SYMANTEC ENTERPRISE SECURITY

Symantec Internet Security Threat Report

Trends for July 05–December 05

Volume IX, Published March 2006

Dean Turner
Executive Editor
Symantec Security Response

Stephen Entwisle
Editor
Symantec Security Response

Oliver Friedrichs
Technical Advisor
Symantec Security Response

David Ahmad
Manager, Development
Symantec Security Response

Joseph Blackbird
Assoc. Software Engineer
Symantec Security Response

Marc Fossi
DeepSight Threat Analyst
Symantec Security Response

Daniel Hanson
DeepSight Threat Analyst
Symantec Security Response

Sarah Gordon
Sr. Principal Research Engineer
Symantec Security Response

David Cole
Director, Product Management
Symantec Security Response

David Cowings
Sr. Business Intelligence Manager
Symantec Business Intelligence

Dylan Morss
Principal Business Intelligence Analyst
Symantec Business Intelligence

Brad Bradley
Sr. Business Intelligence Analyst
Symantec Business Intelligence

Peter Szor
Security Architect
Symantec Security Response

Eric Chien
Security Researcher
Symantec Security Response

Jeremy Ward
Systems Engineer Mgr.
U.K. Sales Communications

Jesse Gough
DeepSight Threat Analyst
Symantec Security Response

Josh Talbot
DeepSight Threat Analyst
Symantec Security Response

Volume IX, Published March 2006

Symantec Internet Security Threat Report

Contents

Executive Summary 4

Symantec Internet Security Threat Report Overview 6

Future Watch 19

Attack Trends 24

Vulnerability Trends 45

Malicious Code Trends 66

Additional Security Risks 83

Appendix A—Symantec Best Practices 102

Appendix B—Attack Trends Methodology 104

Appendix C—Vulnerability Trends Methodology 109

Appendix D—Malicious Code Trends Methodology 114

Appendix E—Additional Security Risks Methodology 115

Executive Summary

The previous edition of the Symantec *Internet Security Threat Report* discussed a significant shift in the threat landscape. In this edition, the new threat landscape is shown to be increasingly dominated by attacks and malicious code that are used to commit cybercrime, criminal acts that incorporate a computer or Internet component. Attackers have moved away from large, multipurpose attacks on network perimeters and toward smaller, more focused attacks on client-side targets.

The threat landscape is coming to be dominated by emerging threats such as bot networks and customizable modular malicious code. Targeted attacks on Web applications and Web browsers are increasingly becoming the focal point for cybercriminals. Whereas traditional attack activity has been motivated by curiosity and a desire to show off technical virtuosity, many current threats are motivated by profit. They often attempt to perpetrate criminal acts, such as identity theft, extortion, and fraud, for financial gain.

This volume of the *Internet Security Threat Report* will offer an overview of threat activity that took place between July 1 and December 31, 2005. This brief summary will offer a synopsis of the data and trends discussed in the main report. As the new threat landscape unfolds, Symantec will continue to monitor and assess threat activity in order to prepare consumers and enterprises for the complex Internet security issues to come.

Attack Trends Highlights

- For the fifth consecutive reporting period, the Microsoft® SQL Server Resolution Service Stack Overflow Attack was the most common attack, accounting for 45% of all attacks.
- Symantec detected an average of 39 attacks per day, down from 57 attacks per day in the first half of 2005.
- The average number of denial of service (DoS) attacks detected per day was 1,402, an increase of 51% from the first half of 2005.
- Of the Web servers that were tested, Windows® 2000 Server with no patches was compromised in the shortest average time, roughly one hour and 17 minutes.
- Symantec identified an average of 9,163 bot-infected computers per day, down from 10,347 last period.
- The United States was the location of 26% of the world's bot-infected computers, the most of any country.
- Financial services was the most frequently targeted industry.
- During the last six months of 2005, the United States was the source country of 31% of attacks, the most of any country

Vulnerability Trends Highlights

- Symantec documented 1,896 new vulnerabilities, the highest recorded number since 1998.
- Symantec documented 40% more vulnerabilities in 2005 than in 2004.
- Web application vulnerabilities made up 69% of all vulnerabilities during this period.
- The average time between the announcement of a vulnerability and the appearance of exploit code was 6.8 days, up from 6.0 days.
- On average, 49 days elapsed between the disclosure of a vulnerability and the release of an associated patch, down from 64 days.
- A 42-day window of exposure existed on average between the release of an exploit and the release of an associated patch by the vendor.
- Of vulnerabilities disclosed during this period, 79% were classified as "easy to exploit," up from 73%.
- Microsoft Internet Explorer had the highest number of new vulnerabilities (including both vendor confirmed and non-vendor confirmed), with 24.
- The Mozilla Firefox browser had the highest number of new vendor-confirmed vulnerabilities, with 13.

Malicious Code Trends Highlights

- Symantec documented more than 10,992 new Win32 viruses and worms, up slightly from 10,866 in the first half of 2005.
- Sober.X was the most widely reported malicious code sample, followed by Nestky.P and Mytob.ED.
- Excluding the high volume of Sober.X reports, 80% of malicious code threatened confidential information, up from 74%.
- Of malicious code targeting instant messaging services, worms made up 91%, compared to 83% in the first half of 2005.
- Modular malicious code accounted for 88% of the top 50 malicious code reported, up from 77%.
- Bot-related malicious code reported to Symantec accounted for 20% of the top 50 malicious code reports, up from 14%.
- Symantec documented 6,542 new variants of Spybot, up from 6,361 in the first half of the year.

Additional Security Risks Highlights

- The most commonly reported adware program was Websearch,[1] which accounted for 19% of the top ten adware programs reported.
- CometCursor was the most commonly reported spyware program, accounting for 42% of the top ten spyware programs.
- In the last half of 2005, Symantec blocked 1.5 billion phishing attempt, a 44% increase over the first half of 2005.
- One in 119 emails was determined to be a phishing attempt, up from one in 125.
- Symantec detected an average of 7.9 million phishing attempts per day, an increase of 39% over the first half of 2005.
- Spam made up 50% of all monitored email traffic.
- Spam associated with financial goods and services was the most common type of spam.
- The United States was the country of origin of 56% of all spam.

[1] http://securityresponse.symantec.com/avcenter/venc/data/adware.websearch.html

Symantec 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 and additional security risks. This summary of the current 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 of the *Internet Security Threat Report* covers the six-month period from July 1 to December 31, 2005.

Symantec has established some of the most comprehensive sources of Internet threat data in the world. The Symantec™ Global Intelligence Network, which includes the Symantec DeepSight™ Threat Management System and Symantec™ Managed Security Services, consists of more than 40,000 sensors monitoring network activity in more than 180 countries and comprehensively tracks attack activity across the entire Internet. 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 also maintains one of the world's most comprehensive databases of security vulnerabilities, covering over 13,000 vulnerabilities affecting more than 30,000 technologies from over 4,000 vendors. In addition to the vulnerability database, Symantec operates BugTraq,™ one of the most popular forums for the disclosure and discussion of vulnerabilities on the Internet. 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. The Symantec *Internet Security Threat Report* is grounded principally on the expert analysis of this data. 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 intends to provide enterprises and consumers with the information they need to help effectively secure their systems now and in the future.

Threats to confidential information

Threats that expose confidential information on a compromised computer are a concern to users in home, small business, and enterprise environments alike. These threats may expose sensitive data such as system information, cached logon credentials, or confidential files and documents that could subsequently be used in cybercrime activities. With the increasing use of online shopping and Internet banking, compromises of this nature can result in significant financial loss, particularly if credit card information or banking details are exposed. Furthermore, these losses can lead to a decline in consumer confidence, thereby affecting organizations that rely on the Internet for revenue generation.

During the last six months of 2005, the percentage of malicious code samples that threaten confidential information declined somewhat. This is not necessarily due to a reduction in these threats; rather, it is likely due to the high volume of Sober.X reports. If Sober.X is removed from consideration, the percentage

of malicious code that threatens confidential information rose from 74% in the previous period to 80% in the current period. This is a significant increase over the 54% of confidential information exposure threats during the same six-month period in 2004.

The increase in confidential information threats this period (Sober.X notwithstanding) can largely be attributed to the large number of Mytob variants in the top 50 malicious code. Mytob variants allow attackers to log keystrokes, steal cached passwords, and download files, all of which are ways of exposing confidential information, which can subsequently be used in cybercrime activities.

Other prevalent information exposure threats can also be used to generate monetary gain for their authors. For instance, variants of the Bancos[2] and Banpaes[3] password-stealing Trojans remained among the top 50 most reported malicious code samples this period. These crimeware threats can be used to steal a user's online banking credentials in order to transfer money out of the victim's account.

Web application vulnerabilities

Web applications are technologies that rely on a browser for their user interface; they are often hosted on Web servers. Vulnerabilities in these technologies are particularly threatening because they are typically exposed to the Internet through a Web server. Because traditional security solutions such as intrusion detection systems and firewalls allow Web traffic onto a network by default, Web-based attacks can leave organizations exposed to attacks that are difficult to detect and prevent. As such, Web application vulnerabilities could allow an attacker to bypass traditional perimeter security measures, such as firewalls. This could enable a successful attacker to then compromise an entire network by gaining access through a single vulnerable system. Vulnerabilities in these technologies can also give an attacker access to confidential information from databases without having to compromise any servers.

Of the vulnerabilities disclosed between July and December 2005, 69% were associated with Web applications. This represents a 15% increase over the first half of 2005 when they made up 60% of all vulnerabilities. In the second half of 2004 they accounted for 49% of all vulnerabilities.

As the number of Web application vulnerabilities grows, Symantec believes that they may serve as an increasingly attractive target for potential attackers to exploit. Organizations should manage their Web-based assets carefully. If they are developing Web applications in-house, developers should be educated about secure development and the use of secure shared components. 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.[4]

Web browser vulnerabilities

Browser vulnerabilities are a serious security concern due to their use in conducting online fraud. They may also be exploited for the propagation of spyware and adware in drive-by downloads and through malicious Web sites. Web browser vulnerabilities also allow attackers to circumvent traditional perimeter security devices such as firewalls and routers. With these protective measures being increasingly deployed in home and enterprise environments alike, the exploitation of Web browser vulnerabilities has become one of the easiest ways to attack users.

[2] http://securityresponse.symantec.com/avcenter/venc/data/pwsteal.bancos.html
[3] http://securityresponse.symantec.com/avcenter/venc/data/pwsteal.banpaes.html
[4] http://www.owasp.org

During the last six months of 2005, 24 new vendor-confirmed and non-vendor-confirmed vulnerabilities were disclosed that affected at least one version of Microsoft Internet Explorer (figure 1). This is the same number that was seen in the previous six-month period. During this reporting period, the increasingly popular Firefox browser from Mozilla was affected by 17 new vendor-confirmed and non-vendor-confirmed vulnerabilities, down from the 32 seen in the previous period. Symantec believes that Internet Explorer will likely remain a popular target for the foreseeable future because of its widespread deployment.

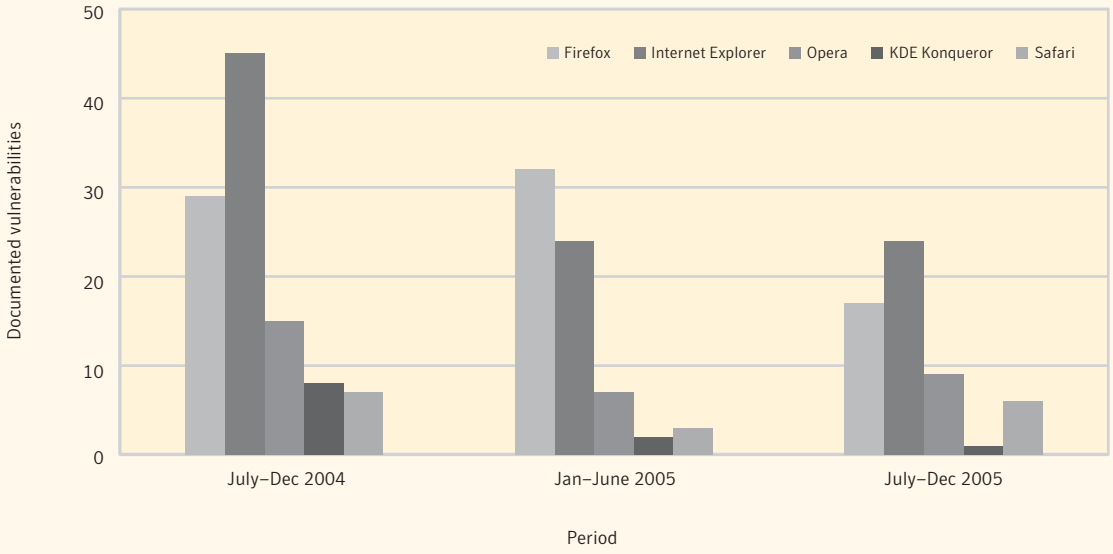

Figure 1. Web Browser vulnerabilities, vendor confirmed and non-vendor confirmed
Source: Symantec Corporation

A slightly different picture appears when assessing only vendor-confirmed vulnerabilities. During this reporting period, the Firefox browser from Mozilla had the highest count of vendor-confirmed vulnerabilities (figure 2). Thirteen out of the 17 vulnerabilities disclosed for Firefox were vendor confirmed, down from 27 out of 32 in the first half of 2005. Twelve out of the 24 vulnerabilities associated with Microsoft Internet Explorer were confirmed by the vendor, a slight decrease from the 14 out of 24 disclosed between January and June 2005.

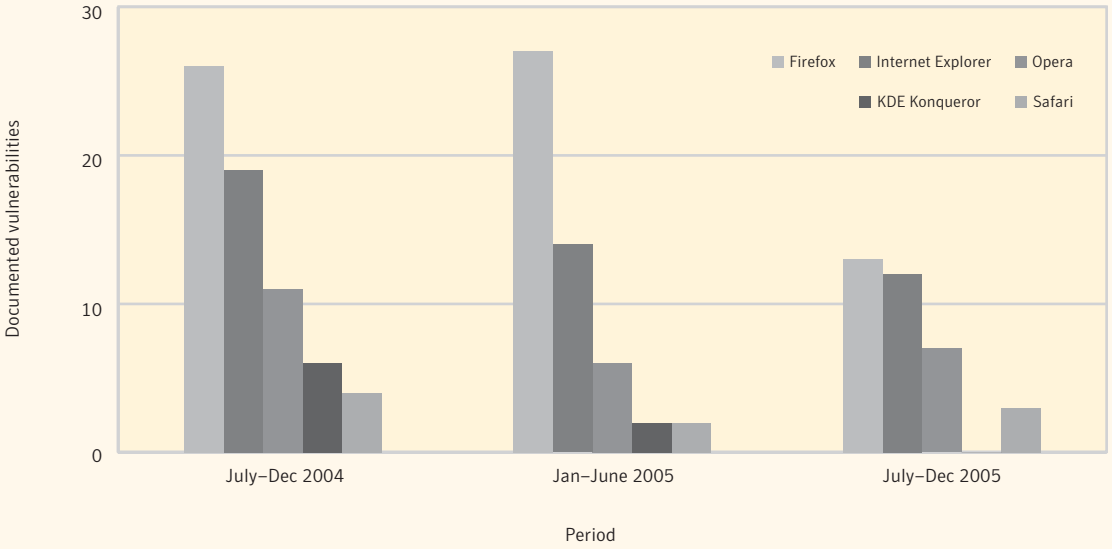

Figure 2. Web browser vulnerabilities, vendor confirmed
Source: Symantec Corporation

When taking only the vendor-confirmed browser vulnerabilities into consideration, Firefox has had the highest vulnerability count for the last three reporting periods. This may be indicative of the transparency that is inherent in the open-source development process. Due to the nature of the open-source development process, Firefox developers may be able to acknowledge and address vulnerabilities more quickly than developers of closed-source browsers.

Total volume of vulnerabilities

The second half of 2005 was marked by a slight increase in the total number of vulnerabilities disclosed. Between July 1 and December 31, 2005, Symantec documented 1,896 new vulnerabilities. This is an increase of one percent over the 1,871 vulnerabilities disclosed in the first half of the year and 34% over the 1,416 vulnerabilities disclosed in the second half of 2004. As was pointed out in the "Web application vulnerabilities" section above, 69% of all vulnerabilities documented by Symantec in the second half of 2005 affected Web applications.

Between July and December 2005, Symantec rated 45% of new vulnerabilities as highly severe, down from 49% in the first half of the year. At the same time, vulnerabilities that were rated as moderately severe increased from 48% to 52% over the past six months. Symantec believes that this is due to an increase in vulnerabilities affecting Web applications, the majority of which are classified as moderately severe.

Symantec recommends that administrators employ an asset management system and a vulnerability alerting service, which can help them to quickly assess the threat that new vulnerabilities pose to their

organization. Symantec also recommends that enterprises invest in resources that provide alerting and patch-deployment solutions. They should also consider engaging a managed security service provider to assist them in monitoring their networks. Administrators should also monitor vulnerability mailing lists and security Web sites for new developments in vulnerability disclosure.

Symantec also recommends that security administrators follow the best practices outlined in Appendix A of this report. Administrators should audit their systems to ensure that no vulnerable Web applications or scripts are being hosted on them. Administrators should also thoroughly review the need for and use of all Web applications. Only those Web applications that are required for enterprise operations should be deployed.

Time to compromise for Internet-connected computers

For the first time, this volume of the *Internet Security Threat Report* is assessing the amount of time it takes for attackers to compromise a newly installed operating system once it has been connected to the Internet. This metric has been developed to give insight into how quickly an Internet-connected computer may become compromised. This will help administrators and users to understand the immediacy of potential threats against Internet-facing computers.

Symantec defines the "time to compromise" as the time that elapses between connection of a computer to the Internet and the instance when it is considered to be compromised.[5] The first group of computers assessed for this metric consisted of Web servers. Of the Web servers that were tested, Windows 2000 Server with no patches had the shortest average time to compromise, at roughly one hour and 17 minutes.[6] Microsoft Windows 2000 Server with Service Pack 4 had the second fastest time to compromise, and the unpatched Microsoft Windows 2003 Web Edition was compromised in the third shortest time. The unpatched RedHat® Enterprise Linux® 3 was not compromised during the test period.

When the servers were fully patched, no compromise occurred. This supports Symantec's assertion that applying patches in a timely manner is an important component of an effective security strategy.

The second group of computers assessed for time to compromise consisted of desktop systems. Microsoft Windows XP Professional with no patches applied had the shortest average time to compromise at one hour and 12 seconds. The Microsoft Windows 2000 Professional operating system without patches and the Microsoft Windows 2000 Professional operating system with Service Pack 4 applied had the second and third shortest times, respectively.

The SuSE™ Linux 9 Desktop, which was deployed in its default configuration and was not patched, was not compromised during the testing period.[7] Furthermore, Microsoft Windows 2000 Professional fully patched, Microsoft Windows XP Professional with Service Pack 2, and Microsoft Windows XP Professional fully patched were not compromised during the reporting period.

Symantec believes that these findings reinforce the notion that organizations should apply all necessary patches in a timely manner. It also illustrates the need to apply updates to newly installed systems from a secure position; that is, prior to connection to the Internet.

[5] Symantec performs automated heuristic analysis on the computer to determine when it is considered to be compromised. It should be noted that multiple failed compromise attempts are often observed prior to a successful compromise.
[6] For a complete listing of operating systems and their time to compromise statistics, please see the "Attack Trends" section of this report.
[7] The testing period for the time to compromise was from November 16 to December 31, 2005.

Window of exposure

Attackers use custom-developed code known as exploit code to take advantage of vulnerabilities to compromise a computer. Once exploit code is developed and released, any unpatched vulnerabilities will be susceptible to compromise. Symantec records the window of time between the disclosure of a vulnerability and the appearance of third-party exploit code designed to take advantage of it. The intent is to determine how long after a vulnerability is announced it will be susceptible to a successful attack.

During the second half of 2005, the average time for exploit code development was 6.8 days. This is an increase of almost a full day over the average time of 6.0 days in the previous six-month period. This may be due to the commercialization of exploit code, which is discussed at length in the "Attack Trends" section of this report. As a result of commercialization of vulnerabilities, the best exploit code developers may have stopped making their findings and creations public. Instead, they may be opting to sell their work to organizations that are willing to pay for vulnerability research. As a result, publicly known exploit code is being created by less experienced exploit developers, leading to an increase in the average exploit code development time.

When a vulnerability is announced, the vendor in whose product it was found must develop and release a set of code known as a patch that will secure the vulnerability. Until the patch is developed, released, and applied computers on which the vulnerability resides may be susceptible to successful attack, particularly if exploit code for that vulnerability is available. The time between the disclosure date of a vulnerability and the release date of a patch is known as the "time to patch." During the second half of 2005, the time to patch was, on average, 49 days. This means that, on average, seven weeks elapsed between the publication of a vulnerability and the release of an associated patch. This is a sharp decrease from the 64 days seen in the first half of the year.

In the time between the availability of exploit code and the application of a patch, computers hosting the vulnerable applications will be exposed to potential compromise. Symantec refers to this time as the "window of exposure." During the last six months of 2005, 42 days elapsed on average between the appearance of exploit code and the release of a patch by the vendor to fix the affected vulnerability. This has dropped considerably from the 58-day window of exposure in the first half of 2005. During this period of time, and until a patch is released, end users and administrators may be forced to implement security "workarounds" without an official fix and networks could be vulnerable to compromise.

With the window of exposure so large, Symantec recommends that administrators employ a good asset management system or vulnerability alerting service. Each of these services can provide an understanding of the threat posed by new vulnerabilities and provide relevant protection and mitigation information. Administrators should also monitor vulnerability mailing lists and security Web sites for new developments. They should also consider installing an intrusion prevention system to block attacks targeting vulnerabilities. Finally, organizations should consider engaging a managed security service provider to assist them in monitoring their networks.

Denial of service attacks

Denial of service (DoS) attacks attempt to limit the target computer's ability to service legitimate network requests, therefore denying services the computer is supposed to provide to legitimate users. They are a

major threat to organizations, especially those that rely on the Internet for communication and to generate revenue. They are particularly dangerous because they are very difficult to defend against. Over the last six months of 2005, Symantec detected an average of 1,402 DoS attacks per day (figure 3). This is an increase of 51% from the first half of 2005, when Symantec detected an average of 927 DoS attacks per day.

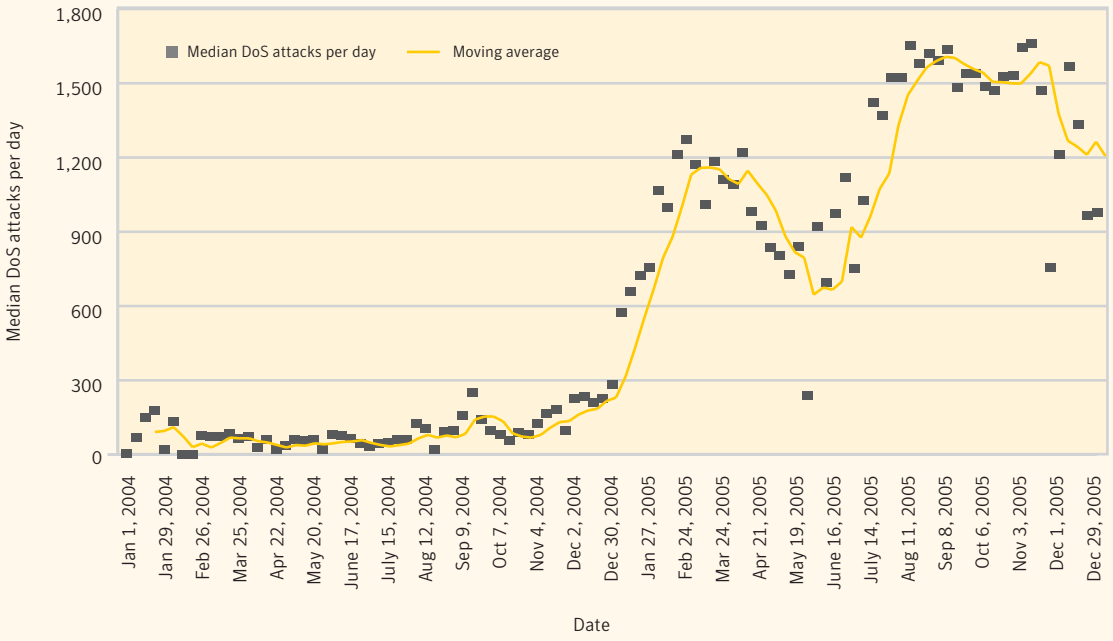

Figure 3. DoS attacks per day
Source: Symantec Corporation

The rise in DoS attacks may indicate that an entrenched and well organized community of attackers is beginning to utilize their resources to carry out more coordinated attacks. Many of these attackers are likely to be owners of bot networks.[8] As Symantec discussed in the previous volume of the *Internet Security Threat Report,* criminal extortion schemes based on DoS attacks are becoming more common.[9] Further, it appears that some of these schemes are achieving their objectives.[10] Symantec believes that as bot networks become larger and more coordinated, and as organizations continue to relent and pay extortionists, this form of attack will continue to increase.

Organizations should ensure that a documented procedure exists for responding to DoS events. Symantec also recommends that organizations perform egress filtering on all outbound traffic. One 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 Internet service provider (ISP). Further, once a DoS attack is identified, the targeted organization will likely need to engage its ISP to help filter the traffic to minimize the impact of the attack.

[8] Bots (short for "robots") 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 communication channels are used to 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.
[9] Symantec *Internet Security Threat Report* Volume VIII (September 2005) http://enterprisesecurity.symantec.com/content.cfm?articleid=1539: p. 11
[10] http://www.networkworld.com/news/2005/051605-ddos-extortion.html

Top bot-infected countries

Recognizing the ongoing threat posed by bot networks, Symantec tracks the distribution of bot-infected computers worldwide. The identification of bot-infected computers is important, as a high percentage increases the potential for bot-related attacks to occur. It could also indicate the level of patching and security awareness amongst computer administrators and users in a given region.

Over the second half of 2005, the United States had the highest number of bot-infected computers of any country (table 1). Twenty-six percent of bot-infected computers worldwide were situated there. Twenty-two percent of all bot-infected computers worldwide were located in the United Kingdom, the second highest number during this period. Nine percent of detected bot-infected computers were located in China, placing it in third position worldwide.

Rank Jul–Dec 2005	Rank Jan–Jun 2005	Country	Percent of bot-infected computers July–Dec 2005	Percent of bot-infected computers Jan–June 2005
1	2	United States	26%	19%
2	1	United Kingdom	22%	32%
3	3	China	9%	7%
4	5	France	4%	4%
5	6	South Korea	4%	4%
6	4	Canada	4%	5%
7	10	Taiwan	3%	2%
8	9	Spain	3%	3%
9	7	Germany	3%	4%
10	8	Japan	2%	3%

Table 1. Top bot-infected countries
Source: Symantec Corporation

For this volume of the *Internet Security Threat Report,* Symantec has monitored the distribution of bot command-and-control servers.[11] Over the last six months of 2005, the United States had the highest proportion of command-and-control servers in the world, accounting for just over 48% of the global total. South Korea ranked second with nine percent of the total and Canada ranked third with six percent.

In addition to having the most bot-infected computers and the most command-and-control servers, the United States also experienced the highest percentage of growth in bot-infected computers. The number of bot-infected computers situated there increased by 39% in the second half of 2005. The rise in the number of bots in the United States is likely closely linked with broadband Internet growth there. China had the second largest increase of bot-infected computers during the last six months of 2005, 37%. China's increase in bot-infected computers is also likely related to its growth in broadband Internet connections. It is also an indicator that China is a popular target for bot network owners.

[11] Bot command-and-control servers are computers that bot network owners use to relay commands and instructions to other computers on their bot networks.

Instant messaging threats

Instant messaging (IM) continues to grow rapidly, with users in both home and enterprise environments estimated at 300 million in 2005. The three largest IM providers—AOL Instant Messenger, MSN Messenger, and Yahoo! Messenger—each report over 1 billion messages sent per day and IM traffic is expected to exceed email traffic by the end of 2006.

Instant messaging can be a potent vector for the spread of malicious code. The infection of one computer can result in messages being broadcast to all users contained in an IM contact list on that machine, creating the potential for rapid proliferation. Furthermore, social engineering tactics can be highly effective as the parties communicating by IM are inherently trusted.

In the second half of 2005, worms were the preferred type of malicious code on all three large IM networks, making up 91% of IM-related malicious code during this period. This is a ten percent increase over the 83% in the first half of 2005. Worms were also used to download other non-IM malicious code during the period. For instance, a worm may send users a link to a Web page exploiting a vulnerability in a Web browser,[12] such as the Microsoft Windows Graphics Rendering Engine WMF SetAbortProc Code Execution Vulnerability.[13] This would allow the malicious code hosted on the Web page to be automatically installed on the computer of a user running a vulnerable browser.

Phishing activity

Phishing is an attempt by a third party to solicit confidential information from an individual, group, or organization, often 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 conduct cybercrime activities for profit.

Over the last six months of 2005, the percentage of emails that Symantec identified as phishing messages was nine percent higher than during the first half of the year. Between July 1 and December 31, 2005, phishing attempts made up 0.84% of the messages processed by Symantec. This is an increase over the first six months of 2005, when 0.77% of the messages processed were phishing messages. While 0.84% may not appear to be a significant number, it means that roughly one out of every 119 email messages scanned was found to be a phishing attempt. This is an increase from the roughly one out of 125 email messages that constituted phishing attempts in the first half of 2005.

The number of phishing attempts blocked by Symantec Brightmail™ AntiSpam in the last six months of 2005 also indicates that phishing activity continues to increase. During this period, Symantec blocked 1.5 billion phishing attempts, a 44% increase over the 1.04 billion phishing attempts detected in the first six months of the year. It is also a 175% increase over the 546 million blocked phishing attempts detected in the last six months of 2004.

Phishing messages that are blocked at the mail servers of Symantec Brightmail AntiSpam customers are reflective of phishing activity targeting email users globally. Based on the activity seen over the last six months of 2005, Symantec believes that it is reasonable to conclude that phishing activity will continue to increase.

[12] http://tc.imlogic.com/threatcenterportal/pubThreatDetail.aspx?ThreatID=3505
[13] http://www.securityfocus.com/bid/16074

Symantec recommends that enterprise users protect themselves against phishing threats by filtering email at the server level through the mail transfer agent (MTA).[14] Although this will likely remain the primary point of filtering for phishing, organizations can also use upstream IP-based filtering, as well as HTTP filtering. DNS block lists (DNSBLs)[15] also offer more general protection and may mitigate some of the risk of phishing emails.

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.[16] Organizations should also keep their employees notified of the latest phishing attacks and how to avoid falling victim to them.[17]

Spam activity

Between July 1 and December 31, 2005, spam made up 50% of all monitored email traffic. This is a decrease from the first six months of 2005 when 61% of all email was classified as spam. It is also lower than the second half of 2004, when just over 60% of email was classified as spam.

This does not necessarily signify any decrease in spam attack attempts to Internet email users. As was the case during the first six months of 2005, this decline is likely due to the fact that network and security administrators are using IP filtering and traffic shaping to control spam.[18] If a message is blocked using these methods, it will not be detected by the Symantec Probe Network, and will thus not contribute to statistics gathered.

The most common type of spam detected in the first six months of 2005 was related to health services and products, which made up 32% of all spam on the Internet during this time. The next largest spam category was commercial products, which made up 30% of all spam. The third most common type of spam was that associated with financial products and services, which made up 15% of all spam.

During the first six months of 2005, 56% of all spam received worldwide originated in the United States. This is likely due to the high number broadband users in that country. The United States was also the country of origin of spam in the first half of 2004, when 51% of spam originated there. China was the second highest country of origin during the current reporting period with 12%, followed by South Korea with nine percent.

Adware and spyware

Traditionally, the Symantec *Internet Security Threat Report* has broken security threats down into three general categories: attacks, vulnerabilities, and malicious code. However, as Internet-based services and applications have expanded and diversified, the potential for computer programs to introduce other types of security risks has increased. For the past several years, Symantec has monitored developments in these concerns. For the past two reporting periods, Symantec has discussed these security risks in the *Internet Security Threat Report*.

[14] Message transfer agents are programs that are responsible for routing email messages to the proper destination.
[15] A DNSBL is simply a list of IP addresses that are known to send unwanted email traffic. The DNSBL is used by email software to either allow or reject email coming from IP addresses on the list.
[16] 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/conline/pubs/alerts/phishingalrt.htm
[17] A good resource for information on the latest phishing threats can be found at http://www.antiphishing.org
[18] IP filtering simply involves comparing inbound connection attempts against a preconfigured list of bad or suspicious IP addresses.Traffic shaping is the use of different IP characteristics—for instance, if an originating IP is determined to be a known source of spam—to selectively determine what connections to allow, deny, or throttle (slow down).

Between July 1 and December 31, 2005, the most commonly reported adware program was Websearch,[19] which accounted for 19% of the top ten adware programs reported. This program was not present in the top ten reported adware programs in the first six months of the year.

Websearch features a number of noteworthy attributes. It modifies the default home page and search settings of Internet Explorer, installs itself as a toolbar to Internet Explorer, and adds a number of icons to the system tray. It also sends user information to a predetermined Web site, including keywords from searches. It also uses an interesting technique known as a "watchdog process" to prevent manual removal of components of the program. If a user attempts to stop a process associated with the adware program, a second running process restarts it as soon as it has been stopped, thereby increasing the difficulty of removing the program.

In the first six months of 2005, CometCursor[20] was the most commonly reported spyware program, accounting for 42% of the top ten spyware programs reported to Symantec. It was the fourth most frequently reported spyware program in the first half of 2005 but was not present in the top ten spyware programs in the second half of 2004. CometCursor is an Internet Explorer browser help object (BHO) that installs a toolbar that has links to affiliate sites.[21] It is bundled with various programs or can be downloaded from a Web page using an ActiveX installer. CometCursor also installs a search bar and logs the compromised system's usage statistics.

Programs that are used to detect and remove adware programs often do so by using signatures that are based on known characteristics of the adware. Adware vendors will frequently update the program in order to evade these signatures to avoid detection and subsequent removal from a system. In some cases the functionality of the adware program may also be updated. During the last six months of 2005 the adware program that self-updated most frequently was Aurora,[22] which did so 13.6 times per day. The top self-updating spyware program was Apropos,[23] which self-updated 1.3 times per day.

Symantec rates the risk level of adware and spyware programs according to how they affect the performance and privacy of compromised computers and whether the program exhibits stealth behavior and/or resists removal from the compromised computer. During the last six months of 2005 Symantec gave three of the top ten adware programs a high risk rating: BetterInternet, Lop, and IEPlugin.[24] A program that is given a high risk rating will exhibit at least one of four characteristics. It may have a significant impact on the system's stability and/or performance. It may expose confidential, sensitive information. It may resist complete removal. Or it may exhibit stealth behaviors, such as silent installation, the absence of a user interface, and concealment of application processes.

Modular malicious code

Modular malicious code initially possesses limited functionality, such as disabling antivirus software and firewalls; however, once it has infected a computer, it can download additional code that has new, potentially more damaging capabilities. These may allow it to further compromise the target computer or to perform other malicious tasks. The intent of the initial modular code is only to establish an outpost on the machine. As such, it is usually stealthy and very small—50kb or less—and difficult to detect.

[19] http://securityresponse.symantec.com/avcenter/venc/data/adware.websearch.html
[20] http://securityresponse.symantec.com/avcenter/venc/data/spyware.cometcursor.html
[21] Browser helper objects (BHOs) are add-on programs that can add legitimate features to a user's browser (IE 4.X and up). For example, document readers used to read programs within the browser do so via BHOs. BHOs can also be used to install security risks on a user's Web browser using ActiveX controls
[22] http://securityresponse.symantec.com/avcenter/venc/data/adware.aurora.html
[23] http://securityresponse.symantec.com/avcenter/venc/data/spyware.apropos.html
[24] For more details on Symantec's risk levels, please see: http://securityresponse.symantec.com/avcenter/enterprise/security_risks/#riskAssessment

In the previous volume of the *Internet Security Threat Report,* Symantec stated that modular malicious code would likely be an issue of concern in the near future.[25] This appears to be the case. Between July and December of 2005, modular malicious code accounted for 88% of the top 50 malicious code reported. This is an increase of 14% over the 77% reported from January to June 2005. It is a further increase of 40% over the 63% reported in the second half of 2004.

Frequently, modular malicious code is used to download applications that gather confidential information without the knowledge and consent of the user. If these applications are used for financial gain, they are referred to as "crimeware."[26] By using modular malicious code, attackers may download and simultaneously install a confidential information threat on a large number of compromised computers. The confidential information exposed by this threat could then be used for the attacker's financial gain.

In order to protect against modular malicious code, administrators should implement strict egress filtering,[27] which can prevent compromised computers within their networks from contacting Web sites where additional malicious code components are kept. This will prevent the second—and frequently more severe—module of the malicious code from being installed on the compromised computer.

Win32 virus and worm variants

Over the second half of 2005, Symantec documented more than 10,992 new Win32 viruses and worms. While this is consistent with the 10,866 detected in the first half of the year, it is a 49% increase over the 7,360 documented in the second half of 2004 (figure 4). The significant increase over 2004 is due to the continued development of Win32 worms that implement bot features that attackers can use for financial gain.

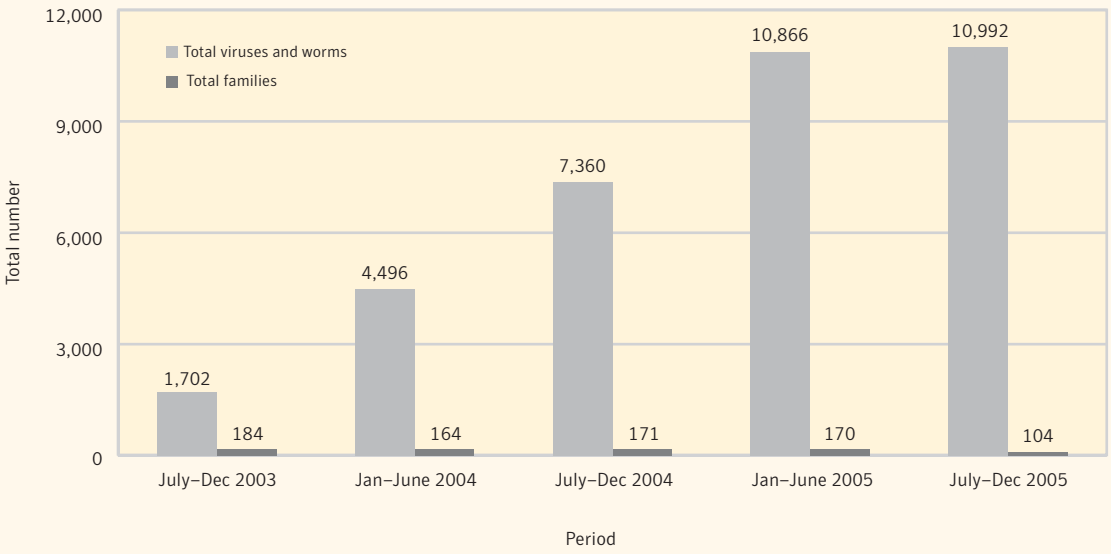

Figure 4. New Win32 virus and worm variants
Source: Symantec Corporation

[25] Symantec *Internet Security Threat Report*, Volume VIII (September 2005) http://enterprisesecurity.symantec.com/content.cfm?articleid=1539: p. 83
[26] Crimeware is an application that aids in the commission of cybercrime activity.
[27] Egress traffic refers to traffic that is leaving a network, bound for the Internet or another network.

While the number of new Win32 viruses and worms per period continues to grow, the number of new Win32 families decreased over the second half of 2005. The number of new families per period had remained relatively consistent over the previous four reporting periods. However, in the current period, the number of new families declined by 39%, from 170 new families in the first half of 2005 to 104 this period. This indicates that there are currently far more variants of existing malicious code families being produced than previously. One example of this is the Spybot family, which now requires four letters to describe a variant such as "W32.Spybot.ABCD". The rise in variants paired with the decline in new families can be partially attributed to the availability of source code for some families.

As of December 31, 2005, the total number of Win32 virus and worm variants surpassed 39,257. In 2005 alone Symantec documented more than 21,830 Win32 variants. Thus, the total number of Win32 virus and worm threats more than doubled during 2005 alone, indicating that these threats will continue to dominate the malicious code landscape for some time to come.

Malicious code propagation vectors

Worms and viruses use various means of transferring themselves from one computer to another. These transportation vectors are collectively known as "propagation mechanisms." Propagation mechanisms can include a number of different vectors, such as Simple Mail Transfer Protocol (SMTP),[28] Common Internet File System (CIFS),[29] peer-to-peer services (P2P), and remotely exploitable vulnerabilities.

SMTP was the most commonly used malicious code propagation vector in the second half of 2005. It was employed by 26 of the top 50 malicious code samples that propagate, accounting for 92% of the volume of top 50 malicious code reports with propagation mechanisms this period. In the first half of 2005 only 19 of the top 50 malicious code samples that propagate used SMTP, accounting for 52% of the volume of the top 50 malicious code reports.

The prevalence of this vector is not surprising since email is one of the most widely employed applications on the Internet. The increase in the use of SMTP this period can be attributed to Sober.X and multiple variants of Mytob, both of which are mass-mailer worms that send copies of themselves from compromised computers by email. In addition to being used as a malicious code propagation vector, SMTP is also used to send Trojans in spam email. This is worrisome for organizations, as Trojans can be used to expose confidential information and install other types of crimeware such as keystroke loggers on targeted systems.

Organizations can protect against SMTP threats by blocking all email attachments at the mail gateway. If there is a business need for email attachments, only those that are considered safe (as determined by an organization's security policy) should be allowed. If other attachment types are accepted, they should always be scanned by antivirus products with up-to-date definitions. Attachments should only be accepted from trusted sources. End users should be educated to only open email attachments that come from trusted sources and that are expected.

[28] SMTP is the protocol by which email is transmitted between mail servers.
[29] CIFS is used for file sharing.

Future Watch

The previous sections of the *Internet Security Threat Report* have discussed Internet security developments between July 1 and December 31, 2005. This section will discuss emerging trends and issues that Symantec believes will become prominent over the next twelve to eighteen months. These forecasts are based on emerging data that Symantec has collected during the current reporting period and are speculative in nature. In discussing potential future trends, Symantec hopes to provide organizations with an opportunity to prepare themselves for rapidly evolving and complex security issues.

Cybercrime expected to rise

Over the past two reporting periods Symantec has observed a worrisome trend in Internet attacks and in the development and use of malicious code. In Volume VIII of the *Internet Security Threat Report*, Symantec took special notice of the shift from hacking for fame to hacking for fortune.[30] This shift in the threat landscape is expected to escalate over the next six to eighteen months. Attackers appear to be moving away from threats that destroy or compromise data and toward the theft of confidential, financial and personal information for financial gain.

Tools that are used in the commission of such activities are often referred to as crimeware. Symantec is forecasting an increase in the number and type of crimeware. Symantec also expects the trade of malicious code in popular forums such as Internet Relay Chat (IRC), Web sites, and black market auction sites to expand. Symantec research has found that the development of malicious code is becoming a coordinated, well funded effort by numerous development teams in different locales.[31] During the last six months of 2005, over 80% of the Top 50 malicious code threats reported to Symantec had the potential for data theft.[32] Over the next twelve to eighteen months, Symantec expects to see an increase in malicious code that is designed specifically to generate profit.

As discussed in this volume of the Symantec *Internet Security Threat Report*, criminals are using technologies that assist them in generating and maximizing revenue. As a result, Symantec expects to see an increase in the number of threats designed specifically for these purposes. Keystroke loggers, spyware, phishing attacks, and Trojans are expected to increase in numbers and in severity. Symantec also expects that the purpose of network-based attacks will continue to shift from one-time compromises and informational sorties to compromises designed to build supporting infrastructures for the facilitation and spread of crimeware.

Increase in malicious code utilizing stealth capabilities

Once malicious code infects a user's computer, it often attempts to remain unnoticed, either by actively hiding or by simply not making its presence on a system known to the user. It may employ different techniques to obscure its presence on the user's computer. Symantec speculates that the number of malicious programs using these methods will continue to grow, with one of the more common—rootkit techniques—experiencing particular growth.[33]

[30] Symantec *Internet Security Threat Report*, Volume VIII (September 2005) http://enterprisesecurity.symantec.com/content.cfm?articleid=1539, p. 4
[31] http://www.symantec.com/avcenter/cybercrime/index_page5.html
[32] This figure excludes from consideration reports of Sober.X, which was the most prominent malicious code report during this period. Please see the "Threats to confidential information" section in the "Malicious Code Trends" report in this document
[33] Definitions of the term "rootkit" vary but for the purposes of this discussion, a rookit is defined as a set of tools designed to hide the presence of a running process and avoid detection and removal of that process.

Rootkit techniques allow certain programs to maintain a persistent and undetectable presence on a machine. Rootkits do not infect machines by themselves, like viruses or worms; rather, they seek to provide an undetectable environment in which malicious code and security risks can execute their functionalities. Attackers will typically exploit vulnerabilities in the target machine or use social engineering techniques to manually install rootkits. In some cases, rootkits can be installed automatically upon execution of a security risk. In other cases, a user could unknowingly download the rootkit simply by browsing to a malicious Web site. Once installed, a rootkit can allow the subversion of system reporting facilities to hide the presence of an attacker, files, and communication, amongst other things.

Symantec speculates that by employing rootkit techniques to evade detection and removal, attackers and cybercriminals may be able to further compromise systems by downloading additional malicious code and, in turn, hide their functions from the operating system and the user. If so, an attacker would be able to perform virtually any function on the system, including remote access, the theft and transmission of confidential information, and the installation of additional security risks such as adware and spyware.

The ability to use rootkit techniques has already been demonstrated in malicious code such as Fanbot[34] and security risks such as adware and spyware.[35] There has also been some discussion about the ability of malicious code to utilize rootkit techniques and hide itself in flash memory on computer motherboards.[36] With the shift in the threat landscape towards cybercrime and the generation of profit, Symantec speculates that an increasing amount of malicious code will utilize rootkit techniques for these purposes.

Increased commercialization of vulnerability research

As discussed in the "Vulnerability Trends" section of this report, the commercialization of vulnerability research is a growing phenomenon. As more commercial vendors have begun purchasing vulnerability information, a marketplace for security research has emerged that extends beyond traditional disclosure forums such as mailing lists and Web sites. Symantec expects that this will have a profound effect on vulnerability research. It could also seriously affect the ability of enterprises and consumers to protect themselves from non-disclosed vulnerabilities and zero-day exploit code.[37]

In the past, unless employed by a vendor directly, a vulnerability researcher would generally disclose his or her work on security Web sites and mailing lists. However, with the emergence of a market for commercialized vulnerability information, security researchers may able to sell vulnerabilities to different purchasers for a range of prices, depending on the severity of the vulnerability and its impact on an organization. Symantec believes that as the market broadens, security researchers will find themselves facing a fractured marketplace that has few standards and regulations. This in turn could lead to calls for legislating the sale of vulnerability information and the possible criminalization of vulnerability research.

As more security researchers choose to disclose their vulnerabilities to third-party commercial entities for profit, Symantec expects that the number of commercially acquired vulnerabilities will increase. Recently, there have been attempts to use popular auctioning venues to sell vulnerabilities to the highest bidder.[38] There have also been attempts to establish specialized vulnerability auctioning venues (which have thus far failed to materialize due to legal uncertainties).[39] This is indicative of a desire within the security community to establish alternative markets to facilitate the sale of vulnerability and exploit code information.[40] This raises the possibility that as competing markets emerge, black market bounties could

[34] https://www-secure.symantec.com/avcenter/venc/data/w32.fanbot.a@mm.html
[35] http://www.symantec.com/avcenter/reference/when.malware.meets.rootkits.pdf
[36] http://www.securityfocus.com/news/11372
[37] Non-disclosed vulnerabilities are often referred to in a process known as closed disclosure, which refers to the practice of disclosing vulnerabilities to only a commercial vulnerability vendor or the affected vendor without notifying other reporting organizations.
[38] http://www.securityfocus.com/news/11363
[39] http://www.security-express.com/archives/dailydave/2005-q2/0308.html
[40] http://www.securityfocus.com/news/11364

be used to commercialize vulnerability research in order to generate exploit code for use in cybercrime, spyware, and corporate espionage.

This could have profound implications for organizations and end users, as vulnerability information will be given a financial value that may motivate researchers to sell that information on either the open market or the black market to the highest bidder, rather than disclosing them publicly on mailing lists and Web sites. While this might stimulate an increase in vulnerability research, it could also force the disclosure of such research underground. If such a situation develops, security administrators could be at risk of not being aware of vulnerabilities on their systems, leaving them susceptible to zero-day attacks.[41]

As a result, Symantec speculates that while the number of publicly disclosed vulnerabilities could decrease, the window of exposure to potential threats could increase, as details about vulnerabilities are held privately for greater periods of time. This could in turn increase the likelihood of leaked vulnerabilities and the development of privately held exploit code. If vulnerability research becomes increasingly marginalized and moves further underground, enterprises, consumers, and small businesses could face longer windows of exposure, thereby increasing their exposure to potential threats.

It should be noted that some vendors may resist the commercialization of vulnerability information as a matter of principle, choosing instead to follow published industry coalition guidelines for vulnerability disclosure.[42] Furthermore, smaller vendors or open-source projects with limited resources may be excluded from the commercialization process if they cannot afford to pay for vulnerability research on their own products. This may place these vendors and projects in a position of competitive disadvantage as well as placing them and their customers at greater security risk.

Non-traditional platform threats expected to emerge

The expansion of consumer entertainment systems, integrated voice and data devices, and online gaming presents new and interesting security challenges. As more of these devices become integrated into existing IP networks, they may present new vectors for attackers to exploit to gain access to more traditional networks. For instance, gaming consoles such as Microsoft's Xbox,® Sony's Playstation® and Playstation® Portable (PSP™) and the Nintendo® DS have begun adding Internet connectivity to their products. This has allowed these devices to connect to traditional IP networks. Networked devices could be compromised and used as platforms from which to launch attacks against other systems on the same network, including the propagation of malicious code.

Sony's PSP is a case in point. On October 6, 2005, it became one of the first handheld gaming devices to be victimized by malicious code.[43] While more traditional attacks such as viruses and worms have yet to appear, these devices could become transfer platforms for malicious code through the use of memory cards, Bluetooth,® and IP technology. It appears that an established community of researchers is already reverse engineering and modifying existing game console platforms.[44] Symantec believes that these consoles could become platforms from which to launch attacks against traditional computer systems. This is of particular concern for the consumer market, as the majority of these devices are connecting through home networks, which may not have the same level of security as enterprise environments.

[41] 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 public knowledge or even known of by the vendor of the affected technology.
[42] http://www.dhs.gov/interweb/assetlibrary/vdwgreport.pdf
[43] http://www.sarc.com/avcenter/venc/data/trojan.pspbrick.html
[44] http://www.xbox-linux.org/wiki/Main_Page

Voice and data devices such as Research in Motion's (RIM) Blackberry™ and Palm's Treo™ 700w have become increasingly popular, with Blackberry subscribers totaling over 1,340,000.[45] Over the past year several vulnerabilities in RIM's software have been disclosed.[46] While no vulnerabilities have been reported in the Treo 700w at the time of writing of this report, its ability to run Window's Mobile could make it susceptible to vulnerabilities targeting applications running on that platform. As integrated voice and data devices, Blackberry and Treo could also be susceptible to voice spam and malicious code directed towards standard wireless technologies.

Malicious code targeting online gaming has already been detected in significant volumes. The online game Lineage has been the target of a Trojan horse that attempts to steal users' passwords. The Lineage Trojan was the most widely reported malicious code sample in the Asia Pacific region in 2005.[47] Furthermore, in August 2005 a worm that stole players' usernames, passwords and other data caused an online game to suspend the trading of users' accounts.[48] The data harvested by these attacks is likely intended to be used in cybercrime activities for financial gain.

Furthermore, there have also been reports of phishing attacks targeting user account information for multi-player online role-playing games. According to these reports, the information obtained through successful attacks is used to steal and sell virtual items on auction sites for real money. Symantec speculates that as virtual online gaming communities increase in popularity, they will become a more prominent target for cybercrime, particularly as the trade in stolen virtual goods is difficult to track.

A "boom" cycle for bots and bot networks

Much of the discussion in the "Vulnerability Trends" section of this report focused on the rise in Web application vulnerabilities and the large number of Web browser vulnerabilities. Symantec speculates that these developments will have important implications for the growth of bots and bot networks worldwide.

As was discussed in the "Attack Trends" section of this report, security administrators have implemented measures such as port blocking to stop communication between bots and bot owners. As a result, attackers will likely adjust their methods of establishing and controlling bot networks. They may begin to use different communication channels and encryption as a means of avoiding capture and detection.[49] This ongoing battle between attackers and security administrators has resulted in a cyclical trend in bot activity. Symantec refers to this as a boom-and-bust cycle in the number of bots and bot networks.[50]

Currently, there appears to be a lull in bot network growth. However, Symantec speculates that this will change as new and more potent attack vectors are developed. The "Vulnerability Trends" section of this report documented the rise in Web application vulnerabilities and the growing number of Web browser vulnerabilities. These vulnerabilities may create the potential for large increases in bots and bot networks. Attacks that target them are usually conducted by HTTP and, as such, may bypass filtering mechanisms that are in place on the network perimeter. Additionally, Symantec has observed increased sophistication in the exploitation of attacks against Web applications, culminating in the development of self-propagating malicious code targeting them. Attackers could exploit widely deployed Web applications and Web browsers to install malicious code, particularly bots.

[45] http://www.geekzone.co.nz/content.asp?contentid=2972
[46] http://search.securityfocus.com/swsearch?query=Blackberry&sbm=bid&submit=Search%21&metaname=alldoc&sort=swishrank
[47] http://securityresponse.symantec.com/avcenter/venc/data/pwsteal.lineage.html
[48] http://www.theregister.co.uk/2005/08/24/fantasy_role_play_worm/
[49] http://news.com.com/Bots+may+get+cloak+of+encryption/2100-7349_3-5952102.html
[50] For further discussion of this trend please see the "Attacks Trends" section of this report.

The widespread deployment of Web applications and Web browsers presents attackers with a large number of easily exploitable targets. For instance, Web browser vulnerabilities can lead to the exploitation of vulnerabilities in operating system components and individual applications, which can lead to the installation of malicious code, including bots. Given the potential for widespread exploitation of Web application and Web browser vulnerabilities, Symantec speculates that a new vulnerability in a widely deployed Web technology could mean a large and rapid increase in the number of bot networks.

Increase in phishing messages and malicious code distributed through instant messaging

As organizations adjust their security measures in response to the changing threat landscape, attackers continue to look for new methods and tactics to avoid detection. As discussed in the "Malicious Code Trends" section of this report, malicious code propagating through instant messaging (IM) is on the rise. Symantec expects this to continue. The increasing adoption and use of IM clients and networks, including the newly released Google Talk™ service, will add to the attack vectors that are available. Additionally, as corporations begin adopting internal IM networks that can connect to the public IM networks, the complexity of these networks and number of connected users will increase. As a result, the number of potential IM targets for malicious code is expected to expand, creating the likelihood for increased attack activity against this vector.

Symantec speculates that phishing will become an increasing security concern for IM services. This activity has traditionally been conducted by email, particularly using spam messages. However, phishers have begun to leverage new delivery mechanisms, such as instant messaging. In 2005, Symantec detected four phishing attempts that were conducted over IM networks, including two in the second half of the year. While this number is small, it indicates that attackers are becoming aware of the potential of IM for this malicious activity.

Phishing is particularly dangerous for IM users because of the nature of IM communications. IM users are inherently trusted by the people on their contact lists; as a result, IM users are less likely to suspect that IM communications could constitute malicious activity. Symantec believes that as the use of IM services increases, phishing attacks targeting IM users will increase accordingly.

Attack Trends

This section of the Symantec *Internet Security Threat Report* will provide an analysis of attack activity for the period between July 1 and December 31, 2005. An attack is defined as any malicious activity carried out over a network that has been detected by an intrusion detection system or firewall. An attack is typically an attempt to exploit a vulnerability in software or hardware. Attack activity for this period will be compared to that presented in the previous *Internet Security Threat Report*.[51] Wherever applicable, suggestions on attack remediation will be made along with references to Symantec's best practices, which are outlined in Appendix A of this report.

The Symantec Global Intelligence Network monitors 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. In addition to these sources, Symantec has developed and deployed a honeypot network that is used to identify, observe, and study complete instances of attacker and malicious code activity.[52] It helps to provide details about how some of the attack activity identified in this section is carried out. These resources combine to give Symantec an unparalleled ability to identify, investigate, and respond to emerging threats. This discussion will be based on data provided by all of these sources.

Security devices can monitor for attacks and suspicious behavior at many different levels on the network. Devices such as intrusion detection systems (IDS), intrusion protection systems (IPS), firewalls, proxy filters, and antivirus installations all contribute to the overall security of an organization. Symantec gathers data from many of these devices. One consequence of this data-gathering scheme is that malicious code data and attack trends data often address the same activity in different ways. For instance, attack trends data is based on the number of infected sources that are attempting to spread. On the other hand, malicious code data is based primarily on reports of attempted propagation. This can lead to different rankings of threats presented in the "Attack Trends" and "Malicious Code Trends" sections of this report.

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

- Top Internet attacks
- Top attacked ports
- Attack activity per day
- Time to compromise Internet-connected computers
- Bot networks
- Top bot-infected countries
- Denial of service attacks
- Top originating countries
- Top targeted industries

Top Internet attacks

The attacks discussed in this section are the most common attacks detected by the Symantec Global Intelligence Network, which includes Symantec Managed Security Services and the Symantec DeepSight Threat Management System. They are determined by the percentage of the total attacking IP addresses

[51] Symantec *Internet Security Threat Report* Volume VII (March 2005) and Volume VIII (September 2005). Both are available at: http://enterprisesecurity.symantec.com/content.cfm?articleid=1539

[52] A honeypot is an Internet-connected system that acts as a decoy, allowing an attacker to enter the system in order to observe the attacker's behavior inside the compromised system.

that perform a given attack. These attacks reflect activity that occurs across the Internet as a whole and is thus indicative of activity that security administrators are likely to observe on their own networks. The majority of these attacks are carried out by malicious code and bot networks, while a smaller proportion are carried out by individual attackers.

The top ten attacks changed significantly over the course of 2005. Six of the attacks for the second half of the year were not in the top ten for the first half and attacks targeting Web-based and email-based services have become more common. Accordingly, attacks that were previously popular have begun to drop off. For example, in the first half of 2005 the Microsoft Windows DCOM RPC Interface Buffer Overrun Attack was the ninth most common; however, over in the second half of the year, it was ranked nineteenth.

In the previous volume of the *Internet Security Threat Report,* Symantec speculated that as perimeter defenses became more prominent, attacks against Web-based services and client-side vulnerabilities would become more common.[53] Attack activity over the past six months appears to support this assertion, as nearly half of the attacks in the top ten targeted Web-based technologies.

In the previous two versions of the *Internet Security Threat Report* (Volume VII and VIII), Symantec speculated that this shift in attacks was due to effective patching and security precautions, as well as ingress and egress filtering of known attacks at the router level, especially by ISPs.[54] These factors have had the effect of reducing the number of computers that are exposed to previously popular and effective attacks, thereby forcing attackers to adopt new tactics.

Between July 1 and December 31, 2005, the Microsoft SQL Server Resolution Service Stack Overflow Attack was the most common attack (table 2). Also known as the Slammer Attack because of its initial association with the Slammer worm,[55] this attack accounted for 45% of attacking IP addresses during this period. This is an increase of 36% over the first half of 2005, when it accounted for only 33% of attacking IP addresses.

In spite of this increase in proportion, the actual number of IP addresses observed carrying out this attack dropped slightly from the previous reporting period. This is due primarily to the drop in prominence of other attacks. As has been discussed, previously popular attacks have become less common, likely as a result of patching and widespread implementation of perimeter security measures. With the reduction in previously common attacks, the Microsoft SQL Server Resolution Service Stack Overflow Attack has increased proportionately despite an overall drop in volume.

The continued prominence of this attack can be attributed to a number of factors. The first is that it is commonly carried out using a single UDP packet.[56] The nature of UDP makes it possible for attackers and malicious code to forge the address of the sender when carrying out an attack, a practice known as spoofing.[57] This may inflate the number of distinct IP addresses that Symantec observes performing the attack. Furthermore, a complete attack can be conducted with a single UDP packet. This allows attackers to launch considerably more attacks, as the complexity of the required network communication is minimal.

The success of this attack may also aided by two other factors. The first is that a number of highly successful bots—such as Gaobot[58] and Spybot[59]—use it. The second is the high volume of computers running vulnerable software. This attack affects both the Microsoft SQL Server and the MSDE (Microsoft Desktop Engine), which is included with some third-party software. This makes patching the exploited

[53] The Symantec *Internet Security Threat Report*, Volume VIII (September 2005): p. 1 http://enterprisesecurity.symantec.com/content.cfm?articleid=1539
[54] The Symantec *Internet Security Threat Report*, Volume VIII (September 2005): p. 21
[55] http://securityresponse.symantec.com/avcenter/venc/data/w32.sqlexp.worm.html
[56] User Datagram Protocol
[57] Spoofing is commonly used to obscure the origin of the attack. This tactic makes investigation and response more difficult by making infected computers and attackers untraceable.
[58] http://securityresponse.symantec.com/avcenter/venc/data/w32.hllw.gaobot.aa.html
[59] http://securityresponse.symantec.com/avcenter/venc/data/w32.spybot.worm.html

vulnerability across the enterprise very difficult, as each affected software package requires its own patch. Furthermore, this vulnerability will be introduced whenever a vulnerable application is installed. If patches are not applied to the software shortly after installation, it is likely that a compromise will occur.

Rank July–Dec 2005	Rank Jan–June 2005	Attack	Percent of attackers July–Dec 2005	Percent of attackers Jan–June 2005
1	1	Microsoft SQL Server Resolution Service Stack Overflow Attack	45%	33%
2	4	Generic HTTP Directory Traversal Attack	5%	4%
3	15	Generic ICMP Flood Attack	3%	1%
4	6	Generic WebDAV/Source Disclosure HTTP Header Request Attack	3%	3%
5	12	Generic HTTP CONNECT TCP Tunnel Attack	3%	2%
6	23	Sendmail Header Processing/Prescan corruption Buffer Overflow Attack	2%	1%
7	10	Generic Cross-Site Scripting in URL Attack	2%	2%
8	13	Microsoft FrontPage Sensitive Page Attack	2%	2%
9	7	Generic X86 Buffer Overflow (TCP NOPS) Attack	2%	3%
10	17	Possible Incoming Malicious Attachment Event	2%	1%

Table 2. Top attacks
Source: Symantec Corporation

The Generic HTTP Directory Traversal Attack was the second most common attack during the second half of 2005. It was used by five percent of the total attacking IP addresses during this period, up from four percent in the previous period. The increase in the prominence of this attack is likely due to a number of reasons, including the shift of attack activity away from network perimeters and toward Web-based applications and services.

The prominence of this attack is also due to the ease with which directory traversal attacks can be conducted, as well as the fact that they are effective against Web servers and a wide range of Web applications. A directory traversal attack requires no complex computer code but only a single HTTP GET request.[60] This allows attackers to issue many attacks against target systems. Furthermore, a successful directory traversal attack offers high potential rewards, such as access to sensitive information—server configurations and application data, for instance—that could, in turn, facilitate further compromise of the target computer.

The third most common attack in the last six months of 2005 was the Generic ICMP Flood Attack, which accounted for three percent of the total attacking IP addresses. This attack was the fifteenth most common in the first half of the year, when it accounted for only one percent of all attacking IP addresses. Denial of service (DoS) attacks that use ICMP flooding are carried out by bombarding a target computer with ICMP echo request or reply packets that are commonly utilized by ping utilities.[61]

[60] An HTTP GET request is issued to a Web server to retrieve resources such as Web pages and image files.
[61] ICMP (Internet Control Message Protocol) is employed by the TCP/IP stack to handle error and control messages.

The rise in popularity of this attack coincides with an increase in the popularity of other forms of DoS attacks, such as SYN flood attacks, which are described in the "Denial of service attacks" discussion below. ICMP flood DoS attacks are popular because they are relatively easy to execute. Publicly available tools and code for these attacks have existed for some time, allowing them to be easily incorporated into malicious code, such as bots.[62] To defend against ICMP flood attacks, Symantec recommends that organizations implement intrusion detection systems. They should also perform ingress and egress filtering on all network communications.[63]

DoS attacks in general appear to be gaining in popularity. The previous volume of the *Internet Security Threat Report* discussed how DoS attacks have been reported in extortion attempts.[64] In such schemes, criminals threaten to render the targeted organization's Web site or online service inaccessible for a period of time if their demands for payment are not met.[65] These DoS extortion schemes are a prime example of cybercrime, the use of computers and the Internet to conduct criminal activities, usually for financial gain.

Top attacked ports

Assessing the top attacked ports allows security personnel to understand which ports (and associated services) attackers may be targeting. This discussion is based on data that is derived from firewall sensors that record each rejected or denied connection attempt. As a result, legitimate port activity should not be represented in the data. This metric does not attempt to provide any specific attack information. It merely reflects attacker interest in a given port. It does not assume that there is necessarily an attack associated with it, nor does it assume that a specific service is being targeted.

The lack of definitive attack information means that it is impossible to distinguish between information-gathering attacks, exploit attempts, or any other type of potentially malicious activity. However, administrators can use this data to assess which ports and services are most commonly being targeted and configure their systems' security accordingly.

[62] See the Bot Networks discussion below for more information on bot network computers.
[63] 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.
[64] The Symantec *Internet Security Threat Report*, Volume VIII (September 2005): p 11
[65] http://www.networkworld.com/news/2005/051605-ddos-extortion.html

Rank July–Dec 2005	Rank Jan–June 2005	Port	Service Description	Percent of attackers July–Dec 2005	Percent of attackers Jan–June 2005
1	3	1026 UDP	Various dynamic services	17%	9%
2	1	445 TCP	CIFS/SMB (Microsoft Windows File Sharing)	12%	18%
3	5	443 TCP	Secure World Wide Web (HTTPS)	8%	7%
4	4	80 TCP	World Wide Web (HTTP) services	8%	7%
5	6	25 TCP	Simple Mail Transfer Protocol (SMTP) services	8%	6%
6	2	135 TCP	DCE-RPC (remote Microsoft Windows communication)	8%	13%
7	10	6346 TCP	Gnutella (file sharing)	5%	3%
8	9	139 TCP	NetBIOS (Microsoft Windows File Sharing)	5%	3%
9	7	4662 TCP	Edonkey (file sharing)	3%	5%
10	17	6881 UDP	BitTorrent (file sharing)	3%	1%

Table 3. Top attacked ports
Source: Symantec Corporation

In the second half of 2005, UDP port 1026 was the most frequently targeted port. It was targeted by 17% of attackers (table 3). This is an 88% increase over the first half of 2005, when it was targeted by nine percent of attackers. This port is typically associated with the Windows Messaging Service. Windows Messaging Service is not related to Windows Messenger or MSN Messenger in any way; rather, it facilitates the Net Send functionality, which allows a user on one computer to send pop-up messages to users on another computer.

The frequency of attacks against this port may be due to the nature of the UDP protocol, which allows attackers to forge the address of the sender when carrying out an attack. This practice, known as spoofing, is commonly employed to obscure the attacker's location. It could also inflate the number of attacking IP addresses and thus increase the prominence of this port.

Activity over UDP port 1026 is also widely used to relay pop-up spam messages on Microsoft Windows computers through the Windows Messenger Service. Although this port is usually strictly controlled by organizations at the network perimeter, home users and small businesses without sufficient security infrastructure could be targeted by spammers. Furthermore, pop-up spam targeting this port is very simple to construct and send in high volume as the entire pop-up can be sent in a single UDP packet. This allows messages to be sent to a large number of computers without requiring excessive resources.

Over the last six months of 2005, TCP port 445 was the second most frequently targeted port, accounting for 12% of all attacking IP addresses. This is a 33% decrease from the first half of the year, when it was targeted by 18% of attackers and was the most frequently targeted port. In the second half of 2004, it was targeted by 35% of attackers.

TCP port 445 has been a popular target due to the many services that run over it. These include Microsoft File and Printer Sharing (often referred to as SMB or CIFS), as well as some remote management functionality, including some remote procedure call (RPC) functionality. Furthermore, several high-profile vulnerabilities are exploitable through this port, such as Microsoft Windows LSASS Buffer Overrun Vulnerability[66] and the Microsoft Windows DCOM RPC Interface Buffer Overflow Vulnerability.[67] Each of these has public exploit code available and each has been targeted by Spybot and Gaobot. This port is also exploitable through the Microsoft Windows Plug and Play Buffer Overflow Vulnerability,[68] which was targeted by Zotob.[69]

In spite of these considerations, attack activity targeting port 445 is dropping. This drop is related to a decline in the number of reports of Gaobot, which uses CIFS as a propagation vector, over the past six months (for more discussion on this, please refer to the "Malicious Code Trends" report in this document). This is likely due to the implementation of stronger perimeter security defenses protecting this port.

Many organizations have secured port 445 and other ports offering Microsoft Windows services after they were successfully targeted by rapidly propagating worms such as Slammer.[70] Furthermore, the widespread implementation of personal firewalls has made attacks against this port less successful, and subsequently made other targets—such as Web servers and Web applications—more desirable.

Over the second half of 2005, the third most frequently targeted port was TCP port 443, which accounted for eight percent of all observed attacking IP addresses. This is a slight increase over the seven percent of attackers who targeted this port in the first half of 2005 when it was the fifth most targeted port.

TCP port 443 is associated with HTTPS, which is used to conduct secure Web transactions. Symantec believes that the prominence of this port—and TCP port 80 (HTTP), which followed very closely behind it in the top attacked port rankings—is due to the changing focus of attackers. As they find attacks against Microsoft Windows-based services less fruitful due to perimeter security enforcement, attackers appear likely to turn their attention to Web-based technologies and services. These technologies and services will often be available over TCP ports 443 and 80. It therefore follows that increased attack activity against these Web-based applications and services will result in increased activity against these two ports.

Attacks against these ports can be very attractive to attackers. Web servers are popular targets for a number of reasons. Attackers can exploit them to steal information that passes through them, such as credit card and bank information. Furthermore, they can serve as potential jump-off points into databases that hold sensitive client or user information. Compromised Web servers can also be used to host phishing sites. Finally, Web servers can be exploited to launch attacks against Web browsers that access them. This trend is supported by observations made in the "Top Internet attacks" discussion above, which shows that attacks targeting computers hosting Web services are becoming more prominent.

Finally, it is interesting to note that UDP port 1434 failed to rank among the top ten targeted ports during this reporting period. This is the port that is targeted by the Microsoft SQL Server Resolution Service Stack Overflow Attack, the top attack for this reporting period. The absence of this port in the top targeted ports is likely due to security policies that have been implemented on many networks. It is likely that administrators have disabled logging of infection attempts on this port for performance reasons or to simplify log auditing.

[66] http://www.securityfocus.com/bid/10108
[67] http://www.securityfocus.com/bid/8205
[68] http://www.securityfocus.com/bid/14513
[69] http://securityresponse.symantec.com/avcenter/venc/data/w32.zotob.a.html
[70] At the time of its release, the SQL Slammer worm was the fastest propagating worm ever, infecting 90% of all vulnerable computers within the first 10 minutes of its release. See the following link for further details: http://www.cs.berkeley.edu/~nweaver/sapphire/

Attack activity per day

The attack activity per day is determined by the number of attacks observed by the median organization in the sample set. As such, it is considered to be indicative of the number of attacks on the Internet as a whole. Organizations can use this metric to compare the number of attacks observed against their networks, potentially giving them insight into any anomalous activity that may arise.

Attacks discussed in this section include all malicious attempts to access a network, including attacks blocked at the firewall and network intrusion detection system levels. These attacks reflect attack activity that security administrators are likely to observe on their own networks.

Figure 5. Attack activity per day
Source: Symantec Corporation

Between July 1 and December 31, 2005, Symantec detected an average of 39 attacks per day (figure 5). In each of the two previous six-month periods, Symantec detected an average of 57 attacks per day. This equates to a decrease of 32% over the last six months of 2005.

Symantec speculates that this drop in the daily attack rate reflects a move away from conventional vectors by attackers. As outlined in both the "Top Internet attacks" and "Top attacked ports" discussions, attackers appear to be shifting their focus away from attacks against Microsoft Windows operating systems services and toward Web-based targets.

While the number of attacks being detected is down, it is likely that attack activity has not diminished to the same degree, if at all. Rather, attacks against Web-based technologies such as Web browsers and Web applications are less likely to be detected using conventional perimeter defenses. As such, they are not likely to be represented in this metric.

Time to compromise of Internet-connected operating systems

For the first time, in this volume of the *Internet Security Threat Report* Symantec is assessing the amount of time it takes for attackers to compromise a newly installed operating system once it has been connected to the Internet. This metric has been developed to give insight into how quickly an Internet-connected computer may become compromised. This will help administrators and users to understand the immediacy of potential threats facing Internet-facing computers and to illustrate the need to apply updates to newly installed systems from a secure position; that is, prior to connection to the Internet.

Attacks can be carried out by exploiting vulnerabilities or weaknesses in computers through two basic vectors:[71] remotely accessible services and client-side services.[72] Vulnerabilities in remotely accessible services may be targeted against a computer on a network without requiring any interaction from a user of the target computer. On the other hand, client-side vulnerabilities require user interaction before exploitation can take place. This discussion only considers attacks against remotely exploitable vulnerabilities and does not consider attacks that require user interaction.

The amount of time a computer is likely to be online prior to being compromised is influenced by a large number of factors, including: the computer's operating system, its configuration, patch levels, the security applications that are installed, and the perimeter security behind which it is placed. Furthermore, the location of the computer on the Internet can also influence the time to compromise. Some ISPs filter certain protocols at their boundary, resulting in reduced risk to computers on that ISP's network. Also, if a computer resides on a network that contains compromised computers, it is more likely to be attacked and compromised itself.

Symantec defines the "time to compromise" as the time that elapses between the moment at which the computer is made available on the network until the moment when it is considered to be compromised. Symantec performs automated heuristic analysis on the computer to determine when it is considered to be compromised. It should be noted that multiple failed attempts to compromise a computer are often observed prior to a successful compromise.

Because filtering and ISP policy can significantly affect the time to compromise of a computer, the data and the related discussion presented in this section may not be directly applicable to computer systems deployed on other ISPs or IP ranges. Rather, this discussion should simply be taken as a comparison of the potential time to compromise of various operating systems and configurations.

In order to assess the time to compromise, Symantec deployed honeypot systems running a cross-section of operating systems: Microsoft Windows 2000, Windows XP, and Windows 2003, as well as Red Hat Enterprise Linux 3 and SuSE Linux 9 Desktop. The Windows systems were deployed with three patch levels: unpatched, patched with the latest service pack, and fully patched. The computer systems were placed online between November 16 and December 31, 2005. All fully patched windows systems were deployed with full patches as of November 16, 2005. This discussion is based on data gathered during that period.

[71] Weakness refers to both programming weaknesses that may compromise security but are not necessarily vulnerabilities as well as weak security policies such as poor password protection.
[72] Client-side services refer to those operations that are conducted by applications that reside on a desktop computer or workstation, such as a browser, an email client, a word processing application. As such, they only provide services to the user that activated them, and are not accessible remotely through a network or the Internet.

Time to compromise—Web servers

The first group of computers assessed for the time to compromise metric consisted of Web servers (table 4). Seven different Web servers and configurations were tested. Where applicable, all installation default settings were maintained. When third-party installations were performed, the installation instructions provided by the vendor were used with no additional security measures taken. All Windows Web systems were deployed with the off-the-shelf version of IIS and the DotNetNuke content management software.[73] Microsoft Desktop Engine (MSDE), a version of the Microsoft SQL Server, was used to provide database support.

Symantec attempted to simulate computers deployed by a moderately experienced administrator with no significant security knowledge. As such, from a security perspective, all of the data described can be regarded as being derived from a worst-case system default installation. Symantec acknowledges and supports the statement that security can be significantly enhanced by hardening systems to minimize the attack profile. For further recommendations, please consult Symantec best practices, which are outlined in Appendix A of this report.

Configuration	Median Average (h:m:s)	Max (h:m:s)	Min (h:m:s)
Microsoft Windows 2000 Server – No Patches	1:16:55	18:27:47	0:01:14
Microsoft Windows 2000 Server – Service Pack 4	1:32:08	17:12:54	0:00:41
Microsoft Windows 2003 Web Edition – No Patches	4:36:55	23:00:13	0:02:08
RedHat Enterprise Linux 3 Web – Unpatched	Not Compromised	Not Compromised	Not Compromised
Microsoft Windows 2000 Server – Fully Patched	Not Compromised	Not Compromised	Not Compromised
Microsoft Windows 2003 Web Edition – Fully Patched	Not Compromised	Not Compromised	Not Compromised
Microsoft Windows 2003 Web Edition – Service Pack 1	Not Compromised	Not Compromised	Not Compromised

Table 4. Time to compromise, Web servers
Source: Symantec Corporation

Of the Web servers that were tested, Windows 2000 Server with no patches had the shortest average time to compromise, roughly one hour and 17 minutes. The minimum time for this server was one minute and 14 seconds and the longest was roughly 18 hours and 28 minutes. As can be seen from the maximum time between successful compromises and the shortest time between successful compromises, a considerable variation is possible. This was true of all three of the servers that were compromised.

[73] DotNetNuke is an open-source Web application framework designed to facilitate the implementation of Web applications including commercial Web sites, online publishing, and custom applications. No public vulnerabilities were reported or patches were applied to this application after it was deployed

The Web server with the second shortest time to compromise was the Microsoft Windows 2000 Server with Service Pack 4 applied. It had a median average compromise time of one hour and 32 minutes. The minimum time to compromise for this setup was 41 seconds, the fastest time of any system. The maximum time was roughly 17 hours and 13 minutes.

Of the three servers that were compromised during this test, the unpatched Microsoft Windows 2003 Web Edition had the longest time to compromise. It had a median average time to compromise of roughly four hours and 37 minutes. The fastest time to compromise for this setup was two minutes and eight seconds. The slowest time was 23 hours.

RedHat Enterprise Linux 3 was tested in an unpatched deployment and running Apache, Mod-PHP, MySQL and PHPNuke. It was not compromised during the assessment period.

In the case of each of the servers tested in this assessment, when the servers were fully patched, no compromise occurred. This supports the assertion that applying patches in a timely manner is part of an effective security strategy.

Time to compromise—desktop computers

The second group of computers assessed for the time to compromise metric consisted of desktop servers. Symantec assessed the time to compromise of seven different desktop operating systems and configurations (table 5). Where applicable, all installation default settings were maintained with the exception of firewalls, which were deactivated. If firewalls are appropriately configured, they would simply not allow any connections to the computer and comparisons between operating systems or patch levels would not be possible.

Configuration	Median Average (h:m:s)	Max (h:m:s)	Min (h:m:s)
Microsoft Windows XP Professional – No Patches	1:00:12	22:13:18	0:00:37
Microsoft Windows 2000 Professional – No Patches	1:03:18	20:18:03	0:01:19
Microsoft Windows 2000 Professional – Service Pack 4	1:14:20	21:02:48	0:00:39
SuSE Linux 9 Desktop	Not Compromised	Not Compromised	Not Compromised
Microsoft Windows 2000 Professional – Full Patch	Not Compromised	Not Compromised	Not Compromised
Microsoft Windows XP Professional – Full Patch	Not Compromised	Not Compromised	Not Compromised
Microsoft Windows XP Professional – Service Pack 2	Not Compromised	Not Compromised	Not Compromised

Table 5. Time to compromise, desktop computers with firewalls deactivated
Source: Symantec Corporation

All of the desktop operating system implementations that were compromised during the assessment period had similar average times to compromise. Furthermore, they all had similar maximum and minimum times to compromise. This is likely due to the fact that they are all vulnerable to many high-profile vulnerabilities, such as the Microsoft Windows LSASS Buffer Overrun Vulnerability[74] and the Microsoft Windows DCOM RPC Interface Buffer Overflow Vulnerability,[75] which are known to be exploited by malicious code.

Of the desktop computers that were assessed, Microsoft Windows XP Professional with no patches had the shortest average time to compromise at one hour and 12 seconds. The maximum time to compromise for this operating system was roughly 22 hours and 13 minutes, while the minimum time was a mere 37 seconds.

The Microsoft Windows 2000 Professional operating system without patches had the second shortest average time to compromise, approximately one hour and three minutes. It had a maximum time of roughly 20 hours and 18 minutes and a minimum time of one minute and 19 seconds.

The Microsoft Windows 2000 Professional operating system with Service Pack 4 applied had the third longest average time to compromise, approximately one hour and fourteen minutes. It had a maximum time of roughly 21 hours and two minutes and a minimum time of 39 seconds, the second shortest of any desktop system tested.

The SuSE Linux 9 Desktop version 9.3 was deployed in its default desktop configuration and was not patched. It was not compromised during the testing period.

Microsoft Windows 2000 Professional fully patched, Microsoft Windows XP Professional with Service Pack 2, and Microsoft Windows XP Professional fully patched were not compromised during the assessment period. This is likely due to a lag time between the release of patches and the production of exploits that can reliably compromise them. These findings enforce the importance of maintaining up-to-date patching levels, as fully patched computers are less likely to be compromised.

Bot networks

Bot networks are groups of compromised computers on which attackers have installed software that listens for and responds to commands, typically using IRC, thereby giving the attacker remote control over the computers. The software used to compromise and control these computers, known as bot software, may be upgraded to include new functionality, including exploit code that can target new vulnerabilities.

Bots can have numerous effects on an all Internet users, including home users, small businesses, and large organizations. A single infected host within a network (such as a laptop that was compromised outside the local network and then connected to the network, either directly or by VPN) can allow a bot to propagate to other computers that are normally protected against external attacks by corporate firewalls. Bots can be used by external attackers to perform DoS attacks against the enterprise's Web site, which can disrupt revenue for e-commerce companies. Furthermore, bots within an organization's network can be used to attack other organizations' Web sites, which can have serious legal consequences.

[74] http://www.securityfocus.com/bid/10108
[75] http://www.securityfocus.com/bid/8205

This metric explores the number of active bot network computers that the Symantec™ Global Intelligence Network detected and identified during the last six months of 2005. 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 will be considered bot-infected computers.

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

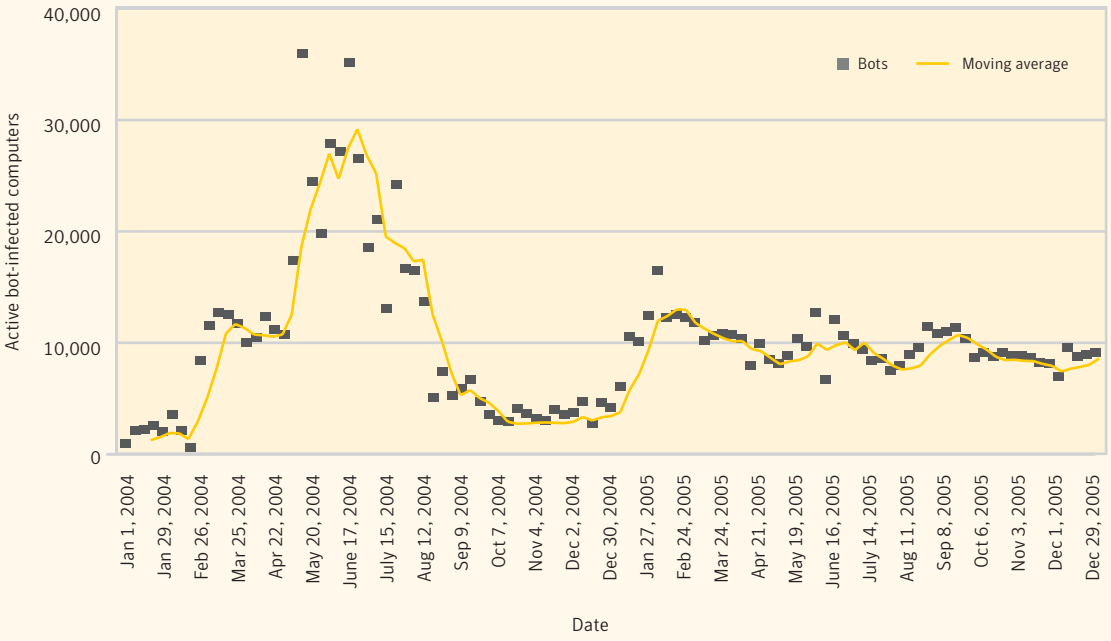

Figure 6. Bot-infected computers detected per day
Source: Symantec Corporation

Over the last six months of 2005, Symantec identified an average of 9,163 bot-infected computers per day (figure 6). This is a drop of 11% from the first half of the year, during which Symantec identified 10,347 bot-infected computers per day. Despite the decrease over the past six months, the number of bot-infected computers that Symantec has detected over the past year appears to have leveled off around the 10,000 bot mark. This leveling off is evident in the daily variance,[76] which has dropped from the previous reporting period (figure 7). As a result, the daily rate of bot-infected computers is becoming regular and more predictable.

[76] The measure of variance in this case is the difference in the numbers of bots seen each day. When evaluating the standard deviation of the daily bot numbers Symantec has observed a 52% decrease, indicating that the variance is dropping and the daily rate of bot-computers is becoming regular and more predictable.

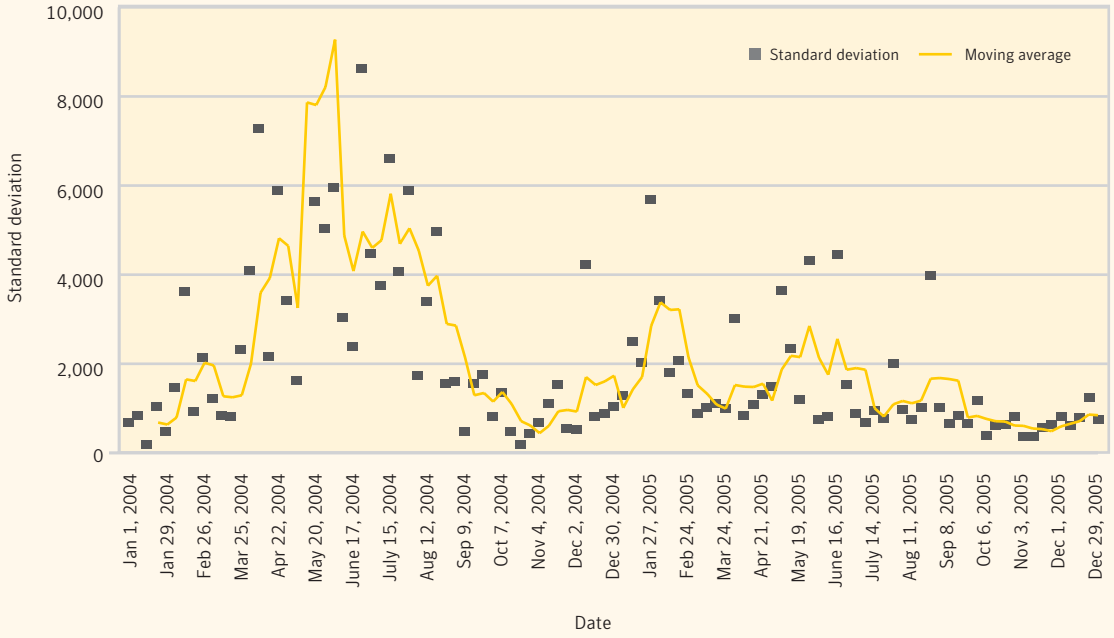

Figure 7. Daily variance in bot-infected computers
Source: Symantec Corporation

Having monitored the daily rates of bot-infected computers since the beginning of January 2004, Symantec has concluded that bot-infected computers follow a boom-and-bust population curve. Between February and June 2004, the number of bot-infected computers experienced significant growth. This boom period was driven by the rapid spread of Spybot and Gaobot.[77]

A subsequent bust cycle occurred between July and December 2004. As security professionals began to harden their computers and networks against the new bot threats, the number of bot infections dropped. Furthermore, the widespread deployment of perimeter security measures, such as firewalls, limited the ability for bots to propagate. As a result, bot infections lessened and the population decreased. Accordingly, during 2005 the number of bot-infected computers appears to have reached the carrying capacity of its environment.

Symantec speculates that if bots begin to exploit an attack vector that bypasses firewalls and perimeter defenses, the population of bot-infected computers could increase rapidly again. This impending boom period could have a greater impact on the Internet than the earlier one because bot network owners have become more organized and experienced. Furthermore, bot technology is much more entrenched due to the public disclosure of bot source code.

Symantec believes that vulnerabilities in Web browsers could fuel the next bot population boom. The widespread deployment of Web browsers, the large number of high-profile vulnerabilities affecting them,

[77] See the Symantec *Internet Security Threat Report* Volume VI (Jan–June 2004) for further information on the spread of Gaobot and Spybot.

and the relatively immature security infrastructure currently protecting them makes them a prime target for widespread bot infection. It is reasonable to conclude that if bot network owners begin to target Web browser vulnerabilities, the population of bot-infected computers will increase rapidly.

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

To reduce exposure to bot-related attacks, end users should employ defense in-depth strategies, including the deployment of antivirus software and a firewall.[78] Creating and enforcing policies that identify and limit applications that can access the network may also be helpful in limiting 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 the purpose of the attachment is known.

Top bot-infected countries

Recognizing the ongoing threat posed by bot networks, Symantec tracks the distribution of bot-infected computers worldwide. In order to do this, Symantec calculates the number of computers worldwide that are known to be infected with bots and assesses what percentage are situated in each country. This measure can help analysts understand how bot-infected computers are distributed globally. The identification of bot-infected computers is important, as a high percentage of infected machines likely indicates a greater potential for bot-related attacks. It could also indicate the level of patching and security awareness amongst computer administrators and users in a given region.

For this volume of the *Internet Security Threat Report* Symantec has also included an analysis of the distribution of bot command-and-control servers. Bot command-and-control servers are computers that bot network owners use to relay commands and instructions to other computers on their bot networks. This analysis should allow administrators to identify and understand the locations from which bot networks are being administered as well as the geographical distribution of bot networks.

Over the last six months of 2005, the United States was the site of the highest number of bot-infected computers of any country (table 6). Twenty-six percent of bot-infected computers worldwide were situated there. This is up from the first half of the year, during which 19% of bot-infected computers were located in the United States, the second highest number of bot-infected computers to the United Kingdom.

[78] 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.

Rank July–Dec 2005	Rank Jan–June 2005	Country	Percent of bot-infected computers July–Dec 2005	Percent of bot-infected computers Jan–June 2005
1	2	United States	26%	19%
2	1	United Kingdom	22%	32%
3	3	China	9%	7%
4	5	France	4%	4%
5	6	South Korea	4%	4%
6	4	Canada	4%	5%
7	10	Taiwan	3%	2%
8	9	Spain	3%	3%
9	7	Germany	3%	4%
10	8	Japan	2%	3%

Table 6. Top bot-infected countries
Source: Symantec Corporation

During the second half of 2005, 22% of all bot-infected computers worldwide were located in the United Kingdom, the second highest number during this period. This is down from the previous six-month period when the United Kingdom had the highest number of bot-infected computers with 32%.

Symantec has observed that bots usually infect computers connected to high-speed broadband Internet through large ISPs and that the expansion of broadband connectivity often facilitates the spread of bots. Frequently, ISPs will focus their resources on meeting growing broadband demand at the expense of implementing security measures, such as port blocking and ingress and egress filtering. As a result, ISPs that are growing or expanding their services rapidly may have security infrastructures that are underdeveloped relative to their needs.

The decrease in the percentage of bot-infected computers in the United Kingdom may indicate that the security infrastructure there is beginning to catch up to the growth of Internet connectivity. As a consequence, the United States, which has extremely high broadband penetration and growth,[79] has regained its place as the most bot-infected country.

Over the last six months of 2005, nine percent of known bot-infected computers were located in China, placing it in third position worldwide. It was also the third ranked country in the first half of 2005, with seven percent of bot-infected computers. China will likely continue to be prominent in this category, as broadband penetration and expansion rates in that country continue to grow at a rapid pace.

In addition to the overall proportion of bot-infected computers residing in each country, Symantec believes that it is also important to monitor which countries are experiencing the largest increase in these compromised systems. During the last six months of 2005, the United States experienced a 39% increase in bot-infected computers, the highest of any country. This rate of growth was 26 percentage points higher than the average increase, 13%. This rise in the number of bots in the United States is likely closely linked with broadband Internet growth there.

[79] http://www.point-topic.com/contentDownload/dslanalysis/world%20broadband%20statistics%20q3%202005.pdf (access requires registration)

China had the second largest increase of bot-infected computers during the last six months of 2005, with 37% growth, which was 24 percentage points above the average increase. China's increase in bot-infected computers is also likely related to its growth in broadband Internet connections. It is also an indicator that China is a popular target for bot network owners. The third largest increase in bot-infected computers took place in France, which had 23% growth in the second half of 2005.

Over the last six months of 2005, the United States had the highest proportion of bot command-and-control servers in the world, accounting for 48% of the total (table 7). South Korea ranked second with nine percent of the total and Canada ranked third with six percent. The global distribution of command-and-control computers does not match the distribution of bot-infected computers in general. This would seem to indicate that many bot network owners control computers in countries outside of their own.

Bot network owners may be inclined to attack computers outside of their country of residence in order to help maintain their anonymity. Doing so may make it difficult for law enforcement agencies to track them. By hopping through a number of computers in different countries attackers can ensure that it is difficult, if not impossible, to determine their geographical location. Furthermore, the likelihood of criminal prosecution for Internet-related crimes may be reduced due to differences in national and International laws and jurisdictional differences.

Attackers are also likely driven to control bot-infected computers outside of their resident country by the need to locate vulnerable targets. The United Kingdom may serve as an example of this. As discussed above and in the previous volume of the *Internet Security Threat Report,* the United Kingdom's rapidly expanding Internet infrastructure has made it difficult for its security infrastructure to keep pace. This in turn has made it a prime target for attackers attempting to expand their bot networks.

Rank July–Dec 2005	Country	Percent of bot-infected computers July–Dec 2005
1	United States	48%
2	South Korea	9%
3	Canada	6%
4	Germany	5%
5	China	4%
6	Taiwan	4%
7	Sweden	3%
8	Japan	3%
9	Argentina	2%
10	United Kingdom	2%

Table 7. Top command-and-control countries
Source: Symantec Corporation

Denial of service attacks

Denial of service (DoS) attacks are a major threat to organizations, especially those that rely on the Internet for communication and to generate revenue. The term "denial of service" refers an attempt to limit the target computer's ability to service legitimate network requests, thereby denying services the computer is supposed to provide to legitimate users.

Although there are numerous methods for carrying out DoS attacks, Symantec derives the data for this metric by measuring attacks carried out by flooding a target with SYN requests.[80] 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, causing a single attacking computer to initiate multiple connections. This results in unsolicited traffic, known as backscatter, being sent to other computers on the Internet. This backscatter is used to derive the number of DoS victims observed throughout the reporting period.

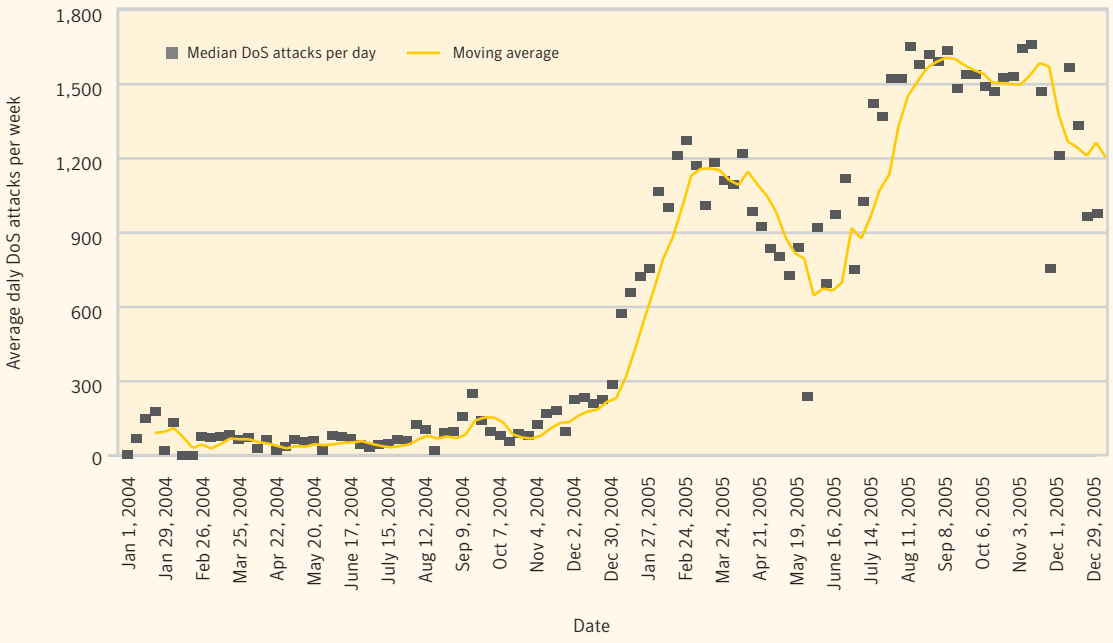

Figure 8. DoS attacks per week
Source: Symantec Corporation

[80] 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.

During last six months of 2005, Symantec detected and identified an average of 1,402 DoS attacks per day (figure 8). This is an increase of 51% over the first half of 2005 when Symantec detected an average of 927 DoS attacks per day.

The rise in DoS attacks indicates that an entrenched and well organized community of attackers—likely bot network owners—may be beginning to better utilize their resources to carry out more attacks. As was discussed in the "Top Internet attacks" section of this discussion, criminal extortion schemes based on DoS attacks are becoming more common.[81] Symantec speculates that as bot networks grow in size and coordination this form of attack will continue to increase.

Defending against DoS attacks that use forged source addresses is difficult, as spoofed addresses make filtering based on the IP address much more complicated. Some operating systems have configuration options that may be utilized to make the computers less prone to resource exhaustion; administrators should optimize this to minimize the effects of DoS attacks.

Organizations should ensure that a documented procedure exists for responding to denial of service events. One 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 will frequently need to engage their upstream ISP to help filter the traffic to mitigate the effects of attacks.

Top originating countries

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.

During the last six months of 2005, the United States was the country of origin of 31% of attacks (table 8), the most of any country. This is a slight drop from the 33% of attacks that originated there in the first half of the year and slightly more than the 30% that originated there in the second half of 2004.

[81] http://www.networkworld.com/news/2005/051605-ddos-extortion.html

Rank July–Dec 2005	Rank Jan–June 2005	Country	Percent of events July–Dec 2005	Percent of events Jan–June 2005
1	1	United States	31%	33%
2	4	China	7%	6%
3	3	United Kingdom	6%	7%
4	2	Germany	5%	7%
5	5	France	4%	5%
6	7	Canada	4%	4%
7	6	Spain	3%	5%
8	8	Japan	3%	4%
9	10	Italy	2%	3%
10	9	South Korea	2%	3%

Table 8. Top originating countries
Source: Symantec Corporation

The position of the United States as the highest source country is not surprising; it has a widespread broadband infrastructure and high Internet usage, providing more platforms from which to launch attacks. However, as other countries continue to add to their Internet infrastructure, particularly their high-speed connections, attacks originating from those countries can be expected to rise. The percentage of attacks originating in the United States can be expected to fall accordingly.

China moved up to the second position for the last six months of 2005, seven percent of the all attacks originated there. The increase of one percentage point from the first six months of 2005 corresponds to a 153% increase in the volume attacks originating in China.

The United Kingdom was the source country for the third highest number of attacks for the second straight reporting period. Attacks originating in the UK accounted for six percent of all attacks. This is a drop from the seven percent of attacks that originated there in the first six months of 2005, when it was also the third highest source country.

Germany had been the source country for seven percent of all attacks in the first half of 2005, when it was the second highest country of attack origin. However, in the second half of the year, only five percent of all attacks originated there, dropping it to fourth position.

In addition to assessing which countries were the sources of the most attacks, it is also worth discussing which of those countries experienced the largest increase in the number of attacks originating there. China experienced the largest overall increase in originating attacks by a large margin. As mentioned previously, attacks originating in China increased by 153%, which is 72 percentage points above the average increase. This increase is likely driven by the growth in Internet connectivity in China. It is also likely a sign that more attackers have become active within the country. Attacks originating in the United States increased by 88%, seven percentage points above the average growth. The United Kingdom had the third highest growth at 80%, which was one percentage point lower than the average increase.

Top targeted industries

This discussion will explore attacks that target specific industries. Although attackers choose their targets for numerous reasons, some select them to compromise computers within a specific industry or organization. For this discussion, a targeted attack is identified as an IP address that has attacked at least three sensors in a given industry to the exclusion of all other industries during the reporting period.

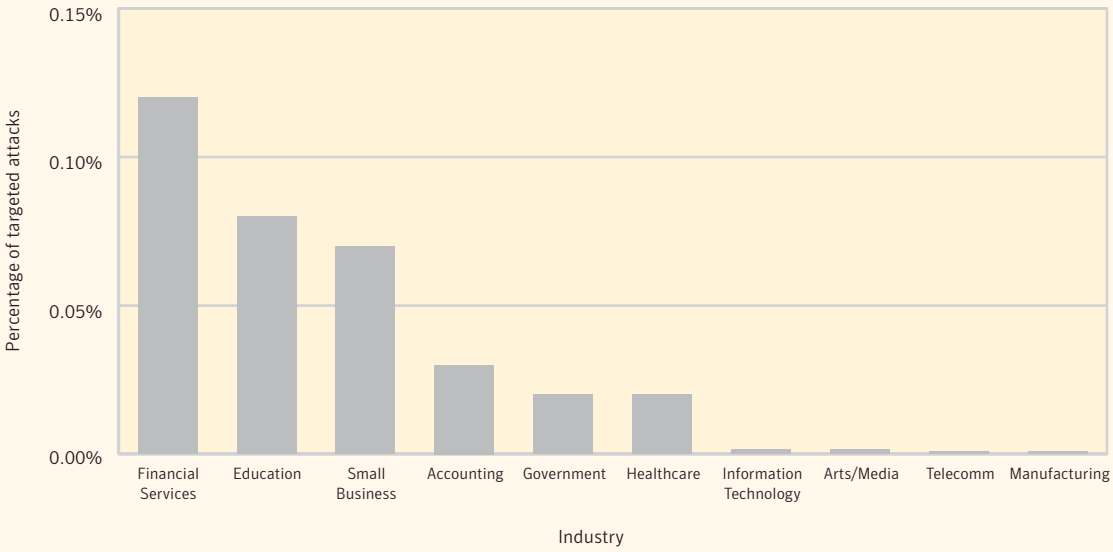

Figure 9. Top targeted industries
Source: Symantec Corporation

Financial services was the most frequently targeted industry between July 1 and December 31, 2005 (figure 9). As has been alluded to elsewhere in this report, Symantec believes that attackers may be turning their attention to cybercrime; that is, criminal activities conducted over the Internet, usually for profit. The financial services industry is typically considered a popular target for attackers hoping to profit from their attacks. The financial services sector was the third most frequent target of targeted attacks in the first half of 2005. Symantec expects that attacks targeted against the financial services industry will continue to rise as attackers become more profit driven.

Education was the second most targeted industry in the last six months of 2005. Educational institutions must provide remote access to tens of thousands of students and staff requiring a wide range of different services. Furthermore, universities often provide access to public terminals that may be abused by both students and the general public. This can make it difficult for network administrators to actively defend against threats. The volume of computers that are connected to this type of network, along with the network resources they possess, makes them very attractive targets for attackers both inside and outside of the network.

Small business was the third most targeted industry during the second half of 2005. Small businesses are less likely to have a well established security infrastructure, making them more vulnerable to attacks. It should be noted that the number of targeted attacks against small businesses might be inflated due to the way in which they access the Internet. In the two previous volumes of the *Internet Security Threat Report,* Symantec suggested that it is likely that multiple small businesses share networks that span a single block of IP addresses. As a result, opportunistic attacks targeting a broadband ISP (rather than any of the specific small businesses hosted on its network) may be noted as targeted attacks, thereby artificially inflating the percentage of targeted attacks against this industry.

Vulnerability Trends

Vulnerabilities are design or implementation errors in information systems that can result in a compromise of the confidentiality, integrity, and/or availability of information stored upon and/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 either actively, 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 of end users, security researchers, hackers, and security vendors.

Symantec carefully monitors vulnerability research, tracking vulnerabilities throughout their lifecycle, from initial disclosure and discussion of the vulnerability to the development and release of a patch or other remediation measure. Symantec operates one of the most popular forums for the disclosure and discussion of vulnerabilities on the Internet. The BugTraq mailing list has approximately 50,000 direct subscribers who receive, discuss, and contribute vulnerability research on a daily basis.[82] Symantec also maintains one of the world's most comprehensive vulnerability databases, currently consisting of more than 13,000 vulnerabilities (spanning more than a decade) affecting more than 30,000 technologies from over 4,000 vendors. The following discussion of vulnerability trends is based on a thorough analysis of that data.

This section of the Symantec *Internet Security Threat Report* will discuss vulnerabilities that have been disclosed between July 1 and December 31, 2005. It will compare them with those disclosed in the two previous six-month periods and discuss how current vulnerability trends may affect potential future Internet security activity. Where relevant, it will also offer protection and mitigation strategies. Symantec's recommendations for best security practices can be found in Appendix A at the end of this report. Readers should note that all numbers presented in this discussion have been rounded off to the nearest whole number. As a result, some cumulative percentages may exceed 100%.

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

- Total number of vulnerabilities disclosed
- Severity of vulnerabilities
- Web application vulnerabilities
- Vulnerabilities with exploit code
- Ease of exploitation
- Exploit code development time
- Patch development and availability time
- Commercial acquisition and disclosure of vulnerabilities
- Web browser vulnerabilities

It should be noted that, unlike other reports in the *Internet Security Threat Report*, the "Vulnerability Trends" report is based on data that often changes over time. This is because entries in the vulnerability database are frequently revised as new information emerges. For instance, vulnerabilities may be

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

attributed to a particular reporting period after that period has ended. Conversely, entries may be removed after a reporting period because they are deemed to have not been vulnerabilities after the period has ended. Because of this, statistics and percentages reported in one volume of the *Internet Security Threat Report* may not agree with information presented in previous and/or subsequent volumes. As a result, some of the comparative data for previous reporting periods that is presented within this report may differ from the data presented in previous volumes of the *Internet Security Threat Report*.

Total number of vulnerabilities disclosed

The second half of 2005 was marked by a slight increase in the total number of vulnerabilities disclosed. Between July 1 and December 31, 2005 Symantec documented 1,896 new vulnerabilities. This is an increase of one percent over the 1,871 vulnerabilities disclosed in the first half of the year. However, it is a more significant increase of 34% over the 1,416 vulnerabilities disclosed in the second half of 2004.

While the increase over the first half of 2005 is slight, the volume seen in the second half of the year is the highest ever recorded. Furthermore, over the past year Symantec documented the highest yearly total volume of vulnerabilities since the establishment of the vulnerability database in 1998. In 2005 Symantec documented 3,767 vulnerabilities, compared to 2,691 in 2004, an increase of 40% (figure 10). The growth in the number of vulnerabilities over the past year has been driven primarily by an increase in discovery and disclosure of vulnerabilities in Web applications.

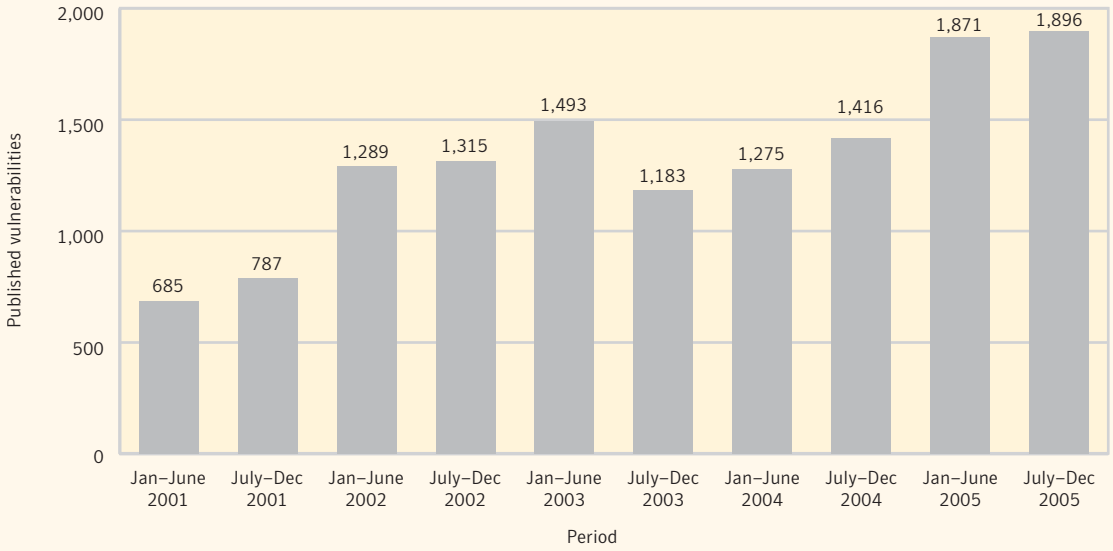

Figure 10. Total volume of vulnerabilities, 2001-2005
Source: Symantec Corporation

As will be discussed in further detail in the "Web application vulnerabilities" section below, 69% of the vulnerabilities documented by Symantec in the second half of 2005 affected Web applications. The increased focus on Web application vulnerabilities reflects the shift toward the World Wide Web as a platform for applications. Many applications that were once stand-alone software suites or client-server solutions are now being implemented as Web applications. Some well-known examples include the Outlook® Web Access email client, the phpMyAdmin database administrator, and the Webmin UNIX system administration application. This has opened the door to new classes of attacks against these new implementations.

The development of advanced research tools has contributed to the high rate of vulnerability discovery over the past year. In the previous volume of the Internet Security Threat Report,[83] Symantec stated that recent advances in technologies that analyze software code have made the discovery of vulnerabilities and the creation of associated exploit code easier than ever before. Disassembly, debugging, and virtualization have all been made easier by the increased availability of associated tools and programs. These tools allow researchers to trigger and then isolate vulnerabilities in closed-source software running in controlled environments. In the past, closed-source software—software that is distributed in a pre-compiled binary format—has been more difficult to analyze. This is because compilation obfuscates program design by reducing high-level software logic to binary machine code. However, technological advancement and research in the area of binary analysis has made auditing binary code for security flaws easier. Symantec believes that this has led to the discovery of greater numbers of vulnerabilities, many of which were previously made inaccessible to researchers by privately held source code.

Symantec recommends that administrators employ a good asset management system or vulnerability alerting service, both of which can help to quickly assess whether a new vulnerability is a viable threat or not. Enterprises should devote sufficient resources to alerting and patch deployment solutions. They should also consider engaging a managed security service provider to assist them in monitoring their networks. Administrators should also monitor vulnerability mailing lists and security Web sites for new developments in vulnerability research.

Severity of vulnerabilities

The severity of a vulnerability is a measure of the degree to which the it allows an attacker access to the targeted system. It measures the potential impact that successful exploitation may have on the confidentiality, integrity, or availability of data stored upon or transmitted over the affected system. For the purposes of the *Internet Security Threat Report*, each vulnerability is categorized in one of three severity levels. These levels are:

Low severity—Vulnerabilities that constitute a minor threat, such as those for which successful exploitation does not result in a complete compromise of the information stored on or transmitted across the system.

Moderate severity—Vulnerabilities that could result in a partial compromise of the affected system, such as those by which an attacker gains elevated privileges but does not gain complete control of the target system.

[83] Symantec *Internet Security Threat Report*, Volume VIII (September 2005), p. 88

High severity—Vulnerabilities that, if exploited successfully, could result in a compromise of the entire system. In almost all cases, successful exploitation can result in a complete loss of confidentiality, integrity, and availability of data stored on or transmitted across the system.

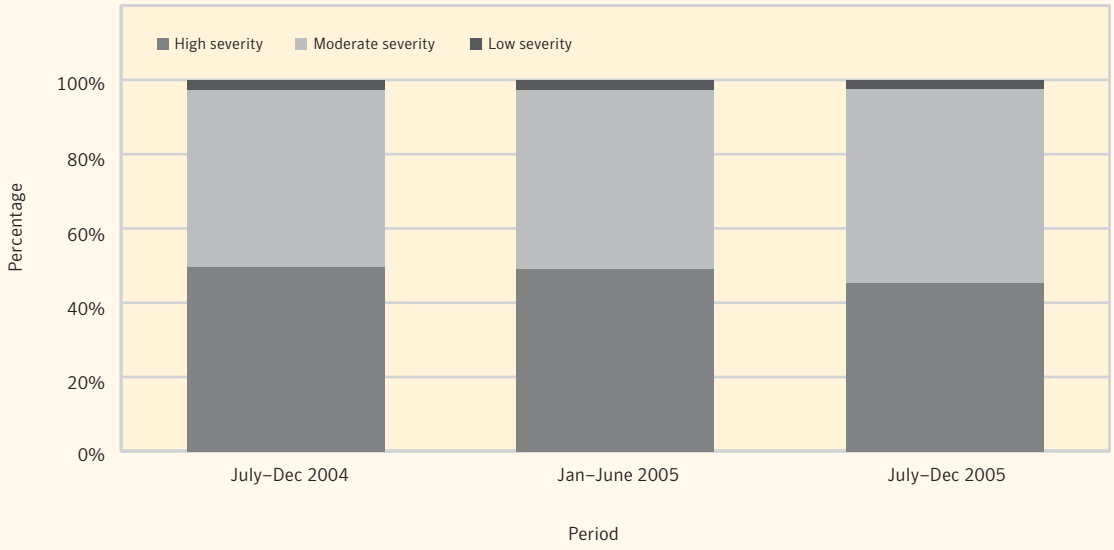

Figure 11. Volume by severity
Source: Symantec Corporation

Over the past four six-month reporting periods Symantec has rated the vast majority of vulnerabilities as either moderate or high severity, with only a small percentage rated low severity.[84] This pattern continued over the current reporting period. During the final six months of 2005, most of the vulnerabilities that Symantec documented were either moderately or highly severe. There were very few low-severity vulnerabilities reported.

Between July and December 2005, Symantec rated 45 % of reported vulnerabilities as high severity (figure 11). This is a decrease of eight percent from the 49% that were rated high severity in the first half of the year. It is also ten percent lower than the second half of 2004 when 50% of vulnerabilities were rated high severity.

During the current reporting period, 52% of vulnerabilities were rated moderately severe. This is eight percent higher than the 48% seen in the first six months of the year. Forty-seven percent of vulnerabilities published in the last six months of 2004 were rated moderately severe. This increase in moderately severe vulnerabilities has occurred at the expense of the high-severity vulnerabilities. Symantec believes that this is due to an increase in Web application vulnerabilities, the majority of which are classified as moderately severe.

[84] In the previous volume of the Symantec *Internet Security Threat Report*, the severity metric was adjusted to remove the bias of remote exploitability. This was done because remotely exploitable vulnerabilities are always rated at least moderately severe. Assessing the severity of vulnerabilities with the criteria of remote exploitability removed presented a different severity composition. The result was that a majority of vulnerabilities were rated moderately severe at the expense of the number of high-severity vulnerabilities. This was true for all periods.

Over the past six months, three percent of all vulnerabilities were classified as low severity. This is consistent with the numbers seen in the two previous reporting periods. In each of those periods, three percent of all vulnerabilities were low severity.

Symantec believes that there are several reasons for the greater number of moderately to highly severe vulnerabilities. First, these vulnerabilities provide researchers with the most reward in terms of the level of potential compromise and peer recognition in the researcher community. It is further likely that a significant number of low-severity vulnerabilities are discovered and not reported because there is little value or attention placed on them.

A second factor may be the use of remote exploitability as a criterion in the Symantec severity rating system. If a vulnerability is remotely exploitable, it will be considered at least moderately severe. Low-severity vulnerabilities, by definition, are "those that attackers cannot exploit across a network." The high prevalence of network connectivity means that most vulnerabilities will be accessed by attackers remotely across a network, so that locally exploitable vulnerabilities—that is, low severity vulnerabilities—are either less common or less commonly reported.

A final factor contributing to this trend is the commercialization of vulnerability information, which will be discussed at greater length later in this section. With the apparent increase in the commercialization of vulnerability research, there appears to be increased financial incentives for researchers to find more severe vulnerabilities.

Web application vulnerabilities

Web applications are technologies that rely on a browser for their user interface, rely on HTTP as the transport protocol, and reside on Web servers. Examples of Web applications include message forums, e-commerce suites (such as "shopping cart" implementations), Web logs, and Web-based email. An increasing number of traditional software vendors are implementing their existing applications with Web-based user interfaces.

Many application service providers deliver their applications to their users exclusively over the Web. Furthermore, many organizations use custom Web applications to provide various internal and external services. For example, intranets are often a combination of commercially developed applications, such as PeopleSoft, and internally developed custom tools.

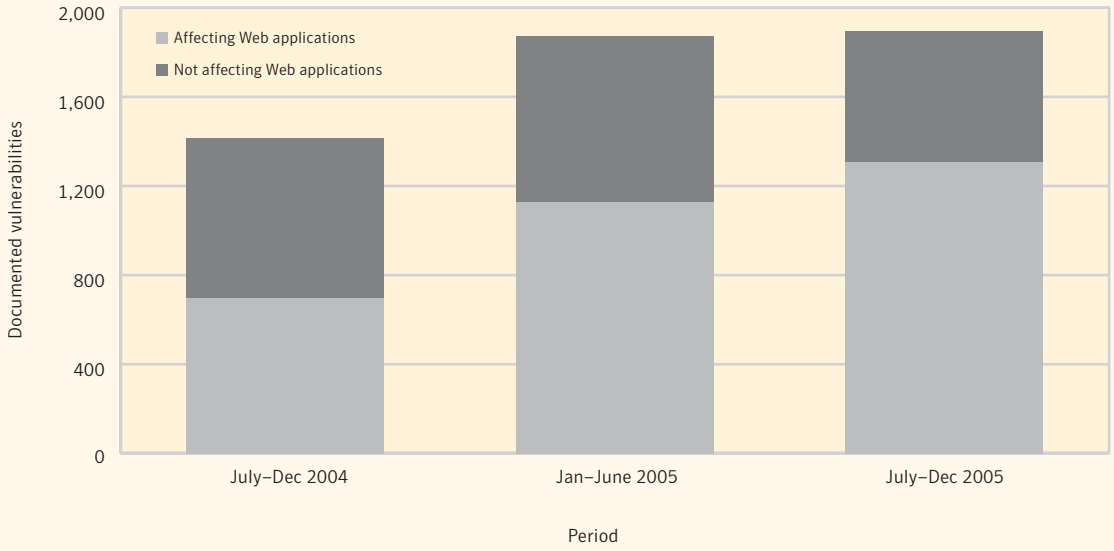

Figure 12. Web application vulnerabilities
Source: Symantec Corporation

Over the past several reporting periods Web application vulnerabilities have increased significantly, a trend that continued over the last six months of 2005. Between July and December 2005, 69% of vulnerabilities were associated with Web applications (figure 12). This is a 15% increase over the first half of 2005 when they made up 60% of all vulnerabilities. In the second half of 2004 they accounted for 49% of all vulnerabilities.

Symantec believes that the rise of Web application vulnerabilities may be due to the ease with which they can be introduced into source code. Furthermore, many small Web applications are developed on an *ad hoc* basis. Advances in Web-based development methods such as AJAX[85] provide a rich set of application capabilities, allowing more people to develop such programs in a shorter period of time. As a result, Web-application developers may not be adequately trained to incorporate security into the programs they develop. Furthermore, the programs may not be sufficiently audited for potential security issues prior to implementation.

As the number of vulnerabilities associated with Web applications grows, Symantec fears that they may serve as an increasingly attractive target for potential attackers to exploit. So far, three instances of malicious code or self-propagating code have been detected that propagate by exploiting vulnerabilities in Web-based applications or services. The first known Web-application worm was Perl.Santy,[86] which affected the widely deployed phpBB forum. The next was a segment of JavaScript code that quickly propagated through Web sites of MySpace users by taking advantage of a vulnerability in the social networking Web site.[87] Most recently, an example of propagating code was reported that exploited a vulnerability in the Mambo content management system.[88] Symantec believes that these are the first examples of what may soon become commonplace: malicious code that spreads through vulnerabilities in Web applications.

[85] "Asynchronous Javascript + XML" - http://www.adaptivepath.com/publications/essays/archives/000385.php
[86] http://securityresponse.symantec.com/avcenter/venc/data/perl.santy.html
[87] http://www.betanews.com/article/CrossSite_Scripting_Worm_Hits_MySpace/112932391
[88] http://www.uniras.gov.uk/niscc/docs/br-20051206-01073.html?lang=en

Adding to the importance of Web applications is the fact that the Web is a ubiquitous medium for the delivery of products and services. This makes understanding and securing against Web-based attacks an important security objective.

Web application vulnerabilities are a particular security concern because they are typically exposed to the Internet through Web servers, which are often the external face of an organization on the Internet. Because traditional security solutions such as intrusion detection systems and firewalls allow Web traffic onto a network by default, Web-based attacks can leave organizations that host Web applications exposed to attacks that are difficult to detect and prevent.

Traditional client-server applications were easy to filter because of their association with specific port numbers. However, with Web applications, data associated with multiple applications can be transmitted through the same ports, making it more difficult to apply appropriate access controls on a per-application basis. Furthermore, it is often difficult to detect attacks reliably in network intrusion detection systems because of the complexity permitted in Web traffic.[89]

Another source of concern is the way in which vulnerable Web applications can be patched. Organizations that rely on the application must wait for the maintainers of the application to apply patches according to their own development and patching schedules. The development and implementation of patches could take a considerably long time, during which organizations deploying the affected application could be vulnerable to compromise.

Finally, the high volume of new vulnerabilities affecting seldom-used technologies could potentially prevent administrators from attending to more serious concerns. Organizations should manage their Web-based assets carefully. If they are developing Web applications in-house, developers should be educated about secure development practices. 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 Web applications.[90]

Symantec recommends that administrators employ a good asset management system to better track which assets are deployed on the network. They should also consider employing a vulnerability alerting service that will notify them of new vulnerabilities and help to quickly assess whether a new vulnerability is a viable threat to the organization or not. Finally, system administrators should also monitor vulnerability mailing lists and security Web sites for relevant new developments.

[89] Web requests and content can be encoded, encrypted (SSL), or otherwise obfuscated rather easily, making reliable detection of attacks in network traffic often infeasible. HTTP proxies may aid against some attacks, though they lack understanding of the application logic.
[90] http://www.owasp.org

Vulnerabilities with exploit code

Exploit code is custom-designed programming code that allows attackers to exploit a specific vulnerability. Also known as an exploit, it is sometimes included with the original advisory that describes the vulnerability. In some cases, the exploit code is written well, so that it reliably exploits the vulnerability in such a way as to maximize its potential to compromise the target. In other cases, it may be developed by the author as proof-of-concept exploit code, which works in some instances but is not robust or well tested. When exploit code is released to the public it is typically made available on security mailing lists and Web sites or on hacker Web sites. If exploit code is available, the vulnerability with which it is associated will be considered easy to exploit.

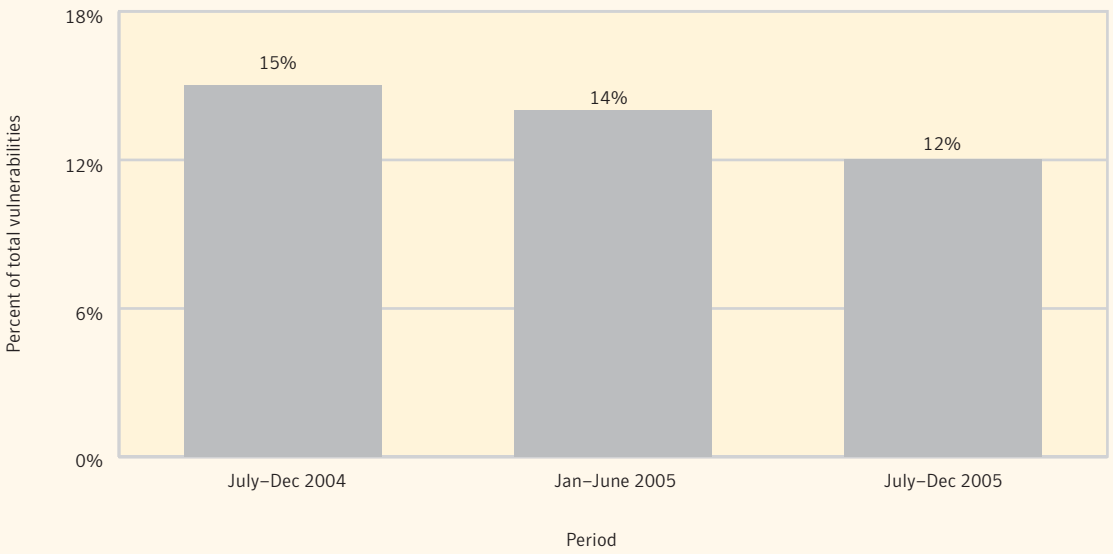

Figure 13. Vulnerabilities with associated exploit code
Source: Symantec Corporation

The proportion of vulnerabilities with exploit code continued to decline in the second half of 2005 (figure 13). Between July and December 2005, exploit code was available for 12% of the vulnerabilities disclosed. This is lower than the 14% proportion seen in the first half of the year. During the same reporting period one year ago, exploit code was available for 15% of all vulnerabilities. The decrease in vulnerabilities with associated exploit code is due to the proportional increase in vulnerabilities that do not require exploit code. These are primarily input validation vulnerabilities affecting Web applications, such as cross-site scripting attacks.[91]

Symantec believes that the decrease may also be related to the commercialization of vulnerabilities and exploit code. There are now several organizations that will buy unpublished vulnerabilities from individuals or groups who discover them.[92] There is no public disclosure of the vulnerability details at the time that the

[91] http://www.cert.org/advisories/CA-2000-02.html
[92] http://www.redherring.com/article.aspx?a=14475
http://www.techworld.com/security/features/index.cfm?fuseaction=displayfeatures&featureid=2125&page=1&pagepos=0

information is transferred from discoverer to purchaser. Once the rights to the vulnerability details, which can often include proof-of-concept code or exploit code, have been transferred, the details can remain in limbo until the vulnerability is reported to the vendor and fixed, leaked, or independently rediscovered and reported publicly.

Vulnerabilities that require exploit code tend to be more severe in nature than those that don't. As a result, the decline in vulnerabilities with exploit code may be attributed to an increasing reluctance by exploit developers to publicize their exploit code, as these exploits have more inherent value. The commercialization of vulnerabilities will be discussed at greater length below.

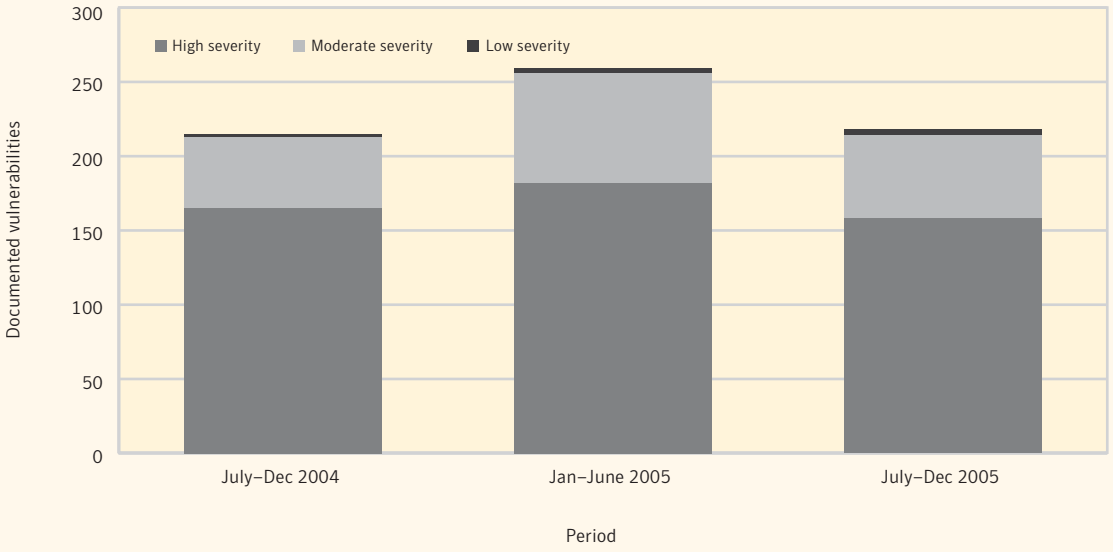

Figure 14. Vulnerabilities with exploit code, by severity
Source: Symantec Corporation

Figure 14 depicts the breakdown of severity of vulnerabilities for which exploit code was available. The basic composition has remained largely consistent over the past three reporting periods. During the last six months of 2005, 72% of vulnerabilities for which there was associated exploit code were rated high severity. This is very similar to the previous period, 70%, and the last six months of 2004, 77%.

Twenty six percent of vulnerabilities with exploit code published in the second half of 2005 were rated moderately severe. This is also quite similar to proportions seen in the past: 29% in the first half of 2005 and 22% in the second half of 2004.

Symantec believes that exploit code writers are focusing their efforts on high-severity vulnerabilities, which are often sufficiently complex to require the use of exploit code. Creating exploit code can require a substantial amount of time and effort. Researchers do not want to spend their limited resources on tools for attacks that do not result in significant impact on the target system.

Ease of Exploitation

Symantec rates each vulnerability according to how difficult it is for an attacker to exploit it to compromise a targeted system. This "ease of exploit" rating assumes that the attacker possesses a general knowledge of vulnerabilities and how to leverage them, with or without exploit code, depending on the vulnerability. Symantec rates each vulnerability as either "easily exploitable," if it requires no exploit or if a required exploit is known to be available, or as "no exploit available," if exploit code is required but is not yet available to the public.

Generally speaking, easily exploitable vulnerabilities do not require sophisticated skills or knowledge for successful exploitation. Anyone with sufficient general technical knowledge or with publicly available exploit code can exploit them. Examples of these are Web server vulnerabilities that can be exploited by simply entering an appropriate URL into a Web browser.[93]

On the other hand, vulnerabilities that are classified as "no exploit available" are more difficult to attack. This is because attackers cannot exploit them using basic knowledge alone and because no known tools to exploit them have been written or made publicly available. To exploit these vulnerabilities, an attacker would be required to write custom exploit code. This significantly raises the level of knowledge, expertise, and effort required for a successful attack, thereby increasing the difficulty and lowering the probability of such an attack. It should be pointed out that while no tools may be publicly available, private exploit code might exist.

In the second half of 2005, 79% of disclosed vulnerabilities were classified as "easy to exploit" (figure 15). This is an increase of eight percent over the first half of the year when 73% of vulnerabilities were considered easy to exploit. In the second half of 2004, 71% of vulnerabilities were easily exploitable. The increase in the current period is primarily due to the increase in vulnerabilities for which no exploit is required. This is almost certainly related to the increase in Web application vulnerabilities, many of which are rated "no exploit required."

[93] For example, the Extensis Portfolio Netpublish Server Server.NP Directory Traversal Vulnerability (http://www.securityfocus.com/bid/15974), a directory traversal vulnerability where a user could specify as a filename a path relative to the script's working directory and obtain unauthorized access to arbitrary files on the Web server file system.

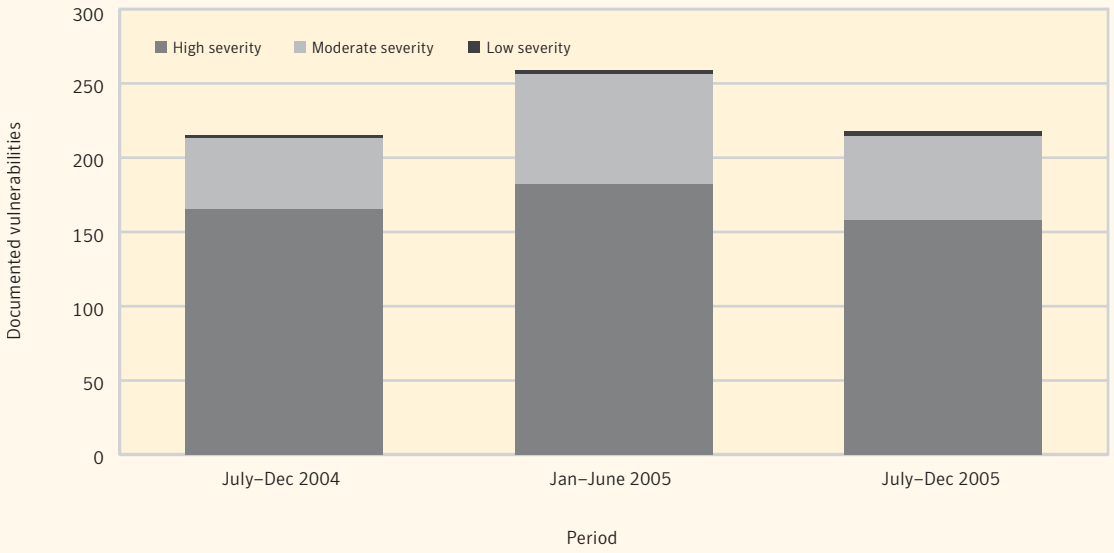

Figure 15. Volume by ease of exploit
Source: Symantec Corporation

In the second half of 2005, 73% of vulnerabilities did not require exploit code. This is 18% higher than the number for the previous six-month period, 62%. In the second half of 2004, 54% percent of vulnerabilities required no exploit code. This increase corresponds with the rise in Web application vulnerabilities, the majority of which can be exploited by a moderately skilled attacker without specific exploit tools. This may be significant because with the rise in easy-to-exploit Web application vulnerabilities, exploitation is open to attackers who previously would have been unable to successfully exploit such vulnerabilities. This could create the potential for a significantly larger pool of attackers.

Exploit code development time

Symantec records the window of time between the publication of an initial vulnerability report and the appearance of third-party exploit code. The intent is to determine how long it takes an individual or group who is not the discoverer of the vulnerability to develop functional exploit code for certain classes of vulnerabilities. The shorter the time between disclosure of a vulnerability and the release of an associated exploit, the more affected computers are vulnerable to attack (until patches become available and are applied). When juxtaposed with the average patch development time, which will be discussed in the next section, this metric is useful in determining a window of exposure to exploitation.

During the second half of 2005, the average time for exploit development was 6.8 days (figure 16). This is an increase of almost a full day over the average time of 6.0 days in the first half of 2005. In the second half of 2004, the average time between the disclosure of a vulnerability and the release of an associated exploit was 6.4 days.

One explanation for the increase observed over the past six months is that the best exploit developers have stopped making their findings and creations public because of the commercialization of exploit code. Instead, they may be opting to sell their work to organizations that are willing to pay for vulnerability research. As a result, publicly known exploit code is likely being produced by less experienced exploit developers, leading to an increase in the average exploit development time. The increase in exploit development time does not appear to signal a trend; however, Symantec will continue to monitor future developments.

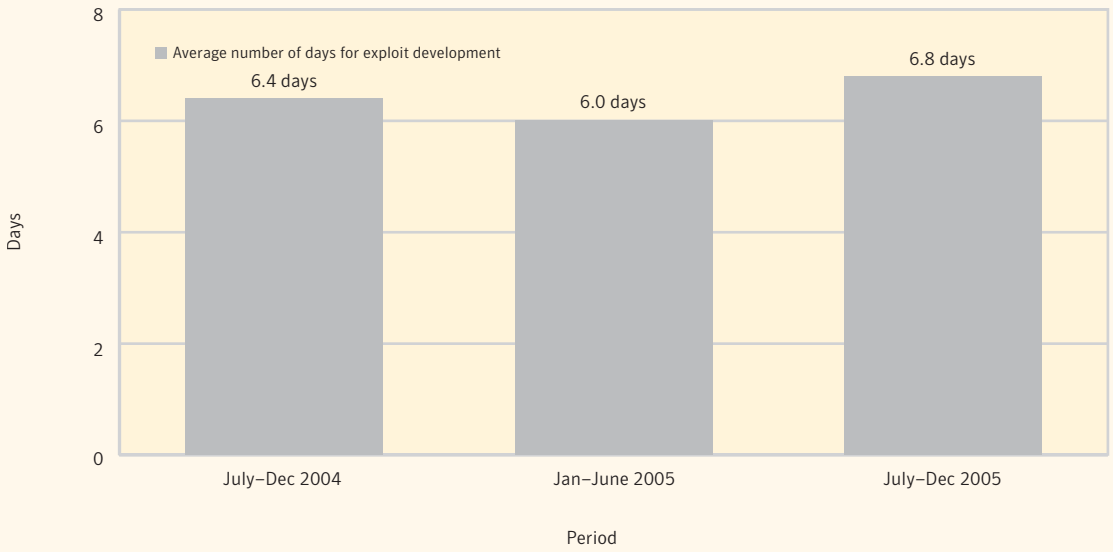

Figure 16. Exploit code development time
Source: Symantec Corporation

The relatively short exploit development time highlights the need for administrators to patch their systems or implement other protective measures as soon as possible. This may be particularly difficult for large organizations, for which applying enterprise-wide patching in a matter of days is very challenging. With the time between vulnerability disclosure and exploit development so short, administrators would benefit from notification of new vulnerabilities and the provision of relevant mitigation or patching information, as well as an understanding of the potential risk of the vulnerabilities.

Patch development and availability time

The time period between the disclosure date of a vulnerability and the release date of an associated patch is known as the "time to patch." If exploit code is created and made public during this time, computers may be immediately vulnerable to widespread attack. An assessment of patch development times was introduced in the previous volume of the Symantec *Internet Security Threat Report*.

This metric only considers specific file-based patches or upgrades, not general solutions. Instances in which the vendor provides a workaround or manual fix steps, for example, are not included. As only vulnerabilities with vendor-issued patches are taken into account, all vulnerabilities considered for this metric are vendor confirmed. It is important to note that the set of vulnerabilities included in this metric is limited: it does not encompass all software from all possible vendors, only software from vendors that are classified as enterprise vendors.

During the second half of 2005, 49 days elapsed on average between the publication of a vulnerability and the release of an associated patch. This is down sharply from the 64 days seen in the first half of the year. In the second half of 2004 the average time was 40 days.

While the time to patch has decreased since the last reporting period, the window of exposure remains considerable. If the average time to exploit development—6.8 days in the last six months of 2005—is taken into account, the window of exposure was 42 days on average. This leaves a large window of opportunity for potential attackers. Until a patch is released, end users and administrators are forced to implement security "workarounds" without an official fix. During this time networks could be vulnerable to compromise.

To minimize the possibility of successful exploitation, administrators need to understand the vulnerabilities and be active in working around them. This may involve making changes to firewall configurations, creating or obtaining IDS/IPS signatures and rules, and locking down services. Administrators should also monitor vulnerability mailing lists and security Web sites for new developments in vulnerability research. They should also monitor mailing lists devoted to the discussion of security incidents or specific technologies, on which prevention and mitigation strategies may be discussed.

Commercial acquisition and disclosure of vulnerabilities

Over the last few years, a number of companies have formed to fill a demand for the commercial acquisition of vulnerability and exploit code information from independent security researchers. This has resulted in the establishment of an *ad hoc* marketplace wherein security researchers may approach companies with their vulnerability and exploit code discoveries and attempt to sell them for financial gain. The emergence of such a market may indicate a shift in the motivation of some security researchers. While many researchers are still motivated by intellectual curiosity, a concern for security issues, or recognition from peers in the security community, more independent security researchers appear to be motivated by the opportunity to sell their research for profit.

For the first time, in this volume of the *Internet Security Threat Report,* Symantec has begun tracking the number of vulnerabilities that are researched and disclosed for commercial profit. This discussion covers those vulnerabilities that were independently researched and then acquired by a third-party commercial entity other than the vendor that is affected by the vulnerability. The information on which this discussion is based was gathered from publicly disclosed vulnerability reports that have been released by the aforementioned commercial entities. This data has been collected by correlating vulnerabilities that were disclosed by companies that engage in this practice and then selecting those vulnerabilities that are known to have been sold to the companies by an independent party.

Commercial entities that engage in the purchase of vulnerabilities and exploits often do so to drive their own business. There are a number of benefits to acquiring vulnerability information before it is made public. First, the information may be redistributed at a price to customers of the entity. Second, it may be incorporated into security products that are maintained by the entity in order to gain an advantage over its competitors. For instance, IDS vendors may use commercially acquired vulnerability information to develop IDS signatures to protect against zero-day exploits.

Total number of commercially acquired vulnerabilities

The first public marketplace for the acquisition of vulnerability and exploit code information was founded in 2002. To establish the history of this marketplace, a sampling of data covering this reporting period and the previous four *Internet Security Threat Report* reporting periods has been included.

Over the last few reporting periods, the number of vulnerabilities that have been commercially disclosed and acquired has increased (figure 17). However, this trend appears to have been reversed over the last six months of 2005. During this period there were 54 commercial vulnerabilities, a decline of 21% from the 68 commercial vulnerabilities in the first half of 2005.

The total number of commercial vulnerabilities has increased steadily on a yearly basis. However, during the current reporting period, two new commercial vulnerability acquisition programs were started. The decline in this period could be attributed to the diversification of the marketplace. Security researchers now have two more options when deciding where to sell their vulnerabilities and exploit code, and their ability to shop around may have affected the rate at which these vulnerabilities have been disclosed.

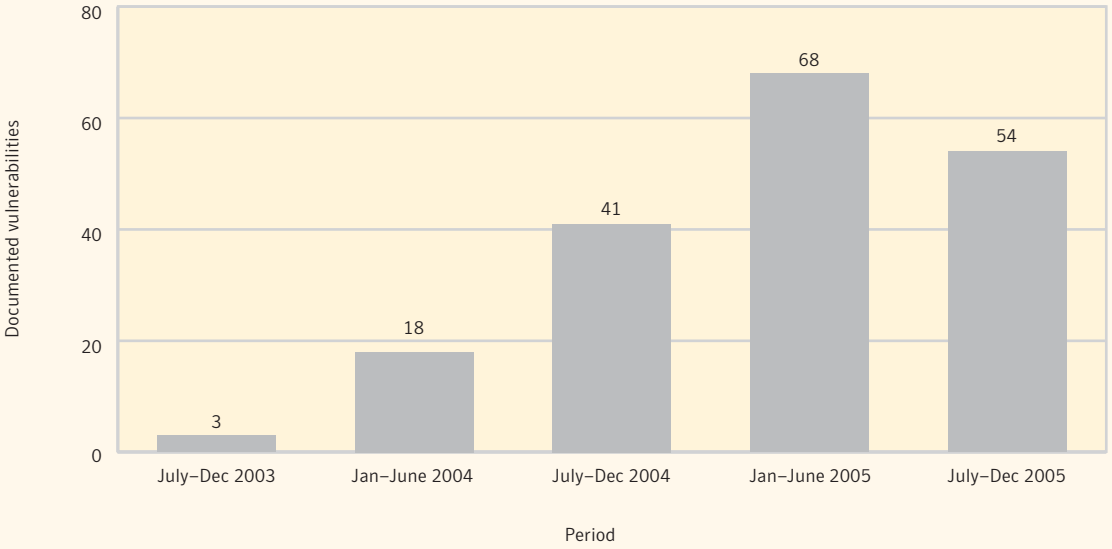

Figure 17. Total number of commercially acquired vulnerabilities
Source: Symantec Corporation

Commercial vulnerabilities—average severity rating

Symantec rates vulnerabilities on a numerical scale based on a number of criteria in order to determine the severity of the vulnerability. Vulnerabilities that are given a numerical rating of seven or higher are considered high severity.[94] An assessment of the average severity rating of commercial vulnerabilities over the past five reporting periods demonstrates that only certain types of vulnerabilities are being purchased by commercial entities.

Over the past five reporting periods, the average commercial vulnerability has been given a high severity rating (figure 18). In the second half of 2005, the average commercial vulnerability was rated 7.9. This is higher than the first half of 2005, when the average was 7.7, and the second half of 2004, when it was 7.8. These averages indicate that the average commercial vulnerability is rated high severity. That is, the average commercial vulnerability is remotely exploitable, poses a high level of privilege compromise, and is relatively easy to exploit. Furthermore, it is likely that the vulnerability affects a widely deployed technology.

[94] For a more in-depth explanation of the Symantec vulnerability severity ratings, please see Appendix C of this report.

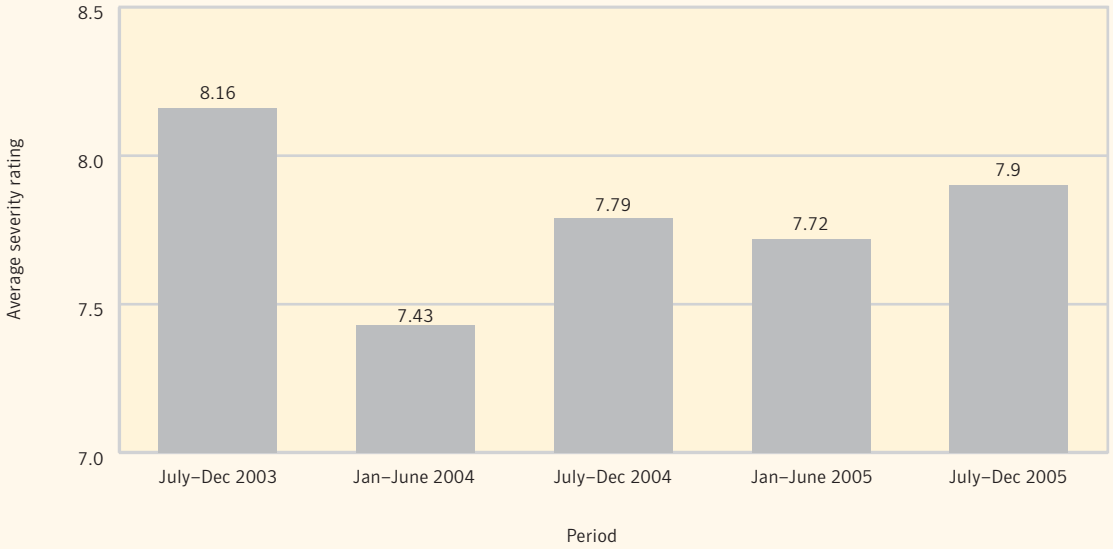

Figure 18. Average security rating, commercially acquired vulnerabilities
Source: Symantec Corporation

Commercial vulnerabilities continue to account for a notable percentage of the total number of high-severity vulnerabilities (figure 19), although the number has declined over the past three reporting periods. In the second half of 2005, commercial vulnerabilities made up four percent of all high-severity vulnerabilities. This is down from five percent in the first half of the year and six percent in the second half of 2004.

This decline means that slightly more high-severity vulnerabilities were reported by sources other than commercial vulnerability vendors, including other vendors and independent researchers, in the last six months of 2005. This could indicate that commercial vulnerability vendors are not providing sufficient enticement to bring in a larger proportion of high-severity vulnerabilities. On the other hand, it could indicate that the vendors and/or researchers are taking longer to publicize the vulnerabilities. However, there is no conclusive publicly available information to make a strong case for this assertion at this point in time.

Another factor in the reduced proportion of high-severity commercial vulnerabilities may be the existence of a black market economy for the sale of vulnerabilities. As independent researchers look for alternative marketplaces for their vulnerabilities, some are sure to resort to selling their vulnerabilities through these black market venues. Sellers and buyers in such black market economies do not stand to benefit from public disclosure of these vulnerabilities; therefore, it is in their best interest to keep this information private for as long as possible. This has likely limited the number high-severity commercial vulnerabilities that have been disclosed publicly.

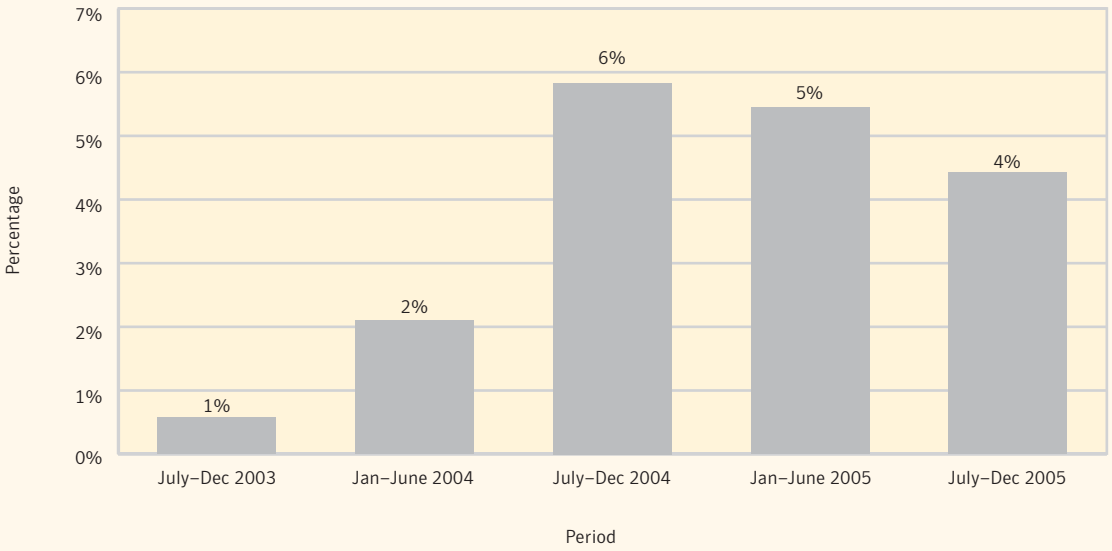

Figure 19. Percentage, high-severity vulnerabilities
Source: Symantec Corporation

The increasing market for commercial vulnerability information poses a potential risk to organizations because information regarding publicly undisclosed vulnerabilities and exploit code may be leaked before they are addressed by the vendor. To address this, Symantec recommends that organizations deploy defense in-depth, including the deployment of intrusion prevention systems and other end-point security solutions. These technologies can harden computers against unknown security threats through host-based behavior blocking and memory corruption protection schemes.

Web browser vulnerabilities

The Web browser is a critical and ubiquitous application that has, in the past few years, become a frequent target for vulnerability researchers. Traditionally, the focus of security researchers has been on the perimeter: servers, firewalls, and other assets with external exposure. However, a notable shift has occurred, as researchers are increasingly targeting client-side systems, particularly desktop computers.

As part of this shift toward client-side issues, vulnerabilities in Web browsers have become increasingly prominent. This metric will offer a comparison of vulnerability data for numerous browsers, namely Microsoft Internet Explorer, Mozilla Firefox, Opera, Safari and KDE Konqueror. The following important caveats should be kept in mind before making any conclusions based on the data:

- This discussion will incorporate two metrics: vendor-confirmed vulnerabilities, and non-vendor-confirmed vulnerabilities.

- Web browser vulnerability counts may not match one-to-one with security bulletins or patches issued by vendors. This is because of the difficult in identifying individual vulnerabilities in often complex browser exploits.
- Not every vulnerability discovered is exploited. As of this writing, there has been no widespread exploitation of any browser except Microsoft Internet Explorer. This is something that Symantec expects to change as alternative browsers become increasingly popular.
- Whereas previous volumes of the *Internet Security Threat Report* have assessed vulnerabilities in all Mozilla browsers, this volume will discuss only the Firefox browser. Firefox is the most popular of the Mozilla browsers (which include the Mozilla browser and Camino) and has become the most widely deployed of the group. The browsers, however, all share the same code base, and, frequently, the same vulnerabilities.

Web browser vulnerabilities—Vendor confirmed and non-vendor confirmed

This section will discuss the total number of Web browser vulnerabilities disclosed over the past six months, including both vendor-confirmed and non-vendor-confirmed vulnerabilities. It will also discuss the average severity rating for these vulnerabilities. As was explained in the "Commercial vulnerabilities" section above, Symantec rates vulnerabilities on a numerical scale based on a number of criteria in order to determine the severity of the vulnerability. Vulnerabilities that are given a numerical rating of seven or higher are considered high severity.[95]

Between July and December 2005, Symantec documented 24 new vulnerabilities that affected at least one version of Microsoft Internet Explorer (figure 20). This is the same number as was seen in the previous six-month period. The totals seen in both periods are still substantially less than the 45 new vulnerabilities seen in the second half of 2004.

The average severity rating for Internet Explorer vulnerabilities was 7.1 during the second half of 2005, up from 7.0 in the first half of the year. According to Symantec's severity rating system, this means that the average Internet Explorer vulnerability was rated high severity.

Of more recent concern are vulnerabilities in the Windows subsystem that may be exposed through Microsoft Internet Explorer. The Windows Metafile Remote Code Execution Vulnerability was a recent high-profile example of this.[96] While this was not an Internet Explorer vulnerability *per se,* it could be exploited automatically through the browser because of Internet Explorer's integration with the operating system. It should be noted that other browsers also present an attack vector to the vulnerability; however, successful exploitation requires additional user intervention because those browsers are not integrated in the operating system.

[95] For a more in-depth explanation of the Symantec vulnerability severity ratings, please see Appendix C of this report.
[96] http://www.securityfocus.com/bid/16074

The increasingly popular Firefox browser from Mozilla was affected by 17 new vulnerabilities in the second half of 2005. This is a decrease of 15 vulnerabilities from the 32 that were disclosed in the first half of 2005. In the second half of 2004, Symantec documented 29 vulnerabilities disclosed for Firefox.

The average severity rating for Firefox vulnerabilities was 7.20 in the second half of 2005, up from 7.14 in the first half of the year. According to Symantec's severity rating system, this means that the average Firefox vulnerability was rated high severity.

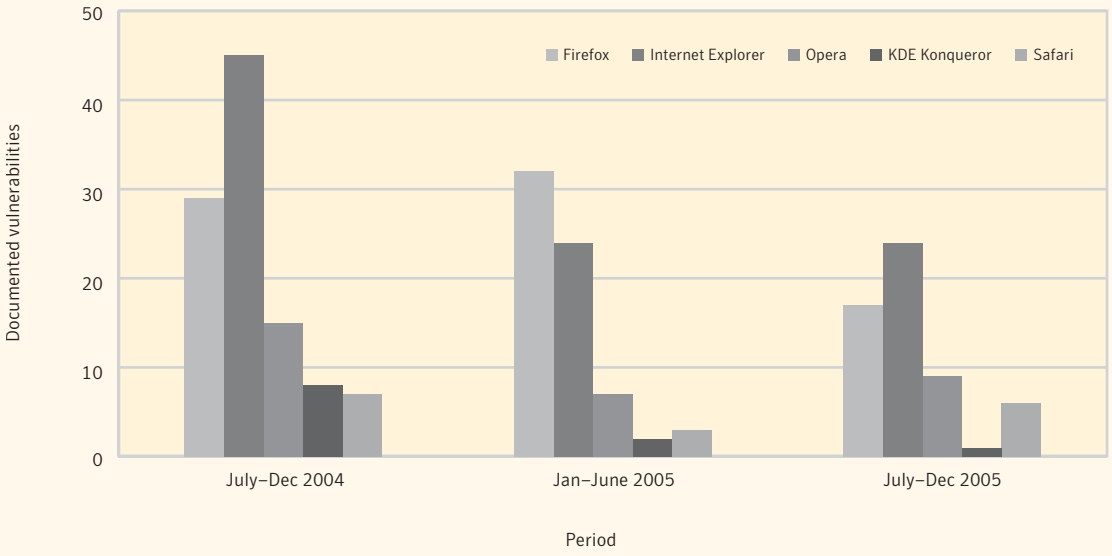

Figure 20. Web Browser vulnerabilities, including vendor confirmed and non-vendor confirmed
Source: Symantec Corporation

Between July and December 2005, Symantec documented nine vulnerabilities in the Opera Web browser, a slight increase over the seven that were disclosed in the first half of the year. Fifteen vulnerabilities were disclosed between July and December 2004. The average severity rating for Opera vulnerabilities in the first half of 2005 was 6.86. In the second half of 2005, the average severity rating was 6.48. This means that, according to Symantec's vulnerability severity rating system, Opera vulnerabilities in 2005 were rated as moderately severe.[97]

During the second half of 2005, there was a single vulnerability associated with the KDE Konqueror browser. This is down from the previous six-month period when two vulnerabilities for this browser were announced. In the second half of 2004, eight Konqueror vulnerabilities were disclosed.

In the second half of 2005, the average Konqueror had a severity rating of 5.30, which is moderately severe. In the first half of 2005, Konqueror vulnerabilities had an average severity rating of 7.25, which would indicate an average rating of high severity.

[97] When taking these numbers into consideration, it should be noted some browsers such as Opera, KDE Konqueror, and Safari may not have a large sampling of vulnerabilities to draw upon. Therefore, the average severity rating may not be a conclusive measure of the typical vulnerability found in these browsers.

Apple's Safari™ was affected by six vulnerabilities between July and December 2005. Symantec documented three Safari vulnerabilities in the first half of the year. This is down from the second half of 2004, when seven vulnerabilities were disclosed for Safari. In the second half of 2005, Safari vulnerabilities scored average severity ratings of 7.73, up from 7.03 in the first half of the year. According to Symantec's severity rating system, this means that the average Safari vulnerability was rated high severity for both reporting periods of 2005.

The vulnerabilities disclosed during the last six months of 2005 appear to indicate a return to a trend seen in earlier reporting periods during which researchers and attackers focused much of their attention on Internet Explorer. Symantec believes that the Microsoft browser will remain a popular target because of its widespread deployment. Researcher interest in Mozilla Firefox remained high during this reporting period. As this and other alternative browsers gain in popularity, it is reasonable to assume that they will also attract greater interest from vulnerability researchers and attackers.

Taking into account both vendor-confirmed and non-vendor-confirmed vulnerabilities, browser vulnerability counts were lower in the second half of 2005 than in previous periods. This may be due to increased awareness of issues related to browser security.

Web browser vulnerabilities—Vendor confirmed

The number of vendor-confirmed Web browser vulnerabilities disclosed during the second half of 2005 is considerably less than the total number of vendor-confirmed and non-confirmed vulnerabilities. Whereas Microsoft Internet Explorer had the highest number of total vulnerabilities over the past six months, the Firefox browser from Mozilla had the highest number of vendor-confirmed vulnerabilities during the same time period (figure 21). Between July and December 2005, 13 out of the 17 vulnerabilities disclosed for Firefox were vendor confirmed. This is down from 27 out of 32 in the first half of 2005 and 26 out of 29 in the second half of 2004.

When taking only the vendor-confirmed browser vulnerabilities into consideration, Firefox has had the highest vulnerability count for the last three reporting periods. This may be indicative of the transparency that is inherent in the open-source development process. Due to the nature of the open-source development process, Firefox developers may be able to acknowledge and address vulnerabilities more quickly than developers of closed-source browsers.

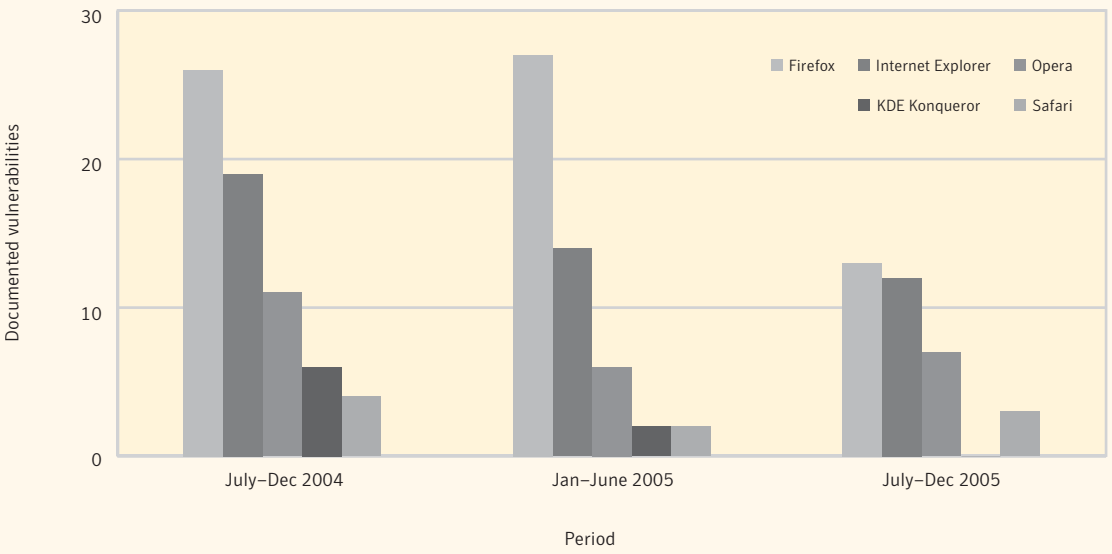

Figure 21. Web browser vulnerabilities, vendor confirmed
Source: Symantec Corporation

During this reporting period, 12 out of the 24 vulnerabilities associated with Microsoft Internet Explorer were confirmed by the vendor. This is a slight decrease from the 14 out of 24 disclosed in the first half of 2005 and the 19 vendor-confirmed vulnerabilities out of 45 in the second half of 2004.

In the second half of 2005, there were seven vendor-confirmed Opera vulnerabilities out of a total of nine disclosed vulnerabilities. This is one more than was seen in the previous period, when six new vendor-confirmed vulnerabilities out of a total of seven were published. In the second half of 2004, 11 new Opera vulnerabilities were confirmed by the vendor out of the 15 that were published.

Between July and December 2005, no vendor-confirmed vulnerabilities were disclosed for the Konqueror browser from KDE. The one vulnerability published in this period was not vendor confirmed. The two vulnerabilities published in the first half of 2005 were both vendor confirmed and six of eight vulnerabilities in the second half of 2004 were vendor confirmed.

Of the six vulnerabilities published for the Apple Safari browser during this reporting period, three were vendor confirmed. In the first half of the year, two out of the three disclosed vulnerabilities were vendor confirmed, as were four of the seven published in the second half of 2004.

Browser vulnerabilities are a serious security concern, particularly due to their use in online fraud and the propagation of spyware and adware. Organizations should closely monitor vulnerability mailing lists and apply necessary patches as required in a timely manner.

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 July 1 and December 31, 2005.

Symantec categorizes malicious code in two ways: families and variants. A family is a new, distinct sample of malicious code. For instance, W32.Sober@mm would have been the founding sample, or the primary source code, of the Sober family. In some cases, a particular family of malicious code may have multiple variants. A variant is a new iteration of the same family, one that has minor differences but that is still based on the original. For instance, Sober.X is a variant of Sober. A new variant is often created when the source code of a successful virus or worm is modified slightly to bypass antivirus detection definitions developed for the original.

The "Malicious Code Trends" section will discuss:

- Top ten malicious code samples
- Win32 viruses and worms
- Exposure of confidential information
- Instant messaging threats
- Modular malicious code
- Propagation vectors
- Bots
- Bot variants

This discussion will include any prevention and mitigation measures that might be relevant to the particular threats being discussed. However, 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—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. Additionally, Symantec recommends that ingress and egress filtering be put in place on perimeter devices to detect anomalous activity.

End users should employ defense in-depth, 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 operating system vendor. 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.

Top ten malicious code samples

Traditionally, mass-mailing worms have dominated the top ten malicious code samples reported to Symantec. In the last edition of the Symantec *Internet Security Threat Report*, however, there were only two mass-mailing worms present in the top ten. The current period represents a return to earlier form, as eight

of the top ten samples reported to Symantec propagated by a mass-mailing component (as indicated by the SMTP vector in table 9). This may indicate that users are still falling victim to social engineering methods that entice them to click on malicious attachments in email.

Rank	Sample	Type	Vectors	Impact
1	Sober.X	Worm	SMTP	Downloads a remote file
2	Netsky.P	Worm	SMTP, P2P	Logs e-Gold account information
3	Mytob.ED	Worm, Bot	SMTP	Allows remote access
4	Mytob.DF	Worm, Bot	SMTP	Allows remote access
5	Spybot	Bot	CIFS, Remotely Exploitable Vulnerability, Back doors	Allows remote access
6	Mytob.EE	Worm, Bot	SMTP	Allows remote access
7	Tooso.L	Trojan	N/A	Disables security applications, downloads a remote file
8	Mytob.KU	Worm, Bot	SMTP	Allows remote access
9	Netsky.Z	Worm	SMTP	Downloads a remote file
10	Mytob	Worm, Bot	SMTP, CIFS, Remotely Exploitable Vulnerability	Allows remote access

Table 9. Top ten malicious code samples
Source: Symantec Corporation

In the last six months of 2005, Sober.X[98] was the most widely reported malicious code sample (table 9). This worm was initially discovered on November 19, 2005 and was upgraded to a category 3 threat on November 22.[99] Despite the fact that it has been in the wild for just over a month, Sober.X was reported more frequently than any other malicious code sample in the entire six-month period.

Sober.X is a mass-mailing worm that relies on social engineering to persuade a user to run its email attachment. Similar to previous variants of the Sober worm, it propagates by sending email messages in both English and German, depending on the Windows regional settings on the compromised computer. Some of the messages it uses to propagate purport to be from the FBI while others appear to be SMTP delivery failure messages. This form of social engineering allowed the worm to propagate rapidly amongst a large number of users.

Additionally, a single computer compromised by a mass-mailing worm can be responsible for sending out a high volume of email messages. Sober.X is programmed to contact several remote Web sites to download a file and execute it on the compromised computer if the date is January 6, 2006 or later. It checks the date by contacting several NTP (Network Time Protocol) servers. However, on January 6 the file was not available. This is likely due to the amount of media attention Sober.X received, which allowed administrators to prepare by blocking network access to the download sites. There is also a possibility that the worm's author was aware that the sites would be monitored by law enforcement officials and did not upload the intended payload to avoid detection.

[98] http://securityresponse.symantec.com/avcenter/venc/data/w32.sober.x@mm.html
[99] A category 3 threat is a malicious code sample that is considered a moderate threat. It is either currently spreading among computer users but reasonably harmless and easy to contain or has not been released into the wild but is potentially dangerous and difficult to contain.

Netsky.P was the second most frequently reported malicious code sample in the second half of 2005.[100] It was first reported in March 2004 and continues to be one of the most frequently reported malicious code samples documented by Symantec. The continued success of this threat is due to its effective social engineering and multiple propagation mechanisms. Netsky.P copies itself to shared network drives and to folders commonly associated with various peer-to-peer file-sharing programs. It also emails itself to addresses gathered from a compromised computer.

The mass-mailing technique also incorporates two additional mechanisms. In an attempt to bypass filtering mechanisms, the worm sends itself in an archive using a .ZIP extension. It may also attempt to exploit a MIME processing vulnerability in Internet Explorer[101] so that the message attachment is automatically executed when the message is viewed or previewed with a vulnerable email client. Netsky.P exposes account information for e-Gold, an Internet payment system.

Mytob.ED was the third most frequently reported malicious code sample during this reporting period.[102] It was one of several variants of the Mytob worm that were widely reported in the current period.[103] This worm contains a bot component that allows an attacker to gain remote control over the compromised computer. It then enables the attacker to perform various actions, including logging keystrokes, stealing cached passwords, and downloading files. Some variants may also propagate by exploiting remote vulnerabilities in Windows services, such as the DCOM RPC vulnerability,[104] the LSASS vulnerability,[105] and the Windows Plug and Play buffer overflow vulnerability.[106]

Win32 viruses and worms

Win32 threats are executable files that operate by using the Win32 API (application program interface), which provides a standard for the development of software on the Windows platform. These forms of malicious code work on at least one Win32 platform.

Win32 threats continued to experience a major rise in volume during 2005. This rise was first noted in the 2003 volumes of the *Internet Security Threat Report*, and it is clear that the tendency continues in the second half of 2005. Over the second half of 2005, Symantec documented more than 10,992 new Win32 viruses and worms (figure 22). While this is consistent with the 10,866 detected in the first half of the year, it is a 49% increase over the 7,360 documented in the second half of 2004.

The significant increase over the last year is due to the continued development of Win32 worms that implement bot features that attackers can use for financial gain. One example of this is the Spybot family,[107] which now requires four letters to describe a variant such as “W32.Spybot.ABCD”.[108] As of December 31, Symantec had catalogued 19,545 Spybot variants.

[100] http://securityresponse.symantec.com/avcenter/venc/data/w32.netsky.p@mm.html
[101] http://www.securityfocus.com/bid/2524
[102] http://securityresponse.symantec.com/avcenter/venc/data/w32.mytob.ed@mm.html
[103] http://securityresponse.symantec.com/avcenter/venc/data/w32.mytob@mm.html
[104] http://www.securityfocus.com/bid/8205
[105] http://www.securityfocus.com/bid/10108
[106] http://www.securityfocus.com/bid/14513
[107] http://securityresponse.symantec.com/avcenter/venc/data/w32.spybot.worm.html
[108] Malicious code variants are named using the family name plus an identifying letter for the variant. Therefore, Spybot.A would be the original sample and subsequent variants are assigned sequential letters, such as Spybot.B, Spybot.C, etc. When Spybot.Z is reached, two letters are used to identify the variant, such as Spybot.AB. So a family with four variant letters has over 17,500 variants.

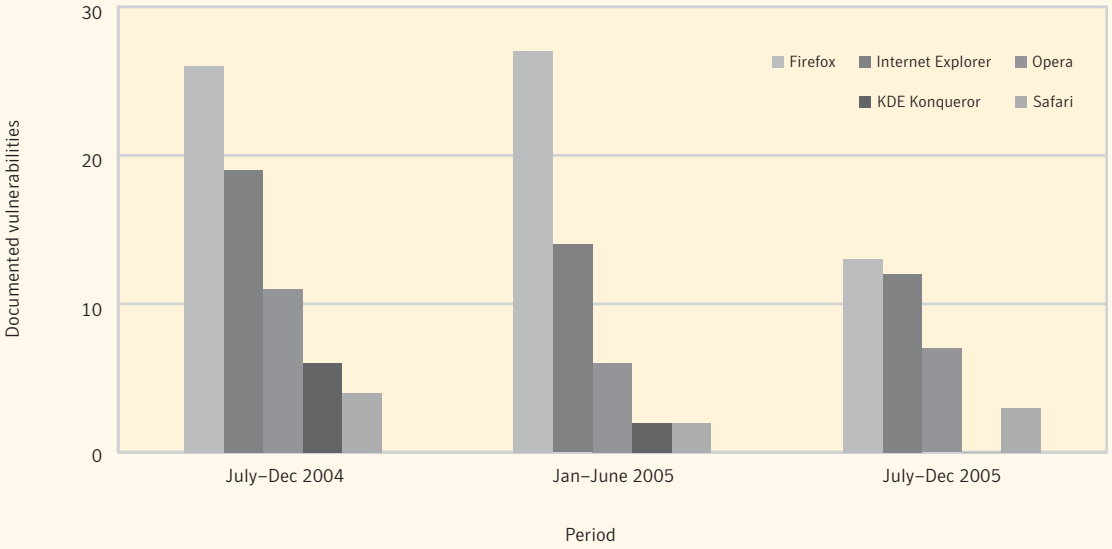

Figure 22. New Win32 viruses and worm variants
Source: Symantec Corporation

Throughout 2005, the number of new Win32 threat variants remained consistently high. As of December 31, 2005 the total number of Win32 variants had surpassed 39,257. In 2005 alone Symantec documented 21,858 Win32 viruses and worms. Thus, the total number of Win32 virus and worm threats more than doubled during 2005 alone, indicating that these threats will continue to dominate the malicious code landscape for some time to come.

While the number of new Win32 viruses and worms continues to grow, the number of new Win32 families decreased in the second half of 2005. The number of new families per period had remained relatively consistent over the previous four periods. However, over the past six months, the number of new families declined by 39%, from 170 new families in the first half of 2005 to 104 in the second half.

The continued rise of Win32 viruses and worms, along with the decrease in the number of new families, indicates that there are far more variants of existing malicious code families being produced than previously. This can partially be attributed to the availability of source code for some families. For example, the source code for some bots, such as Spybot, Gaobot, and, more recently, Mytob, is readily available online. Since it is easier to modify an existing piece of malicious code than to create a new family, it is not surprising to see a large number of variants of existing families rather than entirely new families. As discussed in the "Bot variant" section below, the number of variants for these samples makes up a large portion of the new Win32 variants documented by Symantec.

One of the reasons for the sustained popularity of Win32 malicious code has been the continued success of mass-mailing worms, such as the Sober and Beagle families, which were among the most significant

outbreaks of the year. Because of the predominance of Windows platforms, any mass-mailer worm that hopes to enjoy widespread propagation will target these platforms, thereby leading to the increased development of Win32 viruses and worms.

On the other hand, traditional file infector viruses are less prominent than ever before, primarily because of their limited ability to propagate rapidly. A file infector virus only propagates when an infected host file is shared and executed on another computer. Since an infected file may never be shared, mass mailing is a much more reliable means of propagation. If the malicious code is financially motivated, its creator will likely want it to be installed on the greatest number of computers possible in a short period of time, something that can be accomplished much more readily with a mass-mailer than with a file infection virus.

In the second half of 2005 attackers continued to exploit Windows XP SP2 and Windows Server 2003 systems with increasing success. For example, the Microsoft Windows Graphics Rendering Engine WMF SetAbortProc Code Execution Vulnerability[109] was a zero-day attack, one that required very little understanding for successful exploitation. This vulnerability exists on a variety of platforms going all the way back to Windows 3.0 and up to the 64-bit versions of Windows; however, it was only remotely exploitable on more recent versions.

During the ten days prior to the official release of the patch by Microsoft, 200 individual variations of the attack were reported.[110] Despite the patch, variations of the attack continued to appear, albeit with decreasing frequency. Normally, attackers will "clone" attack code, but in this case many individual attackers were willing to take advantage of the vulnerability by writing their own code prior to the patch. In addition to individual exploits, malicious code written for profit—such as the Bankash.G[111] password-stealing Trojan—also took advantage of this vulnerability.

Exposure of confidential information

Threats that expose confidential information from a compromised computer are a concern to all users, in home, small business, and enterprise environments alike. These threats may expose sensitive data such as system information, confidential files and documents, or cached logon credentials. Some threats, such as back doors, may give a remote attacker complete control over a compromised computer.

Threats to confidential information are a particular concern because of their potential use in cybercrime activities. With the increasing use of online shopping and Internet banking, compromises of this nature can result in significant financial loss, particularly if credit card information or banking details are exposed. For instance, online brokerage accounts have recently been targeted by these threats.[112]

During the last six months of 2005, the percentage of malicious code samples that threaten confidential information in the top 50 malicious code reports declined somewhat. This is not necessarily due to a reduction in these threats; rather, it is likely due to the high volume of Sober.X reports. Since this percentage is derived from the overall volume of the top 50 malicious code reports, the high volume of Sober.X reports during this period may have caused the percentage to seem abnormally low. If Sober.X is removed from consideration, the percentage of malicious code threats to confidential information rose from 74% in the previous period to 80% in the current period (figure 23). This is a significant increase over the 54% of confidential information exposure threats during the same six-month period in 2004.

[109] http://www.securityfocus.com/bid/16074
[110] These utilized the same exploit for this vulnerability, but there were over 200 different shellcode payloads incorporated into the exploit. Each payload is capable of performing different actions on a compromised computer, such as opening a back door or installing malicious code.
[111] http://securityresponse.symantec.com/avcenter/venc/data/pwsteal.bankash.g.html
[112] http://www.sec.gov/investor/pubs/onlinebrokerage.htm

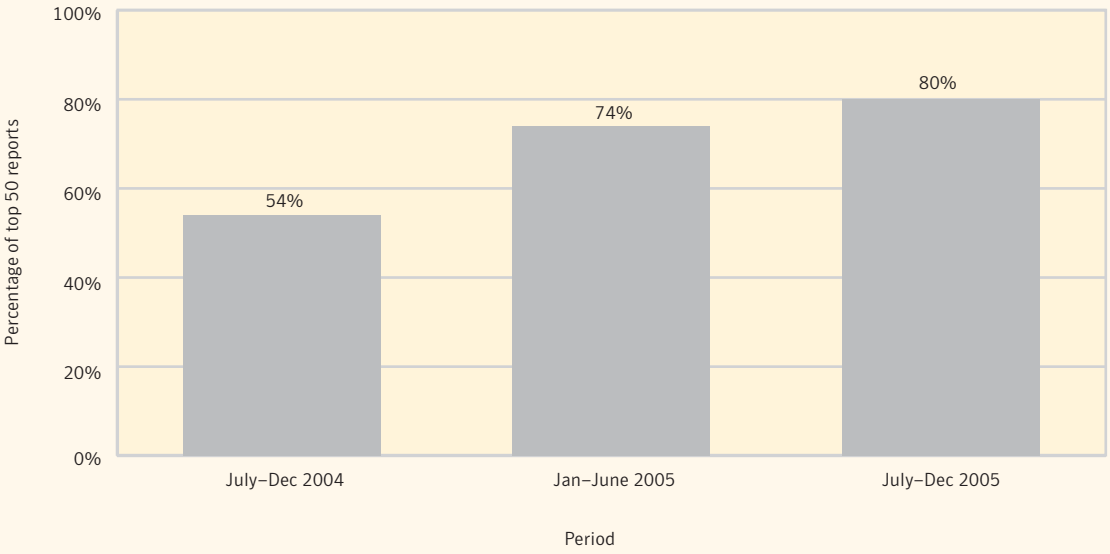

Figure 23. Threats to confidential information, with Sober.X removed from consideration
Source: Symantec Corporation

The increase in confidential information threats this period (Sober.X notwithstanding) can largely be attributed to the number of Mytob variants in the top 50 malicious code reports. Thirteen of the top 50 reports were variants of Mytob, including five of the top ten. As was established in the "Top ten malicious code reports" section above, Mytob variants allow attackers to log keystrokes, steal cached passwords, and download files from the compromised host, all of which are ways of exposing confidential information.

In addition to the Mytob variants, a great number of other threats to confidential information were widely reported this period. Back door server programs such as Graybird[113] and Ranky[114] were seen in significant numbers. These applications allow a remote attacker full access to a compromised computer and all documents stored on them. Graybird also intercepts keystrokes, allowing it to log information such as usernames and passwords entered into various Web pages and applications.

As noted above, the Bankash.G Trojan was installed on computers by exploiting a zero-day vulnerability in Internet Explorer. This Trojan gathers all cached passwords from the compromised computer and also monitors user input on certain Web pages to gather more authentication information. Interestingly, the Web pages this Trojan monitors are not online banking sites, as is common with most password stealers. Instead, Bankash.G monitors several Webmail sites,[115] as well as online commerce sites and other sites, such as Monster.com. Information an attacker could gather by gaining access to a user's Webmail or Monster.com account, such as addresses, phone numbers, social security numbers, and other data, could easily be used to perform identity theft.

Other prevalent information exposure threats can be used to generate monetary gain for their authors. For instance, variants of the Bancos[116] and Banpaes[117] password-stealing Trojans remained among the top 50

[113] http://securityresponse.symantec.com/avcenter/venc/data/backdoor.graybird.html
[114] http://securityresponse.symantec.com/avcenter/venc/data/backdoor.ranky.html
[115] Examples of Webmail sites include Hotmail, Yahoo!, and Gmail.
[116] http://securityresponse.symantec.com/avcenter/venc/data/pwsteal.bancos.html
[117] http://securityresponse.symantec.com/avcenter/venc/data/pwsteal.banpaes.html

most reported samples this period. These crimeware threats can be used to steal a user's online banking authentication credentials in order to transfer money out of the victim's account. In the case of Banpaes, the Trojan actually mimics the interface of online banking Web sites. To protect against threats such as these, when connecting to online banking sites, users should ensure that they are connected to the legitimate site through a secure connection. Additionally, the use of a URL verification service can notify users when they are connected to a site that is attempting to mimic a legitimate site.

Malicious code for mobile devices

Malicious code that targets mobile devices continued to grow through the second half of 2005. The last three volumes of the *Internet Security Threat Report* have discussed the development of malicious code for smart phones. Smart phones are mobile phones that contain a fully-fledged operating system with a wide variety of user-installable software. They may be particularly vulnerable to malicious code, as they appear to have increased exposure through replication vectors such as Multimedia messaging (MMS) and other telephony protocols. Between July and December 2005, new variants of Cabir,[118] Commwarrior,[119] and Skulls[120] were reported.

Additionally, new malicious code for these platforms was developed in the last six months of 2005. The most interesting new sample was the Cardtrp Trojan.[121] Cardtrp was the first cross-platform malicious code with the ability to affect both Symbian and Windows operating systems. When executed on a smart phone, the Trojan will install a variant of Cabir and attempt to copy files to the memory card. If the memory card is then inserted into a card reader on a Windows computer, one or more of these files will automatically be executed. Files that are known to have been copied to the memory card have included various samples of malicious code, including back doors, such as Berbew.N,[122] and worms, such as Wullik[123] and Cydog.[124]

Another new development in smart phone malicious code is the Pbstealer family of Trojans.[125] Pbstealer may be distributed as a file that represents itself as a phone book utility for smart phones in order to entice a user to download and execute it. Once a device has been compromised by one of these Trojans, information such as the user's phonebook, notepad, and calendar to-do list will be transmitted to Bluetooth-enabled devices that are within range. This may pose a serious breach of confidentiality if a corporate device is compromised in this manner, as sensitive contact information and appointments could be transmitted.

As is the case for most malicious code, users can protect themselves against these threats by practicing safe computing behaviors. For instance, they can help prevent infection from these programs by not installing unknown programs or accepting connections from unknown sources.

[118] http://securityresponse.symantec.com/avcenter/venc/data/symbos.cabir.html
[119] http://securityresponse.symantec.com/avcenter/venc/data/symbos.commwarrior.a.html
[120] http://securityresponse.symantec.com/avcenter/venc/data/symbos.skulls.html
[121] http://securityresponse.symantec.com/avcenter/venc/data/symbos.cardtrp.a.html
[122] http://securityresponse.symantec.com/avcenter/venc/data/backdoor.berbew.n.html
[123] http://securityresponse.symantec.com/avcenter/venc/data/w32.wullik@mm.html
[124] http://securityresponse.symantec.com/avcenter/venc/data/w32.hllw.cydog@mm.html
[125] http://securityresponse.symantec.com/avcenter/venc/data/symbos.pbstealer.a.html

Instant messaging threats

Instant Messaging (IM) continues to grow rapidly, with users in both home and enterprise environments estimated at 300 million in 2005. The three largest IM providers—AOL Instant Messenger, MSN Messenger, and Yahoo! Messenger—each report over one billion messages sent per day, and some observers believe that IM traffic will exceed email traffic by the end of 2006.

However, though widespread in adoption, IM is generally unprotected and unmonitored in consumer and enterprise environments, leaving it vulnerable to attacks. This is particularly worrisome for corporate entities, as IM is rapidly becoming a key part of enterprise communications. As one of the most successful and widely deployed applications on the Internet, IM has increasingly become a means for the propagation of viruses, worms, and phishing attacks.

Instant messaging can be a potent vector for the spread of malicious code. The infection of one computer can result in messages being broadcast to all users contained in an IM contact list on that machine, creating the potential for rapid proliferation. Furthermore, social engineering tactics can be highly effective, as the parties communicating by IM are inherently trusted.

In the second half of 2005, worms were the preferred type of malicious code on all three large IM networks. In the second half of 2005, worms constituted 91% of IM-related malicious code, a ten percent increase over the 83% in the first half of 2005 (figure 24). In one instance that Symantec documented, a worm would reply to IM messages in order to make it appear as though the user was legitimately sending a link to a file to their contacts.[126] If a user followed the link, a Spybot variant would be downloaded and potentially executed if the user opened the file.[127]

Worms were also used to download other non-IM malicious code during the period. For instance, a worm may send users a link to a Web page that exploits a vulnerability in a Web browser,[128] such as the Microsoft Windows Graphics Rendering Engine WMF SetAbortProc Code Execution Vulnerability.[129] This would allow the malicious code hosted on the Web page to be automatically installed on the computer of a user running a vulnerable browser.

[126] http://tc.imlogic.com/threatcenterportal/pubThreatDetail.aspx?ThreatID=3255
[127] Detection for this variant was included in the generic W32.Spybot.Worm family detection http://securityresponse.symantec.com/avcenter/venc/data/w32.spybot.worm.html
[128] http://tc.imlogic.com/threatcenterportal/pubThreatDetail.aspx?ThreatID=3505
[129] http://www.securityfocus.com/bid/16074

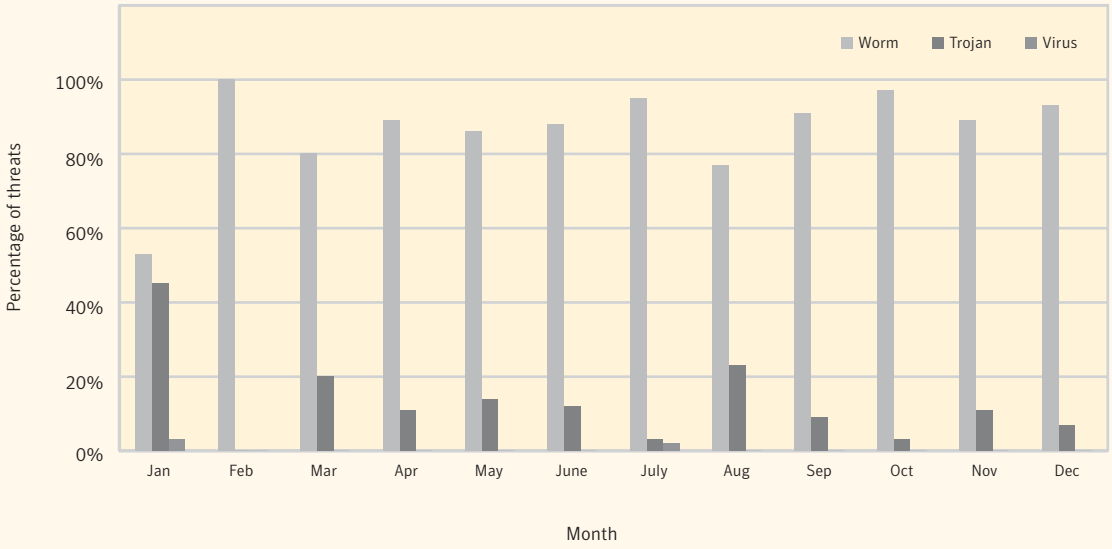

Figure 24. Instant messaging threats
Source: Symantec Corporation

While the number of IM-related worms increased in the second half of 2005, the proportion of Trojans and other malicious code targeting IM either remained steady or decreased slightly. Trojans accounted for nine percent of IM-related malicious code, down 47% from the 17% in the first half of 2005. Viruses, on the other hand, accounted for less than one percent in each period.

To protect against instant messaging threats, users should employ defense in-depth, including the deployment of antivirus software and a personal firewall. Users should also update their antivirus definitions regularly. They should never view, open, or execute any file that is transferred by IM unless it is expected and comes from a trusted source and unless the purpose of the file or link is known. Finally, they should never follow any links sent in an instant message unless the link is sent by a known and trusted source.

Modular malicious code

Modular malicious code is malicious code that initially possesses limited functionality,[130] but that, once installed on a target host, downloads other pieces (or modules) of code with different, usually malicious, functionalities. In the previous volume of the *Internet Security Threat Report,* Symantec stated that modular malicious code would be an issue of concern in the near future. This speculation appears to have been borne out.

Between July and December of 2005, modular malicious code accounted for 88% of the top 50 malicious code reported to Symantec (figure 25). This is a 14% increase over the 77% reported from January to June 2005 and a 40% increase over the 63% in the second half of 2004.

[130] Initial functionalities can include attempting to disable antivirus and firewalls.

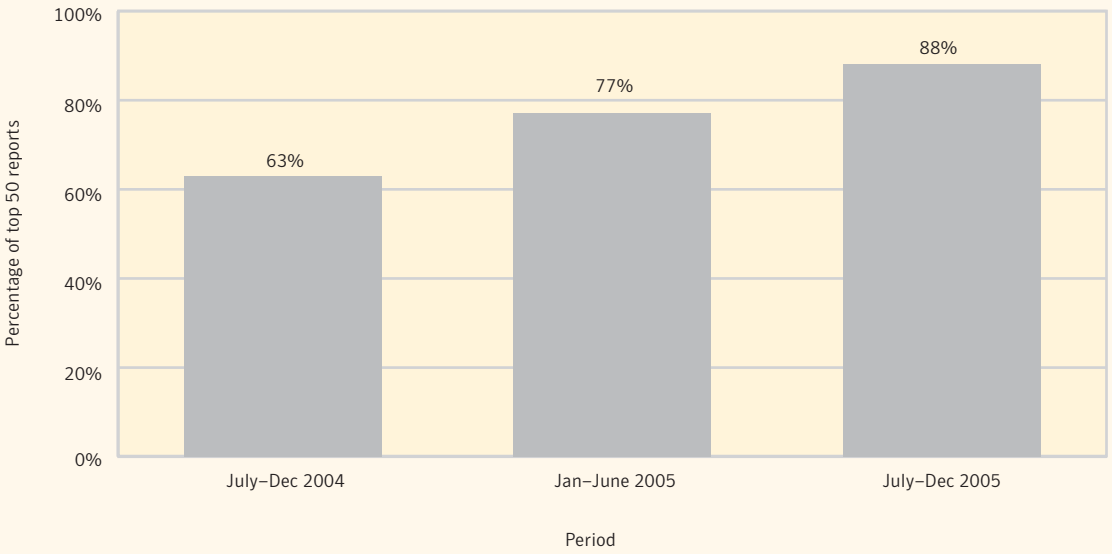

Figure 25. Modular malicious code
Source: Symantec Corporation

Modularity in malicious code can serve different purposes. The malicious code may simply attempt to update itself to a more recent version, as is often the case for bots and back door servers. More Trojans and worms are beginning to employ modularity. This allows a smaller executable with limited functionality to infect a computer and subsequently download a larger executable containing new functionality, such as a bot or back door.

Typically, Trojans and worms that are part of a modular attack will attempt to disable security applications on the computer and, in the case of worms, propagate. The more severe impact from these threats usually comes from the secondary component they download. This may be a Trojan that performs a wider range of actions on the computer, such as logging keystrokes or acting as a proxy server, or, in some cases, adware may be downloaded and installed.

Frequently, modular malicious code is used to download a crimeware application to gather confidential information. As previously noted, threats to confidential information may be used by attackers for financial gain. By using modular malicious code, attackers may download and simultaneously install a confidential information threat on a large number of compromised computers.

The most notable current example of modular malicious code in the second half of 2005 was the Sober.X worm. It began propagating at the end of November 2005 and was upgraded to a Category 3 threat within days. The worm contained an algorithm to begin downloading files from a number of Web sites on January 6, 2006 and every week thereafter.

In order to protect against modular malicious code, administrators may have to implement strict egress filtering against known URLs to prevent compromised computers within their networks from contacting Web sites where additional components are known to be stored. This will prevent the second—and frequently more severe—module of the malicious code from being installed.

Propagation mechanisms

Worms and viruses use various means of transferring themselves from one computer to another. These transportation vectors are collectively referred to as propagation mechanisms. Propagation mechanisms can include a number of different vectors, such as Simple Mail Transfer Protocol (SMTP), Common Internet File System (CIFS), peer-to-peer services (P2P), and remotely exploitable vulnerabilities. Some malicious code may even use other malicious code as a propagation vector by locating a computer that has been compromised by a back door server and using that back door to upload and install itself. It is important to note that many malicious code samples employ multiple vectors in an effort to increase the probability of successful propagation.

In the second half of 2005, SMTP was the most commonly used malicious code propagation vector (figure 26). This is not surprising, as this protocol is heavily involved in the delivery of email, one of the most widely employed applications on the Internet. Twenty-six of the top 50 malicious code samples that propagate did so by SMTP. These samples accounted for 92% of the volume of top 50 malicious code reports with propagation mechanisms this period. In the first half of 2005, only 19 of the top 50 malicious code samples that propagate used SMTP, accounting for 52% of the volume of the top 50 malicious code reports. In the second half of 2004, 34 samples used SMTP, accounting for 81% of the volume of malicious code that propagates. In addition to being used as a malicious code infection vector, SMTP is also used to send Trojans in spam email.

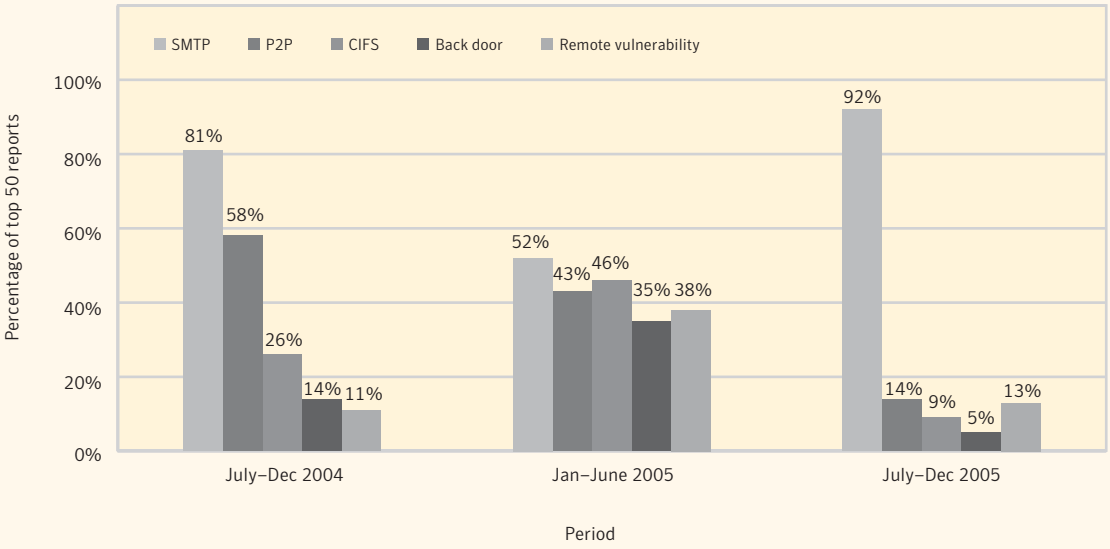

Figure 26. Propagation mechanisms by volume of malicious code reports
Source: Symantec Corporation

In the second half of 2004, the top 50 reported malicious code samples was dominated by variants of the Netsky, Beagle, and Mydoom worms, all of which were mass-mailing worms. As a result, malicious code that propagated by SMTP accounted for 81% of malicious code reports. In the first half of 2005, however, fewer samples of these worms were reported (figure 26) and reported SMTP usage dropped accordingly. The increase in the use of SMTP this period can be attributed to Sober.X and multiple variants of Mytob. Sober.X uses SMTP as its sole propagation vector, as do the majority of Mytob variants. The high number of mass-mailing worms resulted in a decrease of other propagation methods in the top fifty reported samples during this period.

SMTP is a highly effective propagation vector, as proven by the Sober.X worm. This variant accounted for 52% of the volume of the top 50 malicious code reports that propagate. Organizations can protect against SMTP threats by blocking all email attachments at the mail gateway. If there is a business need for email attachments, only those that are considered safe should be allowed. If other attachment types are accepted, they should always be scanned by antivirus products with up-to-date definitions and should only accepted from trusted sources.

In the current period, seven of the top 50 malicious code samples that propagate used CIFS as a vector, accounting for nine percent of reported malicious code that propagates (figure 26). This shows a decline from January to June 2005 when nine of the top 50 samples used this vector, accounting for 46% of malicious code reports that propagate for that period. While 16 unique samples employed CIFS in July to December 2004, these only accounted for 26% of malicious code reports that propagate for the period. The decline in the use of CIFS as a propagation mechanism may be attributed partially to the decline in reports of Gaobot and Randex variants, which make heavy use of this vector.

As was discussed in the introductory paragraph to this section, some malicious code actually uses other malicious code to propagate. Specifically, some samples, such as Gaobot and Randex variants, will search for back door servers that are installed on previously compromised computers and use the back door to install themselves. A fairly recent development in malicious code programming, this strategy takes advantage of the fact that if a computer has already been compromised, it is likely to have a weak security posture. This could allow additional malicious code installations to go undetected.

In the first half of 2005, four of the top 50 samples that propagate did so by this method, accounting for 35% of the top 50 reports for the period. However, it has since declined (figure 26). In the second half of the year, only two of the unique samples in the top 50 malicious code that propagates used this vector, accounting for five percent of the volume of top 50 reports. In the second half of 2004, two samples accounting for 14% of top 50 reports used this vector. As has been noted previously in this discussion, the decline in the current period can likely be attributed to the large volume of Sober.X reports and the decrease in Gaobot and Randex reports.

The use of peer-to-peer (P2P) file-sharing networks as a propagation vector for malicious code also appears to be on the decline. Between July and December 2005, only eight of the top 50 samples—accounting for 14% of the top 50 reports—used P2P networks as a propagation mechanism (figure 26). This is down from nine samples accounting for 43% of reports in the previous period and 19 samples accounting for 58% of reports for the same period in 2004.

The second half of 2004 was dominated by reports of Netsky, Mydoom, and Beagle worm variants, all of which used P2P propagation routines. Since that period, reports of these worms have declined significantly. Additionally, P2P networks have faced several legal challenges in the last year, particularly those networks that may be used to share pirated content.[131] Since most worms that make use of P2P networks use enticing filenames that mimic illicit content, it is possible that malicious code authors have discontinued their use to focus on other propagation mechanisms.

Malicious code that uses remotely exploitable vulnerabilities to propagate is heavily dependent upon the existence of unpatched computers for their ability to spread. The discovery of new remote vulnerabilities that allow code execution also affects the success of this vector. In the current period, ten of the unique samples in the top 50 reports that propagate utilized a remotely exploitable vulnerability to do so (figure 26). This is an increase over the five samples that used this vector in the previous two periods.

While more unique samples employed this vector in the current period, they appear to have been less successful than in the previous period. Between July and December 2005, 13% of malicious code samples that propagate were reported to exploit vulnerabilities. This is down from the 38% of reports in the previous period, but a slight increase over the 11% in the same period last year.

Two of the samples that exploited remote vulnerabilities to propagate in the last six months of 2005 are members of the Esbot family.[132] These bots exploited the Microsoft Windows Plug and Play Buffer Overflow Vulnerability to propagate.[133] Since this vulnerability can only be exploited on Windows 2000 operating systems by a remote, anonymous attacker, the bot's potential infection base is limited, which may account for the lower report volume.

[131] http://www.securityfocus.com/news/10123
[132] http://securityresponse.symantec.com/avcenter/venc/data/w32.esbot.a.html
[133] http://www.securityfocus.com/bid/14513

It is also notable that for the first time since their initial discoveries, variants of the Nimda[134] and Sasser[135] worms were absent from the top 50 reported malicious code samples. This may indicate that more users are patching computers or implementing firewalls and intrusion detection systems to protect against these threats.

Other infection vectors that have been used in the past were not represented in the top 50 malicious code samples this period. These vectors include Network News Transport Protocol (NNTP), and Internet Relay Chat (IRC). While mechanisms to propagate through these vectors were not widely reported, that is not to say that they were not used at all.

Bots

Bots (short for "robots") are programs that are covertly installed on a user's computer in order to allow an unauthorized user to control the computer remotely. Bots are designed to let an attacker create a network of compromised computers known as a bot network, which can be remotely controlled to collectively conduct malicious activities such as DoS attacks.[136]

Bots can have numerous effects on an enterprise. A single infected host within a network (such as a laptop that was compromised outside the local network and then connected to the network, either directly or by VPN) can allow a bot to propagate to other computers that are normally protected against external attacks by corporate firewalls. Bots can be used by external attackers to perform DoS attacks against the enterprise's Web site, which can disrupt revenue for e-commerce companies. Furthermore, bots within an organization's network can be used to attack other organizations' Web sites, which can have serious legal consequences for the organization.

In the second half of 2005, the percentage of bot-related malicious code reported to Symantec increased significantly, accounting for 20% of the top 50 (figure 27). This represents a 43% increase over the first half of 2005, when bots accounted for 14% of the top 50 malicious code reports. It is also a 67% increase over the 12% in the second half of 2004. This is likely due to the high number and pervasiveness of variants of the Mytob worm, which installs a bot on compromised computers.

[134] http://securityresponse.symantec.com/avcenter/venc/data/w32.nimda.e@mm.html
[135] http://securityresponse.symantec.com/avcenter/venc/data/w32.sasser.b.worm.html
[136] For a more in-depth discussion on bot networks and bot network activity, please see the "Bot network" section in the "Attack Trends" report in this document.

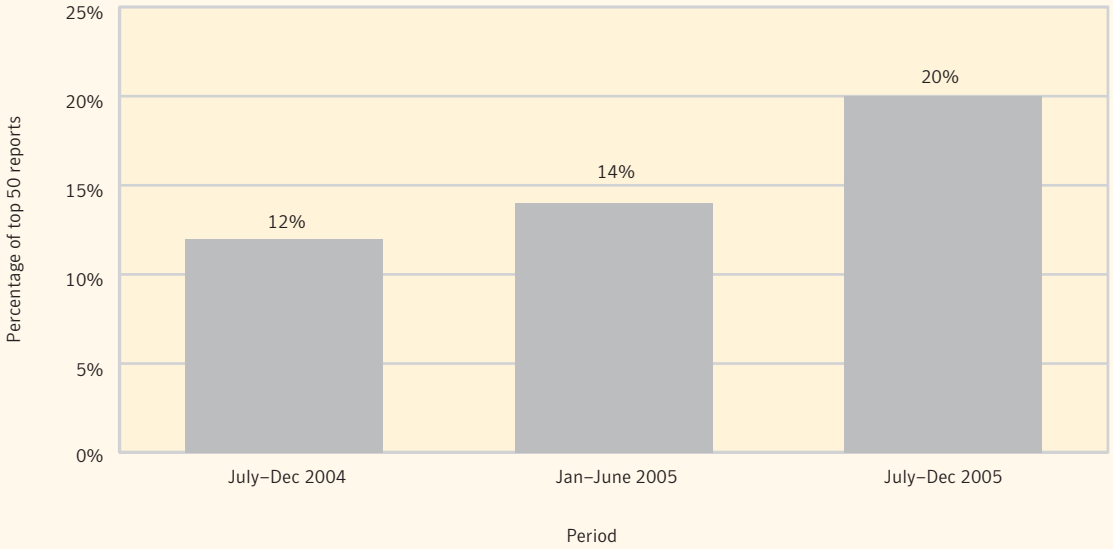

Figure 27. Bots in top 50 malicious code reports
Source: Symantec Corporation

As previously noted, due to the widespread use of email, SMTP is the most commonly used malicious code propagation vector. Mytob is the first bot to rely mainly on SMTP as a propagation vector rather than CIFS and remotely exploitable vulnerabilities, both of which were commonly employed by Gaobot, Spybot, and Randex variants. This shift towards employing new propagation mechanisms in bots may reflect the increasing competition among bot authors for systems to compromise. Because mass mailers are so effective at propagating widely, the incorporation of SMTP as a bot propagation vector may create the potential for much larger bot networks than previous vectors. This development could represent a convergence between traditional malicious code authors and bot network owners.

Bots are frequently used in the commission of cybercrimes. There is evidence to suggest that the original authors of Mytob and Zotob[137] created these bots to aid them in a credit card fraud ring.[138] The bots were used to allow the authors to retrieve financial information from compromised computers, information that could then be used to commit fraud.

Bots can also be used in another aspect of cybercrime called denial of service (DoS) extortion. This type of cybercrime involves an attacker threatening to launch a DoS attack against an organization's Web sites if the organization does not pay the attacker an established amount of money.[139] In another type of bot-conducted cybercrime, companies have reportedly hired attackers to launch DoS attacks against competitors using bot networks.[140]

It should be noted that while there was a significant increase in the number of reported bot samples, bot activity discussed in the "Attack Trends" section of this report did not increase proportionately. There may be a number of reasons for this discrepancy. Since one person may control a number of different bot

[137] http://securityresponse.symantec.com/avcenter/venc/data/w32.zotob.a.html
[138] http://www.washingtonpost.com/wp-dyn/content/article/2005/08/26/AR2005082601201.html
[139] http://www.smh.com.au/news/breaking/hackers-demand-ransom/2006/01/19/1137553695238.html
[140] http://www.techworld.com/security/features/index.cfm?FeatureID=1711

networks, it is likely that he or she would only activate or use a limited number of these networks at once. This way, if one network is discovered by authorities and deactivated, the bot controller will still have other undiscovered networks to fall back on. Additionally, a report of a malicious code sample does not always mean that a computer was successfully compromised.

Bot variants

New variants of existing bots continue to be created at a high rate. Between July 1 and December 31, 2005, Symantec Security Response documented 6,542 new variants of Spybot, a three percent increase over the 6,361 variants in the first half of this year and a 53% increase over the 4,288 samples documented during this period in 2004 (figure 28). Spybot variants typically exploit a single vulnerability as their propagation mechanism. Therefore, the steady increase in variants of this bot may be due to attackers creating multiple variants, each of which is designed to exploit a different vulnerability, which would give the attacker the chance to compromise a wide range of computers.

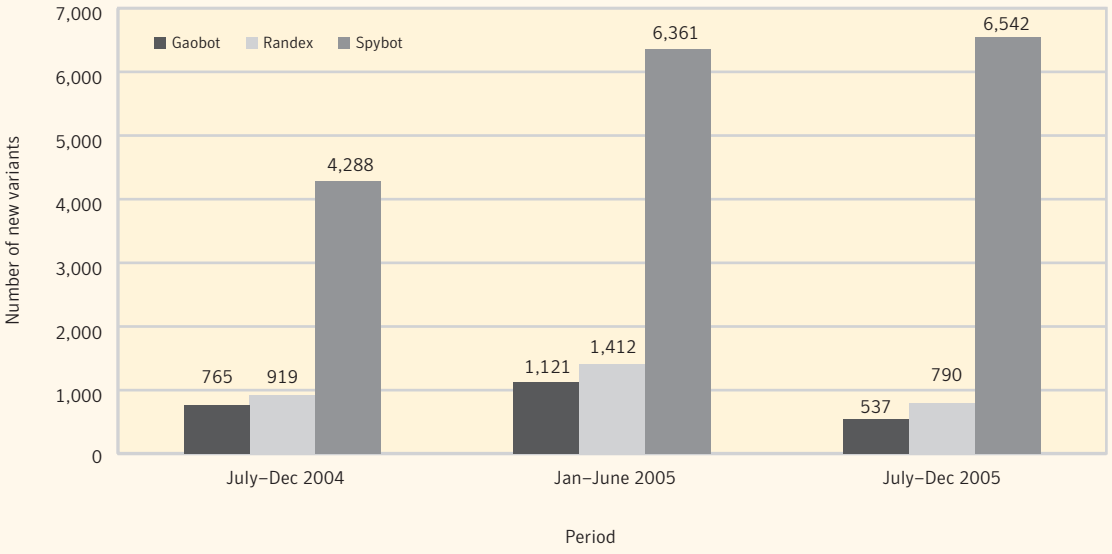

Figure 28. New bot variants
Source: Symantec Corporation

While Spybot variants have been increasing at a steady pace, the production of new variants of Gaobot and Randex appear to have declined in the current period. During the second half of 2005, Symantec documented 790 new variants of Randex, a decline of 44% from the first half of the year when 1,412 new variants were documented. Gaobot also experienced a similar decline. Symantec documented 537 new Gaobot variants in the current period, down 52% from the 1,121 in the first half of the year. As a result, overall Gaobot and Randex reports have declined in the current period while Spybot reports have remained high.

Even though production of new variants of Gaobot and Randex has declined, the number of variants currently documented is still significant. Other than Spybot, no other malicious code families in this period had as many documented variants as these bots. One possible reason for the decline in Gaobot and Randex variants could be interest in newer bot families. For example, Mytob was first reported to Symantec on February 26, 2005. Between that date and December 31, 2005, Symantec documented 430 variants, indicating that there may be a shift towards this newer bot. This may be attributed to the use of SMTP as a propagation mechanism in Mytob.

The continuing increase in the production of bot variants may be driven by a desire on the part of bot authors for maximum return on the time invested in bot creation. Those that produce bots for financial gain may prefer to produce a larger number of variants than create entirely new bots, which can be time consuming. Furthermore, the ease with which an existing bot can be modified to create a new variant may enable less skilled attackers to create a bot network, which might otherwise be beyond their capabilities.

Additional Security Risks

Traditionally, the Symantec *Internet Security Threat Report* has broken security threats down into three general categories: attacks, vulnerabilities, and malicious code. However, as Internet-based services and applications have expanded and diversified, the potential for computer programs to introduce other types of security risks has increased. The emergence of new risks, particularly spam, phishing, spyware, and adware, has necessitated an expansion of the traditional security taxonomy.

Symantec has monitored these new concerns as they have developed, classifying them as "additional security risks." This section will examine developments in additional security risks over the last six months of 2005. In particular, it will examine trends in spyware and adware, phishing, and spam.

Spyware and Adware

While spyware and adware are not categorized as malicious code, Symantec monitors them using many of the same methods used for tracking malicious code. This involves an ongoing analysis of reports and data delivered from over 120 million client, server, and gateway email systems deploying Symantec antivirus security solutions, as well as filtration of 25 million email messages per day. Steps for protection against and mitigation of these security risks are presented at the end of the "Spyware and Adware" section.

Adware

Adware programs are those that facilitate the delivery and display of advertising content onto the user's display device.[141] This may be done without the user's prior consent or explicit knowledge. Adware can be downloaded from Web sites (typically bundled with shareware or freeware), email messages, and/or instant messenger systems. Additionally, a user may unknowingly receive and/or trigger adware by accepting an end user license agreement (EULA) from a software program linked to the adware or by visiting a Web site that downloads the adware.

Depending upon its functionality and the context in which it is deployed, adware can constitute a security risk. In some cases, these programs may gather data from the user's computer, including information related to Internet browser usage or other computing habits, and relay this information back to a remote computer. It may also do so by occupying bandwidth, thereby diminishing the functionality and availability of a computing system.

Top ten reported adware

Between July 1 and December 31, 2005, the most commonly reported adware program was Websearch,[142] which accounted for 19.1% of the top ten adware programs reported (table 10). This program was not present in the top ten adware programs in the first six months of the year.

This program features a number of noteworthy attributes. It modifies Internet Explorer's default home page and search settings, it installs itself as a toolbar to Internet Explorer, and it adds a number of icons to the system tray. This could result in unwanted applications being installed on the system, which could consume system resources. It could also result in the user's browser being redirected to potentially malicious Internet sites.

[141] Typically a monitor, but may be any device including cellular telephone screen or PDA viewer.
[142] http://securityresponse.symantec.com/avcenter/venc/data/adware.websearch.html

Websearch also sends user information to a predetermined Web site, including keywords from searches. One interesting technique that Websearch uses to prevent manual removal of components of the program is a so-called "watchdog process," will be discussed at greater length in the "Anti-removal techniques" section below.

Rank	Risk name
1	Websearch
2	Hotbar
3	BetterInternet
4	Istbar
5	GAIN
6	CDT
7	Aurora
8	Lop
9	BargainBuddy
10	IEPlugin

Table 10. Top ten adware programs
Source: Symantec Corporation

Over the last six months of 2005, Hotbarwas the second most frequently reported adware program.[143] It made up 18.5% of the top ten adware programs. Hotbar is a new entry to the top ten reported adware. First detected in 2003, it adds graphical skins to Internet Explorer, Microsoft Outlook, and Outlook Express toolbars.[144] It also adds its own toolbar and search button to Internet Explorer. These custom toolbars have keyword-triggered advertisements built into them. For example, if a user searches for "mortgages," the toolbar will display mortgage-related advertisements and links from Hotbar's advertising affiliates. Hotbar also monitors the user's Web browsing habits for information that may be used for targeted marketing.

BetterInternet was the third most commonly reported adware program in the second half of 2005,[145] making up 15% of the top ten adware programs. It was the seventh most commonly reported adware program in the first half of 2005. BetterInternet is a browser helper object (BHO) that displays advertisements and downloads and installs files onto the compromised computer. It also gathers system information from a compromised computer, which it may send it to a remote third-party computer.[146]

[143] http://securityresponse.symantec.com/avcenter/venc/data/adware.hotbar.html
[144] A skin is an element of a graphical user interface that can be changed to alter the look of the interface without affecting its functionality. Skins can give an interface an entirely different look than what it originally came with. (Webopaedia: http://www.webopedia.com/TERM/s/skin.html)
[145] http://securityresponse.symantec.com/avcenter/venc/data/adware.betterinternet.html
[146] As the information it gathers is system information rather than personally identifiable information, and as its ad-displaying behavior is relatively aggressive, Symantec categorizes this program as adware rather than as spyware.

Top ten adware programs—risk levels

Symantec categorizes adware programs and rates their risk level based on a number of criteria, including the following:

- The degree to which the presence of a security risk affects the compromised computer's performance.
- The level of privacy that is lost due to the presence of the security risk on a computer.
- The difficulty in removing a security risk from a compromised computer.
- The degree to which the security risk is able to obscure its presence on a computer.[147]

In the second half of 2005, three of the top ten reported adware programs were given a low risk rating (table 11). This means that the presence of the adware program had very little effect on the performance of the computer and the privacy of the user. Furthermore, the adware was installed using normal installation methods and was not difficult to remove using standard uninstall procedures.

Risk name	Risk rating
Websearch	Low
Hotbar	Low
BetterInternet	High
Istbar	Medium
GAIN	Low
CDT	Medium
Aurora	Medium
Lop	High
BargainBuddy	Medium
IEPlugin	High

Table 11. Risk ratings of top ten adware
Source: Symantec Corporation

Four of the top ten reported adware programs during this period were given a medium risk rating (table 11). This means that the program had one or more of the following risk factors:

- It affected computer performance by creating pop-up windows, replacing the browser's home page, and/or redirecting Web pages and search results.
- It affected the user's privacy by tracking Web browsing and similar user behavior. Further, it either did not have a privacy policy (in a EULA, for instance), or the privacy policy it had was inconsistent with observed behaviors.
- Once installed, it either did not provide uninstall capability or did not provide the user with uninstall instructions.
- Finally, it obscured its presence on the computer by employing some, but not all, stealth techniques, such as silent install, a lack of user interface, or the concealment of application processes.

[147] For more information on risk levels, please see http://securityresponse.symantec.com/avcenter/enterprise/security_risks/#riskAssessment

Three of the top ten adware programs reported during the last six months of 2005 were rated as high risk (table 11). This means that the program exhibited one or more of the following characteristics:

- It had a significant impact on the system's stability and/or performance.
- It exposed confidential, sensitive information such as account numbers, passwords, or credit card information. It may have also exposed personal identity information, such as social security numbers (or international equivalents).
- It resisted removal or would only facilitate a partial uninstall.
- It exhibited most or all stealth behaviors, such as silent installation, lack of a user interface, and/or the concealment of application processes.

Top ten reported adware—notable characteristics

Different adware programs have different characteristics. These may relate to the ways in which the adware is installed on the user's computer, the ways in which they resist attempts to remove them, and the risks that the adware programs pose to the security of the user's data. The following sections will discuss some of the characteristics that were seen in the top ten adware programs reported in the second half of 2005.

Anti-removal techniques

Adware programs may use numerous different techniques to resist removal from the user's computer. Five of the top ten adware programs anti-removal techniques (table 12). The following paragraphs will describe some of the anti-removal techniques that Symantec has observed over the past six months.

Risk name	Anti-removal
Websearch	Watchdog processes
Hotbar	NA
BetterInternet	NA
Istbar	Exclusive file lock
GAIN	NA
CDT	Adds to list of trusted sites
Aurora	Process injection
Lop	Auto-updates with automatically repacked versions
BargainBuddy	NA
IEPlugin	NA

Table 12. Anti-removal techniques in top ten adware
Source: Symantec Corporation

Watchdog processes may be part of an adware program. They typically monitor each other to prevent easy removal of the program. If one process is stopped, a second process automatically restarts it and *vice versa*. Of the top ten adware programs reported during the last six months of 2005, only Websearch uses watchdog processes to resist removal.

File locking is a technique that adware programmers employ in order to make it difficult for the file to be scanned by antispyware and antivirus applications. File locking restricts access to a file to one user or process. While this is sometimes done by legitimate applications to prevent sharing violations, it is also used by programs to prevents the file from being read or scanned. Such files need to be accessed by a kernel-mode driver in order to be scanned. Of the top ten adware programs reported to Symantec in the second half of 2005, only ISTBar employs file locking.

Some adware programs lower the overall security of the system by surreptitiously adding unauthorized sites to the list of Web sites that have been designated as trusted by the browser. This allows the adware to download content from Web sites for which a user might otherwise be prompted to authorize, such as ActiveX controls. Content from the unauthorized sites may be automatically installed since they are trusted by the browser. This reduces the security of the targeted computer. Of the top ten adware programs of this reporting period, only CDT adds unauthorized sites to the list of trusted zones in Internet Explorer.

Code injection allows a program to maintain stealth while remaining actively running and gives it access to other processes' address space.[148] Should the injected code be poorly written, it can cause system instability and degrade performance. It can also reduce the security of the system on which it is installed.

Code that is injected into a process may bypass measures such as desktop firewalls, allowing it to do such things as download updates to itself or recreate files or registry keys that are deleted by security software that is attempting to remove the program. For example, Aurora injects itself into explorer.exe to make it difficult to remove and to recreate itself on the system should deletion be attempted. If the copy of Aurora on the computer's disk is deleted, it copies itself to the disk again. This can make it very difficult for system administrators or home users to remove these programs by hand without specialized tools or in-depth knowledge. Of the top ten adware programs this period, only Aurora deployed process injection.

Run-time packers are programs that are used to reduce the size of programs so that they require less time to download. A packer may also be used to obscure the content of a file, so that it cannot be easily recognized by antivirus or antispyware programs (unless they understand the packer format). This technique is commonly used by creators of adware and spyware programs as well as malicious code authors. The adware program Lop is dynamically repacked each time it is downloaded, thereby making detection and removal more difficult.

Self-updating

Programs that are used to detect and remove adware programs often do so by using signatures that are based on known characteristics of the adware. Consequently, some adware vendors update their programs in order to evade detection and removal by these signatures. If the software is updated, then signature-based antispyware products are less likely to recognize it and, therefore, may not be able to remove it. In some cases, the functionality of the adware program may also be updated. Table 13 outlines the top ten most frequently updated adware programs reported to Symantec in the second half of 2005.

[148] Code injection means that the code is either copied to part of the memory address space of another process or that the application initialization registry key is modified to point to a DLL to be loaded by all running applications for the Windows session. This ensures that the code runs each time the system is started.

Risk name	Updates per day
Aurora	13.6
BetterInternet	4.4
Istbar	4.1
Lop	3.6
SurfSideKick	1.8
Websearch	1.6
Henbang	1.3
Iefeats-UserAgent	0.9
SAHAgent	0.9
NaughtyPops	0.7

Table 13. Top ten self-updating adware programs
Source: Symantec Corporation

Risk name	Rogue install
Websearch	No
Hotbar	Yes
BetterInternet	Yes
Istbar	Yes
GAIN	Yes
CDT	Yes
Aurora	Yes
Lop	Yes
BargainBuddy	Yes
IEPlugin	Yes

Table 14. Rogue install in top ten adware
Source: Symantec Corporation

Rogue affiliates

Adware companies often pay affiliate companies for each install of their software that the affiliate company facilitates. This is typically done by making the adware program available for download on the affiliate's Web site. However, in some cases, companies will forcibly install adware programs—that is, without the user's consent—on a user's system by taking advantage of vulnerabilities in a user's Web browser.[149] These firms are known as rogue affiliates. During this reporting period, all of the top ten adware programs except Websearch were installed by rogue affiliates in addition to legitimate affiliates (table 14).

It should be noted that this practice may not continue at the same level in the future. In the second half of 2005, some of the larger adware vendors, such as 180Solutions, stated that they would be distancing themselves from so-called rogue affiliates.[150] However, at this point in time, it is difficult to know whether or not this approach will effectively discourage the practice.[151]

Browser helper objects

Browser helper objects (BHOs) are add-on programs that can add legitimate features to a user's browser. For example, document readers that read programs within the browser do so with BHOs. Some BHOs, however, are used for less legitimate purposes, such as monitoring Web browser usage, detecting events, replacing ads, changing home pages, and creating windows to display information. They can also download program updates or log and export confidential data.

This strategy allows for tight integration with Internet Explorer and facilitates close monitoring of a computer user's Web browsing habits. Six of the top ten adware programs reported in the second half of 2005 were BHOs (table 15).

[149] See http://securityresponse.symantec.com/avcenter/venc/data/download.ject.html, for example.
[150] See http://www.180solutions.com/Press/ReadArticle.aspx?id=30 and http://www.theregister.co.uk/2005/08/16/180_sues_bad_actors/, for example.
[151] See http://blogs.zdnet.com/Spyware/?p=745 and http://blogs.zdnet.com/Spyware/?p=750, for example. http://www.eweek.com/article2/0,1895,1830072,00.asp

Risk name	BHO/Toolbar
Websearch	Yes
Hotbar	Yes
BetterInternet	Yes
Istbar	Yes
GAIN	No
CDT	No
Aurora	No
Lop	Yes
BargainBuddy	Yes
IEPlugin	No

Table 15. BHOs in top ten adware
Source: Symantec Corporation

Risk name	Drive-by download
Websearch	Yes
Hotbar	Yes
BetterInternet	No
Istbar	Yes
GAIN	No
CDT	Yes
Aurora	No
Lop	No
BargainBuddy	Yes
IEPlugin	No

Table 16. Drive-by downloading in top ten adware
Source: Symantec Corporation

Drive-by downloading

Drive-by downloading is the practice of prompting a user to install a program as they browse the Web without the user requesting the installation of the program in the first place. A drive-by download is usually invoked through an automatic Web page refresh or by ActiveX control installers.[152] Five of the top ten adware programs reported in the first half of 2005 are known to have been installed by drive-by download (table 16)

To reduce the risk from adware that is installed through a Web browser, users should consider disabling ActiveX. It is important to note, however, that doing so may also affect the functionality of the Web browser and may prevent certain Web sites and pages from rendering correctly. Some users and applications may require ActiveX, in which case browsers should be configured to require a prompt for ActiveX controls to execute. If the browser presents a dialogue box that is not expected, the user should not click anywhere on the dialogue box. Instead, they should close the browser window immediately.

Spyware

Spyware programs are stand-alone programs that have the ability to scan systems or monitor activity and relay information to other computers or hold it for subsequent retrieval. The data that may be monitored by spyware programs can include, but is not limited to, passwords, log-in details, account numbers, personal information, individual files and/or other personal documents. This can be done through keystroke logging and/or by capturing email and instant messaging traffic.

Spyware may also gather and distribute information related to the user's computer, applications running on the computer, or Internet browser usage. Some spyware applications may be used to monitor user behavior. For example, they may be utilized by corporations to monitor employee Internet usage or by parents to monitor their children's Internet usage. Spyware is a particular concern because of its potential use in identity theft and fraud.

[152] For more information on ActiveX, please visit: http://msdn.microsoft.com/library/default.asp?url=/workshop/components/activex/intro.asp

End users may unknowingly download spyware programs from Web sites (typically in shareware or freeware), email messages, and instant messaging programs. In some cases, the user may unknowingly receive and/or trigger spyware by accepting an end-user license agreement (EULA) from a software program linked to the spyware or by visiting a Web site that downloads the spyware.

It is worth noting that only seven of the top 100 security risk programs reported to Symantec are spyware programs. This may be because many of the programs that steal confidential information and/or that are used in phishing scams are considered by Symantec to be malicious code.[153]

Top ten reported spyware

Over the last six months of 2005, CometCursor[154] was the most commonly reported spyware program, accounting for 42% of the top ten spyware programs reported during this period (table 17). First detected in September 2004, it was the fourth most reported spyware program in the first half of 2005. CometCursor is an Internet Explorer BHO. It installs a toolbar that has links to affiliate Web sites. CometCursor can be bundled with various programs or downloaded from a Web page using an ActiveX installer. It installs a search bar and logs Web browsing activity from the machine on which it is installed. It also gathers the MAC address of the computer on which it is installed and conveys the information back to a remote computer.

Rank	Risk name
1	CometCursor
2	Apropos
3	Marketscore
4	ISearch
5	e2give
6	ActivMonAgent
7	QuickSearch
8	Shopnav
9	Goidr
10	Perfect

Table 17. Top ten spyware programs
Source: Symantec Corporation

Apropos was the second most reported spyware program over the last six months of 2005.[155] It made up 25% of the top ten spyware reports. It was also ranked second in the first half of the year and third in the second half of 2004. An Internet Explorer BHO that is installed via an ActiveX control, Apropos installs a toolbar that links to Web sites and sends information back to its server. This information could include Web search keywords, Web sites visited by the user, software installed on the user's computer, and the IP

[153] http://securityresponse.symantec.com/avcenter/enterprise/security_risks/
[154] http://securityresponse.symantec.com/avcenter/venc/data/spyware.cometcursor.html
[155] http://securityresponse.symantec.com/avcenter/venc/data/spyware.apropos.html

address and computer name of the compromised computer. Generally speaking, the main purpose of this spyware application is to create a profile of the user in order to facilitate delivery of customized advertisements.

Additionally, the application may download and install other files on the user's computer. These files could include adware, spyware, or some sort of malicious code, depending on the wishes of the author or vendor. In some cases, these files may contain functionality that the user consented to in the original EULA; however, in other cases they may contain functionality to which the user has not consented.

The third most reported spyware program in the second half of 2005 was Marketscore.[156] It is a new addition to the top ten, making up nine percent of the top ten reported spyware programs. When Marketscore is installed on a computer it starts a proxy service called OSSProxy. Once this service has executed, all the systems' Internet connections will be routed through the proxy. Subsequently, all traffic transmitted through the proxy can be read by Marketscore, including potentially sensitive information that would normally go over SSL/TLS connections.[157]

Even though Marketscore was the third most commonly reported spyware program this period, it is no longer available for download. Despite this, users are still discovering old installations of it on their computers when they install security software and/or update their definitions.

Adware and spyware—prevention and mitigation

In order to protect against security risks such as adware and spyware, Symantec recommends that all users continue to update their antivirus software regularly. Security administrators and end users should also take extra measures to ensure that patch levels on all computers are up-to-date. Symantec also recommends that users and administrators employ defense in-depth, including the use of a properly configured firewall, regularly updated antivirus software and an intrusion detection system. Finally, Symantec advises users to exercise caution when installing any software through a Web browser and to not download any software from sources that are not known and trusted.

As was established in the preceding discussion, some spyware and adware programs are installed using ActiveX controls. Symantec recommends disabling ActiveX. However, as was also stated earlier, some users and applications may require ActiveX, in which case browsers should be configured to prompt a user before allowing the ActiveX controls to execute.

Symantec recommends that organizations develop, implement, and enforce acceptable usage policies. System administrators should regularly audit the system to ensure that no unauthorized software is installed or operating on the system. Furthermore, administrators and end users should read the EULAs of all software programs before agreeing to their conditions.

One final note of caution should be raised. Symantec recommends that users exercise caution when removing spyware. Programs should be removed as non-intrusively as possible in order to minimize any problems that might result from the removal of the program. In order to avoid such problems, it may be necessary to ignore some non-critical aspects of these programs, such as benign registry keys left behind during the uninstall process, as these keys may be necessary for other programs to run.

[156] http://securityresponse.symantec.com/avcenter/venc/data/spyware.marketscore.html
[157] SSL (Secure Sockets Layer) and TLS (Transport Layer Security) are both protocols that use encryption for the secure for transmission of documents over the Internet.

Phishing

Phishing is an attempt by a third party to solicit confidential information from an individual, group, or organization, often 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 Symantec *Internet Security Threat Report* looks at phishing activity that Symantec detected between July 1 and December 31, 2005.

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 network encompasses more than 600 participating enterprises around the world. It attracts email samples that are representative of traffic that would be received by over 250 million mailboxes. It consists of previously used email addresses as well as email accounts that have been generated solely to be used as probes. The main purpose of the network is to attract spam, phishing, viruses, and other email-borne threats.

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 message, or lure, can be used many times in phishing attacks.

A phishing attempt, on the other hand, can be defined as an instance of a phishing message being sent to a single user. An attempt may consist of one or more different unique phishing messages being sent to the same target. 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.

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.

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

- Six-month volume of phishing messages
- Number of blocked phishing attempts
- Phishing as a percent of email scanned

Six-month volume of phishing messages

The number of phishing messages is determined by tracking the number of unique messages that appear in each batch of messages that the Symantec Probe Network classifies as a phishing attempt. Over the last six months of 2005, the Symantec Probe Network detected 86,906 unique phishing messages (figure 29). This is a decrease of 11% from the 97,592 unique phishing messages that were detected in the first half of 2005.

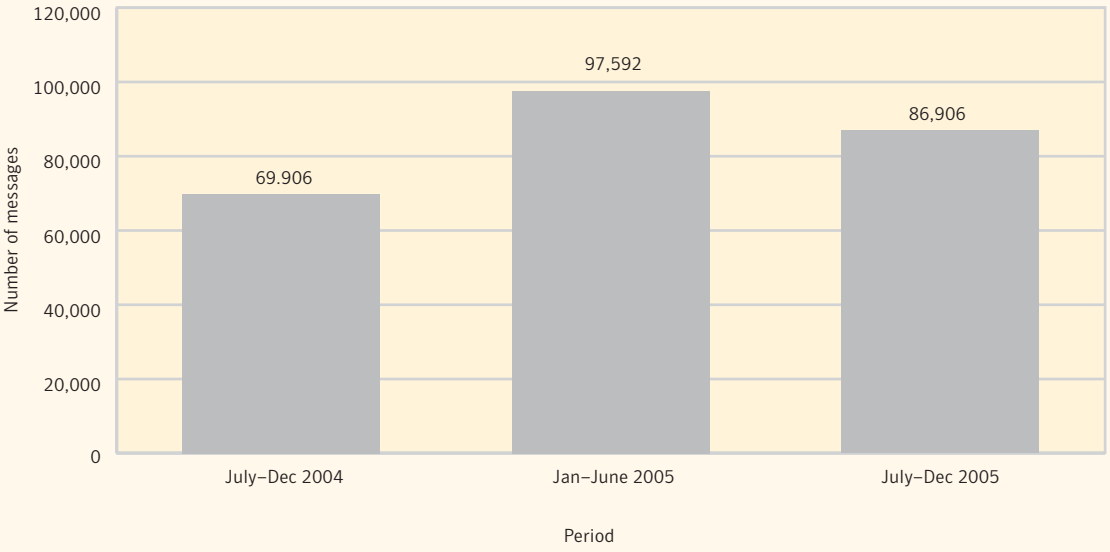

Figure 29. Number of unique phishing messages
Source: Symantec Corporation

Part of this decrease may be due to changes in the data-gathering methods that were used for this report. As stated in the previous *Internet Security Threat Report,* phishers continue to utilize highly randomized phishing attacks in which several sections of email messages, such as the subject line or the domain, are rapidly changed in an attempt to avoid filtering. In order to counter this strategy, during this reporting period, Symantec realigned the low-level heuristics that are used in the first step of phishing discovery. As a result, the number of entities that are actively searched for was reduced by over 25% in an attempt to fine tune sensor performance. This does not mean that phishing attempts for these entities were no longer seen. Rather, it is reflective of the fact that the means by which Symantec detected those attacks was made more focused, so that the results of that search were more meaningful.

More importantly, this should not be interpreted to mean that phishing activity has decreased. For example, in the first half of 2005, it was 40% higher than the second half of 2004. Instead, the change has resulted in a new baseline against which to measure future activity. Symantec's belief that phishing continues to be an area of growth is supported by the data provided in the following two sections of this report.

Blocked phishing attempts

The number of blocked phishing attempts is derived from the total number of phishing messages sent to users that Symantec Brightmail AntiSpam antifraud filters block. Antifraud filters are rules that are created by Symantec Security Response that detect and block known phishing messages. Once the filters have been created they are deployed across the Symantec Brightmail AntiSpam customer base where they prohibit known phishing email messages from reaching end users.

The number of phishing attempts blocked by Symantec Brightmail AntiSpam in the last six months of 2005 indicates a continuation of the increasing phishing activity noted in the previous reporting period (figure 30). In the last half of 2005, Symantec blocked 1.5 billion phishing attempts, a 44% increase over the 1.04 billion phishing attempts detected in the first six months of 2005. It is also a 175% increase over the 546 million blocked phishing attempts detected in the last six months of 2004.

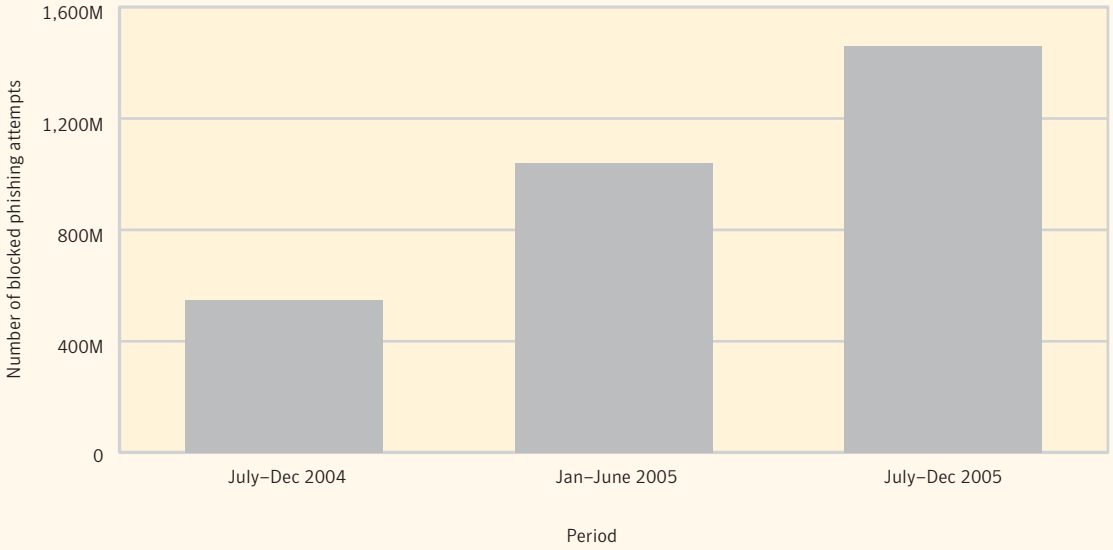

Figure 30. Blocked phishing attempts
Source: Symantec Corporation

Phishing messages that are blocked at the mail servers of Symantec Brightmail AntiSpam customers are reflective of phishing activity targeting email users globally. As a result, Symantec believes that the increase in blocked messages is indicative of a continued growth in phishing activity. Phishing likely continues to increase for three basic reasons: it is relatively easy to perform, it is often effective, and it can be profitable.

Phishing as a percent of email scanned

Symantec calculates phishing attempts as a percentage of the total email scanned by dividing the total number of email messages that trigger antifraud filters by the number of email messages that the Symantec Brightmail AntiSpam solution receives and assesses. These filters are distributed across the Symantec customer base.

Between July 1 and December 31, 2005, phishing attempts made up 0.84% of the email messages processed, or an average of 7.92 million phishing attempts per day (figure 31). This is an increase over the first six months of 2005 when 0.77% of the messages processed were phishing messages, which equated

to 5.70 million phishing attempts per day. In terms of proportions, the percentage of emails that were phishing messages was nine percent higher in the second half of 2005 than the first half. Peak activity during the current reporting period exceeded 17 million phishing attempts per day.

While 0.84% may not appear to be a significant number, it means that roughly one out of every 119 email messages scanned was found to be a phishing attempt. This is an increase from the roughly one out of every 125 email messages that constituted phishing attempts in the first half of 2005.

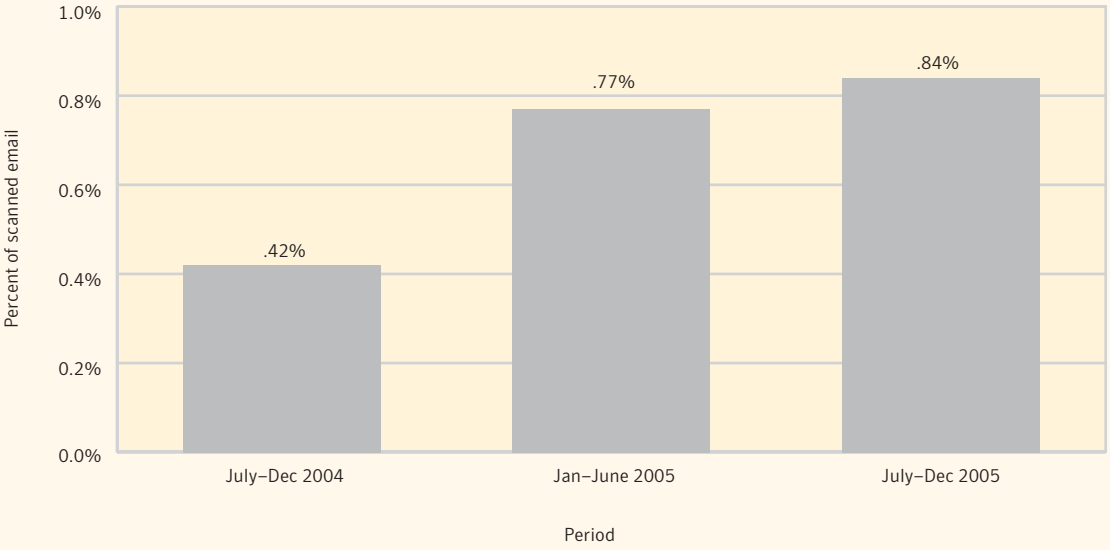

Figure 31. Phishing as a percentage of email scanned
Source: Symantec Corporation

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. Symantec also recommends that organizations use domain-level or email authentication in order to verify the actual origin of an email message. This can protect against phishers who are spoofing mail domains.[158]

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.[159] They should also keep their employees notified of the latest phishing attacks and how to avoid falling victim to them.[160]

[158] 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.
[159] 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/conline/pubs/alerts/phishingalrt.htm
[160] A good resource for information on the latest phishing threats can be found at http://www.antiphishing.org

Organizations can also employ Web server log monitoring to track if and when complete downloads of their Web sites 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. Organizations can detect phishing attacks that use spoofing by monitoring non-deliverable email addresses or bounced email 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.[161] This can be done with the help of companies that specialize in domain monitoring; some registrars even provide this service.[162]

End users should also follow best security practices. 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 the request 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.[163]

Spam

Spam is usually defined as junk or unsolicited email from 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. This section of the *Internet Security Threat Report* will discuss developments in spam activity between July 1 and December 31, 2005.

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 normalization allows for a more accurate representation of data, removing extremely small data samples (that is, smaller customers and test servers).

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 *Internet Security Threat Report* will explore the following:

- Spam as a percentage of all email
- Spam categories
- Top ten countries of spam origin

[161] "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.
[162] See http://markmonitor.com/brandmanagement/index.html for instance.
[163] The IFCC (http://www.ifccfbi.gov/) is a partnership between the FBI and the National White Collar Crime Center:

Spam as a percentage of all email

Symantec calculates the percentage of email that is spam by dividing the total number of emails that are identified as spam by Symantec Brightmail AntiSpam filters by the total of the inbound email messages received by the sample customer base. Between July 1 and December 31, 2005, spam made up 50% of all monitored email traffic. This is a decrease from the first six months of 2005 when 61% of email was classified as spam. It is also lower than the second half of 2004, when just over 60% of email was classified as spam.

While the six-month average remains above 50%, analysis of the month-to-month spam data reveals a decline in the percentage of email that was determined to be spam between July 1 and December 31, 2005 (figure 32). In July, 54% of email was categorized as spam. By the end of December, this number had declined to 50%, a decrease of seven percent over the six-month period.

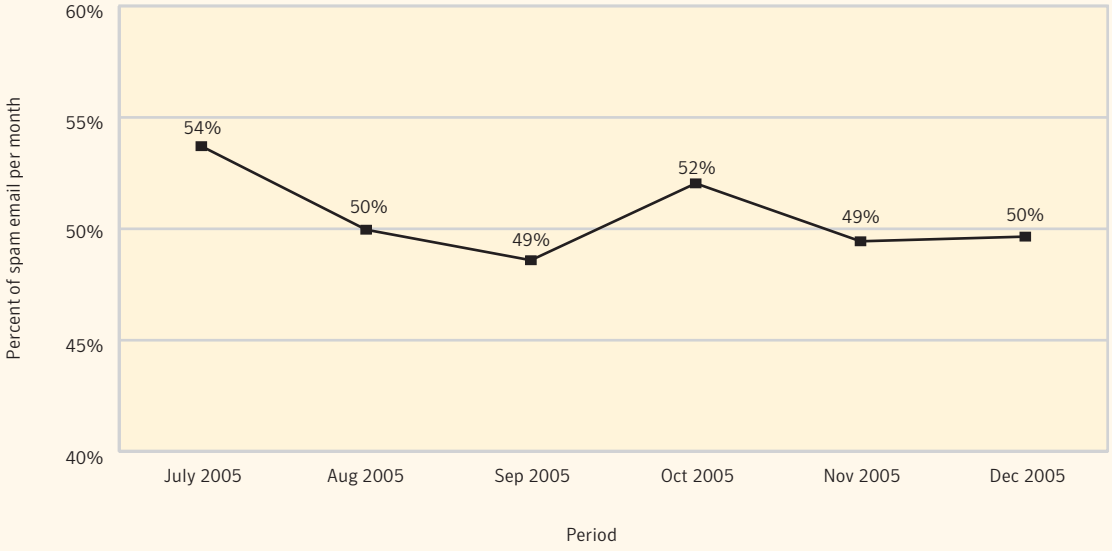

Figure 32. Spam as percentage of email
Source: Symantec Corporation

This does not necessarily signify any decrease in attempts to send spam to Internet email users. Rather, this decline is likely due to the fact that network and security administrators are using IP filtering and traffic shaping to control spam. If a message is blocked using these methods, it will not be detected by the Probe Network and will thus not contribute to statistics gathered. This could contribute to the decrease in detected spam activity over the past six months.

Policy changes made by ISPs may be another factor contributing to the decrease in detected spam. Given the large numbers of spam that have historically originated from compromised ISP accounts, many ISPs have been working with their vendors to implement measures to filter their outbound email traffic. Most

ISPs are thus changing their policies to prohibit their users from sending email directly to the Internet. This prevents users—or, more importantly, Trojans that have been installed on the user's computer—from bypassing the ISP's outbound mail servers and allows the ISP to prevent potential spam from being sent.

Given the large numbers of spam that have historically originated from compromised ISP accounts, many ISPs have been working with their vendors to implement measures to filter their outbound email traffic. The decline in the amount of spam detected over the last six months may be partly because of the success of IP-filtering and traffic shaping in limiting spam. It may also be due to the development of DNS block lists.

Top spam categories

For the first time, in this volume of the *Internet Security Threat Report,* Symantec will assess the most common categories of spam detected on the Internet during the six-month reporting period. The spam categories are assigned by Symantec Email Unit analysts based on spam activity that is detected by the Symantec Probe Network. While some of the categories may overlap, this data provides a general overview of the types of spam that are most commonly seen on the Internet today.

It is important to note that this data is restricted to spam attacks that are detected and processed by the Symantec Probe Network. Internal upstream processing may weed out particular spam attacks, such as those determined to be potential fraud attacks.

The most common type of spam detected in the first six months of 2005 was related to health services and products (figure 33). Health-related spam made up 32% of all spam on the Internet during this time. The next largest spam category was commercial products, which made up 30% of all spam. The next most common type of spam was related to financial products and services. It made up 15% of all spam.

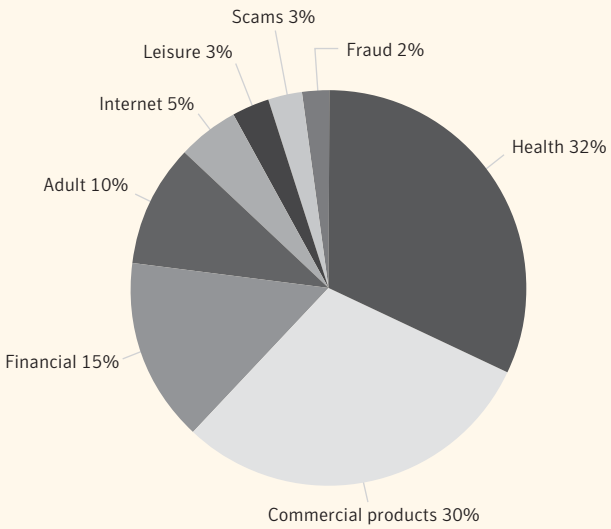

Figure 33. Spam categories
Source: Symantec Corporation

"Adult" spam messages are those that contain pornographic content, sell products of a sexually explicit nature, and/or direct users to a sexually explicit Web site. Adult spam is frequently cited as a concern for organizations because of the need to keep sexually explicit material out of the workplace for legal and human resources concerns. Because of the attention it receives, adult spam is often thought to be the most common type of spam. However, this category has historically only made up around ten percent of all spam.

Although this percentage is low, it should be noted that adult spam has recently made a transition from more sexually explicit, HTML-based graphic content to shorter plain text messages. This is being done to circumvent current detection and prevention methods. It may result in an increase in the amount of sexually explicit spam activity in the near future.

Top ten countries of spam origin

This section will discuss the top ten countries of spam origin. The nature of spam and its distribution on the Internet presents challenges in identifying the location of spammers. Many spammers attempt to redirect attention away from their actual location. In an attempt to bypass block lists, they build coordinated networks of compromised computers known as bot networks, which allow them to send spam from sites that are distant from their physical location (for a more in-depth discussion of bot networks, please refer to the "Attack Trends" report of this *Internet Security Threat Report)*. In doing so, they will likely focus on compromised computers in those regions with the largest bandwidth capabilities. Following this logic, the region from which the spam originates may not correspond with the region in which the spammers are located.

This discussion is based on data gathered and returned by customer installations of Symantec Brightmail AntiSpam. This data includes the originating server's IP address, against which frequency statistics are summarized. Each IP address is mapped to a specific country and charted over time. This limits the number of countries that Symantec monitors for spam origination. For example, if no Symantec customers receive a large volume of email from a particular country, then that country would be less likely to be represented in this metric.

During the last six months of 2005, 56% of all spam detected worldwide originated in the United States (figure 34). This is likely due to the high number of broadband users in that country. The United States was also the top country of spam origin in the first half of 2005, when 51% of spam originated there.

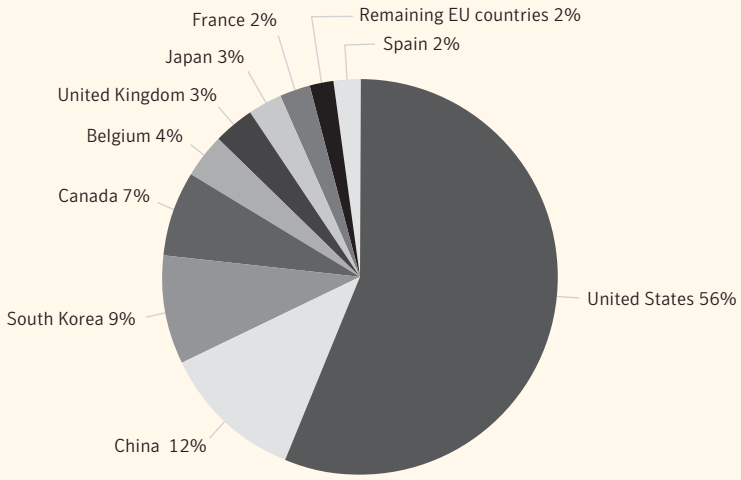

Figure 34. Top ten spam producing countries
Source: Symantec Corporation

During the second half of 2005, China surpassed South Korea as the second highest country of spam origin. Twelve percent of spam during this period originated there, compared to five percent in the first half of the year. Symantec believes that this increase is likely related to the technological, industrial, and political advancements being made in China. Korea followed China in third place. Nine percent of spam originated there during this reporting period.

Country	July–Dec 2005	Jan–June 2005
United States	56%	51%
China	12%	5%
South Korea	9%	14%
Canada	7%	7%
Belgium	4%	3%
United Kingdom	3%	2%
Japan	3%	2%
France	2%	2%
Remaining EU countries	2%	n/a
Spain	2%	1%

Table 18. Top ten countries of spam origin
Source: Symantec Corporation

In the last volume of the *Internet Security Threat Report,* Symantec predicted that the technological advancements of smaller countries would begin to result in higher volumes of spam originating there.[164] Over the past six months evidence has begun to emerge that this is indeed the case. For instance, in the second half of 2005, all of top ten countries outside of the leading four (US, China, South Korea and Canada) experienced an increased share of spam origination (table 18).

[164] Symantec *Internet Security Threat Report*, Volume VIII (September 2005): p. 82

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 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. Enforce an effective password policy.
6. 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.
7. 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.
8. 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.
9. 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.
10. Educate management on security budgeting needs.
11. Test security to ensure that adequate controls are in place.
12. Both spyware and adware can be automatically installed on computers along with file-sharing programs, free downloads, and freeware and shareware versions of software, or by clicking on links and/or attachments in email messages, or via instant messaging clients. Ensure that only applications approved by the organization are deployed on the desktop.

Consumer Best Practices

1. Use an Internet security solution that combines antivirus, firewall, intrusion detection, and vulnerability management for maximum protection against malicious code and other threats.
2. Ensure that security patches are up-to-date and that they are applied to all vulnerable applications in a timely manner.

3. Ensure that passwords are a mix of letters and numbers. Do not use dictionary words. Change passwords often.
4. Never view, open, or execute any email attachment unless the attachment is expected and the purpose of the attachment is known.
5. 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 PC or Macintosh system is vulnerable to threats by using Symantec Security Check at www.symantec.com/securitycheck.
7. All computer users need to know how to recognize computer hoaxes and phishing scams. Hoaxes typically include a bogus email warning to "send this to everyone you know" and/or improper technical jargon that is intended to frighten or mislead users. Phishing scams are much more sophisticated. Often arriving in email, phishing scams appear to come from a legitimate organization and entice users to enter credit card or other confidential information into forms on a Web site designed to look like that of the legitimate organization. Computer users also need to consider who is sending the information and determine if the sender is a trustworthy, reliable source. The best course of action is to simply delete these types of emails.
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. Be aware of the differences between adware and spyware. Adware is often used to gather data for marketing purposes and generally has a valid, benign purpose. Spyware, on the other hand, may be used for malicious purposes, such as identity theft.
10. Both spyware and adware can be automatically installed on a computer along with file-sharing programs, free downloads, and freeware and shareware versions of software, or by clicking on links and/or attachments in e-mail messages, or via instant messaging clients. Therefore, users should be informed and selective about what they install on their computer.
11. Don't just click those "Yes, I accept" buttons on end-user licensing agreements (EULAs). Some spyware and adware applications can be installed after an end user has accept the EULA, or as a consequence of that acceptance. Read EULAs carefully to examine what they mean in terms of privacy. The agreement should clearly explain what the product is doing and provide an uninstaller.
12. Beware 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 and Symantec™ Managed Security Services. Both services refer to attacks in the same way, enabling analysts to combine and analyze attacks together. Symantec combines these two data sources for analysis. In some cases, only one data source is used if attributes required for a particular analysis are not available in the other.

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. The "Top Internet attacks" metric is a good indicator of the overall volume of actual "attack actions" detected over a specified period of time, while the "Attacks per day" metric is a good indicator of the number of attacks observed on a daily basis.

Explanation of research enquiries

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.

Top Internet attacks

Symantec identifies and ranks all the attacks that are detected on networks across the Symantec DeepSight Threat Management System and Symantec Managed Security Services base. This ranking can be seen as representative of the distribution of attacks that an Internet-connected host can expect to observe. Symantec investigates and ranks attacks in three ways. Each approach can give visibility into certain emerging trends. The three ways attacks are tracked and ranked are:

- By the proportion of sensors that detect a given attack.
- By the proportion of attacking IP addresses that perform a given attack.
- By the proportion of aggregate attack volume that is attributable to a given attack.

The proportion of attacking IP addresses that perform a given attack is included in this report, as this gives the best insight into the popularity of the attack.

Top attacked ports

The top port data is gathered solely from the Symantec DeepSight Threat Management System, and represents individual scan attempts from perimeter security devices throughout the world. Not every single port scan can be considered hostile, but port data is often indicative of wide-scale scanning for individual services being targeted for exploitation.

Symantec investigates and ranks targeted ports in three ways. Each approach can give visibility into certain emerging trends. The three ways ports are tracked and ranked are:

- By the proportion of sensors that detect a given attack.
- By the proportion of attacking IP addresses that perform a given attack.
- By the proportion of aggregate attack volume that is attributable to a given attack.

The proportion of attacking IP addresses that perform a given attack is included in this report.

Attack activity per day

Symantec uses a daily attack rate as a rough estimate of the rate of attack activity experienced by networks connected to the Internet. This is used as an indicator of whether the attack rates are rising or falling between reporting periods.

This metric includes all unauthorized access attempts denied at the firewall and the network intrusion detection system level.[165] The number of attacks used for this analysis is the number of attacks that targeted the company that observed the median number of attacks in the sample set. Using the median organization ensures that the daily attack rate is representative of the attack activity across the Internet as a whole. A small number of companies with disproportionately high daily attack rates would cause the mean average to be skewed.

Time to system compromise

Symantec determined the time to system compromise by utilizing data derived from Symantec's honeypot system during the period spanning November 16 – December 31, 2005. Specifically, the average time before a system becomes compromised is calculated as the amount of time between when the computer becomes available on a network until an external connection originating from a malicious application is observed.

In order to accurately evaluate the time to system compromise, Symantec deployed computers running Microsoft Windows 2000, XP, 2003, and two variants of Linux operating systems configured as typical desktop systems and Web server systems with various patching levels.

The desktop configurations were deployed with the default settings for each operating system with the exception of firewall software. As these systems passively wait to be compromised, appropriately configured firewalls would simply not allow any connections to the computer and comparisons between operating systems or patch levels would not be possible. For each Microsoft Windows-based desktop system three levels of patching were maintained: no patching, with the latest service pack, and fully patched, which included up to date patches.

[165] Symantec recognizes that not all attacks are denied at the firewall; however, only those connection attempts that are denied at the firewall (as opposed to those that are permitted) can be treated as attacks.

The Microsoft Windows Web server configurations were deployed with their included version of IIS, DotNetNuke content management software, and MSDE, a version of the Microsoft SQL Server was used to provide database support. The Redhat Enterprise Linux Web server configuration was deployed with Apache, Mod-PHP, MySQL and PHPNuke. All installation default settings were maintained. When third-party installations were performed, the installation instructions identified in the package were used with no additional regard for security. Symantec attempted to simulate computers deployed by a moderately experienced administrator with no significant security knowledge. For each Microsoft Windows-based Web server configuration, three levels of patching were maintained: no patching, with the latest service pack, and fully patched, which included up-to-date patches.

Each of the computers on the honeypot system was deployed within a single ISP. As such, the data in this section should not necessarily be compared to computer systems deployed on other ISPs, or IP ranges, as filtering and ISP policy can significantly affect the time-to-compromise of a system.

Bot networks

Symantec identifies certain scanning patterns and network traffic and cross-references this traffic with rules that define specific coordinated scanning behavior, which would indicate bot network activity. For an originating computer to be flagged as participating in this coordinated scanning, it must fit into that scanning pattern to the exclusion of any other activity. This behavioral matching will not catch every bot network computer, and may identify other malicious code behaving in a coordinated way as a bot network. This behavioral matching will, however, identify many of the most coordinated and aggressive bot-infected computers and ultimately will give insight into the population trends of bot network computers.

Top bot-infected countries

Using the data derived from the “Bot network” discussion of the “Attacks Trends” 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. 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 bot-infected computers.

Denial of service attacks

Although there are numerous methods for carrying out denial of service attacks, Symantec derives this metric by measuring denial of service attacks carried out by flooding a target with SYN requests, 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, causing 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 denial of service attacks observed throughout the reporting period.

SYN flood attacks should not be confused with other types of denial of service attacks. ICMP flooding is another method of carrying out a denial of service attack.[166] This attack is carried out by bombarding a target computer with ICMP messages until it becomes overwhelmed by them, so that it cannot service legitimate requests. ICMP flooding is also employed when carrying out Smurf DoS attacks.[167]

UDP flooding is another popular form of denial of service attack. This type of attack is typically carried out by flooding a target with an excessive number of UDP packets in an attempt to tie up the network resources of the target computer so that it cannot service legitimate requests.

There are other types of denial of service attacks, most of which are based on the exploitation of vulnerabilities in target services. In most cases, sending a malformed message to a target computer hosting a vulnerable service may cause it to crash or freeze, subsequently denying service to legitimate users.

Top originating countries

Symantec identified the national sources of attacks by automatically cross-referencing source 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. Currently, Symantec cross-references source IP addresses of attacks against every country in the world. It is important to note that while Symantec has a reliable process for identifying the source IP address of the host that is directly responsible for launching an attack, it is impossible to verify where the attacker is physically located. It is probable that many of the sources of attack are intermediary systems used to disguise the attacker's true identity and location.

Top targeted industries

For the purposes of the *Internet Security Threat Report,* a targeted attacker is one that is detected attacking at least three companies in a specific industry, to the exclusion of all other industries. Figure 35 represents the industry breakdown of the sensor distribution in the sample set in percentage terms. Industries with less than ten sensors have been excluded from the resulting totals.

The targeted industry attack rate is a measure of the percentage of total attackers that target only organizations in a specific industry. It can indicate which industries are more frequently the targets of focused attacks. This metric may be affected by the overall attack rate experienced by each industry; nevertheless, it provides an indication of the interest that an industry holds for targeted attackers.

[166] Internet Control Message Protocol. ICMP is employed by the TCP/IP stack to handle error and control messages. Its most commonly known functionality, and that exploited by ICMP Flood attacks is the Echo Request, Echo Reply sequence used by ping utilities.
[167] http://securityresponse.symantec.com/avcenter/venc/data/smurf.dos.attack.html

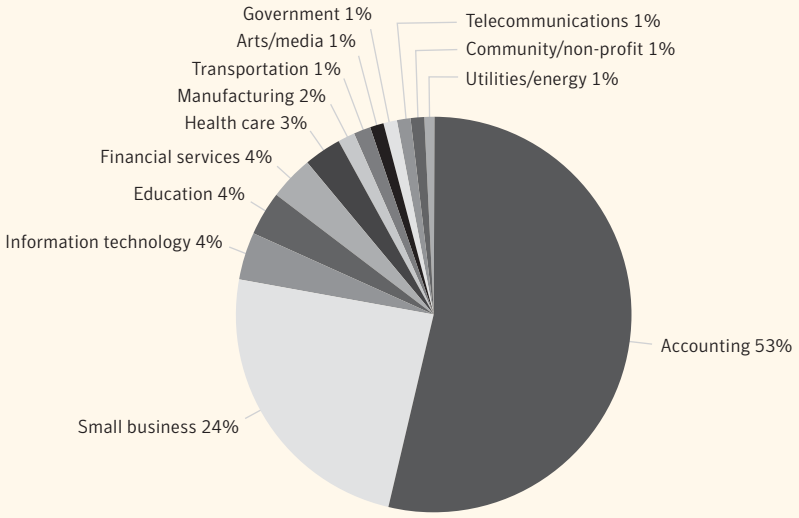

Figure 35. Attack activity by industry
Source: Symantec Corporation

Appendix C—Vulnerability Trends Methodology

The "Vulnerability Trends" report of the Symantec *Internet Security Threat Report* discusses developments in the discovery and exploitation of vulnerabilities over the past six months. 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 16,000 distinct entries. Each distinct entry is created and maintained by Symantec threat analysts who assess the content for accuracy, veracity, and the applicability of its inclusion in the vulnerability database based on available information. The following metrics discussed in the "Vulnerability Trends" report are based on the analysis of that data by Symantec researchers:

- Total number of vulnerabilities disclosed
- Web application vulnerabilities
- Vulnerabilities with exploit code
- Commercialization of vulnerabilities

The ways in 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 a list of affected products. These traits are subsequently used both directly and indirectly for this analysis.

Vulnerability type

After discovering a new vulnerability, Symantec threat analysts classify the vulnerability into one of 12 possible categories based on the available information. These categories focus on defining the core cause of the vulnerability, as opposed to classifying the vulnerability merely by its effect. The classification system is derived from the academic taxonomy presented by Taimur Aslam et al (1996),[168] which defines the 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
- Serialization error

[168] "Use of a Taxonomy of Security Faults" (http://ftp.cerias.purdue.edu/pub/papers/taimur-aslam/aslam-krsul-spaf-taxonomy.pdf)

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

Severity of vulnerabilities

Vulnerability severity is a measure of the degree to which the vulnerability gives an attacker accessibility to the targeted system. It also measures the potential impact that successful exploitation may have for the confidentiality, integrity, and/or availability of the affected system. Symantec analysts calculate a severity score on a scale of one to ten for each newly disclosed vulnerability. The severity score is based on the following factors:

- **Impact**—the relative impact on the affected system if the vulnerability is exploited. For example, if the vulnerability enables the attacker to gain full root access to the system, the vulnerability is classified as "high impact." Vulnerabilities with a higher impact rating contribute to a higher severity score.
- **Remote exploitability**—indicates whether or not the vulnerability can be exploited remotely. Vulnerabilities are classified as remotely exploitable when it is possible to exploit the vulnerability using at least one method from a position external to the system, typically by some type of communication protocol, such as TCP/IP, IPX, or dial-up. Vulnerabilities that are remotely exploitable contribute to a higher severity score.
- **Authentication requirements**—indicates whether the vulnerability can be exploited only after providing some sort of authentication credentials (such as a username and/or password) to the vulnerable system, or whether it is possible to exploit it without supplying any authentication credentials. Vulnerabilities that require no authentication on the part of the attacker contribute to a higher severity score.
- **Availability of the affected system**—rates how accessible the system is to attackers in terms of exploitability. Some vulnerabilities are always exploitable once the attacker has accessed the system. Other vulnerabilities may be dependent on timing, the interaction of other objects or subjects, or be otherwise only circumstantially exploitable. Increased availability of the affected system to attackers will increase the calculated severity.

After gathering information on these four attributes, analysts use a pre-established algorithm to generate a severity score that ranges from one to ten. This system provides for a level of granularity that accounts for various characteristics that are common to all vulnerabilities. The Symantec severity rating system helped to serve as a model for the Common Vulnerability Scoring System (CVSS) standard. For the purposes of this report, vulnerabilities are rated as high, moderate, or low severity based on the scores presented in table 19 below. For the purposes of the *Internet Security Threat Report,* each vulnerability is categorized in one of three severity levels. These levels are:

- **Low severity (0–3)**—vulnerabilities that constitute a minor threat. Attackers cannot exploit the vulnerability across a network and successful exploitation of the vulnerability would not result in a complete compromise of the information stored or transmitted on the system. Low-severity vulnerabilities include non-critical losses of confidentiality (for example, system configuration exposure) or non-critical losses of integrity (for example, local file corruption).

- **Moderate severity (4–6)**—vulnerabilities that result in a partial compromise of the affected system, such as those by which an attacker gains elevated privileges but does not gain complete control of the target system. Moderately severe vulnerabilities include those for which the impact on systems is high but accessibility to attackers is limited. This includes vulnerabilities that require the attacker to have local access to the system or to be authenticated before the system can be exploited.
- **High severity (7–10**)—vulnerabilities that result in a compromise of the entire system if exploited. In almost all cases, successful exploitation can result in a complete loss of confidentiality, integrity, and availability of data stored on or transmitted across the system. High-severity vulnerabilities will allow attackers access across a network without authentication.

Severity level	Severity score range
High	$X \geq 7$
Moderate	$4 \leq X \leq 6$
Low	$X \leq 3$

Table 19. Vulnerability severity range

Ease of exploitation

The ease of exploitation metric indicates how easily vulnerabilities can be exploited. The vulnerability analyst assigns the ease of exploitation rating after thoroughly researching the need for and availability of exploit code for the vulnerability. All vulnerabilities are classified into one of three possible categories, listed below:

- **Exploit code available**—exploit code to enable the exploitation of the vulnerability is publicly available to all would-be attackers.
- **No exploit code required**—would-be attackers can exploit the vulnerability without having to use any form of exploit code. In other words, the attacker does not need to create or use complex scripts or tools to exploit the vulnerability.
- **No exploit code available**—would-be attackers must use exploit code to make use of the vulnerability; however, no such exploit code is publicly available.

For the purposes of this report, the first two types of vulnerabilities are considered “easily exploitable” because the attacker requires only limited sophistication to make use of it. The last type of vulnerability is considered “difficult to exploit” because the attacker must develop his/her own exploit code to make use of the vulnerability.

Exploit code development time

The ability to measure exploit code development time is limited and applies only to vulnerabilities that would normally require exploit code. Therefore, the metric is based on vulnerabilities that Symantec considers to be of sufficient complexity,[169] and that did not have functional exploit code until it was created by a third party. This consideration excludes the following:

- Vulnerabilities that do not require exploit code
- Vulnerabilities with associated exploit code published by the discoverer of the vulnerability
- Vulnerabilities associated with non-functional proof-of-concept code

The date of vulnerability disclosure is based on the date of the first reference found (such as a mailing list post). The date of exploit code publication is the date of the first reference to the exploit code found.

The time lapse between the disclosure of a vulnerability and appearance of exploit code for each applicable vulnerability is determined and computed into a monthly average.

Vulnerability Commercialization

This metric is determined by quantifying the number of vulnerabilities that were disclosed by commercial entities that are involved in the practice of acquiring vulnerability information. As some entities maintain staff to conduct their own vulnerability research, only information regarding those vulnerabilities that were discovered by a party that is known to be independent of the commercial entity are included in the data.

Patch development and availability time

The discussion is based on analysis of the patch and vulnerability data in the Symantec vulnerability database and is intended to assess the average time between the public disclosure date of a vulnerability and the release of an associated patch by the affected vendor. This time lapse is referred to as the "time to patch." The disclosure date of each vulnerability is stored in the vulnerability database, as is the release date of each patch by the vendor.

The time-to-patch metric measures the time lapse between the disclosure date of a vulnerability and the release date of an associated patch by the vendor. Only those patches that are independent objects (such as fixes, upgrades, etc.) can be included. Other remediation solutions—such as workaround steps, for instance—are excluded.

Because of the large number of vendors with technologies that have a very low deployment (these form the majority), only fixes for technologies from enterprise vendors are included. Those vendors are:

- Microsoft
- Sun™
- HP®
- Symantec/VERITAS

[169] Memory corruption vulnerabilities. This includes buffer overflows, integer handling errors, format string vulnerabilities, and others which result in a corruption of system memory.

- EMC®
- IBM®
- Cisco®
- Oracle®

For each individual patch from these vendors, the time lapse between the patch release date and the publishing date of the vulnerability is computed. An average from the aggregate of these is computed for each period.

Web browser vulnerabilities

This metric will offer a comparison of vulnerability data for numerous browsers, namely: Microsoft Internet Explorer, Mozilla Firefox, Opera, Safari and KDE Konqueror. However, in assessing the comparative data, the following important caveats should be kept in mind before making any conclusions:

- The total number of vulnerabilities in the aforementioned browsers were computed for this report. This includes vulnerabilities that have been confirmed by the vendor and those that are not vendor confirmed. This version of the *Internet Security Threat Report* differs from the previous version in that vulnerabilities that are not confirmed are also included in the data. These vulnerabilities were found to be statistically significant, especially given the disparity in patch times between vendors.
- Individual browser vulnerabilities are notoriously difficult to pinpoint and identify precisely. A reported attack may be a combination of several conditions, each of which could be considered a vulnerability in its own right. This may distort the total vulnerability count. Some browser issues have also been improperly identified as operating system vulnerabilities or vice versa. This is, in part, due to increasing operating system integration that makes it difficult to correctly identify the affected component in many cases. Many vulnerabilities in shared operating system components can potentially be exposed to attacks through the browser. This report, where sufficient information is available to make the distinct, enumerates only those vulnerabilities that are known to affect the browser itself.
- Not every vulnerability that is discovered is exploited. As of this writing, there has been no widespread exploitation of any browser except Microsoft Internet Explorer. This is expected to change as other browsers become more popular.

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 forms 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, 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 *Internet Security Threat Report* to the next.

Appendix E—Additional Security Risks Methodology

Symantec products not only help users to protect their data from the threat of viruses, worms, and Trojan horses, but also to evaluate potential security risks from the introduction of other programs as well. Symantec AntiVirus classifies these other programs as additional security risks. Additional security risks include programs that may be categorized, based upon functional criteria, as adware or spyware. Symantec classifies these programs based on a number of characteristics. Once categorized, they can be detected, allowing users to choose whether to keep or remove them based on their personal needs and security policies.

General criteria for additional security risks

A program classified as an additional security risk is an application or software-based executable that is either independent or interdependent on another software program and meets the following criteria:

1. It is considered to be non-viral in nature;
2. It meets criteria for programmatic functionality having potential to affect security;
3. It has been reported to Symantec by a critical number of either corporate or individual users within a given timeframe. The timeframe and number may vary by category or risk.

Symantec further classifies programs based upon functional criteria related to the result of the program's introduction to a computer system. The criteria take into consideration functionality that includes stealth, privacy, performance impact, damage, and removal.

Adware and Spyware

Adware programs are those that facilitate the delivery and display of advertising content onto the user's display device. This may be done without the user's prior consent or explicit knowledge. The advertising is often, but not always, presented in the form of pop-up windows or bars that appear on the screen. In some cases, these programs may gather information from the user's computer, including information related to Internet browser usage or other computing habits, and relay this information back to a remote computer.

Spyware programs are stand-alone programs that can unobtrusively monitor system activity and either relay the information back to another computer or hold it for subsequent retrieval. In some cases, spyware programs may be used by corporations to monitor employee Internet usage or by parents to monitor their children's Internet usage.

Spyware programs can be surreptitiously placed on users' systems in order to gather confidential information such as passwords, login details, and credit card details. This can be done through keystroke logging and by capturing email and instant messaging traffic.

The potential security risks introduced by adware and spyware are discussed according to samples, or individual cases of adware or spyware, reported to Symantec by customers deploying Symantec AntiVirus. While spyware and adware are not categorized as malicious code, Symantec monitors them using many of

the same types of methods used for tracking malicious code development and proliferation. This involves an ongoing analysis of reports and data delivered from over 120 million client, server, and gateway email systems,[170] as well as filtration of 25 million email messages per day. Symantec then compiles the most common reports and analyzes them to determine the appropriate categorization. The discussion of adware and spyware included in the "Additional Security Risks" report is based on Symantec's analysis of these reports.

Phishing

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.

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 attacks. 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 as well as phishing statistics can be separately determined. Symantec Brightmail AntiSpam field data is used to identify general trends in phishing email messages.

Explanation of research enquiries

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.

Six-month growth in phishing messages

Symantec maintains automated systems to identify new potential fraud messages received by the Symantec Probe Network. Messages are grouped into attacks based on similarities in the message bodies and headers. Sample messages are then passed through general fraud heuristics to identify messages as

[170] Systems deploying Symantec antivirus security solutions

potential phishing attempts. Symantec Security Response reviews events that are identified as attacks for the purposes of confirmation and filter development. The Symantec Brightmail Business Intelligence Department reviews phishing attacks in order to develop predictive filters known as Symantec Brightmail AntiSpam Heuristics.

The data presented in this section is based on monthly totals in the number of new unique phishing messages discovered and ruled upon by Symantec Security Response. Security Response addresses only those phishing messages not caught by existing antispam and antifraud filters. Existing filters refer only to those antispam and antifraud filters used across the Symantec Brightmail AntiSpam customer base. Some fraud messages will be captured in the field based upon predictive filters (heuristics); however, not all of Symantec's customers utilize this technology or have upgraded to this technology. Therefore, the messages are still reviewed by Security Response for development of filters that are more widely dispersed.

Blocked phishing attempts

The number of blocked phishing attempts is calculated from the total number of phishing email messages that were blocked in the field by Symantec Brightmail AntiSpam antifraud filters. The data for this section is based on monthly totals.

Phishing as a percent of email scanned

The data for this section is determined by the number of email messages that trigger antifraud filters in the field versus 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.

Spam

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 encompasses 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 as well as phishing statistics can be separately determined. 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.

Sample Set Normalization

Due to the numerous variables influencing a company's spam activity, Symantec focused 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.[171]

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 warranted additional detail.

Spam as a percent of email scanned

The data for this section is determined by the number of email messages that trigger antispam filters in the field versus 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.

Top ten countries of spam origin

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

It should be noted that the location of the computer from which spam is detected being sent is not necessarily the location of the spammer. Spammers can build networks of compromised computers globally and thereby use computers that are geographically separate from their location. Following this logic, the region from which the spam originates may not correspond with the region in which the spammer is located.

[171] Please note that all numbers presented in this discussion have been rounded off to the nearest whole number. As a result, some cumulative percentages may exceed 100%.

About Symantec

Symantec is the world leader in providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information. Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free (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