Microsoft Security Intelligence Report

Volume 7
January through June 2009

Microsoft®

Microsoft Security Intelligence Report

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

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

Authors

Richard Boscovich
Microsoft Internet Safety and Enforcement Team

T J Campana
Microsoft Internet Safety and Enforcement Team

Darren Canavor
Microsoft Security Engineering Center

Bruce Dang
Microsoft Security Engineering Center

Joe Faulhaber
Microsoft Malware Protection Center

Vinny Gullotto
Microsoft Malware Protection Center

Yuhui Huang
Microsoft Malware Protection Center

Jeff Jones
Microsoft Trustworthy Computing

John Lambert
Microsoft Security Engineering Center

Tony Lee
Microsoft Malware Protection Center

Ziv Mador
Microsoft Malware Protection Center

Ritesh Mordani
Microsoft Forefront Online Protection for Exchange

Bala Neerumalla
Microsoft Secure SQL Initiative Team

Jonathan Ness
Microsoft Security Engineering Center

Hamish O'Dea
Microsoft Malware Protection Center

Sasi Parthasarathy
Bing

Anthony Penta
Microsoft Windows Safety Platform

Paul Pottorff
Windows Consumer Product Management

Sterling Reasor
Microsoft Malware Protection Center

Christian Seifert
Bing

Adam Shostack
Microsoft Security Engineering Center

George Stathakopoulos
Microsoft Security Response Center

Adrian Stone
Microsoft Security Response Center

Scott Wu
Microsoft Malware Protection Center

Terry Zink
Microsoft Forefront Online Protection for Exchange

Contributors

Fred Aaron
Microsoft Security Engineering Center

Charles Anthe
Online Management Platform & Solutions

Kai Axford
Microsoft Trustworthy Computing

Doug Cavit
Microsoft Trustworthy Computing

Nicola Cowie
Microsoft Security Engineering Center

Dave Forstrom
Microsoft Trustworthy Computing

Heather Goudey
Microsoft Malware Protection Center

Michael Grady
Microsoft Trustworthy Computing

Roger Grimes
Microsoft IT Information Security

Satomi Hayakawa
Japan Security Response Team

Sue Hotelling
Microsoft Internet Safety and Enforcement Team

Aaron Hulett
Microsoft Malware Protection Center

Japan Security Response Team
Microsoft Japan

Jeannette Jarvis
Microsoft Customer Support Services

Jimmy Kuo
Microsoft Malware Protection Center

Kathy Lambert
Microsoft Legal and Corporate Affairs

Jimin Li
Online Management Platform & Solutions

Ken Malcolmson
Microsoft Trustworthy Computing

Scott Molenkamp
Microsoft Malware Protection Center

Patrick Nolan
Microsoft Malware Protection Center

Price Oden
Microsoft IT Information Security

Ina Ragragio
Microsoft Malware Protection Center

Tim Rains
Microsoft Trustworthy Computing

Mike Reavey
Microsoft Security Response Center

Marc Seinfeld
Microsoft Malware Protection Center

Jinwook Shin
Microsoft Security Engineering Center

Sam Salhi
Microsoft Windows Safety Platform

Matt Thomlinson
Microsoft Security Engineering Center

Alan Wallace
Microsoft Trustworthy Computing

Jeff Williams
Microsoft Malware Protection Center

External Contributors

Andre DiMino
Shadowserver Foundation

Paul Henry
Technical Writer

Hans-Peter Jedlicka
Federal Office for Information Safety, Germany

Leon Aaron Kaplan
National Computer Emergency Response Team of Austria

Huopio Kauto
Computer Emergency Response Team Communications Regulatory Authority, Finland

Hideaki Kobayashi
Information-Technology Promotion Agency, Japan

Toshiaki Kokado
Information-Technology Promotion Agency, Japan

Erka Koivunen
Computer Emergency Response Team Communications Regulatory Authority, Finland

Richard Perlotto
Shadowserver Foundation

Torsten Voss
DFN-CERT, Germany

Table of Contents

Microsoft Security Engineering Center

Microsoft Security Response Center

Afterword

Appendixes

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 seventh 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 *Security Intelligence Report* focuses on the first half of 2009 (1H09), 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), while 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 "Threat Naming Conventions," beginning on page 36.

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 C* of the report.

Key Findings

This report provides the Microsoft perspective on the security and privacy threat landscape over the six-month period from January through June 2009. This section summarizes the key points from the main section of the report.

Malicious and Potentially Unwanted Software

- The most significant trend in 1H09 was the large increase in worm infections detected in many countries and regions worldwide.
- 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.
- In the United States, the United Kingdom, France, and Italy, trojans were the largest single category of threat; in China, several language-specific browser-based threats were prevalent; in Brazil, malware targeting online banking was widespread; and in Spain and Korea, worms dominated, led by threats targeting online gamers.

Operating System Trends

- Infection rates for Windows Vista® were significantly lower than for Windows® XP in all configurations in 1H09.
  - The infection rate of Windows Vista SP1 was 61.9 percent less than that of Windows XP SP3.
  - Comparing release-to-manufacture (RTM) versions, the infection rate of Windows Vista was 85.3 percent less than that of Windows XP.
- The infection rate of Windows Server® 2008 RTM was 56.1 percent less than that of Windows Server 2003 SP2.
- The higher the service pack level, the lower the rate of infection:
  - Service packs include all previously released 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 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.
- Server versions of Windows typically display a lower infection rate on average than client versions. Servers tend to have a lower effective attack surface than computers running client operating systems because they are more likely to be used under controlled conditions by trained administrators and to be protected by one or more layers of security.
- These trends are proving to be consistent over time.

The Threat Landscape at Home and in the Enterprise

- Computers in enterprise environments (those running Microsoft Forefront™ Client Security) were much more likely to encounter worms during 1H09 than home computers running Windows Live™ OneCare™.
- Win32/Conficker, the top threat detected in enterprise environments, was not in the top ten threats in home environments. Several Conficker variants are designed to spread via removable and network shared media, both of which are common in enterprise environments. (In April Microsoft announced security update KB971029, which makes it more difficult for Conficker and similar worms to spread in this manner.)

Worldwide Malware Category Trends

- Miscellaneous Trojans (including rogue security software) remained the most prevalent category.
- Worms rose from 5th place in 2H08 to become the second-most prevalent category in 1H09.
- The prevalence of Password Stealers & Monitoring Tools also rose, due in part to increases in malware targeting online gamers.

Analysis of Malware Hosts

- Miscellaneous Potentially Unwanted Software impressions detected by the SmartScreen Filter in Internet Explorer® 8 increased from 35.0 percent of malware impressions in 2H08 to 44.5 percent in 1H09, while the percentage of computers cleaned declined from 22.8 percent to 14.9 percent for the category. This suggests that SmartScreen and similar technologies may be successfully intercepting these threats before they are downloaded to computers.
- Miscellaneous Potentially Unwanted Software is disproportionally likely to be distributed over the Web. By contrast, worms are rarely distributed by malicious Web sites, accounting for just 1.2 percent of SmartScreen impressions, compared to 21.3 percent of computers cleaned.

Geographic Distribution of Malware Hosting Sites

- More malware distribution sites are discovered on a daily basis than phishing sites.
- Malware hosting tends to be more stable and less geographically diverse than phishing. 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.

Analysis of Phishing Sites

- Phishing impressions rose significantly in 1H09, due primarily to a large increase in phishing attacks targeting social networking sites.
- Phishers continued to target a wider range of Web-site types than in the past, with gaming sites, portals, and the online presences of major corporations being some of the most frequently targeted sites in 1H09.
- After remaining mostly consistent throughout 2H08 and through April 2009, suddenly the number of impressions nearly quadrupled in May and rose even higher in June, due in part to a campaign or campaigns targeting social networks.
- Financial institutions, social networks, and e-commerce sites remain favored targets for phishing attempts.
- Researchers also observed some diversification into other types of institutions, such as online gaming sites, Web portals, and large software and telecommunications companies.

Geographic Distribution of Phishing Sites

- Phishing sites are hosted on free hosting sites, on compromised Web servers, and in numerous other contexts.
- Phishing sites tend to be 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 46 of 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.

E-Mail Threats

- Forefront Online Protection for Exchange (FOPE) blocked 97.3 percent of all messages received at the network edge in 1H09, up from 90.0 percent in 2H08. In total, FOPE blocked more than 98 percent of all messages received.
- Spam in 1H09 was dominated by product advertisements (primarily pharmaceutical products). In total, product advertisements accounted for 69.2 percent of spam in 1H09.

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. Use of this technique was widely observed during 1H09.

- SQL injection usually involves directly passing malicious SQL code 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 commands.
- Beginning in late 2007, 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.

Exploit Trends—Browser-Based Exploits

- For browser-based attacks on Windows XP–based machines, Microsoft vulnerabilities accounted for 56.4 percent of the total. On Windows Vista–based machines, Microsoft vulnerabilities accounted for just 15.5 percent of the total.
- Microsoft software accounted for 6 of the top 10 browser-based vulnerabilities attacked on computers running Windows XP in 1H09, compared to only 1 of the top 10 on computers running Windows Vista.

Microsoft Office Format Files

- The most frequently exploited vulnerabilities in Microsoft Office software during 1H09 were also some of the oldest. More than half of the vulnerabilities exploited were first identified and addressed by Microsoft security updates in 2006.
- 71.2 percent of the attacks exploited a single vulnerability for which a security update (MS06-027) had been available for three years. Computers that had this update applied were protected from all these attacks.
- The majority of Microsoft Office attacks observed in 1H09 (55.5 percent) affected Microsoft Office program installations that had last been updated between July 2003 and June 2004. Most of these attacks affected 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.
- By contrast, the computers in the sample set were significantly more likely to have had recent Windows security updates applied.
- Users who do not keep both their Microsoft Office program installations and Windows operating systems up to date with service packs and security updates are at increased risk of attack.
- Microsoft recommends that computers be configured to use Microsoft Update to keep Windows operating systems and other Microsoft software updated.

Analysis of Drive-By Download Pages

- The majority of drive-by download pages are hosted on compromised legitimate Web sites. 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 servers acting as exploit servers can have massive reach; one exploit server can be responsible for hundreds of thousands of infected Web pages.
- Exploit servers in 2009 were able to infect many thousands of pages in a short period of time.
- The Trojan Downloaders & Droppers category was the most frequently encountered category among drive-by download sites, with 40.7 percent of the total. Trojan downloaders are well suited for delivery by drive-by download because they can be used to install other threats on infected computers.

Industry-Wide Vulnerability Disclosures

- Total unique vulnerability disclosures across the industry decreased sharply in 1H09, down 28.4 percent from 2H08.
- While application vulnerabilities are down from 2H08, operating system vulnerabilities are roughly consistent with the previous period, and browser vulnerabilities actually increased slightly.
- Vulnerabilities rated as High severity by the Common Vulnerability Scoring System CVSS decreased 12.9 percent from 2H08; 46.0 percent of all vulnerabilities were rated as High severity.
- As with severity, the complexity trend in 1H09 is a generally positive one. 54.2 percent of all vulnerabilities were Low complexity in 1H09, down from 57.7 percent in 2H08, and down almost 30 percentage points over the last five years.
- Microsoft vulnerability disclosures have mirrored those for the industry as a whole, though on a much smaller scale. Over the past five years, Microsoft vulnerability disclosures have consistently accounted for about 3–6 percent of all disclosures industry wide.

Microsoft Vulnerability Details for 1H09

- In 1H09 Microsoft released 27 security bulletins, which addressed 87 individual Common Vulnerabilities and Exposures–identified (CVE-identified) vulnerabilities.
- *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. This helps to keep users safer by preventing

potential attackers from learning about newly discovered vulnerabilities before security updates are available.

- In 1H09, 79.5 percent of disclosed vulnerabilities in Microsoft software adhered to responsible disclosure practices, up from 70.6 percent in 2H08.

Exploitability Index

- Forty-one vulnerabilities (47.1 percent) were assigned an Exploitability Index rating of 1, meaning that they were considered the most likely to be exploited within 30 days of the associated security bulletin's release. Microsoft observed ten of these vulnerabilities being exploited in the first 30 days.
- Of the 46 vulnerabilities (52.9 percent) that received Exploitability Index ratings of 2 or 3, indicating that exploitation would be unreliable or unlikely, none were identified to have been publicly exploited within 30 days.

Usage Trends for Windows Update and Microsoft Update

- The prompt adoption of security updates and other software upgrades can significantly mitigate the spread and impact of malware. Microsoft recommends that computers be configured to use Microsoft Update to keep Windows operating systems and other Microsoft software updated.
  - *Windows Update* provides updates for Windows components, and for device drivers provided by Microsoft and other hardware vendors. It also distributes signature updates for Microsoft anti-malware products, and the monthly release of the Malicious Software Removal Tool (MSRT).
  - *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 Update adoption has risen significantly over the past several years, with increasing numbers of Windows Update users choosing to switch to the more comprehensive service.

The Role of Automatic Updating

- Automatic updating is one of the most effective tools that users and organizations can utilize to help prevent the spread of malware.
- Automatic updating ensures that updates are installed, and installed quickly, to protect individual computers and the computing environment.

Regional Variations in Update Service Usage

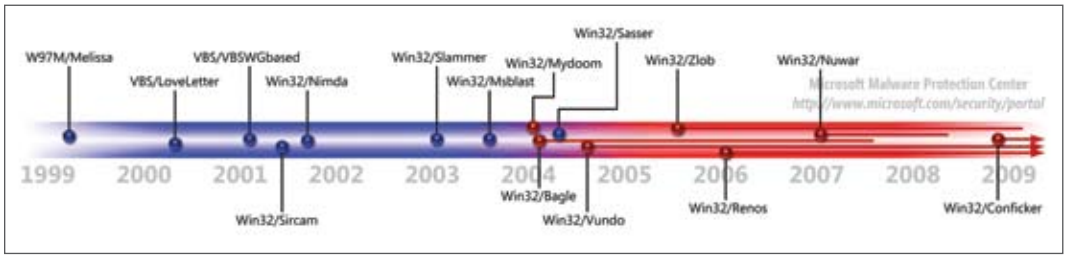
- Use of Microsoft online update services varies worldwide due to a number of factors, including broadband Internet connectivity, software piracy, and the percentage of computers managed in enterprise environments.
- The incidence of software piracy in a location tends to be negatively correlated with usage of Windows Update and Microsoft Update.

Security Breach Trends

- The top category reported for data loss through a security breach in 1H09 continued to be stolen equipment, such as laptop computers (30.0 percent of all data-loss incidents reported), accounting for twice as many incidents as intrusion.
- Security breaches from "hacking" or malware incidents remain less than 15.0 percent of the total.

Executive Foreword

Welcome to the seventh installment of Microsoft's *Security Intelligence Report*, which I hope you will find is the most extensive and comprehensive edition to date. The cover story in this report looks back at the major threats that have attacked customers over the last 10 years, and then the report drills deeply into the current threats that you need to understand and includes what you can do to best manage your risks.



At Microsoft, we remember the pain past incidents caused our customers and we reflect on them frequently. In particular, the Slammer and Blaster attacks that disrupted the Internet in 2003 are vivid reminders of the responsibility we have at Microsoft to ensure our products are as secure and privacy-enhanced as possible.

As you can see from the timeline above, 2003 and 2004 were difficult times. But, you can also see that since then, major security incidents have become less and less frequent. From the data in this report, you'll also note that the scope and impact of major events have changed, as well. For example, from the press surrounding the Conficker worm that has been attacking customers over the past year, it's easy to conclude that Conficker is just as widespread and impactful as Slammer or Blaster—but in most respects, it hasn't been. In 2003, Blaster became one of the most prevalent threats impacting home PC users. Six years later, Conficker didn't even make the Top 10 list among this audience. I don't want to minimize the pain that many of our customers experienced fighting Conficker, because, as you'll read in the report, it was the top threat detected and cleaned in enterprises in the first half of 2009, but Conficker emerged in a much different software industry than Slammer and Blaster.

Indeed, the software industry has matured a great deal since the days of Slammer and Blaster. Since 2003, the software industry has improved its ability to mobilize and coordinate resources to fight threats. Industry partnerships such as the Microsoft Security Response Alliance (MSRA)[1] didn't exist when criminals perpetrated the Slammer and Blaster attacks. These industry partnerships, along with others like the Industry Consortium for Advancement of Security on the Internet (ICASI) have all been founded since 2003 to help protect customers and assist the software industry in responding to major security events faster and more effectively -- because they allow members to share information and coordinate efforts. The Conficker Working Group (CWG) was founded earlier this year, establishing a new model for how the collective industry can work together to mitigate global threats.

The industry was able to proactively get ahead of Conficker by discovering the vulnerability before attackers could use it in widespread attacks. The Security Science team at Microsoft was able to find the MS08-067 vulnerability, which Conficker uses to propagate, and work with the Microsoft Security Response Center (MSRC) to release its update before attackers could use it for a Blaster-type attack. Our industry partners helped protect many customers from attack via the Microsoft Active Protections

[1] MSRA includes programs like the Global Infrastructure Alliance for Internet Safety (GIAIS), the Microsoft Virus Initiative (MVI), the Virus Information Alliance (VIA), the Security Cooperation Program (SCP), and the Microsoft Security Support Alliance (MSSA)

Program (MAPP). MAPP supplies Microsoft vulnerability information to security software partners prior to security update releases from Microsoft. By obtaining security-vulnerability information earlier from the MSRC, partners gain additional time to build customer software protections ahead of Microsoft's public security update release. The program serves security providers, particularly vendors of security software or devices, such as anti-virus, network-based intrusion detection and prevention systems (IDS/IPS), or host-based intrusion prevention systems (HIDS/HIPS). This program enabled the majority of MAPP partners to provide protections to their customers for Conficker 24 hours after the MS08-067 security update was released. This meant that many customers were protected up to a week earlier than traditionally possible, and certainly much earlier than customers could obtain such defense-in-depth protections and threat mitigations in 2003.

With the vulnerability that Slammer exploited, many administrators didn't know whether they needed to apply a security update or that it had to be applied manually. Today, customers are notified and protected much faster; multiple communications channels exist to help customers find and understand information on security vulnerabilities. Security advisories help draw attention to security issues as they unfold, and provide customers with critical information before security bulletins become available. Microsoft's advanced notification service provides customers with an insight into the number and nature of security updates that Microsoft will be releasing each month so they can plan more effectively for the deployment of the updates. Security bulletins provide information on vulnerabilities, along with workarounds and mitigations. As you'll read in this report, over 96 percent of all bulletins contain workarounds and/or mitigations to give customers more information, options and time to make better deployment decisions.

Keeping Microsoft software up-to-date is easier today than it was in the Slammer/Blaster era. With automatic updates for consumers and small businesses, and Windows Server Update Services and System Center Configuration Manager for enterprises, plus the availability of many third-party updating services, customers have quicker access to security information and more help deploying security updates than ever before.

If you aren't familiar with some, or any of these advancements, please review the *Microsoft Security Update Guide* that we published earlier this year. It will help you find and use all of the information, programs, tools and communications channels that Microsoft uses to help protect its customers. The guide can be found here: http://www.microsoft.com/downloads/details.aspx?familyid=C3D986D0-ECC3-4CE0-9C25-048EC5B52A4F&displaylang=en.

The progress that the software industry has made to better protect systems and customers might be small consolation to the users of those 5 million systems that were infected with Conficker in the first half of 2009. Still, it is a significant step forward, given that more than 100 times as many systems were *protected* from Conficker. This is in stark contrast to the Slammer and Blaster attacks of 2003 where many, many more systems were infected. The industry will continue to work together to make the frequency, scale and scope of emerging threats as minimal as possible.

We thank you for your help and efforts to protect the ecosystem, and look forward to continuing to work with you to create a safer, more trusted Internet.

George Stathakopoulos
General Manager, Trustworthy Computing Security
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 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 Malware Protection Center

The 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, 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.

Microsoft Security Engineering Center

The Microsoft Security Engineering Center (MSEC) helps to protect Microsoft customers by providing security guidance to Microsoft Product Groups, helping implement the industry-leading software Security Development Lifecycle (SDL), and deploying applied security science and technology that help improve future products.

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.

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.

Melissa Plus 10: Keeping People Safe in the Age of Malware

Ten Years of Malware and Security Threats, 1999–2009

This year marks the tenth anniversary of the release of W97M/Melissa, which created what many security professionals call the first truly global malware outbreak. Since then, malware and related threats have grown from a novelty to a fact of life that affects the way millions of people work and play online. To understand why this is so, it's important to consider the technological and cultural factors that came together in the final years of the twentieth century to set two powerful forces on a collision course with each other: the new revolution in communications wrought by the rise of the Internet and the age-old desire of some to gain fame and profit at the expense of others.

Desktop Computing in 1999

In retrospect, the rise of malware as a significant threat affecting computer users around the world over the last 10 years might be considered inevitable. The first decade of the twenty-first century has seen a collision between the sudden, meteoric rise of the Internet as a mainstay of modern life for millions of people and a culture of software development and use that had evolved in a time when Internet connectivity was rare—and malicious misuse of the network even rarer.

Many of the security measures computer users take for granted today were unknown or not widely deployed in early 1999. Even in the midst of the so-called "dot-com boom," less than a third of homes in North America and Europe had Internet access,[2] with broadband technologies accounting for less than 10 percent of that overall number.[3] Several different vendors produced antivirus software for personal computers but typically only issued definition updates monthly (or less often). Desktop computer operating systems, like Microsoft Windows 98 and Mac OS 8, were developed in an era before Internet access was widespread or commonplace. They did not include a number of security features considered fundamental today, like software firewalls or access control list–based (ACL-based) file system security. Windows Update, the service that allows Windows users to obtain system updates over the Internet, was in its infancy, and options for updating all the computers in an organization were limited. The lack of a facility for quickly or automatically updating large numbers of computers made it difficult or impossible to respond effectively to a threat event.

Most communication and productivity software during this time period was designed for versatility and convenience, with less attention given to security considerations. The then-current version of the Microsoft Office productivity suite was Office 97, the Standard Edition of which included versions of Microsoft Word, Microsoft Excel®, Microsoft PowerPoint®, and Microsoft Outlook®. Many people were also using Outlook 98, an upgraded version of the messaging and collaboration client offered as a no-cost download to registered users of Outlook 97. The Microsoft Visual Basic® for Applications (VBA) scripting language

[2] Organisation for Economic Co-operation and Development. *Information Technology Outlook 2008*. Paris: OECD Publication Service, 2008, p. 196.
[3] "March 2003 Bandwidth Report." WebSiteOptimization.com. http://www.websiteoptimization.com/bw/0302/

allowed extensive customization and automation of Word, Excel, and PowerPoint, but without many of the security features that VBA developers today take for granted, such as code signing.

Meanwhile, the world was undergoing an unprecedented rise in Internet connectivity that would transform life for people on every continent. The number of Internet users worldwide more than quadrupled between 2000 and 2009 to 1.7 billion people, a quarter of the Earth's population, according to one estimate.[4] At the same time, many parts of the world have shifted from dial-up Internet access at home to broadband access, meaning hundreds of millions more computers are connected to the Internet all day—and often all night, as well. Broadband penetration in the so-called G7 industrialized nations (Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States) rose by an average of more than 50 percent per year between 2001 and 2008.[5] These factors, along with a general lack of understanding of security threats on the part of the general public, combined to create a large and growing attack surface across multiple continents—perfect conditions for the rise of a new generation of malware.

Early Worms and Macro Viruses (1999–c. 2005)

In some ways, the modern era of malware began on Friday, March 26, 1999, when thousands of e-mail systems around the world were overwhelmed by a fast-spreading new threat. Designated W97M/Melissa and typically referred to in media accounts as the *Melissa virus* or *Melissa worm*, the virus caused more than U.S.$100 million in damages worldwide as part of the first truly widespread malware outbreak affecting ordinary computer users.

W97M/Melissa was an example of a *macro virus*—a class of viruses that use an application's macro language, such as the VBA scripting language in Microsoft Office applications, to distribute themselves. Macro viruses were among the first threats to spread widely on the Internet, though they have greatly diminished in prevalence over the past 10 years due to application security measures such as disabling unsigned macros by default. W97M/Melissa was not the first macro virus to spread widely. Earlier threats such as WM/Concept and W97M/Wazzu infected Word documents as early as 1995, spreading when users exchanged infected files through e-mail, by floppy disk, or on a network share. W97M/Melissa propagated much more rapidly than these earlier threats by exploiting the way Word macros could be used to automatically send e-mail messages through Outlook. W97M/Melissa was introduced to the Internet in a Word document posted to the well-trafficked Usenet newsgroup *alt.sex*, posing as a list of passwords for pornographic Web sites. When the infected document was opened in Word 97, W97M/Melissa copied itself to the Normal.dot template file that loads by default when Word is opened so that any subsequent documents created by the user would also be infected by the virus. If Outlook was installed on the computer, the virus then automatically created an infected Word

Encyclopedia

WM/Concept: The first widely known Microsoft Word macro virus, written for Word 6.0. It spreads by infecting documents and templates, including the Normal.dot template.

W97M/Wazzu: A macro virus that infects Microsoft Word documents and templates. When executed, it attempts to insert the text "wazzu" into the infected document at a random location and to relocate existing words randomly.

http://www.microsoft.com/av

[4] "World Internet Users and Population Stats." Internet World Stats. http://www.internetworldstats.com/stats.htm

[5] "Broadband penetration and density." Organisation for Economic Co-operation and Development. December 2008. http://www.oecd.org/sti/ict/broadband

document titled "Important Message From *[user name]*" and used Outlook to send the infected document to the first 50 e-mail addresses in the Outlook Address Book, with the message body "Here is that document you asked for ... don't show anyone else ;-)". Many recipients opened the messages, believing them to have been sent legitimately by friends or acquaintances—an early form of reputation hijacking. The computers of recipients who opened the attachment were themselves infected, and the cycle began again. The result was a torrent of messages that shut down enterprise e-mail systems around the world, including those of global corporations and government agencies.

Over the next few years, a number of other macro viruses caused periodic outbreaks, some even more widespread and damaging than W97M/Melissa. Most used VBA and VBScript to access the victim's Outlook Address Book and send infected files to some or all of the victim's contacts. Like W97M/Melissa, some of the most virulent threats used *social engineering*—manipulating victims through trickery—to entice recipients into opening the infected files, targeting users' motivations and desires with tactics similar to those still used by attackers today. VBS/LoveLetter, which infected millions of computers in 2000, sent messages with the subject line "ILOVEYOU". In another outbreak in 2001, a virus detected as Virus:VBS/VBSWGbased.gen used a payload disguised as a photograph of tennis star Anna Kournikova. Macro virus outbreaks declined significantly after 2001 with the widespread adoption of Office 2000 and subsequent releases, which block or disable macros that are not digitally signed by a trusted source.

Even as macro viruses were receding in prominence, a number of other widespread outbreaks were affecting computer users around the world. These were caused by worms that used e-mail and other network services to replicate and distribute copies of themselves. Some early worms, like 2001's Win32/Sircam, distributed themselves using tactics similar to those of macro viruses, by searching for e-mail addresses in the files of an infected computer and sending copies of the worm to the addresses. Others spread primarily by taking advantage of vulnerabilities in network services and Internet programs. In 2003, Win32/Slammer exploited a vulnerability in Microsoft SQL Server® and Microsoft SQL Server 2000 Desktop Engine (MSDE); Win32/Msblast, also from 2003, targeted the Distributed Component Object Model (DCOM) protocol; Win32/Sasser, from 2004, exploited a vulnerability in the Local Security Authority Subsystem Service (LSASS). Some of the most damaging threats used multiple methods for propagation. Win32/Nimda, released in 2001, spread through e-mail, by infecting application files locally and on network shares, by infecting Microsoft Word, and by exploiting a vulnerability in Microsoft Internet Explorer.

Encyclopedia

VBS/LoveLetter: A family of mass-mailing worms that targets computers running certain versions of Windows. It can spread as an e-mail attachment and through an Internet Relay Chat (IRC) channel. The worm can download, overwrite, delete, infect, and run files on the infected computer.

VBS/VBSWGbased: A generic detection for VBScript code that is known to be automatically generated by a particular malware tool.

Win32/Slammer: A memory resident worm that spreads through a vulnerability present in computers running either MSDE 2000 or SQL Server that have not applied Microsoft Security Bulletin MS02-039.

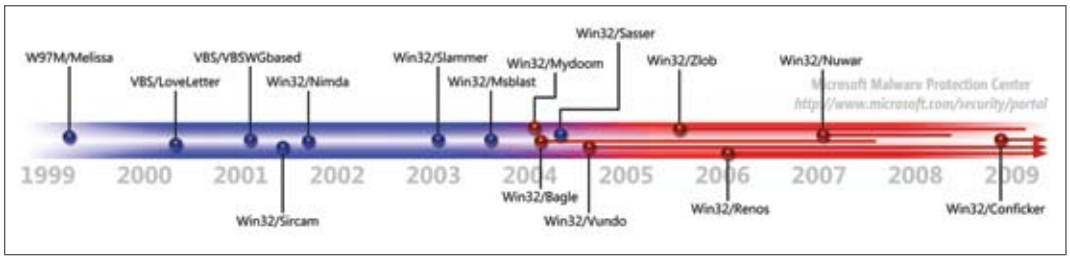
Win32/Msblast: A family of network worms that exploit a vulnerability addressed by security bulletin MS03-039. The worm may attempt Denial of Service (DoS) attacks on some server sites or create a backdoor on the infected system.

Win32/Sasser: A family of network worms that exploit a vulnerability fixed by security bulletin MS04-011. The worm spreads by randomly scanning IP addresses for vulnerable machines and infecting any that are found.

Win32/Nimda: A family of worms that spread by exploiting a vulnerability addressed by Microsoft Security Bulletin MS01-020. The worm compromises security by sharing the C drive and creating a Guest account with administrator permissions.

http://www.microsoft.com/av

FIGURE 1. Timeline of notable malware outbreaks, 1999–2009



Profit-Oriented Malware (c. 2004–Present)

While many of the early worms were extremely destructive and costly in terms of clean-up costs and lost productivity, most were created as pranks or as a means of raising the creators' status in the online "hacker" community. It wasn't long, however, before criminals seized on the opportunities malware provided for theft, blackmail, and other criminal activities. The mass-mailing worm family Win32/Mydoom, which appeared in January 2004, created one of the earliest examples of a *botnet*—a set of computers that are secretly and illicitly controlled by an attacker, who orders them to perform activities such as sending spam, hosting pages used in phishing attacks, stealing passwords or sensitive information, and distributing other malware. The computers in the Mydoom botnet were themselves used to send spam and to conduct distributed denial-of-service (DDoS) attacks.

As for-profit malware became more widespread, the number of headline-grabbing outbreaks diminished. During the heyday of the mass mailers and similar worms, tales of malware outbreaks spread beyond the technical press and achieved a very high profile in the public consciousness, garnering considerable coverage even in media outlets that usually had little or nothing to do with computers or security. For example, Win32/Msblast, also known as "Blaster," was the subject of a 10-page feature article in the January 2004 issue of the U.S. edition of *Vanity Fair*, a popular magazine that ordinarily focuses on high culture and general investigative journalism. The result of all this attention was that most of these worms had an effective lifetime of only a few days, as the highly visible nature of each threat motivated security and IT professionals to act quickly to stop its spread and contain the damage. Moreover, the creators of some of these threats were identified and caught quickly, with security professionals and law enforcement uniting to focus on a common high-priority goal. David L. Smith, the creator of W97M/Melissa, was arrested just six days after introducing the virus to the Internet, following a cooperative effort by antivirus researchers, America Online, the U.S. Federal Bureau of Investigation (FBI), and the State of New Jersey Division of Criminal Justice. To more effectively serve their creators' purposes, new threats tended not only to spread much more slowly and quietly than their predecessors but also to be consistently maintained and updated by their creators in an effort to evade detection by antivirus software.

Encyclopedia

Win32/Mydoom: A family of mass-mailing worms that spread through e-mail. Some variants also spread through P2P networks. It acts as a backdoor trojan and can sometimes be used to launch DoS attacks against specific Web sites.

http://www.microsoft.com/av

Encyclopedia

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

Win32/Vundo: A multiple-component family of programs that deliver pop-up advertisements and may download and execute arbitrary files. Vundo is often installed as a browser helper object (BHO) without a user's consent.

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/Nuwar: A family of trojan droppers that install a distributed P2P downloader trojan. This downloader trojan in turn downloads an e-mail worm component.

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

http://www.microsoft.com/av

Around the same time that Win32/Mydoom began infecting systems around the world, the first variants of a different mass mailer, Win32/Bagle, were appearing on the Internet. Though it received relatively little attention compared to the faster-spreading Win32/Mydoom, Win32/Bagle was the first threat to display many of the behaviors that have come to typify the modern, profit-oriented threat. Many Win32/Bagle variants use multiple mechanisms to avoid detection and removal, such as attempting to disable Windows Update and blocking access to the Web sites of antivirus vendors. Perhaps the biggest indicator of the professional origins of Win32/Bagle, though, was the ongoing release of a large number of variants that were designed specifically to get around mechanisms that antivirus vendors had developed to detect earlier variants—a move that touched off an "arms race" between malware creators and antivirus vendors that continues to this day.

As a result of measures like these, today's prevalent malware families tend to remain active threats for much longer periods of time than their predecessors. As recently as late 2007, Win32/Bagle was still among the top 25 threats detected around the world by the Malicious Software Removal Tool (MSRT); Win32/Vundo and Win32/Zlob, the seventh- and thirteenth-most detected malware families by Microsoft desktop security products in the first half of 2009, were first detected in 2004 and 2005, respectively. Newer families rely more heavily on social engineering than on exploiting vulnerabilities in operating systems and applications, though the exploits that do circulate tend to be more technically sophisticated and appear more quickly following the discovery of a vulnerability.

Another significant development in recent years has been the rise of an underground economy for the distribution and use of malware. Whereas early threats were usually created and released by isolated individuals or small groups, many of the threats that are prevalent today are traded in online black markets, where criminals buy or rent access to exploits, password stealers, software for sending spam, and other illicit tools. Large botnets, such as the one created by Win32/Nuwar (the "storm worm") in 2007 and 2008, are rented out to attackers who use them for activities such as spam campaigns, hosting malware servers and phishing pages, and DDoS attacks.[6] Attackers often use combinations of several different unrelated threats together, with trojan downloaders and trojan droppers, like Win32/Renos, serving as delivery mechanisms for other malware families.

[6] For a more thorough exploration of the "underground economy" of malware creation and use, see "The Threat Ecosystem," in *Microsoft Security Intelligence Report, Volume 5 (January through June 2008)*, pp. 12–23.

Computer Security Today: Working Together to Close the Gap

By early in the twenty-first century, it was clear that computer security in the Internet era would require fundamental changes, not only in the way software was architected and built but also in the way software developers, IT departments, and end users thought about security. It would no longer be adequate to think of security as a separate or isolated component of programs and processes. Security would have to become an integral part of both software and the policies governing its use, at every level. Implementing this vision would involve the creation of entirely new technical, legal, and social structures for dealing with computer security threats. These structures would be built through unprecedented cooperative effort from software vendors (including Microsoft), academia, government and law enforcement, and independent security experts.

Trustworthy Computing

On January 15, 2002, Microsoft then-chairman Bill Gates sent a memo to all full-time employees of Microsoft and its subsidiaries. As with previous company-wide memos, which had led to initiatives like the Microsoft Internet strategy and the .NET Framework, this message proposed a fundamental shift in the company's approach to a central component of its business. The topic was a concept called *Trustworthy Computing (TwC)*.

Gates wrote:

> *Computing is already an important part of many people's lives. Within ten years, it will be an integral and indispensable part of almost everything we do. Microsoft and the computer industry will only succeed in that world if CIOs, consumers and everyone else sees that Microsoft has created a platform for Trustworthy Computing.*
>
> *Every week there are reports of newly discovered security problems in all kinds of software, from individual applications and services to Windows, Linux, Unix and other platforms. We have done a great job of having teams work around the clock to deliver security fixes for any problems that arise. Our responsiveness has been unmatched—but as an industry leader we can and must do better. Our new design approaches need to dramatically reduce the number of such issues that come up in the software that Microsoft, its partners and its customers create. We need to make it automatic for customers to get the benefits of these fixes. Eventually, our software should be so fundamentally secure that customers never even worry about it.*[7]

TwC remains a central tenet underlying every aspect of business at Microsoft, guiding the company's focus on security, privacy, reliability, and positive business practices.[8]

[7] To read the full memo, visit http://www.microsoft.com/about/companyinformation/timeline/timeline/docs/bp_Trustworthy.rtf.
[8] For more information about Trustworthy Computing, visit http://www.microsoft.com/mscorp/twc.

At the heart of Microsoft's TwC security efforts is the Security Development Lifecycle, a methodology that integrates principles of security into every phase of the software development life cycle. Since 2004, use of the SDL has been a mandatory policy at Microsoft, and it has been revised and updated several times. The SDL portal, at http://www.microsoft.com/sdl, offers extensive information that software development teams everywhere can use to learn about and implement the process, including training materials, process guidance, tools and templates for Microsoft Visual Studio®, and more.

As a result of the TwC initiative and the SDL, and of similar efforts implemented by other software vendors, the computing experience is much different—and much safer—in 2009 than it was in 1999. Windows XP Service Pack 2 (SP2), released in 2004, was a major update that introduced an array of new security features, including the Windows Security Center, the improved Windows Firewall, a pop-up blocker in Internet Explorer, and a range of configuration changes to services and programs that helped to make the operating system more secure by default. Data Execution Prevention (DEP) helps prevent exploits that take advantage of buffer overflows, a common technique, when used with CPUs that support it. Windows Vista and Windows Server 2008 introduced additional security features, such as User Account Control (UAC) and Address Space Layout Randomization (ASLR) that made it more difficult for exploits to succeed.

Antivirus protection, once considered optional, is increasingly seen as a necessary precaution for Internet users. Over the last 10 years, as malware creators have developed techniques to evade detection by antivirus software, most antivirus vendors have increased the frequency with which they issue definition updates, initially from monthly to weekly, and then to daily or even more often. Microsoft began providing basic anti-malware protection in early 2005 with the Malicious Software Removal Tool, which is released monthly through Windows Update and Microsoft Update at no cost to registered users of Windows, and removes more than 100 common malware families from infected computers. Since then, Microsoft has developed and released a range of products and tools that provide basic to enterprise-level protection against malware and potentially unwanted software, including Windows Defender, Windows Live OneCare, the Microsoft Forefront line of products, and the upcoming Microsoft Security Essentials. (For more information, see "Appendix C: Data Sources," on page 223.)

Government and Law Enforcement

For their part, government and law-enforcement agencies around the world have had to devote a considerable amount of effort to build a legal infrastructure to successfully deter and respond to cybercrime. Many of the laws that are being used today against malware creators, spammers, and phishers have been written within the last 10 years, as governments around the world have worked to keep up with what are, in many cases, entirely new classes of criminal activity. For example, 18 U.S.C. 1030, the U.S. federal statute that addresses fraud and related activity in connection with computers, was amended in 2008

to specifically cover bot-herding, an activity that did not even exist a decade ago. Even understanding the details of a typical malware-related crime requires a depth of technical knowledge that traditionally has not been a part of prosecutor and law-enforcement training. Law enforcement's ability to track down and capture perpetrators is further hampered by cybercriminals' skill at covering their tracks and in cases where criminals are physically located beyond the reach of cooperating agencies.

Many countries/regions have dedicated law enforcement and investigative resources to fighting computer crime. The International Criminal Police Organization (INTERPOL) and the United Nations Office on Drugs and Crime have developed initiatives to train law-enforcement officers about cybercrime and to facilitate cooperation across borders. In the United States, several departments and agencies of the federal government have dedicated teams working on the issue, including the FBI, the U.S. Secret Service, and other groups within the Departments of Justice and Homeland Security. Law-enforcement agencies at the state and local level also often have computer crime specialists who share information and aid investigations. In the United Kingdom, the Metropolitan Police Service (Scotland Yard) in London and the Serious Organised Crimes Agency coordinate much of that country's response to cybercrime. National police forces in Germany, the Netherlands, Japan, Singapore, Australia, and many other countries/regions have computer crime units staffed by knowledgeable specialists who are able to quickly respond to new threats as they arise. The Convention on Cybercrime, a treaty drafted by the Council of Europe (CoE) in 2001 and ratified by 13 CoE member states and the United States (as of 2009), has been a significant milestone in improving cooperation, investigation, and prosecution of computer crime across national boundaries.[9]

At Microsoft, the Internet Safety Enforcement Team (ISET), part of the Legal and Corporate Affairs (LCA) department, works with these and other law-enforcement agencies around the world to track down malware creators and bring them to justice. At the same time, the team works with lawmakers to craft new legislation that addresses the unique details of computer crime and helps ensure that appropriate laws are in place to punish wrongdoers. Since its formation in 2003, ISET has supported hundreds of criminal and civil enforcement actions worldwide against spammers, phishers, and distributors of spyware and other malicious code. ISET has also engaged with the Federal Trade Commission (FTC) and attorneys general in several U.S. states to investigate and pursue cybercriminals. ISET works to ensure that governments and law-enforcement agencies receive the appropriate tools, necessary training, and extensive technical and investigative support to assist in their efforts to combat global cybercrime and work to make the Internet a safer place for everyone.

Since 2004, ISET has managed the International Botnet Task Force, a worldwide organization of computer-security professionals in industry, academia, and law enforcement. Among other accomplishments, the International Botnet Task Force has provided assis-

[9] For more information about the Convention on Cybercrime, see http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

tance to the FBI, part of the U.S. Department of Justice, in the execution of Operation Bot Roast, an FBI effort to shut down botnets and bring their operators to justice.[10]

Community-Based Defense

With so many software vendors and government agencies working on different aspects of computer crime, and given the global nature of the problem, effective communication and cooperation—among vendors, between government and industry, and across borders and jurisdictional lines—are of paramount importance in stopping threats and punishing their perpetrators. To accomplish this, software developers, government agencies, academia, and independent security researchers have come together to form collaborative groups and initiatives dedicated to fighting different aspects of the common problem.

One of the earliest examples of a comprehensive collaborative effort related to Internet security was the Computer Emergency Response Team (CERT; now called the CERT Coordination Center, or CERT-CC), founded in response to the so-called "Morris worm," which infected a large percentage of the computers on the Internet in November 1988. Headquartered at Carnegie Mellon University in Pittsburgh, Pennsylvania, CERT was created to give experts a central point for coordinating responses to network emergencies. Other teams, also called CERTs (or CSIRTs, for Computer Security Incident Response Teams), were soon formed around the world to respond to incidents involving particular organizations or geographic areas. To facilitate communication and coordination between these response teams, the Forum of Incident Response and Security Teams (FIRST) was formed in 1990. Today FIRST has almost 200 members in 45 countries/regions, representing enterprise, academia, government, and regional CERTs. In addition to threat response, CERTs often provide valuable information and assistance to others in the security community. For example, US-CERT, part of the United States federal government, sponsors the National Vulnerability Database (NVD) (http://nvd.nist.gov), a comprehensive repository of information about software vulnerabilities.

In addition to FIRST, Microsoft participates in a number of collaborative organizations and initiatives dedicated to different aspects of the overall computer security issue, including:

- **The Anti-Phishing Working Group (APWG)**, a global pan-industrial and law-enforcement association focused on eliminating the fraud and identity theft that result from phishing and related techniques. In addition to coordinating information sharing and response between partners, the APWG provides guidance to end users to help them avoid falling victim to phishing scams.
- **The Anti-Spyware Coalition (ASC)**, a group of antispyware software companies, academics, and consumer groups dedicated to building a consensus about definitions and best practices in the debate surrounding spyware and other potentially unwanted

[10] For more in-depth information about some of these legal actions and initiatives, see "Focus on Internet Safety Enforcement," in *Microsoft Security Intelligence Report, Volume 4 (July through December 2007)*, beginning on page 84, and "Legal Action Against Rogues," in *Microsoft Security Intelligence Report, Volume 6 (July through December 2008)*, beginning on page 99.

technologies. Recently, ASC co-authored a brief supporting security software vendor Kaspersky Lab in *Zango v. Kaspersky*, a landmark case heard by the U.S. Court of Appeals for the Ninth Circuit on February 2, 2009. Zango, Inc., a vendor of potentially unwanted software, accused Kaspersky of unlawfully blocking several of its programs. On June 25, 2009, the court ruled in favor of Kaspersky's right to classify software as adware and to filter or block it on that basis.

- **Digital PhishNet**, a collaborative enforcement operation to unite industry leaders in technology, banking, financial services, and online retail services with law enforcement to combat phishing.
- **The Industry Consortium for Advancement of Security on the Internet (ICASI)**, an organization formed in June 2008 by Microsoft, Cisco Systems, IBM, Intel, Juniper Networks, and Nokia. ICASI was created to give global IT vendors a secure forum for sharing sensitive information with each other to facilitate proactive responses to security threats.
- **The Messaging Anti-Abuse Working Group (MAAWG)**, a global organization focusing on preserving electronic messaging from online exploits and abuse with the goal of enhancing user trust and confidence, while ensuring the deliverability of legitimate messages. MAAWG works to address messaging abuse by focusing on technology, industry collaboration, and public policy initiatives.
- **The National Cyber Security Alliance (NCSA)**, a public-private partnership between the U.S. Department of Homeland Security (DHS), corporate sponsors, and nonprofit collaborators to promote cyber security awareness for home users, small and medium-sized businesses, and primary and secondary education. The NCSA maintains StaySafeOnline.org, a Web site that provides computer safety information to home users, primary school educators, and small businesses and promotes National Cyber Security Awareness Month in the United States.
- **Cybercrime Centres of Excellence Network for Training, Research and Education (2CENTRE)**, a new project supporting the creation of national Centres of Excellence in IT Forensics and Cybercrime Investigation in European countries/regions, to partner with a Network Coordination Centre to be established in a European Union member state. The 2CENTRE project was announced at the Cybercrime Conference of the Council of Europe in March 2009. Project commencement is expected to begin in early 2010.

From time to time, these groups themselves unite to spearhead efforts like the Chain of Trust Initiative, launched in May 2009 by the NCSA, the ASC, and StopBadware.org. The Chain of Trust Initiative is intended to strengthen the links between security vendors, researchers, government agencies, Internet companies, network providers, advocacy groups, and education groups in a systemic effort to fight malware.

Recognizing the important role the security response community plays in Microsoft's own security efforts, the company formed the Microsoft Security Response Alliance (MSRA) in 2006 as a framework for partners, vendors, governments, and infrastructure providers to collaborate in a secure and timely manner. The MSRA serves as an umbrella organization for a number of other alliances and initiatives, several of which predate the formation of the MSRA itself. For example, the Microsoft Virus Initiative (MVI) was originally formed in 1997 to facilitate communication between Microsoft and antivirus (AV) software vendors about macro viruses, which led to the development of the Antivirus application programming interface (Antivirus API) supported by Microsoft Office applications to the present day. Figure 2 lists the MSRA member organizations and what they do.

FIGURE 2. Organizations and working groups under the MSRA umbrella

Organization	Focus	Purpose
The Global Infrastructure Alliance for Internet Safety (GIAIS)	Internet service providers (ISPs)	Fosters cooperation between Microsoft and the world's leading ISPs to keep their customers safe on the Internet
The Microsoft Virus Initiative (MVI)	Security researchers, antivirus software vendors	Enables Microsoft to share key technical details of Microsoft technologies with partners, to facilitate development of well-integrated security solutions
Virus Information Alliance (VIA)	Antivirus software vendors	Provides AV partners with detailed technical information about significant viruses affecting Microsoft products and customers
Microsoft Security Cooperation Program (SCP)	Public sector infrastructure, law enforcement, public safety, and education	Provides a framework for information exchange and collaboration between Microsoft and the public sector, primarily in the areas of response and outreach
Microsoft Security Support Alliance (MSSA)	Microsoft original equipment manufacturer (OEM) partners	Provides authoritative and timely information on newly discovered security threats to Microsoft's OEM partners, enabling them to better communicate security information to their customers
Security Alliance for Financial Institutions (SAFI)	Financial institutions	Facilitate collaboration between Microsoft and financial institutions worldwide regarding the threats that such institutions face

Groups and initiatives such as these, along with security conferences such as Black Hat and CanSecWest, contribute to what Microsoft has called *community-based defense*: a strategy for creating a more secure environment for everyone that involves collaboration, sharing best practices, and making investments in security and defense knowledge. The reaction of the worldwide security community in late 2008 and early 2009 to a new, highly aggressive threat is a strong indicator of the effectiveness of this approach.

Case Study: The Conficker Working Group

The appearance in late 2008 of Win32/Conficker, an aggressive and technically complex new family of worms, posed a serious challenge to security responders and others charged with ensuring the safety of the world's computer systems and data. ("Win32/Conficker Update," beginning on page 95, explains the technical details of the Conficker worm and the methods it uses to propagate.) Working together, however, the security community was able to react quickly to the threat and contain much of the damage, in the process establishing a potentially groundbreaking template for future cooperative response efforts.

On October 23, 2008, Microsoft released critical security update MS08-067, addressing CVE-2008-4250, a vulnerability in the Windows Server service that could allow malicious code to spread silently between vulnerable computers across the Internet. The vulnerability affected most currently supported versions of Windows, although architectural improvements in Windows Vista and Windows Server 2008 made them more difficult to exploit than earlier versions. Like the worms that plagued the Internet earlier this decade, malware that exploited the vulnerability would be able to spread without user interaction by taking advantage of the protocols computers use to communicate with each other across networks. For this reason, and because actual attack code that exploited the vulnerability was known to exist in the wild at the time, the MSRC took the unusual step of releasing MS08-067 "out of band" rather than wait for the next scheduled release of Microsoft security updates, which takes place on the second Tuesday of every month. Security Bulletin MS08-067 happened to be released on the last day of the eighth annual meeting of the International Botnet Task Force in Arlington, Virginia, a suburb of Washington, D.C., where attendees agreed to closely monitor developments around what appeared to be the first legitimately "wormable" vulnerability to be discovered in Windows in several years.

The November appearance of Win32/Conficker, the first significant worm that exploited the MS08-067 vulnerability, marked a major challenge for security researchers, due to the aggressive tactics several of its variants used to propagate. Despite this, researchers soon discovered a way to limit or eliminate the Conficker bot-herders' ability to issue instructions to infected computers. As described on page 96, the authors of the Conficker malware used an algorithm to generate 500 new domain names every day (250 for each of the first two Conficker variants discovered) to use for command-and-control servers. Computers infected with Conficker would attempt to contact each of these generated domain names every day. If the authors had a task they wanted the computers in the botnet to perform, they would simply use the same algorithm to generate domain names in advance and register a few of them, which they could then use to host command-and-control servers.

Fortunately, researchers from Microsoft and other organizations were able to reverse-engineer the domain-name-generation algorithms used by the first two variants, designated Worm:Win32/Conficker.A and Worm:Win32/Conficker.B, soon after each variant was discovered. This enabled them to begin registering the domain names before the botnet operators could, thereby impeding the Conficker malware from obtaining new

instructions. Initially, the researchers resorted to registering the domains commercially through the domain name registrars for the eight top-level domains (TLDs) (.com, .net, .org, .info, .biz, .ws, .cn, and .cc) used by Conficker, an approach that quickly became unworkable. Registering 500 domain names per day would cost thousands of (U.S.) dollars per day for the foreseeable future—and the cost would only increase if new variants appeared using different name-generation algorithms. It was clear that more help would be needed.

The Conficker Working Group Is Born

In January 2009, representatives from a number of security research companies and domain registrars, along with the anti-botnet Shadowserver Foundation, began discussing how best to implement a defensive Domain Name Service (DNS) strategy to handle domain registrations. To coordinate the significant amount of e-mail being generated by these discussions, the group established the CONFICKER e-mailing list on January 28, which drew a growing number of security researchers and members from law enforcement, academia, and industry, in addition to members representing each of the eight TLDs used by Conficker. Enlisting the support of the TLD operators would prove to be a vital step in containing the Conficker threat, enabling the group to block domain names more efficiently and at far less expense than would be possible through the commercial registration process.

By early February 2009, working group members had instituted a process for registering as many domain names as possible, before the Conficker operators could register them, and assigning them to IP addresses belonging to six *sinkholes* (server complexes designed to absorb and analyze malware traffic) operated by organizations belonging to the working group. Infected computers looking for command-and-control servers would contact the sinkholes instead, providing researchers with valuable telemetry for analyzing the spread of the worm. A number of Internet service providers (ISPs) were also able to use this telemetry data to identify infected computers. Around the same time, the Internet Corporation for Assigned Names and Numbers (ICANN), which is responsible for allocating IP addresses and managing the Internet domain name system, invited the group to deliver a presentation on its domain registration efforts to a meeting of the ICANN board of directors. The board expressed its support for the program and assigned two staffers to help coordinate it.

Despite these efforts, the Conficker operators were still able to register some domains before the working group could get to them. To mitigate this, researchers at Kaspersky Lab, an anti-malware vendor headquartered in Russia, worked with OpenDNS, a free network resolution service used by many organizations and individuals, to compute a year's worth of Conficker domain names and proactively point them at the group's sinkholes. Any infected computer belonging to an OpenDNS user would not be able to contact any of the Conficker command-and-control servers, even on domains the Conficker operators had been able to secure.

The formation of the Conficker Working Group (CWG) was officially announced to the public on February 12, 2009, as what a number of news stories characterized as an unprecedented example of global cooperation in the computer security industry, and a potential blueprint for dealing with threats in the future. The CWG had grown from an e-mail list for nine individuals to a group of more than 30 member organizations from around the world, coordinating complex activities through a robust communications infrastructure. On the day the CWG was announced, the group had successfully registered every Conficker domain name for the next 10 days, a genuine—if temporary—victory over the Conficker operators.

Setbacks and Triumphs

The domain registration task became exponentially more challenging on March 4, 2009, with the discovery of Worm:Win32/Conficker.D. Investigators reverse-engineered the new variant and determined that it was programmed to generate *50,000* new domain names a day across 110 TLDs, beginning on April 1, 2009. Though this seemed at first like an impossible hurdle to overcome, CWG members immediately began working to counter the effects of the upcoming change. As security researchers continued to analyze the Conficker.D malware, ICANN staffers began contacting the registries responsible for each of the affected TLDs seeking cooperation in registering or blocking the domains, and the CWG compiled "go packs" of information for Internet service providers and enterprises about the steps they should take to help keep their customers and employees safe.

April 1, 2009, came and went, with the world outside the security community noticing little or no change. By that time, however, ICANN had secured the cooperation of all 110 TLDs used by Conficker, and the global DNS community was active and prepared to deal with the Conficker threat. Rapid, effective collaboration across borders and organizational lines had proven instrumental in containing what has been, and remains, a significant threat to the world's computers and information.

The CWG Today

The CWG remains in place today, with more than 300 member organizations representing law enforcement, academia, and industry, and remains vigilant against new developments. In cooperation with ICANN and the DNS community, the CWG continues to block or register the 50,000 domain names generated each day by the Conficker algorithms. Each month the group supplies the 110 affected TLD operators with an updated list of generated domain names covering the next several months, so they can begin implementing countermeasures well in advance. Automated mechanisms verify that each domain name has been blocked before it is scheduled to be used and alert the CWG for any that have not, so activity for those domains can be closely monitored. Once in a while, a domain name generated by the algorithm happens to correspond to an existing domain owned by a legitimate party;

in such cases, the CWG contacts the legitimate domain owner in advance and offers assistance managing the expected spike in traffic coming from infected computers.

In March, the group underwent a reorganization process to add structure and to segment its work by subject area to work more effectively. The group maintains a Web site at http://www.confickerworkinggroup.org with links to information in multiple languages about Conficker and resources that service providers and end users can use to determine if they are infected, and if so, what to do about it.

The fight against Conficker is not over. The five identified variants continue to spread to new computers due to a lack of information or action on the part of some system administrators and end users. Even after Conficker recedes into insignificance, there will likely be other threats of similar magnitude to deal with in the future. As such threats appear, though, collaborative efforts, such as the CWG, can provide the global security community with unequaled tools for mitigation and resolution.

Strategies, Mitigations, and Countermeasures

- Consider adopting a programmatic approach towards addressing the issues and attack vectors uncovered in this report. Examples might include practices dictated by standards such as ISO/IEC 27000, Control Objectives for Information and related Technology (COBIT), or the Payment Card Industry Security Standards Council (PCI SSC). Regardless, the ability to effectively take advantage of a risk management methodology is a key success driver. The Microsoft Security Risk Management Guide (http://technet.microsoft.com/en-us/library/cc163143.aspx) provides both a qualitative and quantitative risk analysis of your environment.
- Limit exposure by not sharing administrator accounts and by enforcing the concept of separation of duties, by both role and by department. In situations involving high-value assets, consider the *split-password* approach, where each administrator has a portion of the password and two or more must be present for system logon. In addition, enable Object Access auditing for items associated with the administrator accounts, so that actions can be monitored.
- Enforce the idea of least privilege, wherein computer accounts are given only those permissions required to perform a job function. Administrators sometimes tend to configure accounts with maximum rights to save time later.
- Ensure that your antivirus product is configured to scan removable media storage devices upon connection. Many threats execute via "virtual CD drives" that run directly from such devices.
- Better protect your whole ecosystem by ensuring that your home computers are secure, as well as your business computers. Consider using Microsoft Security Essentials (http://www.microsoft.com/security_essentials/) to provide real-time protection for your home computers, at no charge to licensed users of Windows.
- Understand that SQL injection attacks can affect any database that is ANSI-99 compliant. Most commercial and open-source databases support this standard. Ensure that input validation is being conducted as data arrives, not only from Web forms but also from data being imported from remote sources, such as partners or vendors.
- Drive security awareness by helping users understand that reputable antivirus providers do not leverage browser pop-up advertisements to promote their products. Users should immediately close any such ads to prevent infection and should understand that using such solutions may actually prevent real antivirus products from doing their jobs.
- Ensure that the signature files for your antivirus solution are up to date and are automatically updated with regularity.

- Stay informed! You must be aware of the threat landscape around you. Information security is a rapidly changing environment, so it's important to keep up with the latest happenings in both the wider industry and in your specific vertical market (such as healthcare or manufacturing). Consider joining one of the many industry associations—like the Information Systems Security Association (ISSA), the Information Systems Audit and Control Association (ISACA), the Information Security Forum (ISF), or Infragard—so you can stay aware of the latest information. Are you aware of the legislation (such as CAN-SPAM) that affects your business?
- Work with your local law-enforcement agencies. If you think you may have been a victim of an attack, or if you suspect something unusual on your network, you should contact law enforcement for assistance. Establishing a good working relationship with your local law-enforcement officers is key to a successful incident-response program.
- Stay up to date on the Microsoft security world by using the Trustworthy Computing blog aggregator at http://www.microsoft.com/twc/blogs.

Microsoft Malware Protection Center

The Microsoft Malware Protection Center 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 underlines Microsoft security products and services such as the Malicious Software Removal Tool, Windows Defender, Forefront Client Security, the SmartScreen Filter in Internet Explorer 8, and (beginning in 2H09) Microsoft Security Essentials. 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

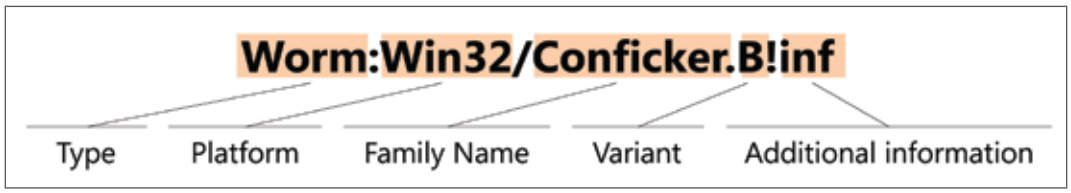
Except where specified, the data in this section has been compiled from telemetry generated from hundreds of millions of computers worldwide by a number of different Microsoft security tools and services, including the MSRT, Windows Live OneCare, the Windows Live OneCare safety scanner, Windows Defender, Microsoft Forefront products, and Microsoft Forefront Online Protection for Exchange (FOPE; formerly Forefront Online Security for Exchange, or FOSE). See "Appendix C: Data Sources," beginning on page 223, for more information on these tools.

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 3.

FIGURE 3. The Microsoft malware naming conventions



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/Conficker") is a reference to a family. When a longer threat name is given (like "Worm:Win32/Conficker.B!inf"), 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/Conficker is referred to simply as Conficker on subsequent mention in some places, and Worm:Win32/Conficker.B simply as Conficker.B.

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 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 1H09 as a whole, are derived

by averaging the CCM for each month in the period. The MSRT data is used because the tool's global reach, large installed base, and regularly scheduled release facilitate the 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. ("Appendix B: Threat Assessments for Individual Locations," beginning on page 181, includes more in-depth information about the threat landscapes in many of the locations listed here.)

FIGURE 4. The 25 locations with the most computers cleaned by Microsoft desktop anti-malware products in 1H09

Country/Region	Computers Cleaned (1H09)	Computers Cleaned (2H08)	Change
United States	13,971,056	13,245,712	5.5% ▲
China	2,799,456	3,558,033	-21.3% ▼
Brazil	2,156,259	1,654,298	30.3% ▲
United Kingdom	2,043,431	2,225,016	-8.2% ▼
Spain	1,853,234	1,544,623	20.0% ▲
France	1,703,225	1,815,639	-6.2% ▼
Korea	1,619,135	1,368,857	18.3% ▲
Italy	1,192,867	978,870	21.9% ▲
Turkey	1,161,133	768,939	51.0% ▲
Germany	1,086,473	1,209,461	-10.2% ▼
Mexico	957,697	915,605	4.6% ▲
Canada	942,826	916,263	2.9% ▲
Taiwan	781,214	466,929	67.3% ▲
Russia	581,601	604,598	-3.8% ▼
Japan	553,417	417,269	32.6% ▲
Poland	551,419	409,532	34.6% ▲
Netherlands	494,997	641,053	-22.8% ▼
Australia	416,435	464,707	-10.4% ▼
Portugal	375,502	337,313	11.3% ▲
Belgium	208,627	267,401	-22.0% ▼
Saudi Arabia	205,157	154,697	32.6% ▲
Sweden	197,242	287,528	-31.4% ▼
Colombia	183,994	164,986	11.5% ▲
Greece	161,639	158,476	2.0% ▲
Denmark	160,001	224,021	-28.6% ▼
Worldwide	**39,328,515**	**37,522,446**	**4.8% ▲**

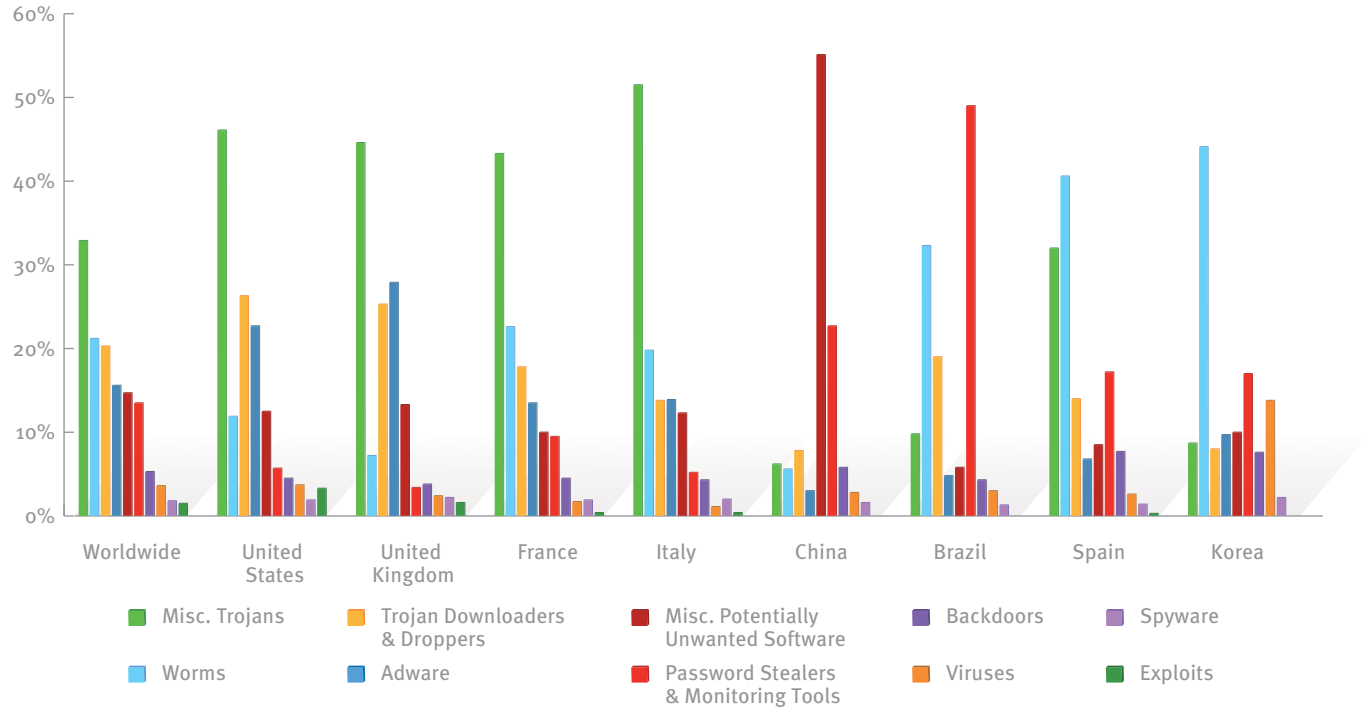
As Figure 4 shows, the number of computers cleaned in individual countries/regions can vary quite a bit from period to period. The largest increase in this figure is the 67.3 percent rise in Taiwan, which is due in part to increased detections of several password stealers that target players of online games, such as Win32/Taterf, Win32/Frethog, and Win32/Corripio. (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)*.) The largest decline in this figure is the 31.4 percent decrease in Sweden, which is due in part to a decline in the prevalence of a number of older families without a commensurate rise in newer threats.

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. "Ten Years of Malware and Security Threats, 1999–2009," beginning on page 18, explains how the malware ecosystem has moved away from highly visible threats, like self-replicating worms, toward less visible threats that rely more on social engineering. This shift means that the spread and effectiveness of malware have become more dependent on language and cultural factors. 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.

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 5 shows the relative prevalence of different categories of malware and potentially unwanted software in the eight locations with the most computers cleaned in 1H09, expressed as percentages of the total number of computers cleaned in each location. (The sum of the infection rates 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 48 for an explanation of the categories used in this figure.

FIGURE 5. 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, 1H09



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/FakeXPA: A rogue security software family that claims to scan for malware and then demands that the user pay to remove non-existent threats. Some variants unlawfully use Microsoft logos and trademarks.

http://www.microsoft.com/av

- In the **United States** and the **United Kingdom**, Miscellaneous Trojans account for the largest single category of threat. The United States and United Kingdom typically display similar mixes of threat categories, with families such as Win32/Alureon and Win32/Vundo relatively common in both locations. Nevertheless, there are also some significant differences in the lists of prevalent families in each location. For example, Win32/FakeXPA, the most prevalent family in the United States in 1H09, was a distant sixth in the United Kingdom.
- **France** and **Italy** also display similar threat landscapes. The top threat in both locations by a wide margin was the Miscellaneous Trojans family Win32/Wintrim, which has a strong presence in Western Europe but is seen much less often elsewhere.
- In **China**, many of the most prevalent families are Chinese-language threats that don't appear in the list of top threats for any other location, such as the browser modifier Win32/BaiduSobar,[11] or password stealers that target players of online games, including Win32/Lolyda and Win32/Frethog.

[11] Figures do not include newer versions of the Baidu Sobar software, which no longer exhibits the behaviors Microsoft uses to classify software as potentially unwanted.

- The threat landscape in **Brazil** is dominated by Portuguese-language password stealers that target online users of Brazilian banks, led by Win32/Bancos, the most prevalent malware threat in Brazil.
- Though widely separated both geographically and culturally, **Spain** and **Korea** are both 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.

Figure 6 illustrates the infection rates of locations around the world, expressed in CCM. See page 37 for an explanation of the CCM metric.

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.

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.

http://www.microsoft.com/av

FIGURE 6. Infection rates by country/region in 1H09

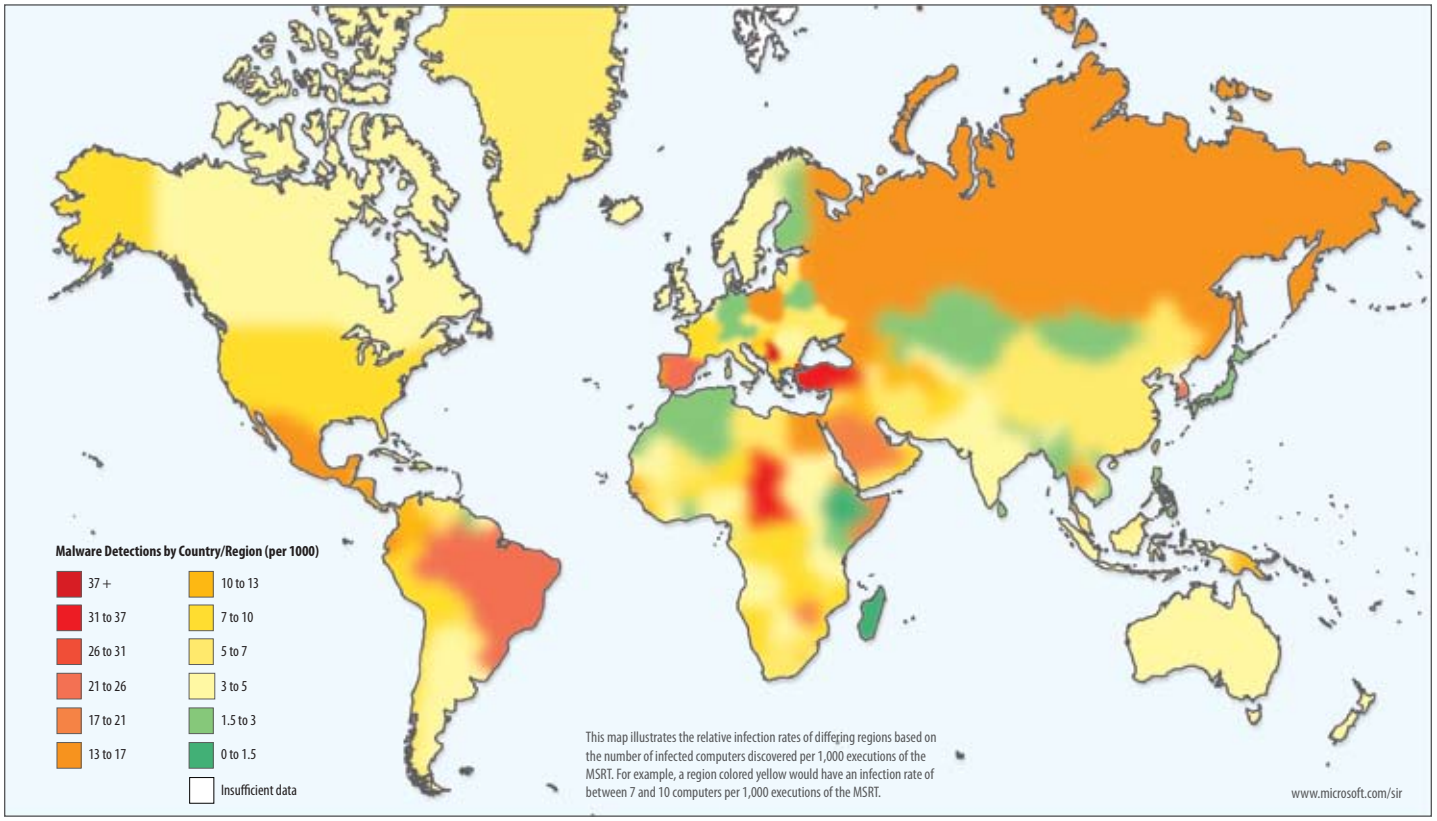


Figure 7 shows the infection rates in locations around the world with at least 1 million average monthly MSRT executions in 1H09, derived by averaging each location's monthly CCM for each of the six months in the period. See "Appendix A: Full Geographic Data," on page 172, for a more comprehensive list with 212 locations, and see "Appendix B: Threat

Encyclopedia

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

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 in order to steal login and account details for popular online games.

http://www.microsoft.com/av

Assessments for Individual Locations," beginning on page 181, for an in-depth look at the threat landscapes for 14 locations around the world, encompassing every inhabited continent and multiple languages and computer usage patterns.

FIGURE 7. Infection rates (CCM) for locations around the world with at least 1 million average monthly MSRT executions in 1H09

Country/Region	CCM (1H09)
Argentina	4.5
Australia	3.9
Austria	2.1
Belgium	4.9
Brazil	25.4
Canada	3.1
Chile	7.6
China	6.7
Colombia	12.9
Czech Republic	5.1
Denmark	3.2
Finland	1.9
France	7.9
Germany	3.0
Greece	9.8
Hong Kong S.A.R.	7.8
Hungary	9.3
India	3.3
Ireland	3.6
Israel	7.6
Italy	6.9
Japan	3.0
Korea	21.3
Malaysia	5.1
Mexico	14.5
Netherlands	4.3
New Zealand	3.4
Norway	3.3
Peru	8.5
Philippines	2.3
Poland	13.0
Portugal	13.7
Romania	4.7
Russia	15.0
Saudi Arabia	20.8
Singapore	4.7
South Africa	5.5
Spain	21.6
Sweden	3.2
Switzerland	3.0
Taiwan	20.4
Thailand	14.0
Turkey	32.3
United Kingdom	4.9
United States	8.6
Venezuela	6.9
World wide	**8.7**

Figure 8 and Figure 9 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 1H09, respectively, among locations with at least 100,000 average monthly MSRT executions.

FIGURE 8. Locations with the lowest infection rates, by CCM, in 1H09 (100,000 monthly MSRT executions or more)

Country/Region	CCM (1H09)
Finland	1.9
Austria	2.1
Puerto Rico	2.1
Philippines	2.3
Vietnam	2.4
Macao S.A.R.	2.4
Tunisia	2.5
Morocco	2.6
Algeria	2.8
Kenya	2.9
Kazakhstan	2.9
Germany	3.0
Switzerland	3.0
Jamaica	3.0
Japan	3.0
Pakistan	3.0
Uruguay	3.1
Canada	3.1
Sweden	3.2
Malta	3.2
Denmark	3.2
Norway	3.3
Luxembourg	3.3
India	3.3
Trinidad and Tobago	3.4

FIGURE 9. Locations with the highest infection rates, by CCM, in 1H09 (100,000 monthly MSRT executions or more)

Country/Region	CCM (1H09)
Serbia and Montenegro	97.2
Turkey	32.3
Brazil	25.4
Spain	21.6
Korea	21.3
Saudi Arabia	20.8
Taiwan	20.4
Guatemala	17.0
Russia	15.0
Mexico	14.5
Thailand	14.0
Egypt	13.7
Portugal	13.7
Ecuador	13.5
Poland	13.0
Honduras	13.0
Colombia	12.9
El Salvador	11.8
Croatia	11.0
Jordan	10.3
Costa Rica	10.0
Greece	9.8
Bahrain	9.3
Hungary	9.3
Macedonia, F.Y.R.O.	8.7

Best Practices Around the World

Over the last several years, a number of countries have consistently exhibited infection rates well below the worldwide average. For this volume of the *Security Intelligence Report*, Microsoft has asked computer security response professionals representing four of these countries to comment about why they believe this to be so and about the best practices their countries follow to keep their residents and resources safe from computer threats.

Austria

Leon Aaron Kaplan, National Computer Emergency Response Team of Austria (http://www.cert.at/)

Austria has roughly 8.2 million inhabitants possessing 9.8 mobile phones. It is often regarded as a "testing grounds" for new mobile phone services, especially UMTS. It is industrially highly developed, achieving 15th place in the Human Development Index (2007/2008).[12] *The Internet sector is well developed, with DSL and cable being the predominant form of access. It has roughly 5.5 million Internet users as of June/08 which equates to 67% of the population, according to a study by the GfK Group. However, Austria is not the birthplace of the IT industry, nor does it have its own Silicon Valley. We might expect the level of IT know-how and security awareness to be about average, and not as high as in some other IT hot spots of the world. So why does Austria have such a low CCM score?*

One potential explanation could be that the "market" is too small, and malware authors prefer to target Germany (a country with 80 million inhabitants) instead of Austria. However, this argument only holds for localized attacks such as phishing. For non-localized malware. such as worms and viruses, an IP address is an IP address, no matter if it is in Austria or not.

Another factor affecting overall IT security seems to be a small and close-knit network of working relationships between technicians working at ISPs. CERT.at employs many people who formerly worked at large ISPs. A takedown request for a website hosting malware is often therefore just a cell phone call away from the right technician. Therefore the window of opportunity for phishing or malware hosting is small in Austria.

Furthermore, many ISPs have strong IT security enforcement policies. For example, the largest Austrian consumer ISP will disconnect a residential customer if a problem caused by malware on the customer's computer (such as spam) persists for a week.

While CERT.at was monitoring the Win32/Conficker worm we came across a very interesting observation: those countries with low software piracy rates were less affected by Conficker. According to the Business Software Alliance,[13] *Austria is one of the countries*

[12] United Nations Development Programme. "Human Development Report 2007/2008." http://hdrstats.undp.org/en/countries/data_sheets/cty_ds_AUT.html

[13] Business Software Alliance. "Sixth Annual BSA-IDC Global Software Piracy Study." http://global.bsa.org/globalpiracy2008/studies/globalpiracy2008.pdf

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.

http://www.microsoft.com/av

with the lowest piracy rates worldwide (24 percent, 5th lowest in the world). [Users in countries with high piracy rates are less likely to use Windows Update to receive critical security updates. For more information about the relationship between piracy rates and usage of Microsoft update services, see "Regional Variations in Update Service Usage," beginning on page 164.]

We believe the low piracy rate, combined with a generally strict IT security enforcement of ISPs and the fact that updates are quickly installed due to fast Internet lines (broadband, cable connection) forms a basis for the generally low infection score in Austria.

Finland

Erka Koivunen, Head of Unit, Computer Emergency Response Team, Finnish Communications Regulatory Authority (http://www.cert.fi)

What is it that makes Finnish networks so safe? A couple of things comes to mind, and then one unavoidable conclusion.

First, the capability to detect needs to be complemented with the ability to take action. CERT-FI has tasked itself with concretely reaching out and finding factual technical information about malicious events taking place in Finland, out of Finland, or towards Finland. As it turns out, there are a plethora of community-driven projects gauging the level of malicious activity all over the internet: honeynets, darknets, log repositories, automated malware analysis tools, and others. What's common for the majority of them is that the findings just sit in databases, with nobody trying to get rid of the troublemakers. Most of the projects are just dying to send the reports out to someone who would take care of finding the compromised ICT systems and helping the victims. Our automated tool, CERT-FI Autoreporter, downloads these reports en masse, anonymises the sources, determines the responsible Finnish network admins, and proceeds to let them know about the breaches, so they can take action.

Second, the lifetime of the malware infections and security breaches needs to be cut down. The general attitude among Finnish network admins is that it's in their own and their customers' interests to act quickly once the reports hit their desks. It saves helpdesk costs, cuts down the amount of malicious traffic, and helps increase customer confidence. As a result, the infected computers get treated fast or risk losing connectivity. Botnet controllers and malware distribution sites have proven to have a hard time staying online in Finnish networks.

Third, the positive regulative atmosphere regarding sensible information security…. There are clear and pragmatic provisions in Finnish legislation granting network admins the right (and at times an obligation) to defend their networks and interconnected IT systems against breaches of technical information security…. The rules start with administrative engagement: appointing responsible network security admins and the so-called abuse helpdesks to handle complaints is mandatory. The more technical stuff includes provisions such as exercising what we call "address hygiene" in core networks (e.g., filtering spoofed

Continued on next page...

and source-routed packets) and restricting broadband subscribers' ability to send spam or participate in denial-of-service attacks. There are also a requirement for ISPs to inform their subscribers about the possible dangers of the Internet and ways to mitigate them. As a side effect, this has greatly boosted the purchase of security software by private consumers.

As a result of all this, the number of "malicious" events in Finnish networks hasn't exceeded the growth of the connected users in the past couple of years. Needless to say, we need to be constantly vigilant and adapt our posture to the changes in the security landscape. This will require some excellent navigation skills in the future, we know.

Ah, the Unavoidable Conclusion I mentioned earlier. While we acknowledge that the Finnish networks appear to be clean, at the same time we understand that this doesn't necessarily make Finland any better prepared for a possible cyber attack than anyone else. We are just less likely to cause headaches for everybody else. In this sense, the description of Earth in the [Douglas Adams] book The Hitchhiker's Guide to the Galaxy *fits Finland quite nicely as well: "Mostly Harmless."*

Germany

Torsten Voss, DFN-CERT (http://www.dfn-cert.de/); Hans-Peter Jedlicka, Federal Office for Information Security (BSI) (http://www.bsi.de/)

Germany has a very large CERT community, with more than thirty commercial, government, and academic CERTs organised in the German CERT-Verbund (http://www.cert-verbund.de). Here is how CERT-Bund and DFN-CERT work to keep infection within their constituency low.

The federal Computer Emergency Response Team (CERT-Bund) is part of the Federal Office for Information Security (BSI) as the IT security provider for the German government. Its main task is to strengthen IT security and to mitigate any potential impact on governmental networks. The BSI also works closely with the German ISP community, which identifies botnet infections and informs the owners of infected computers, in some cases even isolating them under quarantine.

Additionally, a multitude of different awareness-raising initiatives, conducted by different stakeholders from the government and private sectors, provide information for every interested citizen. This includes efficient warning and alerting services for each of the CERTs'/CSIRTs' prime constituencies (http://www.cert-bund.de/), but also for the citizens (http://www.buerger-cert.de/).

DFN-CERT is the Incidence Response Team for the German Research Network (DFN; http://www.dfn.de/) and serves the German academic and research community. One major goal of DFN-CERT's daily work is to actively prevent the distribution of malware in its constituency, resulting in a low malware infection rate.

Besides proactive measures (distribution of information about vulnerabilities and patches), this includes an important reactive service, which is based on a knowledge of IP address ranges and security contacts in the constituency. It consists of the following three steps:

1. *Collection of information about suspicious traffic, either from other CERTs or from the DFN-CERT systems (e.g. honeypots, darknets).*
2. *Cross-referencing of this information with IP addresses in the constituency, which yields knowledge about which site has a problem with a certain machine or IP address.*
3. *Contacting the sites directly and give them detailed reports. This way local security contacts can act quickly, check their systems, and avoid the further spread of malware.*

Japan

Hideaki Kobayashi and Toshiaki Kokado, Information-Technology Promotion Agency, Japan (http://www.ipa.go.jp)

One of the reasons [that the infection rate in Japan is lower than in many other countries] is that Cyber Clean Center (https://www.ccc.go.jp/), a cooperative project between ISPs (76 companies as of June 2009), major security vendors (7 companies, including Microsoft), and Japanese government agencies, has worked on educating users and helping them remove infections from their computers. Thanks to this effort, we have succeeded in reducing the number of computers infected by botnet malware to 1 percent in June 2008, from 2.5 percent in April 2005. At the same time, we have contributed to improving the detection rate of malware on users' computers by providing security vendors with samples collected by honey pots.

However, this is just part of a long-term effort for IPA, which was established in 1970 by the Japanese Ministry of International Trade and Industry (MITI).[14] *The first countermeasure was a virus consultation service IPA started in 1990. The service provides basic answers for questions from companies and people, including "What is a virus?" and "My computer is infected. What should I do?". Information gathered via inquiries, samples, and trend information from administrative agencies is provided to security vendors, which leads to specific actions.*

For the purpose of preventing virus infection, it is necessary to improve the quality of software product security, and efforts have been made to reduce the number of vulnerabilities over the years. For example, over 1.3 million copies of How to Secure Your Website, *a textbook for building Web sites securely and reducing vulnerabilities in Web applications, have been downloaded since its release.*

Apart from that, we have offered a tool that tests for known vulnerabilities in standard protocols, such as TCP/IP, to development companies for free. Our goal is to provide help for developers who are not security specialists, and they have accepted our assistance as

[14] In 2001, MITI was reorganized into the Ministry of Economy, Trade and Industry (METI).

Continued on next page...

beneficial to users. IPA and the Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) have also started Japan Vulnerability Notes *(JVN) to release information in Japanese on vulnerabilities in both Japanese software and software distributed in Japan, and to provide information for enlightenment and prevention of recurrence.*

At the same time, we have worked actively on challenges for the future. For example, we have launched an information security workgroup for home information appliances and cars.

These activities do not have an immediate effect. However, these government-affiliated agencies have continued their IT lifecycle-wide efforts for years, including providing knowhow for secure software development, and gathering information about current threats and countermeasures against them. These measures have created a high level of awareness about information security among the nation, companies, and the entire population. We believe that this high level of awareness helps make Japan a country with such a low malware infection rate.

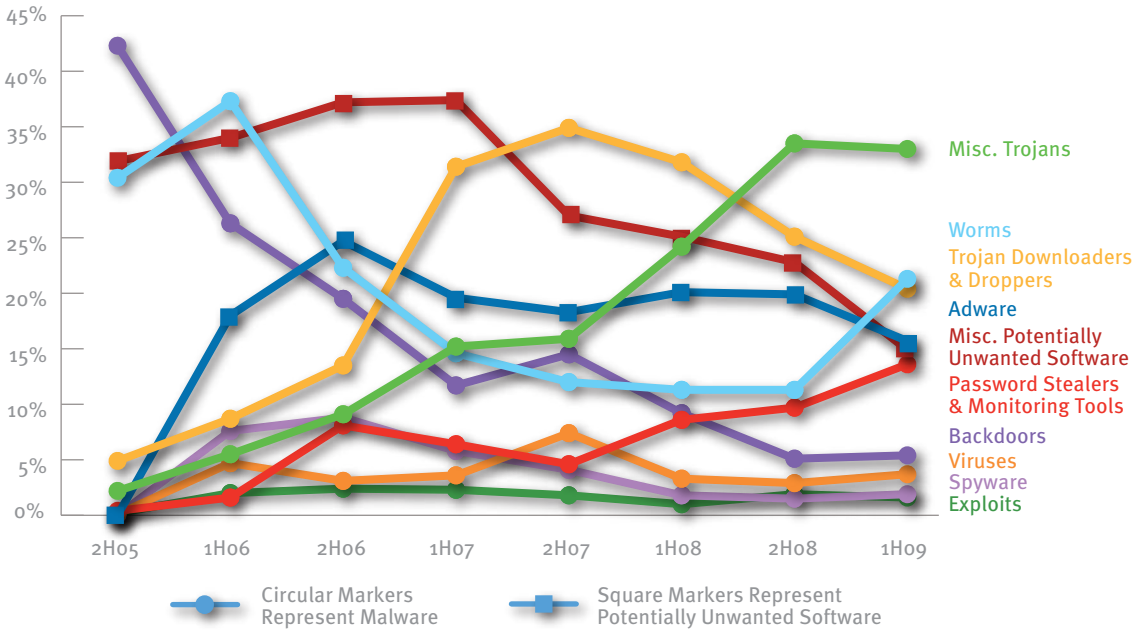
Category Trends

As explained in "Threat Naming Conventions," on page 36, 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.

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 229, for definitions of the other categories described in this section.

Figure 10 shows the relative prevalence of different categories of malware and potentially unwanted software since 2H05, 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 10. Computers cleaned by threat category, in percentages, 2H05–1H09



Miscellaneous Trojans remained the most prevalent category in 1H09, for the second straight period. Notably, Worms rose from fifth place in 2H08 to become the second-most prevalent category in 1H09, largely due to significantly increased detections of the worm families Win32/Conficker and Win32/Taterf, the two most prevalent families worldwide in 1H09. The prevalence of Password Stealers & Monitoring Tools also rose, due in part to increases in several password-stealer families aimed at players of online games. Of the remaining categories, Trojan Downloaders & Droppers, Miscellaneous Potentially Unwanted Software, and Adware all had relative declines, with the others remaining relatively stable from 2H08.

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.

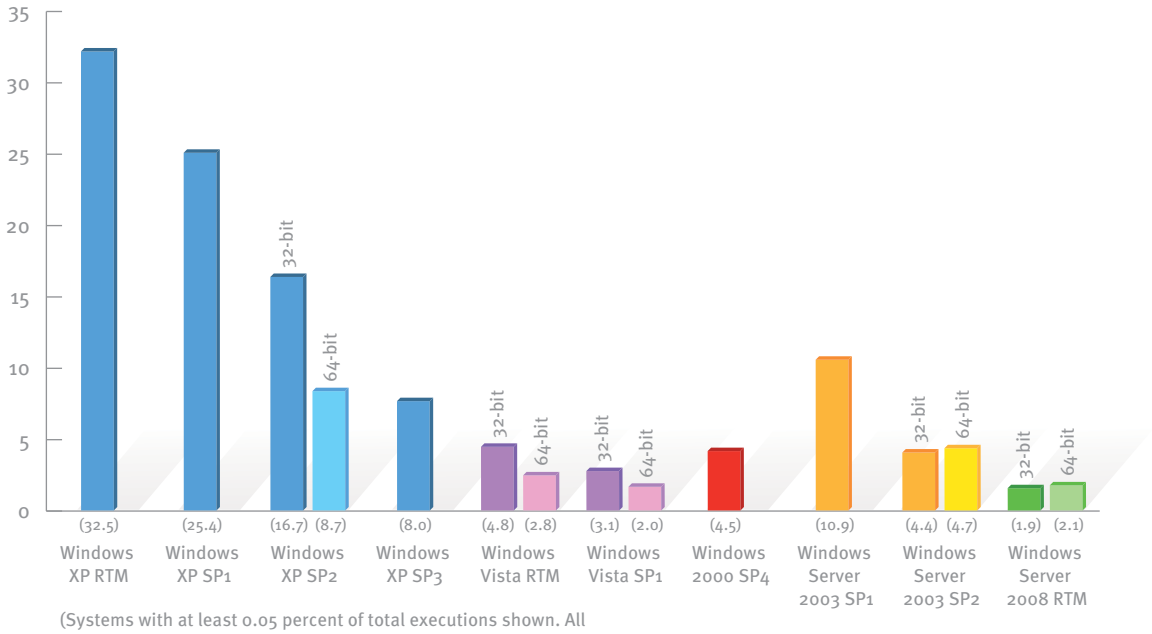
Win32/Taterf: A family of worms that spread through mapped drives in order to steal login and account details for popular online games.

http://www.microsoft.com/av

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 11 shows the infection rate for each Windows operating system/service pack combination that accounted for at least 0.05 percent of total MSRT executions in 1H09. (Note that the infection rate for each version of Windows is calculated separately; the infection rate for a version is not affected by the number of computers running it. See page 37 for a definition of the CCM metric used to calculate infection rates.)

FIGURE 11. Number of computers cleaned for every 1,000 MSRT executions, by operating system, 1H09



(Systems with at least 0.05 percent of total executions shown. All operating system versions shown are 32-bit unless otherwise specified.)

Consistent with previous periods, the infection rate for Windows Vista is significantly lower than that of its predecessor, Windows XP, in all configurations. Specifically:

- Comparing the latest service packs for each version, the infection rate of Windows Vista SP1 is 61.9 percent less than that of Windows XP SP3.[15]
- Comparing the RTM versions of these operating systems, the infection rate of the RTM version of Windows Vista is 85.3 percent less than that of the RTM version of Windows XP.

[15] Windows Vista Service Pack 2 was released on June 30, 2009, the last day of 1H09, and is therefore not included in this analysis.

Similarly, the infection rate of Windows Server 2008 RTM is 56.1 percent less than that of its predecessor, Windows Server 2003 SP2. Server versions of Windows typically display a lower infection rate on average than client versions, especially when comparing the latest service pack version for each operating system. Windows Server 2008, which includes only server editions, has the lowest infection rates of any configuration on the chart, while the Windows XP configurations, intended for home and workplace users, have the highest. Windows 2000 SP4, which includes both server and client editions, falls between the two extremes. Servers tend to have a lower effective attack surface than computers running client operating systems because they are more likely to be used under controlled conditions by trained administrators and to be protected by one or more layers of security. In particular, Windows Server 2003 and its successors are hardened against attack in a number of ways, reflecting this difference in usage. For example, Internet Explorer Enhanced Security Configuration is enabled by default, and the Roles Wizard automatically disables features that are not needed for the configured server role.

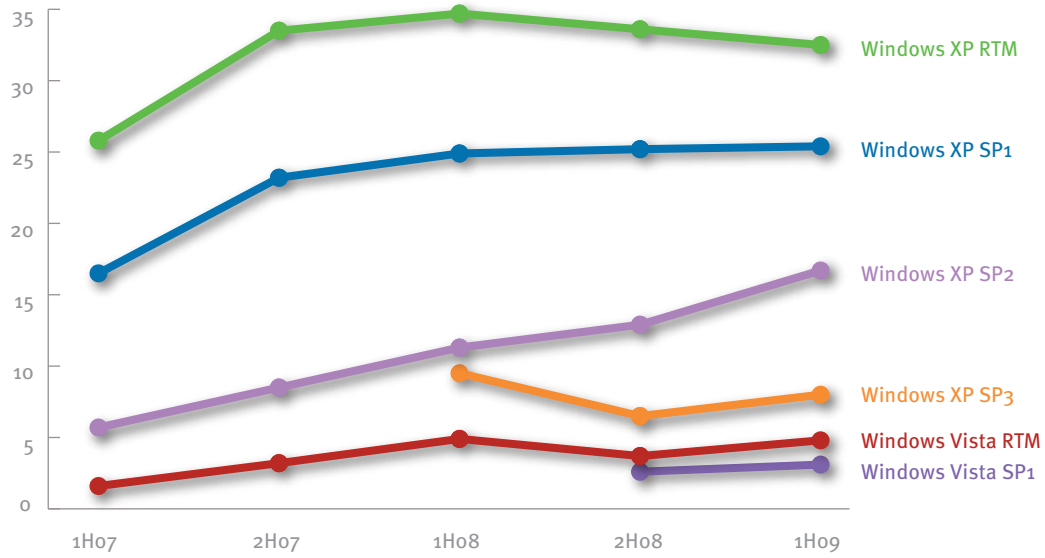
Infection rates for the 64-bit versions of Windows XP and Windows Vista are lower than for the corresponding 32-bit versions of those platforms, a difference that might be attributable to a higher level of technical expertise on the part of people who run 64-bit operating systems. This difference may be expected to decrease as 64-bit computing continues to make inroads among mainstream users. Microsoft's 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 difference between 32-bit and 64-bit Windows Vista is correspondingly lower than that of Windows XP SP2. Technical savvy is unlikely to be a contributing factor for system administrators deciding between 32-bit and 64-bit versions of server operating systems, and indeed the difference is negligible for both Windows Server 2003 and Windows Server 2008.

Figure 11 also shows that computers with more recent service packs installed have significantly lower infection rates than computers with older service packs (or the RTM release) for the same platform. This trend can be observed consistently across client and server operating systems. There are two likely reasons for this:

- 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.

Figure 12 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 1H09.

FIGURE 12. CCM trends for 32-bit versions of Windows Vista and Windows XP, 1H07–1H09



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 even as it has been adopted by larger segments of the computer-using population.

Malware and Potentially Unwanted Software Families

Figure 13 lists the top 25 malware and potentially unwanted software families that were detected on computers by Microsoft desktop security products in 1H09.

FIGURE 13. Top 25 malware and potentially unwanted software families detected by Microsoft anti-malware desktop products worldwide, by number of unique infected computers, in 1H09

	Family	Most Significant Category	1H09	2H08
1	Win32/Conficker	Worms	5,217,862	3,719
2	Win32/Taterf	Worms	4,911,865	1,916,446
3	Win32/Renos†	Trojan Downloaders & Droppers	3,323,198	4,371,508
4	Win32/ZangoSearchAssistant	Adware	2,933,627	3,326,275
5	Win32/Frethog	Password Stealers & Monitoring Tools	2,754,226	1,037,451
6	Win32/FakeXPA*	Miscellaneous Trojans	2,384,497	1,691,393
7	Win32/Vundo†	Miscellaneous Trojans	2,119,606	3,635,207
8	Win32/Alureon	Miscellaneous Trojans	1,976,735	510,281
9	Win32/ZangoShoppingreports	Adware	1,412,476	1,752,252
10	Win32/Agent	Miscellaneous Trojans	1,361,667	1,289,178
11	Win32/BaiduSobar	Misc. Potentially Unwanted Software	1,347,151	1,131,180
12	Win32/Hotbar	Adware	1,312,826	1,477,886
13	Win32/Zlob†	Miscellaneous Trojans	1,286,646	3,772,217
14	Win32/GameVance	Adware	1,225,802	360,813
15	Win32/Wintrim	Miscellaneous Trojans	1,222,446	—
16	ASX/Wimad	Trojan Downloaders & Droppers	1,167,389	1,168,724
17	Win32/Yektel*	Trojan Downloaders & Droppers	1,014,449	381,314
18	Win32/C2Lop†	Miscellaneous Trojans	815,897	597,105
19	Win32/Tibs	Miscellaneous Trojans	803,109	830,809
20	Win32/Bancos	Password Stealers & Monitoring Tools	748,038	738,667
21	Win32/Winwebsec*	Miscellaneous Trojans	719,240	91,396
22	Win32/SeekmoSearchAssistant	Adware	706,500	803,082
23	Win32/Small	Miscellaneous Trojans	673,034	276,347
24	Win32/Cutwail†	Trojan Downloaders & Droppers	642,501	412,686
25	Win32/Koobface†	Worms	640,964	—

(1H09 data for Conficker provided by the Shadowserver Foundation. Asterisks (*) indicate rogue security software families. Daggers (†) indicate families that have been observed to download rogue security software.)

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/FakeXPA: A rogue security software family that claims to scan for malware and then demands that the user pay to remove non-existent threats. Some variants unlawfully use Microsoft logos and trademarks.

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 products such as Win32/FakeXPA.

Win32/Winwebsec: A family of rogue security software programs that have been distributed with several different names. The user interface varies to reflect each variant's individual branding.

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

http://www.microsoft.com/av

For the most accurate possible estimate of the effect of the worm family Win32/Conficker, listed as the most prevalent family of 1H09, the figure given for 1H09 reflects the number of IP addresses infected by the A, B, C, and D variants that were detected on June 30, 2009, by sinkhole installations operated by the Shadowserver Foundation and the Conficker Working Group (CWG). For more information about Conficker and the worldwide response to the threat, see "Win32/Conficker Update," beginning on page 95, and "Case Study: The Conficker Working Group," beginning on page 29.

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. Three of the top 25 families—Win32/FakeXPA, Win32/Yektel, and Win32/Winwebsec—are rogue security software families, and a fourth, Win32/Renos, is often used as a delivery mechanism for rogue security software. Renos and FakeXPA are returnees from 2H08, when they ranked first and seventh respectively. Yektel and Winwebsec are newcomers to the list, having been added to the MSRT in December 2008 and May 2009, respectively. For more information about these threats, see "Win32/Conficker Update," on page 95.

Win32/Taterf and Win32/Frethog, ranked second and fifth respectively, belong to a group of loosely related families that target players of online games and attempt to steal their login credentials. Both families have increased in prevalence relative to 2H08, when they ranked fifth and thirteenth, respectively. For more information, see "Online Gaming-Related Families," on page 62 of *Microsoft Security Intelligence Report, Volume 5 (January through June 2008)*.

User Reaction to Alerts

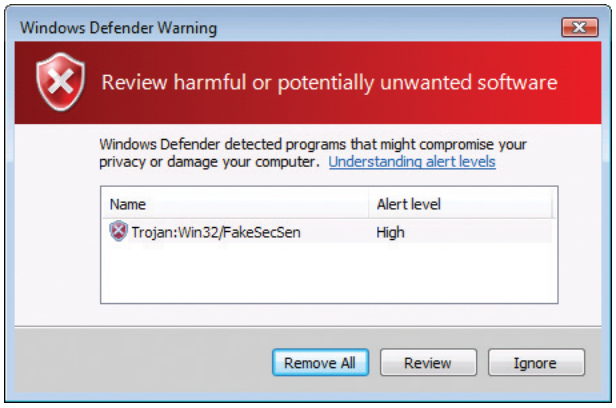
Software cannot always be classified in binary terms as "good" or "bad." Some software inhabits a gray area wherein the combination of behaviors and value propositions presented by the software is neither universally desired nor universally reviled. This gray area includes a number of programs that do things like display advertisements to the user that may appear outside the context of the Web browser or other application and which 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 eliminate false positives and help vendors satisfy the criteria for recategorization.

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. In addition, a choice of actions is given for each family, one of which may be listed as the default action:

- **Ignore**. Ignores the alert once. Users may choose to ignore an alert multiple times for the same piece of potentially unwanted software.
- **Allow** (or **Always Allow**). Adds the software to a list of allowed items so that the user is not prompted about it again. The user may choose to remove the software from the allowed items list in the future.
- **Prompt**. Prompts the user to make a decision about what to do with the software.
- **Quarantine**. Disables the software in such a way that it can be restored at a later point.
- **Remove**. Removes the software from the system. Threats rated with a severity of High or Severe are removed automatically during scheduled scans. 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.

FIGURE 14. A Windows Defender user action prompt for a threat rated High

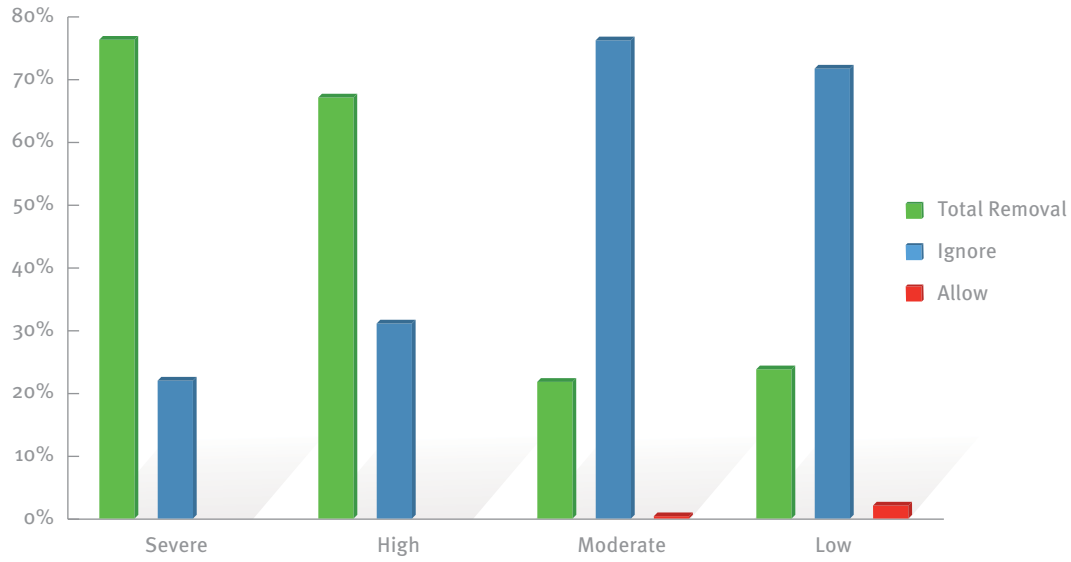


These decisions are influenced by a number of factors, such as the user's level of expertise, how certain they feel about their judgment regarding the software in question, the context in which the software was obtained, societal considerations, and the benefit (if any) being delivered by the software 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 **Ignore** 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 15 shows the actions users took in 1H09 in response to threats labeled Low, Moderate, High, and Severe.

FIGURE 15. User action by threat severity, 1H09



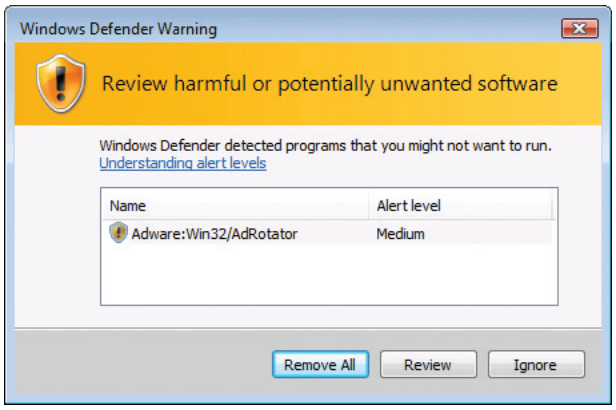
A few important points to keep in mind when interpreting Figure 15 and Figure 17 on page 57:

- "Total Removal" includes **Remove**, **Clean**, **Quarantine**, and cases in which a default removal action was performed (for example, if the user clicked the window's **Close** button without selecting an action).
- This figure does not include data for threats rated High and Severe that were 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 software, 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 Figure 14 illustrates, the user interface presents these threats in an unambiguously 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 pre-selected as the default choice.

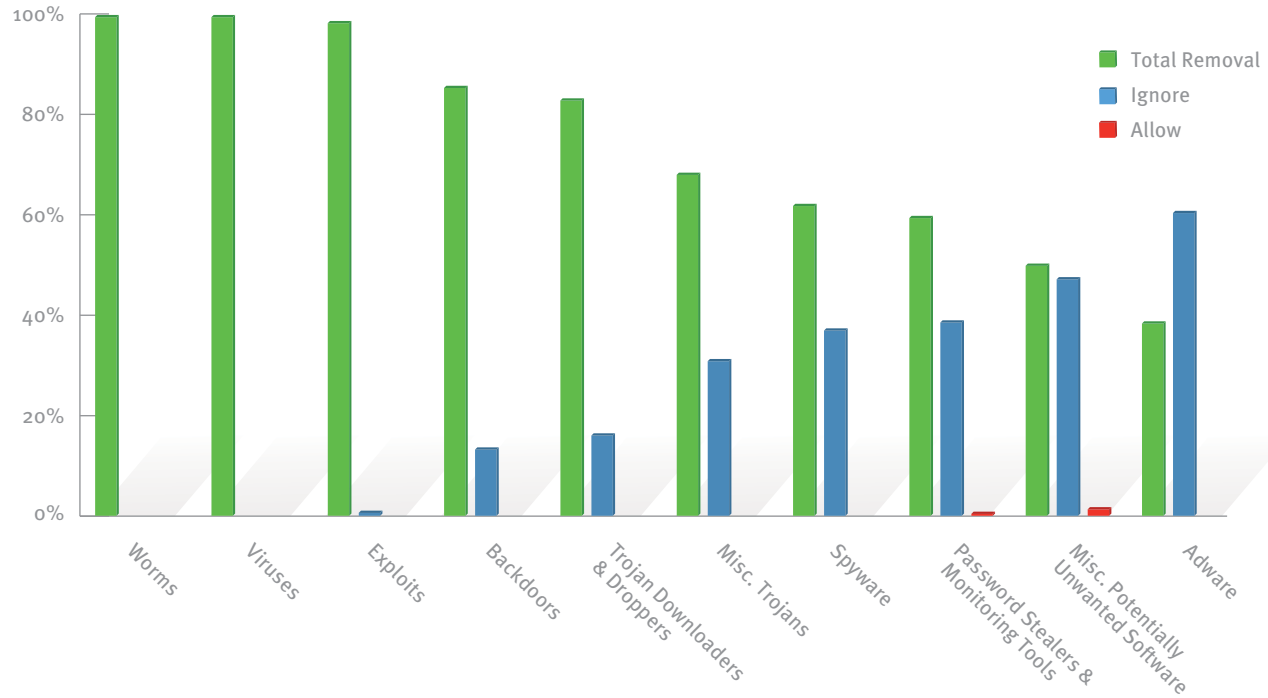
By contrast, users are more likely to choose **Ignore** when dealing with threats labeled Medium and Low. The user interface presents these threats with more nuanced graphics and descriptions than Severe and High threats, as seen in Figure 16. Medium and Low threats are associated with the color yellow, connoting caution rather than danger, and the descriptive text characterizes the detected software as something that the user simply "might not want to run."

FIGURE 16. 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 17.

FIGURE 17. User action by threat category, 1H09



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 are unwanted by some. Notably, **Allow** appears very infrequently in the data, accounting for no more than 1.5 percent of any category. Some users may not understand that an **Allow** option is available for software they want to keep, while others may prefer to ignore the alert, in some cases repeatedly, rather than take an action with more perceived finality.

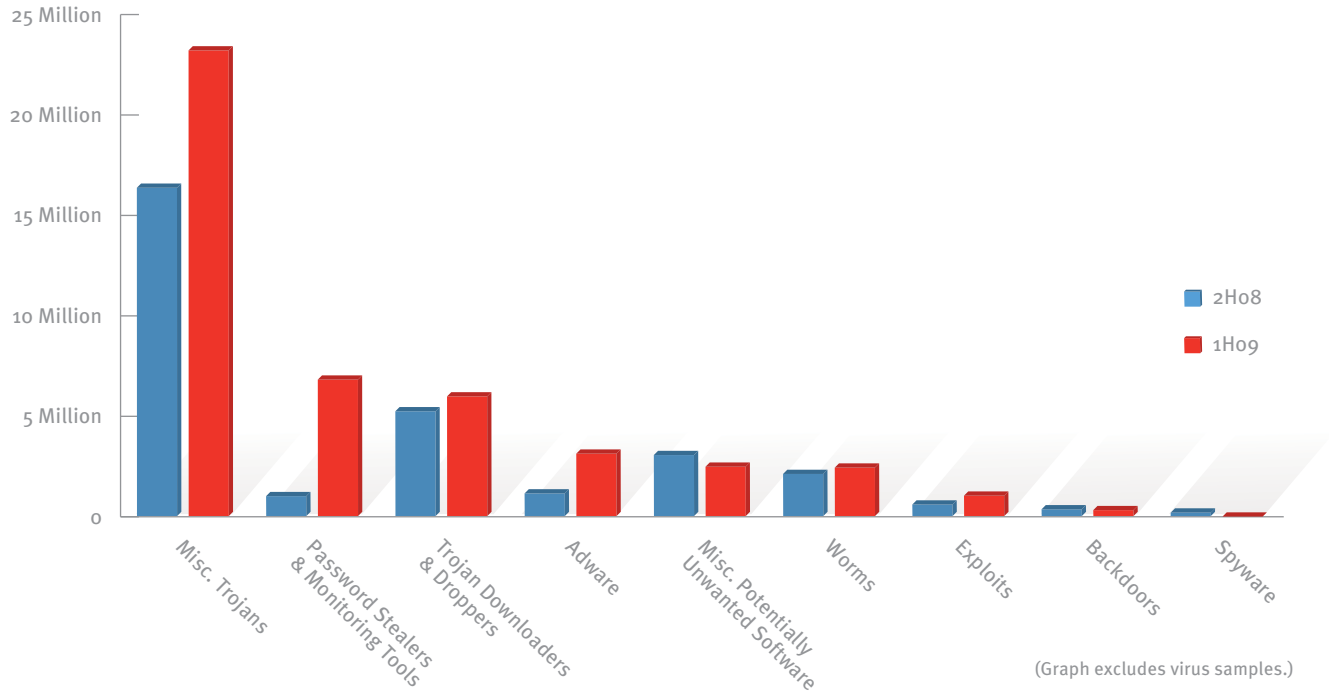
Trends in Sample Proliferation

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.

Nearly 116 million malicious samples were detected in the wild in 1H09. Figure 18 lists the number of unique files detected in each category of threat by Microsoft security products in 1H09, 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 18. Unique samples by category, 1H09 and 2H08

Category	1H09	2H08	Difference
Viruses	68,008,496	62,785,358	8.3%
Misc. Trojans	23,474,539	16,638,333	41.1%
Password Stealers & Monitoring Tools	7,087,141	1,287,106	450.6%
Trojan Downloaders & Droppers	6,251,286	5,511,400	13.4%
Adware	3,402,224	1,422,480	139.2%
Misc. Potentially Unwanted Software	2,753,008	3,332,059	-17.4%
Worms	2,707,560	2,391,722	13.2%
Exploits	1,311,250	869,023	50.9%
Backdoors	589,747	631,520	-6.6%
Spyware	269,556	116,966	130.5%
Total	**115,854,807**	**94,985,967**	**22.0%**



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 encrypting it in a slightly different way.

Figure 19 lists the families with the most unique detected samples in 1H09.

FIGURE 19. Families with more than 1 million unique samples detected in 1H09

Family	Most Significant Category	Total Samples	Total Reports	Reports/ Sample
Win32/Parite	Viruses	40,932,141	66,786,603	1.6
Win32/Virut	Viruses	15,217,839	31,000,119	2.0
Win32/Agent	Miscellaneous Trojans	6,720,422	10,236,876	1.5
Win32/Lolyda	Password Stealers & Monitoring Tools	5,671,251	8,293,764	1.5
Win32/Vundo	Miscellaneous Trojans	5,130,143	27,959,312	5.5
ASX/Wimad	Trojan Downloaders & Droppers	3,339,296	12,835,800	3.8
Win32/Sality	Viruses	3,154,368	6,495,955	2.1
Win32/Chir	Viruses	3,100,250	6,355,073	2.0
Win32/GameVance	Adware	2,785,395	10,263,113	3.7
Win32/Jeefo	Viruses	2,589,942	31,122,241	12.0
Win32/Wintrim	Miscellaneous Trojans	1,989,514	2,661,146	1.3
Win32/Alureon	Miscellaneous Trojans	1,911,121	6,084,014	3.2
Win32/C2Lop	Miscellaneous Trojans	1,866,617	3,859,760	2.1
Win32/FakeXPA	Miscellaneous Trojans	1,672,053	7,615,645	4.6
Win32/InternetAntivirus	Miscellaneous Trojans	1,398,088	4,998,427	3.6

The virus families Win32/Parite and Win32/Virut 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. The adware family Win32/GameVance produces a large number of samples because of unique configuration information that is created after the software is installed. Most of the other families on the list 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.

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 used exclusively 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 enterprise users.

During 1H09, Microsoft offered two products that provide real-time protection against malware and potentially unwanted software—Windows Live OneCare,[17] which is intended for home use, and Microsoft Forefront Client Security, which is intended for enterprise environments. Both of these products use the Microsoft Malware Protection Engine and a common signature set to provide protection against a large database of known threats, but they are typically deployed in very different environments. Comparing the threats encountered by Windows Live OneCare to those encountered by Forefront Client Security can provide insights into the different ways attackers target enterprise and home users and which threats are more likely to succeed in each environment.

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.

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.

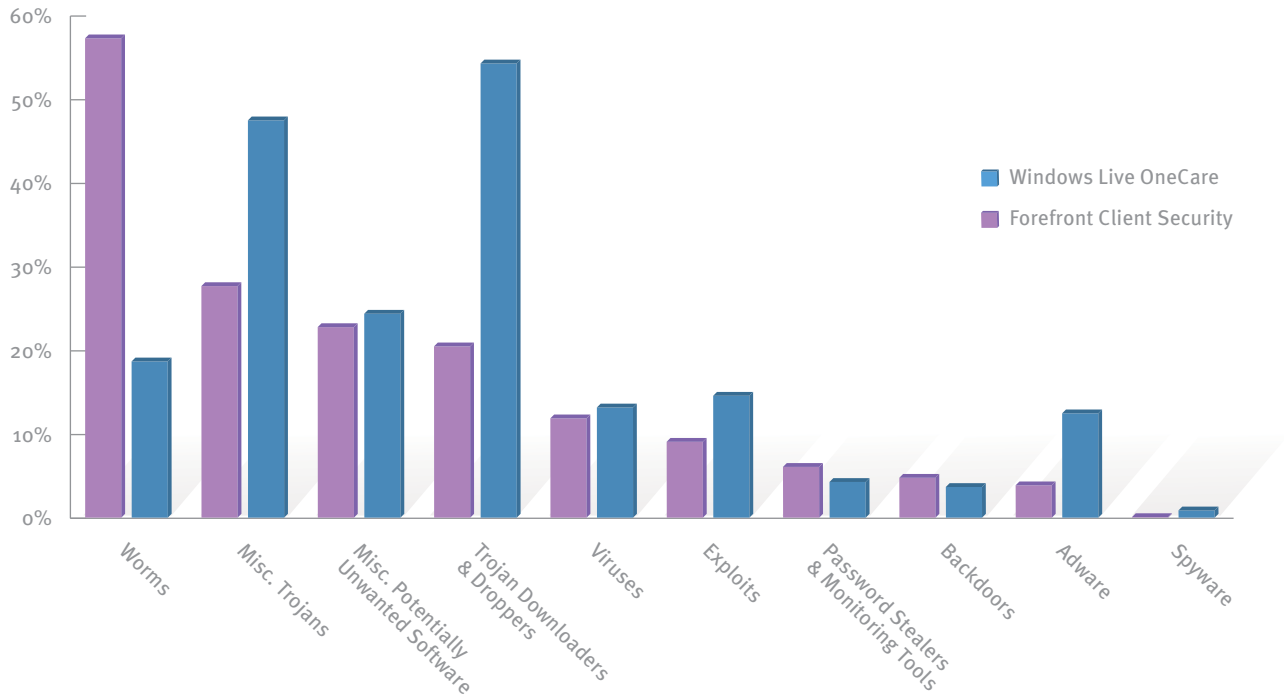
Win32/GameVance: Software that displays advertisements and tracks anonymous usage information in exchange for a free online gaming experience at the Web address "gamevance.com."

http://www.microsoft.com/av

[17] Microsoft discontinued retail sales of Windows Live OneCare on June 30, 2009, but continues to make virus definitions available to active subscribers. In 2H09, Microsoft is introducing a new, streamlined anti-malware solution, Microsoft Security Essentials, which will be made available at no charge to licensed users of Windows. See http://www.microsoft.com/security_essentials/ for details.

Figure 20 shows the relative prevalence of different categories of malware and potentially unwanted software on infected computers running Windows Live OneCare and Forefront Client Security in 1H09, expressed as a percentage of the total number of infected computers cleaned by each program. Totals exceed 100 percent for each program because some computers were cleaned of more than one category of families.

FIGURE 20. Threat categories detected by Windows Live OneCare and Forefront Client Security, by percentage of all infected computers cleaned by each program, in 1H09



As in 2H08, computers in enterprise environments (in other words, computers running Forefront Client Security) in 1H09 were much more likely to encounter worms than computers running Windows Live OneCare, while the systems running Windows Live OneCare encountered significantly greater percentages of trojans, adware, and exploits. Similar percentages of Password Stealers & Monitoring Tools, Miscellaneous Potentially Unwanted Software, Backdoors, and Spyware were detected by both products.

As Figure 21 and Figure 22 show, the top families encountered by Windows Live OneCare and Forefront Client Security were also very different.

FIGURE 21. Top 10 families detected on infected computers by Windows Live OneCare, by percentage of computers cleaned, in 1H09

Windows Live OneCare Top Families	Most Significant Category	Percent
ASX/Wimad	Trojan Downloaders & Droppers	10.3%
Win32/Agent	Miscellaneous Trojans	7.4%
Win32/Renos	Miscellaneous Trojans	5.0%
Win32/Obfuscator	Misc. Potentially Unwanted Software	3.4%
Win32/Pdfjsc	Exploits	3.0%
Win32/Xilos	Viruses	2.9%
Win32/Swif	Trojan Downloaders & Droppers	2.3%
Win32/Alureon	Miscellaneous Trojans	2.3%
Win32/FakeXPA	Miscellaneous Trojans	2.2%
Win32/Autorun	Worms	1.9%

FIGURE 22. Top 10 families detected on infected computers by Forefront Client Security, by percentage of computers cleaned, in 1H09

Forefront Client Security Top Families	Most Significant Category	Percent
Win32/Conficker	Worms	12.3%
Win32/Autorun	Worms	6.6%
Win32/Hamweq	Worms	5.9%
Win32/Agent	Miscellaneous Trojans	5.1%
Win32/Taterf	Worms	3.9%
Win32/Obfuscator	Misc. Potentially Unwanted Software	1.9%
Win32/Renos	Miscellaneous Trojans	1.7%
Win32/RealVNC	Password Stealers & Monitoring Tools	1.6%
Win32/Sality	Viruses	1.6%
AutoIt/Renocide	Worms	1.4%

The malware most encountered by Windows Live OneCare was ASX/Wimad, a detection for a category of malicious Windows Media files. In general, threats involving media files are far more likely to be encountered on home computers, which are presumably more likely to be used to play music and video content from a wide variety of sources than computers in the workplace. Likewise, Win32/Swif is a trojan that exploits a vulnerability in Adobe® Flash Player, which is often used to play multimedia content.

Encyclopedia

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/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.

http://www.microsoft.com/av

Encyclopedia

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

Win32/FakeXPA: A rogue security software family that claims to scan for malware and then demands that the user pay to remove non-existent threats. Some variants unlawfully use Microsoft logos and trademarks.

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

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.

http://www.microsoft.com/av

The Windows Live OneCare list also includes several malware families associated with rogue security software, such as Win32/Renos and Win32/FakeXPA. 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 Still a Significant Threat," on page 100.

By contrast, the Forefront Client Security list is dominated by worms, like Win32/Conficker, Win32/Hamweq, and Win32/Taterf. Worms rely less on social engineering to spread than threats like trojans and downloaders do and more on access to unsecured file shares and removable storage volumes—both of which are often plentiful in enterprise environments. Conficker, in particular, uses several methods of propagation that work more effectively within a firewalled network environment than over the public Internet. (For more information, see "Win32/Conficker Update," on page 95.)

The worm family Taterf is an interesting case. It targets massively multiplayer online role-playing games, which are not common in the workplace, but the techniques it employs (such as infecting removable drives) make it spread more effectively in enterprise environments. Win32/RealVNC is a program that enables a computer to be controlled remotely, similar to Remote Desktop. It has a number of legitimate uses, but it can also be used by an attacker with malicious intent to gain control of a user's computer under some circumstances.

Families appearing on both lists include Renos and Win32/Autorun. Autorun is a family of worms that spread by copying themselves to the mapped drives of an infected computer, including network shares and removable storage volumes. As noted earlier, such resources are common in enterprise environments and, consequently, Autorun is detected much more often in enterprise environments than on home computers.

Malware and Signed Code

Microsoft Authenticode® is a technology that can help ensure the source of code. It does not ensure that code is safe to run, but it can ensure that the code is associated with an entity in a trust chain.[18]

Authenticode certificates are issued by Certificate Authorities (CAs), such as VeriSign (http://www.verisign.com), Comodo (http://www.comodo.com), or GlobalSign (http://www.globalsign.com). CAs are responsible for verifying the identities of the entities to whom they issue certificates. After a CA issues a certificate to an entity, that entity uses a private key to individually sign files. Any tampering or modification of the file or certificate invalidates the signature. Microsoft works closely with CAs to monitor the certificates issued to software vendors, particularly when malware is detected.

[18] For more information on Authenticode and code-signing, see http://msdn.microsoft.com/en-us/library/ms537361.aspx.

Code signing is a powerful method of authoritatively identifying code, assuring its integrity at the time of signing and the identity of the code signer. Signed code can be much easier to research and analyze because of the greater certainty of the association of the signer with the file. For this reason, anti-malware vendors are among the most diligent code signers. This assertion of identity also scales very well—a few code-signing certificates positively identify millions of genuine Microsoft files. Signing also enables features, like 64-bit Windows Vista Kernel Mode Driver Signing, that can help improve security by enforcing a code-signature requirement and helping to prevent unsigned drivers from being modified and loaded. System administrators can use the Software Restriction Policies feature of Windows Server 2003 and Windows Server 2008 to restrict users to applications assigned by approved publishers. AppLocker™, a key feature of Windows 7 and Windows Server 2008 R2, takes this concept a step farther, allowing more flexible rules based on individual digital certificate attributes and other criteria.

Certificates on Detected Files

In theory, malicious code can be code signed in a number of ways. A legitimate publisher could sign malicious code mistakenly, private keys issued to legitimate entities could be stolen and used to sign code, or malware authors can be issued a certificate by a CA. The MMPC has not confirmed any cases of private keys being stolen and used on detected code nor has it confirmed any cases of mistaken signing by a legitimate entity, but it has confirmed many cases of CAs issuing code-signing certificates to malware authors. This usually results when CAs participating in the Microsoft Root Certificate Program issue code-signing certificates to a software publisher who uses the certificate to sign malware. In some cases, the CA is owned and operated by the malware authors, and the first step in infection is tricking users into installing a root certificate. In most cases, though, CAs participating in the Microsoft Root Certificate Program are tricked into issuing a valid certificate to the malware author.

In the first six months of 2009, the MMPC received reports of 3.3 million distinct malware and potentially unwanted software files with valid code signatures, compared to 113 million instances of distinct detected files that were not signed. Of these 3.3 million, 3.1 million were signed by two entities, with the remaining 157,000 code-signed files split between 260 different entities. Fortunately, the majority of certificates used by threats with alert classifications of Severe and High have been revoked by the CAs that issued them. (See "User Reaction to Alerts," beginning on page 54, for more information about alert classification.)

In addition, more than 34,000 virus-infected files with invalid code signatures were reported over 178,000 times. When a virus infects a valid code-signed file, it invalidates the signature.

As a general rule, code-signed threats produce fewer individual unique samples than unsigned files, but each unique sample tends to be reported more often. Aside from the additional expense and effort it takes to create code-signed threats, client-side polymorphism—one of the principal factors that causes threats to generate large numbers of unique samples—cannot be effectively implemented by code-signed malware because it invalidates the digital signature.

FIGURE 23. The 10 families responsible for the most signed-code threat reports in 1H09

Family	Most Significant Category	% of Signed Threat Files	% of Signed Threat Reports
Win32/Hotbar	Adware	0.0%	31.3%
Win32/ZangoSearchAssistant	Adware	0.0%	23.4%
Win32/ZangoShoppingReports	Adware	0.0%	17.1%
Win32/Pointfree	Misc. Potentially Unwanted Software	0.3%	4.7%
Win32/BaiduSobar	Misc. Potentially Unwanted Software	0.0%	3.7%
Win32/Wintrim	Miscellaneous Trojans	52.8%	3.3%
Win32/SeekmoSearchAssistant	Adware	0.0%	2.5%
Win32/RealVNC	Misc. Potentially Unwanted Software	0.0%	1.9%
Win32/GameVance	Adware	29.7%	1.9%
Win32/WinFixer	Misc. Potentially Unwanted Software	0.1%	0.7%

The MMPC's standard practice when encountering code-signed malware spreading in the wild is to create detection signatures for the malware and to contact the issuing CA with details of the file in question, so the CA can review the issued certificate to determine if any action is needed. CAs maintain Certificate Revocation Lists (CRLs) on the Internet, which list mistakenly issued, abused, or other problem certificates. Software like Windows Internet Explorer 8 attempts to check CRLs when verifying code signing of any downloaded code.

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.[19]
- Trojan downloaders and droppers, which were found on 20.4 percent of infected computers in 1H09, 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.

Web-Based Malware Distribution Networks

Malware found on the Web often downloads other malware. These malware distribution networks can be simple or complex. 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.

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

Figure 24 and Figure 25 show category breakdowns for parent threats (threats that downloaded others) and child threats (threats that were downloaded by others), respectively.

FIGURE 24. Threats that downloaded other threats, by category, in 1H09

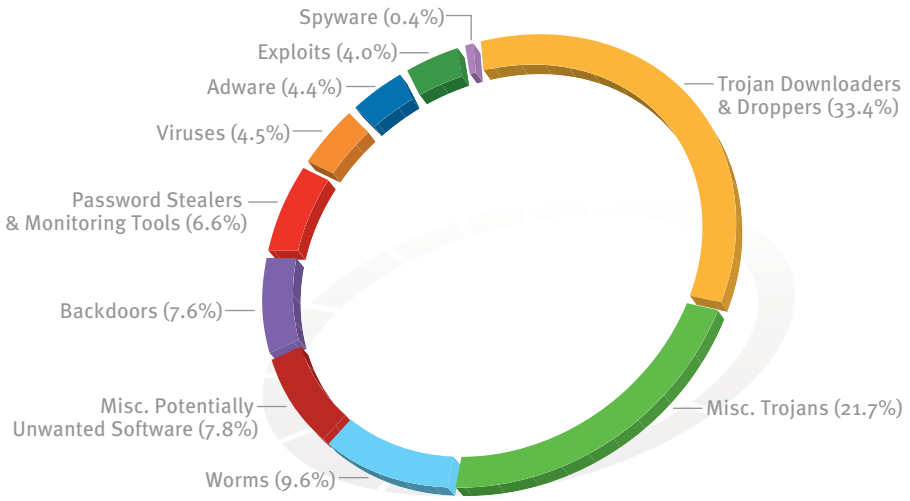
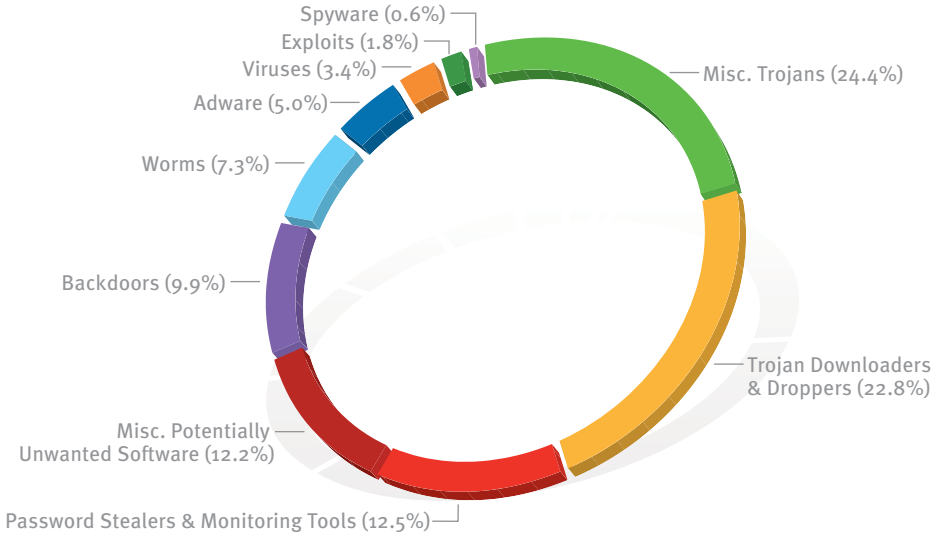


FIGURE 25. Threats that were downloaded by other threats, by category, in 1H09

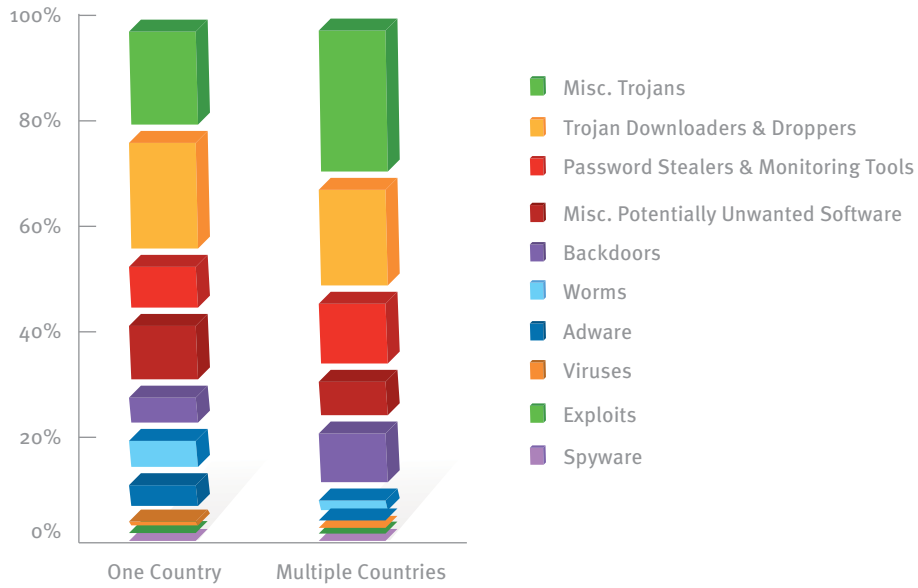


As might be expected, threats in the Trojan Downloaders & Droppers category were observed to download the most threats, followed by Miscellaneous Trojans. Altogether, trojans were responsible for more than half of parent threats and nearly half of child threats. Notably, downloaders and droppers also 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).

Notably, the category breakdown for parent threats is roughly similar to that of child threats, with the significant exception of Password Stealers & Monitoring Tools, which were used as child threats significantly more often than parent threats. Whereas threats such as trojans, worms, and backdoors are often used as a means of compromising computers for other purposes, attackers are more likely to use password stealers directly in service of a goal, in this case to steal sensitive information from victims.

An examination of the individual threat families that are downloaded from malicious URLs embedded in malware reveals that more than a third of them (36.2 percent) are available from URLs hosted in multiple countries. Threats hosted in multiple countries are significantly more likely to be served from compromised computers (such as computers in a botnet) than threats hosted in a single country and significantly less likely to be hosted on servers the attacker controls through consensual hosting arrangements.

FIGURE 26. Breakdown of threats hosted in one country and in multiple countries, by category, in 1H09



As Figure 26 shows, the category breakdown of single-country threats is largely similar to that of multiple-country threats, with a few notable exceptions. Most significantly, adware is responsible for a much larger percentage of single-country families (7.4 percent) than of multiple-country threats (0.9 percent). Many adware families are installed by choice or bundled with other applications, and therefore do not require surreptitious or illicit hosting arrangements like other families do.

Families Often Found Together

Examining some of the more commonly encountered threat combinations can provide insights into the nature of these malware distribution networks. The next several tables show the families that are most often found alongside a sample of currently prevalent threats of different types.

Figure 27 lists the other threats most often detected on computers infected with Win32/InternetAntivirus, a prevalent new rogue security software family.

FIGURE 27. Other threats found on computers infected with Win32/InternetAntivirus

Other Family	Most Significant Category	Percent of Win32/Internet Antivirus-Infected Computers
Win32/Chadem	Password Stealers & Monitoring Tools	27.5%
Win32/Renos	Trojan Downloaders & Droppers	18.8%
Win32/FakeIA	Miscellaneous Trojans	16.9%

Like most rogue security software, Win32/InternetAntivirus is heavily dependent on social engineering to spread. Misleading victims into paying for worthless software is the usual method by which attackers make money with rogue security software, and InternetAntivirus is no different, displaying warnings about a number of nonexistent threats on the user's computer and offering to remove them for a price. In addition to typical rogue security software behavior, however, InternetAntivirus also downloads a password stealer, Win32/Chadem, when installed. Chadem monitors network traffic on the affected computer and attempts to steal user names and passwords for File Transfer Protocol (FTP) sites. The attacker uses the captured credentials to compromise servers and use them to host malware. Chadem was found on 27.5 percent of the computers that were infected with InternetAntivirus, more than any other family.

Other families frequently encountered on computers infected with InternetAntivirus include Win32/FakeIA, another rogue security software family, and Win32/Renos, a downloader that itself is often used to install rogue security software-related families.

Encyclopedia

Win32/FakeIA: A rogue security software family that impersonates the Windows Security Center. It may display product names or logos in an apparently unlawful attempt to impersonate Microsoft products.

http://www.microsoft.com/av

Figure 28, Figure 29, and Figure 30 list the other threats most often detected on computers infected with three different spambots: Win32/Cutwail, Win32/Rustock, and Win32/Waledac.

FIGURE 28. Other threats found on computers infected with Win32/Cutwail in 1H09

Other Family	Most Significant Category	Percent of Win32/Cutwail-Infected Computers
Win32/Renos	Trojan Downloaders & Droppers	16.4%
Win32/Rustock	Backdoors	11.4%

FIGURE 29. Other threats found on computers infected with Win32/Rustock in 1H09

Other Family	Most Significant Category	Percent of Win32/Rustock-Infected Computers
Win32/Cutwail	Trojan Downloaders & Droppers	12.6%
Win32/Vundo	Miscellaneous Trojans	11.0%
Win32/Renos	Trojan Downloaders & Droppers	10.9%

FIGURE 30. Other threats found on computers infected with Win32/Waledac in 1H09

Other Family	Most Significant Category	Percent of Win32/Waledac-Infected Computers
Win32/Tibs	Miscellaneous Trojans	16.3%
Win32/Alureon	Miscellaneous Trojans	12.2%
Win32/Cutwail	Trojan Downloaders & Droppers	9.9%

An infected computer can belong to several different botnets, which overlap to varying degrees. As these figures show, each spambot was detected alongside at least one other spambot with relative frequency. Win32/Renos also appears alongside Cutwail and Rustock with relative frequency, which may be attributable more to the overall prevalence of Renos than to any connection between it and the other two families.

For more information about Waledac, a threat that has become significantly more prevalent in 1H09, see "The Win32/Waledac Botnet and Spam," on page 104.

Encyclopedia

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

Win32/Rustock: A multicomponent family of rootkit-enabled backdoor trojans, developed to aid in the distribution of spam. Recent variants appear to be associated with rogue security software.

Win32/Waledac: A trojan that is used to send spam. It also has the ability to download and execute arbitrary files, harvest e-mail addresses from the local machine, perform denial-of-service attacks, proxy network traffic, and sniff passwords.

http://www.microsoft.com/av

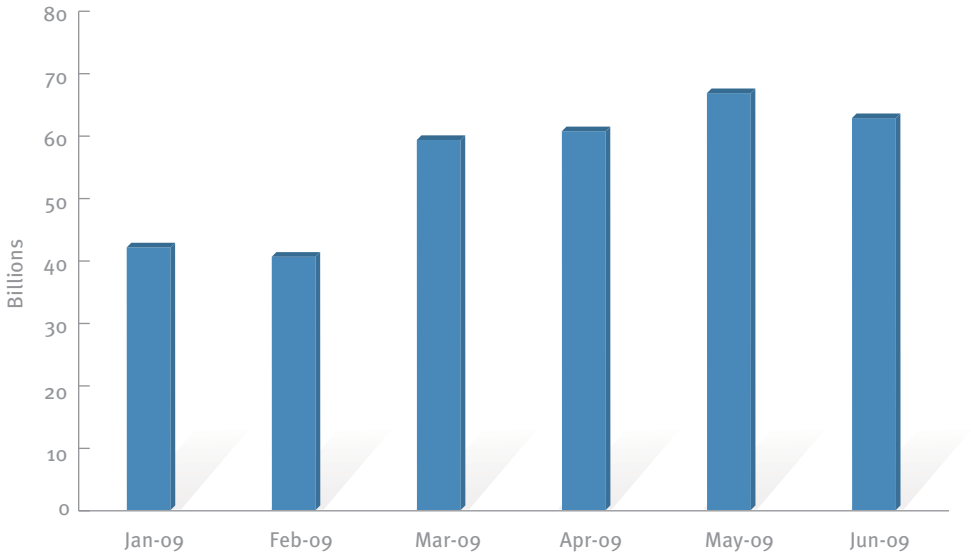
E-Mail Threats

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 82, includes more information about phishing in particular.)

Spam Trends and Statistics

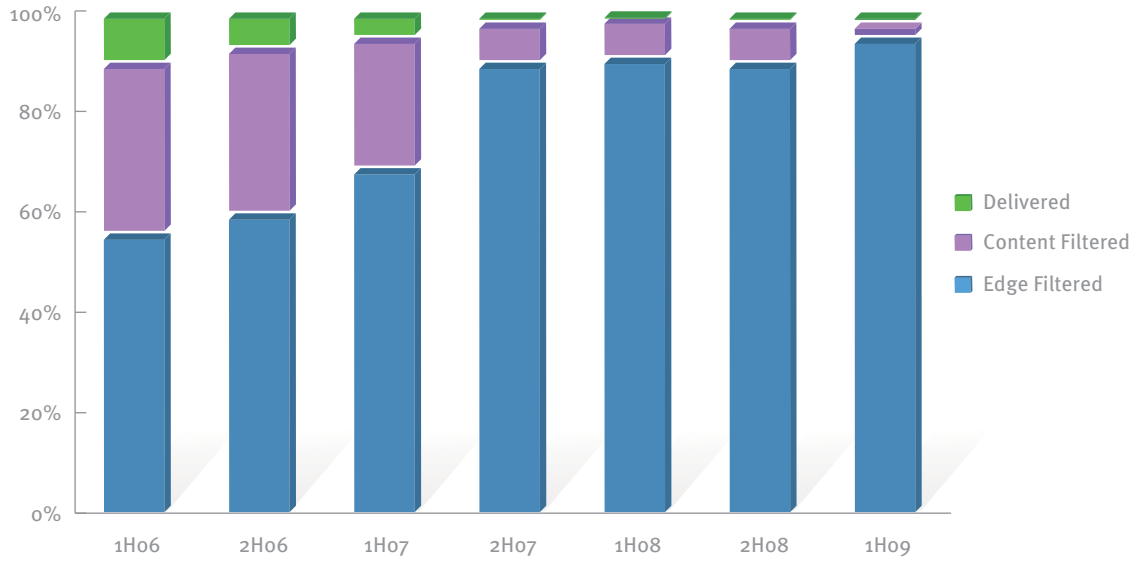
Microsoft Forefront Online Protection for Exchange (FOPE; formerly Forefront Online Security for Exchange, or FOSE) provides enterprise-class spam and malware filtering services for thousands of customers. FOPE performs spam filtering in two stages. The vast majority of spam is blocked by servers at 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 31. Incoming messages blocked by FOPE each month in 1H09



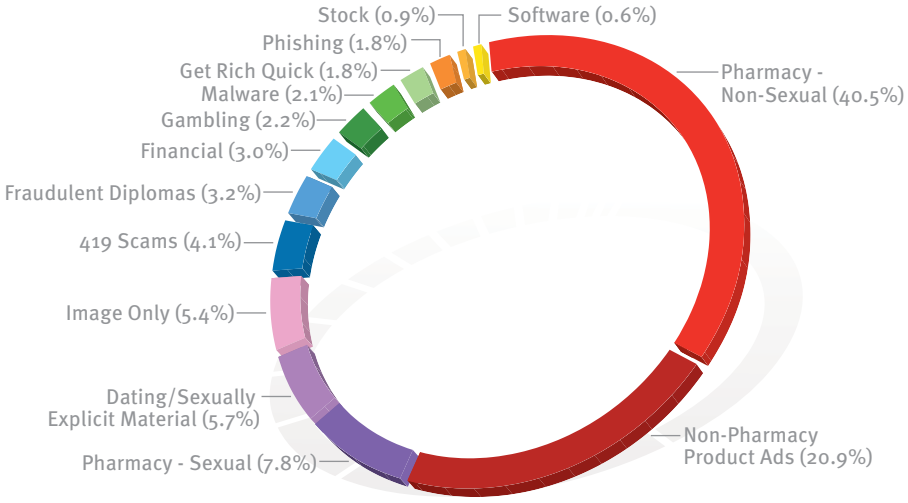
In 1H09 overall, FOPE blocked about 97.3 percent of all unwanted messages at the network edge, compared to 92.2 percent in 2H08. As Figure 32 demonstrates, the effectiveness of edge-filtering techniques, such as IP address reputation checking, SMTP connection analysis, and recipient validation, have 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 32. Percentage of incoming messages blocked by FOPE using edge-blocking and content filtering, 1H06–1H09



As in previous periods, spam in 1H09 was dominated by product advertisements, primarily for pharmaceutical products. Figure 33 shows the subject category breakdown for the messages blocked by the FOPE content filters during 1H09.

FIGURE 33. Inbound messages blocked by FOPE content filters, by category, in 1H09



Advertisements for pharmaceutical products accounted for 48.3 percent of the spam messages blocked by FOPE content filters in 1H09, with advertisements for sexual performance products accounting for 7.8 percent of the overall total. Together with non-pharmacy product ads (20.9 percent of the total), product advertisements accounted for 69.2 percent of spam 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 5.4 percent of the total in 1H09.

Overall, the category breakdown for spam in 1H09 is very similar to that observed during 2H08, with no single category increasing or decreasing by more than 2.7 percent of the overall total. 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.

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 34 shows the countries/regions around the world that sent the most spam, as detected by FOPE from March through June 2009.

FIGURE 34. Locations sending the most spam messages, March–June 2009

Rank	Country/Region	Spam Messages Sent
1	United States	448,089,809
2	China	150,066,661
3	South Korea	137,911,376
4	Brazil	68,195,970
5	Argentina	35,791,082
6	Russia	35,695,413
7	Spain	31,411,007
8	United Kingdom	30,781,792
9	Poland	27,964,107
10	Japan	27,203,794
11	Canada	25,624,928
12	Romania	24,868,889

Rank	Country/Region	Spam Messages Sent
13	Czech Republic	21,881,505
14	India	21,483,789
15	Italy	20,886,430
16	France	19,716,403
17	Germany	18,684,483
18	Turkey	17,750,814
19	Bulgaria	15,420,482
20	Chile	14,712,649
21	Australia	14,666,998
22	Netherlands	13,601,095
23	Colombia	11,731,721
24	Ukraine	10,874,301
25	Taiwan	10,289,608

FIGURE 35. Geographic origins of spam, by percentage of total spam sent, in 1H09

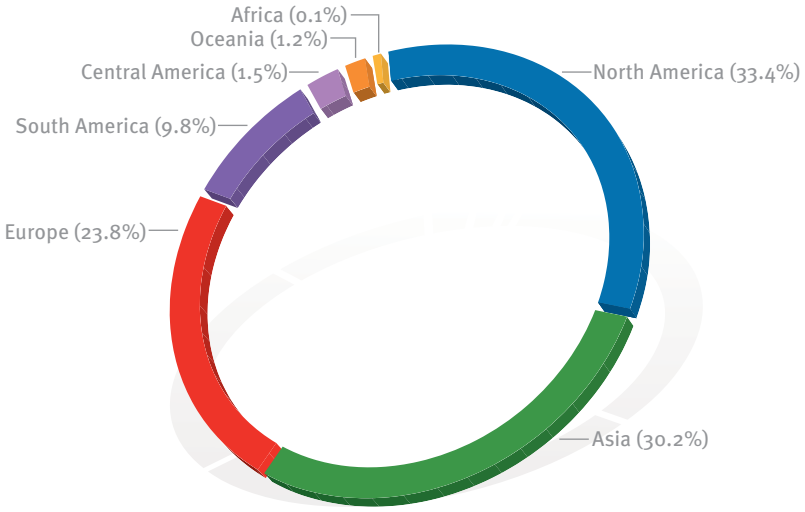
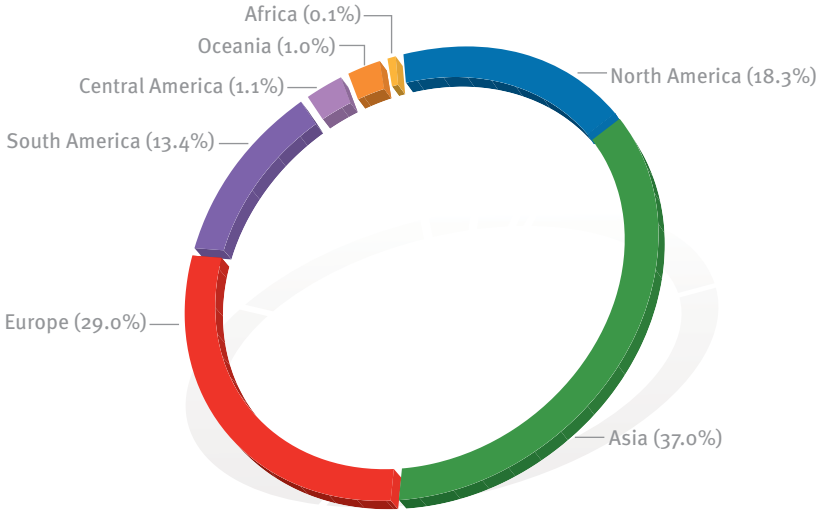


FIGURE 36. Geographic origins of spam, by percentage of all distinct IP addresses sending spam, in 1H09



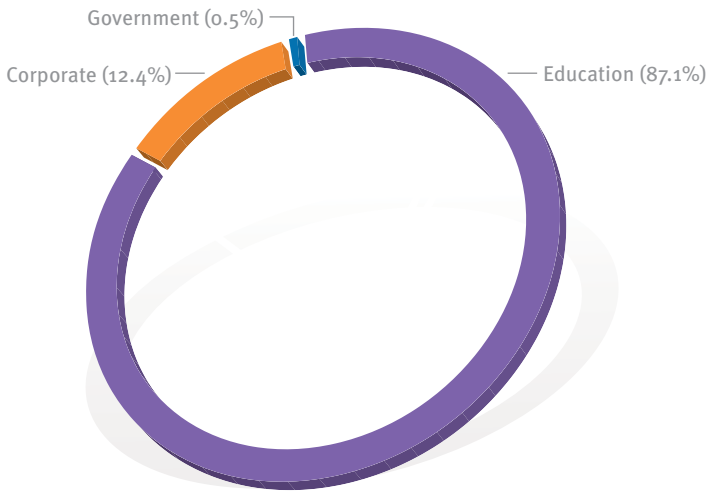
Reputation Hijacking

The spam-filtering algorithms used by large e-mail processors like FOPE typically take reputation into account when processing incoming messages—a message originating from a source with a good reputation is considered significantly less likely to be spam than a message originating from a poorly regarded or unknown source. Most spam is sent through botnets or from IP address ranges that are known to be used by spam operations. Services like FOPE typically block messages originating from sources like these automatically, at the network edge.

Recent periods have seen a rise in spam originating from sources with good reputations, a tactic called *reputation hijacking*. To increase the likelihood that their messages will be seen, spammers look for ways to compromise computers and e-mail servers hosted by organizations with good reputations, such as schools, government departments, and legitimate corporations. For example, spam that originates from an infected computer at a well-known corporation and is relayed through the company's outbound IP address is significantly more likely to be seen by its recipients than spam sent directly from a dynamic IP address assigned to a large home broadband provider (a telltale indicator of botnet activity).

To help its customers maintain safe networks, FOPE monitors the amount of outbound spam sent through its service by tracking complaints from a number of third-party feedback loop sources, including Hotmail, AOL, Comcast, SpamCop, and Yahoo!. As Figure 37 shows, educational institutions are the source of most spam sent through FOPE, by a wide margin, despite accounting for a relatively small portion of FOPE's customer base. Whereas computers in corporate and government settings are usually centrally managed by the IT department, the computing environments at educational institutions often include student-owned computers in dormitories and other living spaces, many of which may not have adequate malware protection.

FIGURE 37. Outbound spam sent through FOPE, by type of organization, in 1H09



Spammers also seek to hijack the reputations of large, Web-based e-mail services, such as Windows Live Hotmail®, AOL, Google's Gmail, and Yahoo!. These services use a number of techniques to prevent spammers from sending large amounts of spam from their domains, so their reputations are generally quite good. Like a number of other e-mail protection services, FOPE does not block messages from these four providers at the network edge. All messages verified as originating from AOL, Gmail, Hotmail, or Yahoo! are subjected to content-based filtering only.

Despite recent increases in reputation hijacking, the majority of the messages originating with these four services are legitimate, by a significant margin. AOL, Gmail, Hotmail, and Yahoo! accounted for 15.1 percent of all mail processed by FOPE's content filters in 1H09 but just 1.6 percent of post-edge spam. Collectively, 8.9 percent of messages sent through the four services were spam, with percentages for individual services ranging from 3.7 percent on the low end to 19.6 percent on the high end.

Malware in E-Mail

Massive malware outbreaks driven by malicious e-mail attachments are rarer today than they have been in the past, in part because popular e-mail providers, such as Windows Live Hotmail, and enterprise services, like FOPE, typically offer anti-malware services in addition to spam filtering. "Threats at Home and in the Enterprise," beginning on page 61, describes why the threats that are most prevalent in enterprise environments are often very different than the threats that most commonly affect home computer users. Comparing the threats detected and removed from e-mail messages by the anti-malware features of FOPE and Hotmail demonstrates that these differences extend to e-mail, as well.

Figure 38 and Figure 39 show the top 10 threats detected and removed by the anti-malware features of FOPE and Hotmail, respectively.

FIGURE 38. Top 10 families detected in e-mail by Forefront Online Protection for Exchange, by percentage of all infected messages, in 1H09

Rank	FOPE Families	Most Significant Category	Percent
1	Win32/Small	Trojan Downloaders & Droppers	39.1%
2	Win32/Virut	Viruses	10.3%
3	Win32/Zbot	Password Stealers & Monitoring Tools	8.5%
4	Win32/DelfInject	Miscellaneous Potentially Unwanted Software	4.3%
5	Win32/Provis	Miscellaneous Trojans	3.4%
6	Win32/VB	Miscellaneous Trojans	3.1%
7	Win32/Prolaco	Worms	2.9%
8	Win32/Netsky	Worms	2.6%
9	Win32/Mydoom	Worms	2.3%
10	Win32/Autorun	Worms	2.1%

Encyclopedia

Win32/Netsky: A mass-mailing worm that spreads by e-mailing itself to addresses found on an infected computer. Some variants contain a backdoor component and perform DoS attacks.

Win32/Mydoom: A family of mass-mailing worms that spread through e-mail. Some variants also spread through P2P networks. Bagle acts as a backdoor trojan and can sometimes be used to launch DoS attacks against specific Web sites.

Win32/Mywife: A mass-mailing network worm that targets certain versions of Microsoft Windows. The worm spreads through e-mail attachments and writeable network shares. It is designed to corrupt the content of specific files on the third day of every month.

W97M/Melissa: A macro worm that spreads via e-mail and by infecting Word documents and templates. It is designed to work in Word 97 and Word 2000, and it uses Outlook to reach new targets through e-mail.

VBS/LoveLetter: A family of mass-mailing worms that targets computers running certain versions of Windows. It can spread as an e-mail attachment and through an IRC channel. The worm can download, overwrite, delete, infect, and run files on the infected computer.

http://www.microsoft.com/av

FIGURE 39. Top 10 families detected in e-mail by Windows Live Hotmail, by percentage of all infected messages, in 1H09

Rank	Windows Live Hotmail Families	Most Significant Category	Percent
1	JS/Redirector	Miscellaneous Trojans	10.4%
2	Win32/Netsky	Worms	8.1%
3	Win32/Mabezat	Virus	4.7%
4	Win32/Helpud	Miscellaneous Trojans	3.9%
5	Win32/Rochap	Trojan Downloaders & Droppers	3.5%
6	Win32/Agent	Miscellaneous Trojans	2.6%
7	Win32/Gamania	Password Stealers & Monitoring Tools	2.3%
8	ASX/Wimad	Trojan Downloaders & Droppers	2.2%
9	Win32/Mydoom	Worms	2.2%
10	Win32/Mywife	Worms	2.1%

Unsurprisingly, mass-mailing worms appear prominently in both lists, including years-old threats like Win32/Netsky (first detected in 2004), Win32/Mydoom (first detected in 2004), and Win32/Mywife (first detected in 2005). Several of these threats spread by infecting older e-mail programs and sending copies of themselves to e-mail addresses on the victims' computers, so reputation filters are less likely to block them at the network edge than some more modern threats.

Several of the "families" on both lists are actually generic detections, which the malware protection engine uses to detect groups of related or similar threats. Win32/Small, the threat detected most often by FOPE, is a generic detection that targets a large number of simple threats, most of which have small file sizes. JS/Redirector, the threat detected most often by Hotmail, is a detection for a malicious JavaScript technique, frequently used by spammers, that redirects users to unexpected Web sites.

Social Engineering and E-Mailed Threats

Dating back to early worms like W97M/Melissa and VBS/LoveLetter, attackers who distribute malware through files attached to e-mail messages have always relied heavily on social engineering to convince people to open malicious attachments. Popular e-mail services, like Windows Live Hotmail, provide protection against such threats by scanning attachments for malware when they are downloaded or uploaded. Differences in the way Hotmail has implemented this protection for different access methods provide an interesting look at the relative effectiveness of the social engineering messages associated with particular threats and threat categories.

Windows Live Hotmail users primarily access their e-mail through two different methods—by visiting the service's Web interface at http://www.hotmail.com using a Web browser, and by synchronizing their messages with a client program installed on the user's computer or mobile device. Hotmail scans all attachments for malware when they are delivered to desktop and mobile clients through synchronization, to protect users who may not have anti-malware software installed on their computers or devices. When a user of the Web-based client receives a message with an attachment, however, Hotmail does not scan the attachment until and unless the user chooses to download the attached file. If the user deletes the message without downloading the attachment, they are never exposed to the malicious file, so it does not need to be scanned. Although fewer users access Hotmail through synchronized clients than through the Web interface, synchronized messages accounted for nearly twice as many malware detections in 1H09 as did Web-delivered messages.

Malicious attachments detected through synchronization may be considered a control group because all such attachments are scanned regardless of whether users choose to open them. By contrast, malicious attachments in messages accessed through the Hotmail Web client are only likely to be detected if the user makes a conscious choice to download them—in other words, if the social engineering message has succeeded. A malware family or category that tends to be distributed with effective social engineering tactics is, therefore, likely to appear with greater relative frequency among Web client detections than among desktop and mobile client detections, whereas the opposite is true of malware distributed with ineffective social engineering tactics.

Breaking down the top 10 families detected by Hotmail in 1H09 by access method illustrates how some social engineering tactics are more effective than others.

FIGURE 40. Top 10 malware families detected by Windows Live Hotmail, by method of access, in 1H09

Family	Most Significant Category	Desktop & Mobile Client Percent	Web Client Percent	Total Percent
JS/Redirector	Miscellaneous Trojans	15.3%	1.1%	10.4%
Win32/Netsky	Worms	10.8%	3.0%	8.1%
Win32/Mabezat	Virus	6.7%	0.9%	4.7%
Win32/Helpud	Miscellaneous Trojans	3.2%	5.3%	3.9%
Win32/Rochap	Trojan Downloaders & Droppers	1.3%	7.7%	3.5%
Win32/Agent	Miscellaneous Trojans	1.6%	4.6%	2.6%
Win32/Gamania	Password Stealers & Monitoring Tools	3.5%	0.1%	2.3%
ASX/Wimad	Trojan Downloaders & Droppers	1.7%	3.2%	2.2%
Win32/Mydoom	Worms	1.9%	2.9%	2.2%
Win32/Mywife	Worms	1.9%	2.5%	2.1%

JS/Redirector and Win32/Netsky both appear with relative frequency among desktop and mobile client detections, but are rare among Web client detections, indicating that the social engineering techniques used to spread these threats are not very successful. As explained earlier, JS/Redirector is a detection for a JavaScript technique used to redirect Internet users to Web pages other than the ones they expect. The technique is simple to implement and is used widely by spammers. As such, e-mail messages containing JS/Redirector often end up in Hotmail's "Junk" folder and are subsequently ignored.

The five-year-old worm Win32/Netsky also appears relatively frequently among desktop and mobile client detections, in part because the short e-mail messages used to distribute Netsky are harder to block using content-based spam filters, like this typical example:

```
From: [address]
To: [address]
Date: 1/9/2009 10:35:46 PM
Subject: Hello

Important data!
```

The brevity that enables these messages to evade spam filters, however, does not appear to lend itself well to effective social engineering. Netsky only accounted for 3.0 percent of Web client detections, suggesting that users are particularly likely to discard such messages without opening the attachments.

An example of a family that uses more effective social engineering to spread is the trojan downloader Win32/Rochap, which accounted for 1.3 percent of desktop and mobile client detections but 7.7 percent of Web client detections. Rochap, which often masquerades as a component of Internet Explorer, spreads using messages that are often tied to closely watched current events, such as the death of pop star Michael Jackson on June 25, 2009. Current events–themed social engineering is a tactic that has been used in connection with a number of other prevalent families in the past, including Win32/Nuwar and Win32/Rustock.

Encyclopedia

Win32/Rochap: A family of multi-component trojans that download and execute additional malicious files. While downloading, some variants display a video from the Web site "youtube.com," presumably to distract the user.

Win32/Nuwar: A family of trojan droppers that install a distributed P2P downloader trojan. This downloader trojan in turn downloads an e-mail worm component.

Win32/Rustock: A multicomponent family of rootkit-enabled backdoor trojans, developed to aid in the distribution of spam. Recent variants appear to be associated with rogue security software.

http://www.microsoft.com/av

A Defense-in-Depth Strategy for E-Mail

The concept of *defense in depth*—deploying defensive measures in multiple layers or at multiple points along a process flow—is a basic tenet of computer security. FOPE provides defense in depth by using three different scanning engines from three different antivirus vendors to detect malware. Each incoming attachment is scanned by each of the three engines in series, and if any of the three engines detects malware, the attachment is blocked.

Most malware scanning engines are very good at scanning for known malware. The primary factors that differentiate them are how good they are at detecting "unknown" or "new" malware and how fast they respond to new malware outbreaks. Some vendors may detect a new threat later than others, and some vendors may be able to create, test, and publish an update faster than others, so the total response time can vary significantly. Defense-in-depth scanning is intended to reduce the impact of this uncertainty, by providing access to the best and fastest protection from a combination of different engines.

Of course, no strategy can guarantee 100 percent protection, and some threats may still be delivered to recipients. Moreover, with a strategy such as this one, there is typically an inflection point beyond which each additional layer produces increasingly diminishing returns. A strategy that employs 10 different scanning engines in series, for example, may not provide significantly better protection than one that uses three or four. System administrators can best benefit from multiple malware engines by selecting vendors with complementary areas of strength rather than focusing on quantity alone.

Malicious Web Sites

Attackers often use Web sites to host phishing pages or distribute malware. Although attackers sometimes set up Web servers of their own, most phishing pages are hosted by legitimate sites belonging to innocent parties that have been compromised through exploits or other techniques. 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, since attackers often create exploits that can download malware to vulnerable computers silently as soon as the user loads the page. Installing 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 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.

Phishing impressions have risen significantly in 1H09, due primarily to a large increase in phishing attacks targeting social networking sites. (A *phishing impression* is a single instance of a user attempting to visit a known phishing site with Internet Explorer and being blocked.) In addition, phishers continued to target a wider range of site types than in the past, with gaming sites, portals, and the online presences of major corporations accounting for some of the most frequently targeted Web sites in 1H09.

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 41. 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.[20]

[20] 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 41. The SmartScreen Filter in Internet Explorer 8 blocks reported phishing and malware distribution sites.

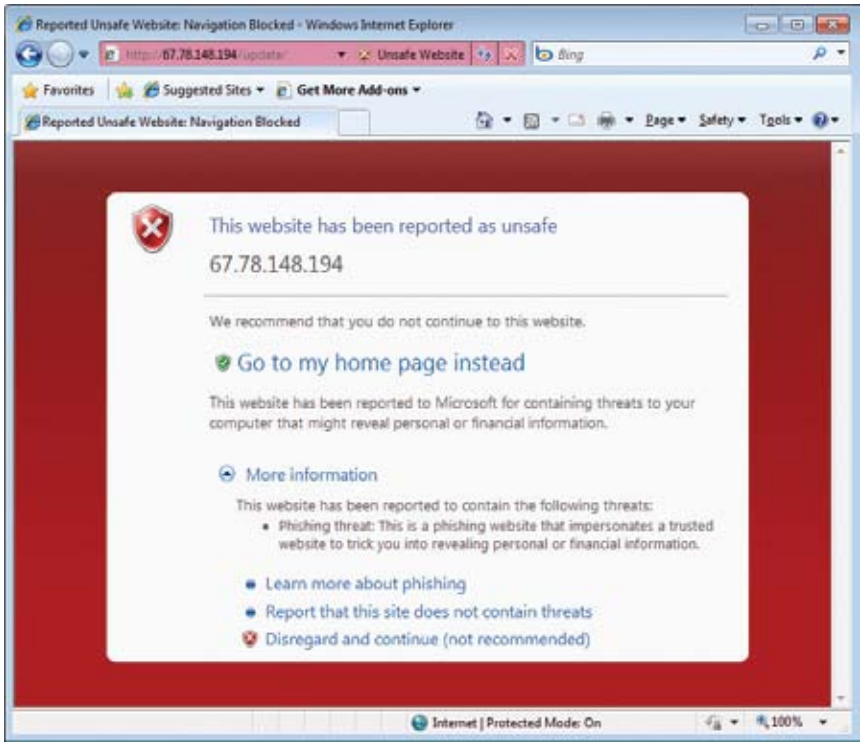
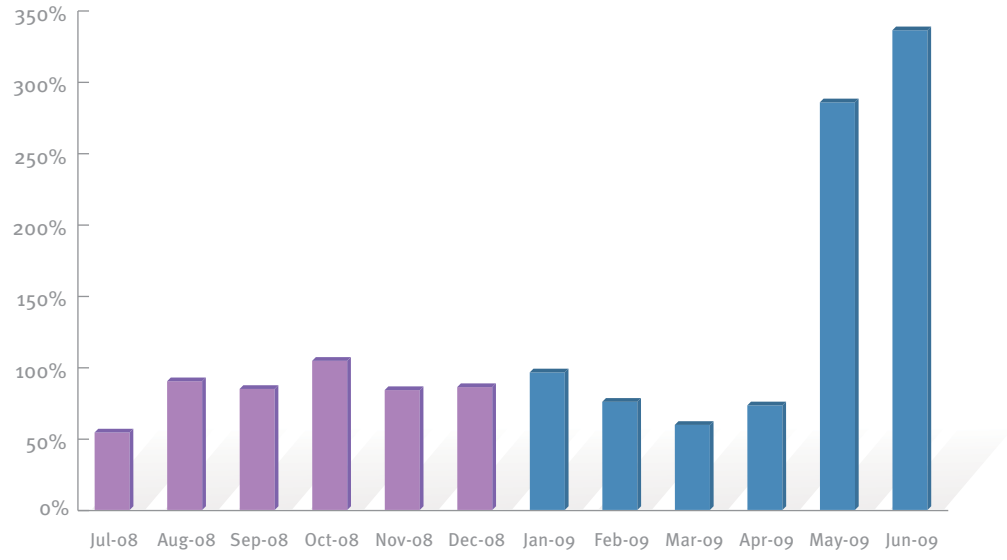


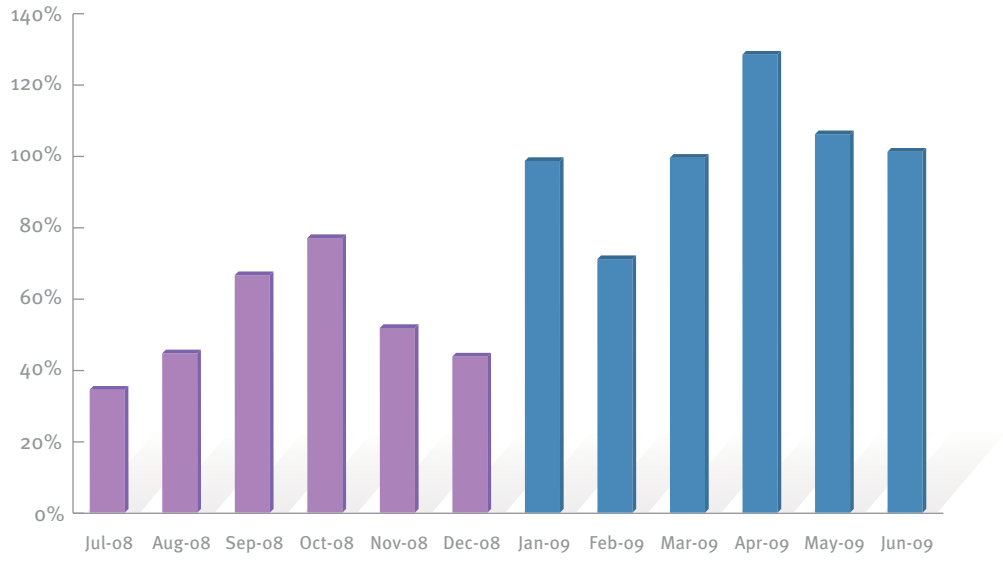
Figure 42 shows the number of phishing impressions recorded by Microsoft each month in 1H09 for each of the most frequently targeted types of institutions. After remaining mostly consistent throughout 2H08 and through April 2009, the number of impressions suddenly almost quadrupled in May and rose even higher in June.

FIGURE 42. Phishing impressions tracked each month in 2H08 and 1H09, indexed to January 2009



This steep increase was not accompanied by a rise in the total number of active phishing pages, which remained more stable from month to month in 1H09 but significantly higher on the whole than in 2H08.

FIGURE 43. Active phishing sites tracked each month in 2H08 and 1H09, indexed to January 2009



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 increase in impressions in May and June was due in large part to a campaign or campaigns targeting social networks, which typically don't require large numbers of active phishing pages, as explained on page 85.

Target Institutions

Financial institutions, social networks, and e-commerce sites remained among the favorite targets for phishing attempts, although researchers have also observed some diversification into other types of institutions, such as online gaming sites, Web portals, and large software and telecommunications companies.

Figure 44 and Figure 45 show the percentage of phishing impressions and active phishing sites, respectively, recorded by Microsoft each month in 1H09 for each of the most frequently targeted types of institutions.

FIGURE 44. Impressions for each type of phishing site each month in 1H09

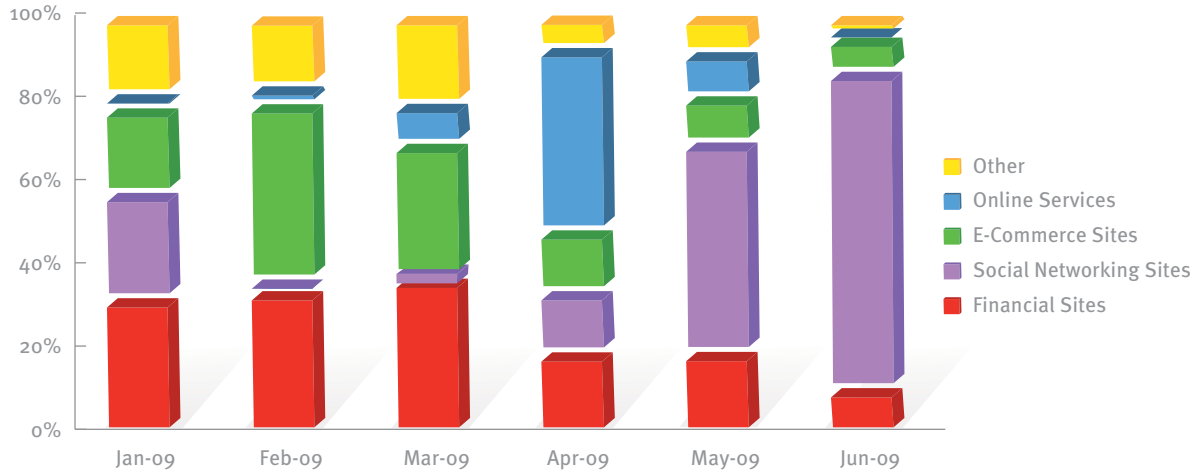
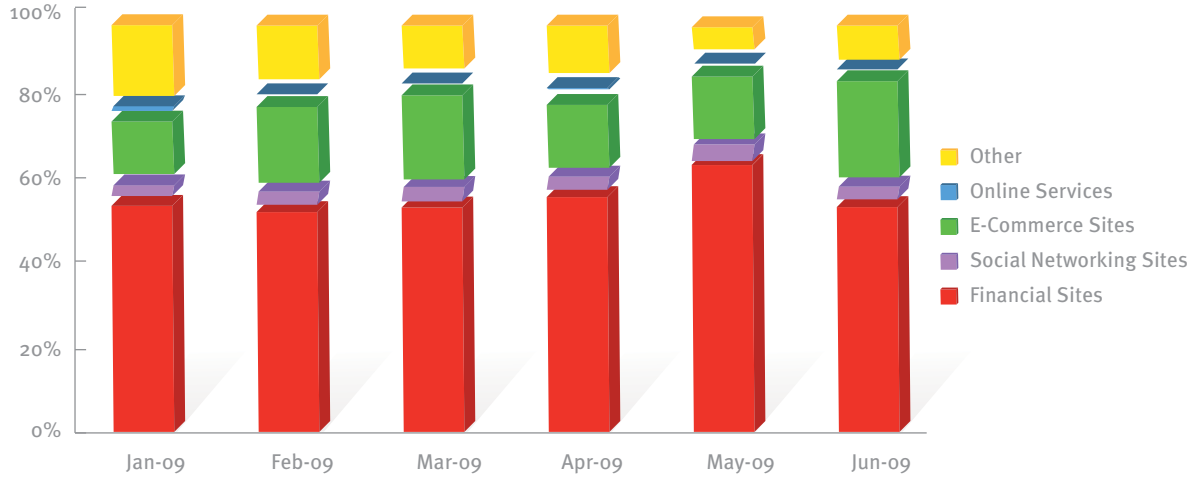


FIGURE 45. Active phishing sites tracked each month, by target institution type, in 1H09



After a surge of phishing impressions that targeted online services in April, the number of impressions targeting social networks rose significantly in May and June, commensurate with the rise in overall impressions shown in Figure 42. By June, social networks accounted for 76.0 percent of all phishing impressions.

At the same time, social networks were only targeted by a very 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 usage on the Internet, so phishers can effectively target many more people per site—in fact, the average social network phishing page received

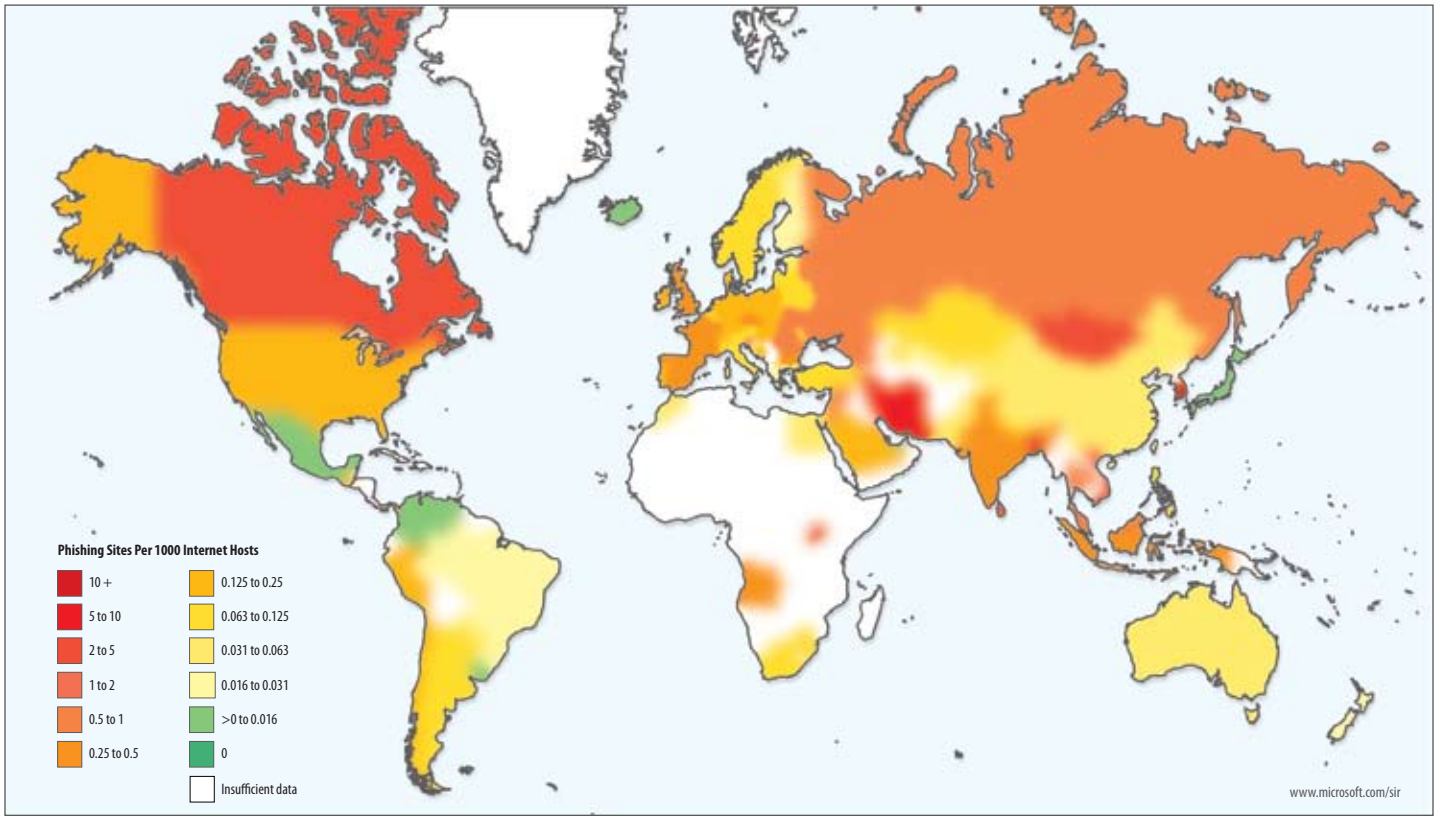
about 16 times as many impressions as the average financial institution phishing page. Although social networks have put a great deal of effort into educating their users about phishing attacks, the relatively high payoff potential suggests that social networks are likely to remain a tempting target for phishers 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.

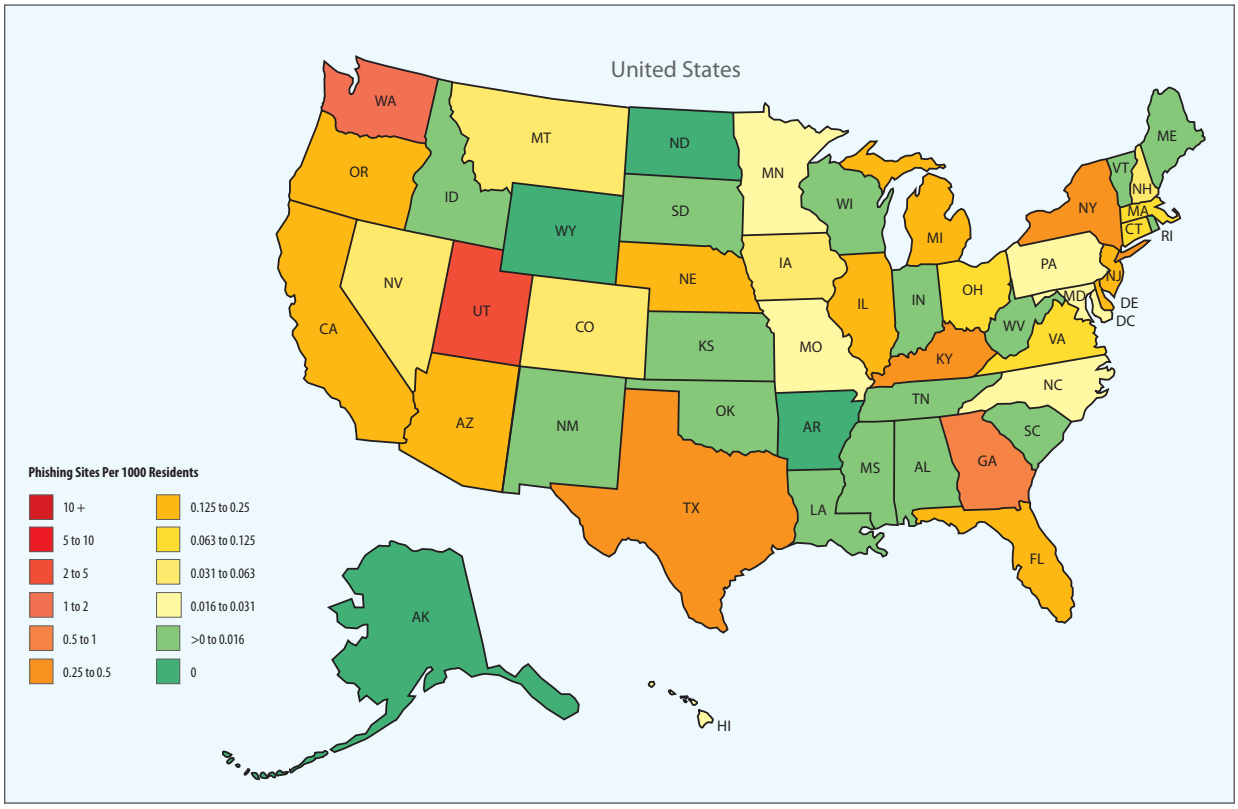
Figure 46 and Figure 47 show the relative concentration of phishing sites in different locations around the world and in U.S. states in 1H09.[21]

FIGURE 46. Phishing sites per 1,000 Internet hosts for locations around the world in 1H09



[21] 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 47 shows the number of phishing pages per 1,000 residents of each state, based on population estimates for 2008 published by the U.S. Census Bureau at http://www.census.gov/popest/states/.

FIGURE 47. Phishing sites per 1,000 residents by U.S. state in 1H09



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 46 of 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 82, 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 and indicates that the server is known to distribute unsafe software. As with phishing sites, Microsoft

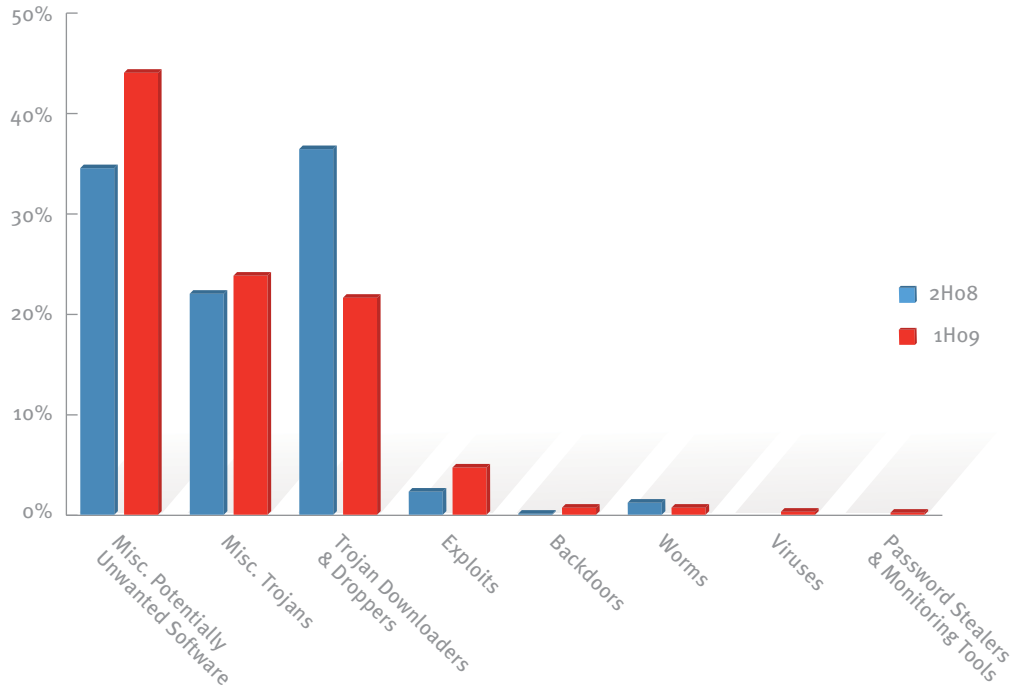
keeps track of how many people visit each malware hosting site and uses the information to improve the SmartScreen Filter and to better combat malware distribution.

The data cited in this section comes from SmartScreen telemetry generated by the final release version of Internet Explorer 8 and from pre-release versions made available to the public since the introduction of Internet Explorer 8 Beta 2 in August 2008.

Types of Malware Distributed over the Web

Figure 48 shows the category breakdown for threats hosted at URLs blocked by the SmartScreen Filter in 2H08 and 1H09.

FIGURE 48. Threats hosted at URLs blocked by the SmartScreen Filter, by category, in 2H08 and 1H09



The Miscellaneous Potentially Unwanted Software, Miscellaneous Trojans, and Trojan Downloaders & Droppers categories dominated the list in both periods, with other categories far behind. Comparing this data to Figure 10, on page 49, 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 most significant difference concerns the Miscellaneous Potentially Unwanted Software category, which increased from 35.0 percent of malware impressions in 2H08 to 44.5 percent in 1H09, while the percent of computers cleaned declined from 22.8 percent to 14.9 percent for the category. (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.

- Trojan Downloaders & Droppers declined significantly as a percentage of both SmartScreen impressions and computers cleaned.
- Miscellaneous Potentially Unwanted Software is disproportionally likely to be distributed over the Web, accounting for 44.5 percent of SmartScreen impressions in 1H09 but only 14.9 percent of computers cleaned. By contrast, worms are rarely distributed by malicious Web sites, accounting for just 1.2 percent of SmartScreen impressions, compared to 21.3 percent of computers cleaned.

FIGURE 49. The top 10 malware families hosted on sites blocked by the SmartScreen Filter in Internet Explorer 8 in 1H09

Rank	Family	Most Significant Category	Percent of Malware Impressions
1	Win32/MoneyTree	Misc. Potentially Unwanted Software	32.8%
2	Win32/Pdfjsc	Exploits	5.2%
3	Win32/Renos	Trojan Downloaders & Droppers	5.1%
4	Win32/FakeXPA	Miscellaneous Trojans	4.6%
5	Win32/Winwebsec	Miscellaneous Trojans	4.5%
6	Win32/PrivacyCenter	Miscellaneous Trojans	4.2%
7	Win32/Obfuscator	Miscellaneous Trojans	4.0%
8	Win32/InternetAntivirus	Miscellaneous Trojans	4.0%
9	Win32/Small	Trojan Downloaders & Droppers	3.7%
10	Win32/FakeRean	Miscellaneous Trojans	3.3%

Figure 49 lists the top 10 malware and potentially unwanted software families blocked by the SmartScreen Filter in 1H08, by user impression. Overall, sites hosting these 10 families constituted 71.4 percent of all malware impressions. Coincidentally, this is almost exactly the same share (71.2 percent) accounted for by the top 10 families in 2H08, although only four families from the 2H08 list carried over to 1H09 (and in significantly different proportion to one another). Win32/MoneyTree, in clear first place with more than six times as many malware impressions as the second-place family, increased from 19.2 percent of all impressions in 2H08 to 32.8 percent in 1H09. Meanwhile, Win32/Renos, the most prevalent family in 2H08 with 21.2 percent of malware impressions, dropped significantly in 1H09 to just 5.1 percent of impressions.

Encyclopedia

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

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

http://www.microsoft.com/av

Encyclopedia

Win32/FakeXPA: A rogue security software family that claims to scan for malware and then demands that the user pay to remove non-existent threats. Some variants unlawfully use Microsoft logos and trademarks.

Win32/Winwebsec: A family of rogue security software programs that have been distributed with several different names. The user interface varies to reflect each variant's individual branding.

http://www.microsoft.com/av

Rogue security software accounts for fully half of the top 10 families, led by Win32/FakeXPA and Win32/Winwebsec. As noted in "Rogue Security Software Still a Significant Threat," on page 100, detections of rogue security software by Microsoft desktop security products declined 20 percent in 1H09, which may be due in part to browser-based anti-malware features, such as the SmartScreen Filter.

Distribution patterns vary greatly by family. Some families spread using a small number of high traffic distribution points, while other families use extremely diverse distribution mechanisms. Renos, the third-most prevalent family blocked by SmartScreen in 1H09, has nearly 10,000 identified distribution points blocked by the SmartScreen Filter, with each site yielding very low levels of traffic in the Internet Explorer 8 user base. At the other extreme, some families use only a handful of distribution points that each received more than 10,000 malware impressions in 1H09.

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 50 and Figure 51 show the geographic distribution of malware hosting sites reported to Microsoft in 1H09, around the world and in the United States.

FIGURE 50. Malware distribution sites per 1,000 Internet hosts for locations around the world in 1H09

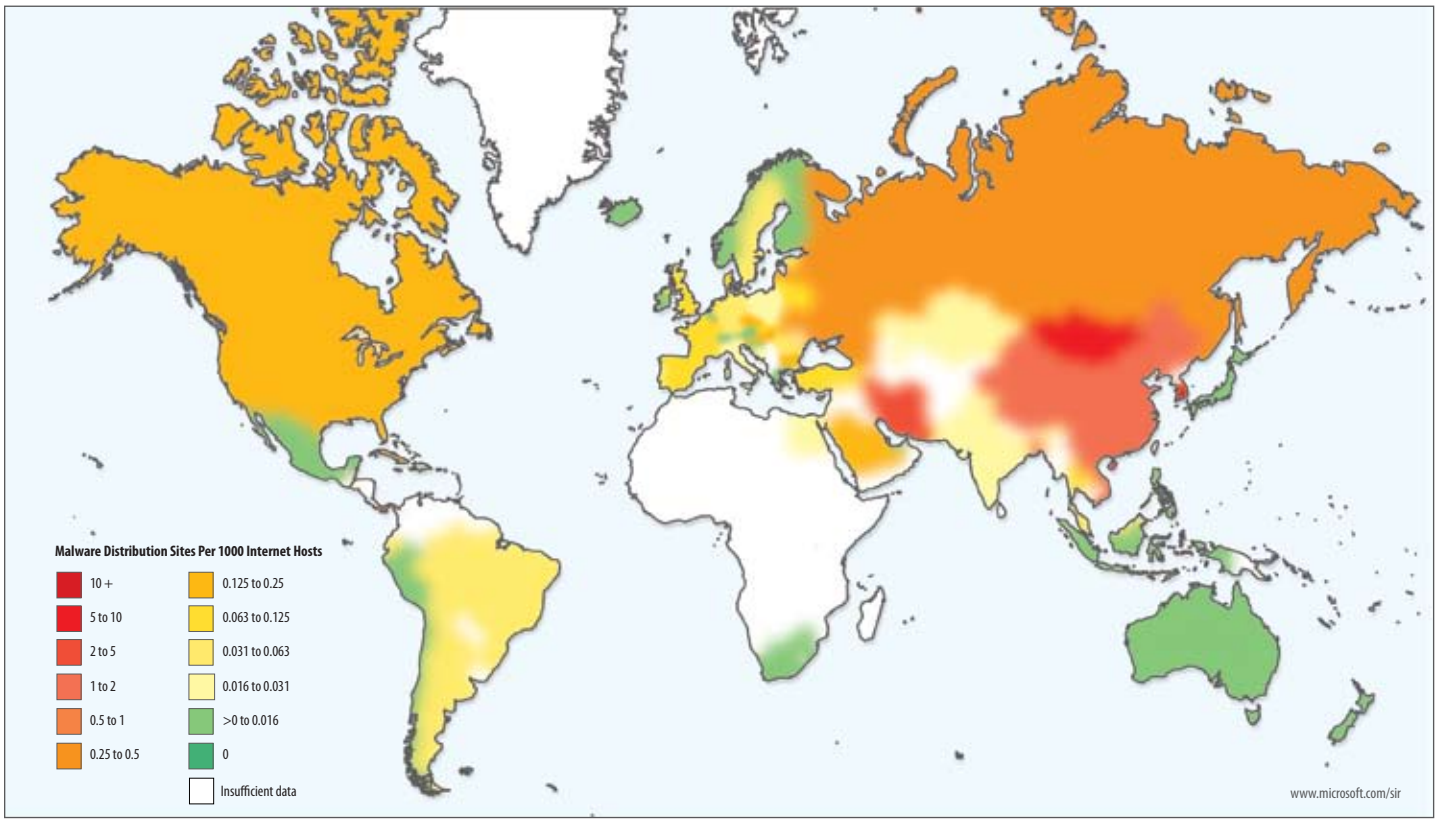
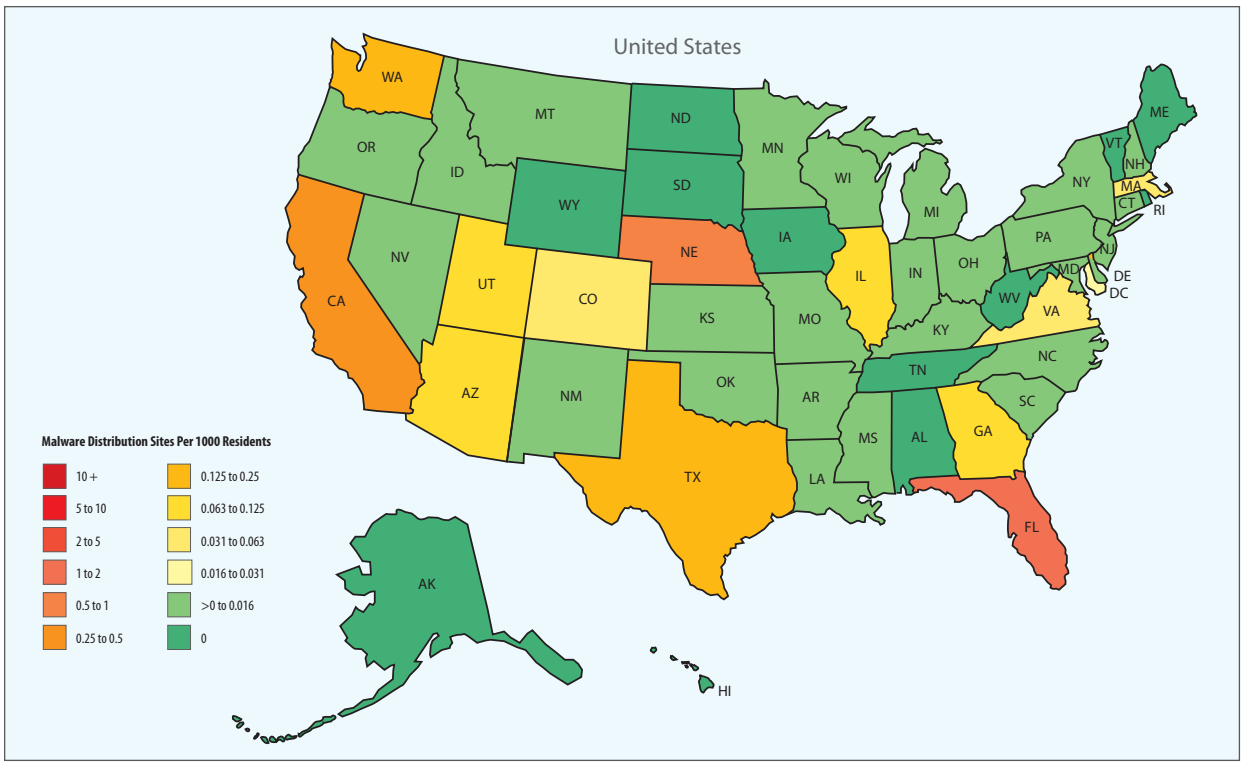


FIGURE 51. Malware sites per 1,000 residents by U.S. state in 1H09



"Malvertising": An Emerging Industry Threat

Microsoft Internet Safety Enforcement Team

"Malvertisements" are becoming an increasingly popular mechanism by which trojans, unwanted software, and deceptive advertisements are distributed to Internet users. The word itself is a portmanteau of "malicious" and "advertising," which fairly approximates the purpose and method behind malvertisements. They incorporate deceptive techniques to deliver malicious code or deceptive advertising to consumers (or both) and are camouflaged as ordinary online advertisements to evade detection by the advertising service companies through which they are inserted.

Malvertisements take advantage of the robust distribution infrastructure built for online advertising as a vehicle to obtain easy and free impressions and to deliver malicious code to Internet users. They present a diffuse and difficult-to-manage threat vector, with multiple points of entry into the online ecosystem: Each advertising network, Web site owner, or other advertising service provider that collects online advertisements and places them into the online advertising stream of commerce is a potential attack surface.

Although malvertisements have been reported since at least 2006, their prominence increased markedly in 2008 when WashingtonPost.com, facebook.com, and MSNBC.com, as well as a number of other prominent Web sites, all suffered through malvertising incidents. In the most high-profile incident to date, in September 2009, highly trafficked sites including NYTimes.com and SFGate.com were hit with malvertisements.

Insertion through advertising service providers is generally accomplished by a combination of social engineering and sophisticated technological deception. In most reported malvertising cases, persons approach an advertising service provider claiming to represent a well-known company wishing to start a campaign with the provider. Often, the contact will represent that he or she works for a boutique advertising agency, and the agency will have an at least minimally convincing online Web presence. The contact may also employ more traditional methods of fraud, such as using forged documents to bolster the credibility and authority of the person placing the malvertisement. These initial "out of the blue" approaches sometimes include requests that the campaigns begin quickly or not at all, so that the advertising service provider's ability to vet the new client is restricted. Payment is never up front, or if it is, it is made through compromised financial accounts; after all, the goal of malvertisers is to take a free ride on the robust online advertising infrastructure, and legitimate means of payment would create a money trail. Standardizing advertisement intake procedures, implementing robust checks, and training intake professionals will help to harden networks against malvertisement insertion by social engineering.

If a malvertisement passes the intake stage, often little can be done except to limit the damage by carefully testing and monitoring new campaigns from unfamiliar sources. Malvertisements themselves employ sophisticated and often layered defenses, which greatly increase the difficulty of detecting malicious code before the malvertisement is deployed. Many malvertisements are packaged in the SWF format used by Adobe Flash, a common format for online advertising. Functionality of malvertisment SWF files can be hidden by various methods, including encryption, resistance to decompilation, obfuscation routines, and white-space characters. Some malvertisements engage in cross-site scripting (XSS) to call other SWF files at other Web pages disguised as benign-looking traffic counting pages. These downstream SWF files are generally not placed online until the underlying malvertisement campaign begins, making detection before that time difficult. The downstream SWF files can examine various browser states and automatically redirect end users to payload delivery Web sites, based on such things as default language, patch status, and time.

Microsoft's Recent Legal Action Against Malvertising

Microsoft has several attack surfaces exposed to malvertisements. These include its services in publishing ads on its own online properties through Microsoft adCenter, brokering ads to publisher sites provided through Microsoft pubCenter, and delivery and tracking services provided to publishers through Microsoft Atlas and Microsoft adManager. Despite a robust anti-fraud unit focused on detecting and preventing malvertisement attacks, Microsoft occasionally suffers a malvertising incident, to which it responds quickly and collects data for potential enforcement actions and for study.

In September 2009, Microsoft's ISET team filed five civil lawsuits against persons responsible for malvertising attacks aimed at two of Microsoft's attack surfaces: adCenter and adManager. Each of these cases involved an SWF malvertisement. In some cases the malvertisements directed browsers to a trojan dropper server, and in others the malvertisements resulted in display of advertisements promoting scareware. Microsoft's lawsuits include claims under a variety of federal and state laws, including the federal Computer Fraud and Abuse Act, the Washington State Computer Spyware Act, and the Washington Consumer Protection Act. The five cases, brought initially against John Doe defendants, are captioned:[22]

- Microsoft Corp. and Microsoft Online Inc. v. John Does 1-20, d/b/a DirectAd Solutions (King County Superior Court No. 09-2-34024-2 SEA)
- Microsoft Corp. v. John Does 1-20, d/b/a Soft Solutions, Inc. (King County Superior Court No. 09-2-34021-8 SEA)

[22] For docket and other information about the cases cited in this section, visit http://dw.courts.wa.gov.

- Microsoft Corp. v. John Does 1-20, d/b/a qiweroqw.com (King County Superior Court Cause No. 09-2-34020-0 SEA)
- Microsoft Corp. v. John Does 1-20, d/b/a ote2008.info (King County Superior Court No. 09-2-34022-6 SEA)
- Microsoft Corp. v. John Does 1-20, d/b/a ITmeter Inc. (King County Superior Court Cause No. 09-2-34023-4 SEA)

Microsoft's primary goals in bringing these lawsuits are to identify the persons behind these particular malvertisement attacks, to obtain appropriate relief, and to stop these persons from carrying out such attacks in the future. In addition, through subpoenas and other investigation, Microsoft will obtain information that will enable deeper study of the methods for malvertisement coding, insertion, and distribution and will combine this information with other telemetrics to develop ways to harden attack surfaces from future malvertisements.

Top Malware and Spam Stories of 1H09

Security headlines in 1H09 were dominated by Win32/Conficker, the aggressive worm that was the most prevalent malware family worldwide in 1H09. Less publicized, but also quite significant, has been the continuing prevalence of rogue security software, with new families appearing and displacing older ones in an ongoing effort to trick unsuspecting computer users into paying for ineffective software they don't need. Other stories of interest in 1H09 involve an automated SQL injection tool that has been used against many Web sites; Win32/Koobface, a new threat that attacks social networks; the spambot Win32/Waledac; and a couple of victories in the fight against spam.

Win32/Conficker Update

The out-of-band release of Security Bulletin MS08-067 on October 23, 2008, presaged the development of a potent new threat. Designated Win32/Conficker, the worm not only takes advantage of the MS08-067 vulnerability but also uses a number of dangerous technical and social engineering techniques to propagate; these had not been widely seen before. "MS08-067: Vulnerability in Windows Server Service," beginning on page 41 of *Microsoft Security Intelligence Report, Volume 6 (July through December 2008)*, explored the early development of the worm, up to Worm:Win32/Conficker.B, released on December 29, 2008. Since then, three more variants have been released into the wild, and security professionals around the world have mobilized to protect their users from this aggressive threat. (For an account of the response to Win32/Conficker at Microsoft and around the world, see "Case Study: The Conficker Working Group," beginning on page 29.)

Win32/Conficker.A and Win32/Conficker.B: The First Variants

On November 21, 2008, the first significant worm that exploits the Windows Server Service vulnerability addressed by MS08-067 was discovered, which Microsoft designated Win32/Conficker. The first variant discovered, Worm:Win32/Conficker.A, only propagates by exploiting this vulnerability. Conficker.A did not spread particularly far or fast, in part because the security update that fixed the vulnerability had been released nearly a month prior; home and enterprise users that installed the security update in a timely manner on all their computers were therefore not at risk of infection from this first variant.

A significantly more dangerous variant, Worm:Win32/Conficker.B, was discovered on December 29, 2008. This variant also exploits the MS08-067 vulnerability but uses two additional propagation methods that allow it to spread much more quickly:

- It attempts to connect to the ADMIN$ share on other computers on the network, first as the logged-in user and then by using a list of 248 weak passwords.
- It drops an autorun.inf file on removable drives that displays a misleading **Open folder to view files** option in the **AutoPlay** dialog box, which installs the malware if selected.

FIGURE 52. Worm:Win32/Conficker.B creates a fake AutoPlay option (in red) on removable disks. An unprotected user who chooses the wrong "Open folder to view files" option may become infected.

After installing itself, Conficker blocks other malware from exploiting the MS08-067 vulnerability—not in an effort to protect the computer, but to prevent other malware from interfering with it. Every time the computer is restarted, in fact, the worm loads and blocks the vulnerability in memory again.

Conficker uses an unusual mechanism, called *HTTP rendezvous*, to issue commands to compromised computers. The Conficker.A and Conficker.B variants include an algorithm that computes 250 new domain names each day, consisting of nonsense strings of characters like *ltxbshpv.net* and *fwnvlja.org*. Conficker.B generates a different list of domain names than Conficker.A due to minor changes in the algorithm used, so the two variants together generate a total of 500 domain names each day. An infected computer attempts to contact each domain on the list each day. The operators would be able to use the same algorithm to generate the domain names in advance and use them as command-and-control points.

Win32/Conficker.C: P2P Functionality

Another new Conficker variant was first detected on February 20, 2009. Definitions from Microsoft and several other vendors initially detected the new variant as Worm:Win32/Conficker.B, leading some to call it "Conficker.B++." However, the new variant included significant new functionality that prompted Microsoft to update its definitions to distinguish it as Worm:Win32/Conficker.C. Among other changes, the new variant added a peer-to-peer (P2P) function that used the MS08-067 vulnerability to facilitate file sharing between infected computers. The P2P mechanism allows the authors to distribute additional malware to infected computers, even if they are not able to register new domain names. Conficker.C was first detected eight days after the formation of the Conficker Working Group (CWG) and may have been released as a response to the fact that its authors could no longer effectively register many of the domain names that the worm algorithmically generated.

Win32/Conficker.D: 50,000 New Domain Names a Day

Worm:Win32/Conficker.D was discovered on March 4, 2009. This variant appears to have been intended as a second, more effective response to the efforts of the CWG to shut down the worm's means of distribution and communication, as described in "Case Study: The Conficker Working Group," beginning on page 29. Conficker.D included changes that increased the number of algorithmically generated domains available to it, while simultaneously making it less dependent on them.

Each of the earlier variants was programmed to monitor 250 new domain names per day for payloads to download and execute. After the CWG decrypted the algorithm the worm used to generate new domain names, it only needed to block access to 500 domain names per day (250 used by Conficker.A and 250 shared by the B and C variants) to effectively control the ability of infected computers to cause further damage. To defeat this countermeasure, Conficker.D included a modified version of this domain-selection algorithm that would cause each infected computer to randomly select 500 domain names to monitor out of a pool of 50,000 algorithmically generated domain names per day. Conficker.D was programmed to begin using this new mechanism on April 1, 2009.

In addition to this change, Conficker.D also included an updated P2P mechanism that enabled it to distribute and receive commands from other Conficker.D–infected computers and Conficker domains. This additional complexity made Conficker.D much less dependent on centralized control than its predecessors. If the Conficker controllers were able to register just one domain name out of the 50,000 names generated on a particular day, about 1 percent of the Conficker.D–infected computers worldwide would be able to receive updates and commands from it. These computers would then be able to use the P2P mechanism to discover other Conficker.D–updated computers and distribute the updates and commands to them, with the cycle repeating until a significant percentage of Conficker.D–infected computers had been contacted.

FIGURE 53. Command-and-control methods used by Win32/Conficker.D

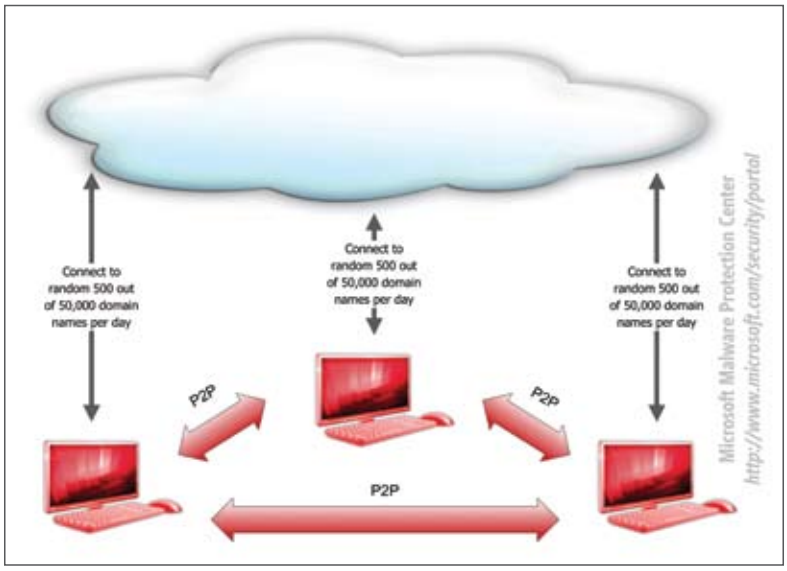
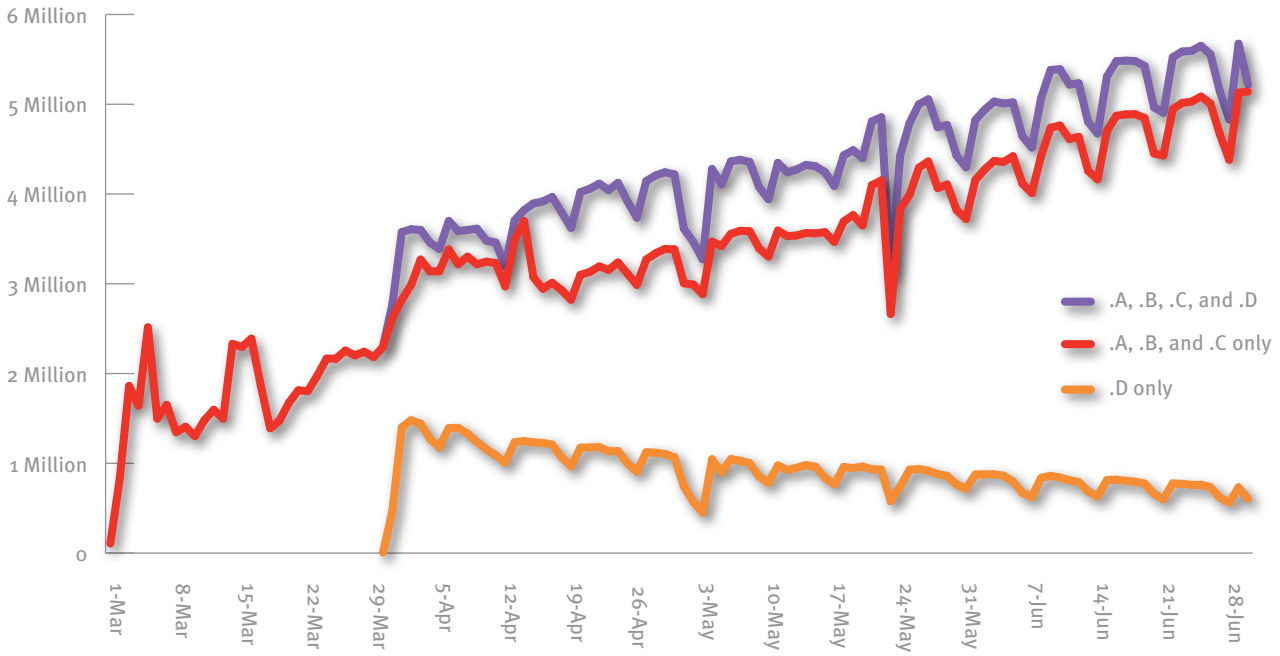


Figure 54 shows the number of infected computers detected each day between March and June 2009 by the sinkhole servers operated by the Shadowserver Foundation.[23] The "saw-tooth" effect apparent in the chart is caused by significant drops in the number of infected computers contacting the sinkhole servers on weekends, reflecting Conficker's tendency to spread across workplace networks with relative ease. The particularly large drop shown for the weekend of May 23, 2009, corresponds to Memorial Day, a major vacation day in the United States.

FIGURE 54. IP addresses infected by variants of Win32/Conficker, March–June 2009



(Data provided by the Shadowserver Foundation)

[23] The Shadowserver Foundation identifies Conficker.C as "Conficker.B++" (see page 96) and Conficker.D as "Conficker.C." The *Security Intelligence Report* uses the Microsoft naming convention for these variants.

What Happened on April 1?

Following the discovery of Worm:Win32/Conficker.D on March 4, 2009, a number of stories published and broadcast by both the general news media and the technical press seized upon the April 1, 2009, date, when Conficker.D was programmed to begin using its new domain-name generation algorithm, and raised the specter of a "doomsday" scenario in which the worm would suddenly awake and wreak unknown havoc on the world's computers. When this failed to occur, another round of stories appeared, declaring the threat to have been overblown and noting the connection to April Fools' Day.

In fact, researchers have never found evidence that any Conficker variant was configured to change its behavior on April 1, other than by changing the way it searched for command-and-control servers. Even this change was not a new behavior but a revision of an existing one, implemented because the efforts of the CWG and its partners had made the old distribution mechanism largely ineffective. Nor is it accurate to suggest, as some stories have, that the Conficker botnet remains dormant, like a predator waiting for the right time to attack. As explained in "The Win32/Waledac Botnet and Spam," on page 104, the Conficker botnet has been used to download rogue security software to infected computers, a fairly typical activity for malware.

In the security response community, of course, April 1 was a very significant date, requiring a great deal of cooperation between security software vendors, ISPs, domain registrars, and others, as explained in "Case Study: The Conficker Working Group," beginning on page 29. The fact that the spread and impact of Conficker.D has been largely contained since then, as shown in Figure 54, is a testament to the working group's effectiveness.

Win32/Conficker.E: Minor Release

Worm:Win32/Conficker.E was discovered on April 8, 2009, with the existing Microsoft definitions initially detecting it as Worm:Win32/Conficker.gen!A. Conficker.E only infects computers that have previously been infected with earlier Conficker variants .B, .C, and .D and serves as an update mechanism for those variants. The Conficker.E installer was programmed to delete itself on May 3, 2009, but it leaves behind a component (detected as Worm:Win32/Conficker.E.dll) that enables P2P communication similar to that used by Conficker.D.

Encyclopedia

Win32/FakeXPA: A rogue security software family that claims to scan for malware and then demands that the user pay to remove non-existent threats. Some variants unlawfully use Microsoft logos and trademarks.

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 products such as Win32/FakeXPA.

Win32/Winwebsec: A family of rogue security software programs that have been distributed with several different names. The user interface varies to reflect each variant's individual branding.

http://www.microsoft.com/av

Rogue Security Software Still a Significant Threat

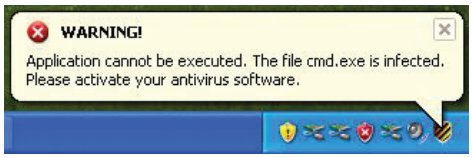
Rogue security software—software that displays false or misleading alerts about infections or vulnerabilities on the victim's computer and offers to fix the supposed problems for a price—has become one of the most common methods that attackers use to swindle money from victims. These are programs that masquerade as legitimate security programs offering protection from malware, spyware, and other threats, but actually use social engineering to obtain money from victims, and offer poor or nonexistent protection. Microsoft security products detected rogue security software–related malware on 13.4 million computers in 1H09, down from 16.8 million in 2H08—an improvement, but still a significant threat. At least part of the decline may be due to browser-based anti-malware features, such as the Internet Explorer 8 SmartScreen Filter, which protect users from exposure to threats like rogue security software before they can become infected. (See "Analysis of Malware Hosts," beginning on page 87, for more information.) A rogue security software family, Win32/FakeXPA, was the sixth-most prevalent threat detected by Microsoft desktop security products worldwide in 1H09; two others, Win32/Yektel and Win32/Winwebsec, ranked seventeenth and twenty-first, respectively.

FIGURE 55. Fake "security scans" from Win32/Winwebsec, left, and Win32/InternetAntivirus, right

Rogue security software 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 "activate" the software to remove them. Some families emulate the appearance of the Windows Security Center or unlawfully use trademarks and icons to misrepresent themselves. Rogue security software spreads through familiar malware distribution

mechanisms, like spam and exploits, and through customized tactics, like a fake Web-based security scanner. After installation, some rogue security software families take other actions to evade detection or to frighten the user into paying. For example, some variants of Win32/Winwebsec, which was added to the MSRT in May 2009, attempts to block most other programs from executing, which not only helps convince the user to pay for the "full version" of the software to repair the damage but also makes it difficult to use legitimate security tools to remove the malware.

FIGURE 56. Win32/Winwebsec blocks common programs, such as the Command Prompt, from executing.



Though fooling users into paying for worthless software remains the primary goal of most rogue security software, several recently released families have begun to branch out and exhibit behaviors common to other threats, such as downloading additional malware to a victim's computer. Win32/Winwebsec has been observed to download Win32/Koobface—which itself sometimes displays pop-up advertisements for rogue security software. Win32/InternetAntivirus, which was added to the MSRT in June 2009, downloads the password stealer Win32/Chadem. (For more information about malware that downloads other malware, see "Threat Combinations," on page 67.)

Rogue security software infections tend to be concentrated in certain geographic areas, typically Western societies and other English-speaking regions. For example, rogue security software families account for 5 of the top 25 families detected in the United Kingdom, but only 1 of the top 25 in Russia, and none in China. Unlike many other types of malware, rogue security software relies heavily on user interaction to spread, which means that it is most effective when presented in a language that the victim understands. Although localized variants exist, most rogue security software is written in English, though not necessarily by native speakers. Rogue security software also tends to target wealthier societies and societies 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, 7 of the top 25 families are rogue security software, whereas in China, where credit cards are relatively rare, none of the top 25 families are rogue security software. (For more information about threats around the world, see "Appendix B: Threat Assessments for Individual Locations," beginning on page 181.)

Encyclopedia

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/InternetAntivirus: A rogue security software program that uses several different names. It also displays a fake "Windows Security Center" message.

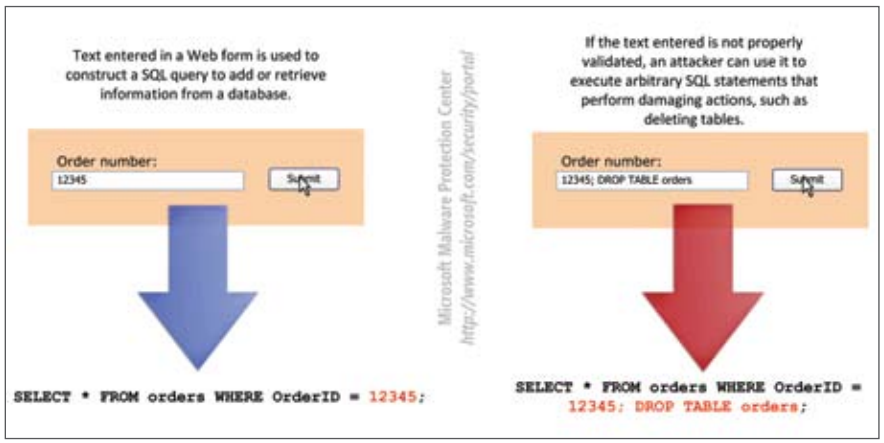
Win32/Chadem: A trojan that steals password details from an infected computer by monitoring network traffic associated with FTP connections.

http://www.microsoft.com/av

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 code 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 or altering sensitive records.[24]

FIGURE 57. 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. The technique has also been used to conduct targeted attacks, including attacks against the Web sites of major antivirus vendors.

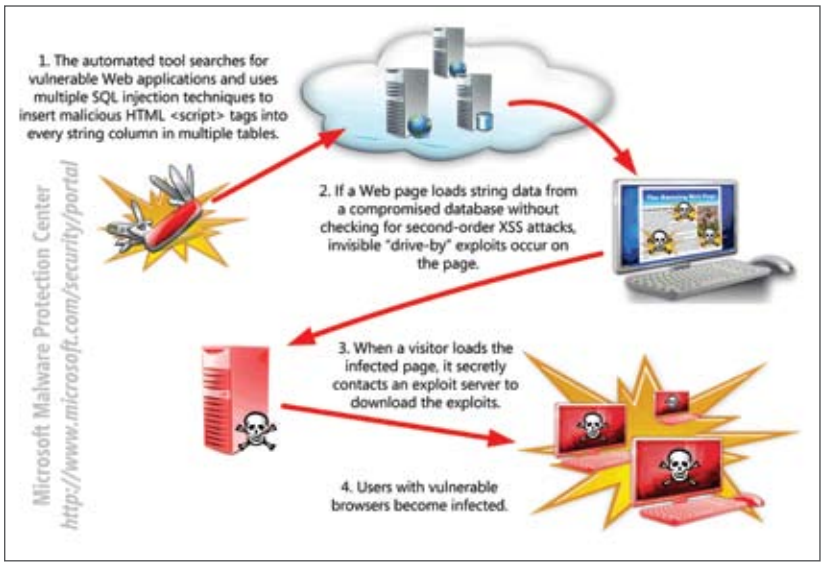
Web applications often construct pages dynamically as they are requested, by retrieving information from a database and using it to populate the page. The goal of the automated mass SQL injection tool is to insert malicious HTML and JavaScript code into the database so that it becomes a part of every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

The tool is believed to begin 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 in order to discover some details about the SQL server and account used by the Web page. It then uses a SQL injection payload to append

[24] 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/en-us/library/ms161953.aspx.

malicious JavaScript code within 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 checks for and disallows 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 58. How the mass SQL injection tool works



Microsoft has published Security Advisory 954462, which includes more information about this class of attacks, and offers guidance for detecting and defending against them. 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)

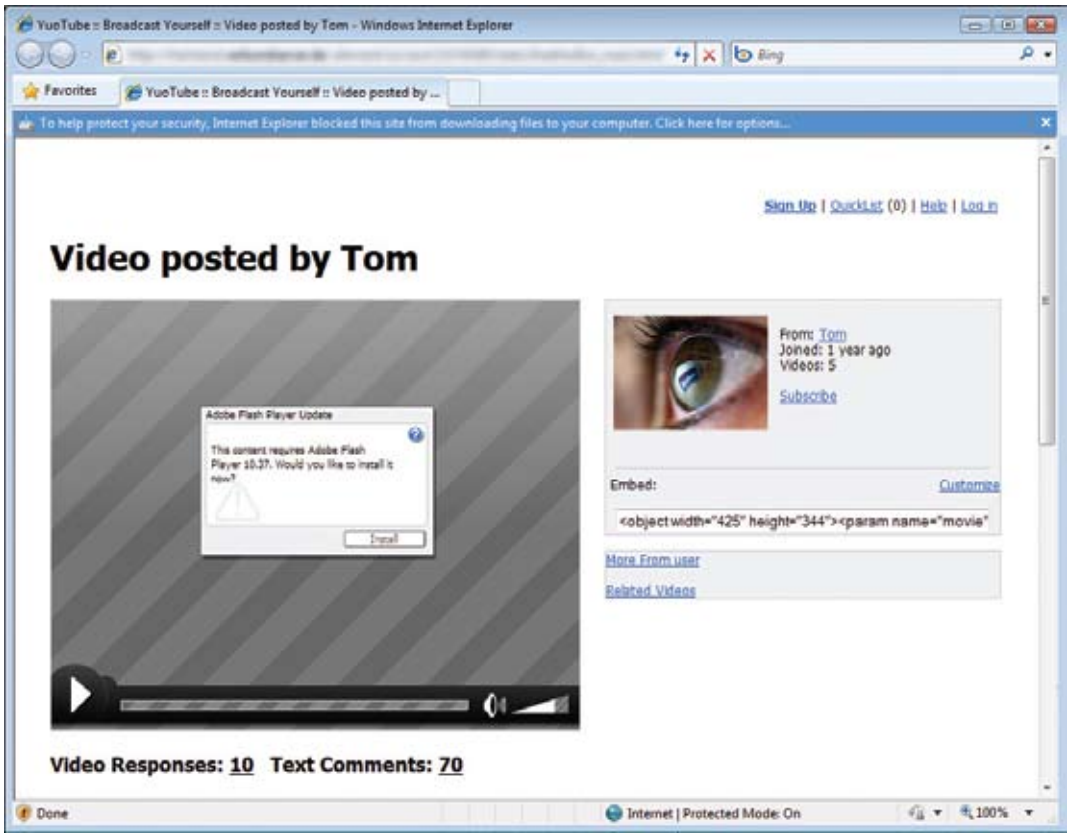
Win32/Koobface Attacks Social Networks

Win32/Koobface is a multi-component family of malware that targets users of popular social networking Web sites, such as Facebook, MySpace, and Twitter. Though it is usually referred to as a worm, Koobface is actually a collection of components that perform different tasks on compromised computers, such as downloading and hosting malware, stealing passwords and other sensitive data, and displaying advertisements for rogue security software. The ability to remove Koobface was added to the MSRT in March 2009.

Overall, Koobface was the twenty-fifth most prevalent family removed from computers by Microsoft desktop security products in 1H09.

Win32/Koobface spreads by sending messages to a victim's social network contacts with text, such as "You should watch my latest video," accompanied by a URL. Recipients who visit the URL are confronted with a message telling them that they must download an updated version of Adobe Flash Player to watch the video. The supplied executable is actually the Koobface installer.

FIGURE 59. The Win32/Koobface installer masquerades as an updated version of Adobe Flash Player.



The bogus Web page and installer are themselves typically hosted on computers infected with Koobface, which includes a component that secretly installs a Web server on a compromised computer.

The Win32/Waledac Botnet and Spam

Win32/Waledac is a trojan that is used to send spam. It also has the ability to download and execute arbitrary files, harvest e-mail addresses from the local computer, perform denial-of-service (DoS) attacks, proxy network traffic, and steal passwords. The ability to

remove Waledac was added to the MSRT in April 2009, and it was the twenty-fourth-most detected family by the MSRT that month.

While early versions of Win32/Waledac were released into the wild as early as December 2007, the family first drew significant attention in December 2008, when attackers sent Christmas-themed postcards through e-mail to spread it to computers. A spam campaign in early 2009 used a false report of a terrorist attack, purportedly from the Reuters news agency, to trick people into downloading the malware (which masqueraded as an update to Adobe Flash Player, like Win32/Koobface). For another spam campaign, the Waledac installer masqueraded as a trial version of a program that supposedly allows one to spy on other people's mobile phone text messages. Social engineering tactics such as these—holiday themes, provocative-sounding bogus news reports, invitations to illicit activity—are familiar to security researchers as tactics that other malware families (notably Win32/Nuwar, the so-called "storm worm"[25]) have used in the past to build *botnets*—networks of compromised computers that are controlled remotely and surreptitiously by one or more individuals to perform various criminal activities.

Waledac is a complex trojan that bears some of the hallmarks of legitimate, professionally developed software, such as an internal versioning system that researchers have used to track the malware's development, beginning with version 0 in December 2007. Version 15, released in the last week of November 2008, was the first version to support "labels," which allow the botnet operators to identify and segment groups of controlled computers in the network and the tasks delegated to them. This factor and others suggest that the creators of Waledac are using an affiliate program to provide a financial incentive for other parties to distribute it, an illustration of the way participants in the new, profit-oriented malware economy have adopted tactics used by legitimate businesses.

A variant of Win32/Conficker has been observed to download an encrypted copy of Waledac from a malware hosting site using a private key, suggesting that the authors of Waledac appear to have established a relationship of some sort with other malware authors. Trojan downloaders, such as Win32/Bredolab, have also been seen to download Waledac binaries from the same site, bearing a different label.

Waledac includes the ability to download files, which it uses to update itself to the latest version. Waledac has also been known to download and install other malware, notably rogue security software such as Win32/Rugzip and Win32/FakeSpypro.

Microsoft Malware Protection Center researchers have written about Win32/Waledac at the MMPC blog (http://blogs.technet.com/mmpc). For more information, see the following blog entries:

- Where's Waledac? (April 14, 2009)
- Where is Waledac—Episode II (May 7, 2009)

[25] For more information, see "A Focus on Win32/Nuwar ('The 'Storm Worm')," in *Microsoft Security Intelligence Report, Volume 4 (July through December 2007)*, page 60.

Encyclopedia

Win32/Nuwar: A family of trojan droppers that install a distributed P2P downloader trojan. This downloader trojan in turn downloads an e-mail worm component.

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/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/Rugzip: A trojan that downloads other malware from predefined Web sites. Rugzip may itself be installed by other malware. Once it has performed its malicious routines, it deletes itself to avoid detection.

Win32/Fakespypro: A rogue security family that falsely claims that the affected computer is infected with malware and encourages the user to buy a promoted product it claims will clean the computer.

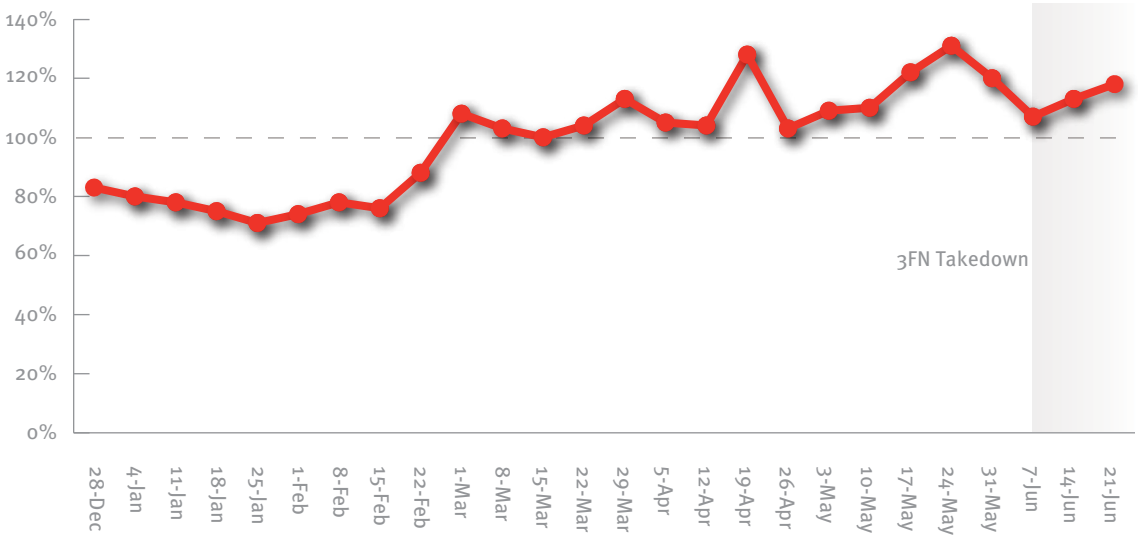
http://www.microsoft.com/av

Rogue ISP 3FN Taken Down

In early June 2009, a U.S. federal district court judge in California ordered Internet service provider 3FN disconnected from the Internet at the request of the U.S. Federal Trade Commission (FTC). The FTC presented evidence that Pricewert LLC, the company that operated 3FN, actively recruited and colluded with "criminals seeking to distribute illegal, malicious, and harmful content including child pornography, spyware, viruses, trojan horses, phishing, and botnet command-and-control servers," according to the FTC. The complaint alleges that Pricewert actively shielded its criminal clientele by either ignoring take-down requests issued by the online security community or shifting its criminal elements to other IP addresses it controlled to evade detection.

The volume of spam as measured by Forefront Online Protection for Exchange was depressed for weeks after McColo, another rogue ISP, was disconnected from the Internet in November 2008,[26] and indeed FOPE detected a small dip in spam following the 3FN takedown, as well. Unlike with McColo, however, spam volumes almost immediately returned to normal this time, suggesting that spammers are learning to diversify their hosting arrangements to avoid service disruptions.

FIGURE 60. Inbound e-mail traffic to FOPE servers, indexed to the period average, in 1H09



[26] For more information about the McColo takedown, see "Spam Volume Drops 46 percent When Hosting Provider Goes Offline," on page 113 of *Microsoft Security Intelligence Report, Volume 6 (July through December 2008)*.

Prolific Spammer Alan Ralsky Pleads Guilty

In June 2009, 64-year-old Alan Ralsky of Michigan, United States, pleaded guilty in federal court to charges that he ran a multimillion dollar international "pump and dump" stock fraud scheme involving the illegal use of bulk commercial e-mail. Federal investigators described Ralsky as one of the world's top spammers.[27]

Ralsky and his son-in-law Scott K. Bradley, 38, also of Michigan, pleaded guilty to wire fraud, money laundering, violation of the U.S. federal CAN-SPAM Act, and other charges. Ralsky faces up to 87 months in prison and a U.S.$1 million fine.

The U.S. Department of Justice characterized Ralsky as one of the world's most notorious illegal spammers. "Today Ralsky, his son-in-law Scott Bradley, and three of their coconspirators stand convicted for their roles in running an international spamming operation that sent billions of illegal e-mail advertisements to pump up Chinese 'penny' stocks and then reap profits by causing trades in these same stocks while others bought at the inflated prices," said U.S. Attorney Terrence Berg in a Justice Department press release. "Using the Internet to manipulate the stock market through spam e-mail campaigns is a serious crime, and this case serves notice that federal law enforcement has [both] the capability and the will to successfully investigate, prosecute and punish such cybercrimes."

According to court records, Ralsky and his associates used botnets consisting of tens of thousands of compromised computers to send spam, earning millions of dollars in the process.

Spam researchers have been tracking Ralsky for more than a decade. According to a 2002 article in *The Detroit News*, Ralsky's spamming career began in 1997 after losing his license to sell insurance.

[27] For more information about the arrests, see http://www.usdoj.gov/opa/pr/2009/June/09-ag-615.html.

Strategies, Mitigations, and Countermeasures

- Demand digitally signed code from software vendors. Although signed code is not always safe, signed code is still much safer on average than unsigned code. Code signing provides a strong link to the author of the code and helps identify files that have been tampered, infected, or have other file corruption. In 1H09, about 97 percent of unique threat files detected were unsigned. Excluding the Win32/GameVance and Win32/Wintrim families, 99.9 percent of all remaining threat files were not code-signed.
- Software vendors should virus-scan and then code-sign all their binary files and installation packages. This helps prevent vendors from accidentally shipping malicious code and also provides a clear link from the files to the vendor. Antivirus vendors can use signed code from other software vendors to prevent and detect false positive detections and to protect their own code from tampering. Nevertheless, as the data presented here makes clear, antivirus vendors should never automatically assume that a signed file cannot be malware.
- Use an e-mail authentication system, like Sender Policy Framework (SPF) or DomainKeys, to identify mail and help reduce domain spoofing. Implementing e-mail authentication is not particularly expensive or difficult, yet is still not done nearly enough.
- Maintain a strong e-mail scanning presence at the edge of the logical network perimeter. Edge filtering remains the most productive of the filtering techniques, accounting for more than 85 percent of spam filtering.
- Consider disabling autorun functionality in your environment to decrease the risk it presents. If you cannot disable autorun due to business reasons, ensure that users are aware that malware can abuse the autorun feature and that they should only select autorun options they recognize.
- Enforce the use of strong passwords for network shares.
- 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. Social engineering attacks over e-mail (phishing) and social engineering attacks over telephone (sometimes called *vishing*) are easy to mitigate by using a known e-mail address or phone number, often included on the back of the credit card or bank statement.
- Users who enjoy virtual worlds and online gaming are subject to targeted attacks to obtain user names and passwords, enabling the criminal to steal virtual assets or other account information. For information on ways to reduce this risk, read http://blogs.technet.com/mmpc/archive/2008/09/03/helpful-suggestions-to-protect-you-from-game-password-stealers.aspx.
- If infected, download and run the Malicious Software Removal Tool (http://www.microsoft.com/security/malwareremove) or make a free call (in North America) to 1-866-PC-SAFETY.

- Home computer users can help keep their machines and the computing ecosystem clean by using the free Microsoft Security Essentials (http://www.microsoft.com/security_essentials/) antivirus program, scheduled for release in many languages in September 2009.
- Insist that your mail servers use both inbound and outbound authentication controls, to protect your brand from harm (a technique called *brandjacking*) and to keep your customers safe from e-mail spoofing. The most popular method for this is the Sender ID Framework (http://www.microsoft.com/mscorp/safety/technologies/senderid/resources.mspx).
- Use a mail client that actively blocks active content and the automatic opening of attachments. Current versions of Microsoft Outlook, Hotmail, and Outlook Express, in conjunction with the security zone settings in Internet Explorer 8, can help deter IFrame attacks and prevent the unintentional opening of executable attachments.
- Inform users that malware can be installed through instant messaging (on both computers and cell phones) and social networking sites, in addition to e-mail. Users should only accept files from people they know.

Microsoft Security Engineering Center

The Microsoft Security Engineering Center helps to protect Microsoft customers by delivering inherently more secure products and services. MSEC's three 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 Assurance* team helps teams ship products that are fundamentally secure by ensuring the requirements of the Security Development Lifecycle 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 Development Lifecycle* 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 pr ivacy into Microsoft software and culture, leading to measurable security and privacy improvements in flagship products such as Windows Vista, Microsoft Office, and SQL Server.

The *Security Science* team protects customers by improving the security and privacy resiliency of Microsoft products through applied security research. Specifically, Security Science 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 118, 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 that 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 161, 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. 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.

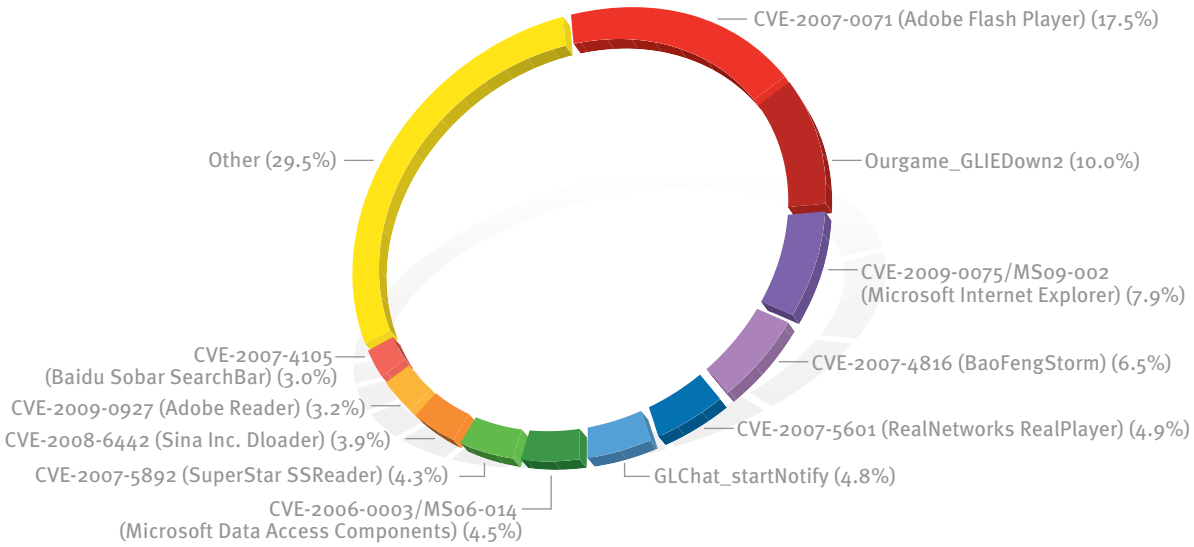
Top Browser-Based Exploits

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. To assess the relative prevalence of browser-based exploits in 1H09, 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 Vista,[28] 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.

Here and throughout this section, exploits affecting vulnerabilities in Microsoft software are labeled with the Microsoft Security Bulletin number pertaining to the vulnerability, if applicable.[29] Exploits affecting third-party software are labeled with the CVE identifier pertaining to the vulnerability, if applicable.

Figure 61 shows the browser-based exploits encountered by users in 1H09, ordered by frequency.

FIGURE 61. Browser-based exploits encountered, by percentage, in 1H09



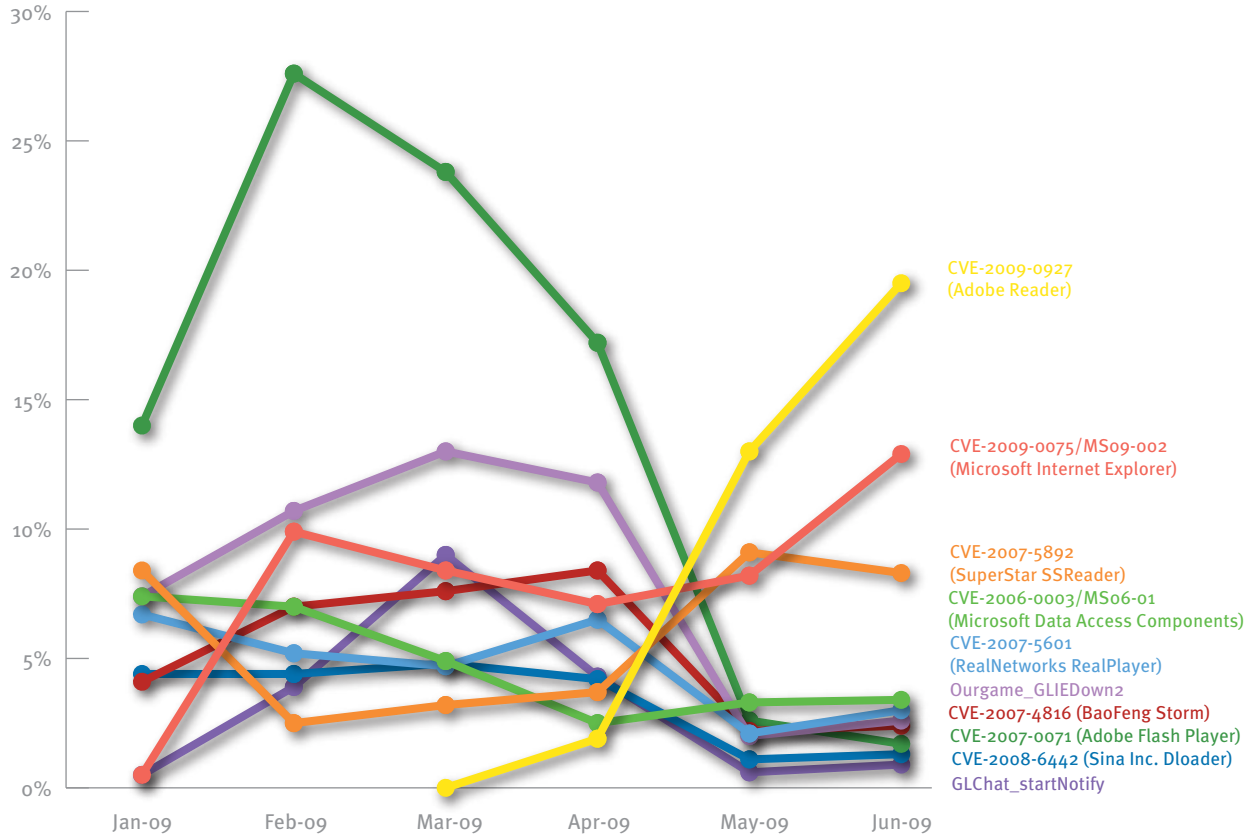
Many of the more prevalent exploits encountered take advantage of vulnerabilities in popular browser add-ons, with media players and games being frequent targets. As in 2H08, the most frequently exploited vulnerability in 1H09 was CVE-2007-0071, a vulnerability

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

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

in Adobe Flash Player, which accounted for 17.5 percent of the infected computers in the sample, up from 10.3 percent in 2H08. The next-most encountered exploit was for a vulnerability in Ourgame GLWorld, an online gaming ActiveX control popular in China. It accounted for 10.0 percent of incidents, up from 7.8 percent in 2H08. CVE-2008-1309, a vulnerability in the RealPlayer browser add-on from RealNetworks that was second on the list in 2H08, fell to just 0.2 percent of incidents. 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 62 shows, the incidence of several of the most prevalent exploits varied significantly from month to month in 1H09.

FIGURE 62. Top 10 browser-based exploits, by percentage of all exploits each month, in 1H09



CVE-2007-0071, the Adobe Flash Player vulnerability that was exploited the most overall in the sample, accounted for 27.6 percent of all exploits in February, but dropped to just 1.7 percent of the sample by June. Meanwhile, CVE-2009-0927, a vulnerability in Adobe Reader that first appeared in the April sample, rose to become the most exploited vulnerability in the June sample, with 19.5 percent of that month's total. Adobe Systems released a security update addressing the CVE-2007-0071 vulnerability in April 2008,[30] so the value

[30] For details and to obtain the security update, visit http://www.adobe.com/support/security/bulletins/apsb08-11.html.

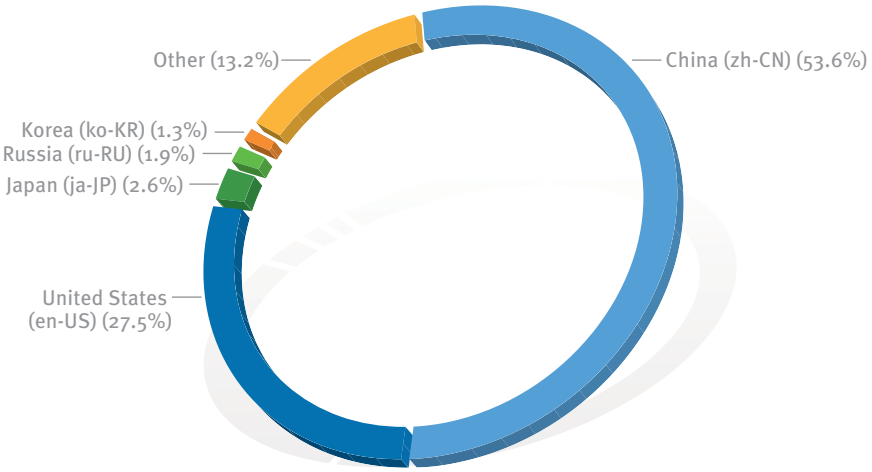
of CVE-2007-0071 exploits to attackers can be expected to have diminished as more users updated their versions of Flash Player. By contrast, CVE-2009-0927, a vulnerability in the Adobe Reader browser add-on, was first identified in March 2009 and was addressed by a security update released the following month.[31] Its rise in prevalence suggests that attackers have taken advantage of the fact that comparatively few users have installed the security update addressing the vulnerability.

Browser-Based Exploits by System Locale

Malware distributors target different parts of the world unequally. Victims are typically lured to exploit pages through a variety of methods, including phishing and hijacked Web pages. By nature, these lures tend to target specific segments of the global population. A phishing message written in German, for example, is more likely to be effective with potential victims who speak German than with those who do not. 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 63 shows the browser-based exploits encountered by users in 1H09, ordered by the system locale of the victim.

FIGURE 63. Browser-based exploits encountered, by system locale of victim, in 1H09



The most common system locale for victims in 1H09 was zh-CN (Chinese language, China), accounting for 53.6 percent of all exploits in the sample, up from 25.6 percent in 2H08. This rise was caused in part by a growth in the popularity of vulnerable versions of several Chinese-language ActiveX controls, including the Ourgame GlobalLink game client and the BaoFeng media player. The second-most common locale was en-US (English language, United States) at 27.5 percent, down from 32.4 percent and first place in 2H08.

[31] For details and to obtain the security update, visit http://www.adobe.com/support/security/bulletins/apsb09-04.html.

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 is very different from that of Windows XP.

Figure 64 and Figure 65 show the relative percentages of exploits against vulnerabilities in Microsoft and third-party software in 1H09 on computers running Windows XP and Windows Vista, respectively.

FIGURE 64. Browser-based exploits targeting Microsoft and third-party software on computers running Windows XP in 1H09

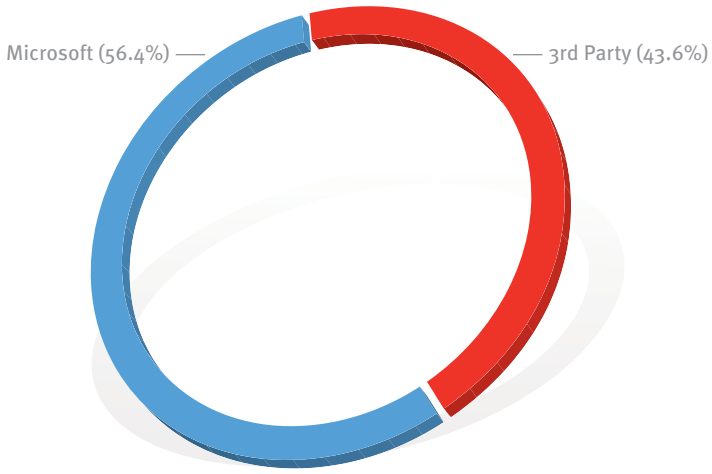
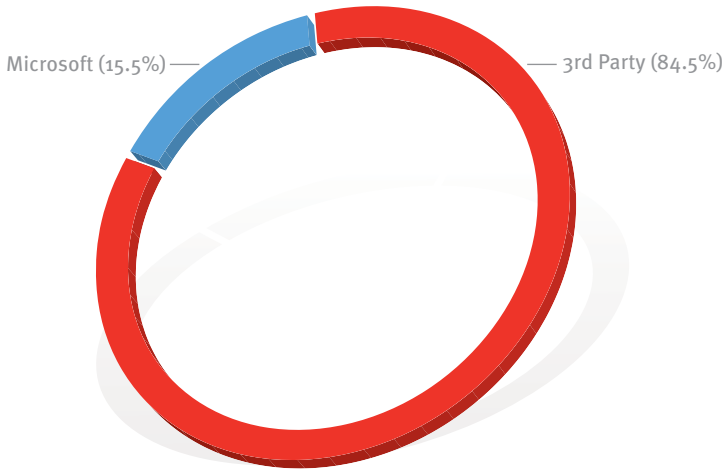


FIGURE 65. Browser-based exploits targeting Microsoft and third-party software on computers running Windows Vista in 1H09



In Windows XP, Microsoft vulnerabilities account for 56.4 percent of all attacks in the sample. In Windows Vista, the proportion of Microsoft vulnerabilities is much smaller, accounting for just 15.5 percent of attacks in the sample. Overall, the share of exploits attributable to Microsoft vulnerabilities has risen on both platforms since 2H08, due to exploitation of vulnerabilities in Internet Explorer that have been addressed by security bulletins MS08-078 (released in December 2008) and MS09-002 (released in February 2009).

Figure 66 and Figure 67 show the 10 vulnerabilities exploited most often in Windows XP and Windows Vista in 1H09, respectively.

FIGURE 66. The 10 browser-based vulnerabilities exploited most often on computers running Windows XP, by percentage of all exploits, in 1H09

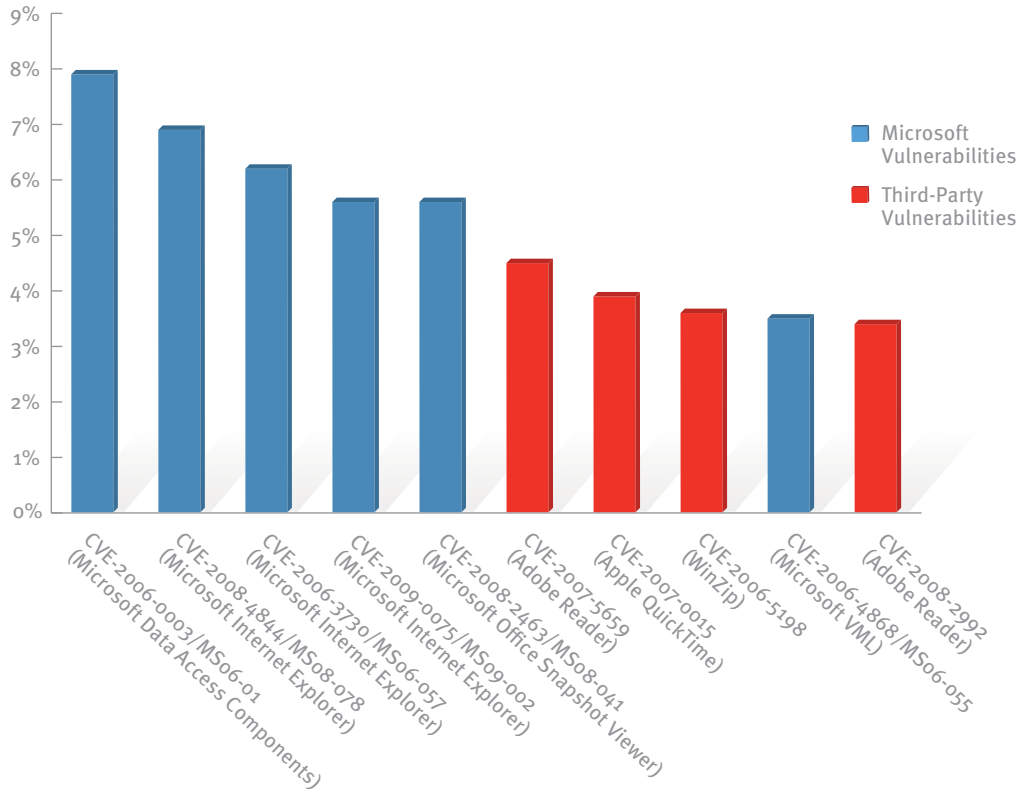
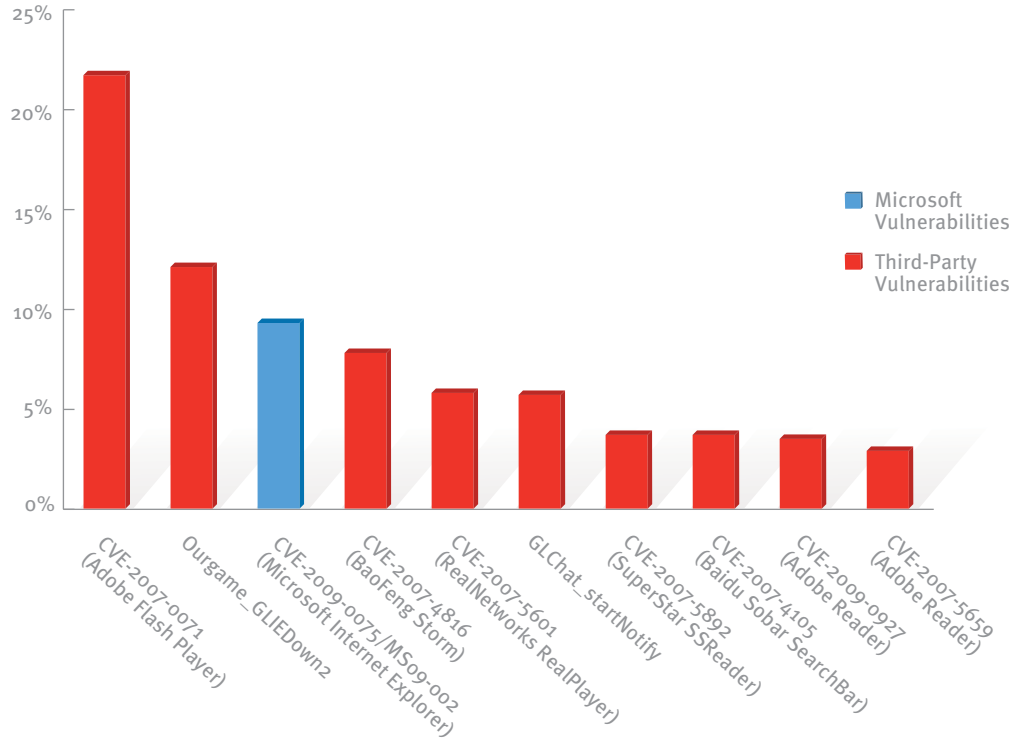


FIGURE 67. The 10 browser-based vulnerabilities exploited most often on computers running Windows Vista, by percentage of all exploits, in 1H09

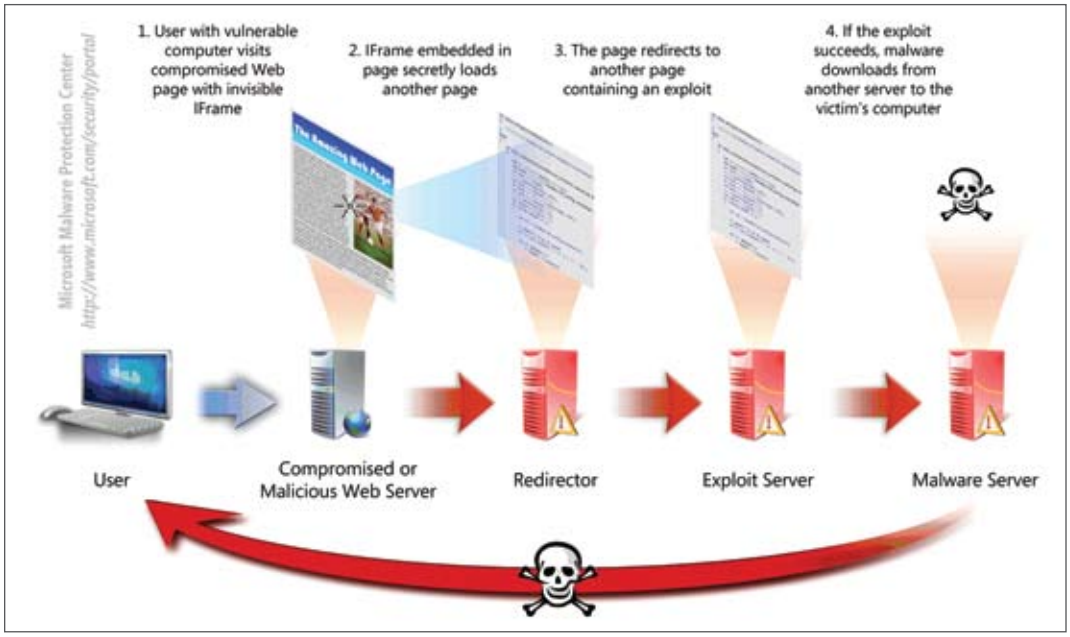


In Windows XP, Microsoft software accounts for 6 of the top 10 vulnerabilities, compared to 1 in Windows Vista. These figures are consistent with 2H08, when Microsoft vulnerabilities accounted for 6 of the top 10 vulnerabilities exploited on Windows XP and zero of the top 10 in Windows Vista.

Analysis of Drive-By Download Pages

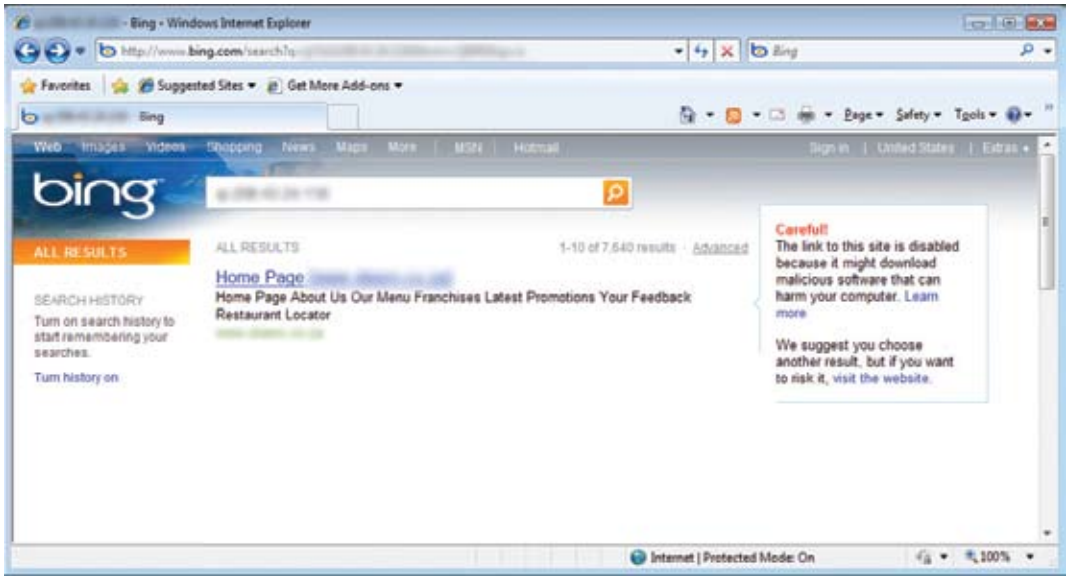
Drive-by download pages are usually hosted on legitimate Web sites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured Web form, like a comment field on a blog. Compromised sites can be hosted anywhere 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™ (formerly Live Search), have taken a number of measures to protect users from drive-by downloads.

FIGURE 68. 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 69. In 1H09, about 0.2 percent of the search results pages served to users by Bing contained warnings about malicious sites.

FIGURE 69. A drive-by download warning from Bing



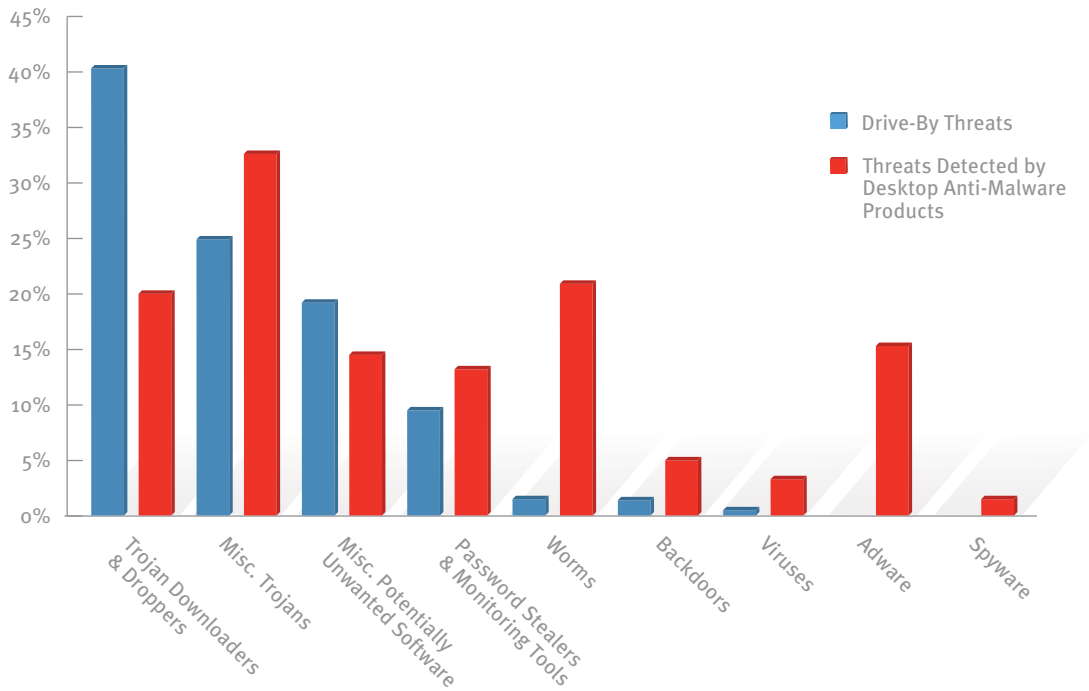
In most cases, the effect of a large drop in traffic originating from search engines (only about 2 percent of Bing users proceed to visit compromised sites after being shown the warning) serves to alert Webmasters that something has gone wrong. Bing works with Webmasters to inform them about compromised 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 Web sites affected has remained fairly consistent, with 0.16 percent of all Web sites hosting at least one malicious page.

Drive-By Malware Types

Figure 70 shows the category breakdown for drive-by download threat payloads (malware delivered through drive-by exploits) detected in 1H09, compared with the breakdown from all Microsoft desktop anti-malware products.

FIGURE 70. Types of threat payloads delivered through drive-by downloads in 1H09

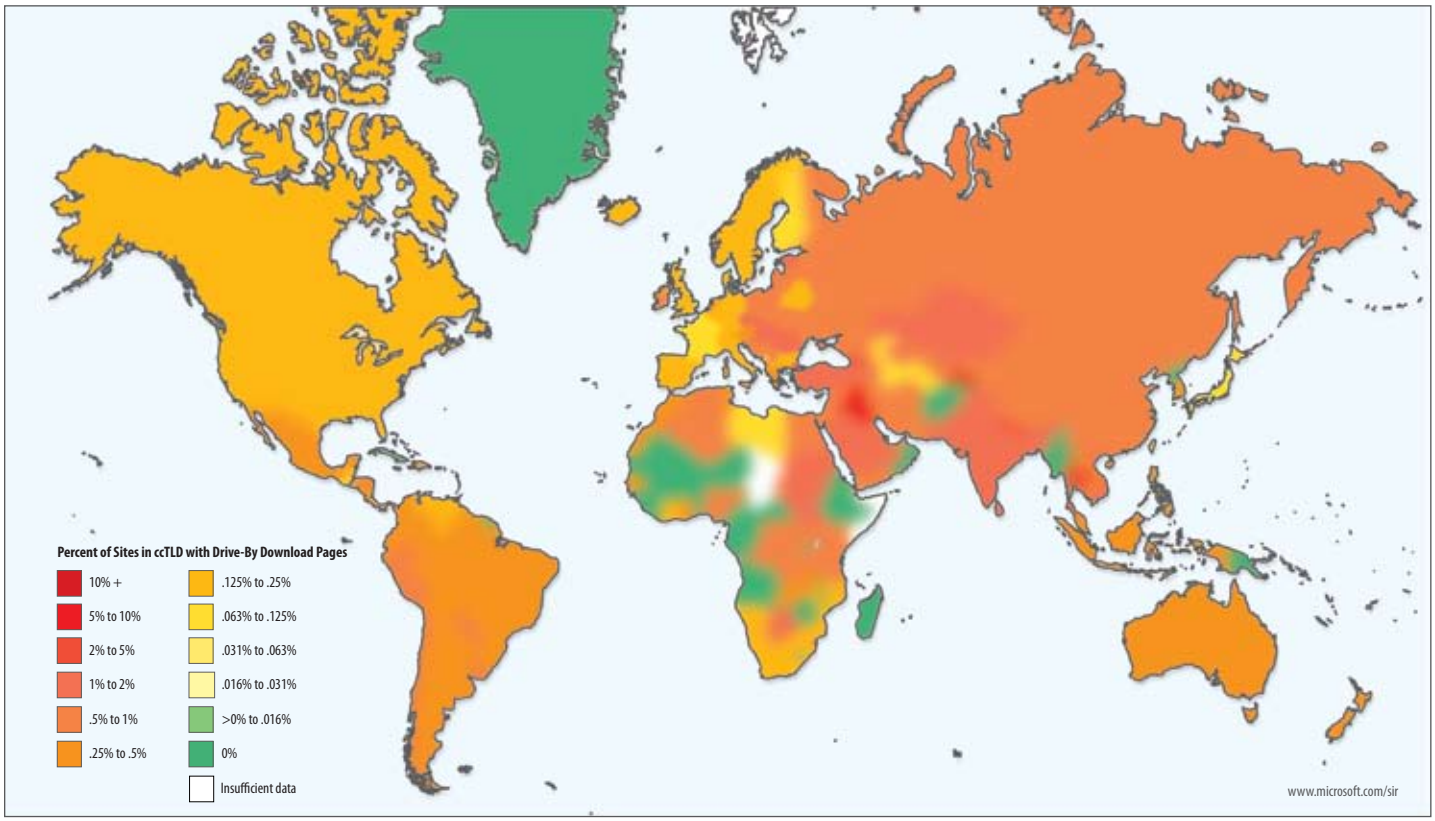


Trojan Downloaders & Droppers is the most frequently encountered category among drive-by download sites, with 40.7 percent of the total, twice as large as the category's share of threats detected by Microsoft desktop anti-malware products. Trojan downloaders are well suited for delivery by drive-by download because they can be used to install other threats on infected computers. Miscellaneous Trojans, Miscellaneous Potentially Unwanted Software, and Password Stealers & Monitoring Tools all account for significant percentages of the remaining threats, consistent with their prevalence among desktop threats.

Geographic Distribution of Drive-By Download Sites

While 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 71 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 1H09.

FIGURE 71. Percentage of Web sites in each country-code top-level domain (ccTLD) that hosted drive-by download pages in 1H09



Among ccTLDs that included at least one site hosting drive-by download pages, percentages varied greatly. More than 2.4 percent of the sites in the .th ccTLD (associated with Thailand) were found to be hosting drive-by download pages, but less than 0.1 percent of the sites in some other large ccTLDs, like .fr (associated with France), were similarly affected. (Note that Figure 71 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 71 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 as ccTLDs do, as illustrated by Figure 72.

FIGURE 72. Percentage of Web sites in each generic top-level domain that hosted drive-by download pages in 1H09

TLD	Percentage of sites hosting drive-by download pages
.int	0.99%
.coop	0.47%
.info	0.39%
.travel	0.34%
.name	0.31%
.biz	0.30%
.org	0.25%
.net	0.25%
.edu	0.22%
.aero	0.12%
.com	0.11%
.mobi	0.04%
.gov	0.03%

The .int TLD, which is reserved for organizations established by international treaty between or among national governments, contains the highest percentage of sites hosting drive-by download pages, with 0.99 percent of all active .int sites found to contain such pages. (Due to its strict eligibility requirements, .int is also one of the smallest of the generic and sponsored TLDs, with an active site count in the hundreds, and so may be considered a statistical outlier.) Most of the more heavily used generic and sponsored

TLDs are clustered between 0.1 and 0.4 percent. Several generic and sponsored TLDs were not found to be hosting any Web sites with drive-by download pages, including .jobs, .museum, and .mil.

Some network operators (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. As Figure 73 shows, 17.8 percent of the sites hosted by one network operator were found to contain drive-by pages, with several others showing site infection rates between 4 and 8 percent.

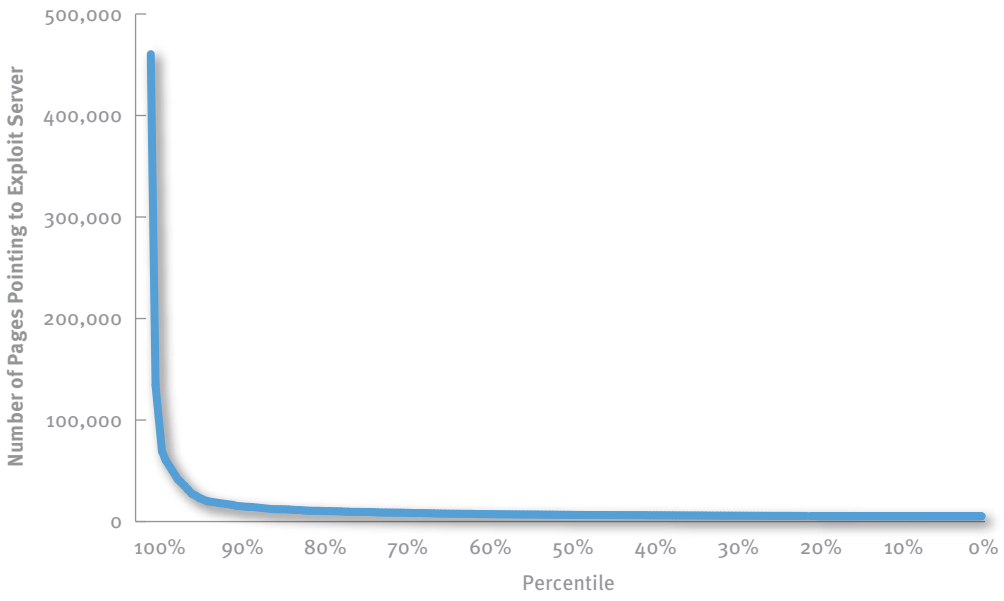
FIGURE 73. The 10 network operators providing hosting services to the largest percentage of compromised hosts in 1H09

Autonomous System (AS) Name	Location	% of Sites Containing Drive-By Pages
COLOSOLUTIONS (Colo Solutions, Inc.)	United States	17.8%
WEB4CE (Web4ce, s.r.o.)	Czech Republic	7.2%
NEOLABS-AS (Neolabs Ltd.)	Kazakhstan	7.1%
OLD-HT-SYSTEMS-AS (JSC Hosting Telesystems autonomous system)	Russia	6.5%
AWAX-AS (AWAX Telecom Ltd)	Russia	6.1%
CLAXTELECOM (Clax Telecom)	Romania	5.7%
ZEELANDNET (ZeelandNet BV)	The Netherlands	5.5%
GEARHOST (GearHost, Inc.)	United States	5.0%
SLOVANET (Slovanet, a.s.)	Slovakia	4.9%
OMEGABYTE-COMPUTER-CORPORATION (Omegabyte Computer Corporation)	United States	4.4%

Distribution of Exploit Servers

Most drive-by download attacks use malware distribution networks, similar to the one depicted in Figure 68 on page 119. Rather than being completely self-contained, the exploit code itself is hosted on a different Web site 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.) Analyzing the URLs that host the malicious code or inline frames themselves reveals that a small handful of exploit servers host the exploits used by the vast majority of drive-by download pages worldwide, as shown in Figure 74.

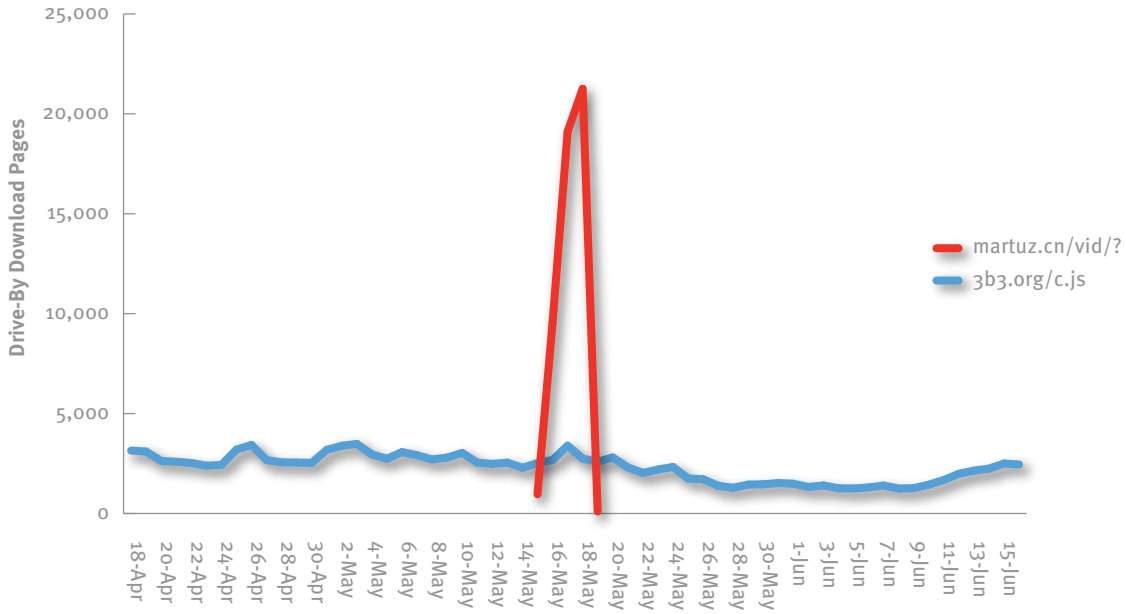
FIGURE 74. Percentile distribution of exploit servers by the number of drive-by pages pointing to each one, 1H09



In 1H09, the top exploit servers—those that provided exploit code for more than 10,000 drive-by download pages each—made up about 11.0 percent of all exploit servers detected but accounted for 74.0 percent of drive-by download pages. This is consistent with 2H08, when the top servers accounted for 12.8 percent of exploit servers and 84.1 percent of drive-by download pages. One significant change is that the number of drive-by pages served by the exploit servers at the very top of the curve has increased exponentially. In 2H08, the most heavily used exploit server in the world had a reach of around 100,000 pages. Most exploit servers still have a reach well below this, but the reach of the top server is much greater in 1H09, at more than 450,000 pages. Despite this, very few of the servers at the top of the list in 2H08 remain there in 1H09. Malware distribution networks tend to be moving targets, with servers constantly appearing and disappearing in different locations.

One illustration of this phenomenon, and a contributing factor to the increased reach of the top servers, was a series of attacks in April and May 2009 in which huge numbers of legitimate Web pages were compromised over a very short period of time. Figure 75 gives an example of one of these attacks.

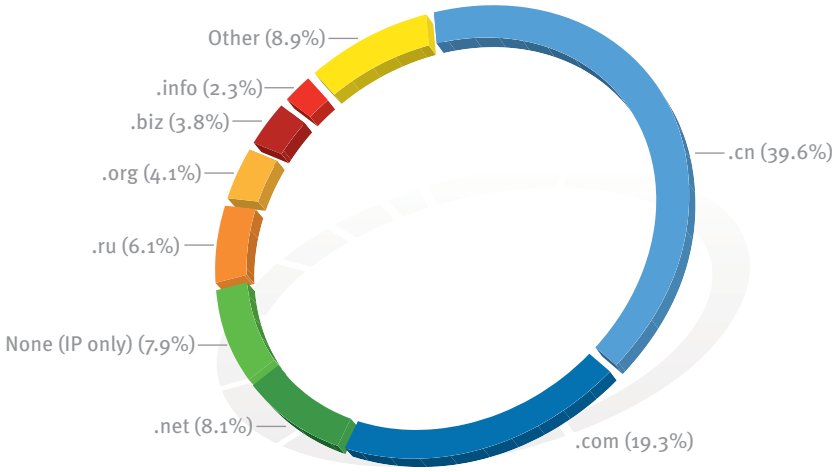
FIGURE 75. Drive-by download pages pointing to exploit servers martuz.cn and 3b3.org during May 2009



The blue line shows the number of drive-by download pages detected daily during a two-month period pointing to a malicious script hosted at 3b3.org, a typical heavily used exploit server. The reach of this server remained steady throughout the period, never varying by more than about 1,000 pages from the mean. By contrast, the red line shows drive-by pages pointing to martuz.cn, an exploit server used in one of the attacks mentioned previously. After being detected for the first time on Friday, May 15, its reach jumped quickly to more than 21,000 active compromised pages by Monday, May 18, before dropping to just 100 active pages the following day, and none after that. Attacks like these have been seen before, but the speed at which the attackers are able to infect legitimate pages is a new development, perhaps made possible by tools such as the sort examined in "Automated SQL Injection Attacks," beginning on page 102.

The TLD distribution of exploit servers is very different from that of the compromised pages that point to them, as illustrated by Figure 76.

FIGURE 76. Drive-by exploit servers, by TLD, in 1H09



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 .cn (39.6 percent) and .com (19.3 percent). About 8 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 populated 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 popular Microsoft Office binary file formats (including .doc, .xls, and .ppt). 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 speed, 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 extracts malware buried inside the document. Real-time antivirus scanning can help mitigate the danger from these attacks in some cases.

Microsoft Office Format Exploits

To assess the use of file formats as an attack vector, Microsoft analyzed a sample of several hundred files that were used for successful attacks in 1H09. The data set was taken from submissions of malicious code sent to Microsoft from customers worldwide.

In total, exploits for 11 different vulnerabilities were identified in the sample set, as shown in Figure 77.

FIGURE 77. Vulnerabilities exploited in Microsoft Office file formats

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
MS06-037	July 2006	Excel File Rebuilding Overflow	CVE-2006-2388
MS06-048	August 2006	PowerPoint Mso.dll Vulnerability	CVE-2006-3590
MS06-060	October 2006	Word Mail Merge Vulnerability	CVE-2006-3651
MS07-014	February 2007	Word Malformed Data Structures Vulnerability	CVE-2006-6456
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

Of these 11 vulnerabilities, 9 had security updates available at the time of attack. The affected users were exposed because they had not applied the updates. Two vulnerabilities (CVE-2009-0238 in Excel and CVE-2009-0556 in PowerPoint) were used in zero-day exploits before security updates were available. Office 2000, Office XP, Office 2003, and the 2007 Microsoft Office system were each affected by at least 1 of the 11 vulnerabilities (see Figure 81, on page 130, for details).

Most of the vulnerabilities exploited in the sample were several years old, and more than half were first identified in 2006. As Figure 78 illustrates, 71.0 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 three years by the end of 1H09.

FIGURE 78. Microsoft Office file format exploits encountered, by percentage, in 1H09

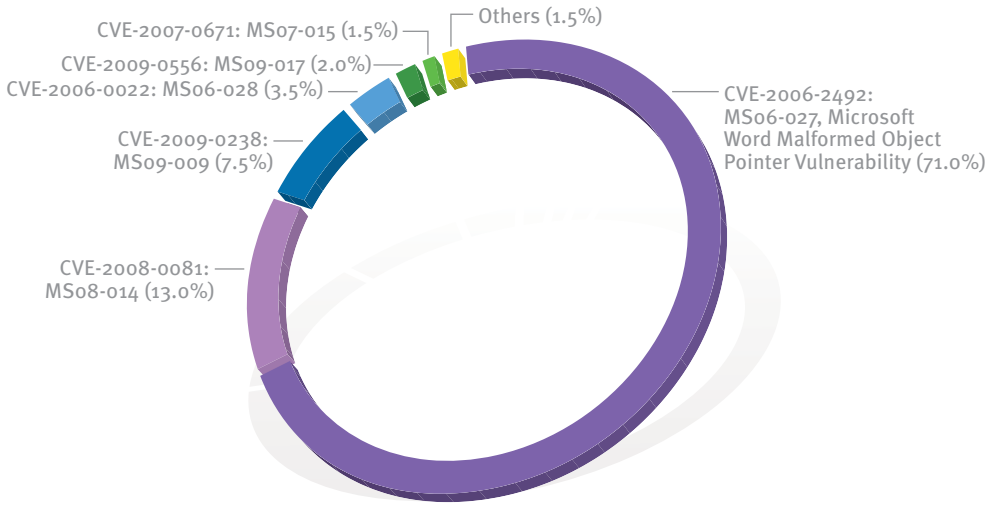
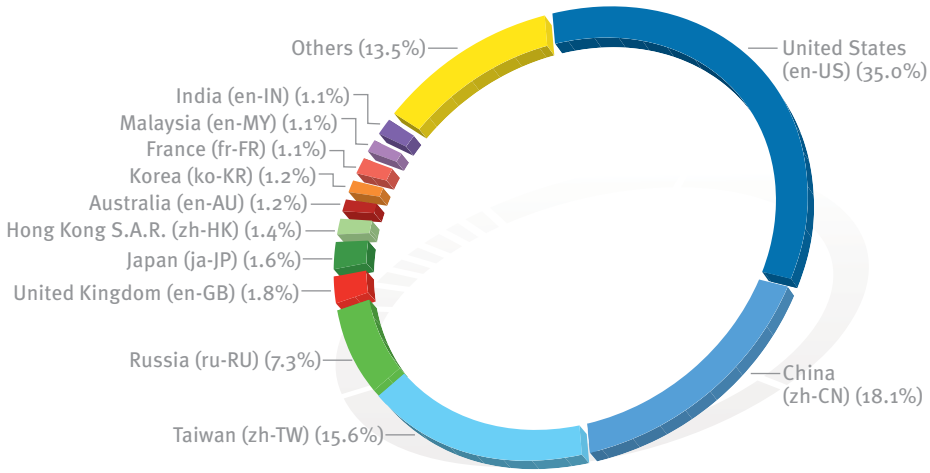


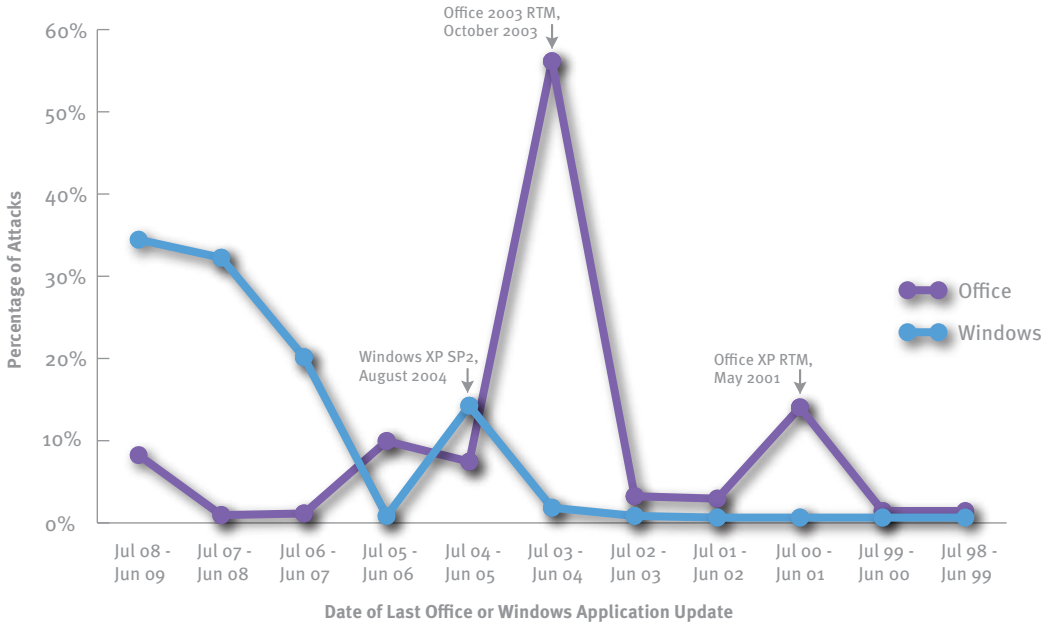
Figure 79 shows Microsoft Office file format exploits ordered by the system locale of the victim. The most common locale for victims was en-US (English language, United States), accounting for 35.0 percent of all incidents, followed by zh-CN (Chinese language, China), with 18.1 percent of incidents.

FIGURE 79. Microsoft Office file format exploits encountered, by system locale of victim, in 1H09



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 80 compares attacks observed in the sample set against Windows and Office during 1H09.

FIGURE 80. Microsoft Office file format exploits encountered, by date of last Windows or Office program update, in 1H09



The horizontal axis shows the last date that the computers in the sample set were updated with security updates for Windows and Office. For example, just 7.6 percent of Office attacks observed in 1H09 affected Office program installations that had been updated between July 2008 and June 2009 (in other words, within one year of the end of 1H09). The majority of Office attacks observed in 1H09 (55.5 percent) affected Office program installations that had last been updated between July 2003 and June 2004. Most of these attacks affected 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.

By contrast, the computers in the sample set were significantly more likely to have had recent Windows security updated applied. More than a third of the Office attacks observed in 1H09 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 1.2 years, compared to 5.6 years for the most recent Office program update. This is not because 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 161.)

To further illustrate the importance of applying all service packs and other security updates, Figure 81 and Figure 82 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 81. Vulnerabilities affecting RTM versions of Office 2000–2007

Vulnerability	Bulletin	Office 2000 RTM	Office XP RTM	Office 2003 RTM	Office 2007 RTM
CVE-2006-0022	MS06-028	Yes	Yes	Yes	No
CVE-2006-2388	MS06-037	Yes	Yes	Yes	No
CVE-2006-2492	MS06-027	Yes	Yes	Yes	No
CVE-2006-3590	MS06-048	Yes	Yes	Yes	No
CVE-2006-3651	MS06-060	Yes	Yes	Yes	No
CVE-2006-6456	MS07-014	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

FIGURE 82. Vulnerabilities affecting Office 2000–2007 with latest service packs installed

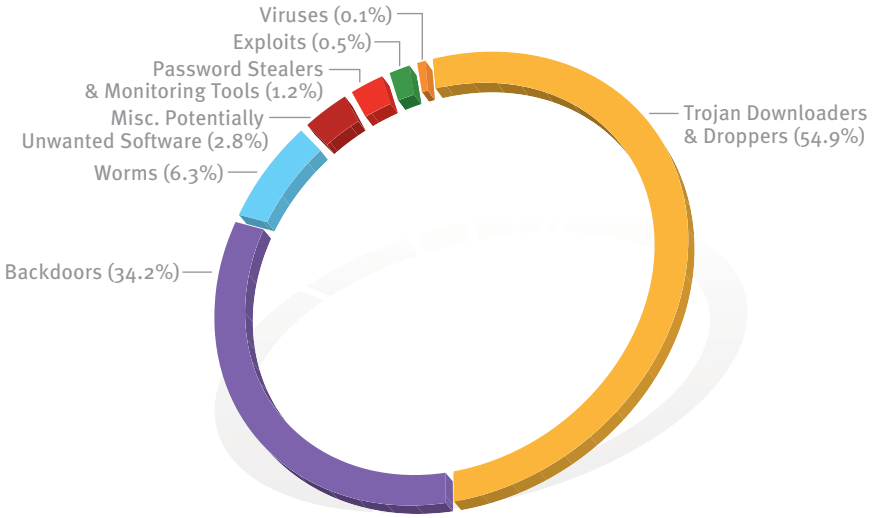
Vulnerability	Bulletin	Office 2000 SP3	Office XP SP3	Office 2003 SP3	Office 2007 SP2
CVE-2006-0022	MS06-028	Yes	Yes	No	No
CVE-2006-2388	MS06-037	Yes	Yes	No	No
CVE-2006-2492	MS06-027	Yes	Yes	No	No
CVE-2006-3590	MS06-048	Yes	Yes	No	No
CVE-2006-3651	MS06-060	Yes	Yes	No	No
CVE-2006-6456	MS07-014	Yes	Yes	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

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 4 of the 11 vulnerabilities. If the Office 2003 RTM users in the sample had installed SP3 and no other security updates, they would have been protected against 98 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 and Office XP are each affected by all 11 of the vulnerabilities exploited in the sample, even with the latest service pack installed. Users of any of these Office versions who install all 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 11 of these vulnerabilities, as of July 2009.

As Figure 83 illustrates, nearly 90 percent of Microsoft Office exploits involve either a trojan downloader or dropper, or a backdoor. These kinds of threats allow attackers to access compromised systems later to install more malware.

FIGURE 83. Categories of payloads delivered by Microsoft Office exploits in 1H09



Encyclopedia

Win32/Buzus: A trojan that downloads malware known as "SpywareIsolator," a rogue security software program.

Win32/Poisonivy: A family of backdoor trojans that allow unauthorized access to and control of an affected machine. Poisonivy attempts to hide by injecting itself into other processes.

http://www.microsoft.com/av

Among trojan categories, the top 10 families together account for more than 70 percent of payloads using trojans. Win32/Buzus, the most prevalent family on the list, holds the top spot because it was used in a large number of apparently related .xls file exploits detected in April 2009.

FIGURE 84. Top 10 trojan families used in Office file exploits in 1H09

Family	Most Significant Category	Percent of Trojans
Win32/Buzus	Trojan Downloaders & Droppers	29.5%
Win32/AgentBypass	Miscellaneous Trojans	11.7%
Win32/Enfal	Miscellaneous Trojans	11.3%
Win32/Small	Miscellaneous Trojans	6.4%
Win32/SystemHijack	Miscellaneous Trojans	3.0%
Win32/ProcInject	Miscellaneous Trojans	3.0%
Win32/Malres	Trojan Downloaders & Droppers	2.6%
Win32/Kirpich	Trojan Downloaders & Droppers	2.3%
Win32/Malagent	Miscellaneous Trojans	2.3%
Win32/Bumat	Miscellaneous Trojans	2.3%

In the Backdoors category, Win32/Poisonivy, the single most prevalent family overall, accounted for 61.4 percent of all backdoor payloads and 21 percent of all exploits.

FIGURE 85. Top 10 backdoor families used in Office file exploits in 1H09

Family	Most Significant Category	Percent of Backdoors
Win32/Poisonivy	Backdoors	61.4%
Win32/Bifrose	Backdoors	7.4%
Win32/Ripinip	Backdoors	5.5%
Win32/Difeqs	Backdoors	4.1%
Win32/Riler	Backdoors	3.9%
Win32/Farfli	Backdoors	2.8%
Win32/Delf	Backdoors	2.5%
Win32/PcClient	Backdoors	2.3%
Win32/Veden	Backdoors	2.3%
Win32/Agent	Backdoors	1.8%

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 what goes wrong with information security. 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 1H09 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.[32] The categories are shown in Figure 86.

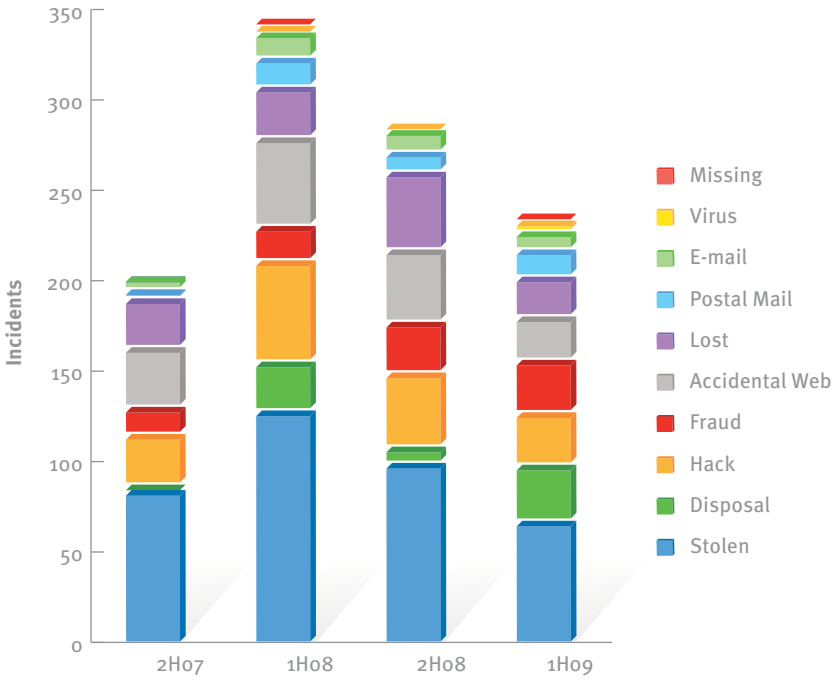
[32] The OSF DataLossDB includes a small number of incidents for which the breach type is listed as "Unknown." These incidents are not included in the data and analysis presented in this report.

FIGURE 86. 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	Email
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 87 illustrates the overall distribution of incidents by type since 2H07.

FIGURE 87. Security breach incidents, by incident type, 2H07–1H09



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

- Although security breaches are often linked in the popular consciousness with hacking incidents involving malicious parties defeating technical security measures to gain unlawful access to sensitive data, more than four-fifths of all breaches tracked in the DataLossDB result from something that the OSF database does not classify as a hack, including 87.7 percent of reported 1H09 breaches. Stolen equipment is the largest single category and accounts for twice as many incidents as intrusion, possibly because equipment theft is easily detected and reported. A number of the incident reports reviewed for this analysis mentioned that intrusions or accidental exposure of information on the Web had been going on for quite a while before they were detected.
- Although still high, the percentage of breaches resulting from theft has declined significantly over the past two years. In absolute terms, theft incidents have fluctuated along with other breach types, ranging from 129 incidents in 1H08 to 68 incidents in 1H09. 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. If encrypted data falls into malicious hands, it is much more difficult for the finder or retriever to extract than unencrypted data is, which is why disclosure laws typically do not require notification when encrypted data is stolen.

- Improper disposal of business records accounts for quite a few incidents and is relatively easy for organizations to address by effectively developing and enforcing policies regarding the destruction of paper and electronic records containing sensitive information.
- Overall, the data 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.

Social Security Numbers and Confidentiality

In the United States, many organizations use the nine-digit federal Social Security number (SSN) to authenticate customers, employees, users, and other people. As the number of jurisdictions adopting breach disclosure laws has increased, the body of information generated by databases such as the DataLossDB has highlighted the significant risks created by the use of SSNs for authentication.

In 1H09, the DataLossDB held information about data confidentiality breaches affecting approximately 323 million SSNs, exceeding the total population of the United States. Some of these records are years or decades old, including a 1984 incident involving the credit-reporting bureau TRW (now Experian) in which 90 million records were put at risk. Even so, the magnitude of these breaches illustrates how authentication schemes that assume the confidentiality of SSNs are fundamentally problematic.

In the context of records management, *identification* and *authentication* are two related, but distinctly different, concepts. Identification means using a unique label or value—the *identifier*—to distinguish a single record from all others. Authentication, by contrast, refers to a system for confirming the identity of a particular person or thing. When a user logs on to Windows, for example, their user name is used for identification and their password is used for authentication.

Social Security numbers are guaranteed to be unique to each person, and most people commit their SSNs to memory with little trouble, two factors that lead organizations to use them as identifiers. (Nevertheless, other factors make SSNs a poor choice for identifiers: They are too short, they lack a check digit, and most people outside the United States don't have one.) The universality and ease of use of SSNs have also

prompted many organizations in the United States to use them for authentication purposes. Compared to passwords, however, SSNs are unsuitable for authentication for multiple reasons:

- **Usage with multiple accounts:** Users typically choose a new password every time they establish a new computer or Web site account, and every password can be unique, although users often choose the same password for multiple accounts. SSNs are used for authentication by countless service providers, and cannot be varied.
- **Complexity rules:** Passwords often must satisfy a minimum length requirement or contain capital letters, lowercase letters, numbers, or symbols in various combinations. SSNs always consist of exactly nine digits.
- **Changeability:** Users are usually allowed to change their passwords frequently and are sometimes required to do so. Most people have the same SSN for their entire lives.
- **Ease of change:** Computers and Web sites usually provide ways for users to easily change their passwords. People are only allowed to change their SSNs in certain rare cases.
- **Secrecy:** Computer users are reminded repeatedly to keep their passwords secret and to avoid sharing them with anyone. People routinely share their SSNs with a wide variety of service providers, and privacy breaches involving SSNs are common.

It is not clear how many individual SSNs belonging to people who are alive today have been affected by incidents recorded in the DataLossDB. The figure cited earlier does not imply that 323 million unique, individual SSNs have been put at risk. It seems certain that some numbers have been disclosed repeatedly, and others have never been disclosed at all. There is likely a correlation with age (people who have had SSNs longer would have been asked to give them out more often, and older people are more likely to have had their SSNs used as their driver's license numbers, a practice that fewer states are using today). There is likely a correlation with privacy sensitivity. Many people have been born since the 1984 TRW breach, and others have passed away. All of these factors make it difficult to estimate the magnitude of the problem to any reliable degree.

It seems likely that over the next few years, as SSNs become easier for criminals to acquire, either through breach incidents or simply by guessing,[33] the use of the SSN as an authenticator will be called harshly into question. Replacing it will not be easy and may not be quick.

[33] See Alessandro Acquisti and Ralph Gross. "Predicting Social Security numbers from public data." *Proceedings of the National Academy of Sciences of the United States of America*, Vol. 106, No. 27 (July 7, 2009): 10975. http://www.pnas.org/cgi/doi/10.1073/pnas.0904891106

Guidance for Organizations: Protecting Against a Data Breach

In order to limit exposure to the risk of a data breach, Microsoft recommends that companies choose and implement data security and privacy policies in the context of a comprehensive data governance strategy, as part of their overall governance, risk, and compliance (GRC) efforts. This strategy should comprise policies, procedures, and standards to enable effective use of the organization's structured and unstructured data, in several ways:

- By improving business decision-making due to increased data accuracy
- By reducing data redundancy and related maintenance costs
- By ensuring compliance with laws and regulations
- By reducing exposure of the company's data to loss or theft

A key component of any data governance program is a technology framework that can help organizations protect and manage personal information, mitigate risk, achieve compliance, and promote trust and accountability. Key elements of this framework include the following:

- **Secure infrastructure:** Products and technologies that provide services such as application level anti-malware checks, and automatic patching of clients and servers which limit the attack surface in core IT infrastructure elements such as the operating system.
- **Identity and access control:** Authentication and authorization technologies that help prevent unauthorized access to information while seamlessly facilitating its availability to legitimate users.
- **Information protection:** Including data encryption, file classification, rights management, and data leak prevention technologies that help safeguard information against data breaches resulting from loss or theft.
- **Auditing and reporting:** Products and technologies that can be used to verify that systems and controls are operating effectively and to identify suspicious or noncompliant activity.

In addition to the above described measures, organizations should have a breach notification response plan in place and tested before needing it. Large organizations that do business in many different locales often have to conform to a complicated mixture of breach notification laws. Rather than trying to enact specific notification practices in every locale, organizations may find it simpler to uniformly adhere to the most stringent applicable requirements wherever possible.

To assist customers in their data governance, risk management, and compliance efforts, Microsoft has developed a number of technology-based tools and guidance documents that can be downloaded at no cost from http://www.microsoft.com/datagovernance. Microsoft will continue to add resources in the future, such as a guide to the creation of a data governance program that is scheduled for publication in early 2010.

Strategies, Mitigations, and Countermeasures

- Install Internet Explorer 8 to take advantage of a number of features that can help you reduce browser-based risk, including:[34]
  - **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 time 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 & Management:** Allows for greater management of ActiveX controls, such as where and how they can load, specify which sites can use the control, as well as 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.
- Avoid browsing to sites that you do not trust. The use of Extended Validation (EV) certificates and the Domain Name Highlighting features in Internet Explorer 8 will assist users in making the proper choices, but awareness that these sites exist are key in protecting your users.
- Have your internal developer 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.
- Determine what security controls your search engine provider has implemented to help reduce the threat posed to your users by drive-by download attacks.
- 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 the revised User Account Control in Windows 7 to ensure that any malware that makes it through the defenses is not capable of elevating its privilege to run as anything higher than a normal user. If an attack requires administrator access, it will not run unless an administrator specifically allows it.

[34] 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.

- Enable Data Execution Prevention (DEP) and Structured Exception Handling Overwrite Protection (SEHOP) in compatible versions of Windows, which can help prevent a class of exploits known as buffer overflows. You can enable DEP and/or SEHOP using the EMET Enhanced Mitigation Evaluation Tool (EMET; http://go.microsoft.com/fwlink/?LinkId=162309). You can enable DEP for Office applications using the FixIt4Me tool (http://go.microsoft.com/?linkid=9668625).
- Encrypt data on all computers and storage devices, including thumb drives. Full volume encryption solutions should be consistent with high encryption algorithms such as AES. You should also ensure that the proper Domain Recovery Agents (DRA) are in place prior to the implementation of a domain policy, in order to ensure that data can be recovered in the event of a lost or damaged encryption key.
- Use the Microsoft Security Assessment Tool (MSAT; http://technet.microsoft.com/en-us/security/cc185712.aspx) to help identify risks in your IT security environment and build a plan to successfully manage the risk.
- 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.
- 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.
- Do not rely on Social Security numbers for authentication purposes. If your organization uses Social Security numbers for account identification, consider whether a different identification scheme would be more appropriate.
- Understand and prioritize critical assets with the business owners to ensure proper coverage of the correct assets. This includes the identification and classification of data into risk categories (i.e., High Business Impact, Medium Business Impact, Low Business Impact). It is imperative that the business owners are an integral part of this process, as they can provide insight into their business and competitive advantage that IT typically cannot. In addition, the determination of what constitutes an "acceptable level of loss" needs to be understood and communicated.
- Coordinate your IT security plan with your security plan to help control access to data centers or other high risk areas.
- 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. Perform small-scale drills (like conference room role-playing scenarios) more frequently, and use them to identify areas for future emphasis.

Microsoft Security Response Center

The **Microsoft Security Response Center** 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 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 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.

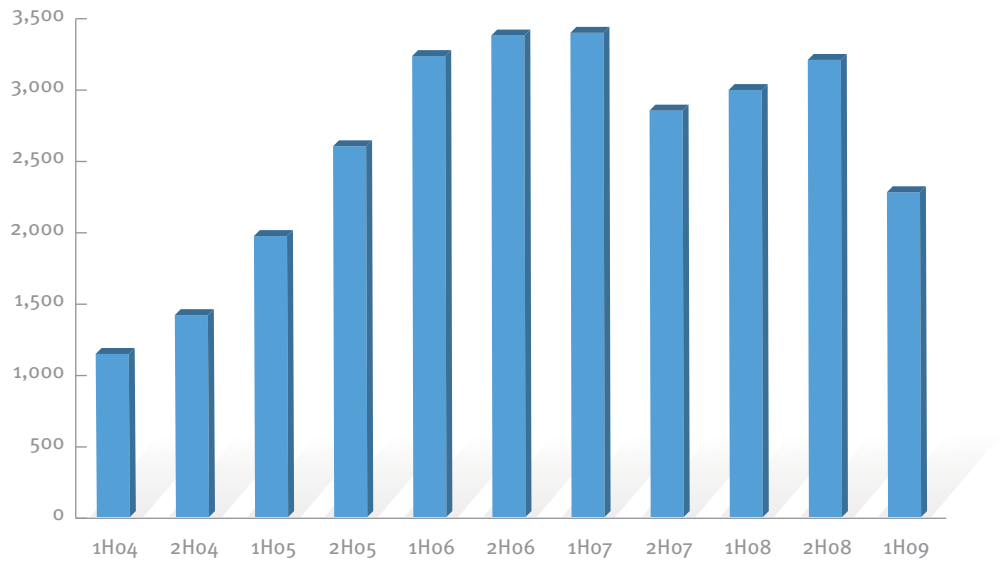
This section of the *Microsoft Security Intelligence Report* analyzes new vulnerabilities that were disclosed during the first half of 2009 and examines trends in vulnerability disclosures since 2004. A *disclosure*, as the term is used in this report, is the revelation of a software vulnerability to 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 150, for Microsoft-specific vulnerability information.

Vulnerability Disclosures

In 1H09, disclosed vulnerabilities across the software industry declined 28.4 percent from the previous half-year period, reversing a trend of small period-to-period increases observed since 2H07. Figure 88 illustrates the number of vulnerability disclosures across the software industry for each half-year period since 1H04.

FIGURE 88. Industry-wide vulnerability disclosures by half-year, 1H04–1H09



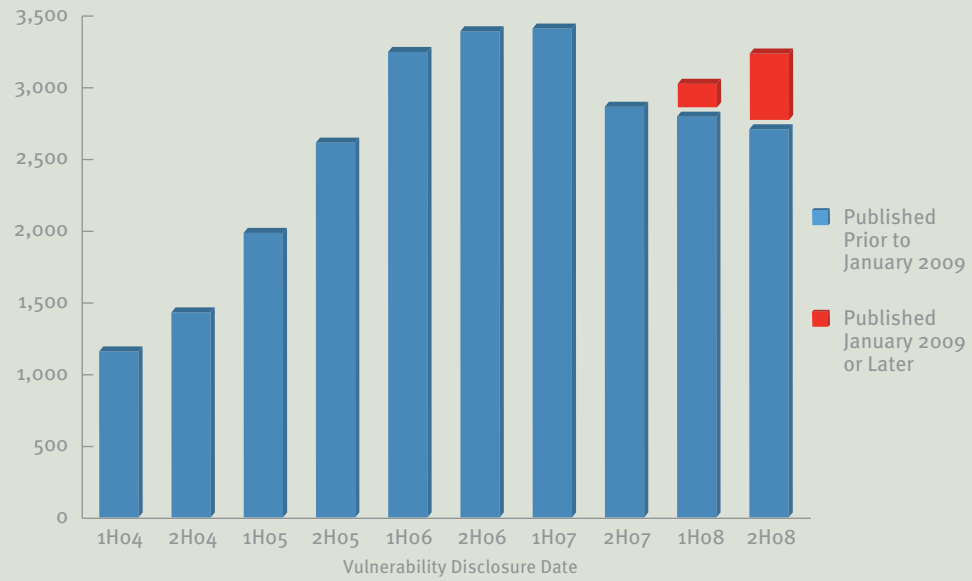
Vulnerability Disclosure Date vs. Publication Date

In this section and in "Vulnerability Reports for Microsoft Products," beginning on page 150, vulnerabilities are counted and charted for trends based upon the date when the vulnerability was first disclosed.

Another key date associated with each vulnerability is its publication date, which is the date the vulnerability is first assigned a Common Vulnerabilities and Exposures (CVE) identifier and published in the Mitre CVE list (http://cve.mitre.org) or the NIST National Vulnerability Database (http://nvd.nist.gov). Usually, but not always, the length of time between the publication and disclosure dates is relatively short and has little impact on the trend analysis. For example, from 2005 through the end of 2007, less than 5 percent of the vulnerabilities disclosed in each half-year period were published more than 30 days beyond the end of the period.

For both 1H08 and 2H08, however, a significant percentage of vulnerabilities disclosed during those periods were not published until 2009—enough to have a noticeable effect on the reported disclosure trend, as shown in Figure 89.

FIGURE 89. Industry-wide vulnerability disclosures and publications by half-year, 1H04–2H08



The blue portion of each bar represents the vulnerability disclosures for each half-year period that had been published as of December 31, 2008. Red represents vulnerability disclosures for each period that have been published since January 1, 2009. These revisions show that what had previously appeared to be a slight downward trend from 2H07 to 2H08 was, in fact, a slight upward trend over the same time.

The chart also shows that the count of vulnerability disclosures for earlier periods has been stable since the beginning of 2009, which raises confidence in the observed trends for those periods.

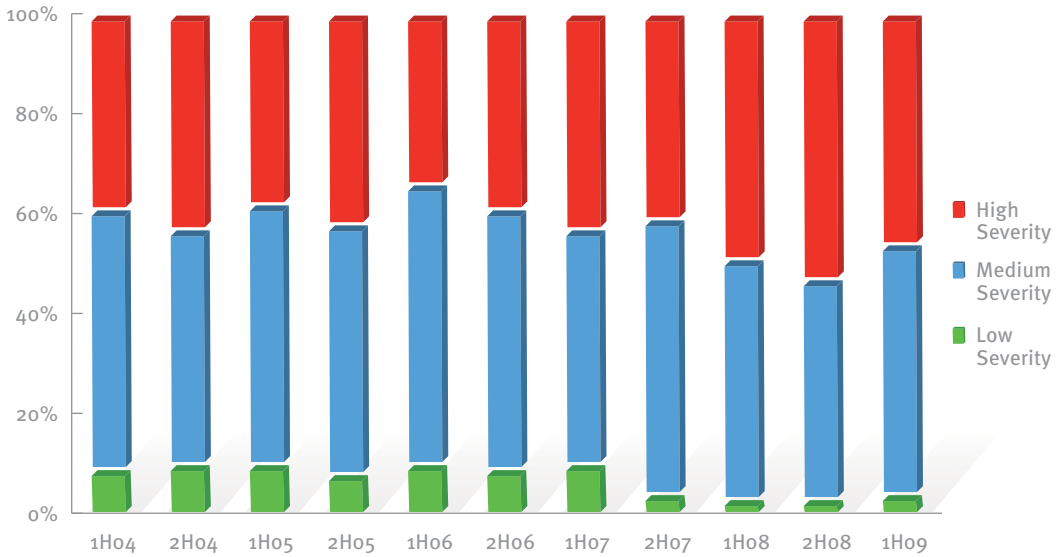
Vulnerability Severity

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. (See "Exploitability Index," on page 155, for information about another metric that can aid in prioritization.)

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.[35]

As Figure 90 illustrates, the drop in total vulnerabilities seen in 1H09 was accompanied by a drop in the percentage of all vulnerabilities rated High severity and a slight increase in the percentage of vulnerabilities rated Low severity. High severity vulnerabilities accounted for 46.0 percent of all vulnerabilities, down from 52.8 percent in 2H08. Low severity vulnerabilities accounted for 4.1 percent of all vulnerabilities, up from 3.2 percent in 2H08. The continuing predominance of High 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 develop more effective attacks, while legitimate researchers focus on finding the vulnerabilities that could cause the most damage if exploited, so software vendors can address them quickly.

FIGURE 90. Industry-wide vulnerability disclosures by severity, 1H04–1H09



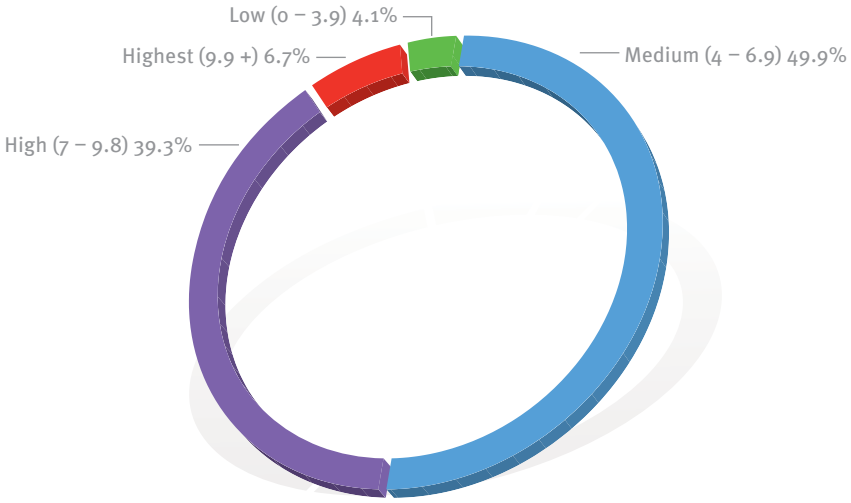
[35] For an explanation of the CVSS scoring methodology, see http://www.first.org/cvss/cvss-guide.html#i3.

Focusing on mitigating the most severe vulnerabilities first is a security best practice. While CVSS, through the National Vulnerability Database (NVD),[36] 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 about 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 91 illustrates the severity breakdown for 1H09. 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 represent 6.7 percent of all vulnerabilities disclosed.

FIGURE 91. Industry-wide vulnerability disclosures by severity, 1H09



[36] 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 92 gives definitions for these designations.[37]

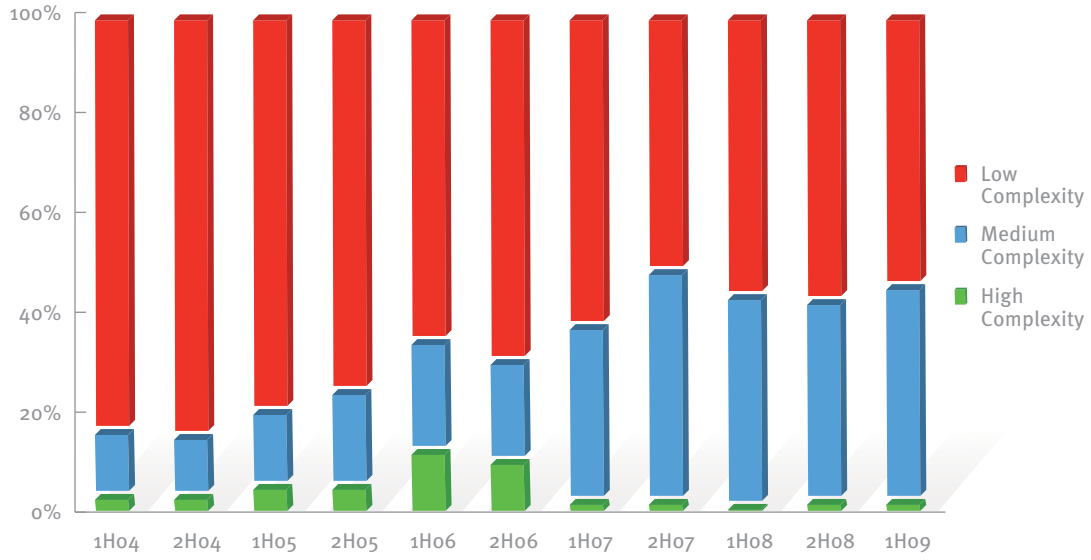
FIGURE 92. NVD complexity rankings and definitions

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).

[37] Definition 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

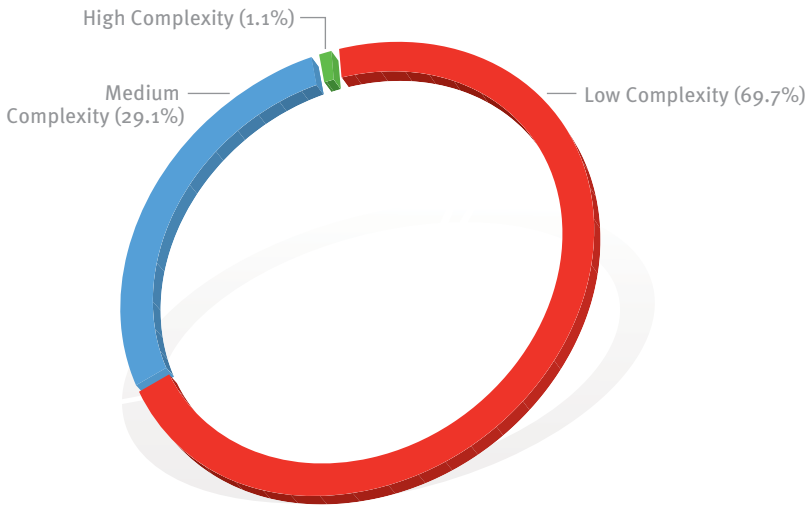
Figure 93 shows the complexity mix for vulnerabilities disclosed in each half-year period since 1H04. Note that Low complexity indicates greater danger, like High severity does in Figure 90.

FIGURE 93. Industry-wide vulnerability disclosures by access complexity, 1H04–1H09



As with severity, the complexity trend in 1H09 is a generally positive one: 54.2 percent of all vulnerabilities were Low complexity in 1H09, down from 57.7 percent in 2H08, and down almost 30 percentage points over the last five years. With more than half of all vulnerabilities designated Low complexity, however, it is clear that vulnerability complexity remains a significant problem. Among High severity vulnerabilities, in fact, 69.7 percent were also designated Low complexity—down from 79.1 percent in 2H08, but still very high. 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.

FIGURE 94. High severity vulnerabilities, by access complexity, in 1H09



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.

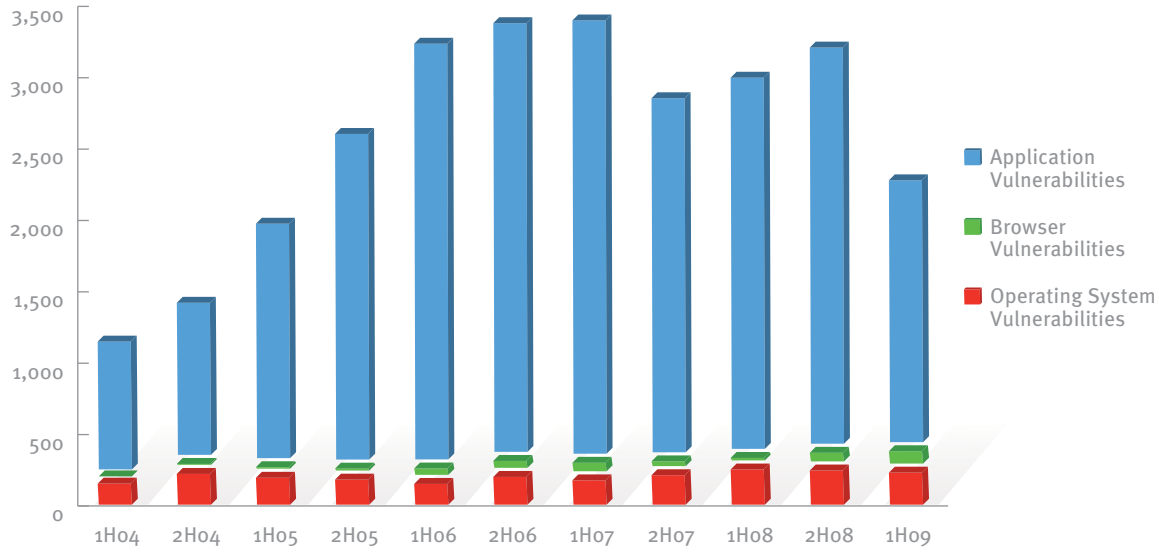
To facilitate analysis of operating system and browser vulnerabilities, this section distinguishes between three different kinds of vulnerabilities:

- *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 Microsoft 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 95 shows vulnerabilities for operating systems, browsers, and other components since 1H04, as determined by this simple model.

FIGURE 95. Industry-wide operating system, browser, and other vulnerabilities, 1H04–1H09

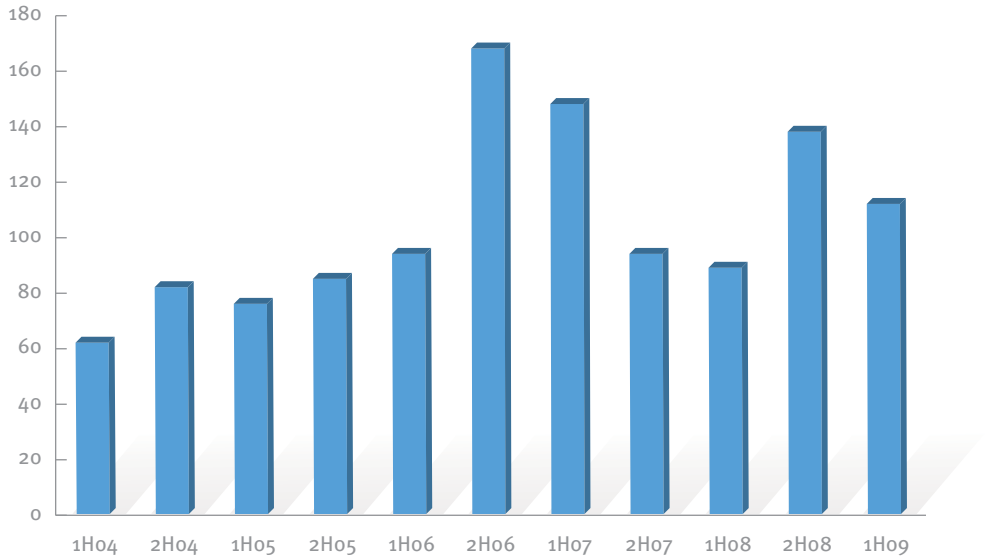


While application vulnerabilities are down sharply from 2H08, operating system vulnerabilities are roughly consistent with the previous period, and browser vulnerabilities actually increased slightly.

Vulnerability Reports for Microsoft Products

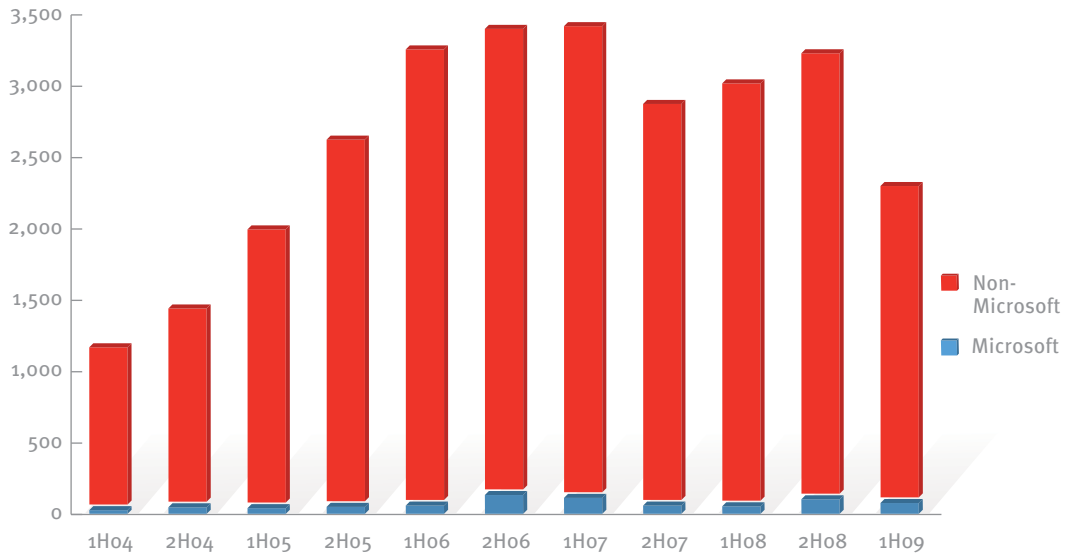
Figure 96 charts vulnerability disclosures for Microsoft products since 1H04. In general, trends for Microsoft vulnerability disclosures have mirrored those for the industry as a whole, though on a much smaller scale.

FIGURE 96. Vulnerability disclosures for Microsoft products, 1H04–1H09



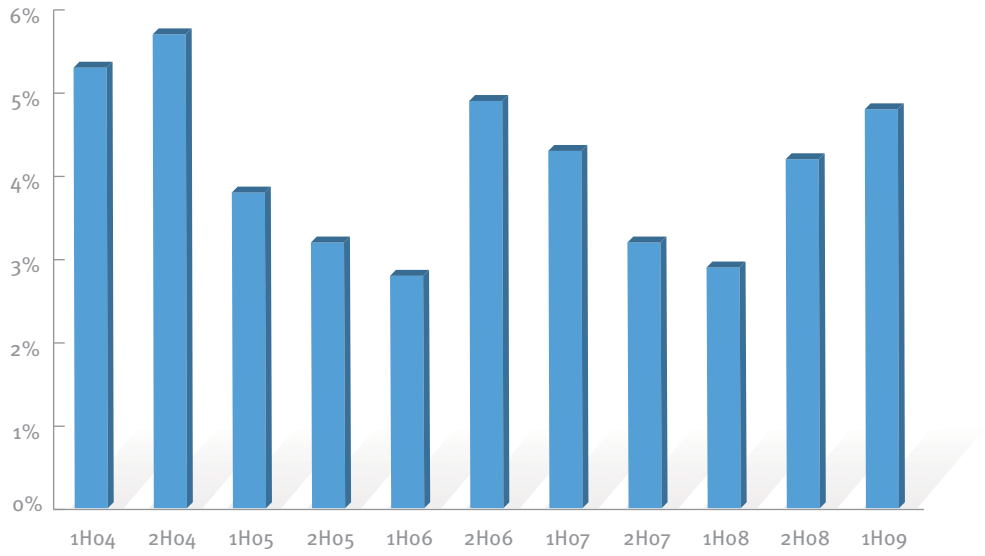
Vulnerability disclosures for Microsoft products decreased from 143 unique vulnerabilities in 2H08 to 115 in 1H09, consistent with the decline in the industry as a whole. Figure 97 provides some perspective for these figures by illustrating the relative share of vulnerability disclosures for Microsoft and non-Microsoft software since 1H04.

FIGURE 97. Vulnerability disclosures for Microsoft and non-Microsoft products, 1H04–1H09



The size and scale of Figure 97 make it difficult to identify trends, so Figure 98 shows Microsoft disclosures as a percentage of total disclosures over the same period. Despite decreasing in absolute terms since 2H08, Microsoft vulnerability disclosures rose slightly as a percentage of all vulnerability disclosures in 1H09 due to the steeper drop in industry-wide disclosures shown in Figure 97. Over the past five years, Microsoft vulnerability disclosures have consistently accounted for about 3 to 6 percent of all disclosures industry wide.

FIGURE 98. Microsoft vulnerability disclosures as a percentage of all industry disclosures, 1H04–1H09

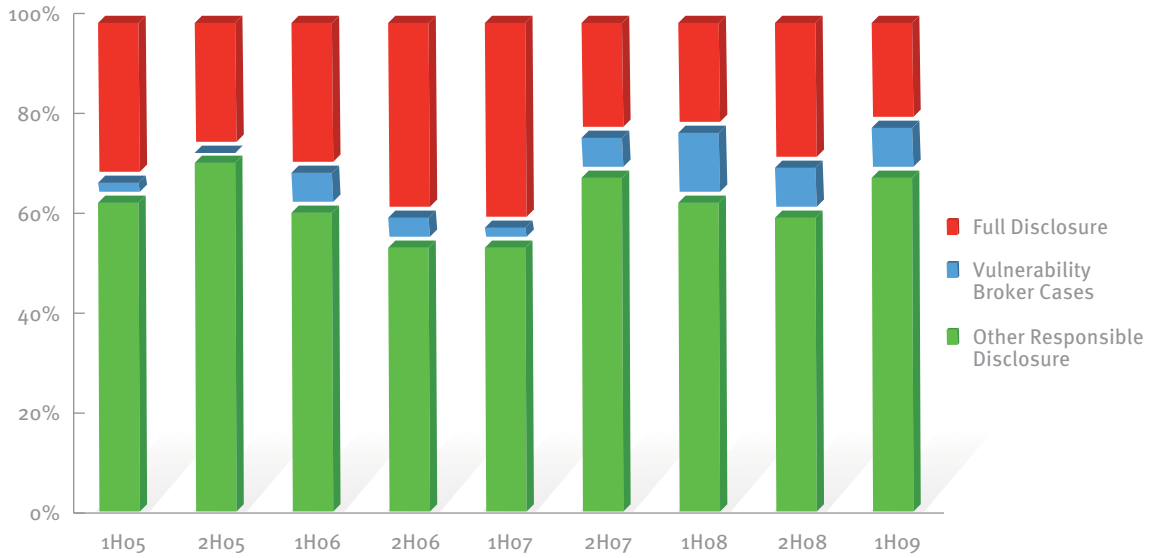


Responsible Disclosures

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



In 1H09, 79.5 percent of Microsoft vulnerability disclosures adhered to responsible disclosure practices, up from 70.6 percent in 2H08 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.

Notably, the percentage of disclosures submitted by vulnerability brokers remained stable in 1H09, at 10.5 percent of all disclosures (up from 9.9 percent in 2H08), while the percentage of responsible disclosures submitted through other means rose significantly, from 60.7 percent in 2H08 to 69.1 percent in 1H09. 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. The historically high responsible disclosure rate seen in 1H09 may be taken as a validation of Microsoft's commitment to address security issues through a variety of approaches.

Microsoft Security Bulletins in 1H09

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 fix 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. Microsoft did not release any out-of-band updates in 1H09.

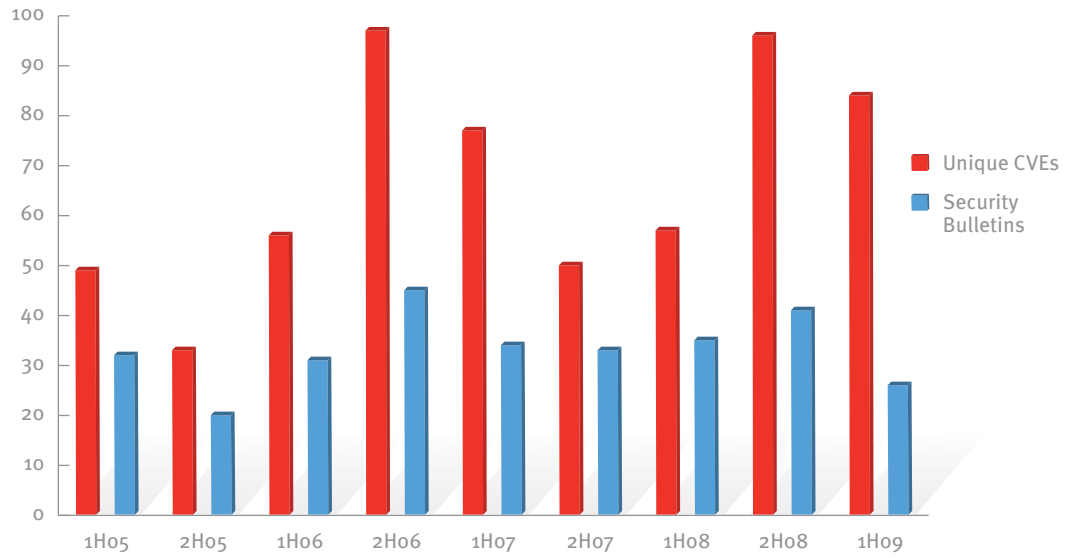
FIGURE 100. Total security bulletins and out-of-band updates released by Microsoft since 1H05

Period	Total Security Bulletins	Out-of-band Security Bulletins
1H05	33	0
2H05	21	0
1H06	32	1
2H06	46	1
1H07	35	1
2H07	34	0
1H08	36	0
2H08	42	2
1H09	27	0

A single security bulletin often addresses multiple vulnerabilities from the CVE database,[38] each of which is listed in the bulletin, along with any other relevant issues. Figure 101 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.)

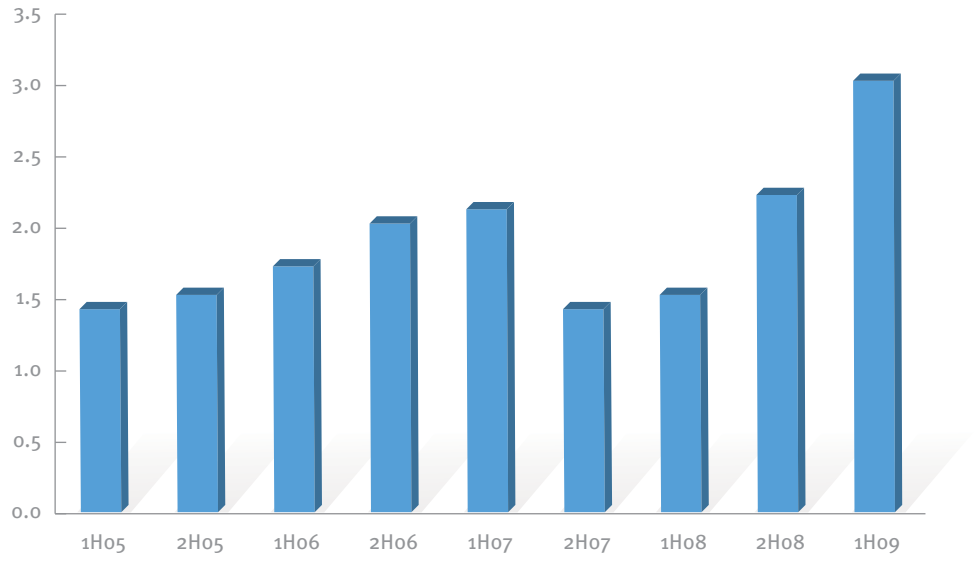
[38] See the National Vulnerability Database (NVD), at http://nvd.nist.gov, to look up vulnerabilities by CVE identifier.

FIGURE 101. Security bulletins released and CVEs addressed by half-year, 1H05–1H09



In 1H09 the MSRC released 27 security bulletins, which addressed 87 individual CVE-identified vulnerabilities, a 12.4-percent decrease over the number of vulnerabilities addressed in 2H08. As Figure 102 shows, the average number of CVEs addressed by each security bulletin has risen over time, from 1.5 in 1H05 to 3.2 in 1H09.

FIGURE 102. Average number of CVEs addressed per security bulletin, 1H05–1H09



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.

More Vendors Adopting Scheduled Release Strategies

Since 2003, Microsoft has released most security updates in groups on the second Tuesday of each month, in order to make it easier for customers to test and deploy new updates and build processes for faster deployment. As attackers increasingly turn to vulnerable browser add-ons as targets for exploitation (as described in "Top Browser-Based Exploits," beginning on page 113), other software vendors have begun to adopt scheduled update release strategies of their own.

On May 20, 2009, Adobe Systems announced that the company was moving to a quarterly cycle for releasing security updates for its popular Adobe Reader and Acrobat programs. In a post on the Adobe Secure Software Engineering Team (ASSET) blog,[39] Brad Arkin, Director of Product Security and Privacy at Adobe, wrote that the company was adopting the scheduled approach as part of a larger initiative aimed at making Adobe Reader and Acrobat more secure and enhancing Adobe's ability to respond to externally discovered vulnerabilities. These quarterly release dates would be scheduled to occur on Tuesdays, to align with Microsoft's own release schedule.

Adobe's quarterly release cycle formally began on June 9, 2009 with the release of security bulletin APSB09-07,[40] which addressed 13 vulnerabilities in Adobe Reader and Acrobat versions for the Windows and Macintosh platforms.

[39] http://blogs.adobe.com/asset/2009/05/adobe_reader_and_acrobat_secur.html
[40] http://www.adobe.com/support/security/bulletins/apsb09-07.html

Exploitability Index

In August 2008, the Microsoft Security Response Center introduced the Exploitability Index as a means to assist customers in evaluating the actual risk and likelihood of exploitation for security issues identified and addressed by Microsoft security updates.[41]

The Exploitability Index assesses the likelihood that code will be released that exploits the vulnerability or vulnerabilities addressed in a security bulletin within the first 30 days after that bulletin's release. The main purpose of the Exploitability Index is to assist customers in prioritizing the deployment of security updates. Exploitability Index ratings enable customers to more effectively evaluate security bulletins with similar Severity ratings but different relative amounts of risk. 1H09 is the first full period that the Exploitability Index has been in operation and available to customers.

[41] For more information about the Microsoft Security Response Center Exploitability Index, visit http://technet.microsoft.com/en-us/library/dd145265.aspx.

Figure 103 explains the ratings assigned for an issue's Exploitability Index and what they mean.

FIGURE 103. Exploitability Index ratings

Exploit Index Rating	Description
1 – Consistent Exploit Code Likely	Exploit code could be created in such a way that an attacker could consistently exploit the vulnerability. For example, an exploit would be able to cause remote code execution of that attacker's code repeatedly and do so in a way that an attacker could consistently expect the same results. This would make it an attractive target for attackers and therefore more likely that exploit code would be created. As such, customers who have reviewed the security bulletin and determined its applicability within their environment could treat this with a higher priority.
2 – Inconsistent Exploit Code Likely	Exploit code could be created, but an attacker would likely experience inconsistent results, even when targeting the affected product. For example, an exploit would be able to cause remote code execution but may only work 1 out of 10 times, or 1 out of 100 times, depending on the state of the system being targeted and the quality of the exploit code. While an attacker may be able to increase the consistency of their results by having better understanding and control of the target environment, the unreliable nature of this attack makes it a less attractive target for attackers. Therefore, it is likely that exploit code will be created, but it is unlikely that attacks will be as effective as other, more consistently exploitable, vulnerabilities. As such, customers who have reviewed the security bulletin and determined its applicability within their environment should treat this as a material update, but if prioritizing against other highly exploitable vulnerabilities, could rank this lower in their deployment priority.
3 – Functioning Exploit Code Unlikely	Exploit code that functions successfully is unlikely to be released. This means that it might be possible for exploit code to be released that could trigger the vulnerability and cause abnormal behavior, but it is unlikely that an attacker would be able to create an exploit that could successfully exercise the full impact of the vulnerability. Given that vulnerabilities of this type would require significant investment by attackers to be useful, the risk of exploit code being created and used is much lower. Therefore, customers who have reviewed the security bulletin to determine its applicability within their environment could prioritize this update below other vulnerabilities within a release.

Figure 104 shows the Exploitability Index rating for vulnerabilities assessed in 1H09.

FIGURE 104. CVEs with exploits discovered within 30 days, by Exploitability Index rating, in 1H09

Forty-one vulnerabilities were assigned an Exploitability Index rating of 1, meaning that they were considered the most likely to be exploited within 30 days of the associated security bulletin's release. Of these, 11 were, in fact, exploited within 30 days. Of the 46 vulnerabilities that received Exploitability Index ratings of 2 or 3, indicating that exploitation would be unreliable or unlikely, none were identified to have been publicly exploited within 30 days.

1H09 Bulletin Severity and Exploitability Index Accuracy

While no system that attempts to predict future vulnerability exploitation is ever likely to be consistently 100 percent accurate, false negatives (vulnerabilities that receive lower Exploitability Index (XI) ratings but which are then exploited within 30 days) are generally much more consequential than false positives (vulnerabilities that receive the highest Exploitability Index rating but are not exploited within 30 days). For system administrators who prioritize security bulletins by Exploitability Index rating, false negatives mean elevated risk from potential exposure to exploitation, whereas false positives do not.

Figure 105 shows how the Exploitability Index ratings for security bulletins released in 1H09 correlated with bulletin severity.[42]

FIGURE 105. Security bulletin severity and exploitability, 1H09

Bulletin Severity	Status	XI Rating 1	XI Rating 2	XI Rating 3
Critical Bulletins	Exploited	5	0	0
	Not Exploited	6	3	2
Important Bulletins	Exploited	3	0	0
	Not Exploited	1	4	1
Moderate Bulletins	Exploited	0	0	0
	Not Exploited	0	1	1

In 1H09, two bulletins received a severity rating of Moderate. Of these, none were assigned an Exploitability Index rating of 1, and none were identified to have been publicly exploited within 30 days.

Nine bulletins received a severity rating of Important. Of these, four were assigned an Exploitability Index rating of 1, indicating that functional reliable exploit code was likely in the first 30 days after the bulletin's release. Three of these four addressed vulnerabilities that were publicly exploited within 30 days, for an aggregate false positive rate of 25 percent.

[42] For more information on the security bulletin severity rating system, visit http://www.microsoft.com/technet/security/bulletin/rating.mspx.

Sixteen bulletins received a severity rating of Critical. Of these, 11 were assigned an Exploitability Index rating of 1. Five of these 11 bulletins addressed vulnerabilities that were publicly exploited within 30 days, for an aggregate false positive rate of 55 percent. The higher false positive rate for Critical security bulletins can be attributed to the conservative approach used during the assessment process to ensure the highest degree of customer protection for the most severe class of issues. This approach is validated somewhat by the fact that none of the vulnerabilities assigned a lower Exploitability Index rating were exploited publicly within 30 days, as noted earlier.

Customers with limited resources and the need to prioritize security bulletin deployments can use Exploitability Index ratings in conjunction with the existing severity rating system to determine the appropriate deployment strategy for their environment. Figure 106, showing severity and Exploitability Index ratings for security bulletins released in June 2009, illustrates how the Exploitability Index can be used to lower risk. A customer that only addresses Critical updates during the first month of release would have remained exposed to exploit code for the vulnerability addressed by security bulletin MS09-020, classified as an Important update. By contrast, a customer that addresses all security bulletins with an Exploitability Index rating of 1 during the first month of release would have been protected from the MS09-020 exploit code.

FIGURE 106. June 2009 security bulletin release severity and Exploitability Index breakdown

Bulletin ID	Bulletin Severity Rating	Exploitability Index Rating	Exploit Code Discovered
MS09-018	Critical	3	
MS09-019	Critical	1	
MS09-020	Important	1	YES
MS09-021	Critical	1	
MS09-022	Critical	1	
MS09-023	Moderate	3	
MS09-024	Critical	1	
MS09-025	Important	1	
MS09-026	Important	2	
MS09-027	Critical	1	

While the MSRC continues to improve its mechanisms for assessing exploitability, and future periods will provide additional information about the accuracy of the Exploitability Index, the data for 1H09 can be taken to support the use of the index as a method for prioritizing security update deployments beyond that which is possible from severity ratings alone, without introducing additional risk.

Mitigations, Workarounds, and Attack Surface Reduction

In addition to creating comprehensive security updates that address vulnerabilities, the MSRC attempts to identify applicable mitigations and workarounds that customers can use to reduce their potential risk from a vulnerability before they are able to deploy the associated security update.

A *mitigation*, or *mitigating factor*, is a default setting, common configuration, or general best practice that could reduce the severity of exploitation of a vulnerability, without typically requiring additional action. For example, for a vulnerability that can only be exploited if an obscure TCP port is open to the Internet, following commonly accepted best practices for enterprise firewalls would be a mitigating factor, because such ports are typically firewalled by default. While a mitigation does not eliminate or address a vulnerability, it does introduce barriers to successful exploitation. The more mitigations a customer is able to take advantage of, the more obstacles an attacker would have to overcome to successfully use the vulnerability in an attack.

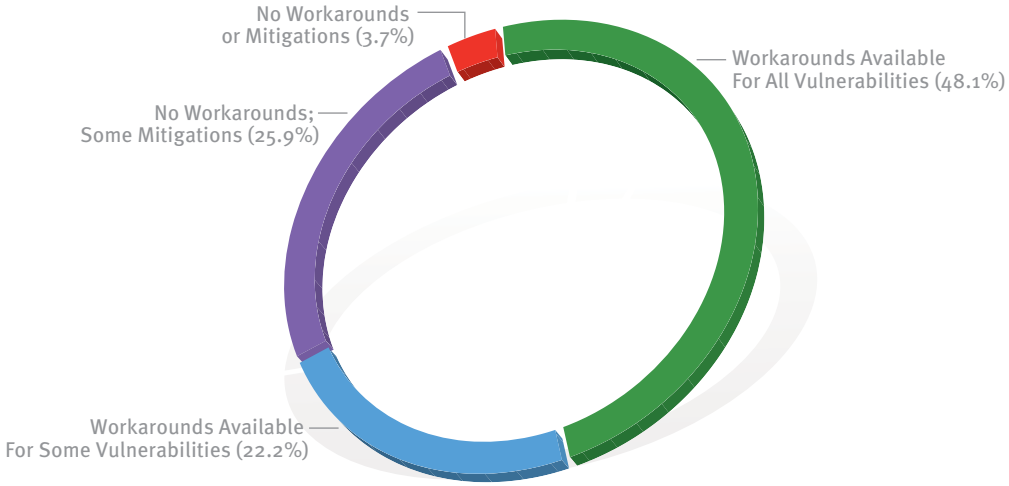
A *workaround* refers to a setting or configuration change that can be implemented to block known attack vectors before the associated security update can be applied. (The same factor or setting can be a mitigating factor for one customer and require a workaround for another. For example, if the TCP port mentioned in the previous paragraph is open, closing it would be a workaround.) Workarounds may not be feasible for everyone. They should be considered and evaluated against functionalities and operational considerations that may be identified as not relevant or needed in a particular computing environment.[43]

In addition to presenting customers with additional information that can be used to assess risk and prioritize update deployment, mitigations and workarounds also allow customers to explore interim alternatives to deploying security updates or to provide additional protection while the update and deployment process is underway. The more mitigations and workarounds customers have at their disposal, the more options and information they can take advantage of to mitigate that overall risk.

[43] For information and best practices regarding Microsoft security updates, see the *Microsoft Security Update Guide*, available from the Microsoft Download Center.

As Figure 107 illustrates, nearly half of the security bulletins released by Microsoft in 1H09 included one or more workarounds for each vulnerability addressed by the bulletin.

FIGURE 107. Workaround and mitigation status for 1H09 security bulletins



"Appendix D: Microsoft Security Bulletins in 1H09," on page 227, includes more information about mitigations and workarounds for each security bulletin released in 1H09.

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 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.

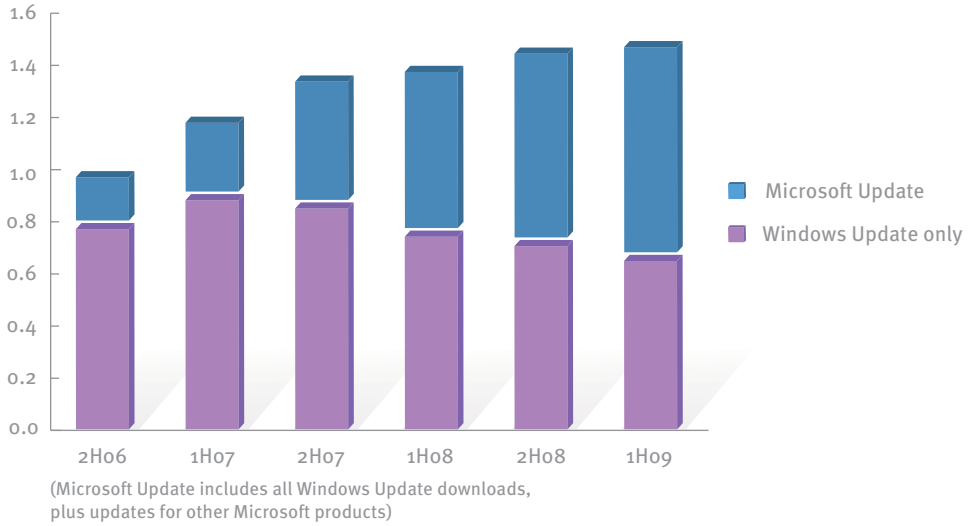
For end users, Microsoft provides two update services that the update clients can use.

- **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.[44] 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.

[44] 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 108 shows, Microsoft Update adoption has risen significantly over the past several years, with increasing numbers of Windows Update users choosing to switch to the more comprehensive service.

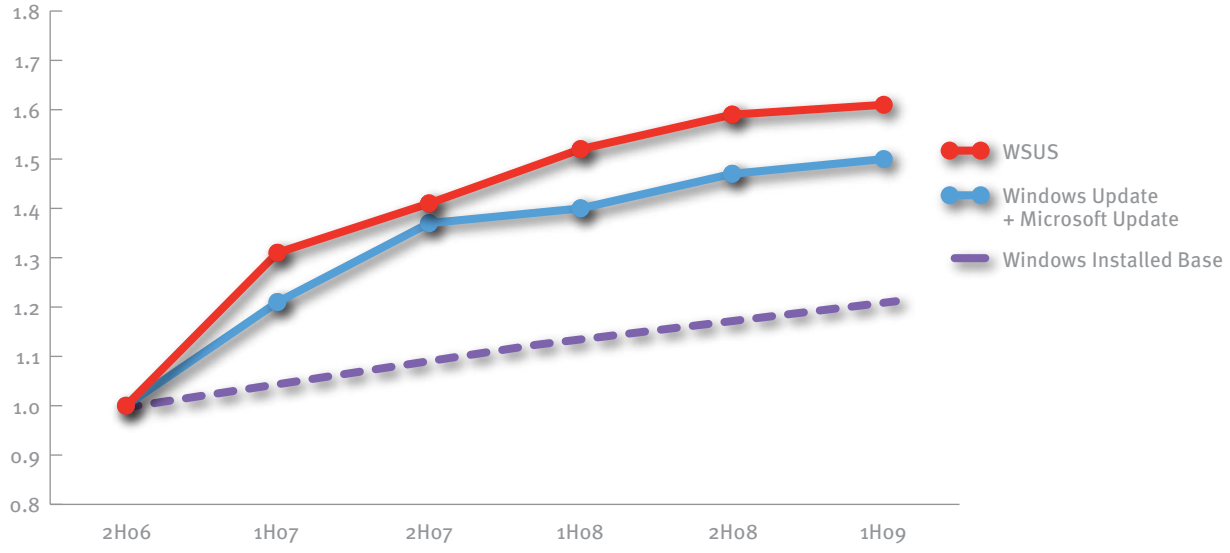
FIGURE 108. Usage of Windows Update and Microsoft Update, 2H06–1H09, indexed to 2H06 total usage



(Microsoft Update includes all Windows Update downloads, plus updates for other Microsoft products)

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 109 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 109. Relative growth in Microsoft WSUS and end-user update services, 2H06–1H09, indexed to 2H06

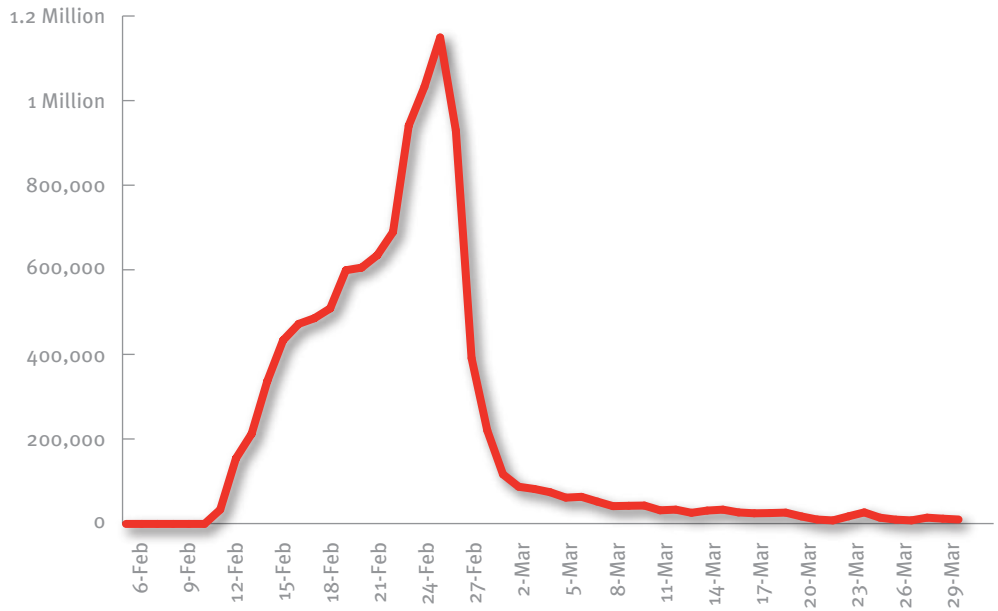


The Role of Automatic Updating

Automatic updating is one of the most effective tools that users and organizations can use to protect themselves. It helps prevent the spread of malware, protects exposed computers, and prevents the spread of new malware designed by reverse engineering the released update. For example, most of the exploits responsible for many of the well-known malware outbreaks discussed throughout this report, such as Win32/Msblast and Win32/Sasser, were discovered after security updates that fixed the associated vulnerability had already been made publicly available. Users and organizations that regularly use automatic updating to apply defensive measures like security updates and antivirus signatures not only reduce their own risk from attack but also help keep infections from spreading further.

The significant and immediate effect that automatic updating can have on stopping the spread of malware is illustrated by an incident from February 2007, when the trojan downloader family Win32/Renos began infecting computers around the world. In some cases, if a computer running Windows Vista is infected with Renos, the malware causes Windows Explorer to crash repeatedly, generating error reports that are sent to Microsoft if Windows Error Reporting is enabled on the computer. Within days, Microsoft was receiving almost 1.2 million error reports a day from computers infected with Renos. On February 27, Microsoft released a signature update for Windows Defender (which is installed by default on Windows Vista) through Windows Update and Microsoft Update that included detections for Renos. Within three days, enough computers had received the new signature update to drop the error reports from 1.2 million per day to less than 100,000 per day worldwide. A few weeks later, the number of error reports caused by Renos had dwindled to insignificant levels.

FIGURE 110. Daily Windows error reports caused by Win32/Renos on Windows Vista in February and March 2007



Encyclopedia

Win32/Msblast: A family of network worms that exploit a vulnerability addressed by security bulletin MS03-039. The worm may attempt DoS attacks on some server sites or create a backdoor on the infected system.

Win32/Sasser: A family of network worms that exploit a vulnerability fixed by security bulletin MS04-011. The worm spreads by randomly scanning IP addresses for vulnerable machines and infecting any that are found.

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

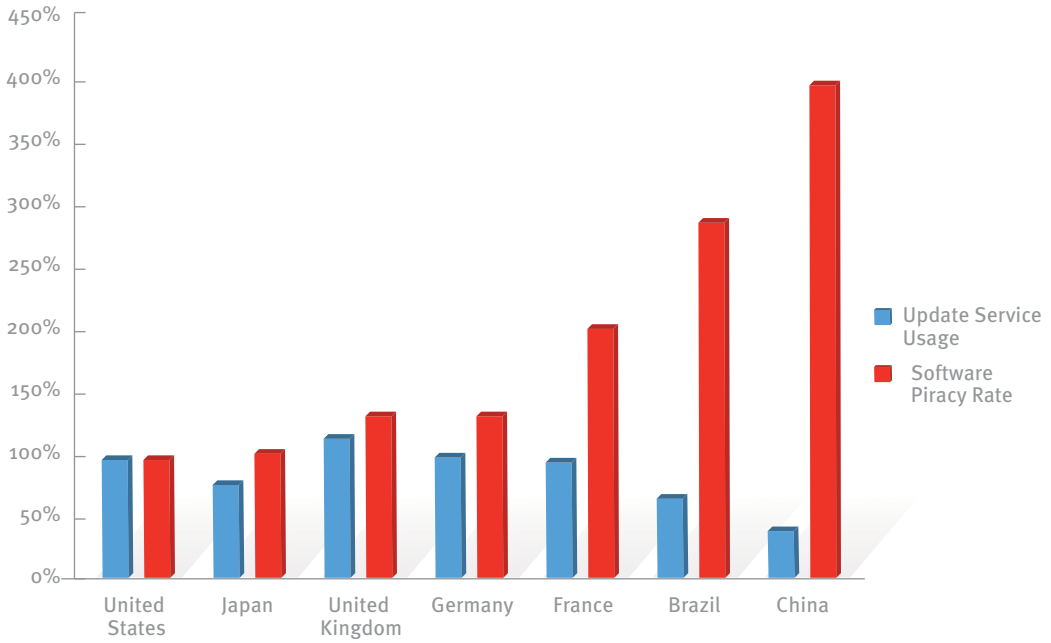
http://www.microsoft.com/av

Regional Variations in Update Service Usage

Use of the Microsoft online update services varies worldwide due to a number of factors, including broadband Internet connectivity, software piracy, and the percentage of computers managed in enterprise environments, which are often updated through mechanisms like WSUS and System Center rather than Windows Update and Microsoft Update.

Figure 111 shows update service usage and software piracy rates for several locations around the world, with the United States as a baseline and the rates for other locations displayed relative to the United States.

FIGURE 111. Update service usage and software piracy rates for seven locations worldwide, relative to the United States



(Software piracy data from the Business Software Alliance, *Global Software Piracy Study*, 2008) http://global.bsa.org/globalpiracy2008/

Myths and Facts About Microsoft Update Services and Software Piracy

Microsoft customer research indicates that there are four primary myths that discourage people from using online update services in regions with high piracy rates, as detailed in Figure 112.

FIGURE 112. Myths about Microsoft update services and software piracy

Myth	Fact
Anti-piracy updates are forcibly installed by Microsoft if users install updates through Windows Update and Automatic Updates.	Users can, through the Windows Update or Automatic Updates control panels, choose how updates are downloaded and installed. Users can choose the updates they want installed. Use of the Windows Update and Microsoft Update Web sites (Windows XP and Windows Server 2003) is gated to require Genuine validation, but there is no restriction on the use of Automatic Updates on the local computer.
Microsoft does not offer security updates to pirated systems.	Microsoft offers all security updates for Windows and all other Microsoft products. They also allow all computers to install the latest service packs, update rollups, critical reliability updates, compatibility updates, and most software upgrades.
Microsoft update services scan computers for pirated software and relay personally identifiable information (PII) back to Microsoft for use in criminal prosecutions.	Microsoft's update services do not collect and forward personally identifiable information back to Microsoft for use in criminal prosecutions. To help mitigate privacy concerns, Microsoft has obtained and continues to renew third-party privacy certification for each version of the Windows update client. For more information about how privacy is protected through Windows Update, refer to the Windows Update privacy statement. For more information on how privacy is protected through genuine software updates, refer to the Microsoft Genuine Advantage Privacy Statement.
Microsoft update services will cause non-genuine computers to crash more often or experience performance problems. Functionality of Windows is reduced on non-genuine computers.	The functionality, reliability, or performance of non-genuine Windows-based computers is not degraded. The following things will occur for a non-genuine computer: • The desktop background will be changed to the color black. • The user will be periodically notified that the computer is non-genuine. • The user may not be offered new software or less-critical (value added) updates that are offered to Genuine Windows-based computers.

Strategies, Mitigations, and Countermeasures

- Configure Windows Update or Microsoft Update on all computers. It is important to check the configured update service 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. A majority of the exploits cited in this report could have been prevented had the updates been installed in a timely manner through Windows Update or Microsoft Update.
- Understand the Microsoft Security Update process and terminology. The newly released Microsoft Security Update Guide, available from the Microsoft Download Center, will help you understand the security update release process and all of Microsoft's supporting resources. It also explains the Microsoft security communication process and provides guidance on how to successfully plan and manage your update management program, including when and how to implement temporary workarounds.
- If you are a security software vendor, 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 Microsoft's monthly security update. When MAPP partners receive vulnerability information early, they can provide updated protections to customers through their security software or devices, such as antivirus, network-based intrusion detection systems, or host-based intrusion prevention systems.
- Subscribe to the Microsoft Security Newsletter. The newsletter offers security tips, information, security bulletins and updates, pertinent articles by Microsoft Security MVPs, and information for improving your role in the IT security industry. You can subscribe at http://www.microsoft.com/technet/security/secnews/default.mspx.
- Obtain security updates and service packs directly from vendors' Web sites and not from P2P sharing, where the update could be modified with malware and redistributed. If this is unavoidable, ensure that the MD5 hash of each file you receive matches that of the original file.
- Ensure that all third-party applications are being updated regularly by the vendor. Check the vendors' Web sites to determine whether any updates have been released and whether you need to apply them to your computers. As Microsoft continues to improve the security of its operating systems and applications, attackers have increasingly redirected their exploitation efforts toward third-party applications and customer-developed internal applications. Ensure that your development team is using the Security Development Lifecycle (SDL; http://www.microsoft.com/sdl) or a similar software security assurance process.
- Uninstall unused software to reduce your attack surface. Malicious code can exploit vulnerabilities in your applications, regardless of how frequently they are used. This includes pre-installed applications on computers purchased from OEMs.
- For downlevel clients, ensure that the Office Document Open Confirmation Tool, available from the Microsoft Download Center, is installed. Installation of this tool would have helped mitigate more than 75 percent of the Office vulnerabilities identified in this report.

Afterword

Call to Action: End to End Trust

End to End Trust is Microsoft's vision for a safer, more trusted Internet, built on security and privacy fundamentals, technology innovations, and the alignment of broad social, economic, political, and IT forces. This vision builds on Microsoft's continued commitment to improving the security and privacy of our products and services. Along with our industry partners, we will continue to build a more secure, private and reliable computing experience. But Microsoft and the technology industry alone cannot create a trusted online experience. For that to happen, industry must not only band together but must work with customers, partners, governments and other important constituencies on a roadmap for taking Trustworthy Computing to the Internet.

An important tool for helping to realize the End to End Trust vision and building a safer Internet is education. Everyone needs to become better educated about online threats and how to defend against them. This includes everyone from people using the Internet at home to IT professionals defending today's networks, to the developers that create the applications that people use. In the cover story of this *Security Intelligence Report* (Melissa Plus 10: Keeping People Safe in the Age of Malware), we describe a number of ways in which Microsoft and other stakeholders in the corporate, government, and academic worlds have collaborated in an ongoing effort to influence these forces and enable real change in today's threat environment. We encourage all readers of the *Security Intelligence Report* to review these practices and find ways to take them forward to help improve the safety, security and privacy of the computing environments they manage or are responsible for.

Additionally software vendors and IT Professionals an can use the resources and information provided at http://www.microsoft.com/endtoendtrust to help take security and privacy fundamentals to the next level by building more secure, privacy-enhanced software and services, cleaning up the ecosystem, and finding ways to work with others in the industry to combat online crime. Developers, network administrators, and others can take advantage of the guidance presented in the "Strategies, Mitigations, and Countermeasures" sections on pages 30, 102, 132, and 158 of this report to protect their networks and systems from current threats, as well as prepare for the future.

The benefits of the Internet clearly outweigh the risks, and we look forward to working with all of you toward a safer, more trusted Internet. For more information on End to End Trust, please visit our website at www.microsoft.com/endtoendtrust.

Microsoft Malware Protection Center Executive Afterword

Thanks for reading volume 7 of the *Microsoft Security Intelligence Report*. I hope that you found it informative and useful, and that the guidance we included in this document helps you better protect your computing environment.

As we discussed in our cover story, the threat landscape has evolved dramatically over the past 10 years. The attack vectors and approaches used to infect computers have changed, as have the motives behind those attacks. In response, software vendors and industry groups have had to adopt and adapt new techniques and programs to combat these threats. I want to share my personal perspective on those changes, reflect on some of the key trends we observed in the previous volume of the *Security Intelligence Report* and highlight some of the important findings in this volume of the report.

It's funny, I recall attending anti-malware industry conferences 10 years ago where one of the topics discussed was the presumed imminent consolidation of the anti-malware vendor industry. Far from shrinking, the sector has continued to expand and evolve, driven by the dramatic rise in the sheer volume of malicious and potentially unwanted software produced by criminals around the world. As this trend developed over the last ten years it has become increasingly important that the major players in the anti-malware space are acting in the best interests of our collective customers.

Microsoft has long been a driver of industry collaboration against IT security threats—see the section "Community-Based Defense" beginning on page 26 of this report—as we believe this is one of the most effective ways to combat these threats. Microsoft has a unique opportunity to engage with a very wide spectrum of software vendors, anti-malware industry organizations, Government bodies and of course customers and partners; engaging and collaborating broadly will continue to be a key strategy for Microsoft as we work together to combat these threats.

In volume 6 of the *Microsoft Security Intelligence Report*, we discussed the "rise of the rogues"—the increase in prevalence of fake anti-malware products that try to convince their victims to give up credit card details and unwittingly install malicious software. The MMPC has added several prevalent rogue security software families to the Malicious Software Removal Tool over the past year and I am pleased to report that we saw a reduction in infections from these threats in the first half of 2009. We will continue to detect and remove these types of threats—any reduction in computer infections is good news but there is always more work to be done.

Also in the first half of 2009, we saw a couple of interesting trends in malware around the world—the return of worms as a significant threat, and a substantial increase in threats targeting players of online games.

One worm threat, Conficker, attracted a lot of media attention late in 2008 and early in 2009. However, the second most prevalent threat worldwide infected almost as many machines. Taterf, a family of worms that spreads via mapped drives and targets online

gamers, was detected and removed from more than twice as many computers worldwide as in the second half of 2008. Taterf was removed from computers more than 4.9 million times in the first half of 2009.

What's *really* interesting is that worms made up four of the top five threats we detected in the enterprise (from our Forefront Client Security product), but only one of the top 10 threats in the home (from Windows Live OneCare). Those four worms in the enterprise all use similar techniques to spread—infected USB and other removable drives, and insecure shared or mapped drives. As you can imagine, once a threat such as this gets inside an enterprise it can be very difficult to remove. It is extremely important, therefore, that system administrators restrict "autoplay" functionality where removable drives are concerned and make sure any shared drives have suitable passwords and access controls. Oh, and maybe consider if all that online gaming on your corporate computers is a risk factor…

We are already hard at work planning future volumes of the *Microsoft Security Intelligence Report*. I am particularly looking forward to our first set of data from the new consumer-focused Microsoft Security Essentials (MSE) offering. MSE uses the same anti-malware technology that Forefront Client Security and Windows Live OneCare use and is available free of charge for genuine Windows users in 19 countries and regions around the world with more to follow in 2010.

In the first week of availability, MSE was installed more than 1.5 million times, and detected almost 4 million threats on just over 500,000 unique computers worldwide—that's a tremendous number of threats neutralized that would otherwise have caused a lot of inconvenience and heartache to many people.

Again, thanks for reading this volume of the *Microsoft Security Intelligence Report*. Please help us to improve future volumes of the report—we always appreciate your feedback and thoughts on how the report can better address your needs. Please send your feedback to the *Microsoft Security Intelligence Report* team at sirfb@microsoft.com.

Vinny Gullotto
General Manager, Microsoft Malware Protection Center
Microsoft Corporation

Appendixes

Appendix A: Full Geographic Data

"Geographic Trends," beginning on page 38, explains how threat patterns differ significantly in different parts of the world. Figure 113 shows the infection rate in 212 different locations around the world, derived from averaging each location's monthly CCM for each of the six months in 1H09. (CCM is the number of computers cleaned for every 1,000 executions of the MSRT. See "Infection Rates and CCM," on page 37, for more information about the CCM metric.)

FIGURE 113. Infection rates for locations around the world, by CCM, in 1H09 and 2H08

Country/Region	CCM (1H09)	CCM (2H08)
Afghanistan	8.1	8.9
Albania	6.3	4.9
Algeria	2.8	2.6
American Samoa	13.8	18
Andorra	2.1	1.9
Angola	3.5	3.9
Anguilla	6.0	9.4
Antigua and Barbuda	0.4	0.7
Argentina	4.5	4.4
Armenia	6.5	6.6
Aruba	2.4	3.4
Australia	3.9	4.7
Austria	2.1	2.3
Azerbaijan	3.8	4.1
Bahamas, The	3.7	2.4
Bahrain	9.3	8.1
Bangladesh	2.4	1.9
Barbados	1.3	1.7
Belarus	2.6	3.6
Belgium	4.9	5.0
Belize	4.7	3.9
Benin	5.3	2.3
Bermuda	1.3	1.5
Bhutan	2.9	4.1
Bolivia	7.6	6.8
Bosnia and Herzegovina	8.2	8.9
Botswana	4.4	7.8
Brazil	25.4	20.9
British Indian Ocean Territory	15.4	19.3
Brunei	4.8	2.9
Bulgaria	5.6	5.6
Burkina Faso	8.0	3.8
Burundi	5.6	5.7
Cambodia	3.5	2.8
Cameroon	5.4	4.9
Canada	3.1	4.0
Cape Verde	10.1	10.5
Cayman Islands	1.1	1.8
Central African Republic	35.1	18.6
Chad	31.4	16.5
Chile	7.6	6.3
China	6.7	11.4
Colombia	12.9	10.0
Comoros	12.7	12.7
Congo, Dem. Rep. of the	8.7	6.6
Congo, Rep. of the	7.0	5.8
Costa Rica	10.0	8.8
Côte d'Ivoire	3.7	2.3
Croatia	11.0	10.8
Cyprus	5.8	4.7
Czech Republic	5.1	5.2
Denmark	3.2	5.9
Djibouti	2.0	1.5
Dominica	5.0	3.3
Dominican Republic	8.5	7.1
Ecuador	13.5	12.6
Egypt	13.7	16.5
El Salvador	11.8	9.6
Equatorial Guinea	2.8	3.8
Eritrea	15.7	17.6
Estonia	4.7	5.3
Ethiopia	1.0	1.4
Falkland Islands (Islas Malvinas)	13.7	18.2
Faroe Islands	3.7	4.4
Fiji Islands	3.8	5.2
Finland	1.9	2.6
France	7.9	7.8
French Guiana	3.2	2.4
French Polynesia	2.9	2.5
Gabon	6.8	12.1
Gambia, The	8.0	9.0
Georgia	11.1	12.2
Germany	3.0	3.6
Ghana	2.4	2.6
Gibraltar	3.3	3.9
Greece	9.8	9.4
Greenland	5.6	5.3
Grenada	2.1	1.6
Guadeloupe	2.9	2.3
Guam	1.1	1.4
Guatemala	17.0	13.9
Guernsey	0.7	0.7
Guinea	6.0	6.6
Guinea-Bissau	24.3	16.7
Guyana	1.9	1.7
Haiti	2.9	3.7
Honduras	13.0	12.9
Hong Kong S.A.R.	7.8	5.8
Hungary	9.3	7.5
Iceland	4.9	6.0
India	3.3	2.8
Indonesia	4.6	3.0
Iraq	12.5	13.9
Ireland	3.6	4.2

Continues on next page

FIGURE 113. Continued

Country/Region	CCM (1H09)	CCM (2H08)
Israel	7.6	7.5
Italy	6.9	5.8
Jamaica	3.0	3.3
Japan	3.0	1.7
Jordan	10.3	9.2
Kazakhstan	2.9	4.2
Kenya	2.9	2.3
Kiribati	11.6	N/A
Korea	21.3	18.3
Kuwait	7.7	9.8
Kyrgyzstan	2.7	2.3
Laos	5.4	4.3
Latvia	6.2	5.8
Lebanon	5.1	5.9
Lesotho	11.2	14.2
Liberia	8.2	10.0
Libya	5.3	6.4
Liechtenstein	1.2	1.8
Lithuania	7.0	7.2
Luxembourg	3.3	2.5
Macao S.A.R.	2.4	1.5
Macedonia, F.Y.R.O.	8.7	8.6
Madagascar	1.3	2.2
Malawi	5.7	5.2
Malaysia	5.1	3.5
Maldives	3.1	3.4
Mali	5.6	3.8
Malta	3.2	3.4
Martinique	3.0	2.2
Mauritania	3.6	2.6
Mauritius	3.5	3.6
Mayotte	10.9	9.8
Mexico	14.5	15.9
Micronesia	20.1	17.4
Moldova	3.9	5.2
Monaco	0.9	1.3
Mongolia	2.2	1.8
Morocco	2.6	2.1
Mozambique	8.7	8.4
Namibia	9.8	14.5
Nauru	145.0	N/A
Nepal	2.2	1.8
Netherlands	4.3	5.9
Netherlands Antilles	1.7	1.8
New Caledonia	2.0	2.4
New Zealand	3.4	4.0
Nicaragua	14.2	11.2
Niger	7.4	4.4
Nigeria	3.6	3.1
Northern Mariana Islands	1.3	1.3
Norway	3.3	6.8
Oman	7.9	7.7
Pakistan	3.0	2.2
Palau	10.4	N/A
Palestinian Authority	6.5	5.5
Panama	7.5	8.9
Papua New Guinea	12.0	8.4
Paraguay	5.6	6.6
Peru	8.5	7.8
Philippines	2.3	1.4
Poland	13.0	8.0
Portugal	13.7	13.4
Puerto Rico	2.1	2.7
Qatar	6.8	6.4
Réunion	1.4	1.6
Romania	4.7	4.3
Russia	15.0	21.1
Rwanda	2.4	1.9
Saint Kitts and Nevis	3.0	11.3
Saint Lucia	3.8	22.3
Saint Vincent and the Grenadines	1.4	18.5
Samoa	8.3	2.4
San Marino	1.4	77.0
São Tomé and Príncipe	13.2	11.1
Saudi Arabia	20.8	10.3
Senegal	12.5	4.5
Serbia and Montenegro	97.2	5.5
Seychelles	10.6	6.6
Sierra Leone	11.6	8.6
Singapore	4.7	13.1
Slovakia	5.6	6.6
Slovenia	6.5	19.2
Solomon Islands	6.6	2.5
Somalia	19.2	2.6
South Africa	5.5	2.5
Spain	21.6	1.4
Sri Lanka	2.9	5.6
Suriname	4.0	14.0
Swaziland	16.2	5.4
Sweden	3.2	4.1
Switzerland	3.0	8.7
Taiwan	20.4	6.4
Tajikistan	3.9	3.6
Tanzania	4.5	8.9
Thailand	14.0	15.8
Togo	4.2	3.8
Tonga	9.1	14.9
Trinidad and Tobago	3.4	4.1
Tunisia	2.5	2.7
Turkey	32.3	20.5
Turkmenistan	10.8	15.1
Turks and Caicos Islands	2.9	2.9
Tuvalu	40.1	N/A
Uganda	3.6	4.0
Ukraine	5.4	7.8
United Arab Emirates	6.2	5.3
United Kingdom	4.9	5.7
United States	8.6	9.1
Uruguay	3.1	2.9
Uzbekistan	4.8	4.9
Vanuatu	24.1	19.1
Venezuela	6.9	5.5
Vietnam	2.4	1.3
Virgin Islands	1.5	1.5
Virgin Islands, British	14.8	12.0
Yemen	6.3	7.9
Zambia	9.9	10.8
Zimbabwe	20.1	20.6

"Malicious Web Sites," beginning on page 82, includes world and U.S. maps showing the geographic distribution of sites hosting malware and phishing pages. Figure 114 through Figure 117 show the data for the individual locations depicted on the maps.

FIGURE 114. Phishing sites per 1,000 Internet hosts for locations around the world in 1H09

Country/Region	Phishing Sites Per 1,000 Internet Hosts
Angola	0.281
Argentina	0.100
Armenia	0.422
Australia	0.049
Austria	0.073
Bangladesh	29.861
Belarus	0.073
Belgium	0.101
Bhutan	0.663
Bosnia and Herzegovina	0.161
Brazil	0.021
Bulgaria	0.452
Canada	1.913
Chile	0.202
China	0.035
Colombia	0.004
Croatia	0.027
Czech Republic	0.424
Denmark	0.161
Egypt	0.034
Estonia	0.034
Finland	0.026
France	0.387
Georgia	1.362
Germany	0.231
Greece	0.022
Guatemala	0.177
Hungary	0.181
Iceland	0.015
India	0.469
Indonesia	0.337
Iran	7.692
Ireland	0.144
Israel	0.123
Italy	0.095
Japan	0.015
Jordan	0.757
Kazakhstan	0.110
Korea	12.219
Kyrgyzstan	0.053
Latvia	0.086
Lebanon	0.027
Lithuania	0.076
Macedonia, F.Y.R.O.	0.054
Malaysia	0.792
Mexico	0.012
Moldova	0.094
Mongolia	2.809
Morocco	0.058
Nepal	0.118
Netherlands	0.234
New Zealand	0.030
Norway	0.064
Pakistan	0.046
Panama	0.891
Paraguay	0.051
Peru	0.206
Philippines	0.078
Poland	0.129
Portugal	0.187
Qatar	1.776
Romania	0.530
Russia	0.934
Saudi Arabia	0.142
Slovakia	0.191
Slovenia	0.908
South Africa	0.070
Spain	0.264
Sri Lanka	2.024
Swaziland	0.387
Sweden	0.071
Switzerland	0.163
Syria	0.891
Taiwan	0.056
Thailand	0.572
Turkey	0.070
Uganda	2.752
Ukraine	0.876
United Arab Emirates	0.013
United Kingdom	0.304
United States	0.200
Uruguay	0.006
Uzbekistan	0.026
Venezuela	0.014
Vietnam	2.234

FIGURE 115. Phishing sites per 1,000 residents by U.S. state in 1H09

State	Phishing Sites Per 1,000 Residents
Alabama	0.004
Alaska	0
Arizona	0.171
Arkansas	0
California	0.147
Colorado	0.050
Connecticut	0.097
Delaware	0.151
Florida	0.157
Georgia	0.821
Hawaii	0.005
Idaho	0.001
Illinois	0.214
Indiana	0.013
Iowa	0.045
Kansas	0.009
Kentucky	0.290
Louisiana	0.003
Maine	0.005
Maryland	0.027
Massachusetts	0.084
Michigan	0.206
Minnesota	0.027
Mississippi	0.008
Missouri	0.028

State	Phishing Sites Per 1,000 Residents
Montana	0.031
Nebraska	0.165
Nevada	0.036
New Hampshire	0.034
New Jersey	0.170
New Mexico	0.008
New York	0.264
North Carolina	0.017
North Dakota	0
Ohio	0.070
Oklahoma	0.010
Oregon	0.240
Pennsylvania	0.028
Rhode Island	0.001
South Carolina	0.005
South Dakota	0.001
Tennessee	0.010
Texas	0.415
Utah	2.968
Vermont	0.003
Virginia	0.107
Washington	1.359
West Virginia	0.004
Wisconsin	0.001
Wyoming	0

FIGURE 116. Malware distribution sites per 1,000 Internet hosts for locations around the world in 1H09

Country/Region	Malware Servers Per 1,000 Internet Hosts
Antigua and Barbuda	0.903
Argentina	0.044
Armenia	0.038
Aruba	0.057
Australia	0.004
Austria	0.011
Bangladesh	1.389
Belarus	0.088
Belgium	0.010
Belize	1.091
Bolivia	0.015
Bosnia and Herzegovina	0.018
Bouvet Island	166.667
Brazil	0.033
Bulgaria	0.158
Canada	0.145
Chile	0.008
China	1.623
Croatia	0.012
Cuba	0.273
Cyprus	3.089
Czech Republic	0.167
Denmark	0.063
Dominican Republic	0.009
Ecuador	0.022
Egypt	0.017
El Salvador	0.087
Estonia	0.034
Finland	0.007
France	0.077
Georgia	0.717
Germany	0.052
Gibraltar	1.050
Greece	0.009
Hong Kong S.A.R.	0.161
Hungary	0.179
Iceland	0.004
India	0.017
Indonesia	0.007
Iran	3.147
Ireland	0.011
Israel	0.218
Italy	0.026
Japan	0.005
Kazakhstan	0.027
Korea	15.065
Laos	0.985
Latvia	0.659
Lebanon	0.027
Lithuania	0.080
Luxembourg	2.556
Macao S.A.R.	7.605
Malaysia	0.061
Malta	0.038
Mexico	0.000
Monaco	0.047
Mongolia	5.618
Netherlands	0.085
New Zealand	0.001
Norway	0.010
Pakistan	0.030
Panama	5.218
Peru	0.007
Philippines	0.011
Poland	0.021
Portugal	0.050
Romania	0.062
Russia	0.290
Saudi Arabia	0.135
Singapore	0.041
Slovakia	0.068
Slovenia	0.197
South Africa	0.003
Spain	0.113
Sweden	0.034
Switzerland	0.011
Taiwan	0.018
Thailand	0.110
Trinidad and Tobago	0.006
Turkey	0.078
Ukraine	0.416
United Arab Emirates	0.003
United Kingdom	0.111
United States	0.165
Vietnam	1.664

FIGURE 117. Malware distribution sites per 1,000 residents by U.S. state in 1H09

State	Malware Servers Per 1,000 Residents
Alabama	0
Alaska	0
Arizona	0.072
Arkansas	< 0.001
California	0.319
Colorado	0.033
Connecticut	0.003
Delaware	0.025
Florida	1.526
Georgia	0.108
Hawaii	0
Idaho	0.004
Illinois	0.100
Indiana	0.009
Iowa	0
Kansas	0.001
Kentucky	0.012
Louisiana	< 0.001
Maine	0
Maryland	0.011
Massachusetts	0.047
Michigan	0.010
Minnesota	0.029
Mississippi	0.004
Missouri	0.002

State	Malware Servers Per 1,000 Residents
Montana	0.002
Nebraska	0.679
Nevada	0.008
New Hampshire	0.003
New Jersey	0.014
New Mexico	0.001
New York	0.024
North Carolina	0.007
North Dakota	0
Ohio	0.010
Oklahoma	0.004
Oregon	0.006
Pennsylvania	0.015
Rhode Island	0
South Carolina	0.001
South Dakota	0
Tennessee	0
Texas	0.173
Utah	0.125
Vermont	0
Virginia	0.038
Washington	0.226
West Virginia	0
Wisconsin	0.001
Wyoming	0

Figure 71, on page 121, illustrates the geographic distribution of drive-by download sites by country-code top-level domain (ccTLD). Figure 118 shows the data for individual ccTLDs.

FIGURE 118. Percentage of Web sites in each ccTLD that hosted drive-by download pages in 1H09

TLD	Associated Country/Region	Percent of Sites
.AC	Ascension Island	0.41%
.AD	Andorra	0
.AE	United Arab Emirates	0.78%
.AF	Afghanistan	0
.AG	Antigua and Barbuda	0.08%
.AI	Anguilla	0
.AL	Albania	0.36%
.AM	Armenia	0.58%
.AN	Netherlands Antilles	0
.AO	Angola	0
.AQ	Antarctica	0
.AR	Argentina	0.48%
.AS	American Samoa	0.12%
.AT	Austria	0.27%
.AU	Australia	0.26%
.AW	Aruba	0
.AX	Åland Islands	0
.AZ	Azerbaijan	1.44%
.BA	Bosnia and Herzegovina	0.59%
.BB	Barbados	0
.BD	Bangladesh	1.56%
.BE	Belgium	0.24%
.BF	Burkina Faso	0
.BG	Bulgaria	0.21%
.BH	Bahrain	0
.BI	Burundi	0
.BJ	Benin	0
.BM	Bermuda	0
.BN	Brunei	0.72%
.BO	Bolivia	0.29%
.BR	Brazil	0.39%
.BS	Bahamas, The	0
.BT	Bhutan	1.40%
.BV	Bouvet Island	0.41%
.BW	Botswana	1.50%
.BY	Belarus	0.21%
.BZ	Belize	0.25%
.CA	Canada	0.13%
.CC	Cocos (Keeling) Islands	0.03%
.CD	Congo, Democratic Republic of the	0.93%
.CF	Central African Republic	0
.CG	Congo, Republic of the	0
.CH	Switzerland	0.17%
.CI	Cote d'Ivoire	0.21%
.CK	Cook Islands	0
.CL	Chile	0.54%
.CM	Cameroon	0
.CN	China	0.79%
.CO	Colombia	0.29%
.CR	Costa Rica	0.28%
.CU	Cuba	0
.CV	Cape Verde	0
.CX	Christmas Island	0.08%
.CY	Cyprus	1.01%
.CZ	Czech Republic	1.75%
.DE	Germany	0.13%
.DJ	Djibouti	0.05%
.DK	Denmark	0.21%
.DM	Dominica	0.89%
.DO	Dominican Republic	0.26%
.DZ	Algeria	0.96%
.EC	Ecuador	0.37%
.EE	Estonia	1.12%
.EG	Egypt	0.74%

Continues on next page

FIGURE 118. Continued

TLD	Associated Country/Region	Percent of Sites
.ER	Eritrea	0
.ES	Spain	0.19%
.ET	Ethiopia	0
.EU	European Union	0.43%
.FI	Finland	0.07%
.FJ	Fiji	0
.FK	Falkland Islands (Islas Malvinas)	0
.FM	Micronesia, Federated States of	0.15%
.FO	Faroe Islands	0.17%
.FR	France	0.07%
.GA	Gabon	0
.GD	Grenada	0.02%
.GE	Georgia	2.20%
.GF	French Guiana	0
.GG	Guernsey	0.65%
.GH	Ghana	0.28%
.GI	Gibraltar	0
.GL	Greenland	0
.GM	Gambia, The	0.63%
.GN	Guinea	0
.GP	Guadeloupe	0
.GQ	Equatorial Guinea	0
.GR	Greece	0.46%
.GS	South Georgia and the South Sandwich Islands	0.13%
.GT	Guatemala	0.08%
.GU	Guam	0
.GW	Guinea-Bissau	0
.GY	Guyana	0.28%
.HK	Hong Kong S.A.R.	0.33%
.HM	Heard Island and McDonald Islands	0
.HN	Honduras	0.56%
.HR	Croatia	0.64%
.HT	Haiti	0
.HU	Hungary	1.62%
.ID	Indonesia	0.31%
.IE	Ireland	0.56%
.IL	Israel	0.27%
.IM	Isle of Man	0.06%
.IN	India	1.05%
.IO	British Indian Ocean Territory	0.06%
.IQ	Iraq	7.89%
.IR	Iran	0.80%
.IS	Iceland	0.23%
.IT	Italy	0.15%
.JE	Jersey	0
.JM	Jamaica	0
.JO	Jordan	0.90%
.JP	Japan	0.10%
.KE	Kenya	0.64%
.KG	Kyrgyzstan	0.59%
.KH	Cambodia	0.56%
.KI	Kiribati	0.04%
.KM	Comoros	7.69%
.KN	Saint Kitts and Nevis	0
.KP	North Korea	0
.KR	Korea (South)	0.37%
.KW	Kuwait	0.74%
.KY	Cayman Islands	0
.KZ	Kazakhstan	1.72%
.LA	Laos	0.32%
.LB	Lebanon	0.54%
.LC	Saint Lucia	0
.LI	Liechtenstein	0.07%
.LK	Sri Lanka	1.13%
.LR	Liberia	0
.LS	Lesotho	0
.LT	Lithuania	0.78%
.LU	Luxembourg	0.15%
.LV	Latvia	0.71%
.LY	Libya	0.12%
.MA	Morocco	0.38%
.MC	Monaco	0.22%
.MD	Moldova	0.79%
.ME	Montenegro	0.05%
.MG	Madagascar	0
.MH	Marshall Islands	0
.MK	Macedonia, F.Y.R.O.	0.23%
.ML	Mali	0
.MM	Myanmar	0
.MN	Mongolia	0.98%
.MO	Macao S.A.R.	0.51%
.MP	Northern Mariana Islands	0
.MQ	Martinique	0
.MR	Mauritania	0
.MS	Montserrat	0.02%
.MT	Malta	0.24%
.MU	Mauritius	0
.MV	Maldives	0.26%
.MW	Malawi	0
.MX	Mexico	0.34%
.MY	Malaysia	0.40%
.MZ	Mozambique	0.14%
.NA	Namibia	0.14%
.NC	New Caledonia	0
.NE	Niger	0
.NF	Norfolk Island	0.06%
.NG	Nigeria	0.82%
.NI	Nicaragua	0.29%
.NL	Netherlands	0.26%
.NO	Norway	0.17%
.NP	Nepal	2.40%
.NR	Nauru	0.16%
.NU	Niue	0.15%

Continues on next page

FIGURE 118. Continued

TLD	Associated Country/Region	Percent of Sites
.NZ	New Zealand	0.36%
.OM	Oman	0
.PA	Panama	0.25%
.PE	Peru	0.72%
.PF	French Polynesia	0.60%
.PG	Papua New Guinea	0
.PH	Philippines	0.25%
.PK	Pakistan	1.20%
.PL	Poland	0.81%
.PN	Pitcairn Islands	0
.PR	Puerto Rico	0.15%
.PS	Palestinian Authority	1.88%
.PT	Portugal	0.18%
.PW	Palau	0
.PY	Paraguay	0.51%
.QA	Qatar	0.55%
.RE	Réunion	0
.RO	Romania	1.37%
.RS	Serbia	0.61%
.RU	Russia	0.85%
.RW	Rwanda	0
.SA	Saudi Arabia	1.10%
.SB	Solomon Islands	0
.SC	Seychelles	0
.SD	Sudan	1.13%
.SE	Sweden	0.14%
.SG	Singapore	0.38%
.SH	Saint Helena	0.18%
.SI	Slovenia	0.90%
.SK	Slovakia	1.66%
.SL	Sierra Leone	0
.SM	San Marino	0
.SN	Senegal	0.27%
.SR	Suriname	0.33%
.ST	São Tomé and Príncipe	0.04%
.SV	El Salvador	0.17%
.SY	Syria	0.99%

TLD	Associated Country/Region	Percent of Sites
.SZ	Swaziland	0.87%
.TC	Turks and Caicos Islands	0.05%
.TF	French Southern and Antarctic Lands	0.03%
.TG	Togo	0
.TH	Thailand	2.45%
.TJ	Tajikistan	5.28%
.TK	Tokelau	0.15%
.TL	Timor-Leste	0.02%
.TM	Turkmenistan	0.10%
.TN	Tunisia	0.28%
.TO	Tonga	0.07%
.TR	Turkey	1.51%
.TT	Trinidad and Tobago	0.10%
.TV	Tuvalu	0.34%
.TW	Taiwan	0.23%
.TZ	Tanzania	0.57%
.UA	Ukraine	0.93%
.UG	Uganda	0.91%
.UK	United Kingdom	0.25%
.US	United States	0.24%
.UY	Uruguay	0.57%
.UZ	Uzbekistan	0.75%
.VA	Vatican City	0
.VC	Saint Vincent and the Grenadines	0.05%
.VE	Venezuela	0.25%
.VG	British Virgin Islands	0.06%
.VI	Virgin Islands	0.88%
.VN	Vietnam	1.07%
.VU	Vanuatu	0.04%
.WF	Wallis and Futuna	0
.WS	Samoa	0.37%
.YE	Yemen	0.76%
.ZA	South Africa	0.22%
.ZM	Zambia	0.46%
.ZW	Zimbabwe	0

Appendix B: 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. "Geographic Trends," beginning on page 38, gives an overview of the way the relative prevalence of different categories of malware varies between different locations.

The next several pages provide infection statistics for 14 locations around the world, encompassing every inhabited continent and multiple languages and computer usage patterns. In addition, see "Best Practices Around the World," beginning on page 44, for guidance from response professionals working in four locations with consistently low infection rates.

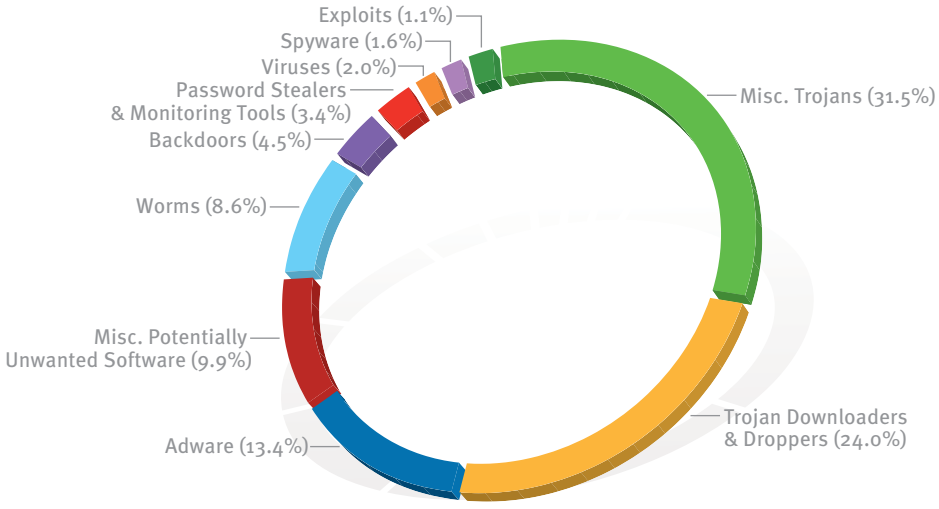
Australia

The infection rate (CCM) in Australia was 3.9 in 1H09, down from 4.7 in 2H08 and significantly lower than the worldwide 1H09 infection rate of 8.7. (*CCM* is the number of computers cleaned for every 1,000 executions of the MSRT. For more information, see page 37.)

Figure 119 and Figure 120 list the most common malware and potentially unwanted software categories and families detected by all Microsoft desktop anti-malware products in Australia in 1H09.

FIGURE 119. Malware and potentially unwanted software in Australia, by category, in 1H09

Category	Infected Computers
Misc. Trojans	168,059
Trojan Downloaders & Droppers	128,185
Adware	71,539
Misc. Potentially Unwanted Software	52,700
Worms	45,789
Backdoors	23,973
Password Stealers & Monitoring Tools	17,968
Viruses	10,428
Spyware	8,721
Exploits	5,935



Notes and observations:

- The threat landscape in Australia was dominated by malware, which accounted for 75.1 percent of all threats detected on infected computers in 1H09, up from 67.3 percent in 2H08.
- The most common category in Australia was Miscellaneous Trojans, which includes all trojan families that are not classified as downloaders/droppers or backdoors. It was detected on 31.5 percent of all infected computers in 1H09, up from 28.3 percent in 2H08, and accounts for 11 of the top 25 families.
- The second-most common category in Australia was Trojan Downloaders & Droppers, which accounted for 24.0 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 1H09.

FIGURE 120. Top 25 families in Australia in 1H09

Rank	Family	Most Significant Category	Infected Computers
1	Win32/Renos	Trojan Downloaders & Droppers	56,732
2	Win32/ZangoSearchAssistant	Adware	46,266
3	Win32/Alureon	Miscellaneous Trojans	43,043
4	ASX/Wimad	Trojan Downloaders & Droppers	27,948
5	Win32/Vundo	Miscellaneous Trojans	23,352
6	Win32/FakeXPA	Miscellaneous Trojans	22,867
7	Win32/Zlob	Trojan Downloaders & Droppers	22,610
8	Win32/ZangoShoppingreports	Adware	21,794
9	Win32/Hotbar	Adware	20,595
10	Win32/Agent	Miscellaneous Trojans	19,990
11	Win32/Taterf	Worms	12,365
12	Win32/Yektel	Trojan Downloaders & Droppers	11,341
13	Win32/Conficker	Worms	10,663
14	Win32/Koobface	Worms	10,625
15	Win32/FakeRean	Miscellaneous Trojans	10,618
16	Win32/Winwebsec	Miscellaneous Trojans	10,413
17	Win32/Tibs	Miscellaneous Trojans	10,373
18	Win32/SeekmoSearchAssistant	Adware	9,555
19	Win32/InternetAntivirus	Miscellaneous Trojans	9,090
20	Win32/C2Lop	Miscellaneous Trojans	7,801
21	Win32/Obfuscator	Miscellaneous Trojans	5,733
22	Win32/Frethog	Password Stealers & Monitoring Tools	5,575
23	Win32/PowerRegScheduler	Miscellaneous Potentially Unwanted Software	5,522
24	Win32/RealVNC	Adware	5,374
25	Win32/Small	Miscellaneous Trojans	5,108

(Conficker data provided by the Shadowserver Foundation)

Notes and observations:

- For the most accurate possible estimate of Win32/Conficker's impact, the figure given reflects the number of IP addresses infected by the A, B, C, and D variants that were detected on June 30, 2009, by sinkhole installations operated by the Shadowserver Foundation and the CWG. For more information about Conficker and the worldwide response to the threat, see "Win32/Conficker Update," beginning on page 95, and "Case Study: The Conficker Working Group," beginning on page 29.
- Five of the top 25 families (Win32/FakeXPA, Win32/Yektel, Win32/FakeRean, Win32/Winwebsec, and Win32/InternetAntivirus) are rogue security software programs. Of these, only Win32/FakeXPA was in the top 25 in 2H08.
- Six of the top 25 families are potentially unwanted software families, compared to 11 in 2H08.
- ASX/Wimad, the sixteenth-most prevalent family worldwide, ranks fourth in Australia. ASX/Wimad is a detection for malicious Windows media files that encourage users to download and execute arbitrary files on an affected computer. When opened with Windows Media Player, these malicious files open a particular URL in a Web browser.
- Win32/Obfuscator, which is not among the top 25 families detected worldwide, ranks twenty-first in Australia. Win32/Obfuscator is a generic detection for programs that have had their purpose obfuscated to hinder analysis or detection by antivirus scanners. They commonly employ a combination of methods, including encryption, compression, anti-debugging, and anti-emulation techniques.
- Win32/PowerRegScheduler, which is not among the top 25 families detected worldwide, ranks twenty-third in Australia. PowerRegScheduler is a product registration system used by some legitimate software programs as a product registration reminder. It is considered potentially unwanted software because it collects personally identifiable information (PII), such as the user's name, address, e-mail, place of purchase, and product serial number. This data is transmitted to PowerRegScheduler's servers and then made available to the publisher of the purchased product.

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.

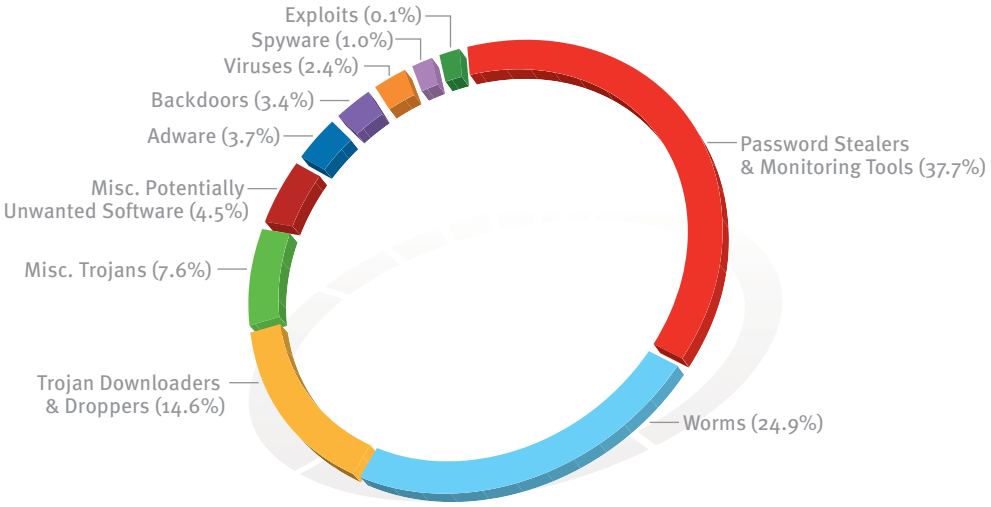
http://www.microsoft.com/av

Brazil

The infection rate (CCM) in Brazil was 25.4 in 1H09, up from 20.9 in 2H08 and significantly higher than the worldwide 1H09 infection rate of 8.7. (*CCM* is the number of computers cleaned for every 1,000 executions of the MSRT. For more information, see page 37.)

Figure 121 and Figure 122 list the most common malware and potentially unwanted software categories and families detected by all Microsoft desktop anti-malware products in Brazil in 1H09.

FIGURE 121. Malware and potentially unwanted software in Brazil, by category, in 1H09



Category	Infected Computers
Password Stealers & Monitoring Tools	1,057,923
Worms	698,056
Trojan Downloaders & Droppers	410,795
Misc. Trojans	214,241
Misc. Potentially Unwanted Software	126,513
Adware	105,141
Backdoors	95,715
Viruses	66,925
Spyware	29,479
Exploits	3,663

Notes and observations:

- The threat landscape in Brazil is clearly dominated by malware, which accounted for 90.8 percent of all families detected on infected computers, up from 83.8 percent in 2H08.
- The most common category in Brazil is Password Stealers & Monitoring Tools, which accounted for 37.7 percent of all families detected on infected computers, down from 43.7 percent in 2H08.
- The second-most common category in Brazil is Worms, which accounted for 24.9 percent of all families detected on infected computers, up from 13.9 percent in 2H08.

FIGURE 122. Top 25 families in Brazil in 1H09

Rank	Family	Most Significant Category	Infected Computers
1	Win32/Conficker	Worms	608,940
2	Win32/Bancos	Password Stealers & Monitoring Tools	599,829
3	Win32/Taterf	Worms	415,744
4	Win32/Banker	Password Stealers & Monitoring Tools	302,824
5	Win32/Frethog	Password Stealers & Monitoring Tools	263,610
6	Win32/Banload	Trojan Downloaders & Droppers	193,840
7	Win32/Small	Trojan Downloaders & Droppers	92,481
8	Win32/C2Lop	Miscellaneous Trojans	72,526
9	Win32/RJump	Worms	62,031
10	Win32/Renos	Trojan Downloaders & Droppers	47,623
11	Win32/Cutwail	Trojan Downloaders & Droppers	43,598
12	Win32/SeekmoSearchAssistant	Adware	42,563
13	Win32/Rustock	Backdoors	42,370
14	Win32/Vundo	Miscellaneous Trojans	36,405
15	Win32/Zlob	Trojan Downloaders & Droppers	32,756
16	Win32/Slenfbot	Worms	31,133
17	Win32/Alureon	Miscellaneous Trojans	31,088
18	Win32/Agent	Miscellaneous Trojans	26,836
19	Win32/ZangoSearchAssistant	Adware	24,878
20	Win32/RealVNC	Password Stealers & Monitoring Tools	24,178
21	Win32/Ldpinch	Password Stealers & Monitoring Tools	21,799
22	Win32/Rbot	Backdoors	19,950
23	Win32/ZangoShoppingreports	Adware	19,191
24	Win32/Ardamax	Password Stealers & Monitoring Tools	17,270
25	Win32/Parite	Viruses	16,768

(Conficker data provided by the Shadowserver Foundation)

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/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.

http://www.microsoft.com/av

Notes and observations:

- Win32/Conficker, the most prevalent family in 1H09, both in Brazil and worldwide, is largely responsible for the rise in the relative prevalence of worms and the corresponding relative drop of password stealers since 2H08.
- For the most accurate possible estimate of Win32/Conficker's impact, the figure given reflects the number of IP addresses infected by the A, B, C, and D variants that were detected on June 30, 2009, by sinkhole installations operated by the Shadowserver Foundation and the CWG. For more information about Conficker and the worldwide response to the threat, see "Win32/Conficker Update," beginning on page 95, and "Case Study: The Conficker Working Group," beginning on page 29.
- Win32/Bancos and Win32/Banker, the second- and fourth-most commonly detected families in Brazil in 1H09, are Portuguese-language password stealers that primarily target customers of Brazilian banks.Win32/Banker is often downloaded by Win32/Banload, the sixth-most commonly detected family in Brazil in 1H09.

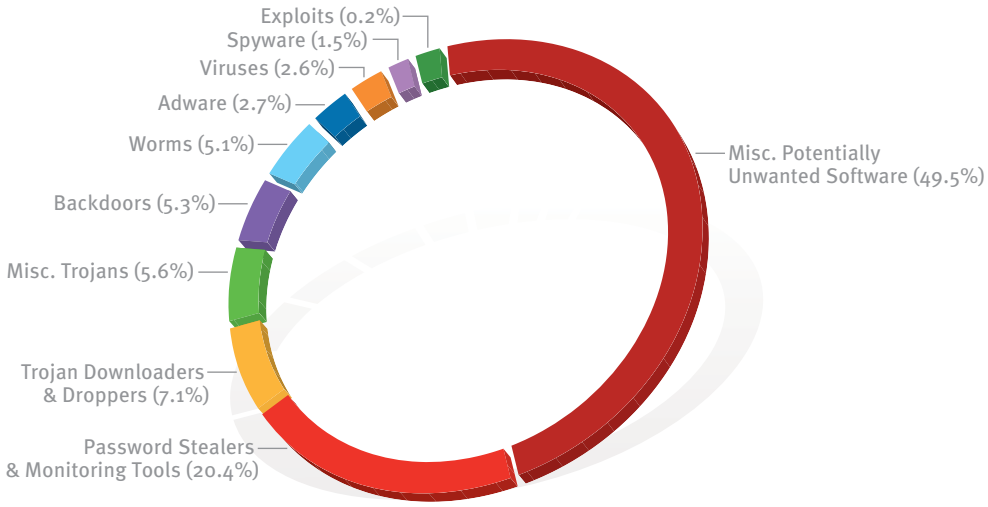
China

The infection rate (CCM) in China was 6.7 in 1H09, down significantly from 11.4 in 2H08 and slightly lower than the worldwide 1H09 infection rate of 8.7. (*CCM* is the number of computers cleaned for every 1,000 executions of the MSRT. For more information, see page 37.)

Figure 123 and Figure 124 list the most common malware and potentially unwanted software categories and families detected by all Microsoft desktop anti-malware products in China in 1H09.

FIGURE 123. Malware and potentially unwanted software in China, by category, in 1H09

Category	Infected Computers
Misc. Potentially Unwanted Software	1,546,579
Password Stealers & Monitoring Tools	637,126
Trojan Downloaders & Droppers	221,084
Misc. Trojans	176,590
Backdoors	166,245
Worms	158,628
Adware	85,617
Viruses	81,858
Spyware	48,259
Exploits	4,804



Notes and observations:

- Potentially unwanted software, including adware and spyware, accounted for 53.7 percent of all families detected on infected computers in China in 1H09.
- The second-most common category in China is Password Stealers & Monitoring Tools, which accounted for 20.4 percent of all families detected on infected computers.

FIGURE 124. Top 25 families in China in 1H09

Rank	Family	Most Significant Category	Infected Computers
1	Win32/Conficker	Worms	1,326,909
2	Win32/BaiduSobar	Miscellaneous Potentially Unwanted Software	1,180,894
3	Win32/Lolyda	Password Stealers & Monitoring Tools	470,723
4	Win32/PossibleHostsFileHijack	Miscellaneous Potentially Unwanted Software	221,181
5	Win32/Frethog	Password Stealers & Monitoring Tools	159,760
6	Win32/Hupigon	Backdoor	154,679
7	Win32/CNNIC	Miscellaneous Potentially Unwanted Software	142,531
8	Win32/Small	Trojan Downloaders & Droppers	104,026
9	Win32/Agent	Miscellaneous Trojans	90,784
10	Win32/Parite	Viruses	60,425
11	Win32/Ceekat	Password Stealers & Monitoring Tools	58,026
12	Win32/Microjoin	Trojan Downloaders & Droppers	57,193
13	Win32/Sogou	Miscellaneous Potentially Unwanted Software	53,895
14	Win32/RJump	Worms	49,162
15	Win32/BaiduSP	Miscellaneous Potentially Unwanted Software	43,049
16	Win32/CnsMin	Spyware	41,119
17	Win32/Baiduiebar	Miscellaneous Potentially Unwanted Software	34,869
18	Win32/Killav	Miscellaneous Trojans	32,857
19	Win32/Cinmus	Miscellaneous Trojans	27,903
20	Win32/Brontok	Worms	22,559
21	Win32/WhenU	Adware	15,309
22	Win32/ConHook	Trojan Downloaders & Droppers	15,307
23	Win32/Rugo	Adware	15,225
24	Win32/Corripio	Password Stealers & Monitoring Tools	15,064
25	Win32/BDPlugin	Miscellaneous Potentially Unwanted Software	13,847

(Conficker data provided by the Shadowserver Foundation)

Notes and observations:

- For the most accurate possible estimate of Win32/Conficker's impact, the figure given reflects the number of IP addresses infected by the A, B, C, and D variants that were detected on June 30, 2009, by sinkhole installations operated by the Shadowserver Foundation and the CWG. For more information about Conficker and the worldwide response to the threat, see "Win32/Conficker Update," beginning on page 95, and "Case Study: The Conficker Working Group," beginning on page 29.
- Many of the most prevalent families are Chinese-language threats that don't appear in the list of top threats for any other location. The Chinese-language browser toolbar, Win32/BaiduSobar, was the second-most prevalent family in China in 1H09,[45] behind Win32/Conficker.
- Much of the decline in the CCM for China from 2H08 to 1H09 can be attributed to a drop in the prevalence of Win32/Lolyda, a password stealer that targets players of online games. Despite this drop, Lolyda was still the third-most prevalent family in China in 1H09.
- Win32/Microjoin, which is not among the top 25 families detected worldwide, ranks twelfth in China. Microjoin is a tool that is used to deploy malware without being detected. It is used to bundle multiple files, consisting of a clean file and malware files, into a single executable.
- Win32/Killav, which is not among the top 25 families detected worldwide, ranks eighteenth in China. Killav is a trojan that terminates a large number of security-related processes, including those for antivirus, monitoring, or debugging tools, and may install certain exploits for the vulnerability addressed by Microsoft Security Bulletin MS08-067.

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/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.

http://www.microsoft.com/av

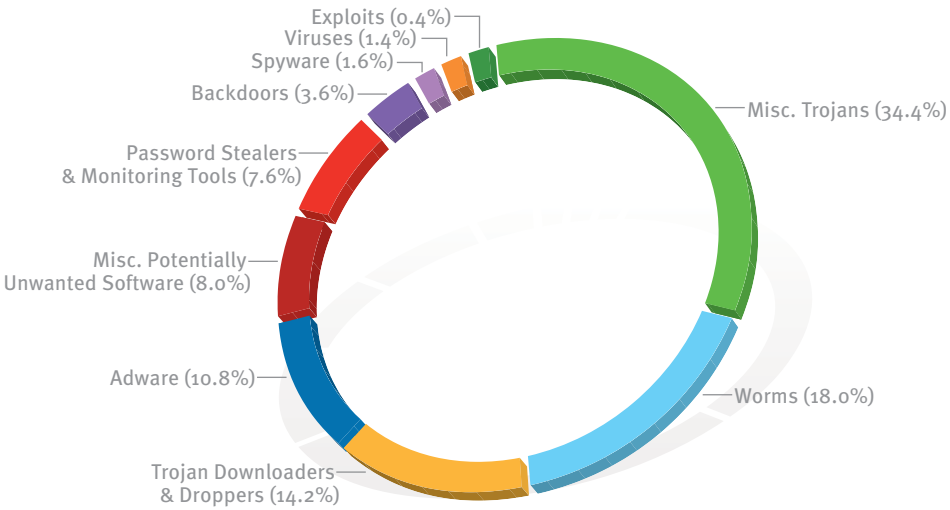
[45] Figures do not include newer versions of the Baidu Sobar software, which no longer exhibits the behaviors Microsoft uses to classify software as potentially unwanted.

France

The infection rate (CCM) for France was 7.9 in 1H09, up from 7.8 in 2H08 and comparable to the worldwide 1H09 infection rate of 8.7. (*CCM* is the number of computers cleaned for every 1,000 executions of the MSRT. For more information, see page 37.)

Figure 125 and Figure 126 list the most common malware and potentially unwanted software categories and families detected by Microsoft security products in France in 1H09.

FIGURE 125. Malware and potentially unwanted software in France, by category, in 1H09



Category	Infected Computers
Misc. Trojans	738,913
Worms	386,517
Trojan Downloaders & Droppers	304,347
Adware	231,460
Misc. Potentially Unwanted Software	171,373
Password Stealers & Monitoring Tools	163,945
Backdoors	77,635
Spyware	33,566
Viruses	30,846
Exploits	7,849

Encyclopedia

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

http://www.microsoft.com/av

Notes and observations:

- The threat landscape in France in 1H09 consisted mostly of malware, which accounted for 79.6 percent of all families removed from infected computers, up from 61.2 percent in 2H08.
- The most common category in France was Miscellaneous Trojans, which includes all trojan families that are not classified as downloaders/droppers or backdoors. It was detected on 34.4 percent of all infected computers, up from 24.7 percent in 2H08, and accounts for 8 of the top 25 families.
- The second-most common category in France was Worms, which accounted for 18.0 percent of all infected computers. Detection of worms in 1H09 was up from 9.6 percent in 2H08, due in large part to increased detections of Win32/Taterf.

FIGURE 126. Top 25 families in France in 1H09

Rank	Family	Most Significant Category	Infected Computers
1	Win32/Wintrim	Miscellaneous Trojans	316,234
2	Win32/Taterf	Worms	222,741
3	Win32/Vundo	Miscellaneous Trojans	127,498
4	Win32/Frethog	Password Stealers & Monitoring Tools	125,491
5	Win32/Renos	Trojan Downloaders & Droppers	104,016
6	Win32/ZangoSearchAssistant	Adware	103,152
7	Win32/Zlob	Trojan Downloaders & Droppers	85,826
8	Win32/Alureon	Miscellaneous Trojans	84,453
9	Win32/C2Lop	Miscellaneous Trojans	73,172
10	Win32/RJump	Worms	61,857
11	Win32/Hotbar	Adware	52,947
12	Win32/ZangoShoppingreports	Adware	52,724
13	Win32/Playmp3z	Adware	38,598
14	Win32/FakeXPA	Miscellaneous Trojans	37,363
15	ASX/Wimad	Trojan Downloaders & Droppers	32,052
16	Win32/Conficker	Worms	31,314
17	Win32/Agent	Miscellaneous Trojans	29,924
18	Win32/Brontok	Worms	29,624
19	Win32/Skintrim	Miscellaneous Trojans	28,905
20	Win32/SpywareSecure	Miscellaneous Potentially Unwanted Software	27,291
21	Win32/Tibs	Miscellaneous Trojans	26,871
22	Win32/SeekmoSearchAssistant	Adware	25,193
23	Win32/Yektel	Trojan Downloaders & Droppers	22,455
24	Win32/Cutwail	Trojan Downloaders & Droppers	21,403
25	Win32/Koobface	Worms	18,538

(Conficker data provided by the Shadowserver Foundation)

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.

http://www.microsoft.com/av

Notes and observations:

- For the most accurate possible estimate of Win32/Conficker's impact, the figure given reflects the number of IP addresses infected by the A, B, C, and D variants that were detected on June 30, 2009, by sinkhole installations operated by the Shadowserver Foundation and the CWG. For more information about Conficker and the worldwide response to the threat, see "Win32/Conficker Update," beginning on page 95, and "Case Study: The Conficker Working Group," beginning on page 29.
- Three of the top 25 families (Win32/FakeXPA,Win32/SpywareSecure, and Win32/Yektel) are rogue security software programs. Of these, only Win32/FakeXPA was in the top 25 in 2H08. FakeXPA and SpywareSecure were both in the top 25 for France in 2H08, while Yektel is new to the list. Detections of SpywareSecure, in particular, have dropped significantly, from first place in 2H08 to twentieth in 1H09.
- Six of the top 25 families are potentially unwanted software families, compared to nine in 2H08.
- Win32/Wintrim, which ranks fifteenth worldwide, was the family most commonly detected on infected computers in France in 1H09. Wintrim is a family of trojans that display pop-up advertisements depending on the user's keywords and browsing history. Its variants can also monitor the user's activities, download applications, and send system information back to a remote server.
- Win32/PlayMP3z and ASX/Wimad, which rank thirteenth and fifteenth in France, respectively, target users who are interested in playing media files. Wimad is a detection for a category of malicious Windows Media files, and Win32/PlayMP3z is an adware program that displays advertisements in connection with a music player. Worldwide, Wimad ranks sixteenth, and PlayMP3z is not among the top 25 families detected on infected computers.

Germany

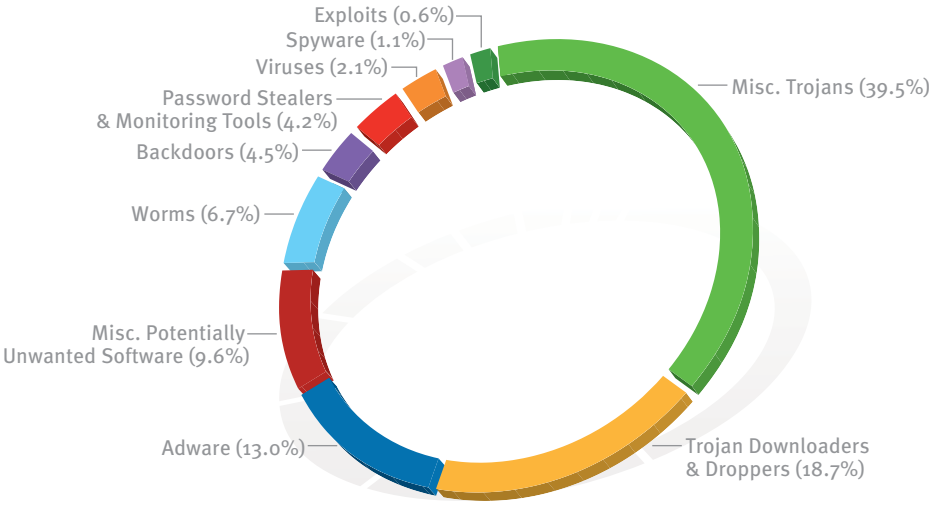
The infection rate (CCM) in Germany was 3.0 in 1H09, down from 3.6 in 2H08 and significantly lower than the worldwide 1H09 infection rate of 8.7. (*CCM* is the number of computers cleaned for every 1,000 executions of the MSRT. For more information, see page 37.)

The infection rate in Germany is consistently among the lowest in the world. See "Best Practices Around the World," beginning on page 44, for information and guidance from security response professionals in four of the world's least infected countries, including Germany.

Figure 127 and Figure 128 list the most common malware and potentially unwanted software categories and families detected by all Microsoft desktop anti-malware products in Germany in 1H09.

FIGURE 127. Malware and potentially unwanted software in Germany, by category, in 1H09

Category	Infected Computers
Misc. Trojans	504,922
Trojan Downloaders & Droppers	239,478
Adware	165,543
Misc. Potentially Unwanted Software	122,731
Worms	86,148
Backdoors	57,462
Password Stealers & Monitoring Tools	54,120
Viruses	26,549
Spyware	13,669
Exploits	7,582



Notes and observations:

- The threat landscape in Germany was dominated by malware, which accounted for 76.4 percent of all threats detected on infected computers in 1H09, up from 62.2 percent in 2H08.
- The most common category in Germany was Miscellaneous Trojans, which includes all trojan families that are not classified as downloaders/droppers or backdoors. It was detected on 39.5 percent of all infected computers in 1H09, up from 28.5 percent in 2H08, and accounts for 8 of the top 25 families.

- The second-most common category in Germany was Trojan Downloaders & Droppers, which accounted for 18.7 percent of all infected computers. Miscellaneous Trojans and Trojan Downloaders & Droppers made up almost half of all families detected on infected computers in Germany in 1H09.

FIGURE 128. Top 25 families in Germany in 1H09

Rank	Family	Most Significant Category	Infected Computers
1	Win32/Wintrim	Miscellaneous Trojans	153,518
2	Win32/Alureon	Miscellaneous Trojans	124,102
3	Win32/Renos	Trojan Downloaders & Droppers	122,589
4	Win32/ZangoSearchAssistant	Adware	79,877
5	Win32/Vundo	Miscellaneous Trojans	75,485
6	Win32/Conficker	Worms	66,659
7	Win32/Zlob	Trojan Downloaders & Droppers	58,090
8	Win32/Agent	Miscellaneous Trojans	44,346
9	Win32/Hotbar	Adware	38,105
10	Win32/ZangoShoppingreports	Adware	34,800
11	Win32/SeekmoSearchAssistant	Adware	33,361
12	Win32/FakeXPA	Miscellaneous Trojans	28,683
13	Win32/Tibs	Miscellaneous Trojans	18,184
14	Win32/FakeRean	Miscellaneous Trojans	17,658
15	Win32/Taterf	Worms	16,506
16	Win32/C2Lop	Miscellaneous Trojans	16,333
17	Win32/Yektel	Trojan Downloaders & Droppers	16,218
18	Win32/Cutwail	Trojan Downloaders & Droppers	15,758
19	Win32/Playmp3z	Adware	15,512
20	Win32/WhenU	Adware	14,174
21	Win32/RealVNC	Adware	13,557
22	Win32/FakeAdpro	Miscellaneous Potentially Unwanted Software	13,481
23	Win32/Rustock	Backdoor	13,059
24	Win32/Rbot	Backdoor	12,807
25	Win32/Frethog	Password Stealers & Monitoring Tools	11,804

(Conficker data provided by the Shadowserver Foundation)

Notes and observations:

- For the most accurate possible estimate of Win32/Conficker's impact, the figure given reflects the number of IP addresses infected by the A, B, C, and D variants that were detected on June 30, 2009, by sinkhole installations operated by the Shadowserver Foundation and the CWG. For more information about Conficker and the worldwide response to the threat, see "Win32/Conficker Update," beginning on page 95, and "Case Study: The Conficker Working Group," beginning on page 29.
- Win32/Wintrim, the most prevalent family in Germany in 1H09, is a family of trojans that display pop-up advertisements depending on the user's keywords and browsing history. Its variants can also monitor the user's activities, download applications, and send system information back to a remote server.
- Game password stealers are less common in Germany than worldwide. Win32/Taterf and Win32/Frethog, which rank second and fifth in the world respectively, rank fifteenth and twenty-fifth in Germany.

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 in order 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

Gulf Cooperation Council States (Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, and United Arab Emirates)

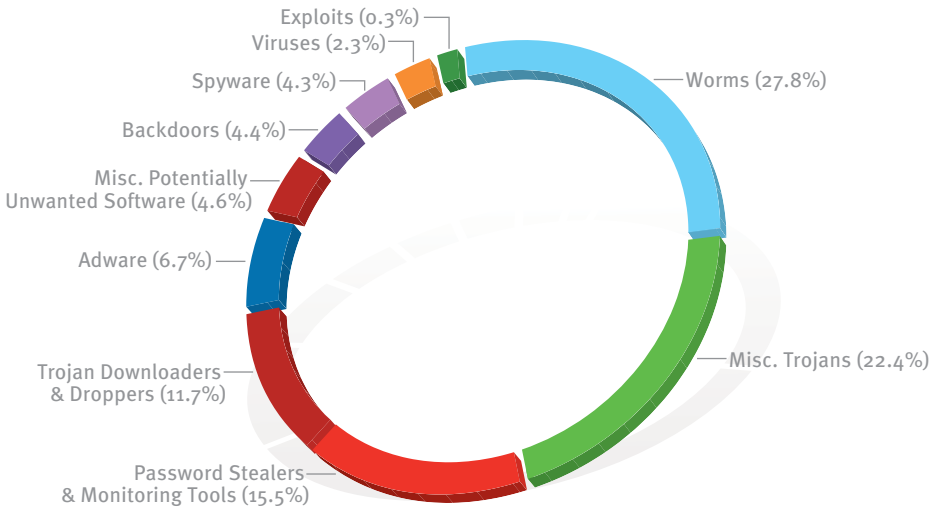
The states of the Gulf Cooperation Council (GCC) had infection rates (CCM) ranging from 6.2 to 20.8 in 1H09. (*CCM* is the number of computers cleaned for every 1,000 executions of the MSRT. For more information, see page 37.) Figure 129 lists the infection rate for each of the GCC member states.

FIGURE 129. Infection rates (CCM) for the states of the Gulf Cooperation Council in 1H09

State	CCM (1H09)	CCM (2H08)
Bahrain	9.3	8.1
Kuwait	7.7	9.8
Oman	7.9	7.7
Qatar	6.8	6.4
Saudi Arabia	20.8	18.5
United Arab Emirates	6.2	5.3

Figure 130 and Figure 131 list the most common malware and potentially unwanted software categories and families detected by all Microsoft desktop anti-malware products in the states of the GCC in 1H09.

FIGURE 130. Malware and potentially unwanted software in the Gulf Cooperation Council states, by category, in 1H09



Category	Infected Computers
Worms	119,764
Misc. Trojans	96,662
Password Stealers & Monitoring Tools	66,820
Trojan Downloaders & Droppers	50,287
Adware	28,897
Misc. Potentially Unwanted Software	20,001
Backdoors	19,142
Spyware	18,551
Viruses	9,697
Exploits	1,127

Notes and observations:

- The threat landscape in the GCC states is clearly dominated by malware, which accounted for 84.4 percent of all threats detected on infected computers in 1H09.
- The most common category in the GCC states was Worms, which accounted for 27.8 percent of families detected on infected computers in 1H09. Win32/Taterf and Win32/Conficker, the top two families detected in the GCC states in 1H09, are both worms.
- The second-most common category in the GCC states in 1H09 was Miscellaneous Trojans, which includes trojan families that are not classified as downloaders/droppers or backdoors. Miscellaneous Trojans accounted for 22.4 percent of families detected on infected computers in 1H09.

FIGURE 131. Top 25 families in the Gulf Cooperation Council states in 1H09

Rank	Family	Most Significant Category	Infected Computers
1	Win32/Taterf	Worms	87,090
2	Win32/Conficker	Worms	74,428
3	Win32/Frethog	Password Stealers & Monitoring Tools	53,575
4	Win32/C2Lop	Miscellaneous Trojans	50,944
5	Win32/Renos	Trojan Downloaders & Droppers	28,074
6	Win32/Agent	Miscellaneous Trojans	13,559
7	Win32/Alureon	Miscellaneous Trojans	10,764
8	Win32/ZangoSearchAssistant	Adware	9,987
9	Win32/Brontok	Worms	9,672
10	Win32/Vundo	Miscellaneous Trojans	8,605
11	Win32/Zlob	Trojan Downloaders & Droppers	8,525
12	Win32/FakeXPA	Miscellaneous Trojans	8,275
13	Win32/SeekmoSearchAssistant	Adware	8,048
14	Win32/ZangoShoppingreports	Adware	6,517
15	Win32/RJump	Worms	6,309
16	Win32/Hotbar	Adware	4,897
17	Win32/Small	Miscellaneous Trojans	4,858
18	Win32/Cutwail	Trojan Downloaders & Droppers	4,592
19	Win32/Yektel	Trojan Downloaders & Droppers	4,071
20	Win32/Ldpinch	Password Stealers & Monitoring Tools	3,992
21	Win32/Advantage	Adware	3,961
22	Win32/Koobface	Worms	3,790
23	Win32/Ardamax	Trojan Downloaders & Droppers	3,587
24	Win32/VB	Miscellaneous Trojans	3,425
25	Win32/Rustock	Backdoor	3,418

(Conficker data provided by the Shadowserver Foundation)

Encyclopedia

Win32/Taterf: A family of worms that spread through mapped drives in order 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.

http://www.microsoft.com/av

Encyclopedia

Win32/MessengerPlus: A non-Microsoft add-on for Microsoft's Windows Live Messenger, called Messenger Plus!. It comes with an optional sponsor program installation, detected as Spyware:Win32/C2Lop.

http://www.microsoft.com/av

Notes and observations:

- For the most accurate possible estimate of Win32/Conficker's impact, the figure given reflects the number of IP addresses infected by the A, B, C, and D variants that were detected on June 30, 2009, by sinkhole installations operated by the Shadowserver Foundation and the CWG. For more information about Conficker and the worldwide response to the threat, see "Win32/Conficker Update," beginning on page 95, and "Case Study: The Conficker Working Group," beginning on page 29.
- Win32/C2Lop, the eighteenth-most common family detected on infected computers worldwide in 1H09, ranks fourth in the GCC states. C2Lop is a trojan that modifies Web browser settings, adds Web browser bookmarks to advertisements, updates itself, and delivers pop-up and contextual advertisements. It is sometimes distributed with the potentially unwanted software family Win32/MessengerPlus.

Japan

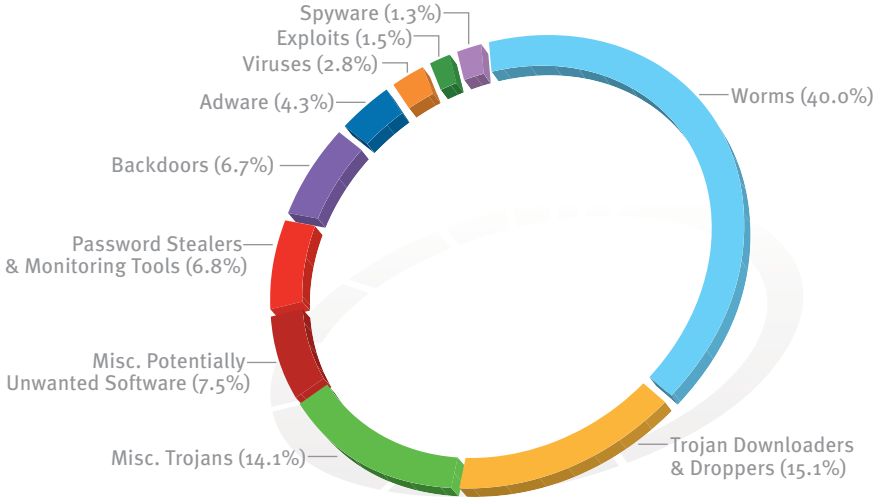
The infection rate (CCM) in Japan was 3.0 in 1H09, up from 1.7 in 2H08 and significantly lower than the worldwide 1H09 infection rate of 8.7. (*CCM* is the number of computers cleaned for every 1,000 executions of the MSRT. For more information, see page 37.)

The infection rate in Japan is consistently among the lowest in the world. See "Best Practices Around the World," beginning on page 44, for information and guidance from security response professionals in four of the world's least infected countries, including Japan.

Figure 132 and Figure 133 list the most common malware and potentially unwanted software categories and families detected by all Microsoft desktop anti-malware products in Japan in 1H09.

FIGURE 132. Malware and potentially unwanted software in Japan, by category, in 1H09

Category	Infected Computers
Worms	255,004
Trojan Downloaders & Droppers	96,062
Misc. Trojans	89,952
Misc. Potentially Unwanted Software	47,580
Password Stealers & Monitoring Tools	43,067
Backdoors	43,015
Adware	27,537
Viruses	17,902
Exploits	9,328
Spyware	8,088



Notes and observations:

- The threat landscape in Japan was dominated by malware, which accounted for 86.9 percent of all threats detected on infected computers in 1H09, up from 62.2 percent in 2H08.
- The most common category in Japan was Worms, which accounted for 40.0 percent of families detected on infected computers in 1H09. Win32/Taterf and Win32/Conficker, the top two families detected in Japan in 1H09, are both worms.
- The second-most common category in Japan in 1H09 was Trojan Downloaders & Droppers, which accounted for 15.1 percent of families detected on infected computers in 1H09.

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.

http://www.microsoft.com/av

FIGURE 133. Top 25 families in Japan in 1H09

Rank	Family	Most Significant Category	Infected Computers
1	Win32/Taterf	Worms	190,557
2	Win32/Zlob	Trojan Downloaders & Droppers	31,184
3	Win32/Renos	Trojan Downloaders & Droppers	26,041
4	Win32/Conficker	Worms	32,330
5	Win32/Alureon	Miscellaneous Trojans	20,010
6	Win32/Agent	Miscellaneous Trojans	16,805
7	Win32/Vundo	Miscellaneous Trojans	14,921
8	Win32/Antinny	Worms	14,063
9	Win32/Frethog	Password Stealers & Monitoring Tools	12,886
10	Win32/Cutwail	Trojan Downloaders & Droppers	12,204
11	Win32/Corripio	Password Stealers & Monitoring Tools	11,768
12	Win32/Hupigon	Backdoor	10,734
13	Win32/Rbot	Backdoor	10,079
14	ASX/Wimad	Trojan Downloaders & Droppers	9,786
15	Win32/Tibs	Miscellaneous Trojans	9,578
16	Win32/Small	Trojan Downloaders & Droppers	9,318
17	Win32/Parite	Viruses	8,721
18	Win32/RJump	Worms	8,561
19	Win32/BaiduSobar	Miscellaneous Potentially Unwanted Software	8,242
20	Win32/Haxdoor	Backdoor	7,662
21	Win32/Lolyda	Password Stealers & Monitoring Tools	6,917
22	Win32/ZangoSearchAssistant	Adware	5,941
23	Win32/Playmp3z	Adware	5,716
24	Win32/FakeXPA	Miscellaneous Trojans	5,286
25	Win32/Rustock	Backdoor	5,177

(Conficker data provided by the Shadowserver Foundation)

Notes and observations:

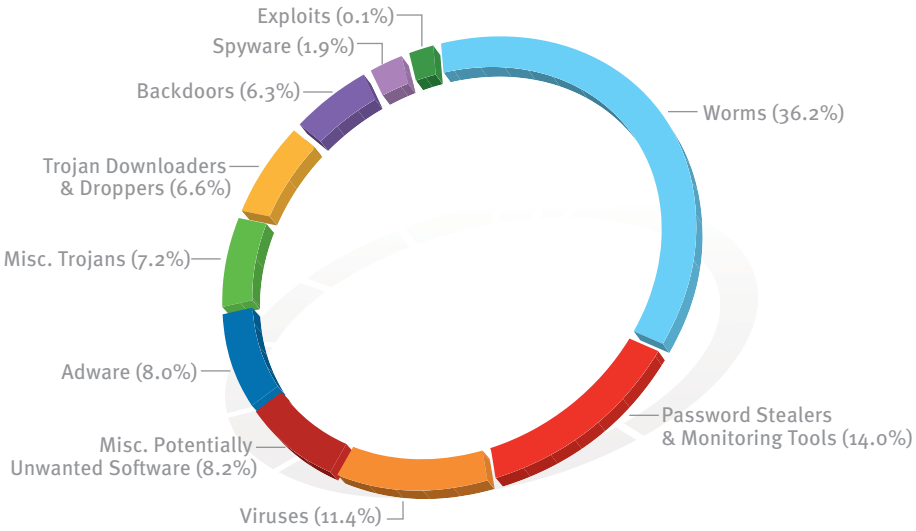
- For the most accurate possible estimate of Win32/Conficker's impact, the figure given reflects the number of IP addresses infected by the A, B, C, and D variants that were detected on June 30, 2009, by sinkhole installations operated by the Shadowserver Foundation and the CWG. For more information about Conficker and the worldwide response to the threat, see "Win32/Conficker Update," beginning on page 95, and "Case Study: The Conficker Working Group," beginning on page 29.
- Win32/Taterf, the second-most common family detected on infected computers worldwide in 1H09, ranked first by a wide margin in Japan, with almost six times as many detections as any other family. Taterf is a family of worms that spread through mapped drives in order to steal login and account details for popular online games. For more information about this class of password stealers, see "Online Gaming-Related Families," on page 62 of *Microsoft Security Intelligence Report, Volume 5 (January through June 2008)*.
- Win32/Antinny, which is not among the top 25 families detected worldwide, ranks eighth in Japan. Antinny is a family of worms that spreads using a Japanese peer-to-peer file-sharing application named Winny. The worm creates a copy of itself with a deceptive file name in the Winny upload folder so that it can be downloaded by other Winny users.
- Win32/Hupigon, which is not among the top 25 families detected worldwide, ranks twelfth in Japan. Hupigon is a family of backdoor trojans that are prevalent in a number of places in Asia. It sometimes drops a keystroke logger and password stealer and may support other malicious add-ons, as well.
- Win32/Haxdoor, which is not among the top 25 families detected worldwide, ranks twentieth in Japan. Haxdoor is a backdoor trojan that allows remote control of the machine over the Internet. The trojan is rootkit-enabled, allowing it to hide processes and files related to the threat. Haxdoor lowers security settings on the computer and gathers user and system information to send to a third party.

Korea

The infection rate (CCM) in Korea was 21.3 in 1H09, up from 18.3 in 2H08 and significantly higher than the worldwide 1H09 infection rate of 8.7. (*CCM* is the number of computers cleaned for every 1,000 executions of the MSRT. For more information, see page 37.)

Figure 134 and Figure 135 list the most common malware and potentially unwanted software categories and families detected by all Microsoft desktop anti-malware products in Korea in 1H09.

FIGURE 134. Malware and potentially unwanted software in Korea, by category, in 1H09



Category	Infected Computers
Worms	715,607
Password Stealers & Monitoring Tools	276,088
Viruses	224,811
Misc. Potentially Unwanted Software	162,802
Adware	158,858
Misc. Trojans	142,451
Trojan Downloaders & Droppers	130,381
Backdoors	125,248
Spyware	36,826
Exploits	1,599

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.

http://www.microsoft.com/av

Notes and observations:

- The threat landscape in Korea was dominated by malware, which accounted for 81.9 percent of all threats detected on infected computers in 1H09.
- The most common category in Korea was Worms, which accounted for 36.2 percent of families detected on infected computers in 1H09. Win32/Taterf and Win32/Conficker, ranked first and third in Korea in 1H09, are both worms.
- The second-most common category in Korea in 1H09 was Password Stealers & Monitoring Tools, which accounted for 14.0 percent of families detected on infected computers in 1H09.

FIGURE 135. Top 25 families in Korea in 1H09

Rank	Family	Most Significant Category	Infected Computers
1	Win32/Taterf	Worms	596,273
2	Win32/Frethog	Password Stealers & Monitoring Tools	249,376
3	Win32/Conficker	Worms	182,159
4	Win32/Virut	Viruses	121,542
5	Win32/Pointfree	Miscellaneous Potentially Unwanted Software	105,130
6	Win32/Parite	Viruses	80,443
7	Win32/Small	Trojan Downloaders & Droppers	78,723
8	Win32/Matcash	Trojan Downloaders & Droppers	72,577
9	Win32/Rbot	Backdoor	52,418
10	Win32/Nieguide	Adware	45,003
11	Win32/Wukill	Worms	36,319
12	Win32/RewardNetwork	Spyware	35,292
13	Win32/RJump	Worms	30,333
14	Win32/Ithink	Adware	28,924
15	Win32/Cutwail	Trojan Downloaders & Droppers	27,522
16	Win32/Corripio	Password Stealers & Monitoring Tools	27,062
17	Win32/Nbar	Adware	26,188
18	Win32/Agent	Miscellaneous Trojans	25,820
19	Win32/Hupigon	Backdoor	24,485
20	Win32/Alureon	Miscellaneous Trojans	20,197
21	Win32/Jeefo	Viruses	18,301
22	Win32/Tibs	Miscellaneous Trojans	15,930
23	Win32/Renos	Trojan Downloaders & Droppers	14,397
24	Win32/Bonuscash	Adware	13,792
25	Win32/Pointad	Adware	12,921

(Conficker data provided by the Shadowserver Foundation)

Notes and observations:

- For the most accurate possible estimate of Win32/Conficker's impact, the figure given reflects the number of IP addresses infected by the A, B, C, and D variants that were detected on June 30, 2009, by sinkhole installations operated by the Shadowserver Foundation and the CWG. For more information about Conficker and the worldwide response to the threat, see "Win32/Conficker Update," beginning on page 95, and "Case Study: The Conficker Working Group," beginning on page 29.
- Win32/Taterf and Win32/Frethog, ranked first and second in Korea in 1H09, both belong to a group of loosely related families that target players of online games, which are popular in Korea, and attempt to steal their login credentials. Win32/Corripio, ranked sixteenth in Korea in 1H09, is another game password stealer. 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)*.
- Several of the top families in Korea are potentially unwanted software families that primarily target Korean-language audiences. Win32/Pointfree, ranked fifth, is a browser modifier that redirects users when invalid Web site addresses or search terms are entered in the Windows Internet Explorer address bar. Win32/Ithink, ranked fourteenth, displays pop-up advertisements; it is usually bundled with other applications. Win32/Nieguide, ranked tenth, is a detection for a DLL file that connects to a Web site and may display advertisements or download other programs.

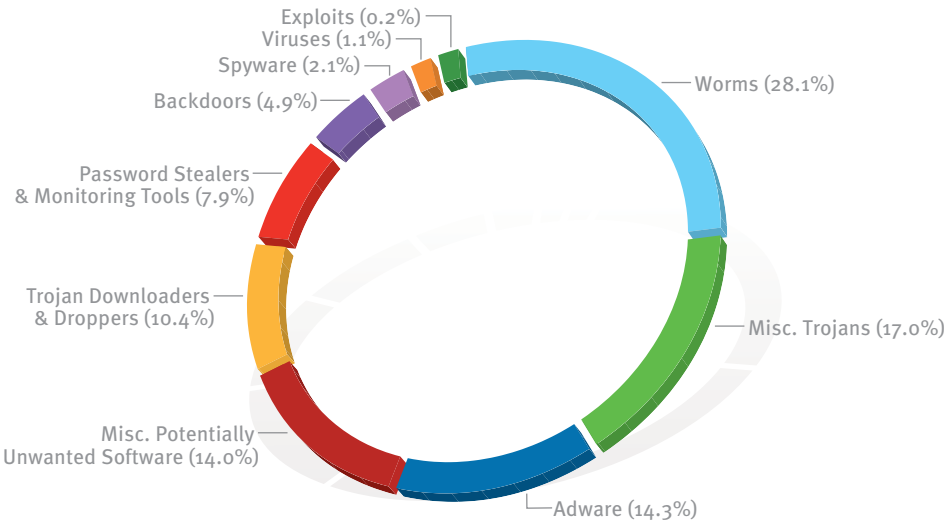
Malaysia

The infection rate (CCM) in Malaysia was 5.1 in 1H09, up from 3.5 in 2H08 and lower than the worldwide 1H09 infection rate of 8.7. (*CCM* is the number of computers cleaned for every 1,000 executions of the MSRT. For more information, see page 37.)

Figure 136 and Figure 137 list the most common malware and potentially unwanted software categories and families detected by all Microsoft desktop anti-malware products in Malaysia in 1H09.

FIGURE 136. Malware and potentially unwanted software in Malaysia, by category, in 1H09

Category	Infected Computers
Worms	32,387
Misc. Trojans	19,664
Adware	16,484
Misc. Potentially Unwanted Software	16,140
Trojan Downloaders & Droppers	12,048
Password Stealers & Monitoring Tools	9,121
Backdoors	5,633
Spyware	2,379
Viruses	1,272
Exploits	288



- The threat landscape in Malaysia is dominated by malware, which accounted for 69.6 percent of all threats detected on infected computers in 1H09.
- The most common category in Malaysia was Worms, which accounted for 28.1 percent of families detected on infected computers in 1H09. Win32/Conficker and Win32/Taterf, the top two families detected in Malaysia in 1H09, are both worms.
- The second-most common category in Malaysia in 1H09 was Miscellaneous Trojans, which includes trojan families that are not classified as downloaders/droppers or backdoors. Miscellaneous Trojans accounted for 17.0 percent of families detected on infected computers in 1H09.

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 in order to steal login and account details for popular online games.

http://www.microsoft.com/av

FIGURE 137. Top 25 families in Malaysia in 1H09

Rank	Family	Most Significant Category	Infected Computers
1	Win32/Conficker	Worms	97,478
2	Win32/Taterf	Worms	13,285
3	Win32/ZangoSearchAssistant	Adware	8,998
4	Win32/BaiduSobar	Miscellaneous Potentially Unwanted Software	8,392
5	Win32/Frethog	Password Stealers & Monitoring Tools	7,011
6	Win32/Renos	Trojan Downloaders & Droppers	6,204
7	Win32/SeekmoSearchAssistant	Adware	5,274
8	Win32/ZangoShoppingreports	Adware	4,383
9	Win32/Hotbar	Adware	3,782
10	Win32/RJump	Worms	3,623
11	Win32/IRCbot	Backdoor	3,144
12	Win32/Agent	Miscellaneous Trojans	2,621
13	Win32/Sogou	Miscellaneous Potentially Unwanted Software	2,471
14	Win32/FakeXPA	Miscellaneous Trojans	2,440
15	Win32/Vundo	Miscellaneous Trojans	2,345
16	Win32/Alureon	Miscellaneous Trojans	2,322
17	Win32/Zlob	Trojan Downloaders & Droppers	2,278
18	Win32/C2Lop	Miscellaneous Trojans	2,030
19	Win32/Winwebsec	Miscellaneous Trojans	1,569
20	Win32/Advantage	Adware	1,567
21	Win32/ConHook	Trojan Downloaders & Droppers	1,552
22	Win32/Small	Miscellaneous Trojans	1,389
23	Win32/InternetAntivirus	Miscellaneous Trojans	1,318
24	Win32/VB	Miscellaneous Trojans	1,305
25	Win32/Webdir	Spyware	1,133

(Conficker data provided by the Shadowserver Foundation)

Notes and observations:

- For the most accurate possible estimate of Win32/Conficker's impact, the figure given reflects the number of IP addresses infected by the A, B, C, and D variants that were detected on June 30, 2009, by sinkhole installations operated by the Shadowserver Foundation and the CWG. For more information about Conficker and the worldwide response to the threat, see "Win32/Conficker Update," beginning on page 95, and "Case Study: The Conficker Working Group," beginning on page 29.
- Three of the top 25 families (Win32/FakeXPA, Win32/Winwebsec, and Win32/InternetAntivirus) are rogue security software programs. Rogue security software is relatively rare in Asia; Malaysia is a notable exception, perhaps due to the relatively high percentage of Malaysians who speak English.
- Likewise, 4 of the top 10 families (Win32/ZangoSearchAssistant, Win32/SeekmoSearchAssistant, Win32/ZangoShoppingReports, and Win32/Hotbar) are related potentially unwanted software families published by the same software vendor. All four rank significantly higher in Malaysia than in other locations in Asia.
- Eight of the top 25 families are potentially unwanted software families.

Encyclopedia

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/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/ZangoShoppingReports: Adware that displays targeted advertising to affected users while they browse the Internet, based on search terms entered into search engines.

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

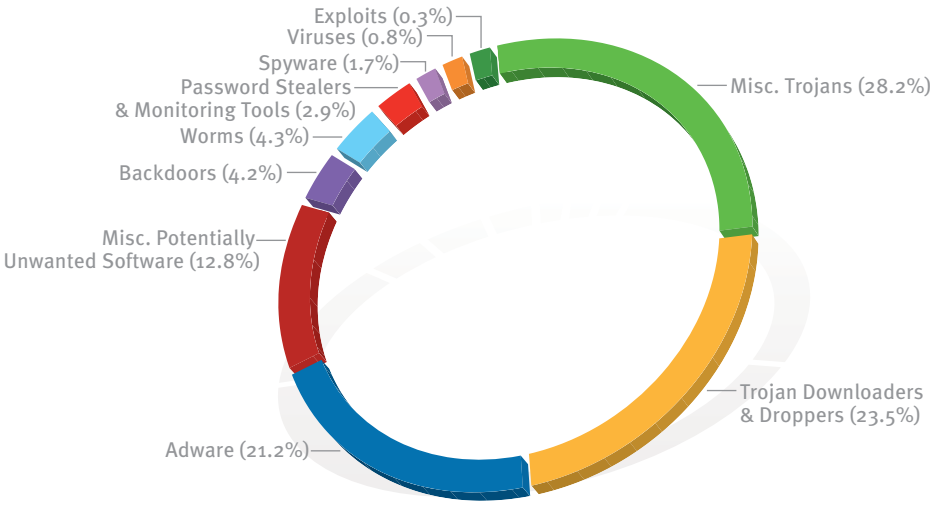
http://www.microsoft.com/av

Norway

The infection rate (CCM) in Norway was 3.3 in 1H09, down from 6.8 in 2H08 and significantly lower than the worldwide 1H09 infection rate of 8.7. (*CCM* is the number of computers cleaned for every 1,000 executions of the MSRT. For more information, see page 37.)

Figure 138 and Figure 139 list the most common malware and potentially unwanted software categories and families detected by all Microsoft desktop anti-malware products in Norway in 1H09.

FIGURE 138. Malware and potentially unwanted software in Norway, by category, in 1H09



Category	Infected Computers
Misc. Trojans	48,805
Trojan Downloaders & Droppers	40,701
Adware	36,561
Misc. Potentially Unwanted Software	22,137
Backdoors	7,335
Worms	7,364
Password Stealers & Monitoring Tools	5,085
Spyware	3,008
Viruses	1,395
Exploits	461

Notes and observations:

- The threat landscape in Norway was dominated by malware, which accounted for 64.3 percent of all threats detected on infected computers in 1H09, down from 66.8 percent in 2H08.
- The most common category in Norway was Miscellaneous Trojans, which includes all trojan families that are not classified as downloaders/droppers or backdoors. It was detected on 28.2 percent of all infected computers in 1H09, down from 39.0 percent in 2H08, and accounts for 11 of the top 25 families.
- The second-most common category in Norway was Trojan Downloaders & Droppers, which accounted for 23.5 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 Norway in 1H09.

FIGURE 139. Top 25 families in Norway in 1H09

Rank	Family	Most Significant Category	Infected Computers
1	Win32/ZangoSearchAssistant	Adware	25,036
2	Win32/Renos	Trojan Downloaders & Droppers	22,196
3	Win32/Vundo	Miscellaneous Trojans	13,172
4	Win32/ZangoShoppingreports	Adware	12,274
5	Win32/Hotbar	Adware	11,528
6	Win32/Zlob	Trojan Downloaders & Droppers	10,016
7	Win32/Alureon	Miscellaneous Trojans	8,271
8	Win32/Microbillsys	Miscellaneous Potentially Unwanted Software	7,886
9	Win32/Koobface	Worms	5,435
10	Win32/FakeXPA	Miscellaneous Trojans	4,897
11	Win32/SeekmoSearchAssistant	Adware	4,844
12	Win32/C2Lop	Miscellaneous Trojans	3,699
13	Win32/Cutwail	Trojan Downloaders & Droppers	3,197
14	Win32/Winwebsec	Miscellaneous Trojans	3,043
15	Win32/Yektel	Trojan Downloaders & Droppers	2,898
16	Win32/Agent	Miscellaneous Trojans	2,753
17	Win32/FakeRean	Miscellaneous Trojans	2,725
18	Win32/Playmp3z	Adware	2,590
19	Win32/Tibs	Miscellaneous Trojans	2,474
20	Win32/InternetAntivirus	Miscellaneous Trojans	2,380
21	Win32/Rustock	Backdoor	2,272
22	Win32/Winfixer	Miscellaneous Trojans	1,984
23	Win32/FakeSecSen	Miscellaneous Trojans	1,597
24	Win32/Advantage	Adware	1,476
25	Win32/Rbot	Backdoor	1,410

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/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

Notes and observations:

- Win32/Conficker, the most prevalent family worldwide in 1H09, was not among the top 25 families detected on infected computers in Norway.
- Worms were rare in Norway in general, with only one worm (Win32/Koobface) appearing among the top 25 families detected on infected computers in 1H09.
- Seven of the top 25 families (Win32/FakeXPA, Win32/Winwebsec, Win32/Yektel, Win32/FakeRean, Win32/InternetAntivirus, Win32/Winfixer, and Win32/FakeSecSen) are rogue security software programs. Of these, FakeXPA, Winfixer, and FakeSecSen were in the top 25 for Norway in 2H08, and the others are newcomers to the list.
- Seven of the top 25 families are potentially unwanted software families, compared to 11 in 2H08.
- Win32/Microbillsys, which is not among the top 25 families detected worldwide, ranks eighth in Norway. Microbillsys is a program that processes payments made to a billing Web site. It is considered potentially unwanted software because it cannot be removed from the Add/Remove Programs list in Control Panel; rather, a user requires an "uninstall code" before the program can be removed.

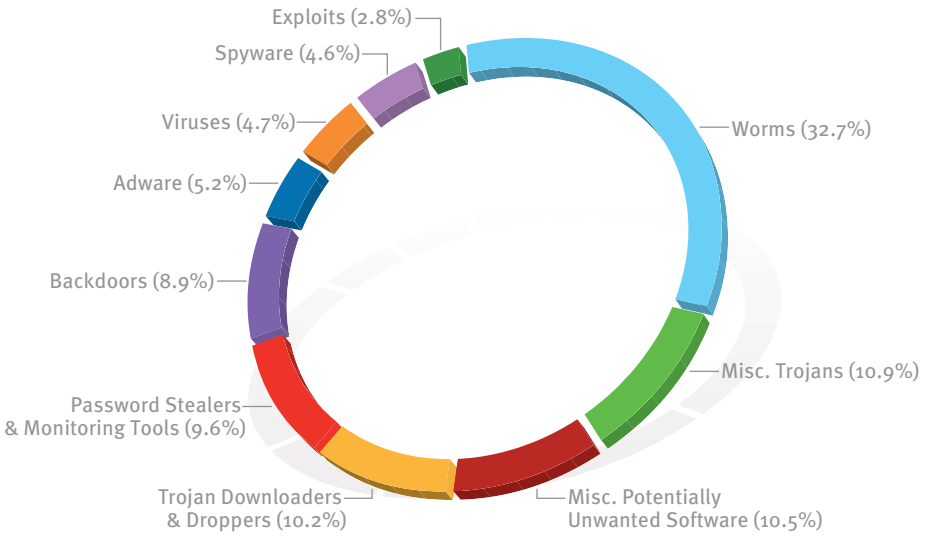
Russia

The infection rate (CCM) in Russia was 15.0 in 1H09, down from 21.1 in 2H08 and significantly higher than the worldwide 1H09 infection rate of 8.7. (*CCM* is the number of computers cleaned for every 1,000 executions of the MSRT. For more information, see page 37.)

Figure 140 and Figure 141 list the most common malware and potentially unwanted software categories and families detected by all Microsoft desktop anti-malware products in Russia in 1H09.

FIGURE 140. Malware and potentially unwanted software in Russia, by category, in 1H09

Category	Infected Computers
Worms	227,113
Misc. Trojans	75,833
Misc. Potentially Unwanted Software	72,687
Trojan Downloaders & Droppers	70,651
Password Stealers & Monitoring Tools	66,386
Backdoors	61,503
Adware	36,133
Viruses	32,387
Spyware	32,219
Exploits	19,664



Notes and observations:

- The threat landscape in Russia was dominated by malware, which accounted for 79.7 percent of all threats detected on infected computers in 1H09, down from 81.1 percent in 2H08.
- The most common category in Russia was Worms, which accounted for 32.7 percent of families detected on infected computers in 1H09, up from 32.2 percent in 2H08. Win32/Conficker and Win32/Taterf, the top two families detected in Russia in 1H09, are both worms.
- The second-most common category in Russia was Miscellaneous Trojans, which includes all trojan families that are not classified as downloaders/droppers or backdoors. It accounted for 10.9 percent of families detected on infected computers in 1H09, down from 13.0 percent in 2H08, and accounts for 6 of the top 25 families.

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 in order to steal login and account details for popular online games.

http://www.microsoft.com/av

FIGURE 141. Top 25 families in Russia in 1H09

Rank	Family	Most Significant Category	Infected Computers
1	Win32/Conficker	Worms	482,476
2	Win32/Taterf	Worms	119,294
3	Win32/Cutwail	Trojan Downloaders & Droppers	33,785
4	Win32/Ldpinch	Password Stealers & Monitoring Tools	28,240
5	Win32/Frethog	Password Stealers & Monitoring Tools	27,512
6	Win32/Renos	Trojan Downloaders & Droppers	26,840
7	Win32/Alureon	Miscellaneous Trojans	25,997
8	Win32/Jeefo	Viruses	22,552
9	Win32/Rustock	Backdoor	18,822
10	Win32/WhenU	Adware	15,306
11	Win32/RJump	Worms	14,812
12	Win32/Wukill	Worms	13,530
13	Win32/Brontok	Worms	12,816
14	Win32/Agent	Miscellaneous Trojans	12,564
15	Win32/Kerlofost	Miscellaneous Potentially Unwanted Software	11,240
16	Win32/IRCbot	Backdoor	11,128
17	Win32/Sdbot	Backdoor	9,395
18	Win32/Advantage	Adware	8,572
19	Win32/Rbot	Backdoor	8,260
20	Win32/Tibs	Miscellaneous Trojans	8,249
21	Win32/Vundo	Miscellaneous Trojans	7,418
22	Win32/Small	Miscellaneous Trojans	7,147
23	Win32/FakeXPA	Miscellaneous Trojans	6,581
24	Win32/GhostRadmin	Miscellaneous Potentially Unwanted Software	6,006
25	Win32/Haxdoor	Backdoor	5,822

(Conficker data provided by the Shadowserver Foundation)

Notes and observations:

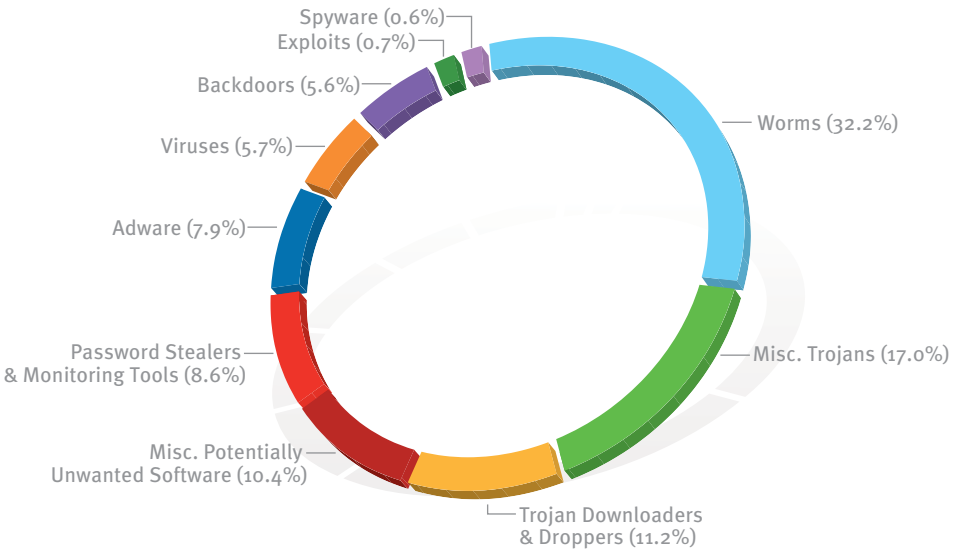
- For the most accurate possible estimate of Win32/Conficker's impact, the figure given reflects the number of IP addresses infected by the A, B, C, and D variants that were detected on June 30, 2009, by sinkhole installations operated by the Shadowserver Foundation and the CWG. For more information about Conficker and the worldwide response to the threat, see "Win32/Conficker Update," beginning on page 95, and "Case Study: The Conficker Working Group," beginning on page 29.
- Rogue security software is consistently rare in Russia. Win32/FakeXPA is the only rogue security software program in the top 25, as it was in 2H08.
- Four of the top 25 families are potentially unwanted software families, down from six in 2H08.
- Win32/Wukill, which is not among the top 25 families detected worldwide, ranks twelfth in Russia. Wukill is a family of mass-mailing e-mail and network worms.
- Win32/Kerlofost, which is not among the top 25 families detected worldwide, ranks fifteenth in Russia. Kerlofost is a browser helper object (BHO) that may modify browsing behavior; redirect searches; report user statistics, behavior, and searches back to a remote server; and display pop-up advertisements.
- Win32/GhostRadmin, which is not among the top 25 families detected worldwide, ranks twenty-fourth in Russia. GhostRadmin is a program that allows a computer to be controlled remotely, similar to Remote Desktop. It has a number of legitimate uses but is considered potentially unwanted software because it can be used by an attacker with malicious intent to gain control of a user's computer under some circumstances.

South Africa

The infection rate (CCM) in South Africa was 5.5 in 1H09, down from 6.6 in 2H08 and lower than the worldwide 1H09 infection rate of 8.7. (*CCM* is the number of computers cleaned for every 1,000 executions of the MSRT. For more information, see page 37.)

Figure 142 and Figure 143 list the most common malware and potentially unwanted software categories and families detected by all Microsoft desktop anti-malware products in South Africa in 1H09.

FIGURE 142. Malware and potentially unwanted software in South Africa, by category, in 1H09



Category	Infected Computers
Worms	30,361
Misc. Trojans	16,026
Trojan Downloaders & Droppers	10,532
Misc. Potentially Unwanted Software	9,842
Password Stealers & Monitoring Tools	8,121
Adware	7,443
Viruses	5,352
Backdoors	5,283
Exploits	704
Spyware	610

Notes and observations:

- The threat landscape in South Africa was dominated by malware, which accounted for 81.1 percent of all threats detected on infected computers in 1H09.
- The most common category in South Africa was Worms, which accounted for 32.2 percent of families detected on infected computers in 1H09. Eight of the top 25 families in South Africa were worms, including 5 of the top 10.
- 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. It was detected on 17.0 percent of all infected computers in 1H09.

FIGURE 143. Top 25 families in South Africa in 1H09

Rank	Family	Most Significant Category	Infected Computers
1	Win32/Taterf	Worms	12,504
2	Win32/Frethog	Password Stealers & Monitoring Tools	5,151
3	Win32/RJump	Worms	5,095
4	Win32/Renos	Trojan Downloaders & Droppers	5,080
5	Win32/Hamweq	Worms	3,893
6	Win32/ZangoSearchAssistant	Adware	3,410
7	Win32/Autorun	Worms	3,238
8	Win32/Agent	Miscellaneous Trojans	2,770
9	Win32/Vundo	Miscellaneous Trojans	2,305
10	Win32/Brontok	Worms	2,247
11	Win32/Zlob	Trojan Downloaders & Droppers	2,204
12	Win32/FakeXPA	Miscellaneous Trojans	2,124
13	Win32/SeekmoSearchAssistant	Adware	2,069
14	Win32/ZangoShoppingreports	Adware	2,059
15	Win32/Alureon	Miscellaneous Trojans	2,007
16	Win32/RealVNC	Miscellaneous Potentially Unwanted Software	2,007
17	Win32/Mabezat	Worms	1,942
18	Win32/Hotbar	Adware	1,860
19	Win32/Virut	Viruses	1,576
20	Win32/Conficker	Worms	1,459
21	Win32/InternetAntivirus	Miscellaneous Trojans	1,336
22	Win32/Rbot	Backdoor	1,320
23	Win32/Ldpinch	Password Stealers & Monitoring Tools	1,210
24	Win32/Yektel	Trojan Downloaders & Droppers	1,155
25	Win32/Wukill	Worms	1,147

(Conficker data provided by the Shadowserver Foundation)

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.

http://www.microsoft.com/av

Notes and observations:

- For the most accurate possible estimate of Win32/Conficker's impact, the figure given reflects the number of IP addresses infected by the A, B, C, and D variants that were detected on June 30, 2009, by sinkhole installations operated by the Shadowserver Foundation and the CWG. For more information about Conficker and the worldwide response to the threat, see "Win32/Conficker Update," beginning on page 95, and "Case Study: The Conficker Working Group," beginning on page 29.
- Three of the top 25 families (Win32/FakeXPA, Win32/InternetAntivirus, and Win32/Yektel) are rogue security software programs.
- Five of the top 25 families are potentially unwanted software families.
- Win32/Hamweq, which is not among the top 25 families detected worldwide, ranks fifth in South Africa. Hamweq is a worm that spreads via removable drives, such as USB memory sticks. It may also be used by a remote attacker to cause the computer to participate in distributed denial-of-service (DDoS) attacks.

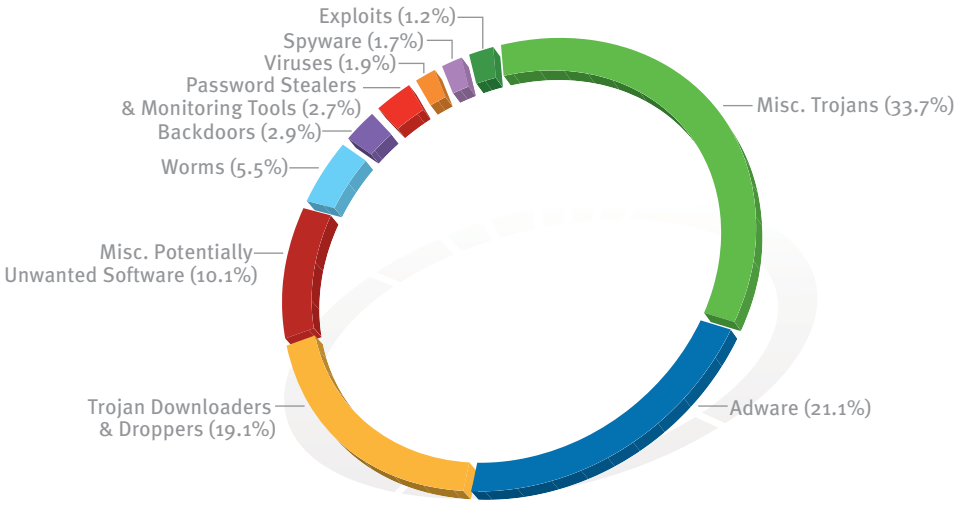
United Kingdom

The infection rate (CCM) in the United Kingdom was 4.9 in 1H09, down from 5.7 in 2H08 and lower than the worldwide 1H09 infection rate of 8.7. (*CCM* is the number of computers cleaned for every 1,000 executions of the MSRT. For more information, see page 37.)

Figure 144 and Figure 145 list the most common malware and potentially unwanted software categories and families detected by all Microsoft desktop anti-malware products in the United Kingdom in 1H09.

FIGURE 144. Malware and potentially unwanted software in the United Kingdom, by category, in 1H09

Category	Infected Computers
Misc. Trojans	914,014
Adware	572,729
Trojan Downloaders & Droppers	518,228
Misc. Potentially Unwanted Software	273,091
Worms	148,934
Backdoors	79,907
Password Stealers & Monitoring Tools	72,350
Viruses	52,095
Spyware	46,620
Exploits	33,858



Notes and observations:

- The threat landscape in the United Kingdom was dominated by malware, which accounted for 67.1 percent of all threats detected on infected computers in 1H09, up from 61.3 percent in 2H08.
- 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 33.7 percent of threats detected on infected computers in 1H09, up from 28.5 percent in 2H08, and accounts for 12 of the top 25 families, including 5 of the top 10 families.
- The second-most common category in the United Kingdom was Adware, which accounted for 21.1 percent of all threats detected on infected computers.

FIGURE 145. Top 25 families in the United Kingdom in 1H09

Rank	Family	Most Significant Category	Infected Computers
1	Win32/ZangoSearchAssistant	Adware	452,977
2	Win32/Renos	Trojan Downloaders & Droppers	269,141
3	Win32/ZangoShoppingreports	Adware	211,049
4	Win32/Hotbar	Adware	197,772
5	Win32/Alureon	Miscellaneous Trojans	160,623
6	Win32/FakeXPA	Miscellaneous Trojans	147,733
7	Win32/Vundo	Miscellaneous Trojans	123,763
8	Win32/Wintrim	Miscellaneous Trojans	106,792
9	Win32/C2Lop	Miscellaneous Trojans	87,304
10	Win32/Yektel	Trojan Downloaders & Droppers	86,759
11	Win32/Agent	Miscellaneous Trojans	86,400
12	ASX/Wimad	Trojan Downloaders & Droppers	83,583
13	Win32/Zlob	Trojan Downloaders & Droppers	76,681
14	Win32/Winwebsec	Miscellaneous Trojans	61,135
15	Win32/Koobface	Worms	54,056
16	Win32/Microbillsys	Miscellaneous Potentially Unwanted Software	52,457
17	Win32/InternetAntivirus	Miscellaneous Trojans	51,779
18	Win32/SeekmoSearchAssistant	Adware	50,049
19	Win32/Conficker	Worms	48,298
20	Win32/Tibs	Miscellaneous Trojans	37,523
21	Win32/FakeRean	Miscellaneous Trojans	33,226
22	Win32/Taterf	Worms	30,910
23	Win32/Obfuscator	Miscellaneous Trojans	27,831
24	JS/Xilos	Viruses	26,935
25	Win32/Small	Miscellaneous Trojans	22,684

(Conficker data provided by the Shadowserver Foundation)

Notes and observations:

- For the most accurate possible estimate of Win32/Conficker's impact, the figure given reflects the number of IP addresses infected by the A, B, C, and D variants that were detected on June 30, 2009, by sinkhole installations operated by the Shadowserver Foundation and the CWG. For more information about Conficker and the worldwide response to the threat, see "Win32/Conficker Update," beginning on page 95, and "Case Study: The Conficker Working Group," beginning on page 29.
- Five of the top 25 families (Win32/FakeXPA, Win32/Yektel, Win32/Winwebsec, Win32/InternetAntivirus, and Win32/FakeRean) are rogue security software programs. Of these, only Win32/FakeXPA was in the top 25 in 2H08.
- Five of the top 25 families are potentially unwanted software families, compared to 11 in 2H08.
- JS/Xilos is the only virus in the top 25. Xilos is a detection for a proof-of-concept JavaScript obfuscation technique, which was originally published in 2002 in the sixth issue of *29A*, an early online magazine for virus creators.
- Win32/Microbillsys, which is not among the top 25 families detected worldwide, ranks sixteenth in the United Kingdom. Microbillsys is a program that processes payments made to a billing Web site. It is considered potentially unwanted software because it cannot be removed from the Add/Remove Programs list in Control Panel; rather, a user requires an "uninstall code" before the program can be removed.

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.

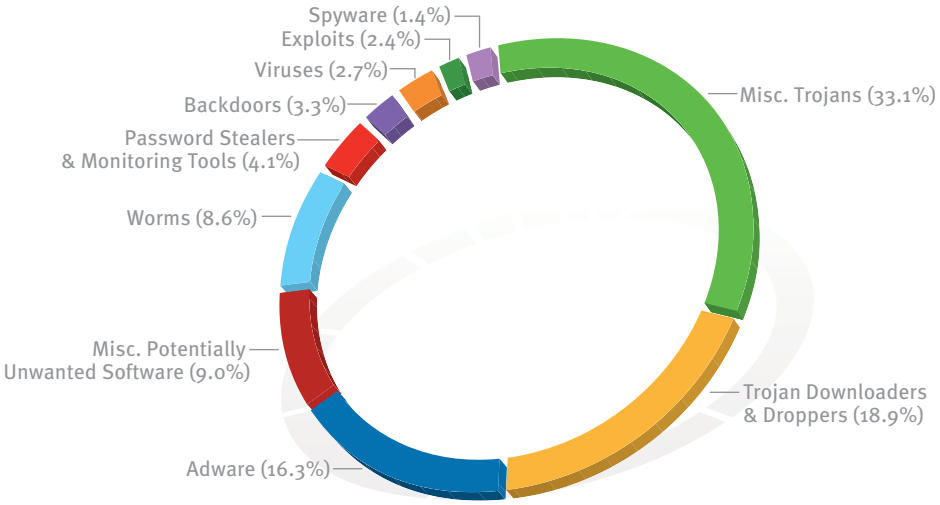
http://www.microsoft.com/av

United States

The infection rate (CCM) in the United States was 8.6 in 1H09, down from 9.1 in 2H08 and very close to the worldwide 1H09 infection rate of 8.7. (*CCM* is the number of computers cleaned for every 1,000 executions of the MSRT. For more information, see page 37.)

Figure 146 and Figure 147 list the most common malware and potentially unwanted software categories and families detected by all Microsoft desktop anti-malware products in the United States in 1H09.

FIGURE 146. Malware and potentially unwanted software in the United States, by category, in 1H09



Category	Infected Computers
Misc. Trojans	6,449,568
Trojan Downloaders & Droppers	3,686,485
Adware	3,185,212
Misc. Potentially Unwanted Software	1,762,475
Worms	1,672,548
Password Stealers & Monitoring Tools	808,307
Backdoors	640,586
Viruses	530,477
Exploits	474,148
Spyware	279,845

Notes and observations:

- The threat landscape in the United States was dominated by malware, which accounted for 73.3 percent of all threats detected on infected computers in 1H09, up from 67.0 percent in 2H08.
- 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. It accounted for 33.1 percent of threats detected on infected computers in 1H09, up from 29.4 percent in 2H08, and accounts for 9 of the top 25 families.
- The second-most common category in the United States was Trojan Downloaders & Droppers, which accounted for 18.9 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 the United States in 1H09.

FIGURE 147. Top 25 families in the United States in 1H09

Rank	Family	Most Significant Category	Infected Computers
1	Win32/FakeXPA	Miscellaneous Trojans	1,848,039
2	Win32/Renos	Trojan Downloaders & Droppers	1,790,015
3	Win32/ZangoSearchAssistant	Adware	1,423,978
4	Win32/GameVance	Adware	1,205,981
5	Win32/Vundo	Miscellaneous Trojans	1,080,845
6	Win32/Alureon	Miscellaneous Trojans	931,933
7	ASX/Wimad	Trojan Downloaders & Droppers	720,757
8	Win32/Yektel	Trojan Downloaders & Droppers	717,324
9	Win32/Taterf	Worms	666,840
10	Win32/ZangoShoppingreports	Adware	663,947
11	Win32/Agent	Miscellaneous Trojans	644,192
12	Win32/Hotbar	Adware	624,974
13	Win32/Zlob	Trojan Downloaders & Droppers	522,068
14	Win32/Winwebsec	Miscellaneous Trojans	504,626
15	Win32/Tibs	Miscellaneous Trojans	492,524
16	Win32/Frethog	Password Stealers & Monitoring Tools	390,031
17	Win32/Koobface	Worms	384,560
18	Win32/Obfuscator	Miscellaneous Trojans	278,197
19	Win32/InternetAntivirus	Miscellaneous Trojans	275,808
20	Win32/SeekmoSearchAssistant	Adware	274,492
21	Win32/Pdfjsc	Exploit	273,990
22	Win32/Rustock	Backdoor	238,894
23	JS/Xilos	Viruses	228,884
24	Win32/OneStepSearch	Miscellaneous Potentially Unwanted Software	218,924
25	Win32/ConHook	Miscellaneous Trojans	200,583

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.

http://www.microsoft.com/av

Notes and observations:

- Win32/Conficker, the most prevalent family worldwide in 1H09, was not among the top 25 families detected on infected computers in the United States.
- Four of the top 25 families (Win32/FakeXPA, Win32/Yektel, Win32/Winwebsec, and Win32/InternetAntivirus) are rogue security software programs. Of these, only Win32/FakeXPA and Win32/Yektel were in the top 25 in 2H08.
- Six of the top 25 families are potentially unwanted software families, compared to 11 in 2H08.
- JS/Xilos is the only virus in the top 25. Xilos is a detection for a proof-of-concept JavaScript obfuscation technique, which was originally published in 2002 in the sixth issue of *29A*, an early online magazine for virus creators.
- Win32/Pdfjsc, which is not among the top 25 families detected worldwide, ranks twenty-first in the United States. Pdfjsc is a family of specially crafted PDF files that exploits vulnerabilities in Adobe Acrobat and Adobe Reader. The files contain malicious JavaScript that executes when opened with a vulnerable program.

Appendix C: 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 *SIR* to deliver the most comprehensive and detailed perspective on the threat landscape available in the software industry:

- Bing, the new 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 2.7 billion times in 1H09, or nearly 450 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. In 2H09, Microsoft is replacing Windows Live OneCare with a new consumer-oriented protection product, Microsoft Security Essentials (MSE), at no charge to licensed users of Windows. For more information on MSE, please visit the product Web page at http://www.microsoft.com/security_essentials.

- The Windows Live OneCare product family also includes the Windows Live OneCare safety scanner (http://safety.live.com), which is a free, online tool that detects and removes malware and potentially unwanted software using the same signature database as the Windows Live OneCare client product. Unlike the Windows Live OneCare client product (but like the MSRT), the Windows Live OneCare safety scanner does not offer real-time protection and cannot prevent a user's computer from becoming infected.
- 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
	Consumers	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
Windows Live OneCare	•		•	•	•	•		Web/Store Purchase
Windows Malicious Software Removal Tool	•		Prevalent malware families				•	Windows Update/ Automatic Updates Download Center
Windows Defender	•				•	•	•	Download Center Windows Vista
Forefront Online Protection for Exchange		•	•	•				Web

Software Vulnerability and Breach Data

The efforts to identify and fix vulnerabilities lacked a common naming mechanism until a consortium led by The MITRE Corporation began publishing the Common Vulnerabilities and Exposures list, which drives a common naming mechanism that can be leveraged by multiple vulnerability databases and security products. The CVE naming conventions provide the most comprehensive list of vulnerabilities worldwide, across software products of all types. This report uses the CVE naming conventions when identifying individual vulnerabilities.

The analysis in this report uses a set of data that has been created by compiling, customizing, and cross-checking several sources of data available on the Internet:

- Common Vulnerabilities and Exposures Web site (http://cve.mitre.org).
  - A large portion of the data analyzed originates from the CVE list maintained at this site, which is currently sponsored by the United States Department of Homeland Security. The naming mechanisms and external references to sources for additional information were particularly valuable.
- National Vulnerability Database Web site (http://nvd.nist.gov).
  - This database superset of the CVE list, which provides additional objective information concerning vulnerabilities, was the source used to determine severity ratings and exploit complexity assessment. The NVD is also sponsored by the DHS, and their data is downloadable in an XML format at http://nvd.nist.gov/download.cfm.
- Security Web sites. The following sites, along with many others, were utilized for detailed verification and validation of vulnerability specifics:
  - http://www.securityfocus.com
  - http://www.secunia.com
  - http://www.securitytracker.com

- Vendor Web sites and support sites. The following sites, along with others, were utilized for confirmation and validation of vulnerability details:
  - https://rhn.redhat.com/errata
  - http://support.novell.com/linux/psdb
  - http://sunsolve.sun.com
  - http://www.microsoft.com/technet/security/current.aspx
  - http://www.ubuntu.com/usn
- OSF DataLossDB (http://datalossdb.org).
  - Data for the "Security Breach Trends" section comes from DataLossDB, a community research project managed by the Open Security Foundation, which is aimed at documenting known and reported data-loss incidents worldwide. Security researchers around the world, including researchers at Microsoft, collaborate to build the database by submitting new incident reports and adding data to existing ones.

Appendix D: Microsoft Security Bulletins in 1H09

Bulletin ID	Product	Bulletin Severity	XI Rating	CVE	Workarounds	Mitigations
MS09-001	Windows	Critical	3	CVE-2008-4114	1	2
			3	CVE-2008-4834	1	2
			3	CVE-2008-4835	1	2
MS09-002	Internet Explorer	Critical	1	CVE-2009-0075	2	5
			1	CVE-2009-0076	2	5
MS09-003	Exchange Server	Critical	2	CVE-2009-0098	1	0
			2	CVE-2009-0099	0	0
MS09-004	SQL Server	Important	1	CVE-2008-5416	1	3
MS09-005	Office	Important	2	CVE-2009-0095	0	2
			2	CVE-2009-0096	0	2
			2	CVE-2009-0097	0	2
MS09-006	Windows	Critical	2	CVE-2009-0081	1	1
			3	CVE-2009-0082	0	1
			3	CVE-2009-0083	0	1
MS09-007	Windows	Important	2	CVE-2009-0085	0	2
MS09-008	Windows	Important	2	CVE-2009-0093	1	1
			2	CVE-2009-0094	1	1
			2	CVE-2009-0233	0	1
			2	CVE-2009-0234	0	1
MS09-009	Office	Critical	2	CVE-2009-0100	2	3
			1	CVE-2009-0238	2	2
MS09-010	Windows, Office	Critical	1	CVE-2008-4841	2	3
			2	CVE-2009-0087	2	4
			1	CVE-2009-0088	1	3
			1	CVE-2009-0235	1	3
MS09-011	Windows	Critical	2	CVE-2009-0084	1	2
MS09-012	Windows	Important	1	CVE-2008-1436	3	1
			1	CVE-2009-0078	3	1
			1	CVE-2009-0079	3	1
			1	CVE-2009-0080	3	1
MS09-013	Windows	Critical	1	CVE-2009-0086	0	1
			1	CVE-2009-0089	0	1
			1	CVE-2009-0550	0	3
MS09-014	Internet Explorer	Critical	3	CVE-2008-2540	0	1
			1	CVE-2009-0550	0	5
			2	CVE-2009-0551	2	5
			3	CVE-2009-0552	2	5
			3	CVE-2009-0553	2	4
			1	CVE-2009-0554	2	5
MS09-015	Windows	Moderate	2	CVE-2008-2540	0	0
MS09-016	ISA Server	Important	3	CVE-2009-0077	0	0
			3	CVE-2009-0237	0	3

Continues on next page

APPENDIX D. Continued

Bulletin ID	Product	Bulletin Severity	XI Rating	CVE	Workarounds	Mitigations
MS09-017	Office	Critical	1	CVE-2009-0220	1	5
			2	CVE-2009-0221	2	4
			1	CVE-2009-0222	1	5
			1	CVE-2009-0223	1	5
			2	CVE-2009-0224	2	4
			2	CVE-2009-0225	1	4
			1	CVE-2009-0226	1	5
			1	CVE-2009-0227	1	5
			1	CVE-2009-0556	2	4
			1	CVE-2009-1128	1	5
			1	CVE-2009-1129	1	6
			1	CVE-2009-1130	2	3
			1	CVE-2009-1131	0	4
			1	CVE-2009-1137	1	6
MS09-018	Windows	Critical	3	CVE-2009-1138	2	1
			3	CVE-2009-1139	2	1
MS09-019	Internet Explorer	Critical	3	CVE-2007-3091	2	4
			3	CVE-2009-1140	2	5
			1	CVE-2009-1141	2	5
			3	CVE-2009-1528	2	5
			2	CVE-2009-1529	2	5
			2	CVE-2009-1530	2	5
			2	CVE-2009-1531	2	5
			1	CVE-2009-1532	2	5
MS09-020	Internet Information Services	Important	3	CVE-2009-1122	2	3
			1	CVE-2009-1535	2	4
MS09-021	Office	Critical	2	CVE-2009-0549	2	3
			1	CVE-2009-0557	1	3
			2	CVE-2009-0558	0	3
			1	CVE-2009-0559	0	3
			3	CVE-2009-0560	2	3
			1	CVE-2009-0561	2	3
			1	CVE-2009-1134	2	3
MS09-022	Windows	Critical	1	CVE-2009-0228	3	1
			3	CVE-2009-0229	1	1
			1	CVE-2009-0230	1	3
MS09-023	Windows	Moderate	3	CVE-2009-0239	0	2
MS09-024	Office	Critical	1	CVE-2009-1533	1	5
MS09-025	Windows	Important	2	CVE-2009-1123	0	1
			1	CVE-2009-1124	0	1
			1	CVE-2009-1125	0	1
			1	CVE-2009-1126	0	1
MS09-026	Windows	Important	2	CVE-2009-0568	0	1
MS09-027	Office	Critical	2	CVE-2009-0563	1	3
			1	CVE-2009-0565	1	4

Glossary

ActiveX control
A software component of Microsoft Windows that can be used to create and distribute small applications through Internet Explorer. ActiveX controls can be developed and used by software to perform functions that would otherwise not be available using 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. While some adware can be beneficial by subsidizing a program or service, other adware programs may display advertisements without adequate consent.

backdoor trojan
A type of trojan that provides attackers with remote access to infected computers. Bots are a sub-category of backdoor trojans. Also see *botnet*.

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. *Second-order 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.

generic
A type of signature capable of detecting a large variety of malware samples from a specific family, or of a specific type.

heuristics
A tool or technique that enhances the ability to identify certain, and potentially common, code patterns. This is useful for making, for example, generic detections for a malware family.

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)*.

macro virus
A type of virus written as a macro for an application (such as Microsoft Word or Excel). A macro virus infects a file by replicating itself as a macro for that file, ensuring that when the file is opened, the virus is run.

Malicious Software Removal Tool
The Windows Malicious Software Removal Tool 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.

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*.

polymorphic
A virus that can mutate its structure to avoid detection by antivirus programs. It can mutate usually by changing a variable or variables in its code without changing its overall algorithm.

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.

second-order cross-site scripting
See *cross-site scripting.*

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.

signature
A set of malware characteristics that can be used to identify it using antivirus/antispyware products.

sinkhole
A server or set of servers designed to absorb and analyze malware traffic.

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.

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*.