Microsoft Security Intelligence Report

January through June 2008

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

Authors

Vinny Gullotto
Microsoft Malware Protection Center

Joe Faulhaber
Microsoft Malware Protection Center

Jeffrey Friedberg
Trustworthy Computing

Jeff Jones
Trustworthy Computing

Jimmy Kuo
Microsoft Malware Protection Center

John Lambert
Security Science

Ziv Mador
Microsoft Malware Protection Center

Mike Reavey
Microsoft Security Response Center

Adam Shostack
Security Engineering

George Stathakopoulos
Microsoft Security Response Center

Scott Wu
Microsoft Malware Protection Center

Jeff Williams
Microsoft Malware Protection Center

Contributors

Daniel Bohm
Exchange Hosted Services (EHS)

Doug Cavit
Trustworthy Computing

Marisela Cerda
Windows Live OneCare

Ziv Fass
Trustworthy Computing

Bruce Fenske
Trustworthy Computing

Dave Forstrom
Trustworthy Computing

Michael Grady
Trustworthy Computing

Satomi Hayakawa
Japan Security Response Center

Yuhui Huang
Microsoft Malware Protection Center

Japan Security Response Team
Microsoft Japan

Jeannette Jarvis
Customer Support Services

Hong Jia
Microsoft Malware Protection Center

David Kennedy
Microsoft Legal and Corporate Affairs

Yi Liao
Exchange Hosted Services (EHS)

Ken Malcolmson
Trustworthy Computing

Bronwen Matthews
Trustworthy Computing

Mark Miller
Trustworthy Computing

Ritesh Mordani
Exchange Hosted Services (EHS)

Aaron Putnam
Microsoft Malware Protection Center

Tim Rains
Trustworthy Computing

Marc Seinfeld
Microsoft Malware Protection Center

Matt Thomlinson
Security Science

Jaime Wong
Microsoft Malware Protection Center

Terry Zink
Exchange Hosted Services (EHS)

External Contributors

Paul Henry

John Schramm

Isaiah Sarju

Key Findings

This report provides the Microsoft perspective on the security and privacy threat landscape over the six-month period from January through June 2008. The lists below summarize the key points from the main sections of the report.

Vulnerability Trends

- The total number of unique vulnerability disclosures across the industry decreased in 1H08, down 4 percent from 2H07 and down 19 percent from 1H07.
- Vulnerability disclosures in Microsoft software in 1H08 continued a multi-period downward trend, both in terms of all disclosures and relative to total industry disclosures.
- In contrast, vulnerabilities rated as High severity by the Common Vulnerability Scoring System (CVSS) increased 13 percent over 2H07, with roughly 48 percent of all vulnerabilities receiving a severity rating of High. This nevertheless represents a 28 percent decline from 1H07.
- Across the entire industry, the percentage of disclosed vulnerabilities rated as Low complexity (and therefore easiest to exploit) also increased, with 56 percent receiving a complexity rating of Low.
- The proportion of vulnerabilities disclosed in operating systems continues to decline; more than 90 percent of vulnerabilities disclosed in 1H08 affected applications, rather than operating systems.

Vulnerability Exploit Details

- In 1H08, 32 percent of vulnerabilities disclosed in Microsoft software had publicly available exploit code, consistent with the trends observed in previous volumes of this report.
- In testing the reliability of the software vulnerability exploits released, only 10.4 percent of vulnerabilities had publicly available exploit code that could consistently be used to exploit the vulnerability; the rest were either unreliable or ineffective.

Browser-Based Exploits

- The most common system locale for victims of browser-based exploits was Chinese, accounting for 47 percent of all incidents, followed by US English with 23 percent of incidents.

- For browser-based attacks on Windows XP-based machines, Microsoft vulnerabilities accounted for 42 percent of the total. On Windows Vista-based machines, however, the proportion of vulnerabilities attacked in Microsoft software was much smaller, accounting for just 6 percent of the total.
- Microsoft software accounted for 5 of the top 10 browser-based vulnerabilities attacked on computers running Windows XP in 1H08, compared to zero of the top 10 on computers running Windows Vista.

Security Breach Trends

- As in 2H07, the top reason reported for data loss through a security breach in 1H08 was stolen equipment, such as stolen laptop computers. 37.2 percent of all data-loss incidents reported were attributed to stolen equipment.
- A much smaller percentage—less than 23 percent—of reported security breaches in 1H08 resulted from incidents classified as "hack" attacks, representing a slight increase over 2H07.

Malicious and Potentially Unwanted Software

- In 1H08, the total amount of malware and potentially unwanted software removed from computers worldwide increased by more than 43 percent compared to 2H07.
- Although patterns of malware detected and removed by Microsoft security products varied across countries and regions, trojan downloaders and droppers constituted more than 30 percent of all malware removed by Microsoft security products worldwide. This trend builds on the significant increases in the volume of trojan downloaders and droppers detected over the past several years.[1]
- As a general rule, infection rates tend to be higher in developing countries/regions than in developed countries/regions, as reported by the Malicious Software Removal Tool (MSRT).
- The infection rate for Windows Vista is significantly lower than that of its predecessor, Windows XP, at any service pack level.
- The infection rates for the 64-bit editions of Windows Vista were both lower than those of their 32-bit counterparts.
- For each version of the operating system, higher service pack levels meant lower rates of infection. This trend can be observed consistently across client and server operating systems half-year period over half-year period.

[1] See previous volumes of the Microsoft Security Intelligence Report at http://www.microsoft.com/sir.

E-Mail Threats

- Many e-mail systems block incoming attached files of types that are often used to transmit malware. In 1H08, eight extensions accounted for 99.8 percent of the attachments blocked by Microsoft Exchange Hosted Services, with just two extensions—.html and .zip—accounting for 97.8 percent of blocked attachments.
- The threat most blocked by Exchange Hosted Services in 1H08—by a wide margin—was HTML/IframeRef, which was blocked more than seven times as often as the second-most prevalent threat. The security update that addresses the particular vulnerability targeted by this exploit was released by Microsoft in December 2004.

Spam and Phishing Trends

- Microsoft Exchange Hosted Services blocked more than 90 percent of messages received over the Internet in 1H08, similar to the trend observed in 2H07.
- Advertisements for pharmaceutical products accounted for 51.5 percent of the spam messages blocked by Exchange Hosted Services in 1H08, with advertisements for sexual performance products, such as Viagra and Cialis, accounting for the majority of those (30.6 percent of the overall total); in most cases, the advertisements are fraudulent. Non-pharmaceutical product advertisements account for another 19.9 percent of the total.
- Of the remainder, most involve overt scams, like "pump and dump" stock schemes and fraudulent university diplomas.
- Phishing attacks only accounted for 2.5 percent of the total number of e-mail messages blocked.
- The total number of active phishing pages at any one time remained roughly consistent throughout 1H08.
- Though U.S.-based financial institutions remain the most frequent target for phishing attempts, Microsoft phishing researchers have seen a gradual move toward targets located in other English-speaking countries, notably the United Kingdom and India.

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 fifth 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 first half of 2008 (1H08), 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 nHyy, where nH 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), while 2H07 represents the period covering the second half of 2007 (July 1 through December 31).

Structure

This report is divided into two main sections. The first, *Trends and Analysis*, begins on page 11. This section presents a high-level overview of security-related trends and occurrences from the first half of 2008, covering vulnerabilities, exploits, breach data, malware and potentially unwanted software, and spam and phishing. Microsoft security professionals have provided their informed analysis of the trends observed during the past six months, and this analysis is presented in this section.

The second section, *Supporting Data and Details*, begins on page 73, and provides more in-depth data relating to many of the subject areas listed above. This section also includes a closer look at the local security landscape for several different locations around the world, as well as a sampling of data from individual Microsoft products.

Data Sources

If you are interested in the products, services, tools, and Web sites used to provide the data for this report, please see the appendix.

Table of Contents

Supporting Data and Details

Executive Foreword

Welcome to the fifth volume of Microsoft's Security Intelligence Report. Every day, you face tough decisions. Microsoft® is committed to providing you with the most relevant and authoritative information so that you can make informed decisions to better manage your risk.

Two years ago, Microsoft released its first Security Intelligence Report. Since then, we have worked extremely hard to evolve and continually enrich this semi-annual report, drawing telemetry from hundreds of millions of computers worldwide to provide our customers, partners, and industry with a more comprehensive and accurate understanding of the threat environment.

Our Security Intelligence Report helps direct Microsoft's security and privacy efforts, product development, and in turn allows us to better adapt to the ever-changing threat landscape. This latest volume confirms that Microsoft is making real progress in securing its products through established processes like our Security Development Lifecycle (SDL). For instance, during the first half of 2008 (1H08), there were fewer disclosures of Microsoft vulnerabilities than for the industry as a whole; in fact, Microsoft vulnerabilities were down 33.6 percent in 1H08.

However, it is alarming to see that more than 90 percent of vulnerabilities disclosed in 1H08 affected applications, and nearly half of all industry vulnerabilities are rated as High Severity. Additionally, 1H08 showed how threats are increasingly affecting a variety of vendors beyond Microsoft. Issues now cross multiple vendors and illustrate how different technologies behave together and then create complex, blended threats. Quite simply, these issues are becoming increasingly taxing for everyone. To protect themselves and secure their systems, networks and mobile devices, customers now must possess an indispensable knowledge of the threat landscape and be more vigilant than ever. Looking at recent major events, such as the DNS cache poisoning vulnerability, cross-site scripting (XSS) threats and poorly-coded ActiveX® controls, it is clear that no single company can manage this alone. Increased industry collaboration and partnership is needed; more than ever, now is the time for community-based defense.

While we have worked hard to get our house in order, we are resolved to foster deeper industry collaboration and share the lessons we have learned to help others with their security journey. We are extending our knowledge about developing secure code by taking our SDL process, training and tools to the software development community, as well as advancing best practices through the new SDL partner network. We bolstered our commitment and pledge for industry collaboration by finding new ways to share information, via new programs such as the Microsoft Active Protections Program (MAPP) and our active involvement in the Industry Consortium for Advancement of Security on the Internet (ICASI). We are addressing the shift in vulnerabilities targeting applications on the Windows platform by forming Microsoft Vulnerability Research (MSVR), which will actively research vulnerabilities in the third-party software most commonly used by Windows customers and then work with vendors to produce updates.

In closing, I'd like to point out that this volume has undergone some notable changes. This includes a new overall layout containing a shorter, more impactful core section, called *Trends and Analysis*. The additional in-depth data that backs up our analysis has been moved to its own section, called *Supporting Data and Details*. As always, we value your feedback, so please let us know what you think by emailing sirfb@microsoft.com. I hope you enjoy reading this report.

George Stathakopoulos

General Manager, Microsoft Product Security
Security Engineering and Communications Group, Trustworthy Computing Group

Trends and Analysis

The Threat Ecosystem

Jimmy Kuo, Microsoft Malware Protection Center
Jeffrey Friedberg, Trustworthy Computing

Malware and other computer security threats come in many shapes and sizes, and they enter the lives of computer users from every direction. There are names and classifications, such as trojans, viruses, botnets, downloaders, and backdoors, and many more colorful descriptors. As specialists in this industry, we often assume that our readers and listeners know what all these terms mean. Still, even specialists sometimes don't have a full understanding of how and why threats get from the keyboards of their creators to the computers and bank accounts of their victims. In this section, we'd like to present an overview of the underground economy of computer crime and how it operates.

The Players

Much of what we know about the environment in which computer criminals operate comes from the criminal cases that have been pursued by law enforcement agencies worldwide. In recent years, increased attention on the part of law enforcement to the problem of computer crime has led to a number of high-profile arrests and trials:

- In 2007, the U.S. Federal Bureau of Investigation announced Operation Bot Roast,[2] an initiative to disrupt and dismantle botnets and bring bot-herders to justice. (See "Anatomy of a Botnet," beginning on page 14, to learn about botnets and how they operate.) To date, 10 individuals have pled, been indicted, or been sentenced in connection with Operation Bot Roast, including developers and distributors of botnet control software and people who used botnets to steal confidential information, defraud people and institutions, and damage computer networks. Microsoft contributed to this effort.
- In Germany, following an 18-month investigation, 10 people were arrested for using a botnet to send phishing e-mail messages masquerading as correspondence from Deutsche Telekom AG, eBay International AG, 1&1 Internet AG, and others. These e-mail messages enticed the recipients to install trojans on their computers that captured the victims' bank account information and transmitted it to the criminals, who then used it to transfer funds out of the victims' accounts. Although the banks were able to stop many of the transfers, the criminals still managed to make off with enough funds to support a rather luxurious lifestyle and plenty of expensive jewelry and cars.
- In Israel, a number of corporate executives have been arrested for allegedly ordering the installation of backdoor programs into competitors' computers to conduct industrial espionage. These programs enabled remote control of the computers and allowed the culprits to transfer picture files and documents from infected computers to intermediate storage locations for retrieval.

[2] For more information, see http://www.fbi.gov/pressrel/pressrel07/botroast112907.htm.

From these and other cases, and through the efforts of researchers at Microsoft and elsewhere, we have been able to piece together a picture of an underground economy in which malware and computer crime services are bought and sold in a black market environment with some remarkable similarities to mainstream commerce.

Despite the growing prevalence of malware, the number of active skilled malware creators may actually be quite small. Although the Microsoft Malware Protection Center analyzes millions of unique malware samples every year, almost all of these are variations belonging to existing malware families, many of which are themselves simply modifications of other families. When Sven Jaschen, the 17-year-old creator of the Win32/Sasser and Win32/Netsky worms, was arrested by German authorities in 2004, as much as 80 percent of the malware code in active circulation at the time was believed to have ultimately originated from him. These statistics are a reason to be optimistic that pursuing and prosecuting the creators can be an effective strategy for combating the spread of malware.

So, who are the creators? Like Jaschen, they tend to be young—in their late teens or early twenties. Many appear to have only tenuous connections to the criminal groups or individuals who ultimately use their code, and they may not know or care how it is used. Owen Walker, an 18-year-old malware writer from New Zealand, who was arrested in November 2007 and went by the name "AKILL" online, made almost NZD$40,000 (about U.S.$28,000 or €19,000) renting out his botnet to adware companies, according to police documents.

Malware buyers and sellers meet using a network of "black market" Web sites designed for exactly that purpose. These sites present a remarkably professional appearance, both outwardly and in the way they operate to match buyers with sellers. Many sites take steps to hide themselves from search engines and use word of mouth, or the online equivalent of it, to promote themselves to prospective buyers and sellers. The discerning criminal can assemble a full attack campaign from the range of specialized offerings at such sites, with few or no questions asked.

FIGURE 1. Black market sites often have a slick, professional appearance

The sites themselves are typically organized around discussion forums, which are divided into multiple subforums focusing on different interests and types of crime. Graphics and layouts are often slick and polished, sometimes with an organized crime motif. Many sites feature a strong anti-U.S. theme.

Much like legitimate online shopping sites, black market sites prominently feature product reviews. In keeping with the familiar adage about the lack of honor among thieves, the malware marketplace is plagued by scam artists, or "rippers" as they are

called, who sell products using false or misleading claims. New sellers with no reputation submit their malware to independent reviewers who are well-known on the forum, who then assess the malware's features and shortcomings for prospective buyers and may even rate the malware using a grade or numeric scale.

Prices are usually quoted in U.S. dollar equivalents, regardless of the nationality of the seller or the prospective buyers, and business is transacted using electronic money transfer systems that provide mutual anonymity to both parties. To close the deal, the seller typically gives an instant messaging (IM) account that buyers can contact privately. To guard against rippers, some sites even offer an escrow service that holds and verifies payments until the buyers have received their merchandise.

Mechanisms

The days are past when worms spread wildly over the Internet and tried to gain control of your computer almost immediately after you turned it on. Such spectacles garnered the quick attention of law enforcement and usually resulted in bad news for the perpetrators. Worms still spread on the Internet today, but on a much smaller scale. Today's computer criminals operate in secrecy, using deception and subterfuge to attract their victims, who may never even know their computers are infected.

Anatomy of a Botnet

A *botnet* is a network of compromised computers that are controlled remotely and surreptitiously by one or more individuals, called *bot-herders*. Computers in the botnet, called *nodes* or *zombies*, are usually ordinary computers with always-on broadband connections, sitting on desktops in homes and offices around the world. Usually, computers belong to botnets because their owners or users have been tricked into installing malware that secretly connects the computer to the botnet and performs tasks like sending spam, hosting malware or other illegal files, and attacking other computers. Often the user never knows his or her computer is being used for nefarious ends.

A botnet is in many ways the perfect base of operations for computer criminals. Botnet malware is designed to operate in the background, without any visible evidence of its existence. Often the victim has no idea that his or her computer is infected and so is less likely to subject it to a malware scan that might detect and remove the infection. By keeping a low profile, botnets are sometimes able to remain active and operational for years. Botnets are also attractive to criminals because they provide an effective mechanism for covering the tracks of the botnet user—tracing the origin of an attack leads back to the hijacked computer of an innocent user, where the trail ends.

Getting a botnet up and running is only the first step. A botnet can be used as a platform for a variety of criminal activities, depending on how the bot-herders choose to configure the individual nodes. In addition to identity theft, botnets have many uses, including:

- **Sending spam**. Much of the spam sent today originates from botnets, which use several different techniques to get their unwanted messages past recipients' mail filters. (See "Spam and Phishing Trends," on page 67, for more information.) In addition to renting out the botnet to spammers, bot-herders also send spam themselves in an effort to increase the size of the network, as described in "Malware Distribution," on page 16.
- **Perpetrating distributed denial of service (DDoS) attacks**. In a DDoS attack, multiple computers attack a target server (typically a Web server) by flooding it with traffic, saturating the target's bandwidth, and rendering it effectively unavailable to other users. Criminals sometimes threaten companies with DDoS in an effort to extort money from them, or they launch DDoS attacks against security researchers or others they believe have wronged them. DDoS has even been used in "cyber-warfare" attacks launched against countries or regions.
- **Hosting malware or illegal content**. Peer-to-peer (P2P) networks are effective mechanisms for retrieving or distributing media content. They work like search engines to locate media that people have made available. Some content is illegal, either to own or to distribute, so criminals often use hijacked computers as a place to store illegal content. Unwitting owners of hijacked computers may be delivered lawsuit papers by rightful content owners for distributing copyrighted material—or arrested by police for distributing child pornography. Hijacked computers are also used to host Web pages used in phishing attacks and to host and distribute additional malware.
- **Perpetrating click fraud**. Criminals sometimes use botnets to generate fraudulent "clicks" on pay-per-click advertisements, such as those hosted by some search engines and other Web sites. The advertiser pays a fee to the advertising network for every click its advertisement receives, so click fraud can be used to financially harm a competitor.

The most common method used for controlling botnets is Internet Relay Chat (IRC), a distributed system for real-time chatting. When the botnet is installed on a victim's computer, it connects to an IRC channel that the bot-herder has established and waits for instructions. From there, all the bot-herder has to do to activate the bots is connect to the channel and type in some predefined commands, and they're off—sending spam, launching DDoS attacks, hosting phishing pages, or whatever else the herder has in mind. Recently, botnets have even used P2P mechanisms for command and control, making them more difficult to shut down once discovered.

Malware Distribution

The first task of a botnet is self-preservation. It is constantly trying to add more or better computers to its army. To accomplish this, bot-herders attract new victims using a number of different methods to lure them. The most common method bot-herders use to deliver lures is spam. The typical spam lure consists of an e-mail message with an enticing subject line reflecting popular interests and intended to appeal to primal emotions and urges, like empathy, guilt, desire, sex, and fear. Many subject lines use fictitious and incendiary topics, often inspired by contemporary headlines. For example, the Win32/Nuwar worm is sometimes called the *storm worm*, a nickname inspired by an early subject line, "230 dead as storm batters Europe," used to propagate the worm in the wake of a severe winter storm that devastated parts of Europe in January 2007.

The body of the message typically contains a link to a URL that the recipient is supposed to click for more information pertaining to the subject line. In reality, the URL can point to a number of different objects, the most direct of which is a link to a trojan. Named after the legendary Trojan Horse of *The Aeneid*, a trojan is a program that "promises" one thing to the recipient but delivers another. Trojans may masquerade as media codecs, security software, browser toolbars, registry cleaners, or other useful software. In all cases, the goal is to convince an unsuspecting user to install the software knowingly and intentionally.

Most malware distributed today includes some trojan characteristics, so security researchers make further distinctions between different subcategories of trojans based on their primary functions. Trojans are especially pernicious because they use a variety of social engineering techniques to convince the user to ignore anti-malware product warnings, operating system alerts, and other technical hurdles by offering an attractive incentive, such as free software, salacious video content, or amusing animated icons. Privilege-separation techniques, such as User Account Control in Windows Vista® or the **sudo** command in Linux and Mac OS X, are of limited effectiveness in stopping trojans because in most cases the victims are simply doing exactly what they think they are doing—installing new software. The most effective defense against trojans is real-time antivirus and anti-malware software that is capable of detecting the trojan and alerting the user.

One specialized type of trojan is called a *downloader*. Downloaders are small programs designed to download and install larger programs or sets of programs, called *packages*, to the infected computer. Downloaders are used to make the initial infection as small and unobtrusive as possible, so as not to provoke suspicion by the user being attacked. They are also employed when the attackers haven't yet decided what to use the infected computers for, or if they are working on behalf of another group that has hired the attackers to deliver a set of infected computers to them for their own purposes.

A similar and related type of program is called a *backdoor*. Backdoors are generally more complex programs with the ability to respond to a set of commands, among which would be a set of "download and update self" commands. The more persistent botnets use backdoor programs that update themselves constantly in an effort to evade detection and removal by anti-malware programs.

Security researchers are in a constant battle with the botnet controllers to develop tools to remove the malware from newly infected computers before the programs can be updated to versions that the tools cannot yet recognize. Using a regularly updated antivirus program that offers real-time protection can also help prevent users from being infected in the first place.

Another way botnets use e-mail to lure new victims is by sending messages containing a URL to a Web page that includes many exploits for vulnerabilities in operating systems and other programs. A *vulnerability* is a weakness in a computer system that can be attacked to produce undesired results, such as the execution of malicious code. Unlike trojans, which must be deliberately executed by the user, an exploit can often install itself without the user's control or knowledge by taking advantage of a vulnerability. Such exploits pose no danger to computers that have had the appropriate security updates applied, but spammers calculate that a significant percentage of users who receive the e-mail and click the link will not have taken advantage of these protections and will become infected via one or more exploits.

Using a regularly updated antivirus program that offers real-time protection can also help prevent users from being infected in the first place.

As with trojan downloaders, the exploit itself is typically very small, in part to minimize the chances that it will be noticed and in part because the nature of the vulnerability being exploited often does not allow a large amount of code to execute. Often the only job of the exploit code is to download and install a package from a Web site or file transfer protocol (FTP) site, which itself is typically on another infected computer in the botnet.

Spam is not the only distribution mechanism for malware. Criminals have used the emerging popularity of instant messaging (IM) systems and social networking sites to infect users that are drawn to these modes of communication. Among younger Internet users, e-mail is giving way to IM conversations or posting messages on each others' "walls." Fundamentally, though, these modes of communication involve transmitting short messages back and forth, just like e-mail, which means they can be used to transmit links to Web pages hosting malware.

In fact, attacks that involve social networks can be much more effective than e-mail–based attacks because they involve infiltrating and exploiting the considerable level of trust users place in their friends. (See "Phishers Targeting Social Networks," beginning on page 69, for details of how attackers infiltrate social networks.) Once inside, the attackers use social engineering techniques to distribute links to dangerous sites, as described earlier. Social

networking sites and the IM mechanism have security measures that provide users with the ability to finely control who can contact them. As a result, users tend to be less skeptical than they are of e-mail message senders and more likely to believe that the originator of the message is truly the person they expect it to be. This inherent trust can also be found with other communication mechanisms, such as Caller ID and mobile phone text messaging, that currently have a relatively low frequency of attacks.

Similarly, criminals use cross-site scripting (XSS) attacks to exploit another form of inherent trust that people use when browsing Web pages. In an XSS attack, the attacker infiltrates a legitimate Web page by either adding additional code to the page (via an exploit on the computer hosting the page) or by infiltrating an existing iFrame on the page, such as one created to show a legitimate banner advertisement. (See "E-Mail Threats," beginning on page 58, for more information about iFrame vulnerabilities and exploits.) A user who visits the page is likely to trust any activity or content that appears on the page because the page itself is considered trustworthy.

Search Engine Manipulation

Another trick that criminals use to lure unwitting users to sites loaded with vulnerability exploits involves "gaming" search engine algorithms so that malicious pages appear high on the list of results that search engines return for common words and phrases. This technique, which is sometimes called *link farming*, involves creating a large number of Web sites that include popular keywords in the text and then creating links from each site to most or all of the others. Search engines generally assign a high score or rank to "popular" sites, as determined by the number of inbound links each site receives from others, and display popular sites higher in the list of search results than less popular sites. By creating networks of sites that all link to each other, these criminals attempt to fool the search engines into giving them prominent placement in results. This trick often surfaces around major gift-giving days so that users shopping for gifts online will be directed to malicious sites instead of to legitimate online stores. Search engine operators change their scoring algorithms regularly to combat this technique, with criminals altering their own tactics in response to accommodate the newer algorithms. Commandeered computers in botnets are typically used to host the network of malicious Web sites.

Users can better protect themselves, after using the search engine to locate prospective sites, by choosing sites with names they recognize. Sponsored sites (sites that pay for advertisements that appear above or alongside the main list of search results) also tend to be safe, as criminals are very unlikely to pay to advertise malicious pages. Of course, using an effective anti-malware product also offers a considerable level of protection.

Networking Tricks

Bot-herders and other computer criminals frequently exploit the Domain Name System (DNS) and Internet Protocol (IP) addresses to cover their tracks and to make it harder to find them and shut their operations down. DNS makes the Internet as we know it possible by associating domain names (like *www.example.com*) with the numeric IP addresses (like 172.27.199.4) that computers use to connect to each other and exchange traffic. Every registered domain on the Internet has at least one authoritative name server that can be queried to determine the domain's IP address. This all happens behind the scenes whenever you visit a Web page, send an e-mail message, or otherwise establish a connection to a computer over the Internet. When domain operators need to change the IP address assigned to the domain, they update a database entry (called an *A record*) on the domain's authoritative name server(s), and future queries for the domain will be answered with the new IP address.

Criminals use a technique called *fast flux* to serve malicious or illegal content, like phishing pages or malware packages, in a way that disguises the server's location and resists efforts to shut down the distribution network. Fast flux involves continually updating the A record for a DNS name, like *www.malware-site.example*, pointing it to several different IP addresses in rapid succession. Each of these IP addresses belongs to a computer in the botnet, all of which are configured to host the desired content. Because the bot-herder has so many computers to work with, this method makes it possible to continue serving malware or other malicious content even if a particular host becomes unreachable. A related technique, called *double flux*, adds an extra layer of indirection, making it harder for investigators to trace the source of an infection.

The Threat Ecosystem in Action

Here is an example to help examine how a typical botnet might be created and put to use. (It is important to note that this is just one example of how things might happen. Techniques discussed are not assumed to be the most common, and any resemblance to real people, places, or events is purely coincidental.)

The story begins with one or more prospective bot-herders—let's assume a single male individual, for now—somewhere in the world. He doesn't have to be able to write malware himself or even to know a great deal about computers. All he needs is money and the URL for one of the malware black market sites discussed earlier. At this site, the prospective bot-herder has access to a variety of tools and resources he can use to create, maintain, and profit from a botnet.

The prospective bot-herder is after two important things—botnet software and a means to distribute it to victims. To do this, the prospective bot-herder buys a package that consists of a malware distribution server and a Web page loaded with exploits, which is designed to be hosted in a hidden iFrame to infect unwitting visitors to a Web site. (See "E-Mail Threats," beginning on page 58, for more information about iFrame vulnerabilities and exploits.) These exploits install a downloader on the victim's computer, which contacts the distribution server and downloads additional packages that then install the botnet software and other tools. Some criminals lure victims to infected Web pages using techniques like blog-comment spam promising free sexually explicit material, pirated MP3 files, or other enticing content. Our subject doesn't want to go to all that trouble, so he also buys a compromised user name and password for a moderately popular blog that averages several hundred unique visitors a day, according to the seller.

Some criminals lure victims to infected Web pages using techniques like blog-comment spam promising free sexually explicit material, pirated MP3 files, or other enticing content.

The bot-herder creates a malware server, loads the iFrame exploit onto the compromised blog, and waits. Most people who visit the blog are running the latest security updates and are not vulnerable to the exploit, and many of the remaining visitors are running antivirus software that detects the infection attempt and protects them from it, but there are enough unprotected visitors that the bot-herder soon has a botnet with several dozen nodes around the world.

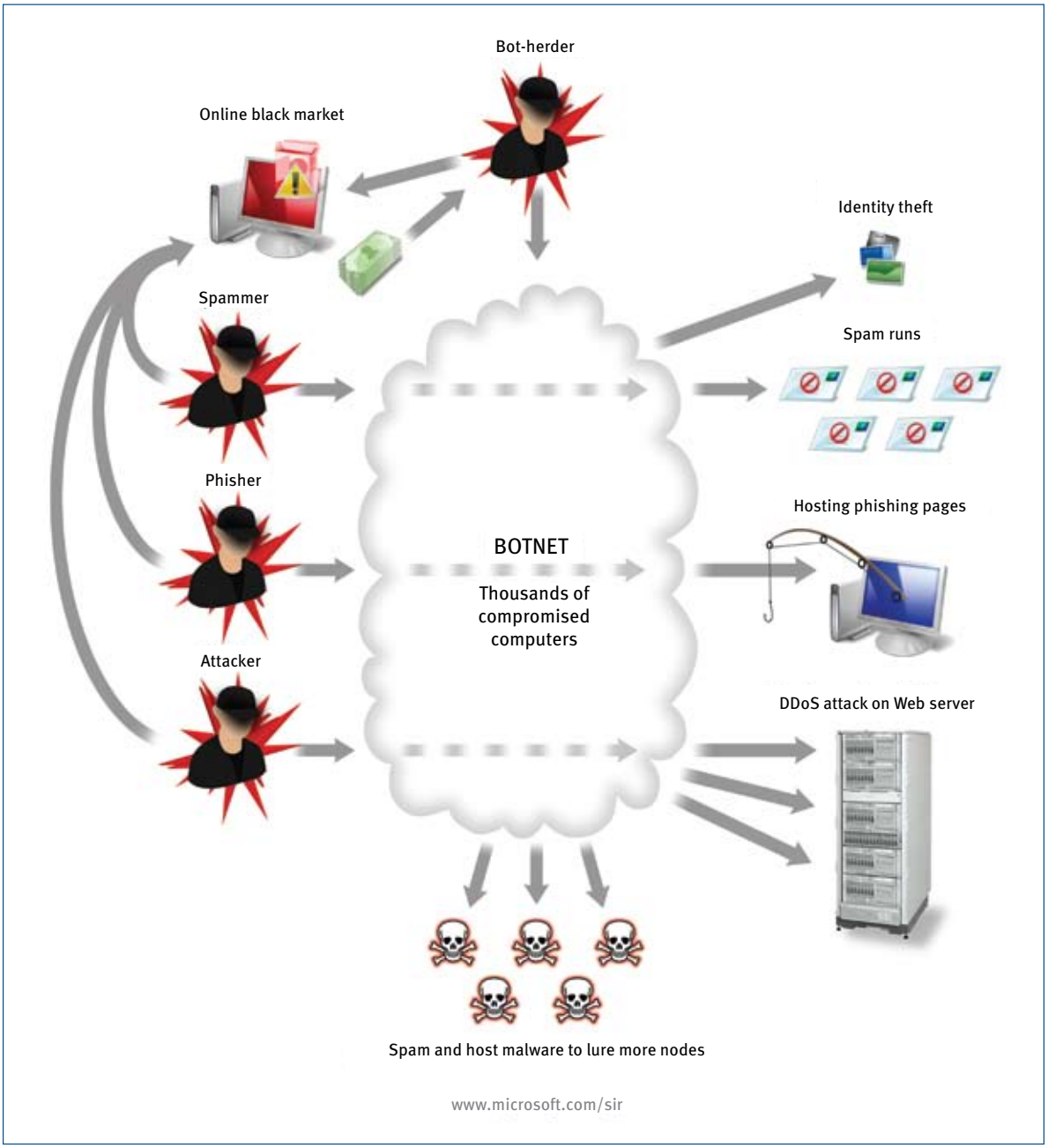
That's a start, but the botnet is not yet nearly large enough to accomplish the bot-herder's goal of making money. The rates bot-herders can charge to rent out access to a botnet are actually quite low, at least for renters in wealthy, developed nations. Adam Sweaney, a U.S.-based bot-herder who pled guilty in September 2007 in U.S. District Court to a one-count felony violation for conspiracy fraud and related activity in connection with computers, was caught after he offered an undercover federal investigator access to more than 6,000 compromised computers for just U.S.$200 per week. For our hypothetical subject to even recoup his initial investment, therefore, he needs to add a lot more nodes to his botnet.

FIGURE 2. Example of how a typical botnet is created

Now that the botnet is up and running, it can be used to add additional nodes directly to itself. The bot-herder designates a handful of nodes as malware servers, using the fast-flux technique to disguise their source and to provide protection in case one or more of them are discovered and shut down. He sets the other nodes to work sending spam with links to exploit-laden pages on the malware servers, using various forms of social engineering to lure recipients to click the link in the message. He also bargains for more compromised credentials so he can add the iFrame exploit to more Web servers. Over time, the botnet gradually grows to encompass a few thousand nodes.

Now the bot-herder is ready to start making money. He begins to advertise the services of his botnet on many of the same malware marketplace forums he used to get his botnet started, offering a menu of services with prices varying by the number of nodes to be rented and the length of time they are to be used. He sets his price according to what he thinks the market will bear, based on the prices charged by others selling similar services. Because he's a new seller with no established reputation, he offers potential buyers a free trial in the form of access to the botnet for a very short time, typically less than an hour. As with many mainstream businesses, a few successful transactions give him a good reputation in the community, which in turn will lead more buyers to his virtual door.

FIGURE 3. Example of a typical botnet in action



The bot-herder now has a regular customer base and mechanisms in place to expand the botnet. Even as he is keeping the botnet going, though, he is trapped in a continuing battle to stay one step ahead of antivirus software and the law enforcement agencies that are trying to put him in jail.

The problem is worldwide. Law enforcement agencies around the world cooperate both with each other and with the software industry to fight it, and they have achieved some positive results. But still, these arrests and captures are few and far between, and we all have to do our best to protect ourselves. Awareness and education are a necessity in that effort.

This is far from a complete picture of the threat ecosystem, obviously, and given the pace of the current arms race, the landscape will undoubtedly look very different in a year or two. The *Security Intelligence Report* is dedicated to helping readers stay on top of these changes with statistics and analyses of trends. Nonetheless, it's important to remember that computer security is about more than just figures and trends—it's about people, too. Understanding the individuals and motivations behind computer crime is the key to fighting it, not only for law enforcement but also for all of the so-called "white hats" who work to protect people, systems, and information from computer-based threats.

Vulnerability Trends

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

This section of the *Security Intelligence Report* analyzes new vulnerabilities that were disclosed during the first half of 2008. It compares trending information for vulnerabilities starting in 2003, with a particular focus on trends that may be emerging over the past few half-year periods.

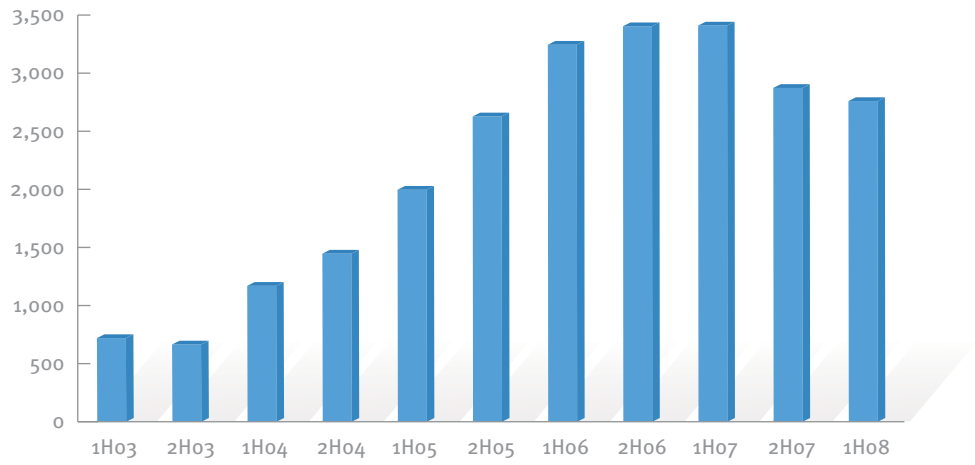
Note that, in this report, the term *disclosure* is used to mean broad and public disclosure and not any sort of private disclosure or disclosure to a limited number of people. This section discusses software vulnerability disclosures for the software industry as a whole, but will examine Microsoft-specific disclosures as well.

Industry Vulnerability Disclosures

In the first half of 2008 (1H08),[3] reported vulnerabilities continued the decline observed in 2H07, but to a much smaller degree, down only 4 percent from the previous half-year period. This represents a 19 percent decrease from the same period the previous year. Disclosures in 2H08 would have to increase by more than 28 percent—a rate of increase not seen since 2005—to achieve a yearly disclosure total for 2008 higher than that of 2007.

Figure 4 illustrates the number of vulnerability disclosures across the software industry for each half-year period since 1H03.

FIGURE 4. Industry-wide vulnerability disclosures by half-year, 1H03–1H08



[3] The nomenclature used throughout the report to refer to different reporting periods is nHyy, where nH 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), while 2H07 represents the period covering the second half of 2007 (July 1 through December 31).

While a 19 percent general decrease in disclosures from a year ago is generally considered good news, it can't really be considered "good" for the industry when more than 15 new software vulnerabilities, on average, continue to be disclosed each day. At these levels, the need for software risk management programs continues to be high.

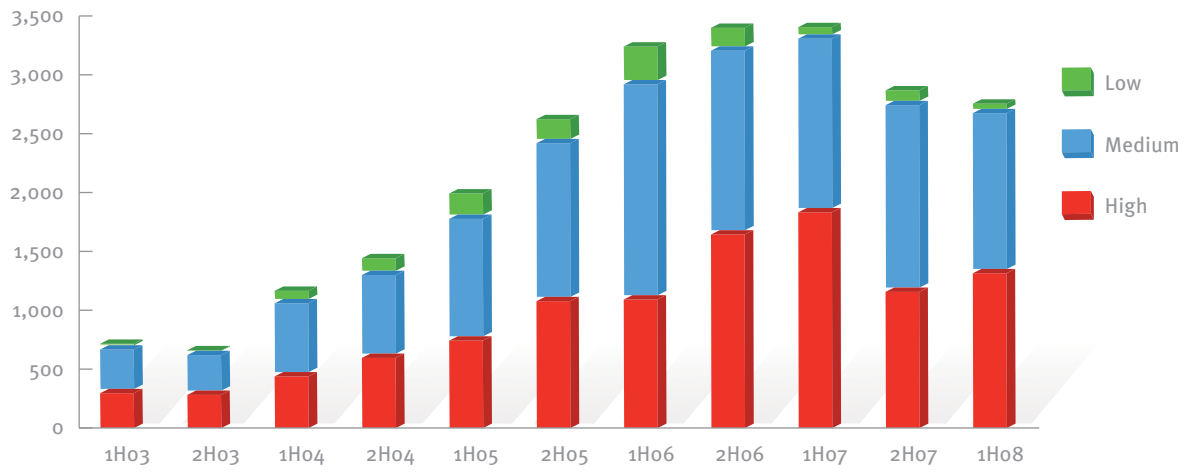
Industry Vulnerability Severity

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.

In the previous volume of the *Security Intelligence Report* (SIR v4), we analyzed severity using both version 1 and version 2 of the Common Vulnerability Scoring System (CVSS)[4] to transition from older reports that had used only CVSSv1 for analysis. CVSSv2 has now been in use for more than a year and has largely been validated as a general improvement for severity ratings, so this report exclusively uses the CVSSv2 severity rating that is scored by the National Institute of Standards (NIST) and documented in the National Vulnerability Database (NVD) at http://nvd.nist.gov.

Examining the chart in Figure 5, we see that the trend for High severity vulnerability does not follow the same pattern as the overall total and actually increases relative to 2H07 by 13 percent.

FIGURE 5. Industry-wide vulnerability disclosures by severity, 1H03–1H08



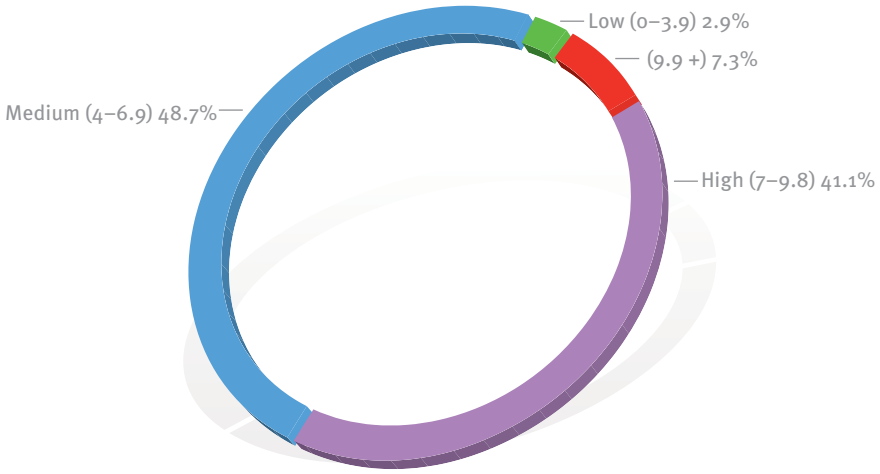
[4] CVSS is an industry standard for assessing the severity of software vulnerabilities. See http://www.first.org/cvss/ for more documentation and details.

Focusing on mitigating the most severe vulnerabilities first is a security best practice. While CVSS, via the NVD, provides a base score across the set of industry vulnerabilities, security professionals should look first to their software vendors for further security information, as 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 industry shift to CVSSv2 has significantly changed the severity mix of vulnerabilities. In the past, administrators could prioritize the vulnerabilities rated High severity, which accounted for less than 15 percent of all vulnerabilities. Now, it is more important to look 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.

Along these lines, the chart in Figure 6 illustrates the severity breakdown for 1H08. 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 7 percent of all vulnerabilities disclosed.

FIGURE 6. Industry-wide vulnerability disclosures by severity, 1H08

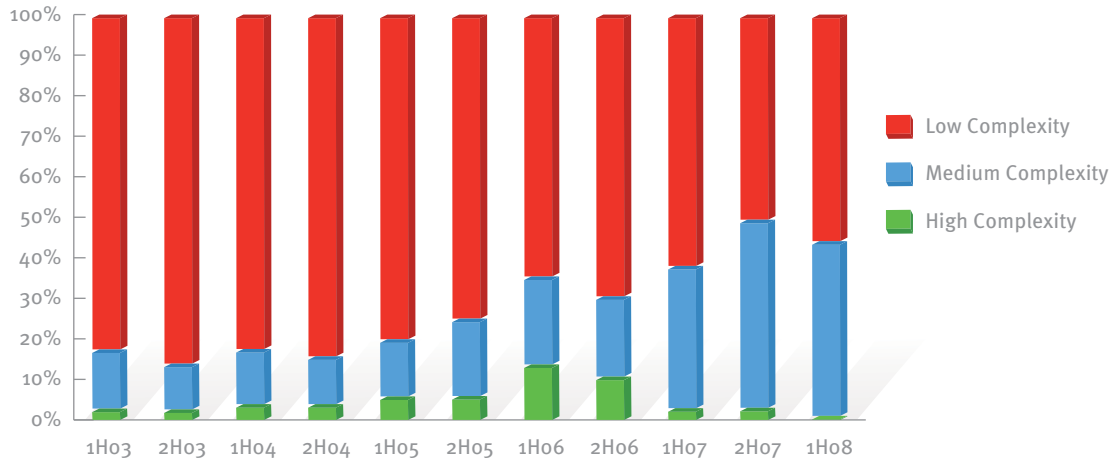


Industry Vulnerability Complexity

CVSSv1 used a simple binary classification of exploit complexity that rated all exploits as either Low complexity or High complexity. CVSSv2 uses three complexity designations: Low, Medium, and High. See Figure 73 in *Supporting Data and Details*, on page 124, for the definitions of these complexity designations.

Figure 7 shows the vulnerability disclosure complexities for each half-year period since 1H03. The percentage of exploits requiring a High degree of complexity has decreased in 1H08, continuing a trend that has been evident for the last several periods, while the percentage of exploits requiring a Low degree of complexity has increased slightly, reversing the recent trend. This is a bad combination because it means that exploits disclosed in 1H08 have been easier to implement on balance than in previous periods.

FIGURE 7. Industry-wide vulnerability disclosures by access complexity, 1H03–1H08



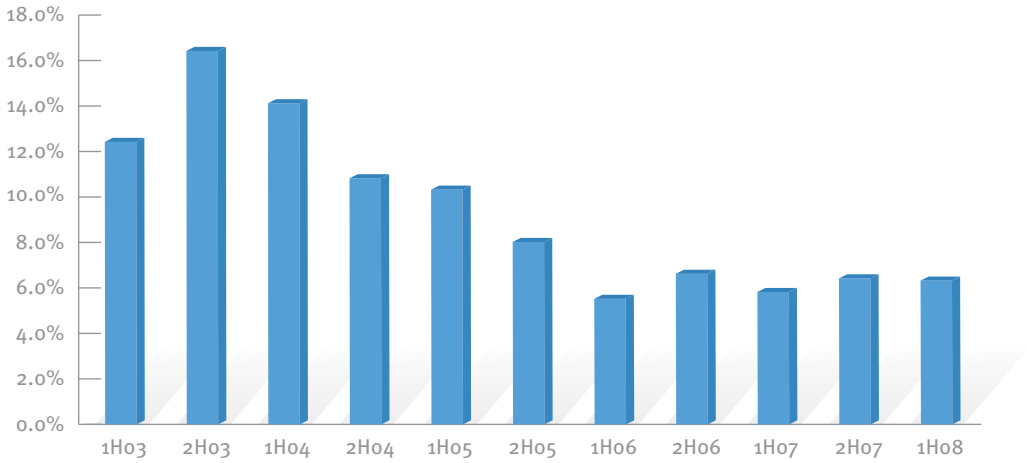
Operating System vs. Non-Operating System Disclosures

Comparing operating system (OS) vulnerabilities to non-OS 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 Security Response Center (MSRC) 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 OS 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, the Mozilla Firefox browser, and others.

Figure 8 shows OS vulnerabilities as a percentage of all disclosed vulnerabilities since 1H03, as determined by this simple model.

FIGURE 8. Operating system vulnerabilities as a percentage of all disclosures, 1H03–1H08



As this chart shows, the percentage of vulnerabilities affecting core OS components has decreased significantly over the past five years and appears to have recently stabilized between 6 and 8 percent.

Microsoft Vulnerability Disclosures

Figure 9 charts vulnerability disclosures for Microsoft products since 1H03. In general, trends for Microsoft vulnerability disclosures have mirrored those for the industry as a whole, though on a much smaller scale.

FIGURE 9. Vulnerability disclosures for Microsoft products, 1H03–1H08

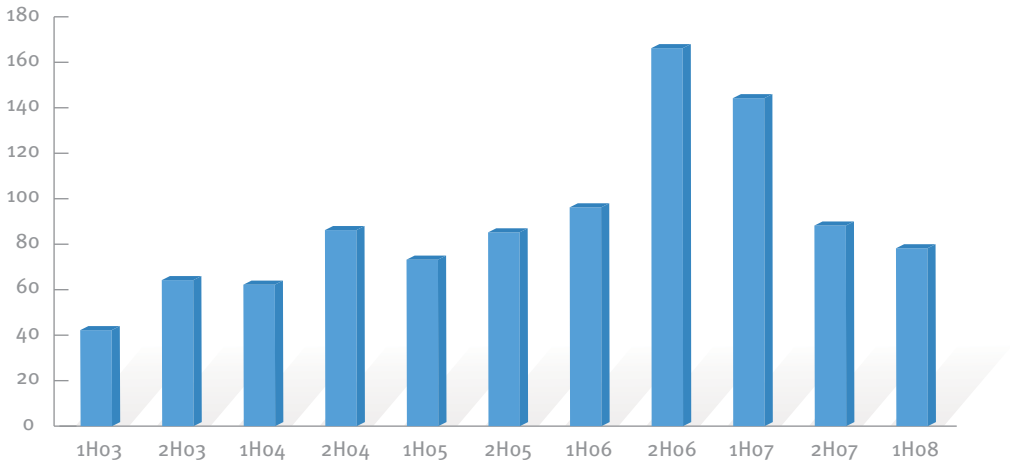
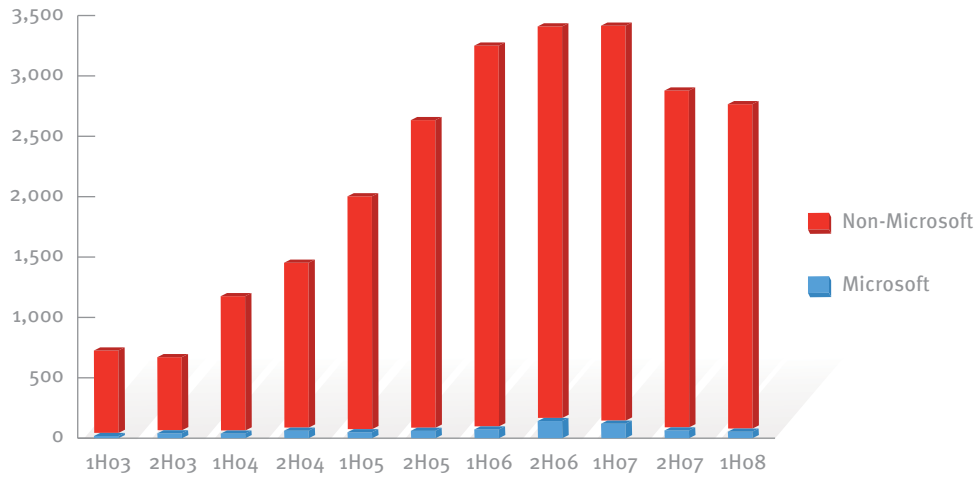


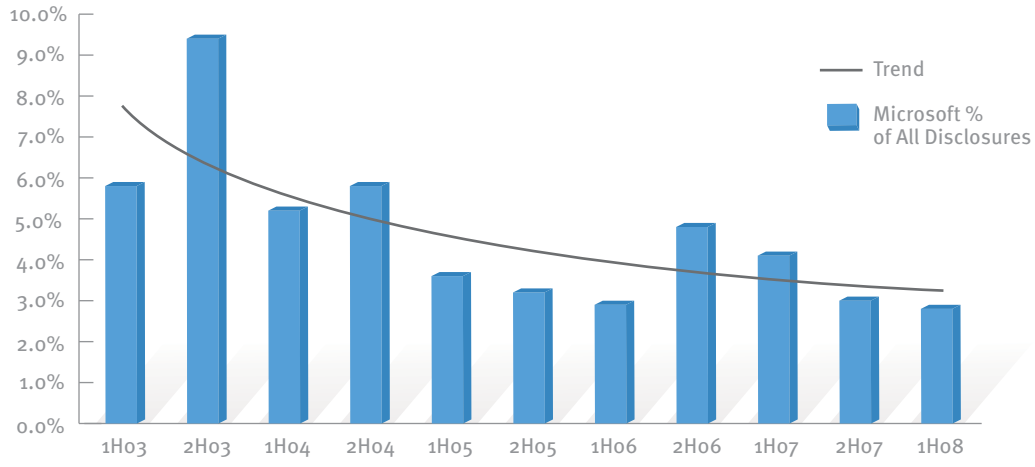
Figure 10 provides some perspective for these figures by illustrating the relative share of vulnerability disclosures for Microsoft and non-Microsoft software over the same period, showing that Microsoft vulnerabilities account for a relatively small percentage of the overall total.

FIGURE 10. Vulnerability disclosures for Microsoft and non-Microsoft products, 1H03–1H08



The size and scale of Figure 10 make it difficult to identify any trends in Microsoft vulnerability disclosures, so Figure 11 shows Microsoft disclosures as a percentage of total disclosures over the same period. As this figure shows, the share of vulnerability disclosures attributed to Microsoft software has shown a positive downward trend since 1H03.

FIGURE 11. Microsoft vulnerability disclosures as a percentage of all industry disclosures, 1H03–1H08



Vulnerability Trends Summary and Conclusion

The total number of unique vulnerability disclosures across the industry again decreased in the first half of 2008, down 4 percent from the second half of 2007 and down 19 percent from the period a year ago.

In contrast to the decrease in total disclosures, vulnerabilities rated as High severity increased 13 percent with respect to the second half of 2007, with roughly 48 percent of all vulnerabilities receiving a rating of High severity, though this still represents a 28 percent decline from 1H07. Compounding the seriousness of the High severity vulnerabilities, the percentage that is easiest to exploit increased as well, with more than half requiring a Low complexity exploit.

On a more positive note for Microsoft customers, Microsoft vulnerability disclosures in 1H08 continue a multi-period downward trend, both in terms of disclosures and relative to the total industry disclosures, providing some broad indication that the Microsoft Security Development Lifecycle (SDL) efforts across all of the product groups may be producing positive results.

Strategy, Mitigations, and Countermeasures

- Both security vendors and IT professionals should adjust their risk management processes appropriately to ensure that operating systems and applications are protected.
  - A Security Risk Management Guide for IT professionals is available at this URL: http://www.microsoft.com/technet/security/guidance/complianceandpolicies/secrisk/default.mspx.
- Microsoft offers free prescriptive guides created by the Solution Accelerators - Security and Compliance team for IT professionals, in addition to security guidance organized by topic, product, and technology: 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, as it provides access to various security-related resources.
- 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: http://www.microsoft.com/technet/security/secnews/default.mspx.

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. The section "The Threat Ecosystem" described how malware distributors 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 installation"). The vulnerabilities targeted by these exploits are typically found 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 "kill bits" that prevent certain vulnerable add-ons from running in Internet Explorer®.)

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 poor-performing exploits and replacing them with new ones. The most highly prized 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 of the time and effort it takes to update vulnerable systems around the world. Even today, exploits for vulnerabilities updated 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.

The Exploit Landscape in 1H08

The previous two volumes of the *Security Intelligence Report* analyzed exploits for software vulnerabilities resolved in security updates for certain Microsoft products. In 1H08, this analysis showed that roughly 32.5 percent (25 out of 77) of all vulnerabilities resolved in security updates had publicly available exploit code, similar to the results found in previous periods. Microsoft Windows 2000® and Windows Server® 2003 were the two operating systems with the largest numbers of publicly released exploits.

The 1H08 analysis uses the same methodology to create the dataset for publicly released exploits; in addition, Microsoft extended the software vulnerability exploit review to examine which exploits could be verified as reliable and which could not. Overall, 10.4 percent (8 of 77) of the vulnerabilities had reliable publicly available exploit code. An additional 22 percent of the vulnerabilities with unverified exploits have the potential to become reliable exploits.

In total, Microsoft released 36 security bulletins addressing 58 vulnerabilities from January through June 2008. Microsoft's vulnerability analysis determined that the total number of vulnerabilities in 1H08 was down 33.6 percent from 2H07 (77 vulnerabilities in 1H08, compared to 116 in 2H07), and the publicly available exploit code decreased 47.9 percent (25 in 1H08, compared to 48 in 2H07). There was a corresponding decrease in the ratio of publicly available exploits to the number of vulnerabilities, from 44.8 percent in 2H07 to 32.5 percent in 1H08.

As a result of these insights, along with customer requests for additional information to further evaluate risk, Microsoft is offering details about the likelihood that functioning exploit code will be released after a Microsoft security update is released. This "Exploitability Index," which appears in the monthly security bulletin summary starting in October 2008, is designed to help identify the roughly 30 percent of vulnerabilities resolved by Microsoft monthly security updates that are likely to have functioning exploit code published. Microsoft expects this guidance to help customers better prioritize their deployment of Microsoft security updates.

For full details of this analysis, see "Exploit Data" in *Supporting Data and Details*, on page 125.

Top Browser-Based Exploits

To assess the relative prevalence of browser-based exploits in 1H08, 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.[5] It also includes data from third-party browsers 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.[6] Exploits affecting third-party software are labeled with the Common Vulnerabilities and Exposures (CVE) list identifier pertaining to the vulnerability, if applicable.[7]

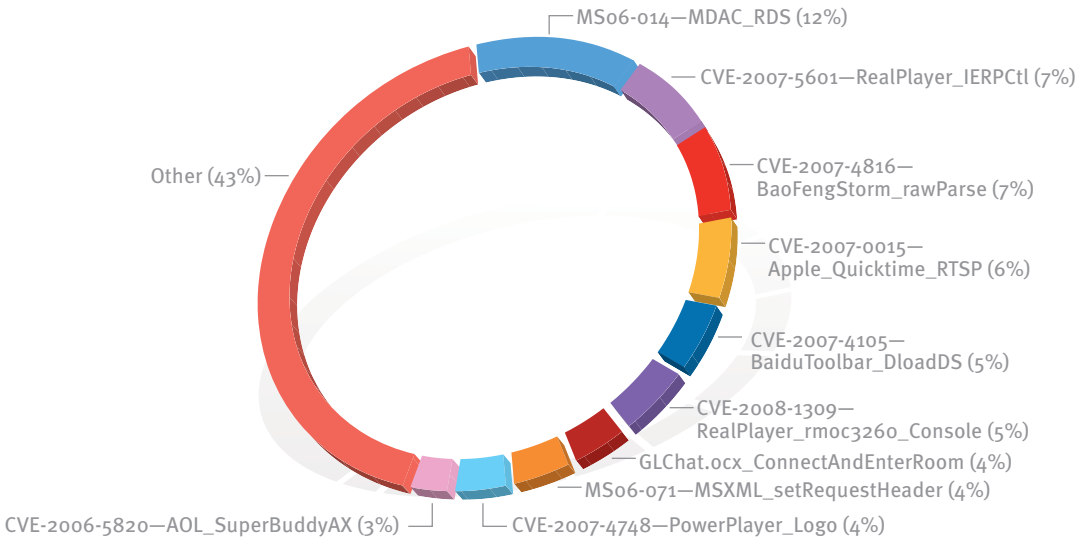
Figure 12 shows the browser-based exploits encountered by users in 1H08, ordered by frequency. For example, MS06-014 represented 12.1 percent of all exploit encounters. The next most encountered exploit was for CVE-2007-5601, a vulnerability in RealPlayer software.

[5] Includes Windows XP with no Service Pack (SP), SP1, SP2, SP3, and Windows Vista release RTM and SP1.

[6] See http://www.microsoft.com/technet/security/Current.aspx to search and read Microsoft security bulletins.

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

FIGURE 12. Browser-based exploits, by percentage, encountered in 1H08

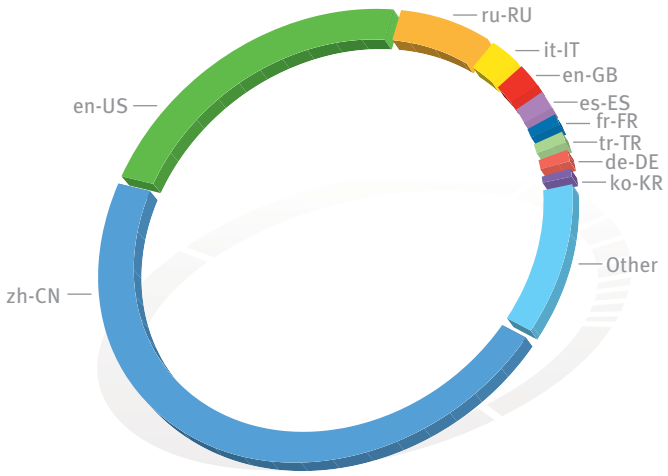


Browser-Based Exploits by System Locale

Malware distributors target different parts of the world unequally. "The Threat Ecosystem" described how malicious people lure victims to exploit pages through a variety of methods, like sending spam or hijacking legitimate Web sites. By nature, these lures tend to target specific segments of the global population. A spam message written in English, for example, is more likely to be effective with potential victims who speak English 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 13 (on the next page) shows the browser-based exploits encountered by users in 1H08, ordered by the system locale of the victim. The most common locale for victims was zh-CN (Chinese), accounting for 47 percent of all incidents, followed by en-US (U.S. English) with 23 percent of incidents.

FIGURE 13. Browser-based exploits, by system locale of victim, encountered in 1H08



de-DE: German language, Germany
en-GB: English language, United Kingdom
en-US: English language, United States
es-ES: Spanish language, Spain
fr-FR: French language, France
it-IT: Italian language, Italy
ko-KR: Korean language, Korea
ru-RU: Russian language, Russia
tr-TR: Turkish language, Turkey
zh-CN: Chinese language, China

Browser-Based Exploits by Operating System and Software Vendor

Every exploit can be traced to a vulnerability in a specific piece of software. Comparing first-party exploits (those that target vulnerabilities in 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 14 and Figure 15 show the relative percentages of exploits in Microsoft and third-party software in 1H08 sampled for Windows XP and Windows Vista, respectively. In Windows XP, Microsoft vulnerabilities account for 42 percent of the total. In Windows Vista, the proportion of Microsoft vulnerabilities is much smaller, accounting for just 6 percent of the total.

FIGURE 14. Browser-based exploits targeting Microsoft and third-party software on computers running Windows XP, 1H08

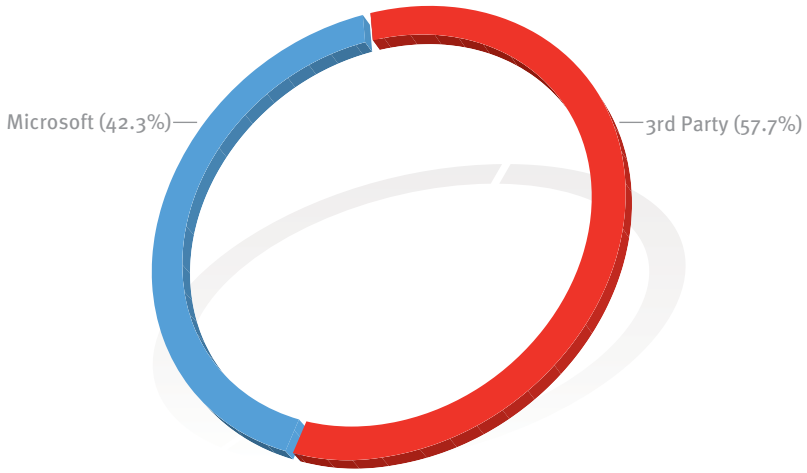


FIGURE 15. Browser-based exploits targeting Microsoft and third-party software on computers running Windows Vista, 1H08

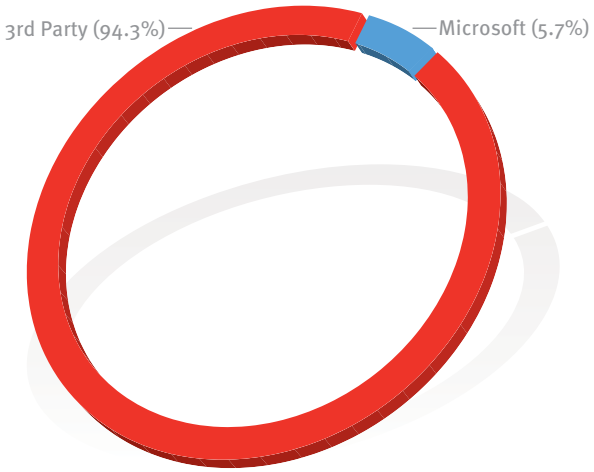


Figure 16 and Figure 17 show the 10 vulnerabilities exploited most often in Windows XP and Windows Vista in 1H08, respectively. In Windows XP, Microsoft software accounts for 5 of the top 10 vulnerabilities, compared to none in Windows Vista. Three vulnerabilities are common to both versions, all in third-party software: CVE-2007-0015, affecting the Apple QuickTime add-on, and CVE-2008-1309 and CVE-2007-5601, affecting the RealPlayer add-on.

The vulnerability exploited most often in Windows XP was MS06-014 (CVE-2006-0003), a vulnerability affecting the Microsoft Data Access Components (MDAC) function that was disclosed and fixed in 2006. In Windows Vista, two of the most commonly exploited vulnerabilities affect ActiveX controls commonly installed in China, consistent with the data presented in Figure 13.

For a closer look at these statistics, see Figure 78 and Figure 79 in *Supporting Data and Details*, on page 132.

FIGURE 16. The 10 browser-based vulnerabilities exploited most often on computers running Windows XP, 1H08

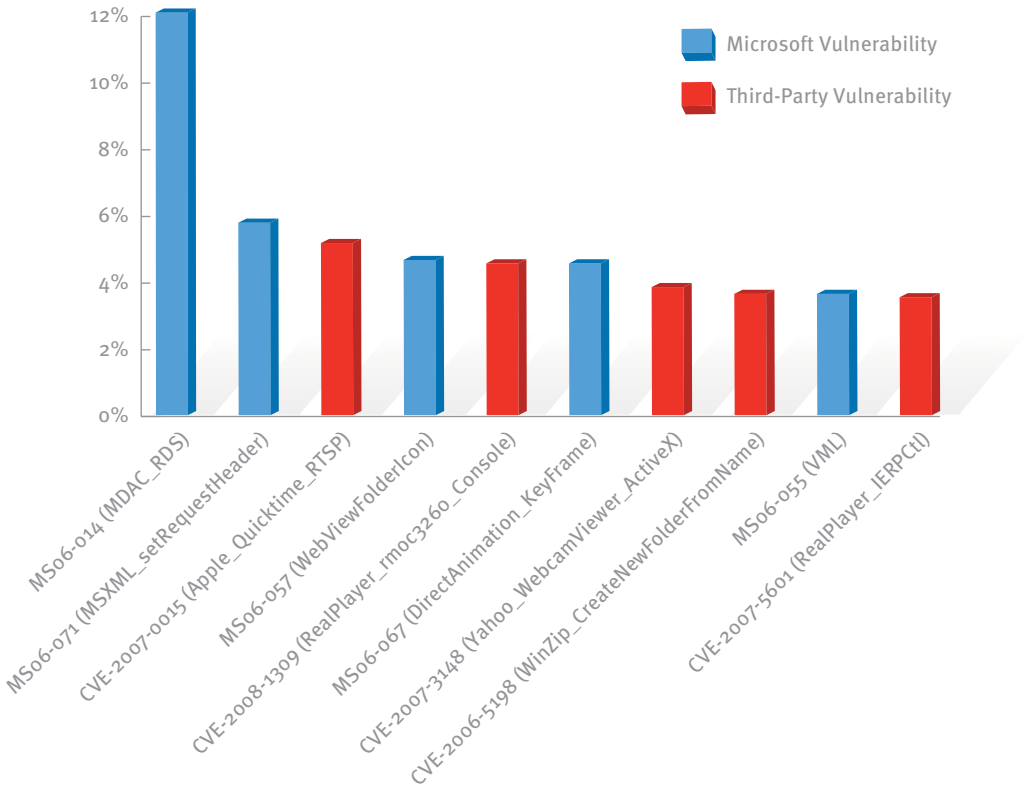
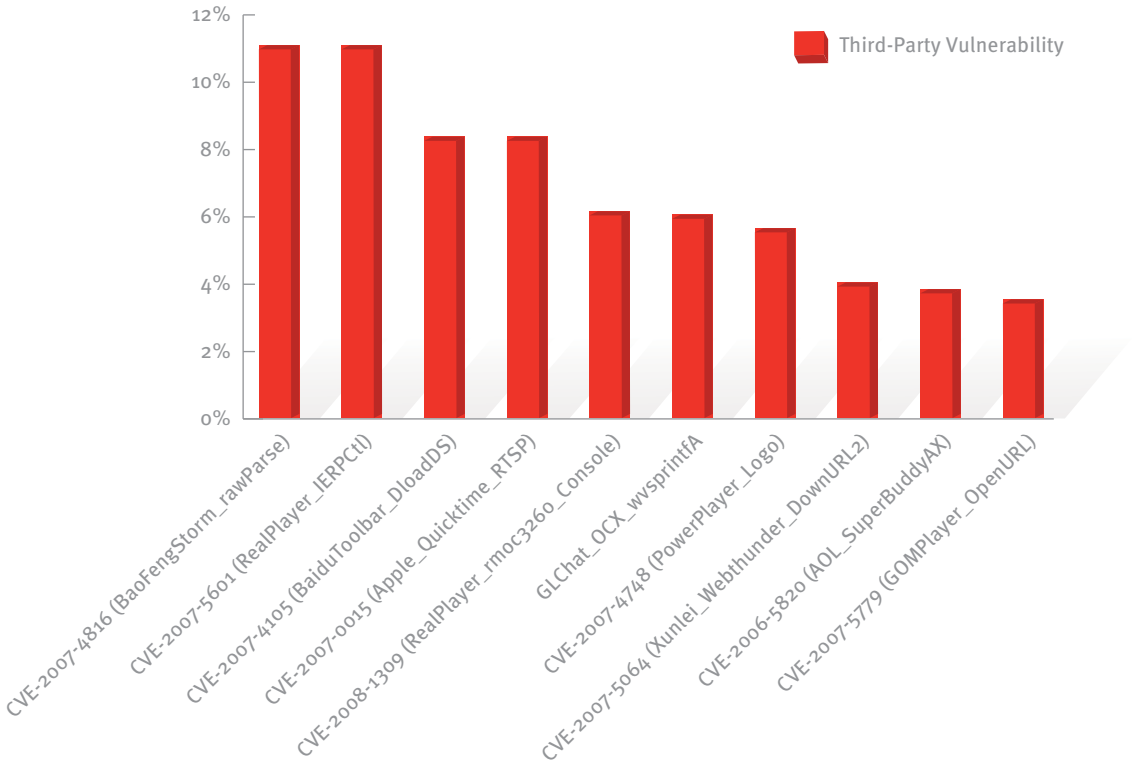


FIGURE 17. The 10 browser-based vulnerabilities exploited most often on computers running Windows Vista, 1H08



At least part of the improvement in the security of Windows Vista over Windows XP can be attributed to the implementation of the Security Development Lifecycle (SDL).[8] A Microsoft-wide initiative and a mandatory policy since 2004, the SDL has played a critical role in embedding security and privacy in Microsoft software and culture. Combining a holistic and practical approach, the SDL introduces security and privacy early and throughout the development process. It has led Microsoft to measurable and widely recognized security improvements in flagship products, such as Windows Vista, Internet Explorer, and SQL Server®. With cyber attacks moving to the application layer, Microsoft is committed to supporting a more secure and trustworthy computing ecosystem by making SDL process guidance, tools, and training available for every developer.

Strategy, Mitigations, and Countermeasures

Steps users can take to avoid being victimized by exploits while browsing include:

- 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.

[8] For more information, see http://www.microsoft.com/SDL.

- Uninstall software you don't actively use. Malicious code can exploit vulnerabilities in software whether you use it or not.[9]
- Use antivirus software 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.
- To avoid attacks that rely on administrative user rights, enable User Account Control in Windows Vista, or log on with a user account that does not have administrative user rights.
- Read e-mail messages in plain text format to help protect you from the HTML e-mail attack vector.

[9] For example, see http://msdn.microsoft.com/en-us/library/bb688194.aspx to manage ActiveX controls.

A Focus on Mitigating Exploit Code

Microsoft partners with many other parties when investigating potential vulnerabilities in Microsoft software. Microsoft looks to mitigate exploitation of vulnerabilities through the collaborative strength of the industry, partners, public organizations, customers, and security researchers. Along the way, Microsoft supports and encourages reasonable or responsible disclosure of vulnerabilities. *Responsible disclosure* means disclosing vulnerabilities privately to an affected vendor so it can develop a comprehensive security update to address the vulnerability before the vulnerability details are public. Ideally, with responsible disclosure, the release of the security update coincides with vulnerability information becoming publicly available. This serves everyone's best interests and ensures that users are not exposed to malicious exploitation while security updates are being developed.

When a security researcher is acknowledged in one of Microsoft's monthly security bulletins, it means that the vulnerability was reported to the Microsoft Security Response Center (MSRC) privately and that the individual security researcher or organization worked with us to help us understand the vulnerability, the extent of the risk to the products and platforms, and possible mitigations. During the technical investigation and development of the update, the vulnerability reporter is continually apprised and updated about the availability of the impending update. In the end, this helps to minimize the threat and impact to customers everywhere by helping to ensure that Microsoft can fix the problem before potential attackers are aware of the vulnerability or are able to leverage the vulnerability for malicious use.

Security researchers that report vulnerabilities to Microsoft live and work all over the world. Consequently, security-related conferences and events are held all over the world. The MSRC sponsors and attends many of these conferences and events. Engaging in the security community by supporting worldwide events helps Microsoft learn about the new areas of focus and industry trends within the security community, tools and techniques, and related cultural and philosophical elements that affect the security landscape. The conferences are a platform for technical information exchange, for new research and relationships to be developed, and for greater understanding of regional trends and research. Attending these events ultimately helps the MSRC provide timely and accurate information that helps better protect customers. Figure 18 and Figure 19 (on the next two pages) illustrate how the MSRC engages the security community by co-sponsoring or attending security conferences worldwide.

While there are many more security conferences held around the world, and as much as Microsoft would like to have a presence at every security conference, the MSRC participates only in those security conferences whereby there is a strict adherence to responsible disclosure.

FIGURE 18. Worldwide conferences co-sponsored and attended by the MSRC, 2H07-2H08

Conference	Start Date	Location
AusCERT	18-May-08	Gold Coast, Australia
Black Hat Europe	25-Mar-08	Amsterdam, Netherlands
Black Hat Federal	18-Feb-08	Washington D.C., United States
Black Hat Japan	23-Oct-07	Tokyo, Japan
Black Hat Vegas	28-Jul-07	Las Vegas, United States
BlueHat China	25-Oct-07	Beijing, China
BlueHat v6	27-Sep-08	Redmond, United States
BlueHat v7	1-May-08	Redmond, United States
CanSec West	26-Mar-08	Vancouver, Canada
CONfidence	16-May-08	Krakow, Poland
DeepSec	20-Nov-07	Vienna, Austria
Ekoparty	30-Nov-07	Buenos Aires, Argentina
EUSecWest	21-May-08	London, United Kingdom
H2HC	8-Nov-07	Sao Paulo, Brazil
HITB Dubai	14-Apr-08	Dubai, United Arab Emirates
HITB KL	3-Sep-07	Kuala Lumpar, Malaysia
Kiwicon	17-Nov-08	Wellington, New Zealand
LayerOne	17-May-08	Los Angeles, United States
PacSec	27-Nov-07	Tokyo, Japan
PakCon	26-Jul-08	Karachi, Pakistan
PH-Neutral 0x7d8	23-May-08	Berlin, Germany
POC	15-Nov-07	Seoul, Korea
SOURCEBoston	12-Mar-08	Cambridge, United States
SyScan Hong Kong	29-May-08	Hong Kong, Hong Kong SAR
SyScan Singapore	5-Jul-07	Singapore, Singapore
ToorCon	19-Oct-07	San Diego, United States
ToorCon	18-Apr-08	Seattle, United States
Troopers	23-Apr-08	Munich, Germany
VN Security	3-Aug-07	Ho Chi Minh City, Vietnam
Xcon	28-Aug-07	Beijing, China
ySтS	24-Oct-07	Sao Paulo, Brazil

FIGURE 19. Worldwide conferences attended by the MSRC and security engineering team, 2H07-2H08

Conference	Start Date	Location
Bellua	30-Oct-07	Jakarta, Indonesia
CCC Camp	8-Aug-07	Berlin, Germany
CCC	27-Dec-07	Berlin, Germany
Defcon	3-Aug-07	Las Vegas, United States
DIMVA	12-Jul-07	Lucerne, Switzerland
DIMVA	10-Jul-08	Paris, France
DSN - IEEE/IFIP International Con on Dependable Systems & Networks	24-Jun-08	Anchorage, United States
ECIW	2-Jul-07	Shrivenham, United Kingdom
ECIW European Con on Info Warfare & Security	30-Jun-08	University of Plymouth, United Kingdom
EICAR	3-May-08	Laval, France
FIRST Con	22-Jun-08	Vancouver, Canada
FIRST Technical Colloquium	25-Mar-08	Tokyo, Japan
FIRST Technical Colloquium	28-Jan-08	Prague, Czech Republic
FloCon	7-Jan-08	Savannah, United States
GFIRST	1-Jun-08	Orlando, United States
hack.lu	18-Oct-07	Luxembourg, Luxembourg
HackCon 3	6-Feb-08	Oslo, Norway
Hacker Space Fest	16-Jun-08	Vitry, France
ISOI Conference (GadiCon)	28-Feb-08	San Jose, United States
ISSA	2-Jul-08	Gauteng, South Africa
IT Underground	7-Nov-07	Warsaw, Poland
OWASP & WASC AppSec	12-Nov-07	San Jose, United States
RSA USA	7-Apr-08	San Francisco, United States
SANS Security West	9-May-08	San Diego, United States
ShmooCon	15-Feb-08	Washington D.C., United States
Security OPUS	1-Feb-08	San Francisco, United States
ShakaCon	10-Jun-08	Honolulu, United States
Softforum	14-Apr-08	Seoul, Korea
Systemics, Cybernetics and Informatics: WMSCI 2008	29-Jun-08	Orlando, United States
T2	11-Oct-07	Kalastajatorppa, Finland
The Last HOPE	18-Jul-08	New York City, United States
UnCon	10-Nov-07	London, United Kingdom
USENIX	6-Aug-07	Boston, United States

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 details of breach incidents from around the world that took place in 2H07 and 1H08, 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 Data Loss Database. The groups are shown in Figure 20.

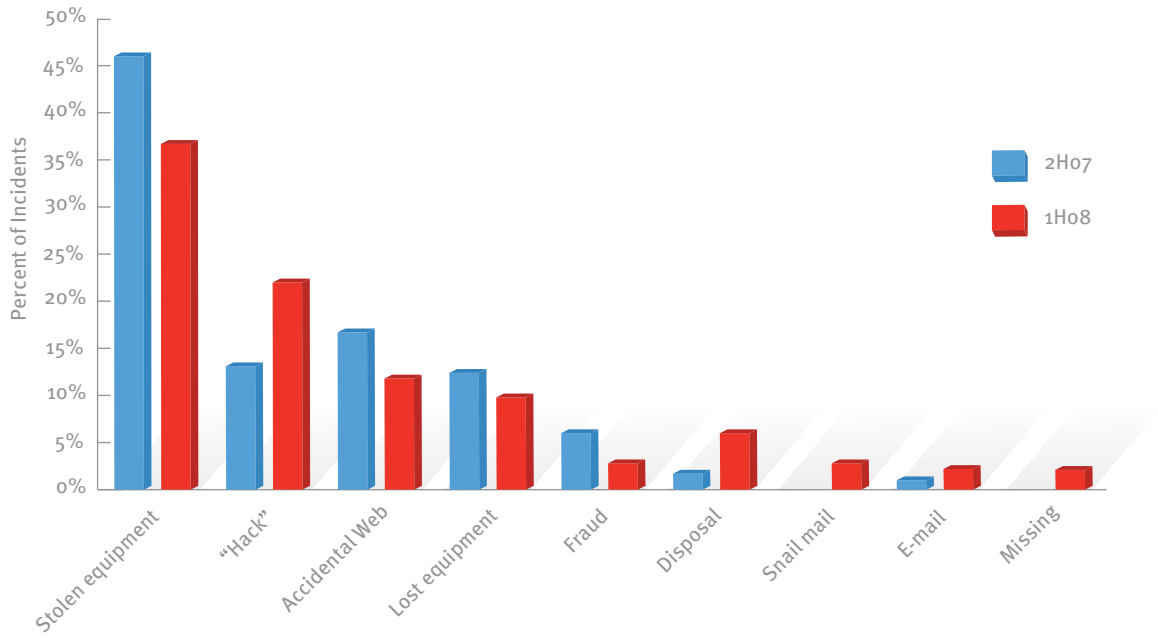
FIGURE 20. Security breach incident categories used in this section

Our Label	Definition	Maps to Attrition.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
Accidental Web	Accidental exposure on a Web site, available to the public with a Web browser	Web
Lost equipment	Reported as lost computers, disks, tapes, or documents	Starts with "lost"
Disposal	Improper disposal of any sort	Starts with "disposal"
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
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 21 illustrates the overall distribution of incidents by type for 2H07 and 1H08.

FIGURE 21. Security breach incidents by type, expressed as percentages of the total, 2H07 and 1H08



Many of the trends observed and analyzed for the previous volume of this report, covering the second half of 2007, remain in evidence for the first half of 2008:

- 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 three-quarters 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 nearly twice as many incidents as intrusion, possibly because equipment theft is easily detected. 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.
- 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.
- Information about the portion of hacking incidents that involved Microsoft products is not easy to obtain from the data provided. The original data is widely variable, and it is difficult to analyze for useful information that could help software developers improve their engineering processes. More complete data could help provide substantial insights into security problems.

Malware, which was cited in the previous volume of this report as being responsible for a small percentage of incidents in previous periods, was not blamed for any incidents reported in 2H07 or 1H08.

Study of breach data provides a unique way to look at issues experienced in the real world and could be an aid to organizations seeking to develop and improve effective information security policies. Unfortunately, the usefulness of the data is limited by a lack of uniform reporting standards and requirements, which leads to variations and omissions in the details reported. It may be worth investigating why the data is so sparse and looking for ways to improve it.

It should be noted that in many cases these security breaches result in the exposure of confidential data, either organizational or personal. The impact of these privacy exposures from a political, business, and personal perspective continues to increase, and these events are extensively covered in the press. Focusing on privacy-loss prevention is increasingly becoming a key activity for IT professionals and management.

Malware and Potentially Unwanted Software Trends

The total amount of malware removed from computers around the world by Microsoft security products in 1H08 was substantially higher than in 2H07, continuing a trend that has been evident for the last several years. See Figure 86 in *Supporting Data and Details*, on page 140, for some of the figures behind this detected increase.

This increase can be attributed to a number of factors:

- The ability of the tools themselves to detect malware continues to improve as researchers analyze samples and refine their detection algorithms.
- Several prevalent malware families were added to the MSRT in 1H08, causing them to be detected for the first time on many previously unprotected computers.
- More computers worldwide are running Windows Vista, which includes Windows Defender (available as a separate download for earlier versions of Windows) and allows the user to download the monthly Microsoft Windows Malicious Software Removal Tool (MSRT) by default.
- Increased usage of Microsoft security products, like Windows Live™ OneCare™ and Microsoft Forefront™ Client Security, has contributed to the increase.
- Any genuine increase in the prevalence of malware and potentially unwanted software would naturally tend to be reflected in the statistics, as well.

Except where specified, the data in this section has been compiled from telemetry generated 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 Exchange Hosted Services (EHS). See the Appendix for more information on these tools.

Measuring the infection rate of a set of computers can be difficult, as malware infections often involve multiple families with differing degrees of relatedness. For consistency, infection rates in this report are expressed using a metric called Computers Cleaned per Mil (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 January and removes infections from 500 of them, the CCM for that location in January is 10.0. A new version of the MSRT is released every month, so figures for multiple months, or for 1H08 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 and regularly scheduled release facilitate the comparison of relative infection rates between different populations of computers.

Geographic Trends

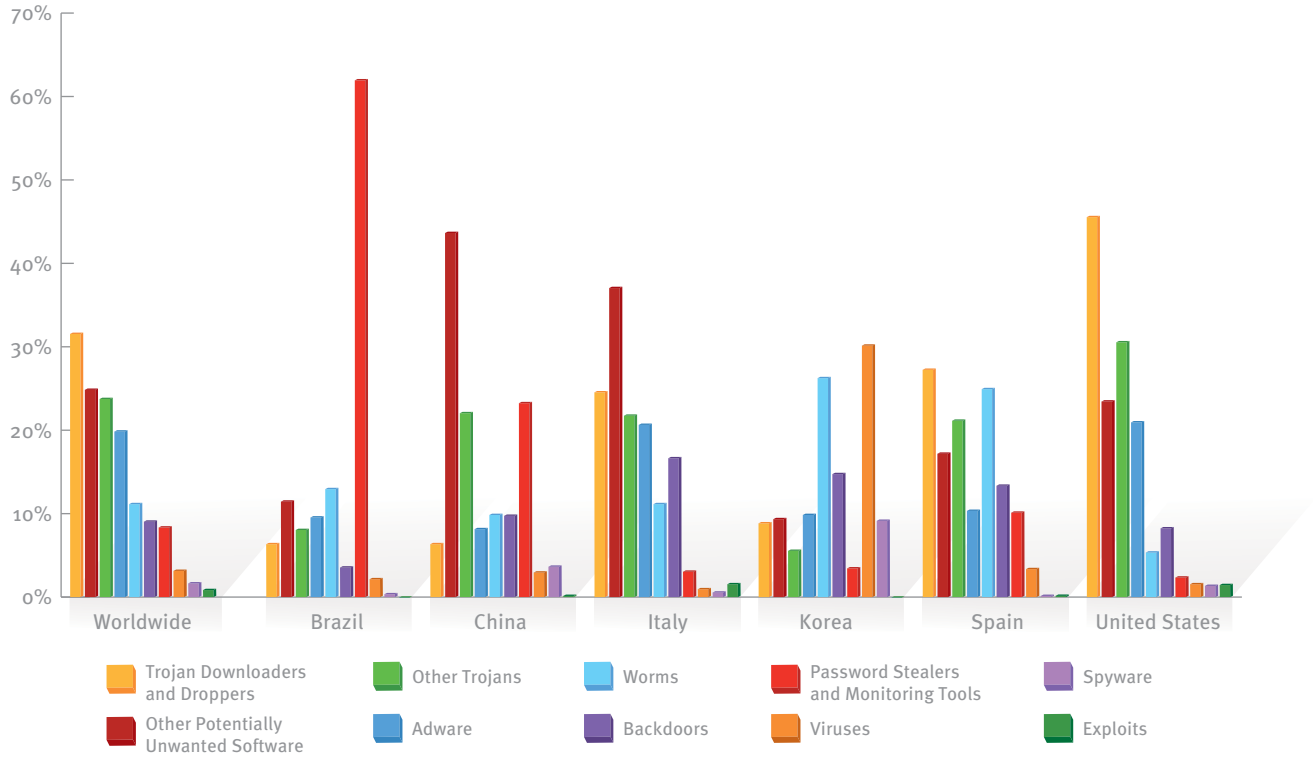
The telemetric data generated by Microsoft security products includes information about the location of the system, as determined by the setting of the **Location** tab or menu in **Regional and Language Options** in the Control Panel. This data makes it possible to compare infection rates, patterns,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

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 away from highly visible threats, like self-replicating worms, toward less visible threats that rely more on social engineering, their spread and effectiveness have become more dependent on language and cultural factors. Some threats are spread using techniques that target people who speak a particular language or who use services that are local to a particular geographic region. Others target vulnerabilities or operating system configurations and applications that are unequally distributed around the globe. As a result, security researchers face a threat landscape that is much more complex than a simple examination of the biggest threats worldwide would suggest.

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.

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 22 shows the relative prevalence of different categories of malware and potentially unwanted software in different locations in 1H08, 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.) The "Other Trojans" category consists of all trojans that are not categorized as downloaders/droppers or backdoors. The "Other Potentially Unwanted Software" category consists of all potentially unwanted software that is not categorized as adware or spyware. See the Glossary, beginning on page 143, for definitions of the other categories described in this section.

FIGURE 22. Threat categories worldwide and in six locations around the world, by incidence among all computers cleaned, 1H08



- In **Brazil**, password stealers, such as Win32/Bancos, dominate by an overwhelming margin, being detected on more than 60 percent of all Brazilian computers cleaned in 1H08. See "Win32/Bancos," on page 60, for more information about these threats.
- **China** is dominated by potentially unwanted software that targets the Chinese-language market, notably pop-up advertisement toolbars, like Win32/Sogou,[10] and browser modifiers, like Win32/BaiduSobar and Win32/CNNIC. Many of the most common families in China are Chinese-language threats that don't appear in the list of top threats for any other location.
- In **Italy**, potentially unwanted software is the largest category of threat, led by the P2P client Win32/BearShare and the advertising toolbar Win32/Hotbar.
- In **Korea**, viruses are the largest category of threat, led by Win32/Virut and Win32/Parite. Viruses often spread through 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,[11] which may contribute to the spread of infected files.

[10] See the Microsoft Malware Protection Center Encyclopedia at http://www.microsoft.com/security/portal/encyclopedia.aspx for additional information on this and other families listed in this section.

[11] As reported by the Organisation for Economic Co-operation and Development (http://www.oecd.org/sti/ict/broadband) in December 2007.

- In **Spain**, worms are unusually prominent, led by Win32/Taterf. (See "Online Gaming-Related Families," on page 62, for more information about this family.)
- In the **United States**, trojan downloaders, like Win32/Zlob, account for the largest single category of threat. (See "Win32/Zlob," on page 59, for more information.)

Figure 39 in *Supporting Data and Details*, on page 74, offers a closer look at this phenomenon, listing the relative prevalence of different categories of malware and potentially unwanted software in the 25 locations around the world with the most detections in 1H08. In addition, "Threat Assessments for Individual Locations" in *Supporting Data and Details*, on page 78, includes detailed statistics and analysis about infection rates, prevalent families and categories, and infection trends over time for 15 selected locations around the world, including the six listed above.

Demographic Trends

As a general rule, infection rates tend to be higher in developing locations than in developed locations, as reported by the MSRT. Figure 23 illustrates the infection rates of locations around the world, expressed in CCM.

FIGURE 23. Infection rates by country/region in 1H08

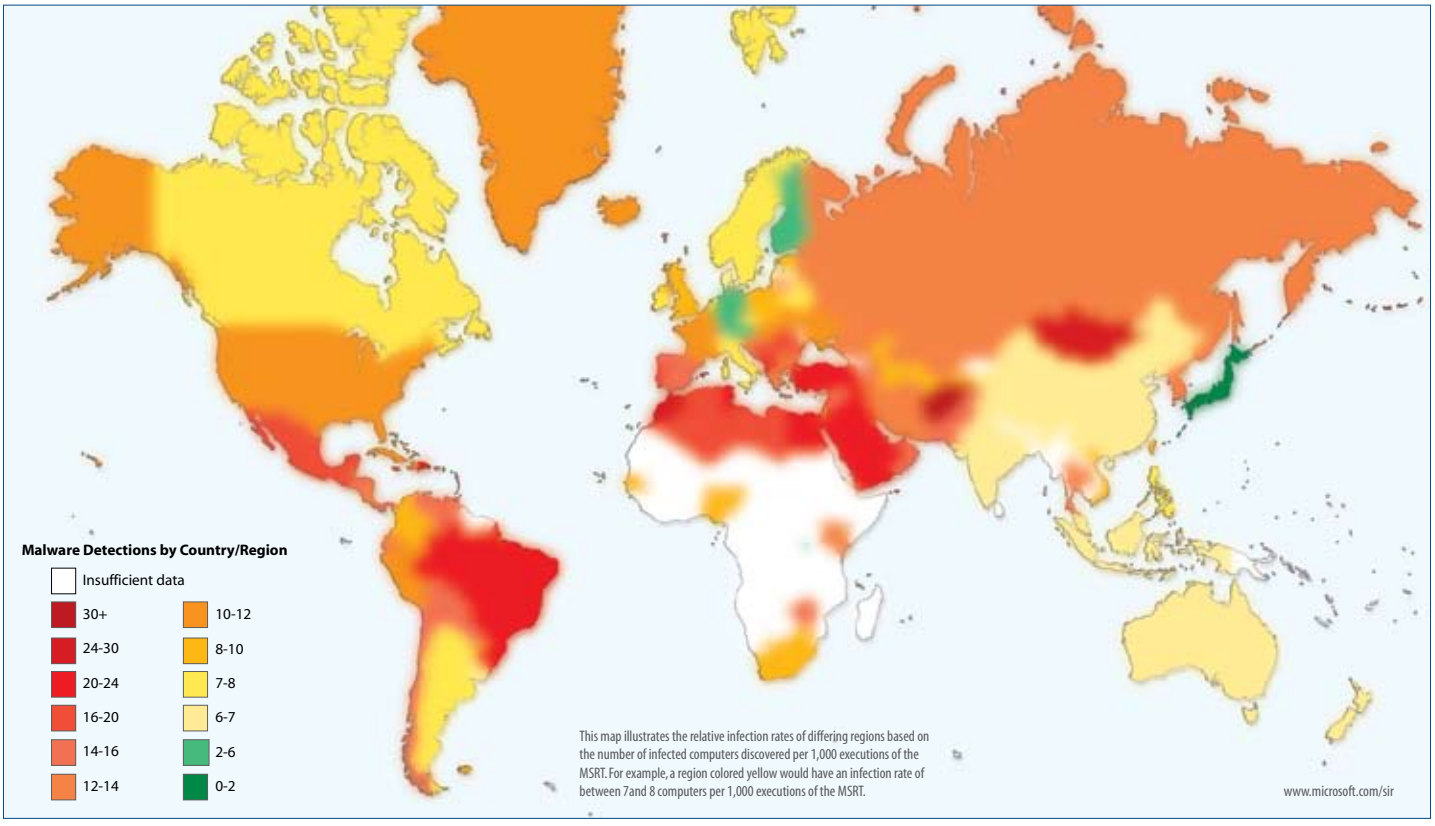


Figure 24 and Figure 25 offer a closer look at these geographic statistics, listing the 25 locations with the lowest infection rates and the 25 locations with the highest infection rates in 1H08, respectively.

FIGURE 24. Locations with the lowest infection rates, by CCM, in 1H08

Country/Region	2H07	1H08	% Chg.
Japan	1.5	1.8	22.8
Rwanda	4.2	4.2	0.3
Austria	4.1	5.2	25.7
Germany	4.4	5.3	19.7
Finland	3.8	5.7	50.9
New Zealand	3.8	6.0	58.4
India	5.5	6.2	12.3
Malaysia	4.6	6.3	35.6
Latvia	5.1	6.3	22.9
Indonesia	6.9	6.4	-7.0
China	4.7	6.6	41.1
Uruguay	5.6	6.6	17.6
Denmark	4.9	6.8	38.7
Australia	4.9	6.9	41.7
Switzerland	5.5	6.9	26.4
Hong Kong SAR	6.1	7.0	15.1
Czech Republic	5.0	7.1	41.6
Italy	5.3	7.1	34.5
Ireland	5.3	7.3	36.4
Philippines	7.3	7.4	2.0
Belarus	7.1	7.6	7.0
Singapore	5.0	7.6	52.2
Sweden	6.1	7.6	25.3
Argentina	6.6	7.7	16.6
Netherlands	5.9	7.8	32.3

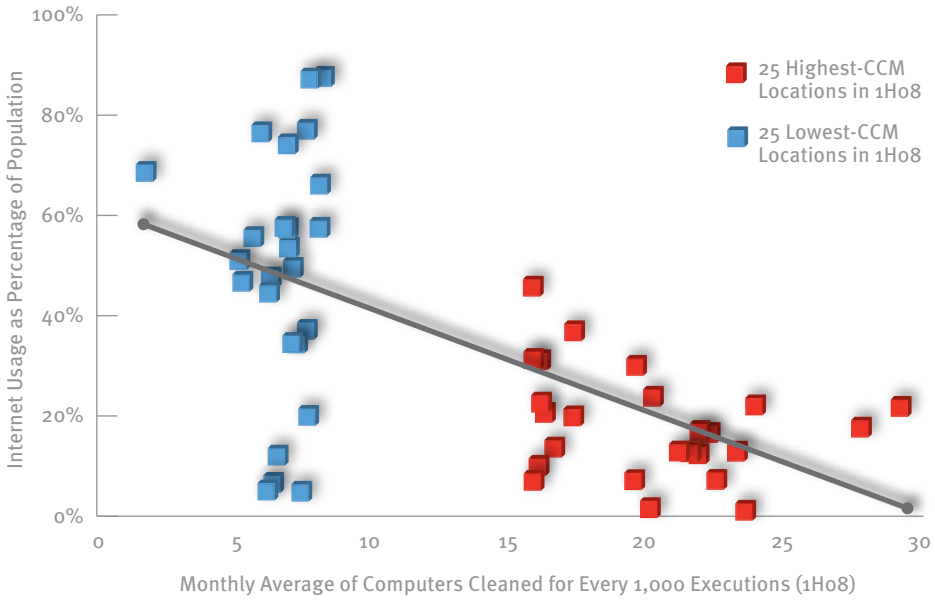
FIGURE 25. Locations with the highest infection rates, by CCM, in 1H08

Country/Region	2H07	1H08	% Chg.
Afghanistan	58.8	76.4	29.9
Bahrain	28.2	29.2	3.4
Morocco	31.3	27.8	-11.4
Albania	30.7	25.4	-17.4
Mongolia	29.9	24.7	-17.6
Brazil	13.2	23.9	81.8
Iraq	23.8	23.6	-1.1
Dominican Republic	24.5	23.2	-5.2
Egypt	24.3	22.5	-7.5
Saudi Arabia	22.2	22.3	0.4
Tunisia	15.9	21.9	37.3
Turkey	25.9	21.9	-15.4
Jordan	20.4	21.6	5.5
Former Yugoslav Republic of Macedonia	16.3	21.1	29.8
Lebanon	20.6	20.2	-1.8
Yemen	17.7	20.1	13.7
Portugal	14.9	19.6	31.7
Algeria	22.2	19.5	-12.2
Libya	17.3	19.5	13.1
Mexico	14.8	17.3	17
United Arab Emirates	18.2	17.3	-4.8
Monaco	13.7	17.0	23.7
Serbia	11.8	16.6	41.4
Bosnia and Herzegovina	12.8	16.3	27.5
Jamaica	15.0	16.3	8.9

(Infection rates are rounded to one decimal place. Percentage changes have been calculated before rounding.)

Comparing the locations on the low-infection list to those on the high-infection list suggests an inverse correlation between infection rate and measurements of computer usage as cited by the CIA World Factbook.[12] Figure 26 illustrates this correlation. (See Figure 41 in *Supporting Data and Details*, on page 77, for the figures behind this chart.)

FIGURE 26. Internet usage rates of the 25 highest-infection and lowest-infection locations in 1H08

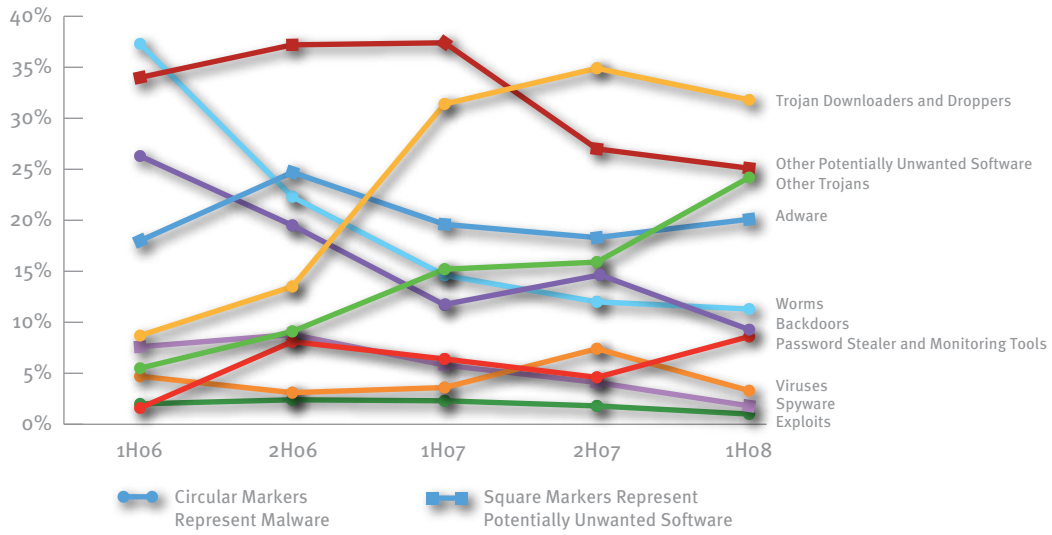


Category Trends

Figure 27 shows the relative prevalence of different categories of malware and potentially unwanted software since 1H06, expressed as a percentage of the total number of computers cleaned during each time period. Totals may exceed 100 percent for each time period because some computers are cleaned of more than one category of families during each time period. (See Figure 81 in *Supporting Data and Details*, on page 134, for the figures behind this chart.)

[12] https://www.cia.gov/library/publications/the-world-factbook/docs/rankorderguide.html

FIGURE 27. Computers cleaned by threat category, in percentages, 1H06–1H08



Malware categories often overlap, and many threats 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 "Other Trojans" category consists of all trojans that are not categorized as downloaders/droppers or backdoors. The "Other Potentially Unwanted Software" category consists of all potentially unwanted software that is not categorized as adware or spyware. See the Glossary, beginning on page 143, for definitions of the other categories described in this section.

Downloaders and Other Trojans

Trojans, including downloaders/droppers and some rogue security programs, continued to account for a large percentage of computers cleaned in 1H08.

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.

As in 2H07, downloaders/droppers remained the most prevalent category of threat, due in large part to the continued prevalence of downloader families Win32/Zlob and Win32/Renos, which together were responsible for more than 96 percent of the computers cleaned in this category. 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 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.

The "Other Trojans" category rose to become the third most prevalent category of threat in 1H08, due mainly to improved detection of a number of widespread trojan families (specifically Win32/Vundo and Win32/Virtumonde, which were added to the MSRT in February).

Potentially Unwanted Software

Potentially unwanted software categories, including adware and spyware, remained high on the list in 1H08, comparable to trojans and other malware categories. 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 54, for more analysis.

Other Threats

Detection of password stealers and monitoring tools, though low in comparison to other threats, jumped in 1H08 due to the addition to the MSRT in June of several password stealers aimed at players of online games. See "Online Gaming-Related Families," on page 62, for more information about these families.

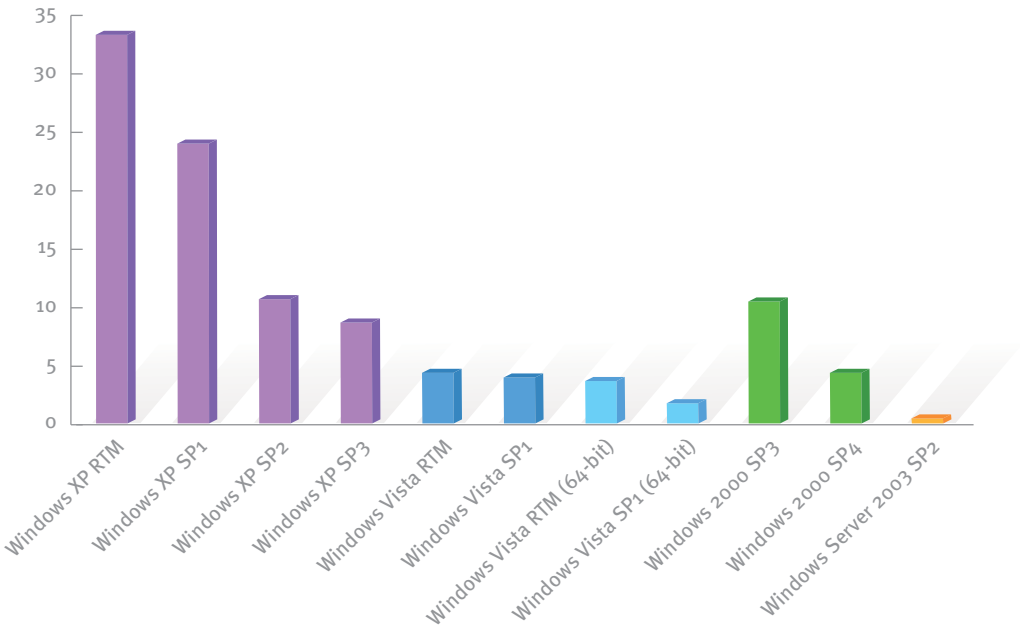
Backdoors and worms, which were two of the most significant categories of threat as recently as two years ago, continued to recede in prominence relative to other categories, as did viruses. Bots are considered a subcategory of backdoors, so the decline in the prevalence of backdoors suggests that the 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 categories also include exploit code that assists in accomplishing the malware's primary function.

See "Selected Prevalent Families," beginning on page 59, for a discussion of the families mentioned in this section.

Operating System Trends

Different Microsoft Windows operating system versions show differing rates of infection due to differences in the way people and organizations use each version, in addition to the different features and service packs that are available for each one. Figure 28 shows the CCM for each Microsoft Windows operating system/service pack combination that accounted for at least 10,000 cleanings or at least 0.1 percent of total MSRT executions in 1H08.

FIGURE 28. Number of computers cleaned for every 1,000 MSRT executions, by operating system, 1H08



For a closer look at these statistics, see Figure 84 in *Supporting Data and Details*, on page 138.

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 48.8 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 56.2 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 85.4 percent less than that of the RTM version of Windows XP.

The gap between Windows XP and Windows Vista has decreased in size somewhat since 2H07, which can be attributed to continued growth of the Windows Vista user base among the general population and to popular malware families' heavy reliance on social engineering, which can deceive users into bypassing security measures, such as User Account Control in Windows Vista. The infection rate for the 64-bit configurations of Windows Vista were both lower than those of their 32-bit counterparts—48.2 percent less for Windows Vista SP1, and 14.4 percent less for the RTM version.

- 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 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 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 2003, which includes only server editions, has the lowest infection rate of any configuration on the chart, while the Windows XP configurations, intended for home and workplace users, have several of the highest. Windows 2000, 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.

User Reaction to Alerts

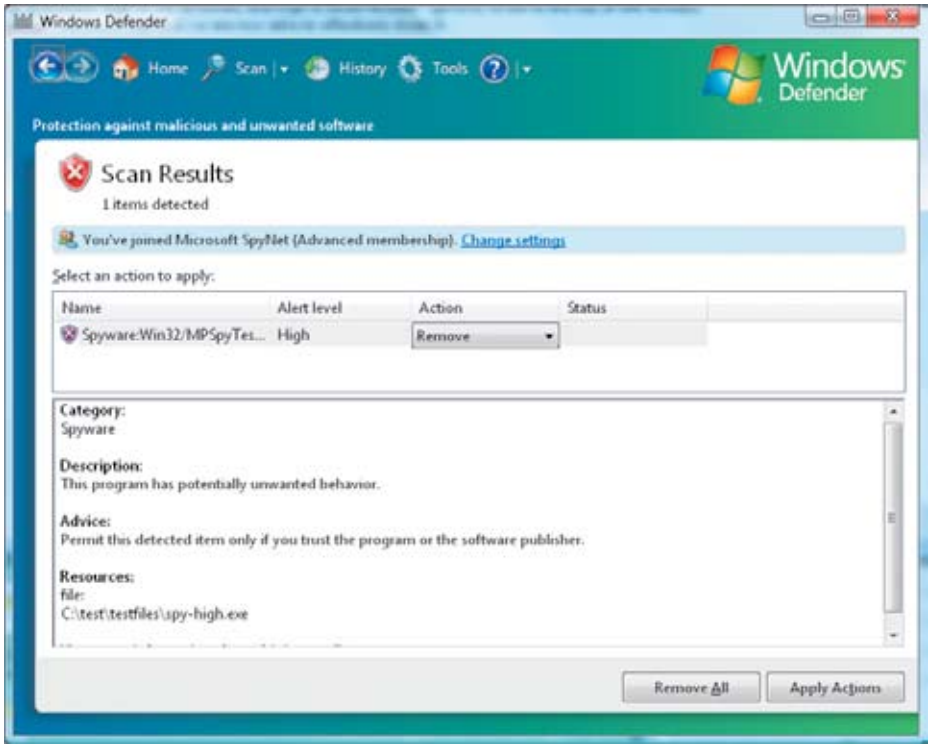
Software cannot always be classified in binary terms as "good" or "bad." Some software inhabits a gray area wherein the combination of behaviors and value propositions presented by the software is neither universally desired nor universally reviled. This gray area includes a number of programs that do things like display advertisements to the user, which are often targeted based on the programs' observation of the user's browsing habits. 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 individual.

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, in addition to a choice of actions, 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 will be removed automatically during scheduled scans. For viruses, a **Clean** option is offered to remove the virus from the infected files and to leave the files on the computer, if possible.

FIGURE 29. A user action prompt from an on-demand scan in Windows Defender



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** indicates a clear, active choice. **Always Allow** usually suggests that the user wants to keep the software. However, users choose **Quarantine** or **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 30 and Figure 31 list the most-removed and least-removed families with more than 100,000 detections in 1H08, 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 30. The 10 most-removed families with more than 100,000 detections, sorted by total percentage of removals and quarantines, 1H08

Threat Family	Alert Level	Default Action	Total Removal %	Ignore %	Always Allow %
Win32/Hamweq	Severe	Remove	99.9%	0.0%	0.0%
Win32/Magistr	Severe	Clean	99.9%	0.0%	0.1%
HTML/Meloits	Severe	Remove	99.9%	0.0%	0.1%
JS/Redirector	Severe	Remove	99.9%	0.0%	0.1%
JS/Decdec	Severe	Clean	99.9%	0.0%	0.1%
Win32/Anicmoo	Severe	Remove	99.9%	0.0%	0.1%
HTML/Repl	Severe	Remove	99.9%	0.0%	0.0%
Win32/Gida	Severe	Remove	99.9%	0.0%	0.1%
Win32/Parite	Severe	Clean	99.7%	0.0%	0.3%
Win32/Delflob	Severe	Remove	99.7%	0.0%	0.2%

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

FIGURE 31. The 10 least-removed families with more than 100,000 detections, sorted by total percentage of removals and quarantines, 1H08

Threat Family	Alert Level	Default Action	Total Removal %	Ignore %	Always Allow %
Win32/BearShare	Moderate	Select Action	9.2%	90.1%	0.7%
Win32/RealVNC	Moderate	Select Action	12.0%	80.5%	7.4%
Win32/SeekmoSearchAssistant	Moderate	Select Action	20.7%	79.3%	0.1%
Win32/RewardNetwork	Low	Select Action	23.1%	76.8%	0.0%
Win32/Hotbar	Moderate	Select Action	23.6%	76.3%	0.1%
Win32/Starware	Low	Select Action	25.2%	74.6%	0.2%
Win32/ZangoSearchAssistant	Moderate	Select Action	26.0%	73.9%	0.1%
Win32/AdPanel	Moderate	Select Action	29.5%	70.4%	0.1%
Win32/Baidulebar	Moderate	Select Action	30.6%	69.3%	0.2%
Win32/BrowsingEnhancer	Moderate	Select Action	31.0%	68.9%	0.1%

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

Users' reactions to warnings about these families varied significantly, indicating clearly 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.
  - Win32/RealVNC and Win32/BearShare have the lowest rate of removal, by a significant margin, among widespread families. RealVNC is a program that enables a computer to be controlled remotely, similar to Remote Desktop. It has a number of legitimate uses, but is considered potentially unwanted software because it can be used by an attacker with malicious intent to gain control of a user's computer under some circumstances. The relatively high **Always Allow** rate for this software (7.4 percent) indicates that many users are aware of the nature of the software and wish to retain it for its perceived value. Nonetheless, an even higher percentage (12.0 percent) chose to **Remove** or **Quarantine** the software immediately, presumably indicating that they did not intentionally install the software.

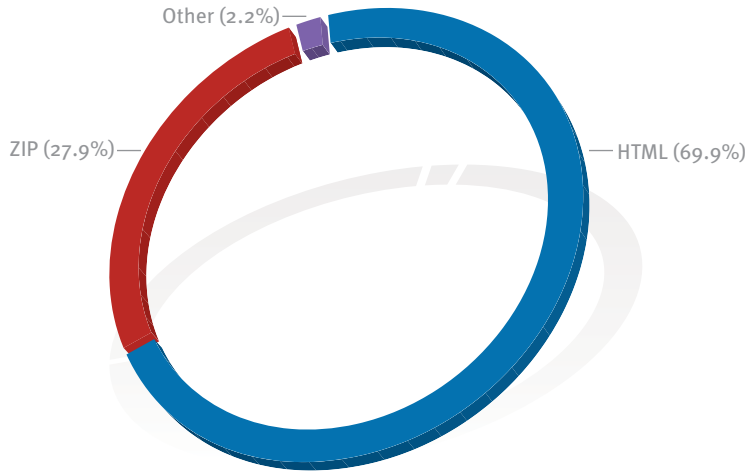
BearShare is a P2P file-sharing client that uses the decentralized Gnutella network. Free versions of BearShare have come bundled with advertising-supported and other potentially unwanted software. The low rate of removal indicates that many users see value in the program and believe its benefits outweigh any specific behaviors that are unwanted by some.

- 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/SeekmoSearchAssistant and Win32/Hotbar offer functionality, such as "smileys," or other free content in exchange for targeted advertising.

E-Mail Threats

Many e-mail systems block incoming attached files of types that are often used to transmit malware. In 1H08, eight extensions accounted for 99.8 percent of the attachments detected by EHS, with just two extensions—.html and .zip—accounting for 97.8 percent of detected attachments.

FIGURE 32. Messages with file attachments detected by EHS, by file type, in 1H08



The threat most detected by EHS in 1H08 by a wide margin was HTML/IframeRef, which was detected more than seven times as often as the second most prevalent threat. HTML/IframeRef is an exploit that involves an inline frame, or iFrame, embedded in an HTML document that is typically sent to the intended victim in an e-mail message. The inline frame, which may be as small as a single pixel (to avoid visual detection), points to a page on a remote Web site that contains malicious code. If the user's computer is vulnerable to this exploit, the malicious code can infect the computer when the e-mail is read. The fix for the vulnerability targeted by this exploit was released by Microsoft in 2004,[13] so computers running Microsoft Windows XP SP2 or later, or which have the latest security updates installed, are not vulnerable to this threat. Other threats commonly detected by EHS in 1H08 include e-mailed phishing attempts and several variants in the Win32/Cutwail family. (See page 61 for more information about this family.)

See Figure 85 in *Supporting Data and Details*, on page 139, for a listing of the top 25 variants blocked by EHS in 1H08 and 2H07.

[13] See Microsoft Security Bulletin MS04-040 for details.

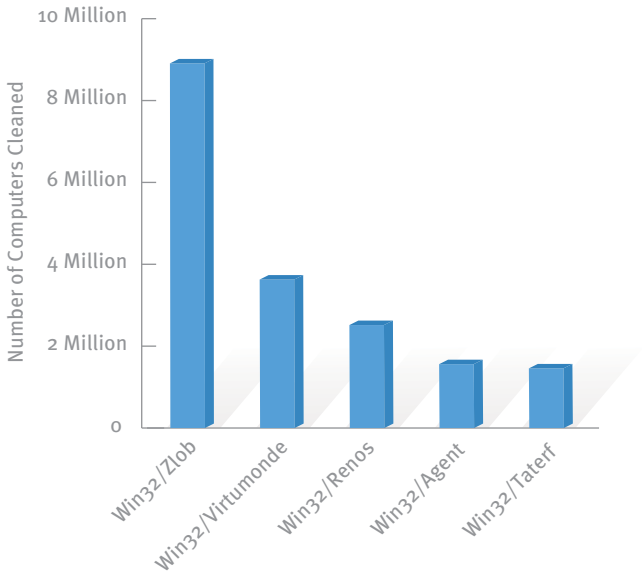
Selected Prevalent Families

These are some of the families that attracted attention in 1H08, due to overall prevalence or increased recent activity. In addition to following the specific guidance provided below, users can help protect themselves from infection by using the information and tips presented at the Microsoft Security Central (http://www.microsoft.com/security) and Microsoft Security At Home (http://www.microsoft.com/protect) Web pages. See "Malware Family Data" in *Supporting Data and Details*, on page 133, for a listing of the top 25 malware and potentially unwanted software families removed from computers by all Microsoft security products in 1H08.

Win32/Zlob

Though not especially notable from either a technical or a social-engineering perspective, Win32/Zlob deserves attention due to the sheer magnitude and persistence of the threat. Since 1H07, Win32/Zlob has been the malware family most detected by Microsoft products by a wide margin. In 1H08, it was removed from more than twice as many computers worldwide as the second most prevalent family.

FIGURE 33. The five families removed from the most computers in 1H08



Win32/Zlob spreads primarily through social engineering. It typically poses as a media codec a user must download to watch video content downloaded or streamed from the Internet. Some Zlob variants even include an end-user licensing agreement (EULA) when installing. Once installed on the target computer, Zlob bombards the user with pop-up advertisements and fake "spyware warnings" that are actually advertisements for rogue security software. It may also reconfigure the Internet Explorer start page and modify the computer's HOSTS file to redirect attempts to access certain Web sites.

To protect themselves from Win32/Zlob, users should pay extra attention when asked to download a media codec and should only download codecs from sites they trust. The Web site http://www.wmplugins.com, which offers legitimate codecs for Windows Media Player users to download, is a good starting place.

Win32/Vundo and Win32/Virtumonde

Win32/Vundo and Win32/Virtumonde are two names for a multi-component malware family that displays pop-up advertisements for rogue security software. In 1H08, it was the second most commonly detected family worldwide, behind Win32/Zlob.

Win32/Virtumonde is often installed through the use of a downloader component that may be distributed to victims through spam or a browser exploit, and is sometimes also bundled with other potentially unwanted software. Once the downloader is installed, it connects to one of a number of different IP addresses around the world to download advertising materials and software updates. Win32/Virtumonde has also been observed to transmit a large amount of system information during this connection, including e-mail and Internet account details, operating system details, information about the computer's network adapter (including its media access control [MAC] address), keyboard layout, crash logs, and other information. Win32/Virtumonde has been observed using encryption techniques to obfuscate its communication with rogue sites.

Once installed, Win32/Virtumonde operates as a browser helper object (BHO) that displays advertisements for rogue security software. These are programs that masquerade as legitimate security programs offering protection from malware, spyware, and other threats, but actually uses social engineering to obtain money from victims while offering 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. Win32/Virtumonde also has the ability to block the display of other pop-up advertisements, presumably as an anti-competitive measure, and may redirect URLs entered by the user to URLs of the program's choice.

Win32/Virtumonde may terminate services associated with several security-related applications. Recent variants have been observed attempting to disable Automatic Updates. These variants may also check whether the MSRT is running and close it if it is detected.

To protect themselves from Win32/Virtumonde, users should avoid clicking links in spam messages and on Web sites they don't trust and should be careful about installing software from unknown or untrusted sources.

Win32/Bancos

Win32/Bancos is a family of data-stealing trojans that captures online banking credentials, such as account login names and passwords, and then relays the captured information to the attacker. Most Win32/Bancos variants target customers of Brazilian banks, though some variants target customers of banks in other locations. Win32/Bancos was the most detected family in Brazil in 1H08 by a wide margin, and the tenth most commonly detected family worldwide.

Win32/Bancos typically searches the system for cached passwords and then monitors open browser windows looking for bank names in the title bar or bank URLs in the address bar. If a victim visits a page with a page title that the trojan is looking for, it typically captures the victim's credentials as they are entered or uses phishing techniques to direct users to fake Web pages disguised to look like the original bank pages. The trojans may also log keystrokes to record credentials that a user enters at banking Web sites.

After capturing the user's credentials, Win32/Bancos sends them to the attackers by e-mail or by posting them to an FTP or Web site controlled by the attackers. Some variants use accounts established with large Web-based e-mail providers to send the stolen credentials, often to another Web-based e-mail account.

Regularly changing the passwords they use to transact business online with banks and other financial services can help users protect themselves against Win32/Bancos and similar threats.

Spammers: Win32/Cutwail and Win32/Oderoor

Although the Win32/Nuwar botnet[14] has received a lot of attention over the past year and a half for its size and spam, its position may have been supplanted to some degree in 1H08 by spam networks created by two other malware families, Win32/Cutwail and Win32/Oderoor.

Win32/Cutwail is a multipurpose threat family that was the twenty-third most prevalent family worldwide in 1H08. Categorized as a downloader, Win32/Cutwail usually downloads a trojan that is used to send spam. It also employs a rootkit and other defensive techniques to avoid detection and removal.

Win32/Cutwail uses e-mail attachments as a significant means of self-propagation—of the top 25 individual variants blocked by EHS in 1H08, 17 were Cutwail variants. (See "E-Mail Threats" on page 58 for more information.)

Win32/Oderoor is a backdoor trojan that is primarily distributed through IM programs. When Win32/Oderoor was added to the MSRT in May 2008, it was the fourth most removed family of the month. Microsoft researchers estimate that the size of the Win32/Oderoor network was about 80 percent of that of the Win32/Nuwar network in 1H08 and was probably responsible for a larger volume of spam.

CAPTCHA Breakers: Win32/Newacc and Win32/Captiya

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.

[14] See "A Focus on Win32/Nuwar," in *Microsoft Security Intelligence Report, July through December 2007*, for more information about this botnet and the malware family behind it.

Spammers have responded by releasing malware that aids in the process of circumventing CAPTCHA. Win32/Newacc, a family of automated spamming tools that was added to the MSRT in March 2008, automatically registers new e-mail accounts on Windows Live Hotmail®, AOL, Gmail, Lycos, and other account service providers. To achieve this, the tool connects to the login page of the targeted e-mail service provider and then downloads the registration form and the associated JPEG format CAPTCHA image. The image file is temporarily stored in the Windows folder and is then submitted to a Web service that performs optical character recognition (OCR) on the file. If the CAPTCHA image is properly decoded, Win32/Newacc submits the registration form using a list of user names provided by a connection with a remote site.

Win32/Cutwail appears to be a significant transmission vector for Win32/Newacc. Win32/Cutwail was observed to download and install Win32/Newacc in a laboratory environment, and 89.3 percent of the computers that were cleaned of Win32/Newacc by the March 2008 version of the MSRT were also cleaned of Win32/Cutwail.

Another CAPTCHA-related family is Win32/Captiya, a low-volume threat that is occasionally distributed with Win32/Newacc. Win32/Captiya is not involved in decrypting CAPTCHA directly. It 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.

Online Gaming-Related Families

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. Perhaps inevitably, this has led to the development of a curious new class of threat—worms and trojans that steal players' gaming passwords on behalf of thieves who can then auction the victim's virtual loot themselves. The most prevalent of these threats has been Win32/Taterf, which is actually a modified version of another worm, Win32/Frethog. Both worms are believed to have been developed in China. Other threats that target online game passwords include Win32/Tilcun, Win32/Ceekat, and Win32/Corripio, in addition to a number of others.

Win32/Taterf owes much of its spread to its method of distribution. The worm spreads by copying itself to the root of all fixed or removable drives on the infected system, creating autorun.inf files wherever it spreads. The autorun.inf file is used to execute the worm whenever the drive is viewed with Windows Explorer. This technique was actually first used by worms several years ago without much success, although the recent popularity of USB flash drives has made it a more effective method of transmission.

Eight password-stealing families were added to the MSRT in June 2008. Just one week after release, these families had been removed from more than 2.5 million unique computers worldwide. In total, the MSRT removed Win32/Taterf and Win32/Frethog from enough computers during the last three weeks of June to make them the tool's fourth and eighth most removed families for all of 1H08, respectively. Figure 34 lists the eight families in order of the number of unique computers cleaned by the June MSRT.

FIGURE 34. Online game password stealers removed by the June 2008 MSRT, by number of unique computers cleaned

Family	Unique Computers Cleaned
Win32/Taterf	1,536,831
Win32/Frethog	808,624
Win32/Tilcun	473,422
Win32/Ceekat	346,683
Win32/Corripio	67,843
Win32/Zuten (including WinNT/Zuten)	54,947
Win32/Lolyda	36,728
Win32/Storark	593

"Serious" gamers may be aiding in the spread of these families due to a general reluctance to run real-time antivirus software in the belief that it imposes an unacceptable performance cost. Gamers who download cracks, cheats, and pirated copies of games from file-trading sites are also at increased risk of infection, as malware distributors often upload trojans masquerading as such programs.

Breaking these figures down geographically shows a pattern, with the People's Republic of China being home to more than twice as many infected computers as the next most infected locale, as shown in in Figure 35.

In China, gaming is often done in Internet cafés or on other public terminals, which are used by large numbers of people and present a greater opportunity for infection than a private computer. For example, if just one person inserts a 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. It is therefore particularly important for operators of public Internet terminals to install antivirus software and keep it up to date. Other best practices would be to prevent customers in those Internet cafés and other public places from installing software on computers at all or to use virtualized disk images to return all computers to a known clean state at the end of each session or business day. (Virtualized images should of course be kept up to date with the latest security updates and antivirus definitions as part of ongoing maintenance.)

FIGURE 35. Unique computers with online game password stealers removed by the June 2008 MSRT in its first week of release, by location

Country/Region	Unique Computers Cleaned
China	777,882
Taiwan	326,320
United States	265,952
Spain	282,439
Korea	230,617
Turkey	124,965
Mexico	92,459
France	64,800
Russia	63,042
Japan	61,901
All Others	314,808

A Focus on Malware and Signed Code

Microsoft Authenticode® is a technology that can help ensure the source of code. It does not ensure that code is safe to run, but it can ensure that the code is associated with an entity in a trust chain.[15]

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

Code signing is a powerful method of authoritatively identifying code, assuring its integrity at the time of signing and the identity of the code signer. Signed code can be much easier to research and analyze because of the certainty of the association of the signer with the file. For this reason, anti-malware vendors are among the most diligent code signers. This assertion of identity also scales very well—a few code-signing certificates positively identify millions of genuine Microsoft files. Signing also enables features, like 64-bit Windows Vista Kernel Mode Driver Signing, that can help improve security by enforcing a code-signature requirement and preventing unsigned code from being modified and loaded.

Certificates on Non-Malicious Files

In the first six months of 2008, 10,600 valid code-signing certificates were reported on more than 1.78 million distinct non-malicious files to the Microsoft Malware Protection Center (MMPC). In the same period, 2,447 invalid certificates were reported on 33,078 files. Invalid certificates can mean the file was altered after signing, there was a problem with the certificate on the local computer, the certificate was revoked, or another failure occurred when the local computer attempted to verify the file.

Nearly the same number of unsigned, non-detected files (1.8 million) were reported in the same time period to the MMPC.

Code signing of files by legitimate vendors appears to be accelerating due to a number of benefits, including the ability to source signed code and code signing providing defense against tampering, corruption, or malware infection in code.

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

MpCmdRun.exe: Demonstrating the Importance of Code Signing

MpCmdRun.exe is the file that Windows Defender uses to schedule scans and download definition updates. Over time, Microsoft has shipped more than two dozen code-signed versions of this file.

In the same time period, more than 30,000 distinct files named MpCmdRun.exe have been reported to Microsoft with no code signature or broken code signing to Microsoft. Code signing can be broken by file corruption from unknown sources, tampering, or malware infection. More than 22 different malware families are known to infect files named MpCmdRun.exe.

For software developers, code signing is an excellent defense against tampering and acts as a warning in the case of malware infection. Of course, before signing any file, it is strongly recommended that a thorough malware check be performed on the file. Microsoft standard practice is to virus-scan and code-sign all code that the company ships.

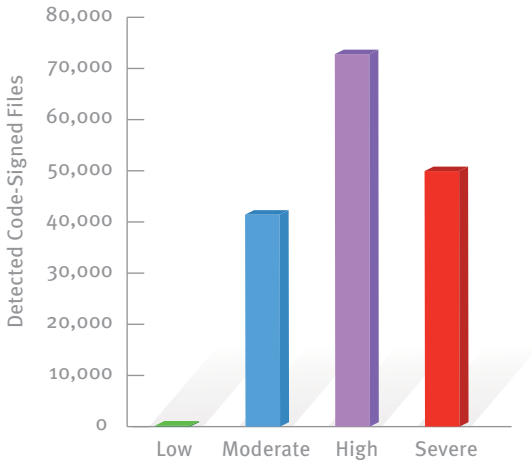
Certificates on Detected Files

In theory, malicious code can be code signed in a number of ways. A legitimate publisher could sign malicious code mistakenly, private keys issued to legitimate entities could be stolen and used to sign code, or malware authors can be issued a certificate by a CA. The MMPC has not confirmed any cases of private keys being stolen and used on detected code, or any cases of mistaken signing by a legitimate entity, but has confirmed many cases of CAs issuing code-signing certificates to malware authors. This usually results when CAs participating in the Microsoft Root Certificate Program issue code-signing certificates to a software publisher who uses the certificate to sign malware. In some cases, the CA is owned and operated by the malware authors, and the first step in infection is tricking users into installing a root certificate. In most cases, though, CAs participating in the Microsoft Root Certificate Program are tricked into issuing a valid certificate to the malware author.

In the first six months of 2008, the MMPC received reports of about 22 million instances of distinct malware files, of which about 173,000 were distinct malware files with code signatures. Of this malware with code signatures, about 38,000 had signatures that were not valid for signing code, so approximately 135,000 validly signed malware files were reported to Microsoft. In total, approximately 0.6 percent of detected malware was validly signed.

Of signed detected files, the severity of the threats tended to be High or Severe, with Low and Moderate threats making up a much smaller number of files.

FIGURE 36. Detected code-signed malware files, by severity, 1H08



When the MMPC encounters code-signed malware spreading in the wild, it creates detection signatures and contacts the issuing CA with details of the file in question so the CA can review the issued certificate to determine if any action is needed. CAs maintain Certificate Revocation Lists (CRLs) on the Internet, which list mistakenly issued, abused, or other problem certificates. Software, like Windows Internet Explorer 7, attempts to check CRLs when verifying code signing of any downloaded code.

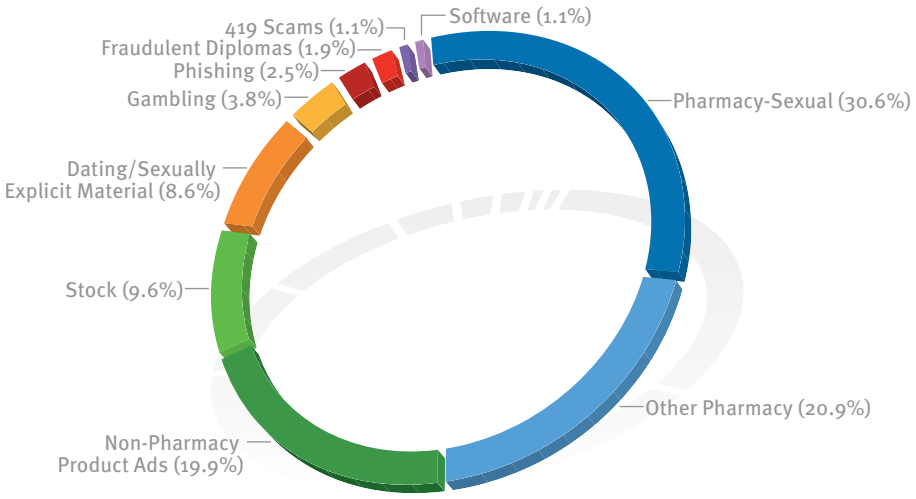
Although certificates are also intended to identify the signing parties, Microsoft has been unable to identify any authors of signed malware in cooperation with CAs because the malware authors exploit gaps in issuing practices and obtain certificates with fraudulent identities.

Spam and Phishing Trends

More than 90 percent of e-mail messages sent over the Internet are spam. Not only does all this unwanted e-mail tax the recipients' inboxes and the resources of e-mail providers, the influx of spam creates the ideal environment for malware attacks and phishing attempts. Blocking spam and phishing is a top priority for e-mail providers, social networks, and other online communities.

Figure 37 shows the spam blocked by Microsoft Exchange Hosted Services (EHS), by category, in the first half of 2008.

FIGURE 37. Inbound messages blocked by EHS, by category, 1H08



Advertisements for pharmaceutical products accounted for 51.5 percent of the spam messages blocked by EHS in 1H08, with advertisements for sexual performance products, such as Viagra and Cialis, accounting for the majority of those (30.6 percent of the overall total). Non-pharmaceutical product advertisements account for another 19.9 percent of the total. Of the remainder, most involve overt scams, like "pump-and-dump" stock schemes and fraudulent university diplomas. Notably, phishing attacks accounted for 2.5 percent of the total number of e-mail messages blocked. Even though 2.5 percent is a small percentage, it is still a significant number, considering the total volume of e-mail messages blocked.

Botnet Tactics Changing

Overall, the amount of spam that successfully evades the blocking and filtering techniques used by services like Windows Live Hotmail and EHS to land in users' inboxes has decreased dramatically from its peak a few years ago, though the trend has been much flatter over the last year or two, indicating a state of rough equilibrium between spammers and e-mail services. This should not be taken as a sign that the pace of advancement and adaptation has slowed on either side, but rather that both spammers and spam fighters continue to adapt to new techniques deployed by their opponents, creating a complicated sort of stalemate in which neither side has managed to gain the upper hand.

Among the recent adaptations made by spammers is a large-scale trend away from sending spam directly from botnets and toward a greater reliance on free e-mail services, like Windows Live Hotmail, for originating spam messages. In previous periods, it was common for bot-herders to install hidden Simple Mail Transfer Protocol (SMTP) servers on controlled computers and send e-mail directly through port 25, the SMTP port. Most residential and small business Internet connections use dynamic IP addressing, which enables bot-herders to take advantage of an additional layer of obfuscation when disguising the source of their spam and makes it difficult for systems receiving e-mail to use blacklists to block message delivery from controlled computers. Recently, however, several larger ISPs and e-mail services have been able to create reasonably accurate lists of dynamic IP address ranges in use worldwide and to use them to block any e-mail sent from a dynamic IP. Although this technique can make it difficult for a legitimate company or organization running a mail server on a dynamic IP account to send mail to these recipients, it has shown some success at cutting down the amount of spam received directly from botnets.

Although botnets still send significant amounts of spam through port 25, they appear to have adapted to the blocking measures described above by shifting large parts of their spam-sending operations to free e-mail providers. Spam sent through services such as Gmail, Windows Live Hotmail, and Yahoo! Mail has doubled or tripled over the past year, enabled by malware that uses techniques such as screen scraping and automated form submittal to send mail through the services' Web interfaces as a human would.

As these services are usually quick to detect and disable accounts used for spamming, spammers must create new accounts in bulk for use during each spamming run. Free e-mail providers have been implementing techniques such as CAPTCHA to discourage bulk account creation for several years. In response, spammers have developed their own techniques to break or circumvent popular CAPTCHA implementations. Some spammers manage to create accounts automatically using software that can correctly decipher the CAPTCHA images used by popular e-mail providers at least part of the time, often with the aid of malware. (See "Spammers: Win32/Cutwail and Win32/Oderoor," on page 61, for more information.) More often, however, spammers simply pay humans to open accounts in bulk, typically in parts of the world where labor is relatively inexpensive. Spam researchers at Microsoft believe that spammers can make money by sending as few as 40–50 messages from each e-mail account before it is shut down.

Reputation Hijacking

An unfortunate effect of this shift to free e-mail providers has been a decline in the value of reputation as a tool for fighting spam. The spam-filtering algorithms used by large e-mail processors typically take reputation into account when processing incoming messages—a message originating from a domain with a good reputation is considered significantly less likely to be spam than a message originating from a poorly regarded or unknown domain. Large, Web-based e-mail services, such as the ones listed earlier, have historically been

relatively successful at preventing spammers from sending large amounts of spam from their domains, so their reputations have typically been quite good. As spammers have become more effective at exploiting these systems, however, their reputations have been damaged. This forces e-mail filters to rely more on resource-intensive content analysis when assessing mail originating from these domains.

Fighting the New Techniques

Facing continued erosion of their reputation, free e-mail providers are aggressively fighting the latest wave of spammer activity. Advances in algorithmic pattern recognition have rendered most of the earliest CAPTCHA implementations ineffective, so researchers continue to develop improved implementations that are more difficult for computers to break yet are still reasonably easy for humans to solve. Implementations currently being used by e-mail services include features like characters that overlap and deviate significantly from a common baseline.

FIGURE 38. A visually complex CAPTCHA image from the Windows Live Hotmail sign-up page

Phishers Targeting Social Networks

Beginning in 2007, phishers have been increasingly targeting users of popular social networking sites for password theft, often using the messaging features of the sites themselves to distribute their attacks. One popular site was victimized by phishers who used cascading style sheets (CSS) to place disguised links on profile pages. When a visitor clicked one of the disguised links, it would lead to a fake logon page hosted externally, implying that the user had to log on to the service to access the desired content. This kind of attack owed much of its effectiveness to the fact that the profile page hosting the rogue CSS—often a compromised account belonging to someone with no connection to the phishers—displayed the correct domain in the browser's address bar and otherwise showed no external indication that there was anything wrong with the page.

This site implemented user interface changes in 1H08 that significantly reduced the effectiveness of phishing attempts, but social networks remain an attractive target for phishers. Often, attackers are not particularly interested in obtaining credentials for the social networking sites *per se* (although having access to compromised accounts can facilitate

future phishing attempts, as described above). Rather, because users often use the same user names and passwords to access multiple Web sites, phishers use these attacks to build lists of credentials that they can try at more traditional phishing targets, like bank sites and online auction sites.

Notably, the total number of phishing pages active at any one time is believed to have remained roughly consistent throughout 1H08, even as the operators of the largest social networking sites have improved their ability to deter attacks. Phishers have responded by shifting their emphasis back to traditional targets, such as banks, and by targeting smaller social networks with fewer users. One beneficial aspect of this shift to smaller social networks is that the phishers are required to distribute their efforts over a larger number of sites, each with its own culture and implementation details, to target the same number of users. This has the effect of making social network phishing more labor-intensive and, therefore, potentially less profitable.

International Phishing Attempts Increase

Though U.S.-based financial institutions remain the most frequent target for phishing attempts, Microsoft phishing researchers have seen a gradual move towards targets located in other English-speaking countries, notably the United Kingdom and India. As a result, these countries are seeing many of the same trends that have been underway in the United States for the past few years. For example, attacks in India formerly targeted large, nationwide financial institutions almost exclusively, but have recently begun to target smaller, regional Indian banks that may not be as prepared to guard against phishing as their larger competitors.

Microsoft Malware Protection Center Executive Afterword

Well, here we are again, six months from our last report, and as you've read, there's more of the same and more and more of the new. We saw trojan downloaders/droppers continue to be the most prevalent threat worldwide, making up more than 30 percent of all the threats we detected in 1H08. This category of threat remains the tool of choice for malware authors, who frequently update their code and their social engineering techniques to attempt to defeat anti-malware products. In fact, because of a very high number of variants and ever-changing social engineering techniques, one family of trojans—Win32/Zlob—remains the top infection detected worldwide despite signatures being included in anti-malware products for two years and updated very frequently to detect new variants.

For this volume of the *Security Intelligence Report* (SIR), we also included some brand new research into the prevalence of browser-based exploits on Windows-based computers around the world. Browser-based applications are becoming ever richer in functionality and more popular with computer users globally. We see more malware authors targeting these applications instead of attacking the operating system and traditional applications, which are becoming increasingly difficult to exploit thanks to innovations like the Security Development Lifecycle (SDL).

We saw some fascinating results from this research: On Windows Vista–based computers, 94 percent of the browser-based exploits targeted non-Microsoft software. The top 10 browser-based exploits on Windows Vista–based computers all targeted non-Microsoft software. This highlights the importance of IT professionals and computer users keeping all of the software on their computers up to date. Services such as Windows Update and Microsoft Update will ensure that Microsoft software is kept up to date, but it is extremely important that third-party software is also correctly updated.

This volume of the SIR also has a different look and feel. We got great feedback on previous volumes of the SIR, but one request was loud and clear: Make the SIR easier to read in terms of describing the threat landscape and what all this data actually means to the IT professional or computer user. Jimmy Kuo, one of our senior security researchers, and Jeffrey Friedberg, from the Trustworthy Computing team, did a great job in describing the "threat ecosystem" and how the various players interact with each other. I hope this helps set some context for the work we do here at Microsoft to make the Internet a safer place to work and play.

One thing that should be clear from the threat ecosystem discussion is that it is more important than ever that computer users and IT professionals keep their defenses and strategies under review, and to think more holistically about security. Given the variety of different ways that users can be compromised, relying on a few simple lines of defense (a firewall, Windows Defender) is no longer enough. A user can be attacked across a surprisingly wide range of vectors now—in addition to the traditional attack vector of infected e-mail attachments, the user can click on a maliciously crafted URL in a spam e-mail and be taken to a spoof phishing Web site, be offered malicious files via a compromised Instant

Messaging (IM) client, download files over a peer-to-peer network that can come with bundled malware, or even receive files in good faith over the company intranet from a colleague whose computer has been previously compromised.

These are only a few of the most common methods used for attacks. When company laptops are frequently used as home computers by users and their families (without the protection of company firewalls or dedicated IT management teams), the attack surface is greatly expanded—a company laptop that has been compromised when a child uses an IM client at home can be brought back into the corporate environment and can threaten the integrity of the entire organization.

So, what is Microsoft specifically doing to help protect users in this ever-changing world? Well, the Microsoft Malware Protection Center (MMPC) will continue to work with our colleagues in the Windows, Microsoft Forefront, and Windows Live OneCare product groups to provide the best anti-malware technology that we can. The MMPC has a global network of research and response laboratories and researchers, which enables us to respond quickly and effectively to new threats as they arise and to make sure our customers have the latest and best updates for their Microsoft anti-malware products. Together with our industry partners, we are working hard to make the online experience as safe and secure as we can.

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

Supporting Data and Details

Global Threats

Geographic Trends" in *Trends and Analysis*, on page 46, explains how threat patterns differ significantly in different parts of the world. Figure 39 offers a closer look at this phenomenon, listing the relative prevalence of different categories of malware and potentially unwanted software in the 25 locations around the world with the most detections in 1H08.

FIGURE 39. Threat categories in the 25 locations with the most detections in 1H08

Location	Trojan Downloaders and Droppers	Other Trojans	Adware	Other Potentially Unwanted Software	Worms	Backdoors	PWS and Monitoring Tools	Viruses	Spyware	Exploits
United States	45.7%	30.7%	21.1%	23.6%	5.5%	8.4%	2.5%	1.7%	1.5%	1.6%
China	6.5%	22.2%	8.3%	43.8%	10.0%	9.9%	23.4%	3.1%	3.8%	0.3%
Spain	27.4%	21.3%	10.7%	18.3%	25.3%	13.1%	10.4%	3.3%	0.3%	0.4%
France	28.3%	25.8%	24.0%	26.5%	15.6%	10.4%	2.9%	1.8%	0.9%	0.6%
United Kingdom	34.0%	23.3%	36.3%	33.5%	3.2%	6.0%	2.6%	0.9%	1.5%	1.2%
Brazil	6.5%	8.2%	9.7%	11.6%	13.1%	3.7%	62.1%	2.3%	0.5%	0.1%
Korea	9.0%	5.7%	10.0%	9.5%	26.4%	14.9%	3.6%	30.3%	9.3%	0.1%
Germany	39.5%	23.2%	25.7%	24.0%	3.7%	8.8%	1.7%	2.0%	0.7%	0.8%
Turkey	13.7%	15.1%	21.1%	15.7%	32.2%	13.8%	4.5%	9.4%	0.7%	0.2%
Italy	24.7%	21.9%	20.8%	37.2%	11.3%	16.8%	3.2%	1.1%	0.7%	1.7%
Canada	37.8%	25.7%	35.5%	36.1%	2.9%	6.2%	1.9%	1.1%	2.1%	3.4%
Netherlands	39.5%	24.5%	26.0%	29.1%	4.0%	10.4%	2.9%	1.1%	1.6%	1.3%
Mexico	21.4%	20.1%	24.0%	25.5%	30.0%	10.6%	9.4%	2.0%	0.6%	0.6%
Taiwan	8.7%	10.7%	4.2%	21.5%	48.9%	9.0%	22.1%	2.1%	0.8%	0.5%
Japan	23.6%	18.2%	13.1%	15.7%	19.2%	13.9%	7.4%	4.2%	10.6%	2.1%
Russia	11.0%	18.2%	14.6%	21.0%	29.3%	7.4%	10.0%	9.3%	0.4%	0.2%
Portugal	18.7%	12.8%	24.3%	17.7%	13.6%	6.2%	33.9%	1.2%	0.8%	0.2%
Poland	18.9%	17.4%	19.4%	32.7%	15.3%	7.3%	3.4%	8.1%	0.6%	0.1%
Australia	34.4%	24.3%	30.5%	39.2%	4.1%	6.8%	2.3%	1.0%	2.8%	2.0%
Sweden	39.5%	24.2%	25.8%	22.7%	2.6%	10.7%	2.3%	1.4%	0.9%	1.0%
Belgium	33.2%	22.8%	35.0%	35.6%	3.9%	6.9%	2.4%	0.8%	1.5%	1.1%
Denmark	38.4%	21.8%	29.8%	26.5%	2.2%	7.9%	1.7%	0.8%	1.1%	0.7%
Norway	41.5%	21.9%	28.8%	26.3%	1.8%	8.2%	1.5%	0.6%	0.9%	0.5%
Saudi Arabia	22.2%	17.5%	7.1%	12.7%	43.4%	7.5%	7.5%	4.7%	0.5%	0.2%
Czech Republic	39.0%	22.3%	25.5%	18.4%	3.0%	8.4%	2.2%	0.6%	1.1%	0.2%
Worldwide	**31.7%**	**23.9%**	**20.0%**	**25.0%**	**11.3%**	**9.2%**	**8.5%**	**3.3%**	**1.8%**	**1.0%**

Figure 40 shows the infection rates in 114 different locations around the world, derived from averaging each location's monthly CCM for each of the six months in 1H08. (CCM is the number of computers cleaned for every 1,000 executions of the MSRT. See "Malware and Potentially Unwanted Software Trends" in *Trends and Analysis*, on page 45, for more information about the CCM metric.)

FIGURE 40. Infection rates for locations around the world, by CCM, in 1H08

Location	2H07	1H08	Change	Location	2H07	1H08	Change	Location	2H07	1H08	Change
Afghanistan	58.8	76.4	29.9%	Faroe Islands	10.5	13.8	31.9%	Luxembourg	7.7	8.7	13.5%
Albania	30.7	25.4	-17.4%	Finland	3.8	5.7	50.9%	Macau SAR	9.5	9.8	3.7%
Algeria	22.2	19.5	-12.2%	France	9.6	10.5	9.4%	F.Y.R.O. Macedonia	16.3	21.1	29.8%
Argentina	6.6	7.7	16.6%	Germany	4.4	5.3	19.7%	Malaysia	4.6	6.3	35.6%
Australia	4.9	6.9	41.7%	Greece	8.8	12.0	36.6%	Mexico	14.8	17.3	17.0%
Austria	4.1	5.2	25.7%	Greenland	5.8	10.2	77.1%	Monaco	13.7	17.0	23.7%
Azerbaijan	13.1	14.2	8.5%	Guatemala	14.3	16.1	12.0%	Mongolia	29.9	24.7	-17.6%
Bahrain	28.2	29.2	3.4%	Honduras	16.0	15.7	-2.2%	Morocco	31.3	27.8	-11.4%
Belarus	7.1	7.6	7.0%	Hong Kong SAR	6.1	7.0	15.1%	Netherlands	5.9	7.8	32.3%
Belgium	6.9	8.9	29.9%	Hungary	9.0	10.1	12.5%	New Zealand	3.8	6.0	58.4%
Belize	10.0	11.8	17.5%	Iceland	8.1	11.0	35.9%	Nicaragua	10.4	13.5	29.4%
Bolivia	12.7	15.5	22.0%	India	5.5	6.2	12.3%	Nigeria	4.9	8.2	68.5%
Bosnia and Herzegovina	12.8	16.3	27.5%	Indonesia	6.9	6.4	-7.0%	Norway	6.3	8.3	32.0%
Brazil	13.2	23.9	81.8%	Iran	15.8	13.5	-14.2%	Oman	13.3	15.3	14.8%
Brunei	6.4	8.5	32.4%	Iraq	23.8	23.6	-1.1%	Pakistan	16.7	15.9	-5.3%
Bulgaria	9.8	12.1	24.0%	Ireland	5.3	7.3	36.4%	Panama	15.2	15.1	-0.8%
Canada	5.8	8.1	39.5%	Israel	9.2	10.5	14.2%	Paraguay	13.7	15.7	14.7%
Caribbean	7.8	11.0	41.2%	Italy	5.3	7.1	34.5%	Peru	8.6	10.2	17.6%
Chile	14.9	14.0	-5.9%	Jamaica	15.0	16.3	8.9%	Philippines	7.3	7.4	2.0%
China	4.7	6.6	41.1%	Japan	1.5	1.8	22.8%	Poland	7.9	8.3	4.7%
Colombia	9.3	9.9	6.0%	Jordan	20.4	21.6	5.5%	Portugal	14.9	19.6	31.7%
Costa Rica	9.1	12.2	33.7%	Kazakhstan	8.9	12.8	43.7%	Puerto Rico	10.9	13.5	24.2%
Croatia	11.3	15.3	35.1%	Kenya	10.5	12.1	15.0%	Qatar	14.9	16.1	8.0%
Czech Republic	5.0	7.1	41.6%	Korea	15.0	13.0	-13.2%	Romania	19.8	16.1	-18.3%
Denmark	4.9	6.8	38.7%	Kuwait	13.5	15.9	17.3%	Russia	11.3	13.3	16.9%
Dominican Republic	24.5	23.2	-5.2%	Latvia	5.1	6.3	22.9%	Rwanda	4.2	4.2	0.3%
Ecuador	12.4	12.3	-0.9%	Lebanon	20.6	20.2	-1.8%	Saudi Arabia	22.2	22.3	0.4%
Egypt	24.3	22.5	-7.5%	Libya	17.3	19.5	13.1%	Senegal	2.7	9.6	255.3%
El Salvador	12.0	13.7	14.4%	Liechtenstein	9.1	10.0	9.4%	Serbia	11.8	16.6	41.4%
Estonia	7.1	8.4	18.7%	Lithuania	7.9	9.4	18.0%	Singapore	5.0	7.6	52.2%

Figure 40 continued on next page...

FIGURE 40. Infection rates for locations around the world, by CCM, in 1H08 (continued)

Location	2H07	1H08	Change	Location	2H07	1H08	Change	Location	2H07	1H08	Change
Slovakia	7.6	10.2	34.3%	Tajikistan	11.0	9.0	-17.9%	United Kingdom	7.0	9.2	32.6%
Slovenia	11.0	11.5	4.2%	Thailand	14.7	12.6	-14.3%	United States	8.9	11.2	25.5%
South Africa	7.6	8.6	12.9%	Trinidad and Tobago	8.7	13.7	56.5%	Uruguay	5.6	6.6	17.6%
Spain	12.9	15.8	23.2%	Tunisia	15.9	21.9	37.3%	Uzbekistan	14.2	12.5	-11.6%
Sweden	6.1	7.6	25.3%	Turkey	25.9	21.9	-15.4%	Venezuela	13.5	14.9	9.7%
Switzerland	5.5	6.9	26.4%	Turkmenistan	—	8.1	N/A	Vietnam	16.8	8.8	-47.4%
Syria	15.2	14.3	-5.7%	Ukraine	9.8	10.8	10.7%	Yemen	17.7	20.1	13.7%
Taiwan	3.3	8.1	146.6%	United Arab Emirates	18.2	17.3	-4.8%	Zimbabwe	12.7	15.2	19.8%
								Worldwide	**8.1**	**10.0**	**23.5%**

(Infection rates are rounded to one decimal place.
Percentage changes have been calculated before rounding.)

In absolute terms, many of these locations demonstrated sharp increases in the number of computers that reported malware or potentially unwanted software in 1H08, with some locations experiencing increases greater than 100 percent. In most of these cases, the number of computers in use is actually quite small, in absolute terms. The sharp increases suggest that new computers are more likely to be infected when they are connected to the Internet in those locations than in locations with larger installed bases and larger numbers of experienced Internet users.

Figure 26 in *Trends and Analysis*, on page 50, illustrates the observed inverse correlation between infection rate and computer usage in different locations around the world. Figure 41 offers more detail, listing the Internet-using percentage of the population for each of the 25 highest-infection and lowest-infection locations around the world.[16]

[16] Internet usage figures are from the CIA World Factbook (https://www.cia.gov/library/publications/the-world-factbook/docs/rankorderguide.html).

FIGURE 41. Internet usage rates of the 25 highest-infection and lowest-infection locations in 1H08

Location	Internet Usage	Infection Rate (CCM)
Bahrain	21.9%	29.2
Morocco	17.8%	27.8
Brazil	22.2%	23.9
Iraq	0.1%	23.6
Dominican Republic	13.0%	23.2
Egypt	7.3%	22.5
Saudi Arabia	16.7%	22.3
Turkey	17.1%	21.9
Tunisia	12.5%	21.9
Jordan	12.9%	21.6
F.Y.R.O. Macedonia	13.0%	21.1
Lebanon	23.9%	20.2
Yemen	1.2%	20.1
Portugal	30.1%	19.6
Algeria	7.3%	19.5
United Arab Emirates	37.0%	17.3
Mexico	20.0%	17.3
Serbia	13.8%	16.6
Bosnia and Herzegovina	20.7%	16.3
Romania	22.8%	16.1
Qatar	31.2%	16.1
Guatemala	10.2%	16.1
Pakistan	7.2%	15.9
Kuwait	31.5%	15.9
Spain	45.9%	15.8

Location	Internet Usage	Infection Rate (CCM)
Norway	87.7%	8.3
Canada	66.2%	8.1
Taiwan	57.6%	8.1
Netherlands	87.4%	7.8
Argentina	20.1%	7.7
Sweden	77.2%	7.6
Singapore	37.3%	7.6
Philippines	5.0%	7.4
Ireland	34.6%	7.3
Italy	49.6%	7.1
Czech Republic	34.6%	7.1
Hong Kong SAR	53.7%	7.0
Australia	74.3%	6.9
Switzerland	57.5%	6.9
Denmark	57.8%	6.8
China	12.2%	6.6
Indonesia	6.7%	6.4
Latvia	47.7%	6.3
Malaysia	44.7%	6.3
India	5.2%	6.2
New Zealand	76.7%	6.0
Finland	55.8%	5.7
Germany	46.9%	5.3
Austria	51.2%	5.2
Japan	68.8%	1.8

While the overall trend of greater computer and Internet use around the world is positive, it is important that newly developing Internet-using populations have ready access to information that can help computer users protect their families and assets from Internet-based threats. Microsoft works with governments and other organizations around the world to provide such educational opportunities through programs like Microsoft Unlimited Potential[17] and other initiatives. Individuals can also learn to protect themselves by reading and following the tips and guidance at http://www.microsoft.com/protect.

[17] For more information about Microsoft Unlimited Potential, see http://www.microsoft.com/unlimitedpotential.

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" in *Trends and Analysis*, on page 46, gives an overview of the way the relative prevalence of different categories of malware varies between different locations.

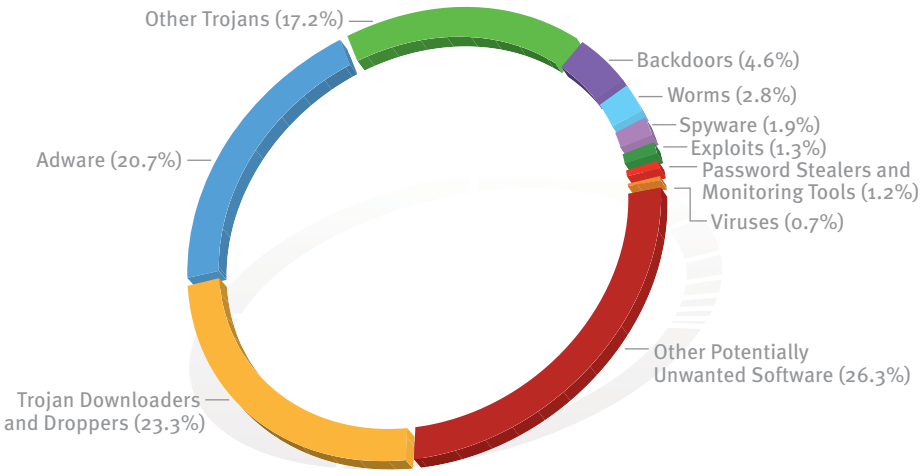
The next several pages provide infection statistics for 15 locations around the world, covering every inhabited continent and many different languages. These locations were chosen as a representative sample of the different threat patterns observed among different populations worldwide.

Australia

The infection rate (CCM) for Australia in 1H08 was 6.9, an increase of 41.7 percent since 2H07. Overall, Microsoft security products detected malware and potentially unwanted software on 55 percent more computers in 1H08 than in 2H07.

Figure 42 and Figure 43 list the most common malware and potentially unwanted software categories and families detected by Microsoft security products in Australia in 1H08.

FIGURE 42. Malware and potentially unwanted software in Australia, by category, in 1H08



Category	Infected computers
Other Potentially Unwanted Software	127,463
Trojan Downloaders and Droppers	112,851
Adware	100,039
Other Trojans	83,467
Backdoors	22,283
Worms	13,400
Spyware	9,226
Exploits	6,449
Password Stealers and Monitoring Tools	5,776
Viruses	3,435

Observations:

- The most common category in Australia is "Other Potentially Unwanted Software," which includes potentially unwanted software families that are not classified as adware or spyware, such as rogue security software. It accounts for 26.3 percent of all infected computers, with the total number of infected computers increasing 40.5 percent since 2H07. "Other Potentially Unwanted Software" accounts for 9 of the top 25 categories.
- The second most common category in Australia is "Trojan Downloaders and Droppers," which accounts for 23.3 percent of all infected computers, with the total number of infected computers increasing 31 percent from 2H07.

FIGURE 43. Top 25 families in Australia in 1H08

Rank	Family	Category	Infected computers
1	Win32/Zlob	Trojan Downloaders and Droppers	83,471
2	Win32/Vundo	Other Trojans	36,332
3	Win32/ZangoSearchAssistant	Adware	30,239
4	Win32/Agent	Other Trojans	27,465
5	Win32/SeekmoSearchAssistant	Adware	17,562
6	Win32/Hotbar	Adware	17,304
7	Win32/Renos	Trojan Downloaders and Droppers	15,991
8	Win32/ZangoShoppingreports	Adware	15,669
9	Win32/Starware	Other Potentially Unwanted Software	14,944
10	Win32/BrowsingEnhancer	Adware	12,483
11	Win32/Winfixer	Other Potentially Unwanted Software	10,967
12	Win32/E404	Other Potentially Unwanted Software	10,356
13	Win32/PossibleHostsFileHijack	Other Potentially Unwanted Software	10,008
14	ASX/Wimad	Trojan Downloaders and Droppers	9,806
15	Win32/Rbot	Backdoors	9,140
16	Win32/Advantage	Adware	8,788
17	Win32/Mirar	Adware	8,714
18	Win32/RealVNC	Other Potentially Unwanted Software	8,436
19	Win32/Vapsup	Other Potentially Unwanted Software	7,902
20	Win32/Fotomoto	Other Potentially Unwanted Software	7,244
21	Win32/PowerRegScheduler	Other Potentially Unwanted Software	7,243
22	Win32/WhenU	Adware	6,691
23	Win32/ConHook	Other Trojans	6,239
24	Win32/Virtumonde	Other Trojans	5,820
25	Win32/SpySheriff	Other Potentially Unwanted Software	5,793

Observations:

- The top 25 families account for 63.4 percent of all infected computers.
- Seventeen of the top 25 families are potentially unwanted software families.
- Of the top 10 families, 4 (Win32/Zlob, Win32/Vundo, Win32/Agent, and Win32/Renos) are malware.
  - Win32/Zlob, the most common threat in the world and in Australia, was detected on 54.1 percent more computers in 1H08 than in 2H07. See "Win32/Zlob" in *Trends and Analysis*, on page 59, for more information about this family of trojan downloaders.
  - Win32/Vundo, also known as Win32/Virtumonde, was added to the MSRT in March 2008 and has been heavily detected by several Microsoft security products. It is the second most common threat in the world and in Australia. See "Win32/Vundo and Win32/Virtumonde" in *Trends and Analysis*, on page 60, for more information about this family of trojans.
  - Win32/Agent is a generic detection for a number of threats that may perform different malicious functions.
  - Win32/Renos, the fourth most common family worldwide, ranks seventh in Australia. It was detected on 21.2 percent fewer computers in Australia in 1H08 than in 2H07.
- Win32/Winfixer, the seventeenth most common family worldwide, ranks eleventh in Australia. It was detected on 37.1 percent fewer computers in Australia in 1H08 than in 2H07. Win32/Winfixer is considered rogue security software, a type of potentially unwanted software. It locates various registry entries, prefetched content, recently accessed files, and other types of data, and identifies them as "privacy violations." Win32/Winfixer then prompts the user to purchase the product to remove the alleged "violations."
- Win32/E404, the twelfth most common family in Australia, is not among the 25 most common families worldwide. Win32/E404 is a browser helper object (BHO) that takes advantage of invalid or mistyped URLs entered in the address bar by redirecting the browser to Web sites containing adware.

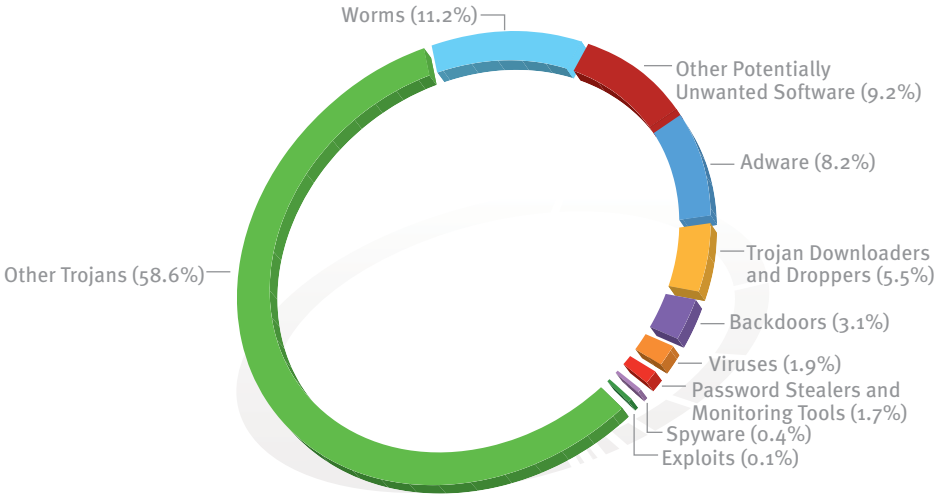
Brazil

The infection rate (CCM) for Brazil in 1H08 was 23.9, an increase of 81.8 percent since 2H07. Overall, Microsoft security products detected malware and potentially unwanted software on 92 percent more computers in 1H08 than in 2H07.

Figure 44 and Figure 45 list the most common malware and potentially unwanted software categories and families detected by Microsoft security products in Brazil in 1H08.

FIGURE 44. Malware and potentially unwanted software in Brazil, by category, in 1H08

Category	Infected computers
Other Trojans	1,294,084
Worms	246,470
Other Potentially Unwanted Software	203,158
Adware	181,405
Trojan Downloaders and Droppers	122,010
Backdoors	69,289
Viruses	43,079
Password Stealers and Monitoring Tools	37,775
Spyware	9,705
Exploits	2,381



Observations:

- The threat landscape in Brazil is clearly dominated by malware. The top four families in Brazil are all malware families.
- The most common category in Brazil is "Other Trojans," which includes trojan families that are not classified as downloaders/droppers or backdoors. It accounts for 58.6 percent of all infected computers, with the total number of infected computers increasing 153.9 percent from 2H07, largely owing to the prevalence of Win32/Bancos and Win32/Banker.
- The second most common category in Brazil is "Worms," which accounts for 11.2 percent of all infected computers, with the total number of infected computers increasing 127.1 percent from 2H07.

FIGURE 45. Top 25 families in Brazil in 1H08

Rank	Family	Category	Infected computers
1	Win32/Bancos	Other Trojans	894,666
2	Win32/Banker	Other Trojans	359,933
3	Win32/RJump	Worms	130,488
4	Win32/Zlob	Trojan Downloaders and Droppers	71,781
5	Win32/Advantage	Adware	54,569
6	Win32/Taterf	Worms	51,618
7	Win32/Vundo	Other Trojans	45,281
8	Win32/PossibleHostsFileHijack	Other Potentially Unwanted Software	44,613
9	Win32/RealVNC	Other Potentially Unwanted Software	34,731
10	Win32/Agent	Other Trojans	31,953
11	Win32/ZangoSearchAssistant	Adware	30,071
12	Win32/ZangoShoppingreports	Adware	29,606
13	Win32/C2Lop	Other Trojans	24,408
14	Win32/WhenU	Adware	24,258
15	Win32/Parite	Viruses	24,139
16	Win32/Rbot	Backdoors	22,891
17	Win32/Renos	Trojan Downloaders and Droppers	21,370
18	Win32/SeekmoSearchAssistant	Adware	20,110
19	Win32/UltraVNC	Other Potentially Unwanted Software	19,001
20	Win32/Alureon	Other Trojans	17,154
21	Win32/BrowsingEnhancer	Other Potentially Unwanted Software	16,346
22	Win32/Cutwail	Trojan Downloaders and Droppers	15,982
23	Win32/Mirar	Adware	15,499
24	Win32/Hotbar	Adware	14,480
25	Win32/Ardamax	Other Potentially Unwanted Software	13,826

Observations:

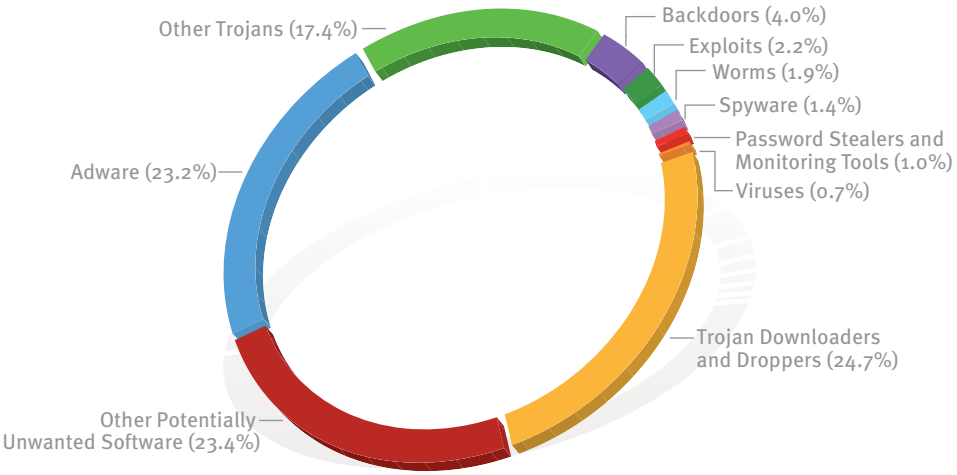
- The top 25 families account for 83.4 percent of all infected computers.
- Thirteen of the top 25 families are potentially unwanted software families.
- Of the top 10 families, 7 are malware.
- The most common threat in Brazil in 1H08 was Win32/Bancos, which was detected on 1,575.8 percent more computers in 1H08 than in 2H07. Win32/Bancos is a family of data-stealing trojans that captures users' online banking credentials, such as account login names and passwords. The Win32/Bancos trojans are written in Visual Basic®, and the majority of the variants target customers of Brazilian banks. See "Win32/Bancos" in *Trends and Analysis*, on page 60, for more information about this family.
- Win32/Banker, the second most common threat in Brazil in 1H08, was detected on 7.1 percent fewer computers in 1H08 than in 2H07. Like Win32/Bancos, Win32/Banker is a trojan that primarily targets Brazilian banks, capturing banking credentials from the victim and transmitting them to the attacker through various means. Many variants of Win32/Banker may appear as greeting card software.
- Win32/RJump, the ninth most common family worldwide, ranks third in Brazil. It was detected on 80.4 percent more computers in Brazil in 1H08 than in 2H07. Win32/RJump is a worm that attempts to spread by copying itself to newly attached media (such as USB memory devices or network drives). It also contains backdoor functionality that allows an attacker unauthorized access to an affected computer.
- Win32/Advantage, the thirteenth most common family worldwide, ranks fifth in Brazil. It was detected on 693 percent more computers in Brazil in 1H08 than in 2H07. Win32/Advantage is a family of adware that displays pop-up advertisements and contacts a remote server to download updates.
- Win32/Taterf, the seventh most common family worldwide, ranks sixth in Brazil. Win32/Taterf is a family of worms that spread via mapped drives to steal login and account details for popular online games. See "Online Gaming-Related Families" in *Trends and Analysis*, on page 62, for more information about this family of worms.
- Win32/PossibleHostsFileHijack, the eighth most common detection in Brazil, is not among the 25 most common detections worldwide. It was detected on 506 percent more computers in Brazil in 1H08 than in 2H07. A detection of Win32/PossibleHosts-FileHijack is an indicator that the computer's HOSTS file may have been modified by malicious or potentially unwanted software. Modifications to the HOSTS file can cause access to certain Internet domains to be redirected or denied. This may prevent the computer from connecting to certain Web sites.

Canada

The infection rate (CCM) for Canada in 1H08 was 8.1, an increase of 39.5 percent since 2H07. Overall, Microsoft security products detected malware and potentially unwanted software on 72 percent more computers in 1H08 than in 2H07.

Figure 46 and Figure 47 list the most common malware and potentially unwanted software categories and families detected by Microsoft security products in Canada in 1H08.

FIGURE 46. Malware and potentially unwanted software in Canada, by category, in 1H08



Category	Infected computers
Trojan Downloaders and Droppers	246,578
Other Potentially Unwanted Software	233,378
Adware	231,394
Other Trojans	173,117
Backdoors	40,244
Exploits	22,301
Worms	18,716
Spyware	13,810
Password Stealers and Monitoring Tools	9,840
Viruses	7,310

Observations:

- The most common category in Canada is "Trojan Downloaders and Droppers," which accounts for 24.7 percent of all infected computers, with the total number of infected computers increasing 107.1 percent from 2H07. Win32/Zlob, ASX/Wimad, and Win32/Renos are the main contributors to this category.
- The second most common category in Canada is "Other Potentially Unwanted Software," which includes potentially unwanted software families that are not classified as adware or spyware, such as rogue security software. It accounts for 23.4 percent of all infected computers and 9 of the top 25 families.

FIGURE 47. Top 25 families in Canada in 1H08

Rank	Family	Category	Infected computers
1	Win32/Zlob	Trojan Downloaders and Droppers	155,644
2	Win32/ZangoSearchAssistant	Adware	106,718
3	Win32/Agent	Other Trojans	67,098
4	Win32/Vundo	Other Trojans	60,153
5	Win32/ZangoShoppingreports	Adware	53,710
6	Win32/Hotbar	Adware	52,324
7	ASX/Wimad	Trojan Downloaders and Droppers	49,264
8	Win32/SeekmoSearchAssistant	Adware	37,578
9	Win32/Renos	Trojan Downloaders and Droppers	32,555
10	Win32/Starware	Other Potentially Unwanted Software	27,940
11	Win32/Winfixer	Other Potentially Unwanted Software	21,316
12	Win32/PowerRegScheduler	Other Potentially Unwanted Software	18,353
13	Win32/BrowsingEnhancer	Adware	17,381
14	Win32/Advantage	Adware	16,806
15	Win32/E404	Other Potentially Unwanted Software	16,274
16	Win32/Mirar	Adware	15,227
17	Win32/Tibs	Other Trojans	15,059
18	Win32/Rbot	Backdoors	14,900
19	Win32/PossibleHostsFileHijack	Other Potentially Unwanted Software	13,930
20	Win32/ConHook	Other Trojans	12,819
21	Win32/Vapsup	Other Potentially Unwanted Software	12,552
22	Win32/SpySheriff	Other Potentially Unwanted Software	12,324
23	Win32/Fotomoto	Other Potentially Unwanted Software	11,584
24	Win32/C2Lop	Other Trojans	11,118
25	Win32/BearShare	Other Potentially Unwanted Software	10,762

Observations:

- The top 25 families account for 64.9 percent of all infected computers.
- Sixteen of the top 25 families are potentially unwanted software families.
- Of the top 10 families, 5 are malware.
- ASX/Wimad, the seventh most common family in Canada, is not among the 25 most common families worldwide. Variants, such as TrojanDownloader:ASX/Wimad, are detections for malicious Windows media files that are used to encourage users to download and execute arbitrary files on an affected computer. When opened with Windows Media Player, these malicious files open a particular URL in a Web browser.
- Win32/Renos, the fourth most common family worldwide, ranks ninth in Canada. It was detected on 22.9 percent fewer computers in Canada in 1H08 than in 2H07.
- Win32/Winfixer, the seventeenth most common family worldwide, ranks eleventh in Canada. It was detected on 9.9 percent fewer computers in Canada in 1H08 than in 2H07. Win32/Winfixer is considered rogue security software, a type of potentially unwanted software. It locates various registry entries, prefetched content, recently accessed files, and other types of data, and identifies them as "privacy violations." Win32/Winfixer then prompts the user to purchase the product to remove the alleged "violations."

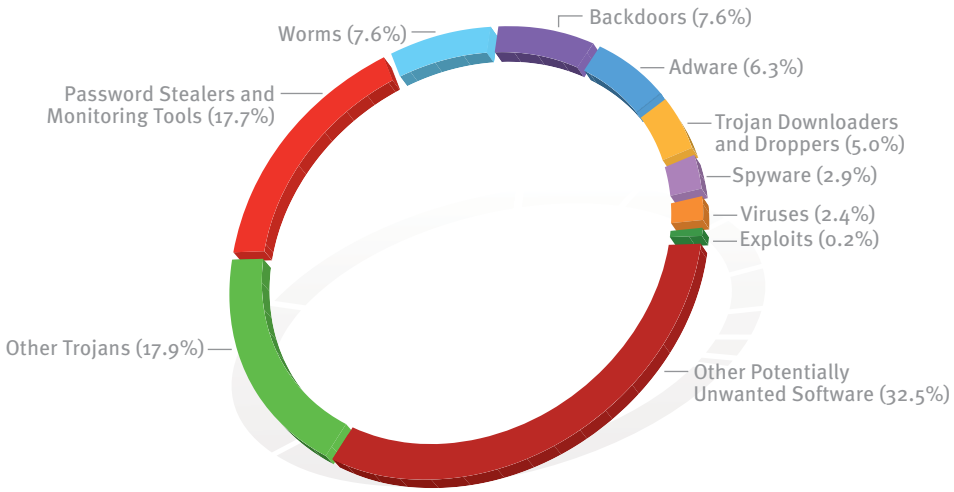
China

The infection rate (CCM) for China in 1H08 was 6.6, an increase of 41.1 percent since 2H07. Overall, Microsoft security products detected malware and potentially unwanted software on 36 percent more computers in 1H08 than in 2H07.

Figure 48 and Figure 49 list the most common malware and potentially unwanted software categories and families detected by Microsoft security products in China in 1H08.

FIGURE 48. Malware and potentially unwanted software in China, by category, in 1H08

Category	Infected computers
Other Potentially Unwanted Software	1,273,421
Other Trojans	701,687
Password Stealers and Monitoring Tools	693,520
Worms	298,681
Backdoors	295,954
Adware	246,471
Trojan Downloaders and Droppers	195,385
Spyware	113,866
Viruses	93,305
Exploits	7,509



Observations:

- The most common category in China is "Other Potentially Unwanted Software," which includes potentially unwanted software families that are not classified as adware or spyware, such as rogue security software. It accounts for 32.5 percent of all infected computers, with the total number of infected computers increasing 35.7 percent from 2H07.
- The second most common category in China is "Other Trojans," which includes trojan families that are not classified as downloaders/droppers or backdoors. It accounts for 17.9 percent of all infected computers, with the total number of infected computers increasing 229.5 percent from 2H07.
- The third most common category in China is "Password Stealers and Monitoring Tools," with Win32/Frethog and Win32/Ceekat being the biggest contributors to this category.

FIGURE 49. Top 25 families in China in 1H08

Rank	Family	Category	Infected computers
1	Win32/BaiduSobar	Other Potentially Unwanted Software	625,013
2	Win32/Frethog	Password Stealers and Monitoring Tools	456,212
3	Win32/Hupigon	Backdoors	386,184
4	Win32/Tilcun	Other Trojans	384,490
5	Win32/CNNIC	Other Potentially Unwanted Software	359,448
6	Win32/Ceekat	Password Stealers and Monitoring Tools	268,746
7	Win32/RJump	Worms	200,524
8	Win32/Sogou	Other Potentially Unwanted Software	169,403
9	Win32/MotePro	Other Trojans	159,943
10	Win32/CnsMin	Spyware	105,209
11	Win32/Baidulebar	Other Potentially Unwanted Software	100,099
12	Win32/Agent	Other Trojans	73,777
13	Win32/Ejik	Other Potentially Unwanted Software	54,302
14	Win32/Zlob	Trojan Downloaders and Droppers	49,858
15	Win32/Parite	Viruses	49,256
16	Win32/Brontok	Worms	44,834
17	Win32/AlibabaIEToolBar	Adware	44,394
18	Win32/Cutwail	Trojan Downloaders and Droppers	43,749
19	Win32/Advantage	Adware	42,792
20	Win32/BDPlugin	Other Trojans	38,329
21	Win32/Zuten	Password Stealers and Monitoring Tools	33,117
22	Win32/Wukill	Worms	30,161
23	Win32/Lolyda	Password Stealers and Monitoring Tools	29,414
24	Win32/WhenU	Adware	27,036
25	Win32/Delf	All Others	26,458

Observations:

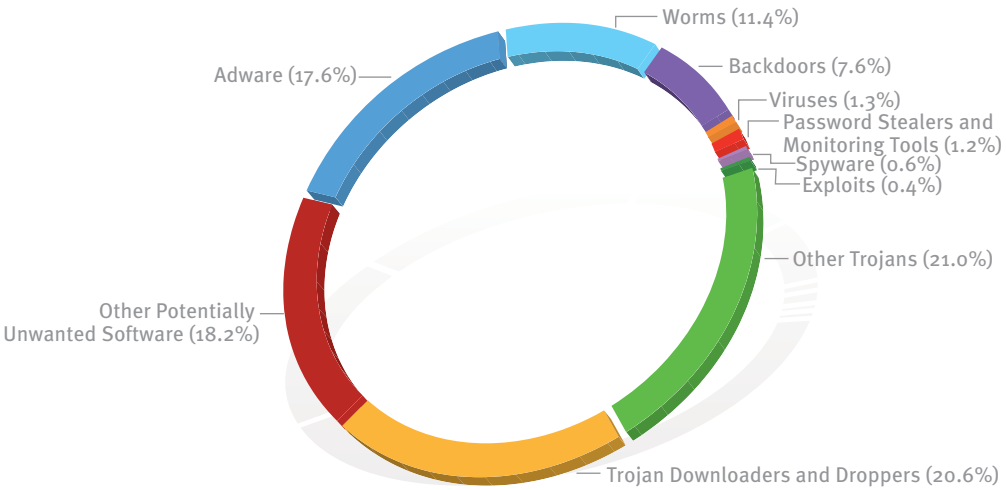
- The top 25 families account for 87.2 percent of all infected computers.
- Nine of the top 25 families are potentially unwanted software families.
- Of the top 10 families, 6 are malware.
- The threat landscape in China is very different from the worldwide threat landscape, with Chinese-language families dominating the list of top threats. Only 1 of the top 10 threats in China, Win32/RJump, is in the top 10 list of worldwide threats.
- Online gaming password stealers, like Win32/Frethog and Win32/Tilcun, appear high on the list of top threats in China, although one password stealer that is very prevalent worldwide, Win32/Taterf, is not among the top 25 threats in China. (See "Online Gaming-Related Families" in *Trends and Analysis*, on page 62, for more information about these families.)
- Three notable families in the top 10 are largely confined to Chinese-language locales and do not appear in the list of the top 25 threats worldwide:
  - Win32/CNNIC is the fifth most common family in China in 1H08. It was detected on 17.1 percent more computers in China in 1H08 than in 2H07.
  - Win32/Sogou is the eighth most common family in China in 1H08. It was detected on 75.8 percent more computers in China in 1H08 than in 2H07.
  - Win32/CnsMin is the tenth most common family in China in 1H08. It was detected on 60.3 percent fewer computers in China in 1H08 than in 2H07.
- Win32/Hupigon, the twenty-fifth most common family worldwide, ranks third in China. Win32/Hupigon is a family of backdoor trojans. A Win32/Hupigon infection includes TrojanDropper:Win32/Hupigon and two to three dynamic-link library (DLL) files that the dropper installs.

France

The infection rate (CCM) for France in 1H08 was 10.5, an increase of 9.4 percent since 2H07. Overall, Microsoft security products detected malware and potentially unwanted software on 27 percent more computers in 1H08 than in 2H07.

Figure 50 and Figure 51 list the most common malware and potentially unwanted software categories and families detected by Microsoft security products in France in 1H08.

FIGURE 50. Malware and potentially unwanted software in France, by category, in 1H08



Category	Infected computers
Other Trojans	584,121
Trojan Downloaders and Droppers	575,060
Other Potentially Unwanted Software	506,976
Adware	488,987
Worms	317,984
Backdoors	211,265
Viruses	36,319
Password Stealers and Monitoring Tools	34,805
Spyware	17,368
Exploits	12,219

Observations:

- The most common category in France is "Other Trojans," which includes trojan families that are not classified as downloaders/droppers or backdoors. It accounts for 21 percent of all infected computers, with the total number of infected computers increasing 114.2 percent from 2H07.
- The second most common category in France is "Trojan Downloaders and Droppers," which accounts for 20.6 percent of all infected computers, with the total number of infected computers increasing 41.3 percent from 2H07.

FIGURE 51. Top 25 families in France in 1H08

Rank	Family	Category	Infected computers
1	Win32/Zlob	Trojan Downloaders and Droppers	374,867
2	Win32/Vundo	Other Trojans	240,112
3	Win32/ZangoSearchAssistant	Adware	153,261
4	Win32/RJump	Worms	151,156
5	Win32/SpywareSecure	Other Potentially Unwanted Software	138,959
6	Win32/MessengerSkinner	Trojan Downloaders and Droppers	81,157
7	Win32/ZangoShoppingreports	Adware	78,256
8	Win32/Advantage	Adware	77,663
9	Win32/Hotbar	Adware	76,987
10	Win32/Agent	Other Trojans	76,695
11	Win32/Renos	Trojan Downloaders and Droppers	76,170
12	Win32/Rbot	Backdoors	69,141
13	Win32/Winfixer	Other Potentially Unwanted Software	67,297
14	Win32/ConHook	Other Trojans	60,819
15	Win32/Taterf	Worms	56,681
16	Win32/BrowsingEnhancer	Adware	55,937
17	Win32/SeekmoSearchAssistant	Adware	53,580
18	Win32/C2Lop	Other Trojans	50,004
19	Win32/Brontok	Worms	49,276
20	Win32/Sdbot	Backdoors	46,274
21	Win32/Virtumonde	Other Trojans	42,806
22	Win32/Mirar	Adware	41,864
23	Win32/WhenU	Adware	39,938
24	Win32/Tibs	Other Trojans	38,108
25	Win32/Cutwail	Trojan Downloaders and Droppers	37,688

Observations:

- The top 25 families account for 66.9 percent of all infected computers.
- Ten of the top 25 families are potentially unwanted software families.
- Of the top 10 families, 5 are malware.
- Win32/Zlob and Win32/Vundo, the first and second most common threats in the world, are also the first and second most common threats in France. See "Win32/Zlob," on page 59, and "Win32/Vundo and Win32/Virtumonde," on page 60, in *Trends and Analysis* for more information about these families.
- Win32/SpywareSecure, the fifth most common family in France, is not among the 25 most common families worldwide. Win32/SpywareSecure is considered rogue security software. It displays misleading warning messages to convince users to purchase a product that removes spyware.
- Win32/MessengerSkinner, the sixth most common family in France, is not among the 25 most common families worldwide. Win32/MessengerSkinner is a trojan downloader that may be distributed in the form of a freeware application. It displays advertisements, downloads additional files, and uses stealth to hide its presence.

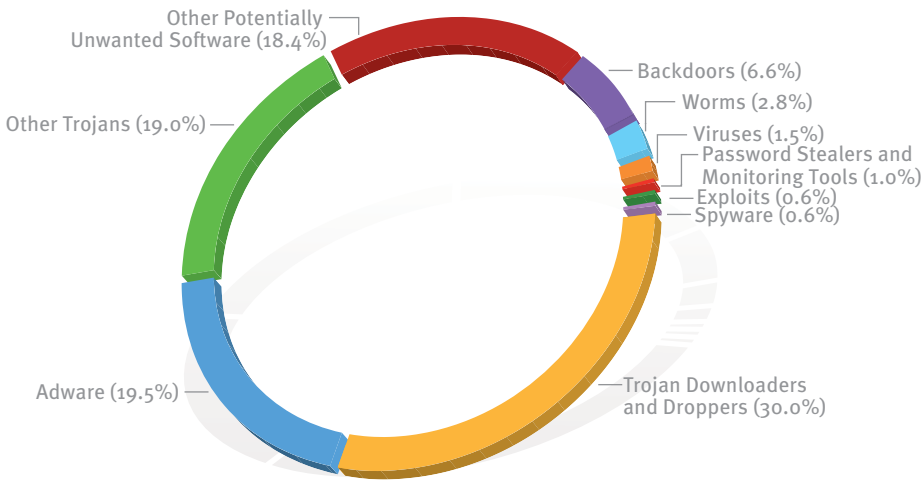
Germany

The infection rate (CCM) for Germany in 1H08 was 5.3, an increase of 19.7 percent since 2H07. Overall, Microsoft security products detected malware and potentially unwanted software on 50 percent more computers in 1H08 than in 2H07.

Figure 52 and Figure 53 list the most common malware and potentially unwanted software categories and families detected by Microsoft security products in Germany in 1H08.

FIGURE 52. Malware and potentially unwanted software in Germany, by category, in 1H08

Category	Infected computers
Trojan Downloaders and Droppers	503,970
Adware	327,240
Other Trojans	319,855
Other Potentially Unwanted Software	309,416
Backdoors	111,698
Worms	47,085
Viruses	25,558
Password Stealers and Monitoring Tools	16,264
Exploits	9,660
Spyware	9,502



Observations:

- The most common category in Germany is "Trojan Downloaders and Droppers," which accounts for 30.3 percent of all infected computers, with the total number of infected computers increasing 32.4 percent from 2H07. Win32/Zlob and Win32/Renos are the main contributors to this category.
- The second most common category in Germany is "Adware," which accounts for 19.7 percent of all infected computers, with the total number of infected computers increasing 79.6 percent from 2H07.

FIGURE 53. Top 25 families in Germany in 1H08

Rank	Family	Category	Infected computers
1	Win32/Zlob	Trojan Downloaders and Droppers	427,563
2	Win32/ZangoSearchAssistant	Adware	130,770
3	Win32/Vundo	Other Trojans	117,307
4	Win32/Renos	Trojan Downloaders and Droppers	71,618
5	Win32/Hotbar	Adware	61,661
6	Win32/Advantage	Adware	56,706
7	Win32/ZangoShoppingreports	Adware	51,585
8	Win32/Winfixer	Other Potentially Unwanted Software	50,254
9	Win32/Rbot	Backdoors	49,765
10	Win32/BearShare	Other Potentially Unwanted Software	47,458
11	Win32/SeekmoSearchAssistant	Adware	45,597
12	Win32/Agent	Other Trojans	45,442
13	Win32/WhenU	Adware	37,535
14	Win32/ConHook	Other Trojans	35,968
15	Win32/Alureon	Other Trojans	31,691
16	Win32/SpywareSecure	Other Potentially Unwanted Software	30,405
17	Win32/Tibs	Other Trojans	23,350
18	Win32/Oderoor	Backdoors	22,739
19	Win32/MessengerSkinner	Trojan Downloaders and Droppers	22,411
20	Win32/Vapsup	Other Potentially Unwanted Software	20,708
21	Win32/BrowsingEnhancer	Adware	20,292
22	Win32/RealVNC	Other Potentially Unwanted Software	19,531
23	Win32/Mirar	Adware	18,663
24	Win32/Virtumonde	Other Trojans	18,453
25	Win32/E404	Other Potentially Unwanted Software	17,428

Observations:

- The top 25 families account for 74.1 percent of all infected computers.
- Fourteen of the top 25 families are potentially unwanted software families.
- Of the top 10 families, 4 are malware.
- Win32/Zlob, Win32/Vundo, and Win32/Renos, three common families worldwide, are also prevalent in Germany.
  - Win32/Zlob, the most common threat in the world and in Germany, was detected on 58 percent more computers in 1H08 than in 2H07. See "Win32/Zlob" in *Trends and Analysis*, on page 59, for more information about this family of trojan downloaders.
  - Win32/Vundo, also known as Win32/Virtumonde, was added to the MSRT in March 2008 and has been heavily detected by several Microsoft security products. It is the second most common threat in the world, and the third most common threat in Germany. See "Win32/Vundo and Win32/Virtumonde" in *Trends and Analysis*, on page 60, for more information about this family of trojans.
  - Win32/Renos, the fourth most common family worldwide and in Germany, was detected on 17.8 percent fewer computers in Germany in 1H08 than in 2H07.
- Win32/Winfixer, the seventeenth most common family worldwide, ranks eighth in Germany. It was detected on 43.6 percent more computers in Germany in 1H08 than in 2H07. Win32/Winfixer is considered rogue security software, a type of potentially unwanted software. It locates various registry entries, prefetched content, recently accessed files, and other types of data, and identifies them as "privacy violations." Win32/Winfixer then prompts the user to purchase the product to remove the alleged "violations."
- Win32/Rbot, the twelfth most common family worldwide, ranks ninth in Germany. It was detected on 17.7 percent more computers in Germany in 1H08 than in 2H07.

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

Overall, Microsoft security products detected malware and potentially unwanted software on 42.6 percent more computers in the states of the Gulf Cooperation Council (GCC) in 1H08 than in 2H07. Figure 54 lists the infection rates (CCM) for each of the GCC member states.

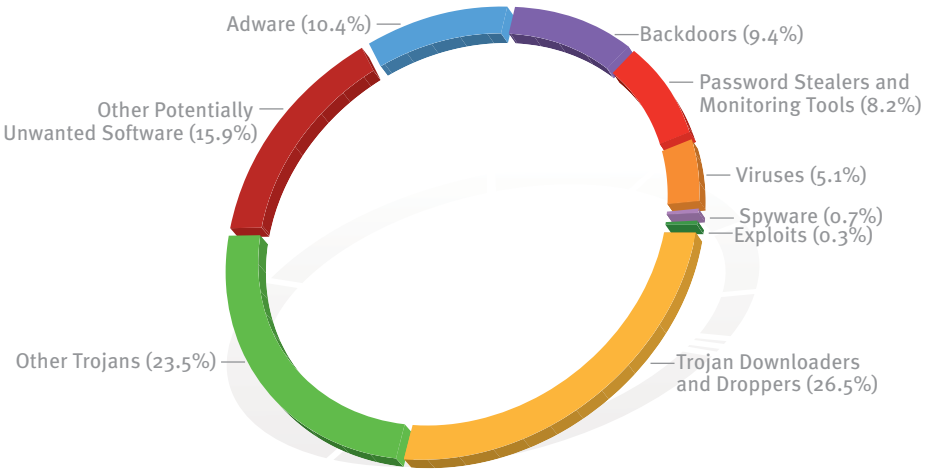
FIGURE 54. Infection rates (CCM) for the states of the Gulf Cooperation Council in 1H08

State	2H07	1H08	% Chg.
Bahrain	28.2	29.2	3.4
Kuwait	13.5	15.9	17.3
Oman	13.3	15.3	14.8
Qatar	14.9	16.1	8.0
United Arab Emirates	18.2	17.3	-4.8
Saudi Arabia	22.2	22.3	0.4

(Infection rates are rounded to one decimal place. Percentage changes have been calculated before rounding.)

Figure 55 and Figure 56 list the most common malware and potentially unwanted software categories and families detected by Microsoft security products in the states of the GCC in 1H08.

FIGURE 55. Malware and potentially unwanted software in Gulf Cooperation Council states, by category, in 1H08



Category	Infected computers
Trojan Downloaders and Droppers	58,738
Other Trojans	52,093
Other Potentially Unwanted Software	35,307
Adware	22,974
Backdoors	20,911
Password Stealers and Monitoring Tools	18,100
Viruses	11,298
Spyware	1,567
Exploits	565

Observations:

- The most common category in the GCC states is "Trojan Downloaders and Droppers," which accounts for 26.5 percent of all infected computers, with the total number of infected computers decreasing 1.5 percent from 2H07.
- The second most common category in the GCC states is "Other Trojans," which includes trojan families that are not classified as downloaders/droppers or backdoors. It accounts for 23.5 percent of all infected computers, with the total number of infected computers increasing 185.5 percent from 2H07.

FIGURE 56. Top 25 families in Gulf Cooperation Council states in 1H08

Rank	Family	Category	Infected computers
1	Win32/Zlob	Trojan Downloaders and Droppers	47,973
2	Win32/Taterf	Worms	38,497
3	Win32/RJump	Worms	35,231
4	Win32/Brontok	Worms	29,938
5	Win32/Renos	Trojan Downloaders and Droppers	15,243
6	Win32/Vundo	Other Trojans	13,203
7	Win32/Frethog	Password Stealers and Monitoring Tools	13,165
8	Win32/C2Lop	Other Trojans	9,024
9	Win32/Agent	Other Trojans	7,446
10	Win32/Oderoor	Backdoors	5,958
11	Win32/SeekmoSearchAssistant	Adware	5,782
12	Win32/ZangoSearchAssistant	Adware	5,516
13	Win32/Cutwail	Trojan Downloaders and Droppers	5,326
14	Win32/Rbot	Backdoors	4,814
15	Win32/Advantage	Adware	4,669
16	Win32/Comscore	Other Potentially Unwanted Software	4,531
17	Win32/Wukill	Worms	4,499
18	Win32/Jeefo	Viruses	4,296
19	Win32/Alureon	Other Trojans	4,117
20	Win32/ZangoShoppingreports	Adware	3,974
21	Win32/Nuwar	Backdoors	3,906
22	Win32/IRCBot	Backdoors	3,592
23	Win32/Tibs	Other Trojans	3,526
24	Win32/Starware	Other Potentially Unwanted Software	3,371
25	Win32/Parite	Viruses	3,156

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

Observations:

- The top 25 families account for 77.5 percent of all infected computers.
- Six of the top 25 families are potentially unwanted software families.
- All of the top 10 families are malware.
- Win32/Zlob, Win32/Renos, and Win32/Vundo, three common families worldwide, are also prevalent in the GCC states.
  - Win32/Zlob, the most common threat in the world and the GCC states, was detected on 5.5 percent more computers in 1H08 than in 2H07. See "Win32/Zlob" in *Trends and Analysis*, on page 59, for more information about this family of trojan downloaders.
  - Win32/Renos, the fourth most common family worldwide, ranks fifth in the GCC states. It was detected on 11 percent fewer computers in the GCC states in 1H08 than in 2H07.
  - Win32/Vundo, also known as Win32/Virtumonde, was added to the MSRT in March 2008 and has been heavily detected by several Microsoft security products. It is the second most common threat in the world and the sixth most common threat in the GCC states. See "Win32/Vundo and Win32/Virtumonde" in *Trends and Analysis*, on page 60, for more information about this family of trojans.
- Win32/Taterf, the seventh most common family worldwide, ranks second in the GCC states. Win32/Taterf is a family of worms that spread via mapped drives to steal login and account details for popular online games. See "Online Gaming-Related Families" in *Trends and Analysis*, on page 62, for more information about this family of worms.
- Win32/RJump, the ninth most common family worldwide, ranks third in the GCC states. It was detected on 17.3 percent more computers in the GCC states in 1H08 than in 2H07. Win32/RJump is a worm that attempts to spread by copying itself to newly attached media (such as USB memory devices or network drives). It also contains backdoor functionality that allows an attacker unauthorized access to an affected computer.

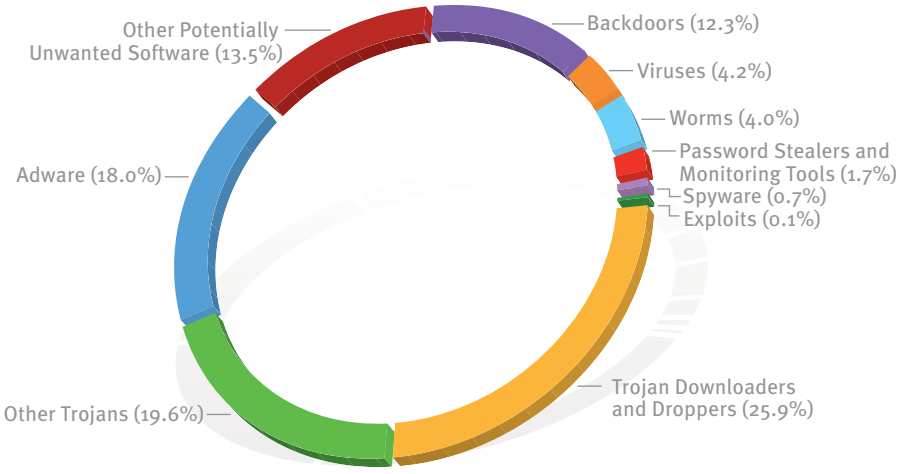
- Win32/Brontok, the twentieth most common family worldwide, ranks fourth in the GCC states. Win32/Brontok is a family of mass-mailing e-mail worms. The worm spreads by sending a copy of itself as an e-mail attachment to e-mail addresses that it gathers from files on the infected computer. It can also copy itself to USB and pen drives. Win32/Brontok can disable antivirus and security software, immediately terminate certain applications, and cause Windows to restart immediately when certain applications run. The worm may also conduct denial of service (DoS) attacks against certain Web sites.
- Win32/C2Lop, the eighth most common family in the GCC states, is not among the 25 most common families worldwide. Win32/C2Lop modifies Web browser settings, adds Web browser bookmarks to advertisements, updates itself, and delivers pop-up and contextual advertisements.
- Win32/Advantage, the thirteenth most common family worldwide, ranks fifteenth in the GCC states. It was detected on 1,084 percent more computers in the GCC states in 1H08 than in 2H07. Win32/Advantage is a family of adware that displays pop-up advertisements and contacts a remote server to download updates.

Hungary

The infection rate (CCM) for Hungary in 1H08 was 10.1, an increase of 12.5 percent since 2H07. Overall, Microsoft security products detected malware and potentially unwanted software on 37 percent more computers in 1H08 than in 2H07.

Figure 57 and Figure 58 list the most common malware and potentially unwanted software categories and families detected by Microsoft security products in Hungary in 1H08.

FIGURE 57. Malware and potentially unwanted software in Hungary, by category, in 1H08



Category	Infected computers
Trojan Downloaders and Droppers	47,472
Other Trojans	35,892
Adware	33,079
Other Potentially Unwanted Software	24,671
Backdoors	22,577
Viruses	7,631
Worms	7,330
Password Stealers and Monitoring Tools	3,208
Spyware	1,226
Exploits	273

Observations:

- The most common category in Hungary is "Trojan Downloaders and Droppers," which accounts for 25.9 percent of all infected computers, with the total number of infected computers increasing 33.6 percent from 2H07. Win32/Zlob, Win32/Renos, and Win32/Cutwail are the main contributors to this category.
- The second most common category in Hungary is "Other Trojans," which includes trojan families that are not classified as downloaders/droppers or backdoors. It accounts for 19.6 percent of all infected computers, with the total number of infected computers increasing 49.4 percent from 2H07.

FIGURE 58. Top 25 families in Hungary in 1H08

Rank	Family	Category	Infected computers
1	Win32/Zlob	Trojan Downloaders and Droppers	41,024
2	Win32/Vundo	Other Trojans	17,081
3	Win32/Advantage	Adware	15,403
4	Win32/Rbot	Backdoors	8,253
5	Win32/Oderoor	Backdoors	7,240
6	Win32/Jeefo	Viruses	6,584
7	Win32/WhenU	Adware	6,231
8	Win32/Renos	Trojan Downloaders and Droppers	6,015
9	Win32/ZangoShoppingreports	Adware	4,839
10	Win32/PossibleHostsFileHijack	Other Potentially Unwanted Software	4,574
11	Win32/Cutwail	Trojan Downloaders and Droppers	4,409
12	Win32/Alureon	Other Trojans	3,090
13	Win32/ZangoSearchAssistant	Adware	3,026
14	Win32/Sdbot	Backdoors	2,965
15	Win32/SeekmoSearchAssistant	Adware	2,921
16	Win32/C2Lop	Other Trojans	2,761
17	Win32/Agent	Other Trojans	2,649
18	Win32/Nuwar	Backdoors	2,446
19	Win32/RealVNC	Other Potentially Unwanted Software	2,279
20	Win32/ConHook	Other Trojans	2,200
21	Win32/Virtumonde	Other Trojans	1,947
22	Win32/Tibs	Other Trojans	1,829
23	Win32/Hotbar	Adware	1,707
24	Win32/BrowsingEnhancer	Adware	1,638
25	Win32/IRCBot	Backdoors	1,589

Observations:

- The top 25 families account for 76.4 percent of all infected computers.
- Nine of the top 25 families are potentially unwanted software families.
- Of the top 10 families, 6 are malware.
- Win32/Zlob, Win32/Vundo, and Win32/Renos, three common families worldwide, are also prevalent in Hungary.
  - Win32/Zlob, the most common threat in the world and in Hungary, was detected on 51.7 percent more computers in 1H08 than in 2H07. See "Win32/Zlob" in *Trends and Analysis*, on page 59, for more information about this family of trojan downloaders.
  - Win32/Vundo, also known as Win32/Virtumonde, was added to the MSRT in March 2008 and has been heavily detected by several Microsoft security products. It is the second most common threat in the world and in Hungary. See "Win32/Vundo and Win32/Virtumonde" in *Trends and Analysis*, on page 60, for more information about this family of trojans.
  - Win32/Renos, the fourth most common family worldwide, ranks eighth in Hungary. It was detected on 15.3 percent fewer computers in Hungary in 1H08 than in 2H07.
- Win32/Oderoor, the fifth most common threat in Hungary, is not among the 25 most common families worldwide. It was added to the MSRT in May 2008. Win32/Oderoor is a backdoor trojan that gives an attacker access and control of the compromised computer. This trojan may connect with remote Web sites and SMTP servers. The primary method of distribution for the Win32/Oderoor family is via instant messaging (IM). Messages are sent via Windows Live Messenger, prompting unsuspecting users to download and execute the trojan from the link provided. See "Spammers: Win32/Cutwail and Win32/Oderoor" in *Trends and Analysis*, on page 61, for more information about this family.
- Win32/Rbot, the twelfth most common family worldwide, ranks fourth in Hungary. It was detected on 5.5 percent more computers in Hungary in 1H08 than in 2H07, indicating that this conventional IRC bot continued to be widely utilized by spammers in Hungary.
- Win32/Jeefo, the sixth most common family in Hungary, is not among the 25 most common families worldwide. This virus, once very prevalent, was much less prevalent relative to other threats worldwide in 1H08, but is still active in Hungary. Win32/Jeefo was detected on 4.3 percent fewer computers in 1H08 than in 2H07.

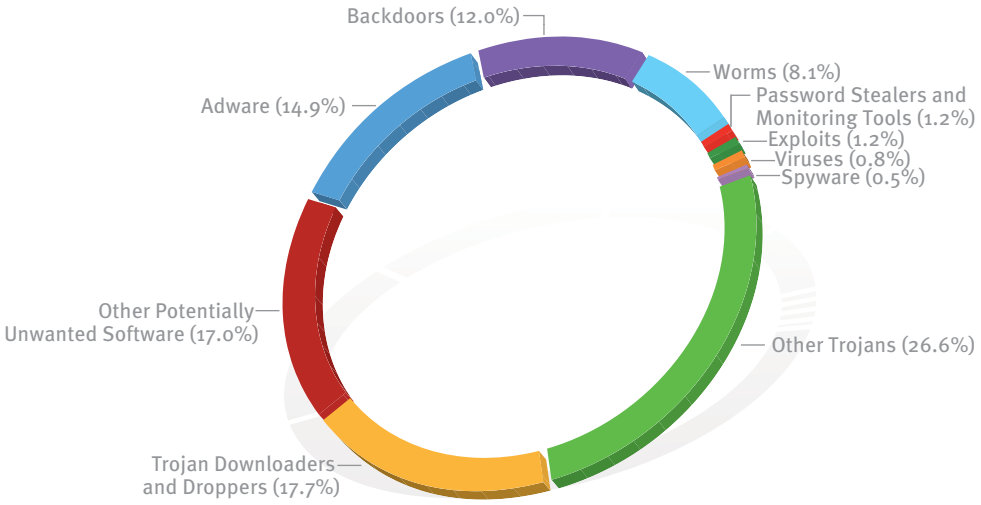
Italy

The infection rate (CCM) for Italy in 1H08 was 7.1, an increase of 34.5 percent since 2H07. Overall, Microsoft security products detected malware and potentially unwanted software on 51 percent more computers in 1H08 than in 2H07.

Figure 59 and Figure 60 list the most common malware and potentially unwanted software categories and families detected by Microsoft security products in Italy in 1H08.

FIGURE 59. Malware and potentially unwanted software in Italy, by category, in 1H08

Category	Infected computers
Other Trojans	338,415
Trojan Downloaders and Droppers	225,731
Other Potentially Unwanted Software	216,269
Adware	189,736
Backdoors	153,278
Worms	103,387
Password Stealers and Monitoring Tools	15,677
Exploits	15,117
Viruses	10,217
Spyware	6,498



Observations:

- The most common category in Italy is "Other Trojans," which includes trojan families that are not classified as downloaders/droppers or backdoors. It accounts for 26.6 percent of all infected computers, with the total number of infected computers increasing 93.4 percent from 2H07. Win32/Vundo and Win32/Agent are the main contributors to this category.
- The second most common category in Italy is "Trojan Downloaders and Droppers," which accounts for 17.7 percent of all infected computers, with the total number of infected computers increasing 58 percent from 2H07. Win32/Zlob, Win32/Renos, and Win32/MessengerSkinner are the main contributors to this category.

FIGURE 60. Top 25 families in Italy in 1H08

Rank	Family	Category	Infected computers
1	Win32/Zlob	Trojan Downloaders and Droppers	133,760
2	Win32/Vundo	Other Trojans	70,365
3	Win32/ZangoSearchAssistant	Adware	58,143
4	Win32/RJump	Worms	56,312
5	Win32/Zonebac	Backdoors	54,918
6	Win32/Rbot	Backdoors	42,379
7	Win32/SpywareSecure	Other Potentially Unwanted Software	41,011
8	Win32/Agent	Other Trojans	39,995
9	Win32/ZangoShoppingreports	Adware	36,015
10	Win32/Advantage	Adware	35,160
11	Win32/MessengerSkinner	Trojan Downloaders and Droppers	32,198
12	Win32/Renos	Trojan Downloaders and Droppers	31,748
13	Win32/Winfixer	Other Potentially Unwanted Software	30,291
14	Win32/BearShare	Other Potentially Unwanted Software	28,777
15	Win32/Adialer	Other Trojans	28,170
16	Win32/WhenU	Adware	25,336
17	Win32/PossibleHostsFileHijack	Other Potentially Unwanted Software	22,581
18	Win32/Hotbar	Adware	22,074
19	Win32/C2Lop	Other Trojans	19,910
20	Win32/Oderoor	Backdoors	19,654
21	Win32/SeekmoSearchAssistant	Adware	17,751
22	Win32/RealVNC	Other Potentially Unwanted Software	17,020
23	Win32/Cutwail	Trojan Downloaders and Droppers	16,949
24	Win32/EGroupSexDial	Other Trojans	16,611
25	Win32/IRCBot	Backdoors	16,074

Observations:

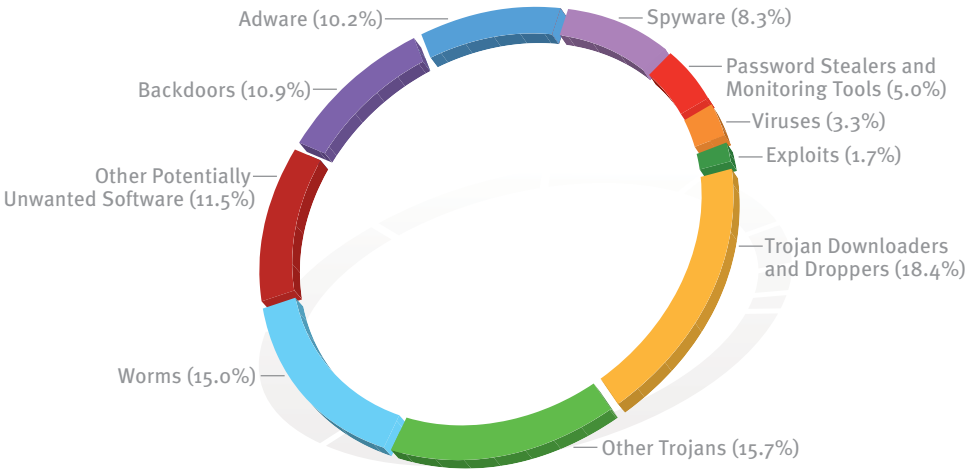
- The top 25 families account for 61.3 percent of all infected computers.
- Eleven of the top 25 families are potentially unwanted software families.
- Of the top 10 families, 6 are malware.
- Win32/Zlob, Win32/Vundo, and Win32/Renos, three common families worldwide, are also prevalent in Italy.
  - Win32/Zlob, the most common threat in the world and in Italy, was detected on 63.1 percent more computers in 1H08 than in 2H07. See "Win32/Zlob" in *Trends and Analysis*, on page 59, for more information about this family of trojan downloaders.
  - Win32/Vundo, also known as Win32/Virtumonde, was added to the MSRT in March 2008 and has been heavily detected by several Microsoft security products. It is the second most common threat in the world and in Italy. See "Win32/Vundo and Win32/Virtumonde" in *Trends and Analysis*, on page 60, for more information about this family of trojans.
  - Win32/Renos, the fourth most common family worldwide, ranks thirteenth in Italy. It was detected on 5.6 percent fewer computers in Italy in 1H08 than in 2H07.
- Win32/SpywareSecure, the seventh most common family in Italy, is not among the 25 most common families worldwide. It was detected on 288.8 percent more computers in Italy in 1H08 than in 2H07. Win32/SpywareSecure is considered rogue security software. It displays misleading warning messages to convince users to purchase a product that removes spyware.
- Win32/RJump, the ninth most common family worldwide, ranks fourth in Italy. It was detected on 79.5 percent more computers in Italy in 1H08 than in 2H07. Win32/RJump is a worm that attempts to spread by copying itself to newly attached media (such as USB memory devices or network drives). It also contains backdoor functionality that allows an attacker unauthorized access to an affected computer.
- Win32/Zonebac, the fifth most common family in Italy, is not among the 25 most common families worldwide. It was detected on 18.6 more computers in Italy in 1H08 than in 2H07.

Japan

The infection rate (CCM) for Japan in 1H08 was 5.3, an increase of 19.7 percent since 2H07. Overall, Microsoft security products detected malware and potentially unwanted software on 19 percent more computers in 1H08 than in 2H07.

Figure 61 and Figure 62 list the most common malware and potentially unwanted software categories and families detected by Microsoft security products in Japan in 1H08.

FIGURE 61. Malware and potentially unwanted software in Japan, by category, in 1H08



Category	Infected computers
Trojan Downloaders and Droppers	127,323
Other Trojans	108,693
Worms	103,420
Other Potentially Unwanted Software	79,682
Backdoors	75,077
Adware	70,713
Spyware	57,333
Password Stealers and Monitoring Tools	34,851
Viruses	22,602
Exploits	11,523

- The most common category in Japan is "Trojan Downloaders and Droppers," which accounts for 18.4 percent of all infected computers, with the total number of infected computers increasing 23.9 percent from 2H07. Win32/Zlob and Win32/Renos are the main contributors to this category.
- The second most common category in Japan is "Other Trojans," which includes trojan families that are not classified as downloaders/droppers or backdoors. It accounts for 15.7 percent of all infected computers, with the total number of infected computers increasing 41.8 percent from 2H07. Win32/Vundo, Win32/Agent, and Win32/ConHook are the main contributors to this category.

FIGURE 62. Top 25 families in Japan in 1H08

Rank	Family	Category	Infected computers
1	Win32/Zlob	Trojan Downloaders and Droppers	83,172
2	Win32/CnsMin	Spyware	46,593
3	Win32/Rbot	Backdoors	45,858
4	Win32/Taterf	Worms	40,749
5	Win32/Vundo	Other Trojans	35,590
6	Win32/Agent	Other Trojans	27,432
7	Win32/Antinny	Worms	21,212
8	Win32/Renos	Trojan Downloaders and Droppers	20,331
9	Win32/Advantage	Adware	18,630
10	Win32/Parite	Viruses	14,270
11	Win32/Frethog	Password Stealers and Monitoring Tools	13,995
12	Win32/Fotomoto	Other Potentially Unwanted Software	13,697
13	Win32/RJump	Worms	12,602
14	Win32/ConHook	Other Trojans	12,174
15	Win32/Winfixer	Other Potentially Unwanted Software	11,654
16	Win32/Virtumonde	Other Trojans	11,117
17	Win32/Sdbot	Backdoors	10,548
18	Win32/Hupigon	Backdoors	10,270
19	Win32/ZangoShoppingreports	Adware	9,881
20	Win32/Cutwail	Trojan Downloaders and Droppers	8,243
21	Win32/RealVNC	Other Potentially Unwanted Software	7,998
22	Win32/AdRotator	Adware	7,915
23	Win32/Alureon	Other Trojans	7,586
24	Win32/Ceekat	Password Stealers and Monitoring Tools	7,404
25	Win32/RewardNetwork	Spyware	7,071

Observations:

- The top 25 families account for 64 percent of all infected computers.
- Seven of the top 25 families are potentially unwanted software families.
- Of the top 10 families, 8 are malware.
- Win32/Zlob, Win32/Vundo, Win32/Renos, and Win32/ConHook, four common families worldwide, are also prevalent in Japan. Win32/Zlob, the most common threat in the world and in Japan, was detected on 66.7 percent more computers in 1H08 than in 2H07. See "Win32/Zlob" in *Trends and Analysis*, on page 59, for more information about this family of trojan downloaders.
- Win32/CnsMin, the second most common family in Japan, is not among the 25 most common families worldwide. It was detected on 45.8 percent fewer computers in Japan in 1H08 than in 2H07.
- Win32/Antinny, the seventh most common family in Japan, is not among the 25 most common families worldwide. It was detected on 18.8 percent fewer computers in Japan in 1H08 than in 2H07.
- Win32/Taterf, the seventh most common family worldwide, ranks fourth in Japan. Win32/Taterf is a family of worms that spread via mapped drives to steal login and account details for popular online games. See "Online Gaming-Related Families" in *Trends and Analysis*, on page 62, for more information about this family of worms.
- Win32/Parite, the tenth most common family in Japan, is not among the 25 most common families worldwide. It was detected on 8.9 percent more computers in Japan in 1H08 than in 2H07. Win32/Parite is a family of polymorphic file infectors that targets computers running Microsoft Windows. The virus infects .exe and .scr executable files on the local file system and on writeable network shares. In turn, the infected executable files perform operations that cause other .exe and .scr files to become infected.

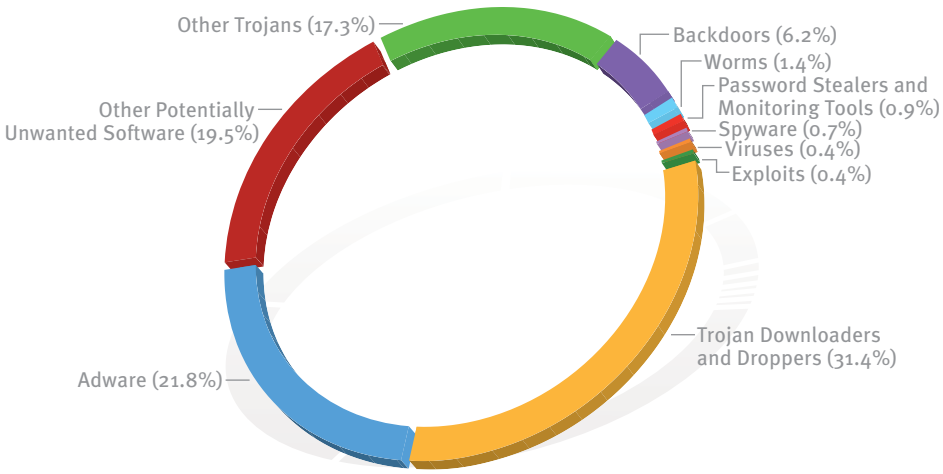
Norway

The infection rate (CCM) for Norway in 1H08 was 8.3, an increase of 32 percent since 2H07. Overall, Microsoft security products detected malware and potentially unwanted software on 46 percent more computers in 1H08 than in 2H07.

Figure 63 and Figure 64 list the most common malware and potentially unwanted software categories and families detected by Microsoft security products in Norway in 1H08.

FIGURE 63. Malware and potentially unwanted software in Norway, by category, in 1H08

Category	Infected computers
Trojan Downloaders and Droppers	82,332
Adware	57,122
Other Potentially Unwanted Software	51,063
Other Trojans	45,450
Backdoors	16,176
Worms	3,645
Password Stealers and Monitoring Tools	2,421
Spyware	1,834
Viruses	1,173
Exploits	976



Observations:

- The most common category in Norway is "Trojan Downloaders and Droppers," which accounts for 31.4 percent of all infected computers, with the total number of infected computers increasing 18.6 percent from 2H07. Win32/Zlob and Win32/Renos are the main contributors to this category.
- The second most common category in Norway is "Adware," which accounts for 21.8 percent of all infected computers, with the total number of infected computers increasing 76 percent from 2H07.
- Eight of the top 25 families are adware families.

FIGURE 64. Top 25 families in Norway in 1H08

Rank	Family	Category	Infected computers
1	Win32/Zlob	Trojan Downloaders and Droppers	72,833
2	Win32/Vundo	Other Trojans	24,938
3	Win32/ZangoSearchAssistant	Adware	17,831
4	Win32/Renos	Trojan Downloaders and Droppers	12,326
5	Win32/ZangoShoppingreports	Adware	11,409
6	Win32/Hotbar	Adware	10,232
7	Win32/Advantage	Adware	9,156
8	Win32/SeekmoSearchAssistant	Adware	9,082
9	Win32/Winfixer	Other Potentially Unwanted Software	8,432
10	Win32/BearShare	Other Potentially Unwanted Software	7,834
11	Win32/Agent	Other Trojans	6,746
12	Win32/Rbot	Backdoors	6,546
13	Win32/BrowsingEnhancer	Adware	6,449
14	Win32/ConHook	Other Trojans	6,331
15	Win32/E404	Other Potentially Unwanted Software	5,167
16	Win32/Mirar	Adware	4,497
17	Win32/WhenU	Adware	3,726
18	Win32/Virtumonde	Other Trojans	3,697
19	Win32/Vapsup	Other Potentially Unwanted Software	3,407
20	Win32/Sdbot	Backdoors	3,206
21	Win32/IRCBot	Backdoors	3,172
22	Win32/PossibleHostsFileHijack	Other Potentially Unwanted Software	3,124
23	Win32/Fotomoto	Other Potentially Unwanted Software	2,803
24	Win32/Alureon	Other Trojans	2,551
25	Win32/RealVNC	Other Potentially Unwanted Software	2,222

Observations:

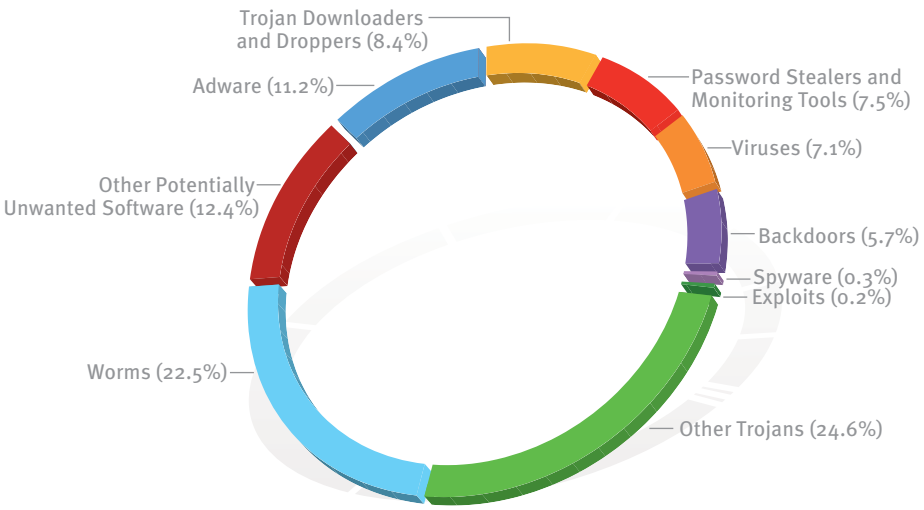
- The top 25 families account for 78.4 percent of all infected computers.
- Fifteen of the top 25 families are potentially unwanted software families.
- Of the top 10 families, 3 are malware.
- Win32/Zlob, Win32/Vundo, and Win32/Renos, three common families worldwide, are also prevalent in Norway.
  - Win32/Zlob, the most common threat in the world and in Norway, was detected on 45.8 percent more computers in 1H08 than in 2H07. See "Win32/Zlob" in *Trends and Analysis*, on page 59, for more information about this family of trojan downloaders.
  - Win32/Vundo, also known as Win32/Virtumonde, was added to the MSRT in March 2008 and has been heavily detected by several Microsoft security products. It is the second most common threat in the world and in Norway. See "Win32/Vundo and Win32/Virtumonde" in *Trends and Analysis*, on page 60, for more information about this family of trojans.
  - Win32/Renos, the fourth most common family worldwide and in Norway, was detected on 28.9 percent fewer computers in Norway in 1H08 than in 2H07.
- Win32/Advantage, the thirteenth most common family worldwide, ranks seventh in Norway. It was detected on 326.9 percent more computers in Norway in 1H08 than in 2H07. Win32/Advantage is a family of adware that displays pop-up advertisements and contacts a remote server to download updates.
- Win32/Winfixer, the seventeenth most common family worldwide, ranks ninth in Norway. It was detected on 22.1 percent fewer computers in Norway in 1H08 than in 2H07. Win32/Winfixer is considered rogue security software, a type of potentially unwanted software. It locates various registry entries, prefetched content, recently accessed files, and other types of data, and identifies them as "privacy violations." Win32/Winfixer then prompts the user to purchase the product to remove the alleged "violations."

Russia

The infection rate (CCM) for Russia in 1H08 was 13.3, an increase of 16.9 percent since 2H07. Overall, Microsoft security products detected malware and potentially unwanted software on 86 percent more computers in 1H08 than in 2H07.

Figure 65 and Figure 66 list the most common malware and potentially unwanted software categories and families detected by Microsoft security products in Russia in 1H08.

FIGURE 65. Malware and potentially unwanted software in Russia, by category, in 1H08



Category	Infected computers
Other Trojans	165,295
Worms	151,804
Other Potentially Unwanted Software	83,683
Adware	75,596
Trojan Downloaders and Droppers	56,799
Password Stealers and Monitoring Tools	50,454
Viruses	48,002
Backdoors	38,549
Spyware	1,981
Exploits	1,109

Observations:

- The most common category in Russia is "Other Trojans," which includes trojan families that are not classified as downloaders/droppers or backdoors. It accounts for 24.6 percent of all infected computers, with the total number of infected computers increasing 462.3 percent from 2H07.
- The second most common category in Russia is "Worms," which accounts for 22.5 percent of all infected computers, with the total number of infected computers increasing 48.7 percent from 2H07.

FIGURE 66. Top 25 families in Russia in 1H08

Rank	Family	Category	Infected computers
1	Win32/RJump	Worms	58,285
2	Win32/Taterf	Worms	47,458
3	Win32/RuPass	Other Trojans	43,953
4	BitAccelerator	Other Potentially Unwanted Software	43,175
5	Win32/Jeefo	Viruses	41,762
6	Win32/Cutwail	Trojan Downloaders and Droppers	39,183
7	Win32/Zlob	Trojan Downloaders and Droppers	31,880
8	Win32/Wukill	Worms	28,988
9	Win32/Alureon	Other Trojans	27,471
10	Win32/Advantage	Adware	26,581
11	Win32/Frethog	Password Stealers and Monitoring Tools	25,456
12	Win32/Brontok	Worms	19,908
13	Win32/Ldpinch	Password Stealers and Monitoring Tools	18,964
14	Win32/WhenU	Adware	17,039
15	Win32/Nuwar	Backdoors	14,632
16	Win32/Vundo	Other Trojans	13,862
17	Win32/Rbot	Backdoors	12,291
18	Win32/ZangoShoppingreports	Adware	10,019
19	Win32/Renos	Trojan Downloaders and Droppers	9,409
20	TrojanClicker	Other Trojans	9,335
21	Win32/Tibs	Other Trojans	7,992
22	Win32/GhostRadmin	Other Potentially Unwanted Software	6,423
23	Win32/Agent	Other Trojans	5,579
24	Win32/VB	Other Trojans	5,488
25	Win32/ZangoSearchAssistant	Adware	4,138

Observations:

- The top 25 families account for 85.1 percent of all infected computers.
- Six of the top 25 families are potentially unwanted software families.
- Of the top 10 families, 8 are malware.
- Only 3 of the top 10 families in Russia (Win32/RJump, Win32/Taterf, and Win32/Zlob) appear in the list of the top 10 families worldwide.
- Win32/Zlob, the most common threat in the world, ranks seventh in Russia. It was detected on 49.2 percent more computers in Russia in 1H08 than in 2H07. See "Win32/Zlob" in *Trends and Analysis*, on page 59, for more information about this family of trojan downloaders.
- Win32/Vundo and Win32/Renos, two very prevalent threats worldwide, are much less prevalent in Russia relative to other threats.
  - Win32/Vundo, also known as Win32/Virtumonde, was added to the MSRT in March 2008 and has been heavily detected by several Microsoft security products. It is the second most common threat in the world but only ranks sixteenth in Russia. See "Win32/Vundo and Win32/Virtumonde" in *Trends and Analysis*, on page 60, for more information about this family of trojans.
  - Win32/Renos, the fourth most common family worldwide, only ranks nineteenth in Russia. It was detected on 10.4 percent fewer computers in Russia in 1H08 than in 2H07.
- Win32/RJump, the ninth most common family worldwide, ranks first in Russia. It was detected on 20 percent more computers in Russia in 1H08 than in 2H07. Win32/RJump is a worm that attempts to spread by copying itself to newly attached media (such as USB memory devices or network drives). It also contains backdoor functionality that allows an attacker unauthorized access to an affected computer.
- In relative terms, malware is significantly more prevalent in Russia than in the world as a whole, and potentially unwanted software is significantly less prevalent. Win32/BitAccelerator and Win32/Advantage are the only two potentially unwanted software families in the top 10.
  - Win32/BitAccelerator, the fourth most common detection in Russia, is not among the 25 most common detections worldwide. Win32/BitAccelerator, first identified in 1H08, is a program that redirects Web search results to other Web sites and may display various advertisements to users while browsing Web sites.
  - Win32/Advantage, the thirteenth most common family worldwide, ranks tenth in Russia. It was detected on 549.9 percent more computers in Russia in 1H08 than in 2H07. Win32/Advantage is a family of adware that displays pop-up advertisements and contacts a remote server to download updates.

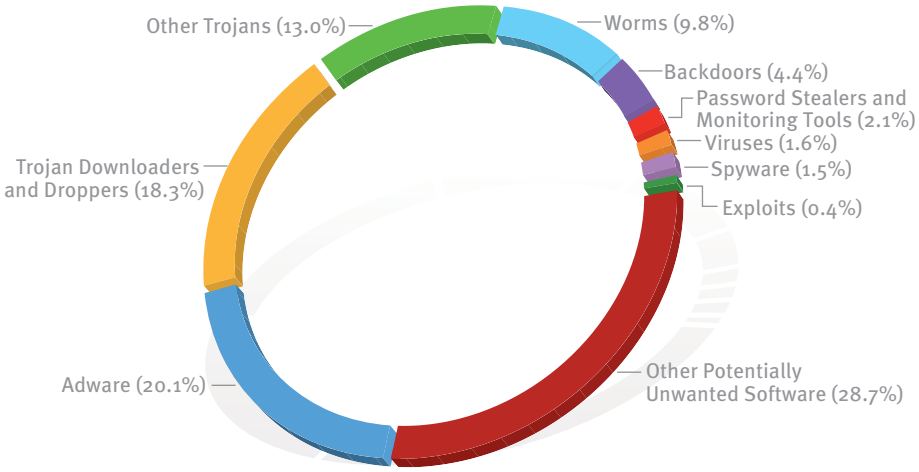
South Africa

The infection rate (CCM) for South Africa in 1H08 was 8.6, an increase of 12.9 percent since 2H07. Overall, Microsoft security products detected malware and potentially unwanted software on 61 percent more computers in 1H08 than in 2H07.

Figure 67 and Figure 68 list the most common malware and potentially unwanted software categories and families detected by Microsoft security products in South Africa in 1H08.

FIGURE 67. Malware and potentially unwanted software in South Africa, by category, in 1H08

Category	Infected computers
Other Potentially Unwanted Software	16,996
Adware	11,890
Trojan Downloaders and Droppers	10,802
Other Trojans	7,715
Worms	5,820
Backdoors	2,611
Password Stealers and Monitoring Tools	1,243
Viruses	934
Spyware	860
Exploits	253



Observations:

- The most common category in South Africa is "Other Potentially Unwanted Software," which includes potentially unwanted software families that are not classified as adware or spyware, such as rogue security software. It accounts for 28.7 percent of all infected computers, with the total number of infected computers increasing 71.3 percent from 2H07. "Other Potentially Unwanted Software" accounts for 8 of the top 25 categories.
- The second most common category in South Africa is "Adware," which accounts for 20.1 percent of all infected computers, with the total number of infected computers increasing 47 percent from 2H07. Eight of the top 25 families are adware families.

FIGURE 68. Top 25 families in South Africa in 1H08

Rank	Family	Category	Infected computers
1	Win32/Zlob	Trojan Downloaders and Droppers	9,609
2	Win32/ZangoSearchAssistant	Adware	3,042
3	Win32/SeekmoSearchAssistant	Adware	2,629
4	Win32/Vundo	Other Trojans	2,509
5	Win32/RealVNC	Other Potentially Unwanted Software	2,442
6	Win32/ZangoShoppingreports	Adware	1,992
7	Win32/Hotbar	Adware	1,974
8	Win32/Renos	Trojan Downloaders and Droppers	1,864
9	Win32/Taterf	Worms	1,758
10	Win32/Agent	Other Trojans	1,742
11	Win32/Starware	Other Potentially Unwanted Software	1,684
12	Win32/RJump	Worms	1,647
13	Win32/Winfixer	Other Potentially Unwanted Software	1,510
14	Win32/Advantage	Adware	1,495
15	Win32/E404	Other Potentially Unwanted Software	1,484
16	Win32/Brontok	Worms	1,262
17	Win32/WhenU	Adware	1,212
18	Win32/BrowsingEnhancer	Adware	990
19	Win32/Vapsup	Other Potentially Unwanted Software	963
20	Win32/Nuwar	Backdoors	917
21	Win32/Rbot	Backdoors	874
22	Win32/UltraVNC	Other Potentially Unwanted Software	839
23	Win32/SpySheriff	Other Potentially Unwanted Software	724
24	Win32/Mirar	Adware	714
25	Win32/PossibleHostsFileHijack	Other Potentially Unwanted Software	650

Observations:

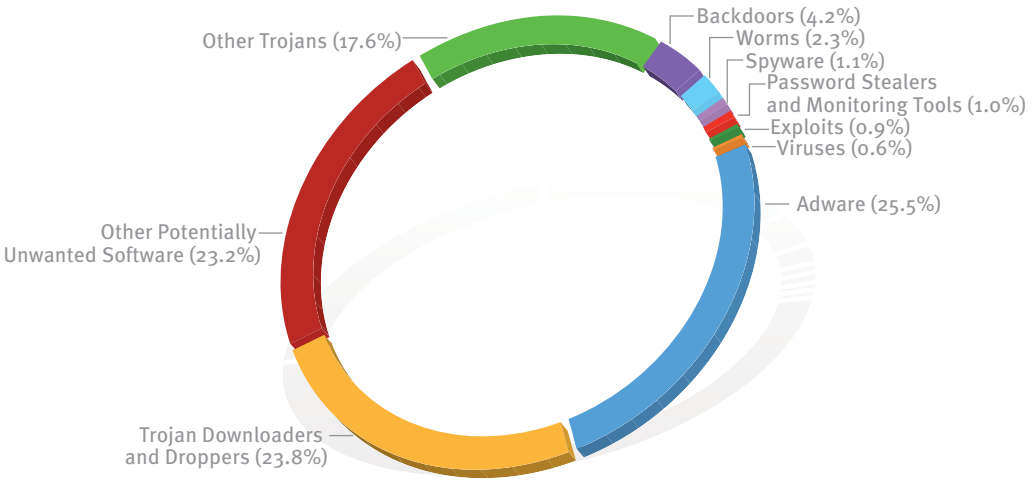
- The top 25 families account for 64.4 percent of all infected computers.
- Sixteen of the top 25 families are potentially unwanted software families.
- Of the top 10 families, 5 are malware.
- Win32/Zlob, Win32/Vundo, and Win32/Renos, three common families worldwide, are also prevalent in South Africa.
  - Win32/Zlob, the most common threat in the world and in South Africa, was detected on 63.3 percent more computers in 1H08 than in 2H07. See "Win32/Zlob" in *Trends and Analysis*, on page 59, for more information about this family of trojan downloaders.
  - Win32/Vundo, also known as Win32/Virtumonde, was added to the MSRT in March 2008 and has been heavily detected by several Microsoft security products. It is the second most common threat in the world and ranks fourth in South Africa. See "Win32/Vundo and Win32/Virtumonde" in *Trends and Analysis*, on page 60, for more information about this family of trojans.
  - Win32/Renos, the fourth most common family worldwide, ranks eighth in South Africa. It was detected on 28 percent fewer computers in South Africa in 1H08 than in 2H07.
- Win32/RealVNC, the fifth most common family in South Africa, is not among the 25 most common families worldwide. RealVNC is a program that enables a computer to be controlled remotely, similar to Remote Desktop. It has a number of legitimate uses but is considered potentially unwanted software because it can be used by an attacker with malicious intent to gain control of a user's computer under some circumstances.
- Win32/Taterf, the seventh most common family worldwide, ranks ninth in South Africa. Win32/Taterf is a family of worms that spread via mapped drives to steal login and account details for popular online games. See "Online Gaming-Related Families" in *Trends and Analysis*, on page 62, for more information about this family of worms.
- Win32/Winfixer, the seventeenth most common family worldwide, ranks thirteenth in South Africa. It was detected on 18.8 percent fewer computers in South Africa in 1H08 than in 2H07. Win32/Winfixer is considered rogue security software, a type of potentially unwanted software. It locates various registry entries, prefetched content, recently accessed files, and other types of data, and identifies them as "privacy violations." Win32/Winfixer then prompts the user to purchase the product to remove the alleged "violations."

United Kingdom

The infection rate (CCM) for the United Kingdom in 1H08 was 9.2, an increase of 32.6 percent since 2H07. Overall, Microsoft security products detected malware and potentially unwanted software on 66 percent more computers in 1H08 than in 2H07.

Figure 69 and Figure 70 list the most common malware and potentially unwanted software categories and families detected by Microsoft security products in the United Kingdom in 1H08.

FIGURE 69. Malware and potentially unwanted software in the United Kingdom, by category, in 1H08



Category	Infected computers
Adware	685,880
Trojan Downloaders and Droppers	641,911
Other Potentially Unwanted Software	624,452
Other Trojans	473,268
Backdoors	113,942
Worms	60,886
Spyware	28,349
Password Stealers and Monitoring Tools	26,478
Exploits	22,962
Viruses	16,359

Observations:

- The most common category in the United Kingdom is "Adware," which accounts for 25.5 percent of all infected computers, with the total number of infected computers increasing 150.6 percent from 2H07.
- The second most common category in the United Kingdom is "Trojan Downloaders and Droppers," which accounts for 23.8 percent of all infected computers, with the total number of infected computers increasing 32 percent from 2H07. Win32/Zlob and Win32/Renos are the main contributors to this category.

FIGURE 70. Top 25 families in the United Kingdom in 1H08

Rank	Family	Category	Infected computers
1	Win32/Zlob	Trojan Downloaders and Droppers	513,048
2	Win32/ZangoSearchAssistant	Adware	353,529
3	Win32/Vundo	Other Trojans	211,324
4	Win32/Hotbar	Adware	175,714
5	Win32/ZangoShoppingreports	Adware	171,432
6	Win32/SeekmoSearchAssistant	Adware	110,587
7	Win32/Renos	Trojan Downloaders and Droppers	105,127
8	Win32/Agent	Other Trojans	104,067
9	Win32/Starware	Other Potentially Unwanted Software	89,341
10	Win32/Winfixer	Other Potentially Unwanted Software	55,359
11	Win32/ConHook	Other Trojans	55,049
12	Win32/BrowsingEnhancer	Adware	53,968
13	Win32/Advantage	Adware	51,843
14	Win32/PossibleHostsFileHijack	Other Potentially Unwanted Software	51,365
15	Win32/Rbot	Backdoors	47,508
16	Win32/BearShare	Other Potentially Unwanted Software	47,277
17	Win32/E404	Other Potentially Unwanted Software	47,191
18	Win32/Fotomoto	Other Potentially Unwanted Software	38,978
19	Win32/Vapsup	Other Potentially Unwanted Software	38,052
20	Win32/Mirar	Adware	36,741
21	Win32/RealVNC	Other Potentially Unwanted Software	33,513
22	Win32/Virtumonde	Other Trojans	33,183
23	Win32/C2Lop	Other Trojans	29,542
24	ASX/Wimad	Trojan Downloaders and Droppers	28,901
25	Win32/WhenU	Adware	28,631

Observations:

- The top 25 families account for 74.7 percent of all infected computers.
- Sixteen of the top 25 families are potentially unwanted software families.
- Of the top 10 families, 4 are malware.
- Win32/Zlob, Win32/Vundo, and Win32/Renos, three common families worldwide, are also prevalent in the United Kingdom.
  - Win32/Zlob, the most common threat in the world and in the United Kingdom, was detected on 45.8 percent more computers in 1H08 than in 2H07. See "Win32/Zlob" in *Trends and Analysis*, on page 59, for more information about this family of trojan downloaders.
  - Win32/Vundo, also known as Win32/Virtumonde, was added to the MSRT in March 2008 and has been heavily detected by several Microsoft security products. It is the second most common threat in the world and ranks third in the United Kingdom. See "Win32/Vundo and Win32/Virtumonde" in *Trends and Analysis*, on page 60, for more information about this family of trojans.
  - Win32/Renos, the fourth most common family worldwide, ranks seventh in the United Kingdom. It was detected on 28 percent fewer computers in the United Kingdom in 1H08 than in 2H07.
- Win32/Winfixer, the seventeenth most common family worldwide, ranks tenth in the United Kingdom. It was detected on 22.1 percent fewer computers in the United Kingdom in 1H08 than in 2H07. Win32/Winfixer is considered rogue security software, a type of potentially unwanted software. It locates various registry entries, prefetched content, recently accessed files, and other types of data, and identifies them as "privacy violations." Win32/Winfixer then prompts the user to purchase the product to remove the alleged "violations."

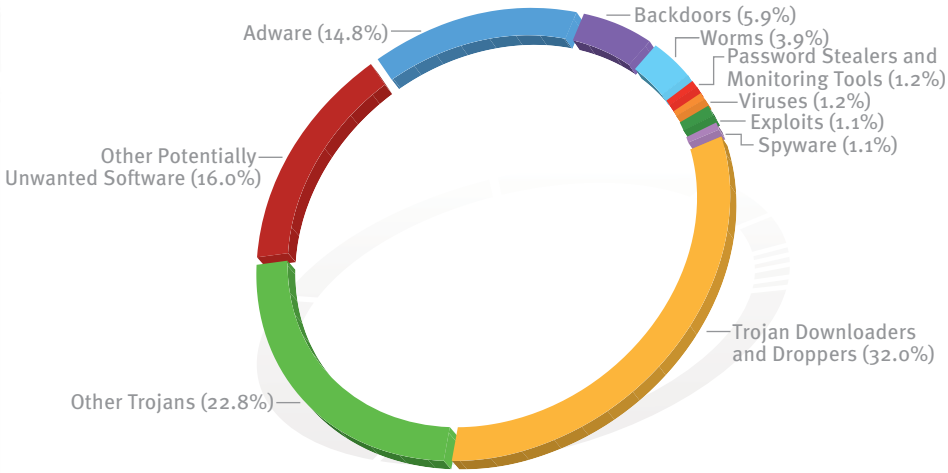
United States

The infection rate (CCM) for the United States in 1H08 was 11.2, an increase of 25.5 percent since 2H07. Overall, Microsoft security products detected malware and potentially unwanted software on 38 percent more computers in 1H08 than in 2H07.

Figure 71 and Figure 72 list the most common malware and potentially unwanted software categories and families detected by Microsoft security products in the United States in 1H08.

FIGURE 71. Malware and potentially unwanted software in the United States, by category, in 1H08

Category	Infected computers
Trojan Downloaders and Droppers	7,044,340
Other Trojans	5,014,874
Other Potentially Unwanted Software	3,528,425
Adware	3,255,585
Backdoors	1,295,060
Worms	847,972
Password Stealers and Monitoring Tools	265,038
Viruses	259,439
Exploits	251,702
Spyware	237,614



Observations:

- The most common category in the United States is "Trojan Downloaders and Droppers," which accounts for 32 percent of all infected computers, with the total number of infected computers increasing 18.7 percent from 2H07.
- The second most common category in the United States is "Other Trojans," which includes trojan families that are not classified as downloaders/droppers or backdoors. It accounts for 22.8 percent of all infected computers, with the total number of infected computers increasing 52.6 percent from 2H07.

FIGURE 72. Top 25 families in the United States in 1H08

Rank	Family	Category	Infected computers
1	Win32/Zlob	Trojan Downloaders and Droppers	5,427,360
2	Win32/Vundo	Other Trojans	2,243,815
3	Win32/ZangoSearchAssistant	Adware	1,300,516
4	Win32/ZangoShoppingreports	Adware	847,420
5	Win32/Agent	Other Trojans	828,372
6	Win32/Hotbar	Adware	761,897
7	Win32/Virtumonde	Other Trojans	594,471
8	Win32/SeekmoSearchAssistant	Adware	541,954
9	Win32/Tibs	Other Trojans	483,515
10	Win32/ConHook	Other Trojans	456,454
11	Win32/Rbot	Backdoors	362,611
12	Win32/Winfixer	Other Potentially Unwanted Software	326,655
13	Win32/Renos	Trojan Downloaders and Droppers	325,562
14	Win32/Starware	Other Potentially Unwanted Software	319,011
15	Win32/Zonebac	Backdoors	297,892
16	ASX/Wimad	Trojan Downloaders and Droppers	270,947
17	Win32/E404	Other Potentially Unwanted Software	264,678
18	Win32/Alureon	Other Trojans	262,860
19	Win32/Nuwar	Backdoors	262,704
20	Win32/Vapsup	Other Potentially Unwanted Software	231,693
21	Win32/SpySheriff	Other Potentially Unwanted Software	221,468
22	Win32/Taterf	Worms	220,533
23	Win32/OneStepSearch	Other Potentially Unwanted Software	207,971
24	Win32/PowerRegScheduler	Other Potentially Unwanted Software	201,032
25	Win32/WhenU	Adware	191,860

Observations:

- The top 25 families account for 65 percent of all infected computers.
- Twelve of the top 25 families are potentially unwanted software families.
- Of the top 10 families, 6 are malware.
- Win32/Vundo, also known as Win32/Virtumonde, was added to the MSRT in March 2008 and has been heavily detected by several Microsoft security products. It is the second most common threat in the world and in the United States. See "Win32/Vundo and Win32/Virtumonde" in *Trends and Analysis*, on page 60, for more information about this family of trojans.
- Win32/Renos, the fourth most common family worldwide, ranks thirteenth in the United States. It was detected on 12.8 percent fewer computers in the United States in 1H08 than in 2H07.
- Win32/Tibs, the eighteenth most common family worldwide, ranks ninth in the United States. It was detected on 163.6 percent more computers in the United States in 1H08 than in 2H07. Win32/Tibs is often used with other malware families as an encryption component.

Vulnerability Data

"Industry Vulnerability Complexity" in *Trends and Analysis*, on page 26, examines the exploit complexity of disclosed vulnerabilities according to the three complexity designations used by CVSSv2. Figure 73 gives definitions for these complexity designations.[18]

FIGURE 73. 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).

[18] Definition from: Mell, Peter, 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.

Exploit Data

Microsoft conducted a survey of publicly available exploits affecting Microsoft products disclosed in 1H08. To perform this survey, researchers collected a broad sample of data from a variety of public sources, including exploit archives, antivirus alerts, mailing lists, hacking Web sites, and exploitation frameworks. Each individual data point was classified and matched to a particular vulnerability, and the results were tabulated.

To verify exploits, researchers tested the code on the latest known vulnerable versions of the affected product. The methodology for generating exploit counts and exploit-testing procedures is as follows:

- If two or more vulnerabilities of a particular product contain multiple reliable exploits in a single security bulletin, the bulletin is only counted once for that product.
- If two or more exploits for a particular Common Vulnerabilities and Exposures (CVE) identifier are available, the CVE is only counted once for all exploits.
- Security bulletins containing multiple CVEs with exploits are counted individually for each CVE. For example, a security bulletin with five CVEs, each of which has its own exploit, is counted five times in the CVE chart, but only once in the security bulletin chart.
- If a bulletin contains multiple CVEs with exploit code affecting different products, the exploit count for the security bulletin chart is determined by the Severity Ratings and Vulnerability Identifiers section of the security bulletin.
- Verified exploits for non-Windows–based core vulnerabilities were tested in a Windows XP SP2 environment with the latest known updates for that component. Windows core vulnerabilities were tested against the latest known updates for the affected operating system.
- Exploits for Microsoft Office suite products and Microsoft component products were tested against the latest version of the product with the latest known updates, based on the severity rating and vulnerability identifier table. For example, MS08-014 contains a publicly available exploit for CVE-2008-0081. Although this CVE identifies Microsoft Office Excel 2000 SP3, Excel 2002 SP3, Excel 2003 SP2, and Office 2004 for Mac as being vulnerable, the only products tested for this CVE were Office Excel 2003 SP2 and Office 2004 for Mac.
- Publicly available proof-of-concept (POC) exploit code is not counted in either the Verified Exploits or Non-Verified Exploits entries.
- Exploits made available for purchase (for example, by Immunity Inc. or Core Security Technologies) are counted as non-verified exploits for all affected products detailed in the Security Rating and Vulnerability Identifier table of a given security bulletin.
- Previous versions of a given product with verified exploit code targeting a newer version of the same product are counted as non-verified exploits.

This review expanded upon the methodology used in the last two volumes of the *Security Intelligence Report*, updating it with the following refinements:

- It includes all products and associated versions listed in the "Affected Software" section of the relevant security bulletins.
- It accounts for Microsoft vulnerabilities publicly disclosed prior to security bulletin release within the month of the security bulletin. For example, the Jet database engine's stack-based buffer overflow vulnerability (CVE-2007-6026) was disclosed prior to the start of 1H08; however, the resolution of this issue was included in May's security bulletin release, so it appears in this dataset.
- A Microsoft security bulletin is counted for a product if any of the vulnerabilities it covers relates to that product. For example, the same Microsoft security bulletin could be counted for both Internet Explorer and Microsoft Windows.
- Cumulative Security Updates for Internet Explorer are counted for Internet Explorer only. Other vulnerabilities in Internet Explorer and affected versions of Windows are accounted for in the security bulletin data chart.
- ActiveX KillBit security bulletins count for operating systems when there is no corresponding component (Internet Explorer) in the operating system. Operating systems with a corresponding component (Internet Explorer) count for the component alone.
- Components that are not part of the core Office suite and that are not packaged with the operating system are classified as individual products. For example, Microsoft Office Visio® is counted as a stand-alone product rather than as part of the Office suite.
- The table in the "Severity Ratings and Vulnerability Identifiers" section of each security bulletin was used to determine the affected products for each CVE.

Figure 74 lists the criteria used for determining whether an exploit was within scope for this research.

FIGURE 74. Criteria for judging exploits

Criteria	Result
Exploit found with shell code or command line	Exploitable
Exploit available in exploitation framework	Exploitable
Exploit code could be purchased from major vendor	Exploitable
Microsoft reports publicly available exploit	Exploitable
Malicious code known to leverage a vulnerability	Exploitable
POC with placeholder, such as a long string, resulting in a denial of service (DoS)	Not Exploitable
POC labeled as a DoS	Not Exploitable
Targeted attacks	Not Exploitable

The total number of vulnerabilities revealed in 1H08 was down 33.6 percent from 2H07 (77 vulnerabilities in 1H08, compared to 116 in 2H07), and the number of publicly available exploits decreased 47.9 percent (25 in 1H08, compared to 48 in 2H07). The percentage of vulnerabilities with publicly available exploits decreased correspondingly, from 44.8 percent in 2H07 to 32.5 percent in 1H08.

Security researchers released 25 exploits for Microsoft products in 1H08. Of the 25 exploits, this study found that 8 exploits (32 percent of the released exploits and 10.4 percent of all vulnerabilities) were reliable. An additional 22 percent of the vulnerabilities with unverified exploits have the potential to become reliable exploits.

The results of this survey are given in Figure 75 and Figure 76 (on the following pages).

FIGURE 75. Exploits by Microsoft Security Bulletin, 1H08

Microsoft Product/Version	# of Security Bulletins	Verified Exploits	Non-Verified Exploits	% of Verified Exploit to Security Bulletin
Windows Internet Explorer				
5	0	0	0	
5.01	4	0	0	
6	4	0	0	
7	3	0	0	
Microsoft Office				
2000	9	0	0	
XP	9	1	1	11.1%
2003	8	2	1	25.0%
X-Mac	0	0	0	
2004-Mac	5	0	0	
2007	4	0	0	
2008-Mac	2	0	0	
Microsoft Windows				
CE	0	0	0	
98	0	0	0	
ME	0	0	0	
2000	11	2	2	18.2%
XP	14	0	2	
2003	14	1	3	7.1%
Windows Vista	12	0	1	
2008	6	0	0	
Internet Information Services (IIS)				
5	1	0	0	
5.1	2	0	0	
6	2	0	0	
7	1	0	0	

Figure 75 continued on next page...

FIGURE 75. Exploits by Microsoft Security Bulletin, 1H08 (continued)

Microsoft Product/Version	# of Security Bulletins	Verified Exploits	Non-Verified Exploits	% of Verified Exploit to Security Bulletin
Visual Studio				
Visual Basic 6	1	0	0	
6	0	0	0	
.NET 2002	1	0	0	
.NET 2003	1	0	0	
BizTalk Server				
2000	1	0	0	
Microsoft Project				
2000	1	0	0	
2002	1	0	0	
2003	1	0	0	
Visio				
2002	1	0	0	
2003	1	0	0	
2007	1	0	0	
Microsoft Works				
Works 6 File Converter	1	1	0	100.0%
Works 7	0	0	0	
Outlook Express/Windows LiveMail				
Windows Live Mail	0	0	0	
Microsoft Exchange				
Exchange Server 5.0	0	0	0	
Other Products				
Commerce Server 2000	1	0	0	
Internet Security and Acceleration Server 2000	1	0	0	
Windows Installer	0	0	0	
Live OneCare	1	0	0	
Antigen for Exchange	1	0	0	
Antigen for SMTP	1	0	0	
Windows Defender	1	0	0	
Forefront Client Security	1	0	0	
Forefront Security for Exchange	1	0	0	
Forefront Security for Sharepoint	1	0	0	
Standalone System Sweeper	1	0	0	
Active Directory	2	0	0	
ADAM	2	0	0	
AD LDS	1	0	0	
SharePoint Services 2.0	0	0	0	

FIGURE 76. Exploits by CVE ID, 1H08

Microsoft Product/Version	# CVE	Verified Exploits	Non-Verified Exploits	% of Verified Exploit to CVE	% of Exploits to CVE
Windows Internet Explorer					
5	1	0	0		
5.01	6	0	0		
6	10	1	0	10.0%	10.0%
7	10	0	2		20.0%
Microsoft Office					
2000	18	0	0		
XP	17	1	1	5.9%	11.8%
2003	16	2	1	12.5%	18.8%
X-Mac	0	0	0		
2004-Mac	12	0	0		
2007	8	0	0		
2008-Mac	5	0	0		
Microsoft Windows					
CE	1	0	0		
98	0	0	0		
ME	0	0	0		
2000	13	2	2	15.4%	30.8%
XP	19	0	2		10.5%
2003	18	1	3	5.6%	22.2%
Windows Vista	14	0	1		7.1%
2008	8	0	0		
Internet Information Services (IIS)					
5	1	0	0		
5.1	2	0	0		
6	2	0	0		
7	1	0	0		
Visual Studio					
Visual Basic 6	5	0	4		80.0%
Visual Studio 6	1	0	0		
.NET 2002	2	0	0		
.NET 2003	2	0	0		
BizTalk Server					
2000	2	0	0		
2002	2	0	0		

Figure 76 continued on next page...

FIGURE 76. Exploits by CVE ID, 1H08 (continued)

Microsoft Product/Version	# CVE	Verified Exploits	Non-Verified Exploits	% of Verified Exploit to CVE	% of Exploits to CVE
Microsoft Project					
2000	1	0	0		
2002	1	0	0		
2003	1	0	0		
Visio					
2002	2	0	0		
2003	2	0	0		
2007	2	0	0		
Microsoft Works					
Works 6 File Converter	3	1	0	33.3%	33.3%
Works 7	1	0	0		
Outlook Express/Windows Live Mail					
Windows Live Mail	1	0	0		
Microsoft Exchange					
Exchange Server 5.0	1	0	0		
Other Products					
Commerce Server 2000	2	0	0		
Internet Security and Acceleration Server 2000 SP2	2	0	0		
Windows Installer	1	0	0		
Live OneCare	2	0	0		
Antigen for Exchange	2	0	0		
Antigen for SMTP	2	0	0		
Windows Defender	2	0	0		
Forefront Client Security	2	0	0		
Forefront Security for Exchange	2	0	0		
Forefront Security for Sharepoint	2	0	0		
Standalone System Sweeper	2	0	0		
Active Directory	2	0	0		
ADAM	2	0	0		
AD LDS	1	0	0		
SharePoint Services 2.0	1	0	1		100.0%

"Top Browser-Based Exploits" in *Trends and Analysis*, on page 32, examines the relative prevalence of browser-based exploits in 1H08, as determined from a sample of data obtained from customer-reported incidents, submissions of malicious code, and Windows error reports. The sample covers multiple operating systems and browser versions from Windows XP to Windows Vista and includes data from third-party browsers using the Trident rendering engine used by Internet Explorer.

Figure 77 lists all browser-based exploits totaling at least 1 percent of the sample, labeled with the relevant Microsoft security bulletin number or CVE identifier, if applicable. See Figure 12 in *Trends and Analysis*, on page 33, for a graphical view of these statistics.

FIGURE 77. Top browser-based exploits encountered in 1H08

Vulnerability Reference (where available)	Affected Component and Method	% of Total Exploits
MS06-014 (CVE-2006-0003)	Microsoft MDAC_RDS	12.1%
CVE-2007-5601	RealPlayer_IERPCtl	7.0%
CVE-2007-4816	BaoFengStorm_rawParse	6.8%
CVE-2007-0015	Apple_Quicktime_RTSP	6.3%
CVE-2007-4105	BaiduToolbar_DloadDS	5.0%
CVE-2008-1309	RealPlayer_rmoc3260_Console	4.9%
GLChat.ocx_ConnectAndEnterRoom	GLChat.ocx_ConnectAndEnterRoom	4.1%
MS06-071 (CVE-2006-5745)	Microsoft MSXML_setRequestHeader	3.9%
CVE-2007-4748	PowerPlayer_Logo	3.8%
CVE-2006-5820	AOL_SuperBuddyAX	3.2%
CVE-2007-5064	Xunlei_Webthunder_DownURL2	2.9%
CVE-2007-5779	GOMPlayer_OpenURL	2.8%
MS06-057 (CVE-2006-3730)	Microsoft WebViewFolderIcon	2.7%
CVE-2007-3076	Zenturi_DownloadFile	2.6%
CVE-2007-3148	Yahoo_WebcamViewer_ActiveX	2.3%
CVE-2006-5198	WinZip_CreateNewFolderFromName	2.2%
MS06-067 (CVE-2006-4446 and -4447)	Microsoft DirectAnimation_KeyFrame	2.1%
ourgame_GLIEDown2_IEStartNative	ourgame_GLIEDown2_IEStartNative	2.0%
CVE-2008-1472	ComputerAssociates_ListCtrl_AddColumn	1.9%
GLChat_OCX_hgs_startNotify	GLChat_OCX_hgs_startNotify	1.9%
CVE-2006-1190	Microsoft createTextRange	1.6%
CVE-2007-5892	SSReader_pdg2_Register	1.6%
MS06-055 (CVE-2006-4868)	Microsoft VML	1.5%
CVE-2007-3296	Xunlei_Webthunder_AddTask	1.4%
CVE-2007-5659	AdobeAcrobat_collectEmailInfo	1.4%
MS03-011 (CVE-2003-0111)	Microsoft JVMBytecodeVerifier	1.3%
MS07-017 (CVE-2007-0038)	Microsoft Animated_Cursor_stack_overrun	1.1%
MS07-004 (CVE-2007-0024)	Microsoft VML	1.0%

Figure 78 and Figure 79 list the 10 vulnerabilities exploited most often in Windows XP and Windows Vista in 1H08, respectively, as determined by analyzing a sample of data obtained from customer-reported incidents, submissions of malicious code, and Windows error reports. See Figure 14 and Figure 15 in *Trends and Analysis*, on page 35, for a graphical view of these statistics.

FIGURE 78. The 10 browser-based vulnerabilities exploited most often on computers running Windows XP, 1H08

Vulnerability	Percent of Sample
MS06-014 (MDAC_RDS)	12.0%
MS06-071 (MSXML_setRequestHeader)	5.8%
CVE-2007-0015 (Apple_Quicktime_RTSP)	5.2%
MS06-057 (WebViewFolderIcon)	4.7%
CVE-2008-1309 (RealPlayer_rmoc3260_Console)	4.6%
MS06-067 (DirectAnimation_KeyFrame)	4.6%
CVE-2007-3148 (Yahoo_WebcamViewer_ActiveX)	3.9%
CVE-2006-5198 (WinZip_CreateNewFolderFromName)	3.7%
MS06-055 (VML)	3.7%
CVE-2007-5601 (RealPlayer_IERPCtl)	3.6%

FIGURE 79. The 10 browser-based vulnerabilities exploited most often on computers running Windows Vista, 1H08

Vulnerability	Percent of Sample
CVE-2007-4816 (BaoFengStorm_rawParse)	11.0%
CVE-2007-5601 (RealPlayer_IERPCtl)	11.0%
CVE-2007-4105 (BaiduToolbar_DloadDS)	8.3%
CVE-2007-0015 (Apple_Quicktime_RTSP)	8.3%
CVE-2008-1309 (RealPlayer_rmoc3260_Console)	6.1%
GLChat_OCX_wvsprintfA	6.0%
CVE-2007-4748 (PowerPlayer_Logo)	5.6%
CVE-2007-5064 (Xunlei_Webthunder_DownURL2)	4.0%
CVE-2006-5820 (AOL_SuperBuddyAX)	3.8%
CVE-2007-5779 (GOMPlayer_OpenURL)	3.5%

Malware Family Data

Figure 80 lists the top 25 malware and potentially unwanted software families that were detected on computers by all of the Microsoft security products in 1H08. See "Selected Prevalent Families" in *Trends and Analysis*, on page 59, for additional details and analysis about some of these families.

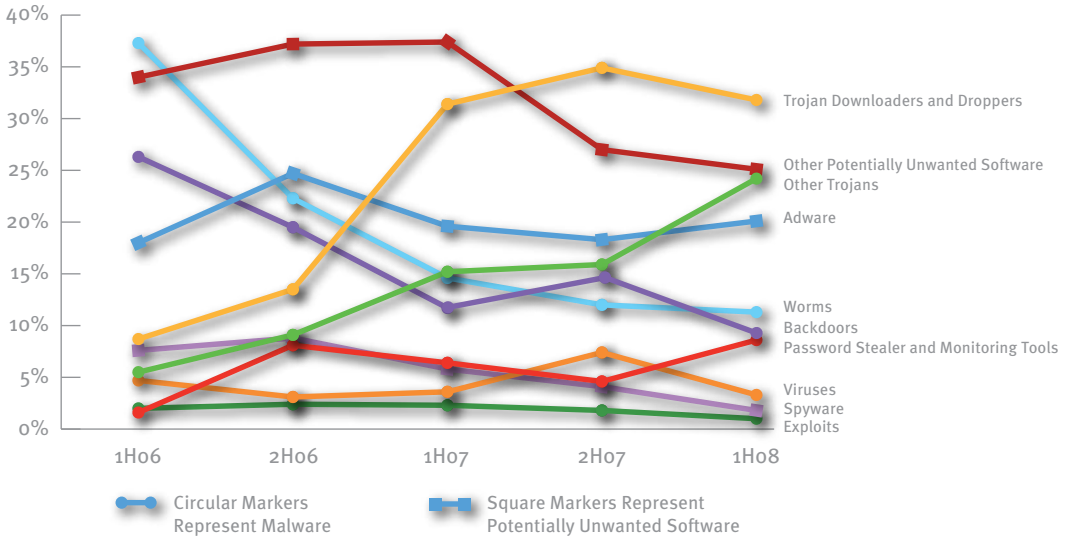
FIGURE 80. Top 25 malware and potentially unwanted software families worldwide in 1H08, by number of unique infected computers

Rank	Family	Infected Computers (2H07)	Infected Computers (1H08)	Change
1	Win32/Zlob	5,562,950	9,016,880	62.1%
2	Win32/Vundo	62,548	3,736,267	5,873.4%
3	Win32/ZangoSearchAssistant	1,237,417	2,712,097	119.2%
4	Win32/Renos	2,949,717	2,624,730	-11.0%
5	Win32/Agent	859,528	1,669,480	94.2%
6	Win32/ZangoShoppingreports	121,554	1,640,440	1,249.6%
7	Win32/Taterf	N/A	1,565,843	N/A
8	Win32/Hotbar	894,987	1,444,231	61.4%
9	Win32/RJump	1,256,009	1,232,663	-1.9%
10	Win32/Bancos	126,297	1,229,276	873.3%
11	Win32/SeekmoSearchAssistant	464,266	1,133,166	144.1%
12	Win32/Rbot	1,230,011	1,103,077	-10.3%
13	Win32/Advantage	211,703	1,042,049	392.2%
14	Win32/Virtumonde	343,610	864,340	151.5%
15	Win32/ConHook	1,433,099	847,354	-40.9%
16	Win32/Frethog	N/A	809,519	N/A
17	Win32/Winfixer	1,161,412	743,166	-36.0%
18	Win32/Tibs	279,507	733,042	162.3%
19	Win32/BaiduSobar	439,038	704,320	60.4%
20	Win32/Brontok	810,041	682,535	-15.7%
21	Win32/WhenU	1,519,224	632,178	-58.4%
22	Win32/Cutwail	18,675	624,113	3,242.0%
23	Win32/Alureon	574,998	601,093	4.5%
24	Win32/Starware	798,706	590,737	-26.0%
25	Win32/Hupigon	727,161	581,126	-20.1%

Figure 81 shows the relative prevalence of different categories of malware and potentially unwanted software since 1H06, expressed as a percentage of the total number of computers cleaned during each time period. Totals may exceed 100 percent for each time period because some computers are cleaned of more than one category of families during each time period. (The line chart below is also reproduced as Figure 27, on page 51, in *Trends and Analysis*.)

FIGURE 81. Computers cleaned by threat category, in percentages, 1H06–1H08

Category	1H06	2H06	1H07	2H07	1H08
Trojan Downloaders and Droppers	8.7%	13.5%	31.4%	34.9%	31.8%
Other Trojans	5.5%	9.1%	15.2%	15.9%	24.2%
Adware	18.0%	24.7%	19.6%	18.3%	20.1%
Other Potentially Unwanted Software	34.0%	37.2%	37.4%	27.0%	25.1%
Worms	37.3%	22.3%	14.6%	12.0%	11.3%
Backdoors	26.3%	19.5%	11.7%	14.5%	9.2%
Password Stealers and Monitoring Tools	1.6%	8.1%	6.4%	4.6%	8.6%
Viruses	4.7%	3.1%	3.6%	7.4%	3.3%
Spyware	7.6%	8.8%	5.8%	4.1%	1.8%
Exploits	2.0%	2.4%	2.3%	1.8%	1.0%



Malware Samples by Category

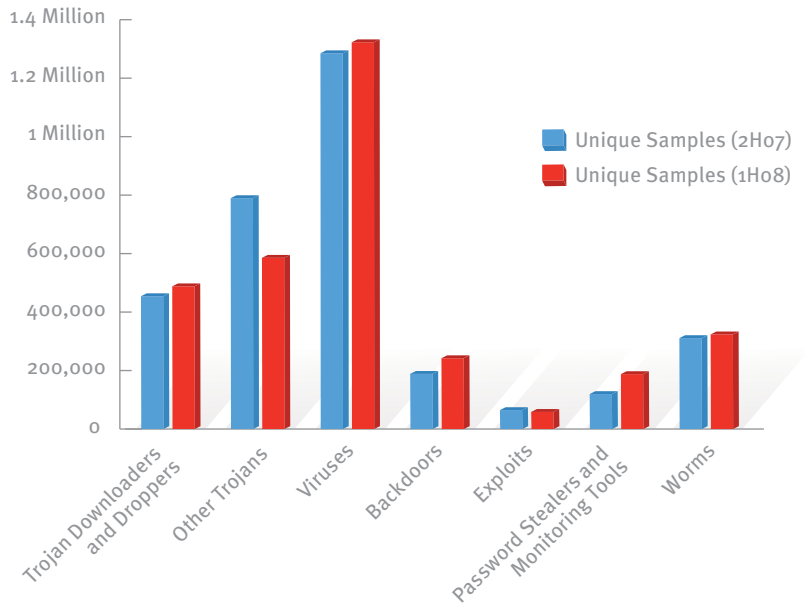
Malware authors attempt to evade detection by continually releasing new variants in an effort to outpace the release of new signatures by antivirus vendors. Counting variants is one way to determine which families and categories of malware are currently most active (in other words, which families and 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 users. The Microsoft Malware Protection Center (MMPC) collects and analyzes unique malware samples from many different sources worldwide in an effort to accurately understand the state of malware development activity.

Figure 82 shows the number of new unique samples collected in each category in 2H07 and 1H08.

> *The Microsoft Malware Protection Center (MMPC) collects and analyzes unique malware samples from many different sources worldwide in an effort to accurately understand the state of malware development activity.*

FIGURE 82. Total unique samples by category, 2H07 and 1H08

Category	Unique Samples (2H07)	Unique Samples (1H08)	Change %
Trojan Downloaders and Droppers	464,061	497,913	6.8%
Other Trojans	799,430	595,439	-34.3%
Viruses	1,295,034	1,332,596	2.8%
Backdoors	198,368	251,994	21.3%
Exploits	74,517	68,337	-9.0%
Password Stealers and Monitoring Tools	129,406	197,599	34.5%
Worms	320,768	333,484	3.8%



Overall, the number and distribution of samples collected in 1H08 were nearly identical to 2H07, contrary to the general trend of increasing malware prevalence and complexity.

The total number of exploit samples collected in 1H08 decreased 8.3 percent from 2H07, continuing a trend that has been observed over the last several periods. One possible explanation is that many of the old vulnerabilities that have been heavily exploited in the past, such as HTML/IframeRef, are fixed on more and more computers and therefore become less effective for attackers. Attackers today rely more on social engineering as a method for spreading malware than in the past.

Backdoor and password stealer/monitoring tool samples increased significantly from 2H07 to 1H08. This suggests that attackers are looking more aggressively to capture sensitive information from victims' computers or to control them for their purposes. As many malware creators and distributors are primarily motivated by the prospect of financial gain, being able to control victims' computers in this way can be lucrative for attackers.

As many malware creators and distributors are primarily motivated by the prospect of financial gain, being able to control victims' computers in this way can be lucrative for attackers.

The large number of virus samples can be attributed to the fact that a virus can infect many different files, each of which is detected as a unique sample.

The number of trojan samples decreased significantly in 1H08. Understanding the reasons for this will require further research.

Malware Samples by Family

Figure 83 lists the families that had the highest numbers of new samples in 1H08.

Some observations:

- Several of the families with the most samples are viruses, like Win32/Virut and DOS/VKit_DA. As noted above, many viruses tend to create large numbers of samples because they can infect many different files, each of which is detected as a unique sample. These figures should not be taken as an indication of large numbers of true variants for these families. Similarly, some worms, such as Win32/Allaple, create many different copies of themselves while replicating.
- Many of the more common families also have large numbers of unique samples. This suggests that virus creators are having some measure of success using large numbers of variants to spread to many computers and evade detection. For example, Win32/Zlob, the most prevalent family in 1H08 by a wide margin, had a new sample released every 97 seconds, on average, during the period—twice the frequency with which attackers released samples during the previous period (2H07). (See "Win32/Zlob" in *Trends and Analysis*, on page 59, for more information about this family.)
- Sometimes malicious code is reused for multiple purposes. For example, Win32/Tibs is well known as the encryption layer for Win32/Nuwar, but it is also used as the encryption layer of other malware families. This explains the high number of samples that were detected as Win32/Tibs.

FIGURE 83. Total unique samples by family, 1H08

Family	New Samples (1H08)
Win32/Virut	164,307
Win32/Zlob	161,234
Win32/Adialer	159,834
Win32/Allaple	89,373
Win32/Tibs	77,828
Win32/C2Lop	72,049
DOS/VKit_DA	71,436
Win32/Hupigon	68,014
Win32/Small	67,787
Win32/Netsky	66,327
Win32/Storark	63,947
Win32/Delf	57,909
Win32/Agent	55,014
Win32/Vundo	50,116
Win32/Obfuscator	47,895
Win32/Luder	47,582
Win32/Nuwar	42,637
HTML/IframeRef	37,165
Win32/Alureon	36,102
Win32/Lovelorn	35,940
Win32/Zonebac	32,392
Win32/Cekar	31,677
Win32/Dialsnif	30,478
Win32/Rbot	30,361
Win32/Frethog	28,841
Win32/Virtumonde	27,529

Operating System Data

"Operating System Trends" in *Trends and Analysis*, on page 53, examines the infection rates for different Microsoft Windows operating system/service pack combinations. Figure 84 offers more detail, listing the CCM for each Microsoft Windows operating system/service pack combination that accounted for at least 10,000 cleanings or at least 0.1 percent of total MSRT executions in 1H08. See Figure 28 in *Trends and Analysis*, on page 53, for a graphical view of these statistics.

FIGURE 84. Number of computers cleaned for every 1,000 MSRT executions, by operating system

Operating System	# of Computers Cleaned per 1,000 Executions
Windows XP RTM	33.8
Windows XP SP1	24.5
Windows XP SP2	11.2
Windows XP SP3	9.2
Windows Vista RTM	4.9
Windows Vista SP1	4.5
Windows Vista RTM (64-bit)	4.2
Windows Vista SP1 (64-bit)	2.3
Windows 2000 SP3	11.0
Windows 2000 SP4	4.9
Windows Server 2003 SP2	1.0

Product-Specific Data

Exchange Hosted Services

"E-Mail Threats" in *Trends and Analysis*, on page 58, explains how Exchange Hosted Services (EHS) detects malware and potentially harmful files attached to incoming messages. Figure 85 provides a closer look at some of these statistics, listing the top 20 malware variants detected by EHS in 1H08 and in 2H07.

FIGURE 85. Top 25 variants detected by EHS in 1H08 (left) and 2H07 (right)

1H08	Threat	Reports
1	Exploit:HTML/IframeRef.gen	51,268,066
2	TrojanDropper:Win32/Cutwail.Y	5,559,282
3	TrojanDownloader:Win32/Cutwail.S	3,806,299
4	VirTool:WinNT/Cutwail.gen!B	2,897,929
5	TrojanDropper:Win32/Cutwail.AD	2,036,444
6	Worm:Win32/Netsky.P@mm	1,818,859
7	VirTool:WinNT/Cutwail.F	1,414,720
8	Exploit:HTML/IFrame_Exploit.D	1,282,456
9	TrojanDropper:Win32/Cutwail.AA	1,251,463
10	TrojanDropper:Win32/Cutwail.W	1,112,980
11	Trojan:Win32/AgentBypass	1,005,041
17	Trojan:WinNT/Cutwail.A!sys	945,203
12	TrojanDropper:Win32/Cutwail.AH	693,684
13	VirTool:WinNT/Cutwail.K	639,370
14	TrojanDropper:Win32/Cutwail.AC	480,294
15	TrojanDropper:Win32/Cutwail.AF	459,324
18	Virus:Win32/Virut.A	399,942
16	TrojanDropper:Win32/Cutwail.Z	388,611
19	Worm:Win32/Netsky.W.dam	371,158
20	VirTool:WinNT/Cutwail.J	344,674

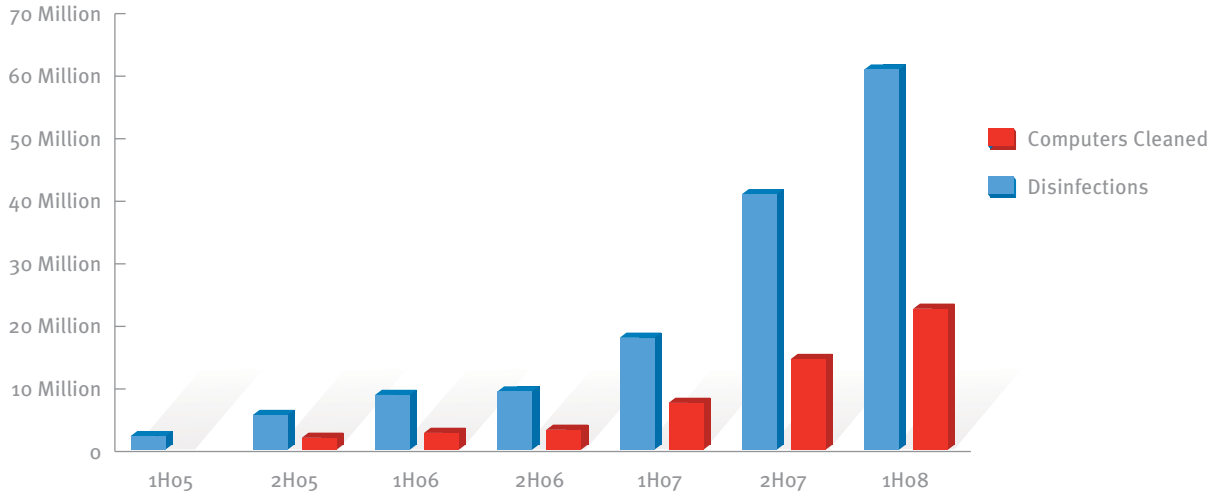
2H07	Threat	Reports
1	VirTool:WinNT/Cutwail.gen!B	1,773,108
2	TrojanDropper:Win32/Cutwail.H	1,668,995
3	TrojanDropper:Win32/Cutwail.T	1,037,455
4	TrojanDropper:Win32/Cutwail.R	863,597
5	Worm:Win32/NetSky.P@mm	587,563
6	Exploit:HTML/IFrame_Exploit.D	495,223
7	TrojanDownloader:Win32/Small	304,097
8	TrojanDownloader:Win32/Stration.AR	299,240
9	Worm:Win32/Netsky.N@mm	176,041
10	TrojanDownloader:Win32/Chepvil.gen!A	119,223
11	Worm:Win32/Netsky.D@mm	118,965
17	Worm:Win32/Mydoom.O@mm	101,578
12	Worm:HTML/Bagle!mail	98,141
13	Virus:Win32/Virut.A	90,540
14	Worm:Win32/Mywife.E@mm!CME24.dam#2	75,911
15	Worm:Win32/Bagle.ZD@mm	74,788
18	Backdoor:Win32/Mydoom.gen	66,222
16	Worm:Win32/Netsky.CY@mm.dam#2	58,844
19	TrojanDropper:Win32/Odrtre.B	56,958
20	Worm:Win32/Mydoom.L@mm	53,056

Malicious Software Removal Tool (MSRT)

Figure 86 shows the total number of disinfections and distinct computers cleaned by the MSRT since 2005. (Note that Microsoft did not begin to measure unique computers cleaned until 2H05, so this data is unavailable for 1H05.)

FIGURE 86. Total malware disinfections and distinct computers cleaned by the MSRT, in half-year increments, since 1H05

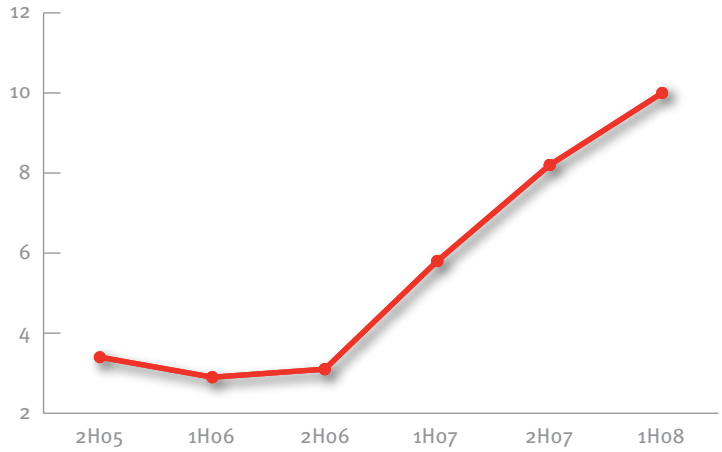
Period	Executions	Disinfections	Computers Cleaned
1H05	845,444,597	3,489,069	N/A
2H05	1,159,738,810	6,870,372	3,226,304
1H06	1,643,541,890	10,078,369	4,013,479
2H06	1,837,242,380	10,626,607	4,505,920
1H07	1,909,866,700	19,217,340	8,808,742
2H07	2,448,399,710	42,168,921	15,823,957
1H08	2,949,176,380	62,084,912	23,854,039



In 1H08, the MSRT removed malware from 23.9 million distinct computers worldwide, a 50 percent increase over the second half of 2007. The number of total disinfections performed in 2H07 rose to 62 million, an increase of 47 percent over 2H07. A *disinfection* is defined as the removal of a distinct type of malware, such as a specific file infector variant, that is present on an infected computer. The number of total disinfections is greater than the number of distinct computers cleaned because the MSRT often detects multiple infections on a single computer and because computers can become reinfected from month to month.

Since the initial release of MSRT, the infection rate measured by the MSRT has gone from a low of 2.9 in 1H06 to the current high of 10.0. Figure 87 shows the average monthly CCM for every six-month period from 2H05 to 2H08.

FIGURE 87. Computers cleaned for every 1,000 executions of the MSRT (CCM), in half-year increments, since 2H05



This increase can be attributed to a number of factors, including detection improvements, the continual addition of new and newly prevalent families to the MSRT, and a general rise in malware prevalence worldwide. See "Malware and Potentially Unwanted Software Trends" in *Trends and Analysis*, on page 45, for more in-depth analysis of the observed increase.

Glossary and Appendix

Glossary

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 (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 of them, 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.

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.

iFrame
Short for *inline frame*. An iFrame is an HTML document that is embedded in another HTML document. Because the iFrame links to 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 Microsoft Windows Malicious Software Removal Tool (MSRT) is designed to help identify and remove specifically targeted, prevalent malware from customer computers and is available at no charge to licensed Windows users. The main release mechanism of 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.

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)*.

Other Potentially Unwanted Software
A classification used by the *Security Intelligence Report* to denote potentially unwanted software families that are not classified as adware or spyware. Other Potentially Unwanted Software includes rogue security software, browser modifiers, remote access programs, and other categories. Also see *Other Trojans*.

Other Trojans
A classification used by the *Security Intelligence Report* to denote trojan families that are not classified as downloaders/droppers or backdoors. Other Trojans includes clickers, notifiers, denial-of-service trojans, and other categories. Also see *Other Potentially Unwanted Software*.

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*.

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.

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.

rogue security software
Software that appears to be beneficial from a security perspective but which provides limited or no security capabilities or generates a significant number of erroneous or misleading alerts, or which may attempt 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.

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.

tool
Software that may have legitimate purposes but that 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. Other forms of viruses include boot sector viruses and replicating worms.

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

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.

Appendix: Data Sources

Software Vulnerabilities

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

By leveraging these sources, in addition to many others, Microsoft has compiled a database of disclosure dates for vulnerabilities that can be used to determine the year, month, and day that each vulnerability was disclosed publicly and broadly for the first time. Note that, in this report, *disclosure* is used to mean broad and public disclosure, and not any sort of private disclosure or disclosure to a limited number of people.

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 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 88 shows the main data sources used in this report to compile data on the prevalence of malicious and potentially unwanted software.

FIGURE 88. 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				•	WU / AU, Download Center
Windows Defender	•				•	•	•	Download Center Windows Vista
Windows Live OneCare Safety Scanner	•		•		•		•	Web
Windows Live OneCare	•		•	•	•	•		Web / Store Purchase
Microsoft Exchange Hosted Filtering		•	•	•				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 Server 2003, Windows XP, and Windows 2000. As of June 2008, the tool detects and removes 111 different malware families, each of which is currently prevalent or was prevalent at the time it was 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 1H08, the MSRT was executing on more than 475 million computers worldwide every month. The majority (79.2 percent) of these executions involved computers running Windows XP, with all but a tiny fraction of these running Windows XP SP2 or later. This is due to the fact that SP2 encourages users to enable Windows Automatic Updates, which allows the MSRT to download and execute automatically. Among other operating systems, Windows Vista continues to rise sharply, accounting for 19.2 percent of all executions in June 2008 and 16.9 percent of all 1H08 executions. Executions on Windows 2000, Windows Server 2003, and Windows Server 2008 were flat throughout the period and together account for less than 4 percent of total executions.

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.

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 3.7 million times in 1H08.

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 1H08, Windows Defender was installed on more than 67.4 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 as an integrated component of the operating system rather than as a separate download, which has significantly increased the program's installed base.

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
- Windows Live OneCare safety scanner
  http://onecare.live.com/scan
- Microsoft Exchange Hosted Services
  http://www.microsoft.com/exchange/services/default.mspx
- 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 Online Safety Technologies (anti-spam and anti-phishing)
  http://www.microsoft.com/safety
- Sender ID Framework
  http://www.microsoft.com/senderid