uganda	0.56%
.uk	United Kingdom	0.16%
.us	United States	0.16%
.uy	Uruguay	0.24%
.uz	Uzbekistan	0.57%
.vc	Saint Vincent and the Grenadines	0.11%
.ve	Venezuela	0.17%
.vg	British Virgin Islands	0.05%
.vi	Virgin Islands	0.51%
.vn	Vietnam	0.73%
.vu	Vanuatu	0.04%
.ws	Samoa	0.24%
.ye	Yemen	0.44%
.za	South Africa	0.19%
	Worldwide	**0.24%**

Figure 26, on page 49, illustrates the geographic distribution of Web sites attacked using automated SQL injection tools, by country-code top-level domain (ccTLD). Figure 96 shows the data for individual ccTLDs.

FIGURE 96. Percentage of Web sites in each ccTLD victimized by automated SQL injection attacks in 2H09

TLD	Associated Country/ Region	Percent of Sites
.ad	Andorra	0.142%
.ae	United Arab Emirates	0.086%
.ar	Argentina	0.014%
.at	Austria	0.005%
.au	Australia	0.014%
.az	Azerbaijan	0.032%
.bd	Bangladesh	0.104%
.be	Belgium	0.010%
.bf	Burkina Faso	0.474%
.bg	Bulgaria	0.004%
.bm	Bermuda	0.138%
.bn	Brunei	0.162%
.bo	Bolivia	0.120%
.br	Brazil	0.036%
.ca	Canada	0.010%
.cc	Cocos (Keeling) Islands	0.009%
.ch	Switzerland	0.003%
.cl	Chile	0.038%
.cn	China	0.036%
.co	Colombia	0.020%
.cr	Costa Rica	0.115%
.cu	Cuba	0.098%
.cz	Czech Republic	0.003%
.de	Germany	0.001%
.dk	Denmark	0.009%
.do	Dominican Republic	0.097%
.ec	Ecuador	0.026%
.ee	Estonia	0.003%
.eg	Egypt	0.131%
.es	Spain	0.017%
.eu	European Union	0.008%
.fi	Finland	0.002%
.fo	Faroe Islands	0.452%
.fr	France	0.002%
.gr	Greece	0.029%
.hk	Hong Kong S.A.R.	0.036%
.hr	Croatia	0.006%
.id	Indonesia	0.027%
.ie	Ireland	0.034%
.il	Israel	0.055%
.in	India	0.052%
.ir	Iran	0.043%
.is	Iceland	0.004%
.it	Italy	0.014%
.jp	Japan	0.001%
.kr	Korea	0.360%
.kw	Kuwait	0.209%
.lb	Lebanon	0.071%
.lu	Luxembourg	0.018%
.lv	Latvia	0.003%
.ma	Morocco	0.085%
.mc	Monaco	0.394%
.mm	Myanmar	2.256%
.mt	Malta	0.101%
.mv	Maldives	0.150%
.mx	Mexico	0.015%
.my	Malaysia	0.010%
.ng	Nigeria	0.127%
.nl	Netherlands	0.005%
.no	Norway	0.017%
.nu	Niue	0.020%
.nz	New Zealand	0.005%
.om	Oman	0.264%
.pe	Peru	0.077%
.ph	Philippines	0.011%
.pk	Pakistan	0.148%
.pl	Poland	0.002%
.ps	Palestinian Authority	0.075%
.pt	Portugal	0.025%
.qa	Qatar	0.143%
.ru	Russia	0.004%
.sa	Saudi Arabia	0.106%
.sc	Seychelles	0.065%
.sd	Sudan	0.324%
.se	Sweden	0.012%
.sg	Singapore	0.048%
.si	Slovenia	0.007%
.sk	Slovakia	0.002%
.sn	Senegal	0.190%
.th	Thailand	0.106%
.to	Tonga	0.003%
.tr	Turkey	0.012%
.tv	Tuvalu	0.007%
.tw	Taiwan	0.033%
.tz	Tanzania	0.693%
.uk	United Kingdom	0.008%
.us	United States	0.004%
.uy	Uruguay	0.038%
.uz	Uzbekistan	0.022%
.ve	Venezuela	0.024%
.vn	Vietnam	0.058%
.ws	Samoa	0.007%
.za	South Africa	0.034%
.zw	Zimbabwe	0.101%
	Worldwide	**0.011%**

The "Malicious Web Sites" section, beginning on page 116, includes world and U.S. maps showing the geographic distribution of sites hosting malware and phishing pages. Figure 97 through Figure 100 show the data for the individual locations depicted on the maps.

FIGURE 97. Phishing sites per 1,000 Internet hosts for locations around the world in 2H09

Country/Region	Phishing Sites Per 1,000 Internet Hosts	Country/Region	Phishing Sites Per 1,000 Internet Hosts
Albania	0.07	Ecuador	0.36
Algeria	15.69	Egypt	0.46
Andorra	0.34	El Salvador	0.49
Argentina	0.06	Estonia	0.08
Armenia	0.25	Finland	0.09
Australia	0.18	France	0.80
Austria	0.15	French Polynesia	0.07
Azerbaijan	0.99	Georgia	2.35
Bahamas, The	1.68	Germany	0.47
Bahrain	0.17	Greece	0.05
Bangladesh	9.03	Guam	47.62
Belarus	2.06	Guatemala	0.27
Belgium	0.69	Hong Kong S.A.R.	1.30
Bhutan	2.64	Hungary	3.49
Bolivia	0.06	Iceland	0.09
Bosnia and Herzegovina	2.08	India	1.08
Botswana	0.14	Indonesia	1.29
Brazil	0.04	Iran	2.32
Brunei	0.80	Iraq	181.82
Bulgaria	2.22	Ireland	0.68
Cambodia	1.21	Israel	2.29
Canada	1.49	Italy	0.32
Cayman Islands	0.05	Jamaica	87.60
Chile	1.67	Japan	0.08
China	0.31	Jordan	0.48
Colombia	0.04	Kazakhstan	8.04
Costa Rica	0.18	Kenya	0.09
Côte d'Ivoire	0.20	Korea	81.26
Croatia	0.16	Kuwait	9.98
Cuba	1.65	Kyrgyzstan	0.10
Cyprus	0.51	Latvia	0.96
Czech Republic	0.64	Lebanon	0.42
Denmark	0.31	Lithuania	0.37
Dominican Republic	0.07	Luxembourg	1.64

(Continued on next page)

FIGURE 97. Continued

Country/Region	Phishing Sites Per 1,000 Internet Hosts
Macao S.A.R.	8.20
Macedonia, F.Y.R.O.	2.20
Malaysia	5.36
Malta	3.38
Mexico	0.02
Moldova	0.18
Monaco	0.04
Mongolia	87.79
Montenegro	4.93
Morocco	0.76
Namibia	0.22
Nepal	0.62
Netherlands	0.60
Netherlands Antilles	0.01
New Zealand	0.55
Nicaragua	0.10
Nigeria	7.29
Norway	0.35
Pakistan	0.62
Panama	5.08
Paraguay	0.03
Peru	0.24
Philippines	3.59
Poland	1.80
Portugal	0.68
Puerto Rico	838.57
Qatar	65.10
Romania	6.29
Russia	1.32
San Marino	4.75
Saudi Arabia	0.48
Serbia	1.42
Seychelles	15.43
Singapore	0.58
Slovakia	0.88
Slovenia	26.94
South Africa	0.10
Spain	2.44
Sri Lanka	6.57
Sudan	83.33
Sweden	0.54
Switzerland	0.24
Taiwan	2.87
Tajikistan	13.17
Tanzania	0.85
Thailand	2.61
Tonga	0.10
Trinidad and Tobago	0.12
Turkey	1.25
Turkmenistan	3.97
Uganda	1.48
Ukraine	4.77
United Arab Emirates	0.05
United Kingdom	1.23
United States	0.37
Uzbekistan	0.04
Venezuela	0.32
Vietnam	3.62
Yemen	53.72
Worldwide	**0.54**

FIGURE 98. Phishing sites per 1,000 residents by U.S. state in 2H09

State	Phishing Sites Per 1,000 Residents
Alabama	0.008
Alaska	0.011
Arizona	0.364
Arkansas	0.026
California	0.426
Colorado	0.374
Connecticut	0.058
Delaware	0.494
Florida	0.390
Georgia	1.688
Hawaii	0.003
Idaho	0.008
Illinois	1.126
Indiana	0.033
Iowa	0.016
Kansas	0.057
Kentucky	0.149
Louisiana	0.015
Maine	0.053
Maryland	0.083
Massachusetts	0.393
Michigan	0.530
Minnesota	0.014
Mississippi	0.018
Missouri	0.257
Montana	0.031
Nebraska	0.344
Nevada	0.307
New Hampshire	0.275
New Jersey	0.673
New Mexico	0.005
New York	0.367
North Carolina	0.116
North Dakota	0.003
Ohio	0.322
Oklahoma	0.082
Oregon	0.150
Pennsylvania	0.194
Rhode Island	0.006
South Carolina	0.015
South Dakota	0.025
Tennessee	0.008
Texas	1.163
Utah	1.766
Vermont	0.005
Virginia	0.479
Washington	1.641
West Virginia	0.004
Wisconsin	0.019
Wyoming	0.002
U.S.	**0.46**

FIGURE 99. Malware distribution sites per 1,000 Internet hosts for locations around the world in 2H09

Country/Region	Malware Servers Per 1,000 Internet Hosts	Country/Region	Malware Servers Per 1,000 Internet Hosts
Afghanistan	21.28	Egypt	0.15
Albania	5.05	Estonia	0.70
Algeria	9.80	Fiji	1.02
Andorra	0.09	Finland	0.02
Anguilla	50.39	France	0.43
Antigua and Barbuda	89.48	Georgia	3.27
Argentina	0.04	Germany	3.28
Armenia	0.17	Gibraltar	3.07
Australia	0.07	Greece	0.10
Austria	0.21	Guam	23.81
Azerbaijan	0.43	Honduras	0.06
Bahamas, The	112.79	Hong Kong S.A.R.	4.95
Bahrain	0.18	Hungary	0.51
Bangladesh	3.33	Iceland	0.54
Barbados	4.26	India	0.13
Belarus	0.38	Indonesia	0.13
Belgium	0.09	Iran	1.95
Belize	1797.15*	Iraq	90.91
Bermuda	0.45	Ireland	0.26
Bolivia	0.01	Israel	7.41
Bosnia and Herzegovina	2.16	Italy	0.12
Brazil	0.16	Jamaica	254.73
British Virgin Islands	786.58	Japan	0.02
Brunei	0.07	Jordan	7.03
Bulgaria	3.95	Kazakhstan	3.11
Canada	20.44	Korea	30.66
Cayman Islands	9.99	Kuwait	6.51
Chile	0.08	Kyrgyzstan	0.01
China	9.03	Laos	0.60
Colombia	0.01	Latvia	3.01
Costa Rica	25.83	Lebanon	0.86
Croatia	0.06	Lithuania	2.09
Cuba	0.28	Luxembourg	27.76
Cyprus	79.31	Macao S.A.R.	151.64
Czech Republic	0.84	Macedonia, F.Y.R.O.	2.82
Denmark	0.32	Malaysia	1.55

* Figures can exceed 100 percent of hosts for a given location because a single host can include many Web sites.

(Continued on next page)

FIGURE 99. Continued

Country/Region	Malware Servers Per 1,000 Internet Hosts
Malta	47.10
Mauritius	0.04
Mexico	0.01
Moldova	0.88
Monaco	0.09
Mongolia	15.27
Montenegro	24.35
Morocco	0.36
Mozambique	0.05
Namibia	4.04
Nepal	0.09
Netherlands	5.06
New Zealand	0.02
Nicaragua	0.01
Nigeria	3.64
Northern Mariana Islands	111.11
Norway	0.42
Pakistan	1.03
Panama	45.49
Peru	0.01
Philippines	0.93
Poland	0.21
Portugal	0.26
Puerto Rico	370.00
Qatar	2.77
Romania	1.05
Russia	2.23
Saint Kitts and Nevis	37.74
Saint Vincent and the Grenadines	33.15
San Marino	0.15
Saudi Arabia	0.31
Serbia	1.70
Seychelles	314.82
Singapore	0.22
Slovakia	1.09
Slovenia	8.32
South Africa	0.03
Spain	1.14
Sri Lanka	2.46
Sudan	41.67
Sweden	2.43
Switzerland	0.41
Taiwan	0.35
Tanzania	0.08
Thailand	0.80
Trinidad and Tobago	0.44
Turkey	0.74
Ukraine	27.05
United Arab Emirates	0.49
United Kingdom	1.02
United States	0.79
Uruguay	0.01
Uzbekistan	0.14
Venezuela	0.08
Vietnam	3.53
Virgin Islands	0.23
Zimbabwe	0.03
Worldwide	**1.30**

FIGURE 100. Malware distribution sites per 1,000 residents by U.S. state in 2H09

State	Malware Servers Per 1,000 Residents
Alabama	0.033
Alaska	0.007
Arizona	7.961
Arkansas	0.149
California	0.860
Colorado	1.568
Connecticut	0.292
Delaware	0.190
Florida	0.774
Georgia	0.706
Hawaii	0.027
Idaho	0.005
Illinois	1.104
Indiana	0.219
Iowa	0.138
Kansas	0.066
Kentucky	0.330
Louisiana	0.041
Maine	0.014
Maryland	0.041
Massachusetts	0.527
Michigan	1.120
Minnesota	0.106
Mississippi	0.045
Missouri	1.042
Montana	0.315
Nebraska	2.128
Nevada	0.094
New Hampshire	0.056
New Jersey	5.010
New Mexico	0.001
New York	0.212
North Carolina	0.034
North Dakota	0.087
Ohio	0.146
Oklahoma	0.018
Oregon	0.076
Pennsylvania	1.340
Rhode Island	0.007
South Carolina	0.062
South Dakota	0.255
Tennessee	0.035
Texas	1.966
Utah	0.342
Vermont	0.005
Virginia	2.169
Washington	0.358
West Virginia	0.005
Wisconsin	0.151
Wyoming	0.007
U.S.	**0.97**

Threat Assessments for Individual Locations

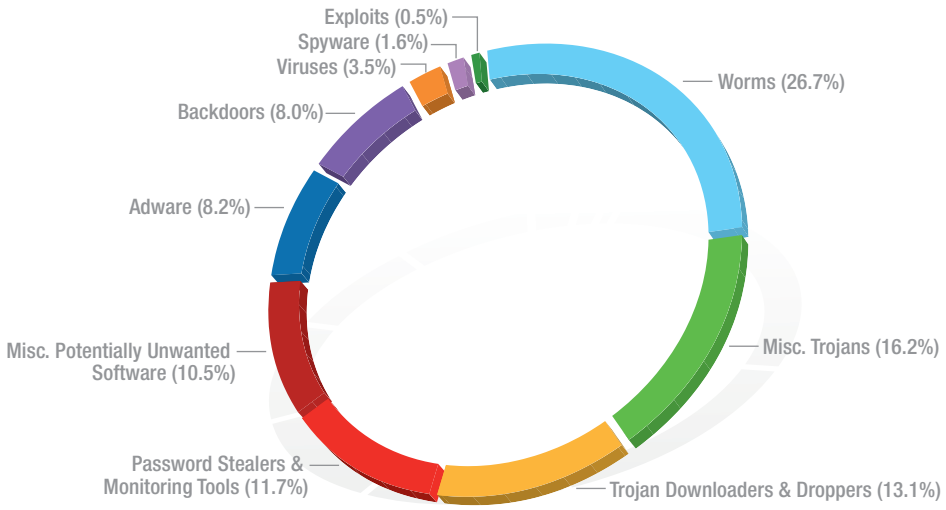
The global threat landscape is evolving, with malware and potentially unwanted software becoming more regional. Starkly different threat patterns are emerging in different locations around the world. The "Geographic Trends" section, beginning on page 71, gives an overview of the way the relative prevalence of different categories of malware varies between different locations. This section provides infection statistics for 26 locations around the world, encompassing every inhabited continent and multiple languages and computer usage patterns.

Argentina

The MSRT detected malware on 4.7 out of every 1,000 computers scanned in Argentina during 2H09 (a CCM score of 4.7—up slightly from 4.5 in 1H09 but significantly lower than the average worldwide CCM of 7.0). Figure 101 and Figure 102 list the malware and potentially unwanted software categories and families detected by all Microsoft desktop anti-malware products in Argentina in 2H09.

FIGURE 101. Malware and potentially unwanted software in Argentina, by category, in 2H09

Category	Infected Computers
Worms	52,400
Miscellaneous Trojans	31,816
Trojan Downloaders & Droppers	25,795
Password Stealers & Monitoring Tools	22,916
Misc. Potentially Unwanted Software	20,702
Adware	16,147
Backdoors	15,669
Viruses	6,842
Spyware	3,189
Exploits	912



Notes and observations:

- The threat landscape in Argentina was dominated by malware, which accounted for 79.7 percent of all threats detected on infected computers in 2H09.
- The most common category in Argentina was Worms. It was detected on 26.7 percent of all infected computers in 2H09 and accounted for 6 of the top 25 families.

- The second-most common category in Argentina was Miscellaneous Trojans, which includes all trojan families that are not classified as downloaders/droppers or backdoors, and accounted for 16.2 percent of all infected computers.
- Together, Miscellaneous Trojans and Trojan Downloaders & Droppers made up almost a third of all families detected on infected computers in Argentina in 2H09.

FIGURE 102. Top 25 families in Argentina in 2H09

Rank	Family	Most Significant Category	Infected Computers
1	Win32/Conficker	Worms	20,498
2	Win32/Taterf	Worms	18,291
3	Win32/C2Lop	Miscellaneous Trojans	9,638
4	Win32/Frethog	Password Stealers & Monitoring Tools	8,977
5	Win32/Bancos	Password Stealers & Monitoring Tools	8,055
6	Win32/IRCbot	Backdoors	7,924
7	Win32/Renos	Trojan Downloaders & Droppers	6,737
8	Win32/Agent	Miscellaneous Trojans	5,178
9	Win32/DoubleD	Adware	4,695
10	Win32/Zlob	Trojan Downloaders & Droppers	4,457
11	Win32/Bredolab	Trojan Downloaders & Droppers	4,376
12	Win32/Cutwail	Trojan Downloaders & Droppers	4,266
13	Win32/Slenfbot	Worms	4,257
14	Win32/Hamweq	Worms	3,959
15	Win32/Vundo	Miscellaneous Trojans	3,813
16	Win32/SeekmoSearchAssistant	Adware	3,756
17	Win32/Autorun	Worms	3,653
18	Win32/Brontok	Worms	3,652
19	Win32/Alureon	Miscellaneous Trojans	3,350
20	Win32/Rustock	Backdoors	2,697
21	Win32/Cmdow	Misc. Potentially Unwanted Software	2,459
22	Win32/Hotbar	Adware	2,269
23	Win32/Bumat	Miscellaneous Trojans	2,116
24	Win32/ZangoSearchAssistant	Adware	2,044
25	Win32/RealVNC	Misc. Potentially Unwanted Software	2,027

Notes and observations:

- Win32/Conficker, the most prevalent family in Argentina in 2H09, is a worm that infects computers across a network by spreading via removable hard drives, exploiting weak passwords on file shares, or exploiting a vulnerability in the Windows Server service. Infection can result in remote code execution when file sharing is enabled. The worm also disables important system services and some security products and may download arbitrary files.
- Game password stealers were common in Argentina during 2H09. Win32/Taterf and Win32/Frethog, which rank first and sixth in the world respectively, ranked second and fourth in Argentina.
- Win32/C2Lop, a trojan that modifies Web browser settings and delivers contextual and pop-up advertisements, was significantly more prevalent in Argentina than it was worldwide. Win32/C2Lop was the third-most prevalent family in Argentina during 2H09, but it was only twenty-third–most prevalent worldwide. Win32/C2Lop may be distributed in a software package called "MessengerPlus!", an add-on for Windows Live Messenger.

Encyclopedia

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

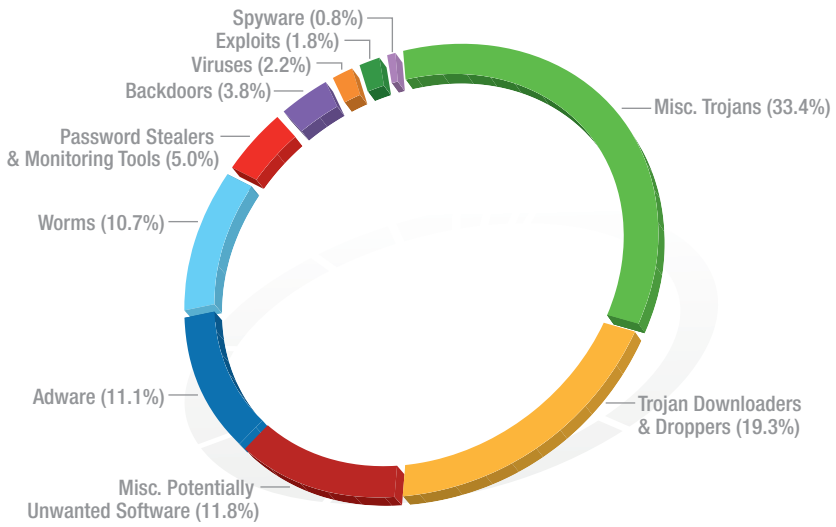
Win32/Frethog: A large family of password-stealing trojans that target confidential data, such as account information, from massively multiplayer online games.

http://www.microsoft.com/av

Australia

The MSRT detected malware on 3.4 out of every 1,000 computers scanned in Australia during 2H09 (a CCM score of 3.4—down from 3.9 in 1H09 and significantly lower than the average worldwide CCM of 7.0). Figure 103 and Figure 104 list the malware and potentially unwanted software categories and families detected by all Microsoft desktop anti-malware products in Australia in 2H09.

FIGURE 103. Malware and potentially unwanted software in Australia, by category, in 2H09



Category	Infected Computers
Misc. Trojans	204,207
Trojan Downloaders & Droppers	117,970
Misc. Potentially Unwanted Software	72,214
Adware	67,915
Worms	65,411
Password Stealers & Monitoring Tools	30,250
Backdoors	23,142
Viruses	13,683
Exploits	11,070
Spyware	5,136

Notes and observations:

- The threat landscape in Australia was dominated by malware, which accounted for 76.2 percent of all threats detected on infected computers in 2H09. This is in line with 1H09, when malware accounted for 75.1 percent of all families detected on infected computers in Australia.
- The most common category in Australia was Miscellaneous Trojans, which includes all trojan families that are not classified as downloaders/droppers or backdoors, and accounted for 33.4 percent of all infected computers.
- The second-most common category in Australia was Trojan Downloaders and Droppers, which accounted for 19.3 percent of all infected computers.
- Together, Miscellaneous Trojans and Trojan Downloaders & Droppers made up more than half of all families detected on infected computers in Australia in 2H09.

FIGURE 104. Top 25 families in Australia in 2H09

Rank	Family	Most Significant Category	Infected Computers
1	Win32/Renos	Trojan Downloaders & Droppers	58,614
2	Win32/Alureon	Miscellaneous Trojans	43,782
3	Win32/FakeXPA	Miscellaneous Trojans	38,461
4	ASX/Wimad	Trojan Downloaders & Droppers	27,918
5	Win32/Agent	Miscellaneous Trojans	22,428
6	Win32/Yektel	Miscellaneous Trojans	21,146
7	Win32/FakeSpypro	Miscellaneous Trojans	20,675
8	Win32/Hotbar	Adware	20,634
9	Win32/ZangoSearchAssistant	Adware	19,528
10	Win32/Koobface	Worms	15,967
11	Win32/Winwebsec	Miscellaneous Trojans	15,210
12	Win32/Conficker	Worms	12,052
13	Win32/PlayMP3z	Adware	11,718
14	Win32/Taterf	Worms	11,568
15	Win32/Hamweq	Worms	10,728
16	Win32/Zlob	Trojan Downloaders & Droppers	9,501
17	Win32/ZangoShoppingreports	Adware	9,438
18	Win32/FakeRean	Miscellaneous Trojans	8,857
19	Win32/Autorun	Worms	8,362
20	Win32/SeekmoSearchAssistant	Adware	7,834
21	Win32/Bredolab	Trojan Downloaders & Droppers	7,795
22	Win32/FakeVimes	Trojan Downloaders & Droppers	7,397
23	Win32/Hiloti	Miscellaneous Trojans	7,379
24	Win32/RealVNC	Misc. Potentially Unwanted Software	7,220
25	Win32/Vundo	Miscellaneous Trojans	6,918

Encyclopedia

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

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

http://www.microsoft.com/av

Notes and observations:

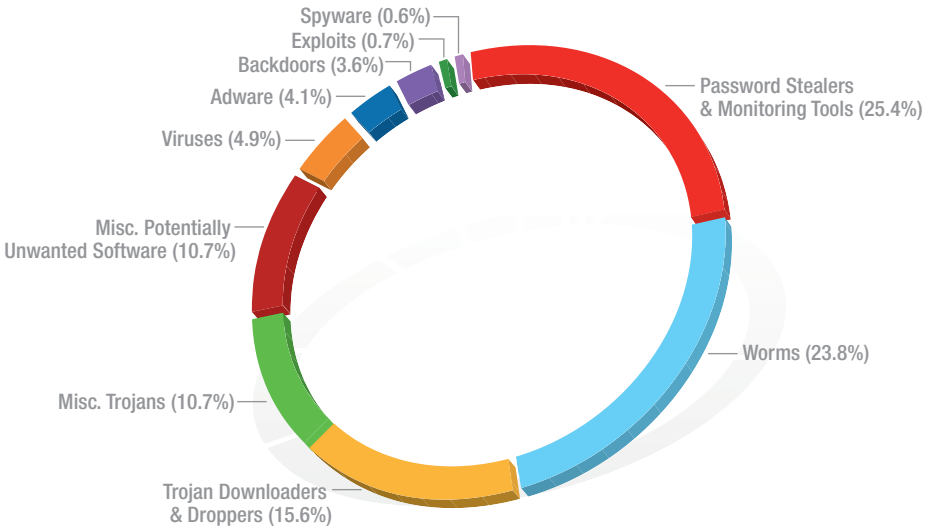
- Win32/Renos, the most prevalent family in Australia in 2H09, is a family of trojan downloaders that install rogue security software. Win32/Renos was the second-most prevalent family detected worldwide during 2H09.
- Game password stealers were not as prevalent in Australia during 2H09 as they were worldwide. Win32/Taterf and Win32/Frethog ranked first and sixth in the world respectively; in Australia, Win32/Taterf ranked only fourteenth and Win32/Frethog did not appear in the top 25 families at all.
- ASX/Wimad was more prevalent in Australia during 2H09 than it was worldwide. ASX/Wimad, a malicious Windows Media file that, when played, opens a specified URL in a Web browser, was the fourth-most prevalent family in Australia during 2H09, but it ranked only twelfth worldwide.
- Win32/PlayMP3z was the thirteenth-most prevalent family detected in Australia during 2H09, but it was not in the top 25 families detected worldwide during the same period. Win32/PlayMP3z is an adware program that displays advertisements in connection with a music player.

Brazil

The MSRT detected malware on 18.0 out of every 1,000 computers scanned in Brazil during 2H09 (a CCM score of 18.0—down from 25.4 in 1H09 and significantly higher than the average worldwide CCM of 7.0). Figure 105 and Figure 106 list the malware and potentially unwanted software categories and families detected by all Microsoft desktop anti-malware products in Brazil in 2H09.

FIGURE 105. Malware and potentially unwanted software in Brazil, by category, in 2H09

Category	Infected Computers
Password Stealers & Monitoring Tools	953,027
Worms	893,071
Trojan Downloaders & Droppers	582,802
Misc. Trojans	399,669
Misc. Potentially Unwanted Software	399,277
Viruses	182,917
Adware	152,690
Backdoors	136,127
Exploits	26,135
Spyware	22,122



Notes and observations:

- The threat landscape in Brazil was dominated by malware, which accounted for 84.7 percent of all threats detected on infected computers in 2H09, down from 90.8 percent in 1H09 and more in line with 2H08, when malware accounted for 83.8 percent of all infected computers.
- The most common category in Brazil was Password Stealers and Monitoring Tools, which accounted for 25.4 percent of all infected computers. This category has decreased from 37.7 percent of the total in 1H09 and 43.7 percent in 2H08.
- The second-most common category in Brazil was Worms, which accounted for 23.8 percent of all infected computers.
- The third-most common category in Brazil was Trojan Downloaders & Droppers, which accounted for 15.6 percent of all infected computers during 2H09. The most common family in this category in Brazil was Win32/Banload, a trojan that downloads password-stealing malware targeting users of online banking.

FIGURE 106. Top 25 families in Brazil in 2H09

Rank	Family	Most Significant Category	Infected Computers
1	Win32/Bancos	Password Stealers & Monitoring Tools	577,261
2	Win32/Taterf	Worms	379,840
3	Win32/Conficker	Worms	308,935
4	Win32/Frethog	Password Stealers & Monitoring Tools	198,827
5	Win32/Banker	Password Stealers & Monitoring Tools	172,603
6	Win32/Banload	Trojan Downloaders & Droppers	169,699
7	Win32/Autorun	Worms	137,467
8	Win32/Small	Trojan Downloaders & Droppers	116,109
9	Win32/Yabector	Miscellaneous Trojans	105,300
10	Win32/Renos	Trojan Downloaders & Droppers	93,970
11	Win32/Hamweq	Worms	90,741
12	ASX/Wimad	Trojan Downloaders & Droppers	89,842
13	Win32/C2Lop	Miscellaneous Trojans	88,627
14	AutoIt/Renocide	Worms	77,084
15	Win32/Agent	Miscellaneous Trojans	73,061
16	Win32/Sality	Viruses	53,621
17	Win32/RealVNC	Misc. Potentially Unwanted Software	49,088
18	Win32/PossibleHostsFileHijack	Misc. Potentially Unwanted Software	45,626
19	Win32/Rimecud	Worms	43,854
20	Win32/VBInject	Misc. Potentially Unwanted Software	37,880
21	Win32/Cutwail	Trojan Downloaders & Droppers	37,392
22	Win32/Bumat	Miscellaneous Trojans	36,688
23	Win32/SeekmoSearchAssistant	Adware	34,588
24	Win32/Alureon	Miscellaneous Trojans	34,559
25	Win32/IRCbot	Backdoors	34,383

Notes and observations:

- Win32/Bancos and Win32/Banker, the first- and fifth-most prevalent families in Brazil in 2H09, are Portuguese-language password-stealing trojans that target specific online banking Web sites commonly located in Brazil. Captured credentials may be sent to the attacker via e-mail or ftp, or they may be sent to a remote server through some other protocol, depending on the variant.
- Win32/Bancos was the sixteenth-most prevalent threat worldwide in 2H09.
- Win32/Banker is often downloaded by Win32/Banload, the sixth-most commonly detected family in Brazil in 2H09.
- Game password stealers were common in Brazil during 2H09, similar to the pattern observed worldwide. Win32/Taterf and Win32/Frethog ranked first and sixth in the world respectively; in Brazil, the threats ranked second and fourth respectively.
- Win32/Conficker, the third-most prevalent family in Brazil in 2H09, is a worm that infects computers across a network by spreading via removable hard drives, exploiting weak passwords on file shares, or exploiting a vulnerability in the Windows Server service. Infection can result in remote code execution when file sharing is enabled. The worm also disables important system services and some security products and may download arbitrary files.

Encyclopedia

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

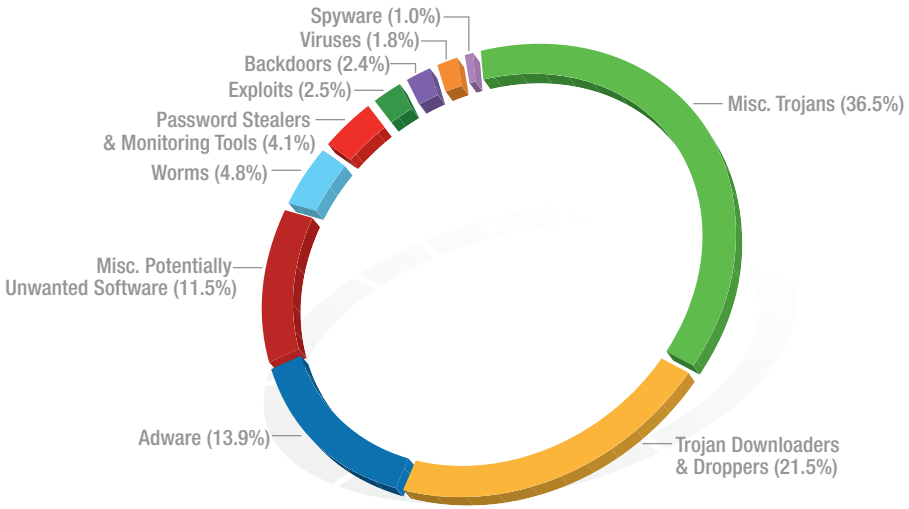
Win32/Frethog: A large family of password-stealing trojans that target confidential data, such as account information, from massively multiplayer online games.

http://www.microsoft.com/av

Canada

The MSRT detected malware on 2.5 out of every 1,000 computers scanned in Canada during 2H09 (a CCM score of 2.5—down from 3.1 in 1H09 and significantly lower than the average worldwide CCM of 7.0). Figure 107 and Figure 108 list the malware and potentially unwanted software categories and families detected by all Microsoft desktop anti-malware products in Canada in 2H09.

FIGURE 107. Malware and potentially unwanted software in Canada, by category, in 2H09



Category	Infected Computers
Miscellaneous Trojans	488,606
Trojan Downloaders & Droppers	288,246
Adware	185,497
Misc. Potentially Unwanted Software	154,155
Worms	64,603
Password Stealers & Monitoring Tools	55,176
Exploits	33,019
Backdoors	31,594
Viruses	24,050
Spyware	13,075

Notes and observations:

- The threat landscape in Canada was dominated by malware, which accounted for 73.6 percent of all threats detected on infected computers in 2H09.
- The most common category in Canada was Miscellaneous Trojans, which includes all trojan families that are not classified as downloaders/droppers or backdoors, and accounted for 36.5 percent of all infected computers.
- The second-most common category in Canada in 2H09 was Trojan Downloaders & Droppers, which accounted for 21.5 percent of all infected computers.
- Together, Miscellaneous Trojans and Trojan Downloaders & Droppers made up 58 percent of all families detected on infected computers in Canada in 2H09.

FIGURE 108. Top 25 families in Canada in 2H09

Rank	Family	Most Significant Category	Infected Computers
1	Win32/FakeXPA	Miscellaneous Trojans	142,554
2	Win32/Renos	Trojan Downloaders & Droppers	125,073
3	ASX/Wimad	Trojan Downloaders & Droppers	113,146
4	Win32/Alureon	Miscellaneous Trojans	90,458
5	Win32/Agent	Miscellaneous Trojans	79,521
6	Win32/Hotbar	Adware	69,750
7	Win32/ZangoSearchAssistant	Adware	67,568
8	Win32/Yektel	Miscellaneous Trojans	59,877
9	Win32/FakeSpypro	Miscellaneous Trojans	59,294
10	Win32/ZangoShoppingreports	Adware	29,041
11	Win32/Winwebsec	Miscellaneous Trojans	25,667
12	Win32/Liften	Miscellaneous Trojans	23,419
13	Win32/FakeVimes	Trojan Downloaders & Droppers	23,401
14	Win32/Vundo	Miscellaneous Trojans	23,244
15	Win32/PlayMP3z	Adware	22,563
16	Win32/Obfuscator	Misc. Potentially Unwanted Software	20,435
17	Win32/Koobface	Worms	17,707
18	Win32/PowerRegScheduler	Misc. Potentially Unwanted Software	16,945
19	Win32/Bancos	Password Stealers & Monitoring Tools	16,776
20	Win32/FakeSmoke	Trojan Downloaders & Droppers	16,756
21	Win32/Zlob	Trojan Downloaders & Droppers	15,610
22	Win32/C2Lop	Miscellaneous Trojans	15,597
23	Win32/SeekmoSearchAssistant	Adware	15,233
24	Win32/Zwangi	Misc. Potentially Unwanted Software	15,085
25	Win32/DoubleD	Adware	13,638

Notes and observations:

- Win32/FakeXPA, the most prevalent family in Canada in 2H09, is a family of programs that claim to scan for malware and displays fake warnings of "malicious programs and viruses." The programs then inform the user that they need to pay money to register the software to remove these nonexistent threats. Win32/FakeXPA was the third-most common family detected worldwide in 2H09.
- Some members of the Win32/FakeXPA family may also download additional malware and have been observed downloading variants of Win32/Alureon, the fourth-most common family detected in Canada during 2H09.
- Game password stealers were not as common in Canada during 2H09 as they were worldwide. Win32/Taterf and Win32/Frethog ranked first and sixth in the world respectively; in Canada neither threat was present in the top 25 list.

Encyclopedia

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

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

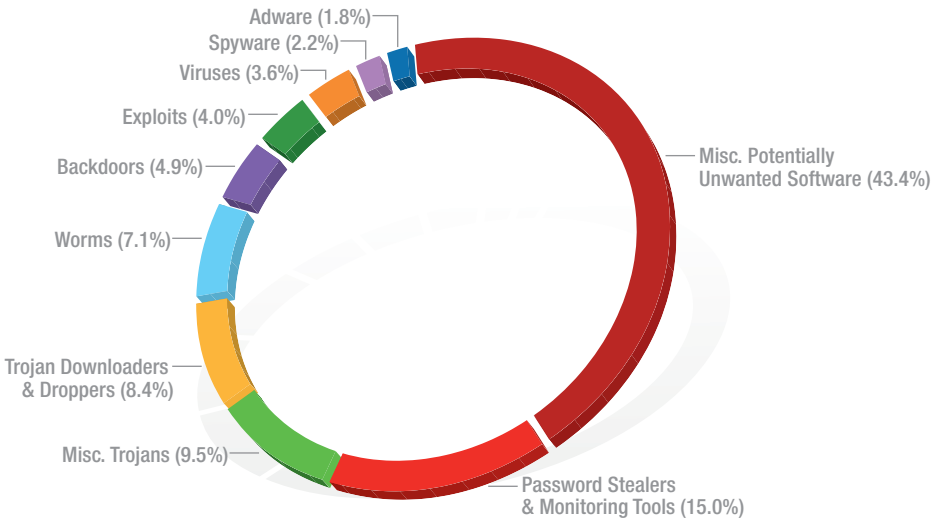
Win32/Frethog: A large family of password-stealing trojans that target confidential data, such as account information, from massively multiplayer online games.

http://www.microsoft.com/av

China

The MSRT detected malware on 7.0 out of every 1,000 computers scanned in China during 2H09 (a CCM score of 7.0—up slightly from 6.7 in 1H09 and equal to the average worldwide CCM of 7.0). Figure 109 and Figure 110 list the malware and potentially unwanted software categories and families detected by all Microsoft desktop anti-malware products in China in 2H09.

FIGURE 109. Malware and potentially unwanted software in China, by category, in 2H09



Category	Infected Computers
Misc. Potentially Unwanted Software	1,934,327
Password Stealers & Monitoring Tools	669,379
Misc. Trojans	425,532
Trojan Downloaders & Droppers	376,528
Worms	318,743
Backdoors	219,803
Exploits	179,728
Viruses	161,466
Spyware	97,215
Adware	79,064

Notes and observations:

- Potentially unwanted software, including adware and spyware, accounted for 43.4 percent of all threats detected on infected computers in China during 2H09. This is down from 53.6 percent in 1H09.
- The second-most common category in China during 2H09 was Password Stealers and Monitoring Tools, which accounted for 15.0 percent of all threats detected on infected computers, down from 20.4 percent in 1H09.

FIGURE 110. Top 25 families in China in 2H09

Rank	Family	Most Significant Category	Infected Computers
1	Win32/BaiduSobar	Misc. Potentially Unwanted Software	1,438,861
2	Win32/Lolyda	Password Stealers & Monitoring Tools	298,427
3	Win32/Frethog	Password Stealers & Monitoring Tools	248,201
4	Win32/Ceekat	Password Stealers & Monitoring Tools	211,248
5	Win32/PossibleHostsFileHijack	Misc. Potentially Unwanted Software	197,270
6	Win32/Conficker	Worms	176,454
7	Win32/Agent	Miscellaneous Trojans	139,207
8	Win32/BaiduSP	Misc. Potentially Unwanted Software	124,715
9	HTML/IframeRef	Exploits	108,986
10	Win32/Obfuscator	Misc. Potentially Unwanted Software	100,373
11	Win32/Bumat	Miscellaneous Trojans	97,755
12	Win32/CNNIC	Misc. Potentially Unwanted Software	97,366
13	Win32/CnsMin	Spyware	89,195
14	Win32/Hupigon	Backdoors	88,406
15	Win32/Small	Trojan Downloaders & Droppers	82,297
16	Win32/Parite	Viruses	69,047
17	Win32/ShellCode	Exploits	58,761
18	Win32/FlyAgent	Backdoors	53,202
19	Win32/Psyme	Miscellaneous Trojans	50,033
20	Win32/Microjoin	Trojan Downloaders & Droppers	44,264
21	Win32/Orsam	Miscellaneous Trojans	41,303
22	Win32/Autorun	Worms	40,364
23	Win32/Baidulebar	Misc. Potentially Unwanted Software	38,184
24	Win32/AgentOff	Miscellaneous Trojans	36,687
25	Win32/Nuj	Worms	35,533

Encyclopedia

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

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

http://www.microsoft.com/av

Notes and observations:

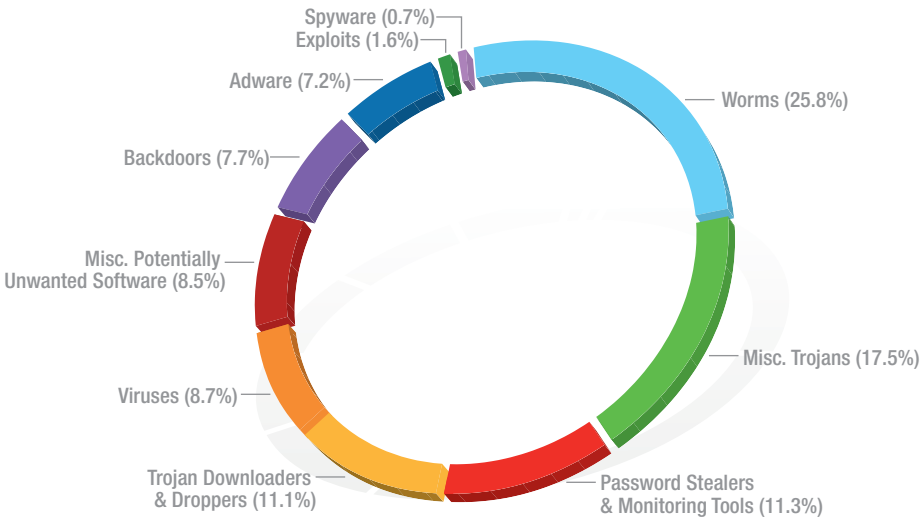
- Many of the most prevalent families detected in China during 2H09 were Chinese-language threats that do not appear in the list of top threats for other locations.
- Win32/BaiduSobar, the most prevalent family in China in 2H09, is a Chinese-language Web browser toolbar that delivers pop-up and contextual advertisements, blocks certain other advertisements, and changes the Internet Explorer home page. Win32/BaiduSobar may also prevent removal by protecting its installed files and registry keys.
- Despite a significant drop in numbers of detections from 1H09, Win32/Lolyda was the second-most prevalent family in China in 2H09. Win32/Lolyda was not in the top 25 threats detected worldwide. Win32/Lolyda is a password stealer that targets players of online games.
- The fourth-most common family in China in 2H09 was Win32/Ceekat. This threat was not in the top 25 threats detected worldwide during the same period. Win32/Ceekat is a collection of trojans that steal information, such as passwords for online games.
- Some globally prevalent game password stealers were not as widespread in China during 2H09 as they were worldwide. Win32/Taterf and Win32/Frethog ranked first and sixth in the world respectively; in China Win32/Frethog ranked third but Win32/Taterf did not appear in the top 25 threats detected.

Egypt

The MSRT detected malware on 8.6 out of every 1,000 computers scanned in Egypt during 2H09 (a CCM score of 8.6—down significantly from 13.7 in 1H09 but still higher than the average worldwide CCM of 7.0). Figure 111 and Figure 112 list the malware and potentially unwanted software categories and families detected by all Microsoft desktop anti-malware products in Egypt in 2H09.

FIGURE 111. Malware and potentially unwanted software in Egypt, by category, in 2H09

Category	Infected Computers
Worms	31,993
Misc. Trojans	21,756
Password Stealers & Monitoring Tools	13,982
Trojan Downloaders & Droppers	13,733
Viruses	10,780
Misc. Potentially Unwanted Software	10,602
Backdoors	9,584
Adware	8,878
Exploits	1,941
Spyware	810



Notes and observations:

- The threat landscape in Egypt in 2H09 was dominated by malware, which accounted for 83.7 percent of all threats detected on infected computers in 2H09.
- The most common category of threat detected in Egypt in 2H09 was Worms, accounting for 25.8 percent of the total.
- The second-most common category in Egypt during 2H09 was Miscellaneous Trojans, which includes all trojan families that are not classified as downloaders/droppers or backdoors, and accounted for 17.5 percent of all infected computers.

FIGURE 112. Top 25 families in Egypt in 2H09

Rank	Family	Most Significant Category	Infected Computers
1	Win32/Taterf	Worms	15,064
2	Win32/Frethog	Password Stealers & Monitoring Tools	9,754
3	Win32/Agent	Miscellaneous Trojans	7,426
4	Win32/Hamweq	Worms	5,846
5	Win32/Renos	Trojan Downloaders & Droppers	5,720
6	Win32/Conficker	Worms	5,547
7	Win32/Sality	Viruses	5,067
8	Win32/Autorun	Worms	4,781
9	Win32/SeekmoSearchAssistant	Adware	3,138
10	Win32/IRCbot	Backdoors	3,045
11	Win32/Koobface	Worms	2,912
12	Win32/Virut	Viruses	2,868
13	Win32/Cutwail	Trojan Downloaders & Droppers	2,680
14	Win32/Alureon	Miscellaneous Trojans	2,604
15	Win32/Bumat	Miscellaneous Trojans	2,230
16	Win32/DoubleD	Adware	2,176
17	Win32/Hotbar	Adware	1,757
18	Win32/Rbot	Backdoors	1,720
19	Win32/ZangoSearchAssistant	Adware	1,658
20	Win32/C2Lop	Miscellaneous Trojans	1,656
21	Win32/VB	Miscellaneous Trojans	1,596
22	HTML/IframeRef	Exploits	1,582
23	Win32/Zlob	Trojan Downloaders & Droppers	1,556
24	Win32/Brontok	Worms	1,396
25	Win32/FlyAgent	Backdoors	1,384

Notes and observations:

- The two most prevalent threats in Egypt during 2H09 both target players of online games and attempt to steal passwords and other player credentials. Win32/Taterf, the number one threat in Egypt and worldwide, is a family of worms that spread via mapped drives to steal login and account details for popular online games. Win32/Frethog, the second-most prevalent threat in Egypt and the sixth worldwide, is a large family of password-stealing trojans that target confidential data, such as account information, from massively multiplayer online games, like World of Warcraft.
- Three of the eight most prevalent threats in Egypt during 2H09 (Win32/Hamweq, Win32/Conficker and Win32/Autorun) spread via mapped drives with weak or missing passwords, removable media (such as USB drives), or a combination of both.
- Win32/Sality was the seventh-most prevalent family in Egypt in 2H09, but it was not present in the top 25 threats worldwide. Win32/Sality is a family of polymorphic file infectors that target Windows executable files with the extensions .src or .exe. The family may also execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.

Encyclopedia

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

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

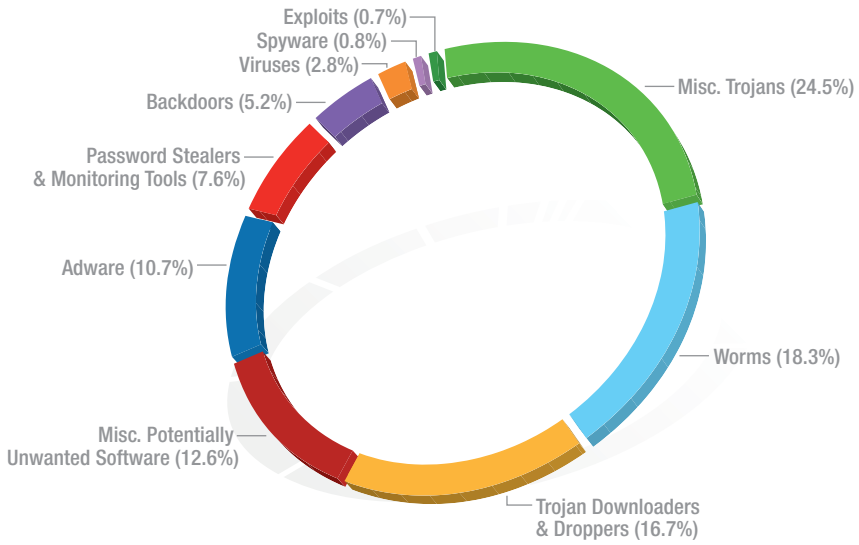
Win32/Autorun: A worm that attempts to spread by being copied into all removable drives.

http://www.microsoft.com/av

France

The MSRT detected malware on 5.6 out of every 1,000 computers scanned in France during 2H09 (a CCM score of 5.6—down from 7.9 in 1H09 and lower than the average worldwide CCM of 7.0). Figure 113 and Figure 114 list the malware and potentially unwanted software categories and families detected by all Microsoft desktop anti-malware products in France in 2H09.

FIGURE 113. Malware and potentially unwanted software in France, by category, in 2H09



Category	Infected Computers
Miscellaneous Trojans	499,266
Worms	372,542
Trojan Downloaders & Droppers	339,744
Misc. Potentially Unwanted Software	256,050
Adware	218,363
Password Stealers & Monitoring Tools	154,191
Backdoors	105,446
Viruses	56,420
Spyware	17,147
Exploits	14,938

Notes and observations:

- The threat landscape in France was dominated by malware, which accounted for 75.8 percent of all threats detected on infected computers in 2H09, down from 79.6 percent in 1H09.
- The most common category in France was Miscellaneous Trojans, which includes all trojan families that are not classified as downloaders/droppers or backdoors, and accounted for 24.5 percent of all infected computers. This is a significant decrease from 34.4 percent in 1H09.
- The third-most common category in France was Trojan Downloaders & Droppers, which accounted for 16.7 percent of all infected computers.
- Together, Miscellaneous Trojans and Trojan Downloaders & Droppers made up more than 40 percent of all families detected on infected computers in France in 2H09.

FIGURE 114. Top 25 families in France in 2H09

Rank	Family	Most Significant Category	Infected Computers
1	Win32/Taterf	Worms	188,536
2	Win32/Renos	Trojan Downloaders & Droppers	143,823
3	Win32/Alureon	Miscellaneous Trojans	118,936
4	Win32/Frethog	Password Stealers & Monitoring Tools	86,694
5	Win32/Vundo	Miscellaneous Trojans	70,901
6	Win32/Wintrim	Miscellaneous Trojans	61,411
7	ASX/Wimad	Trojan Downloaders & Droppers	60,227
8	Win32/Hotbar	Adware	59,194
9	Win32/C2Lop	Miscellaneous Trojans	59,010
10	Win32/ZangoSearchAssistant	Adware	44,655
11	Win32/Conficker	Worms	44,505
12	Win32/Agent	Miscellaneous Trojans	41,221
13	Win32/FakeXPA	Miscellaneous Trojans	39,042
14	Win32/RJump	Worms	35,284
15	Win32/Zlob	Trojan Downloaders & Droppers	34,144
16	Win32/FakeAdpro	Misc. Potentially Unwanted Software	33,078
17	Win32/Brontok	Worms	32,229
18	Win32/DoubleD	Adware	32,044
19	Win32/IRCbot	Backdoors	30,479
20	Win32/PlayMP3z	Adware	29,494
21	Win32/Skintrim	Miscellaneous Trojans	27,576
22	Win32/Yektel	Miscellaneous Trojans	26,620
23	Win32/ZangoShoppingreports	Adware	26,008
24	Win32/Hamweq	Worms	25,593
25	Win32/RealVNC	Misc. Potentially Unwanted Software	24,762

Encyclopedia

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

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

http://www.microsoft.com/av

Notes and observations:

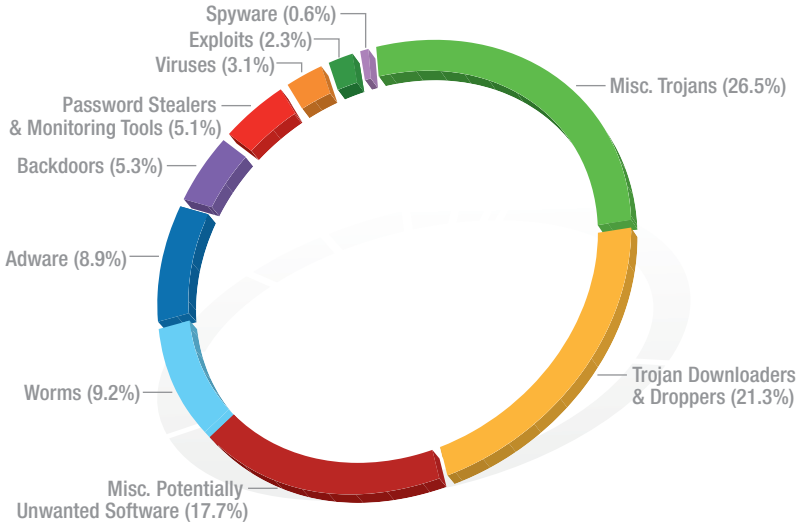
- The top two families detected in France during 2H09 (Win32/Taterf and Win32/Renos) were the same as the top two threats detected worldwide. Win32/Taterf is a family of worms that spread via mapped drives to steal login and account details for popular online games. Win32/Renos automatically downloads rogue security software.
- Game password stealers were very common in France during 2H09. Win32/Taterf and Win32/Frethog, which rank first and sixth in the world respectively, ranked first and fourth in France.
- Win32/Vundo was more prevalent in France during 2H09. Win32/Vundo, a multiple-component family of programs, often installed as a browser helper object (BHO), that deliver pop-up advertisements and may download and execute arbitrary content, was the fifth-most prevalent family in France during 2H09 but only ranked eighteenth worldwide in the same period.
- Win32/Wintrim was the sixth-most prevalent family in France during 2H09, but it was not present in the top 25 families detected worldwide. Win32/Wintrim is a family of trojans that display pop-up advertisements depending on the user's keywords and browsing history. Variants can also monitor the user's activities, download applications, and send system information to a remote server. In 1H09, Win32/Wintrim was the most prevalent family detected in France.

Germany

The MSRT detected malware on 2.2 out of every 1,000 computers scanned in Germany during 2H09 (a CCM score of 2.2—down from 3.0 in 1H09 and significantly lower than the average worldwide CCM of 7.0). Figure 115 and Figure 116 list the malware and potentially unwanted software categories and families detected by all Microsoft desktop anti-malware products in Germany in 2H09.

FIGURE 115. Malware and potentially unwanted software in Germany, by category, in 2H09

Category	Infected Computers
Miscellaneous Trojans	373,861
Trojan Downloaders & Droppers	301,519
Misc. Potentially Unwanted Software	250,346
Worms	129,327
Adware	125,554
Backdoors	75,376
Password Stealers & Monitoring Tools	71,381
Viruses	43,115
Exploits	33,116
Spyware	9,089



Notes and observations:

- The threat landscape in Germany was dominated by malware, which accounted for 72.8 percent of all threats detected on infected computers in 2H09, down from 76.4 percent in 1H09.
- The most common category in Germany was Miscellaneous Trojans, which includes all trojan families that are not classified as downloaders/droppers or backdoors, and accounted for 26.5 percent of all infected computers. This was a significant decrease from 39.5 percent in 1H09, primarily driven by the drop in infections by Win32/Wintrim.
- The second-most common category in Germany was Trojan Downloaders & Droppers, which accounted for 21.3 percent of all infected computers, up from 18.7 percent in 1H09.
- Together, Miscellaneous Trojans and Trojan Downloaders & Droppers made up more than 47 percent of all families detected on infected computers in Germany in 2H09.

Encyclopedia

Win32/Wintrim: A family of trojans that display pop-up advertisements depending on the user's keywords and browsing history. Its variants can monitor the user's activities, download applications, and send system information back to a remote server.

http://www.microsoft.com/av

FIGURE 116. Top 25 families in Germany in 2H09

Rank	Family	Most Significant Category	Infected Computers
1	Win32/Renos	Trojan Downloaders & Droppers	186,937
2	Win32/Alureon	Miscellaneous Trojans	138,350
3	Win32/Conficker	Worms	60,921
4	Win32/Agent	Miscellaneous Trojans	47,704
5	Win32/Yabector	Miscellaneous Trojans	46,173
6	Win32/FakeAdpro	Misc. Potentially Unwanted Software	33,578
7	Win32/Hotbar	Adware	31,766
8	Win32/ZangoSearchAssistant	Adware	30,632
9	Win32/PossibleHostsFileHijack	Misc. Potentially Unwanted Software	27,297
10	Win32/Vundo	Miscellaneous Trojans	26,420
11	Win32/DoubleD	Adware	23,307
12	Win32/RealVNC	Misc. Potentially Unwanted Software	22,366
13	Win32/Wintrim	Miscellaneous Trojans	21,094
14	Win32/Bumat	Miscellaneous Trojans	21,078
15	Win32/Bredolab	Trojan Downloaders & Droppers	18,931
16	Win32/SeekmoSearchAssistant	Adware	18,846
17	Win32/Taterf	Worms	18,744
18	HTML/IframeRef	Exploits	18,181
19	Win32/FakeXPA	Miscellaneous Trojans	17,826
20	ASX/Wimad	Trojan Downloaders & Droppers	17,422
21	Win32/Obfuscator	Misc. Potentially Unwanted Software	16,240
22	Win32/Rustock	Backdoors	16,037
23	Win32/Zlob	Trojan Downloaders & Droppers	15,968
24	Win32/FakeRean	Miscellaneous Trojans	14,935
25	Win32/VB	Miscellaneous Trojans	14,450

Notes and observations:

- Win32/Renos, the most prevalent family in Germany in 2H09, is a family of trojan downloaders that install rogue security software. Win32/Renos was the second-most prevalent family detected worldwide during 2H09.
- Game password stealers were not as common in Germany during 2H09 as they were worldwide. Win32/Taterf and Win32/Frethog ranked first and sixth in the world respectively; in Germany Win32/Taterf ranked only seventeenth, and Win32/Frethog did not appear in the list of the 25 most prevalent threats.
- Win32/Yabector was the fifth-most prevalent family detected in Germany in 2H09, but it did not appear in the top 25 families worldwide during the same period. Win32/Yabector is a detection signature for variants of a threat that notifies a remote Web server of its presence without user consent. It may be bundled with an installation program as the file "ebayshortcuts.exe."

Encyclopedia

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

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

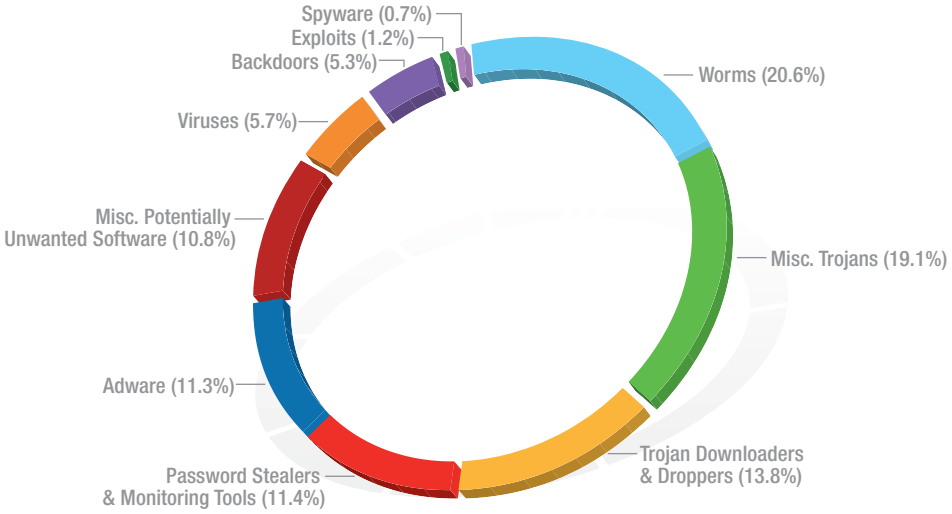
http://www.microsoft.com/av

India

The MSRT detected malware on 2.6 out of every 1,000 computers scanned in India during 2H09 (a CCM score of 2.6, significantly lower than the average worldwide CCM of 7.0). Figure 117 and Figure 118 list the malware and potentially unwanted software categories and families detected by all Microsoft desktop anti-malware products in India in 2H09.

FIGURE 117. Malware and potentially unwanted software in India, by category, in 2H09

Category	Infected Computers
Worms	39,451
Miscellaneous Trojans	36,612
Trojan Downloaders & Droppers	26,514
Password Stealers & Monitoring Tools	21,880
Adware	21,663
Misc. Potentially Unwanted Software	20,660
Viruses	10,982
Backdoors	10,112
Exploits	2,334
Spyware	1,339



Notes and observations:

- The threat landscape in India was dominated by malware, which accounted for 77.1 percent of all threats detected on infected computers in 2H09.
- The most common category in India was Worms, which accounted for 20.6 percent of all infected computers.
- The second-most common category in India was Miscellaneous Trojans, which includes all trojan families that are not classified as downloaders/droppers or back-doors, and accounted for 19.1 percent of all infected computers.
- Together, Miscellaneous Trojans and Trojan Downloaders & Droppers made up more than 32 percent of all families detected on infected computers in India in 2H09.

FIGURE 118. Top 25 families in India in 2H09

Rank	Family	Most Significant Category	Infected Computers
1	Win32/Conficker	Worms	14,402
2	Win32/Renos	Trojan Downloaders & Droppers	14,327
3	Win32/Taterf	Worms	11,485
4	Win32/Ardamax	Trojan Downloaders & Droppers	10,525
5	Win32/Alureon	Miscellaneous Trojans	8,633
6	Win32/Autorun	Worms	7,861
7	Win32/Agent	Miscellaneous Trojans	6,776
8	Win32/Rimecud	Worms	6,263
9	Win32/SeekmoSearchAssistant	Adware	6,014
10	Win32/ZangoSearchAssistant	Adware	5,441
11	Win32/Hamweq	Worms	5,137
12	Win32/Hotbar	Adware	5,029
13	Win32/Frethog	Password Stealers & Monitoring Tools	4,972
14	Win32/IRCbot	Backdoors	3,969
15	Win32/Sality	Viruses	3,947
16	Win32/Virut	Viruses	3,657
17	Win32/DoubleD	Adware	3,354
18	Win32/Killav	Miscellaneous Trojans	3,042
19	Win32/FakeXPA	Miscellaneous Trojans	2,900
20	Win32/ModTool	Misc. Potentially Unwanted Software	2,811
21	Win32/Bredolab	Trojan Downloaders & Droppers	2,714
22	Win32/ZangoShoppingreports	Adware	2,523
23	Win32/VB	Miscellaneous Trojans	2,512
24	Win32/Obfuscator	Misc. Potentially Unwanted Software	2,487
25	Win32/Sohanad	Worms	2,444

Notes and observations:

- Four of the eleven most prevalent threats detected in India during 2H09 (Win32/Taterf, Win32/Hamweq, Win32/Conficker and Win32/Autorun) spread via mapped drives with weak or missing passwords, removable media (such as USB drives), or a combination of both.
- Win32/Renos, the second-most prevalent family in India in 2H09, was also the second-most prevalent threat detected worldwide. Win32/Renos is a family of trojan downloaders that install rogue security software.
- Game password stealers were not as common in India during 2H09 as they were worldwide. Win32/Taterf and Win32/Frethog ranked first and sixth in the world respectively; in India Win32/Taterf ranked third, and Win32/Frethog ranked thirteenth.
- Win32/Ardamax, the fourth-most prevalent family detected in India in 2H09, does not appear in the top 25 families detected worldwide. Win32/Ardamax is a key-logger program that can capture user activity and save it to a text or HTML file. Win32/Ardamax can be configured to send these files via e-mail to a predefined address.

Encyclopedia

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

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

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

Win32/Autorun: A worm that attempts to spread by being copied into all removable drives.

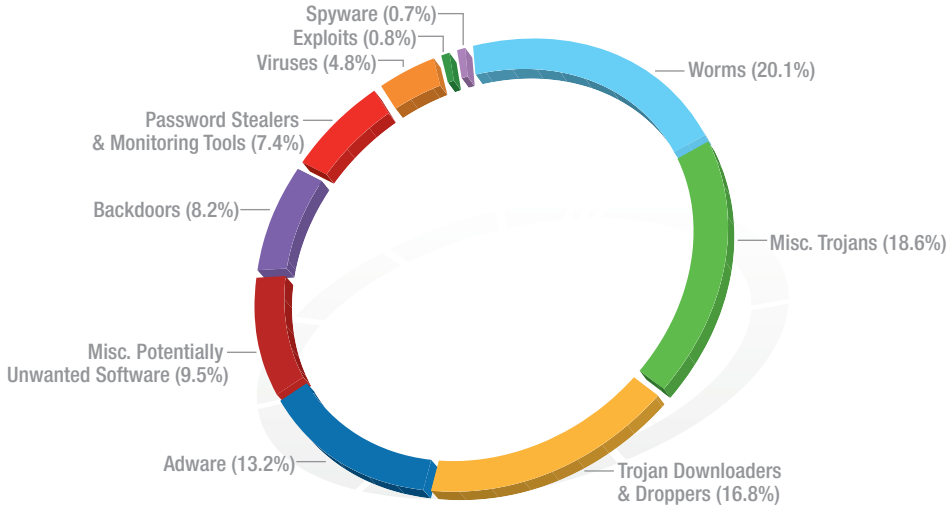
Win32/Frethog: A large family of password-stealing trojans that target confidential data, such as account information, from massively multiplayer online games.

http://www.microsoft.com/av

Israel

The MSRT detected malware on 7.3 out of every 1,000 computers scanned in Israel during 2H09 (a CCM score of 7.3, slightly higher than the average worldwide CCM of 7.0). Figure 119 and Figure 120 list the malware and potentially unwanted software categories and families detected by all Microsoft desktop anti-malware products in Israel in 2H09.

FIGURE 119. Malware and potentially unwanted software in Israel, by category, in 2H09



Category	Infected Computers
Worms	39,498
Miscellaneous Trojans	36,618
Trojan Downloaders & Droppers	33,086
Adware	25,960
Misc. Potentially Unwanted Software	18,608
Backdoors	16,205
Password Stealers & Monitoring Tools	14,617
Viruses	9,392
Exploits	1,506
Spyware	1,380

Notes and observations:

- The threat landscape in Israel was dominated by malware, which accounted for 76.7 percent of all threats detected on infected computers in 2H09.
- The most common category in Israel was Worms, which accounted for 20.1 percent of all infected computers.
- The second-most common category in Israel was Miscellaneous Trojans, which includes all trojan families that are not classified as downloaders/droppers or backdoors, and accounted for 18.6 percent of all infected computers.
- Together, Miscellaneous Trojans and Trojan Downloaders & Droppers made up more than 35 percent of all families detected on infected computers in Israel in 2H09.

FIGURE 120. Top 25 families in Israel in 2H09

Rank	Family	Most Significant Category	Infected Computers
1	Win32/Renos	Trojan Downloaders & Droppers	14,681
2	Win32/Taterf	Worms	12,274
3	Win32/I2ISolutions	Adware	10,767
4	Win32/Koobface	Worms	10,042
5	Win32/DoubleD	Adware	7,670
6	Win32/Hamweq	Worms	6,402
7	Win32/Frethog	Password Stealers & Monitoring Tools	6,292
8	Win32/Agent	Miscellaneous Trojans	6,243
9	Win32/Bredolab	Trojan Downloaders & Droppers	5,517
10	Win32/Cutwail	Trojan Downloaders & Droppers	5,075
11	Win32/Alureon	Miscellaneous Trojans	5,036
12	Win32/Brontok	Worms	4,220
13	Win32/Vundo	Miscellaneous Trojans	3,952
14	Win32/Rbot	Backdoors	3,872
15	Win32/Conficker	Worms	3,697
16	ASX/Wimad	Trojan Downloaders & Droppers	3,526
17	Win32/Rustock	Backdoors	3,483
18	Win32/Autorun	Worms	3,431
19	Win32/C2Lop	Miscellaneous Trojans	3,291
20	Win32/Zlob	Trojan Downloaders & Droppers	3,228
21	Win32/Ldpinch	Password Stealers & Monitoring Tools	2,585
22	Win32/Hotbar	Adware	2,437
23	Win32/IRCbot	Backdoors	2,399
24	Win32/Bumat	Miscellaneous Trojans	2,177
25	Win32/ZangoSearchAssistant	Adware	2,169

Encyclopedia

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

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

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

http://www.microsoft.com/av

Notes and observations:

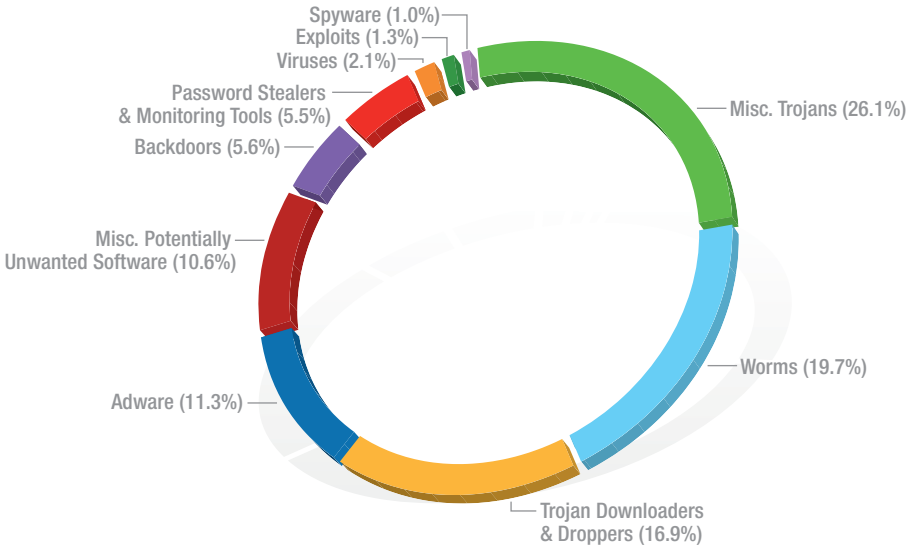
- Three of the top six threats detected in Israel during 2H09 were worms. Two of the worms (Win32/Taterf and Win32/Hamweq) spread via mapped drives with missing or weak passwords and via infected USB drives. Win32/Koobface targets users of popular social networking sites. It spreads by posting messages containing a link to the worm to the pages of other contacts on sites such as Facebook. The worm may download and run additional malware, and it may display pop-up messages or windows that attempt to convince users to install rogue security software.
- Win32/Renos, the most prevalent family in Israel in 2H09, was the second-most prevalent threat detected worldwide. Win32/Renos is a family of trojan downloaders that install rogue security software.
- Game password stealers were common in Israel during 2H09. Win32/Taterf and Win32/Frethog ranked first and sixth in the world respectively; in Israel Win32/Taterf ranked second, and Win32/Frethog ranked seventh.
- Two adware families, Win32/I2ISolutions and Win32/DoubleD, are more prevalent in Israel than they are worldwide. Win32/I2ISolutions is an Internet Explorer chat extension and may report and send user and system information about the affected machine to a remote server. Win32/DoubleD is an adware program that displays pop-up advertising, runs at each system startup, and is installed as an Internet Explorer toolbar.

Italy

The MSRT detected malware on 5.3 out of every 1,000 computers scanned in Italy during 2H09 (a CCM score of 5.3—down from 6.9 in 1H09 and lower than the average worldwide CCM of 7.0). Figure 121 and Figure 122 list the malware and potentially unwanted software categories and families detected by all Microsoft desktop anti-malware products in Italy in 2H09.

FIGURE 121. Malware and potentially unwanted software in Italy, by category, in 2H09

Category	Infected Computers
Miscellaneous Trojans	322,299
Worms	242,982
Trojan Downloaders & Droppers	209,182
Adware	139,670
Misc. Potentially Unwanted Software	130,646
Backdoors	68,697
Password Stealers & Monitoring Tools	68,316
Viruses	25,745
Exploits	15,550
Spyware	12,570



Notes and observations:

- The threat landscape in Italy was dominated by malware, which accounted for 77.2 percent of all threats detected on infected computers in 2H09.
- The most common category in Italy was Miscellaneous Trojans, which includes all trojan families that are not classified as downloaders/droppers or backdoors, and accounted for 26.1 percent of all infected computers.
- The third-most common category in Italy in 2H09 was Trojan Downloaders & Droppers, which accounted for 16.9 percent of all infected computers.
- Together, Miscellaneous Trojans and Trojan Downloaders & Droppers made up 43 percent of all families detected on infected computers in Italy in 2H09.

FIGURE 122. Top 25 families in Italy in 2H09

Rank	Family	Most Significant Category	Infected Computers
1	Win32/Conficker	Worms	102,623
2	Win32/Alureon	Miscellaneous Trojans	92,419
3	Win32/Renos	Trojan Downloaders & Droppers	84,733
4	Win32/Taterf	Worms	83,771
5	Win32/Hotbar	Adware	63,142
6	Win32/Vundo	Miscellaneous Trojans	51,483
7	Win32/Wintrim	Miscellaneous Trojans	46,922
8	Win32/C2Lop	Miscellaneous Trojans	44,356
9	Win32/Frethog	Password Stealers & Monitoring Tools	37,324
10	ASX/Wimad	Trojan Downloaders & Droppers	34,600
11	Win32/DoubleD	Adware	26,805
12	Win32/Agent	Miscellaneous Trojans	23,770
13	Win32/ZangoSearchAssistant	Adware	22,127
14	Win32/FakeCog	Miscellaneous Trojans	22,075
15	Win32/Bagle	Worms	20,745
16	Win32/Skintrim	Miscellaneous Trojans	20,593
17	Win32/IRCbot	Backdoors	17,081
18	Win32/Winwebsec	Miscellaneous Trojans	17,079
19	Win32/Rustock	Backdoors	15,206
20	Win32/Autorun	Worms	14,848
21	Win32/Cutwail	Trojan Downloaders & Droppers	14,797
22	Win32/Zlob	Trojan Downloaders & Droppers	14,241
23	Win32/Hamweq	Worms	14,100
24	Win32/FakeXPA	Miscellaneous Trojans	13,724
25	Win32/RealVNC	Misc. Potentially Unwanted Software	12,874

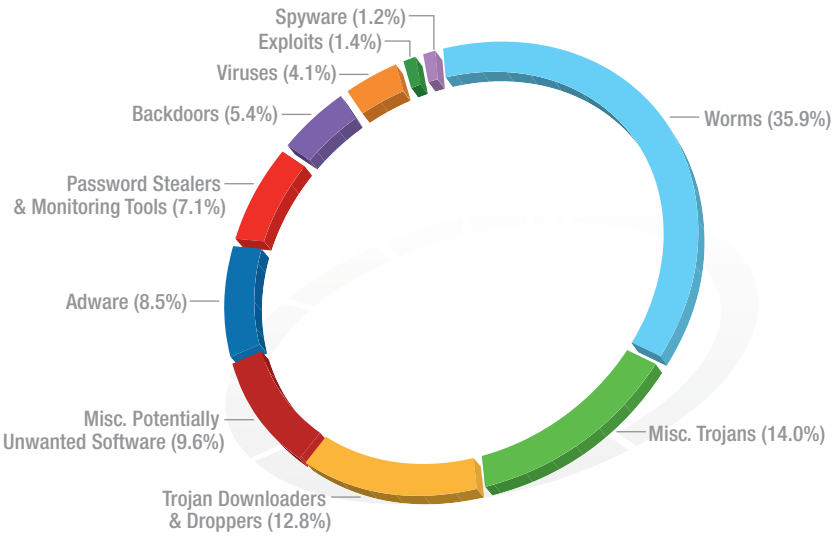
Notes and observations:

- Win32/Conficker, the most prevalent family in Italy in 2H09, is a worm that infects computers across a network by spreading via removable hard drives, exploiting weak passwords on file shares, or exploiting a vulnerability in the Windows Server service. Infection can result in remote code execution when file sharing is enabled. The worm also disables important system services and some security products and may download arbitrary files.
- Win32/Wintrim was the seventh-most prevalent family in Italy during 2H09, but it was not present in the top 25 families detected worldwide. Win32/Wintrim is a family of trojans that display pop-up advertisements depending on the user's keywords and browsing history. Variants can also monitor the user's activities, download applications, and send system information to a remote server.
- Win32/FakeXPA, a family of rogue security software programs, was less prevalent in Italy than it was worldwide in 2H09. Win32/FakeXPA was the third-most prevalent family detected worldwide, but it was only the twenty-fourth-most prevalent family detected in Italy in 2H09.
- Win32/FakeCog, a fake security program that displays false infections in the system to prompt the user into buying it, was the fourteenth-most prevalent family detected in Italy during 2H09, but it did not appear in the top 25 families detected worldwide.

Japan

The MSRT detected malware on 2.3 out of every 1,000 computers scanned in Japan during 2H09 (a CCM score of 2.3—down from 3.0 in 1H09 and significantly lower than the average worldwide CCM of 7.0). Figure 123 and Figure 124 list the malware and potentially unwanted software categories and families detected by all Microsoft desktop anti-malware products in Japan in 2H09.

FIGURE 123. Malware and potentially unwanted software in Japan, by category, in 2H09



Category	Infected Computers
Worms	268,125
Misc. Trojans	104,378
Trojan Downloaders & Droppers	95,923
Misc. Potentially Unwanted Software	71,700
Adware	63,817
Password Stealers & Monitoring Tools	53,295
Backdoors	40,225
Viruses	30,553
Exploits	10,771
Spyware	8,845

Notes and observations:

- The threat landscape in Japan was dominated by malware, which accounted for 80.7 percent of all threats detected on infected computers in 2H09, down from 86.9 percent in 1H09.
- The most common category in Japan was Worms, which accounted for 35.9 percent of all infected computers, down from 40.0 percent in 1H09.
- The second-most common category in Japan was Miscellaneous Trojans, which includes all trojan families that are not classified as downloaders/droppers or backdoors, and accounted for 14.0 percent of all infected computers, down very slightly from 14.1 percent in 1H09.

FIGURE 124. Top 25 families in Japan in 2H09

Rank	Family	Most Significant Category	Infected Computers
1	Win32/Taterf	Worms	193,237
2	Win32/Agent	Miscellaneous Trojans	28,554
3	Win32/Conficker	Worms	27,920
4	Win32/DoubleD	Adware	27,774
5	Win32/Renos	Trojan Downloaders & Droppers	21,975
6	Win32/Zlob	Trojan Downloaders & Droppers	19,535
7	Win32/Frethog	Password Stealers & Monitoring Tools	19,033
8	ASX/Wimad	Trojan Downloaders & Droppers	15,366
9	Win32/PlayMP3z	Adware	14,701
10	Win32/Alureon	Miscellaneous Trojans	14,077
11	Win32/Antinny	Worms	13,623
12	Win32/Cutwail	Trojan Downloaders & Droppers	12,782
13	Win32/Yabector	Miscellaneous Trojans	12,583
14	Win32/RealVNC	Misc. Potentially Unwanted Software	12,019
15	Win32/Corripio	Password Stealers & Monitoring Tools	11,505
16	Win32/FakeRean	Miscellaneous Trojans	10,273
17	Win32/Autorun	Worms	10,249
18	Win32/Parite	Viruses	9,875
19	Win32/Hupigon	Backdoors	8,650
20	Win32/Bredolab	Trojan Downloaders & Droppers	8,526
21	Win32/Rbot	Backdoors	8,014
22	Win32/Hamweq	Worms	7,225
23	Win32/BaiduSobar	Misc. Potentially Unwanted Software	7,186
24	Win32/RJump	Worms	7,173
25	Win32/Small	Trojan Downloaders & Droppers	7,120

Encyclopedia

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

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

Win32/RJump: A worm that attempts to spread by copying itself to newly attached media, such as USB memory devices or network drives. It also contains backdoor functionality that allows an attacker unauthorized access to an affected machine.

Win32/Autorun: A worm that attempts to spread by being copied into all removable drives.

http://www.microsoft.com/av

Notes and observations:

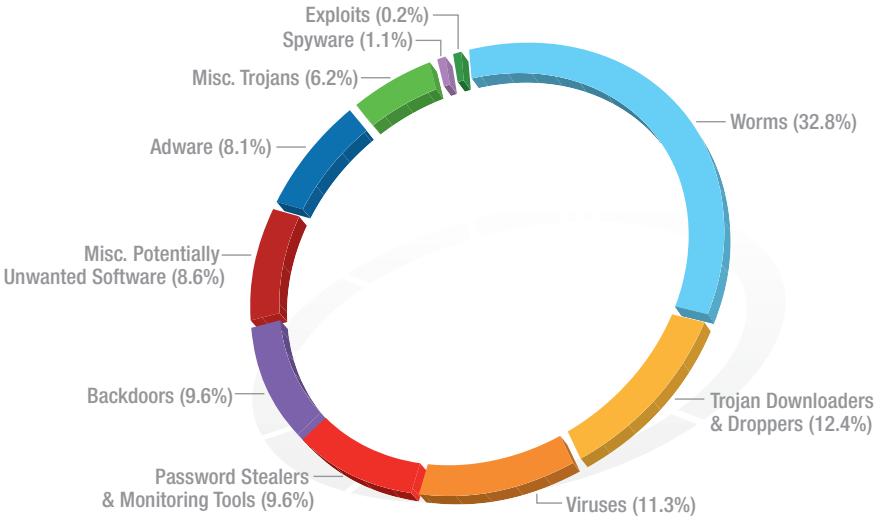
- Win32/DoubleD was the fourth-most common family in Japan, but it was only twenty-fifth worldwide. Win32/DoubleD is an adware program that displays pop-up advertising, runs at each system startup, and is installed as an Internet Explorer toolbar.
- Win32/Zlob was much more prevalent in Japan in 2H09 than it was worldwide. Win32/Zlob is a family of trojans that often pose as a downloadable media codec that displays frequent pop-up advertisements for rogue security software. Win32/Zlob was the sixth-most prevalent family in Japan in 2H09, but it was only the twenty-second–most prevalent family worldwide during the same period.
- Four of the top 25 most prevalent families in Japan during 2H09 (Win32/Hamweq, Win32/Conficker, Win32/RJump and Win32/Autorun) spread via mapped drives with weak or missing passwords, removable media (such as USB drives), or a combination of both.
- Win32/Antinny, which is not among the top 25 families detected worldwide, ranked eleventh in Japan during 2H09. Win32/Antinny is a family of worms that spread using a Japanese peer-to-peer file-sharing application named Winny. The worm creates a copy of itself with a deceptive filename in the Winny upload folder in an attempt to encourage download by other Winny users.
- Win32/Hupigon, which is not among the top 25 families detected worldwide, ranked nineteenth in Japan during 2H09. Win32/Hupigon is a family of backdoor trojans that are prevalent in a number of locations across Asia. It may drop a keystroke logger, password stealer, and other malicious add-ons.

Korea

The MSRT detected malware on 16.0 out of every 1,000 computers scanned in Korea during 2H09 (a CCM score of 16.0—down from 21.3 in 1H09 but still significantly higher than the average worldwide CCM of 7.0). Figure 125 and Figure 126 list the malware and potentially unwanted software categories and families detected by all Microsoft desktop anti-malware products in Korea in 2H09.

FIGURE 125. Malware and potentially unwanted software in Korea, by category, in 2H09

Category	Infected Computers
Worms	543,940
Trojan Downloaders & Droppers	205,651
Viruses	187,952
Password Stealers & Monitoring Tools	159,441
Backdoors	158,733
Misc. Potentially Unwanted Software	143,182
Adware	134,085
Misc. Trojans	102,989
Spyware	18,199
Exploits	4,131



Notes and observations:

- The threat landscape in Korea was dominated by malware, which accounted for 82.1 percent of all threats detected on infected computers in 2H09, up from 81.9 percent in 1H09.
- The most common category in Korea was Worms, which accounted for 32.8 percent of all infected computers, down from 36.2 percent in 1H09.
- The second-most common category in Korea was Trojan Downloaders & Droppers, which accounted for 12.4 percent of all infected computers, up significantly from 6.6 percent in 1H09.
- The category Miscellaneous Trojans, which includes all trojan families that are not classified as downloaders/droppers or backdoors, was significantly lower in Korea than in many other countries and regions around the world at 6.2 percent, down from 7.2 percent in 1H09.

FIGURE 126. Top 25 families in Korea in 2H09

Rank	Family	Most Significant Category	Infected Computers
1	Win32/Taterf	Worms	408,791
2	Win32/Frethog	Password Stealers & Monitoring Tools	80,683
3	Win32/Small	Trojan Downloaders & Droppers	74,307
4	Win32/Virut	Viruses	73,097
5	Win32/Bredolab	Trojan Downloaders & Droppers	68,517
6	Win32/Parite	Viruses	64,252
7	Win32/FakeBye	Misc. Potentially Unwanted Software	61,724
8	Win32/Nieguide	Adware	52,873
9	Win32/Cutwail	Trojan Downloaders & Droppers	45,760
10	Win32/Hamweq	Worms	45,124
11	Win32/Pointfree	Misc. Potentially Unwanted Software	44,875
12	Win32/Conficker	Worms	42,839
13	Win32/Corripio	Password Stealers & Monitoring Tools	41,708
14	Win32/Rustock	Backdoors	39,093
15	Win32/Dpoint	Adware	34,218
16	Win32/Agent	Miscellaneous Trojans	32,872
17	Win32/Wukill	Worms	24,291
18	Win32/FakeRean	Miscellaneous Trojans	24,178
19	Win32/Rbot	Backdoors	24,118
20	Win32/Mydoom	Worms	23,189
21	Win32/Hupigon	Backdoors	21,434
22	Win32/Renos	Trojan Downloaders & Droppers	18,295
23	Win32/Banker	Password Stealers & Monitoring Tools	17,938
24	Win32/Zlob	Trojan Downloaders & Droppers	17,649
25	Win32/Jeefo	Viruses	17,289

Notes and observations:

- Game password stealers were very common in Korea during 2H09. Win32/Taterf and Win32/Frethog ranked first and sixth in the world respectively; in Korea Win32/Taterf ranked first, and Win32/Frethog ranked second. These families were also the top two families detected in Korea during 1H09. Win32/Corripio, ranked thirteenth in Korea in 2H09, is another game password stealer.
- Win32/Small was the third-most detected threat on infected computers in Korea during 2H09. Win32/Small is a trojan that downloads and executes a file from a specified URL. Most commonly, the downloaded file is a dialer application for adult content. Win32/Small was not present in the top 25 families detected worldwide in 2H09.
- Win32/Virut was the fourth-most prevalent family detected in Korea in 2H09, but it was not present in the top 25 families detected worldwide. Win32/Virut is a family of file-infecting viruses that target and infect .exe and .src files accessed on infected systems. Win32/Virut also opens a backdoor by connecting to an IRC server, allowing a remote attacker to download and run files on the infected computer.
- Win32/Bredolab was much more prevalent in Korea in 2H09 than it was worldwide. Win32/Bredolab, a trojan that downloads and executes arbitrary code from a remote server, was the fifth-most prevalent family in Korea in 2H09. It was the twenty-fourth-most common family detected worldwide during the same period.

Encyclopedia

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

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

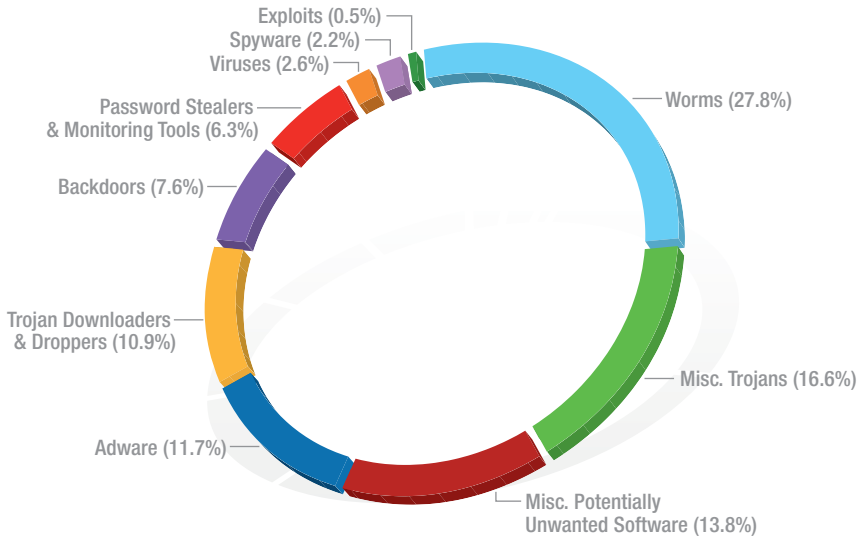
Win32/Corripio: A generic detection for a large number of different trojans that attempt to steal passwords for popular online games, but are otherwise behaviorally dissimilar.

http://www.microsoft.com/av

Malaysia

The MSRT detected malware on 4.0 out of every 1,000 computers scanned in Malaysia during 2H09 (a CCM score of 4.0—down from 5.1 in 1H09 and lower than the average worldwide CCM of 7.0). Figure 127 and Figure 128 list the malware and potentially unwanted software categories and families detected by all Microsoft desktop anti-malware products in Malaysia in 2H09.

FIGURE 127. Malware and potentially unwanted software in Malaysia, by category, in 2H09



Category	Infected Computers
Worms	35,780
Miscellaneous Trojans	21,302
Misc. Potentially Unwanted Software	17,837
Adware	15,112
Trojan Downloaders & Droppers	13,989
Backdoors	9,815
Password Stealers & Monitoring Tools	8,087
Viruses	3,394
Spyware	2,887
Exploits	691

Notes and observations:

- The threat landscape in Malaysia was dominated by malware, which accounted for 72.2 percent of all threats detected on infected computers in 2H09, up from 69.6 percent in 1H09.
- The most common category in Malaysia was Worms, which accounted for 27.8 percent of all infected computers, down from 28.1 percent in 1H09.
- The second-most common category in Malaysia was Miscellaneous Trojans, which includes all trojan families that are not classified as downloaders/droppers or backdoors, and accounted for 16.6 percent of all infected computers, down from 17.0 percent in 1H09.
- The category Trojan Downloaders & Droppers was significantly lower in Malaysia than in many other countries and regions around the world at 10.9 percent, up slightly from 10.4 percent in 1H09.

FIGURE 128. Top 25 families in Malaysia in 2H09

Rank	Family	Most Significant Category	Infected Computers
1	Win32/Conficker	Worms	15,802
2	Win32/Taterf	Worms	11,633
3	Win32/BaiduSobar	Misc. Potentially Unwanted Software	8,010
4	Win32/Renos	Trojan Downloaders & Droppers	7,403
5	Win32/IRCbot	Backdoors	6,028
6	Win32/Frethog	Password Stealers & Monitoring Tools	5,031
7	Win32/Hamweq	Worms	4,813
8	Win32/SeekmoSearchAssistant	Adware	4,510
9	Win32/Agent	Miscellaneous Trojans	3,983
10	Win32/ZangoSearchAssistant	Adware	3,921
11	Win32/Autorun	Worms	3,734
12	Win32/Hotbar	Adware	3,655
13	Win32/Alureon	Miscellaneous Trojans	3,223
14	Win32/DoubleD	Adware	2,201
15	Win32/FakeXPA	Miscellaneous Trojans	2,094
16	Win32/ZangoShoppingreports	Adware	2,067
17	Win32/VB	Miscellaneous Trojans	2,003
18	Win32/Advantage	Adware	1,867
19	Win32/C2Lop	Miscellaneous Trojans	1,736
20	Win32/FakeVimes	Trojan Downloaders & Droppers	1,710
21	Win32/PossibleHostsFileHijack	Misc. Potentially Unwanted Software	1,536
22	Win32/Rimecud	Worms	1,468
23	Win32/Yektel	Miscellaneous Trojans	1,455
24	Win32/Webdir	Spyware	1,374
25	Win32/Winwebsec	Miscellaneous Trojans	1,340

Encyclopedia

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

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

Win32/Yektel: A family of trojans that display fake warnings of spyware or malware in an attempt to lure the user into installing or paying money to register rogue security software programs such as Win32/FakeXPA.

Win32/Winwebsec: A rogue security software family distributed under the names Winweb Security, System Security, and others.

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

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

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

Win32/Autorun: A worm that attempts to spread by being copied into all removable drives.

http://www.microsoft.com/av

Notes and observations:

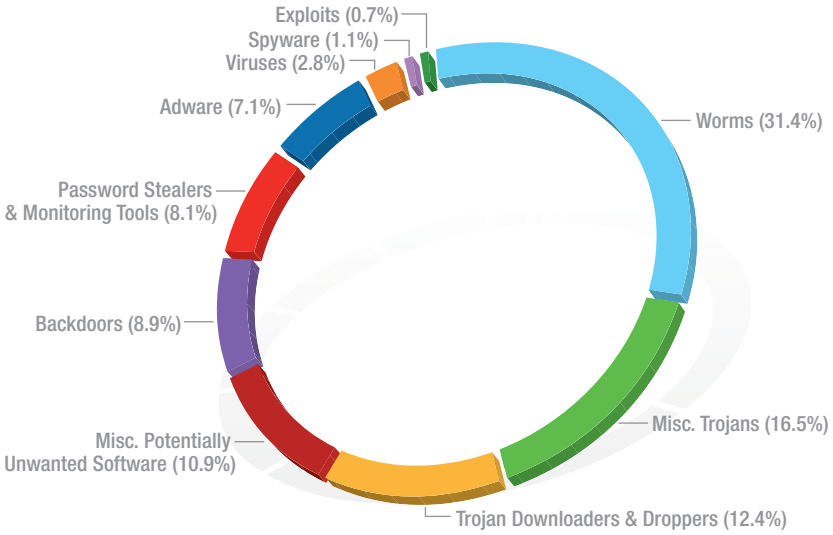
- Four of the top 25 families (Win32/FakeXPA, Win32/FakeVimes, Win32/Yektel, and Win32/Winwebsec) detected on infected machines in Malaysia in 2H09 are rogue security software programs. Rogue security software is relatively rare in Asia, and Malaysia is a notable exception.
- Win32/IRCbot was the fifth-most prevalent family detected in Malaysia in 2H09, but it was not present in the top 25 families detected worldwide in the same period. Win32/IRCbot is a trojan that connects to an Internet Relay Chat (IRC) server and provides attackers with remote access to the infected system. Commands that can be remotely executed include downloading and executing files. Win32/IRCbot also has the ability to send itself to MSN® Messenger contacts.
- Four of the top 25 most prevalent families in Malaysia during 2H09 (Win32/Hamweq, Win32/Conficker, Win32/Rimecud and Win32/Autorun) can spread via mapped drives with weak or missing passwords, removable media (such as USB drives), or a combination of both.

Mexico

The MSRT detected malware on 10.0 out of every 1,000 computers scanned in Mexico during 2H09 (a CCM score of 10.0—down from 14.5 in 1H09 but still higher than the average worldwide CCM of 7.0). Figure 129 and Figure 130 list the malware and potentially unwanted software categories and families detected by all Microsoft desktop anti-malware products in Mexico in 2H09.

FIGURE 129. Malware and potentially unwanted software in Mexico, by category, in 2H09

Category	Infected Computers
Worms	427,553
Miscellaneous Trojans	223,981
Trojan Downloaders & Droppers	168,861
Misc. Potentially Unwanted Software	148,095
Backdoors	121,676
Password Stealers & Monitoring Tools	109,780
Adware	97,006
Viruses	37,915
Spyware	15,615
Exploits	9,448



Notes and observations:

- The threat landscape in Mexico was dominated by malware, which accounted for 80.8 percent of all threats detected on infected computers in 2H09.
- The most common category in Mexico was Worms, which accounted for 31.4 percent of all infected computers.
- The second-most common category in Mexico was Miscellaneous Trojans, which includes all trojan families that are not classified as downloaders/droppers or backdoors, and accounted for 16.5 percent of all infected computers.

FIGURE 130. Top 25 families in Mexico in 2H09

Rank	Family	Most Significant Category	Infected Computers
1	Win32/Taterf	Worms	192,185
2	Win32/Hamweq	Worms	89,936
3	Win32/Conficker	Worms	73,932
4	Win32/Autorun	Worms	72,261
5	Win32/Frethog	Password Stealers & Monitoring Tools	68,579
6	Win32/IRCbot	Backdoors	67,926
7	Win32/C2Lop	Miscellaneous Trojans	58,254
8	Win32/Renos	Trojan Downloaders & Droppers	57,665
9	Win32/Agent	Miscellaneous Trojans	51,776
10	Win32/Brontok	Worms	45,741
11	Win32/Rimecud	Worms	41,962
12	Win32/Alureon	Miscellaneous Trojans	32,107
13	ASX/Wimad	Trojan Downloaders & Droppers	31,532
14	Win32/DelfInject	Misc. Potentially Unwanted Software	30,487
15	Win32/Slenfbot	Worms	25,459
16	Win32/PossibleHostsFileHijack	Misc. Potentially Unwanted Software	23,423
17	Win32/VBInject	Misc. Potentially Unwanted Software	23,312
18	Win32/DoubleD	Adware	23,072
19	Win32/VB	Miscellaneous Trojans	21,188
20	Win32/Zlob	Trojan Downloaders & Droppers	19,393
21	Win32/SeekmoSearchAssistant	Adware	18,085
22	Win32/PlayMP3z	Adware	17,201
23	Win32/Silly_P2P	Worms	17,084
24	Win32/Vobfus	Worms	16,327
25	Win32/Rbot	Backdoors	14,632

Notes and observations:

- Game password stealers were common in Mexico during 2H09. In Mexico Win32/Taterf ranked first and Win32/Frethog ranked fifth; worldwide, Win32/Taterf and Win32/Frethog ranked first passwords or via USB drives.
- Win32/IRCbot was the sixth-most prevalent family detected in Mexico in 2H09, but it was not present in the top 25 families detected worldwide in the same period. Win32/IRCbot is a trojan that connects to an IRC server and provides attackers with remote access to the infected system. Commands that can be remotely executed include downloading and executing files. Win32/IRCbot also has the ability to send itself to MSN Messenger contacts.
- Win32/C2Lop, a trojan that modifies Web browser settings and delivers contextual and pop-up advertisements, was more prevalent in Mexico than it was worldwide. Win32/C2Lop was the seventh-most prevalent family in Mexico during 2H09, but it was only the twenty-third–most prevalent worldwide. Win32/C2Lop may be distributed in a software package called "MessengerPlus!", an add-on for Windows Live Messenger.

Encyclopedia

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

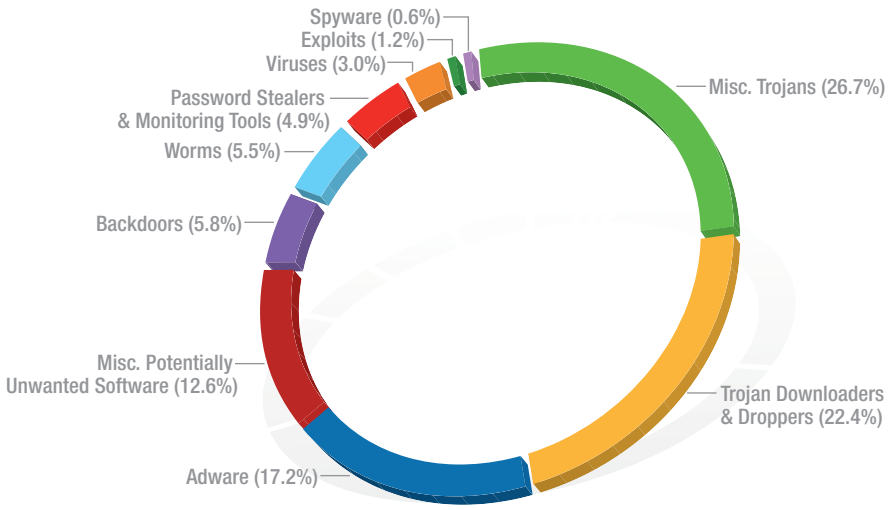
Win32/Frethog: A large family of password-stealing trojans that target confidential data, such as account information, from massively multiplayer online games.

http://www.microsoft.com/av

Netherlands

The MSRT detected malware on 3.3 out of every 1,000 computers scanned in the Netherlands during 2H09 (a CCM score of 3.3—down from 4.3 in 1H09 and significantly lower than the average worldwide CCM of 7.0). Figure 131 and Figure 132 list the malware and potentially unwanted software categories and families detected by all Microsoft desktop anti-malware products in the Netherlands in 2H09.

FIGURE 131. Malware and potentially unwanted software in the Netherlands, by category, in 2H09



Category	Infected Computers
Miscellaneous Trojans	202,211
Trojan Downloaders & Droppers	169,558
Adware	130,503
Misc. Potentially Unwanted Software	95,549
Backdoors	44,266
Worms	41,611
Password Stealers & Monitoring Tools	36,704
Viruses	22,505
Exploits	9,221
Spyware	4,651

Notes and observations:

- The threat landscape in the Netherlands was dominated by malware, which accounted for 69.5 percent of all threats detected on infected computers in 2H09.
- The most common category in the Netherlands was Miscellaneous Trojans, which includes all trojan families that are not classified as downloaders/droppers or backdoors, and accounted for 26.7 percent of all infected computers.
- Together, Miscellaneous Trojans and Trojan Downloaders & Droppers made up more than 49 percent of all families detected on infected computers in the Netherlands in 2H09.

FIGURE 132. Top 25 families in the Netherlands in 2H09

Rank	Family	Most Significant Category	Infected Computers
1	Win32/Renos	Trojan Downloaders & Droppers	72,962
2	Win32/Alureon	Miscellaneous Trojans	64,228
3	Win32/Hotbar	Adware	48,883
4	ASX/Wimad	Trojan Downloaders & Droppers	42,492
5	Win32/ZangoSearchAssistant	Adware	36,130
6	Win32/Agent	Miscellaneous Trojans	26,062
7	Win32/PlayMP3z	Adware	25,366
8	Win32/ZangoShoppingreports	Adware	18,443
9	Win32/FakeXPA	Miscellaneous Trojans	17,711
10	Win32/Rustock	Backdoors	16,751
11	Win32/Zlob	Trojan Downloaders & Droppers	15,853
12	Win32/Bredolab	Trojan Downloaders & Droppers	15,440
13	Win32/Cutwail	Trojan Downloaders & Droppers	13,303
14	Win32/Yektel	Miscellaneous Trojans	11,923
15	Win32/Taterf	Worms	11,867
16	Win32/Vundo	Miscellaneous Trojans	10,932
17	Win32/FakeRean	Miscellaneous Trojans	9,931
18	Win32/Bumat	Miscellaneous Trojans	9,529
19	Win32/Winwebsec	Miscellaneous Trojans	9,511
20	Win32/FakeCog	Miscellaneous Trojans	9,323
21	Win32/WhenU	Adware	8,968
22	Win32/Zwangi	Misc. Potentially Unwanted Software	8,475
23	Win32/SeekmoSearchAssistant	Adware	8,468
24	Win32/Obfuscator	Misc. Potentially Unwanted Software	8,459
25	Win32/Daurso	Password Stealers & Monitoring Tools	8,296

Encyclopedia

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

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

http://www.microsoft.com/av

Notes and observations:

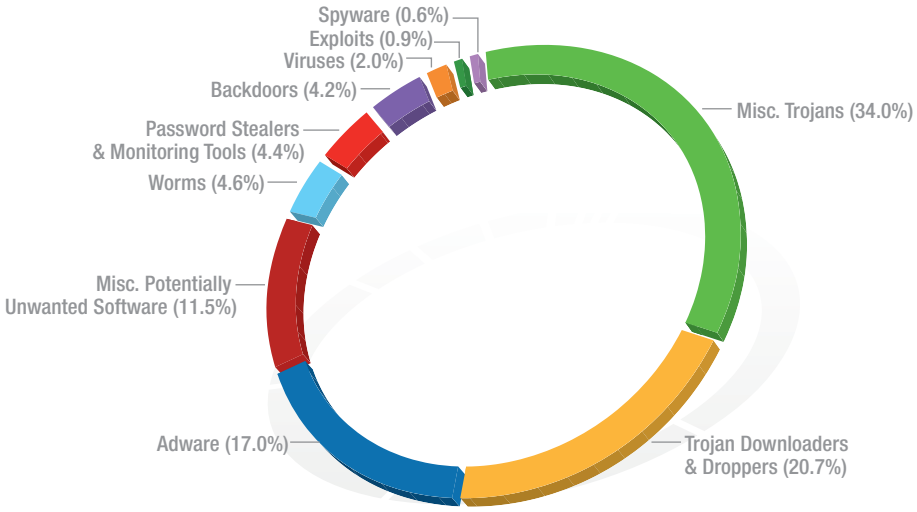
- ASX/Wimad, a malicious Windows Media file that, when played, opens a specified URL in a Web browser, was more prevalent in the Netherlands during 2H09 than it was worldwide. ASX/Wimad was the fourth-most prevalent family in the Netherlands during 2H09, but it ranked only twelfth worldwide.
- Win32/PlayMP3z was the seventh-most prevalent family detected in the Netherlands during 2H09, but it was not in the top 25 families detected worldwide during the same period. Win32/PlayMP3z is an adware program that displays advertisements in connection with a music player.
- Win32/Rustock was the tenth-most prevalent family in the Netherlands in 2H09, but it did not appear in the top 25 families detected worldwide. Win32/Rustock is a multicomponent family of rootkit-enabled backdoor trojans that were historically developed to aid in the distribution of spam e-mail. Recent variants have been associated with the distribution of rogue security software.
- Game password stealers were not as common in the Netherlands during 2H09 as they were worldwide. Win32/Taterf and Win32/Frethog ranked first and sixth in the world respectively; in the Netherlands Win32/Taterf only ranked fifteenth, and Win32/Frethog did not appear in the top 25 families at all.

Norway

The MSRT detected malware on 2.5 out of every 1,000 computers scanned in Norway during 2H09 (a CCM score of 2.5—down from 3.3 in 1H09 and significantly lower than the average worldwide CCM of 7.0). Figure 133 and Figure 134 list the malware and potentially unwanted software categories and families detected by all Microsoft desktop anti-malware products in Norway in 2H09.

FIGURE 133. Malware and potentially unwanted software in Norway, by category, in 2H09

Category	Infected Computers
Miscellaneous Trojans	69,581
Trojan Downloaders & Droppers	42,443
Adware	34,767
Misc. Potentially Unwanted Software	23,649
Worms	9,417
Password Stealers & Monitoring Tools	9,092
Backdoors	8,642
Viruses	4,105
Exploits	1,846
Spyware	1,313



Notes and observations:

- The threat landscape in Norway was dominated by malware, which accounted for 70.8 percent of all threats detected on infected computers in 2H09, up from 64.3 percent in 1H09.
- The most common category in Norway was Miscellaneous Trojans, which includes all trojan families that are not classified as downloaders/droppers or backdoors, and accounted for 34.0 percent of all infected computers, up from 28.2 percent in 1H09.
- The second-most common category in Norway in 2H09 was Trojan Downloaders & Droppers, which accounted for 20.7 percent of all infected computers, down from 23.5 percent in 1H09.
- Together, Miscellaneous Trojans and Trojan Downloaders & Droppers made up more than 54 percent of all families detected on infected computers in Norway in 2H09.

FIGURE 134. Top 25 families in Norway in 2H09

Rank	Family	Most Significant Category	Infected Computers
1	Win32/Renos	Trojan Downloaders & Droppers	24,885
2	Win32/FakeXPA	Miscellaneous Trojans	16,918
3	Win32/Alureon	Miscellaneous Trojans	12,483
4	Win32/Yektel	Miscellaneous Trojans	12,167
5	Win32/Hotbar	Adware	11,540
6	Win32/ZangoSearchAssistant	Adware	10,511
7	Win32/Winwebsec	Miscellaneous Trojans	8,714
8	ASX/Wimad	Trojan Downloaders & Droppers	7,031
9	Win32/Koobface	Worms	6,818
10	Win32/PlayMP3z	Adware	6,166
11	Win32/ZangoShoppingreports	Adware	5,377
12	Win32/Agent	Miscellaneous Trojans	4,354
13	Win32/FakeSpypro	Miscellaneous Trojans	4,308
14	Win32/SeekmoSearchAssistant	Adware	4,010
15	Win32/Zlob	Trojan Downloaders & Droppers	3,169
16	Win32/Vundo	Miscellaneous Trojans	2,969
17	Win32/FakeRean	Miscellaneous Trojans	2,655
18	Win32/WhenU	Adware	2,516
19	Win32/Rustock	Backdoors	2,493
20	Win32/FakeSmoke	Trojan Downloaders & Droppers	2,445
21	Win32/Bredolab	Trojan Downloaders & Droppers	2,363
22	Win32/Cutwail	Trojan Downloaders & Droppers	2,350
23	Win32/Zwangi	Misc. Potentially Unwanted Software	2,168
24	Win32/MyDealAssistant	Adware	2,150
25	Win32/DoubleD	Adware	2,122

Notes and observations:

- Six of the top 25 families in Norway in 2H09 (Win32/FakeXPA, Win32/Yektel, Win32/Winwebsec, Win32/FakeSpypro, Win32/FakeRean, and Win32/FakeSmoke) were rogue security software programs. Of these, FakeXPA, Winwebsec, Yektel, and FakeRean were in the top 25 for Norway in 1H09.
- Nine of the top 25 families were potentially unwanted software families, compared to seven in 1H09.
- Win32/PlayMP3z was the tenth-most prevalent family detected in Norway during 2H09, but it was not in the top 25 families detected worldwide during the same period. Win32/PlayMP3z is an adware program that displays advertisements in connection with a music player.
- Worms remained rare in Norway with only one worm (Win32/Koobface) appearing among the top 25 families detected on infected computers in Norway in 2H09, identical to the pattern observed in 1H09.

Encyclopedia

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

Win32/Yektel: A family of trojans that display fake warnings of spyware or malware in an attempt to lure the user into installing or paying money to register rogue security software programs such as Win32/FakeXPA.

Win32/Winwebsec: A rogue security software family distributed under the names Winweb Security, System Security, and others.

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

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

Win32/FakeSmoke: A rogue security software family distributed under the name WinBlueSoft and others.

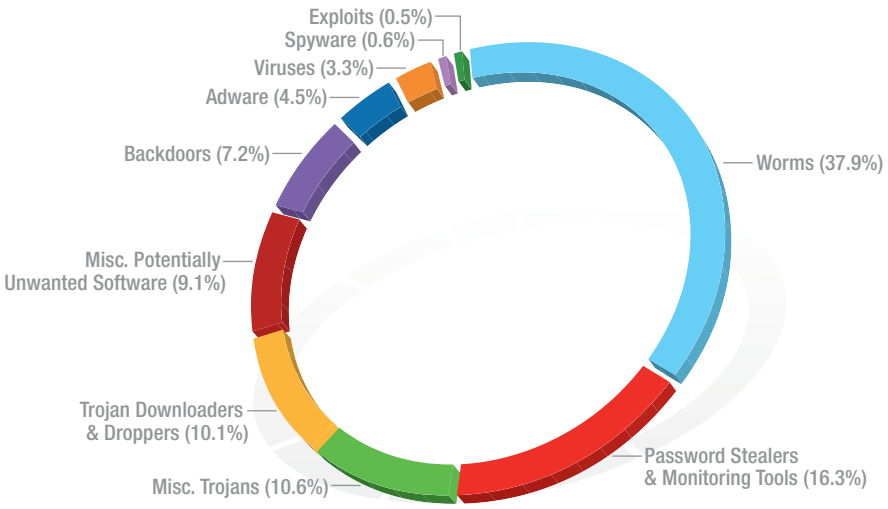
Win32/Koobface: A multi-component family of malware used to compromise computers and use them to perform various malicious tasks. It spreads through the internal messaging systems of popular social networking sites.

http://www.microsoft.com/av

Peru

The MSRT detected malware on 6.4 out of every 1,000 computers scanned in Peru during 2H09 (a CCM score of 6.4—down from 8.5 in 1H09 and lower than the average worldwide CCM of 7.0). Figure 135 and Figure 136 list the malware and potentially unwanted software categories and families detected by all Microsoft desktop anti-malware products in Peru in 2H09.

FIGURE 135. Malware and potentially unwanted software in Peru, by category, in 2H09



Category	Infected Computers
Worms	38,348
Password Stealers & Monitoring Tools	16,522
Misc. Trojans	10,744
Trojan Downloaders & Droppers	10,208
Misc. Potentially Unwanted Software	9,196
Backdoors	7,324
Adware	4,522
Viruses	3,300
Spyware	566
Exploits	459

Notes and observations:

- The threat landscape in Peru was dominated by malware, which accounted for 85.9 percent of all threats detected on infected computers in 2H09.
- The most common category in Peru was Worms, which accounted for 37.9 percent of all infected computers.

FIGURE 136. Top 25 families in Peru in 2H09

Rank	Family	Most Significant Category	Infected Computers
1	Win32/Taterf	Worms	26,939
2	Win32/Frethog	Password Stealers & Monitoring Tools	12,301
3	Win32/Conficker	Worms	6,529
4	Win32/Hamweq	Worms	4,119
5	Win32/IRCbot	Backdoors	2,983
6	Win32/Renos	Trojan Downloaders & Droppers	2,964
7	Win32/PossibleHostsFileHijack	Misc. Potentially Unwanted Software	2,303
8	Win32/Agent	Miscellaneous Trojans	2,204
9	Win32/Bancos	Password Stealers & Monitoring Tools	2,094
10	Win32/C2Lop	Miscellaneous Trojans	2,060
11	Win32/Autorun	Worms	1,904
12	Win32/Small	Trojan Downloaders & Droppers	1,876
13	Win32/Rimecud	Worms	1,768
14	Win32/FlyAgent	Backdoors	1,741
15	Win32/Alureon	Miscellaneous Trojans	1,579
16	Win32/DoubleD	Adware	1,475
17	Win32/Cutwail	Trojan Downloaders & Droppers	1,471
18	Win32/VBInject	Misc. Potentially Unwanted Software	1,162
19	Win32/Zlob	Trojan Downloaders & Droppers	1,056
20	Win32/VB	Miscellaneous Trojans	1,012
21	Win32/Bredolab	Trojan Downloaders & Droppers	920
22	Win32/Rustock	Backdoors	883
23	Win32/DelfInject	Misc. Potentially Unwanted Software	781
24	Win32/Virut	Viruses	772
25	Win32/Hotbar	Adware	769

Encyclopedia

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

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

http://www.microsoft.com/av

Notes and observations:

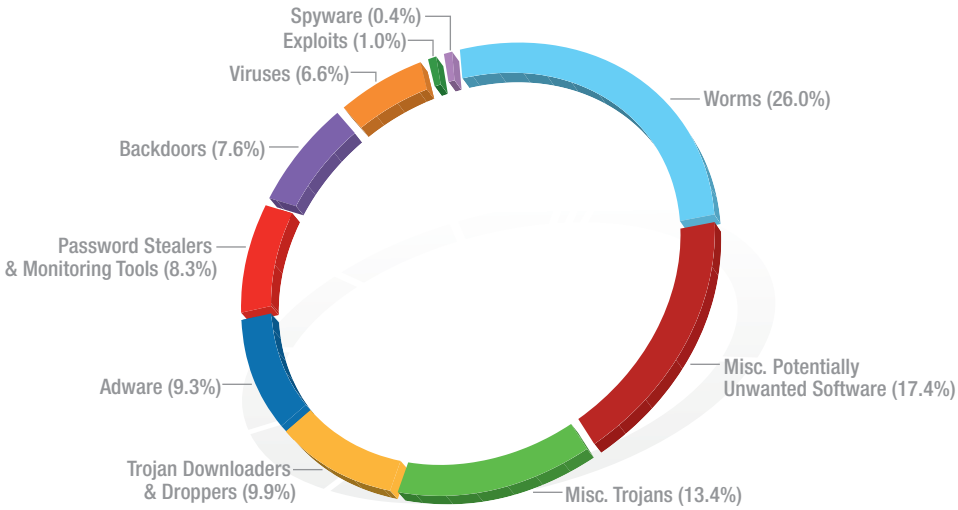
- Three of the top four families detected on infected computers in Peru in 2H09 (and 5 of the top 13 families) were worms. All of these worm families can spread via mapped drives with missing or weak passwords or via USB drives.
- Game password stealers were very common in Peru during 2H09. Win32/Taterf and Win32/Frethog ranked first and sixth in the world respectively; in Peru Win32/Taterf ranked first, and Win32/Frethog ranked second.
- Win32/IRCbot was the fifth-most prevalent family detected in Peru in 2H09, but it was not present in the top 25 families detected worldwide in the same period. Win32/IRCbot is a trojan that connects to an IRC server and provides attackers with remote access to the infected system. Commands that can be remotely executed include downloading and executing files. Win32/IRCbot also has the ability to send itself to MSN Messenger contacts.
- Win32/Small was the twelfth-most detected threat on infected computers in Peru during 2H09. Win32/Small is a trojan that downloads and executes a file from a specified URL. Most commonly, the downloaded file is a dialer application for adult content. Win32/Small was not present in the top 25 families detected worldwide in 2H09.

Russia

The MSRT detected malware on 9.8 out of every 1,000 computers scanned in Russia during 2H09 (a CCM score of 9.8—down from 15.0 in 1H09 but still higher than the average worldwide CCM of 7.0). Figure 137 and Figure 138 list the malware and potentially unwanted software categories and families detected by all Microsoft desktop anti-malware products in Russia in 2H09.

FIGURE 137. Malware and potentially unwanted software in Russia, by category, in 2H09

Category	Infected Computers
Worms	227,179
Misc. Potentially Unwanted Software	152,071
Miscellaneous Trojans	117,324
Trojan Downloaders & Droppers	86,620
Adware	81,347
Password Stealers & Monitoring Tools	72,683
Backdoors	66,112
Viruses	57,289
Exploits	8,904
Spyware	3,590



Notes and observations:

- The threat landscape in Russia was dominated by malware, which accounted for 72.8 percent of all threats detected on infected computers in 2H09, down from 79.7 percent in 1H09 and 81.1 percent in 2H08.
- The most common category in Russia was Worms, which accounted for 26.0 percent of all infected computers in 2H09, down from 32.7 percent in 1H09. The top two families detected in Russia in 2H09 were both worms.
- The second-most common category in Russia was Miscellaneous Potentially Unwanted Software, which accounted for 17.4 percent of all infected computers in 2H09, up significantly from 10.5 percent in 1H09.

FIGURE 138. Top 25 families in Russia in 2H09

Rank	Family	Most Significant Category	Infected Computers
1	Win32/Conficker	Worms	101,722
2	Win32/Taterf	Worms	66,432
3	Win32/Kerlofost	Misc. Potentially Unwanted Software	44,046
4	Win32/Ldpinch	Password Stealers & Monitoring Tools	30,212
5	Win32/Hamweq	Worms	24,207
6	Win32/Bumat	Miscellaneous Trojans	24,076
7	Win32/Renos	Trojan Downloaders & Droppers	23,695
8	Win32/Adsubscribe	Adware	22,055
9	Win32/Meredrop	Trojan Downloaders & Droppers	19,816
10	Win32/Obfuscator	Misc. Potentially Unwanted Software	19,019
11	Win32/Jeefo	Viruses	18,997
12	Win32/MyCentria	Adware	18,838
13	Win32/Fierads	Adware	18,823
14	Win32/Cutwail	Trojan Downloaders & Droppers	18,710
15	Win32/IRCBot	Backdoors	18,336
16	Win32/Alureon	Miscellaneous Trojans	18,277
17	Win32/WhenU	Adware	17,865
18	Win32/Bredolab	Trojan Downloaders & Droppers	17,470
19	Win32/Autorun	Worms	15,803
20	Win32/Agent	Miscellaneous Trojans	15,694
21	Win32/Cmdow	Misc. Potentially Unwanted Software	15,509
22	Win32/Orsam	Miscellaneous Trojans	12,359
23	Win32/Frethog	Password Stealers & Monitoring Tools	12,110
24	Win32/Brontok	Worms	11,730
25	Win32/Rustock	Backdoors	11,173

Notes and observations:

- Three of the top five families detected on infected computers in Russia in 2H09 (and 5 of the top 25 families) were worms. All of these worm families can spread via mapped drives with missing or weak passwords, and/or USB drives. The top two families detected in Russia in 2H09 (Win32/Conficker and Win32/Taterf) were both worms – this was the same pattern observed in 1H09.
- Win32/Kerlofost was the third-most detected family on computers in Russia in 2H09, but it was not present in the top 25 families detected worldwide. Win32/Kerlofost is a DLL file embedded in various programs and registered as a BHO. It may modify browsing behavior, redirect searches, report user statistics, behavior, and searches back to a remote server, and display pop-up advertisements.
- Win32/Ldpinch was the fourth-most detected family on computers in Russia in 2H09, but it was not present in the top 25 families detected worldwide. Win32/Ldpinch is a family of password-stealing trojans. This trojan gathers private user data, such as passwords, from the host computer and sends the data to the attacker at a preset e-mail address. The Win32/Ldpinch trojans use their own Simple Mail Transfer Protocol (SMTP) engine or a Web-based proxy for sending the e-mail, thus copies of the sent e-mail will not appear in the affected user's e-mail client.

Encyclopedia

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

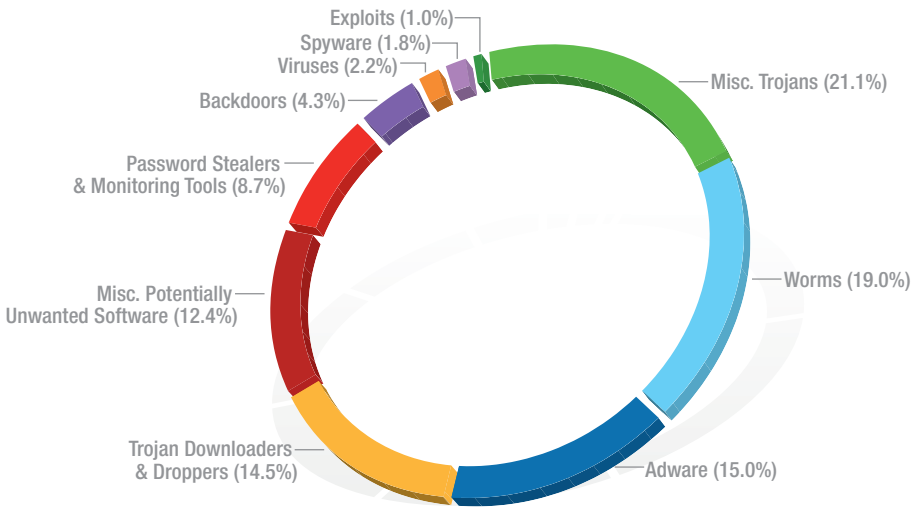
Win32/Taterf: A family of worms that spread through mapped drives to steal login and account details for popular online games.

http://www.microsoft.com/av

Singapore

The MSRT detected malware on 4.6 out of every 1,000 computers scanned in Singapore during 2H09 (a CCM score of 4.6—down slightly from 4.7 in 1H09 and still lower than the average worldwide CCM of 7.0). Figure 139 and Figure 140 list the malware and potentially unwanted software categories and families detected by all Microsoft desktop anti-malware products in Singapore in 2H09.

FIGURE 139. Malware and potentially unwanted software in Singapore, by category, in 2H09



Category	Infected Computers
Miscellaneous Trojans	30,610
Worms	27,600
Adware	21,709
Trojan Downloaders & Droppers	21,108
Misc. Potentially Unwanted Software	18,061
Password Stealers & Monitoring Tools	12,690
Backdoors	6,177
Viruses	3,214
Spyware	2,599
Exploits	1,426

Notes and observations:

- The threat landscape in Singapore was dominated by malware, which accounted for 70.8 percent of all threats detected on infected computers in 2H09.
- The most common category in Singapore was Miscellaneous Trojans, which includes all trojan families that are not classified as downloaders/droppers or backdoors, and accounted for 21.1 percent of all infected computers.
- The second-most common category in Singapore was Worms, which accounted for 19.0 percent of all infected computers.

FIGURE 140. Top 25 families in Singapore in 2H09

Rank	Family	Most Significant Category	Infected Computers
1	Win32/Renos	Trojan Downloaders & Droppers	11,959
2	Win32/Taterf	Worms	10,948
3	Win32/ZangoSearchAssistant	Adware	7,558
4	Win32/Hotbar	Adware	7,154
5	Win32/BaiduSobar	Misc. Potentially Unwanted Software	6,342
6	Win32/Agent	Miscellaneous Trojans	5,648
7	Win32/Hamweq	Worms	5,647
8	Win32/SeekmoSearchAssistant	Adware	5,242
9	Win32/Conficker	Worms	5,040
10	Win32/Alureon	Miscellaneous Trojans	4,958
11	Win32/Bancos	Password Stealers & Monitoring Tools	4,375
12	Win32/C2Lop	Miscellaneous Trojans	4,065
13	Win32/ZangoShoppingreports	Adware	3,773
14	Win32/Frethog	Password Stealers & Monitoring Tools	3,770
15	Win32/FakeXPA	Miscellaneous Trojans	3,743
16	Win32/DoubleD	Adware	3,211
17	Win32/Autorun	Worms	2,998
18	Win32/Yektel	Miscellaneous Trojans	2,606
19	Win32/Koobface	Worms	2,358
20	Win32/IRCbot	Backdoors	2,230
21	Win32/FakeVimes	Trojan Downloaders & Droppers	2,084
22	Win32/Winwebsec	Miscellaneous Trojans	1,877
23	Win32/Bredolab	Trojan Downloaders & Droppers	1,773
24	Win32/PossibleHostsFileHijack	Misc. Potentially Unwanted Software	1,632
25	Win32/Zlob	Trojan Downloaders & Droppers	1,609

Notes and observations:

- Three of the top eight families detected in Singapore in 2H09 were potentially unwanted software. Win32/ZangoSearchAssistant was the third-most prevalent family in Singapore but was only thirteenth worldwide; Win32/Hotbar was the fourth-most prevalent family in Singapore but was only tenth worldwide; Win32/SeekmoSearchAssistant was the eighth-most detected family on computers in Singapore in 2H09 but was not present in the top 25 families detected worldwide. All three of these families display contextual pop-up advertisements based on monitoring browsing and search behavior.
- Five of the top 25 families detected on infected computers in Singapore in 2H09 were worms. All of these worm families can spread via mapped drives with missing or weak passwords or via USB drives.

Encyclopedia

Win32/ZangoSearch-Assistant: Adware that monitors the user's Web-browsing activity and displays pop-up advertisements related to the Internet sites the user is viewing.

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

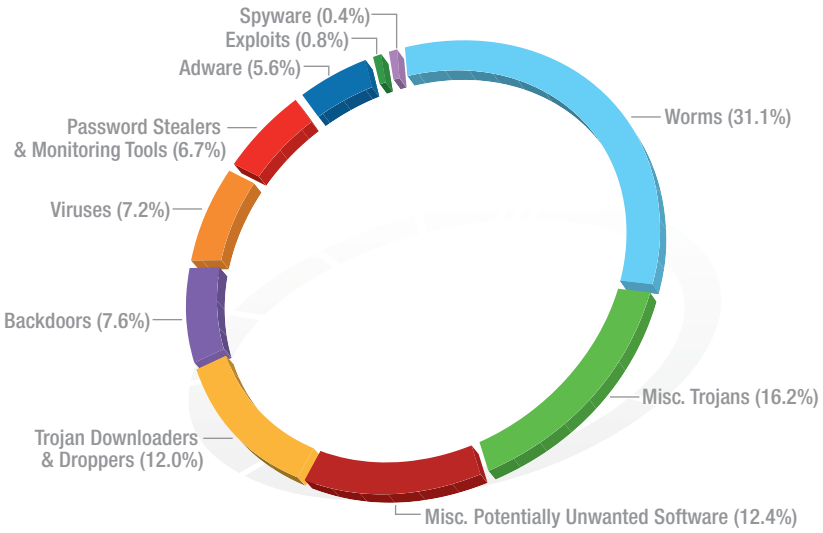
Win32/SeekmoSearch-Assistant: Adware that displays targeted search results and pop-up advertisements based on terms that the user enters for Web searches. The pop-up advertisements may include adult content.

http://www.microsoft.com/av

South Africa

The MSRT detected malware on 4.8 out of every 1,000 computers scanned in South Africa during 2H09 (a CCM score of 4.8—down from 5.5 in 1H09 and still lower than the average worldwide CCM of 7.0). Figure 141 and Figure 142 list the malware and potentially unwanted software categories and families detected by all Microsoft desktop anti-malware products in South Africa in 2H09.

FIGURE 141. Malware and potentially unwanted software in South Africa, by category, in 2H09



Category	Infected Computers
Worms	36,746
Miscellaneous Trojans	19,206
Misc. Potentially Unwanted Software	14,682
Trojan Downloaders & Droppers	14,229
Backdoors	9,024
Viruses	8,480
Password Stealers & Monitoring Tools	7,875
Adware	6,583
Exploits	931
Spyware	529

Notes and observations:

- The threat landscape in South Africa was dominated by malware, which accounted for 81.6 percent of all threats detected on infected computers in 2H09, up very slightly from 81.1 percent in 1H09.
- The most common category in South Africa was Worms, which accounted for 31.1 percent of all infected computers, down slightly from 32.2 percent in 1H09. Four of the top five families detected in South Africa in 2H09 were worms.
- The second-most common category in South Africa was Miscellaneous Trojans, which includes all trojan families that are not classified as downloaders/droppers or backdoors, and accounted for 16.2 percent of all infected computers, down slightly from 17.0 percent in 1H09.

FIGURE 142. Top 25 families in South Africa in 2H09

Rank	Family	Most Significant Category	Infected Computers
1	Win32/Hamweq	Worms	11,765
2	Win32/Taterf	Worms	9,130
3	Win32/Conficker	Worms	7,283
4	Win32/Renos	Trojan Downloaders & Droppers	6,955
5	Win32/Autorun	Worms	5,988
6	Win32/Frethog	Password Stealers & Monitoring Tools	3,751
7	Win32/Virut	Viruses	3,568
8	Win32/IRCbot	Backdoors	3,492
9	Win32/Agent	Miscellaneous Trojans	3,286
10	Win32/Alureon	Miscellaneous Trojans	3,088
11	Win32/FakeXPA	Miscellaneous Trojans	2,929
12	Win32/RealVNC	Misc. Potentially Unwanted Software	2,615
13	Win32/Brontok	Worms	2,390
14	Win32/Mabezat	Worms	2,291
15	Win32/Yektel	Miscellaneous Trojans	2,241
16	Win32/Rimecud	Worms	2,010
17	Win32/VBInject	Misc. Potentially Unwanted Software	1,903
18	Win32/Zlob	Trojan Downloaders & Droppers	1,762
19	Win32/SeekmoSearchAssistant	Adware	1,634
20	Win32/Hotbar	Adware	1,630
21	Win32/Koobface	Worms	1,507
22	Win32/RJump	Worms	1,467
23	Win32/ZangoSearchAssistant	Adware	1,448
24	Win32/Cutwail	Trojan Downloaders & Droppers	1,430
25	Win32/Bredolab	Trojan Downloaders & Droppers	1,307

Notes and observations:

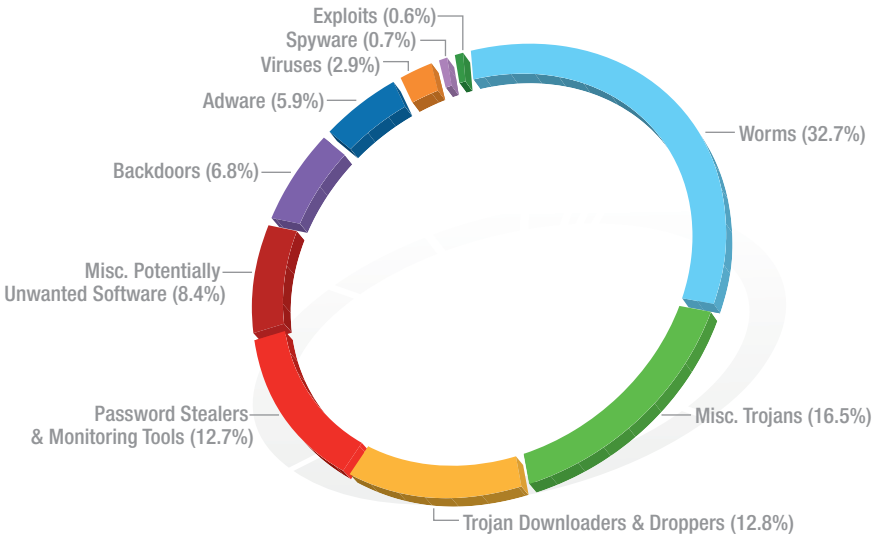
- Four of the top five families detected on infected computers in South Africa in 2H09 (and 9 of the top 25 families) were worms. These worm families can spread via mapped drives with missing or weak passwords or via USB drives.
- Win32/Virut was the seventh-most common family detected on infected computers in South Africa in 2H09, but it was not present in the top 25 families detected worldwide. Win32/Virut is a family of file-infecting viruses that target and infect .exe and .src files accessed on infected systems. Win32/Virut also opens a backdoor by connecting to an IRC server, allowing a remote attacker to download and run files on the infected computer.
- Win32/IRCbot was the eighth-most prevalent family detected in South Africa in 2H09, but it was not present in the top 25 families detected worldwide in the same period. Win32/IRCbot is a trojan that connects to an IRC server and provides attackers with remote access to the infected system. Commands that can be remotely executed include downloading and executing files. Win32/IRCbot also has the ability to send itself to MSN Messenger contacts.
- Win32/Mabezat was the fourteenth-most common family detected in South Africa in 2H09, but it was not present in the top 25 families detected worldwide. Win32/Mabezat is a worm that attempts to spread by copying itself to newly attached media devices, such as USB drives or USB media cards, and even writable network drives. In some samples, Win32/Mabezat can also infect .exe files by prepending its code to the host file.

Spain

The MSRT detected malware on 17.1 out of every 1,000 computers scanned in Spain during 2H09 (a CCM score of 17.1—down from 21.6 in 1H09 but still significantly higher than the average worldwide CCM of 7.0). Figure 143 and Figure 144 list the malware and potentially unwanted software categories and families detected by all Microsoft desktop anti-malware products in Spain in 2H09.

FIGURE 143. Malware and potentially unwanted software in Spain, by category, in 2H09

Category	Infected Computers
Worms	731,083
Miscellaneous Trojans	367,404
Trojan Downloaders & Droppers	287,331
Password Stealers & Monitoring Tools	284,107
Misc. Potentially Unwanted Software	187,460
Backdoors	151,641
Adware	132,556
Viruses	65,176
Spyware	16,724
Exploits	13,982



Notes and observations:

- The threat landscape in Spain was dominated by malware, which accounted for 84.9 percent of all threats detected on infected computers in 2H09.
- The most common category in Spain was Worms, which accounted for 32.7 percent of all infected computers.
- The second-most common category in Spain was Miscellaneous Trojans, which includes all trojan families that are not classified as downloaders/droppers or backdoors, and accounted for 16.5 percent of all infected computers.
- Together, Miscellaneous Trojans and Trojan Downloaders & Droppers made up more than 29 percent of all families detected on infected computers in Spain in 2H09.

FIGURE 144. Top 25 families in Spain in 2H09

Rank	Family	Most Significant Category	Infected Computers
1	Win32/Taterf	Worms	403,115
2	Win32/Frethog	Password Stealers & Monitoring Tools	179,275
3	Win32/Hamweq	Worms	135,798
4	Win32/Conficker	Worms	107,168
5	Win32/Renos	Trojan Downloaders & Droppers	99,614
6	Win32/Alureon	Miscellaneous Trojans	87,902
7	Win32/IRCbot	Backdoors	63,887
8	Win32/C2Lop	Miscellaneous Trojans	59,392
9	Win32/Vundo	Miscellaneous Trojans	56,793
10	Win32/DoubleD	Adware	54,273
11	Win32/Bancos	Password Stealers & Monitoring Tools	47,749
12	Win32/Agent	Miscellaneous Trojans	44,831
13	Win32/Brontok	Worms	38,038
14	Win32/Autorun	Worms	37,879
15	Win32/Zlob	Trojan Downloaders & Droppers	36,197
16	Win32/Slenfbot	Worms	32,252
17	Win32/Cutwail	Trojan Downloaders & Droppers	31,134
18	Win32/Bredolab	Trojan Downloaders & Droppers	29,784
19	Win32/Wintrim	Miscellaneous Trojans	27,027
20	Win32/Rustock	Backdoors	24,132
21	Win32/Cmdow	Misc. Potentially Unwanted Software	22,952
22	ASX/Wimad	Trojan Downloaders & Droppers	21,241
23	Win32/Hotbar	Adware	19,028
24	Win32/Small	Trojan Downloaders & Droppers	18,356
25	Win32/Rbot	Backdoors	17,734

Notes and observations:

- Game password stealers were very common in Spain during 2H09. Win32/Taterf and Win32/Frethog ranked first and sixth in the world respectively; in Spain, Win32/Taterf ranked first and Win32/Frethog ranked second.
- Three of the top five families detected on infected computers in Spain in 2H09 (and 6 of the top 20 families) were worms. These worm families can spread via mapped drives with missing or weak passwords or via USB drives.
- Win32/IRCbot was the seventh-most prevalent family detected in Spain 2H09, but it was not present in the top 25 families detected worldwide in the same period. Win32/IRCbot is a trojan that connects to an IRC server and provides attackers with remote access to the infected system. Commands that can be remotely executed include downloading and executing files. Win32/IRCbot also has the ability to send itself to MSN Messenger contacts.
- Win32/C2Lop was significantly more prevalent in Spain than it was worldwide. Win32/C2Lop, a trojan that modifies Web browser settings and delivers contextual and pop-up advertisements, was the eighth-most prevalent family in Spain during 2H09, but it was only twenty-third most prevalent worldwide. Win32/C2Lop may be distributed in a software package called "MessengerPlus!", an add-on for Windows Live Messenger.

Encyclopedia

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

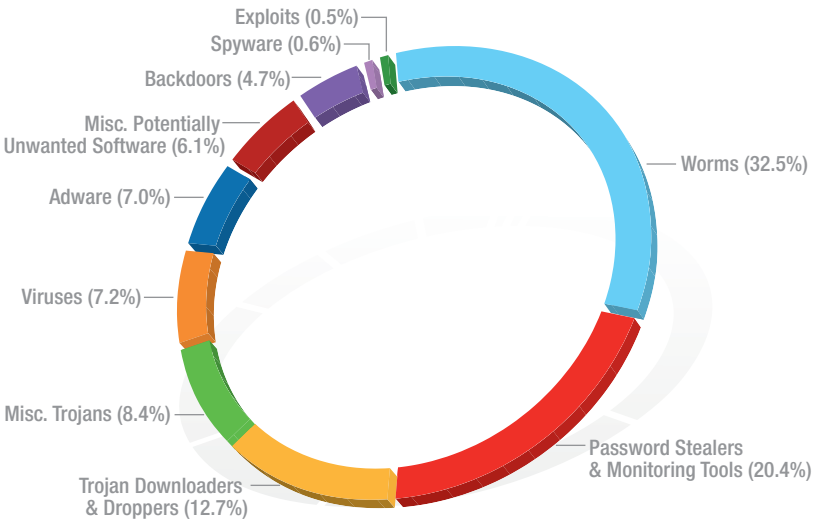
Win32/Frethog: A large family of password-stealing trojans that target confidential data, such as account information, from massively multiplayer online games.

http://www.microsoft.com/av

Turkey

The MSRT detected malware on 20.0 out of every 1,000 computers scanned in Turkey during 2H09 (a CCM score of 20.0—down from 32.3 in 1H09 but still significantly higher than the average worldwide CCM of 7.0). Figure 145 and Figure 146 list the malware and potentially unwanted software categories and families detected by all Microsoft desktop anti-malware products in Turkey in 2H09.

FIGURE 145. Malware and potentially unwanted software in Turkey, by category, in 2H09



Category	Infected Computers
Worms	394,394
Password Stealers & Monitoring Tools	247,256
Trojan Downloaders & Droppers	154,608
Miscellaneous Trojans	102,422
Viruses	87,634
Adware	84,682
Misc. Potentially Unwanted Software	73,683
Backdoors	57,121
Spyware	6,944
Exploits	5,632

Notes and observations:

- The threat landscape in Turkey was dominated by malware, which accounted for 86.4 percent of all threats detected on infected computers in 2H09.
- The most common category in Turkey was Worms, which accounted for 32.5 percent of all infected computers.
- The second-most common category in Turkey was Password Stealers & Monitoring Tools, which accounted for 20.4 percent of all infected computers.

FIGURE 146. Top 25 families in Turkey in 2H09

Rank	Family	Most Significant Category	Infected Computers
1	Win32/Taterf	Worms	315,863
2	Win32/Frethog	Password Stealers & Monitoring Tools	193,200
3	Win32/Renos	Trojan Downloaders & Droppers	49,302
4	Win32/Bredolab	Trojan Downloaders & Droppers	47,902
5	Win32/Cutwail	Trojan Downloaders & Droppers	33,058
6	Win32/Conficker	Worms	31,843
7	Win32/Parite	Viruses	30,162
8	Win32/Brontok	Worms	28,751
9	Win32/PlayMP3z	Adware	26,983
10	Win32/Jeefo	Viruses	24,740
11	Win32/Rustock	Backdoors	24,398
12	Win32/Zlob	Trojan Downloaders & Droppers	22,723
13	Win32/C2Lop	Miscellaneous Trojans	21,768
14	Win32/DoubleD	Adware	18,230
15	Win32/Alureon	Miscellaneous Trojans	16,839
16	Win32/PossibleHostsFileHijack	Misc. Potentially Unwanted Software	15,985
17	Win32/WhenU	Adware	14,522
18	Win32/Agent	Miscellaneous Trojans	13,467
19	Win32/Daurso	Password Stealers & Monitoring Tools	13,206
20	Win32/FakeRean	Miscellaneous Trojans	12,473
21	Win32/IRCbot	Backdoors	10,285
22	Win32/RJump	Worms	10,121
23	Win32/Small	Trojan Downloaders & Droppers	9,864
24	Win32/PerfectKeylogger	Misc. Potentially Unwanted Software	9,754
25	Win32/Hamweq	Worms	9,168

Encyclopedia

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

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

http://www.microsoft.com/av

Notes and observations:

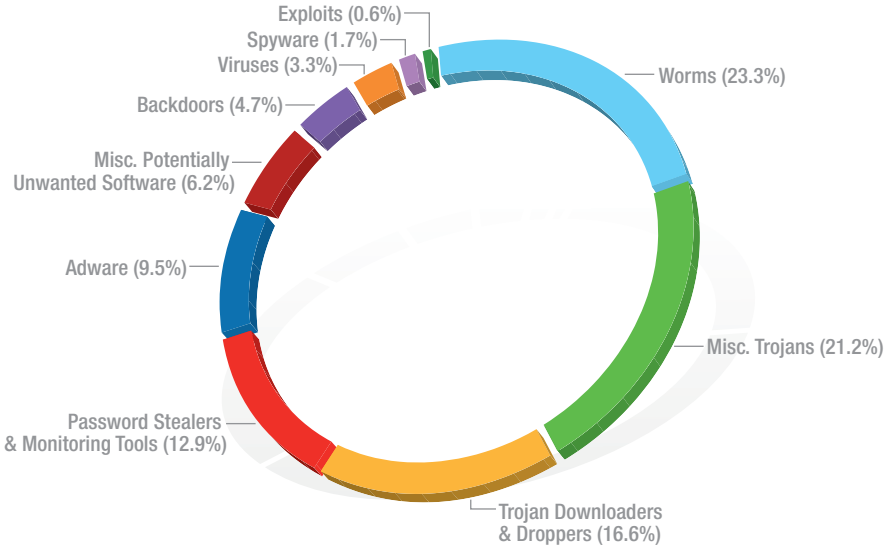
- Game password stealers were very common in Turkey during 2H09. Win32/Taterf and Win32/Frethog ranked first and second in Turkey respectively; worldwide, Win32/Taterf ranked first and Win32/Frethog ranked sixth.
- Win32/Bredolab was much more prevalent in Turkey during 2H09 than it was worldwide. Win32/Bredolab, a trojan that downloads and executes arbitrary code from a remote server, was the fourth-most prevalent family in Turkey in 2H09, but it was the twenty-fourth-most common family detected worldwide during the same period.
- Win32/Cutwail was more prevalent in Turkey in 2H09 than it was worldwide. Win32/Cutwail was the fifth-most common family detected in Turkey, but it was not present in the list of top 25 families detected worldwide. Win32/Cutwail is a trojan that downloads and executes arbitrary files. Downloaded files may be executed from a disk or injected directly into other processes. While the functionality of the files that are downloaded is variable, Win32/Cutwail usually downloads a trojan that is able to send spam. Win32/Cutwail also employs a rootkit and other defensive techniques to avoid detection and removal.
- Win32/Parite was also more prevalent in Turkey during 2H09 than it was worldwide. Win32/Parite was the seventh-most common family detected in Turkey in 2H09, but it was not present in the list of top 25 families detected worldwide in the same period. Win32/Parite is a family of polymorphic file infectors that targets computers running Windows. The virus infects .exe and .scr executable files on the local file system and on writeable network shares. In turn, the infected executable files perform operations that cause other .exe and .scr files to become infected.

United Arab Emirates

The MSRT detected malware on 5.8 out of every 1,000 computers scanned in the United Arab Emirates during 2H09 (a CCM score of 5.8—down from 6.2 in 1H09 and lower than the average worldwide CCM of 7.0). Figure 147 and Figure 148 list the malware and potentially unwanted software categories and families detected by all Microsoft desktop anti-malware products in the United Arab Emirates in 2H09.

FIGURE 147. Malware and potentially unwanted software in the United Arab Emirates, by category, in 2H09

Category	Infected Computers
Worms	17,669
Miscellaneous Trojans	16,131
Trojan Downloaders & Droppers	12,594
Password Stealers & Monitoring Tools	9,808
Adware	7,234
Misc. Potentially Unwanted Software	4,678
Backdoors	3,590
Viruses	2,495
Spyware	1,273
Exploits	482



Notes and observations:

- The threat landscape in the United Arab Emirates was dominated by malware, which accounted for 82.6 percent of all threats detected on infected computers in 2H09.
- The most common category in the United Arab Emirates was Worms, which accounted for 23.3 percent of all infected computers.
- The second-most common category in the United Arab Emirates was Miscellaneous Trojans, which includes all trojan families that are not classified as downloaders/droppers or backdoors, and accounted for 21.2 percent of all infected computers.
- Together, Miscellaneous Trojans and Trojan Downloaders & Droppers made up more than 37 percent of all families detected on infected computers in the United Arab Emirates in 2H09.

FIGURE 148. Top 25 families in the United Arab Emirates in 2H09

Rank	Family	Most Significant Category	Infected Computers
1	Win32/Renos	Trojan Downloaders & Droppers	8,595
2	Win32/Taterf	Worms	7,303
3	Win32/C2Lop	Miscellaneous Trojans	4,029
4	Win32/Conficker	Worms	3,871
5	Win32/Hamweq	Worms	3,647
6	Win32/Bancos	Password Stealers & Monitoring Tools	3,467
7	Win32/Frethog	Password Stealers & Monitoring Tools	3,348
8	Win32/Alureon	Miscellaneous Trojans	2,545
9	Win32/FakeXPA	Miscellaneous Trojans	2,148
10	Win32/Agent	Miscellaneous Trojans	2,047
11	Win32/SeekmoSearchAssistant	Adware	1,862
12	Win32/Hotbar	Adware	1,685
13	Win32/Ardamax	Trojan Downloaders & Droppers	1,538
14	Win32/Koobface	Worms	1,500
15	Win32/ZangoSearchAssistant	Adware	1,497
16	Win32/Yektel	Miscellaneous Trojans	1,476
17	Win32/Autorun	Worms	1,329
18	Win32/Zlob	Trojan Downloaders & Droppers	1,272
19	Wi32/IRCbot	Backdoors	1,087
20	Win32/Brontok	Worms	939
21	Win32/VB	Miscellaneous Trojans	919
22	Win32/GameVance	Adware	910
23	Win32/ZangoShoppingreports	Adware	876
24	Win32/DoubleD	Adware	779
25	Win32/Vundo	Miscellaneous Trojans	755

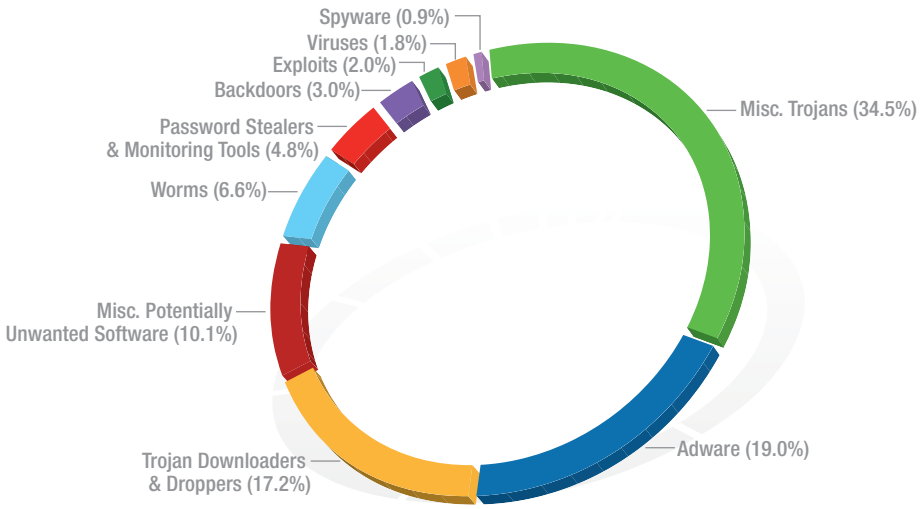
Notes and observations:

- Three of the top five families detected on infected computers in the United Arab Emirates in 2H09 (and 6 of the top 20 families) were worms. These worm families can spread via mapped drives with missing or weak passwords or via USB drives.
- Win32/C2Lop was significantly more prevalent in the United Arab Emirates than it was worldwide. Win32/C2Lop, a trojan that modifies Web browser settings and delivers contextual and pop-up advertisements, was the third-most prevalent family in the United Arab Emirates during 2H09, but it was only twenty-third-most prevalent worldwide. Win32/C2Lop may be distributed in a software package called "MessengerPlus!", an add-on for Windows Live Messenger.
- Win32/SeekmoSearchAssistant was the eleventh-most detected family on computers in the United Arab Emirates in 2H09, but it was not present in the top 25 families detected worldwide. This family displays targeted search results and pop-up advertisements based on terms that the user enters for Web searches. The pop-up advertisements may include adult content. The software may also add its own browser toolbar. The software may install BHOs for monitoring Web search terms and implementing the browser toolbar, may send event logs and other system-related information to a server, and may automatically download and install updates without notifying the user.
- Win32/Ardamax, the thirteenth-most prevalent family detected in the United Arab Emirates in 2H09, does not appear in the top 25 families detected worldwide. Win32/Ardamax is a key-logger program that can capture user activity and save it to a text or HTML file. Win32/Ardamax can be configured to send these files via e-mail to a predefined address.

United Kingdom

The MSRT detected malware on 4.1 out of every 1,000 computers scanned in the United Kingdom during 2H09 (a CCM score of 4.1—down from 4.9 in 1H09 and lower than the average worldwide CCM of 7.0). Figure 149 and Figure 150 list the malware and potentially unwanted software categories and families detected by all Microsoft desktop anti-malware products in the United Kingdom in 2H09.

FIGURE 149. Malware and potentially unwanted software in the United Kingdom, by category, in 2H09



Category	Infected Computers
Miscellaneous Trojans	898,869
Adware	495,268
Trojan Downloaders & Droppers	448,691
Misc. Potentially Unwanted Software	263,314
Worms	171,659
Password Stealers & Monitoring Tools	124,281
Backdoors	78,334
Exploits	53,234
Viruses	47,357
Spyware	23,572

Notes and observations:

- The threat landscape in the United Kingdom was dominated by malware, which accounted for 69.9 percent of all threats detected on infected computers in 2H09, up from 67.1 percent in 1H09.
- The most common category in the United Kingdom was Miscellaneous Trojans, which includes all trojan families that are not classified as downloaders/droppers or backdoors. It accounted for 34.5 percent of all infected computers, up slightly from 33.7 percent in 1H09.
- The second-most common category in the United Kingdom was Adware, which accounted for 19.0 percent of all infected computers, down from 21.1 percent in 1H09.
- Together, Miscellaneous Trojans and Trojan Downloaders & Droppers made up more than 51 percent of all families detected on infected computers in the United Kingdom in 2H09.

FIGURE 150. Top 25 families in the United Kingdom in 2H09

Rank	Family	Most Significant Category	Infected Computers
1	Win32/Renos	Trojan Downloaders & Droppers	245,921
2	Win32/Hotbar	Adware	228,801
3	Win32/FakeXPA	Miscellaneous Trojans	202,921
4	Win32/ZangoSearchAssistant	Adware	184,099
5	Win32/Alureon	Miscellaneous Trojans	176,183
6	Win32/Yektel	Miscellaneous Trojans	117,561
7	Win32/Agent	Miscellaneous Trojans	94,528
8	Win32/ZangoShoppingreports	Adware	86,080
9	ASX/Wimad	Trojan Downloaders & Droppers	77,959
10	Win32/FakeSpypro	Miscellaneous Trojans	74,098
11	Win32/Winwebsec	Miscellaneous Trojans	73,974
12	Win32/DoubleD	Adware	60,517
13	Win32/Conficker	Worms	57,133
14	Win32/C2Lop	Miscellaneous Trojans	54,777
15	Win32/Koobface	Worms	45,817
16	Win32/Liften	Miscellaneous Trojans	44,472
17	Win32/SeekmoSearchAssistant	Adware	41,472
18	Win32/Vundo	Miscellaneous Trojans	39,727
19	Win32/FakeVimes	Trojan Downloaders & Droppers	35,450
20	Win32/FakeRean	Miscellaneous Trojans	34,167
21	Win32/PlayMP3z	Adware	33,339
22	Win32/InternetAntivirus	Miscellaneous Trojans	31,985
23	Win32/Bancos	Password Stealers & Monitoring Tools	31,020
24	Win32/Taterf	Worms	29,619
25	Win32/Zlob	Trojan Downloaders & Droppers	28,883

Encyclopedia

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

Win32/Yektel: A family of trojans that display fake warnings of spyware or malware in an attempt to lure the user into installing or paying money to register rogue security software programs such as Win32/FakeXPA.

Win32/Winwebsec: A rogue security software family distributed under the names Winweb Security, System Security, and others.

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

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

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

Win32/InternetAntivirus: A rogue security software family distributed under the names Internet Antivirus Pro, General Antivirus, and others.

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

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

http://www.microsoft.com/av

Notes and observations:

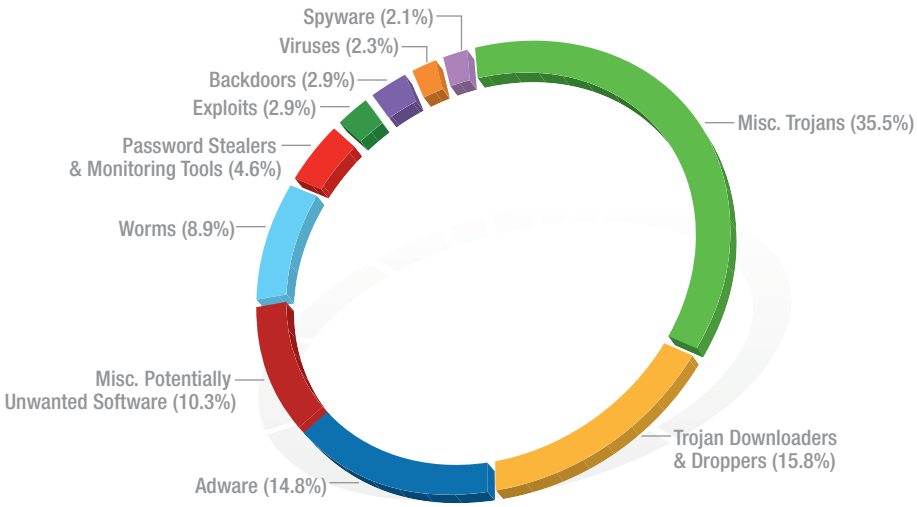
- Seven of the top 25 families in the United Kingdom in 2H09 (Win32/FakeXPA, Win32/Yektel, Win32/Winwebsec, Win32/FakeSpypro, Win32/FakeVimes, Win32/FakeRean, and Win32/InternetAntivirus) were rogue security software programs. Five of these programs were in the top 25 for the United Kingdom in 1H09, with Win32/FakeSpypro and Win32/FakeVimes joining for 2H09.
- Win32/Hotbar was significantly more prevalent in the United Kingdom during 2H09 than it was worldwide. Win32/Hotbar was the second-most prevalent family in the United Kingdom, but it ranked only tenth worldwide. Win32/Hotbar displays a dynamic toolbar and targeted pop-up ads based on its monitoring of Web-browsing activity. The toolbar appears in Internet Explorer and Windows Explorer. The toolbar contains buttons that can change depending on the current Web page and keywords on the page. Clicking a button on the toolbar may open an advertiser Web site or paid search site. Hotbar also installs graphical skins for Internet Explorer, Microsoft Office Outlook®, and Outlook Express. Hotbar may collect user-related information and may silently download and run updates or other code from its servers.
- Win32/Liften was significantly more prevalent in the United Kingdom in 2H09. Win32/Liften was the sixteenth-most prevalent family in the United Kingdom, but it did not appear in the top 25 list worldwide. Win32/Liften is a trojan that stops affected users from downloading security updates. It is downloaded by Win32/FakeXPA, a family of rogue security software programs that was the third-most common family detected in the United Kingdom in 2H09.
- Game password stealers were not as common in the United Kingdom during 2H09 as they were worldwide. Win32/Taterf and Win32/Frethog ranked first and sixth in the world respectively; in the United Kingdom, Win32/Taterf ranked only twenty-fourth and Win32/Frethog did not appear in the top 25 families at all.

United States

The MSRT detected malware on 7.8 out of every 1,000 computers scanned in the United States during 2H09 (a CCM score of 7.8—down from 8.6 in 1H09 but slightly higher than the average worldwide CCM of 7.0). Figure 151 and Figure 152 list the malware and potentially unwanted software categories and families detected by all Microsoft desktop anti-malware products in the United States in 2H09.

FIGURE 151. Malware and potentially unwanted software in the United States, by category, in 2H09

Category	Infected Computers
Miscellaneous Trojans	7,742,149
Trojan Downloaders & Droppers	3,433,563
Adware	3,221,862
Misc. Potentially Unwanted Software	2,244,669
Worms	1,936,394
Password Stealers & Monitoring Tools	993,067
Exploits	632,543
Backdoors	623,454
Viruses	491,209
Spyware	464,055



Notes and observations:

- The threat landscape in the United States was dominated by malware, which accounted for 72.9 percent of all threats detected on infected computers in 2H09, down slightly from 73.3 percent in 1H09.
- The most common category in the United States was Miscellaneous Trojans, which includes all trojan families that are not classified as downloaders/droppers or backdoors, and accounted for 35.5 percent of all infected computers. This is up from 33.1 percent in 1H09.
- The second-most common category was Trojan Downloaders & Droppers, which accounted for 15.8 percent of all infected computers. This is down from 18.9 percent in 1H09.
- Together, Miscellaneous Trojans and Trojan Downloaders & Droppers made up more than 51 percent of all families detected on infected computers in the United States in 2H09.

FIGURE 152. Top 25 families in the United States in 2H09

Rank	Family	Most Significant Category	Infected Computers
1	Win32/FakeXPA	Miscellaneous Trojans	2,282,663
2	Win32/Renos	Trojan Downloaders & Droppers	1,833,624
3	Win32/GameVance	Adware	1,525,763
4	Win32/Alureon	Miscellaneous Trojans	1,440,326
5	Win32/Yektel	Miscellaneous Trojans	993,230
6	Win32/FakeSpypro	Miscellaneous Trojans	977,247
7	Win32/Hotbar	Adware	716,676
8	Win32/Agent	Miscellaneous Trojans	669,886
9	Win32/Winwebsec	Miscellaneous Trojans	660,565
10	ASX/Wimad	Miscellaneous Trojans	659,503
11	Win32/ZangoSearchAssistant	Adware	622,185
12	Win32/Taterf	Worms	518,323
13	Win32/Koobface	Worms	514,909
14	Win32/Vundo	Miscellaneous Trojans	489,891
15	Win32/Conficker	Worms	412,573
16	Win32/FakeVimes	Trojan Downloaders & Droppers	411,225
17	Win32/FakeRean	Miscellaneous Trojans	348,729
18	Win32/ShopAtHome	Spyware	348,211
19	Win32/Liften	Miscellaneous Trojans	341,745
20	Win32/ZangoShoppingreports	Adware	291,804
21	Win32/Pdfjsc	Adware	283,600
22	Win32/PossibleHostsFileHijack	Misc. Potentially Unwanted Software	271,840
23	Win32/Frethog	Password Stealers & Monitoring Tools	252,893
24	Win32/Hamweq	Worms	250,724
25	Win32/Zwangi	Misc. Potentially Unwanted Software	237,575

Notes and observations:

- Six of the top 25 families in the United States in 2H09 (Win32/FakeXPA, Win32/Yektel, Win32/FakeSpypro, Win32/Winwebsec, Win32/FakeVimes, and Win32/FakeRean) were rogue security software programs. Three of these families appear in the top 10 families detected in the United States during 2H09.
- Game password stealers were not as common in the United States during 2H09 as they were worldwide. Win32/Taterf and Win32/Frethog ranked first and sixth in the world respectively; in the United States, Win32/Taterf ranked only twelfth and Win32/Frethog ranked twenty-third.
- Win32/ShopAtHome was the eighteenth-most prevalent family detected in the United States in 2H09, but it did not appear in the top 25 list worldwide. Win32/ShopAtHome is a Web browser redirector that monitors users' Web browsing behavior and online purchases. ShopAtHome, also known as GoldenRetriever and SelectRebates, claims to track points for users' ShopAtHome rebates when they buy products directly from affiliated merchant Web sites without linking through the ShopAtHome Web site.
- Win32/Pdfjsc, which was not among the top 25 families detected worldwide, ranked twenty-first in the United States. Win32/Pdfjsc is a family of specially crafted Portable Document Format (PDF) files that exploit vulnerabilities in versions of Adobe Acrobat and Adobe Reader. The files contain malicious JavaScript that executes when opened with a vulnerable program.
- Win32/Liften was more prevalent in the United States in 2H09 than it was worldwide. Win32/Liften was the nineteenth-most prevalent family in the United States, but it did not appear in the top 25 list worldwide. Win32/Liften is a trojan that stops affected users from downloading security updates. It is downloaded by Win32/FakeXPA, a family of rogue security software programs that was the most commonly detected family in the United States in 2H09.

Encyclopedia

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

Win32/Yektel: A family of trojans that display fake warnings of spyware or malware in an attempt to lure the user into installing or paying money to register rogue security software programs such as Win32/FakeXPA.

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

Win32/Winwebsec: A rogue security software family distributed under the names Winweb Security, System Security, and others.

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

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

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

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

http://www.microsoft.com/av

Mitigation Strategies for Protecting Networks, Systems, and People

Addressing the threats and risks documented in this report requires a concerted effort on the part of people, organizations, and governments around the world. This section presents a number of suggestions for preventing harmful actions from malware, breaches, and other security threats and for detecting and mitigating problems when they occur.

"Practicing What We Preach" is a special message from Microsoft Chief Information Security Officer Bret Arsenault about the practices and policies Microsoft uses internally to protect our people and systems from security threats. Microsoft hopes that readers will benefit from learning about the information security approaches that Microsoft IT has developed.

"Protecting Your Organization" offers guidance for IT administrators in small, medium-sized, and large companies seeking to improve their security practices and to stay up to date on the latest developments.

For software developers, "Protecting Your Software" offers information about developing secure software, including in-house software, and securing Internet-facing systems from attack.

"Protecting Your People" offers guidance for promoting awareness of security threats and safe Internet usage habits within an organization.

Practicing What We Preach

As the Chief Information Security Officer (CISO) for Microsoft, I am responsible for information security risk management for our business. Microsoft IT serves 900,000 devices for 160,000 end users across more than 100 countries worldwide, with approximately 2 million remote connections per month. My team is responsible for the end-to-end governance, compliance, policy, and practice of information security, as well as enterprise business continuity. We partner closely with the Online Services Division Security team, Physical Security, and the Trustworthy Computing (TwC) organization.

As a core contributor to the technology industry, working for Microsoft gives me a unique perspective on the technology stack that we cover, ranging from enterprise solutions and cloud computing to mobile and consumer offerings. Being part of Microsoft IT (MSIT) brings us the added responsibility of being the first to adopt these technologies to ensure that we deliver high-quality products to our end customers while maintaining an acceptable risk posture.

In the information security arena, conversations often involve how to achieve the balance between the needs of the business and the security controls. There are certainly significant pressures on both sides of the equation. The business end wants to accelerate growth and empower the user through developments like mobile devices, connectivity anywhere and at any time, and social networking. On the security end, on the other hand, we have regulatory requirements, cost pressures, and proliferation of data to contend with, among other requirements. The need to balance this equation has traditionally forced security teams to engage with the business in binary terms, with "security" defined as either allowing or disallowing certain business practices in the name of risk and compliance. I share the view that we need to elevate this balance equation by transforming our dialogue from this binary perspective to one that focuses on *how* we can accelerate the needs of the business while improving our security posture. We use the *Security Intelligence Report* to look at trends and guidance as an input that we can map to our risk management program to evaluate priorities, performance, and resource allocations.

TwC has asked us to share some of the controls we have implemented to help us manage our risk—a practitioners' perspective on the *Security Intelligence Report*, if you will. Throughout this section, we offer several examples of steps that we have taken to implement the principles and guidance presented here. These examples, presented in *italic type*, are intended to illustrate how a working department translates ideas and concepts into practical solutions in ways that are compatible with basic business needs.

Bret Arsenault
Chief Information Security Officer
Microsoft Information Security & Risk Management

Protecting Your Organization

Your network provides the underlying infrastructure where your applications are deployed. It is important to secure your network as a vital component of your defense-in-depth strategy.

- Always run up-to-date software from all of your software vendors. System administrators can use Windows Server Update Services (WSUS) or the Microsoft System Center family of management products to review and programmatically apply updates to their managed computers. In addition, a subscription to Microsoft TechNet gives IT professionals a complete set of Microsoft updates on CD or DVD. Individuals and organizations who don't have access to these resources should configure all of their computers to receive the latest Microsoft service packs and security updates automatically from an available update service:
  - **Windows Update** (http://windowsupdate.microsoft.com) provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft anti-malware products and the monthly release of the MSRT. To help secure users against exploitation, Microsoft also uses Windows Update to distribute *kill bits* that prevent certain vulnerable add-ons from running in Internet Explorer.[28] By default, when the user enables automatic updating, the update client connects to the Windows Update service for updates.
  - **Microsoft Update** (http://update.microsoft.com/microsoftupdate) provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software serviced through Microsoft Update or at the Microsoft Update Web site. Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.
  - *The data center update process at Microsoft is based on a release cycle managed by the Microsoft Security Response Center (MSRC). The Data Center Services team is responsible for ensuring that all production servers within the service boundary can be updated by the System Center Configuration Manager (SCCM) platform. Accountability for asset compliance resides with the server/service owners. Compliance reporting accountability lies with Information Security.*

    Each MSRC security update is evaluated by the Information Security and Risk Management team (IS&RM) for applicability within the Microsoft corporate environment. The Microsoft IT environment consists of multiple hierarchies, including

[28] See http://support.microsoft.com/kb/240797 for more information about kill bits. Although Microsoft does not currently provide third-party, non-driver software updates directly through its update services, the Microsoft Vulnerability Research (MSVR) program does notify vendors of potential vulnerabilities in their respective products and assists in the determination of next steps and servicing.

desktop clients, product test labs, pilot clients, and production servers. The update process begins with the Security Test Pass (STP), the process that IS&RM uses to coordinate validation of prerelease update packages throughout the IT environment to ensure quality and compatibility. These prerelease update packages are deployed on a matrix of 50 servers within the Microsoft environment, tested, and then reviewed and approved by the program manager (PM) prior to implementation. The Security Test Pass PM verifies that the update has successfully passed STP and is ready for deployment by completing the "Production Update Sign Off" document for each STP release. The test pass can occur as early as three weeks prior to the official update release date to ensure that the update is validated before being released to customers and partners.

All security updates are deployed according to IS&RM's enforcement schedule. This process ensures that updates are appropriately deployed according to criticality and rating. Once an update has been successfully built, tested, and approved, the security update management team usually releases the update to the public on the second Tuesday of the month.

After the update is released to the public, IS&RM applies the update ratings and schedules the deadline for deploying the update to Microsoft internal assets. All system updates are deployed within 26–33 days to MSIT's production data centers, unless extensions are approved. Following update evaluation, the update is deployed to each server automatically by SCCM or manually by the individual or group that manages the server. By the final week, if the update has not been installed on a particular server, SCCM will deploy a forced remediation patch.

To learn more about how Microsoft IT does update management, see "Securing the Microsoft Environment Using Desktop Patch Management" on the Microsoft TechNet Web site.

- Whichever update server you choose, check it periodically to ensure updates are being installed correctly. This is especially critical after a major malware outbreak or after installing a new operating system on the computer.
- Read *The Microsoft Security Update Guide*, available from the Microsoft Download Center, to better understand the Microsoft security update process and terminology.
- Any software installed on your computers might require periodic updates for security and stability. Ensure that all third-party applications are being updated regularly by the vendor. Check vendors' Web sites periodically to determine whether any new updates have been released.
- Obtain security updates and service packs from vendors directly from the vendors' Web sites and not from peer-to-peer (P2P) sharing, where the update could be modified with malware and redistributed.

- Use the Microsoft Security Assessment Tool (MSAT) (http://technet.microsoft.com/security/cc185712.aspx) to help identify risks in your IT security environment and build a plan to successfully manage the risk.
- Ensure that Group Policy and other settings for your computers and applications strike the right balance between security, functionality, and convenience for your organization. Consider testing your applications with exploit mitigation technologies like DEP and SEHOP enabled in a testing environment to determine the feasibility of enabling them enterprise-wide. (See "Mitigating Exploits with Windows Security Improvements," on page 43, for more information about these and other exploit mitigation technologies.)
- Consider adopting a programmatic approach towards addressing the issues and attack vectors uncovered in this report. Consider using standards, or methodologies such as:
  - ISO/IEC 27000.
  - Control Objectives for Information and Related Technology (COBIT).
  - Payment Card Industry Security Standards Council (PCI SSC).
  - The Microsoft Security Risk Management Guide (http://technet.microsoft.com/library/cc163143.aspx).
  - The Security Compliance Toolkit Series (http://technet.microsoft.com/library/cc677002.aspx).
- Develop a plan to dictate how the IT department should respond to reports of malware attacks or other threats. Appropriate responses might include executing your organization's incident response action plan or contacting local or national law enforcement officials or Computer Emergency Response Teams (CERTs).
  - *Microsoft IT has developed a preventative approach to managing computer vulnerabilities. Designed to reduce the occurrences and severity of attacks, Microsoft IT's security methodology includes the development of processes to reduce open ports and vulnerable systems and services, manage user permissions, regularly assess risks, and regularly monitor compliance with security guidelines. Download "Incident Response—Managing Security at Microsoft" from the Microsoft Download Center to learn more.*
- Consider joining one of the many industry security associations to stay informed.
  - Forum of Incident Response and Security Teams (FIRST) (http://www.first.org)
  - Information Systems Security Association (ISSA) (http://www.issa.org)
  - Information Systems Audit and Control Association (ISACA) (http://www.isaca.org)

- Information Security Forum (ISF) (https://www.securityforum.org)
- International Information Systems Security Certification Consortium, Inc. (http://www.isc2.org)
- International Information Integrity Institute (I4) (https://i4online.com)

- Stay up to date on the Microsoft security world by using the Trustworthy Computing blog aggregator at http://www.microsoft.com/twc/blogs.
- Subscribe to the Microsoft Security Newsletter at http://www.microsoft.com/technet/security/secnews/default.mspx for news, tips, and other guidance aimed at a technical audience.

Protecting Against Malicious and Potentially Unwanted Software

- Install a comprehensive, real-time anti-malware product from a reputable vendor on all of your organization's computers, and ensure that they receive frequent, regular definition or signature file updates.
- Be cautious with software that is not digitally signed by its vendor. Although signed code is not always safe, signed code is still much safer than unsigned code in general. In the second half of 2009, about 98.7 percent of all unique detected threat files were not signed, and most of the threats that were signed had severity ratings of Medium or Low.
- Take advantage of the enhanced security features in Windows Vista and Windows 7:
  - Use the AppLocker™ feature in Windows 7, which uses digitally signed code from the vendor to prevent programs from installing or executing on managed desktops.
  - Enable User Account Control (UAC) to help ensure that any malware that attempts to infect the computer is not capable of elevating its privilege level higher than that of a standard user. UAC has been revised in Windows 7 to give users and IT administrators more control over the notifications it provides. For more information, see Microsoft Knowledge Base article 969417.
  - Enable Data Execution Prevention (DEP), which can help prevent a common class of exploits called *buffer overflows*. (See Microsoft Knowledge Base article 875352 for a detailed description of the DEP feature.)
  - Enable Structured Exception Handling Overwrite Protection (SEHOP) in compatible versions of Windows, which is designed to block exploits that use the Structured Exception Handler (SEH) overwrite technique. (See Microsoft Knowledge Base article 956607 for additional information about the SEHOP feature.)

- Tools can make it easier to enable and manage several of these features. You can enable DEP or SEHOP using the Enhanced Mitigation Evaluation Toolkit (EMET) (http://go.microsoft.com/fwlink/?LinkId=162309). You can enable DEP for Office applications using the FixIt4Me tool (http://support.microsoft.com/kb/971766).
- Consider deploying the 64-bit editions of Windows client and server operating systems to take advantage of features like Kernel Patch Protection (KPP).

See "Mitigating Exploits with Windows Security Improvements," on page 43, for more information about several of these technologies.

- Use software restriction policies to identify the programs running on computers in your domains and to control the ability of those programs to execute. For more information, see "Using Software Restriction Policies to Protect Against Unauthorized Software" on the Microsoft TechNet Web site.
- Consider disabling Autorun functionality in your environment to decrease the risk it presents. See Microsoft Knowledge Base article 967715 for more information.
- Uninstall unused software to reduce your attack surface. Attackers can exploit vulnerabilities in software, whether it is used or not.
- Users running Windows XP or other versions of Windows without UAC should operate as standard users rather than as administrators, if feasible.
- If you are using Office 2003 or the 2007 Microsoft Office release, use the Microsoft Office Isolated Conversion Environment (MOICE) when opening files from unknown or untrusted sources. For more information on MOICE, see article 935865 in the Microsoft Knowledge Base.
- Install the Office Document Open Confirmation Tool, available from the Microsoft Download Center, on client computers to prevent Office documents from opening automatically from Internet Explorer.

Protecting Enterprise Networks

- Use technologies like Microsoft Network Access Protection (NAP) to prevent compromised or poorly configured computers from connecting to your network.
  - *Microsoft IT uses Network Access Protection to ensure the health of computers in two scenarios—within the enterprise and for remote access. The Microsoft intranet includes a community of managed computers that uses Microsoft Domain Isolation IP Security (IPsec) technology and NAP. Machines accessing the intranet remotely use NAP for both Virtual Private Network (VPN) and Microsoft DirectAccess, which establishes bidirectional connectivity with the intranet every time a remote user's DirectAccess–enabled computer connects to the Internet. In January 2010, 359,771 computers were evaluated and silently auto-remediated when necessary by*

the NAP Windows System Health Agent (SHA), a client component that maintains and reports one or more aspects of system health. Of that total, there were 36,147 remote machines in NAP Full Enforcement mode, in which computers that are not in compliance are isolated from the network. The agent checks to see that anti-malware and antispyware programs are installed, signatures are up to date, and real-time monitoring is enabled; that the computer is configured to receive security updates; and that the Windows Update Agent service is enabled. If the Windows Firewall is disabled, the agent enables it and forces it to remain enabled while the computer is connected to the network. In addition, because approximately one-third of the enterprise's domain-joined laptops are regularly taken out of the intranet environment and connected to the public Internet, auto-remediation ensures that important and critical updates are installed. For more information, see "Managing Network Access Protection at Microsoft" at Microsoft TechNet.

Promote Safe Browsing

- Install Internet Explorer 8 to take advantage of a number of features that can help you reduce browser-based risk, including:[29]
  - **SmartScreen Filter**: Helps protect against phishing Web sites, other deceptive sites, and sites known to distribute malware. The filter provides another layer of security and makes it less likely something will compromise the network or systems on the network—reducing the likelihood IT will have to take drastic action. It makes it hard for users to miss the indicator that a site is dangerous and allows the IT department, through Group Policy, to restrict access if a site is determined to be unsafe. The malware-blocking feature saves IT personnel time by reducing the amount of effort they have to spend disinfecting desktop systems.
  - **Cross-Site Scripting (XSS) Filter**: Provides visibility into all requests and responses flowing through the browser. When the filter discovers likely XSS in a request, it identifies and neutralizes the attack if it is replayed in the server's response. The XSS filter is able to better protect users from Web site vulnerabilities without asking questions they are unable to answer or harming functionality on the Web site.
  - **Safer ActiveX control and management**: Allows for greater management of ActiveX controls, such as where and how they can load, specifies which sites can use the control, and which users can load them. Internet Explorer 8 also allows the administrator to help set up the ActiveX control installation process for future ActiveX controls.
- Enable the Phishing Filter for any computers using Internet Explorer 7.

[29] For a more in-depth look at these security features, see "Windows Internet Explorer 8 Technology Overview for Enterprise and IT Pros," a white paper available from the Microsoft Download Center.

- Determine what security controls your search engine provider has implemented to help reduce the threat posed to your users by drive-by download attacks.
- Ensure that Protected Mode is enabled in Internet Explorer 7 and Internet Explorer 8 for Windows Vista and Windows 7. Protected Mode significantly reduces the ability of an attack to write, alter, or destroy data on the user's machine or to install malicious code.
- Ensure that DEP and SEHOP are enabled for Internet Explorer, if available.
- Use Group Policy to enforce the use of the SmartScreen Filter across your organization. A new Group Policy option is available that allows domain administrators to block users from overriding SmartScreen Filter warnings. When Group Policy restrictions are enabled, the option to override the SmartScreen warning screen is removed from the blocking pages and download dialog.
- Use the Internet Explorer Add-on Manager to control which add-ons are allowed to run in the browser.

Guard Against E-Mail Threats

- Use an e-mail authentication system to identify mail and help reduce domain spoofing. Popular approaches include Sender ID (http://www.microsoft.com/mscorp/safety/technologies/senderid/resources.mspx), DomainKeys Identified Mail (http://www.dkim.org), and the Sender Policy Framework (http://www.openspf.org).
- Maintain a strong e-mail scanning presence at the edge of the logical network perimeter.
  - *Microsoft IT's messaging protection challenges are similar to those of other enterprise environments. Like most IT organizations, Microsoft IT faces an ever-escalating stream of spam, viruses, and unwanted message submission attempts to mailboxes, contacts, distribution groups, and public folders. These attacks waste resources, distract recipients, put assets at risk, and provide an avenue for social hacking and phishing scams, among other security issues. In addition to these common threats, Microsoft IT sees advanced attacks that exploit messaging systems, involving spyware, worms, botnets, and polymorphic malware.*

    Inbound mail to Microsoft goes through a three-tiered cleansing process—anti-malware scanning, file removal, and spam filtering. In keeping with Microsoft IT's goal of stopping harmful messages at the earliest possible point, Microsoft IT has deployed Forefront Security for Exchange Server on all mail servers, which uses five different

anti-malware engines to provide protection for incoming and outgoing e-mail. On average, Microsoft filters between 5 and 10 million e-mail messages a day that contain malware or spam and removes more than 100 different types of executable files from incoming messages.

For more information, see "Messaging Hygiene at Microsoft: How Microsoft IT Defends Against Spam, Viruses, and E-Mail Attacks" at Microsoft TechNet.

- Insist that your mail servers use both inbound and outbound authentication controls to protect your brand from being harmed by attackers (a tactic called *reputation hijacking* or *brandjacking*) and to keep your customers safe from e-mail spoofing.
- Use a mail client that actively blocks active content and the automatic opening of attachments. Current versions of Microsoft Outlook, Hotmail®, Outlook Express, and Windows Live Mail, in conjunction with the security zone settings in Internet Explorer 8, can help deter IFrame attacks and prevent the unintentional opening of executable attachments.
- The Messaging Anti-Abuse Working Group (http://www.maawg.org/) recommends the following set of e-mail transmission best practices for Internet and e-mail service providers:[30]
  - Provide e-mail submission services on port 587, as described in RFC 2476.
  - Require SMTP authentication for e-mail submissions, as described in RFC 2554.
  - Abstain from interfering with connectivity to port 587.
  - Configure e-mail client software to use port 587 and authentication for e-mail submission.
  - Block access to port 25 from all hosts on your network other than those you explicitly authorize to perform SMTP relay functions.
- Monitor outbound e-mail traffic patterns and look for deviations from normal behavior, such as abnormally large bursts of e-mail traffic.
- Disable computers or individual e-mail accounts that have been compromised and are being used to send out spam.
- When possible, process abuse complaints from third parties for e-mail that originated from your mail servers. These complaints often point the way to a compromised computer.

[30] Messaging Anti-Abuse Working Group, "Managing Port 25 for Residential or Dynamic IP Space: Benefits of Adoption and Risks of Inaction" (http://www.maawg.org/sites/maawg/files/news/MAAWG_Port25rec0511.pdf).

Prevent and Mitigate Security Breaches

- Encrypt data on all computers and storage devices, including removable storage devices and drives.
- The Windows Security Compliance Toolkit (http://go.microsoft.com/fwlink/?LinkId=160808) contains step-by-step guidance for deploying BitLocker Drive Encryption and the Encrypting File System (EFS) in enterprise environments.
- Use the Data Encryption Toolkit for Mobile PCs (http://technet.microsoft.com/library/cc500474.aspx) to effectively implement BitLocker and EFS for mobile PCs.
- Be aware of the details of breach notification laws in all regions in which you conduct business. Work closely with your general counsel to follow the proper procedure in the event of a security breach. National and local laws vary considerably.
- Consider using Object access auditing for items associated with the administrator accounts so that actions can be monitored.
- Enforce the use of strong passwords throughout your organization.
- Enforce the idea of least privilege, wherein computer accounts are given only those permissions required to perform a job function (http://technet.microsoft.com/library/cc700846.aspx).
- Coordinate your IT security plan with your physical security plan to help control access to data centers or other high risk areas.
- Understand and prioritize critical assets with business unit managers to ensure proper coverage of the correct assets, including identification and classification of data.
- Ensure that an incident response plan is in place and that exercises are conducted regularly so that the staff is able to react quickly and without confusion in a crisis.
  - Develop and implement plans to reduce the likelihood of common types of breaches to mitigate their impact should they occur and to respond if the mitigations are not fully effective.
  - Perform small-scale drills (like conference room role-playing scenarios) frequently, and use them to identify areas for future emphasis.

  See "Responding to IT Security Incidents" on the Microsoft TechNet Web site for additional ideas.
- Do not use Social Security numbers for authentication purposes or as identifiers for employee or customer data. (See http://www.microsoft.com/industry/government/federal/protectinginformation.mspx for additional tips for protecting PII.)

Protecting Your Software

Computer crime poses a significant threat to every organization, large or small. It is therefore critical that software developers embed security and privacy into their software development processes. Benefits can include reducing risk and improving trust by developing software that is inherently more secure, protecting sensitive information, and reducing the total cost of development by finding and eliminating vulnerabilities early in the development process.

- Ensure that your development team is using the Security Development Lifecycle (SDL) (http://www.microsoft.com/sdl) or a similar software security assurance process. Using such a methodology can help reduce vulnerabilities in the software and help manage vulnerabilities that might be found after deployment.
- Software vendors should scan all their binary files and installation packages for malware and then digitally sign them.
  - *The Microsoft Product Release & Security Services (PRSS) Anti-malware Scanning Service is chartered, through corporate compliance policy, with ensuring that all Microsoft products are malware-free during the product release life cycle. The Scanning Service's charter is met by using an automated system that provides a comprehensive, dynamic, and easy-to-use process that implements the latest decompression algorithms combined with numerous state-of-the-art malware scanning tools. As part of the Scanning Service's priorities, the occurrence of false positives at the time of release is mitigated through the Scanning Service's collaboration with the anti-malware industry.*
- Security software vendors should participate in the Microsoft Active Protections Program (MAPP) (http://www.microsoft.com/security/msrc/collaboration/mapp.aspx). Members of MAPP receive security vulnerability information from the Microsoft Security Response Center in advance of the Microsoft monthly security update.

Securing ActiveX Controls

- Application vendors that have security issues with an ActiveX control that they own can request that Microsoft issue a kill bit to prevent their ActiveX control from running in Internet Explorer. Approved requests are processed in a future Update Rollup for ActiveX Kill Bits Security Advisory. Microsoft issues a kill bit only for ActiveX controls that are found to have a vulnerability and only if the owning independent software vendor (ISV) has already produced an updated version of their ActiveX control. ISVs that have vulnerable ActiveX controls can e-mail requests to msvr@microsoft.com, together with answers to the following questions:
  - What is the public URL for the updated ActiveX control?
  - What is the CLSID of the requested ActiveX control to receive a kill bit within Internet Explorer?

- Has this updated ActiveX control received a new CLSID that sets a kill bit to the vulnerable CLSID in the process?
- Is the requested ActiveX control marked as safe-for-scripting or safe-for-initialization?
- Are there older versions of the requested ActiveX control? If the answer is "Yes," what are their CLSIDs?
- What is the primary delivery mechanism to consumers for the requested ActiveX control?
- What is the public URL for the ISV Advisory that discloses the vulnerability?

For help with this process, see article 240797 in the Microsoft Knowledge Base.

- Have your internal development teams use the SiteLock Template for ActiveX Controls technology, available from the Microsoft Download Center, for custom controls that are designed for use only on your internal Web sites. Locking a control to a particular domain makes it harder for other sites to repurpose the control in a malicious manner.

Guarding Against SQL Injection

- Understand how SQL injection works and how to guard against it. SQL injection attacks can potentially affect any ANSI-99–compliant database, regardless of platform or vendor, unless you take steps to validate all your input and wrap or disallow potentially dangerous strings. See "SQL Injection" in *Microsoft SQL Server 2008 Books Online* (http://msdn.microsoft.com/library/ms161953.aspx) for more information and prevention tips.

Protecting Your People

With close to 90,000 employees across 99 sites worldwide, information security awareness and training are critical at Microsoft, as they are for any organization's information security strategy and supporting security operations.

People are, in many cases, an organization's last line of defense against threats such as malicious code, disgruntled employees, and malicious third parties. It is, therefore, important to educate workers on what your organization considers appropriate security-conscious behavior and on the security best practices they need to incorporate in their daily business activities.

Transform your security message from "no" to "how." Demonstrate to your organization how *to be secure rather than telling them what they can or cannot do. Some ideas:*

- *Use innovative media, like podcasts, comics, and challenges, to "socialize" your security messaging.*
- *Create focused, scalable, and prescriptive guidance (for example, "How-Do-I" podcast modules).*
- *Mandate security training for engineers. Microsoft has used the SDL successfully to build products that are both productive and secure, and offers extensive guidance on the SDL principles and guidance at http://www.microsoft.com/sdl.*
- *Use tools and templates like the Microsoft security awareness program tool kit and guide (http://technet.microsoft.com/security/cc165442.aspx) and Microsoft IT's Work Smart Productivity Guides (http://technet.microsoft.com/library/bb687781.aspx) to educate your people about secure practices.*
- Drive security awareness, and stay informed. Teach users to be aware of the threat landscape around them.
  - Users who think they may have been a victim of an attack, or who suspect something unusual on your network, should immediately contact the IT department for assistance.
  - Teach users about the importance of using strong passwords for all of their online accounts, and on your network, and of keeping passwords and personal identification numbers (PINs) secret.
  - Educate users not to click links or call phone numbers from e-mails received from financial institutions, but to instead call the numbers that they have on file. Remind them that financial institutions typically print customer service phone numbers on the backs of credit cards and bank statements, and it is those numbers that users should call.
  - Inform users that malware can be transmitted through instant messages on both computers and mobile devices.

- Users should only open e-mail attachments that they are expecting to receive. When in doubt, users should contact the person who sent the file and confirm that the attachment was intentional and non-malicious.
- Users should install and use an e-mail client that actively blocks active content and the automatic opening of attachments.

- Users often share files between their home and business computers. Protect your whole ecosystem by ensuring that users' home computers are secure.
  - A number of enterprise antivirus providers offer licensing arrangements that allow employers to distribute antivirus software to their employees for home use. Consider taking advantage of one of these arrangements. In addition, several security vendors offer basic real-time protection products at no charge to home computer users.
  - Educate users about the benefits of keeping their computers up to date with Windows Update and Microsoft Update, and the importance of running the monthly release of the Malicious Software Removal Tool (MSRT) to check their computers for specific, prevalent malware threats.
  - Users who think their computers are infected should run the Windows Live OneCare safety scanner (http://safety.live.com) or make a free call (in North America) to 1-866-PC-SAFETY.
- Microsoft provides a number of resources you can share with your users to help keep them safe, including:
  - Microsoft at Work: 10 ways to work more securely (http://microsoft.com/atwork/security/worksecure.aspx)
  - Microsoft at Work: 9 ways to increase the security of your laptop while on the road (http://microsoft.com/atwork/security/laptopsecurity.aspx)
  - Microsoft Online Safety (http://www.microsoft.com/protect)

Afterword

Microsoft Malware Protection Center Executive Afterword

I hope that you have found the information in this eighth volume of the *Microsoft Security Intelligence Report* (SIRv8) enlightening and informative. This volume of the *SIR* is the largest and most comprehensive intelligence document Microsoft has published to date, and I expect you will find information that will help you make better and more informed decisions for securing your organizations' networks.

The Internet today is a sea of opportunity that holds remarkable value, but at times it can be a stormy place to surf. To weather the storm, it's essential to be protected from potential harm. We created the *SIR* to help you protect your assets, which has been our goal since its inception.

In Volume 2 (July through December 2006) of the SIR, we predicted that social media and online games would become major threats in the future. In Volume 5 (January through June 2008) of the SIR, we discussed at length (see page 62) how online games and social media will be used to propagate worms. As we publish this eighth version of the SIR, we see two malware families that have continued to cause active attack storms on the Internet. Although they may have diminished in overall volume, both Win32/Taterf and Win32/Frethog (worms and password stealers that spread using online games) continue to top our malicious software list.

Some storm-clearing can be seen in countries such as Turkey, which still shows high infection rates but has authorities and local service providers looking to mitigate malware such as Win32/Taterf and Win32/Frethog. But it's clear that malware will continue to evolve and target areas that provide reliable payoffs for malware creators. I suspect that online games and social media will continue to be highly sought-after targets.

Speaking of payoffs, we also see that rogue security software continues to pay off for the attackers who create it. However, the only payoff for people who are victimized by those who create rogue security software is potential pain. Users are being scared into believing that their computers are infected with malware and that using rogue security software will provide protection—but rogue security software only deepens the infection.

To help better educate people about rogue security software, the Microsoft Malware Protection Center (MMPC) developed three new consumer-oriented educational videos. These videos are available at http://www.microsoft.com/protect.

In this volume of the *SIR*, we have also expanded our threat assessment for individual countries/regions. The newly expanded "Malware Patterns Around the World" section provides data for 213 locations around the world and delivers deep dive information and observations for a total of 26 countries/regions, which is by far the largest collection of malware information we have ever published. We introduced the concept of deep dives in Volume 5 and, over the years, have received numerous requests to provide additional coverage. The MMPC worked hard to ensure that this section is extensive and provides

considerable detail for each country/region. We have also made the information available on our Web site, which allows you to display the information in a simple and intuitive navigation tool. You can check out the tool at http://www.microsoft.com/sir.

Volume 7 (January through June 2009) of the *SIR* mentioned we would see data from Microsoft Security Essentials that would provide us with a better understanding of malware patterns. We have seen encouraging adoption rates for Microsoft Security Essentials on a global basis. This is a big win against malware and is a great move in providing a safer security ecosystem for everyone. Microsoft Security Essentials will continue to evolve and extend our ability to protect those who use it. When we reviewed the telemetry data in the second half of 2009, we found that more than 7.8 million computers infected with rogue security software were cleaned by Microsoft security products. That's up from 5.3 million computers in the first half of 2009—an increase of 46.5 percent.

Having a solid defense against malware requires installing good anti-malware solutions, ensuring that your operating systems are upgraded and kept up to date, and making certain that all of the applications installed on your systems are also kept up to date—keeping current is essential. In this volume of the *Security Intelligence Report*, we see that application exploits pose very significant risks for computers. Keeping applications patched and current is a critical part of defending your networks against malware storms. The telemetry data has proven consistently that the lowest infection rates are seen on computers running Windows Vista SP2 and Windows 7. The infection rates for both operating systems are less than half the infection rate for computers running Windows XP.

Finally, in this volume we introduced a section called "Mitigation Strategies for Protecting Networks, Systems, and People." We created this section in response to customer requests, and we focused a considerable amount of effort in developing its content. Bret Arsenault, Microsoft Chief Information Security Officer, provides great insight on how Microsoft implements security.

I want to thank you for taking the time to read this eighth volume of the *Security Intelligence Report*. We are always seeking to improve the report—your experience with it and any feedback you provide will help us tremendously. Please take a few minutes to send us a note at sirfb@microsoft.com. We take all comments seriously, and we want to do all we can to ensure that our next report will help you better navigate safe passage through malware storms and will be an even more compelling read.

Vinny Gullotto
General Manager, Microsoft Malware Protection Center
Microsoft Corporation

Appendixes

Appendix A: Threat Naming Conventions

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

A threat name can contain some or all of the components seen in Figure 153.

FIGURE 153. The Microsoft malware naming convention

The *type* indicates the primary function or intent of the threat. The MMPC assigns each individual threat to one of a few dozen different types based on a number of factors, including how the threat spreads and what it is designed to do. To simplify the presentation of this information and make it easier to understand, the *Security Intelligence Report* groups these types into 10 categories. For example, the TrojanDownloader and TrojanDropper types are combined into a single category, called Trojan Downloaders & Droppers.

The *platform* indicates the operating environment in which the threat is designed to run and spread. For most of the threats described in this report, the platform is listed as "Win32," for the Win32 API used by 32-bit and 64-bit versions of Windows desktop and server operating systems. (Not all Win32 threats can run on every version of Windows, however.) Platforms can include programming languages and file formats, in addition to operating systems. For example, threats in the ASX/Wimad family are designed for programs that parse the Advanced Stream Redirector (ASX) file format, regardless of operating system.

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

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

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

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

Appendix B: Data Sources

Microsoft Products and Services

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

- Bing, the search and decision engine from Microsoft, contains technology that performs billions of Web-page scans per year to seek out malicious content. Once detected, Bing displays warnings to users about the malicious content to help prevent infection.
- Windows Live Hotmail has hundreds of millions of active e-mail users in more than 30 countries/regions around the world. Every incoming e-mail message is scanned by Microsoft antivirus technology to help protect users from infection.
- Forefront Online Protection for Exchange protects the networks of thousands of enterprise customers worldwide by helping to prevent malware from spreading through e-mail. FOPE scans billions of e-mail messages every year to identify and block spam and malware.
- Windows Defender is a program, available at no cost to licensed users of Windows, that provides real-time protection against pop-ups, slow performance, and security threats caused by spyware and other potentially unwanted software. Windows Defender runs on more than 100 million computers worldwide.
- The Malicious Software Removal Tool (MSRT) is a free tool designed to help identify and remove prevalent malware families from customer computers. The MSRT is primarily released as an important update through Windows Update, Microsoft Update, and Automatic Updates. A version of the tool is also available from the Microsoft Download Center. The MSRT was downloaded and executed 2.9 billion times in 2H09, or nearly 485 million times each month on average. The MSRT is not a replacement for an up-to-date antivirus solution because of its lack of real-time protection and because it uses only the portion of the Microsoft antivirus signature database that enables it to target specifically selected, prevalent malicious software.
- Microsoft Forefront Client Security is a unified product that provides malware and potentially unwanted software protection for enterprise desktops, laptops, and server operating systems. Like Windows Live OneCare, it uses the Microsoft Malware Protection Engine and the Microsoft antivirus signature database to provide real-time, scheduled, and on-demand protection.
- Windows Live OneCare is a real-time protection product that combines an antivirus and antispyware scanner with phishing and firewall protection. Microsoft has discontinued retail sales of Windows Live OneCare, but continues to make definition updates available to registered users.

- The Windows Live OneCare safety scanner (http://safety.live.com) is a free, online tool that detects and removes malware and potentially unwanted software using the same definition database as the Microsoft desktop anti-malware products. The Windows Live OneCare safety scanner is not a replacement for an up-to-date antivirus solution, because it does not offer real-time protection and cannot prevent a user's computer from becoming infected.
- Microsoft Security Essentials is a basic, consumer-oriented anti-malware product, offered at no charge to licensed users of Windows, which provides real-time protection against viruses, spyware, and other harmful software.
- The Phishing Filter (in Internet Explorer 7) and the SmartScreen Filter (in Internet Explorer 8) offer Internet Explorer users protection against phishing sites and sites that host malware. Microsoft maintains a database of phishing and malware sites reported by users of Internet Explorer and other Microsoft products and services. When a user attempts to visit a site in the database with the filter enabled, Internet Explorer displays a warning and blocks navigation to the page.

The following table summarizes the main security products available from Microsoft.

Product Name	Main Customer Segment		Malicious Software		Spyware and Potentially Unwanted Software		Available at No Additional Charge	Main Distribution Methods
	Consumer	Business	Scan and Remove	Real-Time Protection	Scan and Remove	Real-Time Protection		
Microsoft Forefront Server Security		•	•	•	•	•		Volume Licensing
Microsoft Forefront Client Security		•	•	•	•	•		Volume Licensing
Windows Live OneCare Safety Scanner	•		•		•		•	Web
Microsoft Security Essentials	•		•	•	•	•	•	Download Center
Windows Malicious Software Removal Tool	•		Prevalent Malware Families				•	Windows Updates/ Automatic Updates Download Center
Windows Defender	•				•	•	•	Download Center Windows Vista Windows 7
Microsoft Forefront Online Protection for Exchange		•	•	•				Volume Licensing

Glossary

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

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

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

bot-herder
An operator of a botnet.

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

browser modifier
A program that changes browser settings, such as the home page, without adequate consent. This also includes browser hijackers.

CCM
Short for *computers cleaned per mille* (thousand). The number of computers cleaned for every 1,000 executions of the MSRT. For example, if the MSRT has 50,000 executions in a particular location in January and removes infections from 200 computers, the CCM for that location in January is 4.0 (200 ÷ 50,000 × 1,000). The CCM for a multiple-month period is derived by averaging the CCM for each month in the period.

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

command and control
See *botnet*.

cross-site scripting
Abbreviated *XSS*. An attack technique wherein an attacker inserts malicious HTML and JavaScript into a vulnerable Web page, often in an effort to distribute malware or to steal sensitive information from the Web site or its visitors. Despite the name, cross-site scripting does not necessarily involve multiple Web sites. *Persistent cross-site scripting* involves inserting malicious code into a database used by a Web application, potentially causing the code to be displayed for large numbers of visitors.

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

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

downloader/dropper
See *trojan downloader/dropper*.

exploit
Malicious code that takes advantage of software vulnerabilities to infect a computer.

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

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

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

keylogger
See *password stealer (PWS)*.

Malicious Software Removal Tool

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

malware

Malicious software or potentially unwanted software installed without adequate user consent.

malware impression

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

monitoring tool

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

parser vulnerability

A vulnerability in the way an application processes, or parses, a file of a particular format, which can be exploited through the use of a specially crafted file. Also see *vulnerability*.

password stealer (PWS)

Malware that is specifically used to transmit personal information, such as user names and passwords. A PWS often works in conjunction with a *keylogger*, which sends keystrokes or screen shots to an attacker. Also see *monitoring tool*.

payload

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

persistent cross-site scripting

See *cross-site scripting*.

phishing

A method of identity theft that tricks Internet users into revealing personal or financial information online. Phishers use phony Web sites or deceptive e-mail messages that mimic trusted businesses and brands to steal personally identifiable information (PII), such as user names, passwords, credit card numbers, and identification numbers.

phishing impression
A single instance of a user attempting to visit a known phishing page with Internet Explorer 7 or Internet Explorer 8 and being blocked by the Phishing Filter or SmartScreen Filter. Also see *malware impression*.

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

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

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

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

Sender ID Framework
An Internet Engineering Task Force (IETF) protocol developed to authenticate e-mail to detect spoofing and forged e-mail with the typical tactic to drive users to phishing Web sites and to download malicious software.

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

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

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

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

tool
Software that may have legitimate purposes but may also be used by malware authors or attackers.

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

trojan downloader/dropper
A form of trojan that installs other malicious files to the infected system either by downloading them from a remote computer or by dropping them directly from a copy contained in its own code.

virus
Malware that replicates, commonly by infecting other files in the system, thus allowing the execution of the malware code and its propagation when those files are activated.

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

vulnerability broker
A company or other entity that provides software vendors with vulnerability information provided to it by external security researchers. In exchange for such compensation as the broker may provide, the security researchers agree not to disclose any information about the vulnerability to anyone other than the broker and the affected vendor.

wild
See *in the wild*.

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

XSS
See *cross-site scripting*.

Threat Families Referenced in This Report

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

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

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

Win32/Autorun: A worm that attempts to spread by being copied into all removable drives.

Win32/Bagle: A worm that spreads by e-mailing itself to addresses found on an infected computer. Some variants also spread through P2P networks. Bagle acts as a backdoor trojan and can be used to distribute other malicious software.

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

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

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

Win32/Bredolab: A downloader that can access and execute arbitrary files from a remote host. Bredolab has been observed to download several other malware families to infected computers.

Win32/Ceekat: A collection of trojans that steal information such as passwords for online games, usually by reading information directly from running processes in memory. Different variants target different processes.

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

Win32/Corripio: A generic detection for a large number of different trojans that attempt to steal passwords for popular online games but are otherwise behaviorally dissimilar.

Win32/FakeBye: A rogue security software family that uses a Korean-language user interface.

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

Win32/FakeSmoke: A rogue security software family distributed under the name Win-BlueSoft and others.

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

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

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

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

Win32/GameVance: Software that displays advertisements and tracks anonymous usage information in exchange for a free online gaming experience at the Web address "gamevance.com."

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

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

Win32/InternetAntivirus: A rogue security software family distributed under the names Internet Antivirus Pro, General Antivirus, and others.

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

Win32/Koobface: A multi-component family of malware used to compromise computers and use them to perform various malicious tasks. It spreads through the internal messaging systems of popular social networking sites.

Win32/Lethic: A trojan that connects to remote servers, which may lead to unauthorized access to an affected system.

Win32/Lolyda: A family of trojans that sends account information from popular online games to a remote server. They may also download and execute arbitrary files.

Win32/MoneyTree: A family of software that provides the ability to search for adult content on the local computer. It may also install other potentially unwanted software, such as programs that display pop-up ads.

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

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

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

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

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

Win32/RJump: A worm that attempts to spread by copying itself to newly attached media, such as USB memory devices or network drives. It also contains backdoor functionality that allows an attacker unauthorized access to an affected machine.

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

Win32/SeekmoSearchAssistant: Adware that displays targeted search results and pop-up advertisements based on terms that the user enters for Web searches. The pop-up advertisements may include adult content.

Win32/ShopAtHome: A browser redirector that monitors Web-browsing behavior and online purchases. It claims to track points for ShopAtHome rebates when the user buys products directly from affiliated merchant Web sites.

Win32/Swif: A trojan that exploits a vulnerability in Adobe Flash Player to download malicious files. Adobe has published security bulletin APSB08-11 addressing the vulnerability.

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

Win32/Tikayb: A trojan that attempts to establish a secure network connection to various Web sites without the user's consent.

Win32/Ursnif: A family of trojans that steals sensitive information from an affected computer.

Win32/Virut: A family of file-infecting viruses that target and infect .exe and .scr files accessed on infected systems. Win32/Virut also opens a backdoor by connecting to an IRC server.

ASX/Wimad: A detection for malicious Windows Media files that can be used to encourage users to download and execute arbitrary files on an affected machine.

Win32/Wintrim: A family of trojans that display pop-up advertisements depending on the user's keywords and browsing history. Its variants can monitor the user's activities, download applications, and send system information back to a remote server.

Win32/Winwebsec: A rogue security software family distributed under the names Winweb Security, System Security, and others.

Win32/Yektel: A family of trojans that display fake warnings of spyware or malware in an attempt to lure the user into installing or paying money to register rogue security software programs such as Win32/FakeXPA.

Win32/ZangoSearchAssistant: Adware that monitors the user's Web-browsing activity and displays pop-up advertisements related to the Internet sites the user is viewing.

Win32/Zlob: A family of trojans that often pose as downloadable media codecs. When installed, Win32/Zlob displays frequent pop-up advertisements for rogue security software.

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