SYMANTEC ENTERPRISE SECURITY

Symantec Internet Security Threat Report

Trends for July–December 06

Volume XI, Published March 2007

Executive Summary

Over the past two reporting periods, Symantec has observed a fundamental shift in Internet security activity. The current threat environment is characterized by an increase in data theft and data leakage, and the creation of malicious code that targets specific organizations for information that can be used for financial gain.

Instead of exploiting high-severity vulnerabilities in direct attacks, attackers are now discovering and exploiting medium-severity vulnerabilities in third-party applications, such as Web applications and Web browsers. Those vulnerabilities are often used in “gateway” attacks, in which an initial exploitation takes place not to breach data immediately, but to establish a foothold from which subsequent, more malicious attacks can be launched.

Symantec has observed high levels of malicious activity across the Internet, with increases in phishing, spam, bot networks, Trojans, and zero-day threats. However, whereas in the past these threats were often used separately, attackers are now refining their methods and consolidating their assets to create global networks that support coordinated criminal activity.

This has resulted in an increasing interoperability between diverse threats and methods. For example, targeted malicious code may take advantage of Web-enabled technologies and third-party applications to install a back door, which then downloads and installs bot software. These bots can, in turn, be used to distribute spam, host phishing sites, or launch attacks in such a way as to create a single coordinated network of malicious activity. Once entrenched, these networks can be used in concert as global networks of malicious activity that support their own continued growth.

Dean Turner
Executive Editor
Symantec Security Response

Stephen Entwisle
Senior Editor
Symantec Security Response

Marci Denesiuk
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

Peter Coogan
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

Contributors

David Cole
Director Product Management
Symantec Security Response

Peter Szor
Security Architect
Symantec Security Response

David Cowings
Sr. Business Intelligence Manager
Symantec Business Intelligence

Shravan Shashikant
Pr. Business Intelligence Manager
Symantec Business Intelligence

Igor Moochnick
Sr. Software Engineer
Symantec Instant Messaging Security

This volume of the *Internet Security Threat Report* will offer an overview of threat activity that took place between July 1 and December 31, 2006. This brief summary and the discussion that follows will offer a synopsis of the data and trends that are presented in the main report. Symantec will continue to monitor and assess threat activity in order to best prepare consumers and enterprises for the complex Internet security issues to come.

Internet Security Threat Report Overview

The Symantec *Internet Security Threat Report* provides a six-month update of Internet threat activity. It includes analysis of network-based attacks, a review of known vulnerabilities, and highlights of malicious code. It also assesses numerous issues related to online fraud, including phishing, spam, and security risks such as adware, spyware, and misleading applications. This summary of the *Internet Security Threat Report* will alert readers to current trends and impending threats. In addition, it will offer recommendations for protection against and mitigation of these concerns. This volume covers the six-month period from July 1 to December 31, 2006.

Symantec has established some of the most comprehensive sources of Internet threat data in the world. The Symantec™ Global Intelligence Network, which includes Symantec DeepSight™ Threat Management System and Symantec™ Managed Security Services, tracks attack activity across the entire Internet. It consists of over 40,000 sensors monitoring network activity in over 180 countries. As well, Symantec gathers malicious code data along with spyware and adware 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 20,000 vulnerabilities (spanning more than a decade) affecting more than 45,000 technologies from over 7,000 vendors. Symantec also tracks and assesses certain criminal activities using online fraud monitoring tools.

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. These resources give Symantec analysts unparalleled sources of data with which to identify emerging trends in attacks and malicious code 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.

The Symantec *Internet Security Threat Report* is grounded principally on the expert analysis of data provided by all of these sources. Based on Symantec's expertise and experience, this analysis yields a highly informed commentary on current Internet threat activity. By publishing the analysis of Internet security activity in the Symantec *Internet Security Threat Report*, Symantec hopes to provide enterprises and consumers 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 Highlights

The following section will offer a brief summary of the security trends that Symantec observed during this period based on data provided by the sources listed above. This summary includes all of the metrics that are included in the main report. Following this overview, the Executive Summary will discuss selected metrics in greater depth.

Attack Trends Highlights

- The government sector accounted for 25 percent of all identity theft-related data breaches, more than any other sector.
- The theft or loss of a computer or other data-storage medium made up 54 percent of all identity theft-related data breaches during this period.
- The United States was the top country of attack origin, accounting for 33 percent of worldwide attack activity.
- Symantec recorded an average of 5,213 denial of service (DoS) attacks per day, down from 6,110 in the first half of the year.
- The United States was the target of most DoS attacks, accounting for 52 percent of the worldwide total.
- The government sector was the sector most frequently targeted by DoS attacks, accounting for 30 percent of all detected attacks.
- Microsoft Internet Explorer was targeted by 77 percent of all attacks specifically targeting Web browsers.
- Home users were the most highly targeted sector, accounting for 93 percent of all targeted attacks.
- Symantec observed an average of 63,912 active bot-infected computers per day, an 11 percent increase from the previous period.
- China had 26 percent of the world’s bot-infected computers, more than any other country.
- The United States had the highest number of bot command-and-control computers, accounting for 40 percent of the worldwide total.
- Beijing was the city with the most bot-infected computers in the world, accounting for just over five percent of the worldwide total.
- The United States accounted for 31 percent of all malicious activity during this period, more than any other country.
- Israel was the highest ranked country for malicious activity per Internet user, followed by Taiwan and Poland.
- Fifty-one percent of all underground economy servers known to Symantec were located in the United States, the highest total of any country.
- Eighty-six percent of the credit and debit cards advertised for sale on underground economy servers known to Symantec were issued by banks in the United States.

Vulnerability Trends Highlights

- Symantec documented 2,526 vulnerabilities in the second half of 2006, 12 percent higher than the first half of 2006, and a higher volume than in any other previous six-month period.[2]
- Symantec classified four percent of all vulnerabilities disclosed during this period as high severity, 69 percent were medium severity, and 27 percent were low severity.
- Sixty-six percent of vulnerabilities disclosed during this period affected Web applications.
- Seventy-nine percent of all vulnerabilities documented in this reporting period were considered to be easily exploitable.
- Seventy-seven percent of all easily exploitable vulnerabilities affected Web applications, and seven percent affected servers.
- Ninety-four percent of all easily exploitable vulnerabilities disclosed in the second half of 2006 were remotely exploitable.
- In the second half of 2006, all the operating system vendors that were studied had longer average patch development times than in the first half of the year.
- Sun Solaris had an average patch development time of 122 days in the second half of 2006, the highest of any operating system.
- Sixty-eight percent of the vulnerabilities documented during this period were not confirmed by the affected vendor.
- The window of exposure for vulnerabilities affecting enterprise vendors was 47 days.
- Symantec documented 54 vulnerabilities in Microsoft Internet Explorer, 40 in the Mozilla browsers, and four each in Apple Safari and Opera.
- Mozilla had a window of exposure of two days, the shortest of any Web browser during this period.
- Twenty-five percent of exploit code was released less than one day after vulnerability publication. Thirty-one percent was released in one to six days after vulnerability publication.
- Symantec documented 12 zero-day vulnerabilities during this period, a significant increase from the one documented in the first half of 2006.
- Symantec documented 168 vulnerabilities in Oracle database implementations, more than any other database.

Malicious Code Trends Highlights

- Of the top ten new malicious code families detected in the last six months of 2006, five were Trojans, four were worms, and one was a virus.
- The most widely reported new malicious code family this period was that of the Stration worm.[3]

[2] The Symantec *Internet Security Threat Report* has been tracking vulnerabilities in six-month periods since January 2002.
[3] http://www.symantec.com/security_response/writeup.jsp?docid=2006-092111-0525-99

- Symantec honeypot computers captured a total of 136 previously unseen malicious code threats between July 1 and December 31, 2006.
- During this period, 8,258 new Win32 variants were reported to Symantec, an increase of 22 percent over the first half of 2006.
- Worms made up 52 percent of the volume of malicious code threats, down from 75 percent in the previous period.
- The volume of Trojans in the top 50 malicious code samples reported to Symantec increased from 23 percent to 45 percent.
- Trojans accounted for 60 percent of the top 50 malicious code samples when measured by potential infections.
- Polymorphic threats accounted for three percent of the volume of top 50 malicious code reports this period, up from one percent in the two previous periods.
- Bots made up only 14 percent of the volume of the top 50 malicious code reports.
- Threats to confidential information made up 66 percent of the top 50 malicious code reported to Symantec.
- Keystroke logging threats made up 79 percent of confidential information threats by volume of reports, up from 57 percent in the first half of the year and 66 percent in the second half of 2005.
- Seventy-eight percent of malicious code that propagated did so over SMTP, making it the most commonly used propagation mechanism.
- Malicious code using peer-to-peer to propagate rose from 23 percent of all propagating malicious code in the first six months of 2006 to 29 percent in the last half of the year.
- The majority of malicious code reports during this period originated in the United States.
- During the second half of 2006, 23 percent of the 1,318 documented malicious code instances exploited vulnerabilities.
- MSN Messenger was affected by 35 percent of new instant messaging threats in the second half of the year.

Phishing, Spam, and Security Risks Highlights

- The Symantec Probe Network detected a total of 166,248 unique phishing messages, a six percent increase over the first six months of 2006. This equates to an average of 904 unique phishing messages per day for the second half of 2006.
- Symantec blocked over 1.5 billion phishing messages, an increase of 19 percent over the first half of 2006.
- Throughout 2006, Symantec detected an average of 27 percent fewer unique phishing messages on weekends than the weekday average of 961.

- On weekends, the number of blocked phishing attempts was seven percent lower than the weekday average of 7,958,323 attempts per day.
- Organizations in the financial services sector accounted for 84 percent of the unique brands that were phished during this period.
- Forty-six percent of all known phishing Web sites were located in the United States, a much higher proportion than in any other country.
- Between July 1 and December 31, 2006, spam made up 59 percent of all monitored email traffic. This is an increase over the first six months of 2006 when 54 percent of email was classified as spam.
- Sixty-five percent of all spam detected during this period was written in English.
- In the last six months of 2006, 0.68 percent of all spam email contained malicious code. This means that one out of every 147 spam messages blocked by Symantec Brightmail AntiSpam contained malicious code.
- Spam related to financial services made up 30 percent of all spam during this period, the most of any category.
- During the last six months of 2006, 44 percent of all spam detected worldwide originated in the United States.
- The United States hosted the largest proportion of spam zombies, with 10 percent of the worldwide total.
- The most commonly reported security risk was an adware program named ZangoSearch.
- All of the top ten security risks reported in the last six months of 2006 employ at least one anti-removal technique compared to only five of the top ten security risks in the last reporting period.
- All of the top ten security risks reported during this period employ self-updating.
- Potentially unwanted applications accounted for 41 percent of reports in the top ten new security risks in the second half of 2006.
- Misleading application detections increased by 40 percent in the second half of 2006.

Executive Summary Discussion

This section will discuss selected metrics from the *Internet Security Threat Report* in greater depth, providing analysis and discussion of the trends indicated by the data. The following metrics will be discussed:

- Malicious activity by country
- Data breaches that could lead to identity theft
- Underground economy servers
- Zero-day vulnerabilities
- Threats to confidential information
- Malicious code types
- Phishing
- Spam
- Bot-infected computers

Malicious activity by country

For the first time, in this volume of the *Internet Security Threat Report*, Symantec is evaluating the countries in which 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, malicious code reports, spam relay hosts, and Internet attacks.

Between July 1 and December 31, 2006, the United States was the top country for malicious activity, accounting for 31 percent of the worldwide total (table 1). For each of the malicious activities taken into account for this measurement, the United States ranked number one by a large margin with the exception of bot-infected computers. It ranked second for that criterion, 12 percentage points lower than China.

Overall Rank	Country	Overall Proportion	Malicious Code Rank	Spam Host Rank	Command and Control Server Rank	Phishing Host Rank	Bot Rank	Attack Rank
1	United States	31%	1	1	1	1	2	1
2	China	10%	3	2	4	8	1	2
3	Germany	7%	7	3	3	2	4	3
4	France	4%	9	4	14	4	3	4
5	United Kingdom	4%	4	13	9	3	6	6
6	South Korea	4%	12	9	2	9	11	9
7	Canada	3%	5	23	5	7	10	5
8	Spain	3%	13	5	15	16	5	7
9	Taiwan	3%	8	11	6	6	7	11
10	Italy	3%	2	8	10	14	12	10

Table 1. Malicious activity by country
Source: Symantec Corporation

The high degree of malicious activity originating in the United States is likely driven by the expansive Internet infrastructure there. The United States accounts for 19 percent of the world's Internet users.[4] Furthermore, the number of broadband Internet users in that country grew by 14 percent between December 2005 and July 2006.[5] Despite the relatively well developed security infrastructure in the United States, the high number of Internet-connected computers there presents more targets for attackers to compromise for malicious use. Symantec predicts that the United States will remain the highest ranked country for malicious activity until another country exceeds it in numbers of Internet users and broadband connectivity.

China was the second highest country for malicious activity during this six-month reporting period, accounting for 10 percent of all worldwide malicious activity. Germany was third, with seven percent. The prominence of both of these countries can likely be attributed to the high number of Internet users there, as well as the rapid growth in the country's Internet infrastructure.

Having determined the top countries by malicious activity, Symantec 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 "Malicious activity by country" measurement. The percentage assigned to each country in this discussion equates to the proportion of malicious activity that could be attributed to a single (average) Internet user in that country.

Israel was the most highly ranked country for malicious activity per Internet user. If one person from each of the top 25 countries were to represent their country's Internet-connected population, the average Internet user in Israel would carry out nine percent of the group's malicious activity. Taiwan had the second most malicious activity per Internet user, accounting for eight percent of the sample group's activity. Poland ranked third, accounting for six percent.

Data breaches that could lead to identity theft

Identity theft is an increasingly prevalent security issue. Organizations that store and manage personal identification information must take care to ensure the confidentiality and integrity of such data. Any compromise that results in the leakage of personal identity information could result in a loss of public confidence, legal liability, and/or costly litigation.

In the second half of 2006, the government sector accounted for the majority of data breaches that could lead to identity theft, making up 25 percent of the total (figure 1). Government organizations store a lot of personal information that could be used for the purposes of identity theft. Furthermore, they often consist of numerous semi-independent departments. As a consequence, sensitive personal identification information may be stored in separate locations and be available to numerous people. This increases the opportunity for attackers to gain unauthorized access to this data. Governments may also be more likely to report such breaches than private organizations, which may fear negative market reaction.

[4] http://www.internetworldstats.com
[5] http://www.oecd.org/document/9/0,2340,en_2649_34225_37529673_1_1_1_1,00.html

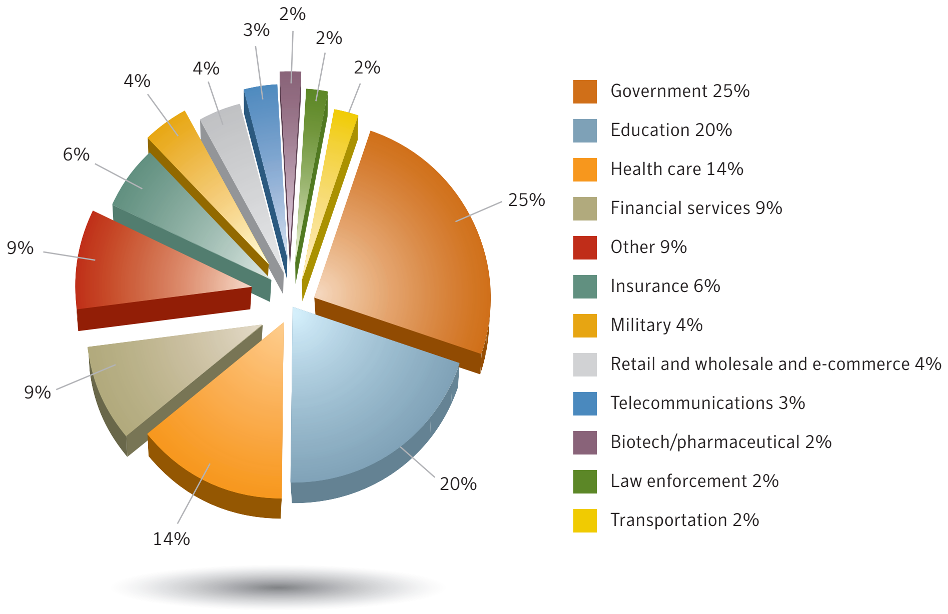

Figure 1. Data breaches that could lead to identity theft by sector
Source: Based on data provided by Privacy Rights Clearinghouse and Attrition.org

During this period, 54 percent of all data breaches that could lead to identity theft were caused by the theft or loss of a computer or data-storage medium (such as a USB memory key or back-up media). Twenty-eight percent of such breaches were caused by insecure policy, which includes a failure to develop, implement, and/or comply with adequate security policy. For example, this could mean posting personal identification information on a publicly available Web site or sending it through unencrypted email.

Most breaches of this type are avoidable. In the case of theft or loss, the compromise of data could be averted by encrypting all sensitive data. This would ensure that even if the data were 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.

Underground economy servers

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.

During the second half of 2006, 51 percent of all underground economy servers known to Symantec were located in the United States, the highest total of any country (figure 2). The prominence of the United States is no surprise, as the expansive Internet infrastructure and continual broadband growth there create numerous opportunities for criminals to carry out malicious activities. Sweden ranked second, accounting for 15 percent of the worldwide total, and Canada ranked third, accounting for seven percent.

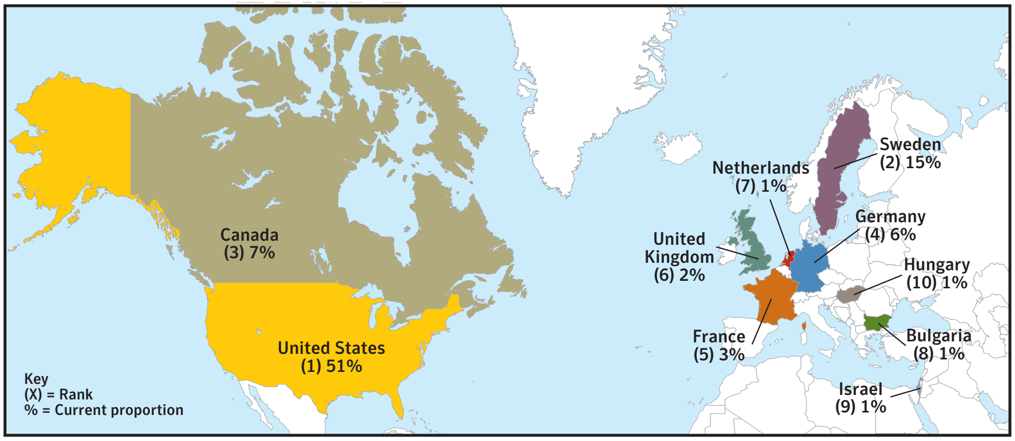

Figure 2. Location of underground economy servers
Source: Symantec Corporation

By far the most credit and debit cards advertised for sale on underground economy servers were issued by banks in the United States. The prominence of the United States is not entirely unexpected, as the vast majority of the data breaches that could lead to identity theft reported during this period took place there.

In order to reduce the likelihood of facilitating identity theft, it is important that organizations take the necessary steps to protect data stored on their computers or transmitted over networks. This should include the development and implementation of a policy requiring that all sensitive data is encrypted. This would ensure that, even if the data were lost or stolen, it would not be accessible. This step should be part of a broader security policy that organizations should develop and implement in order to ensure that any sensitive data is protected from unauthorized access.

Zero-day vulnerabilities

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.

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. They may be used in targeted attacks and in the propagation of malicious code. As Symantec predicted in Volume IX of the *Internet Security Threat Report*, a black market for zero-day vulnerabilities has emerged that has the potential to put them into the hands of criminals and other interested parties.[6]

In the second half of 2006, Symantec documented 12 zero-day vulnerabilities. This is a significant increase over the first half of 2006 and the second half of 2005 when only one zero-day vulnerability was documented for each reporting period.

The second half of 2006 saw a large number of high-profile zero-day vulnerabilities. This activity peaked in September of 2006, when four zero-day vulnerabilities were made known. The majority of these were client-side vulnerabilities that affected Office applications, Internet Explorer, and ActiveX controls. Many of these may have been discovered through the use of fuzzing technologies.

[6] Symantec *Internet Security Threat Report*, Volume IX (March 2006):
http://eval.veritas.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_ix.pdf : p. 21

Zero-day threats appear to be occurring more frequently than in the past. While it is believed that zero-day vulnerabilities have previously posed a threat, the recent rise in incidents may be partially accounted for by increasing capabilities to detect these attacks in the wild. Such capabilities include improved vulnerability-handling procedures within organizations, improved cooperation between enterprises and vendors, and better technologies for the detection and analysis of exploits and malicious code.

In order to protect against zero-day vulnerabilities, Symantec recommends that administrators deploy intrusion detection/intrusion prevention systems (IDS/IPS) and regularly updated antivirus software. Security vendors may be able to 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 the affected vendor has released a patch. Generic signatures may also block zero-day threats, as may behavior-blocking solutions and heuristic technologies.

Threats to confidential information

Some malicious code programs are designed specifically to expose confidential information that is stored on an infected computer. Threats to confidential information are a particular concern because of their potential use in criminal activities. Compromises of this nature can result in significant financial loss, particularly if credit card information or banking details are exposed.

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

In the last six months of 2006, threats to confidential information made up 66 percent of the volume of the top 50 malicious code reported to Symantec (figure 3). This is an increase over the 48 percent reported in the first half of the year and the 55 percent reported during the second half of 2005.

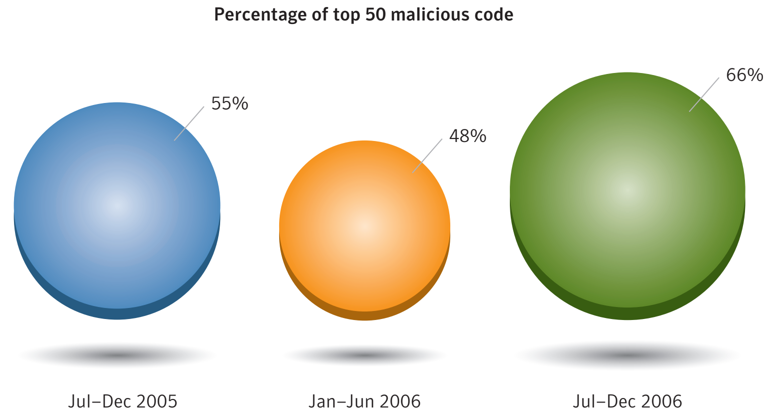

Figure 3. Threats to confidential information
Source: Symantec Corporation

In the second half of the 2006, threats that allow remote access, such as back doors, made up 84 percent of the volume of confidential information threats. Keystroke logging threats made up 79 percent of confidential information threats by volume of reports, and threats that could be used to export user data accounted for 62 percent of confidential information threats during this reporting period.

Malicious code types

During the current reporting period, worms made up 52 percent of the volume of malicious code threats, down from 75 percent in the previous period.[7] However, the number of unique samples of worms in the top 50 malicious code reports remained fairly constant over the last six months of 2006. During this period, 36 worms were reported to Symantec, compared to 38 in the previous period.

The volume of Trojans in the top 50 malicious code samples reported to Symantec increased significantly in the last six months of 2006. During this period, they constituted 45 percent of the volume of the top 50 malicious code samples, a significant increase over the 23 percent last period and the 38 percent reported in the second half of 2005.

As is discussed in the “Future Watch” section of this report, attackers are moving towards staged downloaders, also referred to as modular malicious code. These are small, specialized Trojans that download and install other malicious programs such as a back door or worm. During the current period, 75 percent of the volume of the top 50 malicious code reports contained a modular component such as this.

For the first time, in this edition of the *Internet Security Threat Report*, Symantec is assessing malicious code according to the number of unique samples reported to Symantec and the number of potential infections. This is an important distinction. In some cases, a threat that may create a large number of reports may not cause a large number of potential infections and *vice versa*.

For instance, worms made up 52 percent of malicious code reports in the second half of 2006, but caused only 37 percent of potential infections (figure 4). The main reason for this is that mass-mailing worms generate a significant number of email messages to which they attach their malicious code. Each message that is detected will generate a malicious code report. Because of the high volume of email that one worm can generate, a single infection can result in many reports. However, once a malicious code sample is detected, antivirus signatures are quickly developed that can protect against subsequent infections by that sample. Furthermore, gateway policies and technologies can block the executable attachments that also come with a mass mailer. So, only a small percentage of the high volume of email messages will result in additional infections.

[7] It is important to note that a malicious code sample can be classified in more than one threat type category. For example, bots such as variants of the Mytob family are classified as both a worm and a back door. As a result, cumulative percentages of threat types in the top 50 malicious code reports may exceed 100.

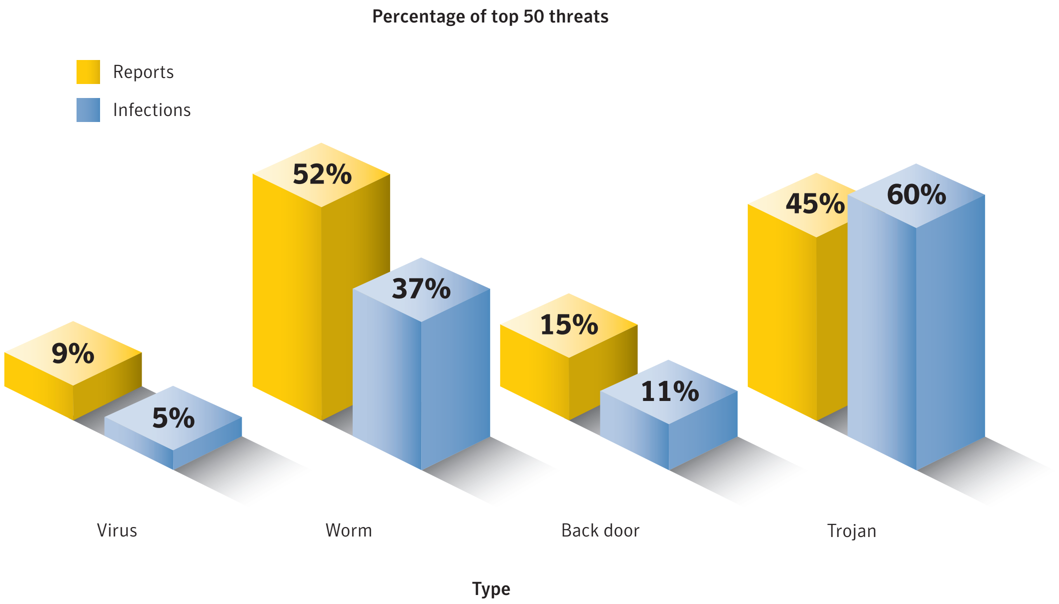

Figure 4. Malicious code types, by reports and by potential infections, July–December 2006
Source: Symantec Corporation

Trojans, on the other hand, only constituted 45 percent of the volume of the top 50 malicious code reports during the last six months of 2006. However, they accounted for 60 percent of potential infections by the top 50 malicious code samples during the same period. Since Trojans do not contain any propagation mechanisms, they do not proliferate as widely as mass-mailing worms, resulting in fewer reports. Because they are frequently installed by exploiting Web browser and zero-day vulnerabilities, a Trojan report is more likely to be the result of an infection. Consequently, the ratio of potential infections to reports is likely to be higher for Trojans than for worms.

Phishing

Over the last six months of 2006, the Symantec Probe Network detected a total of 166,248 unique phishing messages, an average of 904 per day. This total is a six percent increase over the first six months of 2006 when 157,477 unique phishing messages were detected.

In the second half of 2006, Symantec blocked over 1.5 billion phishing messages, an increase of 19 percent over the first half of 2006, and a six percent increase over the second half of 2005. This means that Symantec blocked an average of 8.48 million phishing emails per day over the last six months of 2006.

In the second half of 2006, 46 percent of all known phishing Web sites were located in the United States, a much higher proportion than in any other country. This is likely because a large number of Web-hosting providers—particularly free Web hosts—are located in the United States. Furthermore, the United States has the highest number of Internet users in the world, and it is home to a large number of Internet-connected organizations, both large and small.

Most of the unique brands phished in the last six months of 2006 were in the financial services sector. Organizations in that sector accounted for 84 percent of the brands that were used in phishing attacks this period. This is not surprising, as most phishing attacks are motivated by profit. A successful phishing attack on a financial entity is likely to yield information that an attacker could subsequently use for financial gain.

Spam

Between July 1 and December 31, 2006, spam made up 59 percent of all email traffic monitored by Symantec. This is an increase over the first six months of 2006 when Symantec classified 54 percent of email as spam.

The most common type of spam detected in the latter half of 2006 was related to financial services, which made up 30 percent of all spam on the Internet during this period. Spam related to health services and products made up 23 percent of all spam, while spam related to commercial products was the third most common type of spam, accounting for 21 percent of the total.

The rise in financially-related spam was due mainly to a noticeable increase in stock market "pump and dump" spam. Pump and dump is the name given to schemes in which criminals profit by creating an artificial interest in a stock they own. They buy a penny stock when the price is low. They then artificially pump up demand for the stock by sending out spam that appears to be from a respected stock advisor, but that actually contains false predictions of high performance for the stock. Recipients of the message, trusting the spam content, buy the stock, creating demand for it and thereby raising the price. When the prices are high, the perpetrators of the scheme sell their stock for a profit.[8]

This type of spam has been proven to allow the spammers to generate revenue directly and almost immediately.[9] This alone is likely to make it more appealing than other types of spam.

A spam zombie is a computer infected with a bot or some other malicious code that allows email messages to be relayed through it. Between July 1 and December 31, 2006, ten percent of all spam zombies were located in the United States, making it the highest country in this category. During this period, the United States was one of the top reporting countries for bots such as Spybot and Mytob, which are commonly used to send spam.

China and Germany were the second and third highest countries for spam zombies, hosting nine and eight percent of the worldwide total, respectively. The small variance between the top countries hosting spam zombies is quite different from the distribution of bots during this period. This indicates that not all spam zombies are necessarily bots and that not all bots are used to send spam.

Bot-infected computers

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

[8] http://www.sec.gov/answers/pumpdump.htm
[9] http://papers.ssrn.com/sol3/papers.cfm?abstract_id=920553

Bots allow for a wide range of functionality and most can be updated to assume new functionality by downloading new code and features. Bots can be used by external attackers to perform DoS attacks against an organization's Web site. Furthermore, bots within an organization's network can be used to attack other organizations' Web sites, which can have serious business and legal consequences. Bots can be used by attackers to harvest confidential information from compromised computers, which can lead to identity theft. Bots can also be used to distribute spam and phishing attacks, as well as spyware, adware, and misleading applications.

Between July 1 and December 31, 2006, Symantec observed an average of 63,912 active bot-infected computers per day. This is an 11 percent increase over the previous six-month period. Furthermore, Symantec observed 6,049,594 distinct bot-infected computers during the current reporting period, a 29 percent increase from the previous period. This increase is largely driven by a peak in bot activity in September when a number of vulnerabilities were disclosed that were actively exploited by bots.

Command-and-control servers are computers that bot network owners use to relay commands to bot-infected computers on their networks. In the last six months of 2006, Symantec identified 4,746 bot command-and-control servers, a 25 percent decrease from the first six months of 2006.

A drop in the number of command-and-control servers combined with a rise in the number of bot-infected computers indicates that, on average, bot networks are increasing in size. Bot networks are thus becoming more consolidated. Consolidated bot networks will likely mean that organizations will have to deal with a well entrenched, experienced, and dedicated group of bot network owners instead of a population of hobby hackers.

It could also signal a fundamental change in the way bots communicate with one another. Symantec has seen bots that are structured on a peer-to-peer model, in which the machines connect together rather than connecting to a central command-and-control server. Symantec has also observed that command-and-control servers are beginning to adopt encryption so that they are less visible.

China had the highest number of bot-infected computers during the second half of 2006, accounting for 26 percent of the worldwide total (figure 5). This is an increase of six percentage points over the previous six months. This increase was driven by a rise in the number of bots in the country rather than a decrease in other countries. This coincides with and illustrates a trend that Symantec first discussed in 2005, in which bot activity in China appeared to be increasing.[10] During the second half of 2006, the United States had the second highest number of bot-infected computers, accounting for 14 percent of the worldwide total.

[10] Symantec *Internet Security Threat Report*, Volume VII (March 2005): http://eval.veritas.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_vii.pdf : p. 26

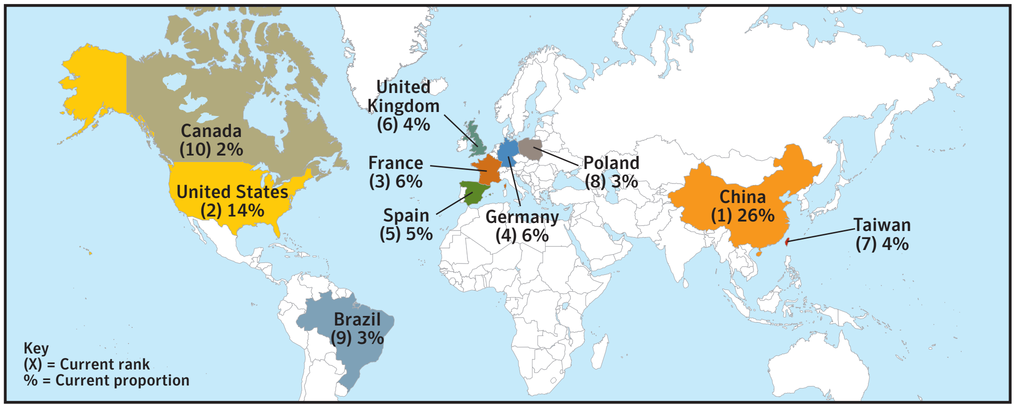

Figure 5. Bot-infected computers by country
Source: Symantec Corporation

The United States was the site of 40 percent of all known command-and-control servers, making it the highest ranked country in this category. The high proportion of command-and-control servers likely indicates that servers in the United States control not only bot networks within the country but offshore as well.

Organizations should monitor all network-connected computers for signs of bot infection, ensuring that any infections are detected and isolated 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 the enterprises notify their ISPs of any potentially malicious activity. Creating and enforcing policies that identify and limit applications that can access the network may also be helpful in limiting the spread of bot infections.

To prevent bot infections, Symantec recommends that ISPs perform both ingress and egress filtering to block known bot traffic.[11] ISPs should also filter out potentially malicious email attachments to reduce exposure to enterprises and end users.

End users should employ defense-in-depth strategies, including the deployment of antivirus software and a firewall.[12] They 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 attachments unless the attachment is expected and comes from a known and trusted source, and unless the purpose of the attachment is known.

[11] 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.

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

Future Watch

This section of the *Internet Security Threat Report* will discuss emerging trends and issues that Symantec believes will become prominent over the next six to twenty-four months. These forecasts are based on emerging research that Symantec has collected during the current reporting period and are speculative in nature. In discussing potential future trends, Symantec hopes to provide organizations and end users with an opportunity to prepare themselves for rapidly evolving and complex security issues. This section will discuss potential security issues associated with the following:

- Windows Vista™
- Windows Vista and third-party software
- New phishing targets and methods
- Spam and phishing targeting mobile devices
- Virtualization

Threats posed to Windows Vista becoming evident

Microsoft's latest operating system, Windows Vista, was released publicly in January 2007. The release of an operating system that is expected to be widely adopted will likely have a significant effect on the security landscape. The previous *Internet Security Threat Report* discussed some of the general security concerns that may be associated with Windows Vista.[13] Over the past six months, Symantec has continued to research potential issues associated with the new Microsoft operating system, which this section will discuss. These issues fall into three categories: vulnerabilities, malicious code, and attacks against the Teredo protocol.

In December 2006, Symantec reported a vulnerability in previous versions of Windows that also affects the version of Windows Vista that was released to consumers in January.[14] This indicates that Microsoft's Security Development Lifecycle,[15] while thorough, does not necessarily identify all potential vulnerabilities. This may be because some vulnerabilities can be extremely subtle.

That said, it appears that Microsoft's implementation of mitigating technologies such as address space layout randomization (ASLR), GS,[16] and data execution prevention (DEP) could reduce the successful exploitation of any vulnerabilities that are discovered. Nevertheless, Symantec expects that new threats for Windows Vista will utilize older exploitation techniques that have been previously successful—such as those developed to successfully exploit Windows XP SP2—in order to bypass improvements in Windows Vista. For example, attackers may revert to attacks that utilize email, P2P, and other social engineering techniques.

Existing malicious code may also pose a problem for Windows Vista. According to research conducted by Symantec, some malicious code that did not originally target Windows Vista may affect the new operating system. This could be problematic because some enterprises may act on the belief that their installations of Windows Vista are immune from older malicious code samples. As a result, they may not deploy appropriate security solutions on new Windows Vista hosts, potentially leaving them vulnerable to infection by older malicious code samples. For instance, Symantec has already noted that some malicious code samples can infect Windows Vista.[17]

[13] Symantec *Internet Security Threat Report*, Volume X (September 2006): http://www.symantec.com/specprog/threatreport/ent-whitepaper_symantec_internet_security_threat_report_x_09_2006.en-us.pdf : p. 28

[14] http://www.symantec.com/enterprise/security_response/weblog/2006/12/vista_vulnerable.html

[15] The Secure 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. See the following for more information: http://www.microsoft.com/presspass/features/2005/nov05/11-21SecurityDevelopmentLifecycle.mspx

[16] GS is a compiler technology. The name is derived from the compiler parameter that is used to enable this functionality. The use of GS will enable stack cookies to be placed around vulnerable functions in order to mitigate stack-based overflows.

[17] For example, please see: http://www.symantec.com/enterprise/security_response/weblog/2006/12/hit_or_miss_vista_and_current.html

The third potential Windows Vista security issue identified by Symantec for this discussion is Teredo. Teredo is a protocol developed by Microsoft to enable the transition between versions of Internet protocol (IP), one of the protocols underlying all Internet-based communications. Teredo is enabled by default in Windows Vista. Computers using Windows Vista can easily be identified through Teredo.

Attacks sent over Teredo will often bypass organizations' network security controls since the protocol is tunneled through network address translation (NAT) over an IPv4 UDP connection. Many security products don't support Teredo and thus would not inspect it. This could make Windows Vista susceptible to attacks through Teredo.[18]

Symantec recommends that enterprises planning a migration to Windows Vista do so first in small, non-critical environments, and that thorough security audits be conducted to reduce possible exposure to attack. In addition, enterprises should ensure that any third-party security solutions they currently use will run on Windows Vista and are deployed in accordance with any existing security policies. Organizations contemplating using IPv6 within Windows Vista rather than Teredo should plan the IPv6 transition carefully, including native access and updated security controls.

Windows Vista release makes third-party software security paramount

With the advent of Windows Vista and the continued use of the Security Development Lifecycle, it is likely that Microsoft-authored code will become more difficult to exploit. As a result, attackers may turn their focus to common third-party applications that are authored by companies that have not employed the Security Development Lifecycle. These third-party applications may not use accepted best software-development practices, such as secure design, secure coding practices, code reviews, or secure developer tools such as Microsoft's Visual Studio.[19] As a result, they may be less secure than Microsoft applications or the Windows Vista platform on which they are deployed.

These third-party applications could include third-party security software (such as antivirus), Web browsers, instant message clients, email clients, and office suites. They may include applications that have a significant user base, either globally or regionally. Symantec has already observed the emergence of a number of zero-day vulnerabilities being exploited in targeted attacks against office suites that are deployed in particular regions.[20]

Due to the security improvements in Windows Vista, third-party drivers may be targeted as a means of gaining kernel-level access on compromised hosts. This is because these applications may not have been developed using the Security Development Lifecycle or other secure development practices. As a result, they may be susceptible to compromise. This could allow attackers to bypass the security improvements in Windows Vista, which are designed to prevent complete compromises, by running applications with non-administrative user privileges.

Only by implementing secure development practices can developers ensure the optimal security of their applications. Failure to employ all available secure coding measures will likely increase the probability of the discovery and successful exploitation of vulnerabilities.

[18] For a more in-depth discussion on the security consequences of Teredo, please visit: http://www.symantec.com/avcenter/reference/Teredo_Security.pdf

[19] Microsoft Visual Studio is important as it introduces a number of security features that can be enabled for unmanaged code. These features include enabling key security features for the application when executed under Windows Vista.

[20] A zero-day attack is one that attacks a vulnerability for which there is no available patch. It also generally means an attack against a vulnerability that is not yet publicly known or known of by the vendor of the affected technology. For example, Justsystem's Ichitaro zero-day was used to transmit a Trojan: http://www.symantec.com/enterprise/security_response/weblog/2006/08/justsystems_ichitaro_0day_used.html

New phishing economies

As phishing becomes entrenched as a mainstream attack activity, antiphishing techniques are improving and phishers are being forced to focus on new targets and adopt new methods. Symantec believes that, in the near future, phishers will expand the scope of their targets to include new industry sectors. For example, they will likely start to target a number of the secondary economies introduced through so-called massively multiplayer online games (MMOGs).[21] MMOGs have become big business and are already attracting large groups of organized criminals who are using digital attacks for financial gain. In December 2006, forty-four suspects were arrested for stealing $90,000 USD worth of digital assets from a single game.[22]

Symantec also expects that phishers will develop new techniques to evade antiphishing solutions. Symantec has already started to see techniques to counter the effectiveness of block lists. For instance, phishers can use multiple unique URLs to direct users to a single Web site. Each URL is discarded after one use, so that even if they are placed on a block list, the lists still will not be able to block other URLs that direct potential victims to the same Web site. In some cases, Symantec has observed thousands of distinct URLs directing users to a single Web site.[23] Finally, attackers may already be using ready-made phishing kits. A phishing kit is a set of tools that an attacker can use to easily construct phishing email messages and Web sites based on a template.

Symantec has also observed that phishers are starting to adopt a technique known as intelligence lead phishing. This is a practice in which the phisher compromises a database or social networking site to obtain user information. This information is then used in a targeted phishing attempt against the user in question. The high degree of personalization made possible by the illicitly gained information can increase the effectiveness of the phishing attempt significantly. As widespread phishing attempts are increasingly choked off by antiphishing technologies, Symantec expects to see more phishing attacks that use these intelligence techniques.

In addition to the evolved phishing techniques outlined above, Symantec expects to see more generic phishing attacks; that is, attacks that are not restricted to spoofing a particular brand. For instance, instead of being required to know which bank the targeted user currently uses, a generic phishing attack could instead prompt the victim to “switch to Bank XYZ.” These more generic phishing attempts can be restricted to a particular country if the phished institution is nationally based, thereby increasing the phisher’s chance of success.

These recently evolved techniques illustrate the need for enterprises and end users to deploy effective antiphishing and antifraud solutions. Enterprises should be aware of and implement effective antiphishing technologies and practices. Enterprises that engage their clients over the Internet should continue to stay abreast of new phishing methods and techniques.[24] They should also monitor abuses of their brand in order to react appropriately and minimize potential damage to the company’s reputation.

End users should follow best security practices, including the use of regularly updated 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.

[21] A massively multiplayer online game is an Internet-based computer game on which hundreds to thousands of players are capable of participating simultaneously.
[22] Please see “Virtual Item Theft Ring Busted” http://playnoevil.com/serendipity/index.php?/archives/1051-Virtual-Item-Theft-Ring-Busted.html
[23] http://www.symantec.com/enterprise/security_response/weblog/2006/12/phishing_2006_the_year_in_revi.html
[24] See the Symantec Phish Report Network, an extensive antifraud community where members contribute and receive fraudulent Web site addresses for alerting and blocking attacks across a broad range of solutions. It is available at: http://www.phishreport.net

Enterprises that use the Internet for any transaction-based activity should ensure that they have implemented phishing detection and response processes and procedures. In addition to providing a structured, standardized response to a phishing incident, this will also ensure that information is passed on to the appropriate resources, thereby protecting against subsequent use of the same attack.

Enterprises should ensure that their users are educated about phishing techniques and are informed of the latest phishing scams. For further information, the Internet Fraud Complaint Center (IFCC) has released a set of guidelines on how to avoid Internet-related scams.[25]

SMiShing—Spam and phishing go mobile

In July 2006, Symantec reported that SMS and MMS had emerged as new vectors for spam and phishing activity.[26] Subsequently, the term SMiShing was coined by the industry to describe this class of threat.

There is a logical evolution from email to SMS and MMS as transport mechanisms for spam and phishing attacks. This is due in part to the fact that the technological and procedural defenses for devices deploying these services may not be as well developed or as widely deployed as those for other platforms. Additionally, users of mobile devices typically perceive messages received by SMS and MMS as being more personal than those received by email on a desktop computer. Furthermore, threats against these surfaces have been rare thus far. As a result, users are more likely to trust those messages and to act on them.

Targeting SMS and MMS may also offer attackers a significant benefit over targeting a specific mobile operating system. SMS and MMS are sufficiently well established and are deployed widely enough that they are available on almost all handsets on all networks. Most legacy and proprietary operating system handsets will support both of these technologies. As a result, they have a much larger target user base than smartphones.

There has been a rise in the amount of SMS-based premium-rate spam over the past few years since the introduction of subscriber-billed SMS.[27] This is a payment model in which the subscriber is billed a considerably higher cost for receiving a message than for sending one. This mechanism is typically used lawfully by the suppliers of ring tones, wallpapers, and other mobile content such as games. It is a convenient way of making micro-payments without having to introduce another payment tool such as a debit or credit card. However, some criminals have utilized the technology to obtain money, which has resulted in a number of national telecommunications regulators stamping out the practice.[28]

Symantec speculates that SMS- and MMS-based phishing and spam will continue to increase. Cellular operators will likely be forced to invest in filtering technologies to combat this growing problem. This issue will be compounded by the fact that there are a number of different Internet-based SMS gateways that could allow users to supply their own originating number or name, which could be spoofed and used to send spam. As the costs of SMS services goes down, the likelihood that these gateways will be used for spam activities will increase.

[25] http://www.fbi.gov/majcases/fraud/internetschemes.htm
[26] SMS (short messaging service) is a service that is used for sending short text messages to mobile phones and other mobile text devices such as pagers. MMS (multimedia messaging service) is a service that allows mobile devices to send phone messages as well as multimedia files, such as images, audio, and video.
[27] http://www.grumbletext.co.uk
[28] http://news.bbc.co.uk/1/hi/technology/4708167.stm

Software virtualization brings new security threats

Software virtualization is a technology that allows one computer (the host) to run one or more distinct virtual computers (the guests). These virtual computers each run independently of the others and have their own virtual hardware, allowing the user to run multiple different operating systems on the same physical hardware.

Software virtualization has become a very powerful tool, bringing with it numerous benefits. However, many users assume that virtual machines provide a foolproof security barrier, leading to a false sense of security. While it is true that virtual machines can insulate against some current attacks, there are others against which they offer no protection. Further, they could potentially make new classes of attack possible. Symantec believes that the potential security implications of software virtualization have not yet been fully investigated and understood.

Guest virtual machines may not run the same security software as the host. For instance, they may not include antivirus software, personal firewalls, or host-based intrusion prevention products. As a result of these omissions, the virtual machines may be more exposed to threats than if they were run on independent hardware. Furthermore, virtual machines will do little to protect the data on the host. Consequently, virtualization technology may not diminish or protect against the threat of application-oriented threats such as phishing and data theft.

Symantec also believes that threats that are specific to virtualization technologies could emerge. With many different virtual machines being used, Symantec believes that these virtualization-specific threats could fall into two distinct classes of threat.

The first type of threat targets the use of real hardware in virtualized machines. Hardware drivers that provide software emulation of hardware acceleration outside of the virtual machine in the host operating system could be targeted from inside the guest operating system. An example of a vulnerability that illustrated this principle was the NVIDIA Binary Graphics Driver for Linux Buffer Overflow Vulnerability.[29] Symantec speculates that this type of vulnerability could be exploited from within the guest operating system to break into the host system. For enterprises that rely on separation through the use of software virtualization technology, the impact of this type of threat could be considerable.

The second type of threat that Symantec believes could emerge is related to the impact that software-virtualized computers may have on random number generators that are used inside guest operating systems on virtual machines. This speculation is based on some initial work done by Symantec Advanced Threat Research in a paper on GS and ASLR in Windows Vista. This research showed that the method used to generate the random locations employed in some security technologies would, under certain circumstances, differ wildly in a software-virtualized instance of the operating system. If this proves to be true, it could have considerable implications for a number of different technologies that rely on good randomness, such as unique identifiers, as well as the seeds used in encryption.

In the short to medium term, enterprises need to fully understand any potential impact that the use of software virtualization may have on the security of their environment and plan accordingly. They should control and monitor host operating systems very strictly, as the expected activity would likely be limited to the starting and stopping of virtual machines. Symantec feels that these threats constitute an important area of research and will continue to investigate and monitor these issues.

[29] http://www.securityfocus.com/bid/20559

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