Microsoft Security Intelligence Report

Volume 6

July through December 2008

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.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Authors

Richard Boscovich
Microsoft Internet Safety and Enforcement Team

Darren Canavor
Microsoft Security Engineering Center

Joe Faulhaber
Microsoft Malware Protection Center

Vinny Gullotto
Microsoft Malware Protection Center

Jeff Jones
Microsoft Trustworthy Computing

John Lambert
Microsoft Security Engineering Center

Paul Laudanski
Microsoft Internet Safety and Enforcement Team

Ziv Mador
Microsoft Malware Protection Center

Ritesh Mordani
Microsoft Forefront Online Security for Exchange

Hamish O'Dea
Microsoft Malware Protection Center

Sasi Parthasarathy
Microsoft Live Search

Anthony Penta
Microsoft Windows Safety Platform

Christian Seifert
Microsoft Live Search

Adam Shostack
Microsoft Security Engineering Center

George Stathakopoulos
Microsoft Security Response Center

Adrian Stone
Microsoft Security Response Center

Matt Thomlinson
Microsoft Security Engineering Center

Scott Wu
Microsoft Malware Protection Center

Terry Zink
Microsoft Forefront Online Security for Exchange

Contributors

Fred Aaron
Microsoft Security Engineering Center

Doug Cavit
Microsoft Trustworthy Computing

Neil Cowie
Microsoft Security Engineering Center

Dave Forstrom
Microsoft Trustworthy Computing

Heather Goudey
Microsoft Malware Protection Center

Michael Grady
Microsoft Trustworthy Computing

Ali Haveliwala
Microsoft Forefront Online Security for Exchange

Satomi Hayakawa
Japan Security Response Team

Aaron Hulett
Microsoft Malware Protection Center

Japan Security Response Team
Microsoft Japan

Jeannette Jarvis
Microsoft Customer Support Services

Hong Jia
Microsoft Malware Protection Center

Allen Jones
Microsoft Security Engineering Center

David Kennedy
Microsoft Legal and Corporate Affairs

Jimmy Kuo
Microsoft Malware Protection Center

Ken Malcolmson
Microsoft Trustworthy Computing

Bronwen Matthews
Microsoft Trustworthy Computing

Mark Miller
Microsoft Trustworthy Computing

Patrick Nolan
Microsoft Malware Protection Center

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

Alan Wallace
Microsoft Trustworthy Computing

Jeff Williams
Microsoft Malware Protection Center

External Contributor

Paul Henry
Technical Writer

Table of Contents

Authors, Contributors, and External Contributor 3

About This Report 7

Scope 7

Reporting Period 7

Data Sources 7

Key Findings 8

Rogue Security Software 8

Industry Vulnerability Disclosures 8

Microsoft Vulnerability Details for 2H08 8

Responsible Disclosure 9

Browser-Based Exploits. 9

Microsoft Office Format File Exploits 9

PDF Format File Exploits 10

Security Breach Trends 10

Malicious and Potentially Unwanted Software 10

Operating System Trends 10

The Threat Landscape at Home and in the Enterprise 11

Geographic Distribution of Malware Hosting Sites 11

E-Mail Threats 12

Malicious Web Sites 12

Drive-By Download Pages 12

Geographic Distribution of Drive-By Download Pages 12

Executive Foreword 13

Is the Threat Landscape Getting Better or Worse—
Does the Answer Really Matter?. 13

Social Engineering as a Weapon 15

Fear, Trust, and Desire: Attackers Target Basic Human Drives . . . 15

Notable Social Engineering Techniques in 2H08 19

Vulnerability Trends 26

Industry Vulnerability Disclosures 26

Industry Vulnerability Severity 27

Industry Vulnerability Complexity 29

Operating System and Browser Vulnerabilities 30

Microsoft Vulnerability Disclosures 31

Vulnerabilities Addressed by Microsoft in 2H08 37

Vulnerability Trends Summary and Conclusion 38

Strategies, Mitigations, and Countermeasures 38

Call to Action—End to End Trust 39

Out-of-Band Microsoft Security Updates in 2H08 40
MS08-067: Vulnerability in Windows Server Service. 41
MS08-078: Vulnerability in Internet Explorer 45
Strategy, Mitigations, and Countermeasures 46

Exploit Trends 47
Top Browser-Based Exploits 47
Document File Format Exploits 51
Strategies, Mitigations, and Countermeasures 59
Call to Action—End to End Trust 61

Security Breach Trends 62
Strategy, Mitigations, and Countermeasures 64
Call to Action—End to End Trust 64

Malware and Potentially Unwanted Software Trends 65
Infection Rates and CCM 65
Geographic Trends 65
Category Trends 72
Operating System Trends 74
Malware and Potentially Unwanted Software Families 77
MSRT New Families in 2H08. 79
User Reaction to Alerts 82
Trends in Sample Proliferation 86
Focus: The Threat Landscape at Home and in the Enterprise 89
Rogue Security Software 92
Legal Action Against Rogues 99
Strategy, Mitigations, and Countermeasures 104
Call to Action—End to End Trust 107

E-Mail Threats 109
Spam Trends and Statistics 109
Spammers Spoof 'Breaking News' E-Mail Newsletters 113
Spam Volume Drops 46 Percent When
Hosting Provider Goes Offline 113
Backscatter Causes 90 Percent of Bounce Messages 115

Malicious Web Sites 116
Analysis of Phishing Sites 116
Analysis of Malware Hosts. 122
Analysis of Drive-By Download Pages. 126
Strategies, Mitigations, and Countermeasures 131

Microsoft Malware Protection Center Executive Afterword 132

Appendix A: Full Infection Chart 134

Appendix B: Threat Assessments for Individual Locations 137

Australia 137

Brazil 140

Canada 143

France 146

Germany 149

Italy 152

Malaysia 155

Mexico 158

Norway 161

Russia 164

United Kingdom 167

United States 170

Appendix C: Data Sources 173

Software Vulnerability and Breach Data 173

Microsoft Security Products 174

Glossary 178

About This Report

Scope

The *Security Intelligence Report (SIR)* is published by Microsoft 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 sixth installment of the *Microsoft 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 second half of 2008 (2H08), 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 1H08 represents the period covering the first half of 2008 (January 1 through June 30).

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 July through December 2008. This section summarizes the key points from the main sections of the report.

Rogue Security Software

- The prevalence of rogue security software has increased significantly over the six-month period, as it has for the past 18 months. Examples of rogue security software social engineering techniques, including screen shots, can be found in this volume of the *Security Intelligence Report (SIR)*. This report also features a focus section on legal actions taken against rogue security software distributors.

Industry Vulnerability Disclosures

- The total number of unique vulnerability disclosures across the industry decreased in the second half of 2008 (2H08)[1], down 3 percent from 1H08. For 2008 as a whole, total disclosures were down 12 percent from 2007.
- In contrast, vulnerabilities rated as High severity by the Common Vulnerability Scoring System (CVSS) increased 4 percent over 1H08; roughly 52 percent of all vulnerabilities were rated as High severity. For 2008 as a whole, the total number of High severity vulnerabilities was down 16 percent from 2007.
- Compounding the seriousness of the High severity vulnerabilities, the percentage of disclosed vulnerabilities that are easiest to exploit also increased; 56 percent required only a Low complexity exploit.
- The proportion of vulnerabilities disclosed industry-wide that affected operating systems continued to decline; more than 90 percent of vulnerabilities disclosed affected applications or browsers.

Microsoft Vulnerability Details for 2H08

- In 2H08, Microsoft released 42 security bulletins that addressed 97 individual vulnerabilities identified on the Common Vulnerabilities and Exposures (CVE) list, a 67.2 percent increase over the number of vulnerabilities addressed in 1H08. For the full year of 2008, Microsoft released 78 security bulletins addressing 155 vulnerabilities, a 16.8 percent increase over 2007.

[1] 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, 1H08 represents the period covering the first half of 2008 (January 1 through June 30), and 2H07 represents the period covering the second half of 2007 (July 1 through December 31).

Responsible Disclosure

- In 2H08, 70.6 percent of Microsoft vulnerability disclosures adhered to responsible disclosure practices, down from 78.2 percent in 1H08. The responsible disclosure percentage for the whole of 2008 was significantly higher than that of the previous year.
- Engaging with the security community directly, and proactively addressing security issues, results in the majority of issues being responsibly reported.

Browser-Based Exploits

- The most common system locale for victims of browser-based exploits was en-US (English language, United States), accounting for 32.4 percent of all incidents, followed by zh-CN (Chinese language, China), with 25.6 percent of incidents.
- For browser-based attacks on Windows XP®–based machines, Microsoft vulnerabilities accounted for 40.9 percent of the total, consistent with the pattern observed in 1H08. On Windows Vista®–based machines, the Microsoft proportion was much smaller, accounting for just 5.5 percent of the total, down from 5.7 percent in 1H08.
- Microsoft software accounted for 6 of the top 10 browser-based vulnerabilities attacked on computers running Windows XP in 2H08, compared to zero of the top 10 on computers running Windows Vista—similar to the pattern observed in 1H08.

Microsoft Office Format File Exploits

- The most frequently exploited vulnerabilities in Microsoft Office system software in the sample set were also some of the oldest—91.3 percent of attacks examined exploited a single vulnerability for which a security fix had been available for more than two years (CVE-2006-2492).
- The most common locale for victims was en-US (English language, United States), accounting for 32.5 percent of all incidents, followed by zh-TW (Chinese language, Taiwan), with 15.7 percent of incidents.
- In most cases, the application versions attacked did not have up-to-date service packs applied. For each version, the clear majority of the attacks affected the release to manufacturing (RTM) version of the application suite that had no service packs applied. In the sample of data analyzed by Microsoft researchers, for example, 100 percent of attacks against Office 2000 affected the RTM version of the application suite, released in 1999.

PDF Format File Exploits

- Use of the PDF format as an attack vector rose very sharply in 2H08, with attacks in July amounting to more than twice as many as in all of 1H08 combined and continuing to double, or almost double, for most of the remaining months of the year.
- Two vulnerabilities accounted for all of the attacks in the sample files examined (CVE-2008-2992 and CVE-2007-5659). Both vulnerabilities have security updates available from Adobe; neither vulnerability exists in current versions of affected Adobe products.

Security Breach Trends

- The top category reported for data loss through a security breach in 2H08 continued to be stolen equipment, such as laptop computers (33.5 percent of all data-loss incidents reported). This category and that of lost equipment account for 50 percent of all incidents reported.
- Security breaches from hacking or malware incidents remain at less than 20 percent of the total.

Malicious and Potentially Unwanted Software

- The most significant trend in 2H08 was the large increase in rogue security software 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. As the malware ecosystem becomes more reliant on social engineering, threats worldwide have become more dependent on language and cultural factors: In China, several malicious browser modifiers are prevalent; in Brazil, malware that targets users of online banks is widespread; and in Korea, viruses (such as Win32/Virut and Win32/Parite) are common.

Operating System Trends

- Different Windows® operating system versions show differing rates of infection, due to variances in the way people and organizations use each version, in addition to the different features and service packs that are available for each one.
- The infection rate for Windows Vista is significantly lower than that of its predecessor, Windows XP, in all configurations.
  - Comparing the latest service packs for each version, the infection rate of Windows Vista SP1 is 60.6 percent less than that of Windows XP SP3.

  - Comparing the RTM versions of these operating systems, the infection rate of the RTM version of Windows Vista is 89.1 percent less than that of the RTM version of Windows XP.

- The infection rate of Windows Server® 2008 RTM is 51.9 percent less than that of its predecessor, Windows Server 2003 SP2.
- The higher the service pack level, the lower the rate of infection. This trend can be observed consistently across client and server operating systems. There are two reasons for this:
  - Service packs include all previously released security updates. They can also include additional security features, mitigations, or changes to default settings to protect users.
  - Users who install service packs generally maintain their computers better than users who do not, and they may also be more cautious in the way they browse the Internet, open attachments, and engage in other activities that can expose 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, since 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.

The Threat Landscape at Home and in the Enterprise

- Computers running Forefront™ Client Security (typically found in corporate environments) were much more likely to encounter worms than were home computers running Windows Live™ OneCare™. Home computers also encountered significantly greater percentages of trojans, trojan downloaders and droppers, adware, and exploits. Similar percentages of backdoors and spyware were detected by both products.

Geographic Distribution of Malware Hosting Sites

- Malware hosting tends to be more stable and less geographically diverse than phishing hosting. This might be the result of relatively recent use of server takedowns and Web reputation as weapons in the fight against malware distribution. This means that malware distributors have not been forced to diversify their hosting arrangements.

E-Mail Threats

- More than 97 percent of e-mail messages sent over the Internet are unwanted: They have malicious attachments, are phishing attacks, or are spam.
- As in previous periods, spam in 2H08 was dominated by product advertisements, primarily pharmaceutical products (48.6 percent of the total). Together with non-pharmacy product ads (23.6 percent of the total), product advertisements accounted for 72.2 percent of spam in 2H08.

Malicious Web Sites

- Most phishing pages target financial organizations; however, in terms of impressions (instances of users attempting to visit a known phishing site, but being blocked), social networks are also commonly targeted.
- The McColo de-peering in mid-November 2008 appears to have had a dramatic effect on phishing impressions, which dropped 46.2 percent from October to November. Visits to phishing sites targeting social networking sites dropped from 34.1 percent of all impressions in October to just 1.1 percent in November.

Drive-By Download Pages

- More than 1 million drive-by download pages were detected monthly by Live Search since early 2H08. That equates to 0.07 percent of all pages indexed (about 1 in 1,500).
- The Top Level Domains (TLDs) with the highest rate of pages that hosted drive-by exploits were .name (0.23 percent of all pages), .edu (0.19 percent), and .net (0.19 percent).
- A small number of servers host the exploits which are used by the vast majority of drive-by download pages.

Geographic Distribution of Drive-By Download Pages

- More than 1 percent of the sites in the .cn country code TLD were found to be hosting drive-by download pages (although this trend seems to be declining), whereas only 0.01 percent of the sites in some other large country code TLDs, like .se and .jp, were similarly affected.
- Nearly half of all country code TLDs had no affected sites at all (most are small registries without many domains).

Executive Foreword

Is the Threat Landscape Getting Better or Worse—Does the Answer Really Matter?

I frequently get asked whether the threat landscape is improving or if it is becoming more dangerous. It's tempting to simply choose a position and support it using a few opportunistic stats from this latest *Microsoft Security Intelligence Report (SIR)*. As you'll read in the report, vulnerability disclosures went down for the third consecutive six month period, but there were still thousands of disclosures during that period of time across the entire software industry. Does this mean things are getting better or worse? In the first half of 2008 the most common victims of browser-based exploits had their system locale set to Chinese language (zh-CN), but this shifted to English language, United States (en-US) in the last six months of 2008. Does this mean things are getting better or worse? I could pull dozens of data points from the report to try to support either conclusion.

At the risk of sounding contrarian, I challenge you to take a more pragmatic approach to this question. Let me use the analogy of a submarine to make the point. Submarines are designed so that they can travel completely submerged in water for long periods of time. One obvious requirement is that the sub must effectively keep water from leaking into its interior. If the design fails to meet this requirement by even a small margin, the entire sub and its crew are at risk.

Managing an IT infrastructure is no different than the submarine analogy. The data in the SIR shows us that criminals on the Internet are constantly trying to gain access to systems using a plethora of attack techniques. Whether the number of techniques that criminals use is increasing or decreasing in a given period, or whether there are more victims in Greece or in Greenland during a given period, shouldn't alter how vigilant you are in defending your IT assets. But like water surrounding a sub, as long as criminals exist you'll need to protect and defend yourself as they constantly try to "seep" in.

This SIR focuses on the second half of 2008 and is based on data from the hundreds of millions of systems we receive data from each month. The SIR will help you understand the threats and the trends we see on the Internet; I hope this intelligence will be enlightening and help you determine if you need to make adjustments to your security posture.

In 2008 we also increased the amount of information and guidance that we provide to the industry and to customers with every security bulletin we release. The Microsoft Exploitability Index is designed to provide additional information to help customers better prioritize the deployment of Microsoft security updates. This index provides customers with guidance on the likelihood of functioning exploit code being developed for vulnerabilities addressed by Microsoft security updates within the first thirty days of that update's release. Additionally, since the amount of time between the release of a Microsoft security update and the release of exploit code for that update continues to shorten, we now offer the Microsoft Active Protections Program (MAPP), to security software providers. Members of MAPP receive security vulnerability information from the Microsoft Security Response Center

(MSRC) in advance of Microsoft's monthly security update. When MAPP partners receive vulnerability information early, they can provide updated protections to customers via their security software or devices, such as antivirus, network-based intrusion detection systems, or host-based intrusion prevention systems. Prior to MAPP, security software providers had to wait until the public release of a security update before building protections. With MAPP, security software providers can deliver protection features to customers more quickly, which helps customers better manage risk.

The goals of such offerings are to give customers more information and more time to make better and more informed decisions about risks, testing and deploying security updates and assessing their security posture. We are also trying to help customers and third parties develop the most secure and privacy-enhanced software possible by sharing our Security Development Lifecycle (SDL) as well as resources like the Microsoft Threat Modeling Tool, and extending these through the SDL Pro Network. Security Science at Microsoft helped us get ahead of criminals planning to use the MS08-067 vulnerability to attack customers and to make some key security innovations in upcoming product releases like Internet Explorer 8.

Looking into the future, Microsoft's End to End Trust vision has helped us understand the direction that Microsoft, industry and governments need to work towards in order to realize a more trustworthy Internet in the future.

Despite all the attacks you read about in the SIR and all the good work that Microsoft and the industry have done over the last half year, are things getting better or getting worse? My challenge to you is to resist using some impressions of how good or bad the threat landscape is to make the business case for security. No one I know would wait for evidence of a crime happening in their neighborhood before installing locks on their doors. Information Technology is no different; managing risk is a necessity today.

As always, we value your feedback, so please let us know what you think by emailing sirfb@microsoft.com. I hope you find this report useful.

George Stathakopoulos
General Manager, Trustworthy Computing Security
Trustworthy Computing Group

Social Engineering as a Weapon

To some extent, computer crime is represented in the popular imagination by the *hacker*, an archetypal underground figure with a talent for defeating weak security measures and exploiting vulnerabilities in computer systems. While these kinds of attacks remain a significant part of the threat landscape, improvements in software development practices and the increased availability and awareness of automatic software update mechanisms have greatly limited the kinds of technical exploit opportunities that are available to attackers. Instead, most attackers today rely heavily on social engineering techniques to mislead victims into unwittingly or even knowingly giving them information and access that would be much harder to take by force. Although media attention on social engineering attacks, like phishing, have raised public awareness of this sort of threat in recent years, attackers continue to find success with a variety of techniques for manipulating people.

Social engineering is a variation on the classic confidence game, versions of which have been recorded for hundreds of years. The targets of social engineering techniques tend to be ordinary people who use computers and the Internet in normal ways. These attacks succeed by exploiting fundamental human drives, motives, and weaknesses, and they are designed to be encountered by average Internet users engaging in thoroughly ordinary, everyday activities, like playing games, searching the Web, banking online, and communicating with friends. Victims can be specifically targeted or used as a means to an end. Many never even know they have been victimized.

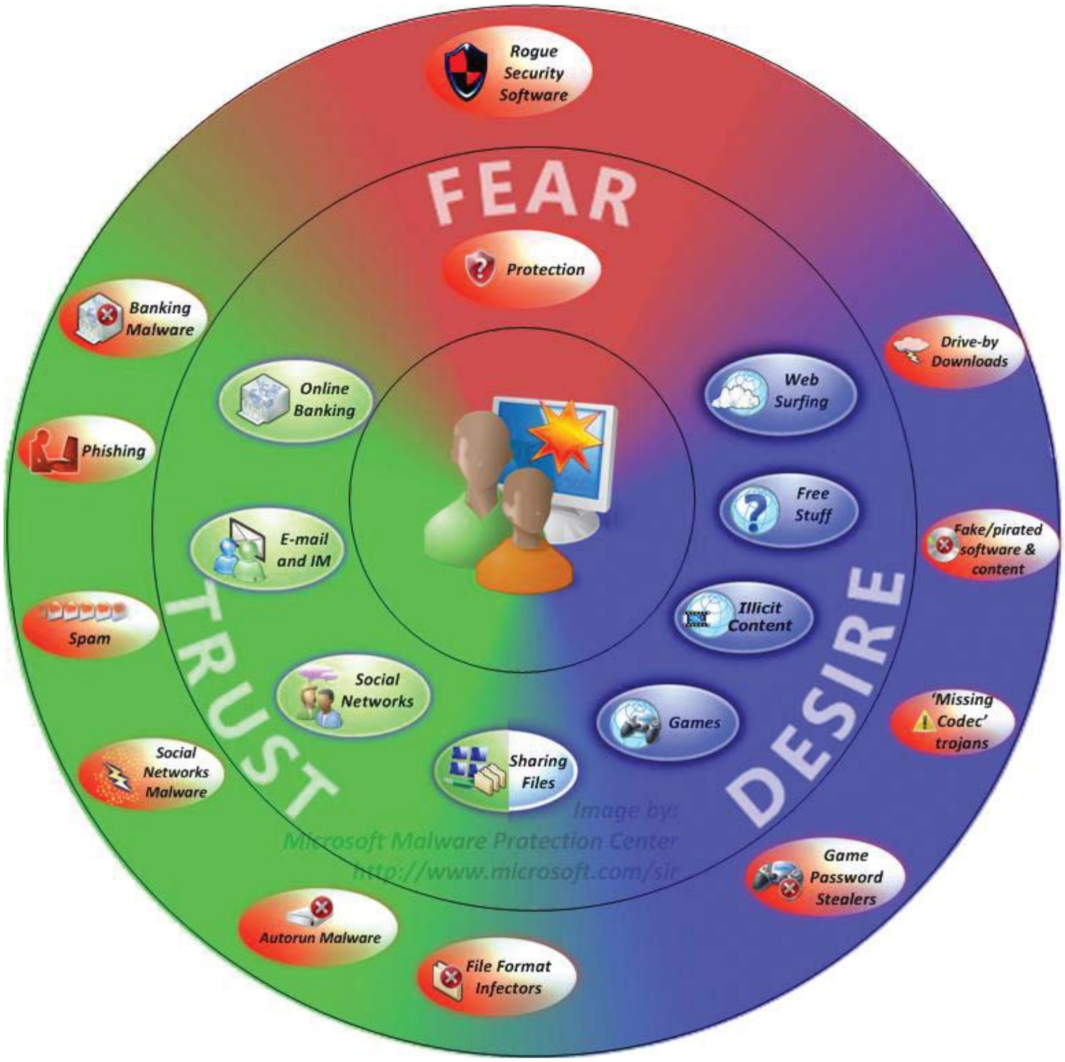
"The Threat Ecosystem," in *Microsoft Security Intelligence Report, Volume 5 (January through June 2008)*,[2] explored the underground economy of malware creation, distribution, and use. Among other things, it discussed the way attackers assemble large networks of secretly controlled computers, called *botnets*, that can be used to send spam, host phishing pages, and perform other illegal activities on behalf of their controllers. Other attackers target victims directly, using malware designed to display unwanted advertisements or steal sensitive information. All of these activities involve gaining control of someone's computer—sometimes through technical means, like exploiting a vulnerability, but more often through social engineering. This section of the *Security Intelligence Report* examines some of the social engineering techniques used by attackers in the second half of 2008 and why they succeed.

Fear, Trust, and Desire: Attackers Target Basic Human Drives

Most social engineering techniques are designed to take advantage of one or more fundamental drives, emotions, and feelings that are common to all human beings. They take advantage of *fear* of loss or damage. They take advantage of the *trust* that people place in other people and entities. And they take advantage of various elementary *desires* people have. (These are complex, multifaceted concepts, and any treatment of them here must necessarily be somewhat simplistic; however, they can nonetheless provide a useful model for understanding how social engineering works.)

[2] To download electronic copies of this and other volumes of the *Security Intelligence Report*, visit http://www.microsoft.com/sir.

FIGURE 1. Attackers use social engineering techniques to target computer users' feelings, emotions, and activities.



Targeting Fear

Fear is one of the strongest motivators of human behavior. In the world of computer security, fear of malware and other threats is often a useful and beneficial reaction, compelling users to install antivirus software and security updates and to practice safe online behavior. Unfortunately, attackers often use social engineering techniques that create fear in an effort to persuade potential victims to give them money. The clearest example of this is in the rise and spread of *rogue security software*.

Rogue security software masquerades as legitimate security programs offering protection from malware, spyware, and other threats, but actually uses social engineering to obtain money or sensitive information from victims and offers little or no real protection. Typically, a rogue security program displays false or misleading alerts about infections or vulnerabilities on the victim's computer and offers to fix the supposed problems for a price. Of the top 25 families detected on computers worldwide by Microsoft security products in 2H08 (see page 77), seven had some connection to rogue security software. See "Rogue Security Software," beginning on page 92, for more information.

Targeting Trust

Like fear, trust is a basic defense mechanism that people use in their lives, and it extends to online life, as well. Computer users are frequently told to be on guard against a variety of threats that can harm them or their computers or that can put their personal information at risk. Yet being on guard all the time is exhausting and can be very difficult. To make things more manageable, therefore, people tend to identify other people and entities that they can place in a "trustworthy" category, and they deal with these people and entities without constant suspicion. Attackers seek to take advantage of this trust to victimize otherwise vigilant people.

Some of the trust relationships that attackers take advantage of include:

- **Trust in one's work environment**. Enterprise computing environments typically include a number of centrally managed security measures, like antivirus software and an enterprise firewall. Users may have a tendency to assume—consciously or otherwise—that the workplace computing environment is basically safe and that the computing resources within it may be regarded without suspicion. An analogy might be drawn to the city walls that repelled invaders in medieval societies—with the walls in place, city inhabitants could go about their daily lives without worrying about threats from external invaders. Of course, one of the consequences of the city-wall mindset is that if invaders find a way to bypass the wall or otherwise get inside the city, attacking may be much easier than in a settlement with no walls at all, because the city inhabitants are not expecting the threat and are not prepared to deal with it. Likewise, many threats seen today are designed to take advantage of the decreased level of suspicion computer users maintain at work.
- **Trust in institutions**. Attackers often assume the identities of trusted institutions, like banks and media outlets, to take advantage of the trust users place in such institutions. The classic example of this kind of exploitation is *phishing*—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. Another example has been the recent rise of spam messages that closely resemble daily e-mail newsletters published by popular news sites, like CNN.com and MSNBC.com. Users who have preexisting subscriptions to these newsletters might click the links in the e-mail message, which lead to spam advertisements or malware. (For more information, see "Spammers Spoof 'Breaking News' E-Mail Newsletters," on page 113.)

- **Trust in friends and acquaintances**. Internet users are accustomed to maintaining constant contact with each other through e-mail, a tendency that attackers have long taken advantage of. In recent years, the emerging popularity of social networking sites and instant messaging (IM) systems have led many users to rely more on these modes to stay in contact with friends, a development that attackers have likewise moved to capitalize on by compromising users' social network accounts and using them to send malicious links to the victim's contacts. Attacks that involve social networks can be much more effective than e-mail–based attacks because they involve abusing the considerable level of trust users place in their friends. Even as users grow savvier about e-mail threats, like spam and phishing, they may be less skeptical of messages sent over social networks and more likely to believe that the originator of a message is truly the person they expect it to be.
- **Trust in one's computer**. People who work with computers on a regular basis become accustomed to the look and feel of different parts of the user interface, and they tend to take them for granted after sufficient exposure to them. Attackers take advantage of this trust by developing malware that closely resembles familiar parts of the operating system—to the point of illegally appropriating graphics and trademarks to avoid suspicion.

When attackers exploit a trust relationship, they damage the very thing they are exploiting. Such attacks harm not only the computer users who fall victim to them, but also the people and institutions whose reputations for trustworthiness have been appropriated and misused. Fighting trust-based attacks is everyone's problem.

Targeting Desire

The power of simple desire—for entertainment, for acquisition, for happiness—as a basic human drive should not be overlooked, and neither should the will of attackers to take advantage of it. Disguised trojans and exploits are abundant in the "bad neighborhoods" of the Internet, such as peer-to-peer (P2P) file-sharing services and Web sites that offer free pornographic content or pirated copies of movies, music, and software. Of course, not all desires are prurient or base; millions of people take to the Internet every day to play games, buy and sell goods and services, and simply seek entertaining or informative content. In a very broad sense, all of these desires involve obtaining something of value, and attackers have developed multiple ways to mislead people into exposing themselves to threats in search of that value.

Notable Social Engineering Techniques in 2H08

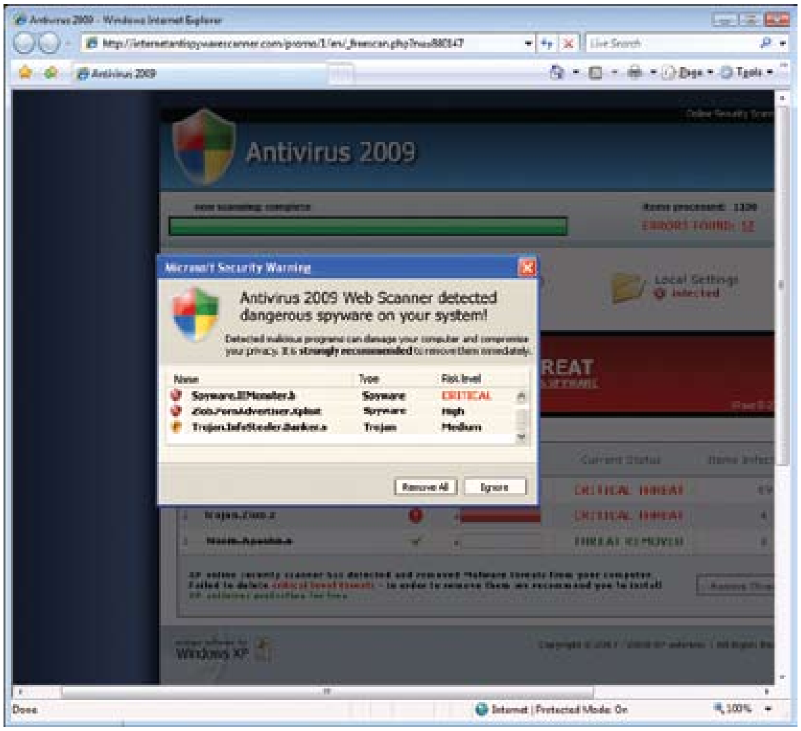
Social engineering attacks observed in 2H08 targeted all of these drives in different ways. Many of the attacks described in this section are discussed in detail elsewhere in the report, as noted.

Rogue Security Software

In a particularly perverse development observed over the past several years, the rise in awareness among the general public of the threat of malware and other computer-related threats has been paired with a rise in rogue security software, which seeks to take advantage of the healthy skepticism and savvy that this awareness has created. Some of the more prevalent rogue security software families appeal both to fear (of malware infection) and trust (of the operating system and its components) in a potent combination that can snare even experienced computer users.

For the unsuspecting user, the rogue security software experience often begins with a visit to a Web site advertising rogue security software. Such sites, which often feature a polished, professional appearance, usually include a link to a "trial" copy of the software. Some sites even use HTML and JavaScript techniques to conduct what appears to be a scan of the visitor's computer and to display a list of dangerous-sounding threats that it supposedly detects.

FIGURE 2. A bogus "online scanner" that attempts to persuade visitors to install rogue security software family Win32/FakeXPA



Microsoft Security Warning

Antivirus 2009 Web Scanner detected dangerous spyware on your system!

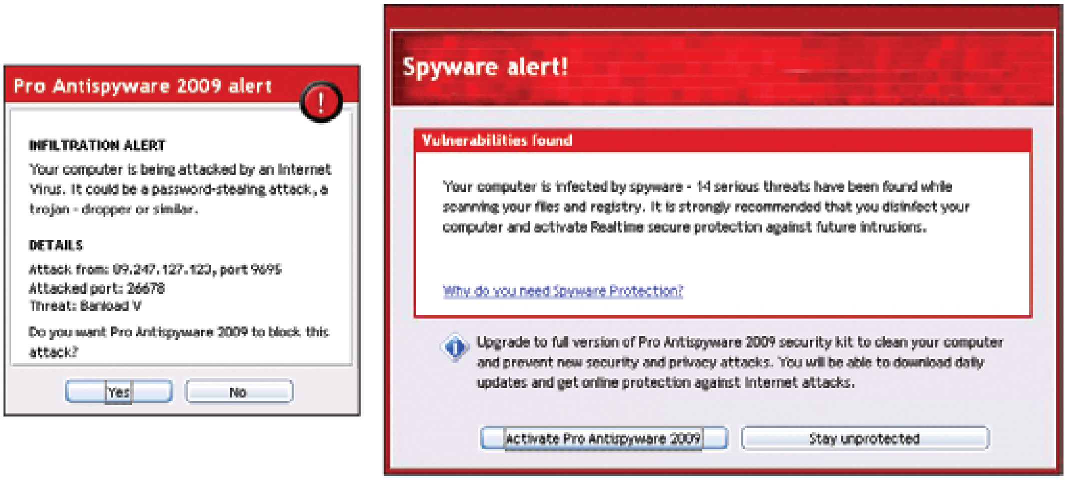
Detected malicious programs can damage your computer and compromise your privacy. It is **strongly recommended** to remove them immediately.

Name	Type	Risk level
Spyware.IEMonster.b	Spyware	CRITICAL
Zlob.PornAdvertiser.Xplsd	Spyware	High
Trojan.InfoStealer.Banker.s	Trojan	Medium

Remove All | Ignore

In other cases, rogue security software is installed by different malware or masquerades as another kind of program. Once installed, it bombards the user with pop-up advertisements and alerts claiming that the computer is infected and that the only way to remove the threats is to pay for the "full" version of the software. Some rogue security programs even display bogus "blue screen" error messages, suggesting that malware is preventing the computer from operating correctly.

FIGURE 3. Fake "alert" messages from rogue security software family Win32/WinSpywareProtect



Pro Antispyware 2009 alert

INFILTRATION ALERT

Your computer is being attacked by an Internet Virus. It could be a password-stealing attack, a trojan - dropper or similar.

DETAILS

Attack from: 09.247.127.123, port 9695
Attacked port: 26678
Threat: Banload V

Do you want Pro Antispyware 2009 to block this attack?

Spyware alert!

Vulnerabilities found

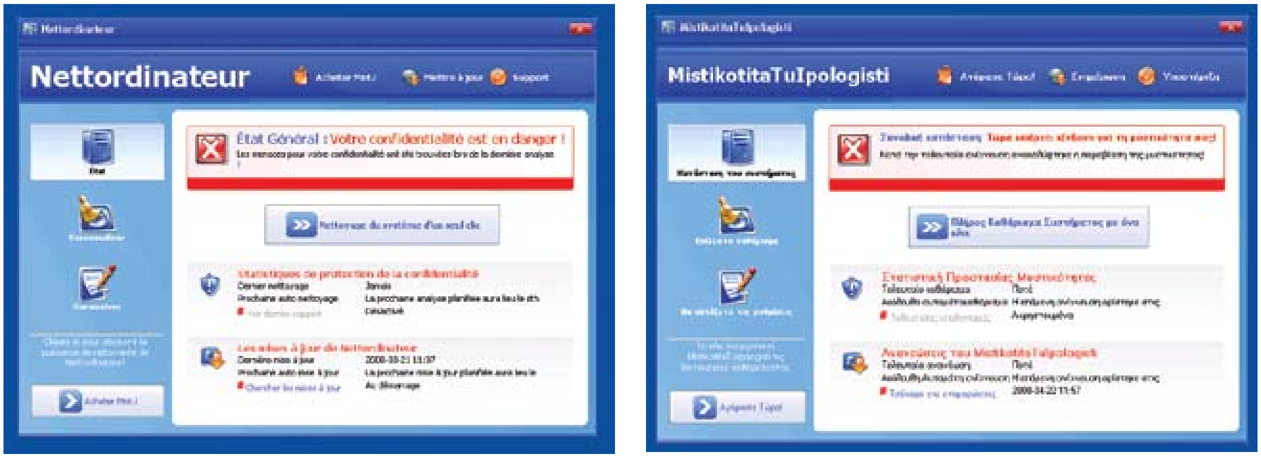
Your computer is infected by spyware - 14 serious threats have been found while scanning your files and registry. It is strongly recommended that you disinfect your computer and activate Realtime secure protection against future intrusions.

Why do you need Spyware Protection?

Upgrade to full version of Pro Antispyware 2009 security kit to clean your computer and prevent new security and privacy attacks. You will be able to download daily updates and get online protection against Internet attacks.

Rogue security software families are among the top threats detected on computers in many countries and regions throughout the world, suggesting that the appeal to users' fear is an effective tactic that transcends barriers of language. English seems to be the primary language used by rogue security software social engineering, although some families have been released in multiple language versions to target the non-English–speaking world.

FIGURE 4. French and Greek language versions of Win32/WinFixer, an older rogue security software family



Nettordinateur

État Général : Votre confidentialité est en danger !

Statistiques de protection de la confidentialité

Les mises à jour de Nettordinateur

MistikotitaTuIpologisti

For more information about these threats, see "Rogue Security Software," beginning on page 92.

Worms and Social Engineering

When self-replicating computer worms entered the public consciousness several years ago, it was in the form of threats, such as Win32/MSBlast, Win32/Sasser, and Win32/Slammer—worms that exploited vulnerabilities in the operating system and applications to spread rapidly and that garnered a lot of attention while doing so. Exploit-based worms such as these have receded from prominence as Microsoft and other software vendors have fixed the vulnerabilities these worms relied on to spread themselves. With these traditional vectors of mass propagation largely closed off to them, today's prominent worms rely much more on social engineering techniques to breach the metaphorical city walls and gain access to environments like enterprise networks that may not be prepared for such threats. A new threat, designated Worm:Win32/Conficker.B, was detected on December 29, 2008. An earlier version, Win32/Conficker.A, had been detected on November 21, 2008, as the first significant threat to exploit MS08-067, a recently revealed vulnerability in the Windows Server service. Win32/Conficker.B exploited the MS08-067 vulnerability too, but it also used a number of other methods to propagate, which made it significantly more prevalent. For more information about the Win32/Conficker family, see "MS08-067: Vulnerability in Windows Server Service," beginning on page 41.)

Win32/Conficker.B is designed to spread in a networked environment, like a workplace. It copies itself to any mapped drives (like network file shares) and removable devices (like CD-ROM drives and USB flash drives) connected to an infected computer. Enterprise users often take advantage of shares and removable devices to exchange files freely with coworkers and with professional contacts outside the organization, making this a significantly more effective means of propagation than exploiting the MS08-067 vulnerability alone. Win32/Conficker.B also attempts to spread to other computers on the network with the aid of a list of weak passwords, like *12345678* and *password1*. Users who choose weak passwords for their network shares in the belief that their computer resources are largely secure from outside threats are vulnerable to infection.

Some threats take an even more aggressive approach, copying themselves to a removable volume and modifying the autorun.inf file to automatically execute the malware as soon as the volume is inserted into an uninfected computer. Microsoft detects such malware as variants of the Win32/Autorun family. Most detections of Win32/Autorun occur in enterprise environments, where removable media, such as USB drives, are often used to exchange files between computers. The autorun tactic is often used by attackers to spread malware from one enterprise network to another. For example, a salesperson may bring a USB drive along on a visit to a customer's facility and insert it into an infected computer, thereby unknowingly picking up malware. When the salesperson returns to their own office and inserts the drive into another computer, the malware spreads to the office network. In 2H08, Win32/Autorun was the family most detected by Microsoft Forefront Client Security, an enterprise antivirus solution; 17.7 percent of the computers that reported malware in those environments reported infections of Win32/Autorun. For more informa-

Encyclopedia

Win32/MSBlast: A family of network worms that exploit a vulnerability fixed 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/Slammer: Slammer is 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/Conficker: A worm that spreads by exploiting a vulnerability in the Windows Server service. Some variants also spread via removable drives and by exploiting weak passwords. It disables several important system services and security products, and downloads arbitrary files.

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

http://www.microsoft.com/av

tion about the different kinds of threats that affect home and enterprise users, see "Focus: The Threat Landscape at Home and in the Enterprise," beginning on page 89.

Autorun malware has surfaced in some unexpected places. In multiple incidents in 2008, a small number of consumer products that were designed to be connected to a computer, such as digital picture frames and MP3 players, were inadvertently infected during the manufacturing or shipping process with autorun malware and then distributed to consumers. As soon as an infected device was connected to a computer, the malware would execute and install itself, often using a number of tactics to evade detection. Several large, reputable retailers have unwittingly sold consumers infected devices, which in some cases have come from well-known manufacturers of consumer products.

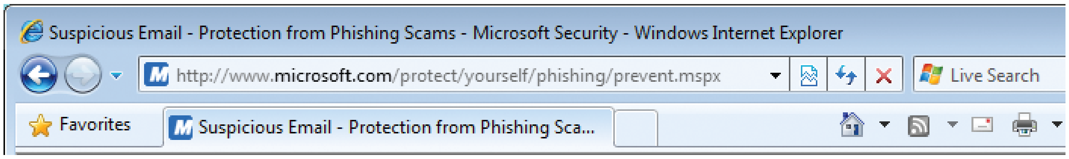
File Format Exploits

Some attack mechanisms require a combination of exploit and social engineering techniques. During the second half of 2008, Microsoft researchers observed attackers using document file format vulnerabilities as an infection technique in much greater numbers than in the past. Attackers are finding vulnerabilities in the way popular business productivity programs, such as the Microsoft Office system and Adobe Reader, parse documents, and attackers are creating specially crafted documents designed to exploit these vulnerabilities. They then use a number of different tactics to lure victims into opening the malicious documents and launching their payloads. For example, an attacker might e-mail a malicious file with a name like "Budget 2009.xls" or "Corporate Policy.PDF" to users at a targeted company. The e-mail message may look legitimate and may appear to come from someone the user knows. In some cases, attackers have gone to great lengths to target particular individuals, crafting malicious documents, such as the agenda of an upcoming conference or a widely circulated legal brief, which the targeted person would have no reason to suspect and may even expect to receive. See "Document File Format Exploits," beginning on page 51, for more information about this class of threat.

Spear Phishing and Whaling

In recent years, institutions of the sort that are often victimized by phishing have made great strides in educating users about the danger and about how to avoid being taken advantage of, and Web browsers such as Windows Internet Explorer® and Google Chrome have added features that make it easier for users to distinguish phishing attempts from legitimate pages.

FIGURE 5. Internet Explorer 8 highlights the domain name in the browser address bar as an anti-phishing measure.


Suspicious Email - Protection from Phishing Scams - Microsoft Security - Windows Internet Explorer
http://www.microsoft.com/protect/yourself/phishing/prevent.mspx
Live Search
Favorites
Suspicious Email - Protection from Phishing Sca...

As users have become more savvy about phishing, however, the phishers have responded by increasing their use of highly targeted attacks, called *spear phishing*. Spear phishers send e-mail messages that appear genuine to all the employees or members within a certain company, government agency, organization, or group. The message might look like it comes from the recipient's employer or from a colleague who might plausibly send an e-mail message to everyone in the company, such as the head of human resources or the person who manages the computer systems. Even a user who knows to be on guard for phishing attempts when receiving an e-mail message appearing to be from a bank or other popular phishing target may not suspect a spear phishing message. A related tactic, called *whaling*, involves targeted attacks on senior executives and other high-ranking people within a company or organization.

Online Banking Malware

A problem related to phishing is that of malware that targets users of online banking and financial services. These threats attempt to locate and extract login credentials from an infected computer and transmit it to a server controlled by the attacker, who then uses the credentials to transfer money out of the victims' accounts. There are two prevalent families of malware that target online banking users, called Win32/Banker and Win32/Bancos; a third family, Win32/Banload, is used as a delivery mechanism for the other two. These families primarily target customers of Brazilian banks—nearly 80 percent of the computers infected with these families in 2H08 were in Brazil—and use Portuguese-language text strings and social engineering.

The social engineering messages used by these families often exploit fear and attempt to create a sense of immediacy. Figure 6 shows one example from an e-mail message received by many users in Brazil in 2008.

Encyclopedia

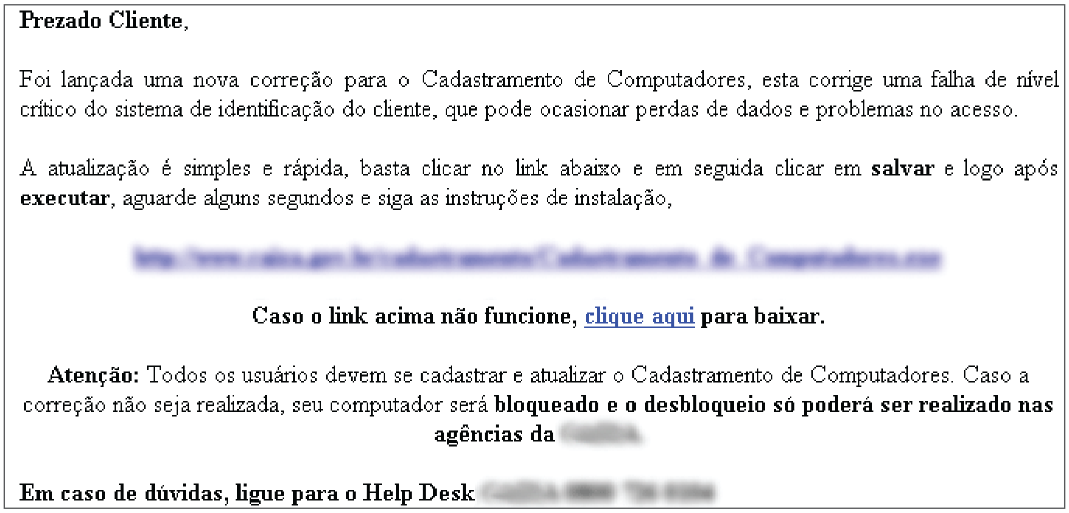
Win32/Banker: A family of data-stealing trojans that captures online banking credentials, mostly for Brazilian banks, and relays them to the attacker. Many variants of Win32/Banker may appear as greeting card software.

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

Win32/Banload: A family of trojans that downloads other malware. These downloaded malware are usually members of the Win32/Banker family.

http://www.microsoft.com/av

FIGURE 6. An example of an e-mail message that spreads Win32/Banker



Prezado Cliente,

Foi lançada uma nova correção para o Cadastramento de Computadores, esta corrige uma falha de nível crítico do sistema de identificação do cliente, que pode ocasionar perdas de dados e problemas no acesso.

A atualização é simples e rápida, basta clicar no link abaixo e em seguida clicar em **salvar** e logo após **executar**, aguarde alguns segundos e siga as instruções de instalação,

[redacted]

Caso o link acima não funcione, clique aqui para baixar.

Atenção: Todos os usuários devem se cadastrar e atualizar o Cadastramento de Computadores. Caso a correção não seja realizada, seu computador será **bloqueado e o desbloqueio só poderá ser realizado nas agências da** [redacted]

Em caso de dúvidas, ligue para o Help Desk [redacted]

In English, the text reads:

Dear customer,

A new fix for registering computers is now available. This fix corrects a critical failure of the client identification system that can cause data loss and access problems.

*The update is simple and fast, just click the link below and then click **Save** and **run** immediately after, wait a few seconds and then follow the installation instructions,*

[Link]

If the link above does not work, click here to download.

Attention:** All users must register and update their computers' registration. Failure to update the registration will cause your computer to be blocked. **Unblocking computers can only be done at one of the [institution name] agencies.

If you have questions, call [institution name]'s help desk at [telephone number]

The computers of users who click the link in the message and run the executable may get infected with the malware, and the users may have money stolen from their accounts.

Malware Targeting Online Gamers

Continuing a trend reported in *Microsoft Security Intelligence Report, Volume 5 (January through June 2008)*, 2H08 brought continued growth of a group of loosely related worms and trojans that target players of online games and attempt to steal their login credentials. The increasing popularity of massively multiplayer online role-playing games (MMORPGs) has created a new online economy in which players auction off hard-won virtual "gold" and in-game equipment for real-world cash. Though the games' makers usually discourage such commerce and often penalize players who are known to engage in it, the possessions and attributes of a well-stocked character can fetch hundreds of U.S. dollars from game devotees. Consequently, a number of threats have arisen that steal players' gaming passwords on behalf of thieves who can then auction the victim's virtual loot themselves. Win32/Taterf, the fifth most prevalent malware family worldwide in 2H08, is among these threats, as are Win32/Lolyda (eighteenth) and Win32/Tilcun (nineteenth). Overall, Microsoft security products removed malware targeting online gamers from more than 4 million computers in 2H08.

Like a number of other families described in this report, Win32/Taterf spreads by copying itself to the root of removable drives on the infected system, creating autorun.inf files wherever it spreads. In many parts of the world, gaming is often done in Internet cafés or on other public terminals, which are used by large numbers of people and which present a greater opportunity for infection than a private computer. If a user inserts a portable USB drive infected with Win32/Taterf into an unprotected public terminal, the computer is compromised and can steal passwords from anyone else who uses the computer until the infection is removed.

Threats Targeting Music and Video Consumers

Targeting people who use their computers to watch videos and listen to music is an old social engineering technique but one that remains effective for attacks that are tailored to those activities. The mechanics of these attacks differ widely, but all involve common entertainment-related computing activities. Win32/Zlob, the second most prevalent threat worldwide in 2H08, typically poses as a missing codec needed to play video files. ASX/Wimad, a detection for a category of malicious Windows Media® files, was the eleventh most prevalent threat in 2H08. Certain Windows Media files can contain hyperlinks to be automatically opened in a Web browser when they are played. ASX/Wimad files include hyperlinks to executable files, often with names like PLAY_MP3.exe that contain malicious payloads. Users may believe that they have to run these files to access desired media content.

* * * *

Attackers' increasing reliance on social engineering is in some ways a natural consequence of the elevated level of attention software vendors are giving to improving the security of their products. Although technical solutions, such as the browser address bar changes discussed earlier, can provide computer users with some assistance in recognizing and avoiding social engineering attacks, any truly effective solution must involve educating users about these techniques and teaching them how to remain safe online. Throughout this report, the "Strategies, Mitigations, and Countermeasures" subsections at the end of most major sections provide actionable guidance that security and IT professionals can use to help create a safer computing environment.

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

Win32/Tilcun: A family of trojans that steals online game passwords and sends this captured data to remote sites.

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.

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.

http://www.microsoft.com/av

Vulnerability Trends

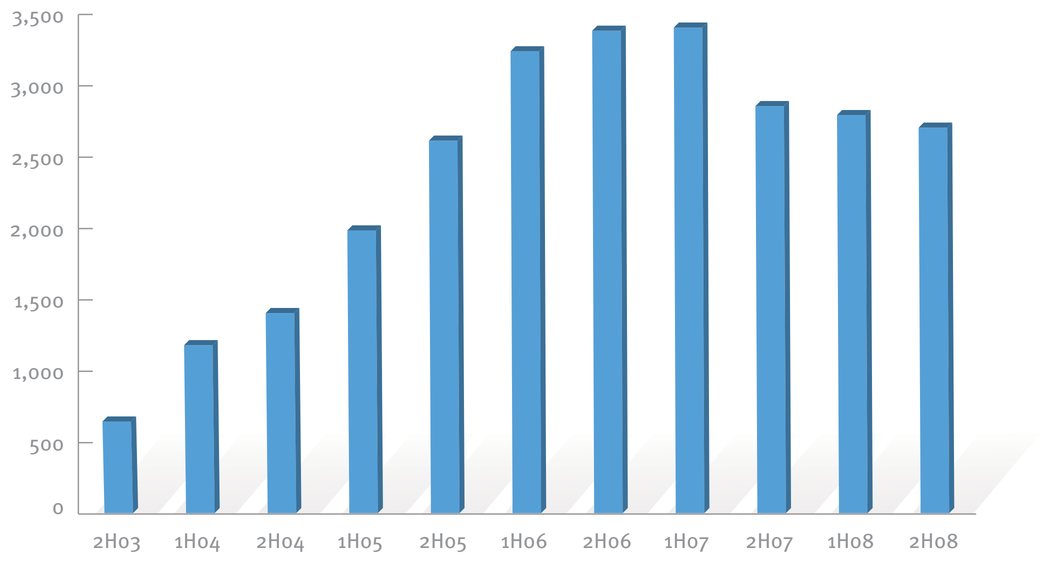
V*ulnerabilities* are weaknesses in software that allow an attacker to compromise the integrity, availability, or confidentiality of that software. Some of the worst vulnerabilities allow attackers to run arbitrary code on the compromised system.

This section of the *Microsoft Security Intelligence Report* analyzes new vulnerabilities that were disclosed during the second half of 2008 and examines trends in vulnerability disclosures since 2003. A *disclosure*, as the term is used in this report, is the revelation of the existence of a 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, but examines Microsoft-specific disclosures, as well.

Industry Vulnerability Disclosures

In 2H08, disclosed vulnerabilities across the software industry declined 3 percent from the previous half-year period, continuing a trend of small period-to-period decreases observed since 2007. This represents a 5 percent decrease from the same period the previous year. Disclosures for the full year of 2008 were down 12 percent from 2007. Figure 7 illustrates the number of vulnerability disclosures across the software industry for each half-year period since 2H03.

FIGURE 7. Industry-wide vulnerability disclosures by half-year, 2H03–2H08



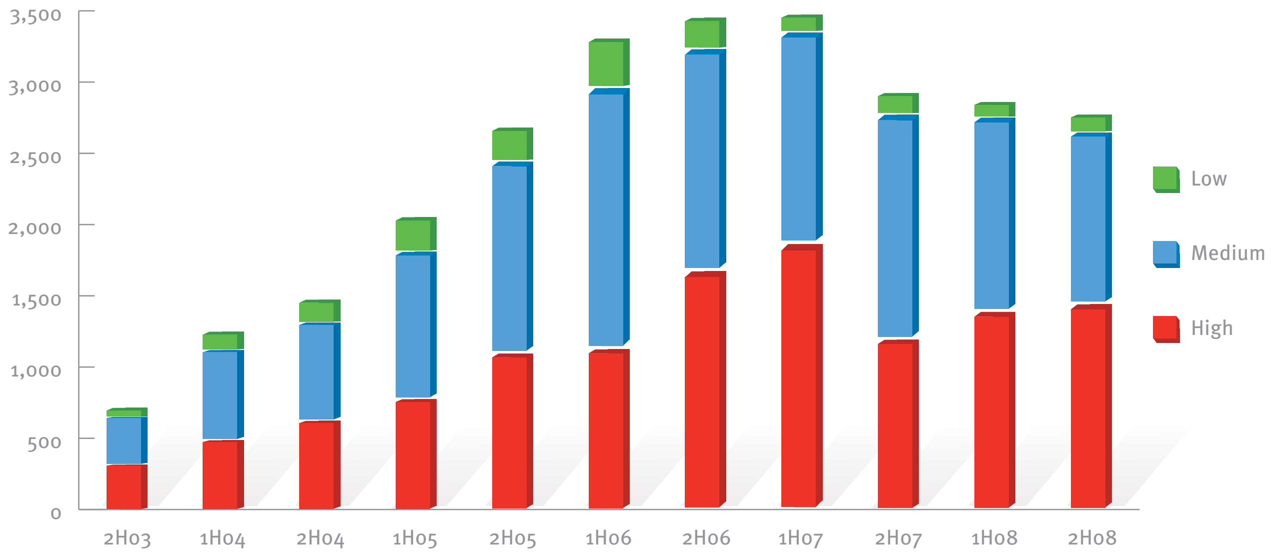
Industry Vulnerability Severity

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 new disclosures.

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.[3]

As Figure 8 illustrates, the trend for High severity vulnerabilities does not follow the same trend as the overall total and actually increased relative to 1H08 by 3.8 percent, continuing the trend observed from 2H07 to 1H08. High severity vulnerabilities accounted for 52.6 percent of all vulnerabilities disclosed in the period. Even after two consecutive periods of increase, however, the overall total number of High severity vulnerabilities disclosed in 2008 decreased 16 percent from the previous year, owing to a steep decline observed between 1H07 and 2H07.

FIGURE 8. Industry-wide vulnerability disclosures by severity, 2H03–2H08



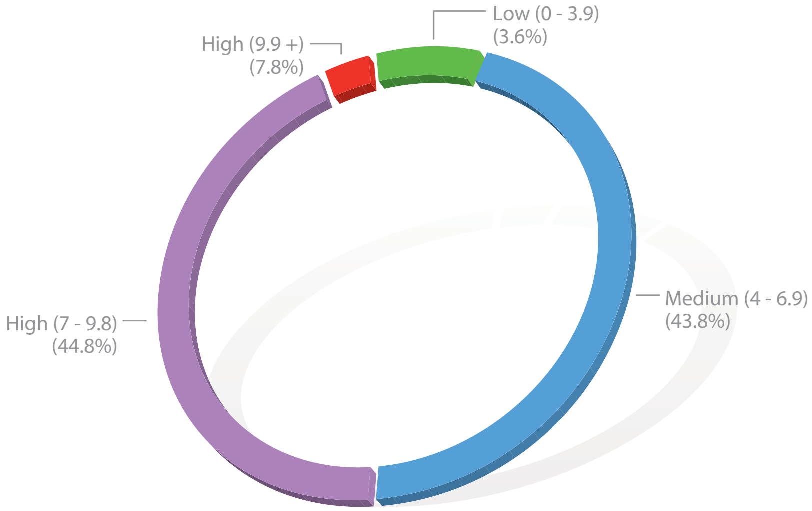
[3] For an explanation of the CVSS scoring methodology, see http://www.first.org/cvss/cvss-guide.html#i3.

Focusing on mitigating the most severe vulnerabilities first is a security best practice. While CVSS, through the National Vulnerability Database (NVD), provides a base score across the set of industry vulnerabilities, security professionals should look first to their software vendors for further security information, since 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 more than half of the vulnerabilities disclosed in 2H08 rated as High severity, administrators need more information to effectively set priorities for responding to vulnerabilities.

Along these lines, the chart in Figure 9 illustrates the severity breakdown for 2H08. 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 roughly 8 percent of all vulnerabilities disclosed.

FIGURE 9. Industry-wide vulnerability disclosures by severity, 2H08



Industry Vulnerability Complexity

CVSS version 2.0 uses three complexity designations: Low, Medium, and High. Figure 10 gives definitions for these designations.[4]

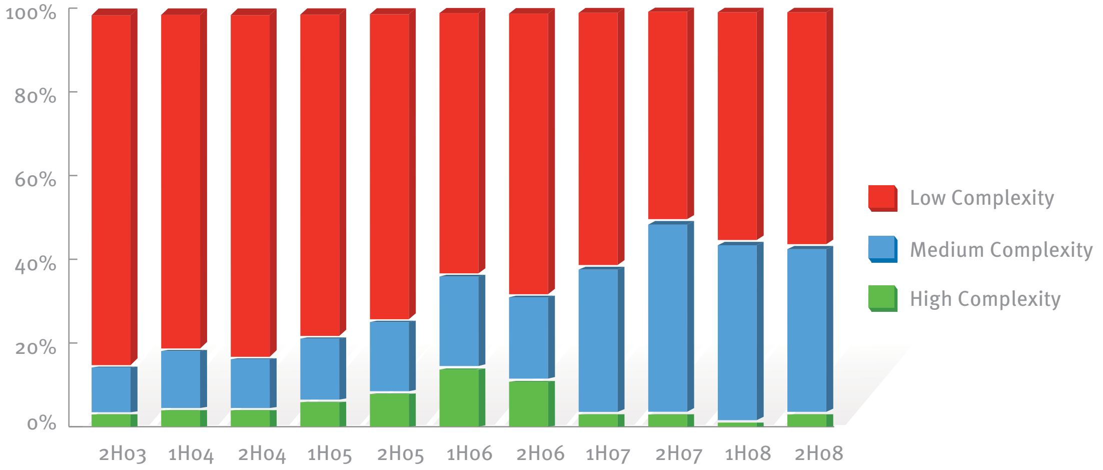
FIGURE 10. NVD complexity rankings and definitions

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

Figure 11 shows the vulnerability disclosure complexities for each half-year period since 2H03. The complexity mix has remained roughly constant in relative terms since 1H08, with the percentage of High complexity vulnerabilities—those that are generally the most difficult to exploit—increasing slightly but remaining very small. As in previous periods, most vulnerabilities disclosed in 2H08 were designated Low complexity, indicating that attackers may have an easy time developing reliable exploits for these vulnerabilities.

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

FIGURE 11. Industry-wide vulnerability disclosures by access complexity, 2H03–2H08



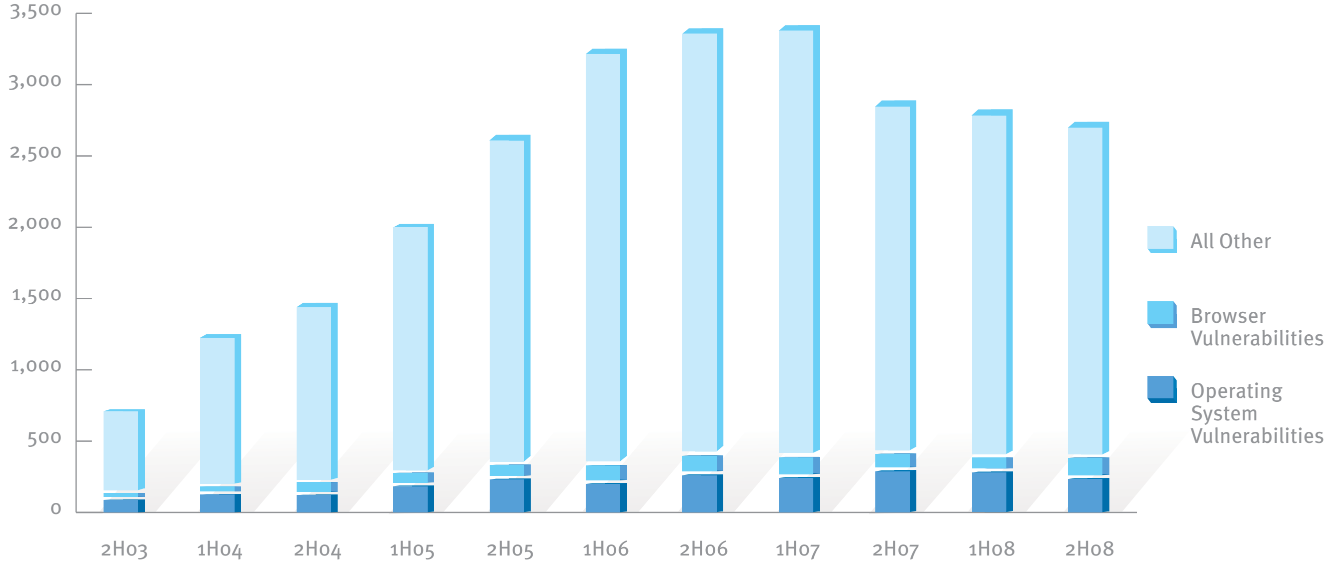
Operating System and Browser Vulnerabilities

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 core operating system vulnerabilities, Microsoft researchers devised a model by which all disclosed vulnerabilities affecting core components of Microsoft Windows, Apple Mac OS X, proprietary Unix systems, or the Linux kernel were classified as operating system vulnerabilities, with everything else classified as application vulnerabilities. Using this model, programs like media players are considered application vulnerabilities, as are Linux components like the X Window System, the GNOME desktop environment, and others.

Figure 12 shows vulnerabilities for operating systems, browsers, and other components since 2H03, as determined by this simple model.

FIGURE 12. Industry-wide operating system, browser, and other vulnerabilities, 2H03–2H08

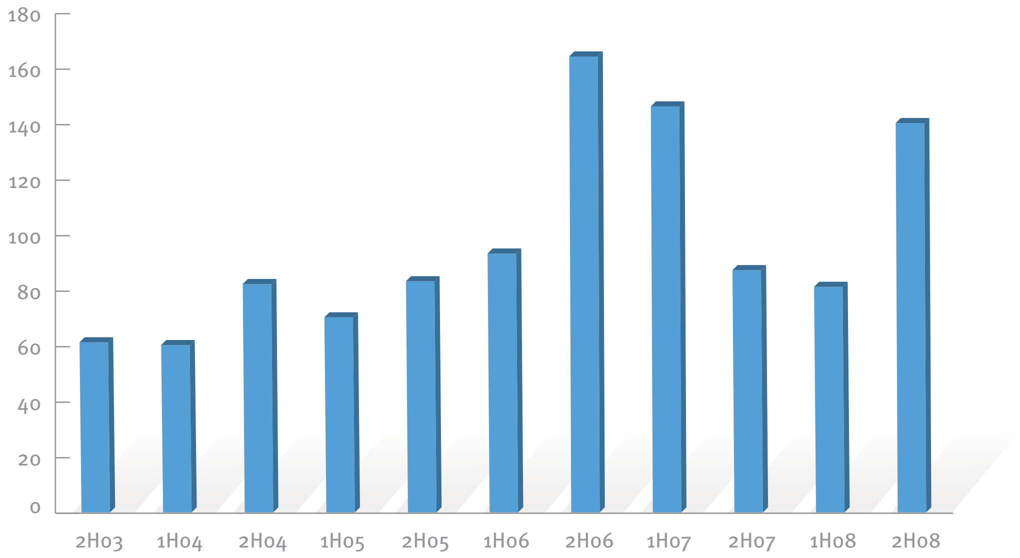


Operating system vulnerabilities accounted for 8.8 percent of all vulnerabilities disclosed in 2H08, down from 10.1 percent in 1H08, while browser vulnerabilities increased to 4.5 percent of the total, up from 2.8 percent.

Microsoft Vulnerability Disclosures

Figure 13 charts vulnerability disclosures for Microsoft products since 2H03. In general, trends for Microsoft vulnerability disclosures have mirrored those for the industry as a whole, though on a much smaller scale.

FIGURE 13. Vulnerability disclosures for Microsoft products, 2H03–2H08



Vulnerability disclosures for Microsoft products increased to 143 unique vulnerabilities (5.2 percent of the total) in 2H08, up from 84 (3.0 percent of the total) in 1H08. This represents a departure from the trend of fewer disclosures seen in the last two periods although, in absolute terms, the total falls short of the recent high marks observed in 2H06 and 1H07. Vulnerability disclosures depend on a number of internal and external factors and rarely happen evenly throughout the course of a year, so it remains to be seen whether this increase is an anomaly or the start of a trend. For the full year of 2008, Microsoft vulnerability disclosures are down 5.0 percent, continuing a trend of year-over-year declines since 2006.

FIGURE 14. Vulnerability disclosures for Microsoft products, by year, 2003–2008

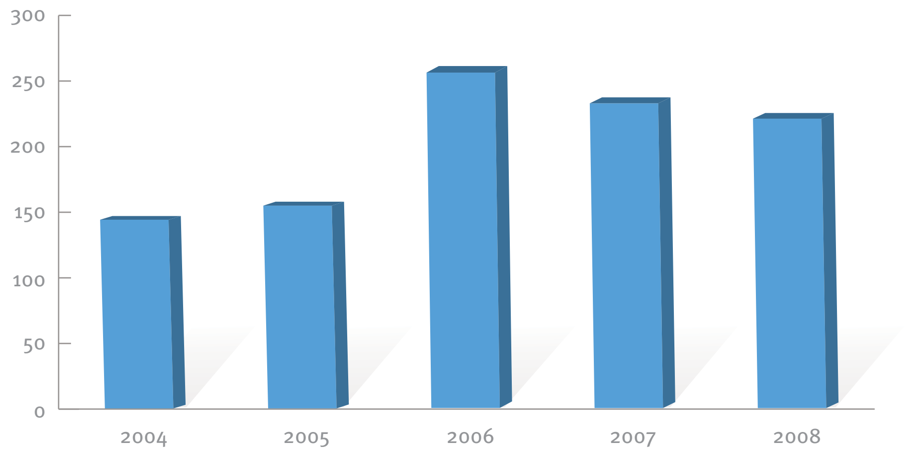
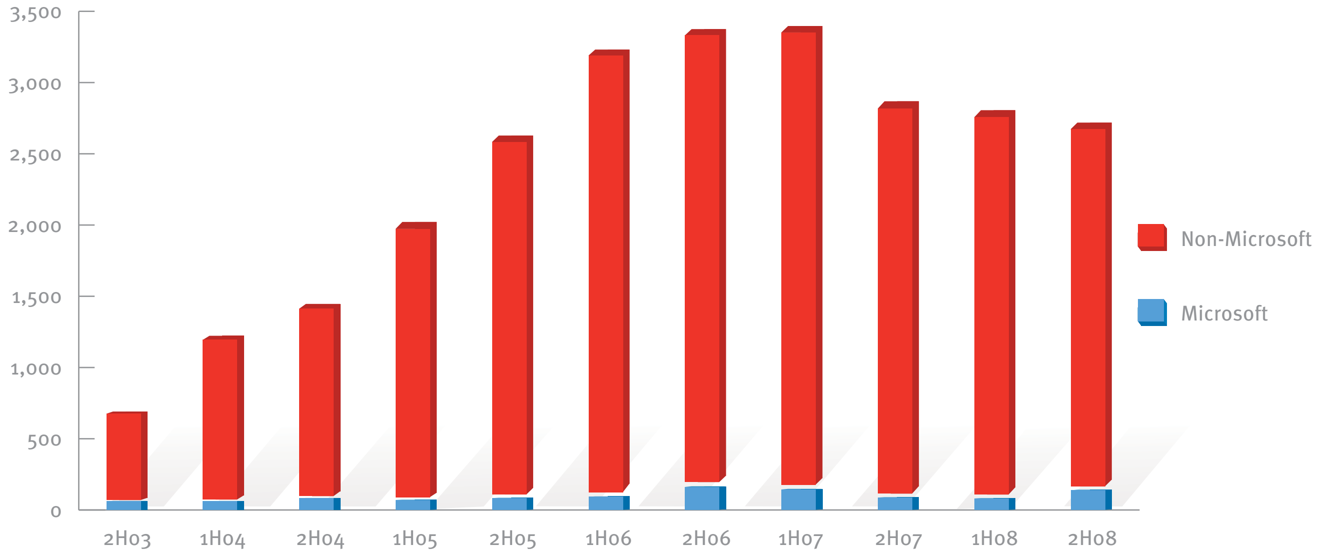


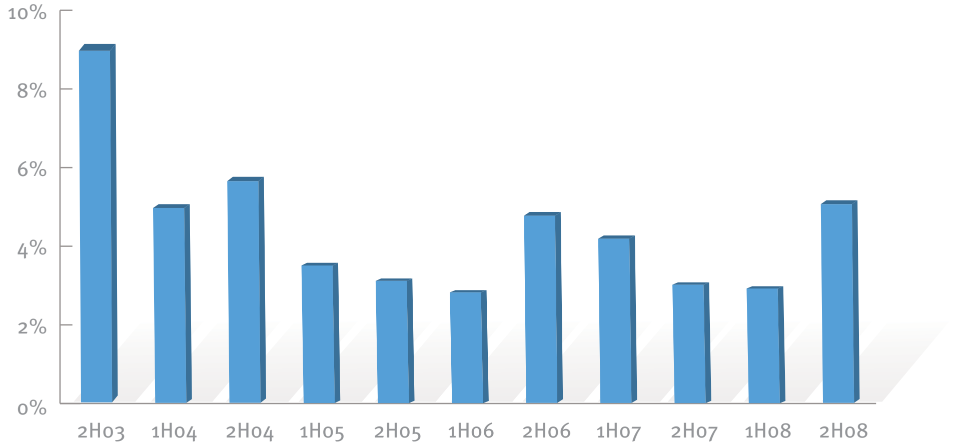
Figure 15 provides some perspective for these figures by illustrating the relative share of vulnerability disclosures for Microsoft and non-Microsoft software since 2H03, showing that Microsoft vulnerabilities continue to account for a relatively small percentage of the overall total.

FIGURE 15. Vulnerability disclosures for Microsoft and non-Microsoft products, 2H03–2H08



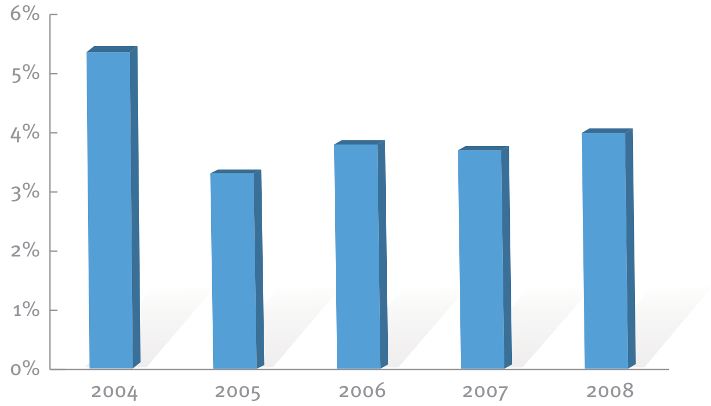
The size and scale of Figure 15 make it difficult to identify trends, so Figure 16 shows Microsoft disclosures as a percentage of total disclosures over the same period.

FIGURE 16. Microsoft vulnerability disclosures as a percentage of all industry disclosures, 2H03–2H08



The percentage of disclosed vulnerabilities attributed to Microsoft products in 2H08 was up from previous periods, although it remains consistent with the recent trend of Microsoft vulnerabilities fluctuating between 3 and 5 percent of industry-wide vulnerabilities. On a year-to-year basis, as shown in Figure 17, Microsoft vulnerabilities accounted for 4.1 percent of industry-wide vulnerabilities in 2008, up slightly from 2007.

FIGURE 17. Microsoft vulnerability disclosures as a percentage of all industry disclosures, by year, 2004–2008

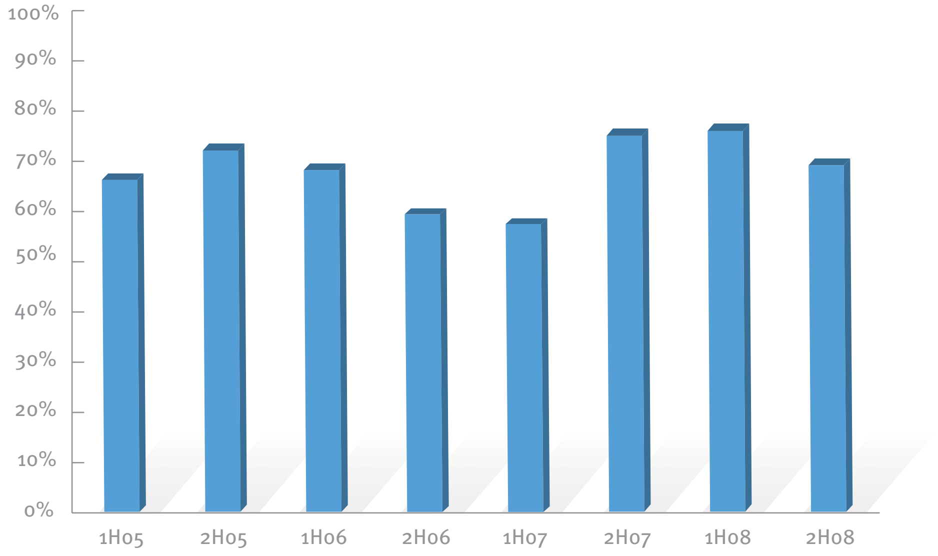


Responsible Disclosures

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

FIGURE 18. Responsible vulnerability disclosures as a percentage of all disclosures involving Microsoft software, 1H05–2H08



In 2H08, 70.6 percent of Microsoft vulnerability disclosures adhered to responsible disclosure practices, down from 78.2 percent in 1H08, although the responsible disclosure percentage for the whole of 2008 was higher than that of the previous year. The last three periods have each had responsible disclosure rates above 70 percent—an encouraging sign following significantly lower rates in previous periods. One development that may have contributed to this overall rise was the lack of any "Month of…" events (like "A Month of Browser Vulnerabilities") in 2008. These events, in which an independent researcher publicly discloses a new alleged vulnerability each day for a month, have happened sporadically since 2006, and the public disclosure of large numbers of vulnerabilities drives down the responsible disclosure rate in the periods in which such events occur.

Engaging with the security community directly, and proactively addressing security issues, results in the majority of issues being responsibly reported. See "Strategies, Mitigations, and Countermeasures," on page 38, for details about some of the programs and initiatives Microsoft has established for working with the community.

The Vulnerability Broker Economy and Microsoft Security Cases

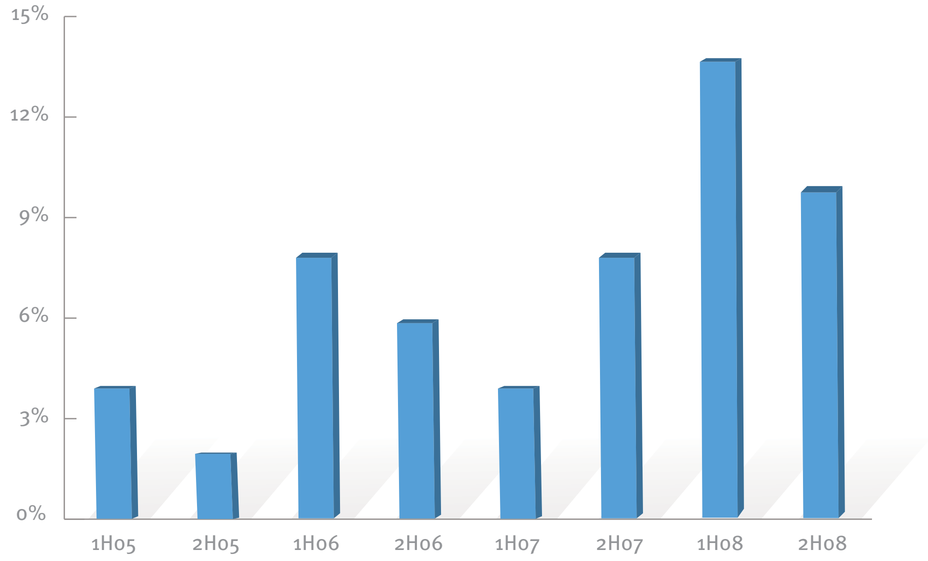
The MSRC receives reports about possible vulnerabilities in Microsoft software through a number of different channels and investigates each report it receives to determine whether vulnerabilities exist and, if so, how to respond to them.[5] The last several periods have seen a significant increase in the percentage of cases brought to the MSRC by vulnerability brokers iDefense and ZDI. A *vulnerability broker* is a company or other entity that provides software

[5] For more information about how the MSRC manages and responds to vulnerability reports, see http://www.microsoft.com/security/msrc/managing_vulnerabilities.mspx.

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.

Figure 19 shows the percentage of cases handled by the MSRC that were submitted by vulnerability brokers for every half-year period since 1H05. (Not all cases are determined to be actual vulnerabilities.)

FIGURE 19. Percentage of cases handled by the MSRC that were submitted by vulnerability brokers, 1H05–2H08



In 2H08, 9.9 percent of cases handled by the MSRC were submitted by vulnerability brokers. Although down from a high of 14.1 percent in 1H08, this percentage is higher than in any half-year period before 2008 and, in fact, the percentage for the whole of 2008 is almost double that of 2007. In general, the percentage of cases submitted by vulnerability brokers has increased significantly since 2005, indicating that vulnerability brokers are having increasing success doing business with external security researchers.

Microsoft classifies vulnerability broker disclosures as responsible disclosures, and figures for these disclosures contribute to the aggregate totals presented in “Responsible Disclosures,” beginning on page 34. 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.

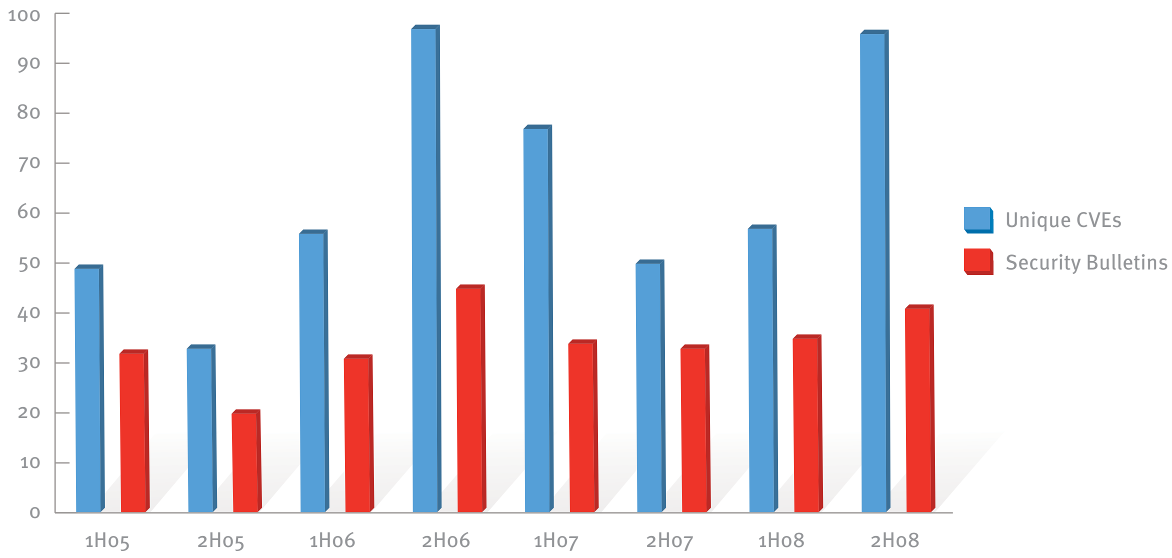
Vulnerabilities Addressed by Microsoft in 2H08

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, "MS08-012" refers to the twelfth security bulletin released in 2008. 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. For information about the two out-of-band security bulletins released in 2H08, see "Out-of-Band Microsoft Security Updates in 2H08" on page 40.

A single security bulletin often addresses multiple vulnerabilities from the CVE database,[6] each of which is listed in the bulletin along with any other relevant issues. 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.

Figure 20 shows the number of security bulletins released and the number of individual CVE-identified vulnerabilities the MSRC has addressed for each half-year period since 1H05. (Note that not all vulnerabilities are addressed in the period in which they are initially disclosed.)

FIGURE 20. Security bulletins released and CVEs addressed by half-year, 1H05–2H08



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

In 2H08 the MSRC released 42 security bulletins, which addressed 97 individual CVE-identified vulnerabilities, a 67.2 percent increase over the number of vulnerabilities addressed in 1H08. For the full year of 2008, the MSRC released 78 security bulletins addressing 155 vulnerabilities, equal to the number addressed in 2006 and a 16.8 percent increase over the number addressed in 2007.

As Figure 20 shows, although the total number of security bulletins in 2H08 was on par with the last several periods, there was a significant increase in the number of CVE identifiers addressed per security bulletin in 2H08, increasing from an average of 1.6 CVE identifiers per security bulletin in 1H08 to 2.3 in 2H08. This can largely be attributed to the releases of MS08-052, MS08-058, MS08-070, MS08-072, and MS08-073, respectively, which as a group addressed 5.8 CVE-identified vulnerabilities each, on average.

Vulnerability Trends Summary and Conclusion

The total number of unique vulnerability disclosures across the industry decreased in the second half of 2008, down 3.1 percent from the first half of 1H08. For the full year of 2008, vulnerability disclosures were down 12 percent from 2007.

In contrast to the decrease in total disclosures, vulnerabilities rated as High severity increased 3.8 percent from 1H08, with 52.6 percent of all vulnerabilities receiving a rating of High severity during the period. The overall total number of High severity vulnerabilities disclosed in 2008 decreased 16 percent from 2007, however. Compounding the seriousness of the High severity vulnerabilities, the percentage of exploits designated Low complexity—those that are easiest to exploit—remained high, accounting for more than half of all exploits.

Strategies, Mitigations, and Countermeasures

- Both security vendors and IT professionals should adjust their risk management processes appropriately to help ensure that all operating systems and applications are protected.
- A Security Risk Management Guide for IT professionals is available at http://www.microsoft.com/technet/security/guidance/complianceandpolicies/secrisk/default.mspx.
- The Solution Accelerators—Security and Compliance team at Microsoft offers free prescriptive guides for IT professionals, in addition to security guidance organized by topic, product, and technology. Learn more at http://www.microsoft.com/technet/security/guidance/default.mspx.

- Organizations should participate in IT security communities to keep abreast of the wide range of potential security issues they may face. The Microsoft Security TechCenter, at http://technet.microsoft.com/security, is a good place to start, and it provides access to various security-related resources.
- Security software vendors should understand the Microsoft Security Response Center Exploitability Index (http://technet.microsoft.com/en-us/library/dd145265.aspx), which 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, and participate in the Microsoft Active Protections Program (MAPP) (http://www.microsoft.com/security/msrc/mapp/overview.mspx), which provides partners with early access to vulnerability information so they can provide updated protections to customers through their security software or devices.
- Read the Microsoft Security Research & Defense blog at http://blogs.technet.com/srd for in-depth information about vulnerabilities, mitigations, and workarounds.
- Subscribe to the Microsoft Security Newsletter. The newsletter offers security tips, information, security bulletins and updates, community news, pointers to security guides, resources, and best practices. You can subscribe at http://www.microsoft.com/technet/security/secnews/default.mspx.

Call to Action—End to End Trust[7]

Building trusted software is an important part of the trusted stack required to facilitate true End to End Trust. To help protect users from vulnerabilities:

- Developers can rewrite code in safer languages, check the code with analytic tools, compile with compilers that reduce vulnerabilities (for example, buffer overruns), and sandbox code when it's executed.
- Developers should leverage code-signing so that source can be better identified and permits users to consider prior experiences, reputation, and other factors in deciding whether to install software.
- To protect against malicious code, there are firewalls, antivirus programs, and antispyware programs available from trusted sources. IT professionals and consumers should take advantage of these defense-in-depth technologies.

To learn more about the End to End Trust vision, please visit www.microsoft.com/endtoendtrust.

[7] Derived/excerpts from: Scott Charney, "Establishing End to End Trust." (http://download.microsoft.com/download/7/2/3/723a663c-652a-47ef-a2f5-91842417cab6/Establishing_End_to_End_Trust.pdf)

Out-of-Band Microsoft Security Updates in 2H08

Prior to 2003, Microsoft did not have a formal schedule for releasing security updates. Updates could be released on any day of the work week, including Fridays, and were usually released without much forewarning. That year, Microsoft began releasing new updates in groups on the second calendar Tuesday of every month.[8] This change was implemented to make testing and deploying the updates both easier and more predictable, allowing customers to build processes for faster deployment. However, in some critical situations when customers are believed to be at serious risk and a quality update can be developed and deployed quickly, Microsoft releases a so-called *out-of-band* security update to fix the vulnerability without waiting for the next regularly scheduled release date.

As Figure 21 shows, out-of-band security updates have been rare since the regular update schedule was introduced in late 2003.

FIGURE 21. Out-of-band updates released by Microsoft since 2003

Year	Total Updates	Out-of-band Updates
2004	45	3
2005	55	0
2006	78	2
2007	69	1
2008	78	2

On average, a vulnerability disclosure warranting an out-of-band release happens about every seven months, but the variance has been large—the longest gap between out-of-band releases so far has been 400 days (between MS04-040 and MS06-001, encompassing all of 2005), while the shortest was only 55 days (between MS08-067 and MS08-078). In all cases, exploits were known to exist in the wild (on active computers detected to the Internet) at the time of the bulletin's release, and in all cases except one, the vulnerability allowed remote code execution. In each case, Microsoft believes that subsequent events have validated the decision to publish an update out of band and recommends that IT departments pay close attention to any new out-of-band updates and deploy them with as little delay as possible.

[8] For more information about this change, see http://www.microsoft.com/technet/security/bulletin/revsbwp.mspx.

FIGURE 22. Details of out-of-band releases since 2003

Date	Title	CVE	Impact	Exploit at time of release
2004-02-02	MS04-004 - IE (URL Address Bar Spoof)	CAN-2003-1025	Spoofing	Yes - Malicious and Compromised Sites
2004-07-30	MS04-025 - IE (BMP)	CAN-2004-0566	Remote Code Execution, Automated attack risk	Yes - Banner Ads
2004-12-01	MS04-040 - IE (IFRAME)	CAN-2004-1050	Remote Code Execution	Yes - Banner Ads
2006-01-05	MS06-001 - Windows (WMF)	CVE-2005-4560	Remote Code Execution, Automated attack risk	Yes - Banner Ads
2006-09-26	MS06-055 - Windows (VML)	CVE-2006-4868	Remote Code Execution, Automated attack risk	Yes - Banner Ads
2007-04-03	MS07-017 - GDI (Animated Cursor)	CVE-2007-0038	Remote Code Execution, Automated attack risk	Yes - Malicious and Compromised Sites
2008-10-23	MS08-067 - Server Service	CVE-2008-4250	Remote Code Execution, Automated attack risk	Yes - Targeted, Gimmiv.A
2008-12-17	MS08-078 - IE (PTR)	CVE-2008-4844	Remote Code Execution	Yes - Malicious and Compromised Sites

As noted in Figure 22, Microsoft released two out-of-band updates in 2H08, addressing vulnerabilities documented in Microsoft Security Bulletin MS08-067 and Microsoft Security Bulletin MS08-078. These updates and the reasons for releasing them out of band are documented here.

MS08-067: Vulnerability in Windows Server Service

On October 23, 2008, Microsoft released critical security update MS08-067, addressing CVE-2008-4250, a vulnerability in the Windows Server service. The vulnerability, which affects most currently supported versions of Windows, could allow remote code execution if an affected system received a specially crafted Remote Procedure Call (RPC) request. On Microsoft Windows 2000, Windows XP, and Windows Server 2003 systems, an unauthenticated user could exploit this vulnerability and run arbitrary code. The vulnerability can only be exploited if Windows Firewall is disabled on the targeted computer, or if Windows Firewall is enabled and file and printer sharing (which uses the RPC ports) is also enabled. On Windows Vista and Windows Server 2008, the exploit requires authentication to succeed, unless password-protected sharing is disabled.[9]

[9] For more information about MS08-67, see http://blogs.technet.com/swi/archive/2008/10/23/More-detail-about-MS08-067.aspx.

Microsoft chose to release this security update out-of-band for two reasons:

- The vulnerability was considered *wormable*, meaning that in certain contexts it allows the attacker to run code on a remote computer by exploiting the vulnerability and without being authenticated. An attack would simply involve sending a malicious and well-crafted RPC packet to the victim's computer.
- There were actual exploits and attacks known at the time of the bulletin release. Though limited and targeted, the existence of the exploits meant that there were malicious people who already had knowledge of the vulnerability and knew how to successfully exploit it.

In practice, most enterprise computing environments are protected by enterprise firewalls and do not allow inbound RPC connections directly into the organization. In addition, many home networks have routers with built-in firewalls that also block inbound RPC connections. In most cases, therefore, a prospective attacker would need to find a way to install malware (probably a trojan downloader or dropper) on a single computer in a household or organization, through social engineering or by exploiting another vulnerability, and use it to introduce the worm, which would then attempt to spread to other computers on the network. An attacker might use a combination of social engineering and exploit to deliver malware into an organization: for example, by e-mailing infected files with official-sounding names to people at a company. Once opened, such malicious files might drop or download an exploit for the MS08-067 vulnerability, which would then start propagating on the network. See "File Format Exploits," on page 22, for more information about this kind of attack.

The most effective way to detect exploits of MS08-067 is by usage of intrusion detection system/intrusion prevention system (IDS/IPS) products, which monitor the network traffic in an organization. MS08-067 attacks propagate using network protocols and don't necessarily involve copying files to victims' computers, so antivirus products that focus on file-scanning may not detect such attacks. The day MS08-067 was published, Microsoft also released a generic detection (designated Exploit:Win32/MS08067.gen!A) for files exploiting MS08-067, which has helped uncover several other attacks.[10]

The first MS08-067–related attacks were targeted and isolated. Microsoft received reports from several countries or regions, mostly in Southeast Asia, of an exploit that drops a trojan and collects information from the victim's computer and sends it to a server in Japan. Designated Win32/Gimmiv, the trojan was added to the Malicious Software Removal Tool (MSRT) in November 2008 and has only been detected on a very small number of computers around the world. On the day the security update was released, another threat that exploits MS08-067 was discovered. Designated TrojanSpy:Win32/Arpoc.A, this trojan drops the Win32/Gimmiv malware; like that threat, TrojanSpy:Win32/Arpoc.A has

Encyclopedia

Exploit:Win32/MS08067.gen!A: A generic detection for code that attempts to exploit a vulnerability in SVCHOST.EXE. If the vulnerability is successfully exploited, it could allow remote code execution when file sharing is enabled.

Win32/Gimmiv: A trojan that gathers system information from the host computer on which it is installed. The trojan may delete itself after performing its data-gathering routine.

TrojanSpy:Win32/Arpoc.A: A trojan that installs TrojanSpy:Win32/Gimmiv.A on vulnerable computers across a local network. The targeted vulnerability is fixed by security bulletin MS08-067.

http://www.microsoft.com/av

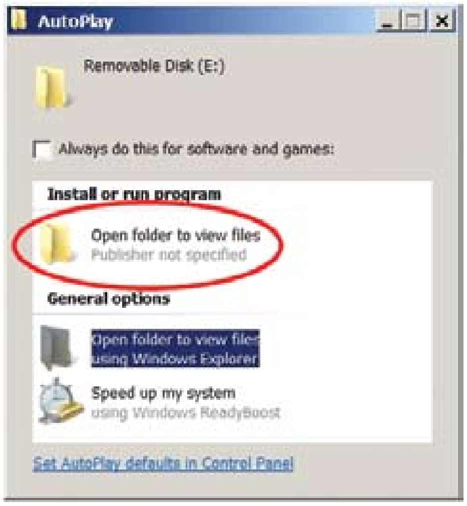
[10] Microsoft also provided participating security software providers with early information about the vulnerability through the MAPP program, to help them develop detections of their own. See page 39 for more information about MAPP.

been detected on very few computers. In the month following the security updates, more exploits of MS08-067 were detected, and most of them had very low prevalence.

On November 21, 2008, the first significant worm that exploits MS08-067 was discovered and designated Win32/Conficker. The first variant discovered, Worm:Win32/Conficker.A, only uses MS08-067 exploits to propagate. The security update that fixed the MS08-67 vulnerability had been released nearly a month prior, so home and enterprise users that installed the security update in a timely manner on all their computers were not at risk of infection. Unfortunately, Microsoft did receive reports of infections from organizations that had not applied the security update on some or all of their computers.

A significantly more dangerous variant, Win32/Conficker.B, was discovered on December 29, 2008. This variant also exploits the MS08-067 vulnerability but uses additional methods to propagate. It attempts to spread itself to other computers on the network, first as the logged-in user on the infected computer, and if that fails, using a list of weak passwords to try to access the ADMIN$ share on the targeted computer. Win32/Conficker.B also 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 23. Win32/Conficker.B creates a fake AutoPlay option (circled) on removable disks; an unprotected user who chooses the wrong "Open folder to view files" option may become infected.



AutoPlay

Removable Disk (E:)

□ Always do this for software and games:

Install or run program

Open folder to view files
Publisher not specified

General options

Open folder to view files
using Windows Explorer

Speed up my system
using Windows ReadyBoost

Set AutoPlay defaults in Control Panel

This dialog box displays two **Open Folder to view files** options. The second one is the native option from Windows, which opens a Windows Explorer window containing the contents of the volume. The option above it, which is circled in the figure and displays the line "Publisher not specified," was previously added by Worm:Win32/Conficker.B when the removable volume was used on an infected computer. A user who inserts the volume into an uninfected computer and selects the top option by mistake may activate the worm and infect the computer.

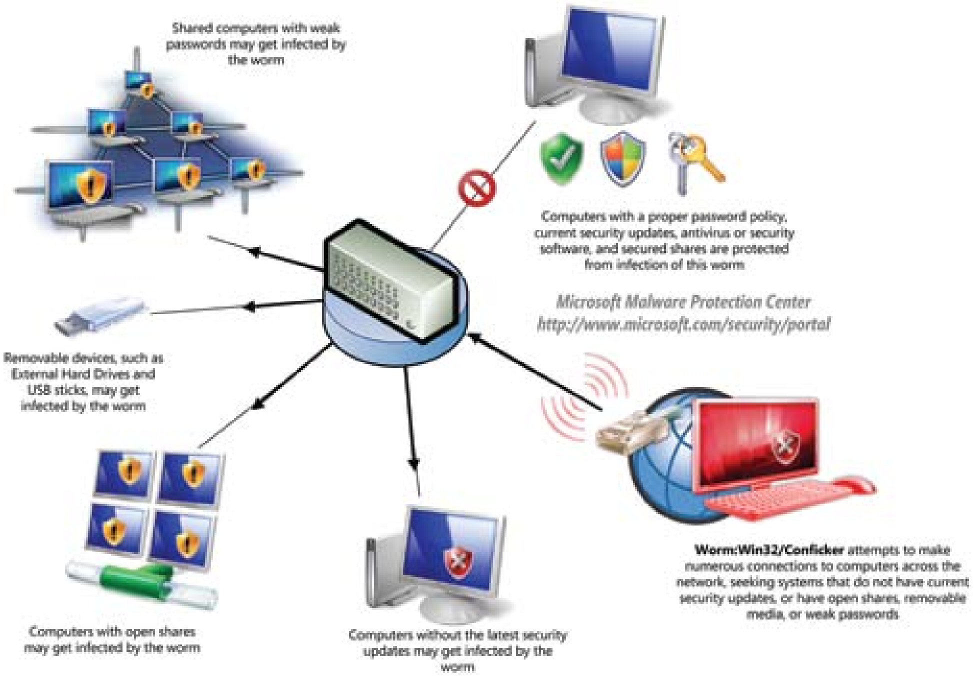
Encyclopedia

Win32/Conficker: A worm that spreads by exploiting a vulnerability in the Windows Server service. 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

Win32/Conficker displays strong self-preservation behavior. After it is installed, it patches the MS08-067 vulnerability in the memory of the infected computer—not in an effort to protect the computer, but to prevent other malware from exploiting the same vulnerability and interfering with it. Every time the computer is restarted, in fact, Win32/Conficker loads and patches the vulnerability in memory again.

FIGURE 24. Win32/Conficker.B uses numerous methods to propagate itself.


Shared computers with weak passwords may get infected by the worm
Computers with a proper password policy, current security updates, antivirus or security software, and secured shares are protected from infection of this worm
Microsoft Malware Protection Center
http://www.microsoft.com/security/portal
Removable devices, such as External Hard Drives and USB sticks, may get infected by the worm
Worm:Win32/Conficker attempts to make numerous connections to computers across the network, seeking systems that do not have current security updates, or have open shares, removable media, or weak passwords
Computers with open shares may get infected by the worm
Computers without the latest security updates may get infected by the worm

Microsoft has published a Knowledge Base article, KB962007, which provides information about how to remove Win32/Conficker. In addition, Microsoft Malware Protection Center researchers have written extensively about Win32/Conficker and MS08-067 at the MMPC blog (http://blogs.technet.com/mmpc). For more information, see the following blog entries:

- Get Protected, Now! (October 23, 2008)
- A Quick Update About MS08-067 Exploits (November 17, 2008)
- Just in Time for New Year's… (December 31, 2008)
- MSRT Released Today Addressing Conficker and Banload (January 13, 2009)
- Centralized Information About the Conficker Worm (January 22, 2009)
- Information about Worm:Win32/Conficker.D (March 27, 2009)

MS08-078: Vulnerability in Internet Explorer

On December 10, 2008, Microsoft released Security Advisory 961051, regarding a newly discovered vulnerability in Microsoft Internet Explorer. A week later, on December 17, MS08-078 (CVE-2008-4844) was released as an out-of-band security update addressing the vulnerability. Microsoft chose to release this update out of band because there were known attacks in the wild affecting increasing numbers of users.

The vulnerability lies in Internet Explorer data-binding code and is exposed when the browser parses a certain combination of XML tags and values. To exploit MS08-078, an attacker creates a Web page (or maliciously modifies the code of a hijacked page, in some cases using SQL injection) that includes the exploit code. See Figure 83, on page 126, for one example of how so-called *drive-by downloads* work. The exploit has been found on a number of pornographic Web sites and is sometimes packaged with exploit code that targets other vulnerabilities. Initially, all of the Web pages hosting the exploit were located in China, though pages hosted in other countries and regions have since been discovered. Users who have been affected by the exploit are located all over the world, including many in the United States.

A user with an unpatched version of Internet Explorer need only navigate to a malicious page to be infected. Typically, the payload is a dropper that installs other malware to the victim's computer; most of the early attacks dropped password stealers, keyloggers, and some trojans. To provide users with additional protection, Microsoft released several new detection signatures in the JS/Mult family to detect HTML pages hosting exploits of MS08-078.

The number of affected users was the highest on December 19, 2008, two days after MS08-078 was released, and declined gradually afterward, as the number of computers with the security update installed increased. The motivation of attackers to use this exploit is also expected to decrease as the security update is installed on more computers. By the end of 2008, Microsoft researchers estimate that roughly 0.2 percent of Internet users had been infected by MS08-078 exploits at least once, and more than 800 different Web pages were known to have hosted exploits.

Microsoft Malware Protection Center researchers have written about MS08-078 at the MMPC blog (http://blogs.technet.com/mmpc). For more information, see the following blog entries:

- Limited Exploitation of Microsoft Security Advisory 961051 (December 11, 2008)
- The New IE Exploits for Advisory 961051, Now Hosted on Pornography Sites (December 13, 2008)

Encyclopedia

JS/Mult: A collection of detection signatures for malicious code on Web pages that attempts to exploit certain vulnerabilities in order to download and run arbitrary files.

http://www.microsoft.com/av

Strategy, Mitigations, and Countermeasures

- Always run up-to-date software. Enable Automatic Updates in Windows, which will help ensure that the latest security updates from Microsoft are downloaded automatically. Periodically check the Web sites of third-party add-on vendors to help ensure that you have the latest security updates for their software.
- Uninstall software, including ActiveX® controls, you don't actively use. Malicious code can exploit vulnerabilities in software, whether you use it or not.
- Use up-to-date antivirus software from a known, trusted source that offers real-time protection and continually updated definition files to detect and block exploits.
- Set Internet and local intranet security zone settings in Internet Explorer to High, which will cause Internet Explorer to prompt the user before running scripts and ActiveX controls in these zones.
    - To minimize disruption, you can add sites you trust to the Trusted Sites zone to avoid the prompts. In particular, consider adding *.windowsupdate.microsoft.com and *.update.microsoft.com to the Trusted Sites zone to facilitate keeping your computer up to date.
    - By default, Internet Explorer on Windows Server 2003 and Windows Server 2008 runs in a restricted mode that is known as *Enhanced Security Configuration*. This mode sets the security level for the Internet zone to High. This is a mitigating factor for Web sites that you have not added to the Internet Explorer Trusted Sites zone.
    - By default, all supported versions of Microsoft Office Outlook®, Microsoft Office Outlook Express, and Windows Mail open HTML e-mail messages in the Restricted Sites zone. This zone helps reduce attacks by preventing scripts and ActiveX controls from executing when HTML e-mail messages are opened. Remember that if you click a link in an e-mail message, the resulting page will open in your Web browser, which could leave you open to attack.
- Avoid browsing to sites that you do not trust.
- To avoid attacks that rely on administrative user rights, enable User Account Control in Windows Vista, or log in with a user account that does not have administrative user rights.

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. 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 malicious 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*). 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 needed or how to obtain it. To help secure users against exploitation, Microsoft uses Windows Update to distribute *killbits* that prevent certain vulnerable add-ons from running in Internet Explorer. See Microsoft Security Advisory 956391 for details.

Most malicious Web sites use *exploit kits* that package together four to six 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 most highly sought-after exploits are *zero-day exploits*, which take advantage of undisclosed or newly disclosed vulnerabilities before the vendor is able to release 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 some users install updates only sporadically or not at all. 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—not just on the more popular or heavily used ones.

Top Browser-Based Exploits

To assess the relative prevalence of browser-based exploits in 2H08, Microsoft analyzed a sample of data obtained from customer-reported incidents, submissions of malicious code, and Windows error reports. The data encompasses multiple operating systems and browser versions, from Windows XP to Windows Vista.[11] It also includes data from third-party browsers (such as Maxthon and UUSee Player) that host the Internet Explorer rendering engine, called Trident.

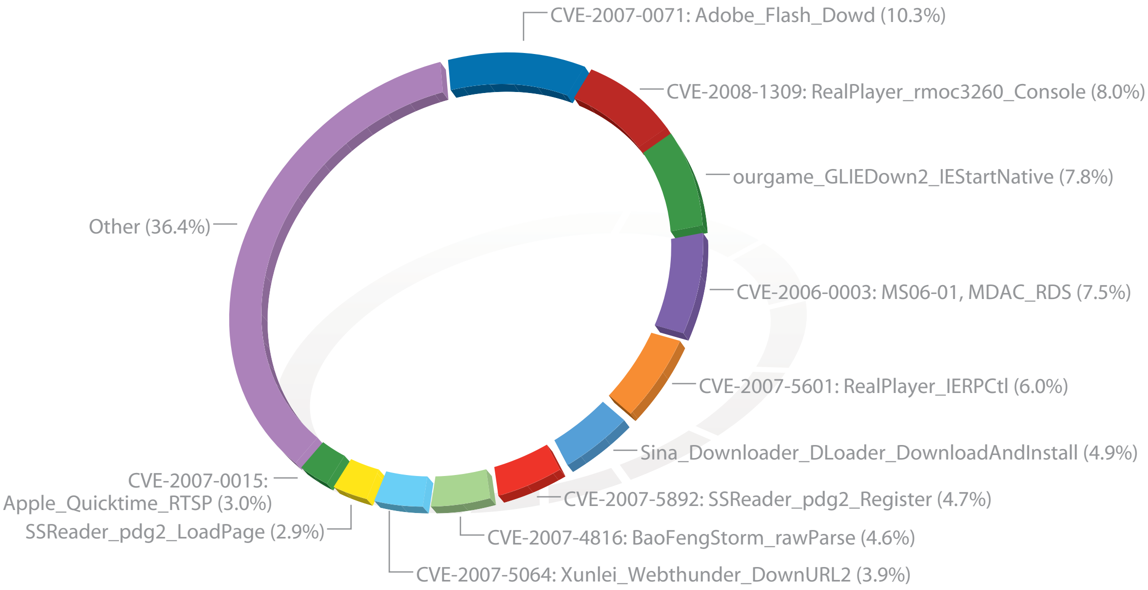
Here and throughout this section, exploits affecting vulnerabilities in Microsoft software are labeled with the Microsoft Security Bulletin number pertaining to the vulnerability, if applicable.[12] Exploits affecting third-party software are labeled with the CVE identifier pertaining to the vulnerability, if applicable.

[11] Includes Windows XP with no Service Pack (SP), Windows XP SP1, Windows XP SP2, and Windows XP SP3; Windows Vista release to manufacturing (RTM) and Windows Vista SP1; and versions of Internet Explorer 6, Internet Explorer 7, and Internet Explorer 8.

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

Figure 25 shows the browser-based exploits encountered by users in 2H08, ordered by frequency. The most frequently exploited vulnerability in 2H08 was CVE-2007-071, a vulnerability in Adobe Flash Player, which accounted for 10.3 percent of the infected computers in the sample. The next most encountered exploit was for CVE-2008-1309, a vulnerability in RealPlayer software, accounting for 8.0 percent of incidents. CVE-2006-0003 (MS06-014), a vulnerability in the Microsoft Data Access Components (MDAC) that accounted for the most encounters in 1H08, fell to fourth, at 7.5 percent.

FIGURE 25. Browser-based exploits, by percentage, encountered in 2H08

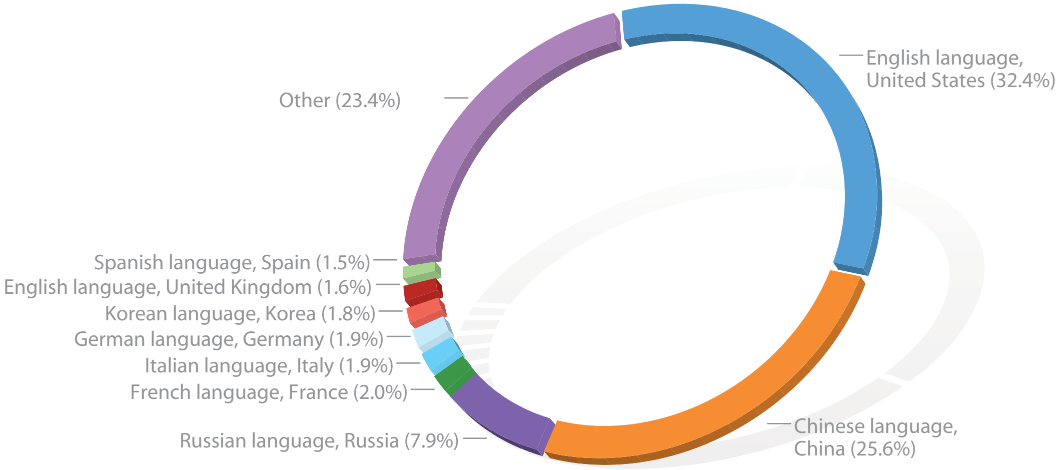


Browser-Based Exploits by System Locale

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 26 shows the browser-based exploits encountered by users in 2H08, ordered by the system locale of the victim. The most common locale for victims was en-US (English language, United States), accounting for 32.4 percent of all incidents, followed by zh-CN (Chinese language, China), with 25.6 percent of incidents. This is a significant drop from the zh-CN locale since 1H08, when it accounted for 47 percent of all incidents. The drop is primarily due to a decrease in attacks on Chinese-language ActiveX controls and a corresponding increase in attacks on the Adobe Reader add-on, which is released in multiple languages.

FIGURE 26. Browser-based exploits, by system locale of victim, encountered in 2H08



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 27 and Figure 28 show the relative percentages of exploits against vulnerabilities in Microsoft and third-party software in 2H08 on computers running Windows XP and Windows Vista, respectively. In Windows XP, Microsoft vulnerabilities account for 40.9 percent of the total. In Windows Vista, the proportion of Microsoft vulnerabilities is much smaller, accounting for just 5.5 percent of the total. These figures are roughly consistent with 1H08, when Microsoft vulnerabilities accounted for 42.3 percent of Windows XP exploits and 5.7 percent of Windows Vista exploits.

FIGURE 27. Browser-based exploits targeting Microsoft and third-party software on computers running Windows XP, 2H08

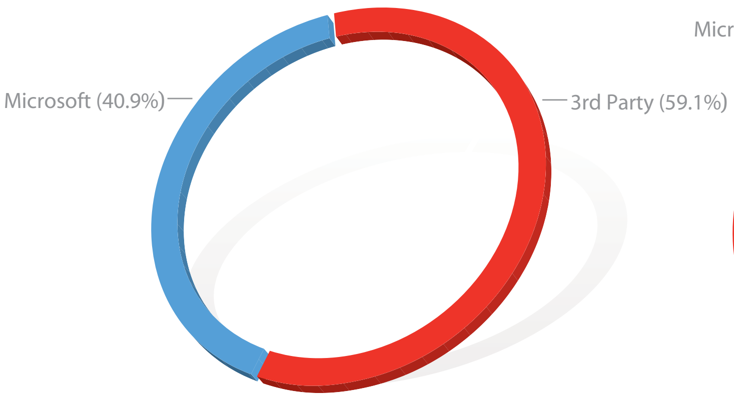


FIGURE 28. Browser-based exploits targeting Microsoft and third-party software on on computers running Windows Vista, 2H08

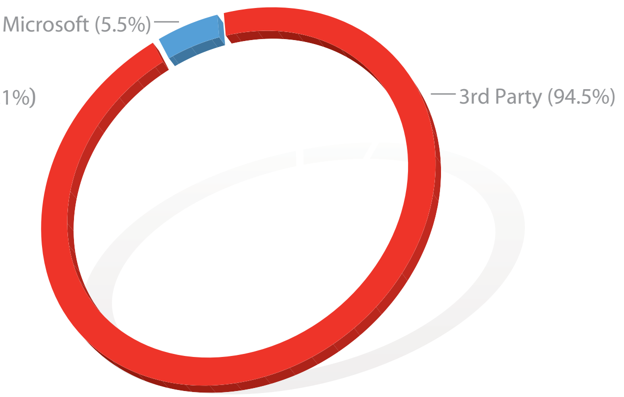


Figure 29 and Figure 30 show the 10 vulnerabilities exploited most often in Windows XP and Windows Vista in 2H08, respectively. In Windows XP, Microsoft software accounts for 6 of the top 10 vulnerabilities, compared to none in Windows Vista. These figures are also consistent with 1H08, when Microsoft vulnerabilities accounted for 5 of the top 10 vulnerabilities exploited on Windows XP and zero of the top 10 in Windows Vista.

FIGURE 29. The 10 browser-based vulnerabilities exploited most often on computers running Windows XP, by percentage of all exploits, in 2H08

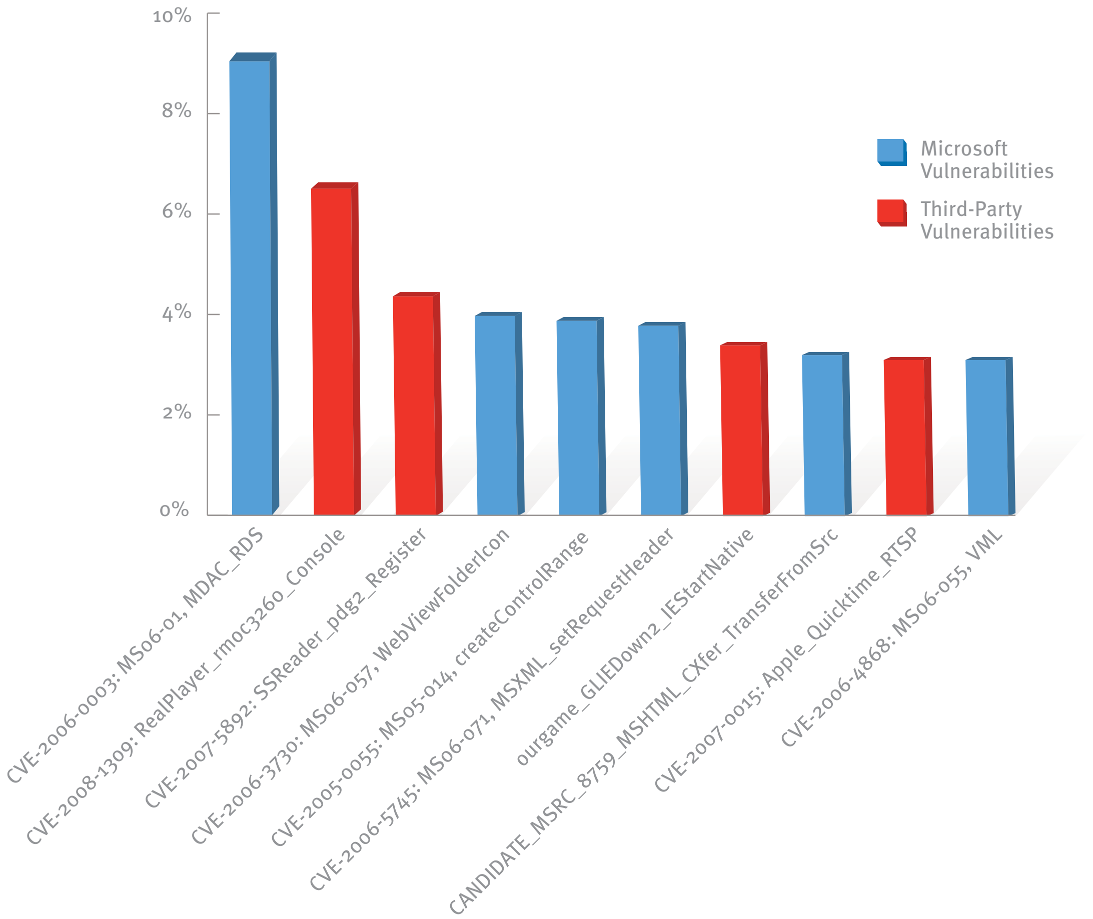
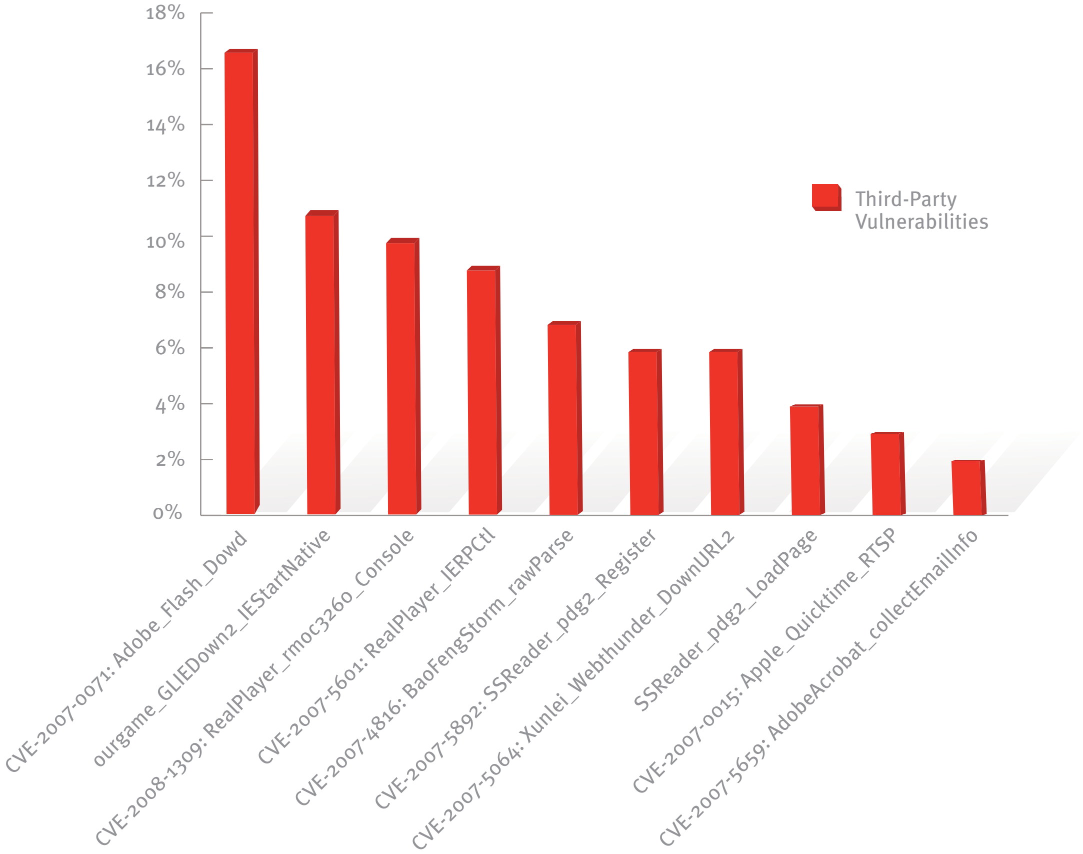


FIGURE 30. The 10 browser-based vulnerabilities exploited most often on computers running Windows Vista, by percentage of all exploits, in 2H08



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) and the Portable Document Format (.pdf) file format used by Adobe Reader. 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 their programs often go out of their way to handle document corruption, which means that they will attempt to parse a malformed section of a file that is designed to exploit a vulnerability. While parser vulnerabilities have been around for a long time and cover a broad range of scenarios, 2H08 saw a sharp increase in the number of file format–based attacks against popular business productivity programs, often in the form of spear phishing and whaling attacks. See page 22 for more information about these techniques.

Infection Vectors

There are two common attack scenarios. In one, the user receives an e-mail with a document attachment. The e-mail 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 of the document as an attached file. (Most complex document formats support built-in file system structures for containing attached files, which an attacker can use to insert a payload that is otherwise invisible in the rendered document.) Real-time antivirus scanning can help mitigate the danger from these attacks in some cases.

Attackers have sometimes been observed to target particular individuals using files they are likely to trust, such as the agenda of an upcoming conference or a widely circulated brief. Once the trojan is installed, the malicious code may also extract a clean, uninfected version of the document and open it, so that the victim sees exactly the document they expected to receive, with no indication that anything is wrong—typically, the victim might see the program window blink a few times as the documents are quickly loaded in succession. If the victim forwards the clean document to other people, the exploit does not travel along with it, since it has already served its purpose and additional propagation would just increase the likelihood of detection.

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 2H08. The data set was taken from submissions of malicious code sent to Microsoft from customers worldwide.

In total, exploits for seven vulnerabilities were identified in the sample set, as shown in Figure 31.

FIGURE 31. Vulnerabilities exploited in Microsoft Office suites file formats

Bulletin	Vulnerability	CVE
MS06-027	Microsoft Word Malformed Object Pointer Vulnerability	CVE-2006-2492
MS06-028	Microsoft PowerPoint Remote Code Execution Using a Malformed Record Vulnerability	CVE-2006-0022
MS07-014	Word Malformed Data Structures Vulnerability	CVE-2006-6456
MS07-015	Excel Malformed Record Vulnerability	CVE-2007-0671
MS07-025	Drawing Object Vulnerability	CVE-2007-1747
MS08-014	Macro Validation Vulnerability	CVE-2008-0081
MS08-042	Word Record Parsing Vulnerability	CVE-2008-2244

All seven vulnerabilities had security updates available at the time of attack; the affected users were exposed because they had not applied the updates. Office 2000, Office XP, Office 2003, and the 2007 Microsoft Office system were each affected by at least one of the seven vulnerabilities, although the sample analyzed did not include any attacks on 2007 Microsoft Office system applications. (For details, see Figure 36 on page 57).

Figure 32 shows these exploits ordered by frequency of attack. The most frequently exploited vulnerabilities were also some of the oldest. Fully 91.3 percent of attacks exploited a single vulnerability (CVE-2006-2492, the Malformed Object Pointer Vulnerability in Microsoft Office Word) for which a security fix had been available for more than two years.

FIGURE 32. Microsoft Office file format exploits, by percentage, encountered in 2H08

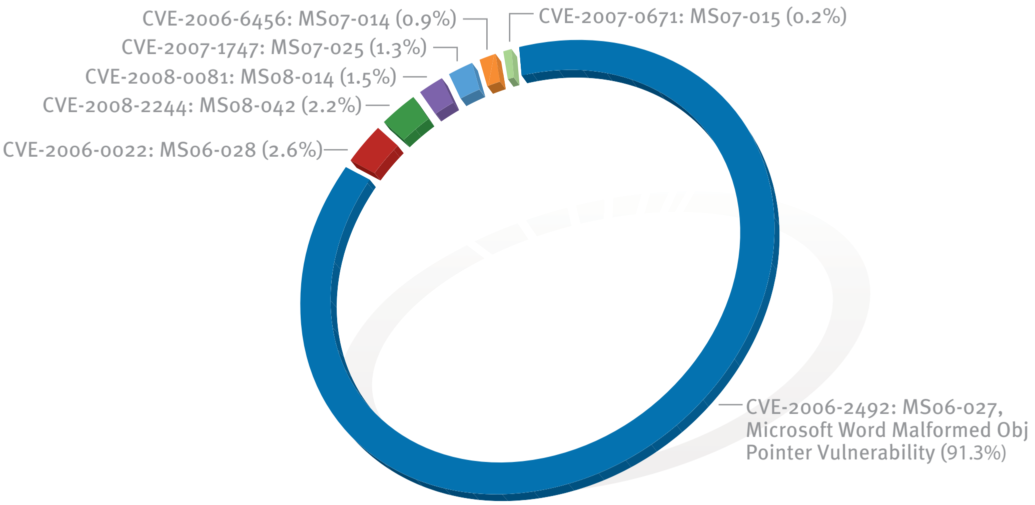
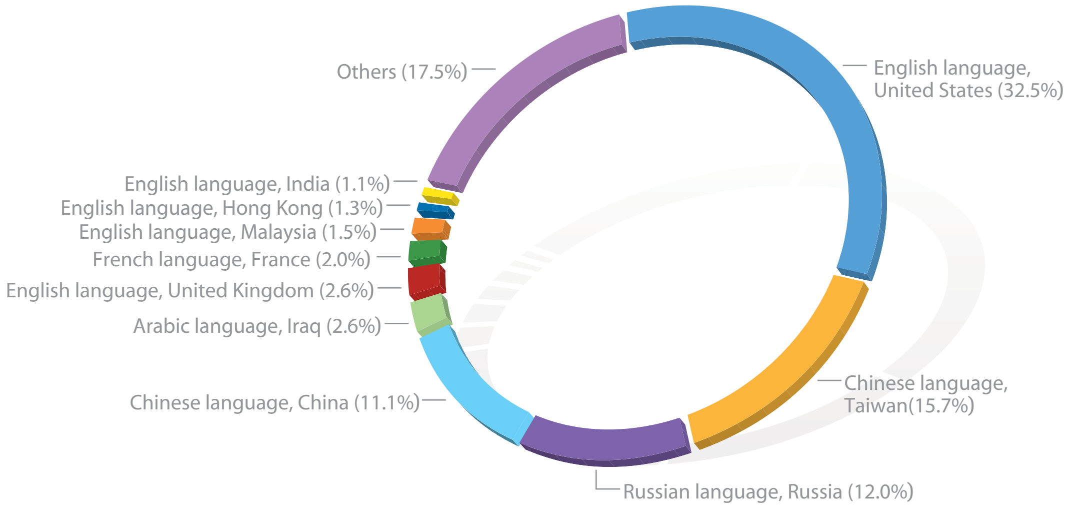


Figure 33 shows Microsoft Office file format exploits ordered by the system locale of the victim. The most common locale for victims was en-US (English language, United States), accounting for 32.5 percent of all incidents, followed by zh-TW (Chinese language, Taiwan), with 15.7 percent of incidents.

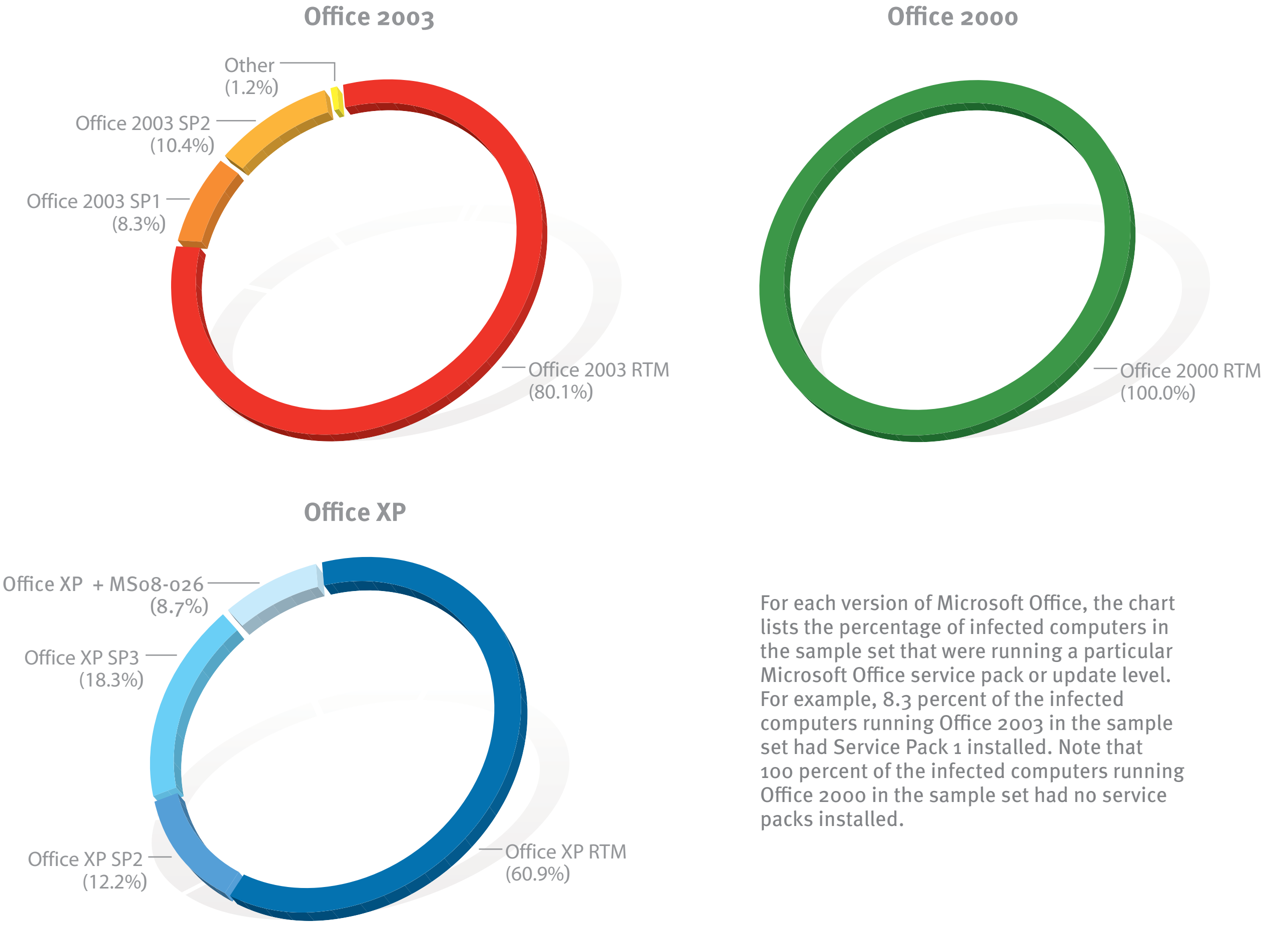
FIGURE 33. Microsoft Office file format exploits, by system locale of victim, encountered in 2H08



(Totals for each family may not equal 100 percent due to rounding.)

Figure 34 shows how attacks affected different combinations of service packs and other updates for Office 2003, Office XP, and Office 2000, respectively.

FIGURE 34. Breakdown of the sample set of targeted computers by Office update level for Office 2003, Office XP, and Office 2000



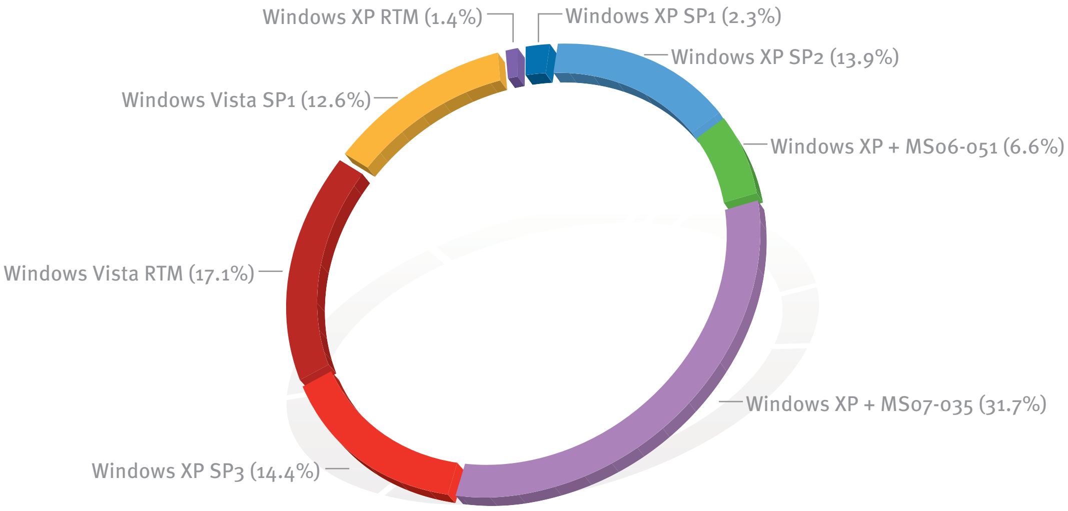
For each version of Microsoft Office, the chart lists the percentage of infected computers in the sample set that were running a particular Microsoft Office service pack or update level. For example, 8.3 percent of the infected computers running Office 2003 in the sample set had Service Pack 1 installed. Note that 100 percent of the infected computers running Office 2000 in the sample set had no service packs installed.

(Totals for each family may not equal 100 percent due to rounding.)

For each version, the clear majority of the attacks affected the RTM version of the application suite with no service packs applied. In the case of Office 2000, for example, 100 percent of the infected computers in the sample were running the RTM version of the application suite, released in 1999. Similarly, the RTM versions of Office XP (60.9 percent of all infected Office XP computers) and Office 2003 (80.1 percent of all infected Office 2003 computers) were disproportionately affected.

This pattern does not apply to the update level of the operating system upon which the applications run. Figure 35 shows the operating system versions and updates being run on the computers in the sample.

FIGURE 35. Microsoft Office file format exploits by operating system update level



Although almost all of the attacks in the sample affected Microsoft Office installations that did not include service packs or relevant updates released within the last four years, 58.7 percent of the attacks affected computers upon which the operating system had been updated at least once since the beginning of 2007. This suggests that many customers have implemented an updating strategy for Windows but have not adopted one for Microsoft Office.

In all cases, applying new security updates quickly and consistently would have prevented all of these attacks from succeeding on any supported version of Microsoft Office. The RTM versions of Office 2000, Office XP, and Office 2003 are each vulnerable to all of the attacks seen in the sample, as are Office 2000 and Office XP with the latest service packs applied; even Office 2003 with the latest service pack is vulnerable to attacks targeting the MS08-042 vulnerability. None of these Microsoft Office versions are vulnerable to any of the attacks seen in the sample set when all service packs and other updates are applied, illustrating the importance of applying all security updates in a timely fashion.

FIGURE 36. Vulnerability of different Microsoft Office versions to attacks seen in 2H08

Microsoft Office Version	MS06-027	MS06-028	MS07-014	MS07-015	MS07-025	MS08-014	MS08-042
Office 2000 RTM	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Office XP RTM	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Office 2003 RTM	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Office 2007 RTM	No	No	No	No	Yes	Yes	No
Office 2000 SP3	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Office XP SP3	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Office 2003 SP3	No	No	No	No	No	No	Yes
Office 2007 SP1	No	No	No	No	No	No	No

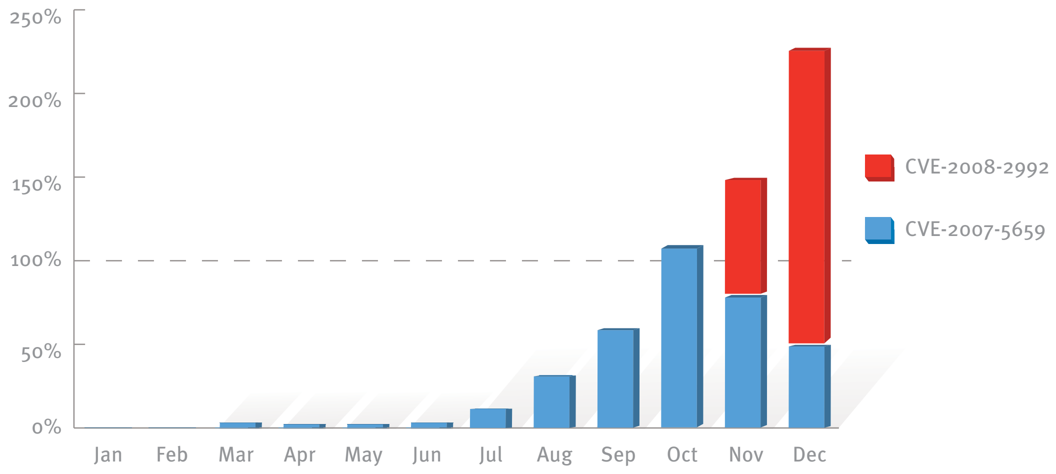
The RTM version of the 2007 Microsoft Office system is only vulnerable to 2.8 percent of the attacks seen in the sample. As with the other versions of Microsoft Office, installing all of the service packs and updates for the 2007 Microsoft Office system protects it from all of the remaining attacks.

PDF Format Exploits

Two vulnerabilities accounted for all of the attacks in the sample. Approximately 60 percent of the attacks exploited CVE-2007-5659, a vulnerability in the **CollabEmailInfo** JavaScript method as implemented in some versions of Adobe Reader. The other 40 percent exploited CVE-2008-2992, a vulnerability in the **util.printf** JavaScript method as implemented in some versions of Adobe Reader. Neither vulnerability affects version 9.0 (the most recent version) of Adobe Reader.

Figure 37 shows attacks on Adobe Reader during each month of 2008.

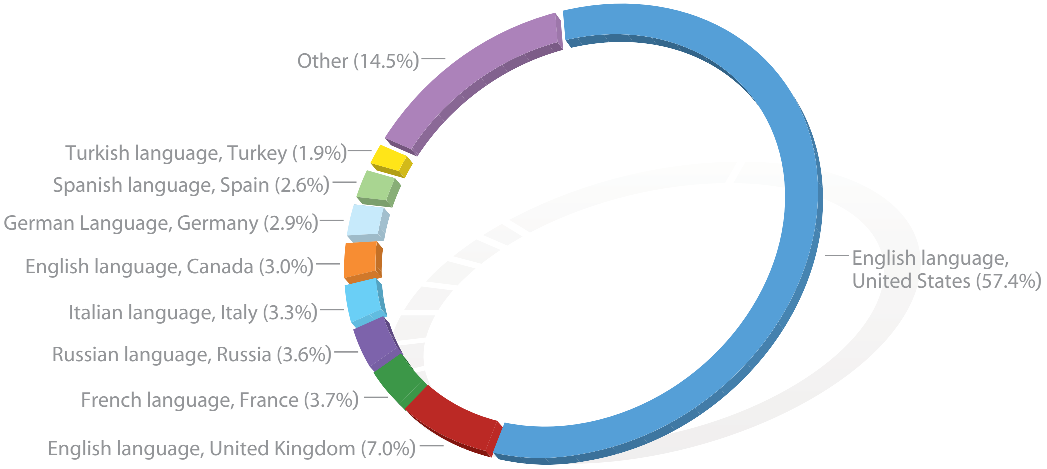
FIGURE 37. Adobe Reader exploits by month in 2008, indexed to the monthly average for 2H08



Use of the PDF format as an attack vector rose sharply in 2H08, with attacks in July amounting to more than twice as many as in all of 1H08 combined and continuing to double or almost double for most of the remaining months of the year. The first exploit for CVE-2008-2992 appeared at the beginning of November 2008—attackers quickly adapted to the new discovery, with 76.3 percent of the attacks in December taking advantage of CVE-2008-2992.

Figure 38 shows PDF 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 57.4 percent of all incidents, followed by en-GB (English language, United Kingdom) with 7.0 percent of incidents.

FIGURE 38. PDF file format exploits, by system locale of victim, encountered in 2H08



(Totals may not equal 100 percent due to rounding.)

As with Microsoft Office, users with fully updated versions of Adobe Reader are not vulnerable to these attacks. Adobe Systems released a security update for Adobe Reader 8 fixing CVE-2007-5659 in February 2008 and another one fixing CVE-2008-2992 in November 2008. Adobe Reader 9, released in June 2008, is not vulnerable to either attack. This information is summarized in Figure 39.

FIGURE 39. Vulnerability of recent Adobe Reader releases to CVE-2007-2629 and CVE-2008-2992

Adobe Reader Version	Vulnerable to CVE-2007-5659?	Vulnerable to CVE-2008-2992?
7.0.0.0	Yes	No
7.0.8.218	Yes	No
8.0.0.456	Yes	Yes
8.1.0.137	Yes	Yes
8.1.3	No	No
9.0.0	No	No

Strategies, Mitigations, and Countermeasures

- Always run up-to-date software. Enable Automatic Updates in Windows, which will help ensure that the latest security updates from Microsoft are downloaded automatically. Periodically check the Web sites of third-party add-on vendors to help ensure that you have the latest security updates for their software.
- Uninstall software you don't actively use. Malicious code can exploit vulnerabilities in software, whether you use it or not.[13]
- Use up-to-date anti-malware software from a known, trusted source that offers real-time protection and continually updated definition files to detect and block exploits.
- Enable Data Execution Prevention (DEP) in compatible versions of Windows, which can help prevent a common class of exploits called *buffer overflows*. See http://support.microsoft.com/kb/875352 for a detailed description of the DEP feature.
- Enable Structured Exception Handling Overwrite Protection (SEHOP) in Windows Vista SP1 and Windows Server 2008, which is designed to block exploits that use the Structured Exception Handler (SEH) overwrite technique. See http://support.microsoft.com/kb/956607 for additional information about the SEHOP feature.
- Set Internet and local intranet security zone settings in Internet Explorer to High, which will cause Internet Explorer to prompt the user before running scripts and ActiveX controls in these zones.
  - To minimize disruption, you can add sites you trust to the Trusted Sites zone to avoid the prompts. In particular, consider adding *.windowsupdate.microsoft.com and *.update.microsoft.com to the Trusted Sites zone to facilitate keeping your computer up to date.
  - By default, Internet Explorer on Windows Server 2003 runs in a restricted mode that is known as *Enhanced Security Configuration*. This mode sets the security level for the Internet zone to High. This is a mitigating factor for Web sites that you have not added to the Internet Explorer Trusted Sites zone.
  - By default, all supported versions of Microsoft Office Outlook and Microsoft Office Outlook Express open HTML e-mail messages in the Restricted Sites zone. This zone helps reduce attacks by preventing scripts and ActiveX controls from executing when HTML e-mail messages are opened. Remember that if you click a link in an e-mail message, the resulting page will open in your Web browser, which could leave you open to attack.
- Avoid browsing to sites that you do not trust.

[13] For example, see http://msdn.microsoft.com/en-us/library/bb688194(VS.85).aspx, for information about managing ActiveX controls.

- To avoid attacks that rely on administrative user rights, enable User Account Control in Windows Vista, or log in with a user account that does not have administrative user rights.
- Read e-mail messages in plain text format to help protect yourself from the HTML e-mail attack vector.
- Use the Microsoft Security Assessment Tool (MSAT) to help assess weaknesses in your IT security environment, and build a plan to address the risks. The MSAT can be downloaded from http://technet.microsoft.com/en-us/security/cc185712.aspx.

Document File Format Exploits

- Configure your computer to use Microsoft Update instead of Windows Update; this will help ensure that you receive security updates for Microsoft Office and other Microsoft applications, in addition to security updates for Windows operating systems. See http://www.microsoft.com/windows/downloads/windowsupdate/microsoftupdate.mspx for an explanation of the differences between Microsoft Update and Windows Update.
- Ensure that Microsoft security update MS06-027 has been applied to any affected software in your environment: http://www.microsoft.com/technet/security/bulletin/MS06-027.mspx.
- Keep your third-party software and your Microsoft software up to date. Updates for Adobe products can be downloaded from http://www.adobe.com/downloads/updates.
- If possible, upgrade your software applications to the most recent versions, since these demonstrate lower rates of attack.
- Avoid opening attachments or clicking links to documents in e-mail or instant messages that are received unexpectedly or from an unknown source.
- Use up-to-date antivirus software from a known, trusted source that offers real-time protection and continually updated definition files to detect and block exploits.

Call to Action—End to End Trust[14]

Security researchers and others will continue to develop exploits against vulnerabilities found in software, some of which will lead to attacks against the installed base of these products. In addition, software developers/vendors will issue security updates that address vulnerabilities—these updates can be reverse-engineered to uncover the vulnerability and enable the development of exploits. The Internet with its rich targets is a magnet for criminal activity—criminal activity that is undeterred due to a lack of accountability. Moreover, the Internet also fails to provide the information necessary to permit lawful computer users to know whether the people they are dealing with, the programs they are running, the devices they are connecting to, or the packets they are accepting, are to be trusted.

Experience shows that most cybercriminal schemes are successful because people, machines, software, and data are not well authenticated and this fact, combined with the lack of auditing and traceability, means that criminals will neither be deterred at the outset nor held accountable after the fact. Thus the answer must lie in better authentication that allows a fundamentally more trustworthy Internet and audit that introduces real accountability.

We must create an environment where reasonable and effective trust decisions can be made. We must also create an environment where accountability—and therefore deterrence—can be achieved. To do this, one must have access to a trusted stack: (1) security rooted in the hardware; (2) a trusted operating system; (3) trusted applications; (4) trusted people; and (5) trusted data. The entire stack must be trustworthy because these layers can be interdependent, and a failure in any can undermine the security provided by the other layers.

Visit the End to End Trust Web site to learn more about the vision and help us get there by working together on the creation of a safer, more trusted Internet: www.microsoft.com/endtoendtrust.

[14] Derived/excerpts from: Scott Charney, "Establishing End to End Trust." (http://download.microsoft.com/download/7/2/3/723a663c-652a-47ef-a2f5-91842417cab6/Establishing_End_to_End_Trust.pdf)

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. The data collection used in this analysis is publicly available.

This section of the report examines the types of breach incidents from around the world that took place in 2H08 and earlier, as downloaded from the Open Security Foundation's OSF Data Loss Database at http://datalossdb.org. 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.

For the purposes of this analysis, the data has been grouped into 10 categories, which are supersets of the coding used by the OSF DataLossDB. The groups are shown in Figure 40.

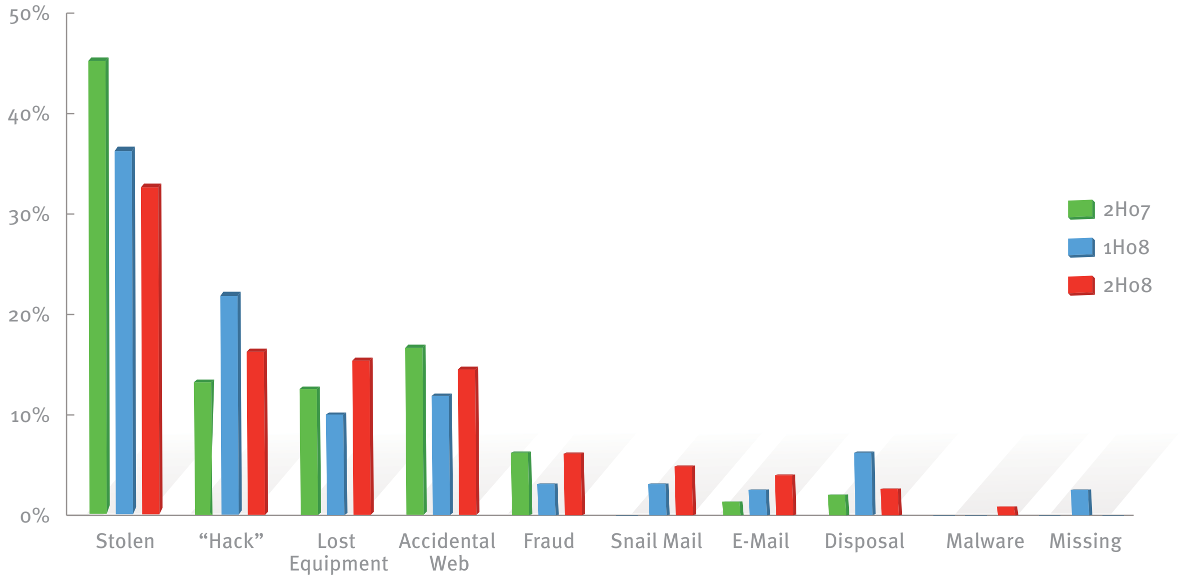
FIGURE 40. Security breach incident categories used in this section

Our Label	Definition	Maps to datalossdb.org BreachType
Stolen equipment	Stolen computers, disks, tapes, or documents	Starts with "stolen"
"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	Starts with "lost"
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 we take no position	Starts with "fraud"
Snail mail	Information exposed by physical mail, either the wrong recipient or the data visible outside the envelope	Snail mail
E-Mail	E-mail sent to an unintended/unplanned recipient	E-mail
Disposal	Improper disposal of any sort	Starts with "disposal"
Malware	Malware was blamed	Virus
Missing	A laptop or laptops gone missing without explanation	Starts with "missing"

In the OSF database, there are 19 incidents for which the breach type is listed as "Unknown." These incidents are not included in the following analysis or totals.

Figure 41 illustrates the overall distribution of incidents by type since 2H07.

FIGURE 41. Security breach incidents by type, expressed as percentages of the total, 2H07–2H08



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 total breaches result from something that the OSF database does not classify as a hack. 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 since 2H07. If this decline is real, and assuming it does not represent an actual decrease in stolen equipment, the decline may mean that organizations are taking more steps to safeguard data against disclosure than they have in the past, such as deploying encryption solutions like Windows BitLocker™ Drive Encryption or adopting policies governing the storage and distribution of PII on mobile equipment.
- 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.

Strategy, Mitigations, and Countermeasures

- Consider a broad set of information security problems when building an information security policy. A security program that focuses entirely on malware, exploits, and hacking will potentially miss up to 80 percent of total incidents that put sensitive information in jeopardy. Consider all stages of the data life cycle, including storage, transit, and destruction, when developing policies.
- Use the Microsoft Security Assessment Tool (MSAT) to help assess weaknesses in your IT security environment, and build a plan to address the risks. The MSAT can be downloaded from http://technet.microsoft.com/en-us/security/cc185712.aspx.
- Encrypt all data on all computers and storage devices—not just on laptops.
- Prepare an incident response plan for personally identifiable data that you collect or store.
- Consider tracking data on security breaches as an input into your security planning.

Call to Action—End to End Trust[15]

Stolen and lost equipment remain the top causes of security breaches. With a trusted stack, in-person proofing, and an identity metasystem, the impact of security breaches can be mitigated.

- Trusted data created and managed by trusted people using trusted applications and operating systems on hardware with security "built in" will be key to ensuring that only users who can demonstrate a correctly authenticated identity claim can access the data.
- Hardware and operating systems must be designed to protect data from unauthenticated access. Security rooted in the hardware (such as Trusted Platform Modules) and trusted operating systems incorporating data encryption technologies (such as BitLocker) will make it significantly more difficult for lost or stolen equipment to be compromised.

Visit the End to End Trust Web site to learn more about the vision, and help us get there by working together on the creation of a safer, more trusted Internet: www.microsoft.com/endtoendtrust.

[15] Derived/excerpts from: Scott Charney, "Establishing End to End Trust." (http://download.microsoft.com/download/7/2/3/723a663c-652a-47ef-a2f5-91842417cab6/Establishing_End_to_End_Trust.pdf)

Malware and Potentially Unwanted Software Trends

The malware landscape in 2H08 was dominated by social engineering threats that exploit the fears, trust, and desires of computer users around the world, for the benefit of attackers seeking profit. Attackers profit from malware by charging spammers to send spam, by misleading victims into thinking they need to install worthless software to protect them from nonexistent threats, by stealing user names and passwords for online banks and games, and through other means. The threats and techniques used in different parts of the world vary, but malware is truly a global problem.

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 Security for Exchange (FOSE). See "Appendix C: Data Sources," beginning on page 173, for more information on these tools.

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 mil*, or *CCM*, which represents 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 July and removes infections from 500 computers, the CCM for that location in July is 10.0. A new version of the MSRT is released every month, so figures for multiple months, or for 2H08 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 that makes it possible to compare infection rates, patterns, and trends in different locations around the world. For this and future volumes, Microsoft is using a new metric derived from the computer's location as configured in **Regional and Language Settings** in the Control Panel. Microsoft believes that this method will provide more accurate geographical statistics, though it is important to note that figures from this volume cannot be directly compared to figures from previous volumes for purposes of determining geographic trends.

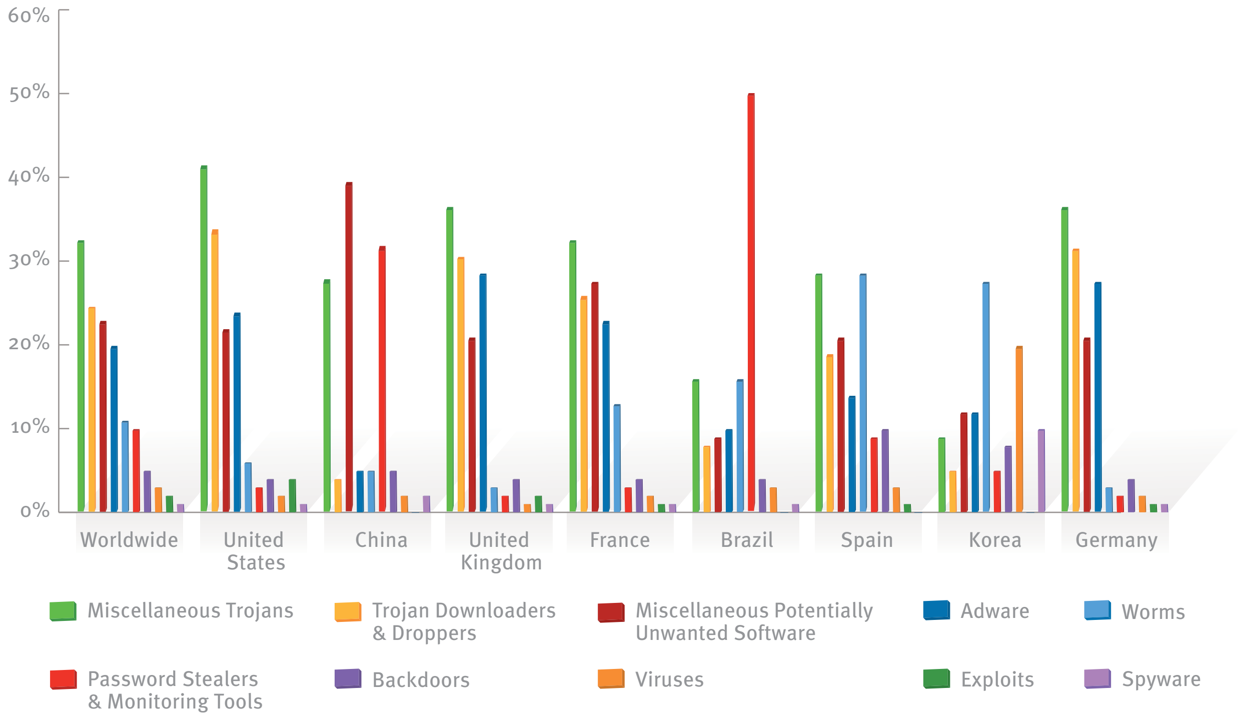
FIGURE 42. The 25 locations with the most computers cleaned by Microsoft anti-malware desktop products in 2H08

Country/Region	Computers Cleaned in 2H08
United States	13,245,712
China	3,558,033
United Kingdom	2,225,016
France	1,815,639
Brazil	1,654,298
Spain	1,544,623
Korea	1,368,857
Germany	1,209,461
Italy	978,870
Canada	916,263
Mexico	915,605
Turkey	768,939
Netherlands	641,053
Russia	604,598
Taiwan	466,929
Australia	464,707
Japan	417,269
Poland	409,532
Portugal	337,313
Sweden	287,528
Belgium	267,401
Denmark	224,021
Norway	203,952
Colombia	164,986
Switzerland	163,156

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. As the malware ecosystem moves toward a greater reliance on social engineering (examined in "Social Engineering as a Weapon," beginning on page 15), the spread and effectiveness of malware has 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 43 shows the relative prevalence of different categories of malware and potentially unwanted software in the eight locations with the most computers cleaned in 2H08, 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 72 for an explanation of the categories used in this figure.

FIGURE 43. 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, 2H08



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

Win32/CNNIC: A browser modifier that enables Chinese keyword searching and support for Chinese-language domain names. It may be bundled with other programs and installed without user consent.

Win32/SpywareSecure: A program that displays misleading warning messages in order to convince users to purchase a product that removes spyware.

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

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

http://www.microsoft.com/av

- In the **United States**, Miscellaneous Trojans, like Win32/FakeXPA, account for the largest single category of threat. The threat landscapes in the **United Kingdom** and **Germany** are similar to that of the United States, though the prevalent malware families are slightly different in all three locations.
- 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. The most prevalent families in China in 2H08 were the browser modifiers Win32/BaiduSobar[16] and Win32/CNNIC, followed by a number of password stealers that target players of online games, including Win32/Tilcun and Win32/Lolyda.
- In **France**, Miscellaneous Potentially Unwanted Software is more prevalent than in some other locations, led by the rogue security software family Win32/SpywareSecure.
- In **Brazil**, password stealers, such as Win32/Bancos and Win32/Banker, dominate by an overwhelming margin, being detected on more than 50 percent of all Brazilian computers cleaned in 2H08. See "Online Banking Malware," beginning on page 23, for more information.
- In **Spain**, worms are unusually prominent, led by Win32/Taterf.
- In **Korea**, viruses like Win32/Virut and Win32/Parite are prevalent. Viruses often spread through peer-to-peer (P2P) networks and community sites where files are exchanged. Korea has one of the highest levels of broadband Internet access penetration per capita in the world,[17] which may contribute to the spread of infected files.

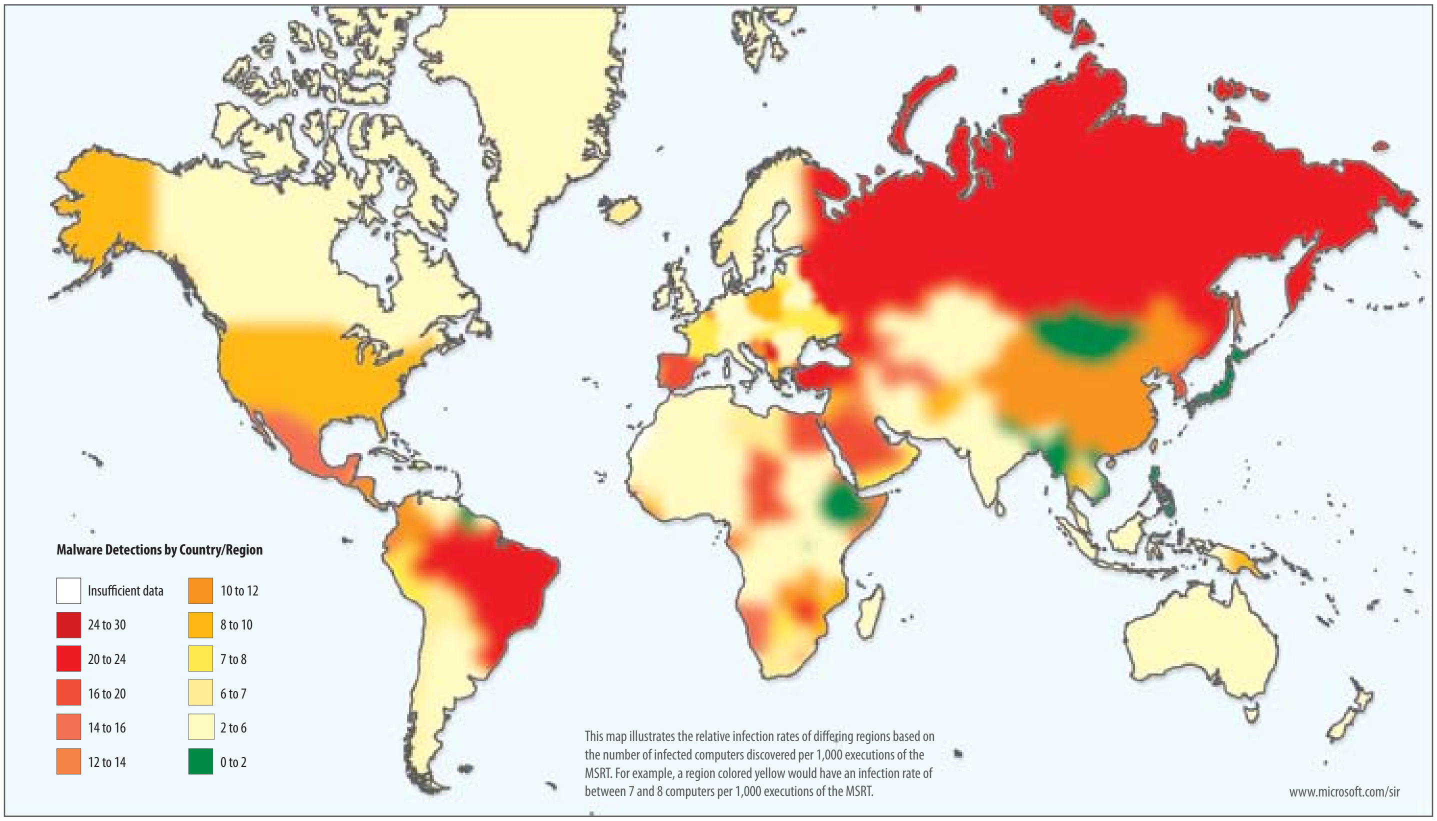
"Appendix B: Threat Assessments for Individual Locations," which begins on page 137, includes more in-depth information about the threat landscapes in many of the locations listed above.

[16] 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.

[17] As reported by the Organisation for Economic Co-operation and Development (http://www.oecd.org/sti/ict/broadband) in June 2008.

Figure 44 illustrates the infection rates of locations around the world, expressed in CCM. See page 65 for an explanation of this metric.

FIGURE 44. Infection rates by country/region in 2H08



This map illustrates the relative infection rates of differing regions based on the number of infected computers discovered per 1,000 executions of the MSRT. For example, a region colored yellow would have an infection rate of between 7 and 8 computers per 1,000 executions of the MSRT.

www.microsoft.com/sir

Figure 45 shows the infection rates in locations around the world with at least 1 million average monthly MSRT executions in 2H08, derived by averaging each location's monthly CCM for each of the six months in the period. See "Appendix A: Full Infection Chart," on page 134, for a more comprehensive list with 215 locations, and see "Appendix B: Threat Assessments for Individual Locations," beginning on page 137, for an in-depth look at the threat landscapes for 12 locations around the world, encompassing multiple continents, languages, and computer usage patterns.

FIGURE 45. Infection rates (CCM) for locations around the world with at least 1 million average monthly MSRT executions in 2H08

Country/Region	CCM (2H08)
Argentina	4.4
Australia	4.7
Austria	2.3
Belgium	5.0
Brazil	20.9
Canada	4.0
Chile	6.3
China	11.4
Colombia	10.0
Czech Republic	5.2
Denmark	5.9
Finland	2.6
France	7.8
Germany	3.6
Greece	9.4
Hong Kong S.A.R.	5.8
Hungary	7.5
India	2.8
Ireland	4.2
Israel	7.5
Italy	5.8
Japan	1.7
Korea	18.3
Malaysia	3.5
Mexico	15.9
Netherlands	5.9
New Zealand	4.0
Norway	6.8
Philippines	1.4
Poland	8.0
Portugal	13.4
Romania	4.3
Russia	21.1
Singapore	4.5
South Africa	6.6
Spain	19.2
Sweden	5.4
Switzerland	4.1
Taiwan	11.7
Thailand	8.9
Turkey	20.5
United Kingdom	5.7
United States	9.1
Venezuela	5.5
Worldwide	**8.6**

Figure 46 and Figure 47 offer a closer look at these geographic statistics, listing the 25 locations with the lowest infection rates and the 25 locations with the highest infection rates in 2H08, respectively, among locations with at least 100,000 average monthly MSRT executions.

FIGURE 46. Locations with the lowest infection rates, by CCM, in 2H08 (100,000 monthly MSRT executions or more)

Country/Region	CCM
Vietnam	1.3
Philippines	1.4
Macao S.A.R.	1.5
Japan	1.7
Morocco	2.1
Pakistan	2.2
Austria	2.3
Luxembourg	2.5
Algeria	2.6
Finland	2.6
Puerto Rico	2.7
Tunisia	2.7
India	2.8
Uruguay	2.9
Indonesia	3.0
Nigeria	3.1
Malaysia	3.5
Germany	3.6
Canada	4.0
New Zealand	4.0
Switzerland	4.1
Ireland	4.2
Kazakhstan	4.2
Romania	4.3
Argentina	4.4

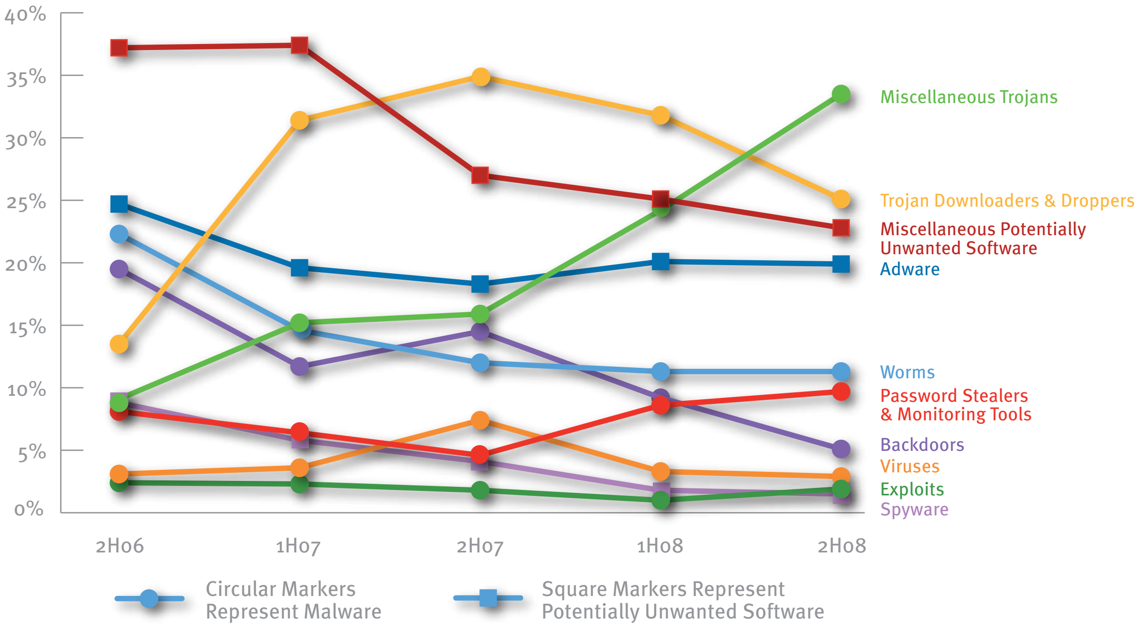
FIGURE 47. Locations with the highest infection rates, by CCM, in 2H08 (100,000 monthly MSRT executions or more)

Country/Region	CCM
Serbia and Montenegro	77.0
Russia	21.1
Brazil	20.9
Turkey	20.5
Spain	19.2
Saudi Arabia	18.5
Korea	18.3
Egypt	16.5
Mexico	15.9
Guatemala	13.9
Portugal	13.4
Ecuador	12.6
Taiwan	11.7
China	11.4
Croatia	10.8
Colombia	10.0
Kuwait	9.8
El Salvador	9.6
Greece	9.4
Jordan	9.2
United States	9.1
Panama	8.9
Thailand	8.9
Costa Rica	8.8
Poland	8.0

Category Trends

Figure 48 shows the relative prevalence of different categories of malware and potentially unwanted software since 2H06, 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 48. Computers cleaned by threat category, in percentages, 2H06–2H08



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 judge 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 178, for definitions of the other categories described in this section.

As in 1H08, a clear separation can be seen in Figure 48 between more prevalent categories and less prevalent ones. Miscellaneous Trojans, Trojan Downloaders & Droppers, Miscellaneous Potentially Unwanted Software, and Adware were all detected on significantly more computers than the other categories.

Trojan Categories

For the first time, the Miscellaneous Trojans category accounted for the most computers cleaned in 2H08, displacing Trojan Downloaders & Droppers. The significant rise in prevalence of the Miscellaneous Trojans category is due primarily to the reclassification of a number of rogue security software families that exhibit clear malicious behavior from the Miscellaneous Potentially Unwanted Software category to the Miscellaneous Trojans category in 2H08. Rogue security software accounts for a significant and growing portion of the malware landscape, and a number of rogue security software families were added to the MSRT in 2H08, so the result has been an increase in the prevalence of the Miscellaneous Trojans category and a corresponding decline in the Miscellaneous Potentially Unwanted Software category. See "Rogue Security Software," beginning on page 92, for more information.

Trojan Downloaders & Droppers, previously the most prevalent category of threat, dropped to second in 2H08, due in large part to a significant decrease in the prevalence of the downloader family Win32/Zlob. Despite this, the prevalence of downloaders and droppers remains high, with several downloader/dropper families among the top families detected worldwide. Downloaders and droppers (often collectively referred to simply as *downloaders*) are 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. Downloaders have emerged as a major threat over the past few years as malware distributors have sought more effective ways to infect computers without being detected. After installing a downloader on a victim's computer through social engineering or an exploit, an attacker can use the downloader as a conduit to download additional programs to the infected computer. The attacker can then use these additional programs to send spam, launch distributed denial-of-service (DDoS) attacks, build a botnet, or engage in other illicit activities. As malware authors develop new ways to profit from malware, they can use preexisting downloader installations to download new code to the controlled computers without engaging in additional social engineering. Downloaders are often persistent, which means that they reinstall and run themselves every time the computer is started or the user logs on.

Encyclopedia

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/Antivirus2008: A program that displays misleading security alerts in order to convince users to purchase rogue security software. It may be installed by Win32/Renos or manually by a computer user.

http://www.microsoft.com/av

Miscellaneous Potentially Unwanted Software and Adware

Miscellaneous Potentially Unwanted Software threats remained prevalent in 2H08. Despite the reclassification of several rogue security software families that displayed unambiguously malicious behavior as Miscellaneous Trojans, a number of rogue security programs, such as Win32/Antivirus2008, remain classified as Miscellaneous Potentially Unwanted Software, and the general rise in the prevalence of rogue security software contributed to the continued high showing of this category. Adware, which is considered a type of potentially unwanted software but is categorized separately, was cleaned at a rate comparable to 1H08. Potentially unwanted software relies heavily on social engineering tactics to convince users to install it, often by presenting a value proposition that users find compelling. See "User Reaction to Alerts," beginning on page 82, for more analysis.

Other Threats

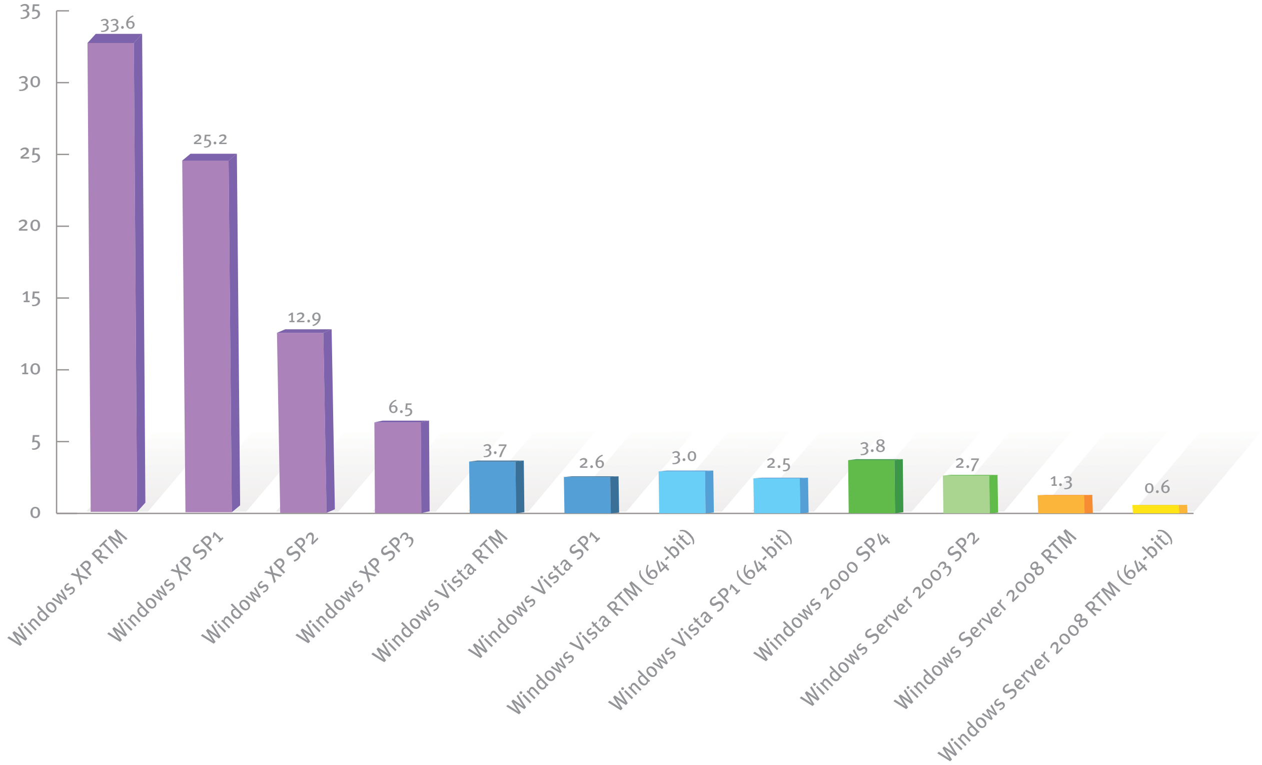
Detection of password stealers and monitoring tools, though low in comparison to some other threats, continues to grow, due to the increasing prevalence of several password stealers aimed at players of online games. See page 24 for more information about these families.

Backdoors and worms, which were two of the most significant categories of threat as recently as two years ago, continued to recede in prominence relative to other categories, as did viruses. Bots are considered a subcategory of backdoors, so the decline in the prevalence of backdoors suggests that the number of computers worldwide infected with bots, though still significant, is decreasing—a welcome development. Although the prevalence of exploits appears negligible as presented above, many of the families classified in other malware categories also include exploit code that assists in accomplishing the malware's primary function. See "MS08-067: Vulnerability in Windows Server Service," beginning on page 41, for information about one example, the worm family Win32/Conficker.

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 49 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 2H08. (Note that the infection rate for a particular version of Windows is not affected by the number of computers running it. See page 65 for a definition of the CCM metric used to calculate infection rates.)

FIGURE 49. Number of computers cleaned for every 1,000 MSRT executions, by operating system, 2H08



The major trends observed include the following:

- 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 60.6 percent less than that of Windows XP SP3.
    - Comparing the *n*-1 service packs for each version, the infection rate of the release to manufacturing (RTM) version of Windows Vista is 71.5 percent less than that of Windows XP SP2.
    - Comparing the RTM versions of these operating systems, the infection rate of the RTM version of Windows Vista is 89.1 percent less than that of the RTM version of Windows XP.
- Similarly, the infection rate of Windows Server 2008 RTM is 51.9 percent less than that of its predecessor, Windows Server 2003 SP2.

- The higher the service pack level, the lower the rate of infection. 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.
- 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 cannot be used to browse untrusted Web pages, by default, and the Roles Wizard automatically disables features that are not needed for the configured server role.

Malware and Potentially Unwanted Software Families

Figure 50 lists the top 25 malware and potentially unwanted software families that were detected on computers by all of the Microsoft security products in 2H08.

FIGURE 50. Top 25 malware and potentially unwanted software families detected by Microsoft anti-malware desktop products worldwide, by number of unique infected computers, in 2H08

Rank	Family	Most Significant Category	Infected Computers
1	*Win32/Renos*	Trojan Downloaders & Droppers	4,371,508
2	Win32/Zlob	Trojan Downloaders & Droppers	3,772,217
3	Win32/Vundo	Miscellaneous Trojans	3,635,207
4	Win32/ZangoSearchAssistant	Adware	3,326,275
5	Win32/Taterf	Worms	1,916,446
6	Win32/ZangoShoppingreports	Adware	1,752,252
7	*Win32/FakeXPA*	Miscellaneous Trojans	1,691,393
8	*Win32/FakeSecSen*	Miscellaneous Trojans	1,575,648
9	Win32/Hotbar	Adware	1,477,886
10	Win32/Agent	Miscellaneous Trojans	1,289,178
11	ASX/Wimad	Trojan Downloaders & Droppers	1,168,724
12	Win32/BaiduSobar	Miscellaneous Potentially Unwanted Software	1,131,180
13	Win32/Frethog	Password Stealers & Monitoring Tools	1,037,451
14	*Win32/Antivirus2008*	Miscellaneous Potentially Unwanted Software	1,034,897
15	Win32/Playmp3z	Adware	996,272
16	Win32/Tibs	Miscellaneous Trojans	830,809
17	Win32/SeekmoSearchAssistant	Adware	803,082
18	Win32/Lolyda	Password Stealers & Monitoring Tools	777,969
19	Win32/Tilcun	Miscellaneous Trojans	774,050
20	Win32/Bancos	Password Stealers & Monitoring Tools	738,667
21	*Win32/SpywareSecure*	Miscellaneous Potentially Unwanted Software	689,647
22	Win32/RJump	Worms	671,438
23	*Win32/Winfixer*	Miscellaneous Potentially Unwanted Software	659,119
24	Win32/C2Lop	Miscellaneous Trojans	597,105
25	Win32/Matcash	Miscellaneous Trojans	516,444

Italics indicate rogue security software-related families.

Encyclopedia

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

Win32/FakeSecSen: A rogue security software family that claims to scan for malware and then demands that the user pay to remove non-existent threats. It appears to be based on Win32/SpySheriff.

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

http://www.microsoft.com/av

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. Win32/Renos, a longtime threat that is often used as a delivery mechanism for rogue security software, rose to become the most prevalent threat in 2H08, up from second in 1H08. Two new trojans, Win32/FakeXPA and Win32/FakeSecSen, became the seventh and eighth most prevalent families in 2H08, respectively. Another rogue security program, Win32/Antivirus2008, occupies the fourteenth position. For more information about these threats, see "Rogue Security Software," beginning on page 92.

Some of the most prevalent threats from 1H08 receded in significance in 2H08. The trojan family Win32/Vundo fell slightly, going from second place in 1H08 to third in 2H08. Most notably, Win32/Zlob, which was the most prevalent family by far in 1H08, fell 58.2 percent to come in at second place behind Win32/Renos. Toward the end of 2008, the authors of Win32/Zlob released a variant that contained a hidden message announcing that they were "closing soon." If this message is accurate, Win32/Zlob may be expected to continue receding in prevalence over the coming periods.

Three families on the list—Win32/Taterf, Win32/Tilcun, and Win32/Lolyda—belong to a group of loosely related families that target players of online games and attempt to steal their login credentials. All three families increased in prevalence since 1H08. For more information, see "Online Gaming-Related Families," on page 62 of *Microsoft Security Intelligence Report, Volume 5 (January through June 2008)*.

ASX/Wimad, a detection for a category of malicious Windows Media files, was the eleventh most prevalent threat in 2H08, up 164.9 percent from 1H08. Certain Windows Media files can contain hyperlinks to be automatically opened in a Web browser when they are played. ASX/Wimad files include hyperlinks to executable files, often with names like PLAY_MP3.exe, that contain malicious payloads. Users may believe they have to run these files to access desired media content.

One family notable for its absence is Win32/Nuwar, which was used to control a botnet consisting of an estimated half million infected computers worldwide. The prevalence of Win32/Nuwar declined from almost 480,000 computers in 1H08 to just 68,453 in 2H08. Win32/Nuwar was added to the MSRT in September 2007 and has been removed from hundreds of thousands of computers since then. It is likely that the botnet operators have stopped maintaining it or have stopped attempting to increase its size.

Notably, none of the top families rely on exploits to spread, although some have been known to be distributed by downloaders that are sometimes installed using exploits. This is consistent with the observed trend in the malware ecosystem of attackers moving toward profit-oriented threats that rely largely on social engineering to propagate. (Nevertheless, the release of new threats, such as Win32/Conficker, serves as a reminder of the importance of installing new security updates in a timely manner.)

MSRT New Families in 2H08

The six monthly updates of the MSRT released in 2H08 included support for the detection and removal of eight additional malware families. The MSRT is not a substitute for a comprehensive, real-time antivirus product and does not detect every threat in the Microsoft antivirus signature database. The families chosen for inclusion in the MSRT are ones that Microsoft researchers believe are, or will be, prevalent enough to justify inclusion in the tool, which runs on hundreds of millions of computers around the world each month.

FIGURE 51. Malware families added to the MSRT in 2H08

New Family	Added in	Computers Cleaned by the MSRT in 2H08
Win32/Horst	July	235,318
Win32/Matcash	August	217,610
Win32/Slenfbot	September	598,178
Win32/Rustock	October	183,858
Win32/FakeSecSen	November	1,205,329
Win32/Gimmiv	November	N/A*
Win32/FakeXPA	December	460,931
Win32/Yektel	December	201,635

* A statistically insignificant number of Win32/Gimmiv infections were detected in 2H08.

Win32/Horst

Many free e-mail providers and other services have implemented CAPTCHA (an acronym for "Completely Automated Public Turing test to tell Computers and Humans Apart") as a mechanism for fighting automated account creation by spammers and other malicious people. CAPTCHAs require users to identify and type a series of distorted letters and numbers—a type of task that computers do poorly but humans do well.

Spammers have responded by releasing malware that aids in the process of circumventing CAPTCHA. The MSRT was first updated to deal with this kind of threat during 1H08, when Win32/Cutwail, Win32/Newacc, and Win32/Captiya were added to the tool. A fourth family, Win32/Horst, was added in July 2008. This family is typically delivered through an executable application that masquerades as an illegal software "crack" or key generator on the eDonkey P2P network. Win32/Horst consists of a number of different components that perform different tasks, but it is primarily designed to send spam through e-mail providers, such as Windows Live Hotmail®, Gmail, AOL, and Yahoo!. Win32/Horst opens e-mail accounts at these providers in bulk and transmits the CAPTCHA images to a server for solving. Although it is impossible to know for certain without access

Encyclopedia

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

Win32/Newacc: An attacker tool that automatically registers new e-mail accounts on Hotmail®, AOL, Gmail, Lycos and other account service providers, using a Web service to decode CAPTCHA protection.

Win32/Captiya: A trojan that transmits CAPTCHA images to a botnet, in what is believed to be an effort to improve the botnet's ability to detect characters and break CAPTCHAs more successfully.

http://www.microsoft.com/av

to the server, Microsoft researchers believe that these images are not being deciphered programmatically; rather, it is more likely that the authors of Win32/Horst employ human solvers to analyze the images and enter the correct strings, a technique often employed in parts of the world where labor is relatively inexpensive. For more information about Win32/Horst and other CAPTCHA threats, see the following posts from the MMPC blog (http://blogs.technet.com/mmpc):

- Horst: Something Old, Something New (August 1, 2008)
- MSRT on CAPTCHA Breaking Malware (August 8, 2008)

Win32/Matcash

Win32/Matcash was added to the MSRT in August 2008. Win32/Matcash is a multicomponent family of trojans that downloads and executes arbitrary files. Some variants of this family may install a toolbar. The toolbar is installed as a browser helper object (BHO), allowing the toolbar to run when the browser is launched. Some variants were associated with known malware distribution sites that were shut down in 2008. Win32/Matcash has been observed to use the Win32/Slenfbot worm as a means of distribution.

Win32/Slenfbot

The worm family Win32/Slenfbot was added to the MSRT in September 2008. Win32/Slenfbot is botnet software that monitors an Internet Relay Chat (IRC) channel for instructions, a mechanism that has been used by malware families, like Win32/Rbot and Win32/IRCbot, for several years. Win32/Slenfbot is notable for the large number of variants that have been detected and for the fact that its source code seems to be tightly controlled by its authors. Many families, such as Win32/Rbot, have source code that is shared among many different groups that produce their own versions with custom functionality, leading to variants that exhibit a mix of different features. With Win32/Slenfbot, by contrast, when a new feature is added, all subsequent variants have that feature, suggesting that all variants are being developed from a single evolving code base. Most changes are minor—different IRC servers and ports, different names for file and registry entries—but many new features have been added since Win32/Slenfbot was first classified as a family in October 2007.

Encyclopedia

Win32/Rbot: A family of backdoor trojans that allows attackers to control the computer through an IRC channel.

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

http://www.microsoft.com/av

Win32/Slenfbot spreads via MSN® Messenger, Windows Live Messenger, and removable drives. It puts a copy of itself inside a .zip archive and sends the .zip file to the victim's Messenger contacts using the Messenger file transfer feature. Parameters, such as the name of the .zip file and the message to use to lure the prospective victim into opening the file (usually things like "Have you ever see this picture I took of myself?"), are provided through IRC and can be updated on the fly by the bot-herders. Once installed, Win32/Slenfbot is used to download additional malware to victims' computers for purposes such as spamming, hosting malware or illegal content, and others.

Win32/Rustock

The rootkit family Win32/Rustock was added to the MSRT in October 2008. Win32/Rustock is a multi-component family of rootkit-enabled backdoor trojans, which were historically developed to aid in the distribution of spam. First discovered in early 2006, Win32/Rustock has evolved to become a prevalent and pervasive threat. Recent variants appear to be associated with rogue security programs.

Normally the trojan consists of three components that are embedded within each other—the dropper, which runs in user mode, the driver's installer, and the actual rootkit driver, both of which run in kernel mode. All of the trojan's components are encrypted, and the actual driver component is also packed with the aPLib compression library.

By the end of 2H08, the MSRT had removed Win32/Rustok from 183,858 infected computers, which is not a particularly large number relative to other families. Despite this, the Win32/Rustock family has been an effective spamming tool with a disproportionate effect on the threat landscape, which has warranted its inclusion in the MSRT.

Win32/Gimmiv

Win32/Gimmiv is a family of trojans that are sometimes installed by exploits of a vulnerability documented in Microsoft Security Bulletin MS08-067. It was added to the MSRT in November 2008. Win32/Gimmiv was the one of the first families of malware associated with the MS08-067 vulnerability that was discovered in the wild. Microsoft researchers were concerned about potential widespread exploitation of the vulnerability and added Win32/Gimmiv to the MSRT to gather any telemetry they could on the trojan's spread. As it happened, Win32/Gimmiv was only detected on a small number of computers in 2H08, although Win32/Conficker, another threat that exploited the MS08-067 vulnerability, subsequently appeared in November and December. For more information, see "MS08-067: Vulnerability in Windows Server Service," beginning on page 41.

Rogue Security Software: Win32/FakeSecSen, Win32/FakeXPA, and Win32/Yektel

Three families associated with rogue security software were added to the MSRT in 2H08—Win32/FakeSecSen, added in November 2008, and Win32/FakeXPA and Win32/Yektel, added in December 2008. Together, these three families accounted for nearly 2 million computers cleaned in 2H08. For more information, see "Rogue Security Software," beginning on page 92.

User Reaction to Alerts

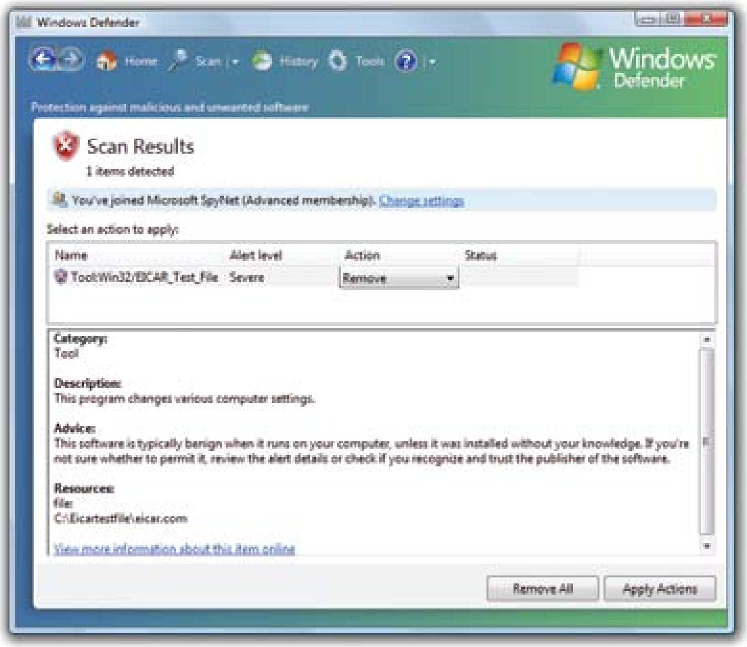
Software cannot always be classified in binary terms as "good" or "bad." Some software inhabits a gray area wherein the combination of behaviors and value propositions presented by the software is neither universally desired nor universally reviled. This gray area includes a number of programs that do 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 they 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.[18]

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.
- **Always Allow**. Ignores the alert from that point forward, even if the software is seen again.
- **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.

[18] 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.

FIGURE 52. A user action prompt from an on-demand scan in Windows Defender



Scan Results

1 items detected

You've joined Microsoft SpyNet (Advanced membership). Change settings

Select an action to apply:

Name	Alert level	Action	Status
Tool:Win32/EICAR_Test_File	Severe	Remove	

Category:
Tool

Description:
This program changes various computer settings.

Advice:
This software is typically benign when it runs on your computer, unless it was installed without your knowledge. If you're not sure whether to permit it, review the alert details or check if you recognize and trust the publisher of the software.

Resources:
file:
C:\Eicartestfile\eicar.com

View more information about this item online

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. **Always 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 53 and Figure 54 list the most-removed and least-removed families detected on at least 100,000 computers in 2H08, along with their alert level, default action, and the percentage of times users respond to a prompt by selecting a removal action (**Quarantine**, **Clean**, or **Remove**).

FIGURE 53. The 10 most-removed families detected on more than 100,000 computers, sorted by total percentage of removals and quarantines, 2H08

Family	Alert Level	Default Action	Total Removal	Ignore	Always Allow
Win32/Roron	Severe	Remove	100.0%	0.0%	0.0%
Win32/RJump	Severe	Remove	100.0%	0.0%	0.0%
Win32/Swif	Severe	Remove	100.0%	0.0%	0.0%
JS/Mult	Severe	Remove	100.0%	0.0%	0.0%
Win32/Lolyda	Severe	Remove	100.0%	0.0%	0.0%
Win32/Wukill	Severe	Remove	99.9%	0.1%	0.0%
JS/Objsnapt	Severe	Remove	99.9%	0.0%	0.1%
JS/Redirector	Severe	Remove	99.9%	0.0%	0.1%
JS/Xilos	Severe	Clean	99.9%	0.1%	0.0%
JS/Decdec	Severe	Remove	99.9%	0.1%	0.0%

Totals for each family may not equal 100 percent due to rounding.

FIGURE 54. The 10 least-removed families detected on more than 100,000 computers, sorted by total percentage of removals and quarantines, 2H08

Family	Alert Level	Default Action	Total Removal	Ignore	Always Allow
Win32/BearShare	Moderate	Select Action	4.1%	95.7%	0.2%
Win32/BitAccelerator	Moderate	Select Action	5.9%	93.9%	0.2%
Win32/Blubtool	Moderate	Select Action	6.9%	93.0%	0.0%
Win32/RServer	Low	Select Action	8.5%	86.0%	5.4%
Win32/UltraVNC	Moderate	Select Action	10.0%	82.6%	7.3%
Win32/GhostRadmin	Low	Select Action	11.3%	84.0%	4.7%
Win32/TightVNC	Moderate	Select Action	13.8%	81.8%	4.4%
Win32/DameWareMiniRemoteControl	Moderate	Select Action	14.7%	78.4%	6.9%
Win32/SeekmoSearchAssistant	Moderate	Select Action	14.9%	85.1%	0.0%
Win32/Nbar	Moderate	Select Action	14.9%	85.0%	0.0%

Totals for each family may not equal 100 percent due to rounding.

Users' reactions to warnings about these families varied significantly, indicating clearly that the alert level given influences users' decision-making process and that users perceive different families to have different value propositions.

- All of the most-frequently removed families had an alert level of Severe, indicating that the threat should be considered unambiguously malicious. By default, as noted above, threats rated Severe that are known to already exist on the system are removed automatically during scheduled scans, so in most cases users are not asked to make a decision about these families at all except when explicitly performing on-demand scans. In addition, the categories used to classify these families have names that are well-known to large segments of the computing public or have clear negative connotations—virus, worm, exploit, trojan.
- The least-frequently removed families all have alert levels of Moderate or Low, indicating less danger to the user. User reaction to these families was more varied and indicated differing perceptions of the value of the software.
  - The P2P file-sharing program Win32/BearShare, older versions of which were sometimes bundled with potentially unwanted software, has the lowest rate of removal among widespread families. The low rate of removal indicates that many users accept the value of the program and believe its benefits outweigh any specific behaviors that are unwanted by some.
  - Win32/RServer, Win32/UltraVNC, Win32/GhostRadmin, Win32/TightVNC, and Win32/DameWareMiniRemoteControl all have much higher **Always Allow** rates than the other families on the list. These are all programs that allow a computer to be controlled remotely, similar to Remote Desktop. They have a number of legitimate uses, but are considered potentially unwanted software because they can be used by an attacker with malicious intent to gain control of a user's computer under some circumstances. The high **Always Allow** rate for these programs indicates that many users are aware of the nature of the software and wish to retain it for its perceived value. Nonetheless, for each program an even higher percentage chose to **Remove** or **Quarantine** the software immediately, presumably indicating that they did not intentionally install the software or did not want it anymore. Most of the rest chose **Ignore**; reasons for this are harder to definitively guess, as stated above.
  - Some of the other software with low rates of removal include value propositions of some kind in exchange for the potentially unwanted behavior. For example, Win32/BitAccelerator and Win32/SeekmoSearchAssistant offer functionality, such as a download manager or Web search help, in exchange for showing advertisements.

Encyclopedia

Win32/BearShare: A P2P file-sharing client that uses the decentralized Gnutella network. Free versions of BearShare have come bundled with advertising-supported and other potentially unwanted software.

Win32/RServer: Commercial remote administration software that can be used to control a computer. These programs are typically installed by the computer owner or administrator and should only be removed if unexpected.

Win32/UltraVNC: A remote access program that can be used to control a computer. This program is typically installed by the computer owner or administrator, and should only be removed if unexpected.

Win32/GhostRadmin: A remote administration tool that can be used to control a computer. These programs are typically installed by the computer owner or administrator and should only be removed if unexpected.

Win32/TightVNC: A remote control program that allows full control of the computer. These programs are typically installed by the computer owner or administrator and should only be removed if unexpected.

Win32/DameWareMini RemoteControl: A detection that is triggered by modified (that is, edited and re-packed) remote control programs based on DameWare Mini Remote Control, a commercial software product.

Win32/BitAccelerator: A program that redirects Web search results to other Web sites and may display various advertisements to users while browsing Web sites.

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

http://www.microsoft.com/av

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 95 million malicious samples were detected in the wild in 2H08, which is more than half a million new, unique malicious files each day. Figure 55 lists the number of unique files detected in each category of threat by Microsoft security products in 2H08, not including damaged or corrupted samples. (Malware often creates corrupted samples when replicating. These samples cannot affect users and are therefore not counted when analyzing samples.)

FIGURE 55. Unique samples by category, 2H08

Category	Unique Files
Viruses	62,785,358
Miscellaneous Trojans	16,638,333
Trojan Downloaders & Droppers	5,511,400
Miscellaneous Potentially Unwanted Software	3,332,059
Worms	2,391,722
Adware	1,422,480
Password Stealers & Monitoring Tools	1,287,106
Exploits	869,023
Backdoors	631,520
Spyware	116,966

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.

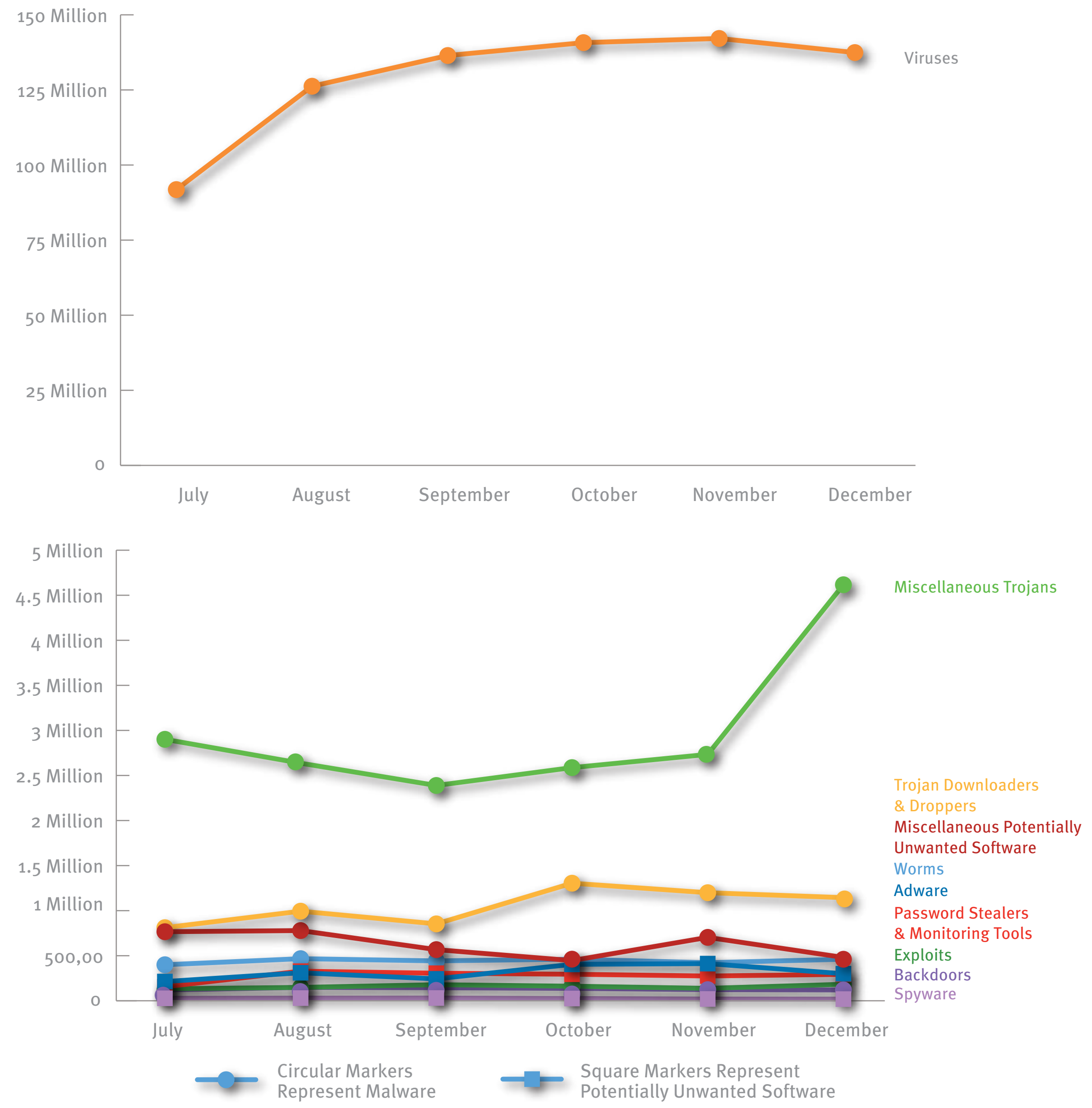
Another factor that tends to inflate the sample count for certain families is polymorphism, which results in the automatic creation of large numbers of unique (but functionally identical) files as part of the malware replication process. There are two general types of polymorphism that affect sample 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 56 shows the month-to-month trends for 2H08.

FIGURE 56. Unique files detected each month by category in 2Ho8



The sharp increase in trojan variants detected in December is due to the spread of a few prevalent families late in the year, notably the rogue security software family Win32/FakeXPA, which was added to the MSRT in December. Unlike some other rogue security software families, Win32/FakeXPA is polymorphic, so it contributes a large number of variants to the total.

Viruses and Miscellaneous Trojans excepted, the number of samples per category was relatively stable from month to month. Comparing this chart to Figure 48 on page 72 shows that, of the four most prevalent categories, Miscellaneous Trojans and Trojan Downloaders & Droppers both have relatively large numbers of samples, while Miscellaneous Potentially Unwanted Software and Adware have relatively few. This is because potentially unwanted software programs are often, though not always, installed intentionally by users because they believe they will benefit from them. These programs are therefore less likely to spawn numerous variants in an effort to avoid detection, as malware families often do.

Top Families by Month

Figure 57 shows the monthly sample counts for the families with the most samples in 2H08. Most of the top families are either viruses or polymorphic threats, for the reasons explained earlier. The virus families Win32/Parite and Win32/Virut had the highest number of samples by a significant margin, each of which had several times as many samples as any other family.

FIGURE 57. Families with the most unique samples by month in 2H08

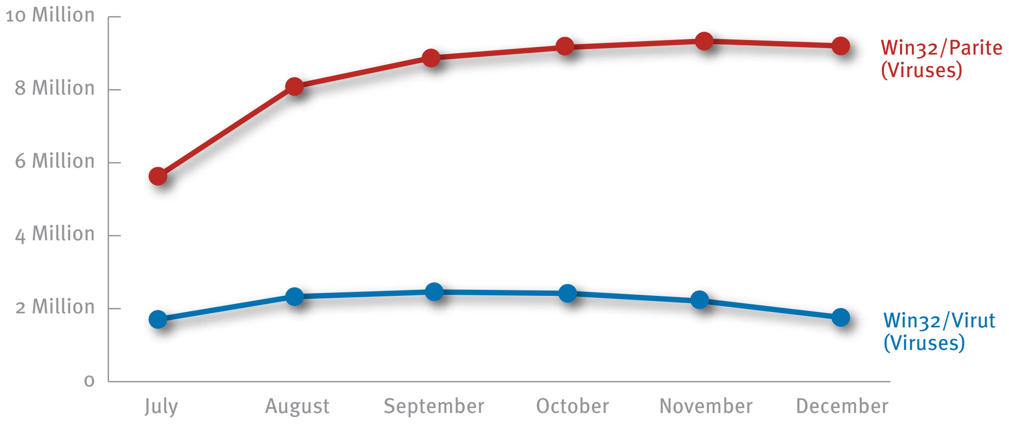
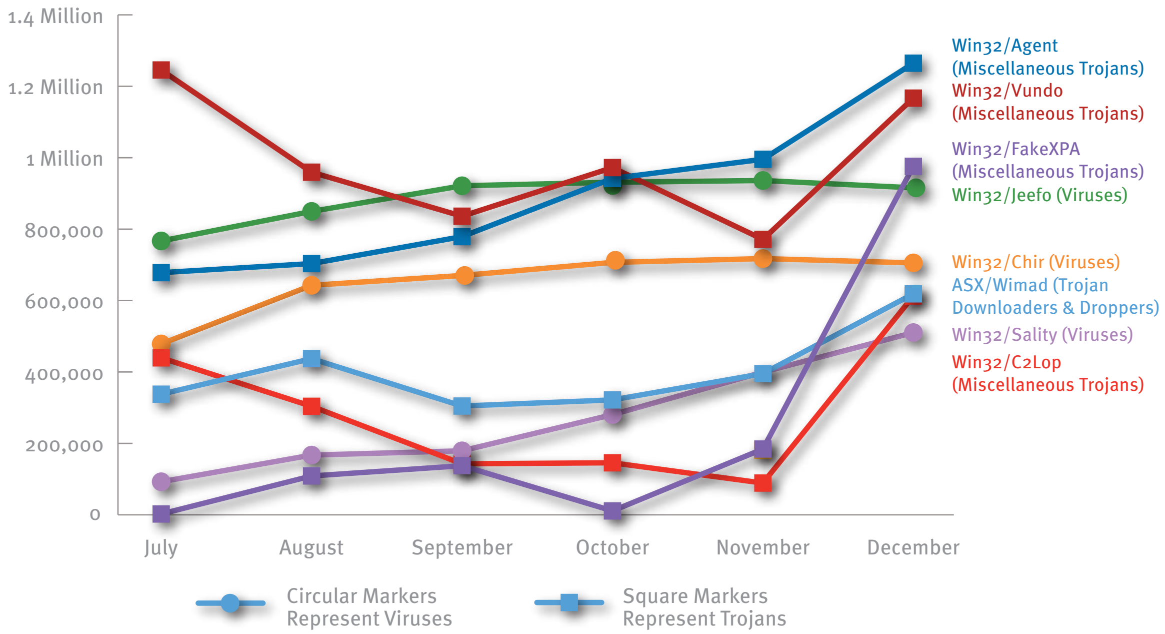


FIGURE 57. Continued



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.

Focus: The Threat Landscape 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.

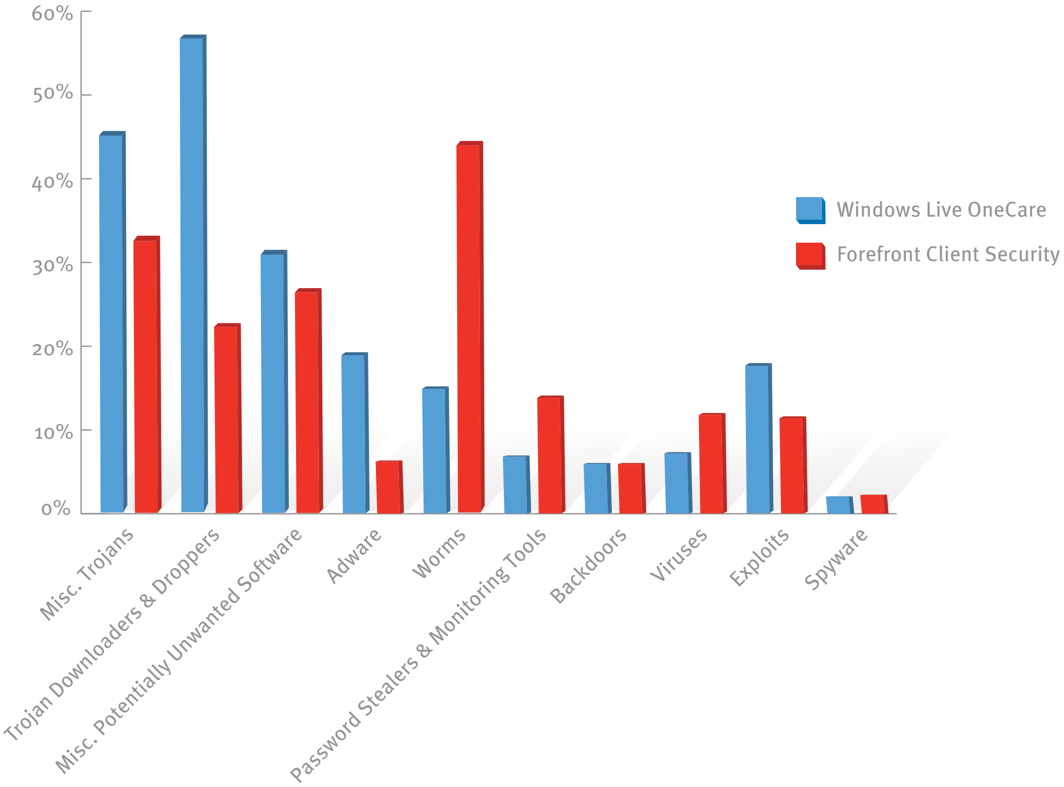
Microsoft currently offers two products that provide real-time protection against malware and potentially unwanted software: Windows Live OneCare,[19] which is intended for home use, and Microsoft Forefront Client Security, which is intended for enterprise environments. Both of these products use the Microsoft Malware Protection Engine and a common

[19] In 2009, Microsoft will discontinue retail sales of Windows Live OneCare and will offer a new, streamlined anti-malware solution, code-named “Morro,” at no charge to licensed users of Windows. See http://www.microsoft.com/Presspass/press/2008/nov08/11-18NoCostSecurityPR.mspx for details.

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.

Figure 58 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 2H08, 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 58. Family categories detected by Windows Live OneCare and Forefront Client Security, by percentage of the total number of infected computers cleaned by each program, in 2H08



As Figure 58 shows, computers running Forefront Client Security 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, downloaders and droppers, adware, and exploits. Similar percentages of backdoors and spyware were detected by both products.

As Figure 59 and Figure 60 show, the top families encountered by Windows Live OneCare and Forefront Client Security were also very different.

FIGURE 59. Top 10 families detected on infected computers by Windows Live OneCare, by percentage of computers cleaned, in 2H08

Windows Live OneCare Top 10 Families	Most Significant Category	Percent
ASX/Wimad	Trojan Downloaders & Droppers	30.9%
Win32/Agent	Miscellaneous Trojans	19.1%
Win32/Renos	Miscellaneous Trojans	13.2%
Win32/Zlob	Miscellaneous Trojans	12.5%
Win32/Vundo	Miscellaneous Trojans	8.8%
Win32/Obfuscator	Misc. Potentially Unwanted Software	6.5%
Win32/ZangoSearchAssistant	Misc. Potentially Unwanted Software	5.5%
Java/ByteVerify	Exploits	5.3%
Win32/FakeXPA	Miscellaneous Trojans	5.1%
Win32/Antivirus2008	Miscellaneous Trojans	5.1%

FIGURE 60. Top 10 families detected on infected computers by Forefront Client Security, by percentage of computers cleaned, in 2H08

Forefront Client Security Top Families	Most Significant Category	Percent
Win32/Autorun	Worms	17.7%
Win32/Hamweq	Worms	17.2%
Win32/Agent	Miscellaneous Trojans	14.7%
Win32/Taterf	Worms	9.9%
Win32/Frethog	Password Stealers & Monitoring Tools	9.4%
Win32/RealVNC	Password Stealers & Monitoring Tools	4.9%
Win32/VB	Trojan Downloaders & Droppers	4.1%
JS/Redirector	Miscellaneous Trojans	3.9%
Win32/Obfuscator	Misc. Potentially Unwanted Software	3.6%
Win32/Brontok	Worms	3.4%

The family 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. The use of home computers for media purposes also explains the prevalence of Win32/Zlob, a trojan that masquerades as a missing codec needed to play video files, often on adult sites. The Windows Live OneCare list also includes several families associated with rogue security software, such as Win32/Renos, Win32/FakeXPA, and Win32/Antivirus2008. 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. For more information, see "Rogue Security Software," beginning on page 92.

By contrast, the Forefront Client Security list is dominated by worms, like Win32/Autorun, Win32/Hamweq, and Win32/Taterf. Worms rely less on social engineering to spread than categories like trojans and downloaders do, does and more on access to unsecured file shares and removable storage volumes, both of which are often plentiful in enterprise environments. Win32/Taterf (along with the related family Win32/Frethog) is an interesting case. It targets massively multiplayer online role-playing games (MMORPGs), 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. The only entries common to both lists are Win32/Agent and Win32/Obfuscator, both of which are actually generic detections that find and remove groups of similar threats.

Encyclopedia

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

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

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

Win32/Obfuscator: A detection for programs that use a combination of obfuscation techniques to hinder analysis or detection by antivirus scanners.

http://www.microsoft.com/av

Rogue Security Software

One of the clearest trends in the telemetric data examined in this report has been a dramatic rise in the prevalence of rogue security software programs. 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. Typically, a rogue security program displays false or misleading alerts about infections or vulnerabilities on the victim's computer and offers to fix the supposed problems for a price. Rogue security software has been around for years[20] but, in recent months, has become a major part of the worldwide threat landscape, with old families exploiting new ways of distribution and new families appearing occasionally. Rogue security software generates hundreds of thousands of U.S. dollars a year in ill-gotten profits for its distributors, along with large numbers of IT help desk calls from worried victims.

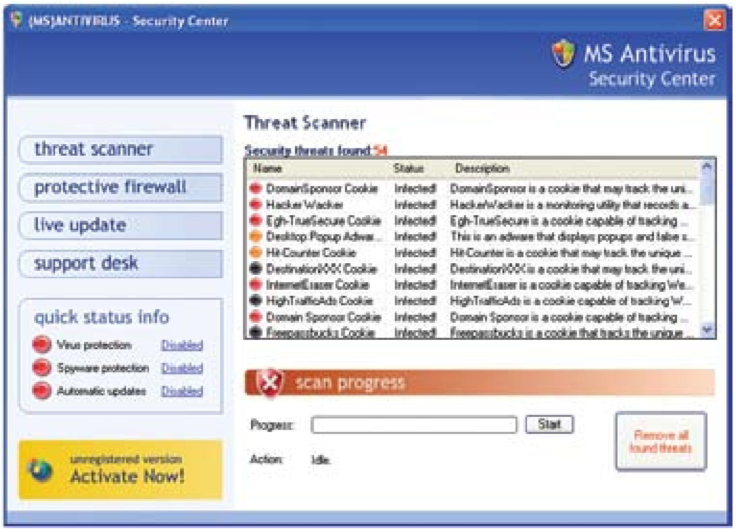
[20] See *Microsoft Security Intelligence Report, Volume 2 (July through December 2006)* for an earlier look at rogue security software.

Profiting from Fear and Trust

Rogue security software uses two primary tactics to lure potential victims—fear and annoyance. The programs are designed to convince victims to pay for the "full versions" of the software to remove and protect themselves from malware or to stop the continual alerts and warnings—or both. Rogue security software families observed in 2H08 have displayed more aggressive behavior on both fronts than earlier versions.

Legitimate antivirus and antispyware programs have familiar, relatively consistent user interfaces and behaviors that have evolved over a number of years and that users tend to trust. Rogue security software authors have long attempted to exploit this trust by giving their programs generic, anodyne names, like "Antivirus 2009," and making them resemble genuine security software in many ways. Recently, many threats have taken this approach a step further, posing as components of the operating system itself or as a familiar search engine. One of the first families observed to exhibit this behavior was Win32/FakeSecSen, which was added to the MSRT in November 2008 and was the eighth most prevalent family in 2H08 overall. Win32/FakeSecSen adds an icon to the Control Panel named **Vista AV** or **MS AV** and fraudulently uses the same four-color shield icon as the Windows Security Center. Double-clicking the icon launches the rogue software, which claims to detect a large number of nonexistent threats and urges the user to "activate" the software by paying for it.

FIGURE 61. The Win32/FakeSecSen user interface, showing nonexistent infections



Threat Scanner

Security threats found 54

Name	Status	Description
DomainSponsor Cookie	Infected!	DomainSponsor is a cookie that may track the uni...
Hacker Wacker	Infected!	HackerWacker is a monitoring utility that records a...
Egh-TrueSecure Cookie	Infected!	Egh-TrueSecure is a cookie capable of tracking ...
Desktop Popup Adwar...	Infected!	This is an adware that displays popups and false s...
HitCounter Cookie	Infected!	HitCounter is a cookie that may track the unique ...
DestinationXXX Cookie	Infected!	DestinationXXX is a cookie that may track the uni...
InternetEraser Cookie	Infected!	InternetEraser is a cookie capable of tracking We...
HighTrafficAds Cookie	Infected!	HighTrafficAds is a cookie capable of tracking W...
Domain Sponsor Cookie	Infected!	Domain Sponsor is a cookie capable of tracking ...
Freepaysbucks Cookie	Infected!	Freepaysbucks is a cookie that tracks the unique ...

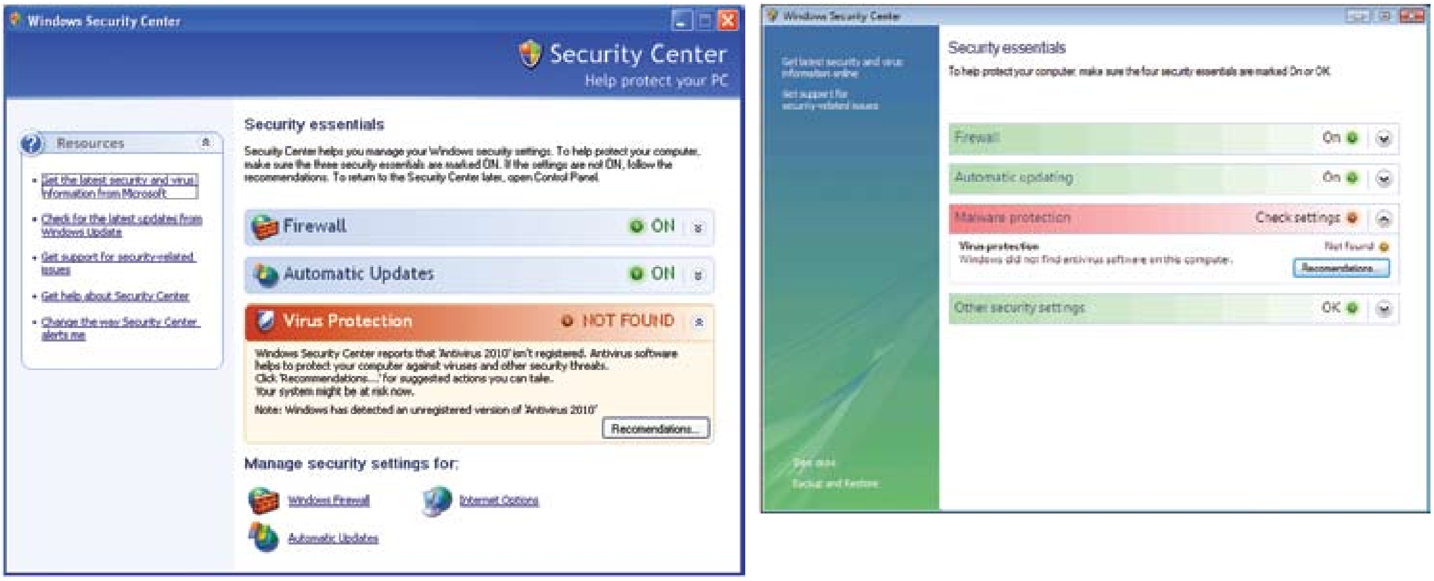
Virus protection	Disabled
Spyware protection	Disabled
Automatic updates	Disabled

Progress:

Action: Idle.

Other rogue security software families, like Win32/FakeXPA, have followed a similar model, displaying variations on the Windows Security Center that are all designed to mislead users into believing that they are not adequately protected from malware.

FIGURE 62. Win32/FakeXPA uses an interface that closely resembles the Windows Security Center on the operating system on which it is running (Windows XP, left, or Windows Vista, right)



Windows Security Center

Security Center
Help protect your PC

Resources

- Get the latest security and virus information from Microsoft
- Check for the latest updates from Windows Update
- Get support for security-related issues
- Get help about Security Center
- Change the way Security Center alerts me

Security essentials

Security Center helps you manage your Windows security settings. To help protect your computer, make sure the three security essentials are marked ON. If the settings are not ON, follow the recommendations. To return to the Security Center later, open Control Panel.

Firewall ● ON

Automatic Updates ● ON

Virus Protection ● NOT FOUND

Windows Security Center reports that 'Antivirus 2010' isn't registered. Antivirus software helps to protect your computer against viruses and other security threats.
Click 'Recommendations...' for suggested actions you can take.
Your system might be at risk now.

Note: Windows has detected an unregistered version of 'Antivirus 2010'

Recomendations...

Manage security settings for:

Windows Firewall
Internet Options
Automatic Updates

Windows Security Center

Get latest security and virus information online
Get support for security-related issues

Security essentials

To help protect your computer, make sure the four security essentials are marked On or OK.

Firewall On ●

Automatic updating On ●

Malware protection Check settings ●

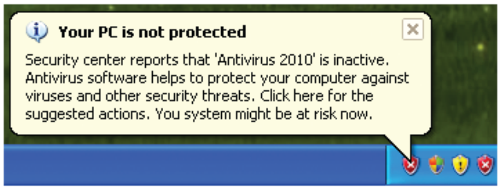
Virus protection Not found ●
Windows did not find antivirus software on this computer.
Recomendations...

Other security settings OK ●

See also
Backup and Restore

Clicking the **Recommendations** button or any of the links in the fake Security Center opens a registration dialog box, which includes a button the user can click to purchase a "license" for the software. Failing to "register" causes Win32/FakeXPA to display repeated alert messages in the notification area.

FIGURE 63. A fake warning message from Win32/FakeXPA

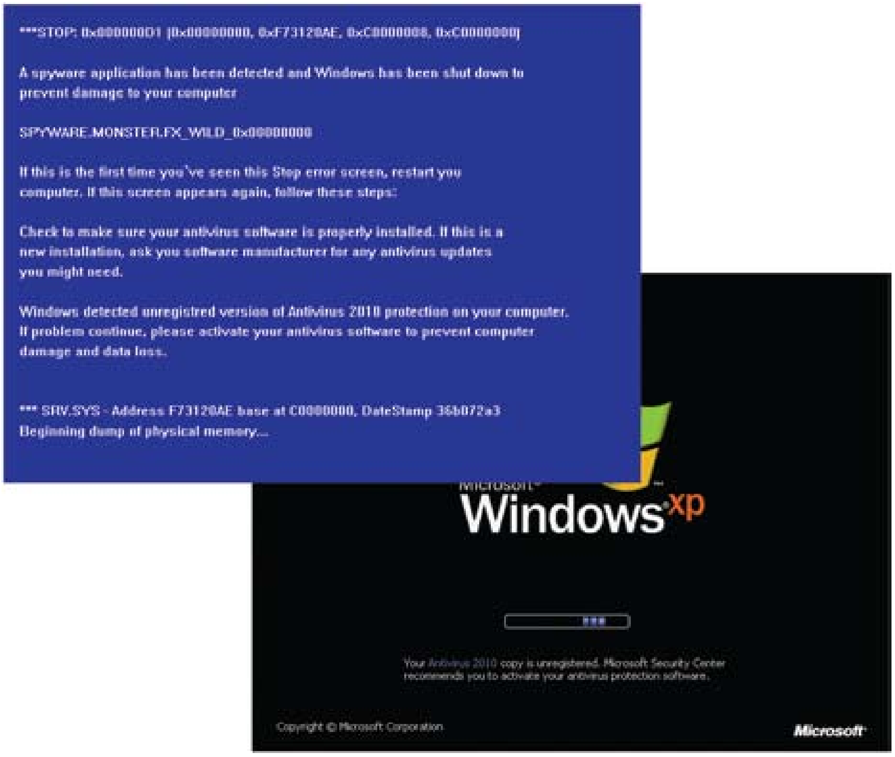


Your PC is not protected

Security center reports that 'Antivirus 2010' is inactive. Antivirus software helps to protect your computer against viruses and other security threats. Click here for the suggested actions. You system might be at risk now.

Some variants of Win32/FakeXPA even display fake “blue screen” error messages, claiming that the system has crashed and that “Windows detected unregistered version of Antivirus 2010 protection on your computer.” The error message is followed by an animation simulating the computer’s restart process, displaying another “Microsoft Security Center” message on the fake startup screen.

FIGURE 64. Bogus “blue screen” and startup screens displayed by Win32/FakeXPA



```
***STOP: 0x000000D1 (0x00000000, 0xF73120AE, 0xC0000008, 0xC0000000)

A spyware application has been detected and Windows has been shut down to
prevent damage to your computer

SPYWARE.MONSTER.FX_WILD_0x00000000

If this is the first time you've seen this Stop error screen, restart you
computer. If this screen appears again, follow these steps:

Check to make sure your antivirus software is properly installed. If this is a
new installation, ask you software manufacturer for any antivirus updates
you might need.

Windows detected unregistred version of Antivirus 2010 protection on your computer.
If problem continue, please activate your antivirus software to prevent computer
damage and data loss.


*** SRV.SYS - Address F73120AE base at C0000000, DateStamp 36b072a3
Beginning dump of physical memory...
```

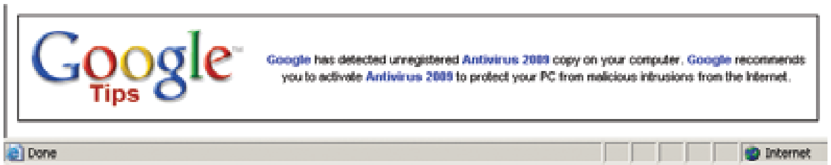
Your Antivirus 2010 copy is unregistered. Microsoft Security Center recommends you to activate your antivirus protection software.

Copyright © Microsoft Corporation

Some variants of Win32/FakeXPA download a trojan called Win32/Yektel, which installs a browser helper object (BHO) that displays warning messages using the Internet Explorer Information bar. The Win32/Yektel BHO also randomly redirects Internet Explorer to a bogus warning page that purports to be from Internet Explorer itself.

As a BHO, Win32/Yektel can also add content to Web pages after Internet Explorer has retrieved them. Late in 2008, Win32/Yektel variants started adding a message to Web pages whenever the page's URL contained the string "google" in it. The message, which purports to be a warning from the Google search engine, urges the user to register the rogue security software for protection.

FIGURE 65. A fake Google warning message created by Win32/Yektel



Google has detected unregistered Antivirus 2009 copy on your computer. Google recommends you to activate Antivirus 2009 to protect your PC from malicious intrusions from the Internet.

Profiting from Annoyance

On the whole, rogue security software families have continued to add more and more intrusive features, like pop-up windows, in an attempt to annoy the user into paying to make them go away. Win32/FakeSecSen, discussed on page 93, displays a "scanner" window that floats above all other windows, and often its **Close** button does nothing at all.

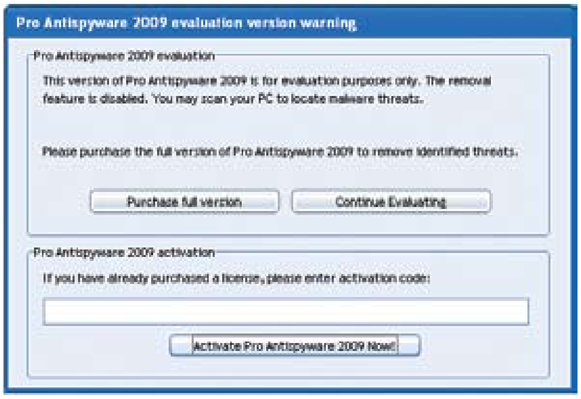
Win32/WinSpywareProtect displays a dialog box to ask the user whether to clean the computer. If the user chooses **No**, it displays another dialog box asking if the user is sure. To dismiss the messages, the user must answer **No** to the first message and then **Yes** to the second one. Any other choice displays a "registration" dialog box urging the user to purchase the software.

Encyclopedia

Win32/WinSpywareProtect: A rogue security software family that may falsely claim that the user's computer is infected and encourages the user to buy a product for cleaning the alleged malware from the computer.

http://www.microsoft.com/av

FIGURE 66. A "registration" dialog box from Win32/WinSpywareProtect



Pro Antispyware 2009 evaluation version warning
Pro Antispyware 2009 evaluation

This version of Pro Antispyware 2009 is for evaluation purposes only. The removal feature is disabled. You may scan your PC to locate malware threats.

Please purchase the full version of Pro Antispyware 2009 to remove identified threats.

Purchase full version
Continue Evaluating
Pro Antispyware 2009 activation

If you have already purchased a license, please enter activation code:

Activate Pro Antispyware 2009 Now!

Win32/WinSpywareProtect also continually shows alerts that slide in from the right side of the screen and others that appear in the center of the screen. These alerts float above any other windows on the screen, and they cannot be closed or minimized, which means that the user can only dismiss them by interacting with the program itself.

Prevalence and Propagation

Figure 50, on page 77, which lists the top 25 families detected on computers worldwide in 2H08, clearly demonstrates the extent to which rogue security software families have become a major part of the threat landscape. Win32/FakeXPA and Win32/FakeSecSen, two of the families discussed in this section, appear in seventh and eighth place on the list respectively. Both families first appeared in 2H08, the only two families in the top 10 to do so, and each one was detected on more than 1.5 million computers. Win32/Antivirus2008, a more general family that includes several different variants, is fourteenth on the list. It was detected on more than 1 million computers in 2H08.

But it may be Win32/Renos, the most prevalent family worldwide in 2H08, that best demonstrates how the rogue threat has grown. Win32/Renos is a broadly defined family that downloads rogue security software. Some variants display fake infection warnings of their own before downloading a rogue scanner to “clean” the infections; others simply install the rogue security software themselves silently. Win32/Renos was detected on 4.4 million distinct computers in 2H08, 15.9 percent more than the second most prevalent family, Win32/Zlob (which itself displays out-of-context advertisements for rogue security software).

Win32/Renos variants are distributed in many different ways. Spam is one common delivery mechanism. In 2H08, for example, Win32/Renos was commonly distributed through spam messages that purported to link to explicit videos of celebrities. Some spam messages link directly to Win32/Renos binaries; others link to Web pages that display messages indicating that the user is missing a required video codec or needs to obtain an updated version of the Adobe Flash Player. The link provided for the download typically points to a trojan downloader, such as Win32/Cbeplay, which downloads Win32/Renos after being installed.

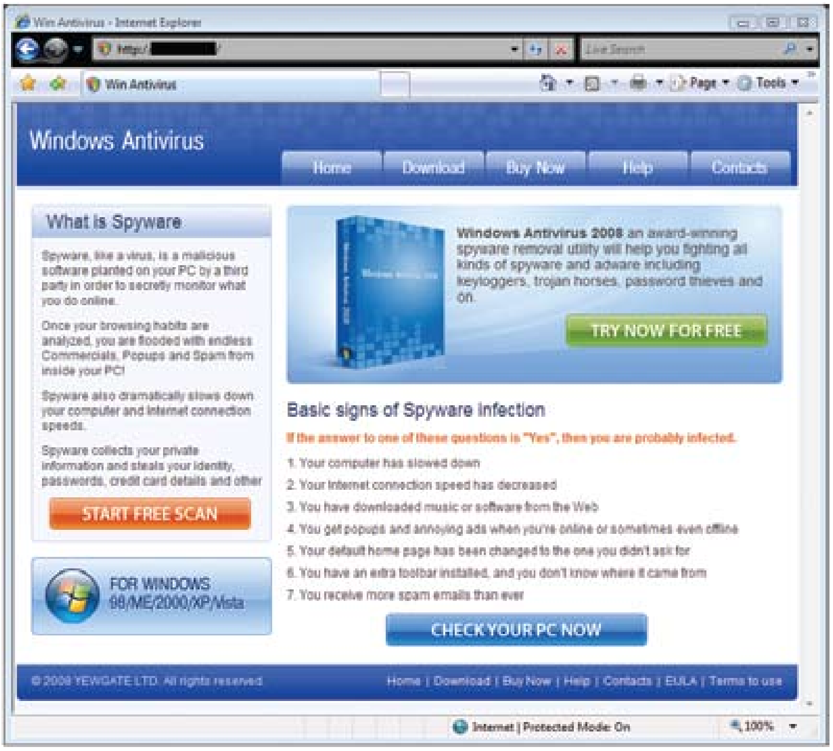
In addition to using traditional malware distribution channels, rogue security programs usually have other ways of distributing themselves. Most rogue security software families have their own Web pages that market the programs as if they were legitimate security products. These sites, which often have a professional appearance, sometimes fraudulently display the names and trademarks of reputable publications and security analysts, falsely claiming to have received awards or positive reviews from them. The sites usually include a link to a “trial” copy of the program and a link to purchase a license.

Encyclopedia

Win32/Cbeplay: A trojan that may upload computer operating system details to a remote Web site, download additional malware, and terminate debugging utilities.

http://www.microsoft.com/av

FIGURE 67. An example of a Web site advertising Win32/FakeSecSen


Win Antivirus - Internet Explorer
http://[redacted]/
Live Search
Win Antivirus
Page
Tools
Home
Download
Buy Now
Help
Contacts
TRY NOW FOR FREE
START FREE SCAN
FOR WINDOWS 98/ME/2000/XP/Vista
CHECK YOUR PC NOW
Home | Download | Buy Now | Help | Contacts | EULA | Terms to use
Internet | Protected Mode: On
100%

Windows Antivirus

What is Spyware

Spyware, like a virus, is a malicious software planted on your PC by a third party in order to secretly monitor what you do online.

Once your browsing habits are analyzed, you are flooded with endless Commercials, Popups and Spam from inside your PC!

Spyware also dramatically slows down your computer and Internet connection speeds.

Spyware collects your private information and steals your identity, passwords, credit card details and other

Windows Antivirus 2008 an award-winning spyware removal utility will help you fighting all kinds of spyware and adware including keyloggers, trojan horses, password thieves and on.

Basic signs of Spyware Infection

If the answer to one of these questions is "Yes", then you are probably infected.

1. Your computer has slowed down
2. Your Internet connection speed has decreased
3. You have downloaded music or software from the Web
4. You get popups and annoying ads when you're online or sometimes even offline
5. Your default home page has been changed to the one you didn't ask for
6. You have an extra toolbar installed, and you don't know where it came from
7. You receive more spam emails than ever

© 2008 YEWGATE LTD. All rights reserved.

Another common mechanism is a fake online scanner. Win32/InternetAntivirus, for example, uses standard HTML and JavaScript to display a Web page that closely resembles the Windows XP **My Computer** window and bogus scanning messages that resemble the Windows Defender user interface.

Of course, these Web pages are only useful if people can be lured to them. Rogue security software authors use several methods to accomplish this, often involving spam and other malware. In 2008, users were lured to the Web site for Win32/FakeXPA through the use of two less-common techniques. One technique uses Adobe Flash Player to replace the contents of the system clipboard with a link to a page that would eventually redirect to the program's Web page, a trick that could be accomplished through the use of Flash content in banner ads appearing on legitimate Web pages. This could lead to users pasting the malicious link into a browser's address bar or pasting it into an e-mail message and sending it to friends or colleagues, for example.

A second technique involves compromising legitimate Web sites and creating rules to redirect visitors from the legitimate Web site to the rogue security program's site, if the HTTP referrer field indicates that the user followed a link from a search engine, such as Live Search, Google, Yahoo!, or AOL. Because most Web site operators tend to visit their own sites directly instead of following links to it from search engines, the operators of a

Encyclopedia

Win32/InternetAntivirus: A program that displays false and misleading malware alerts to convince users to purchase rogue security software. This program also displays a fake "Windows Security Center" message.

http://www.microsoft.com/av

compromised site are unlikely to discover that their sites are compromised unless they encounter the malicious configuration instruction itself during site maintenance or receive reports from site users.

Visitors to the compromised site are usually redirected through several different sites before loading the Win32/FakeXPA Web page. As with Win32/InternetAntivirus, this page shows a series of pop-up windows and pretends to scan the computer, invariably claiming to find something malicious.

Legal Action Against Rogues

Microsoft Internet Safety Enforcement Team

Broadly speaking, rogue security software is deceptive software that is installed *without a person's informed consent*. Microsoft has responded to the increasing threat posed by rogue security software both by implementing technical countermeasures and by developing a strategy to send a strong deterrent message to the people who produce and sell the software.

The Internet Safety Enforcement Team (ISET), a group within the Microsoft Legal and Corporate Affairs (LCA) department, has long advocated using private legal causes of action as a tool to combat online malfeasance and has used such methods against spammers with a fair amount of success, by partnering with government, law enforcement, and industry partners worldwide. When the threat of rogue security software emerged, ISET reached out to this same group of partners to begin developing a statutory framework upon which to base an effective civil enforcement program and to promote awareness of the rogue security software threat among consumers.

Creating the Groundwork for Action

Microsoft has worked extensively with the Office of the Attorney General in Washington State (United States), where the company is headquartered, to update state law to address the threat of Internet-based crime and to bring computer criminals who victimize Washington State citizens to justice. The State of Washington has been a pioneer and a model for other states in many areas of computer crime legislation and, since attackers typically cast a wide net when luring potential victims, this has proven to be an effective strategy for combating even those criminals who reside far outside the state's borders. Microsoft has also worked with lawmakers in other jurisdictions to get effective computer crime legislation passed.

In 2005, the Washington State Legislature unanimously passed the Computer Spyware Act, which prohibited installing software onto a computer when the owner refused to allow the installation or when intentional misrepresentations were made concerning the extent to which such software was required for security or privacy. Within two months of the act's passage, ISET referred a case to the Attorney General's Office for investigation, resulting in a 16-count lawsuit against Secure Computer, LLC, and several principals in connection with the distribution of a product named "Spyware Cleaner."[21] Over the next several years, Microsoft worked with Washington State Attorney General Rob McKenna and the U.S. Federal Trade Commission (FTC) on a number of high-profile civil actions against distributors of rogue software and other threats.

The media coverage that naturally flows from the filing of such lawsuits is an integral component of the strategy of using the judicial process to address the rogue security software threat. The attention garnered by such lawsuits helps counter the threat in many ways. Press coverage brings the discussion of rogue security software from technical journals with limited circulation into the mainstream media, where it is more visible to those who are actually being targeted by attackers. This byproduct of the judicial process cannot be underestimated. Whereas the best executed public service announcement may be overlooked among the vast number of advertisements placed before consumers every day, information in the form of a news report often carries with it a higher rate of retention in the minds of consumers. Ultimately, consumers who are informed of the threat are in a better position to identify rogue security software on their own computers or in advertisements on Web pages and in e-mail and to thereby avoid being victimized themselves.

Government and law enforcement benefit from such news coverage, as well. As with malware and other computer-based crimes, attackers constantly change their methods and techniques in an effort to defeat the technical countermeasures developed to stop them. This constant cat-and-mouse game between those seeking a technical solution and those determined to circumvent such efforts moves at a pace that the legal and legislative process have historically been unable to match. It is here that public-private partnerships prove invaluable in their ability to effectively impact public policy. For example, after the Washington Spyware Act was passed in July 2005, attackers began using the Windows Messenger Service to deliver advertisements for rogue security software. (The Messenger Service, which should not be confused with the instant messaging (IM) programs Windows Messenger and Windows Live Messenger, is a component of some versions of Microsoft Windows and was designed to enable system administrators to broadcast important messages to users. Frequently abused by spammers, the service is disabled by default in Windows XP Service Packs 2 and SP3, and it is not included in Windows Vista or in Windows Server 2008.) In a typical case, attackers use the Messenger Service to display a dialog box on a user's screen warning of a "critical error" on the computer. The message, which appears to originate from the operating system itself, directs the user to visit a Web site selling rogue security software.

ISET quickly communicated the details of this new technique to Microsoft public partners, including the Washington State Office of the Attorney General. Due in part to these efforts, the Attorney General asked the legislature to amend Washington's Spyware Act to address the issue identified by Microsoft regarding Messenger Service fraud, in addition

[21] For more information, see http://www.atg.wa.gov/pressrelease.aspx?&id=5926.

to other potential loopholes that attackers might take advantage of. The amended act was filed on March 19, 2008, and it became effective on June 12 of the same year. In addition to the changes described here, the amended act includes a provision that makes it illegal to deceptively misrepresent the source of a message to a computer user to induce the user to install software. These changes have given Microsoft and the Attorney General's Office new powers to fight rogue security software distributors and other computer criminals.

Legal Actions in 2H08

On September 29, 2008, the Washington State Attorney General and Microsoft held a joint press conference wherein the parties announced several cases filed against rogue security software peddlers. A total of eight cases were filed by both Microsoft and the Attorney General.

In two of its cases, Microsoft amended a previously filed complaint to name defendants. These two cases began as "John Doe" cases filed in February 2008 and were amended to reflect the identification of the defendants responsible behind the bogus software sales. Their identities were determined through the use of the civil discovery process. In one case, the defendant was identified as a Michigan resident, with companies in Michigan and Florida. The other case named a Delaware corporation as the defendant. The remaining five cases filed by Microsoft were new filings that were filed as John Doe matters. The cases filed by Microsoft named the following persons and/or entities as defendants:[22]

- **Scan & Repair Utilities**. Case # 08-2-06494-8 SEA. This case was about a software application that purported to detect and remove malware from a person's computer. Although the application itself did not appear to return false positives, it was promoted through deceptive spam distributed through the Skype network and through a fake Web page. The software was aggressively promoted online, even garnering a good review from a CNET editor, which was later retracted. The discovery process established that the entity behind the distribution of the bogus software was SMP SOFT, LLC, a Delaware corporation.
- **Registry Update**. Case # 08-2-33486-4 SEA. This case involved the misuse of a network-based notification service to cause repeated, alarming pop-up messages to be displayed on Internet-connected computers. Despite having no knowledge of the state of the user's computer, the defendant broadcast pop-up messages that inaccurately warned of "system registry corruption" and that "Windows has found 55 critical system errors." The message then urged users to visit one of several Web pages to download a software called "Registry Update," which would allegedly correct the problems. Through the use of the civil discovery process, it was established that Barry Williams, a resident of Michigan, and two of his wholly owned companies (Inux, Ltd, and AW Telecom) were behind the fraud.

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

- **Antivirus 2009**. Case # 08-2-33372-8-9 SEA. This was a John Doe case filed to determine the identity of the parties behind the rogue security software program called Antivirus 2009. The bogus product would purportedly perform a scan of a user's computer, after which it would detect malware and other programs that could compromise a user's privacy. At the end of the fake scan, a pop-up advertisement with the title "Microsoft Security Warning" appears, directing users to visit a Web site selling the fake software.
- **Win32/WinSpywareProtect**. Case # 08-2-33380-9 SEA. This was a John Doe case filed to determine the identity of the party behind another rogue security program that allegedly performed a scan of a user's computer and identified a number of malware infections. Once the fake scan was completed, a pop-up message appeared that directed users to a Web page to purchase and download a software product to address the nonexistent issues.
- **XPdefender.com**. Case # 08-2-33382-5 SEA. This was a John Doe case seeking to identify those behind the XPdefender.com rogue security software, which misrepresented the need for virus protection due to vulnerabilities on a user's computer. As with similar frauds, the user would receive a pop-up message through the Messaging Service feature, directing the user to a Web page selling the software.
- **MalwareCore**. Case # 08-2-33375-2 SEA. This was another John Doe case seeking to track down the source of rogue security software that used fake scans and pop-up messages to convince consumers to buy bogus software products.
- **WinDefender 2008**. Case # 08-2-33377-9 SEA. This was a John Doe case filed to determine the identities of the parties involved in the distribution of a fake software product sold to remedy non-existent vulnerabilities in a user's computer. As with similar cases, WinDefender 2008 would alert users with a pop-up message, after which it would direct the users to a Web page to purchase worthless downloadable software.

The case filed by the Attorney General listed both individual and corporate defendants:

- **James Reed McCreary IV**. Case # 08-2-33486-4 SEA. As with the cases filed by Microsoft, the defendant was behind a scheme to defraud consumers by utilizing the Messenger Service function of the operating system to warn the user about nonexistent vulnerabilities. The user was thereafter directed to a Web page and was urged to buy worthless software as a supposed solution to the vulnerabilities. The defendant used three corporations to perpetrate the fraud: Branch Software, Inc., Registry Cleaner, and Alpha Red, Inc. The defendant and corporate entities were all located in the State of Texas.

The cases filed by Microsoft and the Washington Attorney General generated substantial news coverage both locally and nationally, including a broadcast news story by a consumer protection reporter from KOMO-TV, the ABC network affiliate in Seattle, which was also aired nationally on MSNBC. The media piece focused on the methods that were used to perpetrate the fraud and examined ways in which consumers could protect themselves from becoming victims of such online scams.

Restitution and Deterrence

Strategic public/private partnerships also facilitate efforts to leverage the judicial process on behalf of the average consumer, helping to ensure that criminals are subjected to two of the core traditional byproducts of any legal action—restitution to the victim and deterrence of future wrongful acts.

"To make the victim whole." The concept of awarding monetary compensation to a plaintiff is based upon the desire of the law to address a wrong. In civil actions, the primary mechanism to achieve this goal is the awarding of damages to the aggrieved party. This attempt to place the victim in the same financial position prior to being defrauded (in the case of financial wrongs) also results in a natural byproduct, commonly referred to in the law as *deterrence*. But the cost of admission for the average consumer is high and the impetus to initiate a legal challenge low. Fraudulent schemes targeting consumers on the Web generally result in relatively minor losses when viewed from the perspective of an individual victim. Moreover, the cases tend to necessitate substantial investment in the discovery practice to even identify those behind the fraud.

Many online purveyors of fraud are adept at obfuscating their true identities through a complex labyrinth of corporations and financial transactions. The expense to decipher such puzzles makes any offensive legal action prohibitively expensive to the average consumer. Microsoft has used its strategy of working through public/private partnerships to achieve results that resemble the impact of a class action. By taking the lead through private legal causes of action and by providing close technical support to public partners in their enforcement efforts through the courts, Microsoft has been able to disrupt many online fraud schemes targeting consumers.

A review of the results obtained as a result of civil cases filed by Microsoft against distributors of rogue software over the last two years supports this observation. A total of 17 cases have been filed to date, 14 of which were originally filed as John Doe cases, with the remaining three filed with named defendants. These cases have resulted in a total of U.S.$485,000 collected in settlements, plus an additional $1.3 million in stipulated and default judgments.

These figures are even higher if one factors in those matters filed by Microsoft strategic public partners, such as the Washington State Attorney General and the FTC. In the Secure Computer matter filed by the Attorney General, for example, the defendant company settled the lawsuit by agreeing to pay $200,000 in civil penalties, $75,000 in restitution, and $725,000 in state attorneys' fees.

More recently, on December 10, 2008, the FTC filed a federal law suit under consumer protection statutes against several individual and corporate defendants, both domestic and foreign, responsible for the notorious Win32/WinFixer family of rogue security software. Prosecutors in the case, which is currently pending in the United States District Court for the District of Maryland, obtained an *ex parte* temporary restraining order freezing assets

Encyclopedia

Win32/WinFixer: A program that locates various registry entries, Windows prefetch content, and other types of data, identifies them as "privacy violations," and urges the user to purchase the product to "fix" them..

http://www.microsoft.com/av

and ordering the preservation of business records associated with the fraudulent enterprise. The complaint alleges that one of the defendants involved in the fraud had collected in excess of $18 million as a result of the scheme. After the matter was filed, reports surfaced that the group behind the Web-based fraud against consumers had scattered approximately $40 million in assets shortly before the case was filed. FTC lawyers are aggressively following the money trail. The case may end up being one of the largest rogue security software fraud schemes ever pursued in the courts.

The mere fact that such cases are filed sends a strong message to groups peddling fraudulent products on the Web. When these same cases extract ill-gotten gains through damages awards, civil fines, or fee reimbursement, the message of deterrence to those contemplating online fraud is that much stronger.

Strategy, Mitigations, and Countermeasures

Installed antivirus software, firewalls, and various content-filtering technologies help mitigate the risk of exposure to malware. However, social engineering attacks can often trick the users into taking action that bypasses or lessens the effectiveness of their existing protection. Countering this increased exposure risk requires educating users to take protective actions, like the following:

- Use an up-to-date anti-malware product from a known, trusted source, and keep it updated. Be cautious not to follow advertisements for unknown software that pretends to provide protection (rogue security software). Access the sites of the reputable vendors directly for getting information or subscriptions to their products and services.
- Keep your operating system up to date with the latest security updates and service packs. Turning on Automatic Updates is highly recommended. Make sure to also install security updates for any other software, including third-party software you have installed on your computer. In particular, make sure to install any available security updates for the add-ons you use with your browser. If you do not need some of the add-ons anymore, it is better to uninstall them.
- Consider upgrading to the most recent version of the software you use. More recent versions, as described by this report, are usually more secure or resilient to malware. This report provides information that can help you assess the risk when using older versions of Windows, Microsoft Office, or Adobe software.
- Consider disabling autorun functionality in your environment. KB article 953252 provides information about how to do that. If you decide to leave the autorun functionality enabled, make sure not to use options in the AutoPlay dialog box which are not familiar to you. They may have been added by malware.
- Consider using a user account which doesn't have administrator privileges for your daily work. The type of damage that malware can do in such accounts is limited com-

pared to the damage potential it has with an administrator account. Also, it is easier to restore the damage if the machine got infected while the malware was running in a non-administrator account.

- Make sure to use passwords for any network share you configure. The password must be strong—see http://www.microsoft.com/protect/yourself/password/create.mspx for guidance on creating and using strong passwords.
- Avoid opening attachments or clicking links in e-mail or instant messages that are received unexpectedly or from an unknown source.
- Use a mail client that suppresses active content and that blocks unintentional opening of executable attachments. Current versions of Microsoft Outlook, Windows Live Mail, and Microsoft Outlook Express, coupled with Microsoft Internet Explorer security zone settings, can help guard against the unintentional opening of executable attachments, and they can help suppress active content in e-mail and protect against IFrame attacks.
- Use a robust spam filter to guard against fraudulent and dangerous e-mail. Also install a phishing filter. Windows Vista and Internet Explorer 7 use the Microsoft Phishing Filter to protect users from known phishing sites. Some e-mail applications, such as recent versions of Microsoft Office Outlook, include phishing detection features in addition to spam filters. Internet Explorer 8 includes an advanced filter called SmartScreen®, which provides further protection against malware and unwanted content.
- If you receive an e-mail from a bank or commerce site, visit their site using a prebookmarked link or by typing in the link from your monthly statement. Don't use links provided in the suspect e-mail.
- Deploy inbound and outbound e-mail authentication to protect both your brand and consumers from e-mail spoofing and forgery and to detect inbound spoofing. The Sender ID Framework (SIDF) is the leading authentication solution, currently being used to send more than half of all legitimate e-mail sent daily worldwide.
- Online gamers are at risk from malware that tries to steal their game assets or game credentials. The following blog post provides a list of steps that gamers can take to greatly reduce the risk: http://blogs.technet.com/mmpc/archive/2008/09/03/helpful-suggestions-to-protect-you-from-game-password-stealers.aspx.
- Download and use the Malicious Software Removal Tool from http://www.microsoft.com/security/malwareremove/default.mspx. This tool will automatically scan your computer once a month for many of the prevalent malware families out there. If you suspect that your computer is infected, consider scanning it with the Windows Live safety scanner, which can detect and remove a large range of malware and potentially unwanted software. You can also call the free 1-866-PC-SAFETY line to get help with cleaning your computer.

- Support new legislation to help take legal action against criminals who distribute malware or other potentially unwanted software.
- Use the Microsoft Security Assessment Tool (MSAT) to help assess weaknesses in your IT security environment and build a plan to address the risks. The MSAT can be downloaded from http://technet.microsoft.com/en-us/security/cc185712.aspx.
- Keep yourself up to date about emerging threats. Microsoft security advisories can help you stay current. You can get more information and register at http://www.microsoft.com/security. You can also read about new threats at http://blogs.technet.com/mmpc/.

The Threat Landscape at Home and in the Enterprise

- Home computer users should configure their computers to use Microsoft Update instead of Windows Update; this will help ensure that they receive security updates for Microsoft Office and other Microsoft applications, along with security updates for Windows operating systems. See http://www.microsoft.com/windows/downloads/windowsupdate/microsoftupdate.mspx for an explanation of the differences between Microsoft Update and Windows Update.
- Use an up-to-date anti-malware product from a known, trusted source, and keep it updated. Be cautious not to follow advertisements for unknown software that pretends to provide protection (rogue security software). Access the sites of the reputable vendors directly for getting information or subscriptions to their products and services.
- Enterprise customers should ensure that policies are in place to secure all file shares and regulate the use of removable media.
- Enterprise customers should use the Microsoft Security Assessment Tool (MSAT) to help assess weaknesses in your IT security environment, and build a plan to address the risks. The MSAT can be downloaded from http://technet.microsoft.com/en-us/security/cc185712.aspx.
- Enterprise customers should not permit massively multiplayer online role-playing game software to be installed or run within the corporate network.
- Enterprise customers should carefully control the use of remote management software, such as RealVNC, within the corporate environment.
- Home users should avoid opening attachments or clicking links to documents in e-mail or instant messages that are received unexpectedly or from an unknown source.
- For detailed help and guidance on securing your home computing environment, visit the Security at Home site at http://www.microsoft.com/protect/default.mspx. IT professionals can find enterprise guidance at http://www.microsoft.com/security.

Rogue Security Software

- Use an up-to-date anti-malware product from a known, trusted source, and keep it updated. Be cautious not to follow advertisements for unknown software that pretends to provide protection. Access the sites of the reputable vendors directly for getting information or subscriptions to their products and services.
- If your anti-malware software does not include antispyware software, you should install a separate program and keep it updated. Windows Defender is included in Windows Vista and is available as a free download for Windows XP users from http://www.microsoft.com/windows/products/winfamily/defender/default.mspx.
- Install a firewall and keep it turned on.
- Always run up-to-date software. Enable Automatic Updates in Windows, which will ensure that the latest security updates from Microsoft are downloaded automatically. Periodically check the Web sites of third-party add-on vendors to ensure that you have the latest security updates for their software.
- Use caution when you click links in e-mail or on social networking sites.
- More information and guidance on rogue security software can be found at http://www.microsoft.com/protect/computer/viruses/rogue.mspx.
- If you believe your computer is infected with rogue security software, or you want to find more information and guidance on these threats, visit http://www.microsoft.com/protect/computer/viruses/rogue.mspx.

Call to Action—End to End Trust[23]

Computers were, of course, designed to run code, without concern about its authorship or the intent of that author. Today there are multiple ways to help protect people from malicious code, including firewalls, antivirus programs, and antispyware programs.

But although these approaches make users safer, criminals are not deterred by such preventive measures. To increase accountability, there is another effort that must be undertaken: code-signing so that source can be better identified. Knowing source permits users to consider prior experiences, reputation, and other factors in deciding whether to install software. This is, of course, more problematic than it sounds for a host of reasons. For example, many exploits use code injection to bypass the loader, which checks to make sure code is signed.

Assuming users routinely reject unsigned code, the market response will be to provide signed code. Even if code is signed, however, it will still fall into one of three buckets. There will be code that is signed by a known entity (for example, Microsoft, Oracle,

[23] Derived/excerpts from: Scott Charney, "Establishing End to End Trust." (http://download.microsoft.com/download/7/2/3/723a663c-652a-47ef-a2f5-91842417cab6/Establishing_End_to_End_Trust.pdf)

Adobe) that is trusted due to past experience, brand reputation or some other factor; there will be code that is signed but known to be malware (such as spyware, which can then be blocked); and there will be code signed by entities that are not known to the user. Depending upon the criteria for obtaining a signature, the signature process itself may provide some deterrent to misconduct, much as extended validation certificates do today by providing a more extensive background investigation of the organization seeking the certificate. If code-signing signatures remain easy to obtain with no proof of physical identity, then any deterrent effect is lost and users have no assurance that malfeasance caused by the code can be addressed.

Visit the End to End Trust Web site to learn more about the vision, and help us get there by working together on the creation of a safer, more trusted Internet: www.microsoft.com/endtoendtrust.

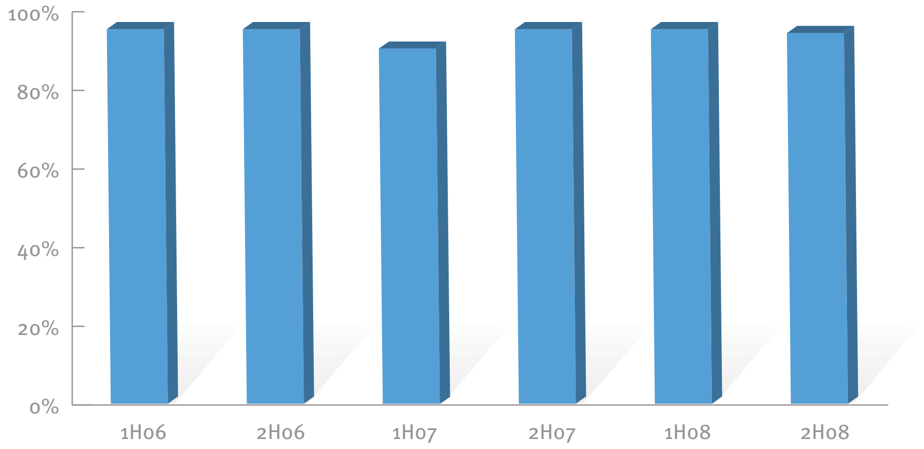
E-Mail Threats

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 also the influx of unwanted e-mail traffic 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.

Spam Trends and Statistics

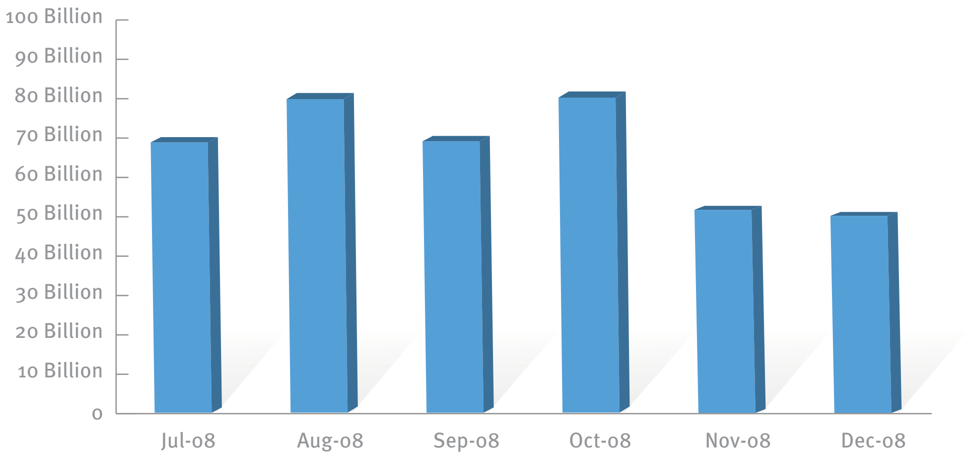
Microsoft Forefront Online Security for Exchange (FOSE; formerly Microsoft Exchange Hosted Services, or EHS) provides enterprise-class spam and malware filtering services for thousands of customers. Figure 68 shows the percentage of incoming e-mail messages that FOSE has filtered as spam in every half-year period since 1H06.

FIGURE 68. Percentage of incoming messages filtered out by FOSE, 1H06–2H08



In 2H08, FOSE filtered 97.3 percent of all e-mail messages it received, delivering only about one out of every 40 messages to intended recipients. This figure was down from 98.4 percent in 1H08; as Figure 69 illustrates, this decline is due to a significant decrease in the volume of spam received in November and December, following the disconnection from the Internet of McColo, a major hosting provider used by spammers. See page 113 for more information about McColo.

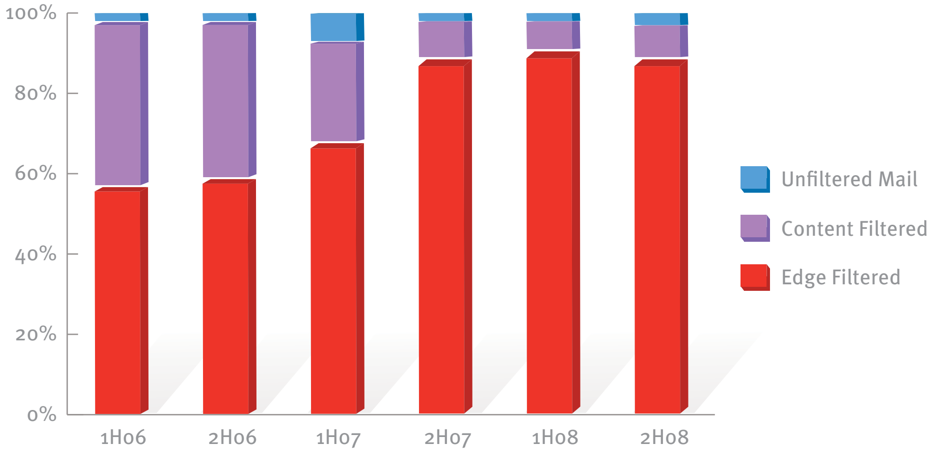
FIGURE 69. Incoming messages blocked by FOSE by month, in 2H08



FOSE performs spam filtering in two stages. The vast majority of spam is blocked by servers at the network edge, which use a number of non-content–based rules to block probable spam or other unwanted messages. Messages that are not blocked at the first stage are scanned using content-based rules, which detect and filter additional e-mail threats, including attachments containing malware.

Figure 70 shows the percentage of messages blocked at each stage in every half-year period since 1H06.

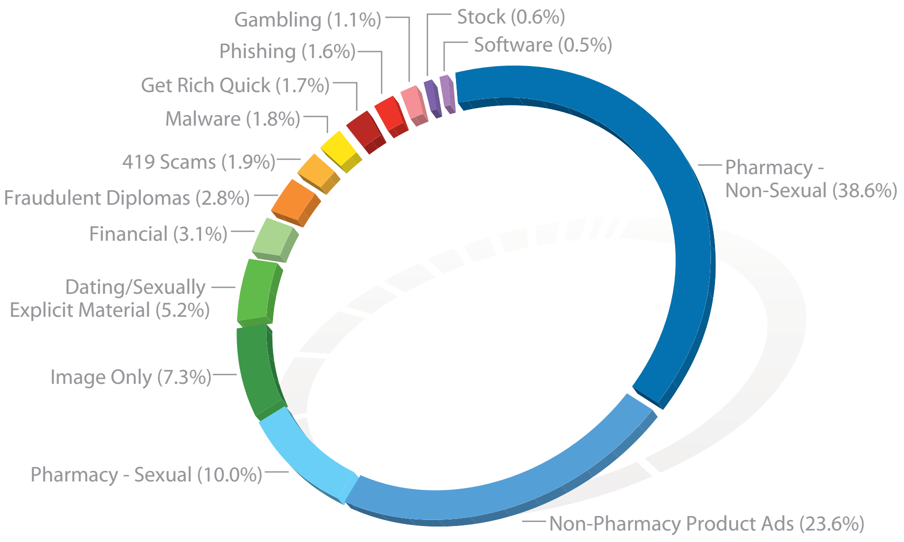
FIGURE 70. Percentage of incoming messages blocked by FOSE using edge-blocking and content filtering, 1H06–2H08



As Figure 70 illustrates, edge-filtering techniques, like IP address reputation checking, SMTP connection analysis, and recipient validation, can be very effective at stopping spam early, obviating the need to perform more resource-intensive content filtering. In 2H08, FOSE edge filters blocked 89.7 percent of all incoming messages, 10.8 times as many as were blocked by content filters.

As in previous periods, spam in 2H08 was dominated by product advertisements, primarily for pharmaceutical products. Figure 71 shows the subject category breakdown for the messages blocked by the FOSE content filters during the last six weeks of 2H08.

FIGURE 71. Inbound messages blocked by FOSE content filters, by category, during the last six weeks of 2H08



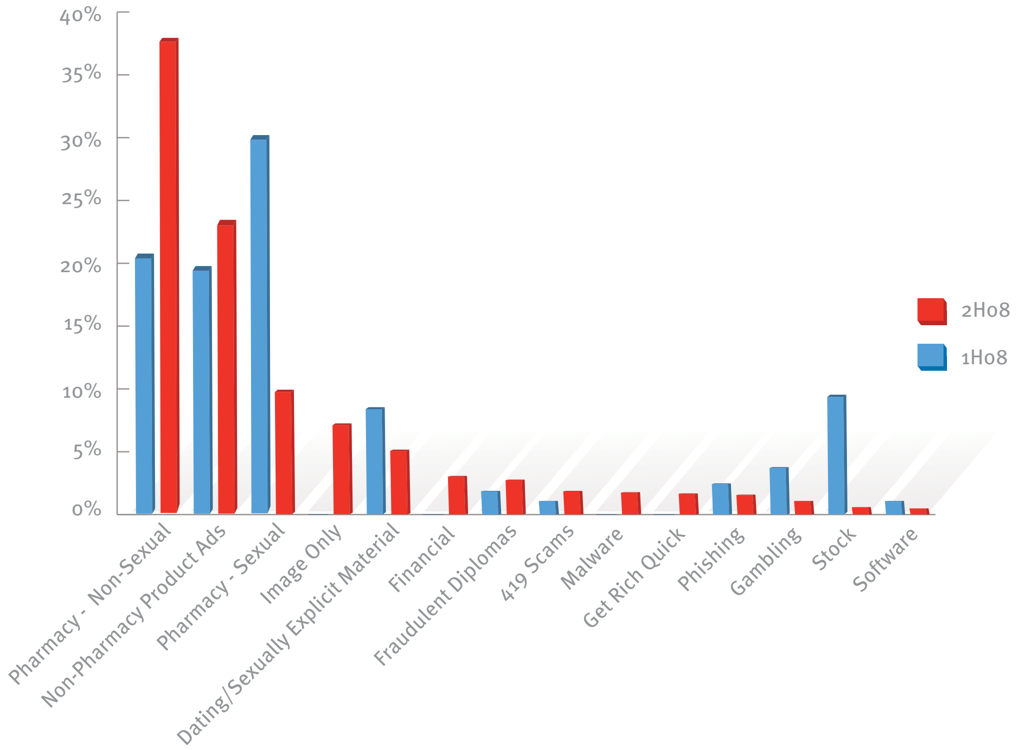
(Totals may not equal 100 percent due to rounding.)

Advertisements for pharmaceutical products accounted for 48.6 percent of the spam messages blocked by FOSE content filters in the last six weeks, with advertisements for sexual performance products, such as Viagra and Cialis, accounting for 10 percent of the overall total. Together with non-pharmacy product ads (23.6 percent of the total), product advertisements accounted for 72.2 percent of spam in the last six weeks.

In an effort to evade content filters, spammers often send messages consisting only of one or more images, with no text in the body of the message. Image-only spam messages accounted for 7.3 percent of the total in the last six weeks.

Comparing the spam subject-matter breakdown from 2H08 with that from 1H08, as in Figure 72, shows how the messages and tactics of spammers evolve over time.

FIGURE 72. Inbound messages blocked by FOSE content filters, by category, 1H08–2H08



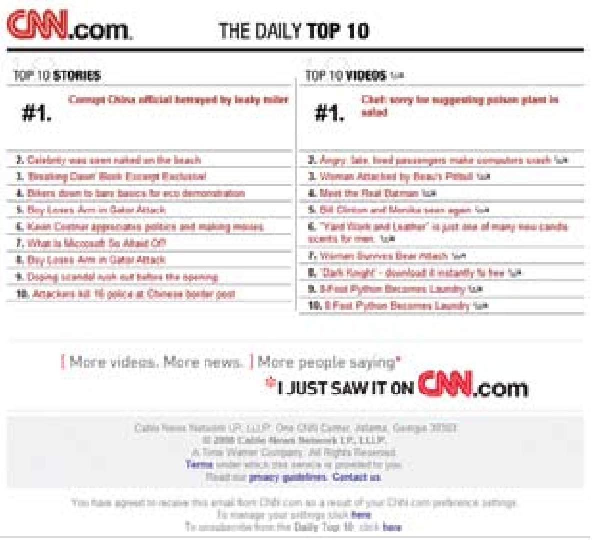
In terms of total volume, the largest increase was detected in the category of non-sexual pharmaceutical products, which nearly doubled its share of the total (38.6 percent in 2H08, up from 20.9 percent in 1H08), and which was matched by a corresponding decrease in the volume of sexually related pharmaceutical products (10.0 percent in 2H08, down from 30.6 percent in 1H08). This perceived shift could be explained in part by an increased use of images in messages touting sexually related pharmaceutical products, which in some cases may make them more difficult to categorize. For example, if a spam message contains pharmacy-related subject and body text, the content filters might categorize it with non-sexual pharmaceutical products even if the messages contain images depicting sexually related products. (Previous volumes of the *Security Intelligence Report* did not include data for image-only spam, so this hypothesis is difficult to verify.)

In relative terms, the most dramatic change was seen in the category of stock-related spam, such as "pump-and-dump" stock schemes. Mirroring the economic downturn experienced by much of the world in 2008, stock-related spam all but disappeared from the FOSE content filters in 2H08, dropping to 0.6 percent of the total from 9.6 percent in 1H08. Non-stock–related financial spam, a newly tracked category in 2H08 that encompasses subjects such as debt consolidation and mortgage refinancing, accounted for 3.8 percent of the total.

Spammers Spoof 'Breaking News' E-Mail Newsletters

Popular news sites, like CNN.com and MSNBC.com, publish e-mail newsletters that aggregate the top news stories each day and are e-mailed to readers who sign up for delivery. In August 2008, Microsoft researchers detected a rise in spam messages that closely resemble these newsletters.

FIGURE 73. A spam message resembling a legitimate e-mail newsletter



CNN.com THE DAILY TOP 10

TOP 10 STORIES

#1. Corrupt China official betrayed by leaky toilet

2. Celebrity was seen naked on the beach
3. 'Breaking Dawn' Book Excerpt Exclusive!
4. Bikers down to bare basics for eco demonstration
5. Boy Loses Arm in Gator Attack
6. Kevin Costner appreciates politics and making movies
7. What is Microsoft So Afraid Of?
8. Boy Loses Arm in Gator Attack
9. Doping scandal rush out before the opening
10. Attackers kill 16 police at Chinese border post

TOP 10 VIDEOS

#1. Chef: sorry for suggesting poison plant in salad

2. Angry, late, tired passengers make computers crash
3. Woman Attacked by Beau's Pitbull
4. Meet the Real Batman
5. Bill Clinton and Monika seen again
6. "Yard Work and Leather" is just one of many new candle scents for men.
7. Woman Survives Bear Attack
8. 'Dark Knight' - download it instantly fo free
9. 8-Foot Python Becomes Laundry
10. 8-Foot Python Becomes Laundry

[More videos. More news.] More people saying*
*I JUST SAW IT ON CNN.com

Cable News Network LP, LLLP. One CNN Center, Atlanta, Georgia 30303
© 2008 Cable News Network LP, LLLP.
A Time Warner Company. All Rights Reserved.
Terms under which this service is provided to you.
Read our privacy guidelines. Contact us.

You have agreed to receive this email from CNN.com as a result of your CNN.com preference settings.
To manage your settings click here.
To unsubscribe from the Daily Top 10, click here.

The messages closely or exactly replicate the format used by the legitimate newsletters and typically feature a mix of real headlines and provocative-sounding false ones. Recipients who click the headline links are taken to Web pages that host spam advertisements or malware, including Win32/Rustock.

Although this tactic resembles phishing, it is properly considered a form of e-mail spoofing because it is not directly intended to fool the recipient into divulging his or her personal information. It is designed to take advantage of the fact that many people subscribe to these newsletters and are far more likely to trust links in a message that resembles one they expect to receive than in a random message that is obviously unsolicited.

Encyclopedia

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

http://www.microsoft.com/av

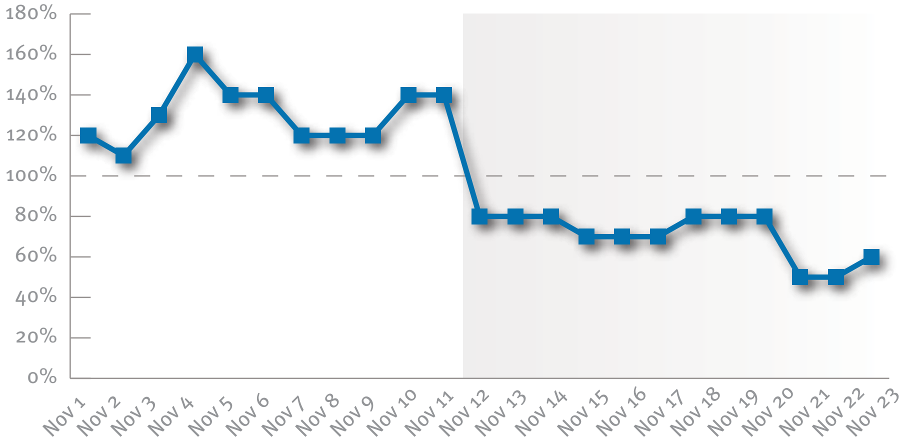
Spam Volume Drops 46 Percent When Hosting Provider Goes Offline

In two high-profile cases in 2H08, hosting providers that provided services to spammers were de-peered (disconnected from the Internet) by their upstream providers, which—in at least one case—had a measurable effect on the amount of spam sent worldwide.

In September 2008, Intercage (also known as Atrivo), a provider that security researchers had accused of providing services to spammers, was de-peered by its upstream providers.[24] Although the Intercage disconnection did not cause a measurable drop in spam as detected by FOSE, it did have the effect of taking down EstDomains, a notorious domain name registrar that was a major supplier of domain names advertised in spam messages.[25] EstDomains subsequently had its registrar status revoked by the Internet Corporation for Assigned Names and Numbers (ICANN), the entity that governs domain name registration for the Internet.

Of more immediate consequence was the November 11, 2008, de-peering of California-based Web hosting company McColo,[26] which caused a 45.9 percent drop in the number of spam messages blocked by FOSE the following day.

FIGURE 74. Spam blocked by FOSE on the days before and after the McColo takedown, indexed to the daily average for the period



McColo was a major hoster of command-and-control servers for botnets, which are responsible for sending most of the spam that is transmitted today. Botnets are networks of computers that have been infected by malware and used for illegal and illicit activities, such as sending spam. The botnet malware is typically configured to surreptitiously monitor a central server, which the botnet operator uses to transmit instructions to the network. When the command-and-control server goes down, the operator is no longer able to order the botnet to send spam.

The McColo shutdown had an unexpectedly long-lasting effect on overall spam levels, as Figure 69 on page 110 illustrates. Overall spam volume for November was down 35.5 percent from October and remained below pre-November levels throughout December.

[24] See Joel Hruska, "Bad seed ISP Atrivo cut off from rest of the Internet." *Ars Technica*. September 23, 2008. (http://arstechnica.com/security/news/2008/09/bad-seed-isp-atrivo-cut-off-from-rest-of-the-internet.ars)

[25] See Brian Krebs, "EstDomains: A Sordid History and a Storied CEO." *Security Fix*. September 8, 2008. (http://voices.washingtonpost.com/securityfix/2008/09/estdomains_a_sordid_history_an.html)

[26] See Brian Krebs, "Major Source of Online Scams and Spams Knocked Offline." *Security Fix*. November 11, 2008. (http://voices.washingtonpost.com/securityfix/2008/11/major_source_of_online_scams_a.html)

Backscatter Causes 90 Percent of Bounce Messages

Backscatter (also known as *outscatter*, *misdirected bounces*, *blowback*, or *collateral spam*) is a side-effect of e-mail spam, viruses, and worms that causes unnecessary e-mail traffic.

When an e-mail server accepts an incoming message for delivery and later determines that it cannot deliver the message to its intended recipient (for example, the recipient's inbox is full, or the recipient's address does not exist), the server is required by the protocols governing Internet e-mail to send a *bounce message* to the sender, informing him or her that the message could not be delivered. A typical bounce message—formally known as a *Non-Deliverable Report/Receipt (NDR)* or *Delivery Status Notification (DSN)*—contains a copy of the original message and a brief explanation of why it could not be delivered. The exact format of the bounce message varies according to the way the mail system sending it is configured.

Unfortunately, e-mail spammers almost always forge the **From:** line when they send messages, in an attempt to avoid being shut down or having their messages blocked. The forged e-mail address may not actually exist, or it may be the real e-mail address of an innocent third party. A typical spamming run may involve sending e-mail to thousands of addresses, not all of which are functional. Any bounce messages generated by sending to these non-functional addresses are addressed and delivered to the forged address in the **From:** line, which typically results in the real owner of the address being deluged with bounce messages—a phenomenon known as *backscatter*. According to Microsoft observations, 90 percent of the bounce messages generated during December 2008 were the result of backscatter.

Mail administrators implementing SMTP and other mail servers can help prevent backscatter by validating the **From:** line of e-mail envelopes before closing the SMTP connection. A bounce message is only generated when the receiving server accepts an incoming message for delivery and does not determine that it cannot be sent until after the connection is closed. By validating recipient addresses during the original connection, the receiving server can reject undeliverable messages immediately without creating backscatter.

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 malicious Web sites are 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 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; likewise, major search engines identify malicious sites in search results and prevent users from unknowingly visiting them. Analyzing the telemetry produced by these tools can provide very valuable information about the nature and spread of malicious Web sites.

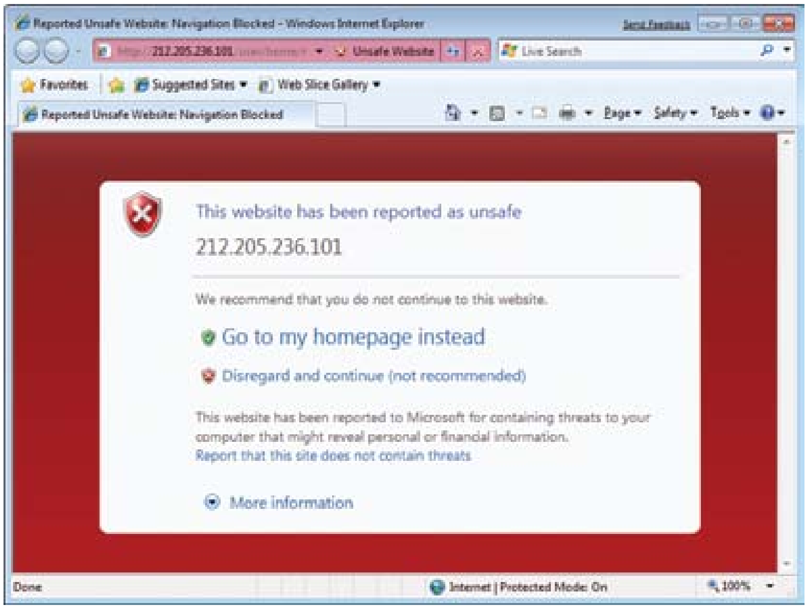
Analysis of Phishing Sites

Although phishers continue to target Internet users at a level commensurate with previous periods, these efforts have become significantly less successful since 1H08, due in large part to the efforts of several popular social networks to educate their users about phishing and how to detect and avoid it. At the same time, Microsoft phishing researchers have made significant improvements in their ability to discover new phishing sites and quickly block them. As a result, even though the number of active phishing sites has increased, each individual site receives far less traffic than phishing sites seen in 1H08.

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. Microsoft keeps track of how many people visit each reported phishing URL and uses the information to improve its filtering technology and its efforts to track suspected phishing sites.[27]

FIGURE 75. The SmartScreen Filter in Internet Explorer 8 blocks reported phishing and malware distribution sites.


Reported Unsafe Website: Navigation Blocked - Windows Internet Explorer
Send Feedback
http://212.205.236.101
Unsafe Website
Live Search
Favorites
Suggested Sites
Web Slice Gallery
Reported Unsafe Website: Navigation Blocked
Page
Safety
Tools
Done
Internet | Protected Mode: On
100%

This website has been reported as unsafe

212.205.236.101

We recommend that you do not continue to this website.

Go to my homepage instead

Disregard and continue (not recommended)

This website has been reported to Microsoft for containing threats to your computer that might reveal personal or financial information.
Report that this site does not contain threats

More information

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

Figure 76 and Figure 77 show the number and types of active phishing sites being tracked by Microsoft each month in 2H08, along with the number of phishing impressions recorded each month. (A *phishing impression* is a single instance of a user attempting to visit a known phishing site with Internet Explorer and being blocked.)

FIGURE 76. Phishing sites tracked each month in 2H08 and their target institution types, indexed to the monthly average for 2H08

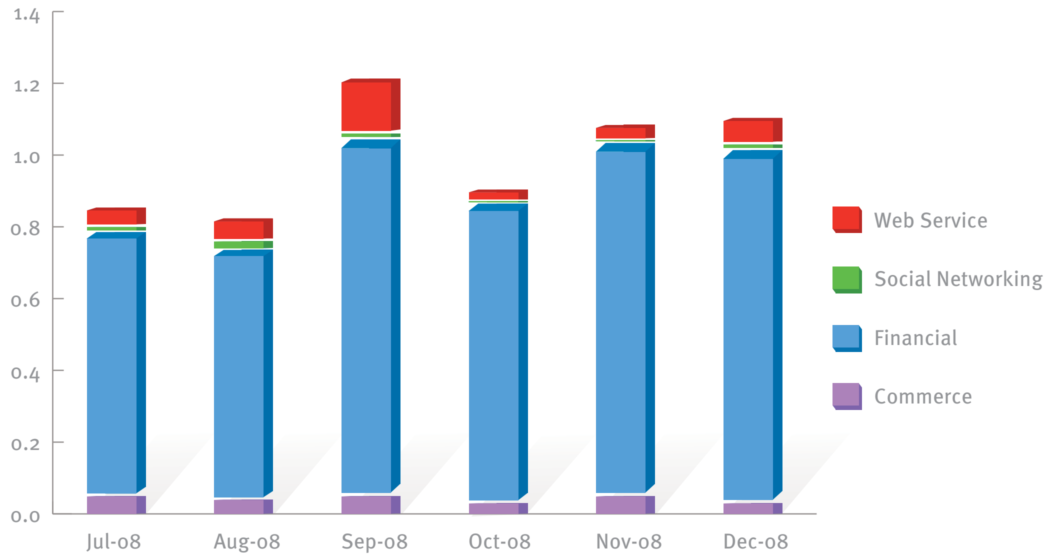
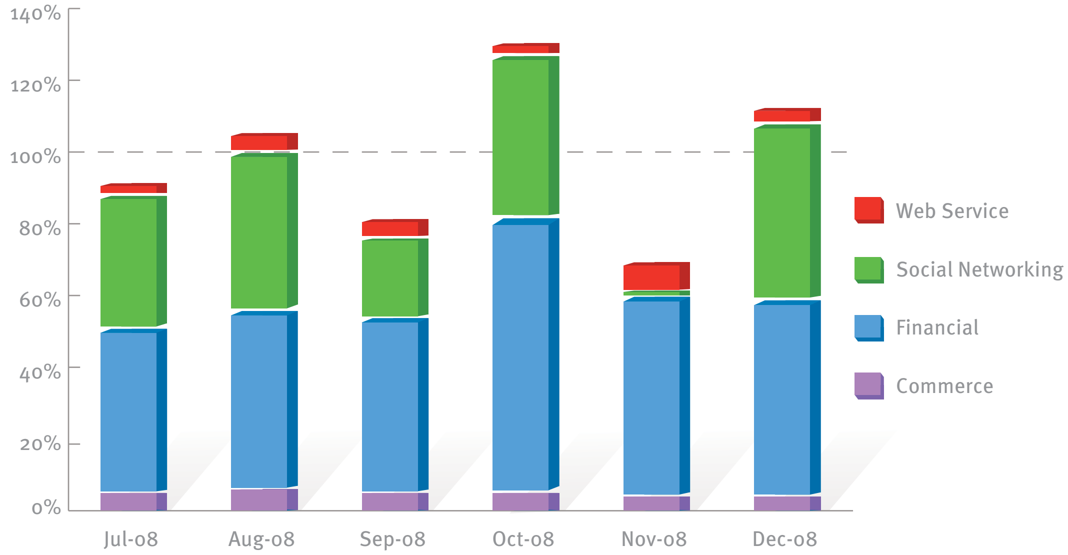


FIGURE 77. Impressions for each type of phishing site each month in 2H08, indexed to the monthly average for 2H08



Two important observations about this data:

- Although phishing sites targeting social networks accounted for less than 1 percent of all active phishing sites on average in 2H08, they were responsible for a much larger portion of phishing impressions, ranging as high as 44.2 percent of all phishing impressions in December. A typical social network phish is likely to trick an order of magnitude more users than a typical financial phish.

  There are a number of explanations for this discrepancy. While financial institutions targeted by phishers can number in the hundreds, 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 addition, phishers often use the messaging features of the sites themselves to distribute their attacks, typically by gaining control of a user's account and using it to send phishing messages to the victim's friends. These attacks can be much more effective than e-mail–based attacks, because they exploit the considerable level of trust users place in their friends. Although social networks have had a great deal of success 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.

- The McColo takedown in mid-November (see "Spam Volume Drops 46 Percent When Hosting Provider Goes Offline," on page 113) appears to have had a dramatic effect on phishing impressions, which dropped 46.2 percent from October to November. The most dramatic decrease came from visits to phishing sites targeting social networking sites, which dropped from 34.1 percent of all impressions in October to just 1.1 percent of impressions in November. This suggests that McColo may have served a number of clients that specialized in phishing attacks that targeted social networks and that when McColo was de-peered, these clients could not access the command-and-control servers they used to send phishing messages.

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 78 and Figure 79 show the geographic distribution of phishing sites reported to Microsoft in 2H08, around the world and in the United States.

FIGURE 78. Distribution of phishing sites by country/region, by percentage of all phishing sites worldwide, in 2H08

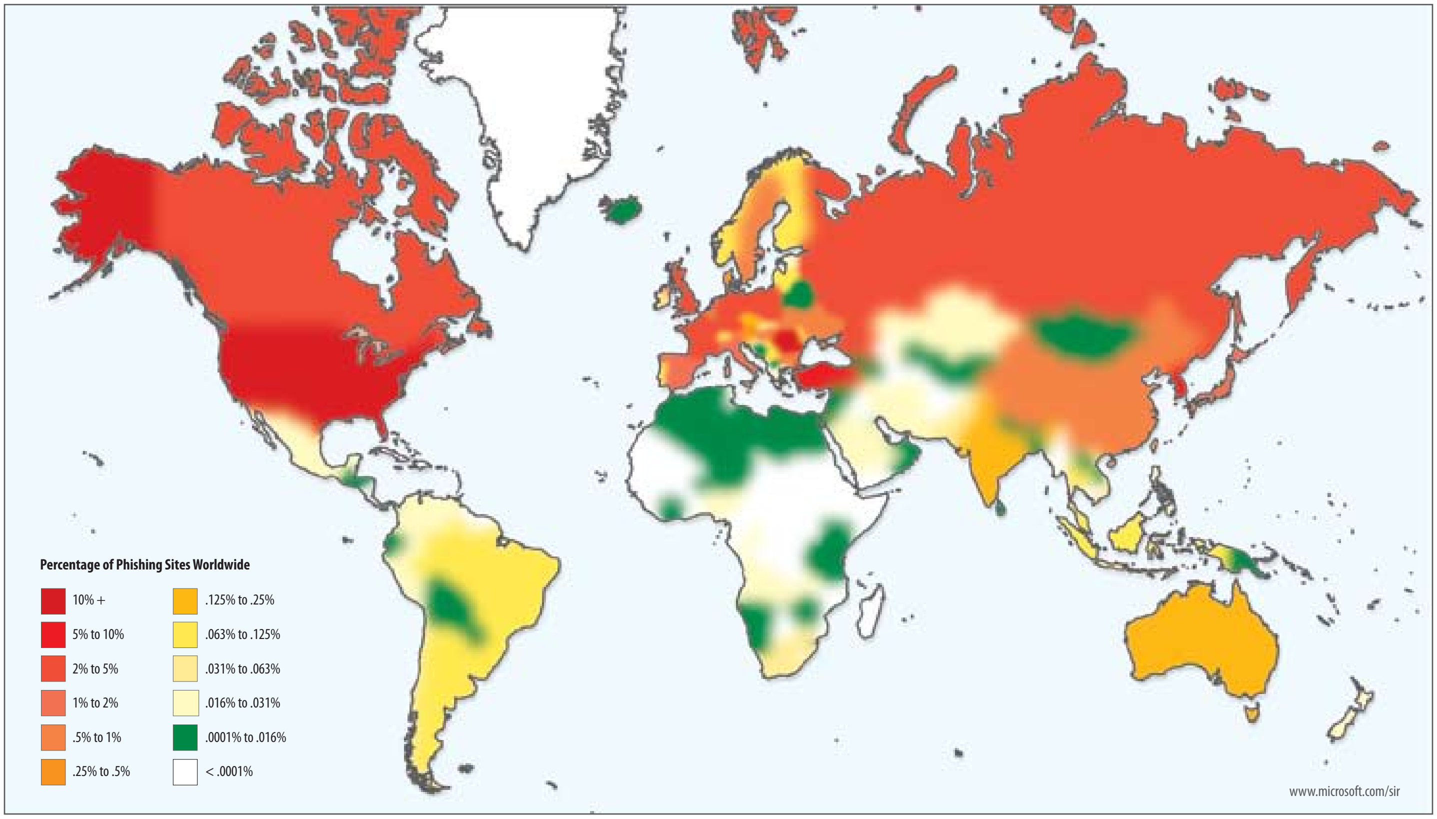
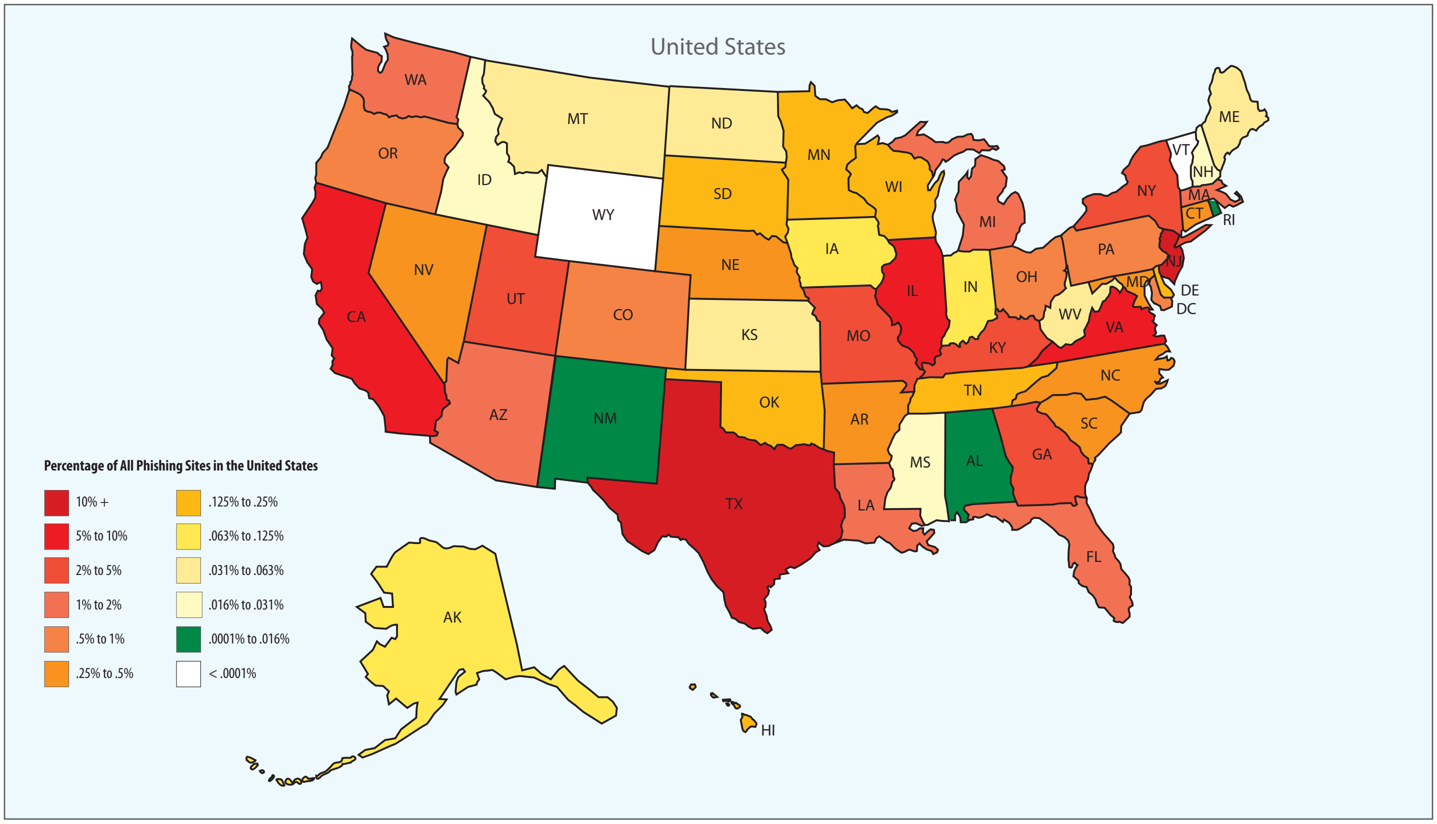


FIGURE 79. Distribution of phishing sites in the United States by state, by percentage of all phishing sites nationwide, in 2H08



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 in 48 of 50 U.S. states and in almost every country and region in the world, with the exception of a handful of locations in Africa and Asia.

Analysis of Malware Hosts

In August 2008, Microsoft released Internet Explorer 8 Beta 2, which included the SmartScreen Filter, a successor to the Phishing Filter in Internet Explorer 7. The SmartScreen Filter continues to provide protection against phishing sites, as described in “Analysis of Phishing Sites” beginning on page 116, and also includes anti-malware support. The SmartScreen anti-malware feature is URL-reputation–based, which means that it evaluates servers hosting downloads to determine if those servers are known to distribute 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.

Telemetry from pre-release versions of Internet Explorer 8 indicates that user impressions of sites hosting malware is significantly higher than impressions of phishing sites, with at least 10 malware impressions recorded for every phishing impression. (A malware impression is a single instance of a user attempting to visit a site known to host malware with Internet Explorer and being blocked.) The distribution of malware families on these sites follows a “long tail” pattern—a handful of malware families dominate malware impressions, but beyond the top families there are a large number of threats that each collect a small fraction of the impressions of the leaders.

Figure 80 lists the top 10 malware and potentially unwanted software families blocked by the SmartScreen Filter in 2H08, by user impression. Overall, sites hosting these 10 families constituted 71.2 percent of all malware impressions.

FIGURE 80. The top 10 malware families hosted on sites blocked by the SmartScreen Filter in Internet Explorer 8, in 2H08

Rank	Family	Most Significant Category	% of Malware Impressions
1	Win32/Renos	Trojan Downloaders & Droppers	21.2%
2	Win32/MoneyTree	Miscellaneous Potentially Unwanted Software	19.2%
3	Win32/FakeXPA	Miscellaneous Trojans	10.4%
4	Win32/Zlob	Trojan Downloaders & Droppers	3.8%
5	Win32/Delflob	Miscellaneous Trojans	3.3%
6	Win32/FakeReprox	Trojan Downloaders & Droppers	3.1%
7	Win32/WinSpywareProtect	Miscellaneous Trojans	3.1%
8	Win32/Small	Trojan Downloaders & Droppers	2.5%
9	Win32/Tracur	Trojan Downloaders & Droppers	2.2%
10	Win32/Antivirus2008	Miscellaneous Potentially Unwanted Software	2.2%

Interestingly, the 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. Win32/Renos, the most prevalent family on the SmartScreen list and overall in 2H08, has nearly 10,000 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 are families like Win32/MoneyTree and Win32/Tracur, which are hosted on smaller numbers of high-traffic sites. Win32/Tracur, for example, has been identified at fewer than 10 sites, but each site received an average of more than 10,000 Internet Explorer 8 impressions in 2H08.

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 81 and Figure 82 on the next page show the geographic distribution of malware hosting sites reported to Microsoft in 2H08, around the world and in the United States.

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/Tracur: A trojan that downloads and executes arbitrary files. It is sometimes distributed by ASX/Wimad.

http://www.microsoft.com/av

FIGURE 81. Distribution of malware hosting sites by country/region, by percentage of all malware hosting sites worldwide, in 2H08

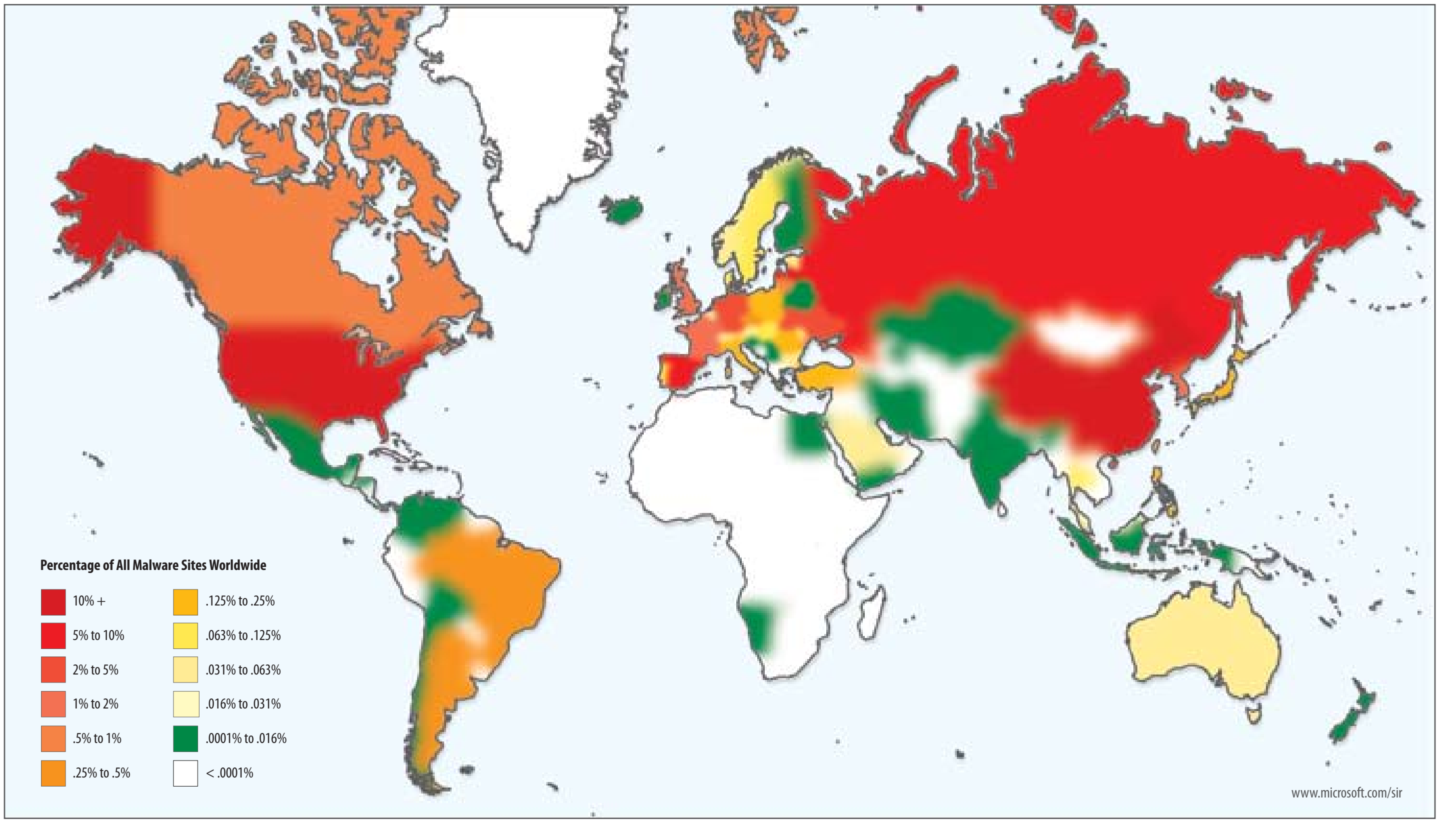
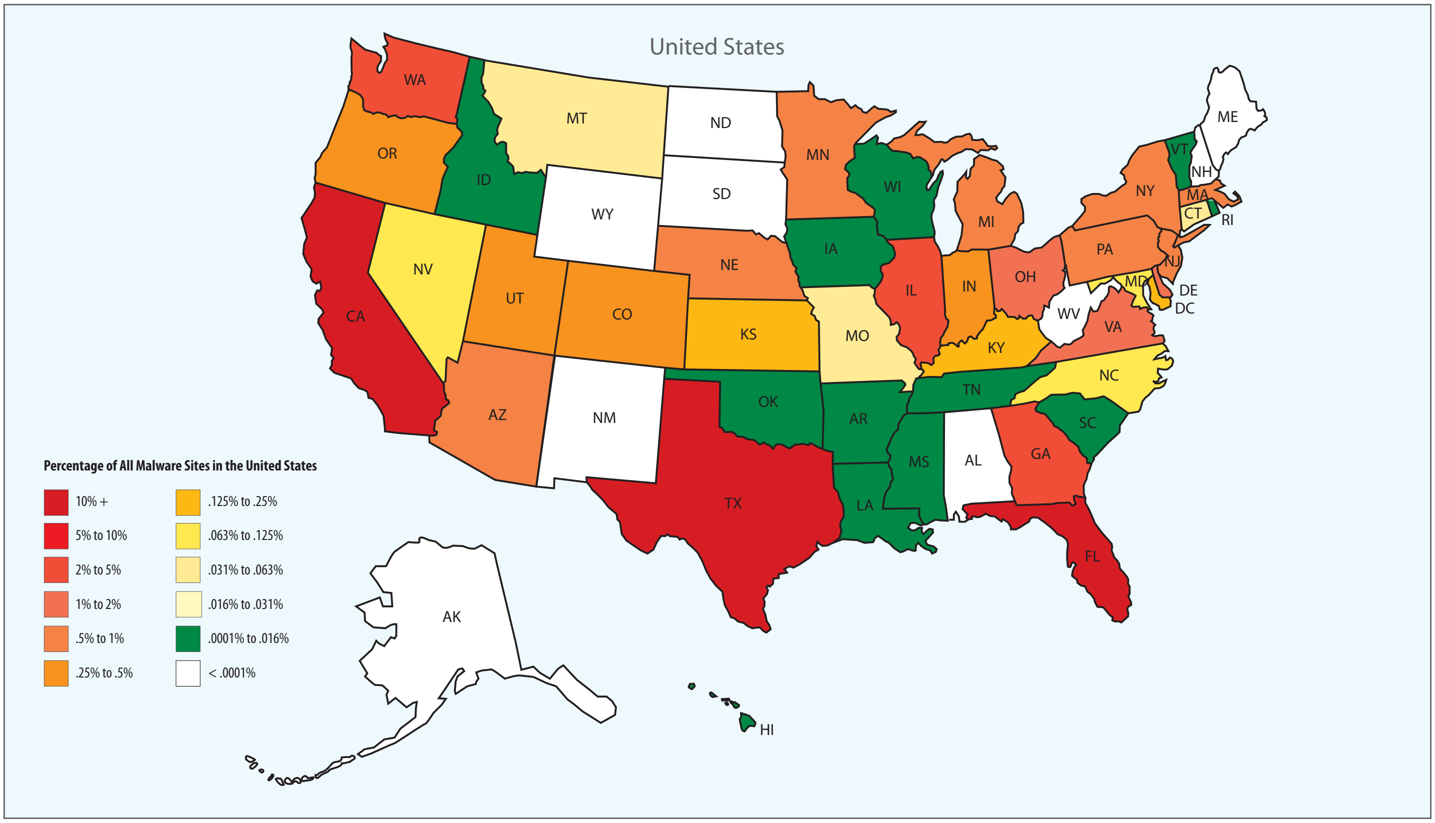


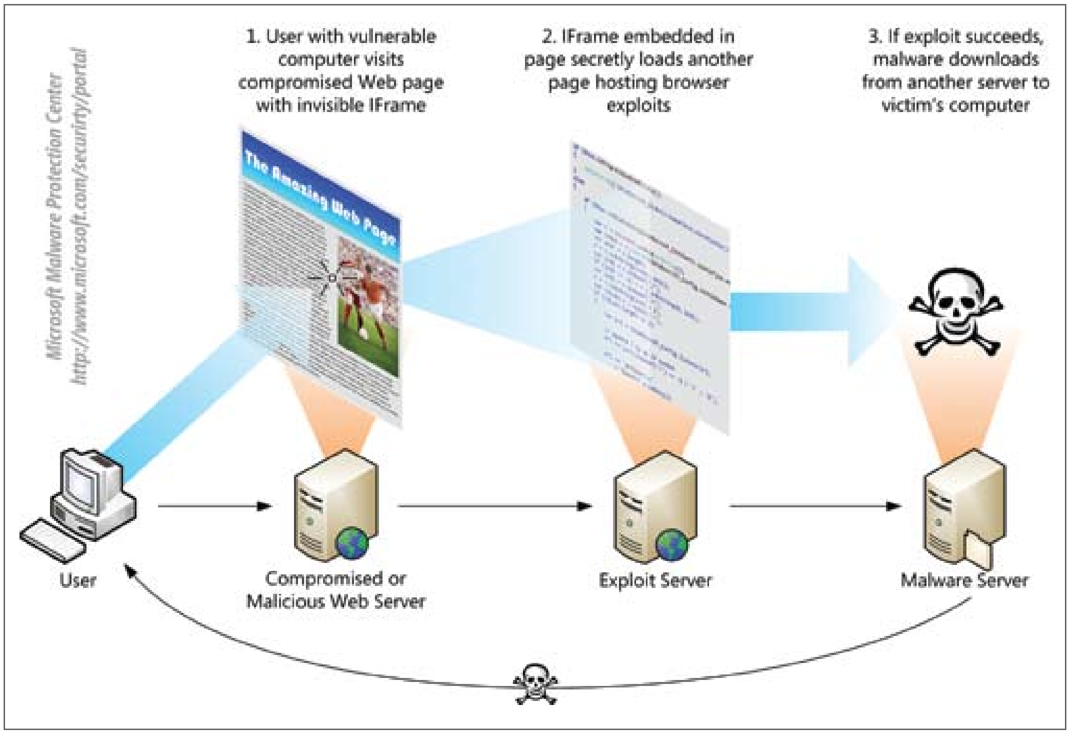
FIGURE 82. Distribution of malware hosting sites in the United States by state, by percentage of all malware hosting sites nationwide, in 2H08



Analysis of Drive-By Download Pages

Some malicious sites rely on social engineering to convince visitors to download malware, using techniques described elsewhere in this report—for example, with bogus warnings that the visitor's computer is infected with malware and offer to sell the visitor software that will remove it, or by claiming that the visitor needs to download a missing codec to play a video on the site. Other sites use *drive-by downloads* to distribute malware—that is, the pages host one or more exploits targeting vulnerabilities in Web browsers or add-ons that enable malicious code to be secretly downloaded to and installed on an unprotected visitor's computer. This technique usually involves posting exploit code to a legitimate Web site, either by gaining access to the site through intrusion or by posting malicious code to a poorly secured Web form, like a comment field on a blog. (For more information about exploits, see "Exploit Trends," beginning on page 47). 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.

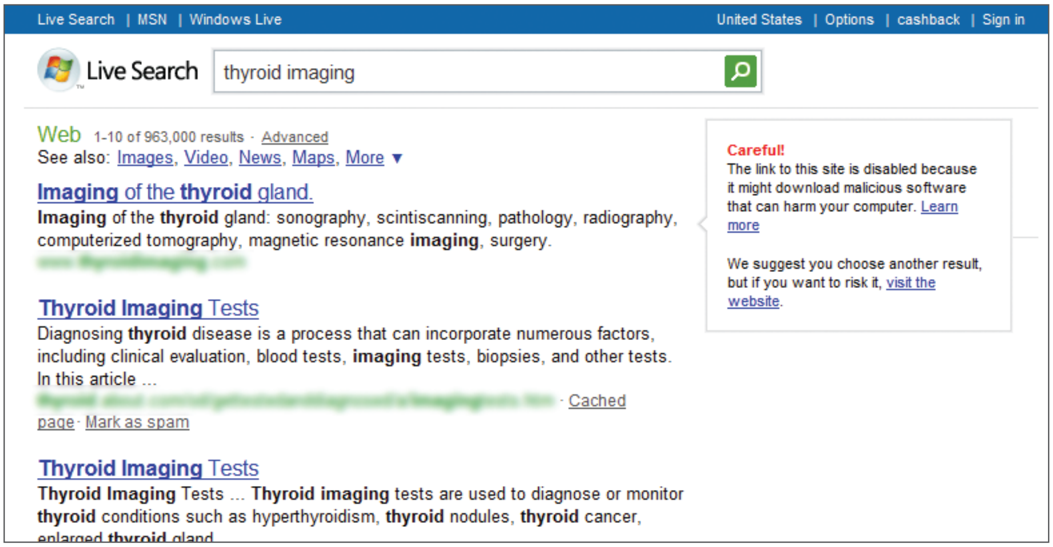
FIGURE 83. One example of a drive-by download attack


Microsoft Malware Protection Center
http://www.microsoft.com/security/portal
1. User with vulnerable computer visits compromised Web page with invisible IFrame
2. IFrame embedded in page secretly loads another page hosting browser exploits
3. If exploit succeeds, malware downloads from another server to victim's computer
The Amazing Web Page
User
Compromised or Malicious Web Server
Exploit Server
Malware Server

In both kinds of cases, attackers rely on traffic being driven to the malicious pages by search engines, such as Live Search. In cases involving social engineering, attackers attempt to manipulate search engines using link-level and page-level spam techniques to artificially raise the position of their sites in the list of results returned by search engines for various common search terms, like “virus” or “porn.” Live Search combats these threats by penalizing sites that use these techniques, which often involves removing the sites from search result listings.

To protect users from drive-by downloads, beginning in 2H08, Live Search launched an ongoing effort to find and track sites that host drive-by downloads and to warn users about the possible danger. As Live Search crawls 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 Live Search 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 84. Live Search works with webmasters to inform them about compromised sites through the Live Search Webmaster Center (http://webmaster.live.com) and provides guidance for the removal of malicious code so that pages can be re-enabled in the index.

FIGURE 84. A drive-by download warning from Live Search


Live Search | MSN | Windows Live
United States | Options | cashback | Sign in
Live Search
Web

thyroid imaging

1-10 of 963,000 results · Advanced

See also: Images, Video, News, Maps, More ▼

Imaging of the thyroid gland.

Imaging of the **thyroid** gland: sonography, scintiscanning, pathology, radiography, computerized tomography, magnetic resonance **imaging**, surgery.

[redacted]

Thyroid Imaging Tests

Diagnosing **thyroid** disease is a process that can incorporate numerous factors, including clinical evaluation, blood tests, **imaging** tests, biopsies, and other tests. In this article ...

[redacted] · Cached page · Mark as spam

Thyroid Imaging Tests

Thyroid Imaging Tests ... **Thyroid imaging** tests are used to diagnose or monitor **thyroid** conditions such as hyperthyroidism, **thyroid** nodules, **thyroid** cancer, enlarged **thyroid** gland

Careful!

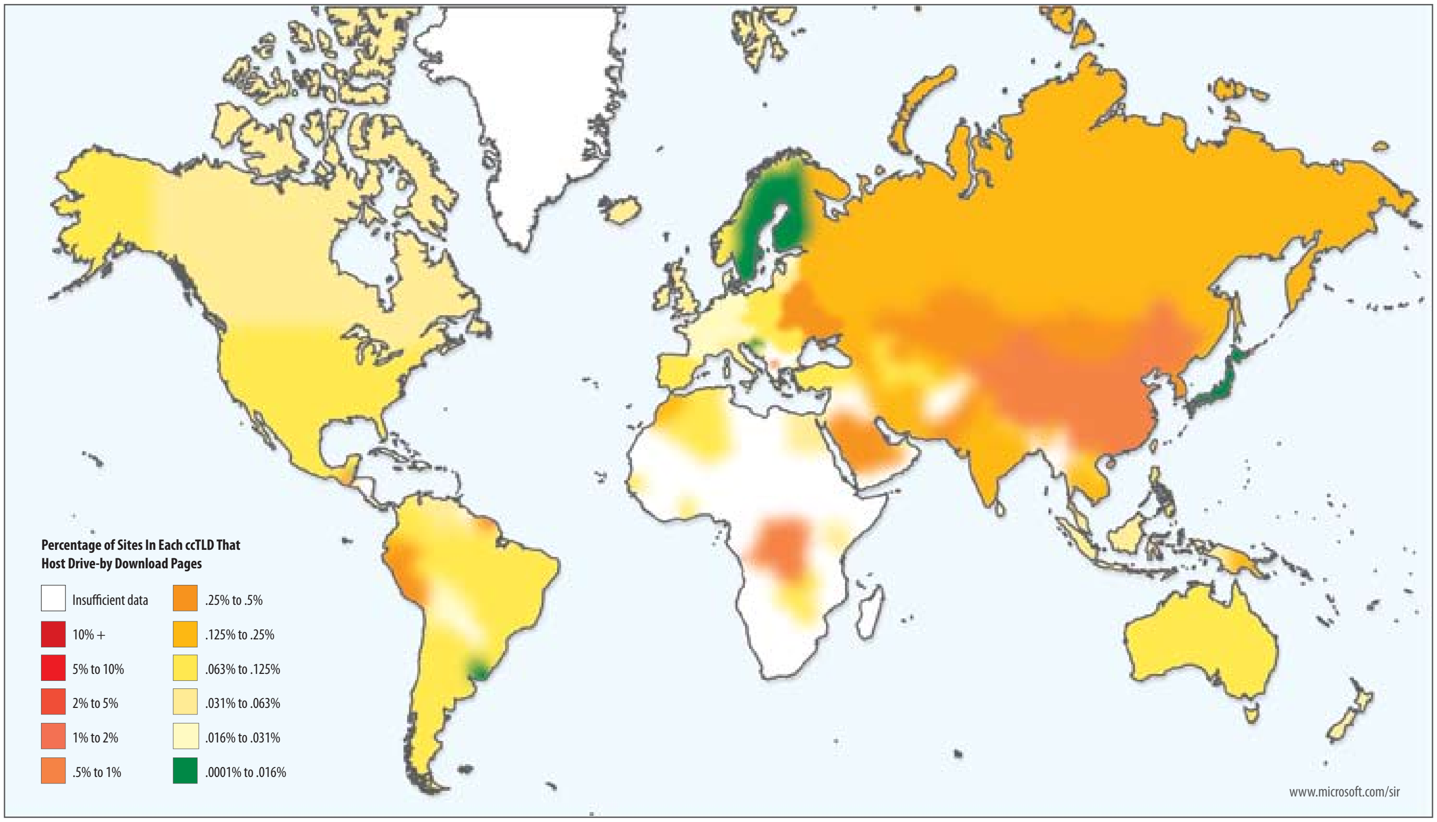
The link to this site is disabled because it might download malicious software that can harm your computer. Learn more

We suggest you choose another result, but if you want to risk it, visit the website.

Geographic Distribution of Drive-By Download Pages

On average, Live Search detected more than 1 million drive-by download pages per month since early 2H08, or about 0.07 percent of all sites indexed. 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 85 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 2H08.

FIGURE 85. Percentage of Web sites in each country-code top-level domain (ccTLD) that host drive-by download pages, in 2H08



Among ccTLDs that included at least one site hosting drive-by download pages, percentages varied greatly. More than 1 percent of the sites in the .cn ccTLD were found to be hosting drive-by download pages (although this trend seems to be declining), but only 0.01 percent of the sites in some other large ccTLDs, like .se and .jp, were similarly affected. Nearly half of all ccTLDs had no affected sites at all (most are small registries without many domains). (Note that Figure 85 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 the appropriate language, so Figure 85 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 86. The .name TLD, which is intended for use by individuals and families, contains the highest percentage of sites hosting drive-by download pages, at 0.23 percent; .edu, used by education institutions in the United States, is in second place, with 0.19 percent. Several generic and sponsored TLDs were not found to be hosting any Web sites with drive-by download pages, including .mobi, .coop, .jobs, .areo, .museum, .int, and .mil. With the exception of .int and .mil (used by international organizations and the United States military, respectively), most of these are relatively new TLDs without many domains compared to some of the others.

FIGURE 86. Percentage of Web sites in each generic top-level domain that hosted drive-by download pages in 2H08

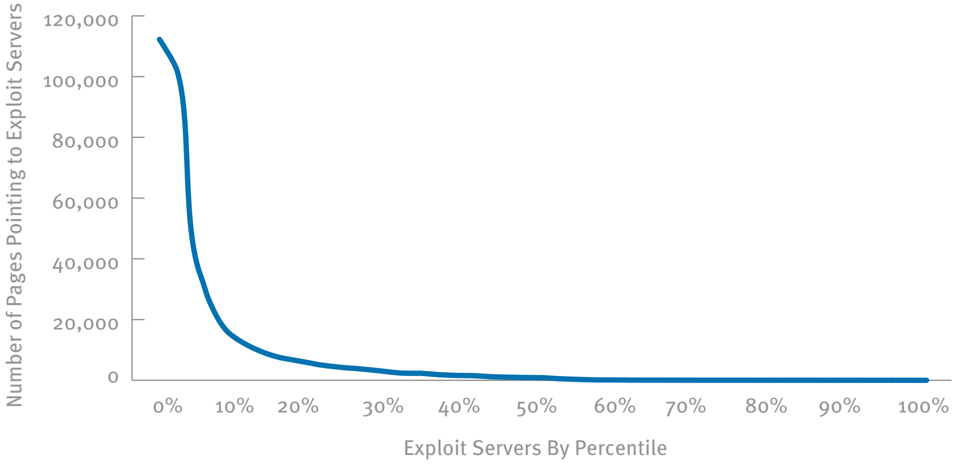
TLD	Percentage of sites hosting drive-by download pages
.name	0.23%
.edu	0.19%
.net	0.19%
.info	0.11%
.org	0.11%
.com	0.09%
.travel	0.04%
.gov	0.01%

Going a level deeper than TLDs and analyzing the network operators (ISPs, data centers, backbone providers, and similar operators) that provide hosting services to sites containing drive-by download pages reveals that more than half of such sites are themselves hosted by just 10 network operators—six in China, three in the United States, and one in Russia.

Distribution of Exploit Servers

In most cases, 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 87.

FIGURE 87. Distribution of exploit servers by the number of drive-by pages pointing to each one, 2H08



In 2H08, the top exploit servers—those that provided exploit code for more than 10,000 drive-by download pages each—made up about 12.8 percent of all exploit servers detected but accounted for 84.1 percent of drive-by download pages. Assuming that it is infeasible for an attacker to create that many Web pages of their own to point to a single exploit server, it is reasonable to conclude that the vast majority of drive-by download pages are legitimate pages that have been compromised by an attacker, rather than malicious pages created by the attackers themselves.

If this is in fact the case, a number of factors could account for the higher concentration of drive-by download pages connected with certain TLDs and network operators:

- The policies and procedures of the affected ISPs and network operators may not facilitate the secure practices and removal of malicious content.
- A low level of security awareness among some groups of customers and Internet users may lead to insecure configurations that can easily be abused by a malicious third party.
- The affected jurisdictions may have lax computer security laws or lax enforcement of the laws that do exist.

Strategies, Mitigations, and Countermeasures

- Use an up-to-date anti-malware product from a known, trusted source, and keep it updated. Be cautious not to follow advertisements for unknown software that pretends to provide protection. Access the sites of the reputable vendors directly for getting information or subscriptions to their products and services.
- Configure your computer to use Microsoft Update instead of Windows Update; this will help ensure that you receive security updates for Microsoft Office and other Microsoft applications, along with security updates for Windows operating systems. See http://www.microsoft.com/windows/downloads/windowsupdate/microsoftupdate.mspx for an explanation of the differences between Microsoft Update and Windows Update.
- Use the most recent version of your Web browser, and keep it up to date by applying security updates and service packs in a timely fashion.
- Web server administrators should make security a priority when maintaining Web sites. Microsoft offers advice and guidance at http://msdn.microsoft.com/en-us/library/aa302432.aspx.
- Set Internet and local intranet security zone settings in Internet Explorer to High, which will cause Internet Explorer to prompt the user before running scripts and ActiveX controls in these zones.
- To minimize disruption, you can add sites you trust to the Trusted Sites zone to avoid the prompts. In particular, consider adding *.windowsupdate.microsoft.com and *.update.microsoft.com to the Trusted Sites zone to facilitate keeping your computer up to date.
- By default, Internet Explorer on Windows Server 2003 and Windows Server 2008 runs in a restricted mode that is known as *Enhanced Security Configuration*. This mode sets the security level for the Internet zone to High. This is a mitigating factor for Web sites that you have not added to the Internet Explorer Trusted Sites zone.

Microsoft Malware Protection Center Executive Afterword

I hope that reading this report gave you a good idea of what happened across the threat landscape over the second half of 2008. It's clear that the methods and types of malicious software being used continue to evolve as the authors and distributors of these threats continue to press on in their goal of gaining command and control of users' computers and use this landscape to steal more money.

The need for a comprehensive security model for data, computers and networks—at home and in the workplace—is more important than ever. Threats have no boundaries on the Internet, and as the global network continues to grow and evolve, new threats and attacks will emerge; this is a certainty. The Internet is a fascinating ecosystem to study from this perspective; like the frog pond in my childhood backyard in Boston, you can see some pretty strange things appearing as time goes by.

The Microsoft Malware Protection Center (MMPC), along with our Microsoft colleagues and industry partners, constantly work to provide tools and guidance to help develop those comprehensive security models and keep the "strange things" out of your computing environment. The MMPC's focus on providing advanced protection through our products and services, delivering world-class response through our global network of research labs, and providing advice and guidance through our varied communication channels to our customers and partners is built on a solid foundation of years of industry-leading experience and dedication to doing the right thing for our customers.

As you can see from the tremendous amount of data included in this report, malicious and potentially unwanted software is becoming an increasingly global phenomenon, with the bad guys creating software that targets users and computers in many languages in many countries. It is also apparent that the bad guys continue to exploit human nature and software applications far more than flaws in Web browsers or operating systems. As major software manufacturers have worked hard to secure their operating systems and applications, the bad guys have moved their focus to third-party applications, browser add-ons, and direct appeals to human emotions to get their software onto victims' computers.

The rise of rogue security software over the past 18 months (with a dramatic spike in the second half of 2008) is a great example of this trend in action—looking at the top 25 malicious and potentially unwanted software families detected worldwide, we saw rogue security software infections increase by more than 48 percent compared with the first half of 2008. I don't think I've seen a type of threat rise like this for many, many years. Computer users have become increasingly aware of the spread of malicious and potentially unwanted software on the Internet. The bad guys are taking advantage of this by persuading users to install rogue security software that provides little or no real protection, and may actually be malicious in nature. These criminals now have the user's valid credit card details, and a wide-open pathway for downloading more malicious software onto the victim's computer.

Microsoft security products and services removed rogue security software from more than ten million computers worldwide during the second half of 2008 and we'll continue to target these threats in the future.

As my colleague George Stathakopoulos discussed in the foreword to this report, individuals and organizations need to be ever vigilant in creating and implementing appropriate security plans. Companies like Microsoft and the security teams involved in the day to day work must play an important role in providing comprehensive, actionable advice and guidance. This report is one tool that Microsoft provides as part of our work to live up to our role as a responsible partner on the Internet. Each section in the report contains strategies, mitigations, and countermeasures that will help secure computers in homes, organizations and businesses.

So who is at risk from malicious and potentially unwanted software on the Internet today? To quote Jack Nicholson in Martin Scorsese's epic Boston-based thriller *The Departed*, "We all are. Act accordingly."

So, make sure that you keep all of the software on your computer up to date, not just your Microsoft software; be careful what you click on when browsing the Internet; and make sure you install up-to-date anti-malware software from a trusted source. Trust me, you'll be a lot safer.

Thank you for reading this report. I hope you found it informative and useful. Please help us to improve future volumes of the *Microsoft Security Intelligence Report*—we are always interested to hear your feedback and thoughts on how we 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

Appendix A: Full Infection Chart

“Geographic Trends,” beginning on page 65, explains how threat patterns differ significantly in different parts of the world.   shows the infection rate in 215 different locations around the world, derived from averaging each location’s monthly CCM for each of the six months in 2H08. (CCM is the number of computers cleaned for every 1,000 executions of the MSRT. See “Infection Rates and CCM,” on page 65, for more information about the CCM metric.)

FIGURE 88. Infection rates for locations around the world, by CCM, in 2H08

Country/Region	CCM
Afghanistan	8.9
Albania	4.9
Algeria	2.6
American Samoa	18.0
Andorra	1.9
Angola	3.9
Anguilla	9.4
Antigua and Barbuda	0.7
Argentina	4.4
Armenia	6.6
Aruba	3.4
Australia	4.7
Austria	2.3
Azerbaijan	4.1
Bahamas, The	2.4
Bahrain	8.1
Bangladesh	1.9
Barbados	1.7
Belarus	3.6
Belgium	5.0
Belize	3.9
Benin	2.3
Bermuda	1.5
Bhutan	4.1
Bolivia	6.8
Bosnia and Herzegovina	8.9
Botswana	7.8
Brazil	20.9
British Indian Ocean Territory	19.3
Brunei	2.9
Bulgaria	5.6
Burkina Faso	3.8
Burundi	5.7
Cambodia	2.8
Cameroon	4.9
Canada	4.0
Cape Verde	10.5
Cayman Islands	1.8
Central African Republic	18.6
Chad	16.5
Chile	6.3
China	11.4
Colombia	10.0
Comoros	12.7
Congo	6.6
Congo (DRC)	5.8
Costa Rica	8.8
Côte d’Ivoire	2.3
Croatia	10.8
Cyprus	4.7
Czech Republic	5.2
Denmark	5.9
Djibouti	1.5
Dominica	3.3
Dominican Republic	7.1
Ecuador	12.6
Egypt	16.5
El Salvador	9.6

FIGURE 88. Continued

Country/Region	CCM
Equatorial Guinea	3.8
Eritrea	17.6
Estonia	5.3
Ethiopia	1.4
Falkland Islands (Islas Malvinas)	18.2
Faroe Islands	4.4
Fiji Islands	5.2
Finland	2.6
France	7.8
French Guiana	2.4
French Polynesia	2.5
Gabon	12.1
Gambia, The	9.0
Georgia	12.2
Germany	3.6
Ghana	2.6
Gibraltar	3.9
Greece	9.4
Greenland	5.3
Grenada	1.6
Guadeloupe	2.3
Guam	1.4
Guatemala	13.9
Guernsey	0.7
Guinea	6.6
Guinea-Bissau	16.7
Guyana	1.7
Haiti	3.7
Honduras	12.9
Hong Kong S.A.R.	5.8
Hungary	7.5
Iceland	6.0
India	2.8
Indonesia	3.0
Iraq	13.9
Ireland	4.2
Israel	7.5
Italy	5.8
Jamaica	3.3
Japan	1.7
Jordan	9.2
Kazakhstan	4.2
Kenya	2.3
Korea	18.3
Kuwait	9.8
Kyrgyzstan	2.3
Laos	4.3
Latvia	5.8
Lebanon	5.9
Lesotho	14.2
Liberia	10.0
Libya	6.4
Liechtenstein	1.8
Lithuania	7.2
Luxembourg	2.5
Macao S.A.R.	1.5
Macedonia, F.Y.R.O.	8.6
Madagascar	2.2
Malawi	5.2
Malaysia	3.5
Maldives	3.4
Mali	3.8
Malta	3.4
Martinique	2.2
Mauritania	2.6
Mauritius	3.6
Mayotte	9.8
Mexico	15.9
Micronesia	17.4
Moldova	5.2
Monaco	1.3
Mongolia	1.8
Morocco	2.1
Mozambique	8.4
Namibia	14.5
Nepal	1.8
Netherlands	5.9
Netherlands Antilles	1.8
New Caledonia	2.4
New Zealand	4.0
Nicaragua	11.2
Niger	4.4
Nigeria	3.1
Northern Mariana Islands	1.3
Norway	6.8
Oman	7.7
Pakistan	2.2
Palestinian Authority	5.5
Panama	8.9
Papua New Guinea	8.4
Paraguay	6.6
Peru	7.8
Philippines	1.4
Poland	8.0
Portugal	13.4
Puerto Rico	2.7
Qatar	6.4
Reunion	1.6
Romania	4.3
Russia	21.1
Rwanda	1.9
Samoa	11.3
São Tomé and Príncipe	22.3
Saudi Arabia	18.5
Senegal	2.4

FIGURE 88. Continued

Country/Region	CCM
Serbia and Montenegro	77.0
Seychelles	11.1
Sierra Leone	10.3
Singapore	4.5
Slovakia	5.5
Slovenia	6.6
Solomon Islands	8.6
Somalia	13.1
South Africa	6.6
Spain	19.2
Sri Lanka	2.5
St. Kitts and Nevis	2.6
St. Lucia	2.5
St. Vincent and the Grenadines	1.4
Suriname	3.5
Swaziland	14.0
Sweden	5.4
Switzerland	4.1
Taiwan	11.7
Tajikistan	6.4
Tanzania	3.6
Thailand	8.9
Timor-Leste	15.8
Togo	3.8
Tonga	14.9
Trinidad and Tobago	4.1
Tunisia	2.7
Turkey	20.5
Turkmenistan	15.1
Turks and Caicos Islands	2.9
Uganda	4.0
Ukraine	7.8
United Arab Emirates	5.3
United Kingdom	5.7
United States	9.1
Uruguay	2.9
Uzbekistan	4.9
Vanuatu	19.1
Venezuela	5.5
Vietnam	1.3
Virgin Islands	1.5
Virgin Islands, British	12.0
Yemen	7.9
Zambia	10.8
Zimbabwe	20.6
Worldwide	**8.6**

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," on page 65, gives an overview of the way the relative prevalence of different categories of malware varies between different locations.

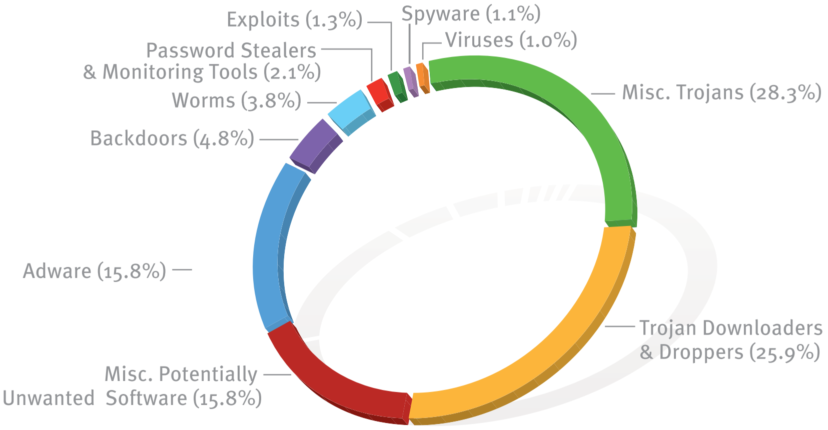
The next several pages provide infection statistics for 12 locations around the world, encompassing multiple continents, languages, and computer usage patterns.

Australia

The infection rate (CCM) for Australia in 2H08 was 4.7, which is significantly lower than the worldwide 2H08 infection rate of 8.6. Figure 89 and Figure 90 list the most common malware and potentially unwanted software categories and families detected by Microsoft security products in Australia in 2H08.

FIGURE 89. Malware and potentially unwanted software in Australia, by category, in 2H08

Category	Infected computers
Miscellaneous Trojans	178,574
Trojan Downloaders & Droppers	163,298
Misc. Potentially Unwanted Software	99,638
Adware	99,539
Backdoors	30,082
Worms	24,030
Password Stealers & Monitoring Tools	13,198
Exploits	8,480
Spyware	7,158
Viruses	6,428



(Totals may not equal 100 percent due to rounding.)

Observations:

- The threat landscape in Australia is dominated by malware families, which account for 67.3 percent of all families detected on infected computers in 2H08.
- The most common category in Australia is Miscellaneous Trojans, which includes all trojan families that are not classified as downloaders/droppers or backdoors. It accounts for 28.3 percent of all families detected on infected computers and 10 of the top 25 families.
- The second most common category in Australia is Trojan Downloaders & Droppers. It accounts for 25.9 percent of all families detected on infected computers.

FIGURE 90. Top 25 families in Australia in 2H08

Rank	Family	Most Significant Category	Infected computers
1	Win32/Renos	Trojan Downloaders & Droppers	78,057
2	Win32/Zlob	Trojan Downloaders & Droppers	72,693
3	Win32/Vundo	Miscellaneous Trojans	56,458
4	Win32/ZangoSearchAssistant	Adware	44,646
5	Win32/FakeSecSen	Miscellaneous Trojans	28,372
6	ASX/Wimad	Trojan Downloaders & Droppers	24,437
7	Win32/PlayMP3z	Adware	23,425
8	Win32/ZangoShoppingreports	Adware	22,391
9	Win32/FakeXPA	Miscellaneous Trojans	21,854
10	Win32/Hotbar	Adware	20,758
11	Win32/Agent	Miscellaneous Trojans	19,077
12	Win32/Antivirus2008	Misc. Potentially Unwanted Software	17,122
13	Win32/Oderoor	Backdoors	12,290
14	Win32/Tibs	Miscellaneous Trojans	12,121
15	Win32/SeekmoSearchAssistant	Adware	10,740
16	Win32/Winfixer	Misc. Potentially Unwanted Software	9,263
17	Win32/Meredrop	Miscellaneous Trojans	9,020
18	Win32/AdRotator	Adware	8,558
19	Win32/RealVNC	Misc. Potentially Unwanted Software	8,037
20	Win32/Vapsup	Misc. Potentially Unwanted Software	7,375
21	Win32/ConHook	Miscellaneous Trojans	7,365
22	Win32/Starware	Misc. Potentially Unwanted Software	7,340
23	Win32/Alureon	Miscellaneous Trojans	7,068
24	Win32/C2Lop	Miscellaneous Trojans	7,037
25	Win32/Busky	Miscellaneous Trojans	7,014

For more information about these families, visit the Microsoft Malware Encyclopedia at www.microsoft.com/av.

Observations:

- The top 25 families were detected on 67.7 percent of all infected computers.
- Fifteen of the top 25 families are potentially unwanted software families, including 4 of the top 10.
- The top four families in Australia (Win32/Renos, Win32/Zlob, Win32/Vundo, and Win32/ZangoSearchAssistant) are also the top four families worldwide, in that order.
- ASX/Wimad and Win32/PlayMP3z, which rank eleventh and fifteenth in the world respectively, are relatively more prevalent in Australia, ranking sixth and seventh. Both families target users who are interested in playing media files—ASX/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.

Many families consist of multiple variants released by attackers in an effort to complicate the detection process. Figure 91 lists the top five individual threats detected in Australia in 2H08.

FIGURE 91. Top five individual threats in Australia in 2H08

Rank	Threat	Infected Computers
1	Adware:Win32/ZangoSearchAssistant	44,640
2	Trojan:Win32/FakeSecSen	28,372
3	Adware:Win32/Playmp3z	23,425
4	Trojan:Win32/FakeXPA	21,854
5	Adware:Win32/Hotbar	20,758

Encyclopedia

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

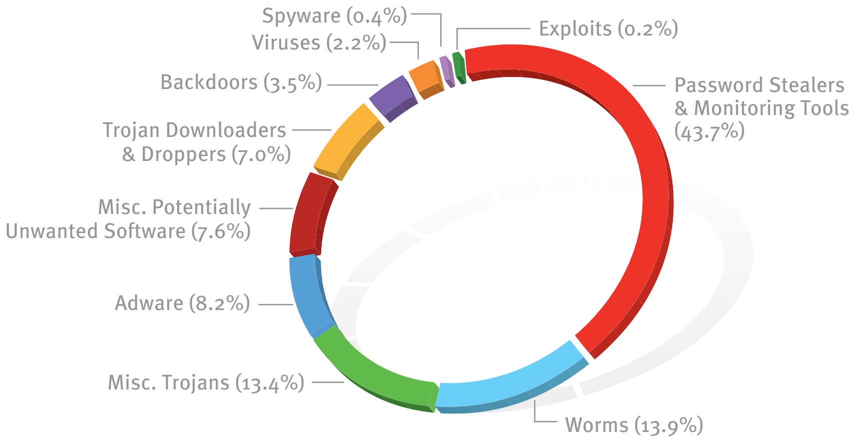
Win32/Playmp3z: An adware family that may display advertisements in connection with the use of a "free music player" from the site "PlayMP3z.biz."

http://www.microsoft.com/av

Brazil

The infection rate (CCM) for Brazil in 2H08 was 20.9 in 2H08, significantly higher than the worldwide 2H08 infection rate of 8.6. Figure 92 and Figure 93 list the most common malware and potentially unwanted software categories and families detected by Microsoft security products in Brazil in 2H08.

FIGURE 92. Malware and potentially unwanted software in Brazil, by category, in 2H08



(Totals may not equal 100 percent due to rounding.)

Category	Infected Computers
Password Stealers & Monitoring Tools	843,698
Worms	267,738
Miscellaneous Trojans	258,542
Adware	158,467
Miscellaneous Potentially Unwanted Software	146,124
Trojan Downloaders & Droppers	135,946
Backdoors	68,326
Viruses	41,687
Spyware	8,570
Exploits	2,923

Observations:

- The threat landscape in Brazil is clearly dominated by malware, which accounted for 83.8 percent of all families detected on infected computers.
- The most common category in Brazil is Password Stealers & Monitoring Tools, which accounted for 43.7 percent of all families detected on infected computers. Most detections in this category were Win32/Bancos and Win32/Banker, the first and second most prevalent families in Brazil in 2H08.
- The second most common category in Brazil is Worms, which accounted for 13.9 percent of all families detected on infected computers.

FIGURE 93. Top 25 families in Brazil in 2H08

Rank	Family	Most Significant Category	Infected Computers
1	Win32/Bancos	Password Stealers & Monitoring Tools	570,121
2	Win32/Banker	Password Stealers & Monitoring Tools	363,752
3	Win32/RJump	Worms	102,073
4	Win32/Taterf	Worms	78,984
5	Win32/Vundo	Miscellaneous Trojans	65,780
6	Win32/Zlob	Trojan Downloaders & Droppers	55,312
7	Win32/Renos	Trojan Downloaders & Droppers	50,939
8	Win32/C2Lop	Miscellaneous Trojans	47,251
9	Win32/ZangoSearchAssistant	Adware	46,721
10	Win32/Slenfbot	Worms	38,416
11	Win32/Playmp3z	Adware	36,419
12	Win32/RealVNC	Miscellaneous Potentially Unwanted Software	30,689
13	Win32/Rbot	Backdoors	26,431
14	Win32/Agent	Miscellaneous Trojans	26,278
15	Win32/ZangoShoppingreports	Adware	24,190
16	Win32/Ldpinch	Password Stealers & Monitoring Tools	23,348
17	Win32/Advantage	Adware	21,158
18	Win32/Frethog	Password Stealers & Monitoring Tools	20,737
19	Win32/Hotbar	Adware	17,969
20	Win32/SeekmoSearchAssistant	Adware	16,670
21	Win32/Parite	Viruses	16,436
22	Win32/UltraVNC	Miscellaneous Potentially Unwanted Software	16,316
23	Win32/PossibleHostsFileHijack	Miscellaneous Potentially Unwanted Software	16,106
24	Win32/Cutwail	Trojan Downloaders & Droppers	15,692
25	Win32/Alureon	Miscellaneous Trojans	14,836

For more information about these families, visit the Microsoft Malware Encyclopedia at www.microsoft.com/av.

Observations:

- The top 25 families were detected on 78.7 percent of all infected computers.
- Win32/Bancos and Win32/Banker, the two most prevalent families on the list, were detected on nearly a quarter of all infected computers in Brazil in 2H08. Win32/Bancos was the twentieth most prevalent family worldwide in 2H08, despite not appearing on the list of most common families for any other top location. For more information, see "Online Banking Malware," beginning on page 23.

Many families consist of multiple variants released by attackers in an effort to complicate the detection process. Figure 94 lists the top five individual threats detected in Brazil in 2H08.

FIGURE 94. Top five individual threats in Brazil in 2H08

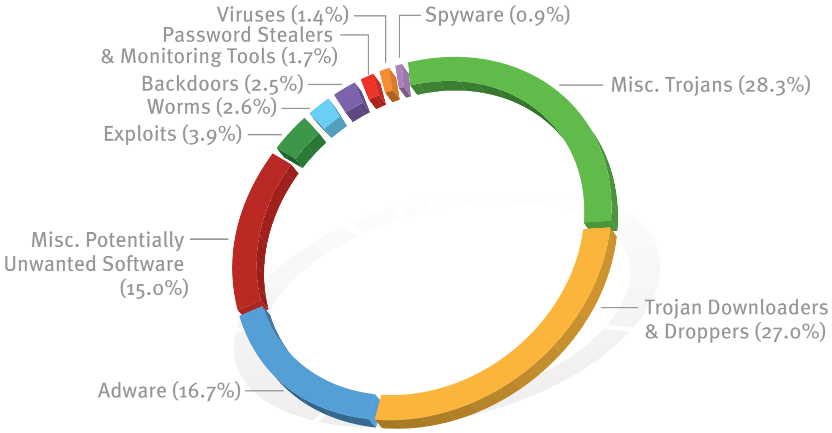
Rank	Threat	Infected Computers
1	TrojanSpy:Win32/Bancos.gen!A	202,420
2	TrojanSpy:Win32/Bancos.gen!C	170,204
3	TrojanSpy:Win32/Banker	146,260
4	TrojanSpy:Win32/Bancos.gen!B	112,995
5	Worm:Win32/RJump.J	72,702

Canada

The infection rate (CCM) for Canada was 4.0 in 2H08, significantly lower than the worldwide 2H08 infection rate of 8.6. Figure 95 and Figure 96 list the most common malware and potentially unwanted software categories and families detected by Microsoft security products in Canada in 2H08.

FIGURE 95. Malware and potentially unwanted software in Canada, by category, in 2H08

Category	Infected Computers
Miscellaneous Trojans	417,094
Trojan Downloaders & Droppers	396,799
Adware	245,790
Miscellaneous Potentially Unwanted Software	220,736
Exploits	57,195
Worms	38,453
Backdoors	37,049
Password Stealers & Monitoring Tools	24,994
Viruses	21,270
Spyware	12,819



(Totals may not equal 100 percent due to rounding.)

Observations:

- The threat landscape in Canada is dominated by malware, which accounted for 67.4 percent of all families detected on infected computers in 2H08.
- The most common family in Canada is Miscellaneous Trojans, which includes all trojan families that are not classified as downloaders/droppers or backdoors. It accounts for 28.3 percent of all infected computers and 10 of the top 25 families.
- The second most common category in Canada is Trojan Downloaders & Droppers. It accounts for 27.0 percent of all infected computers. Three of the top five families in Canada in 2H08 are in this category.

FIGURE 96. Top 25 families in Canada in 2H08

Rank	Family	Most Significant Category	Infected Computers
1	Win32/Renos	Trojan Downloaders & Droppers	143,605
2	Win32/Zlob	Trojan Downloaders & Droppers	143,241
3	Win32/Vundo	Miscellaneous Trojans	141,064
4	ASX/Wimad	Trojan Downloaders & Droppers	137,630
5	Win32/ZangoSearchAssistant	Adware	133,361
6	Win32/ZangoShoppingreports	Adware	70,298
7	Win32/Agent	Miscellaneous Trojans	65,768
8	Win32/FakeXPA	Miscellaneous Trojans	60,418
9	Win32/Hotbar	Adware	57,225
10	Win32/FakeSecSen	Miscellaneous Trojans	52,416
11	Win32/Antivirus2008	Miscellaneous Potentially Unwanted Software	44,314
12	Win32/Playmp3z	Adware	41,399
13	Win32/SeekmoSearchAssistant	Adware	23,989
14	Win32/Tibs	Miscellaneous Trojans	22,212
15	Win32/C2Lop	Miscellaneous Trojans	20,595
16	Win32/PowerRegScheduler	Miscellaneous Potentially Unwanted Software	19,951
17	Win32/Winfixer	Miscellaneous Potentially Unwanted Software	19,049
18	Win32/APSB08-11	Exploits	17,880
19	Win32/ConHook	Miscellaneous Trojans	17,869
20	Win32/Starware	Miscellaneous Potentially Unwanted Software	17,322
21	Java/ByteVerify	Exploits	16,095
22	Win32/Alureon	Miscellaneous Trojans	15,109
23	Win32/Obfuscator	Miscellaneous Potentially Unwanted Software	14,450
24	Win32/WinSpywareProtect	Miscellaneous Trojans	14,360
25	Win32/Meredrop	Miscellaneous Trojans	14,204

For more information about these families, visit the Microsoft Malware Encyclopedia at www.microsoft.com/av.

Observations:

- The top 25 families were detected on 68.3 percent of all infected computers.
- The top three families in Canada (Win32/Renos, Win32/Zlob, and Win32/Vundo) are also the top three families worldwide, in that order.
- Win32/APSB08-11, the eighteenth most common family in Canada, is not among the 25 most common families worldwide, or in any other top location. Win32/APSB08-11 is an exploit for a vulnerability in Adobe Flash Player that can allow an attacker to download and execute malicious code on an infected computer. Adobe Systems has published security bulletin APSB08-11, available at http://www.adobe.com/support/security, which addresses the vulnerability.
- Four of the top 15 families detected in Canada in 2H08 (Win32/Renos, Win32/FakeXPA, Win32/FakeSecSen, and Win32/Antivirus2008) download rogue security software or display misleading warning messages to convince users to purchase a program that supposedly removes spyware.

Encyclopedia

Win32/APSB08-11:
A trojan that attempts to exploit a vulnerability in Adobe Flash Player. In the wild, this trojan has been used to download and execute arbitrary files, including other malware.

http://www.microsoft.com/av

Many families consist of multiple variants released by attackers in an effort to complicate the detection process. Figure 97 lists the top five individual threats detected in Canada in 2H08.

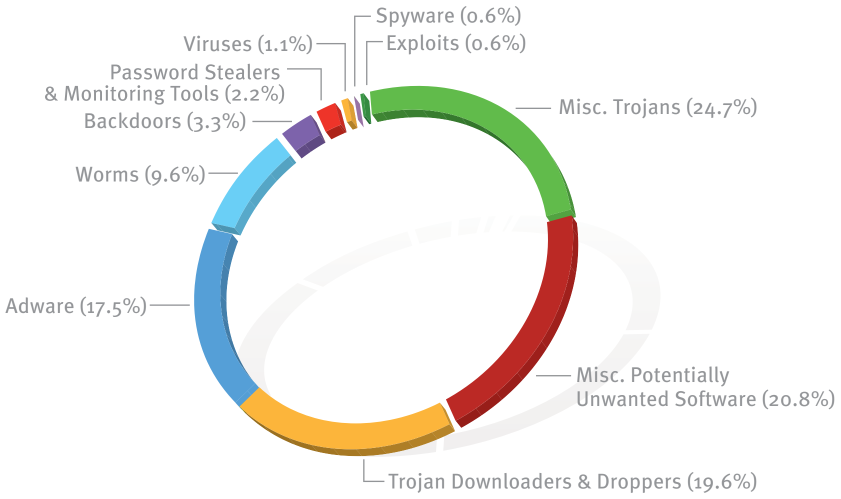
FIGURE 97. Top five individual threats in Canada in 2H08

Rank	Threat	Infected Computers
1	Adware:Win32/ZangoSearchAssistant	133,351
2	TrojanDownloader:ASX/Wimad.gen!A	93,079
3	TrojanDownloader:ASX/Wimad.T	64,887
4	Trojan:Win32/FakeXPA	60,418
5	Adware:Win32/Hotbar	57,225

France

The infection rate (CCM) for France was 7.8 percent in 2H08, which is comparable to the worldwide 2H08 infection rate of 8.6. Figure 98 and Figure 99 list the most common malware and potentially unwanted software categories and families detected by Microsoft security products in France in 2H08.

FIGURE 98. Malware and potentially unwanted software in France, by category, in 2H08



(Totals may not equal 100 percent due to rounding.)

Category	Infected Computers
Miscellaneous Trojans	599,668
Miscellaneous Potentially Unwanted Software	503,102
Trojan Downloaders & Droppers	474,384
Adware	423,697
Worms	233,527
Backdoors	80,909
Password Stealers & Monitoring Tools	53,093
Viruses	27,420
Spyware	14,709
Exploits	13,908

Observations:

- The threat landscape in France in 2H08 consisted mostly of malware, which accounted for 61.2 percent of all families removed from infected computers.
- 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 24.7 percent of all infected computers and accounts for 9 of the top 25 families.
- The second most common category in France was Miscellaneous Potentially Unwanted Software, which includes all potentially unwanted software families that are not classified as spyware or adware. It was detected on 20.8 percent of all infected computers. The most prevalent family in France in 2H08, Win32/SpywareSecure, is in this category.

FIGURE 99. Top 25 families in France in 2H08

Rank	Family	Most Significant Category	Infected Computers
1	Win32/SpywareSecure	Miscellaneous Potentially Unwanted Software	260,488
2	Win32/ZangoSearchAssistant	Adware	219,905
3	Win32/Vundo	Miscellaneous Trojans	201,085
4	Win32/Zlob	Trojan Downloaders & Droppers	186,353
5	Win32/Renos	Trojan Downloaders & Droppers	177,815
6	Win32/RJump	Worms	90,283
7	Win32/Hotbar	Adware	84,870
8	Win32/Taterf	Worms	78,450
9	Win32/MessengerSkinner	Trojan Downloaders & Droppers	74,428
10	Win32/FakeSecSen	Miscellaneous Trojans	73,444
11	Win32/ZangoShoppingreports	Adware	64,823
12	Win32/C2Lop	Miscellaneous Trojans	64,090
13	Win32/Playmp3z	Adware	63,340
14	Win32/Skintrim	Miscellaneous Trojans	49,402
15	Win32/Antivirus2008	Miscellaneous Potentially Unwanted Software	48,186
16	Win32/FakeXPA	Miscellaneous Trojans	47,842
17	ASX/Wimad	Trojan Downloaders & Droppers	43,566
18	Win32/Agent	Miscellaneous Trojans	39,149
19	Win32/Tibs	Miscellaneous Trojans	37,219
20	Win32/Winfixer	Miscellaneous Potentially Unwanted Software	34,664
21	Win32/SeekmoSearchAssistant	Adware	31,000
22	Win32/Matcash	Miscellaneous Trojans	29,307
23	Win32/AdRotator	Adware	28,938
24	Win32/Brontok	Worms	28,766
25	Win32/Wintrim	Miscellaneous Trojans	26,914

For more information about these families, visit the Microsoft Malware Encyclopedia at www.microsoft.com/av.

Encyclopedia

Win32/Skintrim: A trojan that downloads and executes arbitrary files. It may be distributed by as a Microsoft Office Outlook add-on used to display emoticons or other animated icons within e-mail messages.

http://www.microsoft.com/av

The top 25 families were detected on 70.6 percent of all infected computers in France during 2H08.

- The top family in France, Win32/SpywareSecure, was only twenty-first worldwide.
- The top four families worldwide (Win32/Renos, Win32/Zlob, Win32/Vundo, and Win32/ZangoSearchAssistant) were in the top five families detected in France during 2H08.
- Win32/ Skintrim, the fourteenth most common family in France, was not among the 25 most common families worldwide. Win32/ Skintrim is a trojan that downloads and executes arbitrary files, including updates and additional malware, from a predefined Web site, and displays advertisements. This trojan may be distributed by certain Web sites as a Microsoft Office Outlook add-on used to display "emoticons," (icons used to represent emotions) or other animated icons within e-mail messages.
- Five of the top 20 families detected in France in 2H08 (Win32/SpywareSecure, Win32/Renos, Win32/FakeSecSen, Win32/Antivirus2008, and Win32/FakeXPA) download rogue security software or display misleading warning messages to convince users to purchase a program that supposedly removes spyware.

Many families consist of multiple variants released by attackers in an effort to complicate the detection process. Figure 100 lists the top five individual threats detected in France in 2H08.

FIGURE 100. Top five individual threats in France in 2H08

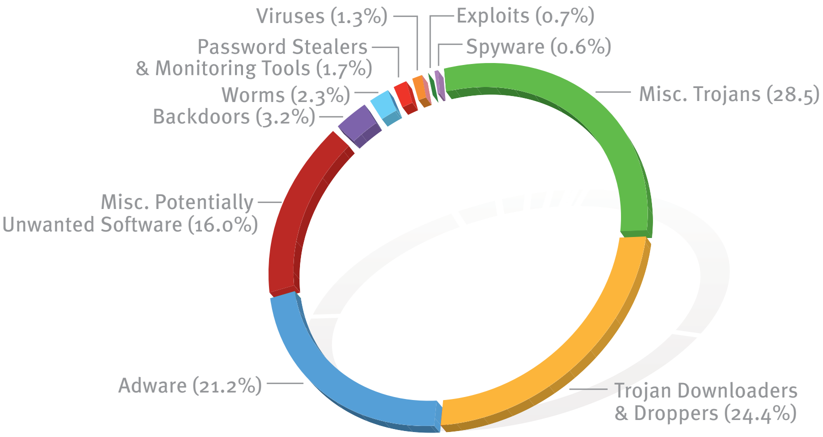
Rank	Threat	Infected Computers
1	Program:Win32/SpywareSecure	260,488
2	Adware:Win32/ZangoSearchAssistant	219,900
3	Adware:Win32/Hotbar	84,870
4	TrojanDropper:Win32/MessengerSkinner	74,428
5	Trojan:Win32/FakeSecSen	73,444

Germany

The infection rate (CCM) for Germany was 3.6 in 2H08, which is significantly lower than the worldwide 2H08 infection rate of 8.6. Figure 101 and Figure 102 list the most common malware and potentially unwanted software categories and families detected by Microsoft security products in Germany in 2H08.

FIGURE 101. Malware and potentially unwanted software in Germany, by category, in 2H08

Category	Infected Computers
Miscellaneous Trojans	452,874
Trojan Downloaders & Droppers	387,609
Adware	336,807
Miscellaneous Potentially Unwanted Software	254,803
Backdoors	51,164
Worms	37,065
Password Stealers & Monitoring Tools	26,504
Viruses	21,155
Exploits	11,307
Spyware	9,383



(Totals may not equal 100 percent due to rounding.)

Observations:

- The threat landscape in Germany was dominated by malware, which accounted for 62.2 percent of all families detected on infected computers 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 28.5 percent of all infected computers and accounts for 10 of the top 25 families.
- The second most common category in Germany was Trojan Downloaders & Droppers. It accounted for 24.4 percent of all infected computers and included the two most prevalent families found. Miscellaneous Trojans and Trojan Downloaders & Droppers made up more than 50 percent of all families detected on infected computers in Germany in 2H08.

FIGURE 102. Top 25 families in Germany in 2H08

Rank	Family	Most Significant Category	Infected Computers
1	Win32/Renos	Trojan Downloaders & Droppers	200,035
2	Win32/Zlob	Trojan Downloaders & Droppers	185,701
3	Win32/ZangoSearchAssistant	Adware	175,802
4	Win32/Vundo	Miscellaneous Trojans	146,392
5	Win32/Hotbar	Adware	74,850
6	Win32/SpywareSecure	Miscellaneous Potentially Unwanted Software	66,016
7	Win32/FakeSecSen	Miscellaneous Trojans	64,986
8	Win32/ZangoShoppingreports	Adware	53,911
9	Win32/SeekmoSearchAssistant	Adware	45,800
10	Win32/FakeXPA	Miscellaneous Trojans	40,978
11	Win32/Playmp3z	Adware	38,470
12	Win32/Agent	Miscellaneous Trojans	36,843
13	Win32/Antivirus2008	Miscellaneous Potentially Unwanted Software	33,482
14	Win32/Alureon	Miscellaneous Trojans	29,794
15	Win32/Winfixer	Miscellaneous Potentially Unwanted Software	27,869
16	Win32/Busky	Miscellaneous Trojans	26,865
17	Win32/Tibs	Miscellaneous Trojans	22,931
18	Win32/WinSpywareProtect	Miscellaneous Trojans	21,070
19	Win32/WhenU	Adware	20,923
20	Win32/Meredrop	Miscellaneous Trojans	20,791
21	Win32/Matcash	Miscellaneous Trojans	19,513
22	Win32/RealVNC	Miscellaneous Potentially Unwanted Software	19,225
23	Win32/MessengerSkinner	Trojan Downloaders & Droppers	18,033
24	Win32/AdRotator	Adware	17,422
25	Win32/Advantage	Adware	17,074

For more information about these families, visit the Microsoft Malware Encyclopedia at www.microsoft.com/av.

Observations:

- The top 25 families were detected on 72.5 percent of all infected computers in Germany during 2H08.
- The top four families worldwide (Win32/Renos, Win32/Zlob, Win32/Vundo, and Win32/ZangoSearchAssistant) were also the top four families detected in Germany during 2H08, although not in that order.

Four of the top 10 families detected in Germany in 2H08 (Win32/Renos, Win32/SpywareSecure, Win32/FakeSecSen, and Win32/FakeXPA) download rogue security software or display misleading warning messages to convince users to purchase a program that supposedly removes spyware.

Many families consist of multiple variants released by attackers in an effort to complicate the detection process. Figure 103 lists the top five individual threats detected in Germany in 2H08.

FIGURE 103. Top five individual threats in Germany in 2H08

Rank	Threat	Infected computers
1	Adware:Win32/ZangoSearchAssistant	175,798
2	Adware:Win32/Hotbar	74,850
3	Program:Win32/SpywareSecure	66,016
4	Trojan:Win32/FakeSecSen	64,986
5	Trojan:Win32/Vundo.gen!R	52,286

Encyclopedia

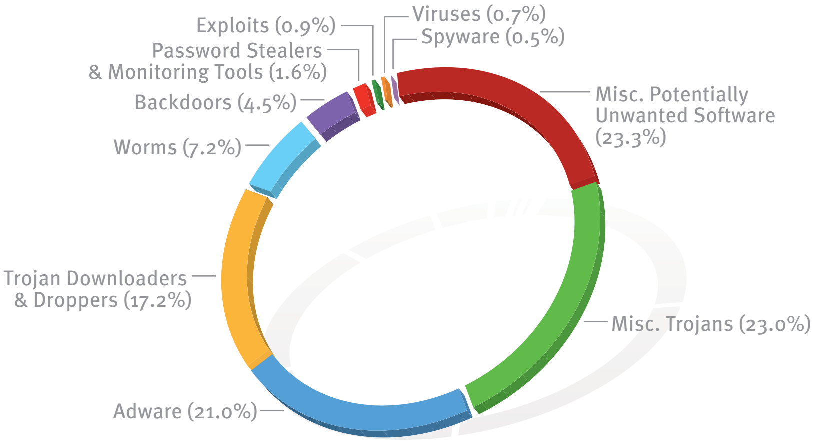
Win32/SpywareSecure: A program that displays misleading warning messages in order to convince users to purchase a product that removes spyware.

http://www.microsoft.com/av

Italy

The infection rate (CCM) for Italy was 5.8 percent in 2H08, which is significantly lower than the worldwide 2H08 infection rate of 8.6. Figure 104 and Figure 105 list the most common malware and potentially unwanted software categories and families detected by Microsoft security products in Italy in 2H08.

FIGURE 104. Malware and potentially unwanted software in Italy, by category, in 2H08



(Totals may not equal 100 percent due to rounding.)

Category	Infected computers
Miscellaneous Potentially Unwanted Software	307,816
Miscellaneous Trojans	304,423
Adware	276,796
Trojan Downloaders & Droppers	227,283
Worms	95,614
Backdoors	59,581
Password Stealers & Monitoring Tools	21,076
Exploits	12,335
Viruses	9,901
Spyware	6,211

Observations:

- The threat landscape in Italy was dominated by malware, which accounted for 55.3 percent of all families detected on infected computers in 2H08.
- The most common category in Italy was Miscellaneous Potentially Unwanted Software, which includes all potentially unwanted software families that are not classified as spyware or adware. It was detected on 23.3 percent of all infected computers in 2H08.
- The second most common category in Italy was Miscellaneous Trojans, which includes all trojan families that are not classified as downloaders/droppers or backdoors. It was detected on 23 percent of all infected computers in 2H08.

FIGURE 105. Top 25 families in Italy in 2H08

Rank	Family	Most Significant Category	Infected Computers
1	Win32/ZangoSearchAssistant	Adware	187,869
2	Win32/SpywareSecure	Miscellaneous Potentially Unwanted Software	143,388
3	Win32/Renos	Trojan Downloaders & Droppers	89,820
4	Win32/Vundo	Miscellaneous Trojans	89,527
5	Win32/Zlob	Trojan Downloaders & Droppers	84,746
6	Win32/ZangoShoppingreports	Adware	62,445
7	Win32/Hotbar	Adware	62,338
8	Win32/Winfixer	Miscellaneous Potentially Unwanted Software	41,157
9	Win32/RJump	Worms	37,740
10	Win32/C2Lop	Miscellaneous Trojans	33,481
11	Win32/FakeSecSen	Miscellaneous Trojans	29,820
12	Win32/Skintrim	Miscellaneous Trojans	28,101
13	Win32/FakeXPA	Miscellaneous Trojans	27,609
14	Win32/Taterf	Worms	26,964
15	Win32/MessengerSkinner	Trojan Downloaders & Droppers	25,440
16	Win32/Agent	Miscellaneous Trojans	24,930
17	Win32/Antivirus2008	Miscellaneous Potentially Unwanted Software	23,906
18	Win32/Rustock	Backdoors	19,224
19	Win32/Tibs	Miscellaneous Trojans	17,207
20	Win32/Playmp3z	Adware	17,030
21	Win32/Horst	Miscellaneous Trojans	16,928
22	Win32/Rbot	Backdoors	15,500
23	Win32/Alureon	Miscellaneous Trojans	14,808
24	Win32/SeekmoSearchAssistant	Adware	13,990
25	Win32/Mobis	Adware	13,894

For more information about these families, visit the Microsoft Malware Encyclopedia at www.microsoft.com/av.

Observations:

- The top 25 families were detected on 69.4 percent of all infected computers in Italy during 2H08.
- The top four families worldwide (Win32/Renos, Win32/Zlob, Win32/Vundo, and Win32/ZangoSearchAssistant) appeared in the top five families detected in Italy during 2H08.
- Five of the top 15 families detected in Italy in 2H08 (Win32/SpywareSecure, Win32/Renos, Win32/Winfixer, Win32/FakeSecSen, and Win32/FakeXPA) download rogue security software or display misleading warning messages to convince users to purchase a program that supposedly removes spyware.

Many families consist of multiple variants released by attackers in an effort to complicate the detection process. Figure 106 lists the top five individual threats detected in Italy in 2H08.

FIGURE 106. Top five individual threats in Italy in 2H08

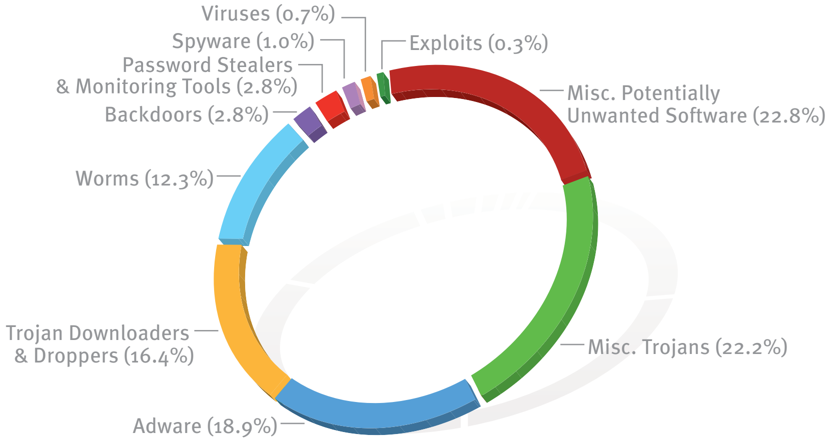
Rank	Threat	Infected Computers
1	Adware:Win32/ZangoSearchAssistant	187,868
2	Program:Win32/SpywareSecure	143,388
3	Adware:Win32/Hotbar	62,338
4	Adware:Win32/ZangoShoppingreports	53,904
5	Program:Win32/WinFixer	41,157

Malaysia

The infection rate (CCM) for Malaysia was 3.5 in 2H08, which is significantly lower than the worldwide 2H08 infection rate of 8.6. Figure 107 and Figure 108 list the most common malware and potentially unwanted software categories and families detected by Microsoft security products in Malaysia in 2H08.

FIGURE 107. Malware and potentially unwanted software in Malaysia, by category, in 2H08

Category	Infected Computers
Miscellaneous Potentially Unwanted Software	22,020
Miscellaneous Trojans	21,425
Adware	18,257
Trojan Downloaders & Droppers	15,830
Worms	11,931
Backdoors	2,709
Password Stealers & Monitoring Tools	2,695
Spyware	930
Viruses	646
Exploits	247



(Totals may not equal 100 percent due to rounding.)

Observations:

- The threat landscape in Malaysia consisted mainly of malware, which accounted for 57.4 percent of all families detected on infected computers in 2H08.
- The most common category in Malaysia was Miscellaneous Potentially Unwanted Software, which includes all potentially unwanted software families that are not classified as spyware or adware. It was detected on 22.8 percent of all infected computers in 2H08.
- The second most common category in Malaysia was Miscellaneous Trojans, which includes all trojan families that are not classified as downloaders/droppers or backdoors. It was detected on 22.2 percent of all infected computers in 2H08.

FIGURE 108. Top 25 families in Malaysia in 2H08

Rank	Family	Most Significant Category	Infected Computers
1	Win32/ZangoSearchAssistant	Adware	9,583
2	Win32/Zlob	Trojan Downloaders & Droppers	8,944
3	Win32/Renos	Trojan Downloaders & Droppers	7,713
4	Win32/BaiduSobar	Miscellaneous Potentially Unwanted Software	6,500
5	Win32/RJump	Worms	5,601
6	Win32/Vundo	Miscellaneous Trojans	5,274
7	Win32/ZangoShoppingreports	Adware	4,559
8	Win32/SeekmoSearchAssistant	Adware	4,541
9	Win32/Sogou	Miscellaneous Potentially Unwanted Software	4,495
10	Win32/Hotbar	Adware	4,173
11	Win32/Taterf	Worms	3,778
12	Win32/FakeXPA	Miscellaneous Trojans	3,141
13	Win32/Antivirus2008	Miscellaneous Potentially Unwanted Software	2,512
14	Win32/FakeSecSen	Miscellaneous Trojans	2,382
15	Win32/Agent	Miscellaneous Trojans	2,207
16	Win32/Playmp3z	Adware	2,085
17	Win32/Starware	Miscellaneous Potentially Unwanted Software	1,569
18	Win32/VB	Miscellaneous Trojans	1,353
19	Win32/Advantage	Adware	1,301
20	Win32/C2Lop	Miscellaneous Trojans	1,233
21	Win32/RealVNC	Miscellaneous Potentially Unwanted Software	1,182
22	Win32/Winfixer	Miscellaneous Potentially Unwanted Software	1,086
23	Win32/Meredrop	Miscellaneous Trojans	1,028
24	Win32/Brontok	Worms	1,006
25	Win32/WinSpywareProtect	Miscellaneous Trojans	893

For more information about these families, visit the Microsoft Malware Encyclopedia at www.microsoft.com/av.

Observations:

- The top 25 families were detected on 74.7 percent of all infected computers in Malaysia during 2H08.
- The top four families worldwide (Win32/Renos, Win32/Zlob, Win32/Vundo, and Win32/ZangoSearchAssistant) appeared in the top six families detected in Malaysia during 2H08.
- Six of the top 25 families detected in Malaysia in 2H08 (Win32/Renos, Win32/FakeXPA, Win32/Antivirus2008, Win32/FakeSecSen, and Win32/Winfixer) download rogue security software or display misleading warning messages to convince users to purchase a program that supposedly removes spyware.

Many families consist of multiple variants released by attackers in an effort to complicate the detection process. Figure 109 lists the top five individual threats detected in Malaysia in 2H08.

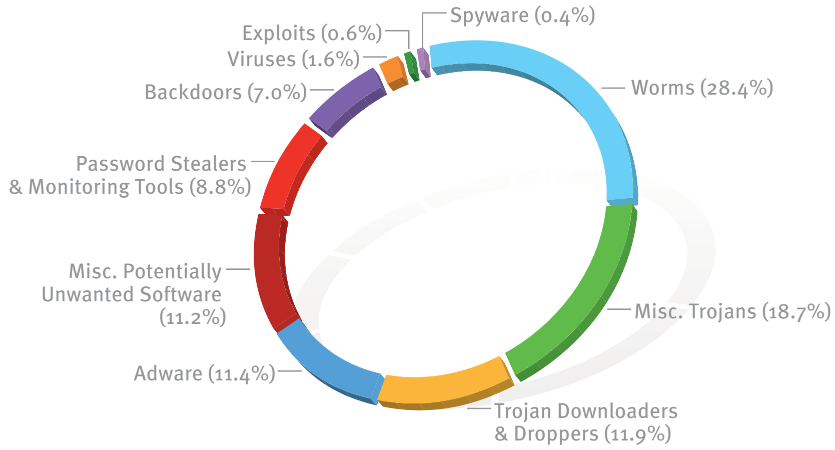
FIGURE 109. Top five individual threats in Malaysia in 2H08

Rank	Threat	Infected Computers
1	Adware:Win32/ZangoSearchAssistant	9,581
2	BrowserModifier:Win32/BaiduSobar	6,500
3	Worm:Win32/RJump.J	4,560
4	Adware:Win32/SeekmoSearchAssistant	4,541
5	Program:Win32/Sogou	4,495

Mexico

The infection rate (CCM) for Mexico was 15.9 in 2H08, which is significantly higher than the worldwide 2H08 infection rate of 8.6. Figure 110 and Figure 111 list the most common malware and potentially unwanted software categories and families detected by Microsoft security products in Mexico in 2H08.

FIGURE 110. Malware and potentially unwanted software in Mexico, by category, in 2H08



(Totals may not equal 100 percent due to rounding.)

Category	Infected Computers
Worms	360,964
Miscellaneous Trojans	238,059
Trojan Downloaders & Droppers	150,962
Adware	145,126
Miscellaneous Potentially Unwanted Software	142,288
Password Stealers & Monitoring Tools	111,342
Backdoors	88,935
Viruses	20,843
Exploits	7,715
Spyware	5,422

Observations:

- The threat landscape in Mexico was clearly dominated by malware, which accounted for 77.0 percent of all families detected on infected computers in 2H08.
- The most common category in Mexico was Worms, which was detected on 28.4 percent of all infected computers in 2H08. It is unusual for worms to rank so highly for a location; worldwide, worms made up only 11.3 percent of the total families removed in 2H08.
- The second most common category in Mexico was Miscellaneous Trojans, which includes all trojan families that are not classified as downloaders/droppers or backdoors. It was detected on 18.7 percent of all infected computers in 2H08.

FIGURE 111. Top 25 families in Mexico in 2H08

Rank	Family	Most Significant Category	Infected Computers
1	Win32/Taterf	Worms	156,886
2	Win32/Slenfbot	Worms	98,664
3	Win32/ZangoSearchAssistant	Adware	73,794
4	Win32/Hamweq	Worms	66,699
5	Win32/Vundo	Miscellaneous Trojans	62,871
6	Win32/Brontok	Worms	56,527
7	Win32/Zlob	Trojan Downloaders & Droppers	56,086
8	Win32/Frethog	Password Stealers & Monitoring Tools	52,836
9	Win32/Renos	Trojan Downloaders & Droppers	48,204
10	Win32/Autorun	Worms	46,935
11	Win32/Agent	Miscellaneous Trojans	45,115
12	Win32/C2Lop	Miscellaneous Trojans	42,744
13	Win32/Ldpinch	Password Stealers & Monitoring Tools	38,430
14	ASX/Wimad	Trojan Downloaders & Droppers	34,138
15	Win32/PossibleHostsFileHijack	Miscellaneous Potentially Unwanted Software	32,373
16	Win32/Playmp3z	Adware	30,661
17	Win32/Sdbot	Backdoors	30,630
18	Win32/Hotbar	Adware	27,843
19	Win32/Rbot	Backdoors	25,907
20	Win32/ZangoShoppingreports	Adware	24,436
21	Win32/FakeXPA	Miscellaneous Trojans	18,998
22	Win32/FakeSecSen	Miscellaneous Trojans	18,735
23	WIN32/VB	Miscellaneous Trojans	17,125
24	Win32/DelfInject	Miscellaneous Potentially Unwanted Software	12,117
25	Win32/Antivirus2008	Miscellaneous Potentially Unwanted Software	11,773

For more information about these families, visit the Microsoft Malware Encyclopedia at www.microsoft.com/av.

Observations:

- The top 25 families were detected on 69.4 percent of all infected computers.
- The top two families in Mexico during 2H08 were both worms. Win32/Taterf is a family of worms that spreads through mapped drives to steal login and account details for popular online games. Win32/Slenfbot is a worm that can spread through MSN Messenger and may spread through removable drives. This worm spreads automatically through shares but must be ordered to spread through Messenger by a remote attacker. The worm also contains backdoor functionality that allows unauthorized access to an affected machine.
- The top four families worldwide (Win32/Renos, Win32/Zlob, Win32/Vundo, and Win32/ZangoSearchAssistant) were in the top 10 families in Mexico during 2H08, although not in that order.
- The number four family in Mexico in 2H08 was Win32/Hamweq. This worm spreads through removable drives, such as USB memory sticks. It contains an IRC-based backdoor, which may be used by a remote attacker to order the affected computer to participate in Distributed Denial of Service attacks or to download and execute arbitrary files.

Many families consist of multiple variants released by attackers in an effort to complicate the detection process. Figure 112 lists the top five individual threats detected in Mexico in 2H08.

FIGURE 112. Top five individual threats in Mexico in 2H08

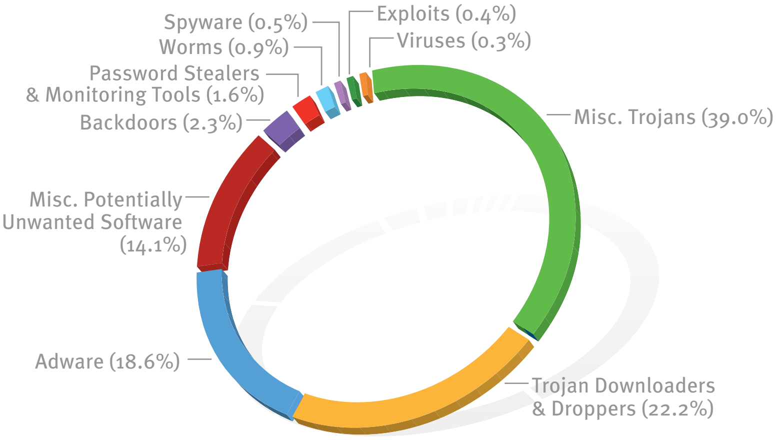
Rank	Threat	Infected Computers
1	Worm:Win32/Taterf.gen!C	79,036
2	Worm:Win32/Slenfbot	75,731
3	Adware:Win32/ZangoSearchAssistant	73,791
4	Worm:Win32/Taterf!inf	72,847
5	Worm:Win32/Hamweq!inf	58,139

Norway

The infection rate (CCM) for Norway was 6.8 in 2H08, which is significantly lower than the worldwide 2H08 infection rate of 8.6. Figure 113 and Figure 114 list the most common malware and potentially unwanted software categories and families detected by Microsoft security products in Norway in 2H08.

FIGURE 113. Malware and potentially unwanted software in Norway, by category, in 2H08

Category	Infected Computers
Miscellaneous Trojans	102,053
Trojan Downloaders & Droppers	58,108
Adware	48,653
Miscellaneous Potentially Unwanted Software	36,834
Backdoors	6,127
Password Stealers & Monitoring Tools	4,068
Worms	2,239
Spyware	1,415
Exploits	1,125
Viruses	786



(Totals may not equal 100 percent due to rounding.)

Observations:

- The threat landscape in Norway was dominated by malware, which accounted for 66.8 percent of all families detected on infected computers 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 39 percent of all infected computers and 11 of the top 25 families.
- The second most common category in Norway was Trojan Downloaders & Droppers. It accounted for 22.2 percent of all infected computers and included two of the three most prevalent families found. Together, Miscellaneous Trojans and Trojan Downloaders & Droppers made up more than 60 percent of all families detected on infected computers in Norway in 2H08.

FIGURE 114. Top 25 families in Norway in 2H08

Rank	Family	Most Significant Category	Infected Computers
1	Win32/Vundo	Miscellaneous Trojans	58,344
2	Win32/Renos	Trojan Downloaders & Droppers	30,630
3	Win32/Zlob	Trojan Downloaders & Droppers	28,224
4	Win32/ZangoSearchAssistant	Adware	20,712
5	Win32/FakeSecSen	Miscellaneous Trojans	16,335
6	Win32/ZangoShoppingreports	Adware	11,934
7	Win32/Playmp3z	Adware	11,720
8	Win32/Hotbar	Adware	10,334
9	Win32/FakeXPA	Miscellaneous Trojans	8,415
10	Win32/Antivirus2008	Miscellaneous Potentially Unwanted Software	7,068
11	Win32/Winfixer	Miscellaneous Potentially Unwanted Software	6,401
12	Win32/SeekmoSearchAssistant	Adware	6,326
13	Win32/Tibs	Miscellaneous Trojans	4,588
14	Win32/ConHook	Miscellaneous Trojans	4,259
15	Win32/Busky	Miscellaneous Trojans	3,794
16	Win32/WinSpywareProtect	Miscellaneous Trojans	3,582
17	Win32/AdRotator	Adware	3,555
18	Win32/Agent	Miscellaneous Trojans	3,427
19	Win32/Vapsup	Miscellaneous Potentially Unwanted Software	3,184
20	Win32/C2Lop	Miscellaneous Trojans	3,098
21	Win32/Cutwail	Trojan Downloaders & Droppers	2,940
22	Win32/Alureon	Miscellaneous Trojans	2,932
23	Win32/Advantage	Adware	2,721
24	Win32/Meredrop	Miscellaneous Trojans	2,515
25	Win32/BrowsingEnhancer	Adware	2,514

For more information about these families, visit the Microsoft Malware Encyclopedia at www.microsoft.com/av.

Observations:

- The top 25 families were detected on 80 percent of all infected computers.
- The top four families worldwide (Win32/Renos, Win32/Zlob, Win32/Vundo, and Win32/ZangoSearchAssistant) were also the top four families in Norway during 2H08, although not in that order.
- Five of the top 11 families detected in Norway in 2H08 (Win32/Renos, Win32/FakeSecSen, Win32/FakeXPA, Win32/Antivirus2008, and Win32/Winfixer) download rogue security software or display misleading warning messages to convince users to purchase a program that supposedly removes spyware.

Many families consist of multiple variants released by attackers in an effort to complicate the detection process. Figure 115 lists the top five individual threats detected in Norway in 2H08.

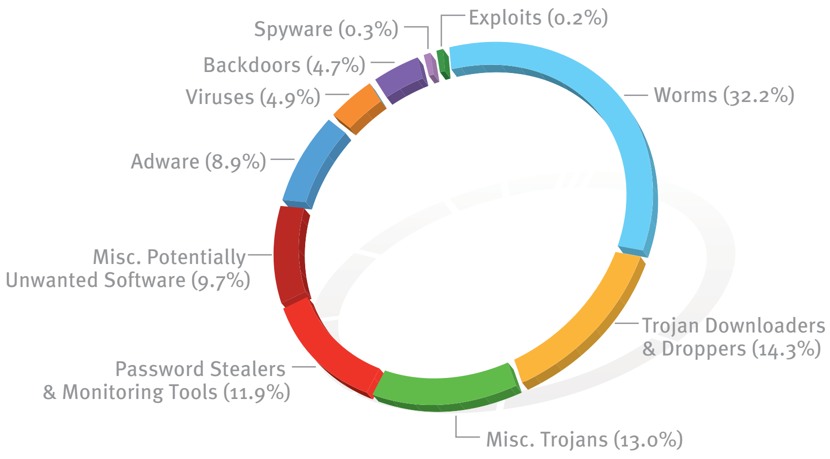
FIGURE 115. Top five individual threats in Norway in 2H08

Rank	Threat	Infected Computers
1	Trojan:Win32/Vundo.BR	23,213
2	Trojan:Win32/Vundo.gen!V	20,905
3	Adware:Win32/ZangoSearchAssistant	20,710
4	Trojan:Win32/FakeSecSen	16,335
5	Adware:Win32/Playmp3z	11,720

Russia

The infection rate (CCM) for Russia was 21.1 in 2H08, which is significantly higher than the worldwide 2H08 infection rate of 8.6. Figure 116 and Figure 117 list the most common malware and potentially unwanted software categories and families detected by Microsoft security products in Russia in 2H08.

FIGURE 116. Malware and potentially unwanted software in Russia, by category, in 2H08



(Totals may not equal 100 percent due to rounding.)

Category	Infected Computers
Worms	231,147
Trojan Downloaders & Droppers	102,727
Miscellaneous Trojans	93,376
Password Stealers & Monitoring Tools	85,517
Miscellaneous Potentially Unwanted Software	69,721
Adware	63,966
Viruses	35,096
Backdoors	33,798
Spyware	2,056
Exploits	1,460

Observations:

- The threat landscape in Russia was clearly dominated by malware, which accounted for 81.1 percent of all families detected on infected computers in 2H08.
- The most common category in Russia was Worms, which was detected on 32.2 percent of all infected computers in 2H08. It is unusual for worms to rank so highly for a location; worldwide, worms made up only 11.3 percent of the total families removed in 2H08. Four of the top 12 families detected on infected computers in Russia in 2H08 were worms.
- The second most common category in Russia was Trojan Downloaders & Droppers. It was detected on 14.3 percent of all infected computers and included 3 of the 10 most prevalent families found.

FIGURE 117. Top 25 families in Russia in 2H08

Rank	Family	Most Significant Category	Infected Computers
1	Win32/Taterf	Worms	179,216
2	Win32/Renos	Trojan Downloaders & Droppers	59,882
3	Win32/Frethog	Password Stealers & Monitoring Tools	52,529
4	Win32/Cutwail	Trojan Downloaders & Droppers	37,455
5	Win32/Jeefo	Viruses	29,255
6	Win32/RJump	Worms	27,306
7	Win32/Ldpinch	Password Stealers & Monitoring Tools	21,895
8	Win32/Wukill	Worms	18,155
9	Win32/Zlob	Trojan Downloaders & Droppers	17,323
10	Win32/Vundo	Miscellaneous Trojans	17,184
11	Win32/WhenU	Adware	15,300
12	Win32/Brontok	Worms	14,397
13	Win32/Advantage	Adware	13,962
14	Win32/BitAccelerator	Miscellaneous Potentially Unwanted Software	12,589
15	Win32/Sezon	Adware	10,816
16	Win32/RuPass	Miscellaneous Trojans	10,139
17	Win32/Meredrop	Miscellaneous Trojans	9,558
18	Win32/Agent	Miscellaneous Trojans	9,536
19	Win32/Rbot	Backdoors	9,460
20	Win32/FakeXPA	Miscellaneous Trojans	9,443
21	Win32/Alureon	Miscellaneous Trojans	8,347
22	Win32/ZangoShoppingreports	Adware	8,019
23	Win32/Tibs	Miscellaneous Trojans	7,169
24	Win32/GhostRadmin	Miscellaneous Potentially Unwanted Software	6,068
25	Win32/Rustock	Backdoors	5,794

For more information about these families, visit the Microsoft Malware Encyclopedia at www.microsoft.com/av.

Observations:

- The top 25 families were detected on 81 percent of all infected computers in Russia during 2H08.
- The top family in Russia, Win32/Taterf, is a family of worms that spreads through mapped drives to steal login and account details for popular online games.
- The top three families worldwide (Win32/Renos, Win32/Zlob, and Win32/Vundo) were second, ninth, and tenth, respectively, in Russia during 2H08. The number 4 family worldwide, Win32/ZangoSearchAssistant, did not appear in the top 25 in Russia.

Many families consist of multiple variants released by attackers in an effort to complicate the detection process. Figure 118 lists the top five individual threats detected in Russia in 2H08.

FIGURE 118. Top five individual threats in Russia in 2H08

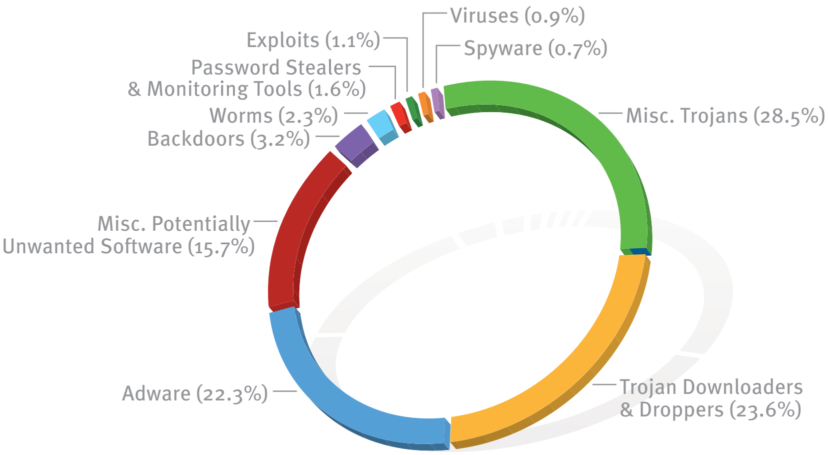
Rank	Threat	Infected Computers
1	Worm:Win32/Taterf!inf	112,301
2	Worm:Win32/Taterf.A.dll	60,008
3	Worm:Win32/Taterf.gen!C	59,381
4	Worm:Win32/Taterf.B.dll	50,598
5	PWS:Win32/Frethog.D	36,830

United Kingdom

The infection rate (CCM) in the United Kingdom was 5.7 in 2H08, which is significantly lower than the worldwide 2H08 infection rate of 8.6. Figure 119 and Figure 120 list the most common malware and potentially unwanted software categories and families detected by Microsoft security products in the United Kingdom in 2H08.

FIGURE 119. Malware and potentially unwanted software in the United Kingdom, by category, in 2H08

Category	Infected Computers
Miscellaneous Trojans	831,506
Trojan Downloaders & Droppers	689,709
Adware	650,310
Miscellaneous Potentially Unwanted Software	458,168
Backdoors	93,481
Worms	66,956
Password Stealers & Monitoring Tools	45,954
Exploits	33,471
Viruses	27,352
Spyware	20,105



(Totals may not equal 100 percent due to rounding.)

Observations:

- The threat landscape in the United Kingdom was dominated by malware, which accounted for 61.3 percent of all families detected on infected computers 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 was detected on 28.5 percent of all infected computers and 9 of the top 20 families.
- The second most common category in the United Kingdom was Trojan Downloaders & Droppers. It was detected on 23.6 percent of all infected computers and included two of the three most prevalent families found. Together, Miscellaneous Trojans and Trojan Downloaders & Droppers made up more than 50 percent of all families detected on infected computers in the United Kingdom in 2H08.

FIGURE 120. Top 25 families in the United Kingdom in 2H08

Rank	Family	Most Significant Category	Infected Computers
1	Win32/ZangoSearchAssistant	Adware	400,596
2	Win32/Renos	Trojan Downloaders & Droppers	329,368
3	Win32/Zlob	Trojan Downloaders & Droppers	325,628
4	Win32/Vundo	Miscellaneous Trojans	270,021
5	Win32/ZangoShoppingreports	Adware	205,727
6	Win32/Hotbar	Adware	179,861
7	Win32/FakeSecSen	Miscellaneous Trojans	125,321
8	Win32/FakeXPA	Miscellaneous Trojans	112,358
9	Win32/Antivirus2008	Miscellaneous Potentially Unwanted Software	86,509
10	ASX/Wimad	Trojan Downloaders & Droppers	84,944
11	Win32/Playmp3z	Adware	83,190
12	Win32/Agent	Miscellaneous Trojans	74,978
13	Win32/SeekmoSearchAssistant	Adware	67,773
14	Win32/C2Lop	Miscellaneous Trojans	60,333
15	Win32/Meredrop	Miscellaneous Trojans	50,837
16	Win32/Winfixer	Miscellaneous Potentially Unwanted Software	50,750
17	Win32/Tibs	Miscellaneous Trojans	48,411
18	Win32/Starware	Miscellaneous Potentially Unwanted Software	42,831
19	Win32/WinSpywareProtect	Miscellaneous Trojans	39,107
20	Win32/ConHook	Miscellaneous Trojans	36,127
21	Win32/Vapsup	Miscellaneous Potentially Unwanted Software	33,488
22	Win32/OneStepSearch	Miscellaneous Potentially Unwanted Software	33,409
23	Win32/Alureon	Miscellaneous Trojans	33,397
24	Win32/Oderoor	Backdoors	32,556
25	Win32/AdRotator	Adware	30,723

For more information about these families, visit the Microsoft Malware Encyclopedia at www.microsoft.com/av.

Observations:

The top 25 families were detected on 73.2 percent of all infected computers in the United Kingdom during 2H08.

- The top four families worldwide (Win32/Renos, Win32/Zlob, Win32/Vundo, and Win32/ZangoSearchAssistant) were also the top four families detected in the United Kingdom during 2H08, although not in that order.
- Four of the top 10 families detected in the United Kingdom in 2H08 (Win32/Renos, Win32/FakeSecSen, Win32/FakeXPA, and Win32/Antivirus2008) download rogue security software or display misleading warning messages to convince users to purchase a program that supposedly removes spyware.

Many families consist of multiple variants released by attackers in an effort to complicate the detection process. Figure 121 lists the top five individual threats detected in the United Kingdom in 2H08.

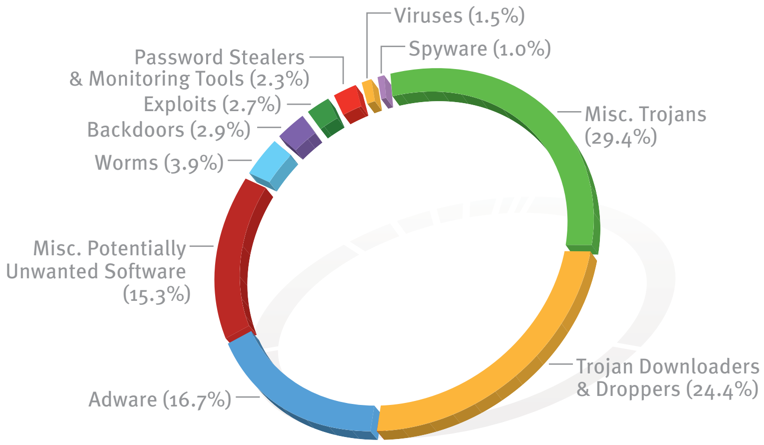
FIGURE 121. Top five individual threats in the United Kingdom in 2H08

Rank	Threat	Infected Computers
1	Adware:Win32/ZangoSearchAssistant	400,562
2	Adware:Win32/Hotbar	179,861
3	Adware:Win32/ZangoShoppingreports	173,699
4	Trojan:Win32/FakeSecSen	125,321
5	Trojan:Win32/FakeXPA	112,358

United States

The infection rate (CCM) for the United States was 9.1 in 2H08, which is comparable to the worldwide 2H08 infection rate of 8.6. Figure 122 and Figure 123 list the most common malware and potentially unwanted software categories and families detected by Microsoft security products in the United States in 2H08.

FIGURE 122. Malware and potentially unwanted software in the United States, by category, in 2H08



(Totals may not equal 100 percent due to rounding.)

Category	Infected Computers
Miscellaneous Trojans	5,501,628
Trojan Downloaders & Droppers	4,569,041
Adware	3,117,308
Miscellaneous Potentially Unwanted Software	2,870,384
Worms	732,193
Backdoors	542,307
Exploits	496,921
Password Stealers & Monitoring Tools	436,968
Viruses	271,522
Spyware	182,692

Observations:

- The threat landscape in the United States was dominated by malware, which accounted for 67.0 percent of all families detected on infected computers 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 was detected on 29.4 percent of all infected computers and 10 of the top 23 families.
- The second most common category in the United States was Trojan Downloaders & Droppers. It was detected on 24.4 percent of all infected computers and included the two most prevalent families found. Together, Miscellaneous Trojans and Trojan Downloaders & Droppers made up more than 50 percent of all families detected on infected computers in the United States in 2H08.

FIGURE 123. Top 25 families in the United States in 2H08

Rank	Family	Most Significant Category	Infected Computers
1	Win32/Renos	Trojan Downloaders & Droppers	2,278,716
2	Win32/Zlob	Trojan Downloaders & Droppers	1,764,039
3	Win32/Vundo	Miscellaneous Trojans	1,620,165
4	Win32/ZangoSearchAssistant	Adware	1,414,794
5	Win32/FakeXPA	Miscellaneous Trojans	1,102,250
6	Win32/ZangoShoppingreports	Adware	900,313
7	Win32/FakeSecSen	Miscellaneous Trojans	848,491
8	ASX/Wimad	Trojan Downloaders & Droppers	685,589
9	Win32/Hotbar	Adware	668,702
10	Win32/Agent	Miscellaneous Trojans	615,302
11	Win32/Antivirus2008	Miscellaneous Potentially Unwanted Software	591,185
12	Win32/Tibs	Miscellaneous Trojans	478,118
13	Win32/SeekmoSearchAssistant	Adware	371,041
14	Win32/Playmp3z	Adware	368,601
15	Win32/GameVance	Adware	353,020
16	Win32/Winfixer	Miscellaneous Potentially Unwanted Software	311,829
17	Win32/ConHook	Miscellaneous Trojans	280,981
18	Win32/Taterf	Worms	276,325
19	Win32/OneStepSearch	Miscellaneous Potentially Unwanted Software	273,950
20	Win32/Yektel	Miscellaneous Trojans	262,384
21	Win32/Matcash	Miscellaneous Trojans	255,486
22	Win32/Busky	Miscellaneous Trojans	202,537
23	Win32/Alureon	Miscellaneous Trojans	196,754
24	Win32/PowerRegScheduler	Miscellaneous Potentially Unwanted Software	186,796
25	Win32/Starware	Miscellaneous Potentially Unwanted Software	185,976

For more information about these families, visit the Microsoft Malware Encyclopedia at www.microsoft.com/av.

Observations:

- The top 25 families were detected on 65.2 percent of all infected computers in the United States during 2H08.
- The top four families worldwide (Win32/Renos, Win32/Zlob, Win32/Vundo, and Win32/ZangoSearchAssistant) were also the top four families detected in the United States during 2H08, in that order.
- Five of the top 20 families detected in the United States in 2H08 (Win32/Renos, Win32/FakeXPA, Win32/FakeSecSen, Win32/Antivirus2008, and Win32/Winfixer) download rogue security software or display misleading warning messages to convince users to purchase a program that supposedly removes spyware.

Many families consist of multiple variants released by attackers in an effort to complicate the detection process. Figure 124 lists the top five individual threats detected in the United States in 2H08.

FIGURE 124. Top five individual threats in the United States in 2H08

Rank	Threat	Infected Computers
1	Adware:Win32/ZangoSearchAssistant	1,414,588
2	Trojan:Win32/FakeXPA	1,102,250
3	Trojan:Win32/FakeSecSen	848,491
4	Adware:Win32/Hotbar	668,702
5	Adware:Win32/ZangoShoppingreports	655,359

Appendix C: Data Sources

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 (CVE) 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 (DHS). The naming mechanisms and external references to sources for additional information were particularly valuable.
- National Vulnerability Database (NVD) 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 (OSF) that 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.

Microsoft Security Products

Telemetry from several customer-focused Microsoft security products and services, including the Malicious Software Removal Tool (MSRT), Windows Defender, Windows Live OneCare, and Microsoft Forefront Online Security for Exchange (formerly Exchange Hosted Services), representing a total user base of several hundred million computers, was used to compile the trends and information provided in this report. Figure 125 shows the main data sources used in this report to compile data on the prevalence of malicious and potentially unwanted software.

FIGURE 125. Data sources

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		
Windows Malicious Software Removal Tool	●		Prevalent Malware Families				●	Windows Update/ Automatic Updates, Download Center
Windows Defender	●				●	●	●	Download Center, Windows Vista
Windows Live OneCare Safety Scanner	●		●		●		●	Web
Windows Live OneCare	●		●	●	●	●		Web / Store Purchase
Forefront Online Security for Exchange		●	●	●				Web
Forefront Client Security		●	●	●	●	●		Volume Licensing

The 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 (WU), Microsoft Update (MU), and Automatic Updates (AU). A version of the tool is also available from the Microsoft Download Center.

The MSRT helps remove specific, prevalent malware from computers that are running Windows Vista, Windows XP, Windows Server 2008, Windows Server 2003, and Windows 2000. As of December 2008, the tool detects and removes 119 different malware families, most of which are currently prevalent or were prevalent at the time they were added. The MSRT is not a replacement for an up-to-date antivirus solution because of its lack of real-time protection and also because it uses only the portion of the Microsoft antivirus signature database that enables it to target specifically selected, prevalent malicious software.

By the end of 2H08, the MSRT was executing on hundreds of millions of computers worldwide every month. More than 95 percent of those executions involved operating system versions (such as Windows XP SP2 and Windows Vista) that encourage users to enable Windows Automatic Updates, which allows the MSRT to download and execute automatically.

Windows Live OneCare is a real-time protection product that combines an antivirus and antispyware scanner with phishing and firewall protection. Unlike the MSRT, which targets a small number of currently active malware families and is issued monthly, Windows Live OneCare uses the complete Microsoft antivirus signature database, retrieving a signature file update daily from Microsoft servers. Unlike the MSRT, which can be downloaded freely by compatible versions of Windows, Windows Live OneCare is a commercial product, offered for purchase by individuals and enterprise customers on a subscription basis. In 2009, Microsoft will discontinue retail sales of Windows Live OneCare and will offer a new, streamlined anti-malware solution, code-named “Morro,” at no charge to licensed users of Windows.

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 Windows Live OneCare safety scanner is available worldwide in dozens of different languages and was used to remove infections from computers 3.5 million times in 2H08.

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. By the end of 2H08, Windows Defender was installed on more than 90 million computers running Windows XP SP2 and later, Windows Server 2003, Windows Vista, and Windows Server 2008—in more than two dozen different languages. Windows Defender is included with Windows Vista and as part of the Desktop Experience feature of Windows Server 2008, and it is also made available as a separate download for users of other operating system versions.

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.

Microsoft Forefront Online Security for Exchange (formerly Microsoft Exchange Hosted Services) offers a number of online tools to help organizations protect their e-mail infrastructures. The spam and malware protection feature incorporates multiple edge blocks and filters to actively help protect businesses' inbound and outbound e-mail from spam, viruses, phishing scams, and e-mail policy violations.

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.

Beginning in 2H08, the Microsoft Live Search search engine offers protection against drive-by downloads in search results. As Live Search crawls 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 Live Search index. Instead, clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software. Live Search works with webmasters to inform them about compromised sites through the Live Search Webmaster Center (http://webmaster.live.com) and provides guidance for the removal of malicious code so pages can be re-enabled in the index.

If you would like more information about the products, services, and tools used as data sources for this report, please use the URLs provided below.

- The Microsoft Malware Protection Center Portal
  http://www.microsoft.com/av
- Windows Malicious Software Removal Tool
  http://www.microsoft.com/malwareremove

- Windows Defender
  http://www.microsoft.com/windowsdefender
- Windows Live OneCare
  http://onecare.live.com
- Codename "Morro" Announcement
  http://www.microsoft.com/Presspass/press/2008/nov08/11-18NoCostSecurityPR.mspx
- Windows Live OneCare safety scanner
  http://onecare.live.com/scan
- Live Search
  http://www.live.com
- Phishing Filter (Internet Explorer 7)
  http://www.microsoft.com/protect/products/yourself/phishingfilter.mspx
- SmartScreen Filter (Internet Explorer 8)
  http://www.microsoft.com/windows/internet-explorer/beta/features/stay-safer-online.aspx
- Microsoft Forefront Client Security
  http://www.microsoft.com/clientsecurity
- Microsoft Forefront Security for Exchange Server
  http://www.microsoft.com/forefront/serversecurity/exchange/download.mspx
- Microsoft Forefront Online Security for Exchange
  http://www.microsoft.com/fose
- Microsoft Online Safety Technologies (anti-spam and anti-phishing)
  http://www.microsoft.com/safety
- Sender ID Framework
  http://www.microsoft.com/senderid

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 mil* (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 500 computers, the CCM for that location in January is 10.0. 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.

disclosure

Revelation of the existence of a vulnerability to a third party. Also see *responsible disclosure.*

disinfect

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

downloader/dropper

See *trojan downloader/dropper.*

exploit

Malicious code that takes advantage of software vulnerabilities to infect a computer.

firewall

A program or device that monitors and regulates traffic between two points, such as a single computer and the network server, or one server to another.

IFrame

Short for *inline frame*. An IFrame is an HTML document that is embedded in another HTML document. Because the IFrame loads another Web page, it can be used by criminals to place malicious HTML content, such as a script that downloads and installs spyware, into non-malicious HTML pages hosted by trusted Web sites.

in the wild

Said of malware that is currently detected in active computers connected to the Internet, as compared to those confined to internal test networks, malware research laboratories, or malware sample lists.

keylogger

See *password stealer (PWS).*

Malicious Software Removal Tool (MSRT)

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

malware

Malicious software or potentially unwanted software installed without adequate user consent.

malware impression

A single instance of a user attempting to visit a site 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 site, with Internet Explorer 7 or Internet Explorer 8, and being blocked by the Phishing Filter or SmartScreen Filter. Also see *malware impression.*

potentially unwanted software

A program with potentially unwanted behavior that is brought to the user's attention for review. This behavior may impact the user's privacy, security, or computing experience.

remote control software

A program that provides access to a computer from a remote location. These programs are often installed by the computer owner or administrator and are only a risk if unexpected.

responsible disclosure

The practice of disclosing vulnerabilities privately to an affected vendor so it can develop a comprehensive security update to address the vulnerability before it becomes public knowledge.

rogue security software

Software that appears to be beneficial from a security perspective but provides limited or no security capabilities, generates a significant number of erroneous or misleading alerts, or attempts to socially engineer the user into participating in a fraudulent transaction.

Sender ID Framework

An Internet Engineering Task Force (IETF) protocol developed to authenticate e-mail to detect spoofing and forged e-mail with the typical tactic to drive users to phishing Web sites and to download malicious software.

social engineering

A technique that defeats security precautions in place by exploiting human vulnerabilities. Social engineering scams can be both online (such as receiving e-mails that ask you to click the attachment, which is actually malware) and offline (such as receiving a phone call from someone posing as a representative from your credit card company). Regardless of the method selected, the purpose of a social engineering attack remains the same—to get the targeted user to perform an action of the attacker's choice.

spam

Bulk unsolicited e-mail. Malware authors may use spam to distribute malware, either by attaching the malware to the message or by sending a message containing a link to the malware. Malware may also harvest e-mail addresses for spamming from compromised machines or may use compromised machines to send spam.

spear phishing

Phishing that targets a specific person, organization, or group, containing additional information associated with that person, organization, or group to lure the target further into a false sense of security to divulge more sensitive information.

spyware

A program that collects information, such as the Web sites a user visits, without adequate consent. Installation may be without prominent notice or without the user's knowledge.

SQL injection

A technique in which an attacker enters a specially crafted Structured Query Language (SQL) statement into an ordinary Web form. If form input is not filtered and validated before being submitted to a database, the malicious SQL statement may be executed, which could cause significant damage or data loss.

tool

Software that may have legitimate purposes but may also be used by malware authors or attackers.

trojan

A generally self-contained program that does not self-replicate but takes malicious action on the computer.

trojan downloader/dropper

A form of trojan that installs other malicious files to the infected system either by downloading them from a remote computer or by dropping them directly from a copy contained in its own code.

virus

Malware that replicates, commonly by infecting other files in the system, thus allowing the execution of the malware code and its propagation when those files are activated.

vulnerability

A weakness, error, or poor coding technique in a program that may allow an attacker to exploit it for a malicious purpose. Also see *parser vulnerability.*

vulnerability broker

A company or other entity that provides software vendors with vulnerability information provided to it by external security researchers. In exchange for such compensation as the broker may provide, the security researchers agree not to disclose any information about the vulnerability to anyone other than the broker and the affected vendor.

whaling

Phishing that targets senior executives and other high-ranking people within a company or group.

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.