SYMANTEC ENTERPRISE SECURITY

symantec™

Confidence in a connected world.

Symantec Government Internet Security Threat Report

Trends for January–June 07

Volume XII, Published September 2007

Dean Turner
Executive Editor
Symantec Security Response

Stephen Entwisle
Senior Editor
Symantec Security Response

Eric Johnson
Editor
Symantec Security Response

Marc Fossi
Analyst
Symantec Security Response

Joseph Blackbird
Analyst
Symantec Security Response

David McKinney
Analyst
Symantec Security Response

Ronald Bowes
Analyst
Symantec Security Response

Nicholas Sullivan
Analyst
Symantec Security Response

Candid Wueest
Analyst
Symantec Security Response

Ollie Whitehouse
Security Architect—Advanced Threat Research
Symantec Security Response

Zulfikar Ramzan
Analyst—Advanced Threat Research
Symantec Security Response

Jim Hoagland
Principal Software Engineer
Symantec Security Response

Chris Wee
Manager, Development
Symantec Security Response

Contributors

David Cowings
Sr. Manager of Operations
Symantec Business Intelligence

Dylan Morss
Manager
Symantec Business Intelligence

Shravan Shashikant
Principal Business Intelligence Analyst
Symantec Business Intelligence

Volume XII, Published September 2007

Symantec Government Internet Security Threat Report

Contents

Government Internet Security Threat Report Overview 4

Attack Trends 8

Vulnerability Trends 40

Malicious Code Trends 47

Phishing Trends 56

Spam Trends 64

Appendix A—Symantec Best Practices 71

Appendix B—Attack Trends Methodology 73

Appendix C—Vulnerability Trends Methodology 76

Appendix D—Malicious Code Trends Methodology 79

Appendix E—Phishing Trends Methodology 80

Appendix F—Spam Trends Methodology 81

Government Internet Security Threat Report Overview

The *Government Internet Security Threat Report* provides a six-month summary and analysis of trends in attacks, vulnerabilities, malicious code, phishing, and spam as they pertain to organizations in government and critical infrastructure sectors. Where possible, it will also include an overview of legislative efforts to combat these activities.

Over the past several reporting periods, Symantec has observed a shift in the threat landscape in which attackers have increasingly moved away from nuisance and destructive attacks towards targets and methods that are driven by financial motives. Today's attackers are increasingly sophisticated and organized, and have begun to adopt methods that are similar to traditional software development and business practices.

In the previous *Internet Security Threat Report*, Symantec observed that global, decentralized networks of malicious activity continued to rise and that, increasingly, regional threat patterns were beginning to emerge. Today, the threat landscape is arguably more dynamic than ever. As security measures are developed and implemented to protect the computers of end users and organizations, attackers are rapidly adapting new techniques and strategies to circumvent them. As a result, the identification, analysis and trending of these techniques and strategies must also evolve.

The ensuing changes have been evident over the first six months of 2007. Based on the data collected during that period, Symantec has observed that the current Internet security threat landscape is characterized by the following:

- Increased professionalization and commercialization of malicious activities
- Threats that are increasingly tailored for specific regions
- Increasing numbers of multistaged attacks
- Attackers targeting victims by first exploiting trusted entities
- Increased convergence of malicious activities

The *Government Internet Security Threat Report* will provide an analysis of attack activity that Symantec observed between January 1 and June 30, 2007 that targets or affects services, organizations, and/or industries of concern to government organizations around the world. For the purposes of this discussion, these government organizations include national, state/provincial, and municipal governments. Furthermore, this discussion will incorporate data and discussion that is relevant to threat activity that affects critical infrastructure industries that support or affect government and military institutions, which include:

- Aerospace
- Agriculture
- Biotech/pharmaceutical
- Government
- Financial services
- Health care
- Internet service providers

- Law enforcement
- Manufacturing
- Military
- Telecommunications
- Transportation
- Utilities and energy

Symantec has established some of the most comprehensive sources of Internet threat data in the world. The Symantec™ Global Intelligence Network tracks attack activity across the entire Internet. Over 40,000 sensors deployed in more than 180 countries by Symantec DeepSight™ Threat Management System and Symantec™ Managed Security Services gather this data. As well, Symantec gathers malicious code data reports from over 120 million client, server, and gateway systems that have deployed Symantec's antivirus products.

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.[1] Symantec also maintains one of the world's most comprehensive vulnerability databases, currently consisting of over 22,000 vulnerabilities (spanning more than a decade) affecting more than 50,000 technologies from over 8,000 vendors.

Finally, the Symantec Probe Network, a system of over two million decoy accounts, attracts email messages from 20 different countries around the world, allowing Symantec 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. Members of the network contribute and receive fraudulent Web site addresses for alerting and filtering across a broad range of solutions. Symantec also tracks and assesses some criminal activities using online fraud monitoring tools.

These resources give Symantec analysts unparalleled sources of data with which to identify emerging trends in malicious activity. The Symantec *Government Internet Security Threat Report* is grounded on the expert analysis of data provided by all of these sources. By publishing the analysis of Internet security activity in this report, Symantec hopes to provide enterprises and consumers in the government sector with the information they need to help effectively secure their systems now and in the future.

[1] The BugTraq mailing list is hosted by SecurityFocus (http://www.securityfocus.com). Archives are available at http://www.securityfocus.com/archive/1

Executive Summary

The following section will offer a brief summary of the security trends that Symantec observed during the first half of 2007 based on data provided by the sources listed above. This summary includes all of the metrics that are included in the *Government Internet Security Threat Report*.

Attack Trends Highlights

- The United States was the top country for malicious activity, accounting for 30 percent of malicious activity detected worldwide.
- Israel had the most malicious activity per Internet user, followed by Canada and the United States.
- The telecommunications sector accounted for 90 percent of all malicious activity originating from critical infrastructure sectors.
- The government sector accounted for 26 percent of data breaches that could lead to identity theft, the second most of any sector.
- 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.
- Hacking was responsible for 73 percent of identities exposed during this period.
- The United States was the target of the most denial of service attacks, accounting for 61 percent of all attacks during this period.
- Symantec observed an average of 52,771 active bot-infected computers per day, a 17 percent decrease from the previous reporting period.
- The lifespan of the average bot-infected computer was four days, an increase from three days in the second half of 2006.
- China had the highest number of bot-infected computers during the first half of 2007, accounting for 29 percent of the worldwide total.
- The United States had the most known command-and-control servers worldwide, accounting for 43 percent of the worldwide total.
- The United States was the top country of attack origin, accounting for 25 percent of worldwide attack activity.
- The top country of origin for attacks targeting the government sector was the United States, which accounted for 19 percent of the total.
- The most common attacks targeting government and critical infrastructure organizations were SMTP-based attacks, which accounted for 36 percent of the top ten attacks.

Vulnerability Trends Highlights

- Of the five operating systems tracked, Microsoft had the shortest average patch development time, at 18 days.
- Symantec documented six zero-day vulnerabilities during this period, down from 12 zero-day vulnerabilities in the second half of 2006.
- Symantec documented 90 unpatched enterprise vulnerabilities during this period.

Malicious Code Trends Highlights

- Threats to confidential information made up 65 percent of potential infections by the top 50 malicious code samples, up from 53 percent in the second half of 2006.
- Eighty-eight percent of confidential information threats had remote access capabilities, up slightly from 87 percent last period.
- Eighty-eight percent of confidential information threats had keystroke-logging capabilities, up from 76 percent in the second half of 2006.
- Of malicious code that propagated, 46 percent did so in email attachments.
- The United States had the highest number of multiple malicious code infections in the world, followed by China and Japan.
- During this period, 44 percent of Trojans were reported from North America, more than any other region.
- EMEA accounted for 43 percent of potential infections caused by worms, more than any other region.
- EMEA accounted for 45 percent of potential virus infections this period, more than any other region.
- EMEA accounted for 40 percent of all potential back door infections worldwide, more than any other region.

Phishing Trends Highlights

- Seventy-nine percent of organizations whose brands were used in phishing attacks were in the financial services sector, down from 84 percent in the second half of 2006.
- The financial services sector accounted for 72 percent of all phishing Web sites, up from 64 percent in the previous period.
- Of all known phishing Web sites, 59 percent were located in the United States, compared with 46 percent in the previous six-month period.
- Domains registered to the government of Thailand were used in 16 percent of phishing URLs hosted on government servers.
- Of the unique government domains used to host phishing Web sites, 23 percent were located in Thailand.

Attack Trends

This section of the *Government Internet Security Threat Report* will provide an analysis of attack activity that Symantec observed between January 1 and June 30, 2007 that targets or affects services, organizations, and/or industries of concern to government organizations around the world. For the purposes of this discussion, attacks are defined as any malicious activity carried out over a network that has been detected by an intrusion detection system (IDS) or firewall.

Attack activity is monitored by the Symantec Global Intelligence Network across the entire Internet. Over 40,000 sensors deployed in more than 180 countries by Symantec DeepSight Threat Management System and Symantec Managed Security Services gather this data. Furthermore, Symantec uses proprietary technologies to monitor bot command-and-control servers and underground economy servers across the Internet.[2] These resources combine to give Symantec an unparalleled ability to identify, investigate, and respond to emerging security threats. This discussion will be based on data provided by all of these sources.

This section of the *Government Internet Security Threat Report* will discuss:

- Malicious activity by country
- Malicious activity by country per Internet user
- Malicious activity originating in government/critical infrastructure
- Data breaches that could lead to identity theft
- Top countries targeted by denial of service attacks
- Bot-infected computers
- Lifespan of bot-infected computers
- Bot-infected computers by country
- Command-and-control servers by country
- Top countries of attack origin
- Top countries of origin for government-targeted attacks
- Attacks by type—notable critical infrastructure sectors

Malicious activity by country

This metric will assess the countries in which the highest 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 sites,[3] malicious code reports, spam zombies,[4] and Internet attacks.

To determine the amount of Internet-wide malicious activity that originated in each country, the mean of the proportion of all of the considered malicious activities that originated in each country was calculated. This average determined the proportion of overall malicious activity that originated from the country in question and was used to rank each country. This section will discuss those findings.

[2] Underground economy servers are used by criminals and criminal organizations to sell stolen information, typically for subsequent use in identity theft. This data can include government-issued identity numbers, credit cards, bank cards and personal identification numbers (PINs), user accounts, and email address lists.

[3] As will be discussed in greater length in the "Phishing Trends" section below, a phishing Web site is one that is designed to mimic the legitimate Web site of the organization whose brand is being spoofed.

[4] A spam zombie is a computer infected with a bot or some other malicious code that allows email messages to be relayed through the infected computer.

Between January 1 and June 30, 2007, the United States was the top country for malicious activity, accounting for 30 percent of activity detected worldwide (table 1). This represents a minimal change from the second half of 2006, when the United States was also the highest ranked country, accounting for 31 percent of the world's malicious activity. For each of the malicious activities taken into account for this metric, the United States ranked number one by a large margin with the exception of bot-infected computers, for which it ranked second behind only China.

Overall Rank	Previous Rank	Country	Overall Proportion	Previous Overall Proportion	Malicious Code Rank	Spam Zombies Rank	Command-and-Control Server Rank	Phishing Web sites	Bot Rank	Attack Rank
1	1	United States	30%	31%	1	1	1	1	2	1
2	2	China	10%	10%	2	3	5	18	1	2
3	3	Germany	7%	7%	7	2	2	2	3	3
4	5	United Kingdom	4%	4%	3	15	6	3	7	5
5	4	France	4%	4%	9	7	12	6	5	4
6	7	Canada	4%	3%	6	31	3	7	8	7
7	8	Spain	3%	3%	10	10	22	13	4	6
8	10	Italy	3%	3%	5	6	8	12	6	8
9	6	South Korea	3%	4%	26	8	4	10	13	12
10	11	Japan	2%	2%	4	20	13	8	16	10

Table 1. Malicious activity by country
Source: Symantec Corporation

It is not surprising that the United States was the site of the most malicious activity, as it is home to 18 percent of the world's Internet users, more than any other country.[5] Furthermore, it has a well established and relatively long-standing Internet infrastructure. As a result, not only are there a lot of attackers there, but they have had a long time to understand the technologies and to hone their skills. Attackers in countries that have less well established traditions of Internet usage or that are still experiencing rapid growth in their Internet infrastructure may not have the same level of user sophistication.

In previous versions of the *Internet Security Threat Report*, Symantec has argued that as Internet infrastructure becomes established, network and end user security should improve. As Internet users become more sophisticated, so does their knowledge of computer security issues overall. However, the prominence of the United States in this discussion, and the attendant level of malicious activity originating there, indicates that this is not always the case. This is likely because attackers are constantly adapting their attacks to circumvent effective security measures, meaning that even users with a high degree of computer security awareness may be at risk of new attack tactics. Given these considerations, and the country's consistently high ranking in each of the high attack categories, the United States will likely remain number one for malicious activity for some time.

China had the second highest amount of malicious activity during the first six months of 2007, accounting for 10 percent of activity detected worldwide, the same rank and percentage as in the previous reporting period. China has the second highest number of Internet users in the world, surpassed only by the United States.[6] However, users in China spend about two billion hours online each week, more than users in the United States, who spend only 129 million hours online.[7]

[5] http://www.internetworldstats.com/stats14.htm
[6] http://www.internetworldstats.com/stats3.htm
[7] http://www.forbes.com/2006/03/31/china-internet-usage-cx_nwp_0403china.html

China ranked in the top three countries for four of the six activities considered for this metric. However, it ranked only 18th in the world for phishing Web sites. The relatively low ranking of phishing Web sites in China may be linked to the strict regulation of Web sites by the Chinese government,[8] which is enforced through Internet filtering tools on every level from Internet service providers (ISPs) to Internet cafés.[9]

China also ranked only fifth for bot command-and-control servers, despite the fact that it ranked number one for bot-infected computers. This discrepancy indicates that many bot-infected computers in China are being controlled by command-and-control servers outside the country. Since the United States has the highest number of command-and-control servers by a large margin, it is likely that bot-network owners in that country are using bot-infected computers in China to conduct attack activity.[10] Thus, some malicious activity attributed to China may not be the result of attackers located there, although the same caveat would also apply to malicious activity originating in other countries as well.

In the first six months of 2007, Germany was the third ranked country for malicious activity. Seven percent of all Internet-wide malicious activity originated there during this period, the same percentage as the second half of 2006, when it was also the third ranked country in this metric. Like both China and the United States, Germany has a well established Internet infrastructure. Furthermore, it has the fourth highest number of Internet users in the world, boasting five percent of the world's Internet users.[11]

Germany ranks highly in spam zombies, phishing Web sites, bot-infected computers, and command-and-control servers. As a result, it is likely that bot networks are prominent in Germany, which would contribute to the high amount of malicious activity originating there.

Having a higher proportion of malicious activity indicates that each computer in the country is more likely to be involved with some form of attack activity. Symantec has observed previously that computers often target computers within their own region or country. As a result, countries with higher proportions of malicious activity are more likely to suffer the effects of such malicious activity. That includes computers in the government sector, as well as other sectors that make up critical infrastructure.

Furthermore, a country in which a high proportion of malicious activity is based is likely to be the country of origin for much of the malicious activity that is aimed at other countries. High volumes of malicious activity originating from any country could have a potential impact on that country's ability to conduct Internet transactions. It is reasonable to speculate that high volumes of malicious activity from a particular country could result in the blocking of traffic originating from individual servers and organizations within that country.

Countries with a high number of Internet users tend to display higher levels of malicious activity (although this is not always the case). For example, the United States has the highest number of Internet users.[12] It also had the highest amount of malicious activity during this period, with 31 percent. China has the second highest number of Internet users,[13] and the second highest amount of malicious activity, with 10 percent.

On a global scale, the distribution of the world's malicious activity seems to be relatively static. It appears that a country that is established as a site of high levels of malicious activity tends to remain so. This suggests that once an attack infrastructure is established in a country, it can be difficult to remove. Although malicious tools and methods may change, the proportion of malicious activity that originates within a country tends to remain relatively static. This is likely to remain the case until new and more effective measures are taken by countries to reduce the malicious activity originating from their networks.

[8] http://www.cbsnews.com/stories/2002/12/03/tech/main531567.shtml
[9] http://news.bbc.co.uk/2/hi/business/2264508.stm
[10] It should be noted that the location of the command-and-control server does not necessarily correspond to the location of the bot-network owner.
[11] http://www.internetworldstats.com/stats4.htm
[12] http://www.internetworldstats.com/stats14.htm
[13] http://www.internetworldstats.com/stats3.htm

Furthermore, in previous volumes of the *Internet Security Threat Report*, Symantec has observed that attacker motivation has changed from fame to fortune.[14] That is, attackers have become increasingly motivated by profit. As a consequence, attacks and malicious activity are likely to remain prominent within a country as long as they remain profitable.

Due to the relative anonymity of online users and the constantly changing threat environment, attempts at legislating behavior may not meet with much success. Rather than relying on legislation to limit malicious activity, it is likely that end users will need to take responsibility for the security of their own computers. For example, they should follow best security practices, use defense-in-depth strategies, and implement sufficient security technologies.[15]

ISPs can play a central role in mitigating malicious activity over the Internet. They have the ability to filter malicious code, attacks, spam, and other forms of malicious traffic as it enters or leaves their networks. Unfortunately, ISPs will often focus their resources on meeting growing broadband demand at the expense of implementing security measures, such as port blocking and ingress and egress filtering.[16] As a result, ISPs that are growing or expanding their services rapidly may have security infrastructures that are underdeveloped relative to their needs.

Symantec recommends that ISPs perform both ingress and egress filtering to block known bot traffic. They should also filter out potentially malicious email attachments to reduce exposure to enterprises and end users.

Enterprises should monitor all network-connected computers for signs of malicious activity, ensuring that any infected computers are removed from the network and disinfected as soon as possible. They should also ensure that all antivirus definitions are updated regularly. As compromised computers can be a threat to other systems, Symantec also recommends that enterprises notify their ISPs of any potentially malicious activity.

Enterprises should also perform filtering on outgoing network traffic, ensuring that malicious activity and unauthorized communications are not taking place. They should also create and enforce policies that identify and restrict applications that can access the network.

Malicious activity by country per Internet user

Having assessed the top countries by malicious activity, Symantec has also evaluated the top 25 of these countries according to the number of Internet users located there. This measure is intended to remove the bias of high numbers of Internet users from the consideration of the “Malicious activity by country” metric.

In order to determine this, Symantec divided the amount of malicious activity originating in each of the top 25 countries by the number of worldwide Internet users who are located in that country. The proportion assigned to each country in this discussion thus equates to the proportion of malicious activity that could be attributed to a single (average) Internet user in that country. The percentage of malicious activity that would be carried out by each person is the amount assigned to each country in the discussion below.

[14] For instance, please see 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. 36

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

[16] Ingress traffic refers to traffic that is coming into a network from the Internet or another network. Egress traffic refers to traffic that is leaving a network, bound for the Internet or another network.

During the first six months of 2007, Israel had the most malicious activity per Internet user of any country in the group. If one person from each of the top 25 countries were assessed as a representation of their country's Internet users, the average user in Israel would carry out 11 percent of the group's malicious activity (table 2). This is a small increase from nine percent in the previous period.

This increase was likely due to a higher proportion of bot-infected computers, command-and-control servers, and spam zombies located in Israel during this reporting period. This indicates that bots are gaining prominence in Israel; in fact, the number of bot-infected computers located there increased by 15 percent between the second half of 2006 and the end of June 2007.

The prominence of Israel in this metric is likely influenced by the amount of time computer users there spend online. According to a survey released in January 2007, users in Israel spend the second highest number of hours online, on average, less than only users in Canada, which ranked second in this metric.[17] The longer computers are online, the greater is the opportunity for attackers to compromise them.

Furthermore, computer security law enforcement resources in Israel may be insufficient to meet current demands. This prompted a reorganization in 2005 that was intended to create a single information technology authority in the country to deal with computer and Internet crime.[18] As a result of these recent changes, the new security organization may be experiencing difficulties in detecting and eliminating security issues. This is corroborated by the extensive industrial espionage scandal that was uncovered in Israel in 2005.[19]

Finally, ISPs in Israel may be failing to help maintain secure networks in the country. This increase may be related to the recent privatization of a large Israeli ISP. When companies become privatized, their budgets and operating practices may be changed, and focus may be diverted away from activities that don't generate direct revenue streams, such as security. If less attention is focused on security, it is possible that bot-infected computers can operate more easily in Israeli cities.

Current Rank	Previous Rank	Country	Current Proportion	Previous Proportion
1	1	Israel	11%	9%
2	5	Canada	6%	5%
3	4	United States	6%	6%
4	3	Poland	6%	6%
5	6	Spain	6%	5%
6	2	Taiwan	6%	8%
7	10	Germany	5%	5%
8	12	Netherlands	5%	4%
9	9	France	4%	5%
10	7	Switzerland	4%	5%

Table 2. Malicious activity by country per Internet user
Source: Symantec Corporation

[17] http://www.websiteoptimization.com/bw/0703
[18] http://www.crime-research.org/news/30.09.2005/152
[19] http://www.msnbc.msn.com/id/8064757

Canada had the second most malicious activity per Internet user, accounting for six percent of the worldwide total. In the previous reporting period, Canada ranked fifth in this category, with five percent of malicious activity per Internet user. Canada had the highest number of hours spent online per person in the first half of 2007.[20] This likely contributes to the country's prominence in this category.

The United States ranked third, accounting for six percent of malicious activity per Internet user. In the second half of 2006, the United States was fourth in this category, but had the same proportion of malicious activity per Internet user. The United States has the highest number of broadband connections in the world, and had the fourth highest number of hours spent online per unique Internet user in the first half of 2007.[21]

The prominence of both Canada and the United states is likely due to the number of hours spent online by the average user and the well established Internet infrastructure in both countries. As was discussed in the "Malicious Activity per Country" metric, the population of Internet users in a country with a well established tradition of Internet use is more likely to have the skills and experience necessary to conduct sophisticated attack activity. As such, it is likely that a higher proportion of the Internet user population would be able to carry out malicious activity, such as creating bot networks, which can then be used for subsequent attack activity.

Both Canada and the United States ranked higher for malicious activity per Internet user in the current period than in the second half of 2006. The current increase is likely driven by a drop in malicious activity per Internet user in both Taiwan and Poland.

Malicious activity by critical infrastructure sectors

For the first time, in this volume of the *Government Internet Security Threat Report*, Symantec is evaluating the amount of malicious activity originating from computers and networks that are known to belong to government and critical infrastructure sectors. To do this, Symantec cross-references the IP addresses of known malicious computers with Standard Industrial Classification (SIC) codes[22] assigned to each industry and provided by a third-party service.[23] Symantec has compiled data on numerous malicious activities that were detected originating from the IP address space of these organizations. These activities include: bot-infected computers, phishing Web sites, spam zombies, and Internet attacks.

This metric is significant because it indicates the level to which government and critical infrastructure organizations have been compromised and are being used by attackers as launching pads for malicious activity. This could potentially expose sensitive information, which could have serious ramifications for government and critical infrastructure organizations.

In the first six months of 2007, 90 percent of all malicious activity originating from critical infrastructure sectors originated from telecommunications organizations (table 3). Attackers may target computers in the telecommunications sector for a number of reasons. These organizations are likely to have a large number of Internet-facing computers. For example, call centers often use a large number of Internet-facing computers to interact with customers. The challenges of managing such computers may contribute to the extremely high proportion of malicious activity originating from this sector. As a consequence, computers in telecommunications organizations likely represent fertile targets for attackers.

[20] http://www.websiteoptimization.com/bw/0703
[21] http://www.websiteoptimization.com/bw/0703
[22] SIC codes are the standard industry codes that are used by the United States Securities and Exchange Commission to identify organizations belonging to each industry. For more, on this, please see http://www.sec.gov
[23] http://www.digitalenvoy.net/

Rank	Sector	Total Percent	Phishing Web Sites	Spam Zombies	Bot-infected computers	Attacks
1	Telecommunications	90%	77%	99%	94%	91%
2	Manufacturing	7%	22%	<1%	2%	4%
3	Financial Services	1%	1%	<1%	1%	2%
4	Health Care	1%	<1%	<1%	1%	1%
5	Military	<1%	<1%	<1%	1%	1%
6	Utilities/Energy	<1%	<1%	<1%	1%	1%
7	Transportation	<1%	<1%	<1%	<1%	<1%
8	Government	<1%	<1%	<1%	<1%	1%
9	Biotech/Pharmaceutical	<1%	<1%	<1%	<1%	<1%
10	Agriculture	<1%	<1%	<1%	<1%	<1%
11	Law Enforcement	<1%	<1%	<1%	<1%	<1%

Table 3. Malicious activity by critical infrastructure sector
Source: Symantec Corporation

Attackers may view telecommunications organizations as excellent platforms from which to launch attacks. Organizations within this sector are likely to have high-bandwidth and high-traffic networks. Such networks would allow an attacker to carry out large attacks, such as DoS attacks, or other malicious activity, such as spam hosting. This is illustrated by the high percentage of spam zombies found in telecommunications, 99 percent of spam zombies in critical infrastructure sectors. High-capacity networks may also allow an attacker to hide attack and bot traffic more effectively. During the current reporting period, 91 percent of attacks and 94 percent of bot-infected computers were situated on telecommunications organizations' networks.

As telecommunications organizations control the flow of data through networks, attackers may be enticed to compromise strategically located computers inside organizations within the industry. Furthermore, the telecommunications sector provides communications for other sectors as well, including government. Successful compromise of computers in the telecommunications industry could thus allow an attacker to eavesdrop on or disrupt key communications in other sectors.

Furthermore, computers within telecommunications organizations may effectively serve as platforms from which to launch attacks against organizations served by the telecommunications firms. As such, attackers who are seeking confidential or sensitive information may specifically target this sector.

Finally, using compromised computers within telecommunications organizations could allow an attacker to deny access to confidential communications by authorized personnel, allowing the attacker to impose his or her own command, control, and communication processes on the compromised systems. This could result in the loss of situational awareness. Were such an attack to be state or group sponsored, access to critical infrastructures could be used to disable key services as a prelude to a larger event or attack.

The manufacturing sector was the origin of the second highest amount of malicious activity during the first half of 2007, accounting for seven percent of the total. Although this proportion is relatively low compared to the telecommunications sector, it is still noteworthy for a number of reasons.

Twenty-two percent of all phishing Web sites within critical infrastructure sectors were found on networks owned by organizations in the manufacturing sector. This is considerably more than the proportion of all other malicious activities originating from the sector and is likely a sign that manufacturing organizations are specifically being targeted by phishers. In the case of manufacturing, phishers are likely using computers within manufacturing organizations to host phishing Web sites to target individuals within those organizations.

It is also worth noting that the manufacturing sector represents a considerably higher proportion of phishing Web sites than the financial sector. This is surprising because, as is discussed in the "Phishing Trends" section of this report, most of the organizations whose brands were used in phishing attacks in the first six months of 2007 were part of the financial services sector. However, what this data points out is that financial services organizations do not actually host many phishing Web sites. This is likely because financial services are a common target of phishing attacks. As a result, financial services organizations are likely well aware of phishing attacks and have taken steps to protect their networks from hosting phishing Web sites.

Finally, due to the potentially fragile nature of process control systems that are used to run manufacturing equipment, the manufacturing industry may be particularly at risk of damages due to bot infections. A single bot-infected computer can disrupt the production of an entire facility with a targeted attack against a vulnerable process control system. This could have significant economic and strategic consequences.

The financial services sector ranked third for malicious activity within critical infrastructure sectors, accounting for one percent of the total detected during this period. Financial services also ranked third in the second half of 2006, also with one percent of malicious activity. Although computers in the financial services sector may represent a lucrative opportunity for attackers with profit motive, due to the small proportion of bots within the sector, it is likely that much of the malicious activity was driven by attacks of opportunity.

Data breaches that could lead to identity theft

Identity theft is an increasingly prevalent security issue, particularly for government organizations, many of which store and manage information that could facilitate identity theft. Compromises that result in the loss of personal data can be quite costly, not only to the people whose identity may be at risk and their respective financial institutions, but also to the organization responsible for collecting and managing the compromised data.

Data breaches that lead to identity theft could damage an organization's reputation, and undermine customer and institutional confidence. With the implementation of recent legislation in some jurisdictions,[24] organizations may also be held liable for data breaches and losses, which could result in fines or litigation.[25] Furthermore, breaches of this sort that take place in government organizations could be used to access sensitive information, which could have significant consequences for a country's national security.

[24] http://www.parliament.the-stationery-office.co.uk/pa/cm199900/cmbills/001/2000001.htm
[25] http://www.fsa.gov.uk/pages/Library/Communication/PR/2007/021.shtml

Using publicly available data,[26] Symantec has determined the sectors that were most often affected by these breaches, as well as the most common causes of data loss. Using the same publicly available data, this metric will also explore the number of identities exposed due to these data breaches. An identity is considered to be exposed if personal or financial data related to the identity is made available for unauthorized viewing or use through the breach.

It should be noted that some sectors may need to comply with more stringent data-breach reporting requirements than others. For instance, government organizations are more likely to be required to report data breaches, either due to regulatory obligation or as part of publicly accessible audits and/or performance reports.[27] Furthermore, 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 may be under-represented in this data set.

In the first half of 2007, the education sector accounted for 30 percent of all known data breaches that could lead to identity theft, more than any other sector (figure 1). This is up from the previous period when education accounted for only 22 percent of the total and was the second ranked sector.

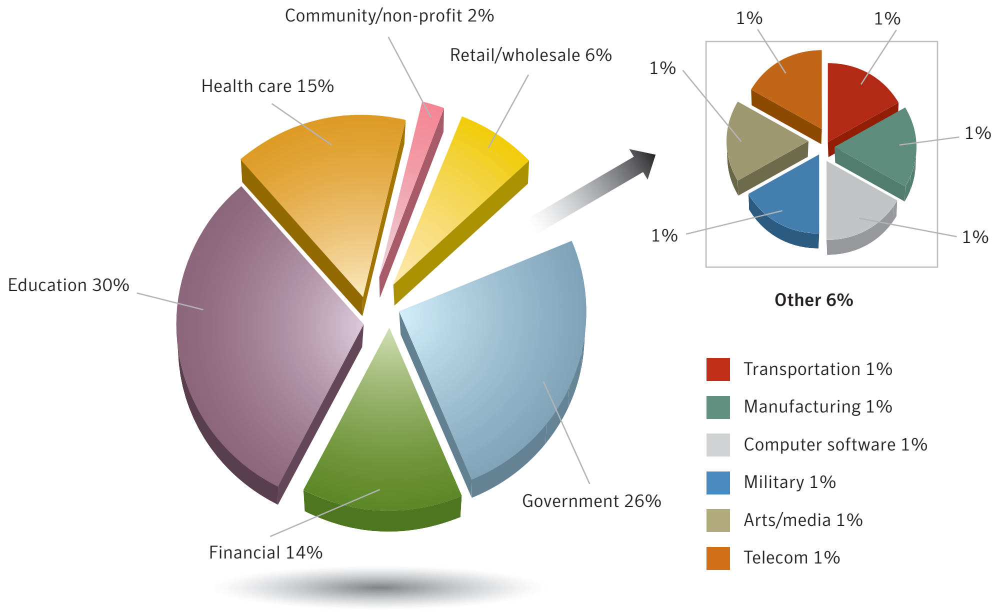

Figure 1. Data breaches that could lead to identity theft by sector
Source: Based on data provided by Attrition.org

Educational organizations store a lot of personal information that could be used for the purposes of identity theft. These organizations—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 by many people. This increases the opportunities for attackers to gain unauthorized access to this data. Adding to this is the fact that research hospitals, which are considered part of the education sector, store considerable amounts of patients' personal data, including medical information.

[26] http://www.attrition.org/dataloss/
[27] 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/

In spite of the high number of data breaches that occurred in the education sector during the first six months of 2007, it only accounted for one percent of all identities exposed during the period (figure 2). This is likely because most data breaches within the education sector were caused by theft or loss of computers or data storage devices. The theft or loss of computers containing identity theft-related information would likely be either opportunistic or motivated by the possibility of more immediate profit generated by selling the found or stolen computer or storage media. Hacking, on the other hand, is more likely to be motivated by the acquisition of valuable data that may facilitate identity theft.[28] Breaches that occur in the education sector are therefore less likely to result in large-scale identity fraud because they result in the exposure of relatively few identities.

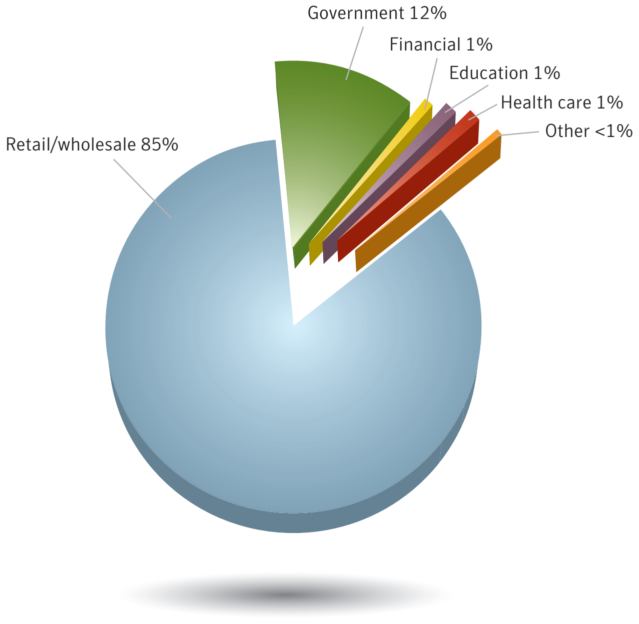

Figure 2. Exposed identities by sector
Source: Based on data provided by Attrition.org

During this reporting period, the government sector accounted for 26 percent of data breaches that could lead to identity theft, making it the second highest sector for this consideration. This sector has the most breaches that could lead to identity theft in the second half of 2006, accounting for 33 percent of the total during that period.

Government organizations, like educational organizations, store a considerable amount of information that could be used for identity theft. Similar to the education sector, these organizations often consist of numerous semi-independent departments. As a consequence, sensitive personal identification information may be stored in separate locations and be accessible by numerous people. This increases the opportunities for attackers to gain unauthorized access to this data.

[28] 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 through Internet-based attacks.

The government sector also ranked second for the overall number of identities exposed during the period, accounting for 12 percent of the total. As was the case with the educational sector, the number of identities exposed is relatively small compared to the number of data breaches in this sector. Thus, breaches that occur in the government sector can be considered less likely to lead to large-scale identity theft than those in other sectors.

The health care sector accounted for 15 percent of data breaches that could lead to identity theft in the first half of 2007. Health care ranked fourth in the previous period, accounting for 11 percent of all breaches that could lead to identity theft. The prominence of the health care sector in this metric is likely due to similar factors that influence the prominence of both education and government as outlined previously. Furthermore, health care organizations store information related to personal health, which could result in damaging breaches of privacy if viewed by unauthorized people.

The health care sector ranked fifth for the overall number of identities exposed, accounting for just over one percent. So, like both education and government sectors, data breaches within the health care sector are less likely to lead to large-scale identity theft than those in other sectors because they expose less identity theft-related data.

During the first half of 2007, the retail/wholesale sector accounted for only six percent of all data breaches that could lead to identity theft, making it the fifth ranked sector during this period. However, the sector was responsible for the largest number of exposed identities, accounting for 85 percent of the total. Breaches in this sector were thus more likely to lead to large-scale identity theft than any other sector. Each data breach would facilitate identity theft to a much greater degree.

The prominence of the retail/wholesale sector was primarily due to the data breach involving the TJX group of retail companies.[29] TJX was a victim of an extensive attack that exposed over 45 million credit and debit card numbers. The number of identities exposed through this breach alone made up over 70 percent of all identities exposed during the period. Due to the nature and extended time span of the compromise, it is likely that these breaches were due to a failure of effective security policies.[30]

Breaches like this may be less likely to occur in the future as the Payment Card Industry (PCI) Data Security Standard (DSS) becomes more widely adopted.[31] The PCI DSS requires vendors accepting payment through credit cards to implement various security measures to protect credit card data.[32] This includes, among other things, the use of strong encryption to transmit credit card data through open networks. In the case of the TJX breach discussed above, the data breach was likely caused by a failure of the company to use secure encryption to protect data transmitted over a wireless network.[33]

Different legislative bodies have also begun passing laws that have been influenced by the PCI DSS. The state of Texas is currently hoping to pass a law that will put PCI DSS into effect.[34] In spring 2007, the state of Minnesota passed the Plastic Card Security Act.[35] The act holds the organizations that collect or manage data that may be exposed in data breaches to also be responsible for the costs of repairing the damages caused by the breach.

[29] http://www.securityfocus.com/brief/441
[30] http://www.theregister.co.uk/2007/05/04/txj_nonfeasance/
[31] Payment Card Industry (PCI) Compliance is a set of security standards that were created by numerous major credit card companies to protect their customers from increasing identity theft and security breaches. For more information, please see http://www.pcicomplianceguide.org/businesscompliance.html
[32] https://www.pcisecuritystandards.org/tech/
[33] http://www.securityfocus.com/brief/496
[34] http://pcidss.wordpress.com/2007/05/11/pci-codified-into-texas-law-nearly/
[35] http://computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=standards_and_legal_issues&articleId=293804&taxonomyId=146

The added consideration of punitive costs may influence large companies to more adequately secure data for which they are deemed responsible, and therefore help reduce the number of breaches overall. However, it is worth noting that this will likely be enforceable only with large breaches, as it may be difficult to trace the source of most instances of identity theft with the breach that originally exposed the identity. Furthermore, Minnesota's Plastic Card Security Act only applies to companies that process more than 20,000 transactions per year. As such, attackers may target smaller companies in the future.

Data breaches that could lead to identity theft by cause

In the first 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 backup medium (figure 3). These made up 46 percent of all such data breaches during this period. Theft or loss accounted for 57 percent of all reported breaches in the previous reporting period. Despite the high percentage of breaches, the theft of loss of computers and storage media only accounted for 11 percent of all identities exposed. Thus, although theft or loss of computers and storage media is extremely common, it can be considered less likely to lead to large-scale identity theft than other causes, as it results in relatively fewer exposed identities.

This is likely because, in many cases, theft or loss of a computer or storage media is driven not by a desire to steal data, but to steal the hardware itself. A person who steals a laptop is likely driven by the desire to simply sell the laptop for financial gain, and not to harvest the data it may store.

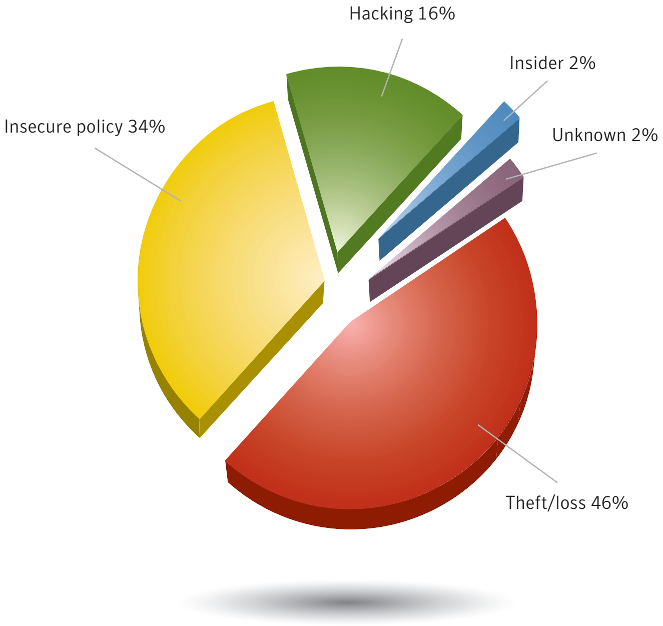

Figure 3. Data breaches that could lead to identity theft by cause
Source: Based on data provided by Attrition.org

The second most common cause of data breaches that could lead to identity theft during this period was insecure policy, which made up 34 percent of all incidents. For the purposes of this discussion, insecure policy is defined as a failure to develop, implement, and/or comply with adequate security policy. An example of insecure policy would be exposing information that could lead to identity by emailing unencrypted data to an unauthorized recipient or posting it on a publicly available Web site. In the previous period, insecure policy also ranked second, accounting for 27 percent of such data breaches.

In the first half of 2007, insecure policy accounted for only three percent of exposed identities. Thus, each breach exposed relatively little personal identity information. This implies that breaches caused by insecure policy are not likely to lead to large-scale identity theft.

In the first six months of 2007, hacking was the third leading cause of data breaches that could lead to identity theft, accounting for 16 percent of the total. 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 the last six months of 2006 hacking also ranked third, accounting for 11 percent of breaches that could facilitate identity theft.

Hacking was responsible for 73 percent of identities exposed during the period (figure 4). The prominence of hacking as a cause of exposed identities was largely driven by the TJX breach that was discussed previously in this section.[36] This high percentage indicates that hacking is more likely to result in wide-scale identity fraud than other causes of data breaches. This is likely because hacking is more clearly purpose-driven than insecure policy or the loss or theft of devices. It is an intentional act with a clearly defined purpose: to steal data that can be used for purposes of identity theft or other fraud.

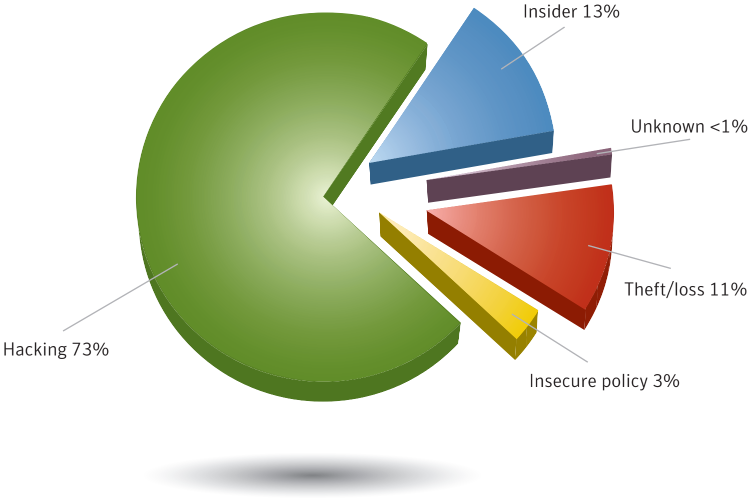

Figure 4. Exposed identities by cause
Source: Based on data provided by Attrition.org

[36] http://www.boston.com/business/ticker/2007/01/tjx_intruders_s.html

Security policies, such as the PCI DSS discussed earlier, can help to protect data and prevent breaches caused by everything from hacking to theft and loss. The measures recommended by the PCI DSS are standard security best practices; they are discussed in detail in the following paragraphs.[37]

Organizations should use strong encryption to store identity-related data. This would ensure that even if the data is lost or stolen, it would not be accessible to unauthorized third parties. This step 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. Furthermore, policies that ensure that computers containing sensitive information are kept in secure locations and are accessed only by authorized individuals should be put in place and enforced. Sensitive data should not be stored on mobile devices that could be easily misplaced or stolen.

Implementing secure policies surrounding networks and the communication of sensitive data can prevent breaches that may lead to identity theft perpetrated by attackers. Strong encryption should always be used to communicate sensitive data over networks.

Organizations can further protect against security breaches that may lead to identity theft from attackers by employing defense-in-depth strategies, including the deployment of IDS/IPS solutions, antivirus and antifraud solutions and a firewall. Antivirus definitions should be updated regularly and all desktop, laptop, and server computers within an organization should be updated with all necessary security patches from their respective vendors.

To help prevent accidental or intentional data leaks, organizations should employ data leakage prevention solutions. Symantec also advises that organizations implement policies that prevent users from viewing, opening, or executing 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.

Top countries targeted by denial of service attacks

Denial of service (DoS) attacks are a significant threat to government organizations. A successful DoS attack can render Web sites or other network services inaccessible to users and employees. This could result in the disruption of internal and external communications, making it difficult or impossible for employees and users to access potentially critical information. It could also result in significant damage to the organization’s reputation that could severely undermine people’s confidence in government competence, defense of government networks, and national security issues.

Although there are numerous methods for carrying out DoS attacks, for the purposes of this discussion, Symantec gauges them by measuring attacks that are carried out by flooding a target with SYN requests.[38] This type of attack works by overwhelming a target with SYN requests and not completing the initial request, which prevents other valid requests from being processed.

In many cases, SYN requests with forged IP addresses are used to carry out an attack, allowing a single attacking computer to initiate multiple connections. This results in unsolicited traffic, known as backscatter, being sent to other computers on the Internet (whose IP addresses were spoofed). Symantec uses this backscatter to determine the number of computers targeted by DoS attacks. Backscatter is only one method of obtaining DoS statistics and for the purposes of this report is only intended to provide a high-level overview of overall DoS activity.

[37] https://www.pcisecuritystandards.org/tech/pci_dss.htm
[38] The TCP protocol requires a three-way exchange to be carried out before any data is sent. The SYN request is the first phase of the three-way exchange. Once a SYN request is received by a server, a SYN-ACK is sent in response. The final step is an ACK response, completing the connection negotiation process.

DoS attacks that are not driven by profit may be motivated by social or political ends. An attack that disrupts the availability of a high-profile Web site, particularly one belonging to a government organization, will get much wider notice than one that takes a single user offline. Some DoS attacks may be used as a means to express the attacker's disagreement with actions or policies associated with the targeted organization.

Governments are often targeted by these attacks. There have been numerous examples of DoS attacks against governments or transnational organizations such as the World Trade Organization.[39] DoS attacks could also be used by governments, militaries, or other groups in the form of sponsored attacks. Although Symantec has limited visibility into such attacks, media reports suggest that DoS and other attacks can and do occur.[40]

At a military and tactical level, DoS attacks are likely to be unsuccessful due to highly sophisticated and redundant communications networks. However, when these types of attacks target public infrastructures that are used by governments or other critical infrastructure organizations, they can meet with some measure of success. In the event of such an attack, important governmental and critical infrastructure communications may be disrupted.

Symantec tracks the geographic location of targets of DoS attacks. Insight into the locations targeted by these attacks is valuable in determining global trends in DoS attack patterns. It may also help administrators and organizations in affected countries to take the necessary steps to protect against or minimize the effects of DoS attacks.

Between January 1 and June 30, 2007, the United States was the target of the most DoS attacks, accounting for 61 percent of all attacks during this period (table 4). The prominence of the United States as a target is not surprising. The country's extensive broadband Internet infrastructure and its high proportion of Internet-connected organizations make it a very attractive target. Also, based on the number of registered domain names, the United States has the most Web sites in the world, with over 55 million.[41] With such a high number of Web sites, the opportunity for a DoS attack is greatly increased. This, along with the fact that a number of high-profile Web-based organizations are based there, likely explains why the United States is the target of so many of these attacks.

Current Rank	Previous Rank	Country	Current Proportion	Previous Proportion
1	1	United States	61%	52%
2	2	United Kingdom	12%	12%
3	3	China	8%	12%
4	4	Germany	2%	3%
5	7	Canada	2%	2%
6	9	Netherlands	2%	2%
7	6	France	2%	2%
8	11	Australia	1%	1%
9	10	Italy	1%	1%
10	13	Spain	1%	1%

Table 4. Top countries targeted by DoS attacks
Source: Symantec Corporation

[39] For example, please see http://www.wired.com/news/politics/0,1283,43137,00.html
[40] http://www.terra.net.lb/wp/Articles/DesktopArticle.aspx?ArticleID=260955&ChannelId=16
[41] http://www.webhosting.info/domains/country_stats

The current global political climate also makes the United States a popular target of DoS attacks. The United States is a political, economic, and military superpower, which makes it a very high-profile target. It is likely that many DoS attacks targeting computers based in the United States are intended to express disagreement with policies developed and implemented by the United States government. They may also represent an attempt to disrupt the execution of those policies.

The United Kingdom was targeted by the second highest number of DoS attacks, accounting for 12 percent of the worldwide total. This is the same percentage and rank as in the second half of 2006. The United Kingdom is likely targeted for similar reasons as the United States.

China was targeted by the third highest number of DoS attacks in the first half of 2007, accounting for eight percent of all detected attacks, down from 12 percent in the previous period. The prominence of China is likely related to its burgeoning Internet infrastructure. Broadband use there is currently expanding rapidly, as it added more broadband connections than any other country in the world between May 2006 and May 2007.[42] Furthermore, China has the second highest number of broadband users in the world.[43] It currently accounts for 13 percent of the world's users and is expected to surpass the United States in users in the next year.[44]

As was noted for the United States and United Kingdom, DoS attacks against targets in China may be politically motivated. China is emerging as a global economic, political, and military power. DoS attackers may be targeting organizations in China because they disagree with policies that are developed and implemented by the Chinese government.

Organizations should ensure that a documented procedure exists for responding to DoS events. One of the best ways to mitigate a DoS attack is to filter upstream of the target. For most organizations, this filtering will involve working in conjunction with their ISP. Symantec also recommends that organizations perform egress filtering on all outbound traffic. DoS victims frequently need to engage their upstream ISP to help filter the traffic to mitigate the effects of attacks.

Bot-infected computers

Bots are programs that are covertly installed on a user's machine in order to allow an attacker to remotely control the targeted system through communication channels such as IRC. These channels allow the remote attacker to compromise and control a large number of computers over a single, reliable channel in a bot network, which can then be used to launch coordinated attacks.

Bots are a significant threat to government organizations. Bot-infected computers that have penetrated a government organization's network can be used to harvest potentially sensitive data and/or gain access to sensitive software and hardware resources. Government organizations may be particularly valued by attackers because they often house collections of data gathered from numerous other government or critical infrastructure resources. This can be especially valuable for financially motivated attackers, who use confidential information to perpetrate online fraud—such as identity theft and phishing—that can be facilitated by such data.

[42] http://www.point-topic.com
[43] http://www.point-topic.com/contentDownload/dslanalysis/world%20broadband%20statistics%20q1%202006.pdf (access requires registration)
[44] http://www.internetworldstats.com/stats3.htm

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. Between January 1 and June 30, 2007, Symantec observed an average of 52,771 active bot-infected computers per day (figure 5), a 17 percent decrease from the previous reporting period.

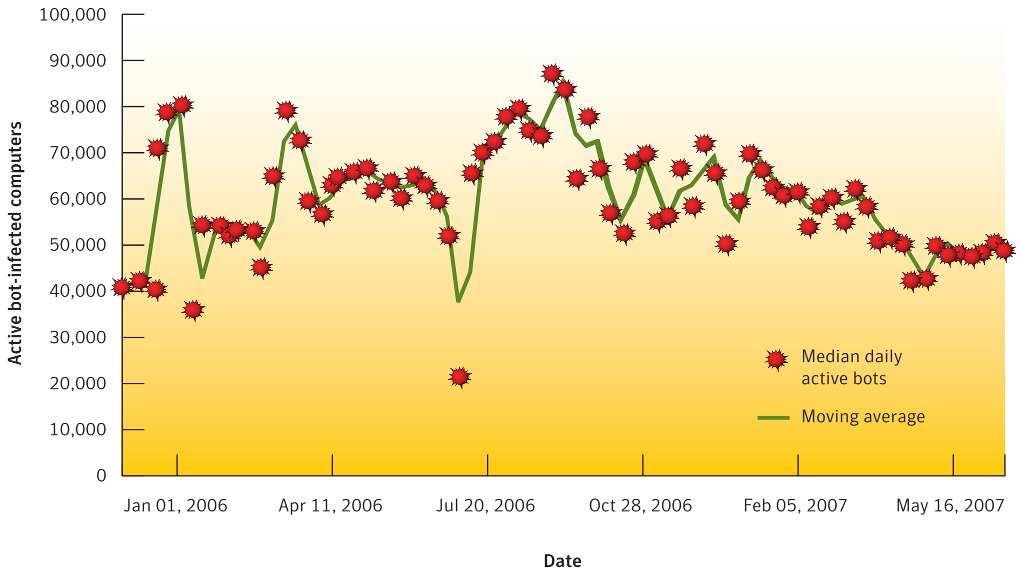

Figure 5. Active bot-infected computers per day
Source: Symantec Corporation

A distinct bot-infected computer is a computer that was active at least once during the period. Symantec observed 5,029,309 distinct bot-infected computers during this period, a 17 percent decrease from the last six months of 2006.

The decrease in bots observed over the past six months is likely due to a change in bot attack methods. As has been discussed in previous volumes of the Symantec *Internet Security Threat Report*, the exploitation of network-based vulnerabilities to spread bots is being slowly abandoned for methods that are more likely to succeed, such as bots that send a mass mailing of themselves.[45] Network-based attacks have been limited somewhat by the introduction of default firewalls in popular operating systems such as Microsoft® Windows® XP, as well as an increasing awareness of computer security issues among organizations and computer users. As a result, their use has declined, which has had the effect of limiting the propagation of bots.

Furthermore, law enforcement initiatives targeting bot networks may also be having some effect. Recently the Federal Bureau of Investigation (FBI) in the United States released information on Operation Bot Roast.[46] This is an ongoing initiative aimed at dismantling bot networks by identifying and arresting bot network owners and taking down the command-and-control servers with which they control their networks. Initiatives such as these could result in a reduction in bots for a number of reasons. Firstly, as bot networks are dismantled, less bot activity will be observed. Secondly, as bot network owners become aware of the scrutiny of law enforcement agencies, they are likely to alter their tactics to avoid detection.

[45] For instance, please see 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. 30
[46] http://www.fbi.gov/pressrel/pressrel07/botnet061307.htm

Bot-infected computers and bot networks have the potential to be problematic for government and critical infrastructure organizations in a number of different ways. The versatility of bot software allows an attacker to remotely control a compromised system. As a result, the possibilities for their use are nearly limitless.

Bots may be used to carry out DoS attacks against government resources as well as organizations that are identified as critical infrastructure sectors. They can also be used in a coordinated effort to gain access to sensitive critical infrastructure systems, such as military, transportation, and utilities and energy. Once access to an organization's network has been obtained, an attacker or bot network owner could easily inflict damage on critical systems, which could result in the destruction, theft, or alteration of confidential or sensitive information.

In some cases, access to confidential information by authorized personnel may be denied or altered, allowing attackers to impose their own command, control, and communication processes on the compromised systems. This could result in the loss of situational awareness. Were such an attack to be state or group sponsored, access to critical infrastructures could be used to disable key services as a prelude to a larger event or attack.

Bot networks can also be used to harvest information in order to facilitate identity theft.[47] There have been several examples of attackers compromising government and military computers to gain access to potentially sensitive information.[48] Such information could be used for strategic purposes in the case of state- or group-sponsored attacks.

Identity theft-related data breaches are particularly sensitive for government and critical infrastructure organizations. Many organizations in these sectors house a significant amount of sensitive personal information that could be used to facilitate identity theft. Furthermore, organizations such as these are often large and complex, which presents increased opportunities for attackers to use social engineering techniques to gain access to potentially sensitive information. As a consequence, attackers targeting this type of data may focus their efforts on government, health care, and other critical infrastructures.

To reduce exposure to bot-related attacks, end users should employ defense-in-depth strategies, including the deployment of antivirus software and a firewall. Creating and enforcing policies that identify and limit applications that can access the network may also help to limit the spread of bot networks. Users 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. 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.

[47] Toxbot is an example of bot network software designed to harvest information for identity theft purposes. For more information on Toxbot, please see http://www.symantec.com/security_response/writeup.jsp?docid=2005-031012-0442-99

[48] http://www.information-age.com/home/information_age_today/hackers_steal_US_gov_information

Lifespan of bot-infected computers

For the first time, in this volume of the *Internet Security Threat Report*, Symantec is assessing the average lifespan of bot-infected computers. The lifespan of a bot is defined as the amount of time that elapses between the first detection of a bot-infected computer and the time that the computer is no longer actively attacking for 30 days, after which time it is assumed to have been disinfected. Gauging the average lifespan of bot-infected computers is important because it allows Symantec to assess how long bot-infected computers are present on a particular network prior to removal.

During the first six months of 2007, the lifespan of the average bot-infected computer was four days (figure 6). This is an increase from the previous period, when the average lifespan was three days. The median lifespan of a bot-infected computer during both periods was one day, which was the same as during the last six months of 2006. This indicates that the majority of bot-infected computers only participated in attacking behavior for a short period, after which they are either identified and disinfected, or are used for activities other than carrying out Internet attacks, such as hosting spam zombies or phishing Web sites. The longest lifespan of a bot-infected computer during the period was 3.2 years. However, bots with such long life spans are rare.

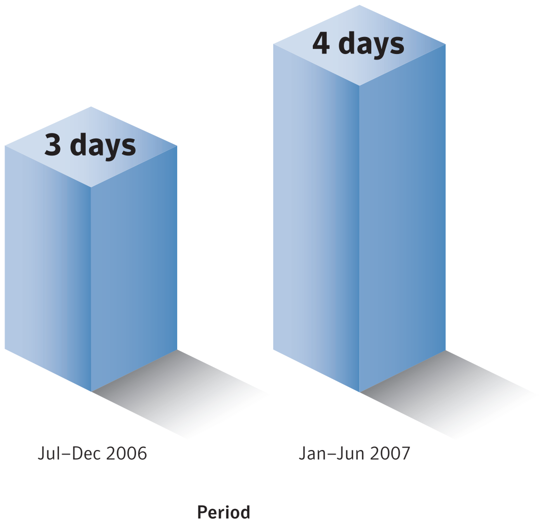

Figure 6. Average lifespan of bot-infected computers
Source: Symantec Corporation

The increase in the average lifespan from three to four days is likely not indicative of a fundamental change. Since the median remained the same, the change in overall average is driven by the longer-lasting bot-infected computers. The increased lifespan of the longer-lasting bot-infected computers has thereby increased the average lifespan. Thus, the bot lifespan is holding steady.

It therefore appears that law enforcement efforts, such as the FBI Bot Roast (which was discussed previously in this document) are not reducing the lifespan of bot-infected computers. This is likely because the focus of those methods is to eliminate infections and keep infected computers free of bot software, and not necessarily to shorten their effective lives. This is supported by the fact that the number of bot-infected computers has decreased during the period (as was discussed in the "Bot-infected computers" section of this report) while their lifespan remains steady.

Bot-infected computers by country

Recognizing the ongoing threat posed by bot networks, Symantec tracks the distribution of bot-infected computers worldwide. This can help analysts understand how bot-infected computers are distributed globally. This is important, as a high percentage of bot-infected computers means a greater potential for bot-related attacks. It could also provide insight into the level of patching and security awareness amongst computer administrators and users in a given region, as initial bot infections usually take advantage of unpatched computer systems.

China had the highest number of bot-infected computers during the first half of 2007, accounting for 29 percent of the worldwide total (table 5). This is a moderate increase from 26 percent in the second half of 2006, when China also had the highest number of bot-infected computers.

Current Rank	Previous Rank	Country	Current Percentage	Previous Percentage	Average Bot Lifespam (Days)
1	1	China	29%	26%	3
2	2	United States	13%	14%	10
3	4	Germany	9%	6%	1
4	5	Spain	6%	5%	2
5	3	France	5%	6%	2
6	12	Italy	4%	2%	3
7	6	United Kingdom	4%	4%	3
8	10	Canada	3%	2%	19
9	13	Israel	3%	2%	3
10	8	Poland	3%	3%	3

Table 5. Bot-infected computers by country
Source: Symantec Corporation

Symantec has observed that bots usually infect computers that are connected to high-speed broadband Internet through large ISPs and that the expansion of broadband connectivity often facilitates the spread of bots. China's Internet infrastructure is currently expanding rapidly.[49] In fact, between May 2006 and May 2007, China added more broadband lines than any other country.[50] China currently has the second highest number of Internet users in the world, with 13 percent of the total.[51]

[49] http://www.vnunet.com/vnunet/news/2163552/china-lead-broadband-world
[50] This data was provided by Point Topic. For more information, please go to http://www.point-topic.com
[51] http://www.internetworldstats.com/stats3.htm

In the first half of 2006, the percentage of worldwide bot-infected computers situated in China increased from nine percent to 20 percent. In the second half of 2006, the rate of increase slowed six percentage points, from 20 percent to 26 percent. In the first half of 2007, it went up only three percentage points. This may be a sign that security awareness, practices and infrastructure are beginning to catch up with the rapid growth of Internet usage in China.

In the first six months of 2007, the United States had the second highest number of bot-infected computers, accounting for 13 percent of the worldwide total. This is almost unchanged from the second half of 2006, when the United States ranked second, accounting for 14 percent of the world's bot-infected computers.

It is not surprising that the United States was the site of the most bot-infected computers, as 18 percent of the world's Internet users are located there, more than any other country.[52] Furthermore, it has a well established and relatively long-standing Internet infrastructure. As a result, not only are there a lot of attackers there, but they have had a long time to understand the technologies and to hone their skills.

Germany had the third highest number of bot-infected computers during this period, accounting for nine percent of the worldwide total. During the second half of 2006, Germany ranked fourth and accounted for six percent of the world's bot-infected computers. Like both China and the United States, Germany has a well established Internet infrastructure. Furthermore, it has the fourth highest number of Internet users in the world, boasting five percent of the world's Internet users.[53]

Command-and-control servers by country

Command-and-control servers are computers that bot network owners use to relay commands to bot-infected computers on their networks. Symantec tracks the global distribution of bot command-and-control servers. During the first half of 2007, the United States had the most known command-and-control servers worldwide (table 6), accounting for 43 percent of the worldwide total. This is a marginal increase from the previous period, when the United States was also the site of the most command-and-control servers, accounting for 40 percent of the worldwide total.

The high proportion of command-and-control servers in the United States indicates that servers there likely control not only bot networks within the country but elsewhere as well. The high proportion of bot-infected computers and command-and-control servers in the United States is driven by that country's extensive Internet and technology infrastructure. As of June 2006, more than 58 million broadband Internet users were located there, the highest number in the world.[54]

[52] http://www.internetworldstats.com/stats14.htm
[53] http://www.internetworldstats.com/stats4.htm
[54] http://www.oecd.org/document/7/0,3343,en_2649_34223_38446855_1_1_1_1,00.html

Current Rank	Previous Rank	Country	Current Proportion	Previous Proportion
1	1	United States	43%	40%
2	3	Germany	7%	6%
3	5	Canada	7%	4%
4	2	South Korea	6%	10%
5	4	China	3%	5%
6	9	United Kingdom	3%	2%
7	6	Taiwan	3%	3%
8	10	Italy	2%	2%
9	7	Sweden	2%	3%
10	11	Turkey	2%	2%

Table 6. Command-and-control servers by country
Source: Symantec Corporation

Germany had the second highest number of command-and-control servers in the first six months of 2007, accounting for seven percent of the worldwide total. This is a slight change from the previous six-month period when Germany accounted for six percent of worldwide command-and-control servers and ranked third in the world.

During the current reporting period, Canada had the third most command-and-control servers in the world, accounting for seven percent of the total. This is an increase from the second half of 2006, when Canada ranked fifth and accounted for four percent of the world's total.

Top countries of attack origin

This section will discuss the top countries of attack origin. This metric only discusses the location of the computer from which the attack originates and not the actual location of the attacker. While it is simple to trace an attack back to the computer from which it was launched, that computer may not be the attacker's own system. Attackers frequently hop through numerous systems or use previously compromised systems to obscure their location prior to launching the actual attack. For example, an attacker in China could launch an attack from a compromised system located in South Korea against a Web server in New York. Further complicating the matter is that international jurisdictional issues often prevent proper investigation of an attacker's real location.

Over the first six months of 2007, the United States was the top country of attack origin, accounting for 25 percent of worldwide attack activity (table 7). This represents a decrease from 33 percent during the last half of 2006. Although it is impossible to identify a single cause for the decrease, it is likely that it is at least partly due to the FBI Bot Roast program, which was discussed earlier in this report.

The prominence of the United States as a country of attack origin is likely due to its large population of Internet users. Further, attackers in the United States have had a longer period to develop the knowledge, skills, and methods to conduct sophisticated attacks than those in some other countries.

Current Rank	Previous Rank	Country	Current Percentage of Events	Previous Percentage of Events
1	1	United States	25%	33%
2	2	China	13%	11%
3	3	Germany	8%	7%
4	4	France	6%	6%
5	6	United Kingdom	5%	5%
6	7	Spain	5%	4%
7	5	Canada	4%	5%
8	10	Italy	3%	2%
9	12	Brazil	2%	2%
10	8	Japan	2%	3%

Table 7. Top countries of attack origin
Source: Symantec Corporation

In an effort to limit attack activity in the country, the United States has had legislation in place since the 1986, when the Computer Fraud and Abuse Act passed into law. Furthermore, the Cyber Security Enhancement Act of 2002 was enacted to increase sentences for computer crimes under the Computer Fraud and Abuse Act. Although there have been many convictions under these laws,[55] they appear to have had little effect on attack activity within the country, as is illustrated by the high number of attacks originating in the United States.

The second highest number of attacks detected in the first half of 2007 originated in China, which accounted for 13 percent of all attacking IP addresses. This is a slight increase from the previous period when China accounted for 11 percent of attacking IP addresses. The high number of attacks that originated in China is likely driven by the rapid broadband Internet growth that is taking place there.[56] In fact, between May 2006 and May 2007, China added more broadband lines than any other country.[57] China currently has the second highest number of Internet users in the world, with 13 percent of the total.[58] It is also likely due to the high number of bot-infected computers there, many of which would be used to launch attacks against computers in other countries.

China has had computer crime laws in place since 1997.[59] Despite these laws, China has continued to account for a high percentage of worldwide attack activity over the past two years.[60] This is an indication that, as has been the case in the United States, computer crime laws do not effectively deter computer criminals and attackers. Attacks originating from China are likely motivated by profit, and will likely remain prominent until such activity is no longer profitable.

Germany was the country of origin of the third highest number of attacks in the first half of 2007, accounting for eight percent of all attacking IP addresses. This is a marginal change from the previous period when Germany accounted for seven percent of all attacking IP addresses. Germany has the fourth highest number of broadband Internet users in the world, which may account for its high attack levels.[61]

[55] http://www.msnbc.msn.com/id/6719246/
[56] http://www.vnunet.com/vnunet/news/2163552/china-lead-broadband-world
[57] This data was provided by Point Topic. For more information, please go to http://www.point-topic.com
[58] http://www.internetworldstats.com/stats3.htm
[59] http://www.cybercrimelaw.net/laws/countries/china.html
[60] For example, please see the Symantec *Government Internet Security Threat Report* (March 2007): http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_govt_03_2007.en-us.pdf : p. 23
[61] http://www.point-topic.com

In general, Europe has high levels of Internet connectivity, which is a necessary precondition to elevated levels of attack activity. Like China and the United States, Germany has several laws regarding computer crime;[62] however, also like those countries, those laws do not seem to be effectively deterring attackers from carrying out attacks. As with China and the United States, these attacks are likely profit driven and will also likely remain prominent until such activity is no longer profitable.

Top countries of origin for government-targeted attacks

Attacks targeting government are driven by a number of factors. The first is criminal intent, as governments store considerable amounts of personal identification data that could be used for fraudulent purposes, such as identity theft. Government databases also store sensitive information that could facilitate criminal activities. This could include critical infrastructure information, sensitive but unclassified information, or other intelligence. In the first half of 2007, the government sector ranked second and accounted for 26 percent of all identity theft-related data breaches.

The second factor motivating attack activity against government targets is political. Government organizations often have a high profile in their region or country. Attacks may target government organizations in order to deny crucial communications services as a means of expressing disagreement with policies and programs that the government has developed and implemented. These attacks are likely a form of protest and are also likely to be made up of attacks such as DoS attacks. For example, during the first half of 2007, the government sector was the sector most frequently targeted by DoS attacks, accounting for 30 percent of all detected attacks. Some attacks, on the other hand, may simply be mischievous in nature. While such attacks may have relatively innocuous intentions, they may still result in the disruption of critical services or the exposure of highly sensitive information.

The top country of origin for attacks detected by sensors based in the government sector in the first half of 2007 was the United States, which accounted for 19 percent of the total (table 8). Attacks against government organizations that originated in the United States are six percentage points lower than Internet-wide attacks originating there. This indicates that attacks originating from within the United States are not targeting the government sector in particular.

[62] http://www.cybercrimelaw.net/laws/countries/germany.html

Current Rank	Previous Rank	Country	Current Percentage of Events	Previous Percentage of Events
1	1	United States	19%	20%
2	3	Spain	14%	11%
3	2	France	10%	12%
4	5	Germany	9%	8%
5	6	Italy	7%	5%
6	4	China	6%	8%
7	7	United Kingdom	4%	4%
8	10	Canada	3%	3%
9	13	Israel	3%	2%
10	12	Poland	3%	2%

Table 8. Top countries attacking government sectors
Source: Symantec Corporation

Spain accounted for 14 percent of attacks targeting government, which is nine percentage points higher than the proportion of total attacks originating there. This indicates that a disproportionate number of attacks originating in Spain target the government sector. There are a number of factors that likely contribute to this.

Spain has experienced a 23 percent increase in broadband connections between May 2006 and May 2007, adding over 1.3 million broadband users during that period.[63] In previous volumes of the *Internet Security Threat Report*, Symantec has observed that a rapid increase in broadband often coincides with a rapid increase in malicious Internet activity such as network-based attacks and bot-infected computers.[64] This is because rapidly expanding ISPs are more likely to focus their resources on meeting growing demand at the expense of implementing security measures, such as port blocking and ingress and egress filtering. As a result, ISPs that are expanding their services rapidly may have security infrastructures that are underdeveloped relative to their needs.

Over the past several reporting periods, malicious activity in Spain has increased noticeably. The country ranked seventh for worldwide malicious activity and fifth for malicious activity per Internet user during this reporting period.

Some of this malicious activity may also involve politically motivated attacks. Politically motivated attacks are likely to be carried out for a number of reasons including blocking access to government Internet-based resources, gaining access to potentially sensitive information, and discrediting the government itself.

The current political climate in Spain may contribute to the high number of attacks targeting the government there. A ceasefire between the national government of Spain and the militant Basque separatist movement known as the Euskadi Ta Askatasuna, or ETA, was threatened by violence early in 2007.[65] The government's attempts to work towards peace with the ETA have met with widespread opposition among the non-Basque population in Spain.[66] This issue is likely to contribute to attack activity targeting government organizations.

[63] This data was provided by Point Topic. For more information, please go to http://www.point-topic.com
[64] For example, please see the Symantec *Government Internet Security Threat Report* (September 2006): http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_x_09_2006.en-us.pdf : p. 43
[65] http://www.iht.com/articles/2007/01/14/news/spain.php
[66] http://www.iht.com/articles/2007/03/11/news/spain.php

France accounted for 10 percent of attacks targeting government organizations, which is four percentage points higher than the proportion of total attacks originating from there. The discrepancy, although less significant than that of Spain, indicates that attacks originating from France are targeting government organizations.

France, like Spain, increased its Internet infrastructure substantially between May 2006 and May 2007, increasing it by 23 percent, or just over 2.5 million new users.[67] Also, France had the fifth most malicious activity worldwide during this period, as well as the ninth most malicious activity per Internet user.

Despite ranking highly in overall worldwide malicious activity as well as worldwide attack activity, China ranked only sixth for attacks targeting the government sector. Furthermore, China's ranking dropped from the fourth position in the last six months of 2006. As discussed in the previous *Government Internet Security Threat Report*, this is surprising for a number of factors. China is a world economic, political, and military power. Given this, it would be reasonable to conclude that the Chinese government may be targeted by attacks that were intended to express opposition to its policies. However, this appears not to be the case.

In the previous *Government Internet Security Threat Report*, Symantec speculated that this may because the majority of attacking computers in China are targeting organizations with the intent of generating profit. Symantec concluded this because China had the highest number of bot-infected computers in the world during this period, but only the fourth highest number of command-and-control computers. During this period, this gap has widened, as China dropped to the fifth highest number of bot command-and-control servers. This would indicate that many of the attacks originating in China are coming from computers that are controlled by servers—and possibly attackers—outside the country. As a consequence, these attacks are likely motivated by profit rather than politics, so that targets within government organizations are not a priority.

Attacks by type—notable critical infrastructure sectors

This section of the *Government Internet Security Threat Report* will focus on the types of attacks detected by sensors deployed in notable critical infrastructure sectors. After outlining the attacks against government and critical sectors as a whole, the following sectors will be discussed in detail:

- Government
- Biotech/pharmaceutical
- Health care
- Financial services
- Transportation

The ability to identify attacks by type assists security administrators in evaluating which assets may be targeted. In doing so, this may assist security administrators in focusing attention on those assets receiving a disproportionate number of attacks.

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

Critical infrastructure organizations are the target of a wide variety of attack types. This reinforces Symantec's assertion that attackers are using numerous methods to compromise and use assets in those sectors. The majority of attacks seen by all sensors in the government and critical infrastructure sectors in the first six months of 2007 were SMTP-based attacks (figure 7), which accounted for 36 percent of the top ten attacks.

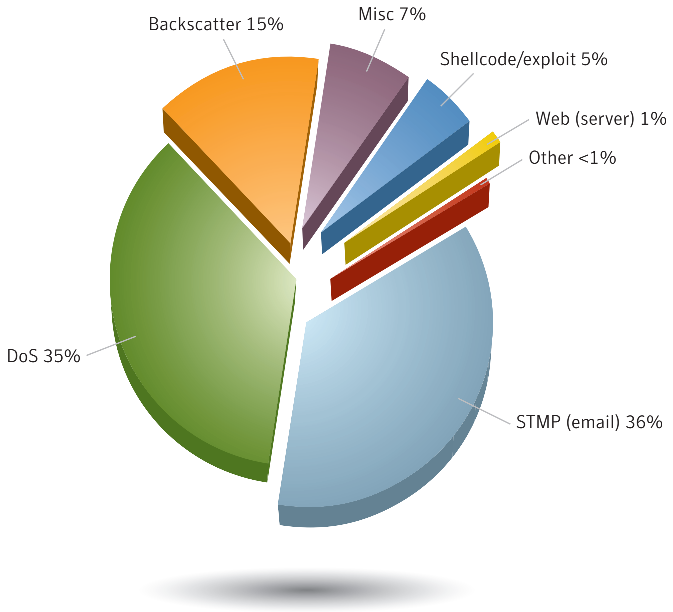

Figure 7. Top ten attack types, government and critical infrastructure
Source: Symantec Corporation

SMTP, or simple mail transfer protocol, is designed to facilitate the delivery of email messages across the Internet. Email servers are likely targeted because, in order to deliver email, external access is required. While most services can be blocked to protect against external attack, allowing access only to trusted users and entities, for email to function effectively it has to be available both internally and externally. The necessity of allowing both internal and external access increases the probability that a successful attack will facilitate access to the network.

Additionally, attackers who are able to compromise email servers can use them to send spam, harvest email addresses for targeted phishing attacks and, in some instances, disrupt email service. Successful SMTP attacks against government organizations could allow attackers to spoof official government communications. Because government and critical information industries rely on email as a communication method, it is essential that they are secured. Symantec recommends that government and critical information industries use secure email protocols. They should also deploy antispam and antifraud solutions and ensure that operating and email solutions are fully patched against all known vulnerabilities.

Top attacks by type—government sector

Backscatter was the most common type of attack observed by sensors deployed in the government sector in the first half of 2007 (figure 8). These attacks made up 66 percent of the top ten attacks observed by government sensors, compared to 22 percent for all government and critical infrastructure sectors.

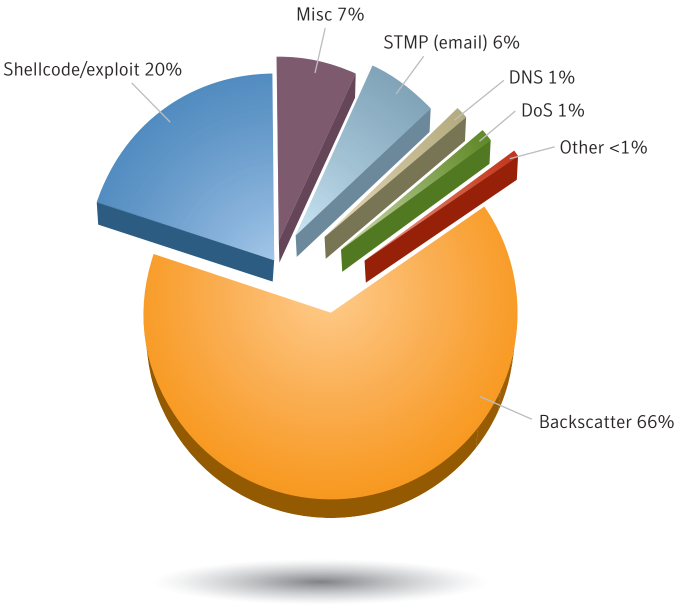

Figure 8. Top ten attack types, government sector
Source: Symantec Corporation

Backscatter, while not a direct attack, is evidence that a DoS attack against another server on the Internet is taking place and is making use of spoofed IP addresses. When one of these spoofed IP addresses matches the address of a Symantec sensor, any error messages that the attacked server sends to the spoofed address will be detected by a Symantec sensor as backscatter.

Generally, backscatter is considered to be a type of Internet background noise,[68] which is typically ignored. However, the percentage of backscatter detected by government sensors is significantly higher than the average detected across all government and critical infrastructure sectors. This may be caused by several factors.

One possible explanation is that stronger policies and procedures are in place to prevent attacks before reaching the network. If potentially malicious traffic is blocked before reaching the network boundary while background noise is ignored, sensors will see a higher percentage of background noise than potentially malicious traffic.

[68] For more information on Internet background noise, see http://www.switch.ch/security/services/IBN/

Another possible explanation for the high percentage of backscatter detected by government sensors may be that attackers launching DoS attacks are intentionally spoofing the IP addresses of government organizations. This may be done to trick the targeted organization into thinking it is being attacked by a government. This tactic may have been used in the first half of 2007 in a number of well documented DoS attacks against Estonia, some of which were said to come from the Russian government.[69] The Russian government denied launching these attacks. However, it may be that the IPs didn't actually belong to the Russian government but were spoofed to make it seem as though the government had launched the attacks.

Top attacks by type—biotech/pharmaceutical sector

The most common attacks detected by sensors deployed in the biotech/pharmaceutical sector in the first six months of 2007 were DoS attacks, which constituted 49 percent of all attacks during this period (figure 9). This is significantly higher than the 35 percent of these attacks that were detected across government and critical infrastructure sectors as a whole during this period.

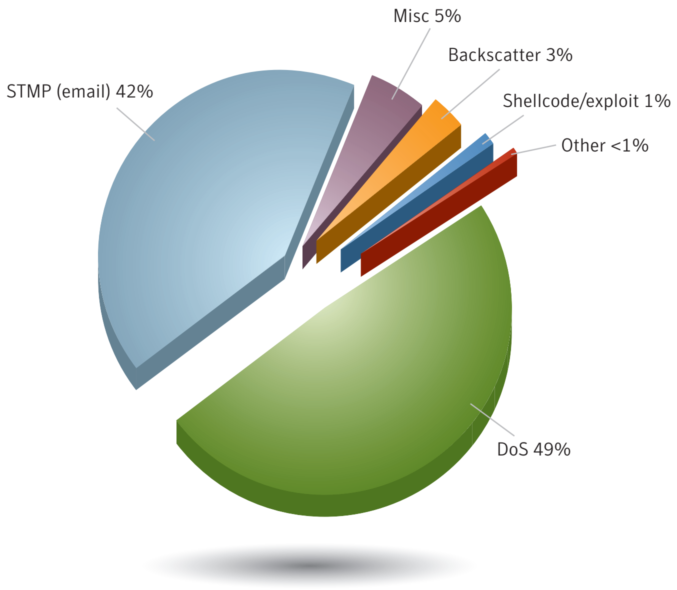

Figure 9. Top ten attack types, biotech/pharmaceutical sector
Source: Symantec Corporation

DoS attacks are often associated with protests, since they are intended to render a site inaccessible in the same way that a physical protest attempts to block access to a service or location. As such, the high percentage of DoS attacks may be an attempt to express disagreement with policies developed and implemented by the targeted organization.

[69] http://www.nytimes.com/2007/05/19/world/europe/19russia.html?ex=1337227200&en=4817e43658c91382&ei=5088

Additionally, some organizations that are categorized as biotech/pharmaceutical companies may rely heavily on an online presence for their operations, particularly online pharmaceutical retailers. These sites may be more liable to be adversely affected by DoS attacks and, as such, targeted by DoS-based extortion schemes. By using a sustained DoS attack to hold this type of site offline, an attacker can disrupt the organization's revenue, and may thus threaten such an attack to extort money from the organization.

Top attacks by type—health care sector

SMTP-based attacks were the most common attacks detected by sensors deployed in the health care sector in the first six months of 2007, accounting for 75 percent of the top ten attacks against the industry (figure 10). This is a higher than the 36 percent of these attacks detected across government and critical infrastructure sectors as a whole during this period, which indicates that attackers using these attacks are specifically trying to compromise email servers in the health care industry. These attacks are likely due to spammers who are attempting to spoof legitimate health care companies in order to sell illegitimate products. If attackers are successful in attempts to send email through compromised servers, consumers could be at risk from misleading or false solicitations, which could in turn affect the reputation of the targeted company.

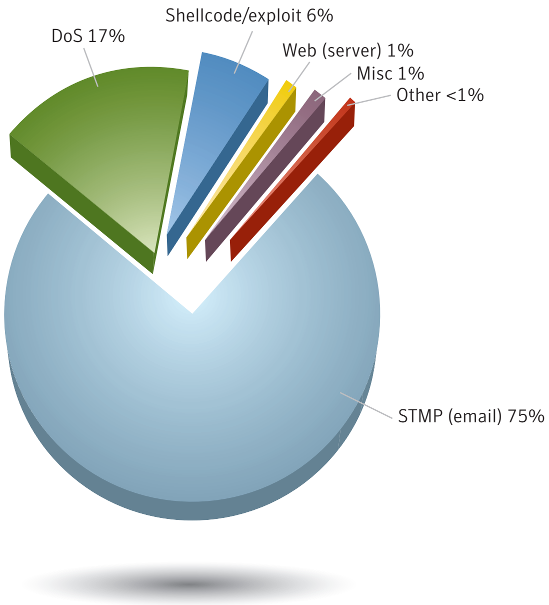

Figure 10. Top ten attack types, health care sector
Source: Symantec Corporation

Top attacks by type—financial services sector

SMTP-based attacks were the most frequent type of attack targeting the financial services sector in the first half of 2007. They accounted for 48 percent of the top ten attacks detected by sensors deployed in the financial services sector (figure 11). Attackers deploying these attacks are likely attempting to compromise email servers for the purpose of sending spam or harvesting email addresses for targeted phishing attacks.

Financial institutions are frequently targeted by phishing attacks, so it is likely that many of the SMTP attacks are related to phishing activity that is attempting to spoof the email addresses of financial institutions. Using an email server that belongs to a financial services institution would lend credibility to a phishing attack targeting the customers of a financial service organization. If phishers are able to take advantage of SMTP servers in financial institutions, it is likely that customers will be more easily phished.

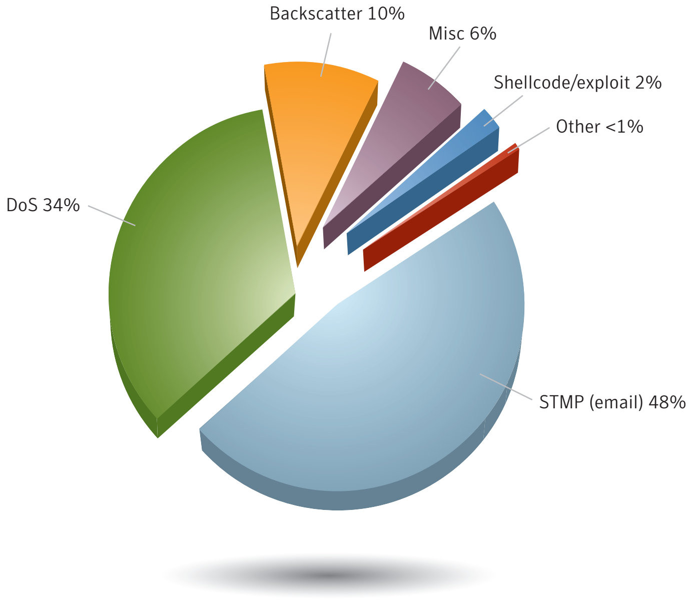

Figure 11. Top ten attack types, financial services
Source: Symantec Corporation

Top attacks by type—transportation sector

During this reporting period, the transportation sector was the target of a high number of DoS attacks (figure 12). Ninety-three percent of the top ten attacks detected by sensors in this sector were identified as DoS attacks, while only 35 percent of top attacks against all government and critical infrastructure were detected as DoS. This indicates that attackers deploying these attacks are targeting the transportation sector specifically. As was discussed in the “Denial of service attacks” section of this report, DoS attacks are generally used to disrupt services and communications. A large-scale attack of this nature could result in the inability to coordinate communications or relief efforts in the event of a national emergency.

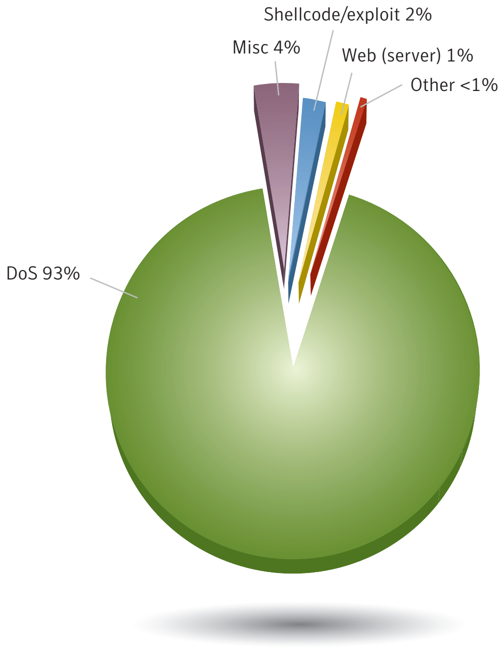

Figure 12. Top ten attack types, transportation sector
Source: Symantec Corporation

Vulnerability Trends

Vulnerabilities are design or implementation errors in information systems that can result in the 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.

New vulnerabilities are discovered and disclosed regularly by a sizeable community made up of end users, security researchers, hackers, security vendors, and, occasionally, by the software vendors themselves. Symantec carefully monitors vulnerability research, tracking vulnerabilities throughout their lifecycle, from initial disclosure and discussion to the development and release of a patch or other remediation measures.

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.[70] Symantec also maintains one of the world's most comprehensive vulnerability databases, currently consisting of over 22,000 vulnerabilities (spanning more than a decade) affecting more than 50,000 technologies from over 8,000 vendors. The following discussion of vulnerability trends is based on a thorough analysis of that data.

This section of the Symantec *Government Internet Security Threat Report* will discuss vulnerabilities that were disclosed between January 1 and June 30, 2007. It will compare them with those disclosed in the previous six-month period, 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
- Zero-day vulnerabilities
- Unpatched enterprise vendor vulnerabilities
- 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 public during this time, computers may be immediately vulnerable to widespread attack. This metric will assess and compare the average patch development times of medium and high-severity vulnerabilities affecting 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™.

Of the five operating systems tracked in the first six months of 2007 (figure 13), Microsoft had the shortest average patch development time at 18 days, based on a sample set of 38 patched vulnerabilities. Of the 38 vulnerabilities, two affected third-party applications. This is lower than the average patch development time of 23 days in the second half of 2006 based on a sample set of 50 vulnerabilities, seven of which affected third-party applications.

[70] The BugTraq mailing list is hosted by SecurityFocus (http://www.securityfocus.com). Archives are available at http://www.securityfocus.com/archive/1

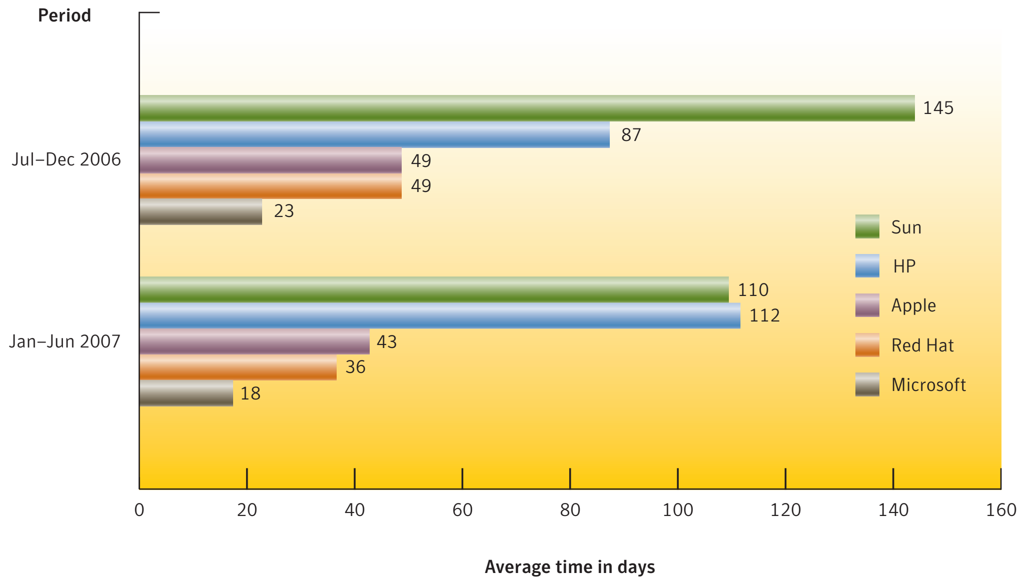

Figure 13. Patch development time for operating systems
Source: Symantec Corporation

Red Hat had the second shortest average patch development time in the first six months of 2007, with an average of 36 days for a sample set of 91 vulnerabilities. Of these, 90 affected third-party applications. The average patch development time is down from 49 days in the second half of 2006, which was based on 149 vulnerabilities, all of which affected third-party applications.

Apple had the third shortest average patch development time in the first half of 2007; it was 43 days for a sample set of 59 vulnerabilities. Nine of those vulnerabilities affected third-party applications. This is a shorter average patch development time than the 49 days reported in the second half of 2006, which was based on a sample set of 32 vulnerabilities, including 12 that affected third-party applications.

Sun had the fourth shortest average patch development time in the first half of 2007, at 110 days for a sample set of 73 vulnerabilities. Sixty-seven of those affected third-party applications. This figure is down from the 145-day patch development time in the second half of 2006. This was based on a sample set of 35 vulnerabilities, 32 of which affected third-party applications.

HP had the longest average patch development time during this reporting period, at 112 days. This was based on a total of 30 vulnerabilities, 28 of which affected third-party applications. The average patch development time for this period was higher than the 87 days reported in the second half of 2006. The previous period was based on a sample set of 70 vulnerabilities, 68 of which affected third-party applications.

Vulnerabilities affecting third-party applications are still a factor in the average patch development time for operating systems. Vendors with fewer third-party applications to patch generally have an advantage over those whose operating systems comprise many third-party components. However, the vulnerabilities affecting these vendors often affect core proprietary components; therefore, the operating systems are more likely to be vulnerable in their default installation.

The numbers from this and previous volumes of the report demonstrate that Red Hat has had the best track record in dealing with third-party vulnerabilities. This may be due to the extent of their involvement with third-party vendors and the open source community, as they often contribute their own patches and work closely with third-party vendors.

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.

Zero-day vulnerabilities represent a serious threat in many cases because there is no patch available for them and because they will likely be able to evade purely signature-based detection. It is the unexpected nature of zero-day threats that causes concern, especially because they may be used in targeted attacks and in the propagation of malicious code.

In the first half of 2007, Symantec documented six zero-day vulnerabilities (figure 14). In the previous six-month period, Symantec documented 12 zero-day vulnerabilities, whereas in the first half of 2006, only one zero-day vulnerability was documented.

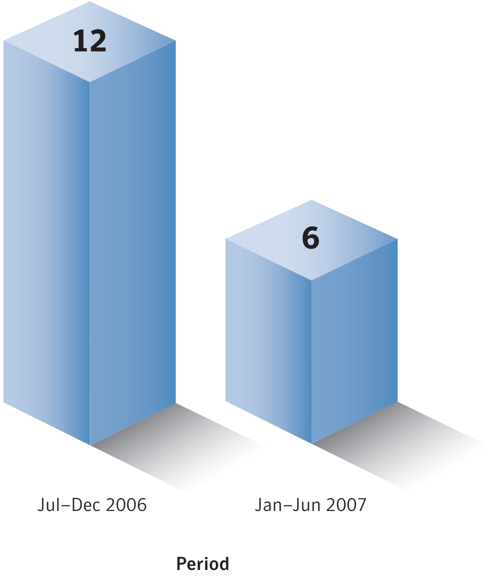

Figure 14. Zero-day vulnerabilities
Source: Symantec Corporation

Of the zero-day vulnerabilities documented during this period, three have affected Microsoft Office applications. This is a drop from the six zero-day vulnerabilities that affected Office in the second half of 2006. The incidence of zero-day Office vulnerabilities may have dropped due to measures taken by Microsoft to patch as many pending Office vulnerabilities as possible.

Microsoft Office has previously been implicated in zero-day attacks against the government sector. In April 2007, the United States Department of State released a statement about a targeted attack on their network that occurred between May and July of 2006.[71] This attack exploited a zero-day vulnerability in Microsoft Word that was addressed by the vendor in August 2006.[72]

In this attack, the attacker employed social engineering to target a specific employee in the East Asia-Pacific region with a malicious document that was crafted to appear relevant to operations in that region. This mode of attack differs from the typical scenario, in which attackers increase their chances of success by casting a wide net over a large number of targets with the belief that compromising a small portion of those targets will yield sufficient returns.

The client-side nature of the vulnerability also limited the number of successful attacks to the number of times the malicious document was opened by potential victims. This instance implies a certain level of confidence and sophistication on the part of the attacker because it appears that a small number of users was targeted and the malicious document would have been opened a limited number of times. The unknown and unpatched nature of zero-day vulnerabilities and the increasing sophistication of attackers suggest that they will likely be deployed in similar low-key targeted attacks.

In Volume IX of the *Internet Security Threat Report* (March 2006), Symantec predicted that a number of official markets and some black markets would emerge for the trading of vulnerability information.[73] Since that report, Symantec has observed the emergence of further venues to sell information about zero-day vulnerabilities.[74] The commercialization of zero-day vulnerabilities is a concern for governments. Various corporate, government, and criminal organizations are competing to acquire information about zero-day vulnerabilities. There is anecdotal evidence that United States government agencies have been involved in the purchase of zero-day vulnerability information.[75]

In order to protect against zero-day vulnerabilities, Symantec recommends that administrators deploy network- and host-based IDS/IPS systems and regularly updated antivirus software. Security vendors may provide rapid response to recently discovered zero-day vulnerabilities in the wild by 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)[76] 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.

[71] http://www.state.gov/m/ds/rls/rm/83256.htm
[72] http://www.theregister.co.uk/2007/04/19/us_state_dept_rooted/
[73] Symantec *Internet Security Threat Report* (March 2006):
http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_ix.pdf : p. 20
[74] http://www.securityfocus.com/news/11474/1
[75] http://www.securityfocus.com/news/11468
[76] 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.

Unpatched enterprise vendor vulnerabilities

In the previous volume of the *Internet Security Threat Report*, Symantec studied the vendor responsiveness to vulnerabilities and found that the majority were not being acknowledged, and therefore patched, by vendors.[77] That analysis provided insight into unpatched vulnerabilities without considering the size of the vendors affected.

This report expands on that analysis by examining 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 reviewed in this section:

- Computer Associates
- 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. Readers should note that the vulnerabilities discussed in this section were known to be unpatched at the time that the data was gathered for this report. They may have been patched in the meantime. It is also possible that some of the 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 mitigations. In many circumstances these measures will not provide complete protection against unpatched vulnerabilities.

In the first half of 2007, Symantec documented 90 unpatched enterprise vulnerabilities that were published during this period (table 9). Of these, 64 affected Microsoft, 13 affected Oracle, four affected Computer Associates, four affected HP, two affected IBM, two affected Symantec, and one vulnerability affected Sun. The rest of the vendors in the enterprise subset had no known vulnerabilities that were unpatched in this period.

[77] 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. 42

Enterprise Vendors	Jan–Jun 2007	Jul–Dec 2006
Microsoft	64	75
Oracle	13	7
Computer Associates	4	0
HP	4	1
IBM	2	5
Symantec	2	1
Sun	1	3
McAfee	0	2

Table 9. Unpatched enterprise vulnerabilities, by vendor
Symantec Corporation

Of the enterprise vulnerabilities published in the second half of 2006, 94 were unpatched. Seventy-five affected Microsoft, seven affected Oracle, five affected IBM, three affected Sun, two affected McAfee, one affected HP, and one vulnerability affected Symantec. No other enterprise vendors had vulnerabilities published during this period that remain unpatched.

Microsoft had the most unpatched vulnerabilities that were disclosed during the second half of 2006 and the first half of 2007. Many of the vulnerabilities in the sample set are considered lower severity, such as denial of service issues affecting client or desktop software. These issues may be considered a low priority by Microsoft. As a result, they may not typically be addressed in monthly security bulletins, but in service packs and other major version updates instead.

While it is likely that many of these vulnerabilities will have minimal impact on enterprises, some denial of service vulnerabilities have the potential for more severe effects, such as code execution. Some vulnerabilities are prematurely thought to be limited to denial of service capabilities because the researcher has not completely investigated the vulnerability or because his or her skills are inadequate to conclusively determine the nature of the vulnerability.

The first half of 2007 did not show an improvement in the number of unpatched Oracle vulnerabilities over the second half of 2006. In addition to that, many vulnerabilities still remain unpatched from that period. In many cases, this may be due to lack of acknowledgement or correlation with publicly available vulnerability reports. When Oracle announces vulnerabilities, many of the issues are identified by an internal tracking number, but are not adequately mapped to other external vulnerability identifiers such as the CVE dictionary.[78] This could cause many publicly known vulnerabilities to remain classified as unpatched because the vendor has not explicitly identified the vulnerabilities by their common names in security bulletins and product updates.

[78] http://cve.mitre.org

Recently, Oracle made improvements to their security reporting procedures, including providing pre-release notification for the security updates and including Common Vulnerability Scoring System ratings in their advisories.[79] The expectation is that these changes will have a positive effect on security reporting and vulnerability remediation. As a result, it is likely that fewer vulnerabilities will remain unpatched for extended periods of time.

Governments should be concerned about unpatched Oracle vulnerabilities in particular because they have the potential to expose confidential or classified information. These vulnerabilities can also have critical implications for organizations that are required to comply with regulatory and legal standards such as HIPAA,[80] Sarbanes-Oxley,[81] and the Gramm-Leach-Bliley Act.[82]

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. 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.

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.[83] If possible, all Web applications should be audited for security prior to deployment. 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.

[78] http://cve.mitre.org
[79] http://www.vnunet.com/articles/print/2172404
[80] http://www.hipaa.org
[81] http://www.sarbanes-oxley.com
[82] http://www.ftc.gov/privacy/privacyinitiatives/glbact.html
[83] 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's 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 reported to Symantec for analysis between January 1 and June 30, 2007. This section of the *Government Internet Security Threat Report* will discuss:

- Threats to confidential information
- Propagation mechanisms
- Computers with multiple infections by country
- Geolocation by type
- Malicious code—prevention and mitigation

This report examines the number and volume of malicious code threats based upon the number of reports received from enterprise and home users. It will also examine malicious code types and propagation vectors based upon potential infections. This allows Symantec to determine which sample of malicious code attempted to infect a computer and the volume of potential infections worldwide.

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 use in criminal activities such as identity theft, which was the most common consumer complaint received by the United States Federal Trade Commission in 2006.[84] With the widespread use of online shopping and Internet banking, compromises that result in unauthorized access to confidential information can result in significant financial loss, particularly if credit card information or banking details are exposed.

Within organizations, exposure of confidential information can lead to significant data leakage. If this involves customer-related data, such as credit card information, it can severely undermine customer confidence as well as violate local laws.[85] Sensitive corporate information—including financial details, business plans, and proprietary technologies—could also be leaked from compromised computers

Government agencies are also at risk from threats to confidential information. If employee data is exposed by these threats, the data could be used to facilitate identity theft, which could then lead to further security compromises. For instance, if the attacker gains access to a user's personal and system information, he or she can use it to craft a targeted social engineering attack tailored to that particular user. Additionally, certain agencies—such as those dealing with health care, revenue and taxation, and pensions—may store personally identifiable information of citizens, including government-issued identification numbers, that could be used for identity theft or related fraud.

[84] http://ftc.gov/opa/2007/02/topcomplaints.htm
[85] Many countries have implemented their own laws in this regard, such as the United Kingdom's Data Protection Act, which can be found at http://www.opsi.gov.uk/ACTS/acts1998/19980029.htm

In the first six months of 2007, threats to confidential information made up 65 percent of potential infections by the top 50 malicious code samples (figure 15). This is an increase over the 53 percent of potential infections in the second half of 2006.

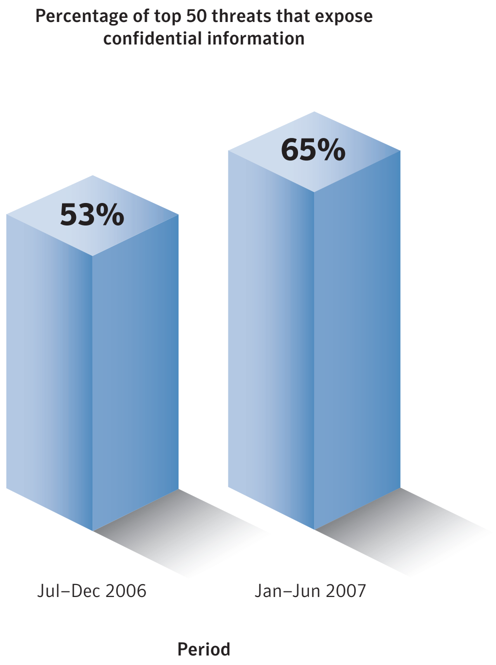

Figure 15. Threats to confidential information
Source: Symantec Corporation

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, remote access threats made up 88 percent of confidential information threats (figure 16), up from 87 percent in the second half of 2006. Back doors typically require a two-way communication channel between the attacker and the compromised computer in order to access unauthorized information. As such, they can be less efficient than an automated mechanism, such as a keystroke logger. This may indicate why threats that allow remote access increased only marginally this period while other types of information-exposure threats increased more significantly.

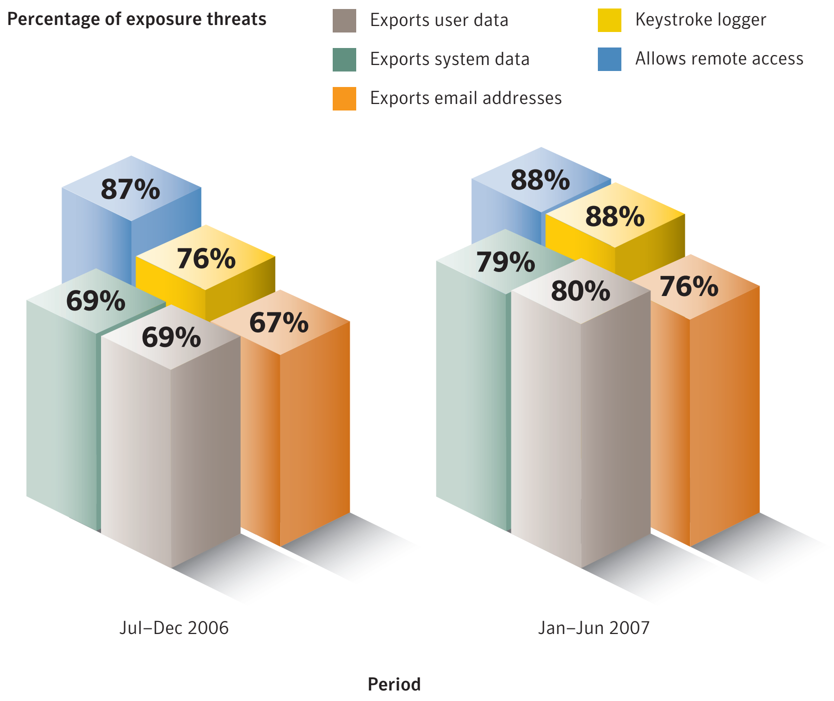

Figure 16. Threats to confidential information by type
Source: Symantec Corporation

Keystroke logging threats made up 88 percent of threats to confidential information, up from 76 percent in the second half of last year. 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 find the user's credentials for different types of accounts, such as online banking and trading accounts, as well as ISP accounts. The attacker can then use this information as a stepping stone to launch further attacks. This makes it easier for the attacker to gather confidential information from a large number of compromised computers than if they had to manually connect to back doors installed on a number of individual computers.

Threats that could be employed to export user data accounted for 80 percent of confidential information threats during the first six months of 2007, up from 69 percent in the previous reporting period. Furthermore, in the first half of 2007, 79 percent of threats to confidential information could be used to export system data, compared to 69 percent in the second 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.

Organizations can take several steps to limit the exposure of confidential information by successful intrusions. 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 so-called man-in-the-middle attacks that intercept data before it is encrypted.[86] 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. This section will assess some of the propagation mechanisms used by malicious code samples that were reported to Symantec in the first half of 2007. It will assess these samples according to the percentage of potential infections caused by each sample. Readers should note that some malicious code samples use more than one mechanism to propagate. As a result, cumulative percentages presented in this discussion may exceed 100 percent.

Due to some methodological changes that Symantec made for this reporting period, this volume of the *Government Internet Security Threat Report* is able to examine propagation mechanisms with increased specificity. For example, where possible, the specific peer-to-peer (P2P) protocols employed as propagation mechanisms have been identified. This will allow administrators to look at more specific port blocking and protocol filtering based upon the specific propagation mechanisms being discussed. It is also important to note that, due to this change, any comparisons to previous reporting periods would not be valid; therefore, they have not been presented here.

In the second half of 2007, 46 percent of malicious code that propagated did so in email attachments (table 10). This is not surprising, given the pervasive use of email. However, as noted in the "Top ten new malicious code families" section of the current *Internet Security Threat Report* (Volume XII), malicious code authors seem to be diversifying their propagation mechanisms by combining worms with a viral file-infection component.

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.

[86] 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.

Rank	Propagation Mechanism	Percentage of Threats
1	File Transfer/Email Attachment	46%
2	File Transfer/CIFS	24%
3	File Sharing/Peer-to-Peer	22%
4	File Sharing/Executables	22%
5	File Sharing/Peer-to-Peer/Kazaa	18%
6	Remotely Exploitable Vulnerability	18%
7	File Sharing/Peer-to-Peer/Morpheus	15%
8	File Sharing/Peer-to-Peer/eDonkey	15%
9	File Sharing/Peer-to-Peer/Winny	5%
10	Backdoor/Kuang2	3%

Table 10. Propagation mechanisms
Source: Symantec Corporation

Of the malicious code that propagated during the first half of 2007, 24 percent did so by the Common Internet File Sharing (CIFS) protocol.[87] Malicious code samples such as Fujacks.E[88] and variants of the Looked[89] family both propagated in significant numbers this period by copying themselves to CIFS shares with weak password protection. Both of these worms also contain a viral component to infect portable executable files. Since they try to infect files on both local and mapped network drives, they effectively use this propagation mechanism multiple times.

This propagation mechanism can be threatening to organizations because file servers use CIFS to give users access to their file shares. If a computer with access to a file server becomes infected by a threat that propagates through CIFS, it could spread to the file server. Since multiple computers within a corporation likely access the same file server, this could facilitate the rapid propagation of the threat within the enterprise.

To protect against threats that use the CIFS protocol to propagate, all network 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 22 percent of all potential infections this period. These samples typically do not attempt to use a specific P2P protocol to propagate; rather they copy themselves to all folders on the compromised computer that contains 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.

[87] 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.
[88] http://www.symantec.com/security_response/writeup.jsp?docid=2007-010509-0134-99
[89] http://www.symantec.com/security_response/writeup.jsp?docid=2004-121709-0657-99

Four specific P2P protocols were commonly used by malicious code to propagate during the first six months of 2007. The Kazaa file-sharing service was used by 18 percent of malicious code samples that propagated, while Morpheus and eDonkey were each used by 15 percent. Finally, the Winny protocol was used by five percent of propagating malicious code 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.

Computers with multiple infections by country

For the first time, in this volume of the *Internet Security Threat Report*, Symantec is assessing the number of times potential malicious code infections are reported from the same computer. This is done using data gathered by proprietary Symantec technologies. While many users may only experience one or two malicious code instances on their computers, some may become infected frequently within a single six-month period. Multiple infections may be due to a lack of knowledge on the user's part or out-of-date antivirus definitions. In some cases, multiple infections may also indicate that the computer was infected by a staged downloader, which is discussed in further detail in the "Staged downloaders—multiple infections by type" section of the current Symantec *Internet Security Threat Report*.

In the current period, the United States was the country with the highest number of multiple infections in the world (table 11). The United States has the highest number of broadband Internet users in the world.[90] Countries with high numbers of online users will likely experience the most potential infections. Since many new malicious code threats download additional components, it stands to reason that computers infected with those threats will also experience the highest number of multiple infections as well. These staged downloaders are mainly Trojans that are installed by malicious Web pages when a user views the page with a vulnerable browser. The initial Trojan usually disables security applications on the computer and downloads and installs additional threats.

Rank	Country	Region
1	United States	North America
2	China	APJ
3	Japan	APJ
4	United Kingdom	EMEA
5	Canada	North America
6	India	EMEA
7	Italy	EMEA
8	France	EMEA
9	Spain	EMEA
10	Germany	EMEA

Table 11. Computers with multiple infections by country
Source: Symantec Corporation

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

China had the second highest number of multiple infections in the current period. China has the second highest number of broadband users and also experienced 24 percent growth in new broadband users in the first half of 2007.[91] With so many new users coming online at such a high rate, it is likely that many of them are unaware of the threats they may encounter.

There appears to have been an increase in regionalized threats during this period. For example, many of the threats observed in China were Trojans designed to steal online gaming account information, while others appear to specifically target Chinese users. These Trojans are usually downloaded onto a computer as the second stage of a multistaged threat, which explains a large bulk of the multiple infections there.

The country experiencing the third highest number of multiple infections in the first half of 2007 was Japan. Japan is also the country with the third highest number of broadband users. This likely indicates that multistaged threats are more successful at installing their secondary components on broadband computers. Because computers with broadband Internet connections are almost always online when the computer is turned on, it allows the Trojan a greater opportunity to download its additional components, particularly if it only performs the downloads at specific times.

Users who experience multiple infections increase their likelihood of suffering serious consequences. Each time they are infected, they risk the theft of confidential information or loss of data. While a user may discover the first infection before the malicious code is able to send personal information back to the attacker, they might not be as fortunate with subsequent infections. For example, in the case of a staged downloader, the first infection may disable the security applications on a compromised computer, while the second infection contains a keystroke logger or some other remote access threat.

Geolocation by type

For the first time, in this edition of the *Internet Security Threat Report*, Symantec is examining 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. For example, 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 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 illustrate how network administrators in different regions can best direct their security efforts.

Between January and June of 2007, 44 percent of Trojans were reported from North America, while 37 percent were reported from the EMEA region (figure 17). This is significantly higher than the 15 percent reported from the APJ region and the four percent from Latin America.

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

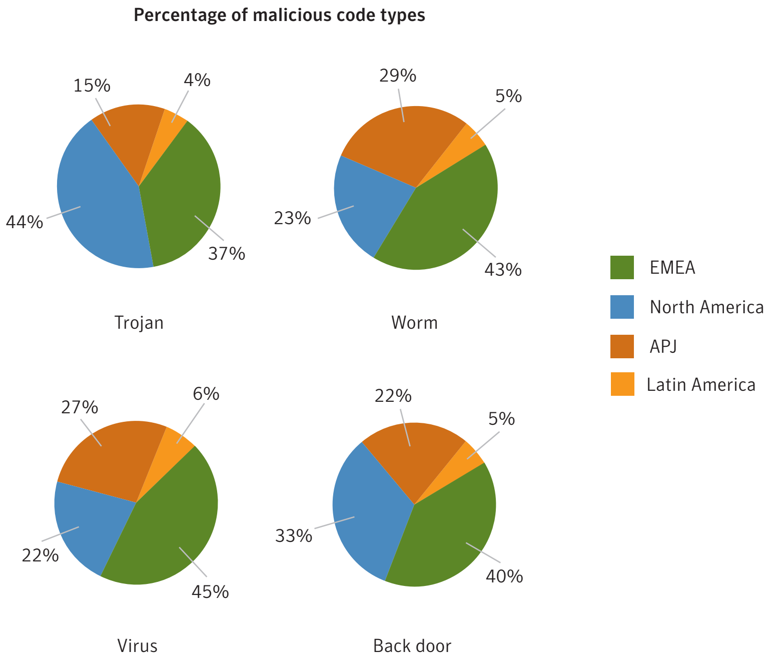

Figure 17. Location of malicious code by type
Source: Symantec Corporation

The concentration of Trojans in North America may be indicative of enterprises and ISPs taking more active steps to prevent the propagation of worms. Such steps include more aggressive blocking and filtering of email attachments at the email gateway to prevent the propagation of mass-mailing worms, and port blocking to prevent the spread of network worms. The prevalence of Trojans in North America could be reflective of the resultant drop in network worms in the region. On the other hand, it could reflect a conscious decision by attackers to move towards Trojans in reaction to the success of tactics that have successfully thwarted worm attacks.

As discussed in the "Malicious code that exploits vulnerabilities" section in the current *Internet Security Threat Report*, many Trojans are now being installed by Web pages that exploit vulnerabilities. This indicates that users and enterprises in regions with higher Trojan concentrations should ensure that their Web browsers, as well as related components and plug-ins, are patched for any potential vulnerabilities.

During this period, EMEA accounted for 43 percent of global potential infections caused by worms. This was followed by the APJ region, which accounted for 29 percent of potential worm infections. North America only accounted for 23 percent of reported worms this period. This may indicate that North American ISPs are implementing more rigid port blocking to limit the spread of network worms, as well as deploying antivirus filtering at the email gateway to limit mass-mailing worms.

Some worms use region-specific subject lines and text in their email messages. For example, the Rontokbro worm's email messages are in Indonesian.[92] However, this worm was seen more in India than in any other country. There is a great deal of commerce between India and Indonesia,[93] which means that it is likely that many enterprise users in Indonesia communicate with counterparts in India by email. Since Rontokbro sends its email messages to all the addresses it gathers from files on a compromised computer, it stands to reason that this worm was sent to many Indian users from business contacts in Indonesia. Rontokbro was also one of the top ten malicious code samples resulting in potential infections in the EMEA region.

The EMEA region accounted for the highest percentage of viruses this period, with 45 percent of the total. The APJ and North America regions accounted for 27 and 22 percent of viruses respectively, while Latin America only accounted for six percent.

As is noted in the "Malicious code types" section of the current *Internet Security Threat Report*, many worms are incorporating a viral component that causes them to be classified as both worms and viruses. Many of the worms causing potential infections in EMEA also employ a viral component, which explains why this region accounts for the greatest percentage of viruses and worms this period.

Potential infections caused by back doors were most frequently reported from the EMEA region, which accounted for 40 percent of all back doors worldwide. North America accounted for 33 percent of potential back door infections in the first half of 2007, while APJ accounted for 22 percent and Latin America accounted for five percent. 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 this period 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.

Malicious code—prevention 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 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.[94]

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.

[92]http://www.symantec.com/security_response/writeup.jsp?docid=2005-092311-2608-99

[93] http://www.hindu.com/2005/11/24/stories/2005112405871200.htm

[94] Ingress traffic refers to traffic that is coming into a network from the Internet or another network. Egress traffic refers to traffic that is leaving a network, bound for the Internet or another network.

Phishing Trends

Phishing is an attempt by a third party to solicit confidential information from an individual, group, or organization, usually for financial gain. Phishers are groups or individuals who attempt to trick users into disclosing personal data, such as credit card numbers, online banking credentials, and other sensitive information. They may then use the information to commit fraudulent acts. This section of the *Government Internet Security Threat Report* will discuss phishing activity that Symantec detected in the first half of 2007.

The data provided in this section is based on statistics derived from the Symantec Probe Network, which consists of over two million decoy email accounts that attract email messages from 20 different countries around the world. The main purpose of the network is to attract spam, phishing, viruses, and other email-borne threats. It encompasses more than 600 participating enterprises around the world, attracting email that is representative of traffic that would be received by over 250 million mailboxes. The Probe Network consists of previously used email addresses as well as email accounts that have been generated solely to be used as probes.

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

Phishing is assessed according to two indicators: phishing messages and phishing attempts. A phishing message is a single, unique message that is sent to targets with the intent of gaining confidential and/or personal information from computer users. Each phishing message has different content, and each one will represent a different way of trying to fool a user into disclosing information. A phishing message can be considered the "lure" with which a phisher attempts to entice a phishing target to disclose confidential information.

A single phishing message can be used in numerous distinct phishing attempts, usually targeting different end users. 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 ensnare a target.

This section of the Symantec *Government Internet Security Threat Report* will discuss the following:

- Phishing activity by sector
- Top countries hosting phishing Web sites
- Government servers hosting Web sites
- Phishing—protection and mitigation

Phishing activity by sector

This metric will assess phishing activity by sector. It will do this in two ways. First, it will identify the sectors in which the organizations that were most commonly phished belong. This means that the organization's brand was used in phishing attacks. Second, it will assess which sectors were targeted by the highest volume of phishing attacks. These considerations are important for enterprises because the use of an organization's brand in phishing activity can have significant negative consequences. It can undermine consumer confidence and damage the organization's reputation. Furthermore, the company may be required to compensate victims of any phishing scams that use the company's brand.

Most of the organizations whose brands were used in phishing attacks in the first six months of 2007 were part of the financial services sector. Organizations in that sector accounted for 79 percent of the brands that were used for phishing during this period (figure 18), compared to the previous period when they accounted for 84 percent. The financial services sector also accounted for the highest volume of phishing Web sites during this period, making up 72 percent of all phishing Web sites reported to Symantec (figure 19). Financial services made up 64 percent of all phishing Web sites in the last half of 2006.

Most phishing activity is conducted for financial gain. A successful phishing attack that mimics the brand of a financial entity is most likely to yield data that can be used for immediate financial gain. It is therefore logical that phishing attacks focus on brands within the financial services sector.

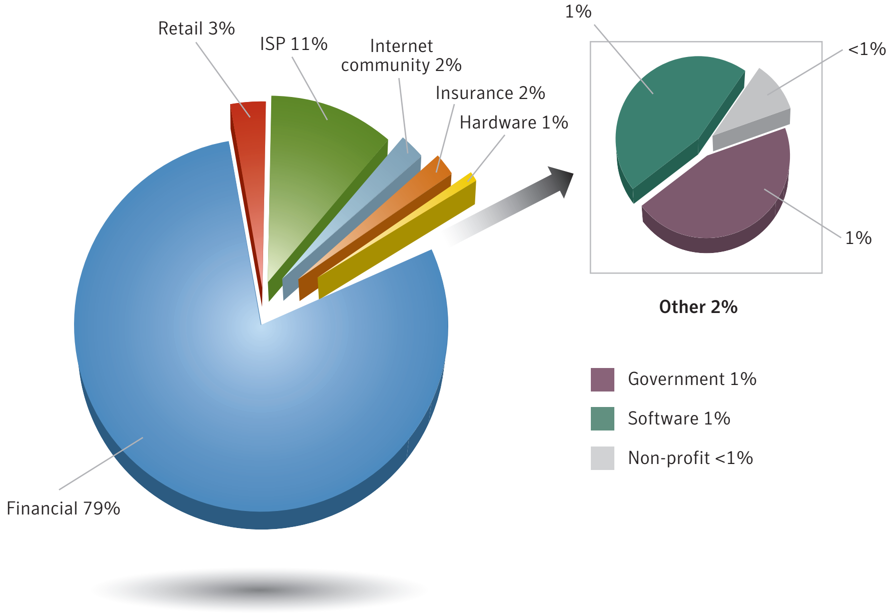

Figure 18. Brands phished by sector
Source: Symantec Corporation

Organizations in the Internet service provider (ISP) sector made up 11 percent of the unique brands used in phishing attacks during this period, making it the second ranked sector. This is an increase over the seven percent of phishing attacks that spoofed ISP brands in the second half of 2006. As noted in the previous edition of the *Internet Security Threat Report*, ISP accounts can be valuable targets for phishers.[95] People frequently use the same authentication credentials (such as usernames and passwords) for multiple accounts, including their email accounts.[96] Thus, information gleaned through phishing attacks may provide access to other accounts, such as online banking. Additionally, attackers could use the free Web-hosting space that is often provided with these accounts to host phishing Web sites, or they could use the accompanying email accounts to send spam or launch further phishing attacks. In some cases, compromised ISP Web-hosting can be used to plant links to other Web sites that the attacker controls in order to boost the rating of the Web site in search engines.[97] Email account passwords were the third most common item advertised for sale on underground economy servers this period, as described in the "Underground economy servers" discussion in the "Attack Trends" section of the current *Internet Security Threat Report*.

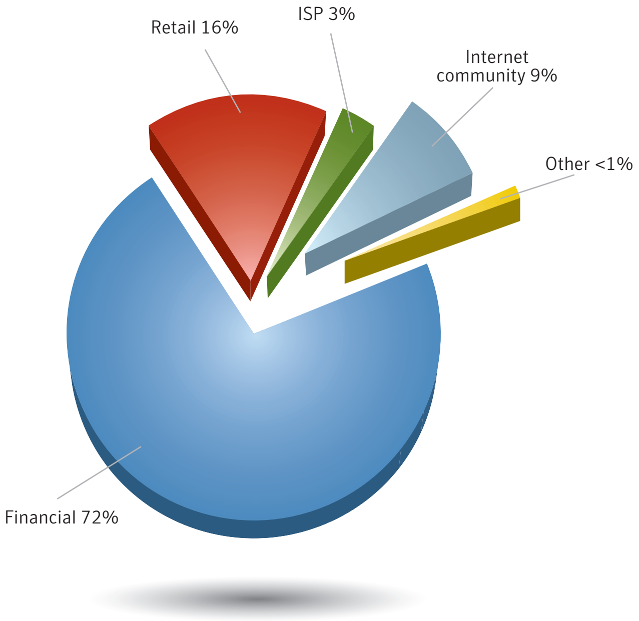

Figure 19. Phished sectors by volume
Source: Symantec Corporation

The retail services sector only accounted for three percent of organizations whose brands were spoofed in phishing activity in the first half of 2007; however, it accounted for 16 percent of the volume of phishing Web sites. In the previous reporting period, the retail sector accounted for five percent of the unique brands spoofed and 34 percent of phishing Web sites.

[95] 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
[96] http://cups.cs.cmu.edu/soups/2006/proceedings/p44_gaw.pdf
[97] For a more detailed discussion of search engine rankings, see the "Malicious Code Trends" section of this report.

The disproportionate number of phishing Web sites in the retail services sector indicates that a small number of retail brands were being heavily phished. This is illustrated by the fact that a large volume of phishing attacks were reported that attempted to spoof the eBay brand. This is not surprising, as an attacker can use a user's eBay account credentials in various ways. First, many eBay accounts are linked to the user's PayPal account. As users often use the same passwords for these accounts, compromising one could give an attacker access to both, which would allow the attacker to transfer funds to him- or herself. Additionally, the attacker could use the account to buy goods from other users and default on the transaction, sell items that do not exist, or even use the account to sell stolen goods or goods purchased from an online retailer using a hijacked account or stolen credit card.

While the retail services sector made up 16 percent of phishing Web sites, this is a significant decrease from the 34 percent reported in the previous six-month period. This is mainly due to a significant rise in the volume of phishing sites targeting the financial sector. Attackers have also started exploring other means of perpetrating fraud upon customers of retail organizations such as eBay. For instance, some Trojans and other attacks[98] can also facilitate identity theft.

Eight of the top ten brands spoofed by attackers in phishing attacks during this period were in the financial sector. Interestingly, one of the most frequently spoofed brands this period was an Internet community. While there is no immediate financial gain to be obtained by attackers who steal a user's account information, it may provide other returns. The attacker could use the account to gather information from the hijacked account's friends, such as email addresses, by sending messages that appear to come from the legitimate user, who would likely be implicitly trusted by the message recipient.[99] Additionally, the attacker can send messages containing links to Web sites that are designed to download malicious code on visitors' computers.[100] Since the link comes from a user's friend, they may be more likely to trust the link and visit the site.[101]

Top countries hosting phishing Web sites

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

This metric will assess the countries in which the most phishing Web sites were hosted in the first six months of 2007. In this case, Symantec counts phishing Web sites as the number of unique IP addresses hosting Web pages used for phishing. This data is a snapshot in time, and does not offer insight into changes in the locations of certain phishing sites over the course of the reporting period. It should also be noted that the fact that a phishing Web site is hosted in a certain country does not necessarily mean that the attacker is located in that country.

[98] Please see http://www.symantec.com/enterprise/security_response/weblog/2007/03/ebay_motor_scam_update.html and http://redtape.msnbc.com/2007/03/how_far_has_vla.html, respectively, for more in-depth discussions.

[99] http://www.symantec.com/enterprise/security_response/weblog/2006/11/an_imaginative_phishing_attack_1.html

[100] http://blog.washingtonpost.com/securityfix/2007/06/web_2pointuhoh_worm_whacks_mys.html

[101] 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

In the first half of 2007, 59 percent of all known phishing Web sites were located in the United States (table 12), a considerable increase over the previous period when 46 percent of phishing Web sites were located there. The United States is home to a large number of Web-hosting providers, including over 30 percent of registered domains.[102] It is also home to the highest number of Internet users in the world.[103] The increase in phishing Web sites located there during this reporting period is likely related to the high number of Trojans reported from North America this period, as is discussed in the "Malicious Code Trends" section of this report. Trojans are frequently used for hosting Web sites used in phishing attacks.

Rank	Previous Rank	Country	Current Percentage	Previous Percentage
1	1	United States	59%	46%
2	2	Germany	6%	11%
3	3	United Kingdom	3%	3%
4	10	Netherlands	2%	2%
5	11	Russia	2%	2%
6	4	France	2%	3%
7	7	Canada	2%	2%
8	5	Japan	2%	3%
9	8	China	1%	2%
10	6	Taiwan	1%	3%

Table 12. Top countries hosting phishing Web sites
Source: Symantec Corporation

Germany was once again the location of the second highest percentage of phishing Web sites this period, with six percent of the worldwide total. This is, however, a decrease from the last six months of 2006 when 11 percent of phishing Web sites were located there. Variations in percentages between periods are likely a result of the opportunistic nature of attackers. Attackers are most likely to host phishing Web sites on any computer they are able to compromise. In many cases, attackers host their phishing Web sites on a computer that was compromised by a bot. Because bots compromise any computer that is vulnerable to the exploits they use to propagate, there is little control on the part of the attacker as to the physical location of computers in their bot network.

The United Kingdom hosted the third highest number of phishing Web sites this period. It held steady at the three percent of worldwide phishing Web sites reported in the previous period. The percentage of bots in the United Kingdom has been dropping in recent periods; however, it is the top country reporting potential malicious code infections in the EMEA region. This may indicate that attackers are using bots less frequently in phishing attacks and are instead using other malicious code to host phishing Web sites.

[102] http://www.webhosting.info/webhosts/tophosts/global/
[103] http://www.pewinternet.org/PPF/r/218/report_display.asp

Government servers hosting phishing sites

For the first time, in this report, Symantec is examining government servers that were reported to be hosting phishing Web sites. These are domains that are registered to government entities that were most likely compromised and used to host phishing sites. In addition to hosting the phishing Web site, the compromised server may contain confidential or sensitive information that the attackers could potentially access.

During the first six months of 2007, domains registered to the government of Thailand were used in 16 percent of phishing URLs hosted on government servers (table 13). At the same time, 23 percent of the unique government domains used to host phishing sites were located in Thailand (table 14). This indicates that Thai government servers were each used to host only a few phishing Web sites. The relatively high number of Thai government domains used in phishing attacks could mean that many of the domains are hosted on a small number of servers. In such a case, compromising a single server hosting multiple domains would give the attacker access to each hosted site.

Rank	Country	Percentage of Phishing URLs on Government Servers
1	Thailand	16%
2	Argentina	11%
3	United States	10%
4	Brazil	8%
5	Colombia	8%
6	Indonesia	8%
7	Ecuador	8%
8	Philippines	5%
9	Turkey	5%
10	Paraguay	3%

Table 13. Top government domains used in phishing URLs
Source: Symantec Corporation

Domains registered to the government of Argentina were used in the second most phishing URLs this period, 11 percent. They also hosted eight percent of the unique government domains hosting phishing Web sites this period. As was the case with Thailand, domains of the government of Argentina appear to only have been used to host a few phishing sites each. This indicates that the phishing attacks hosted on Argentinean domains were likely not as sophisticated as attacks that use phishing toolkits, which generally host many phishing sites on a single domain or server.[104]

[104] 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.

Rank	Country	Percentage of Government Phishing Sites
1	Thailand	23%
2	Indonesia	12%
3	Argentina	8%
4	Brazil	8%
5	Colombia	7%
6	Ecuador	6%
7	China	5%
8	Palestinian Territory	4%
9	Philippines	4%
10	Turkey	4%

Table 14. Top government domains hosting unique phishing Web sites
Source: Symantec Corporation

United States government domains were used in 10 percent of phishing URLs hosted on government servers. However, this was the result of a single government server that was compromised to host multiple phishing Web sites. A large number of phishing URLs were used for the same phishing site, so it is likely that a phishing kit was installed on the server. All of the phishing messages containing URLs pointing to this domain were observed in a short time span, so it is likely that the phishing site was detected soon after these messages were sent, and was subsequently removed.

Phishing—prevention 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.[105] 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.[106]

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.[107] 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.[108]

Organizations can also employ Web server log monitoring to track if and when complete downloads of their Web sites or logos and other images are occurring. Such activity may indicate that someone is using the legitimate Web site to create an illegitimate Web site that could be used for phishing.

[105] 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.
[106] 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.
[107] 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
[108] A good resource for information on the latest phishing threats can be found at: http://www.antiphishing.org

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.[109] So-called typo domains and homographic domains should also be monitored.[110] 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 deploy an antiphishing solution. As some phishing attacks may use spyware and/or keystroke loggers, 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.[111] Additionally, network administrators can review Web proxy logs to determine if any users have visited known phishing sites.

[109] The term 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.

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

[111] 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. It could also cause a loss of service or degradation in the performance of network resources and email gateways. This section of the *Government Internet Security Threat Report* will discuss recent developments in spam.

The data used in this analysis is based on data returned from the Symantec Probe Network as well as data gathered from a statistical sampling of 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 is accomplished through internal production changes that are made to the network, which thus affect the number of new spam attacks it receives as a whole.

This section of the Symantec *Government Internet Security Threat Report* will discuss the selected legislative approaches to combating spam. In recent years, many countries have adopted specific antispam legislation in order to provide governments with the ability to prosecute spammers. This section will examine the approaches taken by several countries and assess their effectiveness in limiting spam. Before entering into too much detail on the specific legislation enacted, we will identify the key points that spam laws often address.

1. **Consent:** The type of consent that must be given by an email recipient in order to receive electronic messages from a given sender. Common examples of this include: opt-in, according to which the receiver must explicitly request that the messages be sent; and opt-out, according to which the sender must provide the receiver with adequate and effective means to request that no more messages are sent.

2. **Misleading information:** In which the sender provides a false return address or falsifies the origin of the message.

3. **Content Identification:** Some laws require that email that has commercial or sexual content be labeled as such by including a specified phrase, or tag, into the header.

4. **Scope:** The extent to which the law applies. Some laws only apply to spam sent from within the country and some apply much more broadly.

The approaches taken by recently enacted antispam laws in Singapore, New Zealand, and Switzerland are examined below. Each of these discussions will include a graph outlining the percentage of spam detected in each country from July 2006 through June 2007.

Singapore—Spam Control Act

The Spam Control Act is intended to provide a legal framework to help combat spam in Singapore.[113] The key points addressed by this act are:

- Consent
  - Recipients have the right to opt-out of further commercial email.
  - The sender must use approved methods to obtain a recipient's email address.
- Misleading information
  - Headers and subject descriptions should be accurate.
  - The email must include an accurate and functional email address or telephone number by which the sender can be readily contacted.
- Content identification
  - The letters "<ADV>" with a space before the title must be included in the subject field or at the beginning of the message if there is no subject header.
- Scope
  - The law only applies to electronic messages that originate in Singapore, are received in Singapore, or are accessed by methods that are based in Singapore.

Civil action can be taken under this act against the sender of bulk unsolicited email that does not meet the requirements of this law. Statutory damages under the law are set at 25 Singapore dollars per message up to a maximum of one million Singapore dollars. Additionally, the plaintiff is entitled to damages equal to the amount of their loss and the cost of their legal fees.

This law was put into effect on June 15, 2007. Laws such as this one are often criticized because they require an opt-out method of consent, instead of an opt-in method. Under this type of law, users will receive unsolicited messages until they explicitly state a desire not to. Spammers often implement a fake opt-out mechanism in order to verify whether or not a given email address is active. Although the fake opt-out mechanism is now illegal in Singapore, this trick is still widely used in spam from around the world.

Once an email account is verified as active, it becomes a valuable commodity and is often sold to other spammers, after which the address will likely receive even more spam. This illustrates the problem associated with relying on opt-out methods. Since the process is not standardized and not accountable, users do not know whether they can trust the opt-out mechanism or if opting out will, in fact, result in the receipt of more unsolicited email messages.

[113] http://www.parliament.gov.sg/Publications/070006.pdf

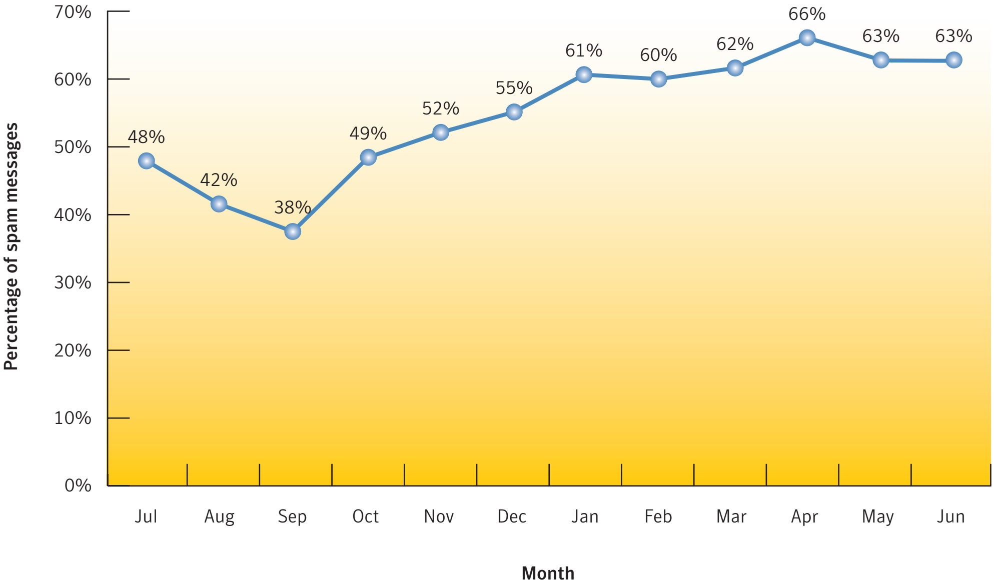

Figure 20. Spam as a percentage of all email from Singapore
Source: Symantec Corporation

Figure 20 shows the percentage of mail sent from Singapore from July 2006 through June 2007 that Symantec identified as spam, as well as the corresponding spam activity on, or around, the dates of these events. Interestingly, it seems the spam law in Singapore was introduced just when it was needed. The percentage of spam email originating in Singapore had been steadily increasing from a low point in September 2006 to the introduction of the law in June 2007. Unfortunately, the cut-off point for the collection of spam data was June 30, 2007, so it is impossible to gauge the effectiveness of the law in this report. If this law is effective, there should be a decrease in the level of spam originating in Singapore in the next period.

New Zealand—Unsolicited Electronic Messages Act

The Unsolicited Electronic Messages Act makes it illegal to send unsolicited commercial email messages without express, inferred, or deemed consent.[113] Inferred consent means consent that may reasonably be inferred from the conduct and the business or family relationships of the recipient individual or organization. Someone is said to have given deemed consent if their email address was posted online without an express "do not email" notice. The sender of the message and anybody knowingly concerned in a violation is liable under this act. The key points addressed in this act are:

- Consent
  - Senders need express, inferred, or deemed consent.
  - Every message requires a functional opt-out mechanism.
- Misleading information
  - Accurate information about the individual or organization that authorized the sending of the message is required.
- Content identification
  - No content identification is required.
- Scope
  - The law only applies to electronic messages that originate in New Zealand, are received in New Zealand, or are accessed by a method that is based in New Zealand.

The maximum fine for individuals is $200,000 NZD for individuals and $500,000 NZD for organizations. The law can also be used as a basis for civil actions. This law is very similar to Australia's spam law, which was introduced in 2003. The Australian law was initially well received because of its opt-in approach to consent, placing the choice to receive commercial messages on the recipient. Some criticisms of this law have arisen because there have been very few convictions under the Australian law and it has not had its full intended effect. The particulars of this law were examined in the previous Symantec *Government Internet Security Threat Report*.[114]

The New Zealand law mirrors the Australian law with the crucial difference in that it extends the definition of consent to include "deemed consent." This type of consent is considered to be given if a person makes a work-related email address available on a publicly accessible site, such as on a Web site, without the inclusion of a disclaimer that states that the individual does not wish to receive unsolicited email at that address.[115] Allowing this type of consent weakens the spam law considerably because posting an email address on a Web site is common practice of many people who do not necessarily want to receive spam, but are unaware of the necessity of posting the disclaimer.

[113] http://www.parliament.nz/NR/rdonlyres/69F835AC-2468-40F8-94E4-240800EE762F/51659/DBHOH_BILL_6896_353991.pdf

[114] Symantec *Government Internet Security Threat Report* (March 2007): http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_govt_03_2007.en-us.pdf : p. 61

[115] http://www.netconcepts.com/nz-anti-spam-act/

The spam law was passed in February 2007, but was not scheduled to come into effect until September 2007. Figure 21 shows the percentage of mail being sent from New Zealand that Symantec identified as spam from July 2006 to June 2007. Spam levels were between 50 and 60 percent from July through October 2006, when they started declining to around 25 to 35 percent range for the first half of 2007. This gives New Zealand the lowest spam percentage among countries in the APJ region.

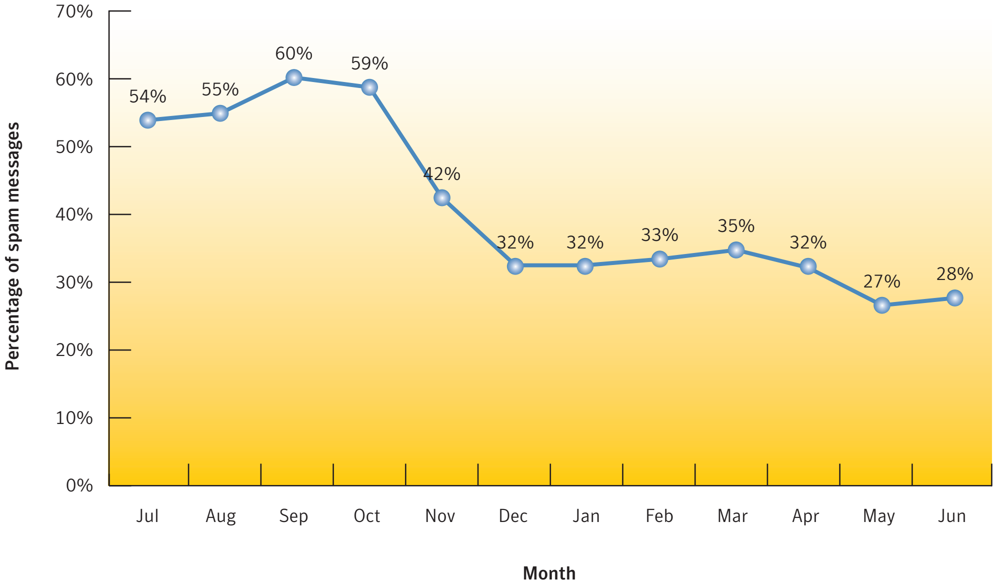

Figure 21. Spam as a percentage of all email from New Zealand
Source: Symantec Corporation

Although the spam law is not yet enforced, spam from New Zealand has already decreased dramatically since the third quarter of 2006. It is possible that this can be attributed to spammers from New Zealand using spam zombies in other countries to send their spam in anticipation of the new legislation. A more likely explanation is that ISPs in New Zealand have decided to implement new security measures in an effort to reduce spam. In June 2007, The Internet Society of New Zealand,[116] the group that oversees the Internet in that country, proposed a code of conduct for ISPs to help them deal with issues related to spam.[117] Many ISPs have already implemented some of the suggestions.

[116] http://www.internetnz.net.nz/
[117] http://www.nbr.co.nz/home/column_article.asp?id=18282&cid=3&cname=Technology

Switzerland—amendment of the anti-competition law

The new amendment of the Swiss anti-competition law includes the first set of spam-specific laws in Switzerland.[118] The new laws provide a legal framework for reducing the levels of spam originating in Switzerland. This amendment prohibits the use of computers to send unauthorized bulk emails. The main provisions of these measures are:

- Consent
  - The sender requires prior consent to send email.
  - The receiver must be given a valid opt-out mechanism.
- Misleading information
  - The sender must be accurately identified in messages.
  - The physical address of the sender must be included.
- Content identification
  - None
- Scope
  - This law only applies to spam that was sent from Switzerland to recipients in Switzerland.

The maximum fine for sending spam under these measures is 100,000 Swiss francs. In addition, Switzerland imposes some strict regulations on ISPs. If a case of spam is reported to an ISP, they must attempt to identify the perpetrator and notify law enforcement. Furthermore, owners of computers that have been used as spam zombies will be held responsible for the spam that is sent through their computers. In the first half of 2006, 54,146 spam zombies were detected in Switzerland, making up just over one percent of the spam zombies in the EMEA region.

One criticism of the law is its limited scope, as it applies only to spam sent from within Switzerland to other computers in Switzerland. The amount of spam sent within Switzerland is a small percentage of the total sent from Switzerland. Even if all the spam of this type were eliminated, the effect on global levels of spam will likely be minimal.

[118] http://www.admin.ch/ch/f/ff/2003/7245.pdf, p7285 and http://www.admin.ch/ch/f/rs/2/241.fr.pdf

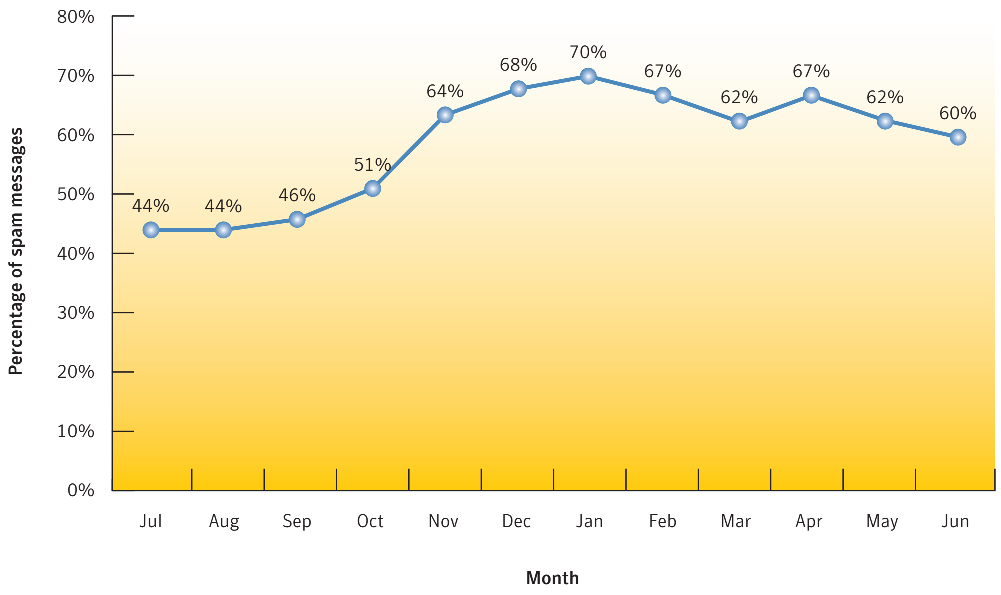

Figure 22. Spam as a percentage of all email from Switzerland
Source: Symantec Corporation

These measures went into effect in April 2007. Figure 22 shows the percentage of mail that was sent from Switzerland that Symantec identified as spam from July 2006 to June 2007 (it should be noted that this data is not restricted to spam that was sent to targets within Switzerland). In the last half of 2006, spam from Switzerland accounted for 56 percent of all email from that country, compared to 66 percent in the first half of 2007. The levels of spam increased from the middle of 2006 to around the time the law came into effect but began falling slightly in the month after the introduction of the law. It is too soon to tell if this decrease in spam is related to the introduction of the legislative measures taken or just a natural fluctuation in the levels of spam. However, as there isn’t anything in the law to prevent Swiss spammers from spamming people in other countries, it may not lead to a noticeable decrease in the amount of spam originating there.

Appendix A—Symantec Best Practices

Enterprise Best Practices

1. 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.
2. Turn off and remove services that are not needed.
3. 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.
4. 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.
5. Consider implementing network compliance solutions that will help keep infected mobile users out of the network (and disinfect them before rejoining the network).
6. Enforce an effective password policy.
7. 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.
8. 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.
9. 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.
10. 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.
11. Educate management on security budgeting needs.
12. Test security to ensure that adequate controls are in place.
13. 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

1. 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.

2. Consumers should ensure that security patches are up-to-date and that they are applied to all vulnerable applications in a timely manner.

3. Consumers should ensure that passwords are a combination of letters and numbers, and should change them often. Passwords should not consist of words from the dictionary.

4. Consumers should never view, open, or execute any email attachment unless the attachment is expected and the purpose of the attachment is known.

5. 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.

6. Consumers should routinely check to see if their operating system is vulnerable to threats by using Symantec Security Check at www.symantec.com/securitycheck.

7. 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.

8. 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.

9. 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.

10. 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.

11. Consumers should be cautious 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, and the Symantec Honeypot Network. Symantec combines data derived from these sources for analysis.

Attack definitions

In order to avoid ambiguity with the findings presented in this discussion, Symantec's methodology for identifying various forms of attack activity is outlined clearly below. This methodology is applied consistently throughout our monitoring and analysis. The first step in analyzing attack activity is to define precisely what an attack is. Attacks are individual instances of malicious network activity. Attacks consist of one IDS or firewall alert that is indicative of a single attack action.

Explanation of research inquiries

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

Malicious activity by country

To determine the top countries for the "Malicious activity by country" metric, Symantec compiled geographical data on each type of malicious activity to be considered, which included: bot network computers, bot command-and-control servers, phishing Web sites, malicious code submissions, spam relay hosts, and Internet attacks. The proportion of each activity originating in each country was determined. The mean of the proportions of each malicious activity that originated in each country was calculated. This average determined the proportion of overall malicious activity that originated from the country in question and was used to rank each country.

Symantec also evaluated the top 25 of these countries according to the percentage of worldwide Internet users located there. Symantec determined the top 25 countries for malicious activity as a proportion of Internet users by employing the same data as above. This measure is meant to remove the bias of high Internet users from the consideration of the "Malicious activity by country" metric. In order to determine this, Symantec divided the amount of malicious activity originating in each of the top 25 countries for malicious activity by the percentage of worldwide Internet users who are located in that country.

The proportion assigned to each country in the discussion thus corresponds to the proportion of malicious activity that could be attributed to a single (average) Internet user in that country. That is, Symantec estimates the amount of malicious activity that could be attributed to the average Internet user from each of the top 25 countries. The proportion of malicious activity that would be carried out by each person is the proportion assigned to each country.

Malicious activity originating from critical infrastructure sectors

To determine the proportion of malicious activity originating from critical infrastructure sectors, Symantec cross-references the IP addresses of known malicious computers with Standard Industrial Classification (SIC) codes assigned to each industry.[119] Symantec has compiled data on numerous malicious activities that were detected originating from the IP address space of these organizations, namely: bot-infected computers, phishing Web sites, spam zombies, and Internet attacks.

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.[120] 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.

Denial of service attacks

Although there are numerous methods for carrying out denial of service (DoS) attacks, Symantec derives this metric by measuring DoS attacks that are carried out by flooding a target with SYN requests. These are often referred to as SYN flood attacks. This type of attack works by overwhelming a target with SYN requests and not completing the initial request, which thus prevents other valid requests from being processed.

In many cases, SYN requests with forged IP addresses are sent to a target, allowing a single attacking computer to initiate multiple connections, resulting in unsolicited traffic, known as backscatter, being sent to other computers on the Internet. This backscatter is used to derive the number of DoS attacks observed throughout the reporting period. Although the values Symantec derives from this metric will not identify all DoS attacks carried out, it will highlight DoS attack trends.

To determine the countries targeted by DoS attacks, Symantec cross-references the target IP addresses of every attack with several third-party, subscription-based databases that link the geographic location of systems to source IP addresses. While these databases are generally reliable, there is a small margin of error.

Bot-infected computers

Symantec identifies bots based on coordinated scanning and attack behavior observed in network traffic. For an attacking computer to be considered to be participating in this 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 network computer, and may identify other malicious code or individual attackers behaving in a similarly coordinated way as a bot network. This behavioral matching will, however, identify many of the most coordinated and aggressive bot-infected computers and will give insight into the population trends of bot network 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.

[119] SIC codes are the standard industry codes that are used by the United States Securities and Exchange Commission to identify organizations belonging to each industry. For more, on this, please see http://www.sec.gov

[120] http://www.attrition.org

This metric explores the number of active bot-infected computers that the Symantec Global Intelligence Network has detected and identified during the first six months of 2007. Identification is carried out on an individual basis by analyzing attack and scanning patterns. Computers generating attack patterns that show a high degree of coordination are considered to be bot-infected computers.

As a consequence of this, Symantec does not identify all bot-infected computers, but only those that are actively working in a well coordinated and aggressive fashion. Given Symantec's extensive and globally distributed sensor base, it is reasonable to assume that the bot activities discussed here are representative of worldwide bot trends, and can thus provide an understanding of current bot activity across the Internet as a whole.

Lifespan of bot-infected computers

Using previously identified bot-infected computers, Symantec determined the life span of these infections by measuring the time between their first and last detected activity. However, to ensure that the lifespan reflects a continuous bot infection, if the identified computer was inactive for 30 days or longer it was considered to be disinfected. As such, any further bot-like activity would be considered a new infection.

Bot-infected computers by countries and cities

This metric is based on the same data as the “Bot-infected computers” discussion of the “Attacks Trends” section of the report. Symantec cross-references the IP addresses of every identified bot-infected computer with several third-party subscription-based databases that link the geographic location of systems to IP addresses.

Bot-infected computers by critical infrastructure sector

In assessing the top sectors by bot-infected computers, Symantec uses Standard Industrial Classification (SIC) codes, which are standard industry codes that are used by the United States Securities and Exchange Commission to identify organizations belonging to each industry.[121] Symantec cross-references the IP addresses of known bot-infected computers with the SIC codes assigned to those IPs in order to determine the distribution of bot-infected computers with critical infrastructure sectors.

Top countries of attack origin

Symantec identifies the national sources of attacks by automatically cross-referencing source IP addresses of every attacking IP with several third-party, subscription-based databases that link the geographic location of systems to source IP addresses. While these databases are generally reliable, there is a small margin of error.

[121] SIC codes are the standard industry codes that are used by the United States Securities and Exchange Commission to identify organizations belonging to each industry. For more, on this, please see http://www.sec.gov

Appendix C—Vulnerability Trends Methodology

The “Vulnerability Trends” report of the Symantec *Government Internet Security Threat Report* discusses developments in the discovery and exploitation of vulnerabilities over the six-month reporting period. This methodology section will discuss how the data was gathered and how it was analyzed to come to the conclusions that are presented in the “Vulnerability Trends” section.

Symantec maintains one of the world’s most comprehensive databases of security vulnerabilities, consisting of over 22,000 distinct entries. Each distinct entry is created and maintained by Symantec threat analysts who vet the content for accuracy, veracity, and suitability for inclusion in the Symantec Vulnerability Database based on available information. The following metrics discussed in the “Vulnerability Trends” section are based on the analysis of that data by Symantec researchers:

- Patch development time for operating systems
- Zero-day vulnerabilities
- Vendor responsiveness
- Database vulnerabilities

The ways in which the data for the remaining metrics is gathered and analyzed will be discussed in the remainder of this methodology.

Vulnerability classifications

Following the discovery and/or announcement 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 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)[122] to define classifications of vulnerabilities. Possible values are indicated below, and the previously mentioned white paper provides a full description of the meaning behind each classification:

- Boundary condition error
- Access validation error
- Origin validation error
- Input validation error
- Failure to handle exceptional conditions
- Race condition error

[122] “Use of a Taxonomy of Security Faults” http://ftp.cerias.purdue.edu/pub/papers/taimur-aslam/aslam-krsul-spaf-taxonomy.pdf

- Serialization error
- Atomicity error
- Environment error
- Configuration error
- Design error

Operating system patch development time

This metric has a similar methodology to the “Patch development time, enterprise vendors” metric, which was explained later 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

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.

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 vulnerabilities

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.

Unpatched vulnerabilities are vulnerabilities that have no vendor remediation at the time that data for the report was collected.[123] This means that 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

[123] 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.

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 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 that 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 that produce 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™ (Computer Associates)
- Cisco®
- EMC
- HP®
- IBM®
- McAfee®
- Microsoft
- Oracle®
- Sun™
- Symantec

Database vulnerabilities

This metric offers a comparison of the vulnerabilities across multiple database vendors and implementations. For the purpose of this report, the following five database implementations are discussed:

- IBM DB2®
- Microsoft SQL Server
- MySQL
- Oracle
- PostgreSQL

The volume of database vulnerabilities is determined by querying the vulnerability database for specific vulnerabilities affecting the aforementioned database implementations. The results are broken out by implementation and reporting period.

Appendix D—Malicious Code Trends Methodology

The trends in the “Malicious Code Trends” section 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 the “Malicious Code Trends” section are based on empirical data and expert analysis of this data. The data and analysis draw primarily from 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 *Government 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.

Appendix E—Phishing Trends Methodology

Phishing attack trends in this report are based on the analysis of data derived from the Symantec Probe Network. Symantec Brightmail AntiSpam data is assessed to gauge the growth in phishing attempts as well as the percentage of Internet mail that is determined to be phishing attempts. Symantec Brightmail AntiSpam field data consists of statistics reported back from customer installations that provide feedback about the detection behaviors of antifraud filters as well as the overall volume of mail being processed.

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.

Phishing attempt definition

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. A phishing attempt is a group of email messages with similar properties, such as headers and content, that are sent to unique users. The messages attempt to gain confidential and personal information from online users.

Symantec Brightmail AntiSpam software reports statistics to Symantec Security Response that indicate 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 is used to identify general trends in phishing email messages.

Explanation of research inquiries

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.

Top countries and cities 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. 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.

Appendix F—Spam Trends Methodology

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 includes accounts in countries in the Americas, Europe, Asia, Africa, and Australia/Oceania.

Spam trends in this report are based on the analysis of data derived from both the Symantec Probe Network as well as Symantec Brightmail AntiSpam field data. Symantec Brightmail AntiSpam software reports statistics to the Brightmail Logistical Operations Center (BLOC) indicating 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. This is 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.

Sample set normalization

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.

Spam as a percentage of all email

The data for this calculation is determined by dividing the number of email messages that trigger antispam filters in the field by the total number of email messages scanned. These filters are distributed across the Symantec Brightmail AntiSpam customer base. The data for this section is based on monthly totals.

Any technical information that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

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

About Symantec

Symantec is a global leader in infrastructure software, enabling businesses and consumers to have confidence in a connected world. The company helps customers protect their infrastructure, information, and interactions by delivering software and services that address risks to security, availability, compliance, and performance. Headquartered in Cupertino, Calif., Symantec has operations in 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

09/07 12755154