SYMANTEC ENTERPRISE SECURITY

symantec™

Confidence in a connected world.

# Symantec Global Internet Security Threat Report

## Trends for 2008

Volume XIV, Published April 2009

**Marc Fossi**
Executive Editor
Manager, Development
Security Technology and Response

**Eric Johnson**
Editor
Security Technology and Response

**Trevor Mack**
Associate Editor
Security Technology and Response

**Dean Turner**
Director, Global Intelligence Network
Security Technology and Response

**Joseph Blackbird**
Threat Analyst
Symantec Security Response

**Mo King Low**
Threat Analyst
Security Technology and Response

**Teo Adams**
Threat Analyst
Security Technology and Response

**David McKinney**
Threat Analyst
Security Technology and Response

**Stephen Entwisle**
Threat Analyst
Security Technology and Response

**Marika Pauls Laucht**
Threat Analyst
Security Technology and Response

**Candid Wueest**
Threat Analyst
Security Technology and Response

**Paul Wood**
Senior Analyst
MessageLabs Intelligence, Symantec

**Dan Bleaken**
Threat Analyst
MessageLabs Intelligence, Symantec

**Greg Ahmad**
Threat Analyst
Security Technology and Response

**Darren Kemp**
Threat Analyst
Security Technology and Response

**Ashif Samnani**
Threat Analyst
Security Technology and Response

Volume XIV, Published April 2009

# Symantec Global Internet Security Threat Report

## Contents

Introduction . . . . 4

Executive Summary . . . . 5

Highlights . . . . 13

Threat Activity Trends . . . . 17

Vulnerability Trends . . . . 35

Malicious Code Trends . . . . 55

Phishing, Underground Economy Servers, and Spam Trends . . . . 73

Appendix A—Symantec Best Practices . . . . 93

Appendix B—Threat Activity Trends Methodology . . . . 95

Appendix C—Vulnerability Trends Methodology . . . . 97

Appendix D—Malicious Code Trends Methodology . . . . 104

Appendix E—Phishing, Underground Economy Servers, and Spam Trends Methodology . . . . 105

## Introduction

The Symantec *Global Internet Security Threat Report* provides an annual overview and analysis of worldwide Internet threat activity, a review of known vulnerabilities, and highlights of malicious code. Trends in phishing and spam are also assessed, as are observed activities on underground economy servers. Previously presented every six months, this volume of the Symantec *Global Internet Security Threat Report* will alert readers to trends and impending threats that Symantec has observed for 2008.

Symantec has established some of the most comprehensive sources of Internet threat data in the world through the Symantec™ Global Intelligence Network. More than 240,000 sensors in over 200 countries monitor attack activity through a combination of Symantec products and services such as Symantec DeepSight™ Threat Management System, Symantec Managed Security Services and Norton™ consumer products, as well as additional third-party data sources.

Symantec also gathers malicious code intelligence from more than 130 million client, server, and gateway systems that have deployed its antivirus products. Additionally, Symantec's distributed honeypot network collects data from around the globe, capturing previously unseen threats and attacks and providing valuable insight into attacker methods.

Symantec maintains one of the world's most comprehensive vulnerability databases, currently consisting of more than 32,000 recorded vulnerabilities (spanning more than two decades) affecting more than 72,000 technologies from more than 11,000 vendors. Symantec also facilitates the BugTraq™ mailing list, one of the most popular forums for the disclosure and discussion of vulnerabilities on the Internet, which has approximately 50,000 subscribers who contribute, receive, and discuss vulnerability research on a daily basis.

Spam and phishing data is captured through a variety of sources including: the Symantec Probe Network, a system of more than 2.5 million decoy accounts; MessageLabs Intelligence, a respected source of data and analysis for messaging security issues, trends and statistics; and other Symantec technologies. Data is collected in more than 86 countries from around the globe. Over eight billion email messages, as well as over one billion Web requests are processed per day across 16 data centers. Symantec also gathers phishing information through an extensive antifraud community of enterprises, security vendors and more than 50 million consumers.

These resources give Symantec's analysts unparalleled sources of data with which to identify, analyze, and provide informed commentary on emerging trends in attacks, malicious code activity, phishing, and spam. The result is the Symantec *Global Internet Security Threat Report*, which gives enterprises and consumers the essential information to effectively secure their systems now and into the future.

## Executive Summary

The Symantec *Internet Security Threat Report* consists primarily of four reports: the *Global Internet Security Threat Report*; the *EMEA Internet Security Threat Report*, for the Europe, the Middle East, and Africa (EMEA) region; the *APJ Internet Security Threat Report*, for the Asia-Pacific/Japan (APJ) region; and the *Government Internet Security Threat Report*, which focuses on threats of specific interest to governments and critical infrastructure sectors. Together, these reports provide a detailed overview and analysis of Internet threat activity, malicious code, and known vulnerabilities. Trends in phishing and spam are also assessed, as are observed activities on underground economy servers.

This summary will discuss current trends, impending threats, and the continuing evolution of the Internet threat landscape based on data for 2008 discussed within the four reports. This summary will also discuss how regional differences can affect malicious activity globally.

There are a number of trends noted in previous volumes of the Symantec *Internet Security Threat Report* that continued in 2008: malicious activity has increasingly become Web-based; attackers are targeting end users instead of computers; the online underground economy has consolidated and matured; and attackers are able to rapidly adapt their attack activities.[1]

Symantec recently examined these trends along with the continued consolidation of malicious activities in the online underground economy in the Symantec *Report on the Underground Economy*.[2] That report found that the underground economy is geographically diverse and able to generate millions of dollars in revenue for (often) well-organized groups. The underground economy is also increasingly becoming a self-sustaining system where tools specifically developed to facilitate fraud and theft are freely bought and sold. These tools are then used for information theft that may then be converted into profit to fund the development of additional tools.

Based on the data and discussions presented in the current Symantec *Internet Security Threat Report*, this summary will examine the primary methods being used to compromise end users and organizations, who is generating these attacks, and what these attackers are after. Finally, this summary will look at emerging trends that Symantec believes will become prevalent in the immediate future.

### How users are being compromised

Web-based attacks are now the primary vector for malicious activity over the Internet. The continued growth of the Internet and the number of people increasingly using it for an extensive array of activities presents attackers with a growing range of targets as well as various means to launch malicious activity.[3] Within this activity, Symantec has noted that most Web-based attacks are launched against users who visit legitimate websites that have been compromised by attackers in order to serve malicious content.

Some of the common techniques used by attackers to compromise a website include exploiting a vulnerable Web application running on the server (by attacking through improperly secured input fields), or exploiting some vulnerability present in the underlying host operating system. In 2008 alone, there were 12,885 site-specific vulnerabilities identified (figure 1) and 63 percent of vulnerabilities documented by Symantec affected Web applications. Attackers can exploit these vulnerabilities in a website or underlying application to modify the pages served to users visiting the site. This can include directly serving malicious

[1] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_exec_summary_internet_security_threat_report_xiii_04-2008.en-us.pdf
[2] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_underground_economy_report_11-2008-14525717.en-us.pdf
[3] http://www.verisign.com/static/043939.pdf

content from the site itself, or embedding a malicious iframe on pages that can redirect a user's browser to another Web server that is under the attacker's control.[4] In this way, the compromise of a single website can cause attacks to be launched against every visitor to that site.

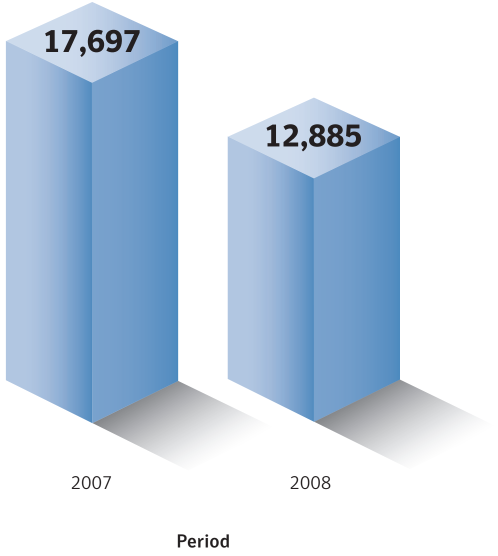

**Figure 1. Site-specific vulnerabilities**
*Source: Based on data provided by the XSSed Project*[5]

In the case of a popular, trusted site with a large number of visitors, this can yield thousands of compromises from a single attack. For example, one attack that targeted the websites of both the United Nations and the UK government, among others, injected malicious code that was designed to load content from an attacker-controlled location into visitors' browsers.[6] Another separate attack successfully defaced the national Albanian postal service website.[7] These types of attacks provide an optimal beachhead for distributing malicious code because they target high-traffic websites of reputable organizations.

In order to compromise the largest possible number of websites with a single mechanism, attackers will attempt to compromise an entire class of vulnerability by searching for commonalities within them and generically automating their discovery and exploitation. This allows attackers to compromise websites with the efficiency commonly found in network worms.

The lengthy and complicated steps being pursued to launch successful Web-based attacks also demonstrate the increasing complexity of the methods used by attackers. While a single high-severity flaw can be exploited to fully compromise a user, attackers are now frequently stringing together multiple exploits for medium-severity vulnerabilities to achieve the same goal. An indication of this is that eight of the top 10 vulnerabilities exploited in 2008 were rated as medium severity.

[4] An iframe is an HTML element that can include Web content from other pages or Web servers to be rendered when the user visits the original page. This tag can be constructed so that it is effectively invisible and the user will not see any of the embedded content when viewing the original page.
[5] Data was provided by the XSSed Project, a site devoted to tracking and verifying reports of site-specific cross-site scripting vulnerabilities: http://www.xssed.com.
[6] http://news.cnet.com/8301-10789_3-9925637-57.html
[7] http://albmasters.com/?p=3

Many enterprises and end users will often make patching high-severity vulnerabilities a top priority, while medium- and low-severity vulnerabilities may be ignored. This could result in the possibility of more computers remaining exposed for longer periods to these vulnerabilities. For example, of the 12,885 site-specific cross-site scripting vulnerabilities identified by Symantec in 2008, only 394 (3 percent) are known by Symantec to have been fixed.[8]

These developments and trends indicate that Web-based threats have not only become widespread, but that they have also increased in sophistication. In particular, Symantec has noticed that some botnets (such as Asprox,[9] which was initially used for phishing scams) are being redesigned to specifically exploit cross-site scripting vulnerabilities in order to inject malicious code into compromised websites.[10]

In many cases, medium-severity vulnerabilities are sufficient to mount successful attacks if attackers are able to execute arbitrary code and perform actions such as accessing confidential information or making network connections. This is made possible because many end users do not require administrative privileges to run or modify the targeted applications. While the danger of client-side vulnerabilities may be limited by best practices, such as restricting Web applications at the administrative level, this is often unrealistic given how integral Web applications are to the delivery of content for many businesses. Medium-severity vulnerabilities affecting client or desktop applications are often sufficient for an attacker to mount successful malicious attacks on individual end users as well as at the enterprise level.

That said, however, a single high-severity vulnerability was the top attacked flaw in 2008. Previous editions of the Symantec *Internet Security Threat Report* noted that there has been a decrease in the volume of network worms, partly due to a lack of easily exploitable remote vulnerabilities in default operating system components. Many network worms exploited such vulnerabilities in order to propagate. Highly successful worms—such as CodeRed,[11] Nimda,[12] and Slammer[13]—all exploited high-severity vulnerabilities in remotely accessible services to spread. These worms prompted changes in security measures, such as the inclusion of personal firewall applications in operating systems that are turned on by default. This helped protect users from most network worms, even if the vulnerability being exploited was not immediately patched.

The high-severity vulnerability in question was a zero-day vulnerability that was discovered in late 2008 in the Microsoft® Windows® Server® Service RPC Handling component that allowed remote code execution.[14] Because remote communication with this service is allowed through the Windows firewall when file and print sharing is turned on, many users would have to apply the patch to be protected from exploitation attempts. Soon after, a new worm called Downadup (also known as Conficker) emerged that exploited this vulnerability.[15] Downadup was able to spread rapidly, partially due to its advanced propagation mechanisms and its ability to spread through removable media devices.[16] By the end of 2008 there were well over a million individual computers infected by Downadup. Once Downadup has infected a computer, it uses a Web or peer-to-peer (P2P) update mechanism to download updated versions of itself, or to install other malicious code onto the compromised computer.

[8] For the purpose of this report, the term cross-site scripting encapsulates two broad classes of vulnerability; this includes traditional cross-site scripting and a category known as HTML injection (or persistent cross-site scripting).
[9] http://www.symantec.com/security_response/writeup.jsp?docid=2007-060812-4603-99
[10] http://www.messagelabs.com/mlireport/MLIReport_Annual_2008_FINAL.pdf : p. 33
[11] http://www.symantec.com/security_response/writeup.jsp?docid=2001-071911-5755-99
[12] http://www.symantec.com/security_response/writeup.jsp?docid=2001-091816-3508-99
[13] http://www.symantec.com/security_response/writeup.jsp?docid=2003-012502-3306-99
[14] http://www.securityfocus.com/bid/31874
[15] http://www.symantec.com/security_response/writeup.jsp?docid=2008-112203-2408-99
[16] https://forums2.symantec.com/t5/Malicious-Code/Downadup-Attempts-at-Smart-Network-Scanning/ba-p/382114 - A233

Downadup has been particularly prolific in the APJ and Latin America (LAM) regions.[17] These regions are also where some of the highest software piracy rates are recorded.[18] Because pirated versions of software are frequently unable to use automated update mechanisms for security patches (in case they are detected and disabled), it is likely many computers in these two regions have not been patched against Downadup. Software piracy rates are often high in many emerging markets with rapidly growing Internet and broadband infrastructures.[19]

From the data gathered for this reporting period, Symantec has also noted other significant malicious activities occurring in countries with rapidly emerging Internet infrastructures. For example, while the United States is still home to a large amount of threat activity and continues to be the top ranked country for malicious activity—mainly due to its extensive broadband penetration and significantly developed Internet infrastructure—Symantec has noted a steady increase in malicious activity in countries not previously associated with such activities. One result of this trend is that these countries can appeal to attackers as potential bases for hosting phishing websites, spam relays, and other malicious content, possibly because rapidly growing ISPs in these areas may have difficulty monitoring and filtering the growing volume of traffic across their networks.

Attackers are also organized enough to implement contingency plans in case their activities are detected. By relocating their activities to a variety of countries, attackers can minimize the chances of being partially or completely shut down. This is demonstrated by events after the shutdown of a U.S.-based ISP toward the end of 2008.[20] It seems that the bot controllers generating much of the attack activity from this ISP had alternative hosting plans.[21] As a result, although Symantec noted a significant drop in malicious activity after the shutdown, particularly in spam, the numbers returned to previous levels soon afterward. It became apparent that the botnet controllers had been able to successfully relocate enough of their bot command-and-control (C&C) servers to other hosts, and were thus able to rebuild their botnets back up to previous numbers. Given that the affected botnets were three of the world's largest, it is not surprising that new locations were quickly found to host these servers due to the significant profits such botnets are able to generate.

## What attackers want

More than ever before, attackers are concentrating on compromising end users for financial gain. In 2008, 78 percent of confidential information threats exported user data, and 76 percent used a keystroke-logging component to steal information such as online banking account credentials. Additionally, 76 percent of phishing lures targeted brands in the financial services sector (figure 2) and this sector also had the most identities exposed due to data breaches. Similarly, 12 percent of all data breaches that occurred in 2008 exposed credit card information. In 2008 the average cost per incident of a data breach in the United States was $6.7 million[22]—which is an increase of 5 percent from 2007—and lost business amounted to an average of $4.6 million.[23]

[17] https://forums2.symantec.com/t5/Malicious-Code/Downadup-Geo-location-Fingerprinting-and-Piracy/ba-p/380993 - A228
[18] http://arstechnica.com/old/content/2008/01/bsa-piracy-economic-impact-is-tens-of-billions-of-dollars.ars
[19] http://findarticles.com/p/articles/mi_m0EIN/is_2008_May_14/ai_n25411795
[20] http://eval.symantec.com/mktginfo/enterprise/other_resources/b-state_of_spam_report_12-2008.en-us.pdf : p. 7
[21] http://www.theregister.co.uk/2008/11/18/short_mccolo_resurrection/
[22] All figures are in U.S. dollars unless otherwise noted.
[23] http://www.encryptionreports.com/download/Ponemon_COB_2008_US_090201.pdf

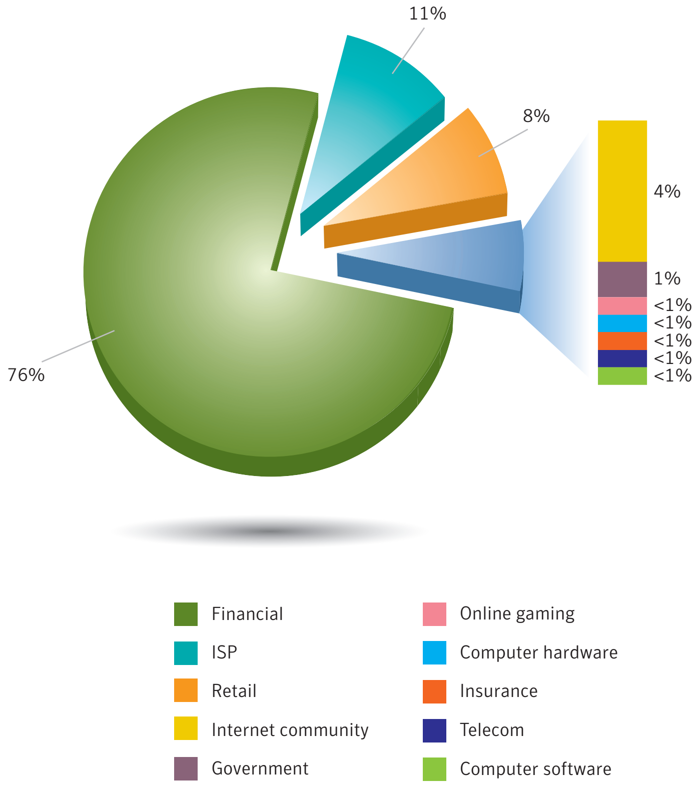

**Figure 2. Phished sectors by volume of phishing lures**
*Source: Symantec Corporation*

Once attackers have obtained financial information or other personal details—such as names, addresses, and government identification numbers—they frequently sell that data on the underground economy.[24] The most popular item for sale on underground economy servers in 2008 was credit card information, accounting for 32 percent of the total (table 1). This is likely due to the fact that there are numerous ways for credit card information to be stolen, and that stolen card data can be easily cashed out. This is because the underground economy has a well-established infrastructure for monetizing such information, again indicating the increased sophistication of the underground economy. Also, because of the large quantity of credit card numbers available, the price for each card can be as low as 6 cents when they are purchased in bulk. Some groups in the underground economy also specialize in manufacturing blank plastic cards with magnetic stripes destined to be encoded with stolen credit card and bankcard data. The manufacture and distribution of these cards requires a well-organized level of sophistication since the cards are often produced in one country, imprinted, and then shipped to the countries from where the stolen data originated.

[24] The underground economy comprises various forums, such as websites and Internet Relay Chat (IRC) channels, which allow criminals to buy, sell, and trade illicit goods and services. For more information see: http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_underground_economy_report_11-2008-14525717.en-us.pdf

| 2008 Rank | 2007 Rank | Item | 2008 Percentage | 2007 Percentage | Range of Prices |
|---|---|---|---|---|---|
| 1 | 1 | Credit card information | 32% | 21% | $0.06–$30 |
| 2 | 2 | Bank account credentials | 19% | 17% | $10–$1000 |
| 3 | 9 | Email accounts | 5% | 4% | $0.10–$100 |
| 4 | 3 | Email addresses | 5% | 6% | $0.33/MB–$100/MB |
| 5 | 12 | Proxies | 4% | 3% | $0.16–$20 |
| 6 | 4 | Full identities | 4% | 6% | $0.70–$60 |
| 7 | 6 | Mailers | 3% | 5% | $2–$40 |
| 8 | 5 | Cash out services | 3% | 5% | 8%–50% or flat rate of $200–$2000 per item |
| 9 | 17 | Shell scripts | 3% | 2% | $2–$20 |
| 10 | 8 | Scams | 3% | 5% | $3–$40/week for hosting, $2–$20 design |

**Table 1. Goods and services available for sale on underground economy servers**
*Source: Symantec*

One result that Symantec has drawn from the observance of increased professionalization in the underground economy is that the coordination of specialized and, in some cases, competitive groups for the production and distribution of items such as customized malicious code and phishing kits has led to a dramatic increase in the general proliferation of malicious code. In 2008, Symantec detected 1,656,227 malicious code threats (figure 3). This represents over 60 percent of the approximately 2.6 million malicious code threats that Symantec has detected in total over time.

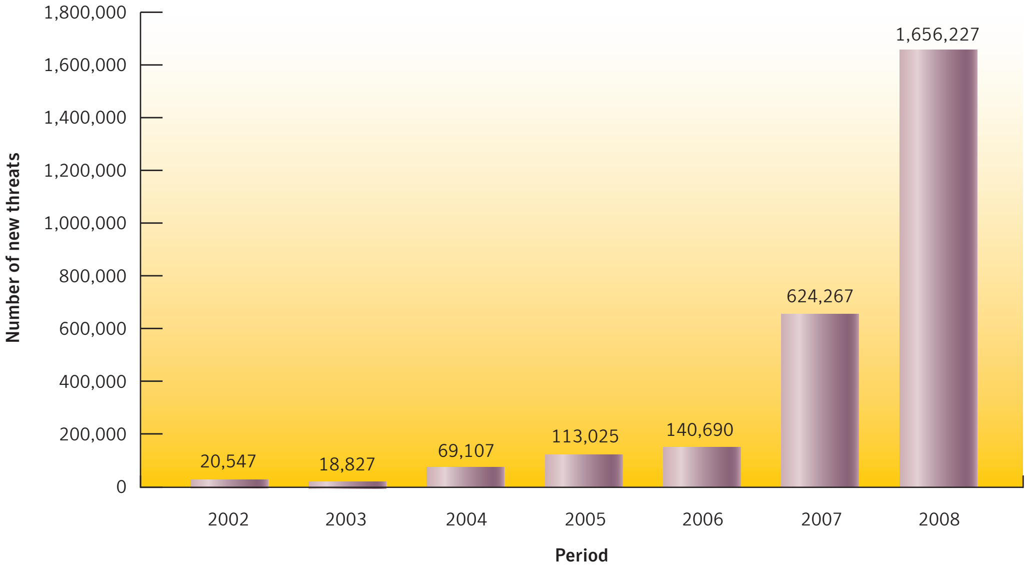

**Figure 3. New malicious code threats**
*Source: Symantec*

A prime example of this type of underground professional organization is the Russian Business Network (RBN). The RBN reputedly specializes in the distribution of malicious code, hosting malicious websites, and other malicious activity. The RBN has been credited with creating approximately half of the phishing incidents that occurred worldwide last year. It is also thought to be associated with a significant amount of the malicious activities on the Internet in 2007.

Since that time there have been two significant cases of ISPs that were shut down because of malicious activity. These ISPs were hosting malicious code, phishing websites, bot C&C servers, and spam relays. This includes the instance noted above, when Symantec saw a 65 percent drop in spam and a 30 percent decrease in bot activity within 24 hours of one particular ISP being taken offline.[25] While it may seem remarkable that the shutdown of a single ISP can result in such drastic decreases in malicious activity within a short time period, as noted, malicious activity is increasingly organized and attackers are now readily prepared for contingencies that might affect their operations. Much of the malicious activity was simply shifted to other locations. In this instance, the ISP even resurfaced briefly to afford the group an opportunity to update the botnets under their control.[26]

In this increasingly sophisticated Internet threat landscape, there is a growing impetus for greater cooperation to address the high degree of organization of groups creating threats on the Internet. This was demonstrated by the aggressive spread of the Downadup worm in the latter months of 2008 and into 2009. Due to its multiple propagation mechanisms, the worm was able to spread rapidly. More worrisome is the fact that the worm contains an update mechanism that could allow new versions of the worm or other threats, such as a bot, to be installed on compromised computers. To combat its rapid spread and aggressive profile, a coalition was formed by stakeholders involved in Internet security.[27] The success of this coalition of identifying how the worm operates, slowing its growth, and limiting its potential danger demonstrates the benefits of increased cooperation among Internet security stakeholders.

## Conclusion

Changes in the current threat landscape—such as the increasing complexity and sophistication of attacks, the evolution of attackers and attack patterns, and malicious activities being pushed to emerging countries—show not just the benefits of, but also the need for increased cooperation among security companies, governments, academics, and other organizations and individuals to combat these changes. Symantec expects malicious activity to continue to be pushed to regions with emerging infrastructures that may still lack the resources to combat the growing involvement of organized crime in the online underground economy. The onus will be on organizations, institutions, and other knowledgeable groups to come together for the benefit of the affected regions. Internet threat activity is truly global, and malicious activity allowed to flourish in one area could quickly spread worldwide.

With the increasing adaptability of malicious code developers and their ability to evade detection, Symantec also expects that overt attack activities will either be abandoned or pushed further underground. For example, if the effort to set up malicious ISPs outweighs the return for attackers before being taken offline, it is likely that attackers will abandon this approach for other attack vectors in order to continue to evade detection and potential apprehension or prosecution. This has already been seen with the use of

[25] Cf. http://eval.symantec.com/mktginfo/enterprise/other_resources/b-state_of_spam_report_12-2008.en-us.pdf : p. 7
and http://www.messagelabs.com/mlireport/MLIReport_Annual_2008_FINAL.pdf : p. 26
[26] http://www.pcworld.com/businesscenter/article/154554/spammers_regaining_control_over_srizbi_botnet.html
[27] https://forums2.symantec.com/t5/Malicious-Code/Coalition-Formed-in-Response-to-W32-Downadup/ba-p/388129 - A241

HTTP and P2P communication channels in threats such as Downadup. Because of the distributed nature of these control channels, it is much more difficult to disable an entire network and locate the individual or group behind the attacks.

The large increase in the number of new malicious code threats, coupled with the use of the Web as a distribution mechanism, also demonstrates the growing need for more responsive and cooperative security measures. While antivirus signature scanning, heuristic detection, and intrusion prevention continue to be vital for the security of organizations as well as end users, newer technologies, such as reputation-based security, will become increasingly important.

The focus of threats in 2008 continued to be aimed at exploiting end users for profit, and attackers have continued to evolve and refine their abilities for online fraud. While some criminal groups have come and gone, other large organizations persist and continue to consolidate their activities. These pseudo-corporations and their up-and-coming competitors will likely remain at the forefront of malicious activity in the coming year.

## Highlights

This section provides highlights of the security trends that Symantec observed in 2008 based on the data gathered from the sources listed in the introduction to this report. Selected metrics will be discussed in greater depth in the sections that follow.

### *Threat Activity Trends Highlights*

- During this reporting period, 23 percent of all malicious activity measured by Symantec in 2008 was located in the United States; this is a decrease from 26 percent in 2007.
- The United States was the top country of attack origin in 2008, accounting for 25 percent of worldwide activity; this is a decrease from 29 percent in 2007.
- The education sector accounted for 27 percent of data breaches that could lead to identity theft during this period, more than any other sector and a slight increase from 26 percent in 2007.
- The financial sector was the top sector for identities exposed in 2008, accounting for 29 percent of the total and an increase from 10 percent in 2007.
- In 2008, the theft or loss of a computer or other data-storage devices accounted for 48 percent of data breaches that could lead to identity theft and for 66 percent of the identities exposed.
- Symantec observed an average of 75,158 active bot-infected computers per day in 2008, an increase of 31 percent from the previous period.
- China had the most bot-infected computers in 2008, accounting for 13 percent of the worldwide total; this is a decrease from 19 percent in 2007.
- Buenos Aires was the city with the most bot-infected computers in 2008, accounting for 4 percent of the worldwide total.
- In 2008, Symantec identified 15,197 distinct new bot command-and-control servers; of these, 43 percent operated through IRC channels and 57 percent used HTTP.
- The United States was the location for the most bot command-and-control servers in 2008, with 33 percent of the total, more than any other country.
- The top Web-based attack in 2008 was associated with the Microsoft Internet Explorer® ADODB.Stream Object File Installation Weakness vulnerability, which accounted for 30 percent of the total.
- The United States was the top country of origin for Web-based attacks in 2008, accounting for 38 percent of the worldwide total.
- The United States was the country most frequently targeted by denial-of-service attacks in 2008, accounting for 51 percent of the worldwide total.

### *Vulnerability Trends Highlights*

- Symantec documented 5,491 vulnerabilities in 2008; this is a 19 percent increase over the 4,625 vulnerabilities documented in 2007.
- Two percent of vulnerabilities in 2008 were classified as high severity, 67 percent as medium severity, and 30 percent as low severity.[28] In 2007, 4 percent of vulnerabilities were classified as high severity, 61 percent as medium severity, and 35 percent as low severity.
- Eighty percent of documented vulnerabilities were classified as easily exploitable in 2008; this is an increase from 2007, when 74 percent of documented vulnerabilities were classified as easily exploitable.
- Of any browser analyzed in 2008, Apple® Safari® had the longest window of exposure (the time between the release of exploit code for a vulnerability and a vendor releasing a patch), with a nine-day average; Mozilla® browsers had the shortest window of exposure in 2008, averaging less than one day.
- Mozilla browsers were affected by 99 new vulnerabilities in 2008, more than any other browser; there were 47 new vulnerabilities identified in Internet Explorer, 40 in Apple Safari, 35 in Opera™, and 11 in Google® Chrome.[29]
- There were 415 browser plug-in vulnerabilities identified in 2008, fewer than the 475 identified in 2007. ActiveX® technologies still constituted the majority of new browser plug-in vulnerabilities, with a total of 287; however, this is substantially down from the 399 ActiveX vulnerabilities identified in 2007.
- Memory corruption vulnerabilities again made up the majority of the type of vulnerabilities in browser plug-in technologies for 2008, with 271 vulnerabilities classified as such.
- In 2008, 63 percent of vulnerabilities affected Web applications, an increase from 59 percent in 2007.
- During 2008, there were 12,885 site-specific cross-site scripting vulnerabilities identified, compared to 17,697 in 2007; of the vulnerabilities identified in 2008, only 3 percent (394 vulnerabilities) had been fixed at the time of writing.
- In 2008, Symantec documented nine zero-day vulnerabilities, compared to 15 in 2007.
- The top attacked vulnerability for 2008 was the Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability.
- In 2008, 95 percent of attacked vulnerabilities were client-side vulnerabilities and 5 percent were server-side vulnerabilities, compared to 93 percent and 7 percent, respectively, in 2007.

[28] Percentages are rounded off to the closest whole number and percentages may not equal 100 percent in some instances.
[29] Google Chrome was released in September 2008.

### *Malicious Code Trends Highlights*

- In 2008, the number of new malicious code signatures increased by 265 percent over 2007; over 60 percent of all currently detected malicious code threats were detected in 2008.
- Of the top 10 new malicious code families detected in 2008, three were Trojans, three were Trojans with a back door component, two were worms, one was a worm with a back door component, and one was a worm with back door and virus components.
- Trojans made up 68 percent of the volume of the top 50 malicious code samples reported in 2008, a minor decrease from 69 percent in 2007.
- Five of the top 10 staged downloaders in 2008 were Trojans, two were Trojans that incorporated a back door component, one was a worm, one of was a worm that incorporated a back door, and one was a worm that incorporated a virus component.
- In 2008, the proportional increase of potential malicious code infections was greatest in the Europe, the Middle East and Africa region.
- The percentage of threats to confidential information that incorporate remote access capabilities declined to 83 percent in 2008; this is a decrease from 91 percent in 2007, although such threats remained the most prevalent exposure type.
- In 2008, 78 percent of threats to confidential information exported user data and 76 percent had a keystroke-logging component; these are increases from 74 percent and 72 percent, respectively, in 2007.
- Propagation through executable file sharing continued to increase in 2008, accounting for 66 percent of malicious code that propagates—up from 44 percent in 2007.
- One percent of the volume of the top 50 malicious code samples modified Web pages in 2008, down from 2 percent in 2007.
- The percentage of documented malicious code samples that exploit vulnerabilities declined substantially, from 13 percent in 2007 to 3 percent in 2008.
- In 2008, eight of the top 10 downloaded components were Trojans, one was a Trojan with a back door component, and one was a back door.
- Malicious code that targets online games accounted for 10 percent of the volume of the top 50 potential malicious code infections, up from 7 percent in 2007.

***Phishing, Underground Economy Servers, and Spam Trends Highlights***

- The majority of brands used in phishing attacks in 2008 were in the financial services sector, accounting for 79 percent, down slightly from 83 percent identified in 2007.
- The financial services sector accounted for the highest volume of phishing lures during this period, with 76 percent of the total; this is considerably higher than 2007, when the volume for financial services was 52 percent.
- In 2008, Symantec detected 55,389 phishing website hosts, an increase of 66 percent over 2007, when Symantec detected 33,428 phishing hosts.
- In 2008, 43 percent of all phishing websites identified by Symantec were located in the United States, considerably less than 2007, when 69 percent of such sites were based there.
- The most common top-level domain used in phishing lures detected in 2008 was .com, accounting for 39 percent of the total; it was also the highest ranking top-level domain in 2007, when it accounted for 46 percent of the total.
- One particular automated phishing toolkit identified by Symantec was responsible for an average of 14 percent of all phishing attacks during 2008.
- Credit card information was the most commonly advertised item for sale on underground economy servers known to Symantec, accounting for 32 percent of all goods and services; this is an increase from 2007 when credit card information accounted for 21 percent of the total.
- The United States was the top country for credit cards advertised on underground economy servers, accounting for 67 percent of the total; this is a decrease from 2007 when it accounted for 83 percent of the total.
- The most common type of spam detected in 2008 was related to Internet- or computer-related goods and services, which made up 24 percent of all detected spam; in 2007, this was the second most common type of spam, accounting for 19 percent of the total.
- Symantec observed a 192 percent increase in spam detected across the Internet, from 119.6 billion messages in 2007 to 349.6 billion in 2008.
- In 2008, 29 percent of all spam recorded by Symantec originated in the United States, a substantial decrease from 45 percent in 2007, when the United States was also the top ranked country of origin.
- In 2008, bot networks were responsible for the distribution of approximately 90 percent of all spam email.

## Threat Activity Trends

This section of the Symantec *Global Internet Security Threat Report* will provide an analysis of threat activity, as well as other malicious activity, data breaches, and Web-based attacks that Symantec observed in 2008. The malicious activity discussed in this section not only includes threat activity, but also phishing, malicious code, spam zombies, bot-infected computers, and bot C&C server activity. Attacks are defined as any malicious activity carried out over a network that has been detected by an intrusion detection system (IDS) or firewall. Definitions for the other types of malicious activities can be found in their respective sections within this report.

This section will discuss the following metrics, providing analysis and discussion of the trends indicated by the data:

- Malicious activity by country
- Data breaches that could lead to identity theft by sector
- Data breaches that could lead to identity theft by cause
- Bot-infected computers
- Bot command-and-control servers
- Top Web-based attacks
- Top countries of origin for Web-based attacks
- Threat activity—protection and mitigation

### Malicious activity by country

This metric will assess the countries in which the largest amount of malicious activity takes place or originates. To determine this, Symantec has compiled geographical data on numerous malicious activities, including: bot-infected computers, phishing website hosts, malicious code reports, spam zombies, and attack origin. The rankings are determined by calculating the mean average of the proportion of these malicious activities that originated in each country.

Malicious activity usually affects computers that are connected to high-speed broadband Internet because these connections are attractive targets for attackers. Broadband connections provide larger bandwidth capacities than other connection types, faster speeds, the potential of constantly connected systems, and typically more stable connections. The top three countries in this metric—the United States, China, and Germany—all have extensively developed and growing broadband infrastructures.[30] China, which passed the United States for the largest number of broadband subscribers for the first time in 2008, has 21 percent of the worldwide broadband subscriber total with 83.3 million subscribers. The United States is second with 20 percent, while Germany is fourth with 6 percent. Each country also experienced a growth of over 20 percent in broadband subscribers from 2007.

In 2008, the United States was the top country for overall malicious activity, making up 23 percent of the total (table 2). This is a decrease from 2007 when the United States was also first, with 26 percent. Within specific category measurements, the United States ranked first in malicious code, phishing website hosts, and attack origin.

[30] http://www.point-topic.com

| 2008 Rank | 2007 Rank | Country | 2008 Overall Percentage | 2007 Overall Percentage | Malicious Code Rank | Spam Zombies Rank | Phishing Websites Host Rank | Bot Rank | Attack Origin Rank |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | United States | 23% | 26% | 1 | 3 | 1 | 2 | 1 |
| 2 | 2 | China | 9% | 11% | 2 | 4 | 6 | 1 | 2 |
| 3 | 3 | Germany | 6% | 7% | 12 | 2 | 2 | 4 | 4 |
| 4 | 4 | United Kingdom | 5% | 4% | 4 | 10 | 5 | 9 | 3 |
| 5 | 8 | Brazil | 4% | 3% | 16 | 1 | 16 | 5 | 9 |
| 6 | 6 | Spain | 4% | 3% | 10 | 8 | 13 | 3 | 6 |
| 7 | 7 | Italy | 3% | 3% | 11 | 6 | 14 | 6 | 8 |
| 8 | 5 | France | 3% | 4% | 8 | 14 | 9 | 10 | 5 |
| 9 | 15 | Turkey | 3% | 2% | 15 | 5 | 24 | 8 | 12 |
| 10 | 12 | Poland | 3% | 2% | 23 | 9 | 8 | 7 | 17 |

**Table 2. Malicious activity by country**
*Source: Symantec*

The slight decrease in overall malicious activity for the United States can be attributed to the drop in spam zombies there. This is likely due to the shutdown of two U.S.-based Web hosting companies that were allegedly hosting a large number of bot C&C servers associated with spam distribution bot networks (botnets).[31] Spam activity decreased worldwide after both shutdowns. In one case, Symantec observed a 65 percent decrease in spam traffic in the 24 hours that followed.[32] Both companies allegedly hosted a large number of bot C&C servers for several large spam botnets: Srizbi,[33] Rustock,[34] and Ozdok (Mega-D).[35] Spam zombies that lack a critical command system are unable to send out spam.

China had the second highest amount of overall worldwide malicious activity in 2008, accounting for 9 percent; this is a decrease from 11 percent in the previous reporting period. Along with the fact that China has the most broadband subscribers in the world, the amount of time spent online by users there could contribute to the high percentage of malicious activity in China. The longer a user is online, the longer the computer is exposed to malicious attack or compromise, and Internet users in China spend more of their leisure time online than users in any other country.[36] Online leisure activities are also typically more likely to include activities on sites that may be vulnerable to attacks. This includes social networking websites, online gaming sites, forums, blogs, and online shopping sites. Dynamic sites, such as forums, for example, are prime targets for attackers using bot-infected computers to propagate and host malicious content since Web application and site-specific vulnerabilities can put these types of site at risk.

The slight drop in China's percentage of malicious activity in 2008 was mainly due to the drop in phishing website hosts and bot-infected computers. China dropped from third for phishing website hosts in 2007 to sixth in 2008, with just under 3 percent of the global total; and, although China maintained its top ranking for bot-infected computers, its global share in this regard decreased from 19 percent in 2007 to 13 percent in 2008.

One possible cause for the decreases may be national initiatives to block websites potentially most susceptible to fraud in an effort to increase online security for users ahead of the 2008 Beijing Olympic Games. Thousands of websites were either shut down or blacklisted as part of this effort, including a

[31] http://voices.washingtonpost.com/securityfix/2008/10/spam_volumes_plummet_after_atr.html
[32] http://eval.symantec.com/mktginfo/enterprise/other_resources/b-state_of_spam_report_12-2008.en-us.pdf
[33] http://www.symantec.com/security_response/writeup.jsp?docid=2007-062007-0946-99
[34] http://www.symantec.com/security_response/writeup.jsp?docid=2006-011309-5412-99
[35] http://www.symantec.com/security_response/writeup.jsp?docid=2008-021215-0628-99
[36] http://www.tnsglobal.com/_assets/files/TNS_Market_Research_Digital_World_Digital_Life.pdf

substantial number of message forums,[37] which, as noted previously, are popular targets of attack from Web application and site-specific vulnerabilities. Thus, any reduction in the number of bot-infected computers should result in a corresponding drop in other attack activity categories, such as spam zombies, because these are often associated with bot-infected computers. China dropped from third in spam zombies in 2007, with 7 percent of the worldwide total, to fourth and 6 percent in 2008.

Another factor that may have contributed to the lower percentage of bot-infected computers in China in 2008 was that many unlicensed Internet cafés there were also shut down and supervision was tightened on the remaining cafés to help address online security risks associated with the casual use of public computers.[38] Public computers tend to be more susceptible to attacks because of the significant amount of varied traffic on such computer terminals. Public computers are frequently used by a great variety of people for many different activities such as email, online shopping, and gaming. The variety of usage and likelihood that transient users are less aware of—or concerned with—security makes such computers attractive to attackers.

In 2008, Germany again ranked third with 6 percent of all Internet-wide malicious activity, down slightly from 7 percent in 2007. In both years, Germany ranked highly in spam zombies and hosting phishing websites—activities that are often associated with bot networks. In 2008, Germany ranked fourth for bot C&C servers, with 5 percent of the total. This high number of bot C&C servers likely indicates that botnets are prominent in Germany, which would contribute to the high amount of overall malicious activity originating there. Also, spam zombies are often focused in regions with high broadband penetration and bandwidth capacity because these conditions facilitate sending out large amounts of spam quickly.

It is reasonable to expect that the United States, China and Germany will continue to outrank other countries in this measurement as they have done so for the past several reports. Beyond these three, however, countries such as Brazil, Turkey, Poland, India, and Russia are expected to continue to increase their share of overall malicious activity because they all have rapidly growing Internet infrastructures and growing broadband populations.[39] Countries that have a relatively new and growing Internet infrastructure tend to experience increasing levels of malicious activity until security protocols and measures are improved to counter these activities.

### Data breaches that could lead to identity theft, by sector

Identity theft continues to be a high-profile security issue, particularly for organizations that store and manage large amounts of personal information. Based on the most recent information available from 2007, roughly 8.4 million U.S. residents were victims of identity theft, which represents approximately 3 percent of the adult population.[40] Not only can compromises that result in the loss of personal data undermine customer and institutional confidence, result in costly damage to an organization's reputation, and be costly for individuals to recover from the resulting identity theft, they can also be financially costly to organizations. In 2008, the average cost per incident of a data breach in the United States was $6.7 million, an increase of 5 percent from 2007, and lost business amounted to an average of $4.6 million.[41] Also, organizations can be held liable for breaches and losses, which may result in fines or litigation.[42]

[37] See http://www.vnunet.com/vnunet/news/2207878/china-cracks-web-porn and http://english.gov.cn/2008-03/29/content_931872.htm
[38] http://www.theglobeandmail.com/servlet/story/RTGAM.20080212.wgtchina0212/BNStory/Technology/home
[39] http://www.point-topic.com
[40] http://www.privacyrights.org/ar/idtheftsurveys.htm#Jav2007
[41] http://www.encryptionreports.com/download/Ponemon_COB_2008_US_090201.pdf.
[42] http://www.fsa.gov.uk/pages/Library/Communication/PR/2007/021.shtml

Using publicly available data, Symantec has determined the sectors that were most often affected by these breaches and the most common causes of data loss.[43] This discussion will also explore the severity of the breach by measuring the total number of identities exposed to attackers, using the same publicly available data.[44]

It should be noted that some sectors may need to comply with more stringent reporting requirements for data breaches than others. For instance, government organizations are more likely to report data breaches, either due to regulatory obligations or in conjunction with publicly accessible audits and performance reports.[45] Conversely, organizations that rely on consumer confidence may be less inclined to report such breaches for fear of negative consumer, industry, or market reaction. As a result, sectors that are not required or encouraged to report data breaches may be under-represented in this data set.

In 2008, the education sector represented the highest number of known data breaches that could lead to identity theft, accounting for 27 percent of the total (figure 4). This is a slight increase from 2007 when the education sector also ranked first with 26 percent of the total.

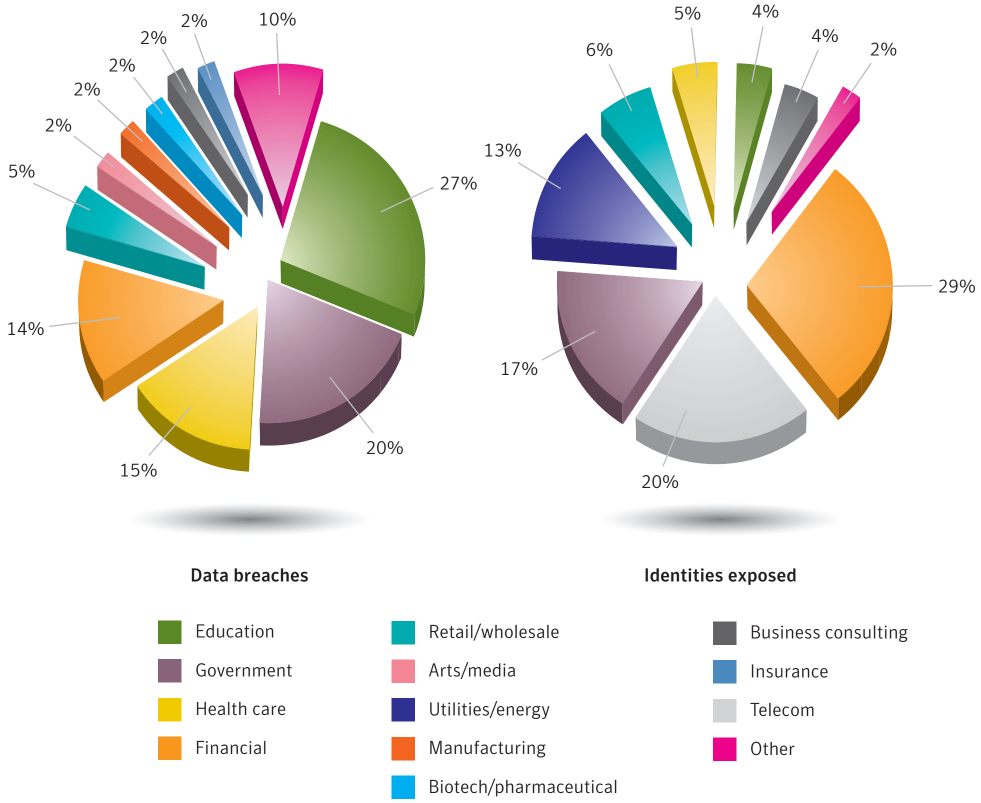

**Figure 4. Data breaches that could lead to identity theft by sector and identities exposed by sector[46]**
*Source: Based on data provided by OSF DataLoss DB*

[43] Open Security Foundation (OSF) Dataloss DB, see http://datalossdb.org
[44] An identity is considered to be exposed if personal or financial data related to the identity is made available through the data breach.
[45] Cf. http://www.privacyrights.org/fs/fs6a-facta.htm and http://www.cms.hhs.gov/HealthPlansGenInfo/12_HIPAA.asp
[46] Due to rounding, percentages might not equal 100 percent.

Educational institutions store a large amount of personal information on students, faculty, and staff that could be used for the purposes of identity theft, including government-issued identification numbers, names, and addresses. Finance departments in these institutions also store bank account information for payroll and may also hold credit card information for people who use this method to pay for tuition and fees. These institutions—particularly larger universities—often consist of many autonomous departments within which sensitive personal identification information may be stored in separate locations and be accessible to many people. This may increase the opportunities for attackers to gain unauthorized access to this data since it may be more difficult to standardize the security, educate everyone with access to the data on the policies, and control access to these dispersed databases.

Despite the high number of data breaches that occurred in the education sector during 2008, it only accounted for 4 percent of all identities exposed during the period and ranked seventh (figure 4). This may be because the educational institutions have relatively smaller databases than those of financial or government institutions and, hence, fewer identities would be exposed in a data breach. One of the largest universities in the United States accounted for less than 80,000 students and employees, while financial and government institutions may store information on millions of people.[47]

Also, one-third of the data breaches in the education sector this period were caused by the theft or loss of computers or data-storage devices. As such, data breaches that occurred in the education sector in this reporting period were not as likely to result in wide-scale identity theft because they resulted in the exposure of fewer identities. These types of breaches only expose the limited amount of data that is stored on the devices.

In 2008, the government sector ranked second and accounted for 20 percent of data breaches that could lead to identity theft. This is a decrease from the previous year, when the government sector represented 23 percent of the total, though still ranking second. This trend is reinforced by the annual Federal Computer Security report card, where the number of government agencies with a failing grade decreased by almost half.[48] The health care sector ranked third in 2008, accounting for 15 percent of data breaches that could lead to identity theft. It also ranked third in 2007, accounting for 14 percent.

Government and health care organizations, like educational institutions, store large amounts of information that could be used for identity theft. Similar to the education sector, these organizations often consist of numerous autonomous departments that store sensitive personal information in separate locations and are accessible to numerous people. As a consequence, these organizations face the same security and control issues as educational institutions. Furthermore, health care organizations store sensitive medical information in addition to personal information, which could result in even more damaging breaches of privacy.

The government sector ranked third for identities exposed during 2008, accounting for 17 percent of the total while the health care sector ranked sixth, accounting for 5 percent of the total. As with the education sector, data breaches within the health care sector resulted in a relatively low number of identities exposed.

[47] http://www.osu.edu/osutoday/stuinfo.php
[48] http://republicans.oversight.house.gov/media/PDFs/Reports/FY2007FISMAReportCard.pdf

## Data breaches that could lead to identity theft, by cause

In 2008, the primary cause of data breaches that could facilitate identity theft was the theft or loss of a computer or other medium on which data is stored or transmitted, such as a USB key or a back-up medium.[49] Theft or loss made up 48 percent of all data breaches in 2008, a decrease from the previous reporting period when it accounted for 52 percent of all reported breaches (figure 5).

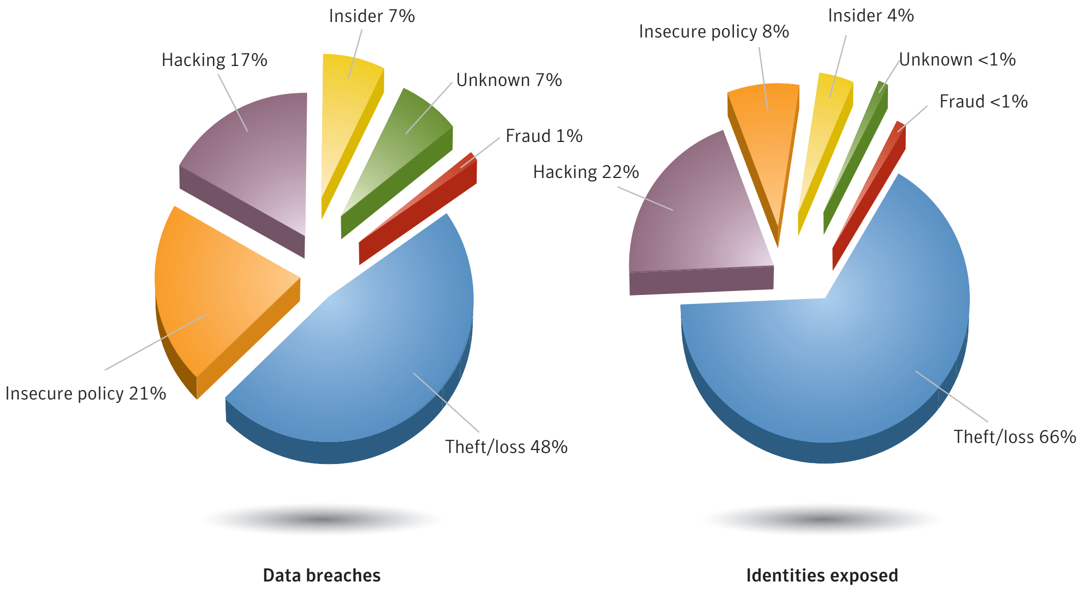

**Figure 5. Data breaches that could lead to identity theft by cause and identities exposed**[50]
*Source: Based on data provided by OSF DataLoss DB*

Theft or loss accounted for 66 percent of all identities exposed in 2008, more than any other cause (figure 5). This was a large increase from 2007, when the number of identities exposed from theft or loss accounted for 24 percent of the total. The main reason for this dramatic increase is that theft or loss was the cause for the three largest breaches that exposed the highest number of identities reported in 2008. These breaches were due to lost or missing disks and exposed personal information relating to an estimated 41 million people.

Although laptops and other storage devices, such as USB memory keys, portable hard drives, and disks, have become smaller, less expensive, and easier to use, their compact size and larger storage capability has increased the opportunity for theft, loss, or misplacement, as well as the potential amount of information breached; a single DVD disk can contain personal information on millions of people. In a recent survey, one in 10 people have lost a laptop, smart phone, or USB flash drive with corporate information stored on it.[51] It may be that the theft of a computer or data-storage device is opportunistic and motivated by the hardware itself and not necessarily its contents, and as such, may not lead to wide-scale identity theft, although there have been cases where information obtained from on a lost disk was discovered in advertisements in the underground economy.

[49] This cause will be referred to as theft or loss for the remainder of the report.
[50] Due to rounding, percentages might not equal 100 percent.
[51] http://www.rsa.com/press_release.aspx?id=9703

To protect against data theft or loss, organizations should restrict the use of outside personal storage devices within their network, monitor the usage of such hardware when permitted, and educate employees on proper usage. Organizations should also include reviews and audits of electronic documents used by employees upon leaving the company. In a recent study, 59 percent of employees admitted to taking company information, such as email addresses, contact information of customers, employee records, and financial records, when leaving the organization.[52] Of these former employees, 79 percent took the information without consent from the company. In 92 percent of the instances, the information was taken on disk, while 73 percent was on removable drives. It is worth noting that only 15 percent of the companies polled had conducted a review or audit of electronic documents taken by employees. Also, sensitive data should be strongly encrypted on any laptop or storage device that may be used outside of the enterprise.

The second most common cause of data breaches that could lead to identity theft during 2008 was insecure policy, which represented 21 percent of all incidents. A data breach is considered to be caused by insecure policy if it can be attributed to a failure to develop, implement, and/or comply with adequate security policy. In 2007, insecure policy also ranked second, accounting for 28 percent of such data breaches. This decrease in the number of data breaches may be due to organizations becoming more diligent and producing stronger security policies such as limiting access to sensitive information to required personnel and the documentation of document transfers. Insecure policy accounted for only 8 percent of exposed identities in 2008 and, thus, each breach exposed only a relatively small number of identities. Although breaches caused by insecure policy in 2008 were not likely to result in wide-scale identity theft, the breaches still exposed approximately 6.5 million identities.[53]

In 2008, hacking was the third leading cause of data breaches that could lead to identity theft, accounting for 17 percent of the total. A data breach is considered to be caused by hacking if data related to identity theft was exposed by attackers external to an organization gaining unauthorized access to computers or networks. Hacking also ranked third in 2007, accounting for 14 percent of breaches that could facilitate identity theft. Hacking is more purpose-driven than insecure policy, theft, or loss: in 2008, over half of the breaches that exposed credit card information were due to hacking. Attackers can take advantage of site-specific and Web-application vulnerabilities to gain access to networks and steal personal information. For this discussion, Symantec considers hacking to be an intentional act with a defined purpose to steal data that can be used for purposes of identity theft or other fraud.

Hacking ranked second for identities exposed in 2008, with 22 percent; this is a large decrease from 2007, when hacking accounted for 62 percent of total identities exposed. The contributing factor for its high ranking in 2007 was a significant data breach in which data on over 94 million credit cards was stolen by attackers hacking into a company's database through unencrypted wireless transmissions and installing programs to capture credit card information.[54] It is estimated that between $63 million and $83 million in credit card fraud across 13 countries can be attributed to this single data breach.[55]

In 2008, two breaches contributed significantly to the high ranking of hacking in this metric: in the first, confidential information on six million Chileans was illegally obtained from government databases by a hacker who publicly posted the information afterward; in the second, credit card information from 4.2 million customers was stolen from a U.S.-based grocery chain by hackers monitoring the credit

[52] http://www.symantec.com/about/news/release/article.jsp?prid=20090223_01
[53] http://datalossdb.org
[54] http://www.msnbc.msn.com/id/21454847/
[55] http://www.securityfocus.com/news/11493

authorization process.[56] Because of the motivation of attackers who use hacking to steal personal financial information, the impact of data breaches due to hacking are severe because they are likely to result in large-scale fraud and high financial cost to affected organizations, credit card issuers, and consumers.

Even though they constitute one of the most challenging issues faced by organizations, data breaches that could lead to identity theft are mostly preventable. For any department that manages or requires access to sensitive information, organizations should develop strong security policies such as strongly encrypting all data, ensuring there are controls in place that restricts access to such information to required personnel, and providing education and resources for all employees on proper security procedures. Network administrators should be closely monitoring network traffic and tracking all activity to ensure that there is no illegal access to databases, as well as testing security processes and systems regularly to ensure their integrity. Organizations should include these steps as part of a broader security policy, and ensure that any security policy is implemented and enforced to protect all sensitive data from unauthorized access.

### Bot-infected computers

Bots are programs that are covertly installed on a user's machine in order to allow an attacker to remotely control the targeted system through a communication channel, such as Internet relay chat (IRC), P2P, or HTTP. These channels allow the remote attacker to control a large number of compromised computers over a single, reliable channel in a botnet, which can then be used to launch coordinated attacks.

Bots allow for a wide range of functionality and most can be updated to assume new functionality by downloading new code and features. Attackers can use bots to perform a variety of tasks, such as setting up denial-of-service (DoS) attacks against an organization's website, distributing spam and phishing attacks, distributing spyware and adware, propagating malicious code, and harvesting confidential information from compromised computers that may be used in identity theft, all of which can have serious financial and legal consequences. Bots are also inexpensive and relatively easy to propagate. In 2008, Symantec observed underground economy advertisements for as little as $0.04 per bot. This is much cheaper than in 2007, when $1 was the cheapest price advertised for bots. Bot-infected computers with a decentralized bot C&C model are favored by attackers because they are difficult to disable, and most importantly, can be lucrative for their controllers. In one example, a botnet owner arrested in New Zealand admitted to earning $21,500 over a two-year span from his activities.[57]

A bot-infected computer is considered active on a given day if it carries out at least one attack on that day. This does not have to be continuous; rather, a single such computer can be active on a number of different days. A distinct bot-infected computer is a distinct computer that was active at least once during the period. In 2008, Symantec observed an average of 75,158 active bot-infected computers per day (figure 6), a 31 percent increase from 2007. Symantec also observed 9,437,536 distinct bot-infected computers during this period, a 1 percent increase from 2007.

[56] Cf. http://news.bbc.co.uk/1/hi/world/americas/7395295.stm or http://www.msnbc.msn.com/id/23678909/
[57] http://www.itworld.com/security/58670/botnet-master-sees-himself-next-bill-gates

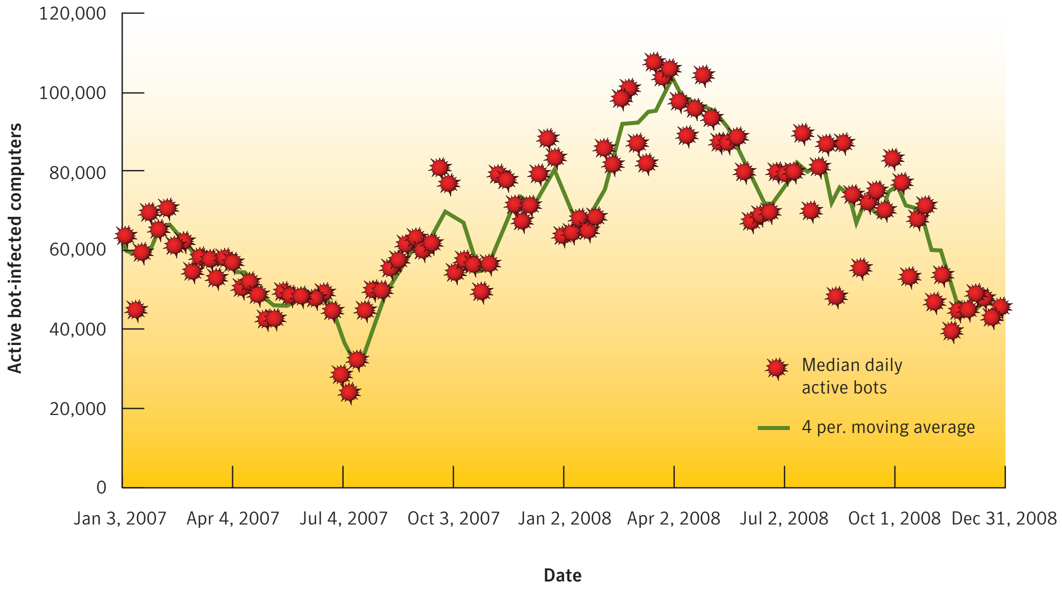

**Figure 6. Active bot-infected computers, by day**
*Source: Symantec*

The decrease in active bot-infected computers at the beginning of 2008 may be due to the reduction in size of the botnet associated with the Peacomm Trojan.[58] The number of bot-infected computers in the botnet was reduced to 5 percent of its previous estimated size, from 2 million bot-infected computers to 100,000.[59] In addition, as stated in **"Malicious activity by country,"** the shutdown of two U.S.-based hosting companies responsible for hosting bot C&C servers for a number of major botnets likely contributed to the decrease in active bot-infected computers in September and November 2008. After the shutdown in September, major botnets, including Srizbi and Pandex,[60] were able to find alternate hosting, which resulted in an increase in bot-infected computers back to pre-shutdown levels. However, the shutdown in November severely crippled Srizbi and Ozdok, and as a consequence, competing botnets, including Pandex, were able to fill the void.[61]

Although the number of active bot-infected computers decreased at the end of the year, it is assumed that botnet owners will seek out new hosts to get their botnets back online, and it is expected that bot numbers will rise again in 2009.[62] One result of all the activity in 2008 is that this shows that botnets can be crippled by identifying and shutting down their bot C&C server hosts, but that this strategy is difficult to implement given the various global hosting options that botnet controllers have at their disposal.

[58] Also known as the Storm botnet.
[59] http://www.messagelabs.com/mlireport/MLIReport_Annual_2008_FINAL.pdf : p. 32
[60] http://www.symantec.com/security_response/writeup.jsp?docid=2007-042001-1448-99
[61] http://www.messagelabs.com/mlireport/MLIReport_Annual_2008_FINAL.pdf : p. 25–26
[62] http://eval.symantec.com/mktginfo/enterprise/other_resources/b-state_of_spam_report_12-2008.en-us.pdf

## Bot command-and-control servers

Symantec tracks the number of bot C&C servers globally because these are what botnet owners use to relay commands to bot-infected computers on their networks. For the first time, in this volume of the Symantec *Global Internet Security Threat Report*, bot C&C servers controlled over HTTP are included in this analysis alongside IRC bot C&C servers.[63] This change in measurement was made due to the trend of botnet owners shifting away from traditional IRC bot C&C communication frameworks and toward managing their botnets through HTTP bot C&C servers. In 2008, Symantec identified 15,197 distinct new bot C&C servers (figure 7), of which 43 percent were over IRC channels and 57 percent over HTTP.

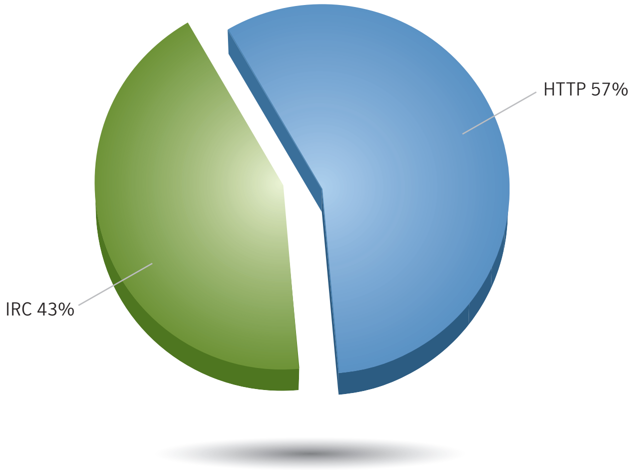

**Figure 7. Bot command-and-control servers, by type**
*Source: Symantec*

Botnet owners are moving away from traditional IRC-based botnets since they are easier to detect, track, filter, and block than botnets based on HTTP traffic. HTTP communications can be used to disguise botnet traffic among other Web traffic in order to make it difficult to distinguish malicious traffic from legitimate HTTP traffic. (Most HTTP bot transmissions are encrypted to avoid detection.) To filter the traffic, organizations would have to inspect the encrypted HTTP traffic and identify and remove bot-related traffic while still allowing legitimate traffic to pass through. Because of this, it is very difficult to pinpoint and disable a bot C&C structure. It is also unreasonable to block HTTP traffic since organizations depend on legitimate HTTP traffic to conduct day-to-day business. Botnet owners have also been switching away from using P2P for bot C&C server communications because such traffic is more easily detected due to the "noise" it creates in transmission. Moreover, many enterprises and other organizations also block P2P ports to prevent such high-bandwidth traffic from entering their networks.

[63] Not included in this measurement are bot C&C servers over P2P protocols; also, as this is the first report in which HTTP bot C&C servers are included in this analysis, 2007 comparisons are unavailable.

Symantec also observed an average of 42 new active bot C&C servers per day in 2008, of which 18 were IRC-based and 24 were HTTP (figure 8). The three largest botnets identified by Symantec in 2008—Srizbi, Rustock, and Pandex—are all HTTP-based.

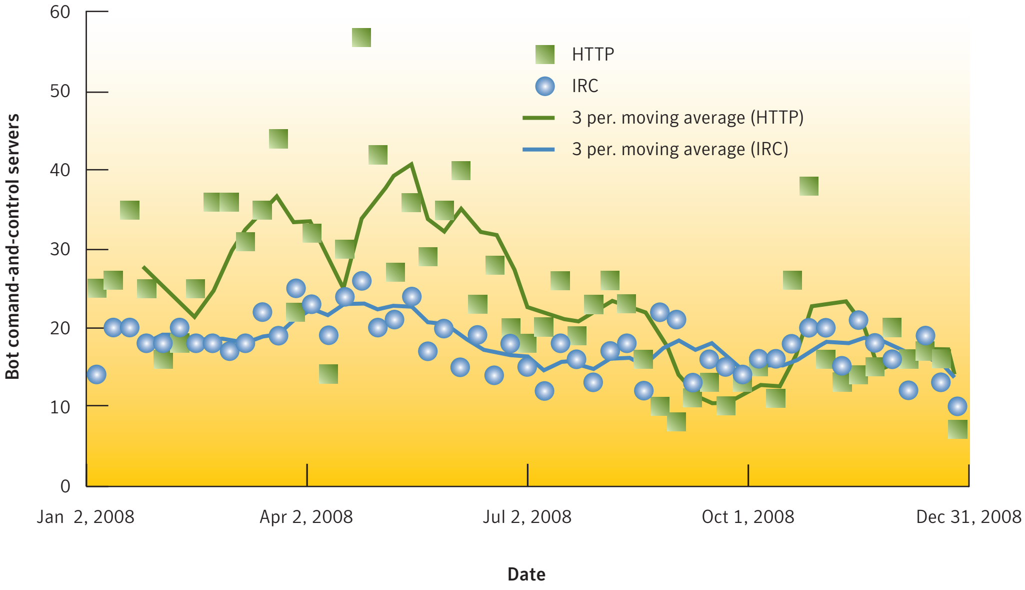

**Figure 8. Bot command-and-control servers, by day**
*Source: Symantec*

The drop in new and active HTTP bot C&C servers in February 2008 is likely due to bot C&C servers for a major HTTP-based botnet, Ozdok, going offline for 10 days during that month.[64] Also, the significant reductions that occurred in September and November 2008 are likely due to the shutdown of two U.S.-based ISPs, as was noted previously in this discussion. The September shutdown resulted in an immediate decrease in activity associated with the Srizbi and Pandex botnets.[65] As mentioned, it is assumed that these botnets found alternate hosting, which would explain the subsequent rise in activity.

The second shutdown in November resulted in a 30 percent decrease in overall botnet traffic and is thought to have severely weakened two of the largest botnets, Srizbi and Rustock.[66] The significant drop in new and active HTTP bot C&C servers in November may be because one of these ISPs was allegedly hosting a large number of bot C&C servers for Srizbi and Rustock, and bots were hard-coded to connect to these servers.[67] It was estimated that the Srizbi botnet had 300,000 bots prior to the shutdown[68] and the Rustock botnet had included over 150,000 bots.[69]

[64] http://www.scmagazineus.com/TRACE-Six-botnets-generate-85-percent-of-spam/article/107603/
[65] http://www.messagelabs.com/mlireport/MLIReport_Annual_2008_FINAL.pdf : p. 25
[66] http://www.messagelabs.com/mlireport/MLIReport_Annual_2008_FINAL.pdf : p. 26
[67] http://eval.symantec.com/mktginfo/enterprise/other_resources/b-state_of_spam_report_12-2008.en-us.pdf
[68] http://itknowledgeexchange.techtarget.com/security-bytes/srizbi-botnet-is-the-biggest-but-does-size-matter/
[69] http://www.scmagazineus.com/The-Rustock-botnet-spams-again/article/112940/

## Top Web-based attacks

The widespread deployment of Web applications along with the ubiquity of easy-to-exploit Web application security vulnerabilities have resulted in the prevalence of Web-based threats. Attackers wanting to take advantage of client-side vulnerabilities no longer need to actively compromise specific networks to gain access to those computers. Instead, they are now focused on attacking and compromising websites in order to mount additional, client-side attacks.

These attack types can be found globally and Symantec identifies each by an associated distinct detection signature. Most attack types target specific vulnerabilities or weaknesses in Web browsers or other client-side applications that process content originating from the Web. This metric will assess the top distinct Web-based attacks originating from compromised legitimate sites and malicious sites that have been created to intentionally target Web users.

The attacks discussed can involve social engineering to entice a victim to view a malicious website, but most attacks exploit trusted high-traffic websites. When the user visits a compromised website, a number of attack methods are used. Malicious content from the website can directly exploit a vulnerability in the browser, a browser plug-in, or a desktop application. An attack such as this may require very little interaction apart from the user visiting the site from where the attack originates. In the case of a drive-by download, the attack will occur without any interaction required from the user.[70]

Attackers also use malicious websites for compromises, such as misleading the user to indirectly authorize a specific technology that then downloads malicious code, or prompting the user to click on a pop-up or banner ad. Attackers can also redirect all traffic from a legitimate website to a malicious website from which the user's computer will then be attacked. In all of these types of Web-based attacks, the user is unaware of the compromise. Once an attacker has compromised a website and injected malicious content, he or she can passively attack visitors of the compromised site. This type of attack is very efficient for attackers because they only have to compromise one Web page in order to affect multiple users. When a user visits a compromised Web page, the attack is carried out through the user's browser.[71] The attack will either target vulnerabilities in the browser itself or it will target third-party applications that are activated by the browser.

All Web-based attack traffic goes through the HTTP or HTTPS protocols. The benefit of this for attackers is that it is unreasonable to block these protocols because legitimate organizations depend on them for their day-to-day business. In addition, filtering a large volume of HTTP traffic would significantly slow throughput traffic. HTTP traffic is also difficult to filter with intrusion detection/intrusion prevention systems (IDS/IPS) because it is difficult to distinguish malicious traffic from legitimate traffic, and HTTP traffic can be encrypted, thus enabling attacks to be obfuscated within legitimate traffic.

Attackers are not only employing manual methods to exploit these issues, but they are also using automated tools, such as Neosploit,[72] to exploit client-side vulnerabilities on a massive scale. Such toolkits are widely available and prepackaged so that people with minimal technical knowledge are able to use them effectively.

[70] A drive-by download is any download that occurs without a user's prior knowledge or authorization and does not require user interaction. Typically this is an executable file.

[71] Cf. "Vulnerability trends" section for discussion on compromises to websites with Web-based vulnerabilities.

[72] http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=Security&articleId=9115599&taxonomyId=17&pageNumber=1

Another attraction of the Web for exploitation is the profusion of dynamic sites that use Web-based applications, such as forums, photo-sharing galleries, blogs, and online shopping applications. Dynamic sites are prime targets for attackers using bot-infected computers to propagate and host malicious content since Web application and site-specific vulnerabilities can put these types of site at risk.

Attackers are also especially attracted to large, popular websites with trusted reputations. This is not only because a successful compromise can reach a greater number of people (who tend to have an inherent trust for legitimate websites and are thus more susceptible to attack), but, as mentioned, it may be difficult to block attacks to these sites using security tools without disrupting legitimate traffic.

These developments and trends indicate that Web-based threats have not only become widespread, but that they also have increased in sophistication and severity. In particular, Symantec has noticed that botnets (such as Asprox, which was initially used for phishing scams) are being redesigned to specifically exploit cross-site scripting vulnerabilities and inject malicious code into compromised websites.[73]

Many Web-based attacks exploit vulnerabilities that are considered medium severity. This means that they can compromise the account of the currently logged in user because the user does not require administrative privileges to run the affected applications. While the danger of client-side vulnerabilities may be limited by best practices, such as restricting Web applications to the administrative level, this is often unreasonable given how integral Web applications are to the delivery of content for many businesses. Medium-severity vulnerabilities affecting client or desktop applications are often sufficient for an attacker to mount successful malicious attacks on single clients, as well as at the enterprise level.

In 2008, the top Web-based attack was associated with the Microsoft Internet Explorer ADODB.Stream Object File Installation Weakness,[74] which accounted for 29 percent of the total globally (table 3). The weakness allows attackers to install malicious files on a vulnerable computer when a user visits a website hosting an exploit. To carry out this attack, an attacker must exploit another vulnerability that bypasses Internet Explorer security settings to allow the attacker to execute malicious files installed by the initial security weakness. This issue was published on August 23, 2003, and fixes have been available since July 2, 2004. Since this was the top Web-based attack in 2008, this may indicate that many computers running Internet Explorer have not been patched or updated and are running with this exposed vulnerability.

| Rank | Web-based Attack | Percentage |
|---|---|---|
| 1 | Microsoft Internet Explorer ADODB.Stream Object File Installation Weakness | 30% |
| 2 | Acrobat PDF Suspicious File Download | 11% |
| 3 | ANI File Header Size Buffer Overflow | 7% |
| 4 | Adobe SWF Remote Code Executable | 7% |
| 5 | Microsoft Internet Explorer DHTML CreateControlRange Code Executable | 6% |
| 6 | SnapShot Viewer ActiveX File Download | 5% |
| 7 | Microsoft Internet Explorer XML Core Services XMLHTTP Buffer Overload | 4% |
| 8 | Quicktime RTSP URI Buffer Overload | 3% |
| 9 | AOL SuperBuddy ActiveX Code Executable | 3% |
| 10 | Microsoft Internet Explorer WebViewFolderIcon ActiveX Control Buffer Overflow | 2% |

**Table 3. Top Web-based attacks**
*Source: Symantec*

[73] http://www.messagelabs.com/mlireport/MLIReport_Annual_2008_FINAL.pdf : p. 33
[74] Cf. http://www.symantec.com/business/security_response/attacksignatures/detail.jsp?asid=50031 or http://www.securityfocus.com/bid/10514

A large number of exploits and malicious applications may depend on this vulnerability as a common way of compromising computers, in tandem with other known vulnerabilities. Therefore, the amount of attack activity is related to the cumulative number of exploits, attack toolkits, and worms targeting this vulnerability as one possible means of compromising computers. It is also likely that the large market share of Microsoft Internet Explorer plays a role in the popularity of this attack.[75] While the vulnerability was patched in 2004, there are likely still enough unpatched computers that are affected by this vulnerability for attackers to continue to benefit from its exploitation.

The second most common Web-based attack in 2008 was related to malicious Adobe® Acrobat® PDF activity,[76] which accounted for 11 percent of Web-based attacks. Specifically, attempts to download suspicious PDF documents were observed. This may indicate attempts by attackers to distribute malicious PDF content to victims via the Web. The attack is not directly related to any specific vulnerability, although the contents of the malicious file would be designed to exploit an arbitrary vulnerability in an application that processes it, such as Adobe Acrobat Reader®. A successful attack could ultimately result in the compromise of the integrity and security of an affected computer. This attack is assumed to be popular to due the common use and distribution of PDF documents on the Web. Also, browsers can be set up to automatically render a PDF document by default. Specific exploit activity related to malicious PDF files was observed in 2008.[77]

The **"Vulnerability Trends"** section of this report notes that the percentage of plug-in vulnerabilities affecting Adobe Acrobat Reader in comparison to the total number of browser plug-in vulnerabilities increased to 4 percent in 2008 from 1 percent in 2007. This demonstrates that Adobe Acrobat Reader is increasingly targeted by attackers. In addition, the reappearance of the Neosploit toolkit in 2008 may have contributed to the popularity of this type of attack as that toolkit is designed to exploit vulnerabilities in PDF documents.[78]

In 2008, the third most common Web-based attack exploited the Microsoft Windows User32.DLL ANI File Header Handling Stack-Based Buffer Overflow Vulnerability,[79] accounting for 7 percent of Web-based attacks in 2008. The ANI (animated cursor file) handler is a default component of the Microsoft Windows operating system and is used by a significant number of widely used Microsoft applications as well as the Windows shell. If successfully exploited, the vulnerability allows an attacker to execute arbitrary code embedded in a malformed ANI file originating from the Web or other sources. This vulnerability was published on January 11, 2005, and fixes have also been available since that time. Exploit code was publicly available the following day. As with the Microsoft Internet Explorer ADODB.Stream Object File Installation Weakness, the prominence of this type of attack indicates that computers in the region are likely not being sufficiently patched and updated.

Vulnerabilities such as those discussed here continue to generate a large amount of observed attack activity because they can be reliably exploited. This makes these vulnerabilities prime candidates for automation. Despite the fact that fixes are available, as mentioned, it is likely that there are still enough unpatched systems in existence that these attacks continue to enjoy success. When attacks prove successful, they are often adopted by a large number malicious code variants and attack toolkits. This can cumulatively create a large amount of observed attack activity. It is also likely that older malicious code variants continue to attempt to automatically exploit these vulnerabilities as a means of propagation.

[75] http://marketshare.hitslink.com/browser-market-share.aspx?qprid=0&qpmr=100&qpdt=1&qpct=3&qptimeframe=Y&qpsp=2008&qpnp=2
[76] http://www.symantec.com/business/security_response/attacksignatures/detail.jsp?asid=23153
[77] https://forums2.symantec.com/t5/Vulnerabilities-Exploits/Pidief-the-Word-for-Exploits/ba-p/305564#A141
[78] http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=Security&articleId=9115599&taxonomyId=17&pageNumber=2
[79] Cf. http://www.symantec.com/business/security_response/attacksignatures/detail.jsp?asid=21719 or http://www.securityfocus.com/bid/12233

## Top countries of origin for Web-based attacks

This metric will assess the top countries of origin for Web-based attacks against users in 2008 by determining the location of computers from which the attacks occurred. Note that attackers, in order to hide their tracks, often redirect users through one or more servers that may be located anywhere globally.

Once an attacker has compromised a legitimate website, users who visit the website will be attacked by several additional means. One way is through a drive-by download, which results in the installation of malicious code without the user's knowledge or consent. Another way is to redirect the user to another website that is used to host malicious code. Sites and servers hosting a variety of malicious exploits can be found worldwide. Multiple domains can be associated with one compromised site, which is used to exploit one or more security vulnerabilities in affected client browsers.

In 2008, computers from the United States were the leading source of Web-based attacks against users, accounting for 38 percent of the total (table 4). There are a number of factors that make the United States the top country of origin for Web-based attacks. This ranking may be due to the more than half a million websites that were compromised in May 2008 with malicious code that was hosted in Russia and the United States. Web forums hosted by PHP-based bulletin board applications were exploited to inject malicious JavaScript™ into forum content. These forums would then infect visitors with variants of the Zlob Trojan[80] disguised as a video codec installer. The exploit changes browser and DNS settings on the infected computer and enables additional attacks, including turning the infected computer into a zombie.[81] This attack follows the trend of attackers inserting malicious code into legitimate high-traffic websites where users are likely to be more trusting of the content, rather than attempting to lure users to visit specially designed malicious sites.

| Rank | Country | Percentage |
|---|---|---|
| 1 | United States | 38% |
| 2 | China | 13% |
| 3 | Ukraine | 12% |
| 4 | Netherlands | 8% |
| 5 | Russia | 5% |
| 6 | United Kingdom | 5% |
| 7 | Canada | 3% |
| 8 | Japan | 2% |
| 9 | Latvia | 1% |
| 10 | France | 1% |

**Table 4. Top countries of origin for Web-based attacks**
*Source: Symantec*

[80] http://www.symantec.com/security_response/writeup.jsp?docid=2005-042316-2917-99
[81] http://www.channelregister.co.uk/2008/05/13/zlob_trojan_forum_compromise_attack/

In 2008, China ranked as the second country of origin for Web-based attacks, with 13 percent of the worldwide total. The main reason for the high rank of China in 2008 is due to compromised websites relating to the 2008 Beijing Olympic Games. The games were one of the largest events of 2008 and attackers exploited the popularity of the event in their attempts to lure and compromise users, as has been seen previously with other major sporting and entertainment events.[82] One example is the Rustock botnet, which sent out emails with links to a news report about the games. Users were prompted to click a link in the email and visit a site, which then prompted them to download a missing codec in order to launch a video. Clicking to obtain the codec actually resulted in the installation of a Trojan.

Attackers may have also used social engineering to lure users to compromised websites under the guise of being associated with the 2008 Beijing Olympic Games, as attacks against Chinese-language websites increased significantly during the games.[83] The extent of these attacks was mitigated, however, by initiatives to increase online security for users ahead of the Games by shutting down or blacklisting thousands of websites potentially most susceptible to fraud, which are popular targets of attack from Web application and site-specific vulnerabilities. Also, thousands of websites in China were compromised when certain Web applications were infected with malicious JavaScript that was planted through the use of SQL-injection attacks.[84] Visitors to these compromised sites had their computers attacked and, if the attacks were successful, Trojans were downloaded onto the computers.[85]

Ukraine ranked third in 2008 for top country of origin for Web-based attacks, accounting for 12 percent of such attacks worldwide. The prominence of Ukraine in this metric is likely due to the compromise of the website of a U.S.-based electronic bill payment processing company.[86] The attackers were able to obtain account credentials to the company's domain using a phishing attack, and were then able to gain access to the company's website. Customers, thinking they were visiting the legitimate website, were redirected to a malicious website hosted on servers in the Ukraine where they were attacked with a Trojan.[87] In addition to the compromise of the bill payment company's website, there were at least 71 domains that were redirected to the malicious Ukrainian server during this time.[88]

Of note, six of the top 10 countries for Web-based attacks in the EMEA region were also in the top 10 countries of origin for Web-based attacks globally, and countries in the EMEA region accounted for 41 percent of the worldwide total, more than any other region. Exploit packs may be one of reasons behind the prominence of the EMEA region in this measurement. Many exploit packs, including MPack,[89] IcePack,[90] and Neosploit,[91] originated in Russia and it is likely that the Russians who developed these attack kits are responsible for much of their continued propagation. These attackers could possibly be compromising websites around the world and redirecting visitors to computers in EMEA that host the exploit code being used to target client-side vulnerabilities in Web browsers.

Also contributing to the prominence of the EMEA region this period were a number of high-profile Web-based attacks that occurred there. One example was in January 2008, when the embassy website of the Netherlands in Russia was compromised and visitors to the site were misled into installing malicious code.[92] Another example occurred in August 2008 when several hundred domains in the Netherlands were compromised and defaced.[93] A third case was when more than a thousand UK websites were compromised

[82] http://news.bbc.co.uk/1/hi/technology/7548870.stm
[83] http://www.networkworld.com/newsletters/gwm/2008/090808msg1.html
[84] http://www.h-online.com/security/Chinese-websites-under-mass-attack--/news/110764
[85] Ibid.
[86] http://www.networkworld.com/news/2008/120508-network-solutions-phishing-came-before.html
[87] http://www.csoonline.com/article/474365/CheckFree_Warns_Million_Customers_After_Hack
[88] http://blog.kievukraine.info/2008/12/digging-deeper-into-checkfree-attack.html
[89] https://forums2.symantec.com/t5/blogs/blogarticlepage/blog-id/vulnerabilities_exploits/article-id/93#M93
[90] https://forums2.symantec.com/t5/Vulnerabilities-Exploits/Honor-Among-Thieves/ba-p/306084#A193
[91] http://blogs.zdnet.com/security/?p=1593
[92] http://www.theregister.co.uk/2008/01/23/embassy_sites_serve_malware/
[93] http://blogs.zdnet.com/security/?p=1788

and users visiting these sites risked being infected with the Asprox Trojan.[94] The success of these attacks on government sites can be attributed, in part, to the inherent trust that visitors to such sites will have, making these visitors more liable to accept prompts to download files if requested.

Web-based attacks are a major threat to computer networks for both enterprises and end users. Attacks such as drive-by downloads are covert and very difficult to mitigate because most users are unaware that they are being attacked. Organizations are thus confronted with the complicated task of having to detect and filter attack traffic from legitimate traffic. Since many organizations rely on Web-based tools and applications to conduct business, it is likely that the Web will continue to be the primary conduit for attack activity favored by malicious code developers.

### Threat activity—protection and mitigation

There are a number of measures that enterprises, administrators, and end users can employ to protect against malicious activity. Organizations should monitor all network-connected computers for signs of malicious activity, including bot activity and potential security breaches, ensuring that any infected computers are removed from the network and disinfected as soon as possible. Organizations should employ defense-in-depth strategies, including the deployment of antivirus software and a firewall.[95] Administrators should update antivirus definitions regularly and ensure that all desktop, laptop, and server computers are updated with all necessary security patches from their operating system vendor. As compromised computers can be a threat to other systems, Symantec also recommends that enterprises notify their ISPs of any potentially malicious activity.

Symantec recommends that organizations perform both ingress and egress filtering on all network traffic to ensure that malicious activity and unauthorized communications are not taking place. Organizations should also filter out potentially malicious email attachments to reduce exposure to enterprises and end users. In addition, egress filtering is one of the best ways to mitigate a DoS attack. DoS victims frequently need to engage their upstream ISP to help filter the traffic to mitigate the effects of attacks.

Symantec also advises that users never view, open, or execute any email attachment unless the attachment is expected and comes from a known and trusted source, and unless the purpose of the attachment is known. By creating and enforcing policies that identify and restrict applications that can access the network, organizations can minimize the effect of malicious activity, and hence, minimize the effect on day-to-day operations. Also, administrators should limit privileges on systems for users that do not require such access and they should also restrict unauthorized devices, such as external portable hard-drives and other removable media.

[94] http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article4381034.ece

[95] Defense-in-depth emphasizes multiple, overlapping, and mutually supportive defensive systems to guard against single-point failures in any specific technology or protection methodology. Defense-in-depth should include the deployment of antivirus, firewalls, and intrusion detection systems, among other security measures.

To reduce the likelihood of identity theft, organizations that store personal information should take the necessary steps to protect data transmitted over the Internet or stored on their computers. This should include the development, implementation, and enforcement of a secure policy requiring that all sensitive data is encrypted. Organizations should implement a data loss protection (DLP) solution that not only prevents data breaches, but also mitigates potential data leaks from within an organization. Access to sensitive information should be restricted and organizations should also enforce compliance to information storage and transmission standards such as the PCI standard.[96] Policies that ensure that computers containing sensitive information are kept in secure locations and are accessed only by authorized individuals should be put in place and enforced. Sensitive data should not be stored on mobile devices that could be easily misplaced or stolen. This step should be part of a broader security policy that organizations should develop and implement in order to ensure that any sensitive data is protected from unauthorized access. This would ensure that even if the computer or medium on which the data were lost or stolen, the data would not be accessible. This step should be part of a broader security policy that organizations should develop and implement in order to ensure that any sensitive data is protected from unauthorized access.

[96] https://www.pcisecuritystandards.org/

## Vulnerability Trends

This section will discuss selected vulnerability trends in greater depth, providing analysis and discussion of the trends indicated by the data. The following metrics will be discussed:

- Window of exposure for Web browsers
- Web browser vulnerabilities
- Web browser plug-in vulnerabilities
- Web browser plug-in vulnerabilities, by type
- Web application vulnerabilities
- Site-specific cross-site scripting vulnerabilities
- Zero-day vulnerabilities
- Top attacked vulnerabilities
- Attacked vulnerabilities by attack vector (client versus server)
- Vulnerabilities—protection and mitigation

### Window of exposure for Web browsers

The window of exposure for Web browsers is the difference in days between the time when exploit code affecting a vulnerability is made public and the time when the affected vendor makes a patch publicly available for that vulnerability. During this time, the computer or system on which the affected application is deployed may be susceptible to attack. The metric is derived from the average amount of time it took to release a patch in comparison to the average amount of time it took for exploit code to be made publicly available. This metric also includes maximum patch times, which is the maximum amount of time required to release a patch for all of the patched vulnerabilities in the data set.

By measuring the amount of time it takes for vendors to release patches for vulnerabilities, it is possible to gain some insight into their overall security responsiveness. Some of the vulnerabilities examined in this metric were patched by the vendor at the time they were announced. This may be reflective of an internal security audit by the vendor, which may have revealed the vulnerability. It may also indicate that security researchers discovered the vulnerability and responsibly disclosed it to the vendor. Other vulnerabilities are independently reported by security researchers prior to the release of a patch. This indicates that security researchers did not coordinate with the vendor to disclose the vulnerability. In some cases, this may mean that the researcher did not responsibly disclose the vulnerability, and in other cases it is possible that the researcher attempted to responsibly report the vulnerability but the vendor was unresponsive. The patch release time is compared against the average time it takes for vulnerability exploits to become publicly available to determine the window of exposure.

The window of exposure takes all of these factors into account to calculate the average time during which end users and organizations are exposed to exploits. During the window of exposure, administrators and end users need to mitigate the possibility of exploitation by employing current best practices and the best available mitigation technologies. For high priority vulnerabilities, organizations must devote resources to mitigation until the vulnerability is adequately addressed and eliminated as a risk.

This metric will examine the window of exposure for the following Web browsers:[97]

- Apple Safari
- Google Chrome
- Microsoft Internet Explorer
- Mozilla browsers
- Opera

In 2008, the average window of exposure for Safari was nine days, based on a sample set of 31 patched vulnerabilities (figure 9). The window of exposure for 2007 was one day, based on a sample set of 31 patched vulnerabilities. The eight-day increase in the window of exposure for Safari is due to a number of independently discovered vulnerabilities. The maximum time for Apple to patch a Safari vulnerability in 2008 was 156 days, which negatively affected the average and is significantly longer than the maximum patch time of eight days in 2007

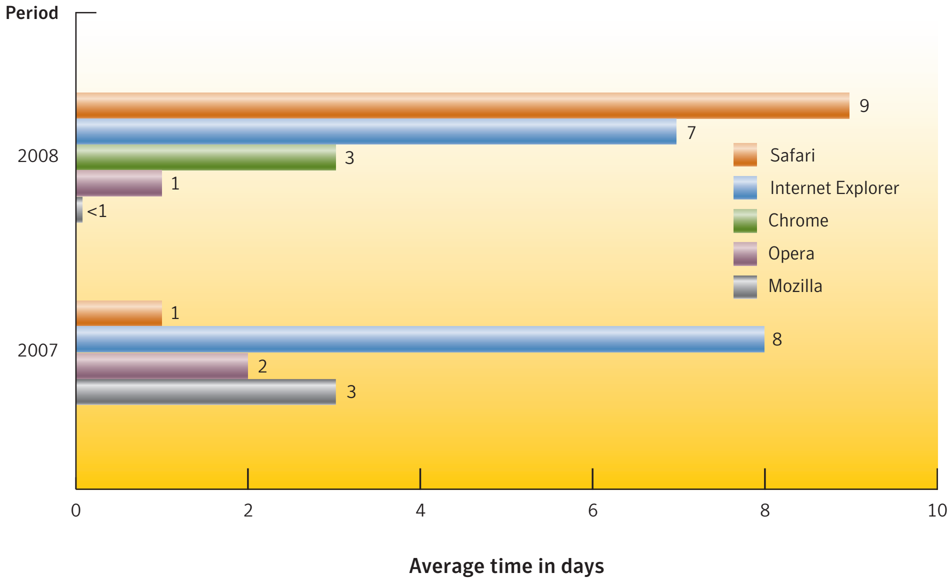

**Figure 9. Window of exposure for Web browsers**
*Source: Symantec*

Internet Explorer had an average window of exposure of seven days in 2008, based on a sample set of 31 patched vulnerabilities. The maximum amount of time to release a patch in 2008 was 147 days. In 2007, the average window of exposure was eight days, based on a sample set of 28 vulnerabilities, and the maximum time to release a patch was 90 days.

In 2008, a zero-day vulnerability affecting Internet Explorer was found to be exploited in the wild. Microsoft addressed this vulnerability within eight days of its discovery. In this case, the response time of eight days to release a patch is less than the average time it took to develop a patch for Internet Explorer in 2008, which was 11 days.

[97] It should be noted that this metric examines all versions of each browser; vulnerabilities affecting multiple versions are counted as a single vulnerability.

For the first time, in this report, Chrome is included in the browsers being assessed by Symantec. Because it was released only recently (September 2008), it is being included here mainly to provide insight into its performance against other browsers thus far and to set a baseline for future reports. In 2008, Symantec documented an average window of exposure of three days for Chrome based on a sample set of six patched vulnerabilities. The maximum patch time for a vulnerability was 11 days.

The window of exposure for Opera in 2008 was one day, based on a sample set of 33 patched vulnerabilities. In 2008, the maximum time to patch a vulnerability was 29 days. In 2007, the window of exposure for Opera was two days, based on a sample set of 14 patched vulnerabilities, and the maximum patch time was 23 days.

Mozilla browsers had a window of exposure of less than one day in 2008, based on a sample set of 83 patched vulnerabilities, and the maximum patch time was 30 days. In 2007, Mozilla browsers had a window of exposure of three days, from a sample set of 103 vulnerabilities, and the maximum patch time was 109 days.

Of all the browser vendors examined, Mozilla browsers maintained the shortest window of exposure while patching more vulnerabilities than other vendors. This may be indicative of their efforts to marshal the security community to responsibly report vulnerabilities through initiatives such as their Bug Bounty program.[98] The result of this effort is that more vulnerabilities are announced by the vendor at the time they are fixed, instead of being publicly reported by security researchers independently of the vendor.

It is also worth noting that independent browser vendors, such as Opera and the Mozilla Foundation, had a shorter window of exposure in 2008 than the major operating system vendors, such as Apple and Microsoft. This may be due to the possibility that vendors whose main product is a Web browser do not have to spread their security response efforts across multiple, disparate products, and can instead focus on the browser. Comparably, major operating system vendors typically have to coordinate security response efforts across a larger number of unpatched vulnerabilities affecting a more diverse product portfolio and organization. Vulnerabilities in other products may take priority based on a number of factors such as the severity of the vulnerability, attack activity in the wild, or the relative ease of developing a patch. Because Chrome is a new addition for this volume, it remains to be seen how Google will fare in the long term as a large vendor whose Web browser technology represents only a small portion of the products and services it offers.

### Web browser vulnerabilities

Web browser vulnerabilities are a serious security concern due to their role in online fraud and in the propagation of malicious code, spyware, and adware. They are particularly prone to security concerns because they are exposed to a greater amount of potentially untrusted or hostile content than most other applications. This is a concern because attacks can originate from malicious websites as well as legitimate websites that have been compromised to serve malicious content. Browsers can also facilitate client-side attacks because of their use of plug-ins and other applications in handling potentially malicious content served from the Web such as documents and media files.

[98] http://www.mozilla.org/security/bug-bounty-faq.html

This metric will examine the total number of vulnerabilities affecting the following Web browsers:

- Apple Safari
- Google Chrome
- Microsoft Internet Explorer
- Mozilla browsers
- Opera

During 2008, 99 vulnerabilities affected Mozilla browsers (figure 10). Forty of these vulnerabilities were considered low severity and 59 were considered medium severity. This is fewer than the 122 vulnerabilities that were documented in 2007 for Mozilla browsers, of which 91 were considered low severity and 31 were considered medium severity.

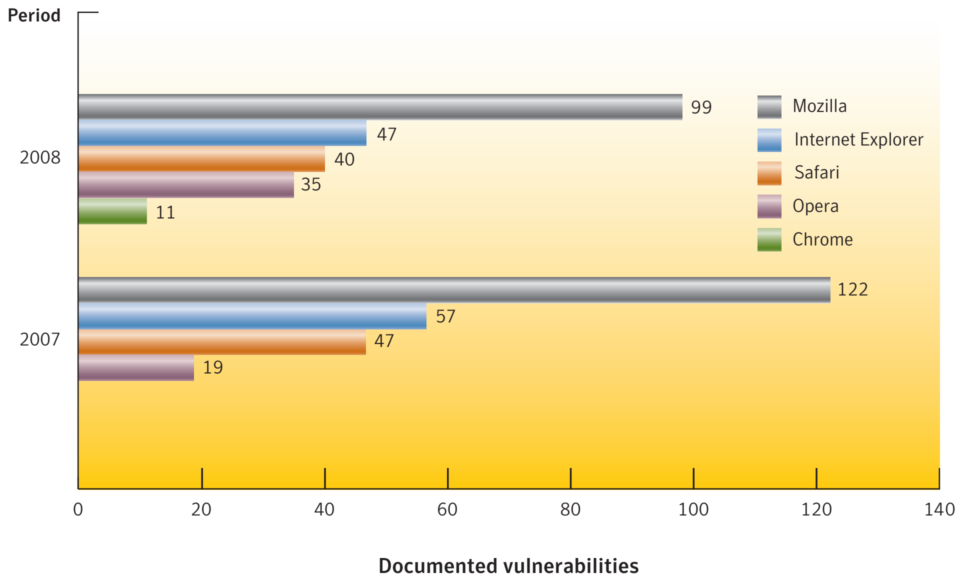

**Figure 10. Web browser vulnerabilities**
*Source: Symantec*

Internet Explorer was subject to 47 new vulnerabilities in 2008. Sixteen of these vulnerabilities were considered low severity and 31 were considered medium severity. This is fewer than the 57 new vulnerabilities documented in Internet Explorer in 2007, of which 28 were considered low severity, 28 were considered medium severity, and one was considered high severity.

Safari was affected by 40 new vulnerabilities in 2008, of which 16 were considered low severity and 24 were considered medium severity. This is less than the 47 vulnerabilities identified in Safari in 2007, of which 27 were considered low severity, 19 were considered medium severity, and one was considered high severity.

In 2008, Symantec documented 35 new vulnerabilities in Opera, of which 12 were considered low severity and 23 were considered medium severity. This is more than the 19 vulnerabilities discovered in Opera in 2007, of which eight were considered low severity and 11 were considered medium severity.

Chrome was affected by 11 vulnerabilities in 2008, of which seven were considered low severity and four were considered medium severity. Chrome was released in September 2008 and no comparison with previous years is possible.

With the exception of Opera (and, as noted, Chrome), there were fewer browser vulnerabilities identified in 2008 than those in 2007. The entrance of Chrome into the browser market and increasing browser market share of Opera may have influenced security research into these browsers and shifted attention away from other browsers. The trend toward fewer total vulnerabilities in browsers may also indicate a shift by the vendors to improve the security of browsers.

However, it is also worth noting that the trend in 2008 was toward more medium-severity vulnerabilities in browsers. This may correlate with the overall trend toward a higher proportion of medium-severity vulnerabilities in relation to all vulnerabilities documented in 2008. This may also be indicative of evolving skills among security researchers and attackers, who are identifying fewer lower-severity vulnerabilities as a result. It should be noted that, in many cases, medium-severity vulnerabilities are sufficient to mount successful attacks if attackers are able to execute arbitrary code and perform actions such as accessing confidential information or making network connections.

It is important for browser vendors to continue to improve browser security given the continuous competition among vendors to develop and include more feature-rich products in their products. In 2008, a number of browser vendors made concerted efforts to demonstrate their commitment to security. In particular, Google released the Browser Security Handbook, which outlines common browser security issues.[99] The goal of this project is to aid browser developers and security researchers in their understanding of these vulnerabilities to help identify and fix these issues. Mozilla has also started the Mozilla Security Metrics project as an attempt to quantify the relative security of their browser products.[100]

Web browsers continue to be an attractive target for attackers. In 2008, Internet Explorer was the target of a zero-day vulnerability in its XML-handling code.[101] This vulnerability was linked with SQL-injection attacks that compromised trusted websites for the purpose of hosting exploit code for the vulnerability.[102] This technique was detailed in the previous volume of the Symantec *Global Internet Security Threat Report*.[103] It is a continuing trend in 2008 for attackers to use Web-application vulnerabilities to compromise legitimate websites from which further attacks can then be launched. This exploit is also noteworthy because it attempts to obfuscate signs of an attack by closing the browser cleanly without any errors once exploitation has occurred. This is a measure undertaken by attackers to extend the survivability of zero-day exploits. A zero-day browser vulnerability is a highly valued asset that attackers work to protect against discovery by victims and security vendors. Prolonging the discovery of a zero-day vulnerability delays the development of vendor patches and security content, such as intrusion prevent signatures that help with mitigation.

[99] http://code.google.com/p/browsersec/wiki/Main
[100] http://blog.mozilla.com/security/2008/07/02/mozilla-security-metrics-project/
[101] https://forums2.symantec.com/t5/Vulnerabilities-Exploits/Yes-There-s-a-Zero-Day-Exploit-for-Internet-Explorer-Out-There/ba-p/371628#A180
[102] https://forums2.symantec.com/t5/Vulnerabilities-Exploits/Rise-of-IE-Zero-Day-Through-SQL-Injection/ba-p/372832#A182
[103] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf : p. 34

Another noteworthy browser security issue in 2008 was the “carpet bombing” flaw discovered in Safari.[104] The vulnerability would cause the browser to download arbitrary files to the victim’s desktop. It was later discovered that this could further be exploited to execute code. This issue was actually a combination of security weaknesses in Safari for Windows, Internet Explorer, and Microsoft Windows that, when exploited in tandem, could result in the deployment of a malicious executable. This is interesting because the deployed environment of the browser was a factor that elevated a relatively minor vulnerability into a major one. This presents a risk for browser vendors when they release products for new platforms, as Apple did with its first non-beta release of Safari 3.1 for Windows in March 2008. This concern may be relevant for Chrome, as Google is expected to release versions of the browser for Linux® and Mac OS® X in 2009.[105]

Administrators should maintain a restrictive policy regarding which applications are allowed within the organization. The security of applications should be evaluated on a platform-by-platform basis to ensure that platform-specific security issues do not arise when the application is installed.

### Web browser plug-in vulnerabilities

This metric will examine the number of vulnerabilities affecting plug-ins for Web browsers. Browser plug-ins are technologies that run inside the Web browser and extend its features. Often these plug-ins allow additional multimedia content from Web pages to be rendered in the browser. They can also enable execution environments that allow applications to be run inside the browser. Browser plug-in vulnerabilities are also used in a range of client-side attacks. Many browsers include various plug-ins in their default installation and provide a framework to ease the installation of additional plug-ins. Plug-ins now provide much of the expected or desired functionality of Web browsers and some may even be required to effectively use the internal sites of enterprises.

The following plug-in technologies will be examined:

- Adobe Acrobat
- Adobe Flash®
- Apple QuickTime®
- Microsoft ActiveX
- Microsoft Windows Media® Player
- Mozilla browser extensions
- Sun® Java™

In 2008, Symantec documented a total of 419 vulnerabilities in plug-in technologies for Web browsers. This is fewer than the 475 vulnerabilities affecting browser plug-ins identified in 2007. Of the total for 2008, 287 vulnerabilities affected ActiveX, which is significantly more than any other plug-in technology (figure 11). Of the remaining plug-ins for which vulnerabilities were documented, there were 45 vulnerabilities identified in Java, 40 in QuickTime, 17 in Acrobat Reader, 16 in Flash Player, five affected Mozilla extensions, and five that affected Windows Media Player.

[104] http://www.securityfocus.com/brief/746
[105] http://news.cnet.com/chrome-gets-mac-deadline-extensions-foundation/?tag=rtcol;newsNow

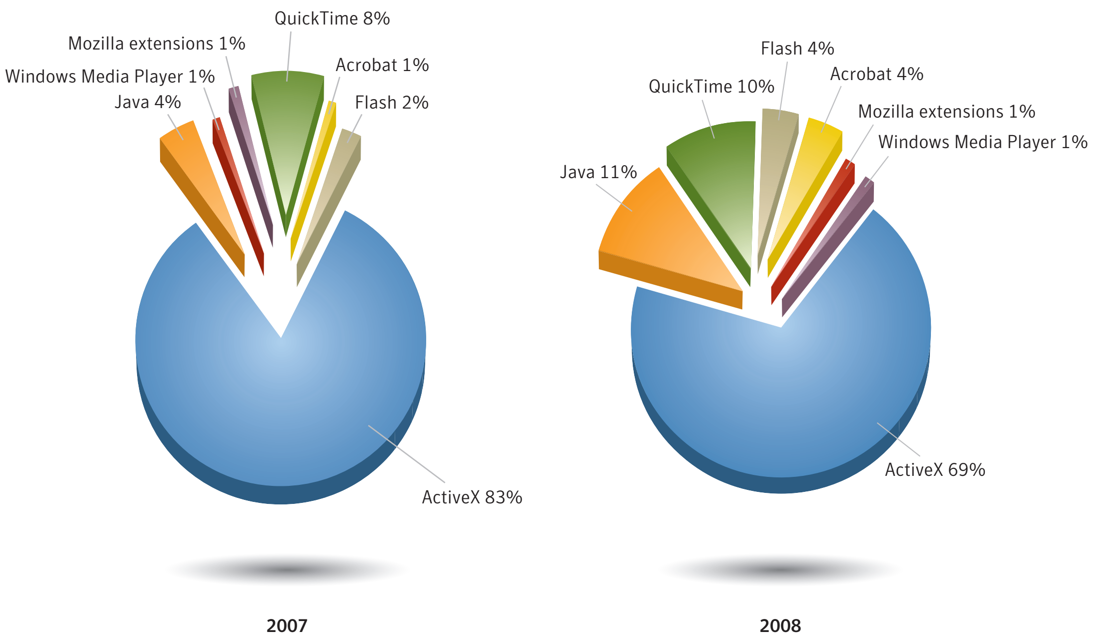

**Figure 11. Web browser plug-in vulnerabilities**
*Source: Symantec*

ActiveX was also affected by the most vulnerabilities in 2007, with a total of 399 out of the 475 vulnerabilities identified. After that, QuickTime ranked second with 37 vulnerabilities, Java was affected by 17, Flash Player had 11, four affected Mozilla extensions, three affected Windows Media Player, and three affected Adobe Acrobat Reader.

ActiveX vulnerabilities are still a popular mode of attack for developers of attack toolkits such as NeoSploit. In 2008, a number of additional exploits for ActiveX added to the NeoSploit toolkit were identified. This includes a vulnerability in the Snapshot Viewer for Microsoft Access®,[106] and another in the Computer Associates BrightStor® application.[107] In fact, to exploit the Microsoft Access Snapshot Viewer vulnerability, attackers went to the length of silently installing the vulnerable control on client computers not previously affected by the vulnerability.[108] This highlights underlying security issues in the ActiveX security model through which attackers are able to silently install vulnerable ActiveX components that are cryptographically signed by a vendor within the trusted certificate store of Internet Explorer.

The prevalence of ActiveX vulnerabilities poses a particular concern to end users and organizations that use Internet Explorer. While the market share of Internet Explorer 7 surpassed that of Internet Explorer 6 in 2008, the fact that ActiveX vulnerabilities are still a popular avenue of attack suggests that the security features of Internet Explorer 7 have not eliminated the ActiveX threat.[109] It appears that end users are overriding these security features and continue to allow insecure ActiveX controls to be installed and executed. Microsoft Internet Explorer 8 is slated to include additional security features to manage the threat of insecure ActiveX controls.[110] It is uncertain whether better ActiveX security in Internet Explorer 8 will have an effect on the number of vulnerabilities in the short term, since there are still many insecure

[106] https://forums2.symantec.com/t5/Vulnerabilities-Exploits/Microsoft-Access-Snapshot-Viewer-Exploited-in-Neosploit-Wrapper/ba-p/335199#A164
[107] https://forums2.symantec.com/t5/Vulnerabilities-Exploits/Neosploit-Updated-with-Exploit/ba-p/314840#A151
[108] https://forums2.symantec.com/t5/Vulnerabilities-Exploits/ActiveX-Vulnerabilities-Even-When-You-Aren-t-Vulnerable-You-May/ba-p/341705#A165
[109] http://www.w3schools.com/browsers/browsers_stats.asp
[110] http://blogs.msdn.com/ie/archive/2008/05/07/ie8-security-part-ii-activex-improvements.aspx

ActiveX controls available for download on the Internet. However, there may be fewer incidents and examples of these vulnerabilities being incorporated into attack toolkits if the security measures being implemented by Microsoft are effective.

Other plug-in technologies such as Acrobat were also subject to exploitation in the wild.[111] For instance, the number of plug-in vulnerabilities in Java rose due to increased interest from the security research community. Java is an attractive target because it runs in most Web browser versions on most operating systems. This means that many of the vulnerabilities in the Java plug-in facilitate the development of cross-platform exploit code. This represents an ideal scenario for attackers because it exposes a large number of targets to simple and reliable exploitation. Attackers seek vulnerabilities that affect widely deployed applications that can be attacked through the Web browser.

### Web browser plug-in vulnerabilities, by type

This discussion will examine some specific vulnerabilities that affect browser plug-ins. To do so, the vulnerabilities covered in the previous metric are classified into various categories based on their security impact. The impact of a vulnerability helps to determine the means by which an attack accomplishes its goal by exploiting the vulnerability. It also helps administrators prioritize the risks posed by a specific vulnerability and develop mitigations that are in proportion to the threat.

The categories below are meant to highlight the primary impact on end users. It should be noted that some vulnerabilities defy categorization due to inadequate public information about the nature of the vulnerability and its potential impact. Vulnerabilities that could not be categorized are noted in the discussion.

Vulnerabilities affecting browser plug-in technologies are classified into the following distinct categories:[112]

- **Memory corruption:** These vulnerabilities allow attackers to corrupt the memory of an application process with malicious input and can allow attackers to execute arbitrary code.
- **Denial-of-service (DoS):** DoS vulnerabilities typically result in an application crash when exploited. Although this could be due to a memory corruption issue, these vulnerabilities are classified as DoS when no potential of arbitrary code execution is apparent.
- **Information disclosure:** These vulnerabilities most often expose sensitive information to an unauthorized party, either as a result of active exploitation or as an inadvertent side effect of an erroneous condition in the application.
- **Content injection:** These vulnerabilities allow the injection of malicious content or allow attackers to bypass third-party input validation filters; they can also enable cross-site scripting attacks.
- **Spoofing:** These vulnerabilities allow an attack to spoof elements of the browser-user interface.
- **Unauthorized file system access:** These vulnerabilities allow attackers to view, modify, or delete files on the computer hosting the affected browser plug-in.

[111] https://forums2.symantec.com/t5/Vulnerabilities-Exploits/Acrobat-util-printf-Exploit-Detected-with-Existing-IPS/ba-p/364088#A176
[112] For a more complete description of these categories, please see Appendix C—Vulnerability Trends Methodologies

- **Command execution:** These vulnerabilities allow a remote attacker to execute operating system commands through an affected browser plug-in.
- **Origin validation:** These vulnerabilities can occur when content from an invalid or unauthorized originating source is treated as valid by a plug-in.
- **Elevated security context:** These vulnerabilities violate a security policy intended to prevent remote content from accessing system properties and capabilities. It should be noted that some vulnerabilities may present an opportunity for elevated security bypass but are more accurately described by another category.

In 2008, of the 415 vulnerabilities identified in browser plug-ins, 271 were classified as memory corruption vulnerabilities (figure 12). This is followed by 61 unauthorized file system access vulnerabilities, 27 elevated security context vulnerabilities, 14 DoS attack vulnerabilities, 13 information disclosure vulnerabilities, nine command execution vulnerabilities, eight origin validation vulnerabilities, four content injection vulnerabilities, and one vulnerability that facilitated spoofing attacks. The remaining seven vulnerabilities could not be classified due to insufficient information about their causes and effects.

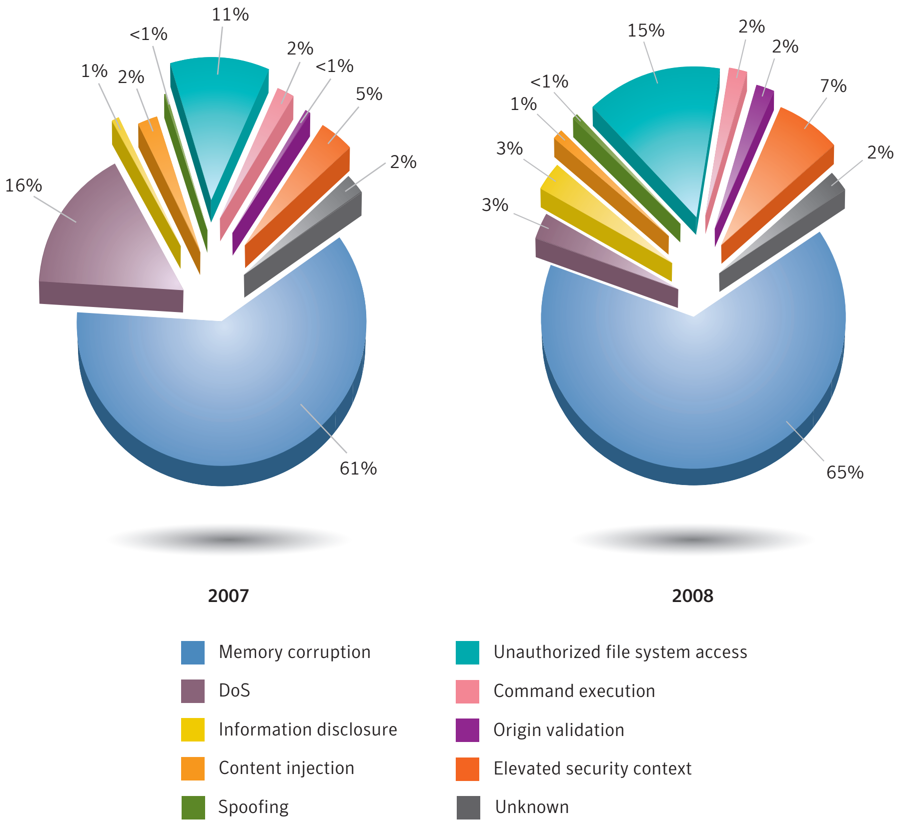

**Figure 12. Web browser plug-in vulnerabilities, by type**
*Source: Symantec*

Memory corruption vulnerabilities also made up the majority of plug-in vulnerabilities in 2007, with 288 being classified as such out of 475 total vulnerabilities identified (table 5). Of the remaining, 76 were considered DoS issues, 54 allowed unauthorized file system access, 24 allowed elevated security context, nine allowed command execution, eight allowed content injection, five vulnerabilities allowed information disclosure, and two were related to origin validation. There were no spoofing vulnerabilities in browser plug-in technologies in 2007 and nine vulnerabilities could not be classified due to a lack of information about the causes and effects of the vulnerabilities.

Memory corruption vulnerabilities constituted the majority of browser plug-in vulnerabilities in both 2007 and 2008. However, the data indicates that DoS vulnerabilities were less prevalent in 2008 than they were in 2007. In 2008, they were displaced by unauthorized file system access vulnerabilities as the second highest proportion of plug-in technology vulnerabilities. In October of 2008, Symantec noted the rise in unauthorized file system access vulnerabilities affecting ActiveX controls.[113] At that time, attackers had integrated a number of exploits for these issues into attack toolkits, proving their effectiveness and popularity among attackers. In the same month, Symantec also observed new attack patterns for unauthorized file system access vulnerabilities that affected ActiveX controls.[114] These attack patterns can allow attackers to exploit unauthorized file system access vulnerabilities to execute arbitrary code.

The decrease of DoS vulnerabilities and increase in vulnerabilities such as unauthorized file system access and elevated security context indicate an evolving skill set among security researchers and attackers. In particular, researchers and attackers are developing their skills to pinpoint higher-severity vulnerabilities that allow remote code execution and other serious consequences. This also explains the prevalence of memory corruption vulnerabilities in browser plug-ins because, if successfully exploited, they will let an attacker run arbitrary code on the affected computer. DoS vulnerabilities in plug-in technologies are often the result of unskilled security research efforts because their effect on client applications is minimal in comparison to DoS vulnerabilities affecting servers. As a result, it is not as worthwhile to discover lower-severity vulnerabilities such as DoS. Security researchers and attackers with an advanced skill set usually prefer to devote their efforts to finding more significant vulnerabilities that will ideally allow the underlying computer to be compromised in some way as a result of exploitation.

| Plug-in | 2008 Top Category | 2007 Top Category |
|---|---|---|
| Adobe Acrobat Reader | Memory corruption | Memory corruption/content injection/ command execution |
| Adobe Flash Player | Memory corruption/origin validation/ elevated security context | Elevated security context |
| ActiveX | Memory corruption | Memory corruption |
| Java | Elevated security context | Elevated security context |
| Mozilla Extensions | Content injection | Content injection |
| QuickTime | Memory corruption | Memory corruption |
| Windows Media Player | Memory corruption | Memory corruption/DoS |

**Table 5. Top categories for Web browser plug-in vulnerabilities**
*Source: Symantec*

[113] https://forums2.symantec.com/t5/Vulnerabilities-Exploits/ActiveX-File-Overwrite-Delete-Vulnerabilities-Continued/ba-p/361308#A175
[114] https://forums2.symantec.com/t5/Vulnerabilities-Exploits/Web-Attacks-Using-Microsoft-Help-and-Support-Center-Viewer/ba-p/360270#A172

For ActiveX, memory corruption vulnerabilities were the top category in 2008, as well as 2007. This is due to efforts among the security community to automate the discovery of these types of vulnerabilities by employing fuzzing tools. There are a number of publicly available fuzzing tools for ActiveX such as AxMan[115] and COMRaider.[116] Tools such as these were highlighted in previous volumes of the Symantec *Global Internet Security Threat Report*, and appear to still be widely used. There were numerous instances of in-the-wild exploitation of memory corruption vulnerabilities in ActiveX controls during 2008. Among the examples observed by Symantec were a vulnerability in the RealPlayer® ActiveX control,[117] a vulnerability in the Cisco WebEx™ control,[118] and a vulnerability in the CA™ BrightStor ActiveX component.[119] Symantec also observed that a new version of the NeoSploit attack toolkit included exploits for a number of vulnerabilities related to ActiveX memory corruption.[120]

For Java, the top category for plug-in vulnerabilities was elevated security context for both 2007 and 2008. This is due to vulnerability discoveries in the sandbox-based Java virtual machine security model.

For QuickTime, the top category for plug-in vulnerabilities in both 2007 and 2008 was memory corruption. Vulnerabilities that arise from handling malicious and malformed media content are common in QuickTime.

In 2008, the top category for plug-in vulnerabilities in the Acrobat Reader plug-in was memory corruption. This is a change from 2007, when memory corruption, content injection, and command execution were all in the top category. Symantec observed a number of exploits in the wild that targeted Acrobat. These include a vulnerability initially discovered in 2007,[121] Trojan attacks related to malicious PDF files,[122] and a buffer overflow in the implementation of a JavaScript function in Adobe Reader.[123] These vulnerabilities were all due to memory corruption conditions that were exposed when the application handled content inside of maliciously crafted PDF files.

For Flash Player, the top categories for vulnerabilities were memory corruption, origin validation, and elevated security content in 2008. In 2007, the top category was elevated security context.

Mozilla extensions had a top plug-in vulnerability category of content injection in 2007 and 2008. This is due to issues in third-party extensions that have allowed hostile HTML and script content to be injected.

For Windows Media Player, memory corruption was the top category for plug-in vulnerabilities in 2008. In 2007, the top categories were memory corruption and DoS. This is due to vulnerabilities in handling malicious and malformed multimedia content, as well as a number of vulnerabilities related to handling of malicious skin packages.[124]

Security research is often focused on areas where an application is perceived to be the weakest from a code quality or security design standpoint. When a particular avenue of attack has proven successful, security researchers and attackers attempt to search for similar vulnerabilities. Plug-in technologies such as ActiveX, Java, Mozilla extensions, and QuickTime have been prone to the same category of vulnerability in consecutive years. In some cases, this indicates that weak points have been identified in these technologies, resulting in repeated discoveries of similar vulnerabilities. Administrators should consider the track record of particular plug-in technologies for common types of vulnerabilities. This

[115] http://www.metasploit.com/users/hdm/tools/axman/
[116] http://labs.idefense.com/software/fuzzing.php#more_comraider
[117] https://forums2.symantec.com/t5/Vulnerabilities-Exploits/Unpatched-RealPlayer-Vulnerability-Being-Exploited-in-the-Wild/ba-p/314841#A152
[118] http://www.securityfocus.com/bid/30578/exploit
[119] http://www.securityfocus.com/bid/28268/exploit
[120] https://forums2.symantec.com/t5/Vulnerabilities-Exploits/Neosploit-Updated-with-Exploit/ba-p/314840#A151
[121] http://www.securityfocus.com/bid/27641/exploit
[122] https://forums2.symantec.com/t5/Vulnerabilities-Exploits/Pidief-the-Word-for-Exploits/ba-p/305564#A141
[123] http://www.securityfocus.com/bid/30035/exploit
[124] Skins are a feature of many applications that allow users to customize the application interface.

can provide guidance into vectors of attack that are likely to target these specific plug-in technologies. Security policies should be adjusted to anticipate these attack vectors, such as using a Web proxy to filter incoming multimedia content and applets and restricting the use of particular plug-ins.

### Web application vulnerabilities

This discussion focuses on the number of vulnerabilities disclosed during this reporting period that affect Web applications compared to the overall volume of vulnerabilities disclosed during the same period. This comparison provides insight into Web application security, which is especially important given the recent trend of attackers compromising trusted websites as a means of exploiting visitors to those sites.

In 2008, 63 percent of identified vulnerabilities affected Web applications (figure 13). This is an increase over 2007, when 59 percent of identified vulnerabilities affected Web applications. The previous volume of the Symantec *Global Internet Security Threat Report* noted a decrease in the proportion of Web application vulnerabilities in 2007.[125] This trend has not continued in 2008.

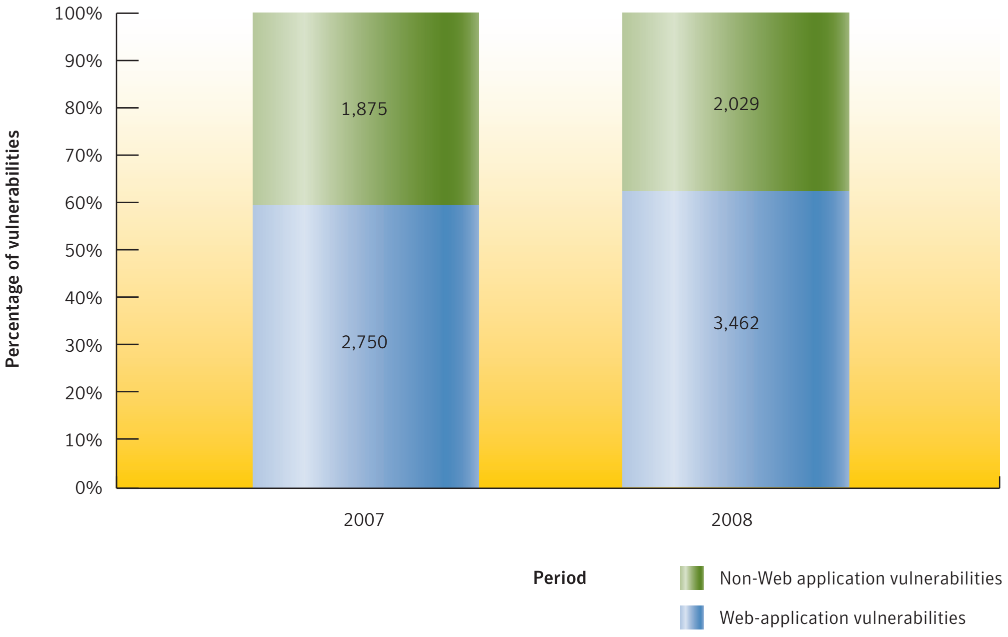

**Figure 13. Web application vulnerabilities**
*Source: Symantec*

In the previous volume of the Symantec *Global Internet Security Threat Report*, it was noted that there was a correlation between the rise in site-specific vulnerabilities and the drop in Web application vulnerabilities. In 2008, there may be a similar correlation as the number of site-specific cross-site scripting vulnerabilities was lower than 2007, while the proportion of Web applications was greater. This indicates that security researchers are dividing their attention between auditing specific websites and Web applications. Security researchers appeared to focus more effort toward Web applications in 2008; however, the number of Web application vulnerabilities discovered in 2008 is still small in comparison to the number of site-specific cross-site scripting vulnerabilities. This may mean that the incentives for discovering site-specific

[125] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf : p. 35

vulnerabilities are still greater for security researchers and attackers. For security researchers, the incentive is often the prestige associated with discovering a vulnerability in a high-profile website. Whereas for attackers, the incentives include finding a broader set of victims for attacks, which may increase the revenue-generating potential of their malicious activities.

In 2008 there were a number of high-profile incidents involving SQL injection vulnerabilities. Early in the year, there was a rise in SQL-injection vulnerabilities targeting Web applications implemented in classic ASP[126] with a Microsoft SQL Server database back-end.[127] The purpose of these attacks was to inject malicious content into compromised sites that would then attempt to exploit subsequent site visitors. Attackers used a technique that allowed them to dynamically inject malicious content into strings throughout the database without detection.[128] This provided a means of generically exploiting vulnerable applications rather than having to develop application-specific payloads.

Many classic ASP applications were prone to SQL-injection vulnerabilities in common variable names that could be easily identified. As a result, attackers developed tools that used search engines to identify vulnerable sites running vulnerable Web applications and exploit them.[129] This functionality was subsequently employed by botnets as a means of propagation.[130] This is noteworthy because it shows that attackers are advancing beyond trying to discover and exploit application-specific or site-specific vulnerabilities. Instead, this incident demonstrates that attackers are looking for the commonalities across an entire class of vulnerabilities to generically automate the discovery and exploitation of vulnerabilities. At this point, such discoveries are rare. However, this incident demonstrates a need for a defense-in-depth strategy that employs security countermeasures at the network, Web application, and database layers.

Late in 2008, SQL injection attacks were also used as a means to propagate exploit code for a zero-day vulnerability in Internet Explorer.[131] While SQL injection vulnerabilities have the potential to compromise sensitive information within the organization hosting a vulnerable website, it is interesting that attackers prefer to inject malicious content to attack other users instead. In the case of these attacks, the actual information assets of the organization have little value to the attackers, whose main objective is to exploit the trust placed in the organization as a means of attacking legitimate users of the website. This diverges from the premise of targeted attacks that are tailored toward a specific enterprise or organization. Instead, the compromised assets are only valuable to the attacker in that they provide a vehicle for indiscriminately attacking site visitors. The nature of the compromised site is less of a concern than the fact that users trust it and do not expect attacks to originate from a site they use on a regular basis. Even the characteristics of the users of a particular site are of little concern, except in that they may be vulnerable to the malicious content injected into the compromised site. This further perpetuates the trend observed in previous volumes of the Symantec *Global Internet Security Threat Report* of attackers shifting their attention toward exploiting trusted websites.

[126] Microsoft maintains classic ASP and the newer ASP.NET implementation. Classic ASP is an interpreted server-side scripting language for developing Web applications. ASP.NET is a server-side Web application development framework that depends on .NET and runs within the Common Language Runtime (CLR). Many sites are still implemented in classic ASP.
[127] http://blogs.technet.com/swi/archive/2008/05/29/sql-injection-attack.aspx
[128] http://blogs.technet.com/neilcar/archive/2008/03/15/anatomy-of-a-sql-injection-incident-part-2-meat.aspx
[129] http://isc.sans.org/diary.html?storyid=4294
[130] http://www.secureworks.com/research/threats/danmecasprox/
[131] https://forums2.symantec.com/t5/Vulnerabilities-Exploits/Rise-of-IE-Zero-Day-Through-SQL-Injection/ba-p/372832

## Site-specific cross-site scripting vulnerabilities

This metric examines vulnerabilities reported in specific websites. Site-specific vulnerabilities are a concern for enterprises because they are often used in multistage attacks that involve a compromise of a trusted website, which can then be used to attack subsequent targets. This means that a legitimate website that was previously considered safe by the organization may become the source of attacks against users within the organization. As a result, some security policies designed to limit the potential for attacks by permitting access to a small group of trusted websites are ineffective because those trusted websites could now become a source of malicious content.

This section will discuss a sub-category of Web-application vulnerabilities known as cross-site scripting vulnerabilities.[132] Cross-site scripting represents a sub-set of possible vulnerabilities that may affect specific websites; therefore, the data presented in this report is only a sample of the possible vulnerabilities that may be present in specific websites. It should also be noted that the data included in this metric does not cover all known public reports of site-specific vulnerabilities, but is limited to user-submitted data gathered by the XSSed Project.[133]

During 2008, there were 12,885 site-specific cross-site scripting vulnerabilities reported, compared to 17,697 in 2007.[134] Of the vulnerabilities reported in 2008, only 394 had been fixed by the website maintainer at the time of writing. This amounts to 3 percent of all site-specific cross-site scripting vulnerabilities reported in 2008. In 2007, 1,240 site-specific cross-site scripting vulnerabilities had been fixed at the time of writing.[135] This equates to 7 percent of the vulnerabilities reported in 2007 that affect specific websites.

The average amount of time it took for a website maintainer to fix a vulnerability in 2008 was 60 days. This is lower than the average of 76 days in 2007. This is a significant amount of time for users of the websites to be exposed to attacks that result from vulnerabilities.

While there were fewer site-specific cross-site scripting vulnerabilities in 2008, this may be indicative of different patterns of security research for the year rather than a quantitative improvement in the security of websites. In particular, there was a rise in the percentage of Web application vulnerabilities in 2008, which may indicate that security researchers have shifted some of their focus toward general Web applications as opposed to specific sites. The reason for the conclusion that site-specific security has not improved is that a small percentage of vulnerabilities are being fixed. Additionally, the amount of time taken to fix vulnerabilities in specific websites is significant. Website maintainers face different challenges in fixing vulnerabilities than do traditional software vendors, such as the potential for downtime or a disruption of services when a fix is rolled out. However, this does not explain the low rate of vulnerability remediation among website maintainers. There may be other factors such as a lack of concern by website maintainers because they do not perceive these issues as a threat. In some cases, the website maintainers may not be aware of the vulnerabilities.

Site-specific cross-site scripting vulnerabilities remain a serious issue for website maintainers and the users of affected sites. They may pose a threat to an enterprise because they can compromise website accounts of users within the organization. Additionally, these vulnerabilities may be used as a means of launching attacks against other computers within an organization. Administrators should monitor public

[132] For the purpose of this report, the term cross-site scripting encapsulates two broad classes of vulnerability; this includes traditional cross-site scripting and a category known as HTML injection (or persistent cross-site scripting).
[133] Data was provided by the XSSed Project, a site devoted to tracking and verifying reports of site-specific cross-site scripting vulnerabilities: http://www.xssed.com.
[134] At the time of writing, not all of the reported vulnerabilities have been processed; this means that the data used in this report does not reflect all of 2008; plus, the XSSed Project started in February 2007 and, as a result, data for all of 2007 was unavailable.
[135] It should be noted that these vulnerabilities were published in 2007, meaning the remainder remain unpatched at the time this report was written.

security intelligence sources for information about vulnerabilities affecting specific websites. If a website is known to be affected by an unpatched vulnerability, the administrator in the enterprise should consider blocking access to the affected site by users within the organization until the vulnerability is addressed. This mitigation should be used in combination with a white-list policy that permits access to approved websites only.

## Zero-day vulnerabilities

A zero-day vulnerability is one that appears to have been exploited in the wild prior to being publicly known. It may not have been known to the affected vendor prior to exploitation and at the time of the exploit activity the vendor had not released a patch. In the absence of available patches, zero-day vulnerabilities represent a serious threat since, in many cases, they likely will be able to evade purely signature-based detection. It is the unexpected nature of zero-day threats that causes concern, especially because they may be used in targeted attacks and in the propagation of malicious code.

In 2008, Symantec documented nine zero-day vulnerabilities, a decrease from the 15 documented in 2007. The decrease in the number of zero-day vulnerabilities is accounted for by a drop in vulnerabilities targeting region-specific applications. In the previous volume of the Symantec *Global Internet Security Threat Report*, it was noted that a number of Chinese- and Japanese-language applications were being targeted by attackers in zero-day attacks during 2007.[136] In 2008, there was only one such zero-day attack, early in the year, targeting two vulnerabilities in the GlobalLink ActiveX control.[137]

During both 2007 and 2008, the majority of vulnerabilities were present in ActiveX controls and the Microsoft Office® suite. The two primary attack vectors for zero-day vulnerabilities in both years were Microsoft Office and Internet Explorer. In 2008, six of the nine zero-day vulnerabilities could be exploited via Internet Explorer and Microsoft Office applications. In 2007, 13 of the 15 zero-day vulnerabilities could be exploited via these two applications.

In 2008, there was a significant event related to a non-client-side vulnerability. In particular, a zero-day vulnerability affecting the Microsoft Server Service was detected based on exploit activity in the wild.[138] Symantec observed multistage attacks on the vulnerability. In particular, Trojan.Gimmiv.A, once installed on a computer, will attempt to download an exploit for the vulnerability as a means to propagate itself on a local network on the compromised computer.[139] This mode of attack has advantages over a widespread worm-based attack across the Internet because it relies on the Trojan to penetrate into the protected internal network of an organization. From there, it can then exploit the vulnerability to compromise potentially less secure computers behind the network perimeter.

While this method of attack is not new in terms of a zero-day attack, it provides a less noisy alternative than developing a self-replicating worm that randomly attacks hosts on the Internet. It is also worth noting, however, that attack activity for this vulnerability subsequently became quite widespread due to public exploits and as propagation method for the Downadup worm (also known as Conficker, the worm is discussed in **"Top attacked vulnerabilities"**). This demonstrates that attacker motivations are diverse: while some attackers prefer to conduct targeted attacks with limited collateral damage, other attackers will take advantage of vulnerabilities such as this to compromise computers *en masse*. Worms remain a popular attack method when they present a viable means for attackers.

[136] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf : p. 39
[137] http://www.securityfocus.com/bid/27626
[138] http://www.securityfocus.com/bid/31874
[139] http://www.symantec.com/security_response/writeup.jsp?docid=2008-102320-3122-99&tabid=1

## Top attacked vulnerabilities

This metric will examine the top 10 attacked vulnerabilities. This data is based on events collected from Symantec intrusion prevention systems (IPS). The events are triggered by IPS signatures that are designed specifically to detect the specific vulnerabilities. When an event is triggered, it does not necessarily indicate that the exploit was successful, but merely that activity identified by the signature has been detected. This normally indicates an attempted attack.

For the purpose of this discussion, the attacked vulnerabilities are divided into their year of publication. This provides insight into which vulnerabilities published in 2007 and 2008 are being attacked in the wild. The discussion will cover the top 10 attacked vulnerabilities from each year, which are ranked according to the amount of activity associated with each vulnerability. This will help to pinpoint trends such as the types of vulnerabilities that are associated with the most attack activity, and the degree to which exploitation for these vulnerabilities has been automated by attackers. Enterprises may benefit from this information because it provides an indication of the types of vulnerabilities that attackers are most likely to employ in attacks and how to best protect against them.

The top attacked vulnerability for 2008 was the Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability (table 6). This was a zero-day vulnerability for which Microsoft released an emergency security bulletin in response to limited targeted attacks in the wild.[140] Attack activity for this vulnerability eventually became widespread, even after it was patched by Microsoft, due to various factors such as malicious code and the release of public exploits.[141] In particular, the Downadup worm uses this vulnerability as a means to propagate.[142] The automated nature of worm propagation is a driving factor behind the amount of attack activity associated with this vulnerability. This vulnerability has a server-side attack vector, meaning that attackers can exploit the vulnerability by sending malicious network traffic to an affected computer, as opposed to enticing a user into performing actions such as visiting a malicious website. As a result, the vulnerability facilitated the development of reliable exploit code that could be easily automated to attack arbitrary computers on the Internet.

| Ranking | BID | Title |
|---|---|---|
| 1 | 31874 | Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability |
| 2 | 30114 | Snapshot Viewer for Microsoft Access ActiveX Control Arbitrary File Download Vulnerability |
| 3 | 32721 | Microsoft Internet Explorer XML Handling Remote Code Execution Vulnerability |
| 4 | 31065 | Microsoft Windows Media Encoder 9 ‘wmex.dll’ ActiveX Control Remote Buffer Overflow Vulnerability |
| 5 | 27305 | Microsoft Excel Macro Validation Uninitialized Variable Manipulation Vulnerability |
| 6 | 30674 | Microsoft Visual Studio ‘Msmask32.ocx’ ActiveX Control Remote Buffer Overflow Vulnerability |
| 7 | 28157 | RealNetworks RealPlayer ‘rmoc3260.dll’ ActiveX Control Memory Corruption Vulnerability |
| 8 | 27578 | Yahoo! Music Jukebox ‘mediagrid.dll’ ActiveX Control Remote Buffer Overflow Vulnerability |
| 9 | 28570 | Microsoft Windows GDI ‘EMR_COLORMATCHTOTARGETW’ Stack Overflow Vulnerability |
| 10 | 27756 | Aurigma Imaging Technology 'ImageUploader4.1.ocx' FileMask Method ActiveX Buffer Overflow Vulnerability |

**Table 6. Top attacked vulnerabilities, 2008**
*Source: Symantec*

[140] http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx
[141] https://forums2.symantec.com/t5/Vulnerabilities-Exploits/Increase-in-Exploit-Attempts-Against-MS08-067/ba-p/367483#A178
[142] http://www.symantec.com/security_response/writeup.jsp?docid=2008-112203-2408-99&tabid=2

In contrast to the top attacked vulnerability for 2008, the remainder of vulnerabilities affected client and desktop software. In particular, the vulnerabilities targeted ActiveX controls and file handling routines in Microsoft desktop applications. This correlates with the conclusion drawn in the "Zero-day vulnerabilities" discussion that Microsoft Internet Explorer and Microsoft Office are primary targets for attackers. This also demonstrates that client-side vulnerabilities make up a large proportion of the vulnerabilities that attackers are exploiting in the wild. These vulnerabilities are likely to be incorporated into attack toolkits, which often employ the shotgun attack methodology, as described in the previous volume of the Symantec *Global Internet Security Threat Report*.[143] Server-side vulnerabilities constitute a smaller proportion but may result in widespread attack activity if it is possible to develop reliable automated exploit code that can be incorporated into worm attacks.

In 2007, Symantec observed a different pattern. The applications targeted by attacks were more diverse, including Adobe Photoshop®, RealPlayer, Apple QuickTime, and Adobe Acrobat Reader (table 7). The majority of top attacked vulnerabilities still targeted desktop applications; however, there were fewer that specifically targeted ActiveX controls. Another difference between the top attacked vulnerabilities in 2007 and 2008 was that none in the latter year targeted Microsoft Office.

| Ranking | BID | Title |
|---|---|---|
| 1 | 23621 | Adobe Photoshop Multiple File Format Buffer Overflow Vulnerability |
| 2 | 21829 | Apple QuickTime RTSP URI Remote Buffer Overflow Vulnerability |
| 3 | 21930 | Microsoft Windows Vector Markup Language Buffer Overrun Vulnerability |
| 4 | 26130 | RealPlayer 'ierpplug.dll' ActiveX Control Import Playlist Name Stack Buffer Overflow Vulnerability |
| 5 | 26549 | Apple QuickTime RTSP Response Header Content-Type Remote Stack Based Buffer Overflow Vulnerability |
| 6 | 24426 | Microsoft Internet Explorer Speech API 4 COM Object Instantiation Buffer Overflow Vulnerabilities |
| 7 | 27246 | 2Wire Routers Cross-Site Request Forgery Vulnerability |
| 8 | 26341 | Apple QuickTime STSD Atom Remote Heap Buffer Overflow Vulnerability |
| 9 | 25748 | Adobe Acrobat Mailto PDF File Command Execution Vulnerability |
| 10 | 22196 | NCTsoft NCTAudioFile2 ActiveX Control Remote Buffer Overflow Vulnerability |

**Table 7. Top attacked vulnerabilities, 2007**
*Source: Symantec*

## Attacked vulnerabilities by attack vector (client versus server)

This metric will examine the proportion of attacked vulnerabilities that have client-side and server-side attack vectors. The data covers the vulnerabilities that were published in 2008 that have had associated attack activity in the wild. Client-side vulnerabilities are those that affect client software such as Web browsers. They also include desktop application vulnerabilities that require interaction on the part of the user to successfully exploit. An example would be a vulnerability in a desktop application that required the user to visit a malicious website or download a malicious file to exploit. These vulnerabilities in desktop applications are frequently exploited through the Web browser, email client, or other network clients such as instant messaging and P2P.

[143] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf : p. 34

A server-side vulnerability is one that usually affects a networked service that is hosted on a computer. The service is often always running and awaits incoming connections from clients. In this case, exploitation typically occurs when the attack sends directly to the service malicious communications that are designed to exploit a particular vulnerability. The vulnerabilities typically do not require user interaction and typically affect a server-related component of the application. By examining the proportion of client-side and server-side vulnerabilities, it is possible to determine which attack vectors are most common for vulnerabilities that are attacked in the wild. This provides insight into the effectiveness of client-side and server-side security measures.

In 2008, 95 percent of attacked vulnerabilities were client-side vulnerabilities (figure 14). Five percent of the attacked vulnerabilities from 2008 were server-side vulnerabilities. In 2007, 93 percent of attacked vulnerabilities were client-side vulnerabilities. The remaining 7 percent in 2007 were server-side vulnerabilities.

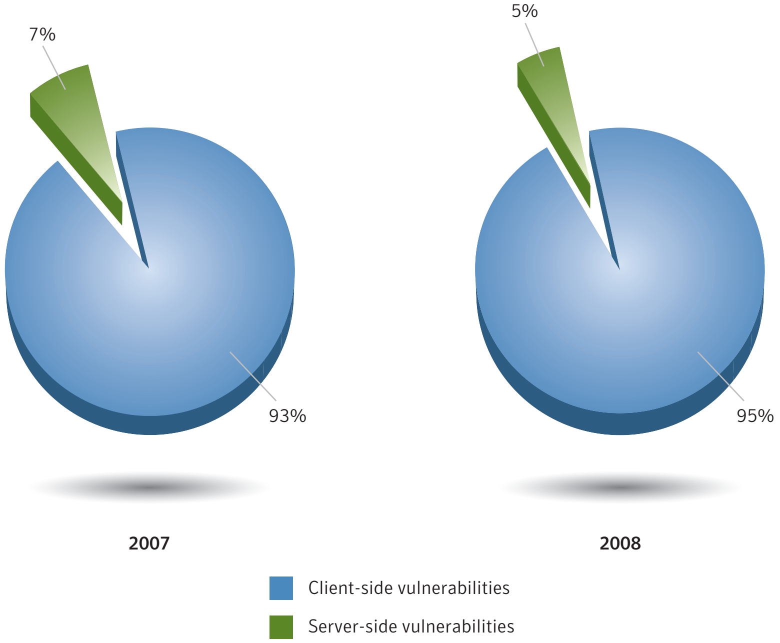

**Figure 14. Attacked vulnerabilities by attack vector, client versus server**
*Source: Symantec*

The differences between 2007 and 2008 are not significant, indicating a continuing trend toward attacking client-side vulnerabilities. This means that among the many vulnerabilities published within the year, attackers are more likely to choose client-side as a basis for their malicious activities. This is due to a number of factors such as network security perimeters, which make it difficult to execute server-side attacks because many networked services are concealed within an organization's internal network. Attackers employ client-side attacks as a means of circumventing these security measures since, instead of trying to penetrate a network's perimeter, the attacker relies on the client to download malicious content or visit a website that includes malicious content that will exploit the victim's client software and desktop applications. From this point, an attacker can install malicious software such as Trojans and bots, steal confidential information, and attack other computers on the network.

As noted in the "Top attacked vulnerabilities" discussion, the top vulnerability of 2008 affected the Microsoft Windows Server Service. This is an example of a vulnerability with a server-side attack vector that possessed a particular combination of traits that made it a successful and lucrative means of attack. These traits include the possibility for reliable and automated exploitation, and a large base of computers running the affected component by default.

It is also worth noting that the Trojan.Gimmiv.A attacks exploiting this vulnerability attempted to bypass the network perimeter by compromising a host and then launching attacks on the host's internal network. To combat such threats, many organizations have erected network perimeter security measures, which have been largely successful in preventing server-side attacks. In many cases, server applications are deployed within the network perimeter and are not exposed to attacks originating from the Internet. Very few services remain exposed to the Internet. The data demonstrates that it is only in rare cases that server-side vulnerabilities are subject to widespread attacks. By and large, attackers have shifted toward client-side attacks. This trend will likely continue until client-side security improves or other more successful and lucrative attack vectors present themselves.

## Vulnerabilities—protection and mitigation

In addition to the specific steps required to protect against the vulnerabilities discussed in this section, there are general steps that should be taken to protect against the exploitation of vulnerabilities. Administrators should employ a good asset management system to track the assets that are deployed on the network and to determine which ones may be affected by the discovery of new vulnerabilities. Administrators should monitor vulnerability mailing lists and security websites to keep abreast of new vulnerabilities affecting their assets. Where possible, patch deployments should be automated to ensure that vulnerabilities are addressed across the organization in a timely manner.

Symantec recommends that administrators employ vulnerability assessment services, a vulnerability management solution, and vulnerability assessment tools to evaluate the security posture of the enterprise. These measures should be incorporated into infrastructure change-management processes. Organizations should employ third-party consulting and penetration testing services to identify security exposures. For any products or applications developed by the organization, code-auditing software and services may help to identify and address vulnerabilities at various stages of development.

Unpatched vulnerabilities should be identified by administrators, and assessed and mitigated according to the risk they present. Where possible, problematic applications with many unpatched vulnerabilities should be removed or isolated. IPS systems can aid in detecting known attacks against such applications and provide generic protection against vulnerabilities. Security information and event management should be deployed to assist in data management within the enterprise infrastructure and aid in policy compliance.

In order to protect against successful exploitation of Web browser vulnerabilities, Symantec advises users and administrators to upgrade all browsers to the latest, patched versions. Symantec recommends that organizations educate users to be extremely cautious about visiting unknown or untrusted websites and viewing or following links in unsolicited emails. Administrators should also deploy Web proxies in order to block potentially malicious script code. Administrators and end users should actively maintain a whitelist of trusted sites and disable individual plug-ins and scripting capabilities for all other sites. This will not prevent exploitation attempts from whitelisted sites, but may aid in preventing exploits from all other sites. Organizations can also implement an egress filtering policy at the network perimeter to regulate outgoing access by end users. Antivirus and host-based IDS and IPS solutions at the desktop level also provide a layer of protection against attacks that originate from the Web.

Enterprises should subscribe to a vulnerability alerting service in order to be notified of new vulnerabilities. They should also manage their Web-based assets carefully. If they are developing Web applications in-house, developers should be educated about secure development practices, such as the Security Development Lifecycle and threat modeling.[144] If possible, all Web applications should be audited for security prior to deployment and only those applications that have been certified should be deployed. Web application security solutions and a number of products and services are available to detect and prevent attacks against these applications.

When deploying applications, administrators should ensure that secure, up-to-date versions are used, and that applications are properly configured to avoid the exploitation of latent vulnerabilities. Symantec recommends the use of secure shared components that have been audited for common Web application vulnerabilities. As much as possible, enterprises are advised to avoid deploying products that are not regularly maintained or that are not supported by the vendor.

[144] The Security Development Lifecycle is a development paradigm that incorporates security at every stage from the initial architecture to programming, and in the quality assurance/testing phases; threat modeling is a security auditing methodology to identify and map out all possible attack vectors for an application.

## Malicious Code Trends

Symantec gathers malicious code intelligence from more than 130 million client, server, and gateway systems that have deployed its antivirus products. Underpinning these products are the Symantec Digital Immune System and Symantec Scan and Deliver technologies, as well as Norton Community Watch, which allow customers to automate the process of reporting viruses and other malicious code threats.

This discussion is based on malicious code samples reported in 2008, with the following trends being analyzed:

- New malicious code threats
- Top 10 new malicious code families
- Malicious code types
- Staged downloaders—multiple infections by type
- Geolocation by type of malicious code
- Threats to confidential information
- Propagation mechanisms
- Malicious code that exploits vulnerabilities
- Malicious code—protection and mitigation

### New malicious code threats

Symantec monitors the proliferation of malicious code by examining the number of new malicious code signatures created to detect threats from period to period. Comparing new signatures against signatures created previously indicates how quickly new malicious code threats are being developed. Periods in which a significant number of new malicious code threats are created indicates how critical it is for both enterprises and home users to maintain updated antivirus signatures, and to implement and maintain robust security measures such as software patches.

In 2008, Symantec created 1,656,227 new malicious code signatures (figure 15). This is a 265 percent increase over 2007, when 624,267 new malicious code signatures were added. Although the percentage increase in signatures added is less than the fairly staggering 445 percent increase from 2006 to 2007, the overall number of malicious code signatures by the end of 2008 grew to 2,674,171. This means that of all the malicious code signatures created by Symantec, more than 60 percent of that total was created in 2008. Furthermore, Symantec blocked an average of more than 245 million attempted malicious code attacks worldwide each month in 2008.

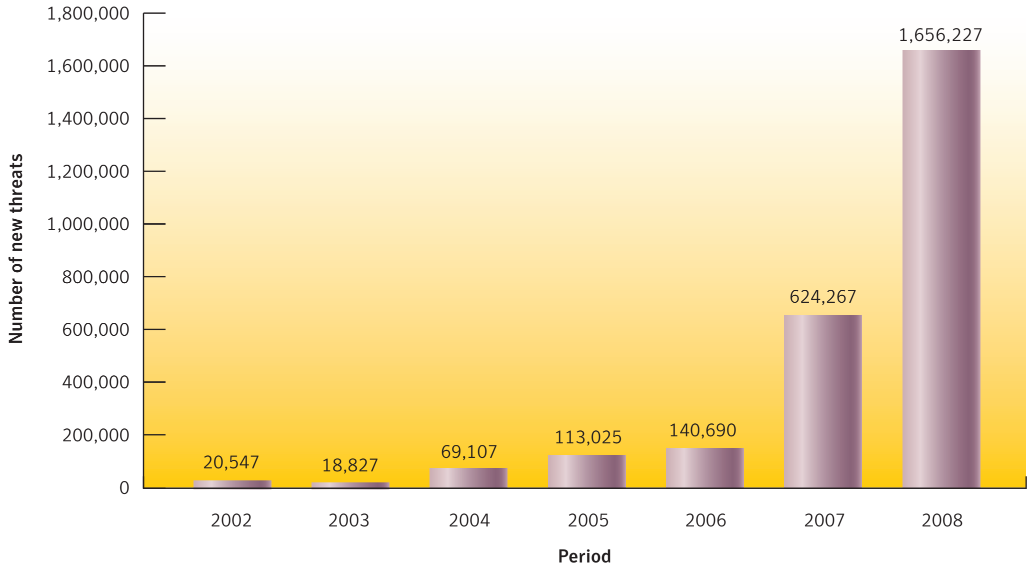

**Figure 15. New malicious code signatures**
*Source: Symantec*

Previous volumes of the Symantec *Global Internet Security Threat Report* have discussed the increasing professionalization of malicious code development.[145] The result is an increase in the speed and efficiency with which malicious code is "brought to market," which would enable an increased number of threats to be developed. A driving force behind the growing speed and efficiency of these developments is the demand for goods and services that facilitate online fraud. This is exemplified by the flourishing profitability of confidential information sales, as was discussed in the recently published Symantec *Report on the Underground Economy*.[146] For example, Symantec estimated the value of total advertised goods on underground economy servers between July 2007 and June 2008 to be $276 million.

Of particular value in the underground economy is malicious code that exposes confidential information. This is because confidential information is critical to several illegal practices, such as identity theft and credit card fraud. Symantec has determined that, in many instances, this code is being developed on a large scale by well-organized programmers, much as applications are developed in a legitimate software enterprise. The demand for malicious code in the underground economy is further illustrated by advertisements specific to such goods, with some advertisers selling the malicious code itself and others requesting the services of malicious code authors. Advertisements for malicious code authors are often looking for the one-time development of specific code to create new variants of existing threats, rather than developing entirely new threats. This is likely because variants of existing malicious code can be developed more easily, and can therefore be brought to market in the underground economy much more quickly.

[145] Cf. http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf : p. 9 and http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_09_2007.en-us.pdf : p. 12
[146] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_underground_economy_report_11-2008-14525717.en-us.pdf : p. 6

## Top 10 new malicious code families

Symantec analyzes new malicious code families detected during each reporting period to determine what threat types and attack vectors are being employed in the most prevalent new threats. This information allows administrators and users to gain familiarity with threats that may gain future notoriety. Insight into emerging threat development trends can help bolster security measures and mitigate future attacks.

In 2008, there were six Trojans in the top 10 new malicious code families detected (table 8). Three of the six Trojans include a back door component and one includes a virus component.[147] The remaining four families consist of worms, one of which has a back door component and one of which has a virus component.

The previous edition of the Symantec *Global Internet Security Threat Report* noted that the prevalence of Trojans is indicative of multistage attacks.[148] A multistage attack typically involves an initial compromise, followed by the installation of an additional piece of malicious code, such as a Trojan that downloads and installs adware. As was the case in 2007, during this reporting period, five of the top 10 new malicious code families that were identified download additional threats. These multistage attacks are examined in greater detail in the **"Staged downloaders—multiple infections by type"** discussion that follows.

During this reporting period, the Brisv Trojan[149] was the most widely reported new malicious code family. Unsurprisingly, this Trojan continues to garner interest beyond 2008, having possibly affected as many as 1.6 million computers during a surge of activity in February 2009.[150] Brisv scans computers for multimedia files, including .asf, .mp2, .mp3, .wma and .wmv. The Trojan then modifies a data marker in the files with a malicious URL. The marker is a part of the Windows Media Audio (WMA) format. Although other applications appear to be unaffected, when the files are opened using Windows Media Player, the marker is automatically processed, causing the application to open a Web browser window and access the malicious URL. Accessing the malicious URL may expose the user to additional threats.

The effectiveness of Brisv is heightened by the possibility that unknowing victims may share the compromised multimedia files with others, through P2P or email, etc. As a result, the compromised files can potentially affect users whose computers were not exposed to the Trojan itself.

Moreover, when Brisv scans for multimedia files, it converts all .mp2 and .mp3 files it encounters into the .wma format prior to injecting the malicious code, even while preserving the original file extensions of the (now) converted files. The reason for converting files into the .wma format is so that Windows Media Player will process the injected marker data properly. This is an example of increased sophistication in malicious code development.

[147] Back door components allow attackers to remotely connect to a compromised computer, typically using a specialized application. Once connected, the attacker can perform numerous actions such as taking screenshots, changing configuration settings, and uploading, downloading, or deleting files.

[148] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf : p. 46

[149] http://www.symantec.com/security_response/writeup.jsp?docid=2008-071823-1655-99&tabid=1

[150] http://voices.washingtonpost.com/securityfix/2009/02/consider_the_source_not_just_t.html

| Rank | Sample | Type | Vectors | Impact |
|---|---|---|---|---|
| 1 | Brisv | Trojan | N/A | Modifies multimedia files, causing Windows Media Player to open malicious URLs |
| 2 | Tidserv | Trojan/back door | N/A | Allows remote access, installs additional threats, and displays advertisements |
| 3 | Auraax | Worm | CIFS | Downloads additional threats |
| 4 | Blusod | Trojan | N/A | Downloads additional threats and displays fake error and alert messages |
| 5 | Ircbrute | Worm/back door | Removable drives | Allows remote access and performs DoS attacks |
| 6 | Spakrab | Trojan/back door | N/A | Allows remote access and sends system data as well as email addresses to the attacker |
| 7 | Wowinzi | Worm/virus/ back door | Mapped and removable drives, CIFS | Steals confidential information, downloads additional threats, and allows remote access |
| 8 | Mandaph | Worm | Mapped drives | Downloads additional threats |
| 9 | Brojack | Trojan | N/A | Modifies Internet settings and removes Web browser plug-ins |
| 10 | Mebroot | Trojan/back door | N/A | Overwrites the Master Boot Record (MBR) and allows remote access |

**Table 8. Top 10 new malicious code families**
*Source: Symantec*

The second ranked new malicious code family in 2008 was the Tidserv Trojan.[151] Tidserv is delivered primarily as a spammed email attachment titled "e-card," although other methods are also used. Tidserv works by installing a rootkit to obfuscate its presence on the computer and then opening a back door for the delivery of additional threats. Tidserv also displays advertisements for various goods, indicating that there may be financial motivation behind the distribution of the Trojan. These ads are hosted remotely and, much like legitimate Internet advertising, the attacker can rotate the ads as desired.

The Auraax worm[152] was the third ranked new malicious code family in 2008. This worm propagates by copying itself to all removable drives and network shares that it can locate. An autorun instruction file is also created in these drives or shares that automatically executes Auraax whenever the drives or shares are accessed.[153] The worm obfuscates itself by overwriting certain kernel drivers with a rootkit.[154] It also downloads additional threats, including misleading applications, onto affected computers.

Once installed, Auraax protects itself by modifying the "hosts" file to prevent users from accessing a list of computer security websites.[155] The URLs of these sites are added to the hosts file and configured so that access to the URLs is redirected to the local address. Interestingly, Auraax also does the same with the URLs of some advertising websites, adding them to the hosts file and making them inaccessible. This is somewhat peculiar behavior because malicious code is more typically used to distribute advertisements and increase hits to advertising Web pages, rather than to hide them. This could be because some of the additional threats downloaded by Auraax attempt to target and replace advertisements by legitimate organizations. By making the websites of those organizations inaccessible, the worm may be attempting

[151] http://www.symantec.com/security_response/writeup.jsp?docid=2008-091809-0911-99&tabid=1
[152] http://www.symantec.com/security_response/writeup.jsp?docid=2008-092409-4704-99&tabid=2
[153] Autorun is a function of the Windows operating system that launches newly detected processes or applications (e.g., the insertion of a CD-ROM or USB drive). Windows searches the root directory of the drive for an autorun information file that contains instructions for what process or application to launch.
[154] A collection of tools (programs) that enable administrator-level access to a computer or network.
[155] The "hosts" file contains a lists of hostnames mapped to IP addresses. This information is used by computers, in conjunction with or in lieu of DNS (domain name system), to locate nodes on the network.

to increase the chances that URLs in the illegitimate advertisements are accessed instead of those in the legitimate ones. This could be particularly deceiving for users because the maliciously placed advertisements may appear in the same locations and styles as those of the legitimate advertisements.

Worth noting here is that the Downadup worm ranked eleventh among the new malicious code families. This is a significantly high ranking considering the worm did not emerge on the threat landscape until November 2008. Had Downadup emerged earlier, it would likely have ranked much higher. The worm did, however, rank seventh among the top 10 new malicious code families in the APJ region, where it initially spread. Although its spread is slowing, Symantec expects Downadup to continue to have a significant impact on the threat landscape in 2009.

## Malicious code types

Analyzing the prevalence of malicious code types provides insight into the general diversity in the threat landscape and, combined with the data of other metrics, helps Symantec more accurately determine emerging trends in malicious code. It should be noted that the volume of top 50 potential malicious code infections in 2008 was more than twice the volume of 2007. Therefore, decreases in percentages may not indicate a year-over-year decline in potential infections.

The percentages of malicious code types in the top 50 potential malicious code infections for 2008 remained largely similar to those in 2007. As in previous reporting periods, Trojans made up the highest percentage of the volume of the top 50 potential malicious code infections (figure 16), although there was 1 percent decrease down to 68 percent in 2008.[156]

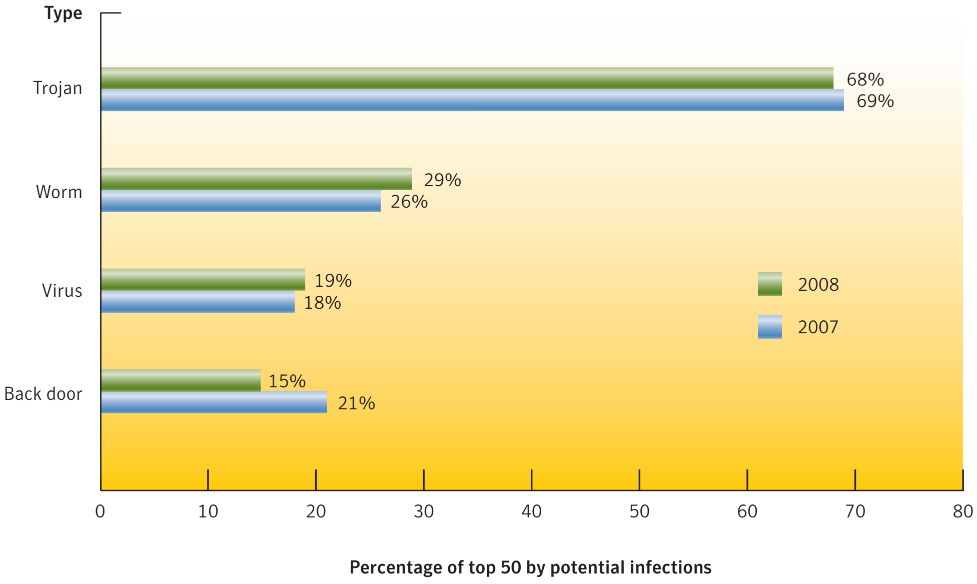

**Figure 16. Malicious code types by volume of potential infections**
*Source: Symantec*

[156] It should also be noted that malicious code samples may be comprised of multiple components that are each classified as different types; as a result, cumulative percentages discussed in this metric may exceed 100 percent.

The previous volume of the Symantec *Global Internet Security Threat Report* discussed the possibility that attackers are gravitating toward the use of a smaller number of more successful Trojans.[157] This means that once a Trojan has had a moderate degree of success, minor variations of it are continuously created and used in new attacks. Using this approach, malicious code developers in the underground economy can increase productivity and bolster the supply of goods for sale in the underground economy. The rapid deployment of variant threats also serves malicious code developers by increasing the pressure on the resources of security organizations and enterprises to respond to these challenges.

The top malicious code sample causing potential infections in 2008 (as well as 2007) was the Vundo Trojan.[158] The main goal of Vundo is to download and install adware on a victim's computer. This attack should be popular with attackers since the adware component is designed to generate revenue from every compromised computer. In some cases, malicious code authors may be contracted by adware developers to install a negotiated number of applications, with no questions asked as to their methods. By implementing the adware installation process into their malicious code, the malicious code authors are becoming more efficient and, thus, increasing productivity. The continued prevalence of this threat into 2008 and its potential for revenue generation is indicative of the increasing commercialization and professionalization of malicious code.

The Gampass Trojan[159] was the second ranked sample causing potential infection in 2008, and also the most downloaded component in multistage attacks in 2008. This is another example of malicious code that is clearly meant to generate revenue. Gampass uses keystroke-logging functionality[160] in order to steal authentication credentials for online gaming accounts. The accounts are then usually sold in the underground economy. For example, Symantec observed advertisements for these accounts ranging from $8 to $50 each in 2008.

The second highest percentage of the top 50 potential malicious code infections for 2008 belonged to worms, which increased to 29 percent from 26 percent in 2007. At that time, there were indications that the decline in worms was leveling off, which is supported by the relatively static percentage of potential worm infections between 2007 and 2008.[161] Two prominent mass-mailing worms that bolstered worm numbers in the previous reporting period were Netsky[162] and Rontokbro.[163] Both of these worms and others from 2007 also accounted for a significant number of potential infections in 2008. This may indicate that attackers are making increased use of lingering threats to take advantage of previously successful attacks.

The third highest percentage of the top 50 potential malicious code infections in 2008 was potential virus infections, which increased to 19 percent in 2008 from 18 percent previously. The slight increase is primarily due to a rise in new worms with a viral infection component. For example, the Wowinzi worm,[164] which ranked eighth in the top new malicious code families for 2008, incorporates a viral infection component and spreads by copying itself to mapped, fixed, and removable drives. Furthermore, many of the prominent worms from 2007 that contain viruses continued to be prevailing threats in 2008, and the number of potential infections increased. By incorporating viral components into worms, malicious code authors can increase infection rates by adding multiple propagation techniques. At the same time, the threat will be more entrenched on compromised computers due to the nature of viral infection.[165]

[157] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf : p. 49
[158] http://www.symantec.com/security_response/writeup.jsp?docid=2004-112111-3912-99
[159] http://www.symantec.com/security_response/writeup.jsp?docid=2006-111201-3853-99
[160] Keystroke logging applications record keystrokes on compromised computers and return the data to the attacker. The data can be filtered to extract fraud-worthy information such as user account credentials for online banking websites, stock trading websites, or online game accounts.
[161] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf : p. 50
[162] http://www.symantec.com/security_response/writeup.jsp?docid=2004-021615-4827-99
[163] http://www.symantec.com/security_response/writeup.jsp?docid=2008-021916-0751-99
[164] http://www.symantec.com/security_response/writeup.jsp?docid=2008-050714-5642-99
[165] http://service1.symantec.com/SUPPORT/nav.nsf/aab56492973adccd8825694500552355/024c927836400f528825675100593eb2?OpenDocument&src=symsug_us

The previous volume of the Symantec *Global Internet Security Threat Report* discussed the increasing use of removable drives as a means for worms and viruses to propagate.[166] This was a popular means of infection when floppy disks were a primary medium for data transfer. However, the use of the propagation mechanism dropped significantly when transfer options over the Internet (such as email, FTP, etc.) became more widespread. The recent popularity of removable storage devices (such as portable media players, USB drives, etc.) has led to a resurgence in use of the propagation mechanism by malicious code authors. Furthermore, the relatively massive storage capacity of some of these devices can facilitate larger threats, as well as potentially allowing malicious code to go unnoticed among other data stored within. Some malicious code is designed to automatically create copies of itself on removable devices that are connected to an infected computer. When an unknowing user removes the infected device and connects it to another computer, the worm then automatically copies itself to the newly attached computer. This could be especially dangerous to enterprises if the infected device is connected to a network. This trend continued in 2008, and is a contributing factor to the increase in potential virus infections.[167]

The only proportional decline in potential infections was primarily due to a drop in back doors. In 2008, back doors made up 15 percent of the volume of top 50 potential malicious code infections, down from 21 percent in 2007. This drop is mainly attributed to the modest increases in other types of malicious code. This may also be an indication that, due to the trend toward multistage attacks, back doors are not being incorporated into new frontline threats, but instead are being used in the later stages of attacks. Furthermore, one tactic that is employed in first-stage attacks is to disable or reduce the software capabilities on affected computers so that threats that are installed during later-stage attacks may have a better chance of going undetected. This would reduce the need for new unique back doors or Trojans.

### Staged downloaders—multiple infections by type

Staged downloaders are threats that download and install other malicious code onto a compromised computer. These threats allow attackers to change the downloadable component to any type of threat that suits their objectives, or to match the profile of the computer being targeted. For example, if the targeted computer contains no data of interest, attackers can install a Trojan that relays spam, rather than one that steals confidential information. As the attackers' objectives change, they can change any later components that will be downloaded to perform the requisite tasks.

Of the top 50 potential malicious code infections, 79 percent downloaded additional threats. In 2008, the Wimad Trojan[168] was the most prevalent downloader component (table 9). This Trojan arrives on computers as a license-protected multimedia file. When the file is opened, Wimad exploits the intended functionality of digital rights management (DRM) technology in order to open a window and access an attacker-controlled URL. When an attacker's Web page is processed, a deceptive message is displayed, enticing the user to click a button. If it is clicked, the Trojan will download other threats, including adware and spyware.

[166] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf : p. 51
[167] Cf. https://forums2.symantec.com/syment/blog/article?blog.id=malicious_code&thread.id=220 or http://www.publicsafety.gc.ca/prg/em/ccirc/2008/in08-007-eng.aspx
[168] http://www.symantec.com/security_response/writeup.jsp?docid=2005-011213-2709-99

| Rank | Sample | Type | Impact |
|---|---|---|---|
| 1 | Wimad | Trojan | Uses Microsoft Windows Media Digital Rights Manager to trick user into downloading files |
| 2 | Vundo | Trojan | Redirects browser to malicious Web page |
| 3 | Zlob | Trojan | Downloads files from remote addresses |
| 4 | Spybot | Worm/back door | Downloads files from remote addresses |
| 5 | Metajuan | Trojan/back door | Downloads files from remote addresses |
| 6 | Imaut | Worm | Downloads files from remote addresses |
| 7 | Pandex | Trojan | Downloads files from remote addresses |
| 8 | Vundo.B | Trojan/back door | Redirects browser to malicious Web page |
| 9 | Sality | Worm/virus | Downloads files from remote addresses |
| 10 | Virantix | Trojan | Downloads files from remote addresses |

**Table 9. Top 10 staged downloaders**
*Source: Symantec*

Adware programs are components that are commonly downloaded by malicious code or sometimes even integrated into the malicious code itself, as is the case with the Adclicker Trojan, which is discussed below. Adware programs can also operate as stand-alone applications. Adware applications are popular because they are effective at generating revenue for malicious code authors; this is because adware generates traffic for advertising services that typically pay on a per-visit or per-view basis. Thus, their popularity as a commonly downloaded component is not surprising; five of the top 10 staged downloaders for 2008 download and install adware programs along with other components and threats.

The second most prevalent downloader component was the Vundo Trojan.[169] Once this Trojan is installed on a computer, it attempts to contact certain IP addresses to download and install its secondary components. One of the files it attempts to install is an adware program that will periodically display pop-up advertisements. If clicked, these ads will generate income for the malicious code author (and possibly the adware developer, if they are not the same person).

The Zlob Trojan[170] was the third most common staged downloader component in 2008. A successful implementation of this Trojan sets the home page, search, and “page not found” pages in the user’s browser to other pages hosting malicious code. Zlob also periodically displays fake security alerts that claim that the compromised computer is infected. If clicked, these error messages will redirect the browser to an attacker-controlled Web page promoting the download of an anti-spyware application that is actually additional malicious code.

The most prevalent downloaded component in 2008 was the Gampass Trojan (table 10). As mentioned previously, Gampass uses keystroke-logging functionality to steal authentication credentials for online gaming accounts. Popular targets include Lineage, Rexue, Jianghu, and Rohan, which are all popular games in the APJ region. Gampass is commonly downloaded by the Mummawow,[171] Wowinzi and Fubalca[172] worms, as well as others.

[169] http://www.symantec.com/security_response/writeup.jsp?docid=2004-112111-3912-99
[170] http://www.symantec.com/security_response/writeup.jsp?docid=2005-042316-2917-99
[171] http://www.symantec.com/security_response/writeup.jsp?docid=2007-032015-4300-99
[172] http://www.symantec.com/security_response/writeup.jsp?docid=2007-062214-3636-99

| Rank | Sample | Type | Impact |
|---|---|---|---|
| 1 | Gampass | Trojan | Steals online gaming account information |
| 2 | Adclicker | Trojan | Generates traffic to websites and banner ads |
| 3 | Graybird | Back door | Allows remote access, logs keystrokes, and steals passwords |
| 4 | Lineage | Trojan | Steals online gaming account information |
| 5 | Horst | Trojan/back door | Allows remote access and ends antivirus and firewall services |
| 6 | LowZones | Trojan | Lowers Internet Explorer security settings |
| 7 | Onlinegame | Trojan | Steals online gaming account information |
| 8 | KillAV | Trojan | Disables security applications |
| 9 | Bancos | Trojan | Steals online banking account information |
| 10 | Banker | Trojan | Logs keystrokes, steals passwords, redirects and intercepts network traffic |

**Table 10. Top 10 downloaded components**
*Source: Symantec*

The second most downloaded component in 2008 was the Adclicker Trojan.[173] This simple Trojan is intended to drive traffic to particular Web pages and click the banner advertisements. Banner advertisements compensate the owner of the website they are hosted on for each view or click-through.[174] Generating traffic to these advertisements by fraudulent means is commonly referred to as click fraud. The significant presence of other threats that are linked to financial gain, along with the flourishing vitality of the underground economy and the related success of Adclicker, may indicate a growing trend toward malicious code developed specifically to facilitate advertisement distribution.

Graybird[175] was the third most frequently downloaded component in 2008. This back door gives an attacker full remote access to a compromised computer. It also captures cached passwords, logs keystrokes, and then sends all of this information to the remote attacker. Furthermore, Graybird allows the attacker to download and install additional threats onto the compromised computer.

Many of the top downloaded components in 2008 ranked similarly to 2007, indicating that these families continue to be prevalent and effective threats. It is also noteworthy that six out of the 10 most downloaded components involve password stealing, keystroke logging, or advertisement promotion—all of which are further indications that profit continues to be the driving motivation for malicious code authors.

[173] http://www.symantec.com/security_response/writeup.jsp?docid=2002-091214-5754-99
[174] A click-through is a link that contains uniquely identifiable information about its originator that a user clicks on. Typically, the originator receives financial compensation for each click-through.
[175] http://www.symantec.com/security_response/writeup.jsp?docid=2003-040217-2506-99

## Geolocation by type of malicious code

Symantec examines the top regions reporting potential malicious code infections as well as the types of malicious code causing potential infections in each region. The increasing regionalization of threats can cause differences between the types of malicious code being observed from one area to the next, such as when threats employ certain languages or localized events as part of their social engineering techniques. Threats that steal confidential information can also be tailored to steal information that is more commonly available in some countries than in others. For instance, Trojans that attempt to steal account information for Brazilian banks are quite common in the LAM region, while malicious code that steals online gaming account information is most frequently observed in the APJ region.[176] Because of the different propagation mechanisms used by different malicious code types, and the different effects that each malicious code type may have, information about the geographic distribution of malicious code can help network administrators improve their security efforts.

It should be noted that the numbers presented in this discussion represent proportional geographic percentages. Therefore, proportional percentage fluctuation from the previous period to the current period does not indicate a change in the absolute number of reports from a specific region.

In 2008, the regional proportion of potential infections from malicious code remained largely unchanged; however, in all cases, the actual number of reports for each malicious code type from each region increased.[177] While there were small variances in some regions, the changes were not representative of significant shifts in the threat landscape. The proportion of reports from the EMEA region increased, which may indicate that the concentration of threats targeting countries in EMEA is growing faster than the concentration in other regions. This may also be a sign that the concentration of malicious code authors, or organizations employing those authors, is greater in EMEA than in other regions. One possible reason for a higher concentration in this region may be due to recent reports of politically motivated attacks during this period.[178] This sort of activity may have increased the demand for capable authors in EMEA.

### Trojans

In 2008, 35 percent of Trojans were reported from the North America (NAM) region, 34 percent from EMEA, 24 percent from APJ, and 6 percent from LAM (table 11). Although the number of Trojans reported from NAM appears to have dropped significantly, this is mainly attributable to the proportional increase in Trojans reported from EMEA, indicating that a similar amount of Trojan activity was reported in both NAM and EMEA in 2008.

| Region | 2008 Percentage | 2007 Percentage |
|---|---|---|
| NAM | 35% | 46% |
| EMEA | 34% | 28% |
| APJ | 24% | 22% |
| LAM | 6% | 4% |

**Table 11. Geolocation of Trojans**
*Source: Symantec*

[176] Cf. http://www.comscore.com/press/release.asp?press=2504 or http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_09_2007.en-us.pdf : p. 81
[177] Cumulative totals might not equal 100 percent due to rounding.
[178] See http://blogs.zdnet.com/security/?p=1670 and http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html

The previous edition of the Symantec *Global Internet Security Threat Report* discussed the continued concentration of Trojans in North America, and posited that attackers may consciously be moving toward Trojan attacks there because of successful efforts by North American-based enterprises and ISPs to thwart worm attacks.[179] In 2008, the number of Trojans reported in EMEA was similar to the number reported in NAM. While the increase in EMEA could be attributed to similar reasons as those given in the previous paragraph, the proportional increase in reports of other malicious code types in EMEA suggests that the increased activity is not a reaction to any specific mitigation efforts.

One possible explanation for the increase in EMEA is that there were a number of attacks against prominent government and corporate websites in the region during 2008.[180] For example, one attack that targeted the websites of both the United Nations and the UK government, among others, injected malicious code that was designed to load content from an attacker-controlled location into visitors' browsers.[181] Another separate attack successfully defaced the national Albanian postal service website.[182] Such attacks are a perfect beachhead for distributing malicious code because they target high-traffic websites of reputable organizations. Successful distribution of malicious code using this method of delivery may have contributed to the increased proportion of Trojans in EMEA in 2008.

### Worms

Forty percent of the potential infections caused by worms in 2008 were reported from the APJ region, followed by EMEA with 36 percent, NAM with 13 percent, and LAM with 11 percent (table 12). The drop in proportion of worms in APJ is mainly attributed to the increase in EMEA and may indicate that worm activity in EMEA will eventually surpass that of APJ. The emergence of the Downadup worm may offset this, however, and cause the percentage of potential worm infections in APJ to rise in 2009 since that is where it has been initially concentrated.

| Region | 2008 Percentage | 2007 Percentage |
|---|---|---|
| APJ | 40% | 44% |
| EMEA | 36% | 32% |
| NAM | 13% | 16% |
| LAM | 11% | 9% |

**Table 12. Geolocation of worms**
*Source: Symantec*

### Back door infections

EMEA accounted for the largest proportion of potential back door infections reported worldwide in 2008, with 39 percent of the total. APJ accounted for the second largest percentage, with 29 percent, followed by NAM at 23 percent, and LAM at 9 percent (table 13). As with the previously discussed types of potential malicious code infection, the proportional increase in reports from EMEA is the primary contributor to decreases in other regions. As is discussed elsewhere in this report, there are indications that back doors are increasingly being incorporated as secondary stages of multistage attacks. Because of this, the proportional increase of back doors in EMEA may be closely related to the observed increase of Trojans reported there.

[179] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf : p. 52
[180] http://news.cnet.com/8301-10789_3-9983940-57.html
[181] http://news.cnet.com/8301-10789_3-9925637-57.html
[182] http://albmasters.com/?p=3

| Region | 2008 Percentage | 2007 Percentage |
|---|---|---|
| EMEA | 39% | 36% |
| APJ | 29% | 30% |
| NAM | 23% | 28% |
| LAM | 9% | 5% |

**Table 13. Geolocation of back door infections**
*Source: Symantec*

While the regional percentages of potential back door infections can show fairly wide variances, it is important to note that the worldwide volume of back door threats was significantly lower than Trojans and worms. Therefore, the percentage variance between regions actually represents a much smaller difference in raw numbers than the percentage differences between worms and Trojans.

### Viruses

The APJ region continued to hold the highest concentration of reported potential infections caused by viruses in 2008, with 41 percent of the worldwide total, although this is a decrease from its 53 percent share in 2007 (table 14). The EMEA region again ranked second, with its share growing to 38 percent in 2008 from 27 percent in 2007. The proportion of potential virus infections concentrated in NAM dropped to 15 percent in 2008 from 17 percent previously, while LAM increased to 6 percent this period from 4 percent previously.

| Region | 2008 Percentage | 2007 Percentage |
|---|---|---|
| APJ | 41% | 53% |
| EMEA | 38% | 27% |
| NAM | 15% | 17% |
| LAM | 6% | 4% |

**Table 14. Geolocation of viruses**
*Source: Symantec*

As was the case with the previous reporting period, the increased proportion of viruses in EMEA was linked to the greater proportion of worms reported from the region, which is because viral infection functionality is a common component incorporated into worms.[183] For example, the Mabezat worm includes a viral infection component and was heavily concentrated in the EMEA region in 2008 (it was one of the top 10 potential infections reported from the region).

[183] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf : p. 53

## Threats to confidential information

Some malicious code programs are designed specifically to expose confidential information that is stored on an infected computer. These threats may expose sensitive data such as system information, confidential files and documents, or logon credentials. Some malicious code threats, such as back doors, can give a remote attacker complete control over a compromised computer. Threats to confidential information are a particular concern because of their potential for use in criminal activities. With the widespread use of online shopping and Internet banking, compromises of this nature can result in significant financial loss, particularly if credit card information or banking details are exposed.

Within the enterprise, the exposure of confidential information can lead to significant data leakage. If it involves customer-related data such as credit card information, customer confidence in the enterprise can be severely undermined. Moreover, it can also violate local laws. Sensitive corporate information, including financial details, business plans, and proprietary technologies, could also be leaked from compromised computers.

In 2008, 83 percent of confidential information threats had a remote access component (figure 17). This was a decrease from 91 percent in 2007. This decrease is mainly attributable to an increase in malicious code that exports user data or logs keystrokes, along with the decrease in the percentage of potential infections from back doors. Another reason may be that attackers are less interested in administering individual compromised computers than they are in simply gathering the available information, which can be accomplished without installing a back door.

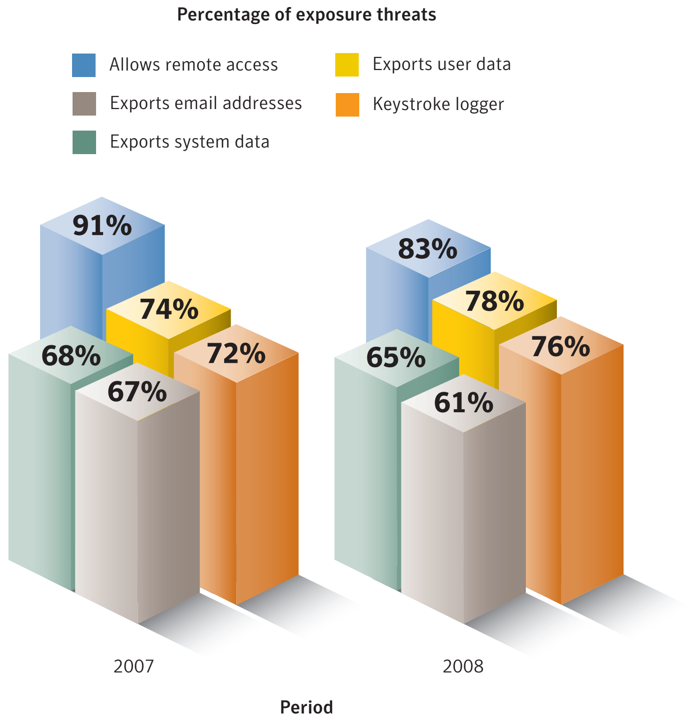

**Figure 17. Threats to confidential information, by type**
*Source: Symantec*

Malicious code that could export user data accounted for 78 percent of threats to confidential information in 2008, up from 74 percent in 2007. Such threats are useful because leaked data can be used to steal a user's identity or aid in further attacks. Increases in this type of exposure are not surprising considering the potential value of harvested information. The third highest exposure type, keystroke logging, further supports this.

Confidential information threats with a keystroke-logging capability made up 76 percent of threats to confidential information, up from 72 percent in 2007. Malicious code incorporating keystroke loggers that target online gaming account credentials continues to be popular. The Wowinzi worm is one such threat and was one of the top 10 new malicious code samples in 2008. Several Trojans and worms such as Gampass, Gammima,[184] and Mumawow[185] have been around for some time and are specifically designed to steal online gaming credentials, and they continue to account for a significant number of potential infections.

Organizations can take several steps to limit the exposure of confidential information by successful intrusions. Data leakage prevention solutions can prevent sensitive data from being stored on endpoint computers. Encrypting sensitive data that is stored in databases will limit an attacker's ability to view and/or use the data. However, this step may require sufficient resources to be made available, as adequately managing encryption keys and ensuring that archived data is actually encrypted can be costly. Furthermore, encrypting stored data will not protect against man-in-the-middle attacks that intercept data before it is encrypted.[186] As a result, data should always be transmitted through secure channels such as SSH, SSL, and IPSec.

### Propagation mechanisms

Worms and viruses use various means to transfer themselves, or propagate, from one computer to another. These means are collectively referred to as propagation mechanisms. Propagation mechanisms can include a number of different vectors, such as instant messaging (IM), Simple Mail transfer protocol (SMTP), Common Internet File System (CIFS), P2P, and remotely exploitable vulnerabilities. Some malicious code may even use other malicious code as a propagation vector by locating a computer that has been compromised via a back door server and using it to upload and install itself. The samples discussed here are assessed according to the percentage of potential infections.

In 2008, 66 percent of potential malicious code infections propagated as shared executable files, up significantly from 44 percent in 2007 (table 15).[187] Shared executable files are the propagation mechanisms employed by viruses and some worms to copy themselves onto removable media. The resurgence in this vector over the past few years coincides with the increased use of removable drives and other portable devices. It is also an easy vector to exploit because old malicious code exploits developed for floppy disks can be easily modified for current removable media devices.

To limit the propagation of threats through removable drives, administrators should ensure that all such devices are scanned for viruses when they are connected to a computer. If removable drives are not needed within the enterprise, endpoint security and policy can prevent computers from recognizing these drives when they are attached. Additionally, best practices policies should be implemented to mitigate the dangers of attaching unauthorized devices to computers within the enterprise.

[184] http://www.symantec.com/security_response/writeup.jsp?docid=2007-032206-2043-99
[185] http://www.symantec.com/security_response/writeup.jsp?docid=2007-032015-4300-99
[186] A "man-in-the-middle attack" is an attack in which a third party intercepts communications between two computers. The "man in the middle" captures the data, but still relays it to the intended destination to avoid detection.
[187] Because malicious code samples often use more than one mechanism to propagate, cumulative percentages may exceed 100 percent.

| 2008 Rank | Propagation Mechanism | 2008 Percentage | 2007 Percentage |
|---|---|---|---|
| 1 | File-sharing executables | 66% | 44% |
| 2 | File transfer/email attachment | 31% | 32% |
| 3 | File transfer/CIFS | 30% | 26% |
| 4 | Remotely exploitable vulnerability | 12% | 15% |
| 5 | File sharing/P2P | 10% | 17% |
| 6 | File transfer/embedded HTTP URI/instant messenger | 4% | 3% |
| 7 | SQL | 3% | 3% |
| 8 | Back door/Kuang2 | 3% | 3% |
| 9 | Back door/SubSeven | 3% | 3% |
| 10 | File transfer/instant messenger | 2% | 1% |

**Table 15. Propagation mechanisms**
*Source: Symantec*

In 2008, 31 percent of malicious code that propagated did so in email attachments, a slight decrease from 32 percent in 2007. The previous volume of the Symantec *Global Internet Security Threat Report* stated that, despite a small increase for the reporting period, propagation through email attachments was surpassed by propagation through file sharing executables.[188] This was noted to likely be the result of diversification by malicious code authors. Although there was an increase again in 2008, the gap between the first and second ranked propagation mechanisms has widened substantially.

One possible reason for the diversification of propagation methods, as well as the resulting gap, is that malicious code authors may not be experiencing as much success with attacks using email attachments as in past years. Increased user awareness and prevention against email-based attacks may be a factor. However, the number of potential infections that use email-based propagation appears to be stable, which may be a result of attackers experiencing increased success with other propagation vectors and opting to use those instead. Despite such factors, email attachments continue to be a common and attractive propagation mechanism for malicious code.

To limit the propagation of email-borne threats, administrators should ensure that all email attachments are scanned at the gateway. Additionally, all executable files originating from external sources such as email attachments or those downloaded from websites should be treated as suspicious. All executable files should be checked by antivirus scanners using the most current definitions.

Malicious code that propagated by the CIFS protocol made up 30 percent of malicious code that propagated in 2008, up from 26 percent in 2007.[189] This indicates that this protocol continues to be a common and effective means for the propagation of malicious threats. The increase may be linked to the diversification of mechanisms discussed above. Two of the top 10 malicious code threats for 2008 employed this propagation mechanism. This includes the Fujacks worm,[190] a long-standing malicious code family in top 10 lists, and the Almanahe worm,[191] a modular threat that includes a viral component that has steadily increased in potential infections since its discovery early in 2007.

[188] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf : p. 57
[189] CIFS is a file sharing protocol that allows files and other resources on a computer to be shared with other computers across the Internet. One or more directories on a computer can be shared to allow other computers to access the files within.
[190] http://www.symantec.com/security_response/writeup.jsp?docid=2006-111415-0546-99
[191] http://www.symantec.com/security_response/writeup.jsp?docid=2007-041317-4330-99

The CIFS propagation mechanism can be a threat to organizations because file servers use CIFS to give users access to their shared files. If a computer with access to a file server becomes infected by a threat that propagates through CIFS, the infection could spread to the file server. Since multiple computers within an organization likely access the same file server, this could facilitate the rapid propagation of the threat within the enterprise. This is increasingly becoming a threat to home environments as well, because home networks with multiple devices are becoming more commonplace.

To protect against threats that use the CIFS protocol to propagate, all shares should be protected with strong passwords, and only users who require the resources should be given access to them. If other users do not need to write to a share, they should only be given “read” permissions. This will prevent malicious code from copying itself to the shared directory or modifying shared files. Finally, CIFS shares should not be exposed to the Internet. Blocking TCP port 445 at the network boundary will help to protect against threats that propagate using CIFS.[192]

An interesting decrease of note during 2008 was in the percentage of threats that propagate by exploiting remote vulnerabilities. While there was relatively stable activity in this type of threat through the majority of the year, that changed when the Downadup worm was discovered late in 2008. Downadup propagates by exploiting the Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability.[193] This worm has attracted a lot of attention because of its sophistication and aggressive infection routine. The first variant of Downadup is estimated to have infected over half a million computers, primarily in the APJ and LAM regions.[194] Symantec is monitoring its evolution to how Downadup affects the percentage of threats that propagate by exploiting remote vulnerabilities into 2009.[195]

### Malicious code that exploits vulnerabilities

Assessing the proportion of malicious code that exploits vulnerabilities helps to show how popular this technique is for developing new variants of malicious code. The exploitation of vulnerabilities as a means of malicious code propagation is an ongoing concern for enterprises because it illustrates the need for administrators to apply patches in a timely manner.

In 2008, only 3 percent of the 2,476 documented malicious code instances exploited vulnerabilities (figure 18).[196] This is a significant decline from the 13 percent proportion of the 2,538 malicious code instances documented for 2007. While the number of new malicious code samples exploiting vulnerabilities has been declining in recent years, the effectiveness of this method of propagation remains strong, as is illustrated by it being the fourth-ranked propagation mechanism in 2008.

[192] TCP port 445 is the default port used to run CIFS on TCP.
[193] http://www.securityfocus.com/bid/31874
[194] https://forums2.symantec.com/t5/Malicious-Code/W32-Downadup-A-and-W32-Downadup-B-Statistics/ba-p/379940#A226
[195] Please see https://forums2.symantec.com/t5/blogs/blogarticlepage/blog-id/malicious_code/article-id/225, https://forums2.symantec.com/t5/blogs/blogarticlepage/blog-id/malicious_code/article-id/227, and https://forums.symantec.com/t5/Malicious-Code/Downadup-Small-Improvements-Yield-Big-Returns/ba-p/381717
[196] The number of documented malicious code instances differs from the number of malicious code submissions. Documented malicious code instances are those that have been analyzed and documented within the Symantec malicious code database.

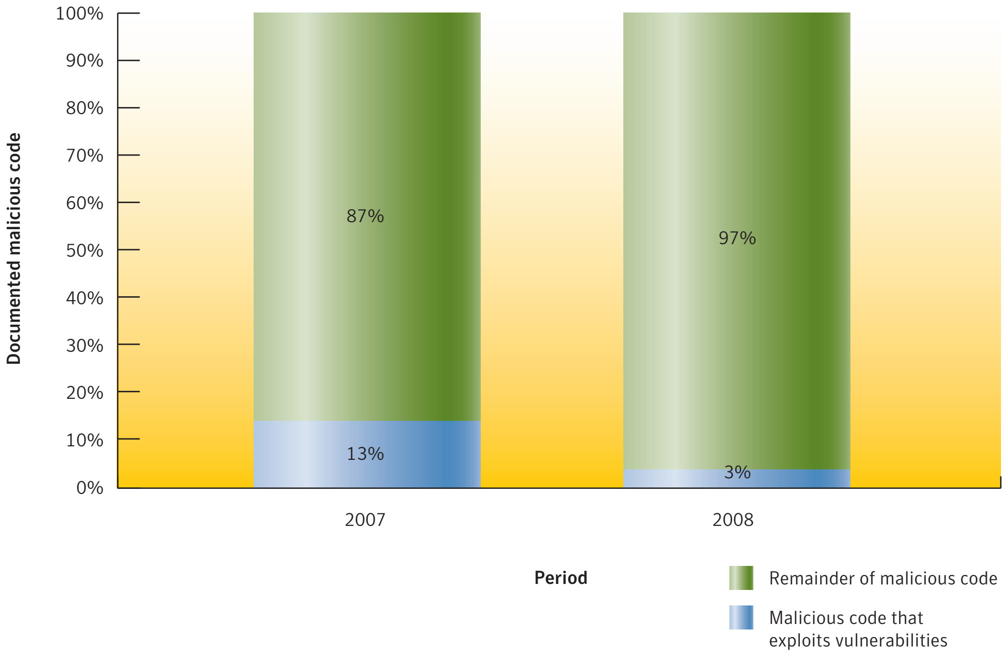

**Figure 18. Malicious code that exploits vulnerabilities**
*Source: Symantec*

As well, while the number of malicious code samples exploiting vulnerabilities has dropped, it is important to note that there are still prevalent examples of successful malicious code families that do so. For example, a threat such as the Downadup worm can be particularly effective against medium and large enterprises because these businesses often need to test patches prior to their deployment due to the use of custom applications and software configurations. The resulting delay in patch implementation widens the window in which infections can occur.

The success of Downadup illustrates that, even though there are fewer new malicious code samples that exploit vulnerabilities, they can still have great success in compromising unpatched computers. As well, while fewer new malicious code samples were identified that exploit vulnerabilities in operating systems, popular third-party client-side applications are still a viable target for malicious code. End users and enterprises should ensure that vulnerabilities in affected software are patched as soon as fixes are available. Intrusion prevention systems and antivirus software can help protect against malicious code that exploits vulnerabilities for which no patch is available.

## Malicious code—protection and mitigation

It is critical that end users and enterprises maintain the most current antivirus definitions to protect against the high quantity of new malicious code threats. IDS, IPS, and other behavior-blocking technologies should also be employed to prevent compromise by new threats. Using a firewall can also prevent threats that send information back to the attacker from opening a communication channel.

Symantec recommends that certain best security practices always be followed to protect against malicious code infection. Administrators should keep patch levels up to date, especially on computers that host public services and applications—such as HTTP, FTP, SMTP, and DNS servers—and that are accessible through a firewall or placed in a DMZ. Email servers should be configured to only allow file attachment types that are required for business needs and to block email that appears to come from within the company, but that actually originates from external sources. Additionally, Symantec recommends that ingress and egress filtering be put in place on perimeter devices to prevent unwanted activity.

To protect against malicious code that installs itself through a Web browser, additional measures should be taken. The use of IPS technologies can prevent exploitation of browser and plug-in vulnerabilities through signatures and behavior-based detection in addition to address space layout randomization (ASLR).[197] End users should employ defense-in-depth strategies, including the deployment of antivirus software and a personal firewall. Users should update antivirus definitions regularly. They should also ensure that all desktop, laptop, and server computers are updated with all necessary security patches from their software vendors. They should never view, open, or execute any email attachment unless it is expected and comes from a trusted source, and unless the purpose of the attachment is known.

[197] ASLR is a security mechanism that randomizes data in memory to prevent the success of attacks that leverage memory corruption vulnerabilities, such as buffer overflows.

## Phishing, Underground Economy Servers, and Spam Trends

Phishing is an attempt by a third party to solicit confidential information from an individual, group, or organization by mimicking (or spoofing) a specific brand, usually one that is well known, often for financial gain. Phishers attempt to trick users into disclosing personal data, such as credit card numbers, online banking credentials, and other sensitive information, which they may then use to commit fraudulent acts.

Phishing generally requires an end user to enter their credentials into an online data entry field. This is one of the characteristics that distinguishes phishing from spam-based scams (such as the widely disseminated 419 scam and other social engineering scams).[198] The data that end users enter can then be used for fraudulent purposes.

Spam is usually defined as junk or unsolicited email sent by a third party. While it is certainly an annoyance to users and administrators, spam is also a serious security concern because it can be used to deliver Trojans, viruses, and phishing attempts.[199] Spam can also be used to deliver drive-by downloaders, which require no other end user interaction than navigation to the URLs contained in the spam messages. Large volumes of spam could also cause a loss of service or degradation in the performance of network resources and email gateways.

This section will assess phishing and spam trends that Symantec observed in 2008; it will also discuss items that were offered for sale on underground economy servers during this time period, as this is where much of the profit is made from phishing and spam attacks. Underground economy servers are black market forums for advertising and trading stolen information and services. This discussion will assess underground economy servers according to the different types of goods and services advertised. It should be noted that this discussion may not necessarily be representative of Internet-wide activity; rather, it is intended as a snapshot of the activity that Symantec monitored during this period.

The results used in this analysis are based on data returned from the Symantec Probe Network, as well as the Symantec Brightmail AntiSpam™ customer base. Specifically, statistics are gathered from enterprise customers' Symantec Brightmail AntiSpam servers that receive more than 1,000 email messages per day. This removes the smaller data samples (that is, smaller customers and test servers), thereby allowing for a more accurate representation of data.

The Symantec Probe Network consists of millions of decoy email addresses that are configured to attract a large stream of spam attacks. An attack can consist of one or more messages. The goal of the Symantec Probe Network is to simulate a wide variety of Internet email users, thereby attracting a stream of traffic that is representative of spam activity across the Internet as a whole. For this reason, this network is continuously optimized in order to attract new varieties of spam attacks.

In addition to the Symantec Probe Network, phishing information is also gathered through the Symantec Phish Report Network, an extensive antifraud community of organizations and end users.[200] Members of the Symantec Phish Report Network contribute and receive fraudulent website addresses for alerting and filtering across a broad range of solutions.

[198] http://nortontoday.symantec.com/features/security_at_30.php
[199] http://news.bbc.co.uk/2/hi/technology/6676819.stm
[200] http://www.phishreport.net/

This section will address the following metrics:

- Phishing activity by sector
- Phishing website hosts
- Top countries hosting phishing websites and top targeted sectors
- Automated phishing toolkits
- Underground economy servers—goods and services available for sale
- Spam by category
- Top countries of spam origin
- Percentage of spam from botnets
- Phishing, underground economy servers, and spam—protection and mitigation

### Phishing activity by sector

This section will explore phishing activity in two ways. First, it will analyze the unique brands being spoofed in phishing attacks according to the sector to which they belong. Second, it will explore the sectors whose brands were most frequently spoofed by phishing lures. These considerations are important for an enterprise because the use of its brand in phishing activity can significantly undermine consumer confidence in its reputation.

Previous volumes of the Symantec *Global Internet Security Threat Report* assessed phishing data based on the number of phishing websites that were targeted by the highest volume of phishing attacks.[201] However, in this volume, phishing activity will be assessed by sector according to the number of so-called phishing lures that are detected spoofing a company's brand. Phishing lures are URLs that lead end users to phishing websites and are usually delivered by spam email (also known as phishing email). Multiple lures can lead to the same phishing website.

Phishers are becoming increasingly adept at adapting their lures in order to direct end users to their phishing sites. For instance, in economically constrained circumstances, phishers may adopt lures that spoof well-known financial institutions and promise users access to low-interest loans. As a result, tracking phishing lures may give security analysts insight into what new tactics phishers are using.

The majority of brands used in phishing attacks in 2008 were in the financial services sector, accounting for 79 percent of the total, down slightly from the 83 percent reported in 2007 (table 16). The financial services sector also accounted for the highest volume of phishing lures during this period, at 76 percent, considerably higher than 2007 when the volume for financial services was 52 percent (figure 19).

It is likely that the increase in the percentage of phishing lures spoofing financial services is not so much due to an increase in the number of these lures, but to a drop in the number of lures spoofing Internet community-related brands, particularly social networking sites, as will be discussed later in this section. The rise in phishing lures that spoof financial services is reflected in the significant amount of credit card information that was offered on underground economy servers in 2008, as is discussed in the **"Underground economy servers"** discussion.

[201] A phishing website is a site that is designed to mimic the legitimate website of the organization whose brand is being spoofed. In many cases, it is set up by the attacker to capture authentication information or other personal identification information from victims; any information gathered is then typically used in identity theft or other fraudulent activity.

| Sector | 2008 Percentage | 2007 Percentage |
|---|---|---|
| Financial | 79% | 83% |
| ISP | 8% | 7% |
| Retail | 4% | 4% |
| Insurance | 2% | 2% |
| Internet community | 2% | 2% |
| Telecom | 2% | <1% |
| Computer hardware | 1% | 1% |
| Government | 1% | 1% |
| Computer software | <1% | 1% |
| Transportation | <1% | 1% |

**Table 16. Unique brands phished, by sector**
*Source: Symantec*

Phishing is often carried out for the purpose of financial gain. Brands and activities associated with the financial sector are most likely to yield data that could be used in financially motivated attacks, such as bank account credentials. As a result, it is not surprising that the majority of phishing activity detected in 2008 targeted brands in the financial sector.

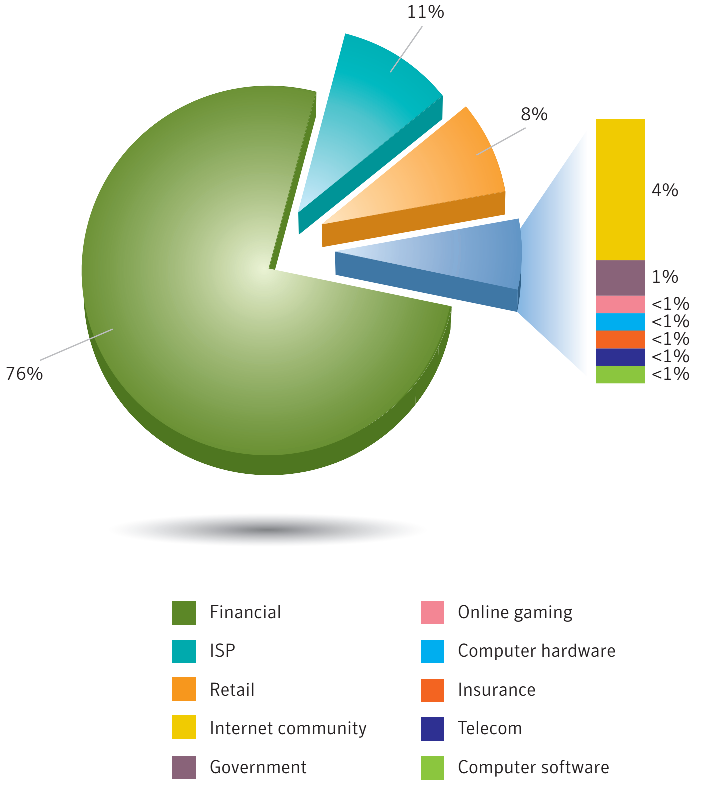

**Figure 19. Phished sectors by volume of phishing lures**
*Source: Symantec*

There are several items in the "Underground economy servers" discussion that illustrate the preponderance of financial services in phishing activity. The top two most frequently advertised items observed on underground economy servers during 2008 were credit card information and bank account credentials, in that order. Together, these two categories accounted for more than half of the goods and services advertised in 2008.

Many phishing attacks that spoof financial services brands will prompt users to enter credit card information or banking credentials into fraudulent sites. If this is done, the phishers can then capture and sell such information in the underground economy. This has been made easier for phishers because of the increasingly widespread acceptance of online banking. For example, 44 percent of Internet users in the United States perform some degree of online banking, as do 64 percent of users in Canada and 46 percent of those in France.[202] Because of this, end users may be more easily fooled into entering their information into fraudulent websites that mimic the brand of their financial services provider.

The 4 percent reduction in the number of financial sector brands being spoofed by phishing lures during 2008 may indicate increased awareness of phishing schemes and how to avoid falling victim to them. Information campaigns driven by specific financial institutions, as well as a heightened awareness of phishing schemes targeting financial services, have likely made it more difficult for phishers to carry out successful phishing attacks against companies offering those services. By the same token, it may also be a reflection of the fact that a number of financial institutions either ceased operations or changed their business offerings during 2008, thereby reducing the number of financial service brands available for phishers to spoof.[203]

ISPs were the second ranked sector for brands spoofed by phishing lures in 2007, making up 8 percent of the total. This is a 1 percentage point increase from 2007, when it also ranked second. The ISP sector also ranked second in the volume of phishing lures for 2008, accounting for 11 percent of the total, up from 4 percent in 2007. Again, the percentage increase in the volume of lures spoofing ISPs was likely due to a drop in the number of lures spoofing brands associated with Internet communities, as will be discussed shortly.

ISP accounts, which often include email accounts, can be valuable targets for phishers because people frequently use the same authentication credentials (such as usernames and passwords) for multiple accounts, including email accounts. With a little effort on the part of the attacker, this information could provide access to other accounts, such as online banking accounts.

Attackers also sometimes use the free Web-hosting space that is often included in ISP accounts to put up phishing websites, or use the accompanying email accounts to send spam or launch further phishing attacks. Compromised ISP Web-hosting accounts can also be used to host Web-based exploits, which would give an attacker a greater number of potential targets. Compromised Web space can also be used to plant links to other websites that an attacker controls in order to boost the search engine rankings of those sites.

In addition, having access to an email account could allow the attacker to spam the victim's contact list—and likely enjoy greater success with this ploy because people tend to trust email from people they know. This assertion is enforced by email accounts/passwords and addresses being the third and fourth most common goods available on underground economy servers in 2008, respectively.

[202] http://www.comscore.com/press/release.asp?press=2524
[203] http://www.economist.com/finance/displayStory.cfm?story_id=12294688&source=features_box_main

The third most spoofed sector for 2008 was retail services, which accounted for 4 percent of organizations whose brands were spoofed by phishing attacks in 2008, the same percentage as 2007. The retail sector also ranked third in volume of phishing lures, accounting for 8 percent of the total for 2008, down from 12 percent recorded in 2007.

The retail sector is a logical target of phishers for several reasons. First, online retailers regularly conduct transactions that require the input of financial information, which could be fraudulently obtained and used for financial gain. By successfully mimicking a retailer's website, phishers will try to persuade users to attempt a purchase and enter their credit card information. They may also be able to persuade users to enter account information (such as usernames and passwords) that can then be used to access the account on the retailer's legitimate website. This can in turn be used to fraudulently order goods that are charged to the user's account. Many online stores give customers the option of storing credit card and billing information to facilitate the checkout process. Access to this information also gives phishers access to the victim's billing address, which is used by merchants as a security feature.

As has been mentioned previously, the volume of phishing lures spoofing brands associated with Internet communities, such as social networking sites, dropped significantly over the past year, from 31 percent in 2007 to only 4 percent in 2008. The previous two volumes of the Symantec *Global Internet Security Threat Report* discussed the rapid rise in lures targeting this sector and postulated that it was likely due to the increase in usage of these sites, as well as the fact that users associated with these communities generally tend to be trusted by other users.

Given the rapid rise of phishing activity targeting this sector in previous years, and the notable drop in volume in 2008, it is likely that companies in this sector have taken steps to either bolster security against phishing activity or limit its effectiveness. This could include increased network security measures and increased user awareness and education.

It is also likely that many of these communities have improved their ability to quickly identify phishing websites and have them taken down, reducing the window of exposure of end users to such websites. It may also be the case that phishers have concluded that there are more direct ways to obtain information that can be used for financial gain, such as spoofing brands associated with financial services organizations.

## Phishing website hosts

This metric will assess the volume of distinct phishing website hosts observed by Symantec. A phishing website host is a computer that has been identified to be hosting one or more phishing websites during the period. Some phishing hosts may host numerous different phishing websites; however, these hosts are counted only once for the purpose of this discussion. The number of phishing hosts is an important consideration because it may give security analysts an indication of the number of different people or groups involved in phishing activity at any one time. By the same token, it may also provide a good sense of the number and type of automated phishing toolkits in use at any one time.

It should be noted that, in an effort to create a more accurate overview of the extent of phishing sites, Symantec has made minor methodological changes for this metric. As a result, data reported in the previous volume has been revised and updated for this volume.

In 2008, Symantec detected 55,389 phishing website hosts. This is an increase of 66 percent over 2007 when Symantec detected 33,428 phishing hosts. The increase in phishing website hosts is likely tied to the continued use of automated phishing toolkits. Phishing toolkits allow phishers to carry out phishing attacks much more easily by automatically creating phishing websites that spoof the websites of legitimate brands. Attackers can therefore concentrate on identifying and procuring phishing website hosts instead of the time-consuming job of coding phishing websites themselves.

As noted in the previous two volumes of the Symantec *Global Internet Security Threat Report*, the adoption of phishing website toolkits has made phishing attacks much easier and more time efficient. As will be discussed in **"Automated phishing toolkits"** below, one prevalent phishing kit was responsible for an average of 14 percent of all phishing attacks during 2008, with spikes up to 26 percent. The fact that this level of phishing activity can be generated with minimal effort on the part of phishers illustrates how easy it is for phishers to generate high volumes of phishing activity. Symantec believes that this is likely to continue in the foreseeable future.

As noted elsewhere, phishing is generally conducted for financial gain. This is illustrated by the fact that the financial sector was targeted by 76 percent of phishing lures in 2008 and that brands associated with financial services organizations made up 79 percent of all spoofed brands for the year. Furthermore, as has been discussed in previous volumes of the Symantec *Global Internet Security Threat Report*, phishing has been adopted as a revenue-generating activity by some organized crime groups.[204] Those discussions focused on the online criminal activities of the RBN, who specialized in the distribution of malicious code, hosting malicious websites, and other malicious activity (as discussed further in "Top countries hosting phishing websites and top targeted sectors," which follows). Symantec believes that phishing activity will likely continue to increase as long as it continues to be a profitable and lucrative enterprise.

### Top countries hosting phishing websites and top targeted sectors

This metric will assess the countries in which the most phishing websites were hosted in 2008. This data is a snapshot in time, and does not offer insight into changes in the locations of certain phishing sites over the course of the reporting period. It should also be noted that the fact that a phishing website is hosted in a certain country does not necessarily mean that the attacker is located in that country.

In 2008, 43 percent of all phishing websites detected by Symantec were located in the United States (table 17). This is considerably less than 2007, when 69 percent of phishing websites originated there. Of the phishing websites situated in the United States, 82 percent spoofed brands associated with financial services. This is in keeping with the Internet-wide average, since 76 percent of phishing websites detected across the Internet as a whole were associated with financial service organizations.

It is worth noting that of the top 10 countries for phishing websites in 2008, only the United States experienced a drop in activity. All other countries in the top 10 experienced growth (albeit relatively minor in most cases) or stayed relatively the same. Because the United States hosted such a vast majority of phishing websites in 2008, it is reasonable to conclude that the changes in percentage were due to a drop in the absolute number of these websites being hosted in the United States, rather than a rise in those situated in other countries. This could be related to the shutdown of ISPs that were being used for large volumes of spam activity, as is discussed in **"Top countries of spam origin,"** further below in this report.

[204] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf : p. 11

| Rank | Country | 2008 Percentage | 2007 Percentage | 2008 Top Sector Targeted in Country | 2008 Percentage of Lures Targeting Top Sector |
|---|---|---|---|---|---|
| 1 | United States | 43% | 69% | Financial services | 82% |
| 2 | Poland | 6% | 1% | Financial services | 94% |
| 3 | China | 4% | 3% | ISP | 50% |
| 4 | France | 4% | 2% | Financial services | 87% |
| 5 | South Korea | 4% | 4% | Financial services | 88% |
| 6 | Russia | 3% | 2% | Financial services | 60% |
| 7 | Germany | 3% | 3% | Financial services | 79% |
| 8 | United Kingdom | 3% | 3% | Financial services | 86% |
| 9 | Canada | 3% | 2% | Financial services | 77% |
| 10 | Italy | 2% | <1% | Financial services | 67% |

**Table 17. Top countries hosting phishing websites and top targeted sectors**
*Source: Symantec*

Of the phishing websites hosted in the United States in 2008, 82 percent targeted the financial services sector. As noted in “Phishing activity by sector,” attacks that spoof financial companies give phishers the best opportunity to attain information that can be used for financially rewarding attacks. In 2007, the Internet community sector was the sector most commonly spoofed by phishing websites based in the United States, accounting for 55 percent of the total, while financial services ranked second with 41 percent.

It is likely that phishers based in the United States have moved away from Internet community-based phishing websites due to countermeasures undertaken by companies in this sector to guard against phishing attacks—most likely through user-education campaigns. It may also be that phishers have moved toward financial services because this sector provides more opportunities for profit. With the current economic downturn, end users may be more susceptible to phishing attacks that advertise low interest rates for mortgages and credit cards or that claim to be associated with the administration of financial institutions that are undergoing some sort of restructuring or cessation.

Poland hosted the second highest percentage of phishing websites in 2008, with 6 percent of the total. This is a significant change from 2007, when Poland hosted just 1 percent of phishing websites and was only the fourteenth-ranked country in this category. Poland’s increased rank in 2008 may also be due to remotely situated attackers compromising computers in Poland to use them to host phishing websites, possibly due to recent crackdowns on fraudulent activity in other countries. For instance, in November 2007, the Russia-based operations of the Russian Business Network (RBN) were reportedly shut down.[205] The RBN reputedly specializes in the distribution of malicious code, hosting malicious websites, and other malicious activity, including the development and sale of the MPack toolkit. The RBN has been credited for creating approximately half of the phishing incidents that occurred worldwide last year, and reputedly associated with a significant amount of malicious Internet and computer activities in 2007. It is possible that when its operations in Russia were shut down, it relocated some of its operations to Poland, therefore contributing to the high number of phishing websites detected there in 2008.

[205] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf : p. 11

China hosted the third highest percentage of phishing websites in 2008, with 4 percent of the total. This is up from fourth rank and 3 percent in 2007. The sector most commonly targeted by phishing websites hosted in China in 2008 was the ISP sector, which was spoofed by 50 percent of all known sites there. In 2007, the financial services sector was the sector most commonly spoofed by phishing websites based in China, with 44 percent of the total.

Of the top 10 countries for phishing websites, China was the only one in which the top targeted sector was ISPs. Financial services was the most commonly targeted sector for all of the other top 10 countries. As discussed previously in **"Phishing activity by sector,"** ISPs make valuable targets for phishers because of the potential wealth of personal information from the ISP accounts of end users that is often fairly easily accessed by skilled attackers and which provides many avenues for further malicious exploits.

## Automated phishing toolkits

A phishing toolkit is a set of scripts that allows an attacker to automatically create websites that spoof the legitimate websites of different brands, including the images and logos associated with those brands. The scripts also help to generate corresponding phishing email messages. As each script generates pseudo-random phishing URLs with a distinctive pattern,[206] the particular script used to generate a particular phishing URL can be identified from that pattern. All phishing URLs reported to Symantec can be sorted and grouped according to those specific patterns.

Phishing toolkits are developed by groups or individuals who, along with using the kits themselves, sell the kits in the underground economy. Toolkits sold in the underground economy often go unnamed. Unlike legitimate software, for which naming plays an important marketing role, phishing toolkits often become popular based on who has produced them. As a consequence, phishing toolkits discussed here cannot be named specifically and will instead be referred to by number.

Kit 1 was responsible for an average of 14 percent of all phishing attacks during 2008, with spikes up to 26 percent during the summer months (figure 20). This kit is a domain-based phishing toolkit. Domain-based phishing toolkits require the phisher to own and register a unique domain, such as "aphishingsite.com" and host it somewhere like a bot network or on an ISP. The phisher can then create phishing links with random subdomains, such as "mybank.aphishingsite.com," "anotherbank.aphishingsite.com," and so on.

On the other hand, defacement-based phishing toolkits do not require the registration of domains or DNS servers so they are easier to setup. Defacement-based phishing toolkits require a phisher to compromise existing Web pages, after which the phisher can simply upload the page of the spoofed brand. Defacement-based toolkits are often favored by phishers because of their ease of use and light setup requirements. For example, in 2008, Symantec detected many image-hosting sites and guestbooks that were compromised and used for phishing attacks.

[206] For example, http://www.loginhere.id-123456.spoofed-brand.tld/r1/abcd/login.php and http://www.loginhere.id-456789.spoofed-brand.tld/r1/wxyz/login.php

Kit 1 only targets a popular Webmail service and uses domain names that are often related to images or pictures, such as “pzychaos.xmas-party-pics.com” or “racz.ani.cool-crazy-pics.com.” They are often sent via the Webmail service itself to other users, with text such as “Hey see the new images from me.”

Kit 1 activity dropped sharply through August and then rose sharply again in December. This indicates that security administrators may have implemented measures to defend against these attacks, thereby reducing their effectiveness. It is likely that the phishers modified the kit in response to this drop-off, leading to the resurgence in activity in December. This may indicate that attackers were hoping to use it for the approaching Christmas season to disseminate Christmas-related phishing lures.

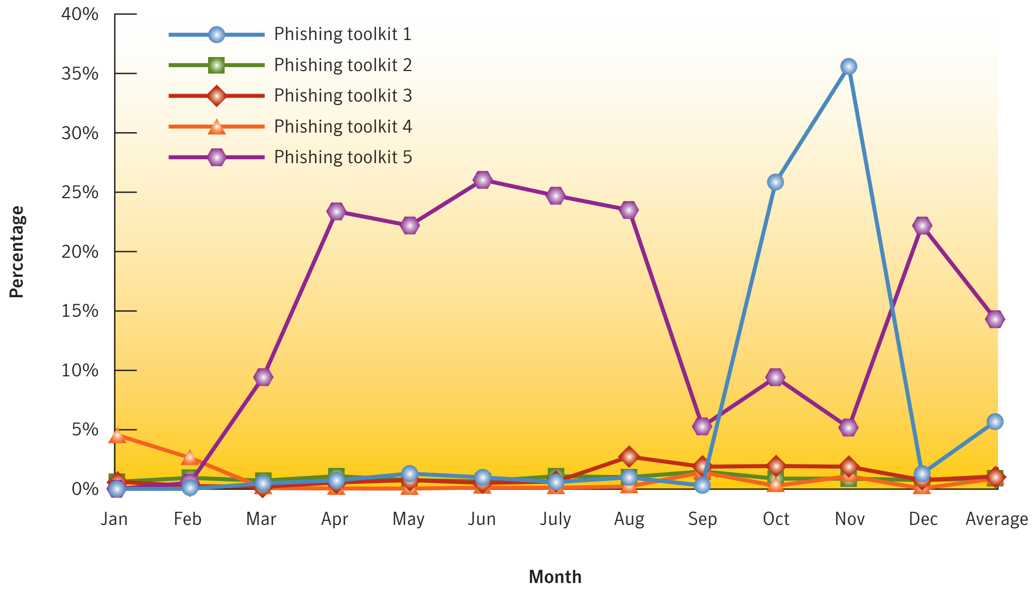

**Figure 20. Activity of most common automated phishing toolkits**
*Source: Symantec*

Phishing Kit 5 appeared in September 2008. It was responsible for 26 percent of that month’s phishing attacks, followed by 36 percent in October 2008. After this spike, its usage dropped to less than 2 percent. This attack targeted a single non-financial brand, which responded by adopting new security features for its online services, causing the sudden drop-off. Over the course of the entire year, Kit 5 was responsible for slightly less than 6 percent of all phishing activity.

## Underground economy servers—goods and services available for sale

This discussion focuses on the most frequently advertised items for sale observed on underground economy servers. Underground economy servers are black market forums for the promotion and trade of stolen information and services. This information can include government-issued identification numbers, credit cards, credit verification values, debit cards, personal identification numbers (PINs), user accounts, email address lists, and bank accounts. Services include cashiers, scam page hosting, and job advertisements such as for scam developers or phishing partners. Much of this commerce occurs within channels on Internet Relay Chat (IRC) servers. For an in-depth analysis of how the underground Internet economy functions, please see the Symantec *Report on the Underground Economy*, published November 2008.[207]

The measure of goods and services available for sale is by distinct messages, which are considered to be single advertisements for a good or service, though the same advertisement may appear thousands of times. To qualify as a new message there must be variations, such as price changes or other alterations in the message.

In 2008, the most frequently advertised item observed on underground economy servers was credit card information, accounting for 32 percent of all goods (table 18). This was an increase from 21 percent in 2007. Credit card information advertised on the underground economy consists of the credit card number and expiry date, and may also include the name on the card (or business name for corporate cards), billing address, phone number, CVV2 number, and PIN.[208] One reason for this ranking may be because there are many ways credit card information can be obtained for fraud. This includes phishing schemes, monitoring merchant card authorizations, the use of magnetic stripe skimmers, or breaking into databases and other data breaches that expose sensitive information.[209]

| 2008 Rank | 2007 Rank | Item | 2008 Percentage | 2007 Percentage | Range of Prices |
|---|---|---|---|---|---|
| 1 | 1 | Credit card information | 32% | 21% | $0.06–$30 |
| 2 | 2 | Bank account credentials | 19% | 17% | $10–$1000 |
| 3 | 9 | Email accounts | 5% | 4% | $0.10–$100 |
| 4 | 3 | Email addresses | 5% | 6% | $0.33/MB–$100/MB |
| 5 | 12 | Proxies | 4% | 3% | $0.16–$20 |
| 6 | 4 | Full identities | 4% | 6% | $0.70–$60 |
| 7 | 6 | Mailers | 3% | 5% | $2–$40 |
| 8 | 5 | Cash out services | 3% | 5% | 8%–50% or flat rate of $200–$2000 per item |
| 9 | 17 | Shell scripts | 3% | 2% | $2–$20 |
| 10 | 8 | Scams | 3% | 5% | $3–$40/week for hosting, $2–$20 design |

**Table 18. Goods and services available for sale on underground economy servers[210]**
*Source: Symantec*

[207] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_underground_economy_report_11-2008-14525717.en-us.pdf
[208] Card Verification Value 2 (CVV2) is a three- or four-digit number on the credit card that is used for card-not-present transactions, such as purchases over the Internet or telephone. This is meant to improve security for credit cards and to verify that the person completing the transaction is in fact, in possession of the card.
[209] Magnetic stripe skimming devices are small machines designed to scan and retain data contained in the magnetic stripes on credit and debit cards.
[210] Descriptions and definitions for the goods and services discussed in this section can be found in Appendix E—Phishing, Underground Economy Servers, and Spam Trends Methodology

The frequent use of credit cards also influenced their high rank in 2008. For example, the 23.6 billion credit card transactions in the United States in 2007 represent a growth of 6 percent over the previous year.[211] High frequency use and the range of available methods for capturing credit card data would generate more opportunities for theft and compromise and, thus, lead to an increased supply on underground economy servers. Despite the economic slowdown of the last half of 2008, both the number of online purchases by credit card and the amount of purchases increased. Online spending for 2008 has been growing since the previous year with sales increasing 6 percent for the third quarter.[212] Also, there was a 15 percent increase in sales for so-called Cyber Monday from the previous year in the United States.[213] Many online stores were offering financing options, no payments for 90 days, and heavy discounts to attract customers.

Credit cards may also be popular on underground economy servers because using fraudulent credit card information for activities such as making online purchases is relatively easy. Online shopping can be easy and fast, and a final sale often requires only basic credit card information. Someone knowledgeable enough could potentially make many transactions with a stolen card before the suspicious activity is detected and the card is suspended. Once the purchases have been completed and the merchandise delivered, it can then be fenced for a profit. Also, online merchants who have yet to implement multi-level security features are likely attractive to criminals who wish to conduct fraudulent transactions without hassle.

Another factor that contributes to the popularity of credit cards is that they are typically sold in bulk packages on underground economy servers. Not only do advertisers offer discounts for bulk purchases or include free numbers with larger purchases, but having an extensive list of cards enables individuals to quickly try a new number if a card number does not work or is suspended. Also, having a larger number of credit cards numbers included should theoretically increase the likelihood of having active/valid cards in the bulk package.

The price range of credit cards in 2008 remained consistent with the prices from the previous year, ranging from $0.06 to $30 per card number. There were three main factors that influenced the price of credit cards: the amount of information included with the card, rarity of the card type, and bulk purchase sizes. Credit cards that bundled in personal information—such as government-issued identification numbers, addresses, phone numbers, and email addresses—were offered at higher prices. Cards that included security features such as CVV2 numbers, PINs, and online verification service passwords were also offered at higher prices.

The rarity of the credit card information is often associated with the location of the issuing bank and the type of card. Information from regions such as Europe, Asia, and the Middle East is typically offered at higher prices than elsewhere because the supply of credit card information for these regions is rarer. For example, cards from countries such as Sweden or Belgium were the most costly, at an average of $20 each, while cards issued from the United States were the least expensive.

The lower price range for credit cards was also due to bulk purchase discounts offered by sellers. Credit cards are typically sold in bulk, with lot sizes from as few as 10 credit cards to as many as 5,000. Common bulk amounts and rates observed by Symantec during this reporting period were 100 credit cards for $150 ($1.50 each), 140 credit cards for $120 ($0.86 each), and 5,000 credit cards for $300 ($0.06 each).

[211] http://www.bis.org/publ/cpss85p2.pdf : table 7

[212] http://www.comscore.com/press/release.asp?press=2560

[213] http://online.wsj.com/article/SB122831827531375837.html. Cyber Monday is the first Monday after U.S. Thanksgiving, which has come to mark the beginning of the online shopping season. This is typically the busiest online shopping day of the year.

As with other areas of the underground economy, the availability of the item seems to determine its price: an increase in supply will decrease the price of the goods. There are more credit cards in circulation in the United States than in any other country in the world—1.3 billion cards by the end of 2007, which is an average of over four credit cards per person.[214] In comparison, there were only 67 million credit cards in circulation in the United Kingdom, which is an average of one per inhabitant and only 5 percent of the U.S. total. This correlates with the originating location percentages of credit cards advertised on underground economy servers for this reporting period: cards issued by U.S.-based institutions accounted for 67 percent of the total, while cards from UK-based institutions accounted for 11 percent. This ratio also corresponds to advertised bulk package prices: UK cards were typically advertised at rates three to four times higher than U.S. cards.

The second most commonly advertised good on underground economy servers during 2008 was bank account credentials, accounting for 19 percent of all advertised goods. This was a slight increase from 17 percent observed in 2007. Bank account credentials may consist of account numbers, bank transit numbers, account holder names and/or company names, and may include online banking passwords. Also, most sellers advertised the type of account and the balances for the stolen bank accounts. Attackers can steal bank account credentials using the same methods as were outlined in the discussion of credit cards previously in this section.

The popularity of bank account credentials may be due to a shift toward online banking. As mentioned earlier, in the United States, 44 percent of Internet users perform some degree of online banking.[215] That number is even higher in Canada and France, where 64 percent and 46 percent of Internet users bank online, respectively.[216] The potential increased availability of such sensitive information would likely also result in
an increase in attempts to steal banking credentials through phishing attempts or the use of malicious code such as banking Trojans. For example, Symantec observed an 86 percent increase in potential banking Trojan infections in the second half of 2007.

Bank account credentials are attractive to attackers because they offer the opportunity to withdraw currency directly. Withdrawing currency from a bank account has the advantage of a more immediate payout than with online purchases, which would need to be sold to realize a purely financial reward. Also, attackers have access to the full balances in the bank accounts, unlike credit cards where the credit limits imposed will not allow access to the maximum potential balances. Bank account balances advertised were also considerably higher than credit card limits; in 2008, the average advertised bank account balance was just over $176,000, while the average credit card limit was just over $3,400. It is likely that advertisers are skewing the average by promoting bank accounts with high balances, specifically from corporate accounts, to attract customers. Symantec observed advertisements with balances ranging from $3,000 to one with over $2.4 million. Beyond straightforward account cash outs, bank accounts can also be used as intermediary channels to launder money or to fund other online currency accounts that only accept bank transfers for payments.

The advertised price for bank account credentials varied as widely as it did in 2007, with prices ranging from $10 to $1,000, depending on the amount of funds available, the location of the account, and the type of account. Corporate and business accounts were advertised for considerably higher prices than those of personal bank accounts as they typically had higher balances on average. Symantec observed one EU business bank account—purportedly holding a balance of $400,000—being advertised for sale for $600.

[214] http://www.bis.org/publ/cpss85p2.pdf : tables 10 and 10b
[215] http://www.comscore.com/press/release.asp?press=2318
[216] http://www.comscore.com/press/release.asp?press=2524

In addition, EU accounts were advertised at a considerably higher average price than their U.S. counterparts, which may be because EU accounts are rarer than U.S. accounts on underground economy servers. Furthermore, bank account credentials that bundled in additional information such as names, addresses, dates of birth, and mothers' maiden names were advertised at higher prices, presumably because this added information could potentially be used for further identity fraud.

Email accounts were the third most common item advertised for sale on underground economy servers in 2008, making up 5 percent of all advertised goods, an increase from 4 percent in 2007. Gaining possession of email passwords can allow access to email accounts, which can be used for sending out spam and/or for harvesting additional email addresses from contact lists. Recipients of the spam emails may be more trusting of emails coming from a known email address. Moreover, along with email, many ISPs include free Web space in their account packages, which many people rarely access. Once the ISP accounts are compromised, these free spaces can be used to host phishing sites or malicious code without the knowledge of the victims.

In addition, compromised email accounts will often provide access to additional sensitive personal information such as bank account data, student identification numbers, mailing address and phone numbers, or access to other online accounts (such as social networking pages, online stock accounts, etc.) that is stored in saved personal emails. From there, it is often simple for someone to use the password recovery option offered on most online registration sites and have a new password sent via email to gain complete access to these accounts. This danger is compounded by the fact that many people have of using the same password for multiple accounts. The fraudulently gained personal information can then be used to conduct identity theft and fraud.

The advertised prices of email accounts depended on the ISP of the account; larger ISPs that offered large amounts of Web space were advertised at higher prices than ones with smaller space. Web-based email accounts from various ISPs around the world were advertised, although the location used to register the account did not factor into the advertised price since users could obtain the same type of access worldwide. Accounts registered in Europe, the United States, and the Middle East were advertised at the same prices for this reporting period, ranging from $1 to $100 for each account.

The distribution of goods and services advertised on underground economy servers continues to be focused on financial information, such as credit card information and bank account credentials. This seems to suggest that criminals are more focused on purchasing goods that allow them to make large quantities of money quickly on underground economy servers rather than on exploits that require more time and resources, such as scam pages and email lists for spamming. This trend is likely to continue until steps are taken to make it more difficult to obtain and use this financial information.

As part of their best practices to help prevent fraud, credit card companies, credit card issuers, and banks have been taking more secure measures to verify and authenticate users, such as multi-factor authorization or using technologies such as chip and PIN on the credit cards they issue.[217] By instituting effective multi-factor authentication and multi-level security systems, banks and credit card companies can make it more difficult for criminals to exploit stolen financial information. Also, security features such as Smart Card-based credit cards using the EMV standard for security verification,[218] or credit cards with chip & PIN technology for card-present transactions can make it more difficult for criminals to obtain and use financial information.

[217] http://www.chipandpin.co.uk/reflib/Consumer_digi-guide_Post_14_Feb_FINAL.PDF
[218] EMV is a standard for authenticating credit and debit card payments. The name originates from the initial letters of Europay, MasterCard, and Visa, who together developed the standard. Cf. http://www.emvco.com/about_emvco.aspx

Another technology currently being tested in the United Kingdom for card-not-present transactions, such as online shopping, are credit cards with one-time codes. To complete the transaction, credit card holders enter their PIN into the built-in keypad on the back of the card. Once the correct PIN is entered, the card will display a six-digit one-time code to be used to authenticate the transaction.[219] This code would be unique for each specific transaction. Even if the card is stolen or lost, a criminal would need the PIN to use the card.

Moreover, consumers who fear identity theft and payment fraud may be moving toward Internet-based payment services and other non-credit card electronic payment services. These types of services have become more popular because they do not expose the credit or debit card information that is used to set up the accounts and, as with some credit card issuers, often offer full protection from unauthorized transactions. In addition, they allow people without credit cards to make online purchases.

Nonetheless, even though consumers seem to be moving toward other non-credit card electronic payment services for online payments, credit cards are still the most popular payment method. People may prefer to use credit cards over other payment options because of the added bonuses sometimes associated with using them, such as zero liability, flight points, cash-back options, travel options, or dividend bonuses. In the United States, the value of credit card transactions for 2006 was estimated at just over $2.1 trillion—the equivalent of nearly $7,000 for each person in the United States.[220]

### Spam by category

Spam categories are assigned based on spam activity that is detected by the Symantec Probe Network. While some of the categories may overlap, this data provides a general overview of the types of spam that are most commonly seen on the Internet today. It is important to note that this data is restricted to spam attacks that are detected and processed by the Symantec Probe Network. Internal upstream processing may weed out particular spam attacks, such as those that are determined to be potential fraud attacks.

The most common type of spam detected in 2008 was related to Internet- or computer-related goods and services, which made up 24 percent of all detected spam (figure 21). In 2007, this was the second most common type of spam, accounting for 19 percent of the total. This type of spam is typically used to promote Web hosting and design, as well as other online commodities such as phishing and spam toolkits. Since phishing and spam toolkits cannot typically be advertised by legitimate means, such as through banner ads on websites, spam may be the most effective way to promote them.

The increase in spam associated with Internet- or computer-related goods and services is reflected in the items that were most commonly available on underground economy servers in 2008, as discussed in “Underground economy servers” previously. Email addresses, which are usually purchased for the sake of spamming, were the fourth most commonly advertised good.

Furthermore, scams ranked tenth in items for sale on underground economy servers in 2008. Scams advertised on these servers consist of creating scam Web pages, creating and disseminating scams, or hosting scam pages. Fraudsters promote these items, and buyers can often find them advertised on underground economy servers. This spamming activity in turn adds to the growth of the underground economy servers. Some of the phishing scams result in the harvesting of credit card and bank account credentials, which are then sold on underground economy servers.

[219] http://www.visaeurope.com/pressandmedia/newsreleases/press377_pressreleases.jsp
[220] http://www.bis.org/publ/cpss85p2.pdf : tables 9 and 9d

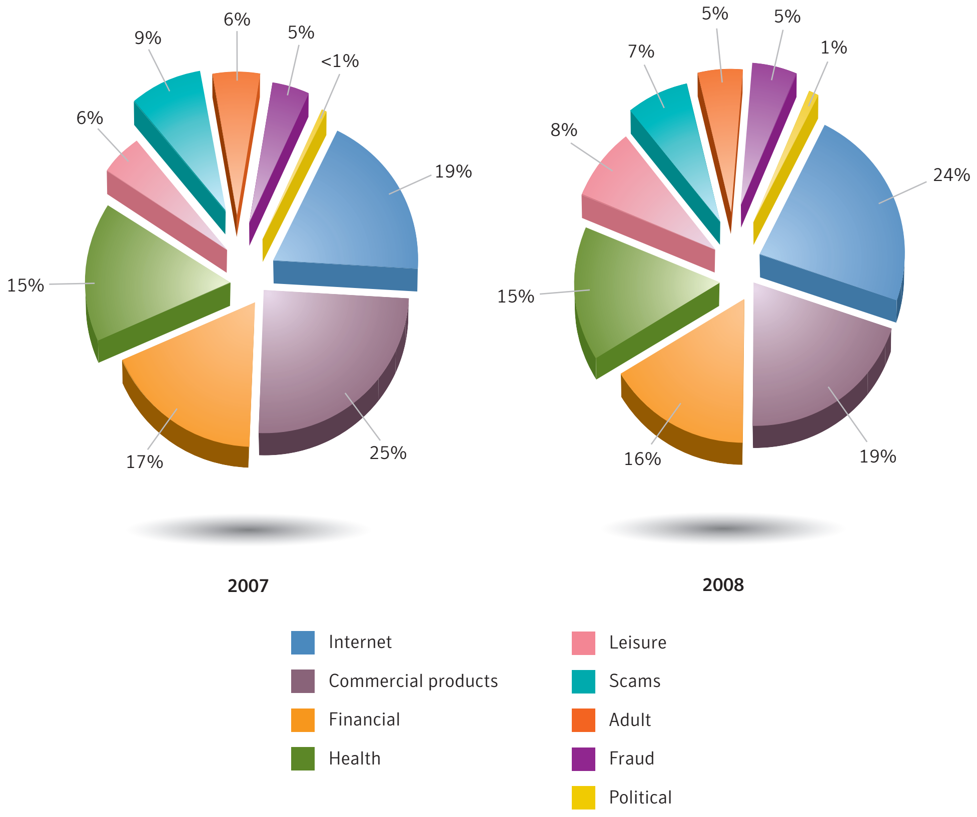

**Figure 21. Top spam categories**
*Source: Symantec*

The second most common type of spam detected in 2008 was related to commercial products, which made up 19 percent of all spam detected by Symantec sensors. In 2007, commercial spam was the most common type of spam, accounting for 25 percent of the total. Commercial products spam usually consists of advertisements for commercial goods and services. Such spam is frequently used to sell designer goods such as watches, handbags, and sunglasses. The profits from the sale of these products can be substantial given that the goods sold are often cheaply made counterfeits.

For 2008, Internet-related spam and commercial-products spam not only switched places from the previous year, but also percentages. Symantec believes this may be the result of the economic downturn. It is possible that, with the drop in consumer confidence, people are less inclined to buy the types of goods and services advertised by commercial-product spam.

Spam related to financial services made up 16 percent of all spam detected in 2008, making it the third most common type of spam during this period. Financial services spam contains references or offers related to money, the stock market, or other financial "opportunities." This is almost unchanged from 2007, when financial services spam was also the third most common type of spam, with 17 percent of the total. While it might be expected that spam offering stock market tips or other financial opportunities would drop off during a period of market uncertainty, it is likely that such a drop-off would be negated by an increase in spam offering such recession-related enticements as low-interest loans and easy access to credit.

### Top countries of spam origin

This section will discuss the top 10 countries of spam origin. This discussion is based on data gathered by customer installations of Symantec Brightmail AntiSpam. This data includes the originating server's IP address, against which frequency statistics are compared. Each IP address is mapped to a specific country and charted over time. The nature of spam and its distribution on the Internet presents challenges in identifying the location of people who are sending it because many spammers try to redirect attention away from their actual geographic location. In an attempt to bypass DNS block lists, they use Trojans that relay email, which allow them to send spam from sites distinct from their physical location. In doing so, they tend to focus on compromised computers in those regions with the largest bandwidth capabilities. As such, the region in which the spam originates may not correspond with the region in which the spammers are located.

Over the past year, Symantec observed a 192 percent increase in spam detected across the Internet, from 119.6 billion messages in 2007 to 349.6 billion in 2008. This is despite the shutdown of two major botnets in November, which is discussed in greater depth in the following paragraphs. After the shutdowns, Symantec saw a 65 percent decrease in spam activity. This lasted for a period of several weeks before returning to normal levels when the botnets were reestablished elsewhere.

During 2008, 29 percent of all spam originated in the United States (table 19), a decrease from 45 percent in 2007, when it was also the top country of spam origin. The prominence of the United States is not surprising, given that it has the second highest number of broadband Internet users in the world.[221] This is important because broadband connections are usually high-speed connections that are often constantly connected to the Internet. This allows spammers to send out high volumes of spam at any time of the day.

| 2008 Rank | 2007 Rank | Country | 2008 Percentage | 2007 Percentage |
|---|---|---|---|---|
| 1 | 1 | United States | 29% | 45% |
| 2 | 8 | Russia | 6% | 3% |
| 3 | 15 | Turkey | 5% | 1% |
| 4 | 2 | China | 4% | 4% |
| 5 | 12 | Brazil | 4% | 2% |
| 6 | 7 | United Kingdom | 3% | 5% |
| 7 | 6 | Germany | 3% | 3% |
| 8 | 9 | Italy | 3% | 2% |
| 9 | 5 | Poland | 2% | 3% |
| 10 | 10 | Spain | 2% | 2% |

**Table 19. Top 10 countries of spam origin**
*Source: Symantec*

[221] http://www.point-topic.com

Despite this, the rate of growth of spam originating in the United States was slower than the rate of growth across the Internet in general. In 2008, spam messages increased by 89 percent in the United States, from approximately 54 billion to roughly 102 billion messages. While this increase may seem significant, it is well behind the 192 percent increase in spam activity across the Internet as a whole.

The slower increase in spam originating in the United States is likely due to the November 2008 shutdown of the McColo ISP, which was believed to be responsible for a considerable amount of spam activity. This shutdown is thought to have affected the percentage of email identified as spam because McColo was allegedly hosting a significant number of bot C&C systems (as detailed in the bot discussions of the "Threat Activity Trends" section of this report). The volume change was measured directly in the Symantec Probe Network, which saw a 65 percent drop in traffic in the 24 hours after the shutdown.[222] Symantec believes that the ISP was being used to host bot C&C servers for a number of botnets that were responsible for propagating spam.[223] While the shutdown of McColo resulted in a temporary slowdown of spam originating in the United States, by mid-December spam volumes had slowly crept back up to within 80 percent of their levels before the shutdown, as old botnets were brought back online, and new botnets were created.[224]

Russia was the second ranked country for originating spam in 2008, with 6 percent. This is a significant increase from 2007, when 3 percent of spam originated in Russia and it ranked eighth. While it accounted for a relatively small percentage of worldwide spam, Russia was the site of a very large increase, with the amount of spam originating there increasing by 445 percent over the course of 2008.

This increase is likely due to two factors. First, Russia is one of the four largest emerging broadband markets worldwide.[225] Second, there is a considerable amount of organized crime activity based in Russia, much of which focuses on fraudulent online activity.[226] MessageLabs Intelligence reported that 12 percent of all malicious websites blocked in 2008 were registered with .ru, the TLD for websites registered in Russia.[227]

Turkey had the third highest volume of spam in 2008, with 5 percent of all detected spam. This is a significant increase from 2007 when Turkey had the fifteenth highest volume of spam, with only 1 percent. Not only is this a considerable jump in rankings, but the volume of spam originating in Turkey increased by nearly 1,200 percent.

The volume of spam originating in Turkey in 2008 was not steady, but increased from August until the end of the year. During this time, Turkey was the second ranked country of origin, with the volume of spam varying from 6 to 8 percent of the global total.[228] This may be related to the migration of bot C&C servers following the shutdown of McColo and other ISPs linked to malicious activities during the same period. Analysts believe that those ISPs were being used by spammers to distribute their attacks.[229] Once the ISPs were shut down, spammers were forced to relocate. It appears from the increase in spam activity originating in Turkey during that period that they may have relocated some of their servers there.

[222] http://eval.symantec.com/mktginfo/enterprise/other_resources/b-state_of_spam_report_12-2008.en-us.pdf : p. 7
[223] http://www.messagelabs.com/mlireport/MLIReport_2008.09_Sep_Final.pdf
[224] http://eval.symantec.com/mktginfo/enterprise/other_resources/b-state_of_spam_report_01-2009.en-us.pdf : p. 7
[225] http://www.messagelabs.com/mlireport/MLIReport_Annual_2008_FINAL.pdf : p. 29
[226] http://www.guardian.co.uk/technology/2007/nov/15/news.crime
[227] http://www.messagelabs.com/mlireport/MLIReport_2008.09_Sep_Final.pdf : p. 50
[228] http://www.symantec.com/business/theme.jsp?themeid=state_of_spam#
[229] Cf. http://voices.washingtonpost.com/securityfix/2008/10/spam_volumes_plummet_after_atr.html , http://www.crn.com/security/212002220, or http://www.messagelabs.com/mlireport/MLIReport_2008.09_Sep_Final.pdf

## Percentage of spam from botnets

In 2007, botnets became the dominant force in terms of distributing not only spam, but also malicious code and phishing scams. The processing power of large botnets allows them to generate high volumes of spam. The distributed processing power of botnets makes them an ideal platform for launching large-scale spam campaigns. Because of their distributed nature, even taking down a large number of individual bots and entire botnets has little effect on the percentage of spam for which they are responsible.

In 2008, botnets were responsible for approximately 90 percent of all spam email (figure 22). In August 2008, spam volumes rose more than twofold as a result of the continued, aggressive approaches taken to expand botnet capacity, especially with the Srizbi and Cutwail botnets, which both grew in size by 20 to 25 percent by mid-2008.

As noted in “Bot-infected computers,” Symantec observed over 9 million distinct bot-infected computers during 2008. With such a large number of bots available to attackers, it is likely that many would be used to generate profit. It was discussed in the recent Symantec *Report on the Underground Economy* that many botnets are available to be rented or purchased on underground economy channels. A spammer could purchase one of these botnets and earn income by using it to send large volumes of spam.

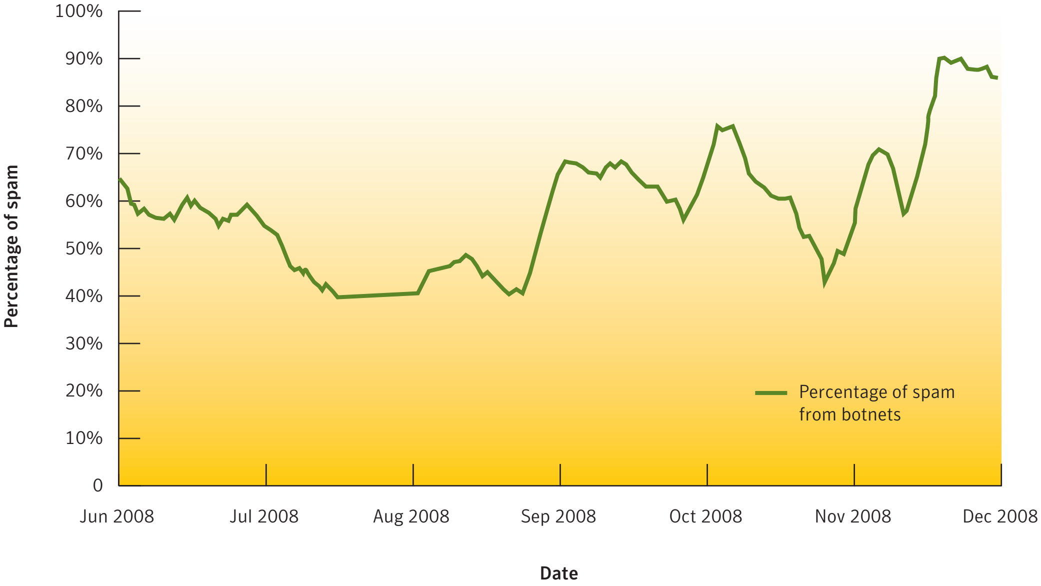

**Figure 22. Percentage of spam from botnets**
*Source: Symantec*

Spam activities were disrupted somewhat with the previously discussed shutdowns of two ISPs in late 2008.[230] While these shutdowns reduced spam levels temporarily, they returned to previous levels shortly thereafter. This is likely due in large part to the ability of spammers to create new botnets and to rework existing botnets. Further, while it is likely that a large number of bots and other spam relays were taken offline, the bot owners may have simply increased the output from their remaining botnets.

Additionally, the shift toward HTTP bot C&C structures, discussed in "Bot command-and-control servers," means that many botnets will be more difficult to disable since there is no longer a need for a centralized controller. Removing large numbers of bots—such as by the shutdown of ISPs—will cause temporary reductions in spam volumes, but attackers have shown the ability to relocate and resume their operations in relatively short periods of time.

### Phishing, underground economy servers, and spam—protection and mitigation

Symantec recommends that enterprise users protect themselves against phishing threats by filtering email at the server level through the mail transfer agent (MTA). Although this will likely remain the primary point of filtering for phishing, organizations can also use IP-based filtering upstream, as well as HTTP filtering.

DNS block lists also offer protection against potential phishing emails.[231] Organizations could also consider using domain-level or email authentication in order to verify the actual origin of an email message. This can protect against phishers who are spoofing email domains.[232]

To protect against potential phishing activity, administrators should always follow Symantec best practices, as outlined in Appendix A of this report. Symantec also recommends that organizations educate their end users about phishing.[233] They should also keep their employees notified of the latest phishing attacks and how to avoid falling victim to them, and provide a means to report suspected phishing sites.[234]

Organizations can also employ Web-server log monitoring to track if and when complete downloads of their websites, logos, and images are occurring. Such activity may indicate that someone is attempting to use the legitimate website to create an illegitimate website for phishing.

Organizations can detect phishing attacks that use spoofing by monitoring non-deliverable email addresses or bounced email that is returned to non-existent users. They should also monitor the purchasing of cousin domain names by other entities to identify purchases that could be used to spoof their corporate domains.[235] So-called typo domains and homographic domains should also be monitored.[236] This can be done with the help of companies that specialize in domain monitoring; some registrars also provide this service.

The use of antiphishing toolbars and components in Web browsers can also help protect users from phishing attacks. These measures notify the user if a Web page being visited does not appear to be legitimate. This way, even if a phishing email reaches a user's inbox, the user can still be alerted to the potential threat.

[230] http://www.securityfocus.com/brief/855

[231] A DNS block list (sometimes referred to as a black list) is simply a list of IP addresses that are known to send unwanted email traffic. It is used by email software to either allow or reject email coming from IP addresses on the list.

[232] Spoofing refers to instances where phishers forge the "From:" line of an email message using the domain of the entity they are targeting with the phishing attempt.

[233] Cf., basic guidelines on how to avoid phishing at the United States Federal Trade Commission: http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.htm

[234] Cf. http://www.antiphishing.org for information on the latest phishing threats.

[235] "Cousin domains" refers to domain names that include some of the key words of an organization's domain or brand name; for example, for the corporate domain "bigbank.com", cousin domains could include "bigbank-alerts.com", "big-bank-security.com", and so on.

[236] Typo domains are domain names that use common misspellings of a legitimate domain name, for example the domain "symatnec.com" would be a typo domain for "symantec.com". A homographic domain name uses numbers that look similar to letters in the domain name, for example the character for the number "1" can look like the letter "l".

End users should follow best security practices, as outlined in Appendix A of this report. They should use an antiphishing solution. As some phishing attacks may use spyware and/or keystroke-logging applications, Symantec advises end users to use antivirus software, antispam software, firewalls, toolbar blockers, and other software-detection methods. Symantec also advises end users to never disclose any confidential personal or financial information unless and until they can confirm that any request for such information is legitimate.

Users should review bank, credit card, and credit information frequently. This can provide information on any irregular activities. For further information, the Internet Fraud Complaint Center (IFCC) has also released a set of guidelines on how to avoid Internet-related scams.[237] Additionally, network administrators can review Web proxy logs to determine if any users have visited known phishing sites.

Consumers could also take more security precautions to ensure that their information will not be compromised. When conducting higher-risk Internet activities, such as online banking or purchases, consumers should do so only on their own computers and not public ones. Further, they should not store passwords or bank card numbers. They should also avoid following links from within messages (whether in email, instant messages, online forums, etc.) as these may be links to spoofed websites; instead, they should manually type in the URL of the website. Also, consumers should be aware of the amount of personal information that they post on the Internet, as criminals may take advantage of this public information in malicious activities such as phishing scams.

[237] http://www.fbi.gov/majcases/fraud/internetschemes.htm

## Appendix A—Symantec Best Practices

### Enterprise best practices

- Employ defense-in-depth strategies, which emphasize multiple, overlapping, and mutually supportive defensive systems to guard against single-point failures in any specific technology or protection method. This should include the deployment of regularly updated antivirus, firewalls, intrusion detection, and intrusion protection systems on client systems.
- Turn off and remove services that are not needed.
- If malicious code or some other threat exploits one or more network services, disable or block access to those services until a patch is applied.
- Always keep patch levels up to date, especially on computers that host public services and are accessible through the firewall, such as HTTP, FTP, email, and DNS services.
- Consider implementing network compliance solutions that will help keep infected mobile users out of the network (and disinfect them before rejoining the network).
- Enforce an effective password policy.
- Configure mail servers to block or remove email that contains file attachments that are commonly used to spread viruses, such as .VBS, .BAT, .EXE, .PIF, and .SCR files.
- Isolate infected computers quickly to prevent the risk of further infection within the organization.
- Perform a forensic analysis and restore the computers using trusted media.
- Train employees to not open attachments unless they are expected and come from a known and trusted source, and to not execute software that is downloaded from the Internet unless it has been scanned for viruses.
- Ensure that emergency response procedures are in place. This includes having a backup-and-restore solution in place in order to restore lost or compromised data in the event of successful attack or catastrophic data loss.
- Educate management on security budgeting needs.
- Test security to ensure that adequate controls are in place.
- Be aware that security risks may be automatically installed on computers with the installation of file-sharing programs, free downloads, and freeware and shareware versions of software.
- Clicking on links and/or attachments in email messages (or IM messages) may also expose computers to unnecessary risks. Ensure that only applications approved by the organization are deployed on desktop computers.

### Consumer best practices

- Use an Internet security solution that combines antivirus, firewall, intrusion detection, and vulnerability management for maximum protection against malicious code and other threats.
- Ensure that security patches are up to date and that they are applied to all vulnerable applications in a timely manner.
- Ensure that passwords are a mix of letters and numbers, and change them often. Passwords should not consist of words from the dictionary.
- Never view, open, or execute any email attachment unless the attachment is expected and the purpose of the attachment is known.
- Keep virus definitions updated regularly. By deploying the latest virus definitions, you can protect your computer against the latest viruses known to be spreading in the wild.
- Routinely check to see if your operating system is vulnerable to threats by using Symantec Security Check at www.symantec.com/securitycheck.
- Deploy an antiphishing solution. Also, never disclose any confidential personal or financial information unless and until you can confirm that any request for such information is legitimate.
- Get involved by tracking and reporting attack attempts. With Symantec Security Check's tracing service, users can quickly identify the location of potential hackers and forward the information to the attacker's ISP or local police.
- Be aware that security risks may be automatically installed on computers with the installation of file-sharing programs, free downloads, and freeware and shareware versions of software.
- Avoid clicking on links and/or attachments in email or IM messages, as these may also expose computers to unnecessary risks.
- Read end-user license agreements (EULAs) carefully and understand all terms before agreeing to them as some security risks can be installed after an end user has accepted the EULA or as a consequence of that acceptance.
- Be aware of programs that flash ads in the user interface. Many spyware programs track how users respond to these ads, and their presence is a red flag. These ads may be spyware.

## Appendix B—Threat Activity Trends Methodology

Threat activity trends in this report are based on the analysis of data derived from the Symantec Global Intelligence network, which includes the Symantec DeepSight™ threat Management System, Symantec Managed Security Services, the Symantec Honeypot network, and proprietary Symantec technologies. Symantec combines data derived from these sources for analysis.

### Malicious activity by country

To determine the top countries for the "Malicious activity by country" metric, Symantec compiles geographical data on each type of malicious activity to be considered, namely: bot-infected computers, phishing website hosts, malicious code reports, spam zombies, and attack origin. The proportion of each activity originating in each country is then determined. The mean of the percentages of each malicious activity that originates in each country is calculated. This average determines the proportion of overall malicious activity that originates from the country in question and the rankings are determined by calculating the mean average of the proportion of these malicious activities that originated in each country.

### Data breaches that could lead to identity theft

Symantec identifies the proportional distribution of cause and sector for data breaches that may facilitate identity theft based on data provided by the Open Security Foundation (OSF) Dataloss DB.[238] OSF reports data breaches that have been reported by legitimate media sources and have exposed personal information including name, address, Social Security number, credit card number, or medical history. The sector that experienced the loss along with the cause of loss that occurred is determined through analysis of the organization reporting the loss and the method that facilitated the loss.

### Bot-infected computers

Symantec identifies bot-infected computers based on coordinated scanning and attack behavior that is observed in global network traffic. An active bot-infected computer is one that carries out at least one attack per day. This does not have to be continuous; rather, a single computer can be active on a number of different days. Attacks are defined as any malicious activity carried out over a network that has been detected by an intrusion detection system (IDS) or firewall.

For an attacking computer to be considered to be participating in coordinated scanning and attacking, it must fit into that pattern to the exclusion of any other activity. This behavioral matching will not catch every bot-infected computer, and may identify other malicious code or individual attackers behaving in a coordinated way as a botnet. This behavioral matching will, however, identify many of the most coordinated and aggressive bot-infected computers. It will also give insight into the population trends of bot-infected computers, including those that are considered to be actively working in a well-coordinated and aggressive fashion at some point in time during the reporting period.

[238] http://datalossdb.org

### Bot command-and-control servers

Symantec tracks the number of new bot C&C servers detected worldwide. Only IRC and HTTP bot C&C server trends will be evaluated in the methods botnet owners are using to communicate with their bot-infected computers.

### Top Web-based attacks

To evaluate this metric, Symantec identifies each distinct attack delivered via the Web, hereafter referred to as Web-based attack, hosted on malicious websites that are detected by intrusion prevention technology. A Web-based attack is any attack that is carried out against a client-side application originating from the Web. Symantec determines the top Web-based attacks based by determining the most common attacks carried out against users. Due to the nature of Web-based attacks, the total number of attacks carried out is a good measure of the success and popularity of the attack.

Each attack discussed targets a specific vulnerability or weakness in Web browsers or other client-side applications that process content originating from the Web. These attacks can vary in their delivery methods; some rely on misleading a user into downloading a malicious file, while others occur without any knowledge or interaction by the user.

### Top countries of origin for Web-based attacks

Symantec identifies the Web-based attacks by country by determining the geographic origin that conducts the attack on computers upon visiting a website. Note that the server hosting the exploit may not necessarily be the same server that the user has visited due to redirection. A user could visit a website that redirects their Web browser to a malicious server in another country.

## Appendix C—Vulnerability Trends Methodology

Symantec operates one of the most popular forums for the disclosure and discussion of vulnerabilities on the Internet, the BugTraq™ mailing list,[239] which has approximately 50,000 direct subscribers who contribute, receive, and discuss vulnerability research on a daily basis. Symantec also maintains one of the most comprehensive vulnerability databases, currently consisting of over 32,000 vulnerabilities (spanning more than two decades) affecting more than 72,000 technologies from over 11,000 vendors.

### Vulnerability classifications

Following the discovery and/or disclosure of a new vulnerability, Symantec analysts gather all relevant characteristics of the new vulnerability and create an alert. This alert describes important traits of the vulnerability, such as the severity, ease of exploitation, and a list of affected products. These traits are subsequently used both directly and indirectly for this analysis.

### Vulnerability types

After discovering a new vulnerability, Symantec threat analysts classify the vulnerability into one of 12 possible categories based on the available information. These categories focus on defining the core cause of the vulnerability, as opposed to classifying the vulnerability merely by its effect.

The classification system is derived from the academic taxonomy presented by Taimur Aslam, et al (1996),[240] which provides a full description of the possible values below:

- Boundary condition error
- Access validation error
- Origin validation error
- Input validation error
- Failure to handle exceptional conditions
- Race condition error
- Serialization error
- Atomicity error
- Environment error
- Configuration error
- Design error

### Window of exposure for Web browsers

The window of exposure is calculated for vulnerabilities associated with the following Web browsers:

- Google Chrome
- Apple Safari
- Microsoft Internet explorer
- Mozilla browsers
- Opera

[239] The Bugtraq mailing list is hosted by SecurityFocus (http://www.securityfocus.com). Archives are available at http://www.securityfocus.com/archive/1
[240] "Use of a taxonomy of Security Faults": http://ftp.cerias.purdue.edu/pub/papers/taimur-aslam/aslam-krsul-spaf-taxonomy.pdf

Symantec records the window of time between the publication of an initial vulnerability report and the appearance of third-party exploit code; this is known as the exploit code development time. The time period between the disclosure date of a vulnerability and the release date of an associated patch is known as the patch development time. The time lapse between the public release of exploit code and the time that the affected vendor releases a patch for the affected vulnerability is known as the window of exposure. The average window of exposure is calculated as the difference in days between the average patch development time and the average exploit code development time. During this time, the computer or system on which the affected application is deployed may be susceptible to attack, as administrators may have no official recourse against a vulnerability and must resort to best practices and workarounds to reduce the risk of attacks. Explanations of the average exploit development time and the average patch development time are included below.

### Exploit code development time for Web browsers

The cumulative exploit code development time for each vulnerability affecting a Web browser is calculated. Each cumulative time is then divided by the number of vulnerabilities affecting that browser to determine the average exploit code development time for that browser. The exploit development time average for each browser is then compared. This metric is used to compute the window of exposure, which amounts to the difference between the average patch development time and the average exploit code development time.

### Patch development time for Web browsers

The cumulative patch development time for vulnerabilities affecting each browser is calculated. Each cumulative time is then divided by the number of vulnerabilities affecting that browser to determine the average patch development time for that browser. The patch development time average for each browser is then compared. This metric is used to compute the window of exposure for Web browsers, which amounts to the difference between the average patch development time and the average exploit code development time.

### Web browser vulnerabilities

This metric compares vulnerability data for major Web browsers, namely: Google Chrome, Microsoft Internet Explorer, Mozilla browsers (including Firefox), Opera, and Apple Safari. However, in assessing the comparative data, it should be noted that for this report the total number of vulnerabilities in these Web browsers is computed, including both vendor confirmed and non-vendor confirmed vulnerabilities.

Previous versions of the Symantec *Global Internet Security Threat Report* have discussed vulnerabilities according to whether they were vendor confirmed or non-vendor confirmed, because vulnerabilities that were not confirmed were also included in the data. This differentiation was important, especially given the disparity in patch times between vendors. However, starting with Volume X of the Symantec *Internet Security Threat Report*, this convention is no longer followed and no differentiation is made between vendor-confirmed vulnerabilities and non-vendor-confirmed vulnerabilities when calculating the total number of vulnerabilities.

Individual browser vulnerabilities are difficult to precisely identify. A reported attack may be a combination of several conditions, each of which could be considered a vulnerability in its own right, which may distort the total vulnerability count. Some browser issues have also been improperly identified as operating system vulnerabilities or vice versa. This is partly due to increased operating system integration that makes it difficult to correctly identify the affected component in many cases. Additionally, some browsers are available for mobile and desktop platforms. Therefore, the following caveats exist for this metric:

- Many vulnerabilities in shared operating system components can be exposed to attacks through the browser. This report enumerates only those vulnerabilities that are known to affect the browser itself where sufficient information is available to make the distinction.
- Vulnerabilities in mobile versions of a browser are only counted if they also affect the desktop version of the browser application. This metric is mainly concerned with evaluating vulnerabilities in desktop Web browsers and not their mobile equivalents.

### Web browser plug-in vulnerabilities

Browser plug-ins are technologies that extend the functionality of the Web browser. They may be developed by the vendor or by a third-party. Some plug-ins provide support for additional application programming languages or environments, such as Java or Flash Player. Others are applications in their own right that run in the browser. Examples of these include ActiveX objects for Internet explorer, and Mozilla extensions and add-ons.

This metric enumerates publicly documented vulnerabilities that affect browser plug-ins. These vulnerabilities are further classified, when applicable, into general groups of browser plug-in technologies. Symantec makes an effort to identify all vulnerabilities affecting the various classes of browser plug-in.

Vulnerabilities that affect the browser itself are not included in the data for this metric when it is possible to make this distinction. In cases where a Web browser ships with a particular plug-in, vulnerabilities affecting that plug-in will be counted. Although in this case, the plug-in may be included in the default browser installation, it is still considered a separate technology and not a native feature of the browser. Native features are considered to be features intrinsic to the primary function of the browser such as support for HTTP/HTTPS, HTML rendering, JavaScript, and other standards that are commonly implemented in most Web browsers. Technologies such as Java and Flash Player may be common to many Web browsers but they are intended to extend their functionality to support additional types of content and are typically optional components.

The definition of browser plug-ins for this report is limited to technologies that are hosted on the same computer as the browser, and whose installation and configuration is managed through the browser or operating system. This distinguishes them from content that is intended to run inside the browser but is typically external to the browser such as Java applets or Flash movies. This content is rendered or executed by a browser plug-in but is not considered to be a plug-in in its own right.

### Web browser plug-in vulnerabilities, by type

This metric will examine some specific vulnerabilities that affect browser plug-ins. To do so, the vulnerabilities covered in the previous metric are classified into various categories based on their security impact.

The categories below are meant to highlight the primary impact on end-users. It should be noted that some vulnerabilities defy categorization due to inadequate public information about the nature of the vulnerability and its potential impact. For example, a number of vulnerabilities reportedly allow remote code execution, but the information available at the time of writing is inadequate to determine the effect of such techniques. Therefore, these vulnerabilities cannot be classified into the categories listed below. The number of vulnerabilities for each period that cannot be categorized is noted in the discussion.

Vulnerabilities affecting browser plug-in technologies will be classified into the following categories:

- **Memory corruption:** This is a class of vulnerabilities that allows attackers to corrupt the memory of an application process with malicious input. This category consists of stack- and heap-based buffer overflow conditions, and a number of other erroneous conditions that could let an attacker influence the execution of a application process by altering the contents of its memory. These vulnerabilities have a potential to let attackers execute arbitrary code.
- **Denial-of-service:** Denial-of-service vulnerabilities are vulnerabilities that typically result in an application crash when exploited. This may be due to a failure to handle exceptional conditions. Some of these vulnerabilities may be due to an underlying memory corruption issue. However, for this report, such vulnerabilities are classified as denial-of-service when there is believed to be no potential of arbitrary code execution.
- **Information disclosure:** These vulnerabilities are issues whose main effect is to expose sensitive information to an unauthorized party. This may occur as a result of active exploitation or may be an inadvertent side effect of an erroneous condition in the application. For the purpose of this report, this category does not include vulnerabilities that potentially disclose the contents of files on the affected computer.
- **Content injection:** These vulnerabilities directly facilitate injection of malicious content such as HTML and script code or they allow attackers to bypass input validation filters on third-party websites that are designed to prevent content injection. These vulnerabilities could allow cross-site scripting attacks.
- **Spoofing:** These are vulnerabilities that allow an attack to spoof elements of the browser user interface. Such attacks may facilitate spoofing of content to make a phishing site appear more authentic to victims of the attack.
- **Unauthorized file system access:** This category includes vulnerabilities that allow attackers to view, modify, or delete files on the computer hosting the affected browser plug-in. Such vulnerabilities have collateral effects such as the ability to gain unauthorized access to sensitive information, delete critical system files, or execute arbitrary code. This would include vulnerabilities that force a victim into silently downloading and executing a malicious executable.

- **Command execution:** Command execution vulnerabilities are those that allow a remote attacker to execute operating system commands through an affected browser plug-in. This would include a vulnerability that directly allows an attacker to submit commands to an operating system command such as a shell. This would also include vulnerabilities that let an attacker execute specific programs on the affected computer with attacker-specified arguments.
- **Origin validation:** These are vulnerabilities that occur when content from an invalid or unauthorized originating source is treated as valid by the browser plug-in technology. Vulnerabilities that bypass the "same origin policy" are an example, because they allow content from an external domain to access properties of a site that the user is browsing.
- **Elevated security context:** These vulnerabilities specifically violate a security policy that is intended to prevent remote content (such as from a Web page) from accessing system properties and capabilities. Vulnerabilities that bypass the Java plug-in virtual machine sandbox are an example of elevated security context. Another example is vulnerabilities that allow an attacker to execute malicious content in the context of a different security zone in Internet Explorer. It should be noted that for the purpose of this report, some vulnerabilities may present an opportunity for elevated security bypass but are more accurately described by another category such as unauthorized file system access.

## Site-specific cross-site scripting vulnerabilities

Data for this metric is provided by the XSSed project,[241] an online archive of publicly known cross-site scripting vulnerabilities that affect specific websites. The XSSed project gathers its data from security researchers who report specific instances of vulnerabilities in websites. Each submission is verified before it is published in the XSSed archive. The archive stores additional information such as the publication date, affected domain, proof-of-concept examples, and the fix status of the vulnerability. This information allows for the following statistics to be gathered:

- The number of vulnerabilities reported over a specific period of time;
- The number of vulnerabilities patched by the maintainers of the affected sites;
- The average time that it took for site maintainers to patch vulnerabilities.

The data in this metric is limited to the vulnerabilities that security researchers report to the XSSed project, which is not intended to be a complete database of all publicly known site-specific cross-site scripting vulnerabilities. Therefore, the metric is intended to provide insight into site-specific vulnerabilities, but does not provide a complete picture of all publicly known activity.

## Zero-day vulnerabilities

For the purpose of this metric, a zero-day vulnerability is one for which there is sufficient public evidence to indicate that the vulnerability has been exploited in the wild prior to being publicly known. It may not have been known to the vendor prior to exploitation, and the vendor had not released a patch at the time of the exploit activity. This metric is derived from public sources and the Symantec vulnerability database. This metric is meant to calculate the number of high-profile, publicly documented zero-day vulnerability instances during the relevant reporting periods.

[241] http://www.xssed.com/

### Top attacked vulnerabilities

Symantec IPS systems monitor attack activity in the wild. Symantec has 24 million sensors deployed throughout the world, which have recorded over 360 million events. This metric examines the top attacked vulnerabilities detected by Symantec IPS systems. Whether or not an event is associated with a vulnerability is determined by the signature that was triggered for the event. Each event in the data set used for metric is indicative of possible attack activity for a specific vulnerability, but does not necessarily mean that the attack was successful or that the attacked computer was compromised.

The top attacked vulnerabilities are determined on a yearly basis. For each year, Symantec examines the vulnerabilities published during the year with the most associated attack activity. The vulnerabilities are then ranked from one to ten from the highest amount of attack activity to the lowest amount of attack activity.

### Attacked vulnerabilities by attack vector (client versus server)

This metric examines attack activity targeting vulnerabilities. The attacked vulnerabilities are examined on a yearly basis. For each year, the vulnerabilities published during the year that are associated with attack events are categorized into the following attack vectors:

- **Client:** These are attacks that attempt to exploit client-side vulnerabilities . Client-side vulnerabilities affect client software such as Web browsers. They also include desktop application vulnerabilities that require user-interaction on the part of the user to successfully exploit.
- **Server:** These are attacks that attempt to exploit server-side vulnerabilities. A server-side vulnerability is one that usually affects a networked service that is hosted on a computer. The service is often always running and awaits incoming connections from clients.

After the attacked vulnerabilities have been categorized, Symantec determines that percentage of the total with client attack vectors in relation to the percentage of the total with server attack vectors.

### Severity of vulnerabilities

This metric also employs the CVSS, using its base score field criteria to determine the inherent properties of a vulnerability, such as:

- The degree of confidentiality, integrity, or availability of data that may be affected by the vulnerability;
- Local versus remote exploitability;
- Whether or not authentication is required for exploitation;
- And/or if there are additional factors that may complicate exploitation of the vulnerability.

These values are not adjusted for temporal factors such as the availability of exploit code. The base score is intended to be a static value that should only change if additional information is made available that changes the inherent characteristics of the vulnerability. The base score can have a value of zero to 10.

For the sake of categorizing vulnerabilities by their respective severities, the following standard is used:

- **Low severity (base score of 0–3):** Successful exploitation of these vulnerabilities will have a minimal impact on the confidentiality, integrity, and availability of data stored upon or transmitted over systems on which the vulnerability may be found. These vulnerabilities also tend to be local in nature, have a high degree of access complexity, and may require authentication to be exploited successfully.
- **Medium severity (base score of 4–7):** Successful exploitation of these vulnerabilities could allow a partial compromise of the confidentiality, integrity, and availability of data stored upon or transmitted over systems on which the vulnerability may be found, although this may not always be the case. These vulnerabilities can be exploited remotely over a network and may have a lower access complexity or may or may not require authentication to successfully exploit.
- **High severity (base score of 8–10):** these vulnerabilities have innate characteristics that present the highest threat profile. Successful exploitation often allows a complete compromise of the confidentiality, integrity, and availability of data stored upon or transmitted over systems on which the vulnerability may be found. These vulnerabilities are exploited remotely across a network, have a low degree of access complexity, and usually do not require authentication prior to successful exploitation.

Base scores are computed from related fields in the Symantec Vulnerability Database. They are then categorized into low, medium, and high and broken out by reporting period.

## Appendix D—Malicious Code Trends Methodology

Malicious code trends are based on statistics from malicious code samples reported to Symantec for analysis. The data is gathered from over 130 million client, server, and gateway systems that have deployed Symantec's antivirus products in both consumer and corporate environments. The Symantec Digital immune System and Scan and Deliver technologies allow customers to automate this reporting process. Observations in this section are based on empirical data and expert analysis of this data. The data and analysis draw primarily from the two databases described below.

### Infection database

Symantec developed the Symantec AntiVirus research Automation (SARA) technology to help detect and eradicate computer viruses. This technology is used to analyze, replicate, and define a large subset of the most common computer viruses that are quarantined by Symantec Antivirus customers.

On average, SARA receives hundreds of thousands of suspect files daily from both enterprise and individual consumers located throughout the world. Symantec then analyzes these suspect files, matching them with virus definitions. An analysis of this aggregate data set provides statistics on infection rates for different types of malicious code.

### Malicious code database

In addition to infection data, Symantec Security response analyzes and documents attributes for each new form of malicious code that emerges both in the wild and in a "zoo" (or controlled laboratory) environment. Descriptive records of new forms of malicious code are then entered into a database for future reference. For this report, a historical trend analysis was performed on this database to identify, assess, and discuss any possible trends, such as the use of different infection vectors and the frequency of various types of payloads. In some cases, Symantec antivirus products may initially detect new malicious code heuristically or by generic signatures. These may later be reclassified and given unique detections. Because of this, there may be slight variance in the presentation of the same data set from one volume of the Symantec *Global Internet Security Threat Report* to the next.

### Geographic location of malicious code instances

Several third-party subscription-based databases that link the geographic locations of systems to IP addresses are used along with proprietary Symantec technology to determine the location of computers reporting malicious code instances. While these databases are generally reliable, there is a small margin of error. The data produced is then used to determine the global distribution of malicious code instances.

### Percentage of malicious code that exploits vulnerabilities

Symantec maintains a malicious code database to analyze and document individual instances of malicious code dating back to 1998. The database includes metadata for classifying malicious code by type, discovery date, and by threat profile, in addition to providing mitigating factors and manual removal steps. Where applicable, this database includes correlations between malicious code instances and vulnerabilities from the Symantec vulnerability database. This capability was used as a basis for the data in this metric. Symantec examined the means by which the malicious code propagated, and counted those that propagate by exploiting vulnerabilities.

## Appendix E—Phishing, Underground Economy Servers, and Spam Trends Methodology

Phishing and spam attack trends in this report are based on the analysis of data captured through the Symantec Probe Network, a system of more than 2.5 million decoy accounts, MessageLabs Intelligence, and other Symantec technologies in more than 86 countries from around the globe. Over eight billion email messages, as well as over one billion Web requests, are scanned per day across 16 data centers. Symantec also gathers phishing information through an extensive antifraud community of enterprises, security vendors and more than 50 million consumers.

The Symantec Probe Network data is used to track the growth in new phishing activity. It should be noted that different monitoring organizations use different methods to track phishing attempts. Some groups may identify and count unique phishing messages based solely on specific content items such as subject headers or URLs. These varied methods can often lead to differences in the number of phishing attempts reported by different organizations.

Symantec Brightmail AntiSpam data is also used to gauge the growth in phishing attempts as well as the percentage of Internet mail determined to be phishing attempts. Data returned includes messages processed, messages filtered, and filter-specific data.

Symantec has classified different filters so that spam statistics and phishing statistics can be determined separately. Symantec Brightmail AntiSpam field data includes data reported back from customer installations providing feedback from antispam filters as well as overall mail volume being processed.

Symantec Brightmail AntiSpam only gathers data at the SMTP layer and not the network layer, where DNS block lists typically operate because SMTP-layer spam filtering is more accurate than network-layer filtering and is able to block spam missed at the network layer. Network layer-filtering takes place before email reaches the enterprise mail server. As a result, data from the SMTP layer is a more accurate reflection of the impact of spam on the mail server itself.

Due to the numerous variables influencing a company’s spam activity, Symantec focuses on identifying spam activity and growth projections with Symantec Brightmail AntiSpam field data from enterprise customer installations having more than 1,000 total messages per day. This normalization yields a more accurate summary of Internet spam trends by ruling out problematic and laboratory test servers that produce smaller sample sets.

This section will provide more detail on specific methodologies used to produce the data and statistics in this report. While most methodologies are adequately explained in the analysis section of the report, the following investigations warrant additional detail.

### Phishing activity by sector

The Symantec Phish Report Network (PRN) is an extensive antifraud community whose members contribute and receive fraudulent website addresses for alerting and filtering across a broad range of solutions. These sites are categorized according to the brand being phished and its sector. PRN members and contributors send in phishing attacks from many different sources. This includes a client detection network that detects phishing websites as the clients visit various websites on the Internet. It also includes server detection from spam emails. The sender confirms all spoofed websites before sending the address of the website into the PRN. After it is received by the PRN, Symantec spoof detection technology is used to verify that the website is a spoof site. Research analysts manage the PRN console 24 hours a day, 365 days of the year, and manually review all spoof sites sent into the PRN to eliminate false positives.

### Top countries hosting phishing websites and top targeted sectors

The data for this section is determined by gathering links in phishing email messages and cross-referencing the addresses with several third-party subscription-based databases that link the geographic locations of systems to IP addresses. In this case, Symantec counts phishing websites as the number of unique IP addresses hosting Web pages used for phishing. While these databases are generally reliable, there is a small margin of error. The data produced is then used to determine the global distribution of phishing websites.

### Phishing site top-level domains

The data for this section is determined by deriving the top-level domains of each distinct phishing website URL. The resulting top-level domains are tabulated and compared proportionately.

### Automated phishing toolkits

The data in this section is derived from URLs gathered by the Symantec PRN. The URLs are sorted and grouped according to specific patterns indicating they were generated by an automated script or phishing kit. Each phishing kit generates URLs with a distinct signature and can be grouped according to these distinguishing characteristics. The monthly total of each group of URLs indicates the level of use of each automated phishing kit.

### Underground economy servers—goods and services available for sale

This metric is based on data that is gathered by proprietary Symantec technologies that observe activity on underground economy servers and collect data. Underground economy servers are typically chat servers on which stolen data, such as identities, credit card numbers, access to compromised computers, and email accounts are bought and sold. Each server is monitored by recording communications that take place on them, which typically includes advertisements for stolen data. This data is used to derive the data presented in this metric. It should be noted that this discussion might not necessarily be representative of Internet-wide activity; rather, it is intended as a snapshot of the activity that Symantec observed during this period.

Description of goods and services advertised on underground economy servers may vary from vendor to vendor. The following list shows typical goods and services that are found on these servers and general descriptions of each:

- **Bank account credentials:** may consist of name, bank account number (including transit and branch number), address, and phone number. Online banking logins and passwords are often sold as a separate item.
- **Cash out:** a withdrawal service where purchases are converted into true currency. This could be in the form of online currency accounts or through money transfer systems and typically, the requester is charged a percentage of the cashout value as a fee.
- **Credit card information:** includes credit card number and expiry date. It may also contain the cardholder name, Credit Verification Value 2 (CVV2) number, PIN, billing address, phone number, and company name (for a corporate card). CVV2 is a three or four-digit number on the credit card and used for card-not-present transactions such as Internet or phone purchases. This was created to add an extra layer of security for credit cards and to verify that the person completing the transaction was in fact, in possession of the card.
- **Email accounts:** includes user ID, email address, password. In addition, the account may contain personal information such as addresses, other account information, and email addresses in the contact list.
- **Email addresses:** consists of lists of email addresses used for spam or phishing activities. The email addresses can be harvested from hacking databases, public sites on the Internet, or from stolen email accounts. The sizes of lists sold can range from 1 MB to 150 MB.
- **Full identities:** may consist of name, address, date of birth, phone number, and government-issued number. It may also include extras such as driver’s license number, mother’s maiden name, email address, or “secret” questions/answers for password recovery.
- **Mailers:** an application that is used to send out mass emails (spam) for phishing attacks. Examples of this are worms and viruses.

- **Proxies:** Proxy services provide access to a software agent, often a firewall mechanism, which performs a function or operation on behalf of another application or system while hiding the details involved, allowing attackers to obscure their path and make tracing back to the source difficult or impossible. This can involve sending email from the proxy, or connecting to the proxy and then out to an underground IRC server to sell credit cards or other stolen goods.
- **Shell scripts:** used to perform operations such as file manipulation and program execution. They can also be used as a command line interface for various operating systems.

### Top countries of spam origin

The data for this section is determined by calculating the frequency of originating server IP addresses in email messages that trigger antispam filters in the field. The IP addresses are mapped to their host country of origin and the data is summarized by country based on monthly totals. The percentage of spam per country is calculated from the total spam detected in the field.

It should be noted that the location of the computer from which spam is detected being sent is not necessarily the location of the spammer. Spammers can build networks of compromised computers globally and thereby use computers that are geographically separate from their location.

### Percentage of spam from botnets

The data for this section is determined by analysis of emails triggering antispam filters, what proportion are detected as originating from a known botnet. The identity and location of spam-sending botnets are tracked by MessageLabs Intelligence knowledgebase, and is based on the profile of the spam and its headers as it is being transmitted. Each botnet exhibits a unique profile and the information is tracked accordingly, including its location.

NO WARRANTY. The technical information is being delivered to you as is and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained herein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.

## About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

For specific country offices and contact numbers, please visit our website. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
20330 Stevens Creek Blvd.
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com

04/09 20016963