SYMANTEC ENTERPRISE SECURITY

Confidence in a connected world.

Symantec Global Internet Security Threat Report

Trends for July–December 07

Volume XIII, Published April 2008

Dean Turner
Executive Editor
Director, Global Intelligence Network
Symantec Security Response

Marc Fossi
Manager, Development
Symantec Security Response

Eric Johnson
Editor
Symantec Security Response

Trevor Mack
Associate Editor
Symantec Security Response

Joseph Blackbird
Threat Analyst
Symantec Security Response

Stephen Entwisle
Threat Analyst
Symantec Security Response

Mo King Low
Threat Analyst
Symantec Security Response

David McKinney
Threat Analyst
Symantec Security Response

Candid Wueest
Analyst
Symantec Security Response

Volume XIII, Published April 2008

Symantec Global Internet Security Threat Report

Contents

Introduction

The Symantec *Global Internet Security Threat Report* provides a six-month update of worldwide Internet threat activity. It includes analysis of network-based attacks, a review of known vulnerabilities, and highlights of malicious code. It also assesses trends in phishing and spam activity. The report also provides protection and mitigation recommendations for these concerns. This volume covers the six-month period from July 1 to December 31, 2007.

Symantec has established some of the most comprehensive sources of Internet threat data in the world. The Symantec™ Global Intelligence Network encompasses worldwide security intelligence data gathered from a wide range of sources, including more than 40,000 sensors monitoring networks in over 180 countries through Symantec products and services such as Symantec DeepSight™ Threat Management System and Symantec Managed Security Services™, and from other third-party sources. Symantec gathers malicious code reports from over 120 million client, server, and gateway systems that have deployed its antivirus product, and also maintains one of the world's most comprehensive vulnerability databases, currently consisting of over 25,000 recorded vulnerabilities (spanning more than two decades) affecting more than 55,000 technologies from over 8,000 vendors. Symantec also operates 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 direct subscribers who contribute, receive, and discuss vulnerability research on a daily basis.

As well, the Symantec Probe Network, a system of over two million decoy accounts in more than 30 countries, attracts email from around the world to gauge global spam and phishing activity. Symantec also gathers phishing information through the Symantec Phish Report Network, an extensive antifraud community of enterprises and consumers whose members contribute and receive fraudulent Web site addresses for alerting and filtering across a broad range of solutions.

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 Symantec *Global Internet Security Threat Report* gives enterprises and consumers essential information to effectively secure their systems now and into the future.

Highlights

This section provides highlights of the security trends that Symantec observed during this period based on the data gathered from the sources listed above. Selected metrics will be discussed in greater depth in their respective sections following these highlights.

Attack Trends Highlights

- During this reporting period, the United States accounted for 31 percent of all malicious activity, an increase from 30 percent in the first half of 2007.
- The United States was the top country of attack origin in the second half of 2007, accounting for 24 percent of worldwide activity, a decrease from 25 percent in the first half of 2007.
- The education sector accounted for 24 percent of data breaches that could lead to identity theft during this period, more than any other sector. This was a decrease from the previous reporting period, when it accounted for 30 percent of the total.
- Government was the top sector for identities exposed, accounting for 60 percent of the total, a significant increase from 12 percent in the first half of 2007.
- Theft or loss of computer or other data-storage medium was the cause of the most data breaches that could lead to identity theft during this reporting period, accounting for 57 percent of the total. It accounted for 61 percent of the identities exposed in the second half of 2007, more than any other sector.
- The United States was the top country for hosting underground economy servers, accounting for 58 percent of the total identified by Symantec, a decrease from the first half of 2007, when it accounted for 64 percent of the total.
- Bank accounts were the most commonly advertised item for sale on underground economy servers known to Symantec, accounting for 22 percent of all items, an increase from the first half of 2007, when they made up 21 percent.
- Symantec observed an average of 61,940 active bot-infected computers per day in the second half of 2007, an increase of 17 percent from the previous period.
- The average lifespan of a bot-infected computer during the last six months of 2007 was four days, unchanged from the first half of 2007.
- The United States had the most bot-infected computers, accounting for 14 percent of the worldwide total, a slight increase from 13 percent in first half of 2007.
- Madrid was the city with the most bot-infected computers, accounting for three percent of the worldwide total.
- In the last six months of 2007, Symantec identified 4,091 bot command-and-control servers. This is an 11 percent decrease from the previous reporting period, when 4,622 bot command-and-control servers were identified. Of these, 45 percent were located in the United States, more than any other country.
- The United States was the country most frequently targeted by denial-of-service attacks, accounting for 56 percent of the worldwide total. This is a decrease from 61 percent reported in the first half of 2007.

Vulnerability Trends Highlights

- Not including site-specific vulnerabilities, Symantec documented 2,134 vulnerabilities in the second half of 2007, 13 percent less than the first half of 2007.
- Three percent of vulnerabilities documented in this period were classified as high severity, 61 percent as medium, and 36 percent as low. In the first half of 2007, nine percent of documented vulnerabilities were considered high severity, 51 percent medium, and 40 percent low.
- Fifty-eight percent of vulnerabilities documented in the second half of 2007 affected Web applications, down from 61 percent in the first half of 2007.
- Seventy-three percent of vulnerabilities documented in this period were classified as easily exploitable, compared to 72 percent in the first half of 2007.
- All operating system vendors except Apple® and Sun® had shorter average patch development times. Microsoft® had the shortest patch development time, at six days; Sun had the longest patch development time, at 157 days.
- Over half of patched medium- and high-severity operating system vulnerabilities for Microsoft, HP®, and Sun in the second half of 2007 were browser and client-side vulnerabilities. During the first half of 2007, browser and client-side vulnerabilities made up the majority of patched operating system vulnerabilities for all vendors but Apple.
- The window of exposure for enterprise vendors was 46 days in the last six months of 2007, compared to 55 days in the previous six months.
- Safari had the shortest window of exposure of any browser in the last six months of 2007, with an average exposure of less than one day from a sample set of 18 patched vulnerabilities. Safari also had the shortest window of exposure during the first six months of 2007, an average of three days from a sample set of 13 patched vulnerabilities.
- During the second half of 2007, there were 88 vulnerabilities reported in Mozilla browsers, 22 in Safari, 18 in Internet Explorer, and 12 in Opera. In the previous six month period, Internet Explorer was subject to 39 vulnerabilities, Mozilla to 34, Safari to 25, and Opera to seven.
- Symantec documented 239 browser plug-in vulnerabilities in the last six months of 2007, compared to 237 during the first six months. During the second half of 2007, 79 percent of these vulnerabilities affected ActiveX components, compared to 89 percent in the first half.
- In the second half of 2007, 58 percent of all vulnerabilities affected Web applications. This is less than the 61 percent in the first half of 2007.
- Symantec identified 11,253 site-specific cross-site scripting vulnerabilities in the last six months of 2007, compared to 6,961 in the first half (though with measurement beginning only in February).
- Symantec documented nine zero-day vulnerabilities in the second half of 2007, all of which affected third-party applications for the Windows platform. There were six zero-day vulnerabilities in the first half of 2007.

- Eighty-eight vulnerabilities that affected enterprise vendors in the second half of 2007 remain unpatched at the end of the reporting period. This is an increase over the 81 unpatched enterprise vulnerabilities in the first half of 2007. Microsoft had the most unpatched vulnerabilities in both reporting periods.
- Symantec documented 92 vulnerabilities that affected security products during the second half of 2007, down from 113 in the first half of the year. Of the 92 vulnerabilities, 15 were classified as high severity, 48 as medium, and 29 as low.

Malicious Code Trends Highlights

- In the second half of 2007, 499,811 new malicious code threats were reported to Symantec, a 136 percent increase over the first half of 2007.
- Of the top 10 new malicious code families detected in the last six months of 2007, five were Trojans, two were worms, two were worms with a back door component, and one was a worm with a virus component.
- During the second half of 2007, Trojans made up 71 percent of the volume of the top 50 malicious code samples, a decrease from 73 percent in the first six months of 2007.
- Forty-three percent of worms originated in the Europe, Middle East, and Africa (EMEA) region.
- North America accounted for 46 percent of Trojans for this period.
- Threats to confidential information made up 68 percent of the volume of the top 50 potential malicious code infections reported to Symantec.
- Of all confidential information threats detected this period, 76 percent had a keystroke logging component and 86 percent had remote access capabilities, a decrease for each from 88 percent in the previous period.
- Forty percent of malicious code that propagated did so through executable file sharing, a significant increase from 14 percent in the first half of 2007, making this the most commonly used propagation mechanism during this period.
- Seven percent of the volume of the top 50 malicious code samples modified Web pages this period, up from three percent in the previous period.
- During the second half of 2007, 10 percent of the 1,032 documented malicious code samples exploited vulnerabilities. This is lower than the 18 percent proportion of the 1,509 malicious code instances documented in the first half of 2007.
- Seven of the top 10 staged downloaders this period were Trojans, two were worms, and one was a worm with a viral infection component.
- Of the top 10 downloaded components for this period, eight were Trojans and two were back doors.
- Malicious code that targets online games made up eight percent of the volume of the top 50 potential malicious code infections, up from five percent in the previous period.

Phishing Trends Highlights

- The Symantec Probe Network detected a total of 207,547 unique phishing messages, a five percent increase over the first six months of 2007. This equates to an average of 1,134 unique phishing messages per day for the second half of 2007.
- Eighty percent of all unique brands used in phishing attacks were in the financial sector, compared to 79 percent in the previous period.
- During this period, 66 percent of all phishing Web sites spoofed financial services brands, down from 72 percent in the first half of 2007.
- In the second half of 2007, 66 percent of all phishing attacks detected by Symantec were associated with Web sites located in the United States. Two social networking sites together were the target of 91 percent of phishing attacks with Web sites hosted in the United States.
- The most common top-level domain used in phishing Web sites for this period was .com, accounting for 44 percent; the second most common top-level domain used by phishing Web sites was .cn, accounting for 23 percent.
- Symantec observed 87,963 phishing hosts worldwide this period, an increase of 167 percent from the 32,939 observed in the first half of the year.
- Sixty-three percent of all phishing hosts identified were in the United States, a much higher proportion than in any other country.
- Three phishing toolkits were responsible for 26 percent of all phishing attacks observed by Symantec in the second half of 2007.

Spam Trends Highlights

- Between July 1 and December 31, 2007, spam made up 71 percent of all email traffic monitored at the gateway, a 16 percent increase over the last six months of 2006, when 61 percent of email was classified as spam.
- Eighty percent of all spam detected during this period was composed in English, up from 60 percent in the previous reporting period.
- In the second half of 2007, 0.16 percent of all spam email contained malicious code, compared to 0.43 percent of spam that contained malicious code in the first half of 2007. This means that one out of every 617 spam messages blocked by Symantec Brightmail AntiSpam contained malicious code.
- Spam related to commercial products made up 27 percent of all spam during this period, the most of any category and an increase from 22 percent in the previous period.
- During the last six months of 2007, 42 percent of all spam detected worldwide originated in the United States, compared to 50 percent in the previous period.
- The United States hosted the most spam zombies of any country, with 10 percent of the worldwide total, representing no change from the first six months of 2007.
- In the second half of 2007, the daily average percentage of image spam was seven percent. This is down from a daily average of 27 percent during the first six months of 2007.

Attack Trends

This section of the Symantec *Global Internet Security Threat Report* will provide an analysis of attack activity, as well as other malicious activity, data breaches, and the trade of illicit information that Symantec observed between July 1 and December 31, 2007. The malicious activity discussed in this section includes not only attack activity, but also phishing, malicious code, spam zombie, and command-and-control 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 activity can be found in the sections following "Attack Trends."

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
- Data breaches that could lead to identity theft by sector
- Data breaches that could lead to identity theft by cause
- Underground economy servers
- Underground economy servers—goods and services available for sale
- Bot-infected computers
- Bot command-and-control servers
- Attacks—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, namely: bot-infected computers, bot command-and-control servers, phishing Web site hosts, malicious code reports, spam zombies, and Internet attacks. The rankings are determined by calculating the mean average of the proportion of these malicious activities that originated in each country.

Between July 1 and December 31, 2007, the United States was the top country for malicious activity, making up 31 percent of worldwide malicious activity (table 1). This represents a small change from the first half of 2007, when the United States was also first, with 30 percent. For each of the malicious activities in this metric, the United States ranked first by a large margin.

Current Rank	Previous Rank	Country	Current Percentage	Previous Percentage	Bot Rank	Command-and-Control Server Rank	Phishing Web Sites Host Rank	Malicious Code Rank	Spam Zombies Rank	Attack Origin Rank
1	1	United States	31%	30%	1	1	1	1	1	1
2	2	China	7%	10%	3	5	2	2	4	2
3	3	Germany	7%	7%	2	2	3	7	2	3
4	4	United Kingdom	4%	4%	9	6	7	3	12	5
5	7	Spain	4%	3%	4	19	15	9	9	4
6	5	France	4%	4%	8	13	6	11	7	6
7	6	Canada	3%	4%	13	3	5	4	35	7
8	8	Italy	3%	3%	5	10	11	10	6	8
9	12	Brazil	3%	2%	6	7	13	21	3	9
10	9	South Korea	2%	3%	15	4	9	14	13	10

Table 1. Malicious activity by country
Source: Symantec Corporation

Malicious activity usually affects computers that are connected to high-speed broadband Internet. Since broadband connections provide larger bandwidth capacities than other connection types, and the connections are frequently continuous, it is not surprising that the United States had the most malicious activity, since it has the most established broadband infrastructure in the world: 94 percent of U.S. households have access to available broadband connections, and its 65.5 million broadband subscribers represent 20 percent of the world's total, more than any other country.[1]

China had the second highest amount of worldwide malicious activity during the last six months of 2007, accounting for seven percent, a decrease from 10 percent in the previous reporting period. China ranked high in most of the contributing criteria, which is not surprising since China has the second highest number of broadband subscribers in the world, with 19 percent of the worldwide broadband total.[2]

The main reason for China's percentage decrease was the large drop in bot-infected computers there in the second half of 2007. China dropped to third for bot-infected computers in the second half of 2007, with eight percent, a large decrease from the first half of 2007, when it had 29 percent and ranked first. This decrease is attributable to a significant reduction in the availability of many Web sites, forums, and blogs in China for several months during this period.[3] Dynamic sites such as forums and blogs are prime targets for attackers using bots to propagate and host malicious content. Symantec believes that, because of their scalability, bots are responsible for much of the malicious attack activity that is observed, and any serious reduction in the number of bots should result in a corresponding drop in total attack activity. This is also supported by the decrease in China of spam zombies, which are often associated with bot-infected computers. China dropped from third in spam zombies in the first half of 2007, with nine percent of the worldwide total, to fourth and six percent in the second half of 2007.

[1] http://www.point-topic.com
[2] http://www.point-topic.com
[3] http://www.msnbc.msn.com/id/21268635/

Another possible reason for the change in malicious activity originating in China this period was that China ranked second for hosting phishing Web sites, accounting for four percent of the worldwide total. This was a large increase from the previous reporting period, when it ranked eighteenth with one percent of the total. One possible cause for the increase may be the recent rise in phishing scams and fraudulent Web sites attempting to exploit the popularity of the upcoming 2008 Beijing Olympics.[4] Such activities will likely continue in the lead-up to the August 8, 2008 Olympics start date.

Furthermore, the increase may have been influenced by the shutdown of the Russian Business Network (RBN) in November 2007 and its subsequent emergence in China, which may have a less well-established security infrastructure or security laws than Russia.[5] Russia dropped in rank for hosting phishing Web sites, from fifth in the previous period to eighth in this period. The RBN reputedly specializes in the distribution of malicious code, hosting malicious Web sites, and other malicious activity, including the development and sale of the MPack toolkit.[6] The RBN has been credited for creating approximately half of the phishing incidents that occurred worldwide last year, and hosts Web sites that are responsible for a large amount of the world's Internet crime.[7]

In the last six months of 2007, Germany again ranked third, with seven percent of all Internet-wide malicious activity, the same percentage as in the first half of 2007. As with the previous reporting period, Germany ranked high in spam zombies, command-and-control servers, hosting phishing Web sites, and bot-infected computers. Factors that influence its high rank include a well-established Internet infrastructure and a high number of broadband subscribers, as Germany ranks in the top five countries for broadband subscribers in the world, with six percent of the total.[8]

It is reasonable to expect that the United States, Germany, and China will continue to rank as the top three countries for the highest amount of malicious activity as they also added the greatest number of broadband subscribers over the course of 2007: the United States added 4.2 million broadband subscribers, China added 6.8 million, and Germany added 2.4 million.[9]

On a global scale, the distribution of malicious activity seems to be relatively static, with the countries listed in the top 20 remaining unchanged from the first half of 2007. This follows a trend first noted in Symantec *Internet Security Threat Report Volume XII* that a country that is established as a frequent source of malicious activity tends to remain so.[10] This is likely to remain the case until more effective measures—such as increased filtering for malicious activity, securely-coded applications, and more education for end users—are taken to reduce the amount of originating malicious activity.

[4] http://www.symantec.com/enterprise/security_response/weblog/2007/11/scam_related_to_the_2008_beiji.html and http://www.chinaeconomicreview.com/it/2007/10/10/man-convicted-of-fraud-for-phony-olympics-web-site/
[5] http://www.scmagazineus.com/ls-this-the-end-of-the-Russian-Business-Network/article/96289/ and http://www.pcworld.com/article/id,139465-page,1-c,privacysecurity/article.html
[6] http://www.symantec.com/enterprise/security_response/weblog/2007/05/mpack_packed_full_of_badness.html
[7] http://www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202461_pf.html
[8] http://www.point-topic.com
[9] http://www.point-topic.com
[10] http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_09_2007.en-us.pdf : p. 31.

Data breaches that could lead to identity theft

Identity theft continues to be a high-profile security issue, particularly for organizations that store and manage large amounts of personal information. Not only can compromises that result in the loss of personal data undermine customer and institutional confidence and result in costly damage to an organization's reputation, but data breaches can also be financially costly to organizations: the average cost per incident of a data breach in the United States was $6.3 million and lost business amounted to an average of $4.1 million.[11] Also, organizations can be held liable for breaches and losses, which may result in fines or litigation.[12]

By the end of 2007, 39 states in the United States had introduced breach notification legislation that regulates the responsibilities of organizations conducting business within the particular state after a data breach has occurred.[13] The state of California was the benchmark for such legislation, adopting data breach notification laws in 2003.[14] The laws require anyone who conducts business in the state to notify owners of the information exposed immediately after a security breach, with failure to do so resulting in possible civil action and fines. Other countries have also introduced legislation to tackle identity fraud, including Canada and New Zealand, both of whom issued guidelines for dealing with privacy breach notification in 2007.[15]

Other initiatives in the United States include the Federal Agency Data Breach Protection Act, which requires federal agencies to notify citizens whose information has been compromised by a data breach,[16] and the Gramm-Leach-Bliley Act (GLBA), enacted in 2002, which stipulates that financial institutions must ensure the security of clients' nonpublic personal information. The added consideration of punitive costs may influence organizations to develop more robust security strategies, which may help reduce the number of breaches overall.

Data breaches that could lead to identity theft by sector

Using publicly available data,[17] Symantec has determined the sectors that were most often affected by these breaches, as well as the most common causes of data loss. This metric will also explore the severity of the breach by measuring the total number of identities exposed to attackers through the data breach, using the same publicly available data. An identity is considered to be exposed if personal or financial data related to the identity is made available through the data breach.

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.[18] 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 the second half of 2007, the education sector represented the highest number of known data breaches that could lead to identity theft, accounting for 24 percent of the total (figure 1). This is a decrease from the previous reporting period when the education sector accounted for 30 percent of the total, when it also ranked first.

[11] http://www.vontu.com/uploadedfiles/global/Ponemon-Cost-of-a-Data-Breach-2007.pdf : The report defines per incident costs as including "process-related activities" such as investigations into the breach, breach notification to affected individuals, credit report monitoring for customers and/or the reissuing of a new account or credit card.
[12] http://www.fsa.gov.uk/pages/Library/Communication/PR/2007/021.shtml
[13] http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm
[14] http://www.news.com/Law-aims-to-reduce-identity-theft/2100-1017_3-1022341.html
[15] http://www.privcom.gc.ca/information/guide/2007/gl_070801_01_e.asp and http://www.privacy.org.nz/the-privacy-act-and-codes/
[16] http://www.govtrack.us/congress/bill.xpd?bill=h109-6163
[17] http://attrition.org/dataloss/
[18] For example, the Fair and Accurate Credit Transactions Act of 2003 (FACTA) of California. For more on this act, please see: http://www.privacyrights.org/fs/fs6a-facta.htm. Another example is the Health Insurance Portability and Accountability Act of 1996. For more information see: http://www.cms.hhs.gov/HIPAAGenInfo/

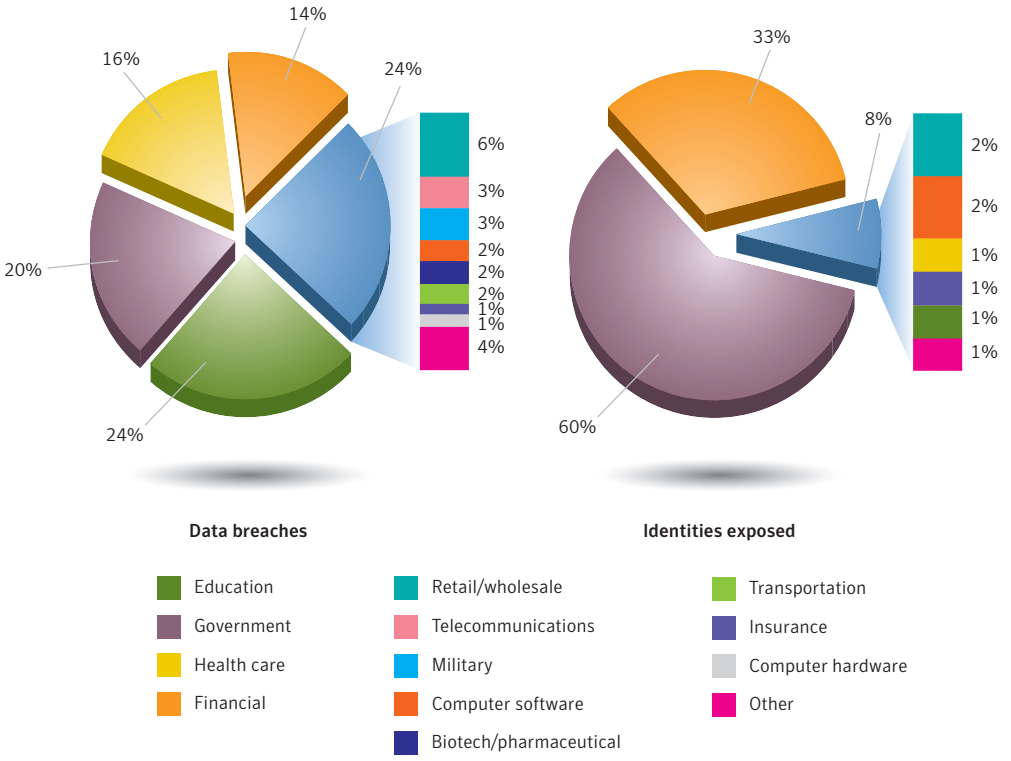

Figure 1. Data breaches that could lead to identity theft by sector and identities exposed
Source: Based on data provided by Attrition.org

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, addresses, and birthdates. These institutions—particularly larger universities—often consist of many semi-independent departments in 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 and access control of these dispersed databases.

Despite the high number of data breaches that occurred in the education sector during the last six months of 2007, it only accounted for one percent of all identities exposed during the period (figure 1). This is likely because 43 percent of the data breaches in the education sector this period were caused by the theft or loss of computers or data-storage devices. Unlike hacking,[19] in which data breaches can last for an extended period and expose numerous identities, breaches caused by theft or loss can only be opportunistically taken advantage of. 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.

[19] A data breach is considered to be caused by hacking if identity theft-related data was exposed by an attacker or attackers by gaining unauthorized access to computers or networks.

During this reporting period, 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 reporting period, when the government sector represented 26 percent of the total, though still ranking second.

Government organizations, like educational institutions, store large amounts of information that could be used for purposes of identity theft. Similar to the education sector, these organizations often consist of numerous semi-independent departments that store sensitive personal information in separate locations and are accessible to numerous people. As a consequence, government organizations face the same security and control issues as educational institutions.

The government sector had the highest overall number of identities exposed during the period, accounting for 60 percent of the total. There were a number of high profile data loss incidents during the period. One incident involved Her Majesty's Revenue and Customs (HMRC) in the United Kingdom, when two unencrypted disks containing personal records on 25 million people were lost during transfer from HMRC to the National Audit Office.[20] There were also other breaches reported in the UK, including the theft of a laptop containing military applicants' details.[21] Although the HMRC disks have not been recovered and there have been no subsequent incidents to suggest that the information involved is in the public domain, high profile breaches such as these underscore the vital importance of implementing the latest data loss prevention technologies and strategies.

The health care sector ranked third for this period, accounting for 16 percent of data breaches that could lead to identity theft. It also ranked third in the previous period, accounting for 15 percent. The prominence of the health care sector may be due to similar factors that influenced the prominence of both the education and government sectors, such as the storage of large amounts of sensitive personal information in many locations. Furthermore, health care organizations store sensitive medical information, which could result in potentially even more damaging breaches of privacy.

The health care sector ranked fifth for the number of identities exposed this period, accounting for just over one 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. Thus, breaches in this sector were less likely to result in wide-scale identity theft than in the other sectors since they exposed a small number of identity-theft related data, such as financial information or government-issued identity numbers.

The financial sector was ranked fourth in the number of data breaches that could lead to identity theft in the second half of 2007, accounting for 14 percent of the total. However, the sector accounted for 33 percent of the overall number of identities exposed, ranking second. The Fidelity National Information Services data breach, in which information on 8.5 million credit cards, bank accounts, and personal data was stolen by a former employee, contributed to the large percentage of identities exposed in this sector in the second half of 2007.[22]

[20] http://news.bbc.co.uk/1/hi/uk_politics/7103566.stm
[21] http://www.timesonline.co.uk/tol/news/politics/article3213274.ece
[22] http://jacksonville.bizjournals.com/jacksonville/stories/2007/11/26/daily23.html

The distribution of data breaches that could lead to identity theft by sector appears to be relatively constant, as the sectors listed in the top four have not varied from Symantec *Internet Security Threat Report XI*. Since these four sectors—education, government, heath care, and financial—are required to store large amounts of personal information on an ongoing basis, this trend seems likely to continue. Moreover, Symantec has observed that the top sector for the number of identities exposed correlates with large-scale breaches that occur in the reporting period. In other words, the large-scale breaches associated with those organizations are the main contributors for the disproportionate amount of identities exposed in their sector.

Data breaches that could lead to identity theft by cause

In the second half of 2007, 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.[23] Theft or loss made up 57 percent of all data breaches during the second half of 2007, and accounted for 46 percent of all reported breaches in the previous reporting period (figure 2).

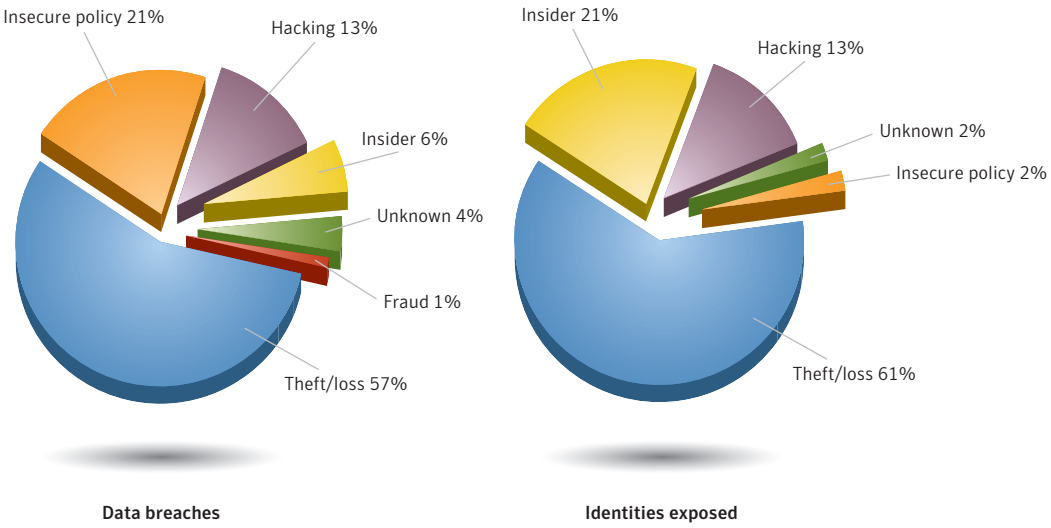

Figure 2. Data breaches that could lead to identity theft by cause and identities exposed
Source: Based on data provided by Attrition.org

Theft or loss accounted for 61 percent of all identities exposed in the second half of 2007, more than any other cause (figure 2). This was a large increase from first half of 2007, when the number of identities exposed from theft or loss accounted for 11 percent of the total. It is likely that theft is opportunistic and motivated by the hardware itself and not necessarily its contents, and as such, may not lead to wide-scale identity theft. Examples of data breaches due to theft or loss that contribute to these increased percentages include the HMRC loss in the United Kingdom, and the Resona Bank loss in Japan, in which 980,000 customers' names and account numbers went missing.[24]

[23] This cause will be referred to as theft or loss in the remainder of the report.
[24] http://www.darkreading.com/document.asp?doc_id=128692

Although laptops and other storage devices, such as USB memory keys, have become smaller and easier to use, their compact size and larger storage capability increases the opportunity for theft, loss or misplacement, as well as the potential amount of information breached. To protect against data theft or loss, organizations should restrict the use of outside personal storage devices within their network, and monitor the usage of such hardware when permitted.

The second most common cause of data breaches that could lead to identity theft during this period 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 the first half of 2007, insecure policy also ranked second, accounting for 34 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.

In the second half of 2007, insecure policy accounted for only two percent of exposed identities. Therefore, each breach exposed a relatively small number of identities and, thus, breaches caused by insecure policy in the second half of 2007 were not likely to result in wide-scale identity theft.

In the last six months of 2007, hacking was the third leading cause of data breaches that could lead to identity theft, accounting for 13 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. During the first six months of 2007, hacking also ranked third, accounting for 16 percent of breaches that could facilitate identity theft.

Hacking was responsible for 13 percent of identities exposed during the period, ranking third in the second half of 2007. The prominence of hacking in this reporting period was primarily due to the TD Ameritrade data breach, in which hackers using pump-and-dump spam compromised a database that contained contact information on 6.3 million customers of one of the largest discount brokers in the United States.[25] Hacking is more purpose-driven than insecure policy, theft, or loss; it is an intentional act with a defined purpose to steal data that can be used for purposes of identity theft or other fraud.

Most breaches that could lead to identity theft are avoidable. In the case of theft or loss and hacking, the compromise of data could be averted by strongly encrypting all sensitive data and educating users on the proper procedures for using such programs. Although it is likely that theft is motivated by a desire for the hardware itself and not the contents of it, encryption would ensure that even if the data is lost or stolen, it would not be accessible to unauthorized third parties. Also, network administrators should be closely monitoring network traffic and tracking all activity to ensure that access to data is controlled. Security processes and systems should be regularly tested to ensure their integrity. These steps should be part of a broader security policy that organizations should develop, implement, and enforce in order to ensure that all sensitive data is protected from unauthorized access.

[25] http://www.securityfocus.com/news/11488

Underground economy servers

Underground economy servers are black market forums used by criminals and criminal organizations to advertise and trade stolen information and services, typically for use in identity theft. This information can include government-issued identification numbers such as Social Security 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.

The geographic locations of underground economy servers are constantly changing due to the nature of these servers, which are often hosted as channels on public IRC servers. Once a fraud-related IRC channel becomes popular, it is often either shut down by the IRC server administrators or abandoned by its users due to legal liability and the increased possibility of being caught. As such, the location of an underground economy server is primarily driven by convenience and the lifespan of a server may be short. Furthermore, the geographic location of the server is typically not of any consequence to those involved because users of underground economy servers do most of their business electronically.

Criminals advertise their goods and services on IRC servers by listing available items and their prices. Potential buyers will privately contact the sellers to make the deal and finalize payment. Payment options for these goods are either conducted through online currency exchange services or exchange of goods. Unwilling to risk exposure, many purchasers will use the services of cashiers who will convert the information for a fee into true currency, either in the form of online currency accounts or through money transfers. In exchange for the service, cashiers will take a percentage of the cash-out amount.[26] Members of underground economy servers are usually self-policing, reporting rippers[27] to the administrators of the IRC servers, and also broadcasting this information to warn each other. Often, repeat rippers will be kicked off and banned from the servers.

Underground economy servers—goods and services available for sale

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.

During the second half of 2007, bank account credentials, including account numbers and authentication information, were the most frequently advertised item observed on underground economy servers, making up 22 percent of all goods (table 2). This was a slight increase from 21 percent in the first half of 2007. The advertised price for bank account credentials varied as widely as it did in the first six months of 2007, with prices ranging from $10 to $1,000 USD, depending on the amount of funds available and the location of the account. Bank accounts that included higher balances, such as business accounts, and EU accounts, were advertised for considerably more. Furthermore, bank accounts that bundled in personal information such as names, addresses and dates of birth were advertised at higher prices.

[26] Cash-out is a term used on underground economy servers where purchases are converted into true currency. This could be in the form of online currency accounts or through money transfer systems.
[27] Rippers are vendors on underground economy servers that conduct fraudulent transactions.

Current Rank	Previous Rank	Goods and Services	Current Percentage	Previous Percentage	Range of Prices
1	2	Bank accounts	22%	21%	$10–$1000
2	1	Credit cards	13%	22%	$0.40–$20
3	7	Full identities	9%	6%	$1–$15
4	N/A	Online auction site accounts	7%	N/A	$1–$8
5	8	Scams	7%	6%	$2.50/week–$50/week for hosting, $25 for design
6	4	Mailers	6%	8%	$1–$10
7	5	Email addresses	5%	6%	$0.83/MB–$10/MB
8	3	Email passwords	5%	8%	$4–$30
9	N/A	Drop (request or offer)	5%	N/A	10%–50% of total drop amount
10	6	Proxies	5%	6%	$1.50–$30

Table 2. Breakdown of goods and services available for sale on underground economy servers[28]
Source: Symantec Corporation

The small increase in the proportion of bank account credentials advertised may be due to a number of reasons. It is easier to withdraw funds from bank accounts compared to other financial means, such as credit cards, since fraud detection is not as effective. One of the main goals of most criminals who conduct business on underground economy servers is to easily cash out their purchases. Criminals can quickly cash out bank accounts to secure, untraceable drops using wire transfers or services offered by cashiers, sometimes in less than 15 minutes. Also, many wire transfer companies and currency exchange services no longer accept credit cards as forms of payment for all countries.[29]

Another possible reason for the continued prominence and increased availability of bank account credentials advertised is that Symantec observed an 86 percent increase in potential banking Trojan infections in the second half of 2007, which could result in more bank account credentials being stolen and then advertised on underground economy servers.

Credit cards were the second most commonly advertised item on underground economy servers during this reporting period, accounting for 13 percent of all advertised goods. This was a decrease from 22 percent in the first six months of 2007. The decrease in credit cards being advertised may be due to several reasons. With the recent high-profile reports on lost credit card data, such as the TJX loss, consumers and credit card companies may be more diligent in monitoring customers' credit card activities and quicker to inform customers of suspicious transactions, and subsequently, reducing the window of opportunity for criminals to exploit stolen credit cards. Also, as stated above, it is more difficult to cash out credit cards as many wire transfer companies and currency exchange services do not accept them as a form of payment.

Furthermore, consumers, fearing identity theft and payment fraud, have been moving away from paying for online purchases with credit cards and towards Internet-based payment services, such as PayPal 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 often offer full protection from unauthorized payments. They accounted for over 30 percent of the U.S. online payment market, a volume increase of 34 percent from 2006.[30]

[28] Descriptions and definitions for the goods and services discussed in this section can be found in "Appendix B—Attack Trends Methodology."
[29] http://www.asianagold.com/faq.html
[30] http://www.businessweek.com/technology/content/nov2007/tc20071120_575440.htm?campaign_id=rss_tech

The price range of credit cards in the second half of 2007 remained consistent with the prices from the first half of the year, ranging from $0.40 to $20 USD per card number. Two of the main factors affecting the cost of credit cards on underground economy servers were the location of the issuing bank and the rarity of the card. Cards from the European Union cost more than those from the United States. One reason for the higher prices may be due to the availability of credit cards, since there was eight times the number of credit cards in circulation in the United States than in the European Union.[31] Rarer cards, such as those from smaller countries or smaller credit card companies, were typically twice as expensive as their more popular counterparts.

Credit cards issued by banks in the United States constituted 62 percent of the total credit cards advertised in the second half of 2007, a drop from 85 percent in the first half of 2007. It may be possible that demand for credit cards from banks in the United States may have fallen due to a decrease in popularity and hence, their selling price on underground economy servers is lower.

Criminals who sell credit cards on underground economy servers will advertise bulk rates and give samples to attract buyers. Once the buyer is satisfied that the card is still active, an exchange can be made. Some bulk amounts and rates observed by Symantec during the last six months of 2007 were 50 credit card numbers for $40 USD ($0.80 each), and 500 credit card numbers for $200 USD ($0.40 each). This is a decrease from the bulk rates advertised in the first half of 2007, when the lowest bulk purchase price identified was $1 USD each for 100 cards. It is possible that, as credit cards lose their popularity on underground economy servers, vendors will lower their prices to try to sell them off.

Full identities were the third most common item advertised for sale on underground economy servers, making up nine percent of all advertised goods, an increase from six percent in the first half of 2007. The popularity of full identities may be due to their versatility and ease of use. With a full identity, a criminal can easily obtain government issued documents, commit credit card fraud, open bank accounts, obtain credit, purchase and/or steal homes,[32] or even evade arrest by masquerading as someone else. In one case, the CEO of an identity theft prevention company was a victim of identity theft when someone used his social security number, which was prominently displayed on the company's Web site, to obtain a $500 loan.[33]

Symantec observed that the cost of full identities depended on the location of the identity. As with bank accounts and credit cards, EU identities were advertised at prices half again higher than U.S. identities. The higher prices may be indicative of increased demand and lower supplies of identities from the European Union. The popularity of EU identities may be due to the flexibility of their use, since citizens there are able to travel and conduct business freely throughout the union without a passport.[34] This flexibility may allow criminals to use the identities easily across all EU countries.

The distribution of goods and services advertised on underground economy servers continues to be focused on financial information, such as bank account credentials and credit card information. This is not surprising, as one of the main objectives for criminal activities in underground economy servers is to generate money. 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.

[31] http://www.ecb.int/stats/payments/paym/html/index.en.html and http://www.bis.org/publ/cpss78p2.pdf
[32] http://www.citynews.ca/news/news_3092.aspx
[33] http://blog.wired.com/27bstroke6/2007/06/lifelock_founde_1.html
[34] http://ec.europa.eu/justice_home/fsj/freetravel/frontiers/fsj_freetravel_schengen_en.htm

To help prevent fraud, credit card companies and banks could take more secure measures to verify and authenticate users. The Federal Financial Institutions Examination Council (FFIEC) requires banks in the United States to upgrade to a multi-factor authentication (MFA) security system for online banking.[35] The FFIEC also projected that 67 percent of Canadian banks will have a MFA solution in place by the end of 2007, even though banks there are not bound by any requirement to upgrade.[36] 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,[37] or an embedded security token in a credit card that generates one-time pass codes,[38] can make it more difficult for criminals to obtain and use financial information.

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 emails as these may be links to spoofed Web sites. Instead, they should manually type in the URL of the Web site. 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.

Bot-infected computers

Bots are programs that are covertly installed on a user's machine to allow an unauthorized user to remotely control the targeted system through a communication channel, such as IRC, peer-to-peer (P2P), or HTTP. These channels allow the remote attacker to control a large number of compromised computers 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 DoS attacks against an organization's Web site, distributing spam and phishing attacks, distributing spyware and adware, propagating malicious code, and harvesting confidential information that may be used in identity theft; all of which can have serious financial and legal consequences.

Symantec identifies bot-infected computers based on coordinated scanning and attack behavior that is observed in network traffic. The bot-infected computers identified have attempted to exploit vulnerabilities in network services to propagate and may include bot-infected computers that are part of networks controlled by various communication channels such as IRC, P2P, or HTTP. This behavioral matching will not catch every bot-infected computer, specifically bot-infected computers that have used non-traditional propagation methods, and may identify other malicious code or individual attackers behaving in a coordinated way like a botnet. However, this behavioral matching will identify many of the most coordinated and aggressive bot-infected computers.

[35] Multi-factor authentication depends on two or more of the following factors for a user: something they have (bank card, RSA token, smart card), something they know (password, PIN), and something they are (retinal scan, fingerprint). For example, online banking is a single-factor authentication while banking at an ATM is multi-factor.
[36] http://www.ffiec.gov/press/pr081506.htm
[37] 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. See http://www.emvco.com/about.asp for more information.
[38] http://www.incard.com/products.html

Between July 1 and December 31, 2007, Symantec observed an average of 61,940 active bot-infected computers per day (figure 3), a 17 percent increase from the previous reporting period. An active bot-infected computer is one that carries out an average of 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. Symantec also observed 5,060,187 distinct bot-infected computers during this period, a one percent increase from the first six months of 2007. A distinct bot-infected computer is a distinct computer that was active at least once during the period.

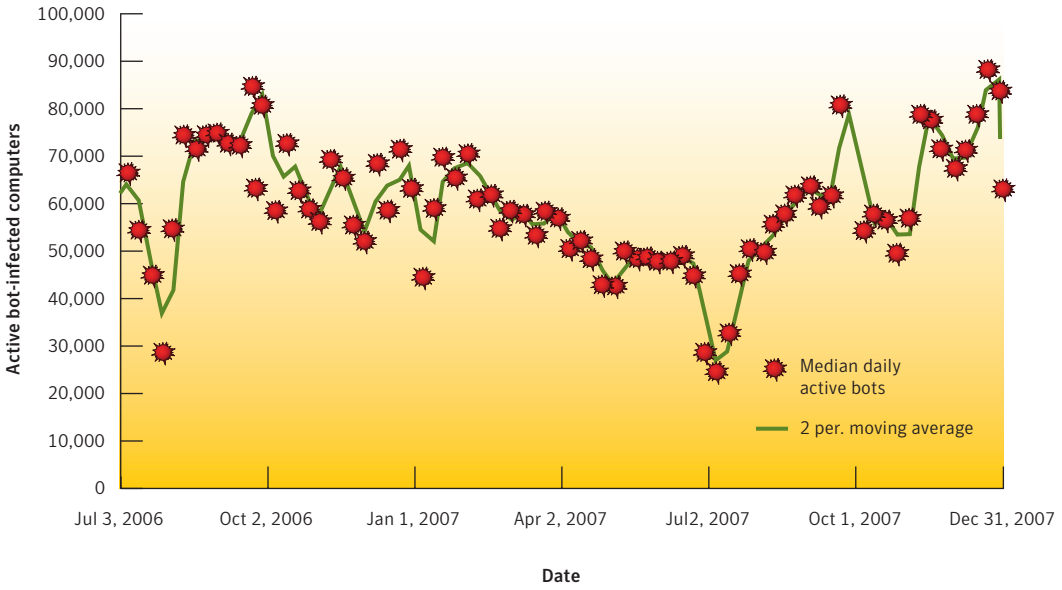

Figure 3. Active bot-infected computers by day
Source: Symantec Corporation

The increase in both active and distinct bot-infected computers observed in the second half of 2007 may be due to their popularity among attackers, and because platforms such as P2P and HTTP increase their effectiveness. Attackers may favor bot-infected computers because they are able to perform a wide range of functions, are effective in the attacks they mount, and are relatively easy and inexpensive to propagate. They are also difficult to disable with a decentralized command-and-control model, and most importantly, can be used for substantial financial gain. Illegal botnet activity can be highly lucrative and this may be one of the reasons they continue to be so popular. It is reasonable to speculate that most botnet owners profit from their activities; in one case, an owner admitted to earning $19,000 USD for illegally installing adware through bots he controlled.[39]

[39] http://www.securityfocus.com/news/11495

Bot command-and-control servers

Bot command-and-control servers are computers that botnet owners use to relay commands to bot-infected computers on their networks, usually through IRC channels. In the last six months of 2007, Symantec identified 4,091 bot command-and-control servers (figure 4). This is an 11 percent decrease from the previous reporting period, when 4,622 bot command-and-control servers were identified.

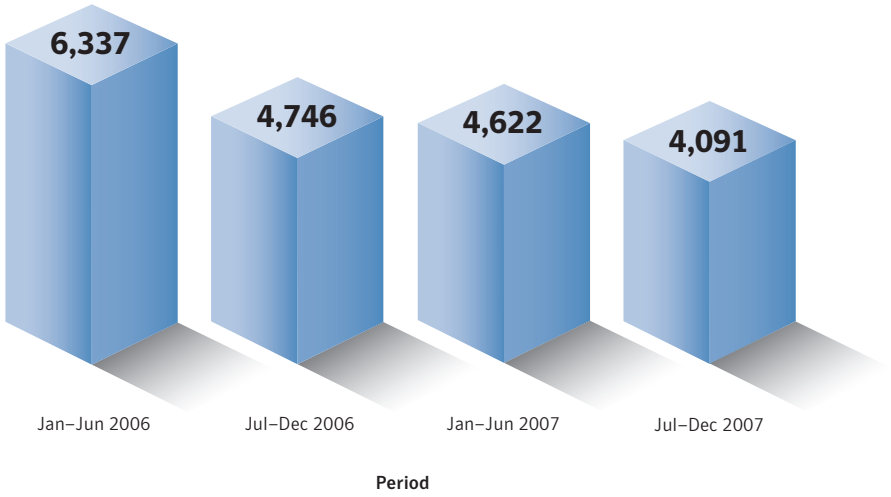

Figure 4. Bot command-and-control servers
Source: Symantec Corporation

The decrease in the number of bot command-and-control servers detected reflects the growing trend in the methods botnet owners are using to communicate with their bot-infected computers. There is a large shift away from traditional IRC bot command-and-control communication frameworks for botnet owners.[40] They are adopting new platforms and communication channels that have a decentralized command-and-control architecture, thus providing better security for their botnets and making them more difficult to detect and disable. Examples of these are P2P networks such as the botnets associated with the Peacomm and Nugache Trojans.[41] P2P botnet owners typically use a fast-flux domain name service scheme,[42] where control of the botnet is diffused through a number of computers within the network. Because the botnet does not have a centralized command-and-control server, P2P botnets can be broken up into smaller pieces for more stealthy operations, making them difficult to detect and disable.

Law enforcement initiatives targeting botnets and bot command-and-control servers also may have contributed to the decrease in the number of command-and-control servers in the second half of 2007. In Operation Bot Roast II, the second phase of an ongoing investigation into the criminal use of botnets in the United States, the Federal Bureau of Investigation (FBI) arrested suspected botnet owners from across the United States who were linked to multi-million dollar phishing and spamming scams, and stealing personal information that could lead to identity theft.[43] Since the investigation began in June 2007, eight people have been indicted for crimes related to botnet activity, over one million victim computers have been uncovered, and over $20 million in economic losses have been reported.[44]

[40] http://www.darkreading.com/document.asp?doc_id=117924
[41] http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1286808,00.html
[42] http://news.zdnet.com/2100-1009_22-6222896.html ; Fast-flux basically allows a single URL to resolve to a number of different IP address, or computers, by changing the URL's DNS mapping rapidly and constantly.
[43] http://www.fbi.gov/pressrel/pressrel07/botroast112907.htm
[44] http://www.fbi.gov/pressrel/pressrel07/botroast112907.htm

Initiatives such as these will likely result in a reduction in bot-infected computers and bot command-and-control servers. As botnet owners become aware of the scrutiny of law enforcement agencies, they are likely to alter their tactics to avoid detection, such as breaking the botnet into smaller sizes in attacks or using a decentralized command-and-control structure. Also, as botnets are disabled by the authorities, less bot activity and bot command-and-control servers will be observed.

Attacks—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.[45] 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.

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 secure policy requiring that all sensitive data is encrypted. Also, organizations should enforce compliance to information storage and transmission standards such as the PCI standard. 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.

[45] 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.

Vulnerability Trends

Vulnerabilities are design or implementation errors in information systems that can result in a compromise of the confidentiality, integrity, or availability of information stored upon or transmitted over the affected system. They are most often found in software, although they exist in all layers of information systems, from design or protocol specifications to physical hardware implementations. Vulnerabilities may be triggered actively, either by malicious users or automated malicious code, or passively during system operation. The discovery and disclosure of a single vulnerability in a critical asset can seriously undermine the security posture of an organization.

This section of the Symantec *Global Internet Security Threat Report* will provide a thorough analysis and discussion of vulnerabilities that have been disclosed between July 1 and December 31, 2007. It will compare these with those disclosed previously and discuss how current vulnerability trends may affect potential future Internet security activity. The following metrics will be discussed:

- Patch development time for operating systems
- Patch development time for operating systems by type of vulnerability
- Window of exposure for Web browsers
- Web browser vulnerabilities
- Browser plug-in vulnerabilities
- Web application vulnerabilities
- Site-specific cross-site scripting vulnerabilities
- Zero-day vulnerabilities
- Unpatched enterprise vendor vulnerabilities
- Vulnerabilities in security products
- Vulnerabilities—protection and mitigation

Patch development time for operating systems

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. If exploit code is created and made available during this time, computers may be immediately vulnerable to widespread attack. This metric will assess and compare the average patch development times for five different operating systems: Apple Mac OS X, Hewlett-Packard HP-UX, Microsoft Windows, Red Hat® Linux (including enterprise versions and Red Hat Fedora), and Sun Microsystems Solaris. Since third-party applications are often a factor in the average patch development time, the number of third-party applications in the data set for each vendor is also discussed.[46]

Of the five operating systems assessed in the last six months of 2007, Microsoft Windows had the shortest average patch development time of six days based on a sample set of 22 patched vulnerabilities (figure 5).[47] None of the vulnerabilities affected third-party applications.[48] This is shorter than the average patch development time of 18 days in the first six months of 2007, based on a sample set of 38 vulnerabilities, including two vulnerabilities that affected third-party applications.

[46] Many operating system vendors ship and maintain third-party applications such as Web browsers, servers, office suites, etc. with their operating systems. These are applications that are developed by a third-party vendor but because they are distributed with the operating system, patches for these applications are usually distributed to users by the operating system vendor.
[47] The term "sample set" is used throughout the report and is meant to refer to all data that matches the criteria laid out in the methodology and not a random sampling of data.
[48] Microsoft differs from other vendors because Windows does not ship with many third-party applications. As a result, Microsoft does not generally release patches for third-party applications.

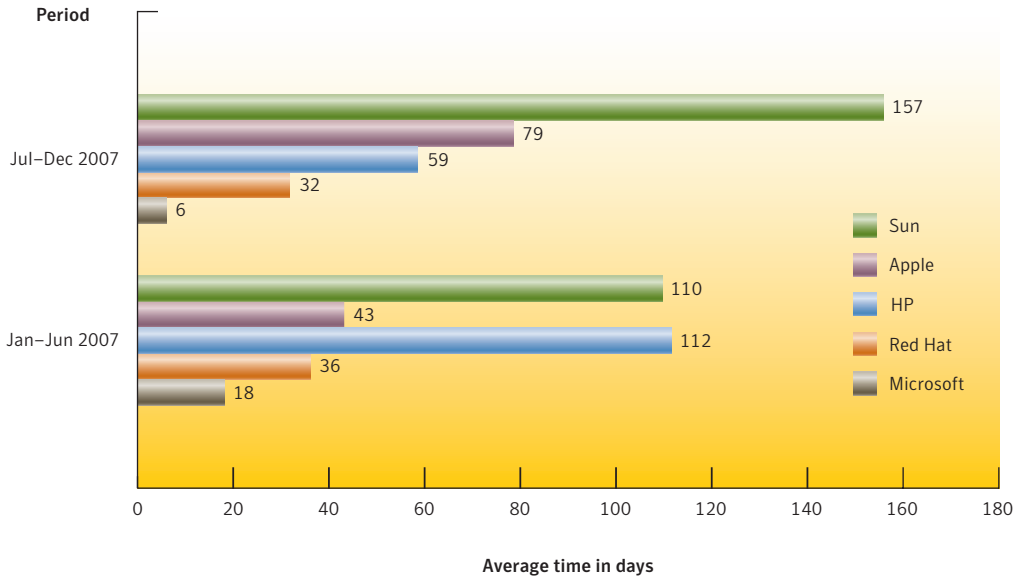

Figure 5. Patch development time for operating systems
Source: Symantec Corporation

Red Hat had the second shortest average patch development time during this reporting period, with an average of 32 days for a sample set of 136 vulnerabilities. All of these vulnerabilities affected third-party applications. This figure is less than the average of 36 days in the first half of 2007, which was derived from a sample set of 91 vulnerabilities. Ninety of these vulnerabilities affected third-party applications.

HP had the third shortest average patch development time in the second half of 2007, at 59 days for a sample set of 21 vulnerabilities, 20 of which affected third-party applications. This is an improvement over the first half of 2007, in which it had an average patch development time of 112 days for a sample set of 30 vulnerabilities, 28 of which affected third-party applications.

Apple had the fourth shortest average patch development time during this reporting period. Its average was 79 days for 86 vulnerabilities, including 47 third-party vulnerabilities. This period is longer than the 43-day average recorded in the first six months of 2007, during which the average was calculated from a sample set of 59 vulnerabilities, nine of which affected third-party applications.

Sun had the longest average patch development time in the second half of 2007, at 157 days for a sample set of 27 vulnerabilities, 23 of which affected third-party applications. This is longer than the 110-day average in the first half of 2007, which was calculated from 73 vulnerabilities and of which 67 affected third-party applications.

Apple and Sun were the vendors most challenged by the task of maintaining a large body of third-party applications that ship with their operating systems. This is in contrast to Red Hat, which has demonstrated consistently lower average patch development times than these vendors despite having a larger number of third-party vulnerabilities to patch.

HP showed an improvement over the previous period, due to faster patch times with specific applications, such as Mozilla browsers. This may indicate that HP has made browser vulnerabilities a priority. Third-party software exposes operating systems to attack, and vendors that distribute third-party software in their operating systems are uniquely challenged because the effectiveness of their patch deployment regimen relies on external factors such as the availability of a patch from the third-party vendor. Organizations often depend upon the updates provided by their operating system vendors, as opposed to seeking out patches from upstream vendors. Therefore, operating system vendors should put a high priority on patching the third-party applications that ship with their products.

Microsoft fares well in this comparison because it does not generally maintain many third-party applications. However, because of variables such as market share among desktop users and enterprises, in addition to security enhancements in Microsoft's later operating system releases, many of the third-party applications that are attacked in the wild are running on Microsoft Windows, as discussed later in the "Browser plug-in vulnerabilities" section. This is due to the fact that security enhancements in Microsoft Windows provide less protection for third-party applications than they do for Microsoft applications.[49]

Enterprises must thus depend more on after-market security products to mitigate vulnerabilities in third-party applications. Conversely, other operating systems have developed security measures that are intended to prevent attacks against the operating system and its third-party applications. It is reasonable to speculate that this trend will continue until there is a change in the variables that make third-party applications on Microsoft Windows an attractive target, such as market-share and the lack of default protection for third-party applications.

Patch development time for operating systems by type of vulnerability

Assessing the patch development time for operating systems provides insight into the types of applications and vulnerabilities that are present in the operating systems that are examined in the previous metric. The sample sets are limited to vulnerabilities that are considered medium or high severity and are divided into the following categories:

- **Web browser:** Vulnerabilities affecting Web browsers that ship with the operating systems discussed.
- **Client-side:** Vulnerabilities that affect network client software and software that accepts content from network clients. These vulnerabilities do not directly affect Web browsers; however, in many cases the Web browser is a means of exploiting these issues.
- **Local:** Vulnerabilities that affect applications that can only be exploited by a user who is logged in locally to the operating system.
- **Server:** Vulnerabilities that affect network server software.

Some vulnerabilities did not fit into these categories because they lack common characteristics or do not fit discretely into the categories described above. These uncategorized cases are noted in the discussion.

[49] ASLR on Windows Vista does not protect third-party applications by default. Third-party applications must be recompiled with the appropriate security flags to receive the benefits of this security measure.

Of the 86 patched vulnerabilities that affected Apple Mac OS X in the second half of 2007, eight affected browsers, 31 were client-side vulnerabilities, 15 were local, 15 affected servers, and 17 did not fall into any of these categories (figure 6). In the first half of 2007, Apple patched eight browser vulnerabilities, 21 on the client-side, 17 that were local, 11 server vulnerabilities, and two that could not be categorized according to the criteria described above.

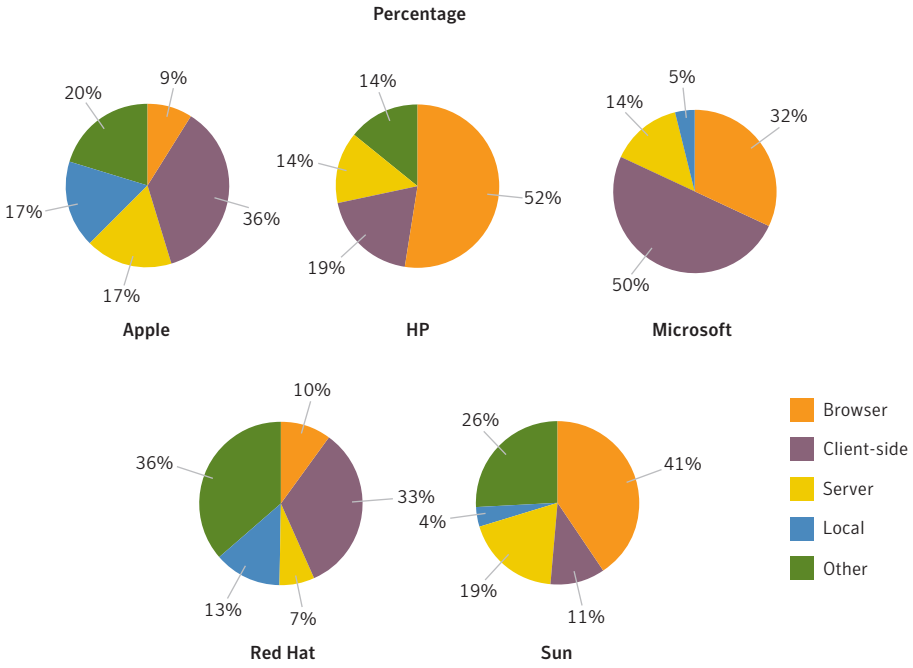

Figure 6. Operating system time to patch by type of vulnerability
Source: Symantec Corporation

From the sample set of 21 vulnerabilities for HP in the last six months of 2007, 11 affected browsers, four were client-side vulnerabilities, three affected servers, and three did not fit into any category. This is compared to 30 patched vulnerabilities in the first six months of 2007, which were made up of 13 browser vulnerabilities, three client-side, three local, nine affecting servers, and two that could not be categorized.

In the second half of 2007, 22 patched vulnerabilities in Microsoft Windows were categorized. Seven of these affected browsers, 11 were client-side vulnerabilities, one was local, and three affected servers. In the first half of 2007, Microsoft Windows had 38 patched vulnerabilities, of which 15 affected browsers, 13 were client-side, eight were local, and two affected servers.

Red Hat had 136 patched vulnerabilities during the last six months of 2007, 14 of which were browser vulnerabilities, 45 that were client-side, 18 that were local, 10 that affected servers, and 49 that did not fit into these categories. Of 91 patched vulnerabilities during the first half of 2007, 18 affected browsers, 31 were client-side, 10 were local, 13 affected servers, and 19 did not fall into any category.

Of the 27 patched vulnerabilities in Sun Solaris during the second half of 2007, 11 affected browsers, three were client-side, one was local, five affected servers, and seven could not be categorized. The 73 patched vulnerabilities in the first half of 2007 consisted of 41 browser vulnerabilities, of which nine were client-side, 11 were local, nine affected servers, and three did not fall into the above categories.

Browser and client-side vulnerabilities continue to make up a large portion of the patched operating system vulnerabilities. For vendors such as Microsoft, as much as 82 percent of patched medium- to high-severity vulnerabilities affected browsers or were client-side issues. The types of applications affected by these vulnerabilities are often less secure than traditionally more exposed server applications.

In many cases client-side vulnerabilities are caused by errors in parsing irregular or malformed files and other content. Applications that support complex file and data formats are particularly prone to this type of vulnerability, making them an ideal target for fuzzers. As a result, attackers and security researchers have concentrated their efforts on these applications. Likewise, vendors are struggling to secure these applications and make them more robust when handling irregular input.

Many browser and client-side vulnerabilities affect software that is installed by default or required for business operations. Desktop users within the enterprise are exposed to attack as they perform normal business operations such as sharing documents and files, browsing the Web, and reading email. As detailed in the discussion of browser plug-in vulnerabilities and site-specific cross-site specific vulnerabilities, Symantec has found that legitimate Web sites are being compromised to serve malicious content to users; enterprise users are even more threatened since trusted Web sites may be the source of attacks.

Window of exposure for Web browsers

The window of exposure 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.

This metric will assess the window of exposure for vulnerabilities in selected Web browsers. For this version of the Symantec *Global Internet Security Threat Report*, Symantec will be supplementing the discussion of the Web browser window of exposure with the maximum amount of time that elapsed between the disclosure of a single vulnerability and the release of an associated patch. Maximum patch times indicate the longest period of time required for a patch to be released to the public.

During the second half of 2007, Safari had a window of exposure of less than one day,[50] a decrease from the three-day window in the first half of 2007 (figure 7). The sample set for Safari in the second half of 2007 was 18 vulnerabilities, compared to 13 vulnerabilities in the first half of 2007. The maximum patch time for Safari was eight days in the last six months of 2007, and eight days in the first six months as well.

In the last six months of 2007, Opera had a window of exposure of two days based on a sample set of nine patched vulnerabilities. This is a decrease from the window of exposure of four days in the first half of 2007, which was based on a sample set of five patched vulnerabilities. In the current reporting period, Opera had a maximum patch development time of 21 days. The maximum in the previous reporting period was 23 days.

[50] The actual average was 0.4 days, which rounds down to 0.

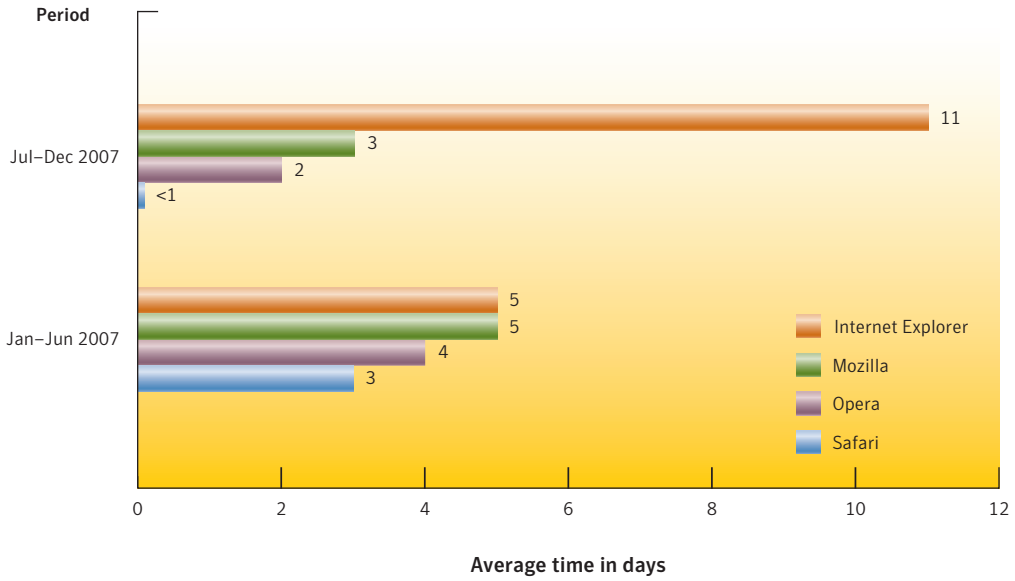

Figure 7. Window of exposure for Web browsers
Source: Symantec Corporation

During the last six months of 2007, Mozilla had a window of exposure of three days based on a sample set of 82 patched vulnerabilities. This is a decrease from the window of exposure of five days in the first half of 2007, which was based on 22 patched vulnerabilities. During the current reporting period, Mozilla had a maximum patch development time of 109 days. In the first half of the year, the maximum patch development time was 83 days.

In the second half of 2007, Microsoft Internet Explorer had a window of exposure of 11 days based on a sample set of 11 patched vulnerabilities. This is an increase from the five-day time period in the first half of 2007, which was based on a sample set of 17 patched vulnerabilities. The maximum patch development time for Internet Explorer vulnerabilities during the current reporting period was 87 days. In the first half of 2007, the maximum patch development time was 90 days.

During the second half of 2007, Microsoft Internet Explorer experienced an increased window of exposure because of a delayed response to a handful of vulnerabilities that were independently announced by security researchers. All other vendors were subject to shorter windows of exposure during the same period.

The exploit development time for all vendors in both reporting periods was zero days. This indicates that exploits were released within a day of vulnerability publication and often in tandem with a vulnerability announcement. This shows a tendency on the part of security researchers to release exploits as they announce vulnerabilities, but may also indicate that exploit development for browsers has been refined to the point where exploits can be developed with little delay. This practice puts pressure on the vendor to address the vulnerability in a shorter time frame because the availability of exploit code puts users at risk.

The window of exposure of browsers remains quite short in comparison to the amount of time that operating systems are typically exposed. This may be because operating systems require more resources to maintain due to their complexity and the number of applications that are included. It is also likely that browser vendors acknowledge the serious risk posed to desktop users by vulnerabilities in browser software. However, the prevalence of browser plug-in vulnerabilities, discussed below, is an indicator that browsers are still a major target of malicious activity.

Web browser vulnerabilities

The Web browser is a critical and ubiquitous application that has become an increasingly popular subject for vulnerability researchers over the past few years. Traditionally, the focus of security researchers has been on the perimeter—servers firewalls, and other assets with external exposure. However, client-side vulnerabilities are now becoming a focus for research and attacks, alike. As part of this shift toward client-side issues, vulnerabilities in Web browsers have become increasingly prominent, which in turn poses a threat to end-users.

Web browser vulnerabilities are a serious security concern due to their role in online fraud and the propagation of spyware and adware. They are particularly prone to security concerns because they come in contact with more potentially untrusted or hostile content than most other applications. This is a concern because attacks can originate from malicious Web sites or legitimate Web sites that have been compromised to serve malicious content. It is also true that browsers can play a role in client-side attacks because of their ability to invoke plug-ins and other applications when handling potentially malicious content served from the Web such as documents and media files.

During the second half of 2007, 88 vulnerabilities affected Mozilla browsers (figure 8). Of these, 19 were considered to be medium severity and 69 were considered low. This total is an increase from the 34 vulnerabilities that affected Mozilla browsers in the first half of 2007. Of those, 12 were considered medium severity and 22 were low.

Safari was affected by 22 vulnerabilities in the second half of 2007. One was considered high severity, 12 were medium, and nine were low. This is a decrease from the 25 Safari vulnerabilities that were documented in the first half of 2007, of which seven were medium severity and 18 were low.

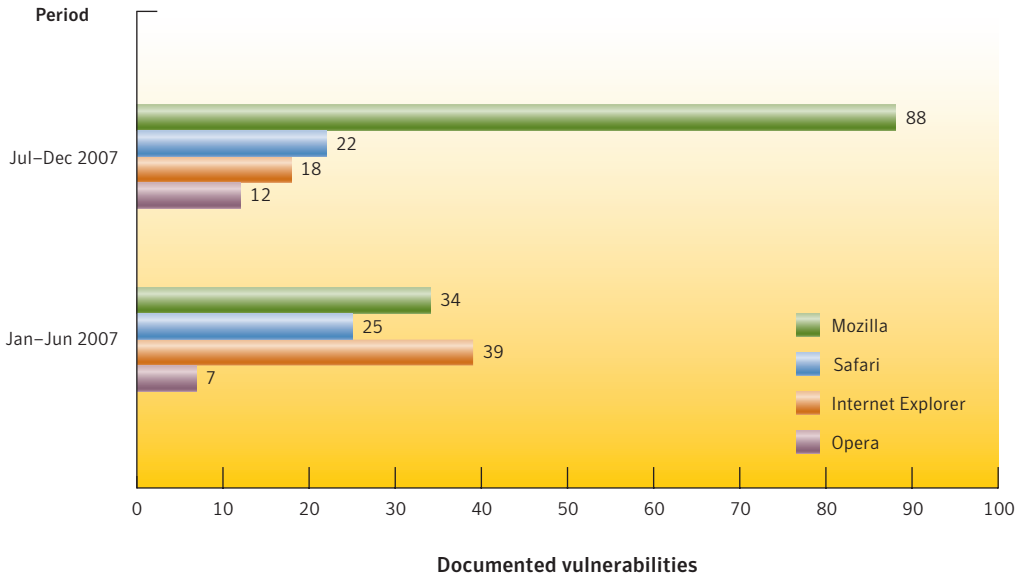

Figure 8. Web browser vulnerabilities
Source: Symantec Corporation

In the second half of 2007, Symantec documented 18 vulnerabilities in Internet Explorer. Of these, 13 were considered medium severity and five were low. This is less than the 39 vulnerabilities documented in the first half of 2007, of which one was considered high severity, 15 were medium, and 23 were low.

In the last six months of 2007, 12 vulnerabilities were documented in Opera. Of these, eight were medium severity and four were low. This is fewer than the seven vulnerabilities that affected Opera in the first half of 2007, of which three were considered medium severity and four were low.

While fewer vulnerabilities were discovered in Internet Explorer during this period, Mozilla was subject to a sharp increase. The decrease in Internet Explorer vulnerabilities may be due to the focus on security in Internet Explorer 7. The increase in Mozilla vulnerabilities was a by-product of internal and community-driven security audits of the browser.

The number of vulnerabilities in Safari also exceeded those reported in Internet Explorer. Increased adoption of browsers from vendors such as Mozilla and Apple has driven increased interest by security researchers. However, as security researchers have focused more efforts in discovering vulnerabilities in these browsers, the theory that this would result in much greater levels of malicious activity targeting these browsers in the wild has not yet been borne out. The growth in browser market-share for browsers such as Mozilla Firefox is a driving factor in the increased attention by security researchers.[51] However,

[51] http://www.w3schools.com/browsers/browsers_stats.asp

this does not necessarily result in more attack activity in the wild. Although Internet Explorer was subject to fewer vulnerabilities that are inherent to the browser in comparison to Mozilla, exploit activity in the wild indicates that it is still the gateway for third-party vulnerabilities affecting ActiveX and other browser plug-in technologies.

Browser plug-in vulnerabilities

Browser plug-ins are technologies that run inside the Web browser and extend its features. They can include plug-ins that allow additional multimedia content from Web pages to be rendered in the browser. They can also include execution environments that allow applications to be run inside the browser. 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. Some plug-ins may even be required to use public Web sites and/or an organization's internal sites. Browser plug-in vulnerabilities are implicated in some client-side attacks and present similar challenges to the enterprise.

The following browser plug-in technologies were examined for vulnerabilities:

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

In the second half of 2007, Symantec documented 239 vulnerabilities affecting browser plug-ins (figure 9). Of these, 190 affected ActiveX components, 19 affected the Apple QuickTime plug-in, 13 affected the Sun Java plug-in, 11 affected Adobe Flash, four affected the Windows Media Player plug-in, one affected Adobe Acrobat, and one vulnerability affected Mozilla browser extensions.

In the first half of 2007, 237 vulnerabilities were documented in browser plug-ins. Of these, 210 affected ActiveX components, 18 affected the Apple QuickTime plug-in, four affected the Sun Java plug-in, three affected Mozilla extensions, and two vulnerabilities affected Adobe Acrobat.

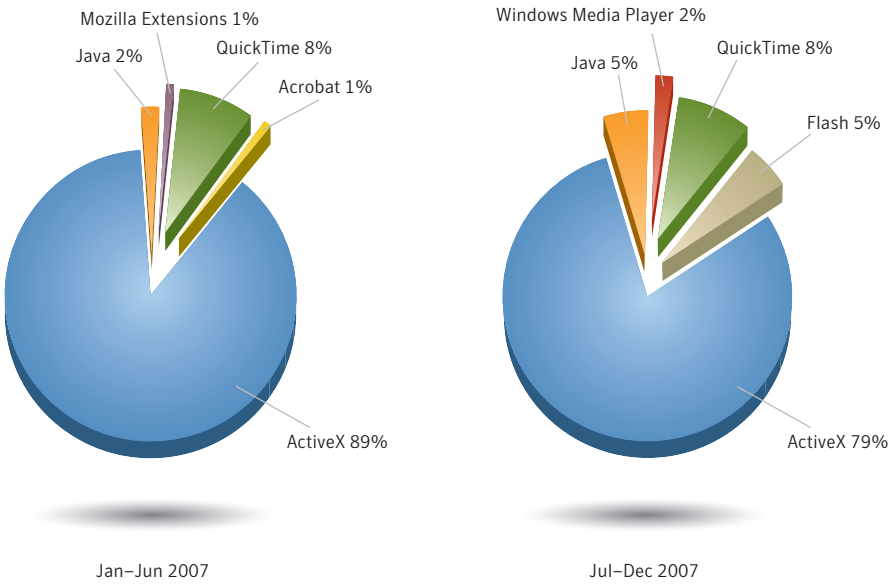

Figure 9. Browser plug-in vulnerabilities
Source: Symantec Corporation

Browser plug-in vulnerabilities continue to be prevalent because technologies such as ActiveX remain an easy target for security researchers and attackers alike, mostly due to fuzzer programs such as AxMan[52] and COMRaider.[53] This may indicate that there is a lack of secure development practices among ActiveX application developers. However, ActiveX is also an attractive target because many users may not be aware that they have installed vulnerable controls, and because of the relative difficulty of removing or patching ActiveX controls once they have been installed. The largest proportion of plug-in vulnerabilities affects ActiveX, which indicates that Internet Explorer is still the primary attack vector for plug-in vulnerabilities. However, the vast majority of these vulnerabilities affect third-party ActiveX controls.

The release of Internet Explorer 7 included security enhancements to limit the exploitation of ActiveX vulnerabilities; however, this has not appeared to have reduced the prevalence of ActiveX vulnerabilities. This may be a measure of the effectiveness of these security enhancements or it may indicate that many at-risks users have not upgraded to Internet Explorer 7. Enterprises may be reluctant to upgrade due to potential incompatibilities with corporate and external Web sites, or with business applications. While Microsoft has gone a long way to improve the security of Microsoft Windows and its applications, ActiveX is still a critical security exposure on the Microsoft Windows platform.

In August 2007, Symantec observed in-the-wild exploitation of a Microsoft DirectX ActiveX vulnerability.[54] An exploit for this vulnerability was later incorporated into the IcePack Web-attack toolkit.[55] In the last six months of 2007, Symantec has also detected zero-day exploitation of many ActiveX vulnerabilities in the wild, including vulnerabilities in GlobalLink,[56] Real Networks RealPlayer,[57] and SSReader Ultra Star Reader.[58] A significant ActiveX vulnerability was also discovered in December 2007 that affected many HP laptop models.[59] A vulnerability in Apple QuickTime was also subject to in-the-wild exploitation during this period.[60]

[52] http://www.metasploit.com/users/hdm/tools/axman
[53] http://labs.idefense.com/software/fuzzing.php#more_comraider
[54] http://www.securityfocus.com/bid/25279
[55] http://explabs.blogspot.com/2007/09/new-exploit-this-weekend.html
[56] http://www.securityfocus.com/bid/26244
[57] http://www.securityfocus.com/bid/26130
[58] http://www.securityfocus.com/bid/26247
[59] http://www.securityfocus.com/bid/26950
[60] http://www.securityfocus.com/bid/26549

Shotgun attacks from trusted Web sites are often the *modus operandi* for attackers who are exploiting browser plug-in vulnerabilities. A shotgun attack is one that attempts to compromise a victim by exploiting multiple vulnerabilities. Attackers choose this method to improve the likelihood of successful compromise since the victim may be patched against some of the vulnerabilities, or there may be other factors that impact the reliability of the attack. Sophisticated shotgun attacks also employ browser version detection to avoid attacking clients that do not run vulnerable versions of affected applications.

Plug-in vulnerabilities figured into the compromises of a number of high-profile and trusted Web sites during this reporting period. In September, the Syrian Embassy of London was compromised by attackers and used to serve browser plug-in exploits using the MPack toolkit.[61] A similar attack also occurred in August against the Indian Syndicate Bank.[62] When attackers compromise trusted sites in this manner, the attack is engineered to make it appear as though the Web site is functioning normally, while malicious content is served to users of the site through embedded iframes that otherwise render the attack invisible to the victim. This can pose a greater risk if the site is designated by the browser to be a trusted site, which means that fewer security restrictions are placed on the site. Lowered security settings for trusted sites increase the exposure of vulnerable plug-ins. This is especially true in case of ActiveX because the security measures imposed by Internet Explorer depend on the trust level assigned to the Web site, although similar scenarios also exist with other plug-in technologies.

The fact that many zero-day vulnerabilities and attacks-in-the-wild exploit plug-in vulnerabilities is an indicator of their importance in the threat landscape. Many enterprises have enacted restrictive policies to limit the sites users may access. Attackers are overcoming this hurdle by compromising even those limited sites and using them as a means to exploit plug-in and other client-side vulnerabilities. However, it may also be the case that, while organizations often implement a security policy to limit the sites and applications that may be used, this policy may not extend to cover browser plug-ins. Furthermore, attackers risk arousing suspicion when they attempt to use social engineering techniques to entice victims into visiting a malicious Web site. If they can launch their attacks through a Web site that the user visits regularly and trusts, then they avoid having to entice users into visiting suspicious Web sites.

End users and administrators can use a number of measures to protect against the effects of vulnerabilities. IPS technologies can prevent exploitation of some browser plug-in vulnerabilities through signature- or behavior-based approaches in addition to ASLR and memory protection.[63] Antivirus software may also aid in protecting organizations from browser plug-in exploits through heuristic signatures.

While attacks are likely to originate from Web sites that are trusted as well as those that are not, Web browser security features can help reduce exposure to browser plug-in exploits, as can whitelisting. Specifically, administrators and end users should actively maintain a whitelist of trusted Web sites, and should 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. Only plug-ins that have been audited and certified should be installed on workstations throughout the organization. Organizations can also implement a whitelist policy at the network perimeter to regulate outgoing access by end-users. Content filtering may also be employed to strip potentially malicious content from trusted and untrusted sites.

[61] http://www.websense.com/securitylabs/alerts/alert.php?AlertID=806
[62] http://www.websense.com/securitylabs/alerts/alert.php?AlertID=794
[63] Address space layout randomization is a security measure to complicate exploitation of some classes of vulnerabilities by randomizing the layout of process address space to make it less predictable to attackers.

Web application vulnerabilities

Web applications are technologies that use a browser for their user interface, rely on HTTP as the transport protocol, and reside on Web servers. Examples of Web-based applications include content management systems, e-commerce suites (such as shopping cart implementations), Weblogs, and Web-based email.

The online presence of an organization is often facilitated through Web applications, particularly as an increasing number of traditional software vendors are bolstering their existing applications with Web-based user interfaces, or converting them over entirely. Web applications may be the site of vulnerabilities that can be exploited to gain unauthorized access to computers on which they are deployed. Users within the organization may also be affected by insecure Web sites, which may present a risk of compromise and/or a threat to confidential information.

Web security is becoming more important as more enterprises outsource their business applications to a software-as-a-service model.[64] The integrity and security of these services is critical to the enterprises that depend on them. This trend means that enterprises have less control over the security of business applications and must place more trust in vendors who provide business services over the Web. Furthermore, these services are a valuable asset to attackers because they provide a means of distributing exploit code and malicious code to unsuspecting users. In addition, Web applications may be deployed across a number of individual servers and can have an impact on these systems and other systems that interact with the application.

In the second half of 2007, 58 percent of all vulnerabilities affected Web applications (figure 10). This is less than the 61 percent in the first half of 2007. This drop in the proportion of Web application vulnerabilities is a continuing trend. In the previous volume of the Symantec *Internet Security Threat Report*, the potential impact of site-specific vulnerability findings was discussed as a possible cause for this trend.[65] From an attacker's standpoint, rather than try to compromise numerous smaller sites, it is better to compromise a specific popular site with a single vulnerability as this increases the chances of compromising a larger number of hosts.

[64] Software-as-a-service is when a software application is accessed over the Internet rather than being installed directly on the user's computer.
[65] Site-specific vulnerabilities are those that affect the custom or proprietary Web-application code for a specific Web site.

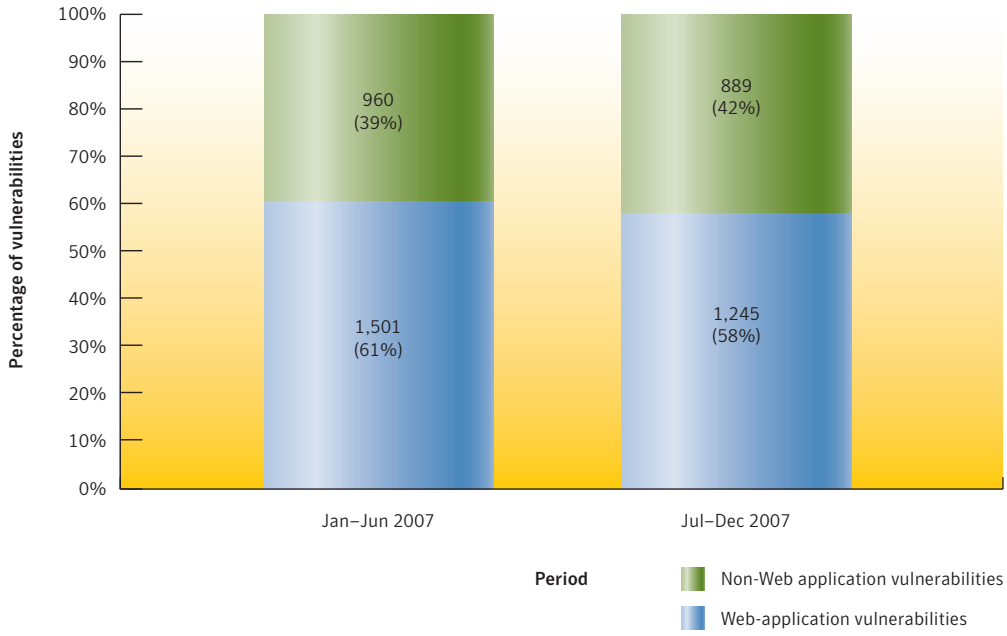

Figure 10. Web application vulnerabilities
Source: Symantec Corporation

Given that they can facilitate more sophisticated or multistage attacks, vulnerabilities in Web sites are a significant part of the threat landscape. Web application vulnerabilities provide attackers with a diverse set of targets because the majority of these issues affect obscure applications that are deployed on a small number of sites. However, attackers are discovering that they can reach a greater number of targets by focusing on major sites with broad user-bases. Attackers can benefit from the trust in the brand of such sites, but it also allows them to steal credentials or launch other attacks en masse. Social networking sites are especially attractive because they can allow attacks to propagate quickly through a victim's social network. This is the reason for the shift to site-specific vulnerabilities.

Site-specific cross-site scripting vulnerabilities

In the previous volume of the Symantec *Internet Security Threat Report*, site-specific vulnerabilities were discussed as a possible cause for the drop in Web applications as a proportion of all documented vulnerabilities. In this report, Symantec investigates this trend in detail using data provided by a site-specific vulnerability database.[66] In particular, this section will discuss a sub-category of Web-application vulnerabilities known as cross-site scripting. It should 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.

[66] 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.

Vulnerabilities that are specific to particular Web sites are a concern because compromised Web sites serve as a means of launching other attacks against users, especially if those sites are trusted. As is discussed throughout this report, this has shown to be an effective strategy in launching multistage attacks and exploiting client-side vulnerabilities.

Cross-site scripting vulnerabilities present a direct threat to users of affected Web sites because they allow attackers to access session cookies. A successful cross-site scripting attack can let an attacker hijack a user's session on an affected Web site, effectively stealing his or her credentials and allowing the attacker to perform actions posing as the user. They also play an important role in more sophisticated attacks because they have the potential to let attackers distribute malicious content through a compromised site. Malicious content can take the form of exploits, malicious code, defacement of site content, or phishing attacks. This can compromise an enterprise's trust in legitimate Web sites since attacks can originate from sites deemed safe by the security and usage policies of the organization.

During the last six months of 2007, there were 11,253 site-specific cross-site scripting vulnerabilities (figure 11) that were documented by the XSSed project. At the time of writing, only 473 of these vulnerabilities had been fixed by the maintainer of the affected Web site. In the first six months of 2007, the total was 6,961, although data collection only began in February,[67] which factors into the lower total. Of the 6,961, only 330 had been fixed at the time of writing.[68]

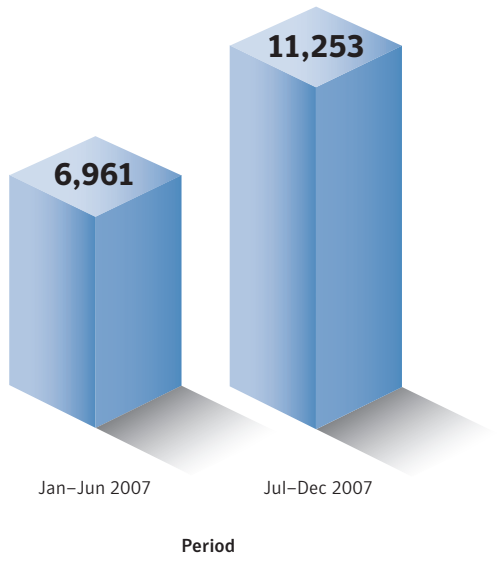

Figure 11. Site-specific cross-site scripting vulnerabilities
Source: Based on data provided by the XSSed Project

The average patch development time for site-specific cross-site vulnerabilities can be determined by measuring elapsed time between the publication date of the vulnerability and the patch date by the maintainer of the affected Web site. In the second half of 2007, the average patch development time was 52 days (figure 12), down from the average of 57 days in the first half of 2007.

[67] The XSSed Project started in February 2007.
[68] This report was written at the end of 2007.

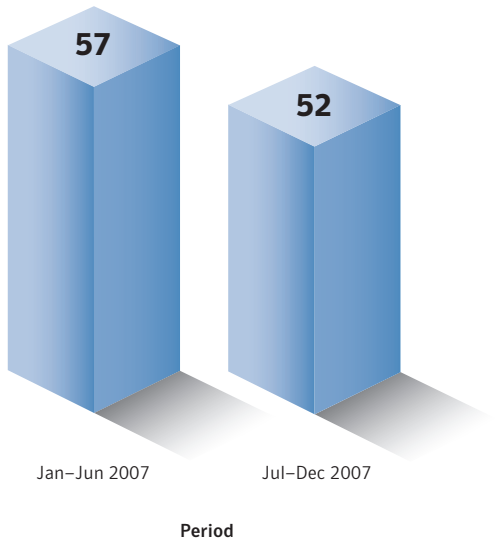

Figure 12. Site-specific cross-site scripting vulnerabilities time to patch, in days
Source: Based on data provided by the XSSed Project

Site-specific vulnerabilities are a growing concern. The number of cross-site scripting vulnerabilities that affected specific sites in 2007 exceeds the total number of traditional vulnerabilities tracked. Moreover, the numbers presented in this section are also only representative of site-specific vulnerabilities that are reported voluntarily by security researchers to the XSSed Project archive. Other types of Web-application vulnerabilities are not covered. Symantec also has no insight into privately discovered vulnerabilities that have not been reported to the public. This would imply that there are many more vulnerabilities that are not publicly known. Furthermore, the numbers show that very few of these issues are being remedied by the maintainers of the vulnerable Web sites. Additionally, the average patch development time is greater than 50 days for the minority of vulnerabilities that are being addressed.

This trend is a concern because it indicates that site maintainers in general have a very poor track record of addressing vulnerabilities in their Web sites. When attackers discover a vulnerability in a site, they can expect that the site maintainer will not address the vulnerability in a reasonable amount of time, if at all. Therefore, any malicious content that is injected into a vulnerable site, such as exploits for other vulnerabilities, will likely remain for a prolonged period or indefinitely. This can have a negative impact on the brand of a vulnerable site, but it is also a concern for businesses that rely on services provided by the site as part of their day-to-day operations. Not only do these vulnerabilities pose a risk to the confidential information that is stored on the sites, but they are also increasingly implicated in multistage attacks that compromise desktop systems.

Web site maintainers can reduce their exposure to site-specific vulnerabilities by conducting a security audit for common vulnerabilities affecting their sites. Web application code should be audited prior to being released to production systems. When developing Web applications, organizations should investigate

the availability and applicability of secure libraries to perform validation of user-supplied input. Secure development practices and threat modeling should also be employed when developing Web-based applications. Web-application firewalls may also detect and prevent exploitation of Web-based vulnerabilities on production sites.

Individual Web users should also exercise caution when browsing the Web. Since these attacks can result in hijacking of open sessions, users should make sure to log out of Web sites when their session is complete. Users should also be wary of visiting untrusted or unfamiliar sites. Scripting and active content can also be disabled when casually browsing the Web.

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 vendor prior to exploitation and the vendor had not released a patch at the time of the exploit activity.

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. A black market for zero-day vulnerabilities has emerged that has the potential to put them into the hands of criminals and other interested parties.[69]

In the second half of 2007, Symantec documented nine zero-day vulnerabilities, compared to six in the first half of the year. All the zero-day vulnerabilities documented during this period targeted third-party applications for Microsoft Windows. This is a shift from previous reporting periods, where a portion of the zero-day vulnerabilities affected Microsoft Office™. Eight of the nine zero-day vulnerabilities were also client-side in nature, the majority of which affected ActiveX components. Seven of the nine targeted popular Japanese and Chinese applications such as JustSystem Ichitaro, Lhaz, GlobalLink, SSReader Ultra Star Reader, and Xunlei Web Thunder.

In this period, it appears that attackers have shifted from exploiting zero-day vulnerabilities in globally-deployed applications such as Microsoft Office to more regionally-oriented applications. Attackers tend to be opportunistic in nature; once an avenue of attack has proven successful, they often search for similar vulnerabilities in the same types of applications. It is likely that there is an active community of attackers based in the respective regions who have discovered that it is lucrative enough to focus on users within their own region instead of exploiting vulnerabilities with a higher profile on the global scale. This makes sense because it is in their best interest to strike a balance between vulnerabilities that affect a large user base versus lower profile issues that are less likely to draw public attention. High profile vulnerabilities are more likely to be patched or mitigated by organizations, whereas there is a greater likelihood that lower profile vulnerabilities will remain unpatched for a longer period.

In order to protect against zero-day vulnerabilities, Symantec recommends that administrators deploy network and host-based IDS/IPS[70] systems as well as regularly updated antivirus software. Security vendors may provide rapid response to recently discovered zero-day vulnerabilities in the wild by

[69] Symantec *Internet Security Threat Report*, Volume IX (March 2006): http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_ix.pdf : p. 20
[70] Intrusion detection (IDS) and intrusion prevention (IPS) software.

developing and implementing new or updated IDS/IPS and antivirus signatures before a patch has been released by the affected vendor. Behavior-blocking solutions and heuristic signatures may also provide protection against zero-day vulnerabilities.

In addition, some IPS systems may provide further protection against memory corruption vulnerabilities in the form of address space layout randomization (ASLR), and by making memory segments non-executable. These measures may complicate the exploitation of such vulnerabilities and make it more difficult for attack payloads to execute; however, this security measure may not protect all applications by default.

Unpatched enterprise vendor vulnerabilities

Symantec examines the number of unpatched vulnerabilities affecting enterprise vendors whose applications are widely deployed and considered to be mission-critical in nature. The following enterprise vendors are examined in this section:

- CA™
- Cisco®
- EMC®
- HP
- IBM®
- McAfee®
- Microsoft
- Oracle™
- Sun
- Symantec

Unpatched vulnerabilities are publicly documented security issues that are not known to be patched by the vendor responsible for maintaining the affected application. It should be noted that the vulnerabilities discussed were known to be unpatched when the data was gathered and may have since been patched by the time of publication. There is also the chance that some vulnerabilities were patched by the vendor without a public announcement; in such cases there is insufficient publicly available information to label these issues as patched. It is also important to note that some unpatched vulnerabilities remain in this state because they affect unsupported products, or because the vendor has provided specific workarounds that address the vulnerability until a patch is available.

These vulnerabilities are a serious concern for enterprises because they cannot be resolved without applying best practices, workarounds, and/or mitigations. In many circumstances these measures will not provide complete protection against unpatched vulnerabilities.

In the second half of 2007, Symantec documented 88 unpatched enterprise vulnerabilities that were published during this period (table 3). Of these, 39 affected Microsoft, 22 affected IBM, 10 affected Computer Associates, eight affected HP, five affected Sun, three affected Oracle, and one affected Symantec. No other vendor was subject to unpatched vulnerabilities during this period.

Enterprise Vendors	Current	Previous
Microsoft	39	61
IBM	22	1
Computer Associates	10	1
HP	8	3
Sun	5	1
Oracle	3	13
Symantec	1	1
McAfee	0	0

Table 3. Unpatched vulnerabilities, by vendor
Source: Symantec Corporation

In the first half of 2007, Symantec documented 81 unpatched enterprise vulnerabilities. While some vendors addressed unpatched vulnerabilities, the majority remain unpatched six months later. Of the 81 unpatched enterprise vulnerabilities remaining, 61 affected Microsoft, 13 affected Oracle, three affected HP, one affected Computer Associates, one affected IBM, one affected Sun, and one affected Symantec. No other enterprise vendors had outstanding vulnerabilities during this time.

During the first and second half of 2007, Microsoft was affected by more unpatched vulnerabilities than any other vendor. Many of the unpatched vulnerabilities are lower-impact issues such as DoS vulnerabilities against Internet Explorer and other applications. It is still the case that these issues may be addressed outside of Microsoft's monthly security patches. It is also possible, however, that some vulnerabilities may be deemed higher severity if new information or exploits surface that increase the risk to users.

Such was the case with a particular IIS vulnerability that was initially published in 2005.[71] It remained unpatched until July 2007 because the issue was originally believed to be limited to DoS and considered low priority to Microsoft. The vulnerability fell into a category of software bugs previously thought to be non-exploitable to execute arbitrary code. However, security researchers investigated the vulnerability further and discovered a way that remote attackers might exploit the issue.[72] It is rare for security researchers to find a method of exploiting software bugs that were previously considered non-exploitable. However, many DoS vulnerabilities are simply not researched enough to eliminate the possibility of executing arbitrary code. This lack of research presents an opportunity for attackers, especially if it has caused vendors to delay releasing patches because they underestimate the potential threat.

IBM was affected by more unpatched vulnerabilities than all vendors other than Microsoft in the last six months of 2007. This is likely due to outstanding vulnerabilities affecting products such as Lotus Notes® and Domino®, the Tivoli line of products, and IBM WebSphere, which is a concern given the widespread enterprise deployment of these products.

[71] http://www.securityfocus.com/bid/15921
[72] http://www.securityfocus.com/news/11477

Vulnerabilities in security products

In this report, Symantec discusses vulnerabilities affecting security products, which should be critical to the operational and security infrastructure of any organization. Vulnerabilities in these products can weaken the security posture of any organization and can potentially compromise the ability of an enterprise to prevent attackers from threatening critical assets. Vulnerabilities in security products can also prevent organizations from performing essential security functions such as implementing best practices, mitigating vulnerabilities, fending off malicious code, securing the network perimeter and other layers, and enforcing policy compliance.

For the purpose of this discussion, Symantec examines vulnerabilities that affect the following categories of security product:

- Antivirus
- Firewalls
- Intrusion detection systems (host- and network-based)
- Intrusion prevention systems (host- and network-based)
- Network access control (NAC)

Symantec documented 92 vulnerabilities that affected security products during the second half of 2007 (figure 13). Of these, 15 were classified as high severity, 48 as medium, and 29 as low. This is fewer than the 113 vulnerabilities that affected security products during the first half of 2007, of which 23 were classified as high severity, 58 as medium, and 32 as low. During the last six months of 2007, four percent of all vulnerabilities documented during the period affected security products, down slightly from five percent during the first six months of the year.

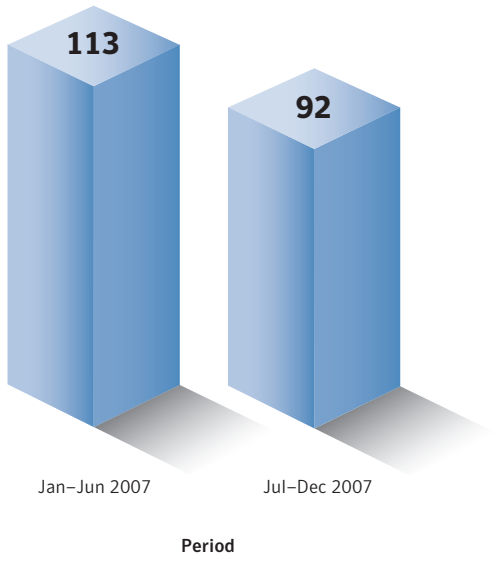

Figure 13. Vulnerabilities in security products
Source: Symantec Corporation

It is worth noting that during both reporting periods in 2007 the majority of vulnerabilities in security products affected antivirus technologies, though the number declined over the two periods from 67 percent to 53 percent. However, that antivirus technologies still comprise the majority is an indicator that both security researchers and attackers are focusing on antivirus technologies.

This trend is significant because antivirus technologies often provide a layer of defense against client-side attacks and other malicious activity targeted at desktop users. As these attacks become more common, antivirus and other desktop security technologies have become prone to scrutiny by security researchers. It is important to the enterprises that invest in these products that they are relatively free of vulnerabilities when they ship. Many vulnerabilities in security products are actually discovered as a result of security vendors conducting research into competitors' products. This competition will likely benefit security products in the long run and result in fewer vulnerabilities in production security software. In the meantime, the cost to enterprises remains high due to the exposure that these vulnerabilities present and the overhead associated with patching vulnerabilities affecting critical security systems.

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 what assets are deployed on the network and to determine which ones may be affected by the discovery of new vulnerabilities. Vulnerability management technologies should also be used to detect known vulnerabilities in deployed assets. Administrators should monitor vulnerability mailing lists and security Web sites to keep abreast of new vulnerabilities in Web applications.

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. 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. Event management should also be integrated into the enterprise infrastructure to 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 Web sites 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.[73] 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.

[73] 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 that involves formally identifying and mapping out all possible attack vectors for an application.

Malicious Code Trends

Symantec gathers malicious code data from over 120 million desktops that have deployed Symantec antivirus products in consumer and corporate environments. The Symantec Digital Immune System and Scan and Deliver technologies allow customers to automate this reporting process. This discussion is based on malicious code samples analyzed by Symantec for analysis between July 1 and December 31, 2007.

In previous editions of the Symantec *Internet Security Threat Report*, the number and volume of threats analyzed were based upon the number of malicious code instances received from enterprise and home users. This report will also examine malicious code according to potential infections. This allows Symantec to determine which malicious code sample was attempting to infect computers and the number of potential infections worldwide.

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

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

New malicious code threats

The number of new malicious code threats detected by Symantec in a given reporting period allows administrators and users to keep track of the productivity of malicious code writers during that time. Periods in which large amounts of new malicious code are created require frequent updating of antivirus signatures, as well as the implementation of other security measures such as patching against Web-browser and browser plug-in vulnerabilities that are frequently exploited to install malicious code on computers. As noted in the "Vulnerability Trends" section of this report, there were 140 documented vulnerabilities in the most popular Web browsers this period, compared to 105 in the previous period. The growing number of browser vulnerabilities provides attackers with greater opportunities to exploit the browser in order to install malicious code.

In the last six months of 2007, Symantec detected 499,811 new malicious code threats (figure 14). This is a 136 percent increase over the previous period, when 212,101 new threats were detected, and a 571 percent increase over the last half of 2006. In total, there were 711,912 new threats detected in 2007, compared to 125,243 threats in 2006, an increase of 468 percent. This brings the overall number of malicious code threats identified by Symantec to 1,122,311, as of the end of 2007. This means that almost two thirds of all malicious code threats currently detected were created during 2007.

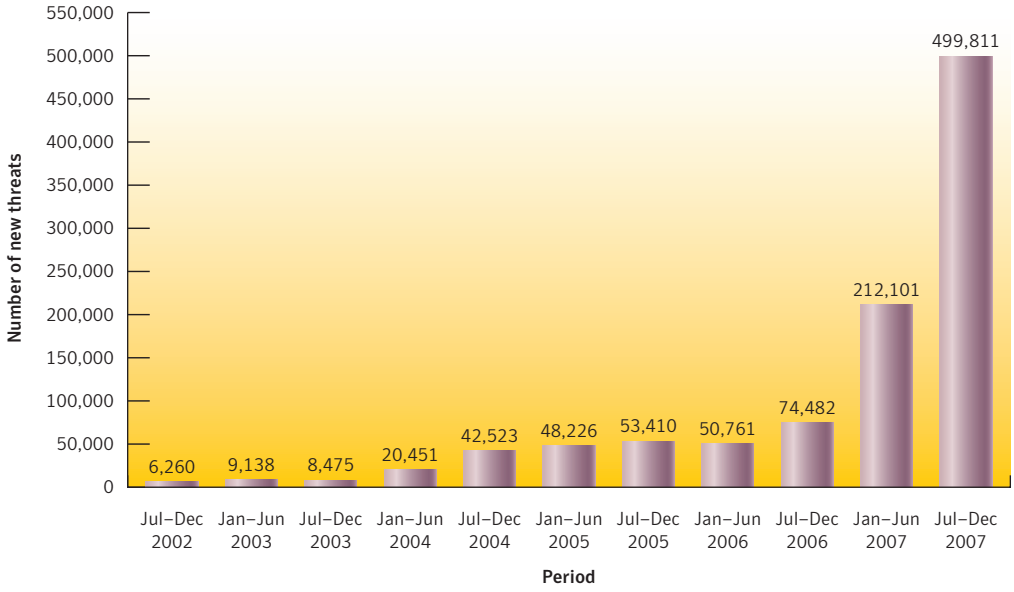

Figure 14. New malicious code threats
Source: Symantec Corporation

The continued increase in threats this period is mainly attributed to the continuing increase in new Trojans. As noted in Volume XII of the Symantec *Internet Security Threat Report*,[74] the prevalence of staged downloaders consisting of an initial Trojan designed to establish a beachhead from which additional threats can be installed contributed significantly to the number of new threats. Since the initial stage usually involves minimal functionality, it is relatively easy for attackers to create numerous variations of these simple Trojans.

The significant increase in new threats over the past year is also indicative of the increasing professionalization of malicious code and the existence of organizations that employ programmers dedicated to the production of these threats. A group of programmers can create a larger number of new threats than can a single malicious code author. As these groups of programmers must be paid, professionally written malicious code requires a profit return. It is in the interests of these organizations to constantly produce new threats to infect the largest number of computers. Many of these threats can be used for financial gain by performing actions such as stealing confidential information that can be sold online. These proceeds can then be used to pay the programmers to continue creating new threats. The combination of these factors results in a high volume of new malicious code samples that threaten users online.

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

[74] Symantec *Internet Security Threat Report*, Volume XII (September 2007): http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_09_2007.en-us.pdf : p. 78

Top 10 new malicious code families

Of the top 10 new malicious code families detected in the last six months of 2007, five were Trojans, two were worms, two were worms with a back door component, and one was a worm with a virus component (table 4). As noted in the previous edition of the Symantec *Internet Security Threat Report*, the prevalence of Trojans in the top new malicious code families is indicative of multistage attacks. These are attacks in which an initial compromise takes place in order to install another piece of malicious code, such as a Trojan, which then downloads and installs additional threats.

Rank	Sample	Type	Vectors	Impacts/Features
1	Invadesys	Worm	CIFS	Lowers security settings and modifies Web pages
2	Niuniu	Worm/virus	CIFS	Modifies Web pages
3	Farfli	Trojan	N/A	Downloads other threats and modifies Internet Explorer start page
4	Pidief	Trojan	N/A	Exploits Adobe Acrobat vulnerability to lower security settings and download other threats
5	Blastclan	Worm	CIFS	Disables security applications
6	Scrimge	Worm/back door	IM	Allows remote access
7	Neeris	Worm/back door	IM	Allows remote access
8	Advatrix	Trojan	N/A	Lowers security settings and displays targeted advertising
9	Fakeavalert	Trojan	N/A	Displays fake antivirus alerts and lowers security settings
10	Ascesso	Trojan	N/A	Downloads other threats and sends spam

Table 4. Top 10 new malicious code families
Source: Symantec Corporation

The most widely reported new malicious code family during this reporting period was the Invadesys worm.[75] This worm propagates by copying itself to all fixed, removable, and mapped network drives. It lowers security settings on the compromised computer by terminating certain processes. The worm may also delete files with certain extensions such as .avi and .mpg. However, the most notable impact of this worm is that it prepends its code to any Web pages on the compromised computer.

Users frequently store the pages for personal Web sites on their local drive and upload any modified pages. Web pages that are infected by Invadesys would potentially be uploaded to the user's hosting provider the next time modifications are uploaded. This could result in visitors to the user's site being compromised when they view an infected page. The tendency of malicious code modifying Web pages is part of a growing trend, as is discussed in the "Malicious code that modifies Web pages" section in this report.

The Niuniu[76] worm was the second most common new malicious code family this period. This worm is similar to the Invadesys worm in that it propagates by copying itself to all fixed, removable, and mapped network drives on the compromised computer. The worm also modifies the user's Internet Explorer start page to a Web site that the attacker likely controls.

[75] http://www.symantec.com/security_response/writeup.jsp?docid=2007-111215-5430-99
[76] http://www.symantec.com/security_response/writeup.jsp?docid=2007-101018-5756-99

Also, like Invadesys, Niuniu adds code to any Web pages it finds on the compromised computer. However, rather than adding code to infect users who view the pages, Niuniu adds an invisible iframe HTML tag to the pages. This tag will redirect the user's browser without his or her knowledge to a Web page that is likely under the attacker's control. This can be used to redirect the user to a Web page that hosts malicious code or attempts to exploit a Web browser vulnerability. This technique is similar to that employed in the MPack attack seen in the first half of 2007.

The Farfli Trojan[77] was the third most commonly reported new malicious code family in the second half of 2007. This Trojan is capable of downloading and installing other threats onto the compromised computer. This is a continuation of the trend of increasing multistage attacks that was noted in the previous version of the Symantec *Internet Security Threat Report*.[78] In a multistage attack, an initial compromise takes place that is intended to facilitate the launch of subsequent attack activity.

In addition to installing other threats on the compromised computer, Farfli also changes the user's Internet Explorer homepage to one the attacker likely controls. This is presumably done to generate revenue for the attacker through affiliate advertising clicks. For each compromised computer that opens the page, the attacker would receive payment from banner advertising.

It is also notable that this Trojan changes the search settings for the Maxthon and TheWorld Web browsers.[79] The settings are changed to use the same revenue-generating pages as previously described. What is noteworthy is that these two Web browsers do not have the same market share as other browsers that are more commonly targeted. This may indicate that Farfli was written to target a certain group of users. Both of these browsers are developed and maintained by Chinese companies, which may indicate that the author of the Trojan is specifically targeting Chinese users. Further, since the Trojan changes the search settings to use a popular Chinese search engine, this may also indicate that Chinese users are being targeted. This exemplifies the continuing trend of regionalization of malicious code that was noted in the previous version of the Symantec *Internet Security Threat Report*.[80]

It is interesting to note that in the current period two of the top 10 new families, Scrimge[81] and Neeris,[82] both used instant messaging as a propagation vector. Instant messaging appears to have lost favor as a propagation vector amongst malicious code authors who have shifted towards the use of malicious Web pages to install Trojans. However, these worms send instant messages in various languages including English, French, German, Spanish, and Italian. As a result, these families were most frequently reported to cause potential infections in the EMEA region. More than half of worldwide potential infections of these malicious code families occurred in that region. It is likely that the presence of these samples in the top 10 new malicious code families this period is not indicative of a widespread resurgence of instant messaging as a propagation mechanism, but rather demonstrates the success of regionalized threats.

[77] http://www.symantec.com/security_response/writeup.jsp?docid=2007-072901-5957-99
[78] Symantec *Internet Security Threat Report*, Volume XII (September 2007): http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_09_2007.en-us.pdf : p. 75
[79] Maxthon and TheWorld are Web browsers that make use of the Internet Explorer and Firefox rendering engines. As a result, they behave in a similar manner to these browsers and are also susceptible to the same vulnerabilities.
[80] Symantec *Internet Security Threat Report*, Volume XII (September 2007): http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_09_2007.en-us.pdf : p. 81
[81] http://www.symantec.com/security_response/writeup.jsp?docid=2007-080614-3458-99
[82] http://www.symantec.com/security_response/writeup.jsp?docid=2007-091208-1650-99

Malicious code types

During the current reporting period, Trojans made up 71 percent of the volume of the top 50 potential malicious code infections (figure 15), a slight decrease from 73 percent in the first half of 2007, but still more than the 60 percent in the same period of 2006. It is interesting to note that, while the volume of Trojans in the top 50 decreased only slightly since the first half of the year, the number of distinct Trojans in the top 50 decreased from 22 in the first half of the year to 16 in the last six months of 2007.

This may indicate that attackers are gravitating towards the use of a smaller number of more successful Trojans. Once attackers discover that a Trojan has had a moderate degree of success, they usually begin creating minor variations of it. As a result, there will be a large number of different Trojans, each producing a smaller number of potential infections combined with heavy usage of those that have the greatest success in compromising users and executing their payload. This is reflected in the decrease of Trojans in the top 50 samples and the large increase in new malicious code threats. Six of the top 10 malicious code samples causing potential infections this period were Trojans.

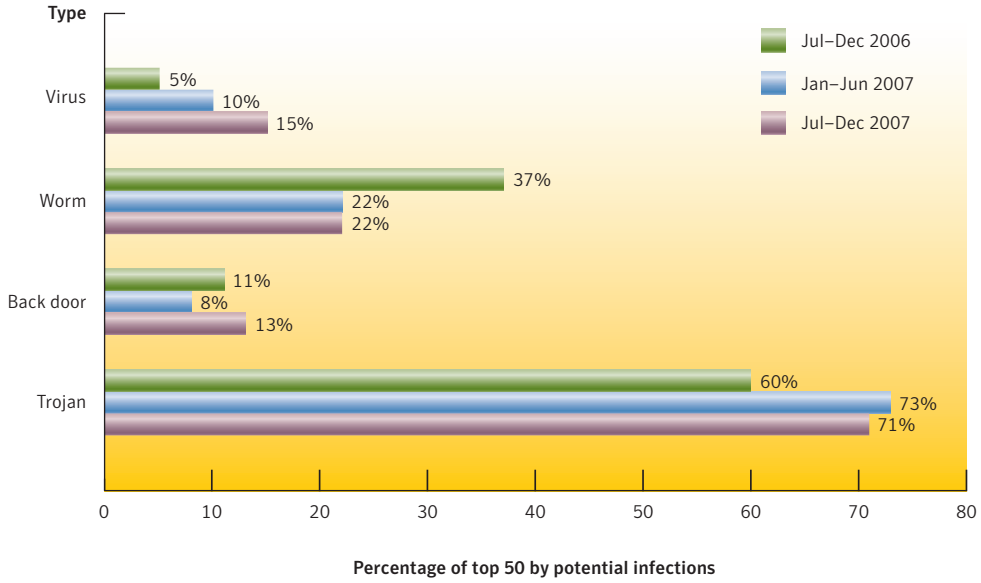

Figure 15. Malicious code types by potential infections
Source: Symantec Corporation

The top malicious code sample causing potential infections this period was the Vundo Trojan,[83] which downloads and installs an adware component. It is not surprising that attackers favor this threat since the adware component allows the attacker to generate revenue from every compromised computer. As is discussed in the "New malicious code threats" discussion in this report, attackers are usually motivated by financial gain. This revenue generation may also be further indicative of the increasing commercialization and professionalization of malicious code. Since commercial and professional malicious code may involve the employment of individuals to create and maintain the code, income is required to compensate the work.

[83] http://www.symantec.com/security_response/writeup.jsp?docid=2004-112111-3912-99

Trojans are also frequently used to steal information that an attacker can sell or profit from in other ways. For example, the Gampass Trojan[84] can be used to steal a user's online gaming account information, which can then be sold to other gamers.

The Silentbanker Trojan[85] can be used to steal a user's online banking credentials and divert legitimate transactions. This Trojan includes sophisticated mechanisms to steal funds from a user's online banking account. Silentbanker is also able to modify information in the transaction summary Web page that the bank displays to the user, fooling the user into thinking that the transaction has been successfully completed. This Trojan also has the ability to intercept secure communications and bypass two-factor authentication.[86] The techniques employed by this Trojan indicate that it was most likely created by an attacker or group of attackers with advanced programming skills. This may be indicative of the professionalization of malicious code. Since Silentbanker targets over 400 different online banking Web sites, it is likely that the attackers are attempting to maximize the financial return for the time and skill invested in creating the Trojan.

During the last six months of 2007, worms made up 22 percent of the volume of the top 50 potential malicious code infections reported to Symantec, unchanged from the first half of the year. Previously, Symantec had speculated that the reason the percentage of worms had declined was from an increase in Trojans and viruses, but it appears that the decline of worms may have leveled off. While worms have declined in popularity among attackers who prefer the stealth of Trojans, there will likely always be a certain number of new worms created along with continued incidences of older worms.

In the second half of 2007, worm numbers were bolstered by the Netsky[87] and Rontokbro[88] mass-mailers. It is interesting to note that these worms were discovered in 2004 and 2005, respectively. This is indicative of the success these worms have had, and how threats that propagate through social engineering such as these will continue to affect users long after their initial outbreaks. Typically, worms that propagate by exploiting vulnerabilities tend to decrease in volume as computers are patched or upgraded to newer operating system versions that are secured against the same issue.

Viruses made up 15 percent of the volume of the top 50 potential malicious code infections in the last six months of 2007, up from 10 percent in the previous six-month period and five percent in the last half of 2006. As noted in the previous edition of the Symantec *Internet Security Threat Report*,[89] the increase in viruses is mainly due to new worms that also incorporate a viral infection component.

In this period, there were also viruses such as Mumawow,[90] which downloads other threats onto a compromised computer. Previously, worms and Trojans were the primary malicious code types that were used as the first stage of multistage attacks. This shows that attackers are experimenting and evolving their techniques. Since attackers are always looking for new ways to compromise computers, it is not surprising that they have varied their methods by using viruses.

[84] http://www.symantec.com/security_response/writeup.jsp?docid=2006-111201-3853-99
[85] http://www.symantec.com/security_response/writeup.jsp?docid=2007-121718-1009-99
[86] Two-factor authentication involves the use of two separate mechanisms to verify a person's identity such as the combination of a password and a token or biometric device.
[87] http://www.symantec.com/security_response/writeup.jsp?docid=2004-032110-4938-99
[88] http://www.symantec.com/security_response/writeup.jsp?docid=2005-092311-2608-99
[89] Symantec *Internet Security Threat Report*, Volume XII (September 2007): http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_09_2007.en-us.pdf : p. 79
[90] http://www.symantec.com/security_response/writeup.jsp?docid=2007-061400-4037-99

The increasing use of firewalls has limited the ability of network worms to propagate and effective file-attachment blocking has also slowed the distribution of mass-mailing worms. However, there has been an increase in the use of removable media in both home and enterprise environments.[91] USB drives are increasingly used to transfer files too large to email or that consume too much bandwidth over the network. These devices are prime targets for attackers to use for propagating traditional file-infector viruses.

In addition to USB drives, many portable media players can also act as removable drives. A user may unknowingly copy an infected file onto the device from his or her home computer, then connect it to a computer inside the enterprise, resulting in potential infections. This is the same principle that allowed viruses to propagate through floppy disks before the widespread expansion of the Internet.

Geolocation by type

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. For example, threats may use 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 common in some countries than in others. Trojans that steal account information for Brazilian banks are quite common in the Latin America region, while malicious code that steals online gaming account information is most frequently observed in the Asia-Pacific and Japan (APJ) region. Because of the different propagation mechanisms used by different malicious code types, and the different effects that each malicious code type may have, the geographic distribution of malicious code can help network administrators in specific regions improve their security efforts.

Between July 1 and December 31, 2007, 46 percent of Trojans were reported from North America, 31 percent from EMEA, 20 percent from APJ, and three percent from Latin America (table 5). There were only slight changes in the geographic distribution of potential infections from Trojans this period compared to the first half of 2007. In the previous period, Trojans originating in EMEA were bolstered by high profile attacks from the Peacomm Trojan[92] and MPack kit.[93] Since there were fewer single, large, Trojan-based attacks centered in EMEA this period, the concentration of Trojans reported there subsequently declined.

Region	Current	Previous
North America	46%	43%
EMEA	31%	36%
APJ	20%	17%
Latin America	3%	4%

Table 5. Location of Trojans
Source: Symantec Corporation

[91] http://www.us-tech.com/RelId/669342/ISvars/default/New_Production_Technologies_fo.htm
[92] http://www.symantec.com/enterprise/security_response/weblog/2007/01/trojanpeacomm_building_a_peert.html
[93] http://www.symantec.com/enterprise/security_response/weblog/2007/06/italy_under_attack_mpack_gang.html

The continued concentration of Trojans in North America is likely a continuation of the trend that was reported in the previous edition of the Symantec *Internet Security Threat Report*,[94] in which it was speculated that the concentration of Trojans in North America may be indicative of enterprises and ISPs taking more active steps to prevent the propagation of worms. As a result, attackers may consciously be moving towards Trojans because of successful efforts to thwart worm attacks.

During this period, EMEA accounted for 43 percent of global potential infections caused by worms, followed by APJ at 33 percent, and North America at 18 percent (table 6). This may indicate that North American ISPs are implementing more rigid port blocking to limit the spread of network worms, as well as antivirus filtering at the email gateway to limit mass-mailing worms.

Region	Current	Previous
North America	18%	23%
EMEA	43%	36%
APJ	33%	35%
Latin America	6%	6%

Table 6. Location of worms
Source: Symantec Corporation

North America and EMEA experienced the greatest changes in the proportion of potential infections caused by worms this period. However, the change is not due to a change in the concentration of worms in North America, but from the increase in the proportion in EMEA. As noted above, the concentration of Trojans in EMEA decreased this period, which caused an increase in the proportion of reported worms in the region. For example, the Stration worm[95] was one of the top 50 malicious code samples causing potential infections in EMEA, but not in North America. However, the proportion of the volume of this worm observed in EMEA was lower than North America because of the much higher volume of Trojans in the North America region.

Potential infections caused by back doors were most frequently reported from EMEA, which accounted for 40 percent of all back doors worldwide. North America accounted for 30 percent of potential back door infections in the second half of 2007, while APJ accounted for 26 percent and Latin America accounted for four percent (table 7). It is important to note that, while the regional percentages of potential back door infections show a fairly wide variance during this period, the worldwide volume of back door threats was significantly lower than Trojans and worms. As a result, the percentage variance between regions actually represents a much smaller difference in raw numbers than the percentage differences between worms and Trojans.

[94] Symantec *Internet Security Threat Report*, Volume XII (September 2007): http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_09_2007.en-us.pdf : p. 82
[95] http://www.symantec.com/security_response/writeup.jsp?docid=2006-092111-0525-99

Region	Current	Previous
North America	30%	33%
EMEA	40%	38%
APJ	26%	24%
Latin America	4%	5%

Table 7. Location of back doors
Source: Symantec Corporation

The APJ region accounted for the highest percentage of viruses this period, with 44 percent of the total, while EMEA and North America accounted for 34 and 19 percent, respectively. Latin America only accounted for three percent of the total (table 8).

Region	Current	Previous
North America	19%	21%
EMEA	34%	27%
APJ	44%	45%
Latin America	3%	7%

Table 8. Location of viruses
Source: Symantec Corporation

The increased proportion of viruses in EMEA is linked to the proportion of worms there. Many new worms also contain a viral infection component to aid in propagation. For example, one of the top reported malicious code samples from the EMEA region this period, the Fujacks worm, also infects files on a compromised computer. Other worms causing potential infections reported in EMEA also employ a viral component, which may be a contributing factor in the proportional increase of viruses and worms from this region.

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, 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. It should be noted that threats that expose confidential information may employ more than one method to do so; as a result, cumulative percentages discussed in this metric may exceed 100 percent.

In the last six months of 2007, threats to confidential information made up 68 percent of the volume of the top 50 malicious code samples causing potential infections (figure 16). This is an increase over the 65 percent reported in the first half of 2007 and the 53 percent from the same period in 2006.

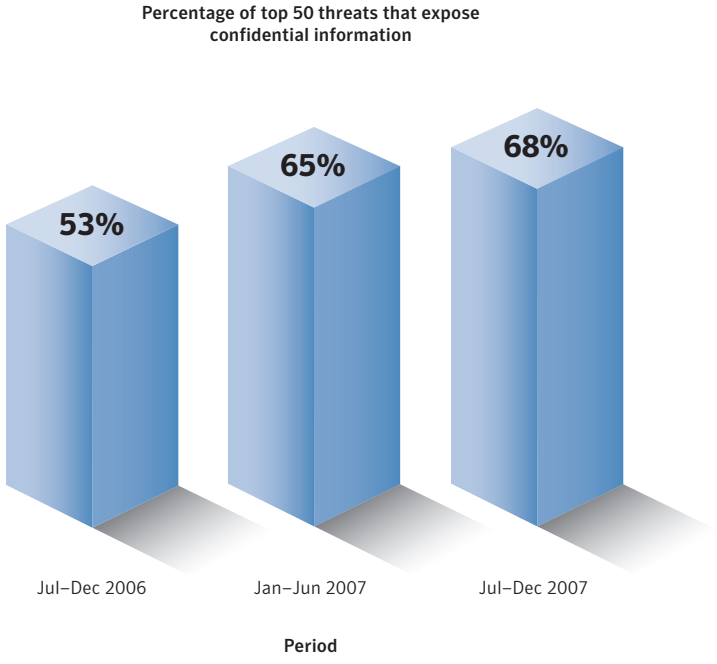

Figure 16. Threats to confidential information by volume
Source: Symantec Corporation

Malicious code can expose confidential information in a variety of ways. The most common method is by allowing remote access to the compromised computer through a back door. In this method, the attacker typically uses a specialized application to connect to the compromised computer. He or she can then perform numerous actions such as taking screenshots, changing configuration settings, and uploading, downloading, or deleting files.

In this reporting period, 86 percent of confidential information threats had a remote access component (figure 17), compared to 88 percent in the first half of 2007 and 87 percent in the last half of 2006. While this exposure type dropped slightly in the current period, it still remains more popular than other techniques. This is likely because remote access, such as a back door, gives the attacker extensive control over the compromised computer, allowing for the theft of any information on the computer, the installation of other threats, or the use of the computer for other purposes, such as relaying spam or hosting a phishing Web site.

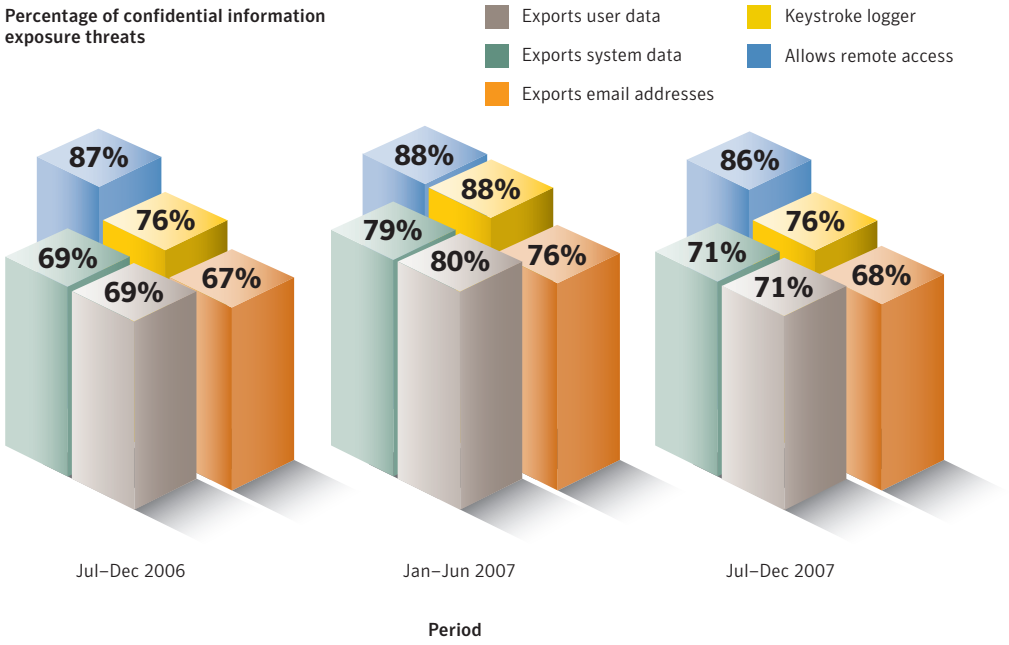

Figure 17. Threats to confidential information by type
Source: Symantec Corporation

Confidential information threats with keystroke logging capability made up 76 percent of threats to confidential information, down from 88 percent in the first six months of 2007, although 76 percent was recorded in the second half of 2006. A keystroke logger records keystrokes on a compromised computer and either emails the log to the attacker, or uploads it to a Web site under the attacker's control. The attacker can use these logs to extract the user's credentials for different types of accounts, such as online banking, trading sites, or ISP account access. The information can then be used as a stepping stone to launch further attacks. For example, the attacker could use the stolen ISP account credentials to set up a phishing site on the free hosting space typically included with these accounts.

Threats that could be employed to export user data accounted for 71 percent of confidential information threats during the last six months of 2007, down from 80 percent in the previous reporting period, but still higher than the 69 percent in the last six months of 2006. In the second half of 2007, 71 percent of threats to confidential information could be used to export system data, compared to 79 percent in the

first half of 2007 and 69 percent in the last half of 2006. These forms of data leakage can be used to steal a user's identity or launch further attacks. Attackers with access to the user's personal and system data can use it to craft a more targeted social-engineering attack tailored to that particular user.

In the first half of 2007, all of the confidential information exposure types experienced an increase as more threats employed multiple mechanisms; however, in the current reporting period all exposure types declined. This means that in the current period a greater percentage of threats only employed one or two mechanisms. This may be a result of attackers attempting to produce more specialized confidential information threats that target specific information. A threat that employs fewer exposure mechanisms will typically be smaller in size than one that employs more. Smaller threats leave less of a footprint on the resources of the compromised computer and may remain unnoticed for a longer period of time.

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 will require that sufficient computing resources be made available, as encrypting and decrypting the data for business use consumes processing cycles on servers. Furthermore, encrypting stored data will not protect against man-in-the-middle attacks that intercept data before it is encrypted.[96] 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. The samples are assessed according to the percentage of potential infections. Readers should note that some malicious code samples use more than one mechanism to propagate, which may cause cumulative percentages presented in this discussion to exceed 100 percent.

In the second half of 2007, 40 percent of malicious code that propagated did so as shared executable files (table 9), a significant increase from 14 percent in the first half of 2007. Shared executable files are the propagation mechanism employed by viruses and some worms that copy themselves to removable media. As stated in the "Malicious code types" section above, the increasing use of USB drives and media players has resulted in a resurgence of malicious code that propagates through this vector.

This vector lost popularity among malicious code authors when the use of floppy disks declined and attackers instead concentrated on other more widely used file transfer mechanisms such as email and shared network drives. However, as use of removable drives has become more widespread, attackers have again begun to employ this propagation technique. Although current removable drives differ from floppy disks, the principle remains the same, enabling attackers to make simple modifications to old propagation techniques.

[96] A "man-in-the-middle attack" is a form of 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. This can allow the attacker to intercept communications on a secure or encrypted channel.

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, endpoint security and policy can prevent computers from recognizing these drives when they are attached. Additionally, policy and user education should be implemented to prevent users from attaching unauthorized devices to computers within the enterprise.

Rank	Propagation Mechanism	Current	Previous
1	File sharing executables	40%	14%
2	File transfer/email attachment	32%	30%
3	File transfer/CIFS	28%	15%
4	File sharing/P2P	19%	20%
5	Remotely exploitable vulnerability	17%	12%
6	SQL	3%	<1%
7	Back door/Kuang2	3%	2%
8	Back door/SubSeven	3%	2%
9	File transfer/embedded HTTP URI/Yahoo! Messenger	2%	<1%
10	Web	1%	1%

Table 9. Propagation mechanisms
Source: Symantec Corporation

In the last six months of 2007, 32 percent of malicious code that propagated did so in email attachments. While the percentage increased slightly over the 30 percent in the first six months of 2007, executable file sharing overtook this vector, as previously noted. The previous edition of the Symantec *Internet Security Threat Report*[97] noted that this is likely due to diversification of malicious code authors, although email attachments still remain an attractive propagation mechanism for malicious code because of the pervasive use of email.

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 downloaded from Web sites 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 Common Internet File Sharing (CIFS) protocol[98] made up 28 percent of malicious code that propagated in the second half of 2007, an increase over the 15 percent in the previous period. As noted in the previous version of the Symantec *Internet Security Threat Report*,[99] this propagation vector was employed by samples such as Fujacks, which remains one of the top three malicious code samples causing potential infections.

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.

[97] Symantec *Internet Security Threat Report*, Volume XII (September 2007): http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_09_2007.en-us.pdf : p. 85
[98] 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.
[99] Symantec *Internet Security Threat Report*, Volume XII (September 2007): http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_09_2007.en-us.pdf : p. 86

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.

Malicious code using peer-to-peer (P2P) protocols to propagate accounted for 19 percent of all potential infections this period. Since there are a wide variety of P2P protocols available for malicious code to use as propagation mechanisms, they have been further broken down by protocol in the discussion that follows.

The most frequently used methods of P2P propagation employed by malicious code this period did not attempt to use a specific P2P protocol to propagate; rather, they copied themselves to all folders on a computer containing the character string "shar". P2P applications commonly create folders containing the word "share"—such as "shared folder"—so these malicious code samples will successfully propagate through many of them. These threats accounted for 66 percent of all P2P threats this period (table 10).

Rank	Peer-to-Peer Protocol/Method	Percentage of P2P
1	File sharing/P2P/shared directories	66%
2	File sharing/P2P/Kazaa	60%
3	File sharing/P2P/eDonkey	46%
4	File sharing/P2P/Morpheus	46%
5	File sharing/P2P/Winny	14%

Table 10. P2P propagation mechanisms
Source: Symantec Corporation

The Kazaa file-sharing service was used by 60 percent of malicious code samples that propagated through P2P networks, while Morpheus and eDonkey were each used by 46 percent. Finally, the Winny protocol was used by 14 percent of malicious code propagating through various P2P protocols this period.

Since P2P applications are typically not permitted on corporate networks, any P2P clients are likely installed without the knowledge or consent of network administrators. Enterprises should take measures to prevent P2P clients from being installed on any computers on the network. They should also block any ports used by these applications at the network boundary. End users who download files from P2P networks should scan all such files with a regularly updated antivirus product.

Malicious code that modifies Web pages

In late May, 2007, the MPack[100] attack kit was first observed in the wild. This kit relied on compromised Web pages to redirect users to an MPack server that attempted to exploit Web browser and plug-in vulnerabilities in order to install malicious code on computers. This kit experienced great success because it took advantage of the trust many users place in certain Web sites. Since the Web browser is the primary gateway to the Internet for most users, Web pages that they visit frequently—such as online forums and other Internet communities—are a useful means of compromising computers for attackers. This method of shotgun attacks is described in more detail in the "Vulnerability Trends" section of this report.

For the first time in this edition of the Symantec *Global Internet Security Threat Report*, Symantec is examining malicious code samples that modify Web pages on a compromised computer. Only threats that modify pages in order to propagate or redirect users were examined. Those that simply deface the pages by adding text or simple images are not included in this metric.

In the last six months of 2007, seven percent of the volume of the top 50 malicious code samples modified Web pages, up from three percent in the first half of the year (figure 18). In the second half of 2006, none of the top 50 malicious code samples attempted to modify Web pages on the compromised computer. It is likely that the success of threats like the MPack kit has encouraged attackers to use Web pages to install malicious code in recent months.

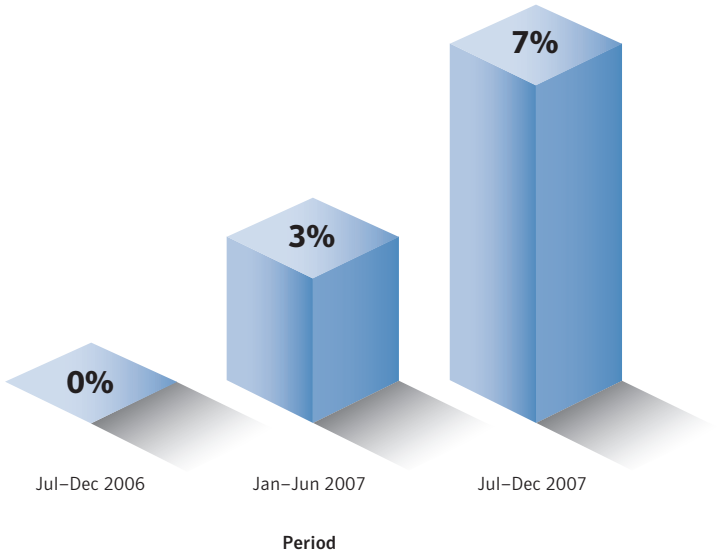

Figure 18. Malicious code that modifies Web pages
Source: Symantec Corporation

[100] http://www.symantec.com/business/security_response/writeup.jsp?docid=2007-052712-1531-99

There were two common themes to the top malicious code samples that modified Web pages this period. The first was threats that added their own code to Web pages, like the Invadesys worm. When a user visits a Web page infected by this worm, it will attempt to execute its code on the computer when the Web browser renders the page. Since the worm is written in Visual Basic script, it is a format that browsers can interpret and execute, which in turn infects the visiting user.

The other common method of modifying Web pages this period was to add an iframe tag to the page. 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. An iframe can be invisible and the user will not see any of the embedded content when viewing the original page. The Fujacks worm[101] employs this method to redirect the user's browser to a malicious Web site. This site can then exploit vulnerabilities in the user's browser to download and install further threats.

In many cases, the Web pages modified by malicious code do not reside on Web servers. However, if users maintain their own sites, it is likely that they would keep a copy of the site on their own computers and upload pages to their hosting providers whenever they make updates. When the updated pages are uploaded, they would likely include the modifications made by the malicious code. As a result, other users who trust the compromised sites would be at risk. This could be particularly harmful if the compromised user maintains a popular software application because a greater number of users are likely to visit the site. Additionally, an enterprise employee responsible for maintaining pages on a public-facing Web site who becomes infected by one of these threats may unknowingly upload malicious pages. This could significantly harm the reputation of the affected organization.

When mass-mailing worms dominated the top malicious code samples, users' email address books mainly determined their circle of contacts. While this is still the case, users also now frequently keep in contact with friends, family, and associates through personal Web sites and social networking sites. In many cases, users' social networking profiles will also link to their personal Web site. Since many sites incorporate dynamic content that requires a certain trust level in the user's browser in order to render correctly, this can also allow malicious content to execute through the browser.

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 as it illustrates the need for administrators to apply patches in a timely manner. During the second half of 2007, 10 percent of the 1,032 documented malicious code instances exploited vulnerabilities (figure 19).[102] This is lower than the 18 percent proportion of the 1,509 malicious code instances documented in the first half of 2007. While the number of new samples exploiting vulnerabilities declined in the current reporting period, this method of propagation remains effective, as is illustrated by its presence in the top 10 propagation mechanisms, discussed above.

[101] http://www.symantec.com/security_response/writeup.jsp?docid=2007-010509-0134-99
[102] 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.

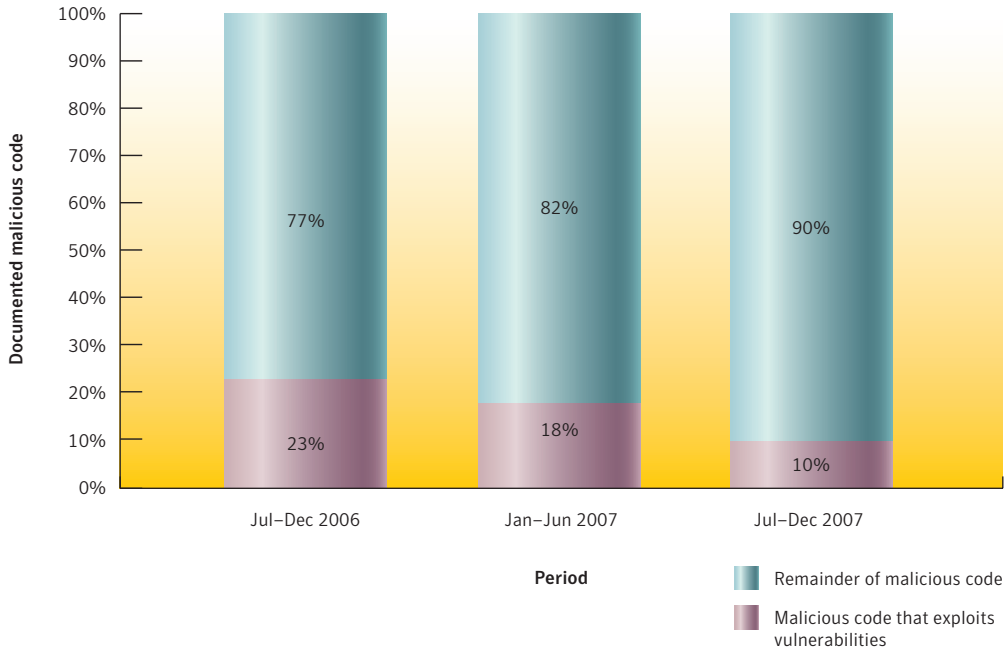

Figure 19. Malicious code that exploits vulnerabilities
Source: Symantec Corporation

The decline in the number of malicious code samples exploiting vulnerabilities may be related to the increasing use of the Web to install malicious code on computers. For example, the number of site-specific cross-site scripting vulnerabilities is increasing, as is noted in the "Vulnerability Trends" section of this report. These vulnerabilities can be used to install malicious code on the computers of users visiting the affected Web sites. Since the vulnerability affects the Web site itself and the exploit is not a component of the malicious code sample, those samples will not be counted as malicious code that exploits vulnerabilities.

While the number of malicious code samples exploiting vulnerabilities has dropped, it is important to note that the Pidief Trojan,[103] one of the top 10 new malicious code families this period, exploits a vulnerability in Adobe Acrobat to execute its code.[104] The Trojan arrives as a portable document format (PDF) file that exploits the vulnerability to execute the Trojan's code when the document is viewed on a computer running a vulnerable version of the software. This Trojan also disables the Windows firewall and downloads and executes additional threats on the computer.

This illustrates that even though there are fewer new malicious code samples exploiting vulnerabilities, they can still have success in compromising unpatched computers. As well, while fewer new malicious code samples exploit vulnerabilities in operating systems, popular third-party client-side applications are still a viable target for malicious code. Users should avoid becoming complacent and ensure that they patch vulnerabilities in affected software when fixes become available. Intrusion prevention systems and antivirus software can help protect against malicious code that exploits vulnerabilities for which no patch is available.

[103] http://www.symantec.com/security_response/writeup.jsp?docid=2007-102310-3513-99
[104] http://www.securityfocus.com/bid/25748

Staged downloaders—multiple infections by type

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

In the second half of 2007, the most prevalent downloader component was the Vundo Trojan (table 11).[105] 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. This adware program likely generates revenue for the malicious code author.

Rank	Sample	Type	Download Mechanism
1	Vundo	Trojan	Redirects browser to malicious Web page
2	Zlob	Trojan	Downloads files from remote addresses
3	Metajuan	Trojan	Downloads files from remote addresses
4	Pandex	Trojan	Downloads files from remote addresses
5	Fujacks	Worm/virus	Downloads files from remote addresses
6	Stration	Worm	Downloads files from remote addresses
7	Nebuler	Trojan	Downloads files from remote addresses
8	Skintrim	Trojan	Downloads files from remote addresses
9	Linkoptimizer	Trojan	Downloads files from remote addresses
10	Svich	Worm	Downloads files from remote addresses

Table 11. Top 10 staged downloaders
Source: Symantec Corporation

The Zlob Trojan[106] was the second most common staged downloader in the current period. This Trojan sets the user's Internet Explorer home, search, and "not found" pages to Web pages hosting malicious code. It also periodically displays fake security alerts that claim that the computer is infected. When users click the error messages, they will be directed to a Web page hosting malicious code.

Metajuan[107] was the third most common staged downloader in the second half of 2007. This Trojan attempts to contact a remote Web site and downloads and installs other threats from it. The Trojan may also display advertisements when the user visits certain Web sites, likely in an effort to provide revenue for the malicious code author.

The most prevalent downloaded component in the second half of 2007 was the Adclicker Trojan (table 12).[108] This simple Trojan is intended to drive traffic to Web pages and banner advertisements. Banner advertisements compensate the owner of the Web site they are hosted on for each view or click-through.[109] Generating fraudulent traffic to these advertisements is commonly referred to as click fraud.

[105] http://www.symantec.com/security_response/writeup.jsp?docid=2004-112111-3912-99
[106] http://www.symantec.com/security_response/writeup.jsp?docid=2005-042316-2917-99
[107] http://www.symantec.com/security_response/writeup.jsp?docid=2007-030112-0714-99
[108] http://www.symantec.com/security_response/writeup.jsp?docid=2002-091214-5754-99
[109] 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.

Rank	Sample	Type	Impact
1	Adclicker	Trojan	Generates traffic to Web sites and banner ads
2	Graybird	Back door	Allows remote access, logs keystrokes, and steals passwords
3	Lineage	Trojan	Steals online gaming account information
4	Formador	Back door	Allows remote access, logs keystrokes, and steals passwords
5	Gamania	Trojan	Steals online gaming account information
6	LowZones	Trojan	Lowers Internet Explorer security settings
7	KillAV	Trojan	Disables security applications
8	SpamThru	Trojan	Relays spam email messages
9	Bancos	Trojan	Steals online banking account information
10	Anserin	Trojan	Logs keystrokes and steals online banking account information

Table 12. Top 10 downloaded components
Source: Symantec Corporation

Graybird[110] was the second most frequently downloaded component this period. This back door gives an attacker full remote access to the compromised computer. It also steals cached passwords and logs keystrokes, and sends this information to the remote attacker. Further, Graybird allows the attacker to download and install additional threats on the computer.

The third most commonly downloaded component this period was the Lineage Trojan.[111] This Trojan steals account information for the Lineage online game and emails it to the attacker. This account information can be sold to other users or the attacker can sell individual game items from the account.

Malicious code—protection and mitigation

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 ASLR.

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.

[110] http://www.symantec.com/security_response/writeup.jsp?docid=2003-040217-2506-99
[111] http://www.symantec.com/security_response/writeup.jsp?docid=2005-011211-3355-99

Phishing 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, usually well-known brand, usually 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.

Symantec assesses phishing according to two indicators: phishing attempts and phishing messages. A phishing attempt can be defined as an instance of a phishing message being sent to a single user. Extending the fishing analogy, a phishing attempt can be considered a single cast of the lure (the phishing message) to try to catch a target. A single phishing message can be used in numerous distinct phishing attempts, usually targeting different end users.

A phishing Web site is a site that is designed to mimic the legitimate Web site of the organization whose brand is being spoofed. In many cases, it is set up by the attacker to capture a victim's authentication information or other personal identification information, which can then be used in identity theft or other fraudulent activity.

This section will discuss selected phishing metrics in greater depth, providing analysis and discussion of the data gathered by Symantec between July 1 and December 31, 2007. The following metrics will be discussed:

- Phishing activity by sector
- Top countries hosting phishing Web sites and top targets phished
- Phishing site top-level domains
- Phishing Web site hosts
- Automated phishing toolkits
- Phishing—protection and mitigation

Phishing activity by sector

This section will explore phishing activity in two ways. First it will analyze the unique brands phished by their sector, which looks at only the number of brands used and their corresponding sectors that were phished, and not each specific phishing attack. Second, it will explore which sectors were targeted by the highest volume of phishing attacks. These considerations are important for an enterprise because the use of its brand in phishing activity can significantly undermine consumer confidence in its reputation.

The majority of brands used in phishing attacks in the last six months of 2007 were in the financial services sector, accounting for 80 percent (figure 20), virtually unchanged from the 79 percent reported in the previous period. The financial services sector also accounted for the highest volume of phishing Web sites during this period, at 66 percent (figure 21), down from 72 percent in the first half of 2007. Since most phishing activity pursues financial gain, successful attacks using brands in this sector are most likely to yield profitable data, such as bank account credentials, making this sector an obvious focus for attacks.

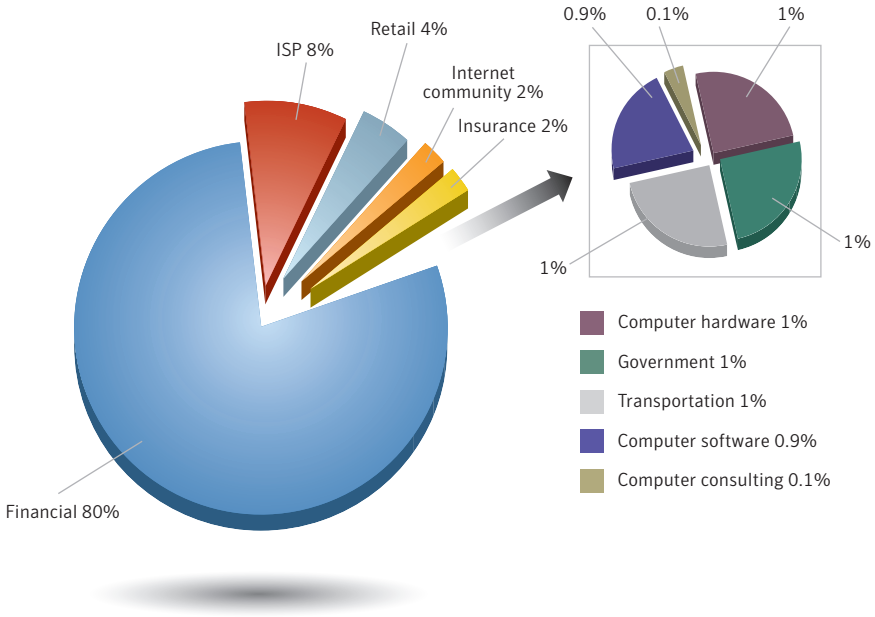

Figure 20. Unique brands phished by sector
Source: Symantec Corporation

The drop in volume of phishing Web sites targeting financial organizations during the period is worth noting. The drop is potentially driven by the increased knowledge and awareness of phishing schemes, and how to avoid falling victim to them. Information campaigns driven by financial institutions, as well as warning emails and a general heightened awareness of phishing schemes targeting financial services has likely made it more difficult for phishers to carry out successful phishing attacks against them.

Internet service providers (ISPs) were ranked second in unique brands used in phishing attacks during this period, at eight percent. This is a slight decrease from 11 percent in the first half of 2007. The ISP sector also accounted for the second highest volume of phishing attacks during the period, accounting for 18 percent.

As noted in previous editions of the Symantec *Internet Security Threat Report*,[112] ISP 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.[113] This information may provide access to other accounts, such as online banking.

Additionally, attackers could use the free Web-hosting space often included in these accounts to put up phishing sites, 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. Also, compromised Web space can be used to plant links to other sites the attacker controls in order to boost the search engine rankings of those sites.

[112] Symantec *Internet Security Threat Report*, Volume XI (March 2007): http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf : p. 69
[113] http://cups.cs.cmu.edu/soups/2006/proceedings/p44_gaw.pdf

Not coincidentally, email account passwords rank in the top 10 most common items advertised for sale on underground economy servers this period, as described in the "Underground economy servers" discussion in the "Attack Trends" section of this report.

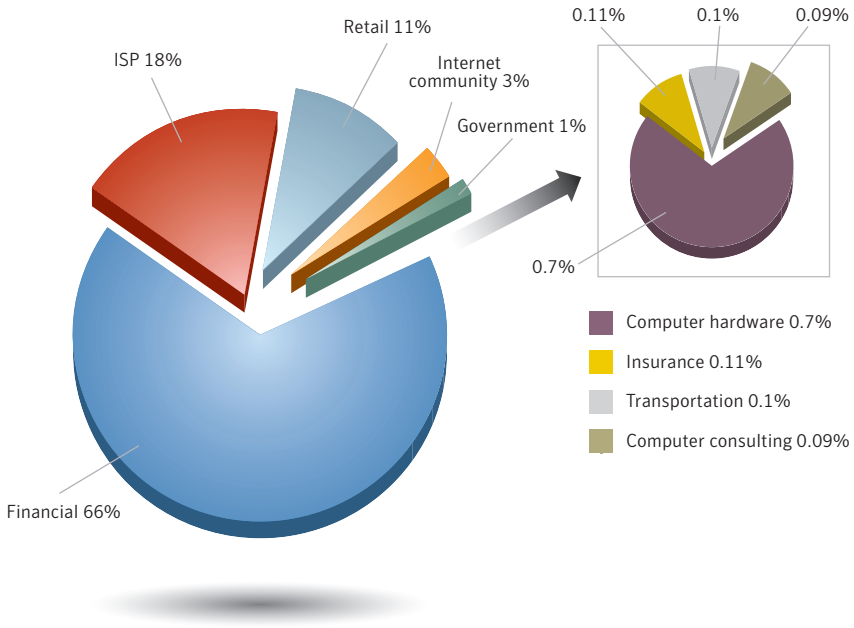

Figure 21. Phished sectors by volume of phishing Web sites
Source: Symantec Corporation

The retail services sector accounted for four percent of organizations whose brands were spoofed by phishing attacks in the second half of 2007, and for 11 percent of the volume of phishing Web sites. In the previous reporting period, the retail sector accounted for three percent of the unique brands spoofed and 16 percent of the volume. This represents a continuing trend towards a shrinking gap between brands phished and the volume of phishing Web sites targeting this sector.

The higher number of Web sites used to carry out attacks spoofing retail brands during previous periods was likely part of an exploratory phase for phishers to establish the value of successful phishing attacks targeting organizations in this sector. The shrinking gap between brands phished and the volume of phishing Web sites, which is driven by a drop in the volume of phishing Web sites, indicates an end to this exploratory phase. As the possible financial gains of spoofing retail organizations are established, phishers will adjust their rate of attacks accordingly.

Also, the drop in the volume of attacks may be because successful phishing attacks that spoof retail organizations may require more effort on the attacker's behalf to achieve financial gain compared to the financial sector, and therefore may be less profitable. A phisher gaining access to bank account information simply has to cash out the account to get at the funds, while having access to online retailer accounts may require goods to be shipped to a physical address and involve more risk of discovery for the attacker.

Six of the top 10 brands spoofed by attackers in phishing attacks during this period were in the financial sector. Interestingly, the second most frequently spoofed brand was a social networking site.[114] While there may seem to be no immediate financial gain from stealing account information from a social networking site, attackers could use the compromised account to gather detailed information about the user and the user's friends.[115] Furthermore, many social networking sites allow their users to control the content of their associated site, which would allow an attacker that has compromised such a site to host seemingly legitimate links that point to malicious Web sites, to host malicious code, to spam users associated with the compromised account, and to even host phishing Web sites.[116] Using a compromised social networking site account to host a phishing Web site that targets the social networking site itself will increase the chances of such an attack at being successful.

Top countries hosting phishing Web sites and top targets phished

This metric will assess the countries in which the most phishing Web sites were hosted and the most popular targets within each country. Phishing Web sites differ from phishing hosts, which are computers that can host one or more phishing Web sites, and which are discussed in the "Phishing activity by sector" metric above, as well as in the "Malicious activity by country" metric in the "Attack Trends" section of this report. This data is a snapshot in time, and does not offer insight into changes in the locations of certain phishing sites since the data was analyzed. It should also be noted that the fact that a phishing Web site is hosted in a certain country does not necessarily mean that the site is being controlled by attackers located in that country.

In the second half of 2007, 66 percent of all phishing attacks detected by Symantec were associated with Web sites located in the United States (table 13). For phishing attacks with Web sites hosted in the United States, all of the top 10 targets are also headquartered there. The top target phished on Web sites hosted in the United States was a social networking site. Together with another social networking site, these two sites accounted for 91 percent of phishing attacks with Web sites hosted in the United States. Of the remaining top 10 targets phished in the United States, four were financial services, though they only accounted for three percent of phishing attacks with Web sites hosted in the United States. Since the majority of phishing attacks that were detected were associated with Web sites that spoof social networking sites, it is plausible to assume that phishing these is more lucrative than phishing financial organizations, as discussed previously in "Phishing activity by sector."

[114] For more on phishing attacks that target social networking sites, please see: http://www.symantec.com/enterprise/security_response/weblog/2006/09/contextaware_phishing_realized.html
[115] http://www.symantec.com/enterprise/security_response/weblog/2006/11/an_imaginative_phishing_attack_1.html
[116] http://blog.washingtonpost.com/securityfix/2007/06/web_2pointuhoh_worm_whacks_mys.html

Rank	Country	Percentage	Top Target Phished
1	United States	66%	Social networking site
2	China	14%	Social networking site
3	Romania	5%	Social networking site
4	Guam	5%	Social networking site
5	France	1%	Online auction site
6	Germany	1%	Online payment system
7	Italy	1%	Online auction site
8	Canada	1%	Online portal
9	Sweden	1%	Telecommunications provider
10	Netherlands	1%	Social networking site

Table 13. Top countries hosting phishing Web sites and top targets phished
Source: Symantec Corporation

During the last six months of 2007, China hosted the second most phishing Web sites, with 14 percent of the total. The top target phished by Web sites hosted in China was the same social networking site most commonly phished by Web sites in the United States, accounting for 96 percent of phishing Web sites hosted in China. The second ranked target of phishing Web sites hosted in China was a popular Chinese online retailer; despite ranking second, it accounted for only one percent of the phishing Web sites there.

Of the top 10 targets phished by Web sites hosted in China, seven had head offices in the United States. These seven accounted for 98 percent of the phishing sites in China. The other three targets phished by hosts in China were organizations with head offices in China, although all three also operate internationally. The focus on phishing targets based in the United States shows that these organizations are a lucrative target for phishers who host their sites on computers in China. This could mean that phishers hosting sites in China are actually located in the United States, as stolen information would be easier for people in the United States to use. For example, cashing out a U.S. bank account could be done more easily and without arousing as much suspicion from a location within the United States than would cashing out the bank account from China. Because banks monitor spending activities on bank accounts to detect fraudulent activity, withdrawing money from a U.S. bank account from a location in China is more likely to be flagged and blocked than would withdrawing money from the same bank account from a location in the United States.

Furthermore, it is possible that phishing Web sites in China may be left in place for longer periods, making hosting a site there more desirable. China has the second highest amount of malicious activity worldwide, as is discussed in the “Attack Trends” section of this report. Therefore, it is reasonable to assume that phishers have an easier time hosting and maintaining their phishing sites there. It could also be that the stolen information is being sold in the underground economy, meaning that the phishers hosting sites on computers in China are simply stealing the most profitable information and are not necessarily located in the United States.

Romania ranked third for phishing Web sites during the period, accounting for five percent of all phishing Web sites detected. The prominence of Romania for phishing Web sites is indicative of the amount of Internet-fraud related activity originating there. Romania is not only prominent in phishing activity, but it ranks high (relative to its population) in various other forms of Internet-related fraud, including online auction fraud.[117] It has been speculated that the prominence of Romania in Internet fraud as well as other malicious activity is related to the culture surrounding computers there. In the social and intellectual climate in Romania, computer knowledge is viewed as very desirable and has been since the country was a satellite of the Soviet Union.[118] As a consequence, a high proportion of computer users in Romania are technically knowledgeable and, thus, there exists the likelihood that a higher number of users there could be using their knowledge for malicious activity.

The same social networking site that was most commonly targeted in the United States and China was also the most common target of phishing attacked with sites hosted on computers in Romania, accounting for 98 percent of the total. Seven of the top 10 targets phished in Romania during this period were organizations with head offices in the United States, three of which were financial services organizations. An Italian ISP and a bank in the United Kingdom were also among the targets spoofed by Web sites hosted on computers in Romania.

Phishing site top-level domains

For the first time, this volume of the Symantec *Global Internet Security Threat Report* will discuss top-level domains (TLDs) associated with all phishing Web sites detected by Symantec.[119] This discussion is important because it illustrates the TLDs that are the most commonly used in phishing attacks, beneficial in aiding phishing attacks, and easily used by phishers.

The most common TLD used in phishing Web sites between July 1 and December 31, 2007 was .com, accounting for 44 percent of the total (table 14). This is not surprising for a number of reasons. Phishers not only benefit from its familiarity, but since it is the most common TLD overall,[120] it is natural that it is also the most commonly used TLD for phishing Web sites. The .com domain is also unrestricted and is available to anyone who wishes to register a .com domain name, making it easy for phishers to register these domains.

Rank	Top-level Domain	Description	Percentage
1	.com	Unrestricted commercial	44%
2	.cn	China	23%
3	.net	Unrestricted	6%
4	.org	Unrestricted	3%
5	.de	Germany	2%
6	.ru	Russia	2%
7	.fr	France	1%
8	.co.uk	United Kingdom commercial	1%
9	.info	Unrestricted	1%
10	.es	Spain	1%

Table 14. Top 10 phishing site top-level domains
Source: Symantec Corporation

[117] http://www.ic3.gov/crimeschemes.aspx#item-2
[118] http://www.cbsnews.com/stories/2003/10/20/tech/main578965.shtml
[119] In a domain name, the top-level domain is the part that is furthest to the right. For example, the ".com" in symantec.com. There are two types of top-level domains: generic and country specific. Examples of generic domains are .com, .net, and .org, while country-specific top-level domains include .cn for China, and .uk for the United Kingdom, as well as others.
[120] http://www.verisign.com/static/043379.pdf

The second most commonly used TLD by phishing Web sites was .cn, accounting for 23 percent of the total. Although .cn was originally restricted to domain names registered in China, it has since been made available internationally.[121] The prominence of .cn is not surprising due to its prevalence in China. China has ranked consistently high in the past two years for hosting phishing Web sites, for housing active bot-infected computers, and for originating attacks. It has also ranked second for overall malicious activity for the past year, as is discussed in the "Attack Trends" section of this report. It is likely that, because China has such high levels of malicious activity in general, phishers have an easier time attaining and maintaining phishing Web sites in the country.

The third most common TLD used by phishing Web sites during this reporting period was .net, which accounted for only six percent of the total. Compared to both the .com and .cn top-level domains, the percentage of phishing sites using .net is quite low. The ranking of .net is likely attributable to two factors. First, it is one of the most common TLDs,[122] and phishers may use it because it is well known and relatively unsuspicious. Second, it is also unrestricted, making it easy for phishers to register domain names with it.

Phishing Web site hosts

For the first time, this volume of the Symantec *Global Internet Security Threat Report* will be discussing the volume of distinct phishing Web site hosts observed by Symantec. A phishing Web site host is a computer that is identified to have been hosting one or more phishing Web sites during the period. Some phishing hosts may host numerous different phishing Web sites; however, these hosts are counted only once for the purpose of this discussion. This consideration is important because it allows Symantec to gauge and understand increases or decreases in phishing activity.

Between July 1, 2007 and December 31, 2007, Symantec observed 87,963 phishing hosts (figure 22). This is an increase of 167 percent from the first half of 2007, when Symantec detected only 32,939 phishing Web site hosts. Between the second half of 2006, when 13,353 phishing Web site hosts were detected, and the second half of 2007, Symantec observed a dramatic increase of 559 percent in phishing Web site hosts.

[121] http://www.neulevel.cn/
[122] http://www.icannwiki.org/Domain_Statistics

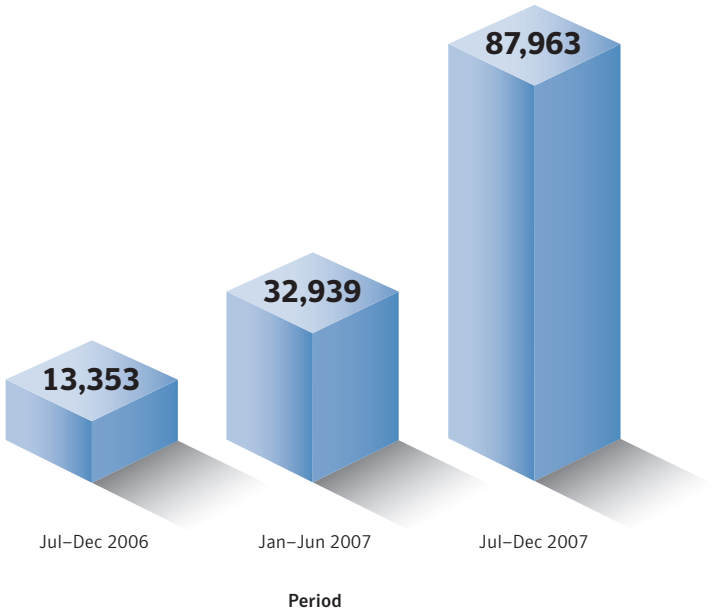

Figure 22. Phishing Web site hosts
Source: Symantec Corporation

There are several factors contributing to this increasing trend that Symantec is observing. Along with the growth in availability and adaptability of phishing toolkits that allow phishers to work faster with greater efficiency, the adoption of fast-flux botnet communication infrastructure in botnets has also facilitated the growth in the number of phishing Web site hosts. Fast-flux basically allows a single URL to resolve to a number of different IP addresses, or computers, by changing the DNS mapping of the URL rapidly and constantly. In other words, a single URL can be used to point to a number of different computers at different times. This functionality has allowed phishers to host phishing Web sites across a botnet. Through fast-flux, when one phishing Web host is blocked or taken down, the attacker can change the DNS entry so that the URL will point to a different computer that has not been blocked or taken down, but that is hosting the same phishing Web page, allowing the phisher to carry out phishing attacks for longer periods. This is a major contributor to the rise in phishing Web site hosts over the past year.

Phishing toolkits have also allowed phishers to carry out phishing attacks much more easily by automating the construction of a phishing Web site; attackers can concentrate on identifying and procuring phishing Web site hosts instead of the tedious job of building phishing Web sites from by hand. The adoption of phishing Web site toolkits is a prominent trend, as noted in the “Automated phishing toolkits” discussion on the next page. During this period, the top three phishing toolkits accounted for 26 percent of all phishing attacks, whereas the top three toolkits accounted for 42 percent in the previous period. The indication is that, because the top three toolkits did not dominate as much this period, there are more toolkits sharing the workload, which highlights the widespread adoption of toolkits as a valuable tool for malicious activity. Consequently, carrying out phishing attacks and deploying phishing Web sites has become easier and is facilitating the growth in phishing Web site hosts.

Overall, since phishing is a financially lucrative type of attack, Symantec predicts that the number of phishing Web site hosts will continue to rise until effective means of countering them are put in place. Furthermore, as the adoption of fast-flux type communication schemes continues to grow, so will the number of phishing Web site hosts.

Automated phishing toolkits

A phishing toolkit is a set of scripts that allows an attacker to automatically set up phishing Web sites that spoof the legitimate Web sites 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, 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 and are sold in the underground economy. As such, they illustrate the trend that Symantec has observed towards an increase in the commercialization of the development and distribution of threats and malicious services. This trend also indicates that phishing is an organized and commercial activity. Toolkits sold on the underground economy often go unnamed. Unlike legitimate software, where naming plays a large role in marketing the product, phishing toolkits often become popular based on who has produced them. As a consequence, phishing toolkits discussed here cannot be named specifically.

Three phishing toolkits were responsible for 26 percent of all phishing attacks observed by Symantec in the second half of 2007 (figure 23). This is a decrease from the first half of 2007, when three phishing toolkits were responsible for 42 percent of all phishing attacks. Furthermore, two of the three most prevalent phishing toolkits from the first half of 2007 were no longer commonly used in the second half of the year and, as such, are not discussed here. This is one indication that the popularity of phishing toolkits changes quickly.

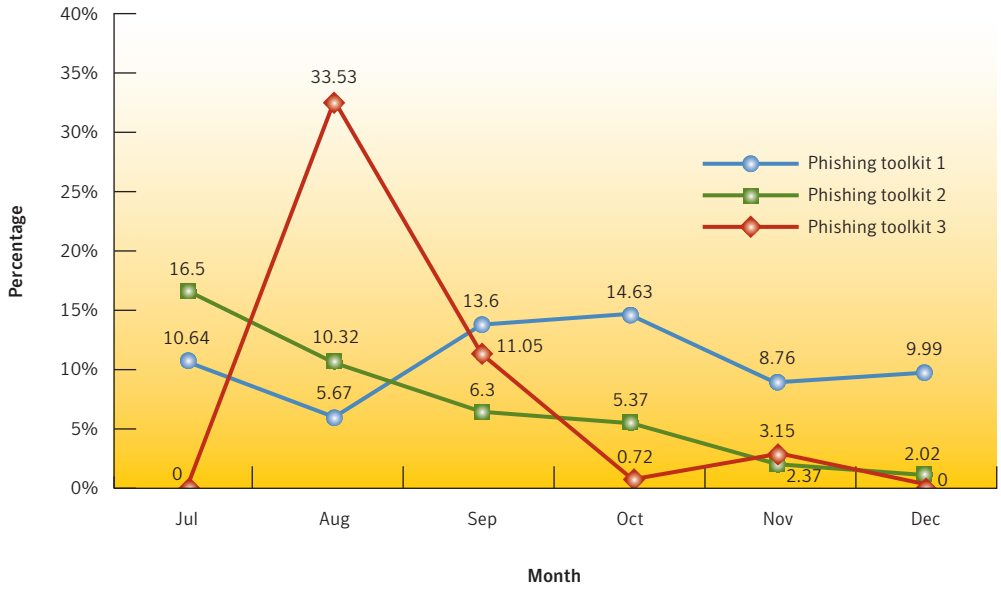

Figure 23. Use of automated phishing toolkits
Source: Symantec Corporation

The rapid change in preferred toolkits is likely driven by a need for phishers to adapt and constantly change the toolkits they use to avoid detection by antiphishing software. This is likely the driving factor behind the dramatic upward spike and subsequent decline of Phishing toolkit 3 during this period. Its drop in popularity between August and October likely indicates that the phishing kit was identified by antiphishing software, and so it became ineffective and had to be replaced. This also indicates that the number of toolkits is increasing and that attackers are using a greater number of different toolkits, resulting in the total amount of attacks being distributed over more toolkits.

The results still indicate a high percentage of automation used in phishing attacks, which allows attackers to quickly set up a fraudulent Web site and to send a high volume of phishing messages that spoof several brands to a large number of recipients with minimal effort. Being able to deploy a large number of phishing Web sites increases an attacker's chances of a successful attack. It is also likely that as the awareness around phishing grows, phishing attacks will become less successful, forcing phishers to deploy more Web sites to remain successful. Of the remaining attacks, some did use phishing toolkits other than the three most prevalent ones, while others used techniques other than phishing toolkits.

Phishing—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.[123] 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.[124]

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.[125] They should also keep their employees notified of the latest phishing attacks and how to avoid falling victim to them, as well as provide a means to report suspected phishing sites.[126]

Organizations can also employ Web-server log monitoring to track if and when complete downloads of their Web sites, logos, and images are occurring. Such activity may indicate that someone is attempting to use the legitimate Web site to create an illegitimate Web site 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.[127] So-called typo domains[128] and homographic domains[129] should also be monitored. 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.

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.[130] Additionally, network administrators can review Web proxy logs to determine if any users have visited known phishing sites.

[123] 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.
[124] 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.
[125] For instance, the United States Federal Trade Commission has published some basic guidelines on how to avoid phishing. They are available at: http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.htm
[126] A good resource for information on the latest phishing threats can be found at: http://www.antiphishing.org
[127] "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.
[128] 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".
[129] 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".
[130] http://www.fbi.gov/majcases/fraud/internetschemes.htm

Spam Trends

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 as it can be used to deliver Trojans, viruses, and phishing attempts.[131] It could also cause a loss of service or degradation in the performance of network resources and email gateways. This section of the Symantec *Global Internet Security Threat Report* will discuss developments in spam activity between July 1 and December 31, 2007.

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 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, the Probe Network is continuously optimized in order to attract new varieties of spam attacks.

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

- Top spam categories
- Top countries of spam origin

Top spam categories

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 the first half of 2007 was related to commercial products, which made up 27 percent of all spam detected by Symantec sensors, an increase from the 22 percent detected in the previous period (figure 24). Commercial products spam usually consists of advertisements for commercial goods and services. It is frequently used to sell designer goods, such as watches, handbags, and sunglasses, the profits from which can be substantial given that the goods sold are often cheaply-made counterfeits. In other cases the spammers may simply be attempting to collect credit card and personal information for use in identity theft.

[131] http://news.bbc.co.uk/2/hi/technology/6676819.stm

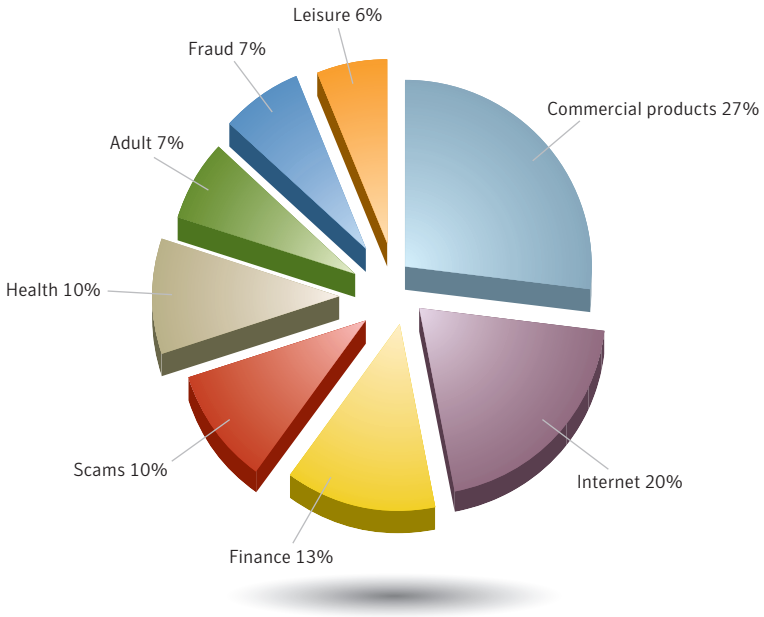

Figure 24. Top spam categories
Source: Symantec Corporation

Internet-related spam rose to 20 percent this period, from 17 percent in the first half of 2007. This type of spam is typically used to promote Web hosting and design, as well as other online commodities like phishing and spam toolkits. Since phishing and spam toolkits cannot typically be advertised by legitimate means, such as through banner ads on Web sites, spam tends to be the only way to promote them. Along with the more common use of phishing toolkits, this can account for the increase in Internet-related spam.

Spam related to financial services made up 13 percent of all spam detected in the last six months of 2007, making it the third most common type of spam during this period. This continues a decline first observed in the first six months of 2007, when it ranked second and accounted for 21 percent of all spam detected. This was driven by the continuing decline in stock market pump-and-dump spam.[132] The drop in pump-and-dump spam was triggered by actions taken by the U.S. Securities and Exchange Commission, which limited the profitability of this type of spam by suspending trading of the touted stocks.[133]

Top countries of spam origin

This section will discuss the top 10 countries of spam origin. 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 allows 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.

[132] For further discussion on pump-and-dump spam, please see the Symantec *Internet Security Threat Report* Volume XII (September 2007): http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_09_2007.en-us.pdf : p. 107
[133] http://www.sec.gov/news/press/2007/2007-34.htm

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.

During the second half of 2007, 42 percent of all spam originated in the United States (table 15), a decrease from 50 percent in the previous period. Despite the decrease, the United States had an eight percent increase in volume of spam messages. The drop in percentage from the United States can be explained by the increase in volume of spam originating in other countries, namely Russia, which will be discussed below.

The prominence of the United States is not surprising, given that it has the highest number of broadband Internet users in the world.[134] The United States was the top country of spam origin for the first half of 2007, as well as the last half of 2006.

Current Rank	Previous Rank	Country/Region	Current Percentage	Previous Percentage
1	1	United States	42%	50%
2	3	United Kingdom	5%	4%
3	14	Russia	4%	2%
4	2	China	4%	4%
5	7	Poland	3%	3%
6	6	Taiwan	3%	3%
7	4	Japan	3%	4%
8	8	Germany	3%	2%
9	5	South Korea	3%	3%
10	15	Spain	2%	1%

Table 15. Top 10 countries/regions of spam origin
Source: Symantec Corporation

The United Kingdom ranked second for spam origin in the second half of 2007, accounting for five percent. During the first half of 2007, the United Kingdom ranked third and accounted for four percent. Although the rise in rank and percentage of the United Kingdom did correspond to a moderate rise in spam volume from the country, the changes are due primarily to changes in the volume percentages and rank of other countries, primarily Russia and China.

China fell from second to fourth during the period, with a corresponding decrease in spam volume of 131 percent. This drop is considerable, and is likely linked to the drop in bot-infected computers in the country.[135] One possible explanation is the unavailability of a number of Web sites, forums, and blogs in China for several months during this period.[136] Dynamic Web sites are often used by attackers to propagate and host malicious content, which in turn is often used to send spam.

[134] http://www.point-topic.com
[135] For a discussion on bot-infected computers, please see the "Attack Trends" discussion in this report.
[136] http://www.msnbc.msn.com/id/21268635/

Russia was the third ranked country during the second half of 2007, accounting for four percent of all spam volume. This corresponds to a 236 percent increase over the first half of 2007 when Russia ranked fourteenth and accounted for only two percent of all spam detected. Symantec also observed a 231 percent increase in the number of spam zombies detected in Russia during the current reporting period. As well, there was a 107 percent increase in active bot-infected computers in Russia over the previous period. This increase in malicious activity is likely attributable to the Russian Business Network (RBN) and its facilitation of malicious activity. Earlier this year, it was reported that the RBN allowed malicious content to be hosted on their Web space, thereby potentially facilitating malicious activity originating from Russia.[137] It is likely that the RBN's involvement in malicious activity contributed to this rise before it dropped offline in November.[138]

Over time, the RBN has been blamed for a large amount of malicious activity.[139] It has been suggested that the publicity surrounding the organization was partly responsible for its disappearance.[140] With the RBN's disappearance, there could be a corresponding drop in malicious activity originating from Russia in the coming months. However, it is also possible that the group did not discontinue its activities, but are attempting to avoid further publicity by taking its activities underground.

[137] http://blog.washingtonpost.com/securityfix/2007/10/mapping_the_russian_business_n.html
[138] http://www.theregister.co.uk/2007/11/08/rbn_offline/
[139] http://www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202461_pf.html
[140] http://www.networkworld.com/news/2008/011408-crime-hubs-can-be-downed.html?fsrc=rss-security

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, mail, 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

- Consumers should use an Internet security solution that combines antivirus, firewall, intrusion detection, and vulnerability management for maximum protection against malicious code and other threats.
- Consumers should ensure that security patches are up to date and that they are applied to all vulnerable applications in a timely manner.
- Consumers should ensure that passwords are a mix of letters and numbers, and should change them often. Passwords should not consist of words from the dictionary.
- Consumers should never view, open, or execute any email attachment unless the attachment is expected and the purpose of the attachment is known.
- Consumers should keep virus definitions updated regularly. By deploying the latest virus definitions, consumers can protect their computers against the latest viruses known to be spreading in the wild.
- Consumers should routinely check to see if their operating system is vulnerable to threats by using Symantec Security Check at www.symantec.com/securitycheck.
- Consumers should deploy an antiphishing solution. They should never disclose any confidential personal or financial information unless and until they can confirm that any request for such information is legitimate.
- Consumers can get involved in fighting cybercrime by tracking and reporting intruders. 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.
- Consumers should 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.
- Some security risks can be installed after an end user has accepted the end-user license agreement (EULA), or as a consequence of that acceptance. Consumers should read EULAs carefully and understand all terms before agreeing to them.
- Consumers should 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. When users see ads in a program's user interface, they may be looking at a piece of spyware.

Appendix B—Attack Trends Methodology

Attack 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. This includes bot-infected computers, bot command-and-control servers, phishing Web sites, malicious code infections, spam relay hosts, and Internet attacks. 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 is used to rank 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 Attrition.org.[141] Attrition.org 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.

Underground economy servers

This metric is based on data that is gathered by proprietary Symantec technologies that monitor 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.

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:

Full identities: Full identities may consist of name, address, date of birth, phone number, and Social Security number. It may also include extras such as driver's license number, mother's maiden name, email address, or "secret" questions/answers.

Credit cards: Credit cards may include name, credit card number, PIN, billing address, phone number, and company name (for a corporate card). Credit Verification Values (CVV) typically are not included in this and can be purchased separately.

[141] http://www.attrition.org/dataloss/dlunplugged.html

Bank accounts: Bank accounts 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.

Email passwords: These can include account information for emails including users ID, email address and password. In addition, the account will contain personal information and email addresses in the contact list.

Mailers: A mailer is an application that is used to send out mass emails (spam) for phishing attacks. Examples of this are worms and viruses.

Email addresses: These consist of lists of email addresses used for spam or phishing activities. The sizes of lists sold can range from 1 MB to 150 MB.

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.

Scams: Vendors sell malicious Web pages that pose as legitimate pages for phishing scams. They also offer services for hosting the pages, usually priced per week, given the transitory lifespan of many phishing sites.

Online auction site accounts: Information for online auction site accounts is often put up for sale, including user ID and password. In addition, the account will contain personal information such as name, address, phone number and email address.

Drop (request or offer): A drop is either a secure location where goods or cash can be delivered or a bank account through which money can be moved. The drop locations may be an empty apartment or some other scouted location. Criminals often change the billing addresses of credit cards and bank accounts to safe drops that are untraceable. Bank account drops are a convenient way to cash out bank accounts, credit cards, or other online financial accounts such as PayPal or eGold. Services for drops can often be accompanied by cashier services.

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.

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, which has approximately 50,000 direct subscribers who contribute, receive, and discuss vulnerability research on a daily basis.[142] Symantec also maintains one of the most comprehensive vulnerability databases, currently consisting of over 25,000 vulnerabilities (spanning more than two decades) affecting more than 55,000 technologies from over 8,000 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 type

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),[143] 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

Patch development time for operating systems

This metric has a similar methodology to the "Patch development time for enterprise vendors" metric, which was explained earlier in this methodology. However, instead of applying it to enterprise-scale vendors, the patch development time average is calculated from patched vulnerabilities for the following operating systems:

- Apple Mac OS X
- Hewlett-Packard HP-UX
- Microsoft Windows
- Red Hat Linux (including enterprise versions and Red Hat Fedora)
- Sun Microsystems Solaris

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

The sample set includes only vulnerabilities that are considered medium severity or higher, based on their CVSS base score. An average is calculated from the patch release times for each vulnerability in the reporting period per operating system. The patch development time average for each operating system is then compared.

Window of exposure for Web browsers

This metric has a similar methodology to the "Window of exposure for enterprise vendors" metric. However, instead of applying it to enterprise-scale vendors, the window of exposure is calculated for vulnerabilities associated with the following Web browsers:

- Safari
- Internet Explorer
- Mozilla browsers
- Opera

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 on the next page.

Web browser vulnerabilities

This metric compares vulnerability data for major Web browsers, namely: Internet Explorer, Mozilla browsers (including Firefox), Opera, and 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 *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 notoriously 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:

- 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.
- Not every vulnerability that is discovered is exploited. For the most part, there has been no widespread exploitation of any browser except Internet Explorer. This is expected to change as other browsers become more widely deployed.

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. Others are applications in their own right that run in the browser. Examples of these include ActiveX objects for Internet Explorer, Mozilla extensions, or Opera widgets.

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 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.

Site-specific cross-site scripting vulnerabilities

Data for this metric is provided by the XSSed Project, an online archive of publicly known cross-site scripting vulnerabilities that affect specific Web sites.

The XSSed Project gathers its data from security researchers who report specific instances of vulnerabilities in Web sites. 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

This metric quantifies the number of zero-day vulnerabilities that have been documented during the relevant reporting periods of the current *Internet Security Threat Report*. 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.

Unpatched enterprise vendor vulnerabilities

Unpatched vulnerabilities are vulnerabilities that have no vendor remediation at the time that data for the report was collected.[144] This metric tracks the number of unpatched vulnerabilities affecting enterprise-scale technologies. Individual vendors are identified and correlated with the number of unpatched vulnerabilities affecting them. It is possible that some vendors will have no vulnerabilities affecting them during a given reporting period or that none of the vulnerabilities affecting them are considered unpatched.

The status of some vulnerabilities may have changed since data was collected; vendors may have released patches for vulnerabilities included in the data set and new vulnerabilities may have been published that are considered unpatched. The nature of unpatched vulnerabilities means that the data may include vulnerabilities that are unverified and may have been reported by a single source with no other corroboration. However, the data also includes vulnerabilities that have been acknowledged but not fixed

[144] For the purpose of this report, patched vulnerabilities are those with vendor-supplied patches or upgrades. Vendor-supplied or third-party workarounds are not counted as patches.

by the vendor. In rare instances, the legitimacy of a vulnerability may be in dispute, but in all such cases these disputes remain unresolved at the time of data collection. Symantec excludes all vulnerabilities that are provably false from this and other metrics in the report.

It is also important to note that the set of vulnerabilities included in this metric is limited and does not represent all software from all possible vendors. Instead, it only includes vendors who are classified as enterprise vendors. The purpose is to illustrate the window of exposure for widely deployed mission-critical software. Because of the large number of vendors with technologies that have a very low deployment (which form the majority), only exploits for technologies from enterprise vendors (that is, those that generally have widespread deployment) are included. Vulnerabilities in those vendors' products will likely affect more enterprises than those in less widely deployed technologies. Those vendors are:

- CA
- Cisco
- EMC
- HP
- IBM
- McAfee
- Microsoft
- Oracle
- Sun
- Symantec

Vulnerabilities in security products

Symantec keeps track of products that are affected by vulnerabilities. Each product is classified into one or more categories based on the functions it performs. In this manner, it is possible to determine which vulnerabilities affect security products. Since many products may have security features, it is necessary to identify products whose main purpose is to provide security to enterprise and desktop systems. Therefore, each vulnerability is analyzed to determine whether it affects a product in one of the following categories:

- Antivirus
- Firewalls
- Intrusion detection systems (host- and network-based)
- Intrusion prevention systems (host- and network-based)
- Network Access Control (NAC)

Each vulnerability is further categorized based its severity, which is done using the same methodology as the "Severity of vulnerabilities" metric.

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.

Exploit code development time for enterprise vendors

The ability to measure exploit code development time is limited and applies only to vulnerabilities that would normally require exploit code. Therefore, this metric is based on vulnerabilities that Symantec considers to be of sufficient complexity, and for which functional exploit code was not available until it was created by a third party. This consideration, therefore, excludes the following:

- Vulnerabilities that do not require exploit code (unconfirmed exploitability);
- Vulnerabilities associated with non-functional proof-of-concept code (proof-of-concept exploitability).

The date of vulnerability disclosure is based on the date of the first publicly available reference (such as a mailing list post). The date of exploit code publication is the date of the first publicly known reference to the exploit code. Because the purpose of this metric is to estimate the time it takes for exploit code to materialize as a result of active development, exploit code publication dates that fall outside of the 30-day range from initial vulnerability publication are excluded from this metric. It is assumed that exploit code that was published after this period was not actively developed from the initial announcement of the vulnerability.

Because this metric only considers the appearance of the first functional exploit, it is possible that reliable exploits that improve upon the initial exploit may appear later. These exploits may take much longer to develop, but are not considered because the window of exposure begins as soon as the first functional exploit surfaces.

The time lapse between the disclosure of a vulnerability and the appearance of exploit code for that vulnerability is determined. The aggregate time for all vulnerabilities is determined and the average time is calculated. This metric is incorporated when computing the window of exposure, which is the difference between the average patch development time and the average exploit development time.

Patch development time for enterprise vendors

The patch development time is the time period between the disclosure date of a vulnerability and the release date of an associated patch. Only those patches that are independent objects (such as fixes, upgrades, etc.) are included in this analysis. Other remediation solutions—such as workaround steps, for instance—are excluded.

For each individual patch from these vendors, the time lapse between the patch release date and the publish date of the vulnerability is computed. The mean average is calculated from the aggregate of these. As some vendors may release more patches than others for a particular vulnerability, Symantec considers only the first instance of a single patch for each vulnerability. This metric is incorporated when computing the window of exposure, which is calculated as the difference between the average patch development time and the average exploit development time.

Window of exposure for enterprise vendors

Symantec records the time lapse between the publication of an initial vulnerability report and the appearance of third-party exploit code; this is known as the exploit 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.[145] 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 exploit development time and the average patch development time. (Explanations of the exploit development time average and the patch development time average are included below.) During this time, the computer or system on which the affected application is deployed may be susceptible to attack, as administrators have no official recourse against the vulnerability and must resort to best practices and workarounds to reduce the risk of exploitation.

It is important to note that the set of vulnerabilities included in this metric is limited and does not represent all software from all possible vendors. Instead, it only includes vendors who are classified as enterprise vendors. The purpose is to illustrate the window of exposure for widely deployed mission-critical software.

[145] This statistic only considers specific file-based patches or upgrades, and not general solutions. Instances in which the vendor provides a workaround or manual fix, for example, are not included.

Because of the large number of vendors with technologies that have a very low deployment (which form the majority), only exploits for technologies from enterprise vendors (that is, those that generally have widespread deployment) are included. Vulnerabilities in those vendors' products will likely affect more enterprises than those in less widely deployed technologies. Vendors included are:

- CA
- Cisco
- EMC
- HP
- IBM
- McAfee
- Microsoft
- Oracle
- Sun
- Symantec

Operating system time to patch by type

This is an analysis of the patched vulnerabilities in the data set for the "Operating system patch development time" metric. For each vendor studied in that metric, each vulnerability is divided into one of the following categories:

Browser vulnerabilities: These vulnerabilities threaten Web browser applications through remote attack vectors.

Client-side vulnerabilities: These vulnerabilities threaten network client applications or non-networked applications that process malicious data that may arrive through another networked application. Remote attack vectors may exist, but client-side vulnerabilities usually require some amount of user interaction on the part of the victim to be exploited.

Local vulnerabilities: These are vulnerabilities that require local access in order to be successfully exploited. Local attacks may affect a large variety of applications that may or may not include network capabilities. The differentiator is that these vulnerabilities are not exploitable by remote attackers unless they can log on to the system and run commands as an unprivileged user.

Server vulnerabilities: These are vulnerabilities that affect server applications. Server applications are typically defined as applications that are accessible to remote clients via connections on a range of TCP/UDP ports. Server vulnerabilities generally do not require user interaction on the part of the victim beyond enabling and starting the service so that it listens for incoming requests.

Other: These are vulnerabilities that do not fall discretely into any of the previous categories. They can include applications for which the distinction is blurred between server and client, or hardware platforms in which the affected component cannot be described by any of the other categories.

These categories are generally defined by the attack vector and by the type of application that is affected. The specific categories were devised so that the majority of vulnerabilities could easily be classified within them, with little overlap between categories, so that the total percentage of all categories would equal 100 percent.

Easily exploitable vulnerabilities

This metric covers vulnerabilities that attackers can exploit with little effort based on publicly available information. The vulnerability analyst assigns an exploit availability rating after thoroughly researching the need for and availability of exploits for the vulnerability.

This metric replaces the "Ease of exploitation" metric (in the Symantec *Internet Security Threat Report* prior to Volume XI), to accommodate Symantec's adoption of the exploitability rating in the Common Vulnerability Scoring System (CVSS) V1.0.[146]

CVSS classifies all vulnerabilities into one of four possible categories:

Unconfirmed: Would-be attackers must use exploit code to make use of the vulnerability; however, no such exploit code is publicly available.

Proof-of-concept: Would-be attacks must use exploit code to make use of the vulnerability; however, there is only proof-of-concept exploit available that is not functional enough to fully exploit the vulnerability.

Functional: This rating is used under the following circumstances:

- Exploit code to enable the exploitation of the vulnerability is publicly available to all would-be attackers; and/or,
- Would-be attackers can exploit the vulnerability without having to use any form of exploit code;

In other words, the attacker does not need to create or use complex scripts or tools to exploit the vulnerability.

High: The vulnerability is reliably exploitable and there have been instances of self-propagating malicious code exploiting the vulnerability in the wild.

For the purposes of this report, the last two categories are considered "easily exploitable" because the attacker requires only limited sophistication to exploit the vulnerability. The first two categories are considered more difficult to exploit because attackers must develop their own exploit code or improve an existing proof-of-concept to make use of the vulnerability.

[146] http://www.first.org/cvss/v1

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, as described above, 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. Symantec gathers data from over 120 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

To help detect and eradicate computer viruses, Symantec developed the Symantec AntiVirus Research Automation (SARA) technology. Symantec uses this technology 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 *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. This database contains 8,000 distinct entries, with the earliest discovery 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 and Spam Methodology

Phishing and spam attack trends in this report are based on the analysis of data derived from the Symantec Probe Network and from Symantec Brightmail AntiSpam data.

The Symantec Probe Network is a system of over two million decoy accounts that attract email messages from 20 different countries around the world. It encompasses more than 600 participating enterprises and attracts email samples that are representative of traffic that would be received by over 250 million mailboxes. The Probe Network covers countries in the Americas, Europe, Asia, Africa, and Australia/Oceania.

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

Phishing activity by sector

The Symantec Phish Report Network (PRN) is an extensive antifraud community whose members contribute and receive fraudulent Web site 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 Web sites as the clients visit various Web sites on the Internet. It also includes server detection from spam emails. The sender confirms all spoofed Web sites before sending the address of the Web site into the PRN. After it is received by the PRN, Symantec spoof detection technology is used to verify that the Web site 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 Web sites

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 Web sites 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 Web sites.

Phishing site top-level domains

The data for this section is determined by deriving the top-level domains of each distinct phishing Web site 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.

Spam

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.

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help businesses and consumers secure and manage their information. Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our Web site. 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

04/08 13585530-1