symantec™

Symantec Internet Security Threat Report

Trends for January 05–June 05

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 VIII, Published September 2005

Symantec Internet Security Threat Report

Contents

Internet Security Threat Report Volume VIII—The Changing Threat Landscape

This edition of the Symantec *Internet Security Threat Report* marks a shift in the threat landscape. Attackers are moving away from large, multipurpose attacks on network perimeters and towards smaller, more focused attacks on client-side targets. The new threat landscape will likely be dominated by emerging threats such as bot networks, customizable modular malicious code, and targeted attacks on Web applications and Web browsers. 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.

This volume of the *Internet Security Threat Report* will offer an overview of threat activity that took place between January 1 and June 30, 2005. This brief summary and the overview that follows will offer a synopsis of the data and trends discussed in the main report. As the new threat landscape emerges, Symantec will continue to monitor and assess threat activity in order to best prepare consumers and enterprises for the complex Internet security issues to come.

Malicious code for profit

During the first six months of 2005, new methods of using malicious code for financial gain were observed with increasing frequency. One example submitted to Symantec during this period was a malicious code program that downloaded adware onto a compromised computer. Each time the program was downloaded, the malicious code author earned a fee. Symantec has also uncovered evidence indicating that bot networks are available for hire. These can be used for malicious purposes, such as extorting money from e-commerce sites by threatening denial of service (DoS) attacks.[1]

Exposure of confidential information

Threats to confidential information can result in significant financial loss, particularly if credit card information or banking details are exposed. These concerns are becoming more worrisome as online shopping and Internet banking continue to increase. Between January 1 and June 30, 2005, malicious code that exposed confidential information represented 74% of the top 50 malicious code samples reported to Symantec, up from 54% the previous six months. The rise in confidential information threats is probably due to the rapid proliferation of bots during this period.

Malicious code variants increase dramatically

Over the first half of 2005, Symantec documented more than 10,866 new Win32 viruses and worms, an increase of 48% over the 7,360 documented in the second half of 2004. It is also an increase of 142% over the 4,496 documented in the first half of 2004. This massive increase in variants is important because each variant represents a new, distinct threat against which administrators must protect their systems and for which antivirus vendors must create a new antivirus definition. This trend is also important because it signifies a shift away from broadly disseminated threats, such as mass-mailing worms, and towards malicious code that is modular and customizable.

---

[1] See http://www.newscientist.com/channel/info-tech/mg18725125.900 and http://www.theregister.co.uk/2004/07/21/cyber_shakedown_taken_down/ for instance.

Bot activity continues to increase

In the first six months of 2005, Symantec identified an average of 10,352 bots per day, up from less than 5,000 per day in December 2004. Symantec believes that the increase in bot activity has driven a corresponding increase in DoS attacks. This may be related to financial motives, as DoS attacks have been reported in extortion attempts. Symantec also observed a dramatic increase in bot variants in the first half of 2005.

Malicious code for mobile devices

Malicious code for mobile devices continued to make headway in the first six months of 2005. In March, the first Multimedia Messaging Service (MMS) worm was discovered. The threats created demonstrate some of the robust capabilities of malicious code for mobile devices despite the fact that the number of threats reported in the wild is still relatively small. This can be expected to change, as platform complexity and connectivity have risen to sufficient levels for a widespread outbreak.

Vulnerability disclosure increases substantially

Between January 1 and June 30, 2005, Symantec documented 1,862 new vulnerabilities. This is the highest number recorded since the *Internet Security Threat Report* began tracking new vulnerabilities in six-month intervals. 49% of these vulnerabilities were classified as high severity. 59% of all vulnerabilities were found in Web application technologies. These vulnerabilities are particularly dangerous because they can allow an attacker to access confidential information from databases without having to compromise any servers.

Mozilla browsers have the most vulnerabilities

During the first half of 2005, 25 vendor confirmed vulnerabilities were disclosed for the Mozilla browsers, the most of any browser. 18 of these were classified as high severity. During the same period, 13 vendor confirmed vulnerabilities were disclosed for Microsoft Internet Explorer, eight of which were high severity.

Six-month growth in phishing and spam

Phishing continued to increase over the first six months of 2005. During this reporting period, Symantec blocked 1.04 billion phishing attacks, compared to 546 million in the last six months of 2004, a 90% increase in messages blocked. This means that between January 1 and June 30, 2005, the volume of phishing messages grew from an average of 2.99 million messages a day to 5.70 million. One out of every 125 email messages scanned by the Symantec Brightmail AntiSpam™ solution was a phishing attempt, an increase of 100% from the last half of 2004. During this period, spam made up over 61% of all email traffic, a slight increase over the second half of 2004.

Exploit development and patch development time

In the second half of 2005, the average time between the disclosure of a vulnerability and the release of an associated exploit was 6.0 days. During the same period, on average, 54 days elapsed between disclosure of a vulnerability and the release of a patch by the vendor. This means that, on average, a period of 48 days existed between the release of an exploit and the release of an associated patch. During this time, systems are either vulnerable or administrators are forced to create their own workarounds to protect against exploitation.

Internet Security Threat Report Highlights

Vulnerability Trend Highlights

- Symantec documented 1,862 new vulnerabilities, the highest number since Symantec started tracking vulnerabilities in six-month increments.

- The time between the disclosure of a vulnerability and the release of an associated exploit was 6.0 days.

- The average patch-release time for the past 6 months was 54 days. This means that, on average, 48 days elapsed between the release of an exploit and the release of an associated patch.

- 97% of vulnerabilities were either moderately or highly severe.

- 73% of reported vulnerabilities this period were classified as easily exploitable.

- 59% of vulnerabilities were associated with Web application technologies.

- 25 vulnerabilities were disclosed for Mozilla browsers and 13 for Microsoft® Internet Explorer.

Attack Trend Highlights

- For the fourth consecutive reporting period, the Microsoft SQL Server Resolution Service Stack Overflow Attack was the most common attack, accounting for 33% of all attacks.

- Symantec sensors detected an average of 57 attacks per day.

- TCP port 445, commonly implemented for Microsoft file and printer sharing, was the most frequently targeted port.

- Symantec identified an average of 10,352 bots per day, up from 4,348 in December 2004.

- On average, the number of DoS attacks grew from 119 to 927 per day, an increase of 679% over the previous reporting period.

- 33% of Internet attacks originated in the United States, up from 30% last period.

- Between January 1 and June 30, 2005, education was the most frequently targeted industry followed by small business.

Internet Security Threat Report **Highlights** *continued*

Malicious Code Trend Highlights

- Symantec documented more than 10, 866 new Win32 virus and worm variants, a 48% increase over the second half of 2004 and a 142% increase of the first half of 2004.

- For the second straight period, Netsky.P was the most reported malicious code sample. Gaobot and Spybot were the second and third most reported, respectively.

- Malicious code that exposes confidential information represented 74% of the top 50 malicious code samples received by Symantec.

- Bot-related malicious code reported to Symantec made up 14% of the top 50 reports.

- 6,361 new variants of Spybot were reported to Symantec, a 48% increase over the 4,288 new variants documented in the second half of 2004.

Additional Security Risks

- Adware made up 8% of the top 50 reported programs, up from 5% in the previous reporting period.

- Eight of the top ten adware programs were installed through Web browsers.

- Six of the top ten spyware programs were bundled with other programs and six were installed through Web browsers

- Of the top ten adware programs reported in the first six months of 2005, five hijacked browsers.

- Messages that constitute phishing attempts increased from an average of 2.99 million per day to approximately 5.70 million messages.

- Spam made up 61% of all email traffic.

- 51% of all spam received worldwide originated in the United States.

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 overview of the current *Internet Security Threat Report* will alert readers to current trends and impending threats. In addition, it will offer recommendations for protection against and mitigation of these concerns. This volume covers the six-month period from January 1 to June 30, 2005.

Symantec has established some of the most comprehensive sources of Internet threat data in the world. Symantec DeepSight™ Threat Management System and Symantec™ Managed Security Services consist of more than 24,000 sensors monitoring network activity in over 180 countries. As well, Symantec gathers malicious code data along with spyware and adware reports from over 120 million client, server, and gateway systems that have deployed Symantec's antivirus products. Symantec also maintains one of the world's largest databases of security vulnerabilities, detailing 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 an unparalleled pool of data with which to identify and analyze emerging trends in Internet security activity.

Symantec calls this combination of capabilities for the collection, analysis, and interpretation of security data the Global Intelligence Network. The Global Intelligence Network supports detailed analysis of emerging threats and early access to unmatched security intelligence that organizations can trust and use to mitigate risks and manage information security.

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 this report, Symantec hopes to provide enterprises and consumers with the information they need to help effectively secure their systems now and in the future.

Malicious code for profit

In the previous volume of the *Internet Security Threat Report*, Symantec stated that malicious code that can be used to generate profit appears to be on the rise.[2] The discussion in that volume focused mainly on the growing use of malicious code to relay bulk unsolicited email (spam) for profit. This trend has continued through the first half of 2005. During this period, 64% of the top 50 malicious code samples reported to Symantec allowed email relaying,[3] compared to 53% in the last six months of 2004 and 37% in the first half of that year.

During the first six months of 2005, new methods of using malicious code for financial gain were observed with increasing frequency. One example is Gpcoder.[4] This Trojan encrypts data files such as documents, spreadsheets, and database files on the compromised computer. It then creates a file in each folder

---

[2] The Symantec *Internet Security Threat Report*, Volume VII (March 2005): p. 59: http://enterprisesecurity.symantec.com/content.cfm?articleid=1539
[3] Email relaying is the practice of sending spam through a compromised computer. Enterprises whose systems are detected sending spam may be placed on a blacklist, a list of email addresses or IP addresses from which spam is known to originate or which spammers are known to utilize. Blacklists can be used to filter out unwanted email, such as spam. Email that is sent by organizations that are placed on a blacklist may be blocked from reaching its destination.
[4] http://securityresponse.symantec.com/avcenter/venc/data/trojan.gpcoder.html

containing information on how the user can obtain a decoder for the files. Reportedly, the user must pay $200 for the decoder software. Malicious code that downloads adware onto a compromised computer may also be used for profit. For example, the Lazar Trojan[5] downloads and installs adware that displays pop-up advertisements in the user's Web browser. The malicious code author receives a fee each time the adware is installed on a computer.

The Symantec DeepSight Threat analyst team has uncovered evidence indicating that bot networks that can be used for malicious purposes are available for hire. In July 2005, in an Internet relay chat (IRC) discussion that the DeepSight team was monitoring, a self-proclaimed bot network owner revealed the size, capacity, and price of a bot network that he was making available. Customized bot binary code was also available for between U.S.$200 and U.S.$300.[6] These communications indicate that it is not uncommon for those who maintain control of these bot networks to provide full or partial access to the compromised systems for a fee.

Symantec believes that financial incentives will motivate malicious code authors to create more malicious code and that it will become stealthier and more selective. Security administrators and consumers should pay special attention to the changing nature of these threats and ensure that their antivirus definitions are up-to-date.

Exposure of confidential information

Threats that expose confidential information on a compromised computer are a concern to all users. These threats may expose system information, sensitive files and documents, and/or cached authentication credentials. Some threats, such as back doors, may give a remote attacker complete control over a compromised computer. 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.[7]

Between January 1 and June 30, 2005, malicious code that exposed confidential information represented 74% of the top 50 malicious code samples reported to Symantec. This is an increase over the previous reporting period, in which 54% of the top 50 samples exposed confidential information, and over the 44% reported in the first half of 2004.

The rise in confidential information threats is primarily due to the proliferation of bots; however, other new threats also contributed to this trend. For example, the Mytob[8] family of mass-mailing worms includes remote access capabilities, which could allow remote attackers access to a compromised system and the data stored on it. During the month of June 2005, 97 variants of Mytob were reported to Symantec. These variants were produced in extremely rapid succession, with numerous new variants being observed in the wild on the same day. Such rapid production of new variants is likely intended to attempt to bypass existing antivirus definitions and, by extension, to overwhelm security administrators trying to keep their systems up-to-date.

[5] http://securityresponse.symantec.com/avcenter/venc/data/trojan.lazar.html
[6] This service is marketed with the claim that because such binaries are unique, they will not be detected by current antivirus definitions. Although it is possible to create a unique binary to avoid detection by existing antivirus definitions, most antivirus products will often be able to identify the threat using a generic definition or a heuristic signature.
[7] http://www.securityfocus.com/news/11219
[8] http://securityresponse.symantec.com/avcenter/venc/data/w32.mytob.db@mm.html

Malicious code variants increase dramatically

The Symantec *Internet Security Threat Report* discusses malicious code in two ways: families and variants. A family is a new, distinct sample of malicious code. For instance, W32.Netsky@mm would have been the founding sample, or the primary source code, of the Netsky 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, 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.

Over the first half of 2005, Symantec documented more than 10,866 new Win32 viruses and worms, an increase of 48% over the 7,360 documented in the second half of 2004 (figure 1). It is also an increase of 142% over the 4,496 documented in the first half of 2004. As of June 30, 2005, the total number of Win32 variants surpassed 28,000.

The massive increase over the past six months is due to the increase of Win32 variants that use and implement bot features—such as remote access through IRC channels and denial of service capabilities— that attackers often use for financial gain.[9] For instance, the bots Spybot,[10] Gaobot,[11] and Randex[12] have risen dramatically because their source code is available to the public, making the creation of variants relatively quick and easy. The number of new variants is all the more remarkable considering that the number of existing families has not changed appreciably over the past four reporting periods.
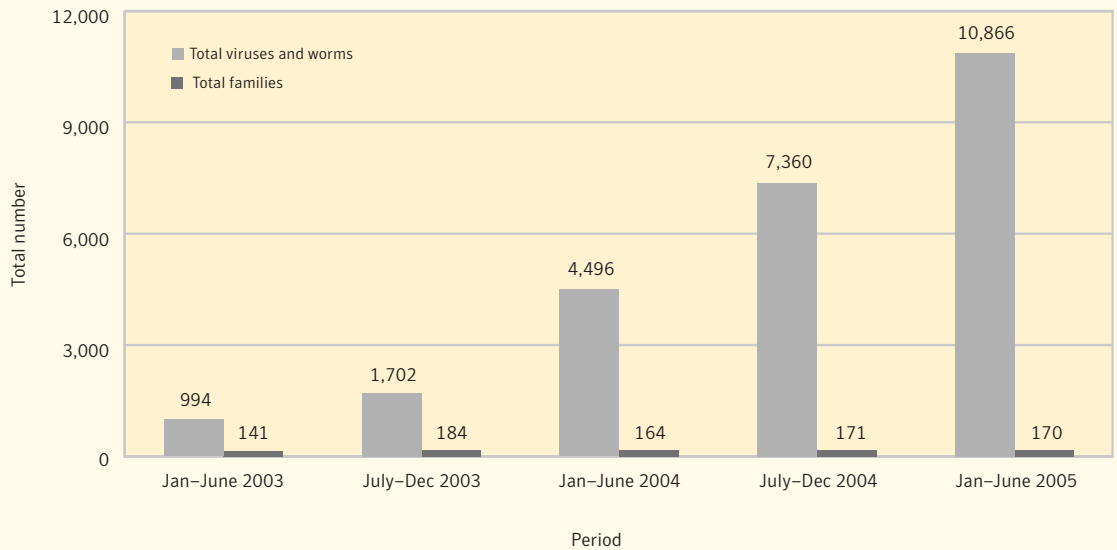

Figure 1. New Win32 virus and worm variants, 2003–2005

 [9] For example, there were 97 variants of the Mytob worm released in the month of June alone. This worm also implements bot features.
 [10] http://securityresponse.symantec.com/avcenter/venc/data/w32.spybot.worm.html
 [11] http://securityresponse.symantec.com/avcenter/venc/data/w32.hllw.gaobot.gen.html
 [12] http://securityresponse.symantec.com/avcenter/venc/data/w32.randex.gen.html

The increase in variants is problematic for organizations because each one represents a new threat against which administrators must secure their systems and for which antivirus providers must develop and provide updates. To protect against the numerous variants, Symantec recommends that best security practices always be followed.

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 types that are required for business needs. Additionally, Symantec recommends that ingress and egress[13] filtering be put in place on perimeter devices to detect anomalous activity.

End users should employ defense in-depth,[14] including 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 the attachment is expected and comes from a trusted source, and the purpose of the attachment is known.

Bot activity continues to increase

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.

In the second half of 2004, the number of bot computers identified by Symantec fell from over 30,000 per day in late July to below 5,000 per day by the end of December. However, in the first six months of 2005 bot network activity experienced a resurgence, increasing to an average of 10,352 bots per day. Symantec believes this increase in bot network activity is due to attacker reaction to vendor patching and other security measures that were put in place in the last half of 2004. It is likely that bot network owners have been required to modify their attack methods in order to maintain viability in the face of these changes.

One of the primary functions of bot networks is to perform DoS attacks. Between January 1 and June 30, 2005, the number of DoS attacks grew by more than 680% to 927 per day on average (figure 2). Symantec believes that this increase in DoS activity is largely due to the corresponding increase in bot network activity.[15] It may be related, at least in part, to financial motivation, as DoS attacks have been reported in extortion attempts.[16] Fortunately, while the number of DoS attacks appears to have increased substantially, large enterprises have not experienced any notable impact from these attempts.

---

[13] 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.
[14] 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.
[15] Regression analysis was performed on the data with the extreme outliers removed. The analysis produced a coefficient of determination of 0.85, meaning that 85% of the variation in DoS attacks can be explained by the linear relationship between bot numbers and DoS attacks. Only 15% of the variation remains unexplained.
[16] See http://www.newscientist.com/channel/info-tech/mg18725125.900 and http://www.theregister.co.uk/2004/07/21/cyber_shakedown_taken_down/ for instance.
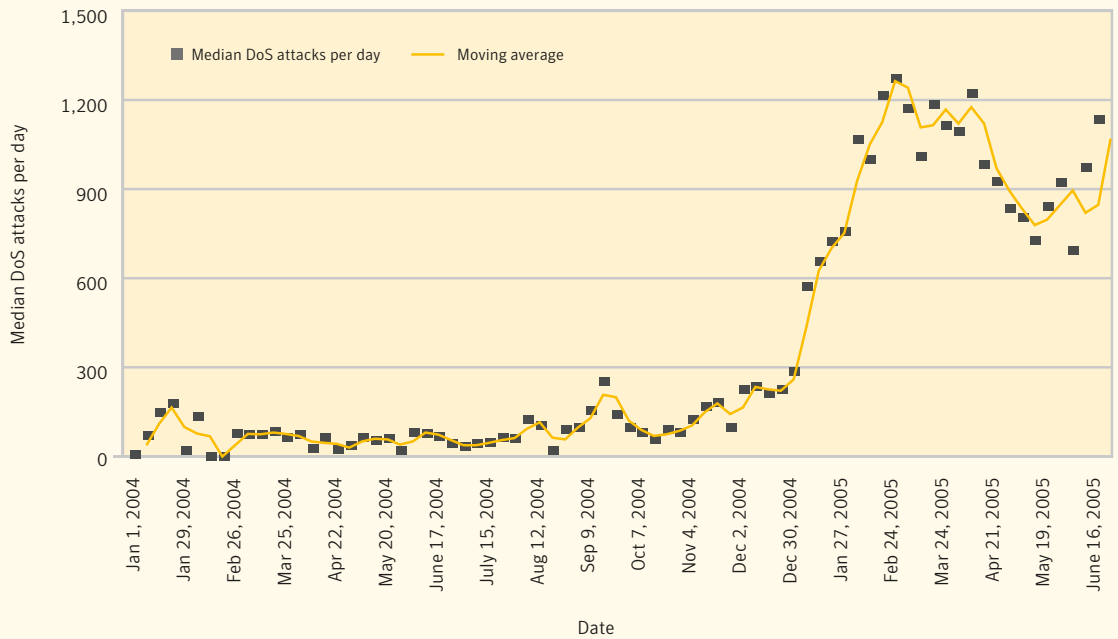
Figure 2. DoS attacks per day
Source: Symantec Corporation

The number of new bot variants continues to climb (figure 3). For instance, in the current period, 6,361 new variants of Spybot were reported to Symantec, a 48% increase over the 4,288 new variants documented in the second half of 2004. While the number of new Gaobot[17] and Randex[18] variants decreased slightly between the first and second half of last year, they rose again in the first half of 2005. During this period, there were 1,412 new Randex variants, an increase of 54%, and 1,121 new Gaobot variants, an increase of 47%. As has been stated previously in this overview, the increase in variants is problematic for organizations because each one represents a new threat against which administrators must secure their systems and for which antivirus providers must develop and provide updates.
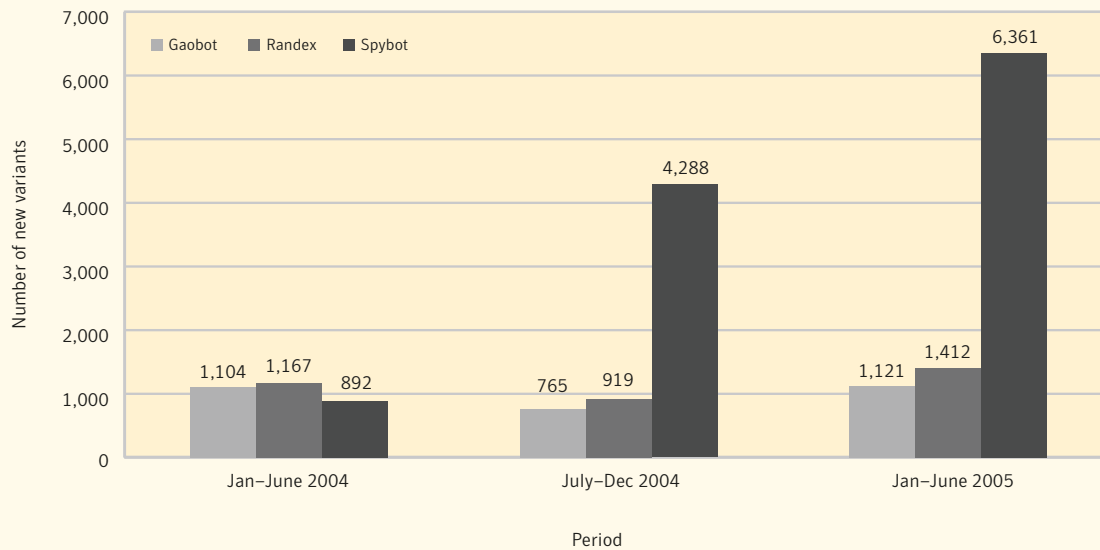
[17] http://securityresponse.symantec.com/avcenter/venc/data/w32.hllw.gaobot.html
[18] http://securityresponse.symantec.com/avcenter/venc/data/w32.randex.gen.html

Figure 3. Number of new bot variants
Source: Symantec Corporation

During the first six months of 2005, the United Kingdom was the country with the highest proportion of bot-infected computers worldwide. 32% of known bot-infected computers were located there. The United Kingdom was also the highest ranked country in the second half of 2004, with 25% of all bot-infected computers situated there. This increase in bot-infected computers is likely due to the rapid growth in broadband Internet that the United Kingdom has experienced.[19]

To help mitigate the risk of bot infection, Symantec recommends that Internet service providers (ISPs) and enterprises perform both ingress and egress filtering, blocking the most common services that are targets for bot network infection, and allowing only those services and IP address ranges that are required for enterprise operations. ISPs should also filter potentially malicious email attachments, as bots are often propagated by malicious code. End users should employ the same methods on home routers and firewalls. Administrators and end users should update antivirus definitions regularly. As compromised computers can be a threat to other systems, Symantec also recommends that enterprises notify their ISP of any malicious activity as part of an incident response plan.

Malicious code for mobile devices

In September 2004, the Symantec *Internet Security Threat Report* predicted that malicious code for mobile devices would become a threat.[20] In the March 2005 volume, Symantec reported that the number of variants of malicious code for mobile devices in the wild had indeed increased.[21] During the current reporting period, malicious code for mobile devices continued to make headway; however, it consisted primarily of proof-of-concept malicious code (and variants thereof) for mobile devices, particularly smart phones.[22]

[19] http://www.point-topic.com/content/dslanalysis/World%20Broadband%20Statistics%20Q1%202005.pdf (access requires registration)
[20] Symantec *Internet Security Threat Report*, Volume VI (September 2004) p. 37: http://enterprisesecurity.symantec.com/content.cfm?articleid=1539
[21] The Symantec Internet Security Threat Report, Volume VII (March 2005) p. 54: http://enterprisesecurity.symantec.com/content.cfm?articleid=1539
[22] Smart phones are mobile phones that contain a full-fledged operating system with a wide variety of user-installable software.

In March, the first MMS worm, Commwarrior,[23] was discovered. While previous malicious code for Symbian devices[24] used only Bluetooth as a propagation vector, Commwarrior also uses MMS. This is significant because Bluetooth requires physical proximity between an infected device and a target in order to propagate. MMS requires only a connection between a phone and the network in order to send messages and files to other phones. This has the potential to expand the scope of an outbreak from the local to the global level.

The first half of 2005 saw a rise in the number of Skulls[25] variants. Skulls is a Trojan that targets the Symbian operating system, likely because it is the most robust operating system for phones. The Trojan overwrites numerous default phone applications, such as the phone book, email viewer, and to-do list. This can render the device inoperable as critical operating system files are also overwritten. Six new variants of Skulls appeared in the first half of 2005, tripling the number of known variants.

While the number of mobile device threats continues to increase, the number reported in the wild is still relatively small. The threats created demonstrate some of the robust capabilities of malicious code for these devices. It is somewhat surprising that no automatically propagating malicious code has yet been developed and released into the wild, particularly as platform complexity and connectivity have risen to sufficient levels for a widespread outbreak.

Vulnerabilities increase substantially

The first half of 2005 was marked by a substantial increase in the number of vulnerabilities disclosed. Between January 1 and June 30, 2005, Symantec documented 1,862 new vulnerabilities. This is the highest number recorded since the *Internet Security Threat Report* began tracking new vulnerabilities in six-month intervals. It is an increase of 31% over the 1,416 new vulnerabilities documented in the last half of 2004. It is also 46% more than the 1,275 new vulnerabilities seen in the same six-month period one year ago. Of these vulnerabilities, Symantec classified 909, or 49% of the total volume, as high severity. This is one percentage point less than the previous six-month period, during which 50% were rated high severity.

Symantec recommends that administrators employ an asset management system and a vulnerability alerting service, which can help to quickly assess whether a new vulnerability is a viable threat or not. Symantec also recommends that enterprises 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 disclosure.

Much of the increase in the total volume of vulnerabilities during this period was due to a substantial rise in Web application vulnerabilities. During the first six months of 2005, 1,100 of all documented vulnerabilities, or 59%, were found in Web application technologies. This is a 59% increase over the 694 Web application vulnerabilities noted in the last six months of 2004 and a 109% increase over the 527 disclosed during first half of that year.

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. As such, they may allow an attacker to bypass

---

[23] http://securityresponse.symantec.com/avcenter/venc/data/symbos.commwarrior.a.html
[24] Devices that use Symbian operating systems include mobile phones, smart phones and other mobile devices from assorted vendors including Nokia, Siemens, Sony, Motorola, Arima and BenQ.
[25] http://securityresponse.symantec.com/avcenter/venc/data/symbos.skulls.html

traditional perimeter security measures, such as firewalls. Having done so, a successful attacker may then compromise an entire network by gaining access through a single vulnerable system. Vulnerabilities in these technologies can also allow an attacker to access confidential information from databases without having to compromise any servers.

Security administrators are urged to follow the best practices outlined in "Appendix A" of this report. Symantec also recommends that administrators audit their systems to ensure that no vulnerable Web applications or scripts are being hosted. They 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.

Mozilla browsers have the most vulnerabilities

The Web browser is a critical and ubiquitous application that has become a frequent target for vulnerability researchers. In the past, the focus of security has been on the perimeter: servers, firewalls, and other systems with external exposure. However, a notable shift has occurred, with client-side systems—primarily end-user systems—becoming increasingly prominent targets of malicious activity. More and more, Web browser vulnerabilities are becoming a preferred entry point into systems.

During the first half of 2005, the Mozilla browsers, including Firefox, had the most vulnerabilities of all browsers. During this period, 25 vendor confirmed Mozilla vulnerabilities were disclosed, compared to 32 in the previous reporting period and two in the first half of 2004. 18 of the 25 Mozilla vulnerabilities in this period, or 72%, were classified as high severity. This is up from the 14 high-severity Mozilla vulnerabilities in the second half of 2004 and one in the first half of 2004.

During the first six months of 2005, 13 vendor confirmed Microsoft Internet Explorer vulnerabilities were disclosed. This is a decrease from the 31 documented in the second half of 2004.[26] During the first half of 2004, seven Internet Explorer vulnerabilities were confirmed by Microsoft.

The average severity rating of the vulnerabilities associated with Internet Explorer during the first six months of 2005 was high. Eight of the 13 Internet Explorer vulnerabilities disclosed during the current period, or 62%, were considered high severity. 18 Internet Explorer vulnerabilities were considered high-severity in the last six months of 2004, amounting to 58%. In the first half of 2004, four of the seven, or 57%, were rated high severity.

[26] It should be noted that in the last *Internet Security Threat Report*, only 13 vulnerabilities associated with Internet Explorer were classified as vendor confirmed. This number has since been revised to 31 post-publication due to delayed confirmation of the vulnerabilities by the vendor

Six-month growth in phishing and spam

In the two previous volumes of the *Internet Security Threat Report*, Symantec identified phishing as an emerging security threat. Phishing is an attempt by a third party to solicit confidential information from an individual, group, or organization, often for financial gain. These attempts are often conducted through a Web browser using social engineering. In many cases, the information gathered is used to commit fraudulent acts.

During this reporting period, Symantec blocked 1.04 billion phishing attempts, compared to over 546 million in the last six months of 2004, a 90% increase in blocked attempts between the two periods (figure 4). This means that between January 1 and June 30, 2005, the volume of phishing messages grew from an average of 2.99 million attempts a day to 5.70 million.
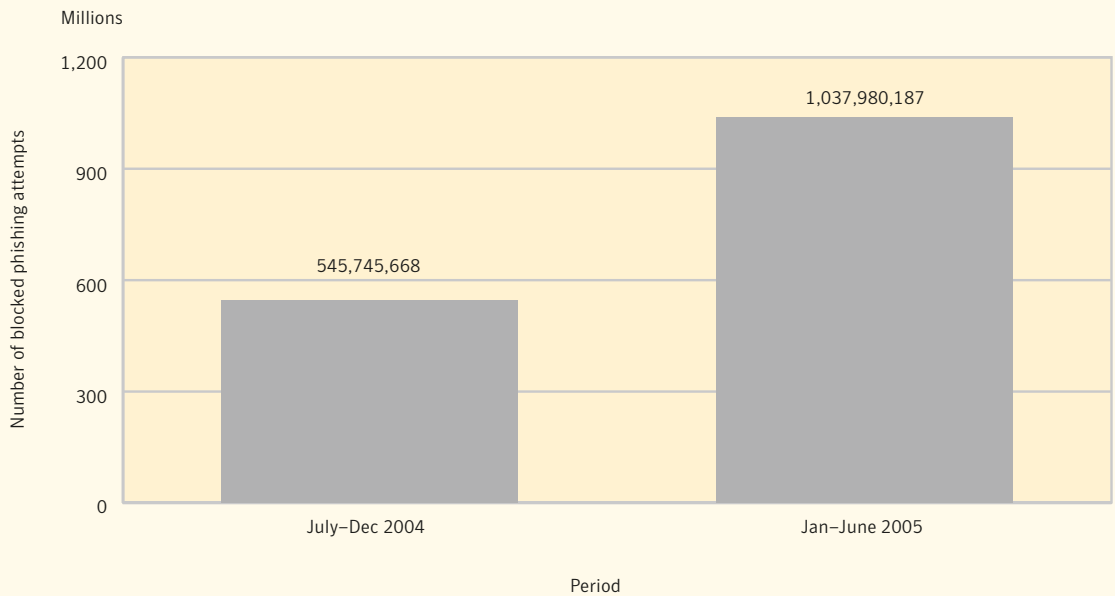
Millions

Figure 4. Blocked phishing attempts, July 2004–June 2005

Between January 1 and June 30, 2005, one out of every 125 email messages scanned was a found to be a phishing email. This is an increase from one out of every 250 email messages in the second half of 2004. In reality, what this means is that if an end user were to receive an average of 25 email messages per day, that user would then be receiving at least one phishing message every week.

Spam is usually defined as junk or unsolicited email from a third party. While it is 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. Furthermore, high volumes of spam can create denial of service conditions in which email systems are so overloaded that legitimate email and network traffic are unable to get through.

During the first six months of 2005, spam made up approximately 61% of all email traffic. This is a slight increase over the last six months of 2004 when just over 60% of email was classified as spam. 51% of all spam received worldwide originated in the United States. To minimize the volume of spam on their networks, Symantec recommends that administrators implement IP filtering and traffic shaping.[27] Symantec also recommends that ISPs employ outbound filtering, which can significantly reduce the distribution of spam from compromised ISP accounts and bot networks. Administrators should consider blocking port 25 except for authorized network users who need to send SMTP mail. They should also consider applying rate-limiting control in order to limit the ability of potential spam relays to send high volumes of email.

All end users should follow best security practices to protect themselves against malicious code infection that could turn their computers into spam relays. End users should also implement antispam technology on their computers.

Patch development time

For the first time, Symantec is including a discussion of the average patch development time in this volume of the *Internet Security Threat Report*. This is intended to assess time between the public disclosure date of a vendor confirmed vulnerability and the release of an associated patch by the affected vendor. This time is very important to system administrators because once a vulnerability is disclosed publicly, it is vulnerable to exploitation until the vendor releases an appropriate patch.

During the first half of 2005, on average, 54 days elapsed between disclosure of a vulnerability and the release of a patch by the vendor (figure 5). This is a slight increase over the 49-day average of the previous period. This ends a two-year trend of decreasing response time. That trend was most likely due to increased pressure from customers for vendors to address security concerns in response to high-profile vulnerabilities and malicious code.

---

[27] 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).
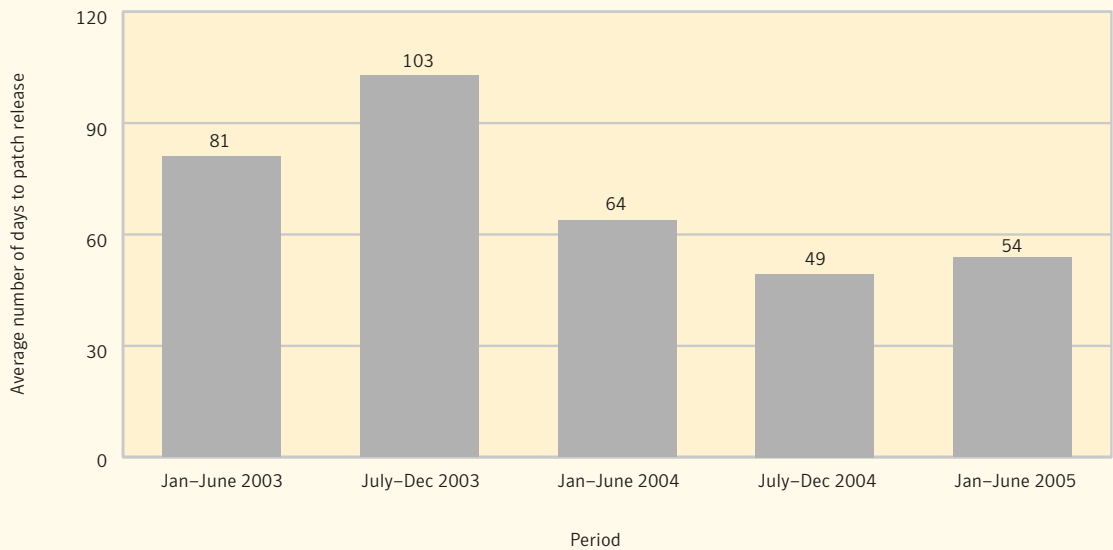
Figure 5. Average number of days to patch release
Source: Symantec Corporation

The 54-day average patch development time combined with the average exploit development time of 6.0 days means that there is an average time lapse of 48 days between the release of an exploit and the release of an associated patch. To minimize the possibility of successful exploitation during this time, administrators need to be aware of and understand the vulnerabilities and be active in working around them. This may involve making changes to firewall configurations, creating intrusion detection system (IDS) and intrusion protection system (IPS) signatures and rules, and locking down services. Administrators should monitor mailing lists devoted to the discussion of security incidents or specific technologies, on which prevention and mitigation strategies may be discussed.

Top adware and spyware programs

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 adware and spyware, and for the past two reporting periods, Symantec has discussed these risks in the *Internet Security Threat Report*.

During the first six months of 2005, adware made up 8% of the top 50 programs reported to Symantec, up from 5% in the previous reporting period. ShopAtHomeAgent, was the most common adware program, accounting for 18% of the top ten adware programs reported. Adware can be installed in a number of ways, including as part of an end user license agreement (EULA) for a third-party program, bundled with other software (usually freeware downloaded from the Internet), or through Web browsers. Eight of the top ten adware programs reported to Symantec in the first six months of 2005 were installed through Web browsers.

Webhancer was the top spyware program during the first six months of 2005, accounting for 29% of the top ten spyware programs reported. Spyware programs are installed in much the same way as adware programs. During this reporting period, six of the top ten spyware programs were delivered by bundling with other programs and six were installed through Web browsers.

Attack Trends

This section of the Symantec *Internet Security Threat Report* will provide an analysis of attack activity for the period between January 1 and June 30, 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 attack activity presented in the two previous *Internet Security Threat Reports*.[28] 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.

Symantec has established some of the most comprehensive sources of Internet attack data in the world. Over 24,000 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[29] that is used to identify, observe, and study complete instances of attacker and malicious code activity. It helps provide details about some of the attack activity identified in this section. 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 heterogeneous data gathering is that malicious code data and attack trends data often address the same activity in different ways. For instance, attack trends data is ranked based on the number of infected sources attempting to spread; on the other hand, malicious code data is based on a number of criteria, including reports of infection. This can lead to different rankings of threats presented in the "Attack Trends" and "Malicious Code" sections of this report.

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

• Top Internet attacks
• Top attacked ports
• Attack activity per day
• Bot networks
• Denial of service attacks
• Top bot-infected countries
• Top originating countries
• Targeted attack activity by industry

---

[28] Symantec *Internet Security Threat Report*, Volume VI (January 1 to June 30, 2004) and Volume VIII (July 1 to December 31, 2004). Both are available at: http://enterprisesecurity.symantec.com/content.cfm?articleid=1539
[29] 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.

Top Internet attacks

For the purposes of this discussion, the top attacks are the most common attacks detected by Symantec Managed Security Services and Symantec DeepSight Threat Management System. They are determined by the percentage of the total attacking IP addresses performing a given attack. These attacks reflect attack 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.

In the first six months of 2005, the top attacks changed considerably from those seen in the second half of 2004 (table 1). Seven of the top attacks for the current reporting period are new to the top ten, suggesting that there has been a major shift in Internet attack activity. Symantec speculates that this change was caused by effective patching and security precautions, such as those implemented by Microsoft® Windows XP Service Pack 2, as well as ingress and egress[30] filtering of known attacks at the router level, especially by Internet service providers (ISPs). These factors have had the effect of reducing the number of computers that are exposed to previously popular and effective attacks. As a result, attackers have been forced to adopt other attacks.

Rank Jan–June 2005	Rank July–Dec 2004	Attack	Percent of attackers Jan–June 2005	Percent of attackers July–Dec 2004
1	1	Microsoft SQL Server Resolution Service Stack Overflow Attack	33%	22%
2	14	Muhammad A. Muquit Count.cgi Attack	7%	1%
3	41	Generic HTTP Chunked Encoding Overflow Attack	4%	<1%
4	11	Generic HTTP Directory Traversal Attack	4%	2%
5	44	Debian Linux HTTPD Attack	4%	<1%
6	8	Generic WebDAV/Source Disclosure HTTP Header Request Attack	3%	2%
7	12	Generic X86 Buffer Overflow (TCP NOPS) Attack	3%	2%
8	16	Generic SMTP Pipe Attack	3%	1%
9	3	Microsoft Windows DCOM RPC Interface Buffer Overrun Attack	3%	7%
10	101	Microsoft RPCSS DCOM Interface Long Filename Heap Corruption Attack	2%	<1%

Table 1. Top Attacks, Jan–June 2005
Source: Symantec Corporation

[30] 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.

The Microsoft SQL Server Resolution Service Stack Overflow Attack was the most common attack between January 1 and June 30, 2005, accounting for 33% of attacking IP addresses. This is up from 22% in the last half of 2004, an increase of 50%. This attack, sometimes referred to as the Slammer Attack because of its initial association with the Slammer worm,[31] has been the most common attack for the past four six-month reporting periods. As discussed in the "Malicious Code Trends" section of this report, two common bots[32]—Gaobot[33] and Spybot[34]—have been known to exploit this vulnerability, which has likely contributed to the frequent detection of this attack.

The continued prominence of this attack can be attributed to a number of other factors as well. The first is that this attack is commonly carried out using a single UDP packet. 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). This may inflate the number of distinct IP addresses that Symantec observes performing the attack. 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.

Another reason for high detection rate of the Microsoft SQL Server Resolution Service Stack Overflow Attack is that 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. Furthermore, this allows a complete attack to be attempted whether SQL Server is running or not, causing most network intrusion detection systems to categorize every attempted attack as a complete attack.

Finally, the success of this attack is aided by the high volume of computers running vulnerable software. The Microsoft Desktop Engine (MSDE) is a variant of the SQL Server engine, which means it is also vulnerable to Slammer or Slammer-related attacks. The MSDE is included in many third-party applications that are widely deployed by organizations. This makes patching this vulnerability across the enterprise very difficult, as each affected software package requires its own patch. Furthermore, this vulnerability will be reintroduced 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.

The Muhammad A. Muquit Count.cgi Attack was the second most common attack during this reporting period. It was performed by 7% of attacking IP addresses between January 1 and June 30, 2005, up from 1% in the last six months of 2004, during which it was not ranked in the top ten attacks. This attack targets a buffer overflow in the Count.cgi Web-based script,[35] which was discovered in 1997.

The third most common attack between January 1 and June 30, 2005 was the Generic HTTP Chunked Encoding Overflow Attack, which accounted for 4% of all attacking IP addresses. This is an increase from less than 1% during the last six months of 2004, during which it was not included in the top ten attacks.

The Muhammad A. Muquit Count.cgi Attack and the Generic HTTP Chunked Encoding Overflow Attack share certain similarities that likely contribute to the increased frequency of both attacks. These similarities include:

• Both attacks target computers hosting Web servers and other Internet services. Compromising computers hosting Web servers may allow an attacker to subsequently carry out attacks against vulnerable Web browsers.

[31] http://securityresponse.symantec.com/avcenter/venc/data/w32.sqlexp.worm.html
[32] 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.
[33] http://securityresponse.symantec.com/avcenter/venc/data/w32.hllw.gaobot.aa.html
[34] http://securityresponse.symantec.com/avcenter/venc/data/w32.spybot.worm.html
[35] http://www.securityfocus.com/bid/128

- Both attacks utilize long-standing, publicly available exploits that can be easily incorporated into existing malicious code, such as bots.[36]

- Complete attacks can be sent to target computers with a single request, allowing an entire attack to be sent to a computer regardless of whether a vulnerable script or Web-server is present. Consequently, most intrusion detection systems will categorize every attempted attack as a complete attack. As a result, many alerts for these attacks will actually be false positives, thereby artificially inflating their frequency.

Despite the potential for high levels of false positives, these two attacks represent a particular danger to organizations. In the past, attackers who gained access to a computer with the privilege level of the Web server application could merely deface a Web site or conduct local privilege escalation attacks against the compromised computer. However, due to the large number of high-profile Web browser vulnerabilities,[37] attackers can now use compromised Web servers to host exploits aimed at Web browsers. This could have a major impact on an organization that has been compromised, as attacks could be launched against the organization's Web-based customers.

Symantec recommends that administrators apply up-to-date patches to all Web server applications and services. This will reduce exposure to the Generic HTTP Chunked Encoding Overflow as well as other Web-based attacks. Symantec also recommends that administrators audit their systems to ensure that no vulnerable Web applications or scripts are being hosted. This will reduce exposure to critical vulnerabilities in Web applications.

Top attacked ports

Assessing the top attacked ports allows security personnel to understand which ports (and associated services) attackers may be paying particular interest to. This discussion is based on data that is derived from firewall sensors that record each rejected or denied connection attempt; therefore, legitimate port activity should not be represented. This metric does not attempt to provide any specific attack information. It reflects only 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. Administrators can use this data to assess which ports and services are most commonly being targeted and configure their systems' security accordingly.

[36] A public exploit for the Muhammad A. Muquit Count.cgi Attack can be viewed at http://www.securityfocus.com/bid/128.
[37] See the "Web browser vulnerabilities" discussion in the "Vulnerability Trends" section of this report.

Symantec Internet Security Threat Report

Rank Jan–June 2005	Rank July–Dec 2004	Port	Service Description	Percent of attackers Jan–June 2005	Percent of attackers July–Dec 2004
1	1	445 TCP	CIFS/SMB (Microsoft Windows File Sharing)	18%	35%
2	2	135 TCP	DCE-RPC (remote Microsoft Windows communication)	13%	17%
3	3	1026 UDP	Various dynamic services	9%	8%
4	12	80 TCP	World Wide Web (HTTP) services	7%	2%
5	13	443 TCP	Secure World Wide Web (HTTPS)	7%	2%
6	10	25 TCP	Simple mail transfer protocol (SMTP) services	6%	2%
7	4	4662 TCP	Edonkey (file sharing)	5%	6%
8	5	1027 UDP	Various dynamic services	4%	5%
9	15	139 TCP	NetBIOS (Microsoft Windows File Sharing)	3%	2%
10	6	6346 TCP	Gnutella (file sharing)	3%	5%

Table 2. Top attacked ports
Source: Symantec Corporation

During the first six months of 2005, TCP port 445 was the most targeted port (table 2). It was targeted by 18% of attacking IP addresses, a considerable drop from the second half of 2004, when it was targeted by 35% of attackers. The prominence of this port is likely due to the fact that it is it is commonly used for Microsoft file and printer sharing. It is also used to implement remote procedure call (RPC) functionality. RPC is used in many widely deployed Microsoft Windows applications, and, as a result, is commonly targeted by attackers. Furthermore, a number of remote vulnerabilities may be exploited through this port.

Thorough analysis of the Symantec honeypot system and DeepSight data has identified Gaobot and Spybot variants as heavy attackers of TCP port 445. Both bots target this port in order to exploit the Microsoft Windows LSASS Buffer Overrun Vulnerability[38] and the Microsoft Windows DCOM RPC Interface Buffer Overflow Vulnerability.[39] Attacks that attempt to gain access to file shares through brute-forced username and password guessing also target this port. Furthermore, all services offered through TCP port 139 can be accessed through this port, further increasing its popularity amongst attackers.

The substantial decrease in attacker interest in this port over the past six months is likely a sign that perimeter controls implemented with firewall rule sets and network intrusion detection signatures, among other measures, have been effective in slowing exploitation attempts. Due to the large number of high-severity vulnerabilities targeting this port, it has become common practice to restrict access to it using firewall rule sets. As a consequence, it is reasonable to assume that the majority of the activity targeting this port is related to port scanning.[40] This theory is substantiated by the fact that attacks targeting vulnerabilities over port 445 have become less common in the top ten Internet attacks over the past six months.

[38] http://www.securityfocus.com/bid/10108
[39] http://www.securityfocus.com/bid/8205
[40] Port scanning is a reconnaissance attack used by attackers to determine whether a port is open prior to attacking it.

Between January 1 and June 30, 2005, TCP port 135 was the second most targeted port. It was targeted by 13% of attackers. It was also the second most targeted port in the second half of 2004, when it was targeted by 17% of attackers. Port 135 is proportionally at its lowest since 2003, when it accounted for 33% of attacking hosts. At that time, both the Welchia[41] and Blaster[42] worms were targeting vulnerabilities in services that are accessible through port 135. The drop-off since 2003 may be partly attributed to the expiry of the Welchia worm, which had an end-of-life date of January 1, 2004. As with the decrease in TCP port 445 activity, this decrease may also be due to effective configuration of perimeter security devices such as firewalls and intrusion detection systems.

The third most targeted port between January 1 and June 30, 2005 was UDP port 1026. This port was targeted by 9% of attacking IP addresses during this period, up from 8% in the second half of 2004. However, this value may be inflated due to the ability of attackers to forge the source address in UDP messages.

TCP port 80 accounted for a total of 7% of attacking IP addresses in the first half of 2005. For the last six months of 2003 and the first six months of 2004, TCP port 80 had ranked amongst the top two attacked ports; however, in the last six months of 2004, it accounted for only 2% and did not rank among the top ten attacked ports. Over the first half of 2005 it regained its popularity, rising to fourth position in the top ten. The recent rise reflects an 86% increase in the number of attacking IP addresses targeting this port.

Symantec expects that, as more Web browser and Web application vulnerabilities are discovered, the popularity of TCP port 80 relative to other ports will continue to rise. Attackers who can compromise computers hosting Web services can subsequently launch attacks against vulnerable 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, UDP port 1434, the port affected by the Microsoft SQL Server Resolution Service Stack Overflow Attack, the top attack for this reporting period, failed to rank among the top ten. The absence of this port in the top targeted ports is likely due to security policies implemented on many networks. Many administrators may have disabled logging of infection attempts on this port for performance reasons or to simplify log auditing.

Attack activity per day

This section will discuss the attack activity per day as observed by organizations connected to the Internet. The attack activity per day is determined by the number of attacks observed by the median organization in the sample set and, as such, 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.

For this volume of the Symantec *Internet Security Threat Report*, this metric has been redesigned to include all unauthorized access attempts blocked at the firewall and network intrusion detection system level. Previously, each attack was identified through an analyst's observations, which would be centered only on the most critical attacks. The new approach ensures that all malicious activity is included. As a result of this redesign, the number of attacks reported this period would be considerably higher than those seen in

[41] http://securityresponse.symantec.com/avcenter/venc/data/w32.welchia.worm.html
[42] http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.worm.html

previous volumes of the *Internet Security Threat Report*. However, in order to maintain the validity of any period-to-period comparisons, the number of attacks per day over the previous two reporting periods has been adjusted according to this new approach. The numbers presented in the following discussion reflect these adjustments.
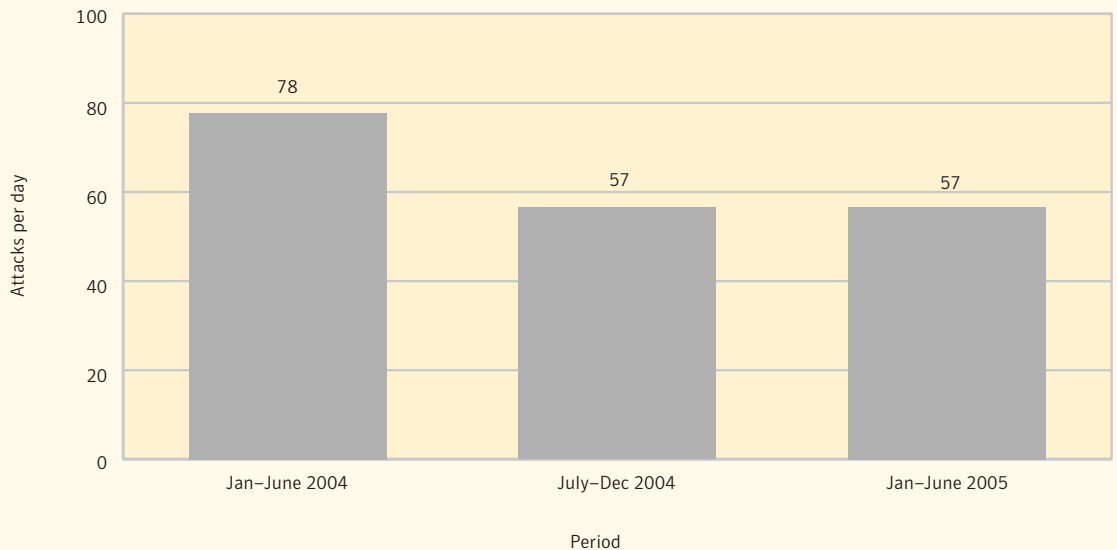

Figure 6. Attacks per day, Jan–June, 2005
Source: Symantec Corporation

Between January 1 and June 30, 2005, Symantec detected an average of 57 attacks per day (figure 6). This is consistent with the second half of 2004, when 57 attacks per day were also detected. The relatively constant rate of attacks per day for the last six months of 2004 and the first six months of 2005 is likely due to the lack of any substantial worm outbreaks in that time. With this in mind, it should be noted that the attack activity per day would rise drastically over a very short period if a major malicious code outbreak occurs.

Bot networks

This metric will explore the proliferation and activity of bot networks. Bot networks are groups of compromised computers on which attackers have installed software that listens for and responds to commands—typically over an IRC channel—allowing the attacker remote control over the computers. The software currently being used can be upgraded to incorporate exploits targeting new vulnerabilities.

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. Additionally, bots can be used to perform DoS attacks against the enterprise's Web site, which can disrupt revenue for ecommerce companies, or against other organizations' Web sites, which can have serious legal consequences.

Symantec identifies bot networks by analyzing coordinated scanning and attack patterns. This coordinated activity allows Symantec to identify bot network computers that might otherwise go undetected. Since identification of these computers is based on coordinated behaviors, it cannot be considered exhaustive. Nevertheless, the identified computers help provide an understanding of the current trends of bot networks.
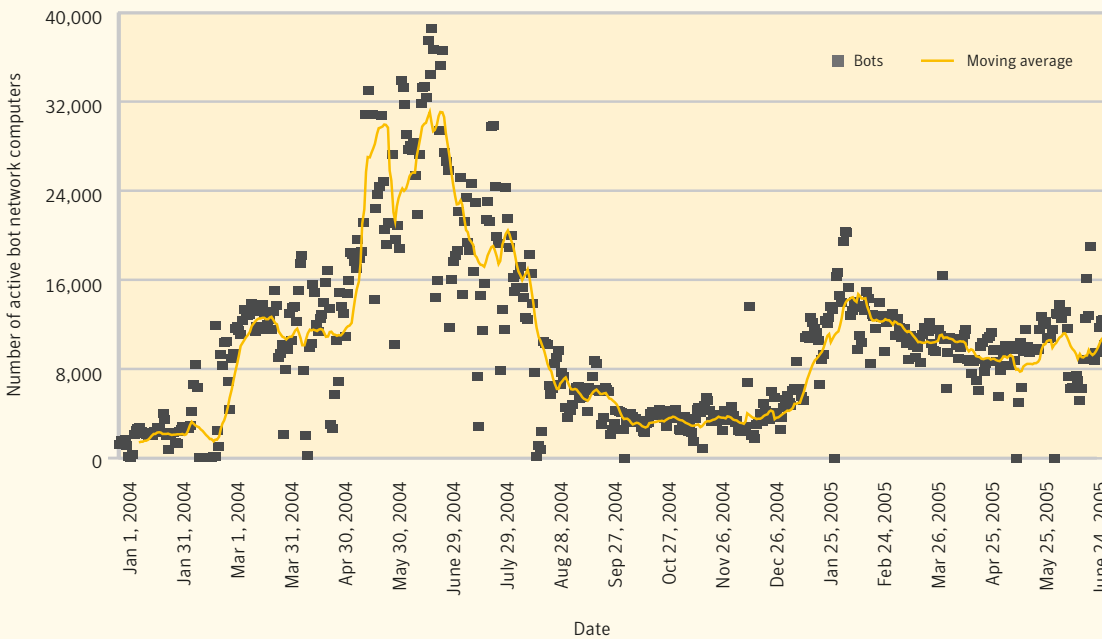

Figure 7. Bot network computers
Source: Symantec Corporation

In the past six months bot network activity has increased to a median[43] average of 10,352 unique bots identified per day (figure 7). This is an increase of over 138% from the average of 4,348 bots identified per day in December 2004. Symantec believes this increase in bot network activity is a reaction to security implementations put in place in the last half of 2004.

In the previous *Internet Security Threat Report*, Symantec speculated that a dramatic drop in bot network activity that took place in August 2004 was due in part to the release of Microsoft Windows Service Pack 2, which included patches for vulnerabilities commonly exploited by bots. Furthermore, default blocking of ports that are associated with vulnerabilities commonly targeted by bot networks was also speculated to have reduced bot network activity. As hosts vulnerable to exploitation become less common, bot networks must work harder to maintain their current size and continue to grow. It is likely that in order to maintain viability, bot network owners stepped up their attack activity, resulting in increasingly coordinated efforts.

The rise in bot network activity is reflected in the increase in bot variants that is documented in the "Malicious Code Trends" section of this document. The rise in the number of bot variants is likely a sign that the number of bot network owners is also increasing, as it is unlikely that an individual bot network owner will use more than one variant.

Attack activities commonly associated with bot networks, such as DoS attacks, have grown in similar fashion over the past six months (please see the "Denial of service" discussion below). Symantec believes that this increase in DoS attack activity is an indicator that overall bot network activity has risen. Attackers have been forced to be more aggressive to maintain their collection of compromised computers and, by extension, DoS attacks have increased as well.

As shown by figure 7, bot network activity during the first half of 2005 peaked on or around February 24. This may be due to the fact that a large number of new software and computers are typically deployed by new users during and after the December holiday season. New users are less likely to be security minded, making them relatively easy targets for attackers.

The peak in activity may also coincide with infrastructure changes that are implemented during this period by educational institutions and other organizations. Information technology infrastructure changes and updates typically take place during slow business periods such as the post-holiday season in North America and Europe. This ultimately results in the deployment of large numbers of corporate and personal computers and new software during the period near the beginning of the year. It is likely that vulnerable computers and software are among those that are newly deployed or redeployed. This may also contribute to the increase in bot network activity.

To prevent bot infections, Symantec recommends that ISPs perform both ingress and egress filtering to block known bot network traffic and that antivirus definitions are updated regularly. Furthermore, all systems within the organization's network should be monitored for signs of bot infection, ensuring that any infections are detected and isolated as soon as possible. ISPs should also filter out potentially malicious email attachments to reduce exposure to enterprises and end users. As compromised computers can be a threat to other systems, Symantec also recommends that the enterprises notify their ISPs of all malicious activity.

[43] The median average was used here because the data was not normally distributed throughout both reporting periods; therefore, the median provides a more meaningful comparison between the two periods.

To reduce exposure to bot-related attacks, end users should employ defense in-depth,[44] including antivirus software and a firewall. 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 should 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.

Denial of service attacks

DoS attacks are a major threat to corporations that rely on Internet connectivity to carry out their operations. These attacks are a particular threat to companies that rely primarily on the Internet to generate revenue. DoS attacks are typically carried out by flooding a targeted computer with requests for data in order to slow or block legitimate access to services it provides.

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 (short for synchronization) requests.[45] 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 referred to as backscatter being sent to other computers on the Internet. This backscatter is used to derive the number of DoS attacks observed throughout the reporting period (figure 8).
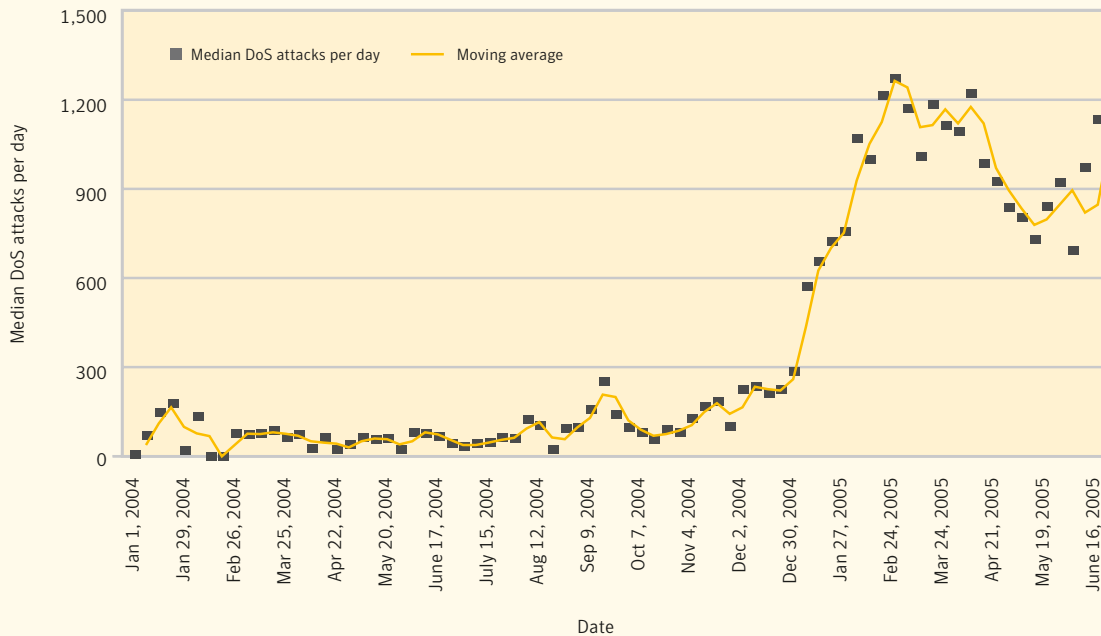

Figure 8. DoS attacks per day
Source: Symantec Corporation

Between January 1 and June 30, 2005, the number of DoS attacks grew by more than 680% to 927 per day on average. This is an increase over the last six months of 2004, during which Symantec observed an average of 119 DoS attacks per day. Symantec believes that this increase strongly correlates to the rise bot network activity outlined previously in the "Bot networks" discussion and illustrated in figure 7.[46]

As was stated previously, one of the primary functions of bot networks is to perform DoS attacks. Large bot networks are able to conduct broadly based DoS attacks; however, smaller bot networks and bot networks that do not wish to have their compromised computers identified must rely on other methods, such as SYN flood attacks using forged source addresses. Furthermore, functionality allowing for this type of DoS attack is likely incorporated into many bots, as public code for implementing it has been available for some time. Despite restrictions put in place in Microsoft Windows XP Service Pack 2 that are intended to prevent this type of attack,[47] publicly available network drivers exist that can be used to bypass it.[48]

As a consequence of this, it is likely that the increased bot activity seen in the first half of this year is contributing to the increased DoS activity.[49] This may be related to financial motivation, as DoS attacks have reportedly been threatened in extortion attempts.[50] In order to inhibit the ability of computers on their network to send data with forged source addresses, Symantec recommends that organizations perform egress filtering on all outbound traffic. This will reduce the potential for SYN flood attacks.

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 systems are distributed globally. The identification of bot-infected computers is important, as a high percentage of infected machines could mean 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.

During the first six months of 2005, the country with the highest proportion of bot-infected computers worldwide was the United Kingdom, with 32% (table 3). The United Kingdom was also the highest ranked country in the last half of 2004, with 25% of all bot-infected computers worldwide situated there.

Symantec has observed that bots predominantly infect computers connected to high-speed, broadband Internet through large ISPs. It has also been observed that rapid expansion of broadband connectivity facilitates the spread of malicious software, including bots. This is likely due to the failure of security infrastructures in keeping up with rapid broadband growth. As a result, Symantec believes it is reasonable to conclude that the increase in bot-infected computers in the United Kingdom is likely due to the rapid growth in broadband Internet there.[51]

---

[46] Regression analysis was performed on the data with the extreme outliers removed. The analysis produced a coefficient of determination of 0.85, meaning that 85% of the variation in DoS victims can be explained by the linear relationship between Bot numbers and DoS attacks. Only 15% of the variation remains unexplained.
[47] http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/sp2netwk.mspx
[48] http://www.winpcap.org/
[49] It should be noted that it is possible that there is a confounding factor that Symantec does not have insight into. For instance, there may be another variable influencing both the perceived bot network and DoS activity. Due to the strong correlation, however, Symantec believes that the bot network activity is a major driving factor in the observed DoS attacks.
[50] http://www.newscientist.com/channel/info-tech/mg18725125.900
[51] http://www.point-topic.com/content/dslanalysis/World%20Broadband%20Statistics%20Q1%202005.pdf (access requires registration)

Rank Jan–June 2005	Rank July–Dec 2004	Country	Percent of bot-infected computers Jan–June 2005	Percent of bot-infected computers July–Dec 2004
1	1	United Kingdom	32%	25%
2	2	United States	19%	25%
3	3	China	7%	8%
4	4	Canada	5%	5%
5	6	France	4%	4%
6	9	South Korea	4%	3%
7	7	Germany	4%	4%
8	10	Japan	3%	3%
9	5	Spain	3%	4%
10	8	Taiwan	2%	3%

Table 3. Top countries by percentage of bot-infected computers
Source: Symantec Corporation

For the second straight reporting period, the United States had the second highest percentage of bot-infected computers, with 19%. This is down from 25% in the second half of 2004. China was home to the third-highest percentage of bot-infected computers during the first six months of 2005, with 7%. It maintains the third position for the second straight six-month period, although its overall numbers dropped one percentage point over the past six months.

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 hide 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.

For the first six months of 2005, the United States continued to be the country from which the majority of attacks originated (table 4). 33% of all attacks originated there. This represents a rise of three percentage points following three reporting periods of declining rates. In the last six months of 2004, 30% of attacks originated in the United States, down from 37% in the first half of the year. The high rate of attacks originating in the United States is attributable to the high rate of broadband use there. Symantec believes that with the continued growth of broadband Internet in the United States[52] it will likely be the highest country of attack origin for the foreseeable future.

[52] http://www.point-topic.com/content/dslanalysis/World%20Broadband%20Statistics%20Q1%202005.pdf (access requires registration)

Rank Jan–June 2005	Rank July–Dec 2004	Rank Jan–June 2004	Country	Percent of events Jan–June 2005	Percent of events July–Dec 2004	Percent of events Jan–June 2004
1	1	1	United States	33%	30%	37%
2	3	5	Germany	7%	8%	5%
3	6	6	United Kingdom	7%	4%	4%
4	2	2	China	6%	8%	6%
5	7	7	France	5%	3%	4%
6	9	8	Spain	5%	3%	3%
7	5	3	Canada	4%	4%	6%
8	8	12	Japan	4%	3%	1%
9	4	9	South Korea	3%	4%	3%
10	10	11	Italy	3%	2%	2%

Table 4. Top originating countries
Source: Symantec Corporation

Germany was the second highest country of attack origin during the first six months of 2005, accounting for 7% of attacks. This represents a jump from third position in the second half of 2004 despite a one-percentage point drop in the number of worldwide attacks originating there. The United Kingdom rose from sixth place in the second of 2004 to third position this period, accounting for 7% of Internet-wide attacks, an increase of three percentage points.

Targeted attack activity by industry

Attackers choose their targets for various reasons. Some attackers are simply opportunistic, randomly attacking vulnerable computers regardless of the owner or organizational affiliation of the target. Other attackers select their targets specifically in order to compromise computers within an organization or a specific industry. This metric explores attacks targeted at specific industries. 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 within the reporting period.

For this volume of the *Internet Security Threat Report*, this metric has been redesigned to include a broader range of data than had been used for previous volumes of the report. A realignment of the existing sensor base has given Symantec a more representative sample of attack data that includes all observed attacks, including those seen by firewall and intrusion detection system sensors.
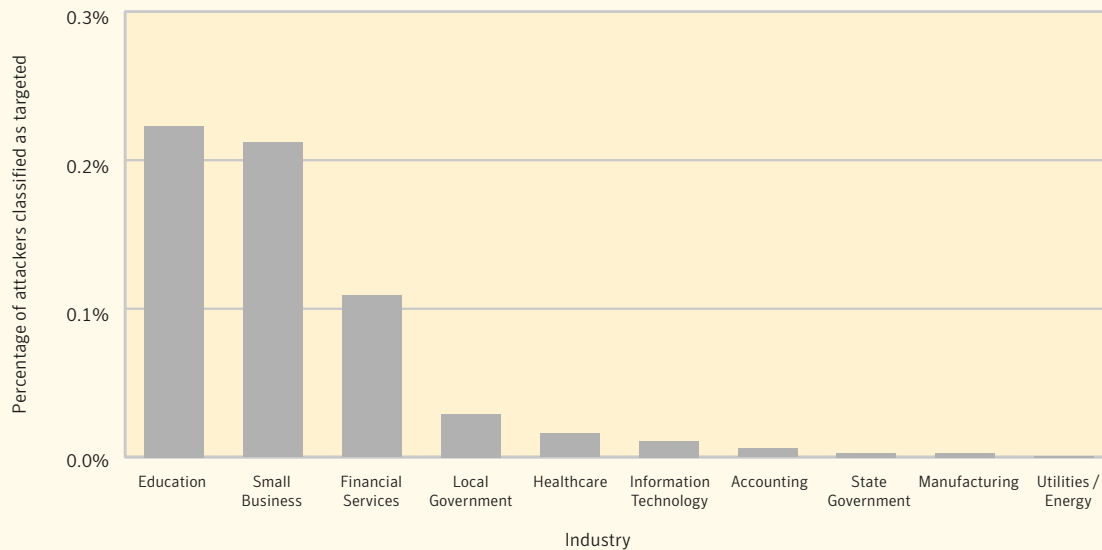
Figure 9. Targeted attacks by industry
Source: Symantec Corporation

Between January 1 and June 30, 2005, education was the most frequently targeted industry (figure 9). This is likely due to the nature of networks in educational organizations. In addition to providing large numbers of public terminals, a single educational institution must facilitate remote access for tens of thousands of users requiring numerous different services. This can make it difficult for network administrators to actively defend against threats. Furthermore, the volume of computers that are connected to the 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 second most targeted industry between January 1 and June 30, 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 have 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.

Financial services was the third most frequently targeted industry between January 1 and June 30, 2005. This industry is generally considered to be a popular target for attackers hoping to profit from their attacks. Symantec expects targeted attacks against the financial services industry to increase as the focus of attackers becomes increasingly profit driven.[53] (For more on profit-driven attacks, please see "Malicious code for profit" in the "Malicious Code Trends" report below.)

[53] See http://www.securityfocus.com/columnists/278, for example.

Vulnerability Trends

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

New vulnerabilities are discovered and disclosed regularly by a large community of end users, security researchers, hackers, and security vendors. The discovery and disclosure of a single vulnerability in a critical asset can seriously undermine the security posture of an organization.

Symantec carefully monitors vulnerability research, tracking vulnerabilities throughout their lifecycle, from initial disclosure and discussion to the development and release of a patch or other remediation measure. Symantec operates one of the most popular forums for the disclosure and discussion of vulnerabilities on the Internet. The BugTraq mailing list[54] has approximately 50,000 direct subscribers, who receive, discuss, and contribute vulnerability research on a daily basis. Symantec also maintains one of the world's most comprehensive vulnerability databases, currently consisting of over 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 were disclosed between January 1 and June 30, 2005. It will compare them with those disclosed in the two previous six-month periods and discuss how current vulnerability trends may affect future Internet security activity. Where relevant, it will also offer 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
- Adjusted severity of remotely exploitable vulnerabilities
- Web application vulnerabilities
- Ease of exploitation
- Vulnerabilities with exploit code
- Exploit development time
- Patch development and availability time
- Web browser vulnerabilities

---

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

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, due to additional information that has become available after the reporting period has ended, vulnerabilities may be attributed to a particular reporting period after that time. Conversely, entries may be removed after a reporting period because they are deemed to not be vulnerabilities after the reporting period has ended.

Because of this, statistics and percentages that are reported in one volume of the *Internet Security Threat Report* may not agree with information presented in 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 first half of 2005 was marked by a substantial increase in the total number of vulnerabilities disclosed. Between January 1 and June 30, 2005, Symantec documented 1,862 new vulnerabilities. This is the highest number documented in one reporting period since the *Internet Security Threat Report* began tracking new vulnerabilities in six-month intervals (figure 10). It also represents an increase of 31% over the 1,416 new vulnerabilities documented in the second half of 2004 and an increase of 46% over the 1,275 new vulnerabilities seen in the same six-month period one year ago.
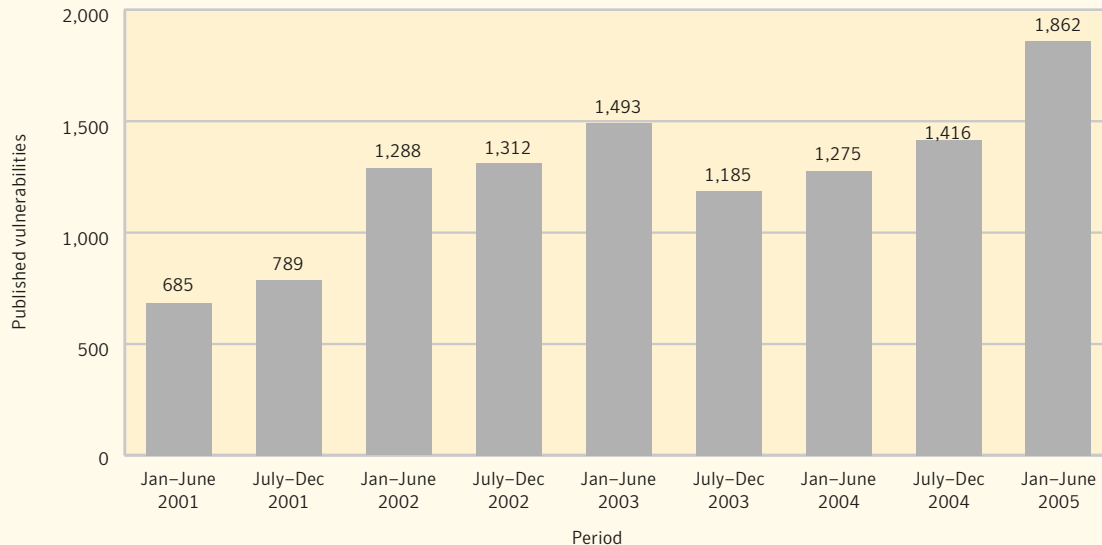

Figure 10. Total vulnerabilities, Jan. 2001–June 2005
Source: Symantec Corporation

The 1,862 vulnerabilities disclosed in the first six months of 2005 equates to an average of 72 new vulnerabilities per week or just over 10 per day. This is 18 more vulnerabilities per week than the 54 seen in the last six months of 2004. During the first six months of 2004, an average of 49 new vulnerabilities were disclosed per week.

The increasing trend observed over the past 18 months has been driven by a sharp increase in Web application vulnerabilities. As will be discussed in the "Web application vulnerabilities" section below, these constitute 59% of documented vulnerabilities in the current reporting period.

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 it gives an attacker access to the targeted system. It measures the potential impact that successful exploitation of the vulnerability may have on the confidentiality, integrity, and/or availability of information stored on or transmitted across the affected system. For the purposes of the *Internet Security Threat Report*, each vulnerability is classified in one of three severity categories. These levels are as follows:

Low severity—vulnerabilities that constitute a minor threat. Attackers cannot exploit these vulnerabilities across a network and successful exploitation does not result in a complete compromise of the information stored on or transmitted across the system.

Moderate severity—vulnerabilities that result in a partial compromise of the affected system. An attacker may gain elevated privileges but does not gain complete control of the targeted 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—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 (that is, remotely) without authentication.

Between January 1 and June 30, 2005, Symantec classified 909 vulnerabilities, or 49% of the total volume, as high severity (figure 11). This is one percentage point lower than the previous six-month period in which 704 vulnerabilities, or 50%, were rated high severity. It is also four percentage points higher than the first half of 2004, when 577 vulnerabilities, or 45% of the total, were considered high severity.
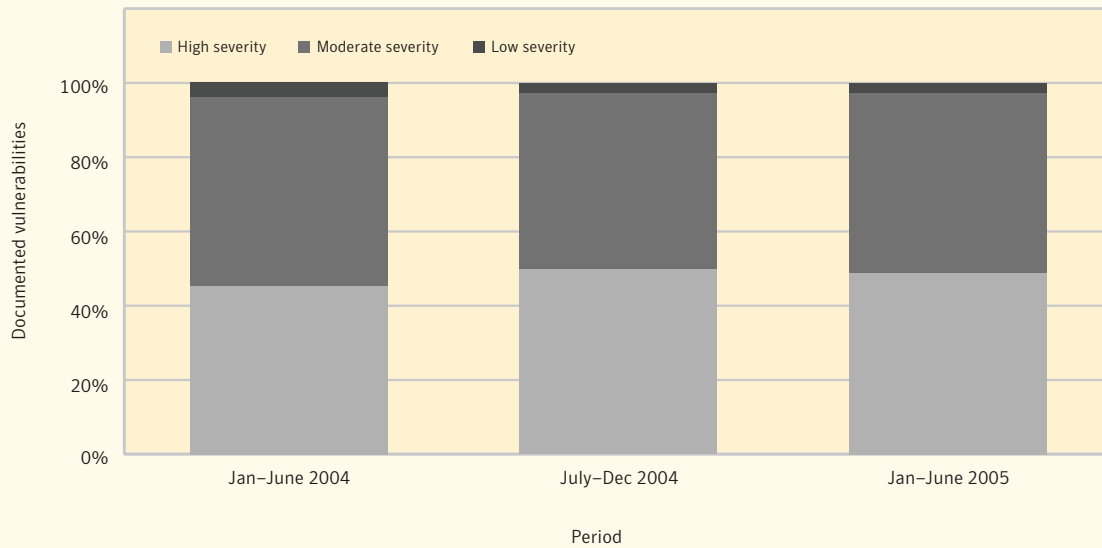
Figure 11. Vulnerabilities by severity, Jan. 2004–June 2005
Source: Symantec Corporation

During the first half of 2005, 900 vulnerabilities, or 48% of the total volume, were classified as moderately severe. The same percentage was seen in the second half of 2004 when 672 were rated moderately severe. This is slightly lower than the 646, or 51%, that were classified as moderately severe in the first half of 2004.

During the first half of 2005, 53 vulnerabilities, or 3% of the total volume, were categorized as low severity. The same proportion was noted in the second half of 2004, down slightly from the 4% of the total volume that was rated low severity in the first half of 2004.

As illustrated in figure 11, Symantec has rated the vast majority of vulnerabilities as either moderate or high severity over the past three reporting periods. In previous volumes of the *Internet Security Threat Report*, Symantec has stated that it is reasonable to conclude that there is a correlation between the high severity rating of a vulnerability and the recognition accorded the researcher by peers in the research community. As a result, researchers may not be particularly interested in finding or publishing low-severity threats. Low-severity threats may also be fewer because the "low hanging fruit" (that is, the more easily discovered vulnerabilities) has already been picked, so that only more severe (presumably more difficult) vulnerabilities remain to be discovered.

A third reason for the small number of low-severity vulnerabilities may be the use of remote exploitability as a criterion in the Symantec severity rating system. If a vulnerability is remotely exploitability (that is, it can be exploited across a network) it will be considered at least moderately severe. Low-severity vulnerabilities, by definition, are "those that attackers cannot exploit across a network;" that is, they are not remotely exploitable. 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 increasingly less common. The following section will discuss the severity ratings with the criterion of remote exploitability removed from consideration.

Adjusted severity of remotely exploitable vulnerabilities

For some time, the majority of vulnerabilities documented by Symantec have been classified as remotely exploitable. That is, most vulnerabilities reported can lead to attacks that occur from across a network, including the Internet. During the first half of 2005, 84% of the disclosed vulnerabilities were remotely exploitable, compared to 82% in the second half of 2004 and 81% in the same period one year ago. The high numbers are likely due to the overwhelming prevalence of networked single-user workstations and client-server applications as well as near universal acceptance of and reliance on the Internet.

In a world where accessible targets are just a few network hops away, locally exploitable vulnerabilities—that is, those that require physical access on multi-user systems—are not likely to be appealing to vulnerability researchers. This is because, in addition to requiring physical proximity, many of these vulnerabilities require attackers to have valid user accounts. Each of these factors severely limits the pool of potential targets. Remote vulnerabilities, particularly those that do not require authentication, are much more appealing to attackers, as vulnerable systems will be more numerous and more accessible. Consequently, vulnerabilities that are remotely exploitable have become much more common than those that are not.

As was stated previously, the high proportion of remotely exploitable vulnerabilities also explains the prevalence of vulnerabilities that are rated moderately to highly severe. The Symantec vulnerability rating formula considers any remotely exploitable vulnerability to be at least moderately severe. Therefore, the presence of remote exploitability may cause an otherwise low-severity vulnerability to be given a higher severity ranking. This will likely increase the number of vulnerabilities that are considered moderately to highly severe. In order to assess whether this is in fact the case, Symantec assessed the severity of vulnerabilities that would be ranked as moderately to highly severe (due to remote exploitability) with the remote exploitability criterion removed.

With the remote exploitability criterion removed from the severity rating formula, the distribution of vulnerability severity ratings is slightly different than it is with remote exploitability included (figure 12). The most noteworthy change is that the proportion of moderately severe vulnerabilities increases when the remote exploitability criterion is removed.
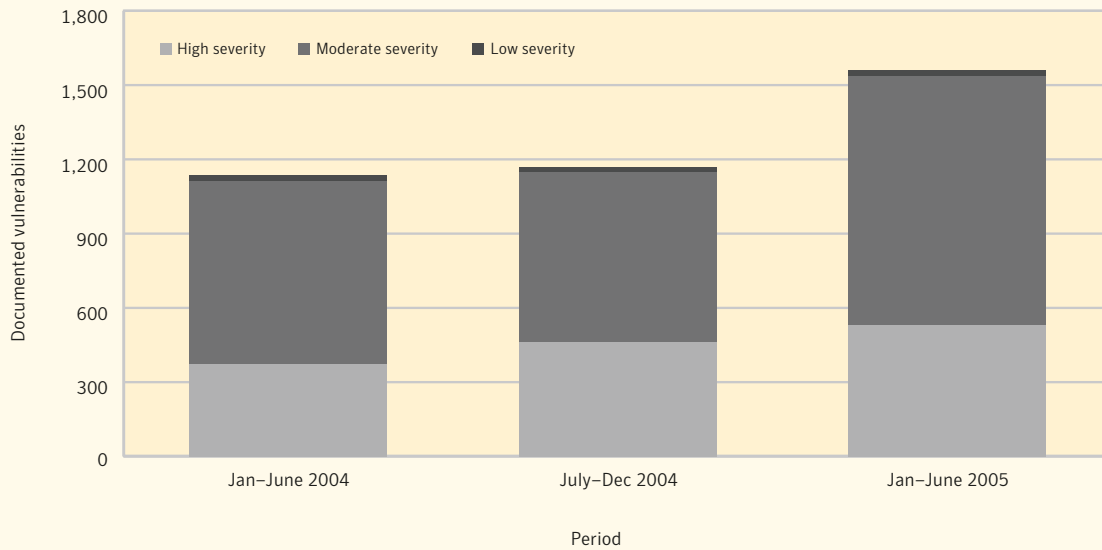
Figure 12. Adjusted severity of remotely exploitable vulnerabilities
Source: Symantec Corporation

When evaluating the severity of vulnerabilities with remote exploitability removed from consideration, the proportion of high-severity vulnerabilities decreases significantly. This is true for vulnerabilities disclosed in each of the past three six-month periods. Of the remotely exploitable vulnerabilities disclosed in the first half of 2005, when adjusted for remote exploitability, 532 vulnerabilities, or 29% of the total volume, were rated as highly severe compared to 49% prior to adjustment. In the second half of 2004, 40% of the total volume was considered high severity when adjusted for remote exploitability, compared to 50% prior to adjustment. 33% were considered high severity after adjustment during the same reporting period one year ago, compared to 45% with remote exploitability included.

When excluding remote exploitability from consideration, the proportion of vulnerabilities that were considered to be moderately severe increased in each of the last two six-month reporting periods. In the first six-months of 2005, after adjustment 1,005 remotely exploitable vulnerabilities were rated moderately severe, which is 54% of the total volume, compared to 48% with remote exploitability included in the categorization. This is a decrease of five percentage points from the 59% of the previous six-month period, compared with 48% prior to adjustment. It is a further decrease from the 65% disclosed in the first six months of 2004, compared to 51% with remote exploitability taken into account.

When remote exploitation capability is removed from consideration, only 1% of all remotely exploitable vulnerabilities disclosed between January 1 and June 30, 2005 were classified as low severity. This is down from the 3% that were considered low severity prior to adjustment. It is also lower than each of the two previous six-month periods, during which 2% of vulnerabilities would be ranked low severity after adjustment, compared to 3% prior to adjustment in the second half of 2004, and 4% in the first half of the year.

When remotely exploitable vulnerabilities are re-evaluated based solely on criteria other than remote exploitability, the majority documented in all periods is moderately severe. Interestingly, the proportion of the total rated as low severity remains low—lower, in fact, than in the general sample of vulnerabilities.

Web application vulnerabilities

Web applications are technologies that rely on a browser for their user interface; they are often hosted on Web servers. An increasing number of software vendors deliver applications over the Web. Furthermore, many organizations have developed custom Web-based applications to provide various internal and external services. The increase in the use of the Web as an application platform has resulted in an increase in Web application vulnerability research.
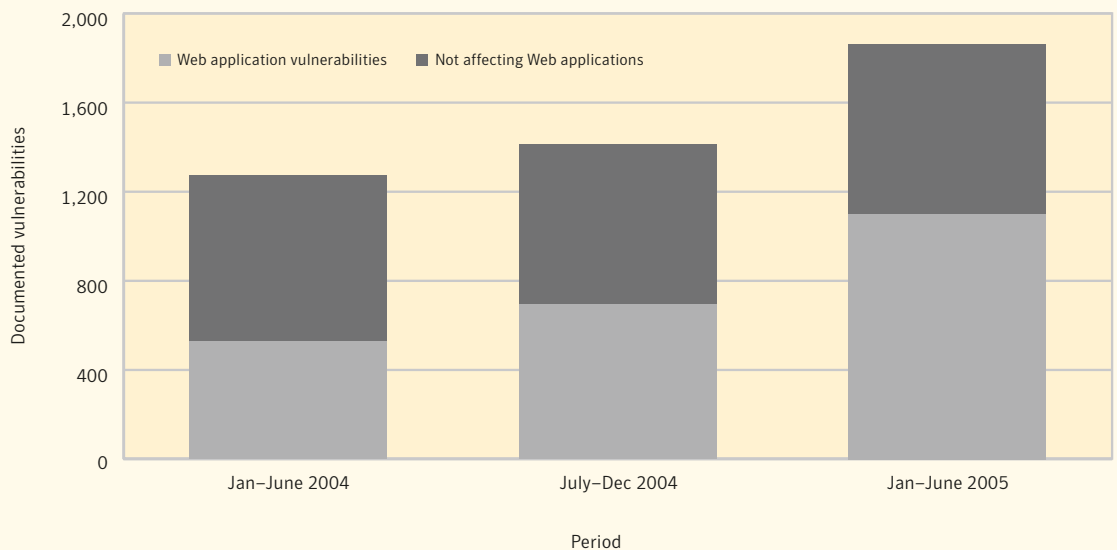

Figure 13. Web applications vulnerabilities
Source: Symantec Corporation

During the first six months of 2005, the majority of vulnerabilities documented by Symantec affected Web applications (figure 13). During this period, 1,100 vulnerabilities, or 59% of the total volume, were classified as Web application vulnerabilities. This is a 59% increase over the 694 Web application vulnerabilities disclosed in the last six months of 2004 and a 109% increase over the 527 published during first half of 2004.

Vulnerabilities in Web-based applications are often underestimated as a security risk. Many of these vulnerabilities are low-complexity bugs that are discovered in one of the many relatively simple customized PHP, Perl, ASP, and other server-side Web scripts that are available on the Internet as freeware. For instance, there are thousands of Web scripts[55] currently deployed in various contexts. Many of these are vulnerable

---

[55] Web scripts are small programs that provide application functionality to Web sites. For example, relatively simple Web scripts power most guest book programs, Web site message forums, and photo galleries.

to cross-site scripting and SQL injection attacks[56] that exploit input validation[57] vulnerabilities. These vulnerabilities may not pose severe threats in and of themselves due to minimal deployment; however, administrators are forced to deal with higher numbers of potential threats and must assess the risk that each one poses to the enterprise. More serious threats may be overlooked or missed because of the large number of these vulnerabilities and the time and attention administrators must dedicate to them, despite the low risk that they may pose.

Vulnerabilities in these technologies are particularly threatening because they are typically exposed to the Internet through a Web server. As such, they may allow an attacker to bypass traditional perimeter security measures, such as firewalls. Having done so, a successful attacker may then compromise an entire network by gaining access through a single vulnerable system. Vulnerabilities in these technologies can also allow an attacker to access confidential information from databases without having to compromise any servers.

Security administrators are urged to follow the best practices outlined in "Appendix A" of this report. Symantec also recommends that administrators audit their systems to ensure that no vulnerable Web applications or scripts are being hosted. They 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.

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 exploit them, with or without an exploit, depending on the vulnerability. Symantec rates a vulnerability as "easily exploitable" if it requires no exploit or if a required exploit is known to be available. If exploit code is required but is not yet available to the public, Symantec will rate the vulnerability as "no exploit available."

Generally speaking, "easily exploitable" vulnerabilities do not require sophisticated skills or knowledge to exploit. Anyone with sufficient general technical knowledge or with publicly available tools can exploit them. Examples of these include Web server vulnerabilities that can be exploited by simply entering an appropriate URL into a Web browser.

On the other hand, vulnerabilities that are classified as "no exploit available" are more difficult to attack successfully. 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, thus 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 exploits might exist. For instance, some individuals or groups may choose to keep exploits private in order to prevent the development of security countermeasures. However, without a public exploit, these vulnerabilities won't likely be widely exploited.

---

[56] Cross-site scripting attacks are a type of attack against users of a Web-based application rather than the server hosting the application. They exploit vulnerabilities in the application to spoof content. These attacks can have many possible consequences, including hijacked user accounts. SQL injection attacks are attacks on the database server used by a Web-based application that are made possible by inadequate security checks in the application. The consequences also vary, from unauthorized disclosure of potentially sensitive data to complete compromise of the database.

[57] Input validation vulnerabilities occur when an application fails to check externally supplied data for validity (such as data from a user). Data of an unexpected form can sometimes cause security failures if the vulnerable application has not implemented validation checks.

Symantec Internet Security Threat Report

During the first six months of 2005, 1,356 vulnerabilities were classified as easy to exploit (figure 14). This means that 73% of all vulnerabilities disclosed during this period either required no exploit code or had some type of exploit code available. This is two percentage points higher than the 71% seen in last six months of 2004. During the first half of 2004, 70% of all vulnerabilities were considered easy to exploit.
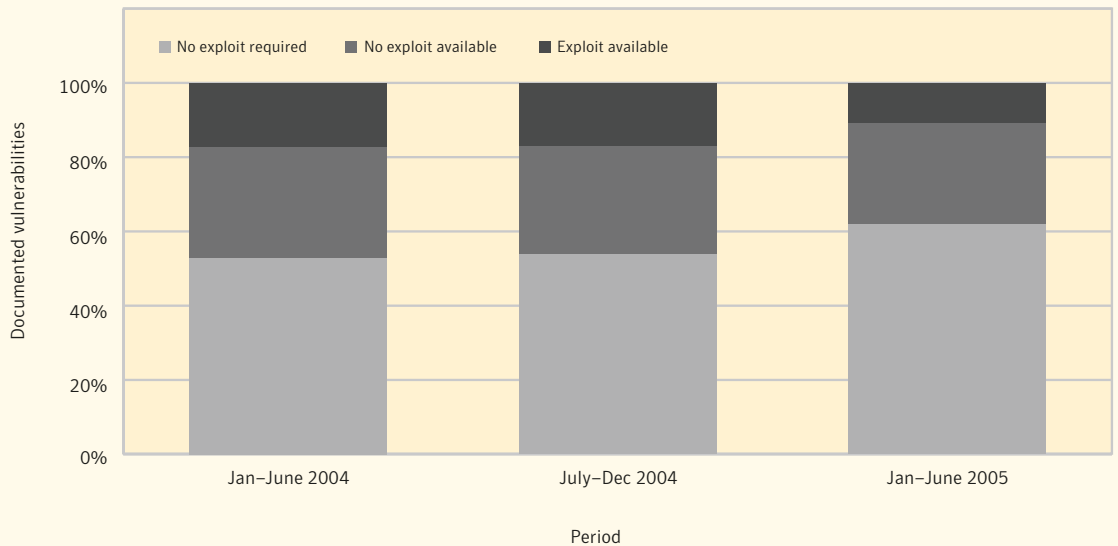

Figure 14. Ease of exploit breakdown, Jan 2004–June 2005

In the first half of 2005, 1,153 vulnerabilities, or 62% of the total, required no exploit code. This is up substantially from the previous six-month period, during which 54% of vulnerabilities required no exploit code. In the same period one year ago, 53% of vulnerabilities required no exploit code.

The increase in the percentage of vulnerabilities requiring no exploit code corresponds to the increase in Web-application vulnerabilities. Such an increase would reasonably be expected, as Web application vulnerabilities typically do not require sophisticated exploit tools or techniques for successful exploitation. However, the overall percentage of easy-to-exploit vulnerabilities has not increased to the same degree because there are fewer vulnerabilities, proportionately, that have exploit code available.

Vulnerabilities with exploit code

Exploit code is sometimes included with the original advisory that describes the vulnerability. In other cases, the author may develop it as a proof of concept. When exploit code is released to the public it is typically made available on mailing lists such as BugTraq or hacker Web sites. If exploit code is available, the vulnerability with which it is associated will be considered easy to exploit.

Of the vulnerabilities that were disclosed during the first half of 2005, associated exploit code was available for 251, or 13% of the total volume (figure 15). In terms of raw numbers, this is greater than the last six months of 2004, during which exploit code was available for 201 vulnerabilities. However, this number is proportionally lower than the 15% that was seen in the last half of 2004, which represented the 18-month peak. The percentage for vulnerabilities published in the first half of 2004 was also 14%.
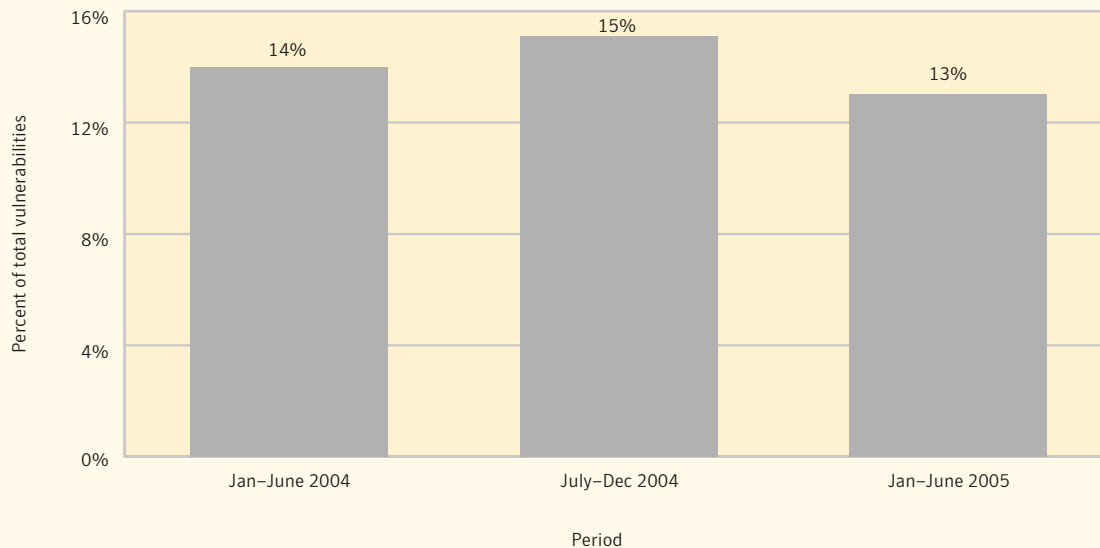

Figure 15. Vulnerabilities with associated exploit code
Source: Symantec Corporation

While the percentage of vulnerabilities with associated exploit code during this period has dropped, the real number increased from 201 to 251. The increase in total vulnerabilities with associated exploit code is therefore still a concern, despite the proportional decrease. Furthermore, these percentages can be expected to change slightly from volume to volume of the *Internet Security Threat Report*¸ as new exploit programs are added to older vulnerabilities and older vulnerabilities with associated exploit tools are added to the database.

The amount of effort researchers will spend on developing exploit code may be determined by the impact that a vulnerability is likely to have on a targeted system. They are not likely to expend time and energy developing exploit code for vulnerabilities that will not give them high-level access to the targeted systems. With this in mind, it is not surprising that most vulnerabilities for which an exploit tool is available are considered high severity. However, there has been a noteworthy change in proportions over the past two reporting periods (figure 16). In the first half of 2005, 70% of vulnerabilities with associated exploit code were rated high severity. This is a decrease from the 77% published in the previous period. For the first half of 2004, this percentage was 64%.
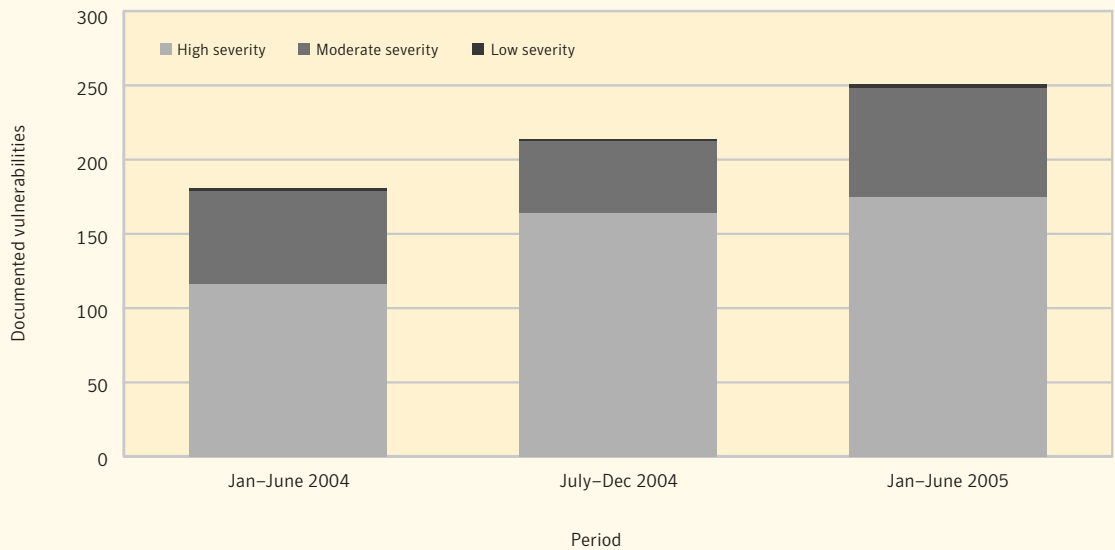

Figure 16. Vulnerabilities with exploit code, by severity, over 18 months
Source: Symantec Corporation

Exploit development time

A window of exposure exists between the disclosure of a vulnerability and the availability of a patch or other remediation measure. If exploit code is created and made public during this time, computers may be immediately vulnerable to widespread attack. The shorter the time between disclosure of a vulnerability and the release of an associated exploit, the sooner computers are vulnerable to attack (until patches become available).

Previous volumes of the *Internet Security Threat Report* have included analysis of the average time lapse between the disclosure of a vulnerability and the publication of an associated exploit. During the first six months of 2005, the average time for exploit development was 6.0 days (figure 17). This is a slight decrease from the average time of 6.4 days for exploits to be released in the previous six-month period. The average time for exploits to be developed and released in the first half of 2004 was 5.8 days.
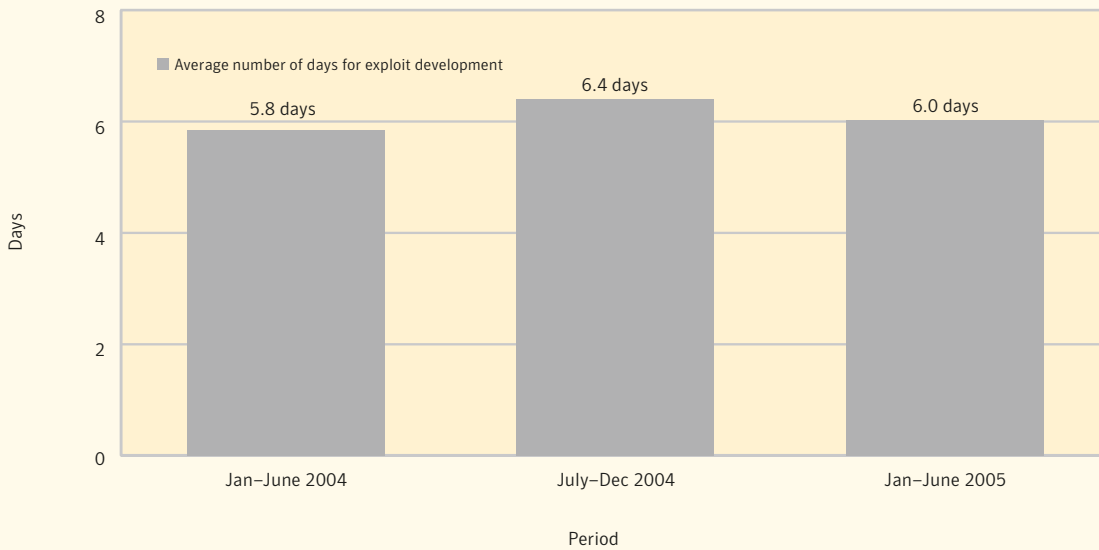
Figure 17. Exploit development time
Source: Symantec Corporation

The continued short time to exploit availability highlights the need for administrators to patch their systems or implement other measures to protect against new threats 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 disclosure and exploit development so short, administrators would benefit from notification of a new vulnerability, an understanding of the potential threat posed by the vulnerability and relevant mitigation or patching information. 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. They should also monitor vulnerability mailing lists and security Web sites for new developments. 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.

Patch development and availability time

For the first time, Symantec is assessing the average patch development and availability time in this volume of the *Internet Security Threat Report*. This discussion will gauge the average time between the public disclosure of a vulnerability and the release of an associated patch by the affected vendor. This analysis is based on the patch and vulnerability data in the Symantec vulnerability database. The disclosure date of each vulnerability is stored in the vulnerability database, as is the release date of each patch by the affected vendor.[58] The time period between the disclosure date of a vulnerability and the release date of an associated patch is referred to as "the time to patch." It should be noted that this metric only considers specific file-based patches or upgrades issued by enterprise vendors[59] and not general solutions. For example, instances where the vendor provides a workaround or steps for a manual fix are not included.

During the first half of 2005, on average, 54 days elapsed between the publication of a vulnerability and the release of an associated patch by an enterprise vendor (figure 18). This is an increase over the average of 49 days in the second half of 2004. This represents a slight reversal of a trend over the past two years, during which response times decreased. The trend towards decreasing times to patch, which started in the first half of 2004, was most likely due to increased pressure from customers for vendors to address security concerns, likely a response to high-profile vulnerabilities and malicious code.
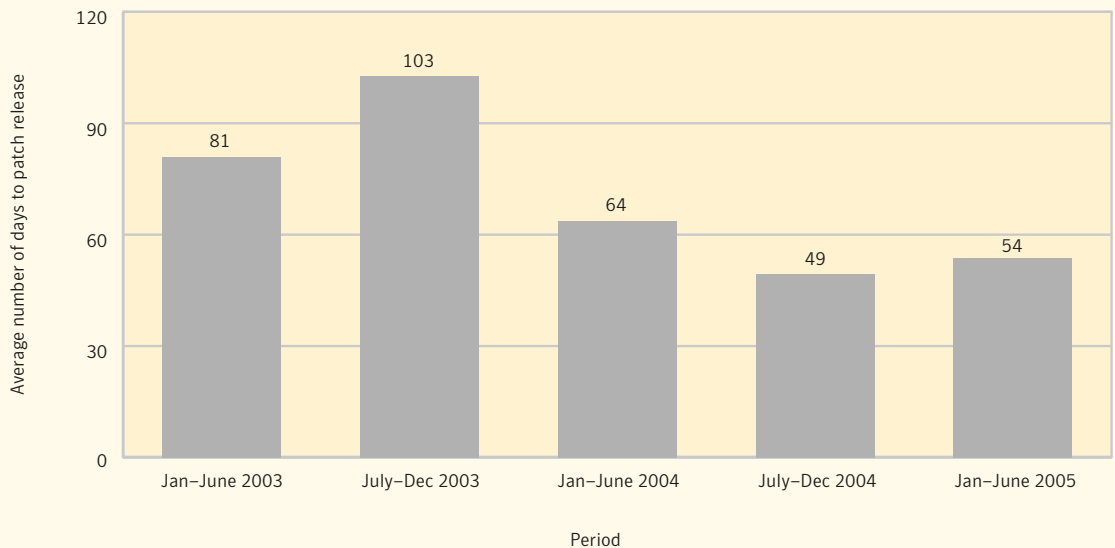

Figure 18. Average number of days to patch release

It is unsettling to think of a situation in which an exploit is available to attackers within a week (as indicated in the previous section) while there is no patch made available to administrators for nearly two months. This leaves a large window of opportunity for potential attackers. In fact, the 54-day average patch development time, combined with the average exploit development time of 6 days means that an average time of 48 days exists between the release of an exploit and the release of an associated patch. While the appearance of an exploit can speed patch release, there are still many instances where end users and administrators are forced to implement security "workarounds" without an official fix. During this time, networks will be vulnerable to compromise.

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

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. In the past, the focus of security has been on the perimeter: servers, firewalls, and other systems with external exposure. However, a notable shift has occurred, as client-side systems—primarily end-user desktop hosts—are becoming increasingly prominent. The Symantec *Internet Security Threat Report* has monitored this trend over the past several reporting periods.

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

• Only verifiable vulnerabilities that were confirmed by the vendor were taken into consideration.

• Web browser vulnerability counts may not match one-to-one with security bulletins or patches issued by vendors. This is because of the complexity in identifying individual vulnerabilities in browser exploits.

• Not every vulnerability discovered is exploited. As of this writing, no widespread exploitation of any browser except Microsoft Internet Explorer has occurred. However, Symantec expects this to change as alternative browsers become increasingly widely deployed.

As has been stated previously in this report, readers should be aware that this discussion is based on data that may change over time, as entries in the vulnerability database are constantly revised as new information emerges. As vendors confirm vulnerabilities and/or release patches, vulnerability totals may increase. As a result, statistics and percentages reported in one volume of the *Internet Security Threat Report* may not agree with the same information as it is presented in subsequent volumes.

During the first half of 2005, more vulnerabilities were disclosed for the Mozilla browsers, including Firefox, than for any other browser (figure 19). During this period, 25 vulnerabilities affecting the Mozilla family of browsers were disclosed, compared to 32 in the second half of 2004. During the first half of that year, only two vulnerabilities were disclosed for the Mozilla browsers.

The average severity of the Mozilla vulnerabilities in the first half of 2005 was high. 18 of the 25 Mozilla vulnerabilities in this period, or 72%, were rated high severity. This is up from 44% in the second half of 2004. There was a single high-severity vulnerability associated with Mozilla browsers in the first half of 2004. The increase of high-severity vulnerabilities may be due to attention being paid by researchers to the Firefox browser, which has been widely touted as a secure alternative to Microsoft Internet Explorer.
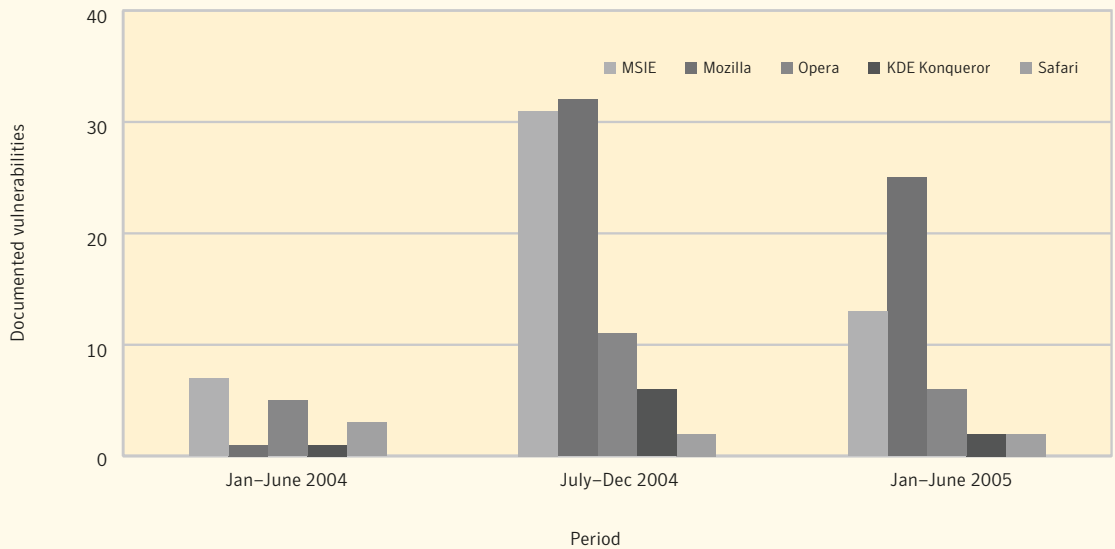

Figure 19. Browser vulnerabilities, Jan. 2004–June 2005
Source: Symantec Corporation

During the first six months of 2005, there were 13 vendor confirmed vulnerabilities disclosed for Microsoft Internet Explorer. This is a sharp decrease from the 31 documented in the second half of 2004. (It should be noted that in the last *Internet Security Threat Report*, only 13 vulnerabilities associated with Internet Explorer were classified as vendor confirmed. After publication, this number was revised to 31 due to delayed confirmation of the vulnerabilities by the vendor.) During the first half of 2004, seven Internet Explorers vulnerabilities were disclosed and confirmed by Microsoft. The average severity rating of the vulnerabilities associated with Internet Explorer during the first six months of 2005 was high.

During the first half of 2005, eight of the 13 Internet Explorer vulnerabilities, or 62%, were considered high severity. This is an increase over the 58% in the last six months of 2004 and the 57% of vulnerabilities that were rated high severity in the first half of that year.

During the first six months of 2005, six new vulnerabilities were disclosed for the Opera browser. This is a decrease from the previous reporting period, during which Symantec documented 11 Opera vulnerabilities. In the first half of 2004, five vulnerabilities were found for Opera.

The Opera vulnerabilities disclosed during the first half of 2005 had an average severity rating of moderate. Of the six vulnerabilities documented in the current reporting period, three were rated as high severity, or 50%. 27% of Opera vulnerabilities disclosed in the second half of 2004 were considered high severity. There were no high-severity Opera vulnerabilities documented by Symantec in the first half of 2004.

Between January 1 and June 30, 2005, two vendor confirmed vulnerabilities were disclosed for Apple's browser for Mac OS X, Safari, the same number as in the preceding six-month reporting period. In the first half of 2004, three vulnerabilities for Safari were disclosed.

The average severity rating for Safari vulnerabilities disclosed during the first half of 2005 was moderate. Only one of the two Safari vulnerabilities disclosed during this period was considered high severity. There were no high-severity Safari vulnerabilities disclosed in 2004.

For the first time, in this volume of the *Internet Security Threat Report* Symantec is assessing vulnerabilities for the Konqueror browser. Between January 1 and June 30, 2005, two vendor confirmed vulnerabilities were discovered in this browser. This is a decline from the six reported in the preceding six-month period. Konqueror was associated with a single vulnerability published in the first half of 2004.

The average severity rating for Konqueror vulnerabilities disclosed during the first half of 2005 was moderate. Of the two Konqueror vulnerabilities documented by Symantec in the first half of 2005, only one was rated high severity. In the previous six-month period, only one out of the six Konqueror vulnerabilities was considered high severity. The lone vulnerability associated with Konqueror from the first half of 2004 was not high severity.
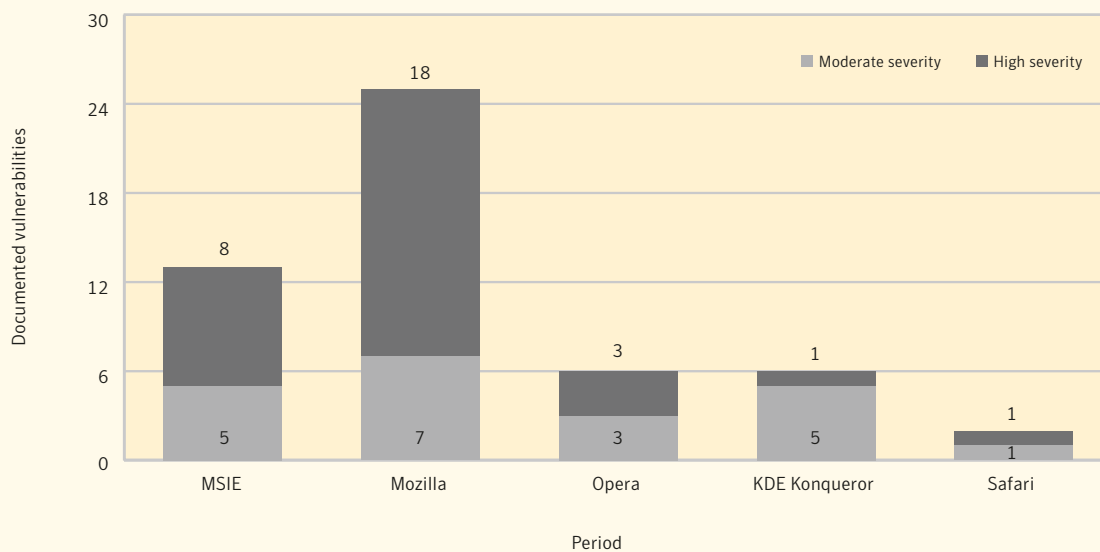

Figure 20. Browser vulnerabilities by severity, Jan 1–June 30, 2005
Source: Symantec Corporation

The fact that Mozilla browsers had the most vendor confirmed vulnerabilities over the past two six-month periods may suggest that Mozilla is currently acknowledging and fixing vulnerabilities more quickly than other vendors. This could be because the Mozilla browsers are open source and may be more responsive to reports of new vulnerabilities and subsequently developing and delivering associated patches. For instance, except in certain instances,[60] Microsoft releases fixes on a relatively fixed schedule rather than as needed, potentially increasing their acknowledgement time.

Overall, there are fewer high-profile Web-browser vulnerabilities in the current reporting period than have been seen in previous reports; this is particularly notable in the case of Internet Explorer. This may reflect the preventative security measures being taken by many vendors in response to widely exploited security threats. Drive-by-downloading—the use of vulnerabilities in browsers to force software installs (such as spyware, which itself has come to be associated with browser insecurity)—has also become common, forcing vendors to act quickly in response to user complaints.

[60] For instance, MS04-037, a vulnerability exploitable through MSIE, was released outside of their regular cycle. See:
http://www.microsoft.com/technet/security/advisory/903144.mspx

Malicious Code Trends

This section of the Symantec *Internet Security Threat Report* will analyze developments in malicious code over the first half of 2005. Symantec gathers data from over 120 million desktops that have deployed Symantec's antivirus products in consumer and corporate environments. The Symantec Digital Immune System™ and Scan and Deliver technologies allow customers to automate this reporting process. This discussion is based on malicious code samples reported to Symantec for analysis between January 1 and June 30, 2005.

Symantec categorizes malicious code in two categories: families and variants. A family is a new, distinct sample of malicious code. For instance, W32.Netsky@mm would have been the founding sample, or the primary source code, of the Netsky 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. 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. For instance, Netsky.P is a variant of Netsky.

The "Malicious Code Trends" section will discuss:

- Top ten malicious code samples
- Win32 viruses and worms
- Exposure of confidential information
- Threats to mobile devices
- Malicious code for P2P, IM, IRC, and CIFS
- Bots
- Bot variants
- Malicious code for profit

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 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 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 trusted source, and the purpose of the attachment is known.

Top ten malicious code samples

In previous editions of the Symantec *Internet Security Threat Report*, mass-mailing worms dominated the top ten malicious code samples reported to Symantec. In this edition, there were only two mass-mailers in the top ten, Netsky.P and Sober.O (table 5). This is due, in part, to the lack of any successful new mass-mailers in the last six months, with the exception of Sober.O. While there were a large number of moderately successful Mytob variants, no single variant enjoyed the level of success that Netsky or Sober variants have had.

Rank	Sample	Type	Vectors	Impact
1	Netsky.P	Worm	SMTP, P2P	Logs e-Gold account information
2	Gaobot	Bot	CIFS, Remotely Exploitable Vulnerability, Back doors	Allows remote access
3	Spybot	Bot	CIFS, Remotely Exploitable Vulnerability, Back doors	Allows remote access
4	Tooso.F	Trojan	NA	Disables security applications, downloads a remote file
5	Tooso.B	Trojan	NA	Disables security applications, downloads a remote file
6	Redlof.A	Virus	Email	Infects several file types
7	Lemir	Trojan	NA	Steals account information for Legend of Mir online game
8	Lineage	Trojan	NA	Steals account information for Lineage online game
9	Sober.O	Worm	SMTP	Downloads and executes a remote file
10	KillAV	Trojan	NA	Disables security applications

Table 5. Top ten malicious code samples reported to Symantec
Source: Symantec Corporation

As in the previous six-month period, Netsky.P[61] remained the most reported malicious code sample in the first half of 2005. It has been one of the most widely reported samples of malicious code since its discovery in March 2004.

This particular variant of Netsky utilizes multiple propagation techniques. It emails itself to addresses gathered from a compromised computer. It also copies itself to shared network drives and to folders commonly associated with various peer-to-peer file sharing programs. 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 vulnerability[62] 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.

---

[61] http://securityresponse.symantec.com/avcenter/venc/data/w32.netsky.p@mm.html
[62] http://www.securityfocus.com/bid/2524

Gaobot and Spybot remain in the top ten malicious code reports for this period, as they were for the second half of 2004. As noted in previous editions of the *Internet Security Threat Report*, the use of bots continues to increase, possibly due to the large amount of and variance in functionality they can incorporate. Whereas Gaobot and Spybot were the third and fourth most reported malicious code samples in the second half of 2004, they rose to second most and third most respectively in this period. This is likely due less to any increase in the prevalence of the two bots and more to the drop-off in Sober.l activity. This drop-off may be due to a combination of factors, including the fact that as users update their antivirus definitions, reports of the malicious code will drop off even though it may continue to circulate.

Between January and June 2005, Trojans dominated the top ten reported samples, most notably two variants of the Tooso Trojan.[63] The B and F variants of this Trojan do not contain any mass-mailing code, but they were mass mailed by variants of the Beagle[64] worm.[65] These Trojans disable and remove several antivirus and security applications from a compromised computer. They then disable access to antivirus and security-related Web sites by overwriting the HOSTS file to redirect requests. Finally, the Trojans attempt to download and execute a file from a remote Web site.

Win32 viruses and worms

Win32 threats are executable programs that operate by using the WIN32 API. These forms of malicious code work on at least one Win32 platform. During the first six months of 2005, Win32 threats continued the increase in volume that was first noted in 2003 (figure 21).

Over the first half of 2005, Symantec documented more than 10,866 new Win32 viruses and worms, an increase of 48% over the 7,360 documented in the second half of 2004. It is also an increase of 142% over the 4,496 documented in the first half of 2004. As of June 30, 2005, the total number of Win32 variants had surpassed 28,000. The substantial rise in numbers over the past six months is due to the tremendous increase of Win32 worms that implement bot features—such as remote access through IRC channels and denial of service capability—that attackers can use for financial gain. (Please see the "Malicious code for profit" section below for an in-depth discussion of this recent development in malicious code.)

[63] http://securityresponse.symantec.com/avcenter/venc/data/trojan.tooso.html
[64] http://securityresponse.symantec.com/avcenter/venc/data/w32.beagle.a@mm.html
[65] Tooso.B was mass mailed by Beagle.BG and Beagle.BH while Tooso.F was mass mailed by Beagle.BN.
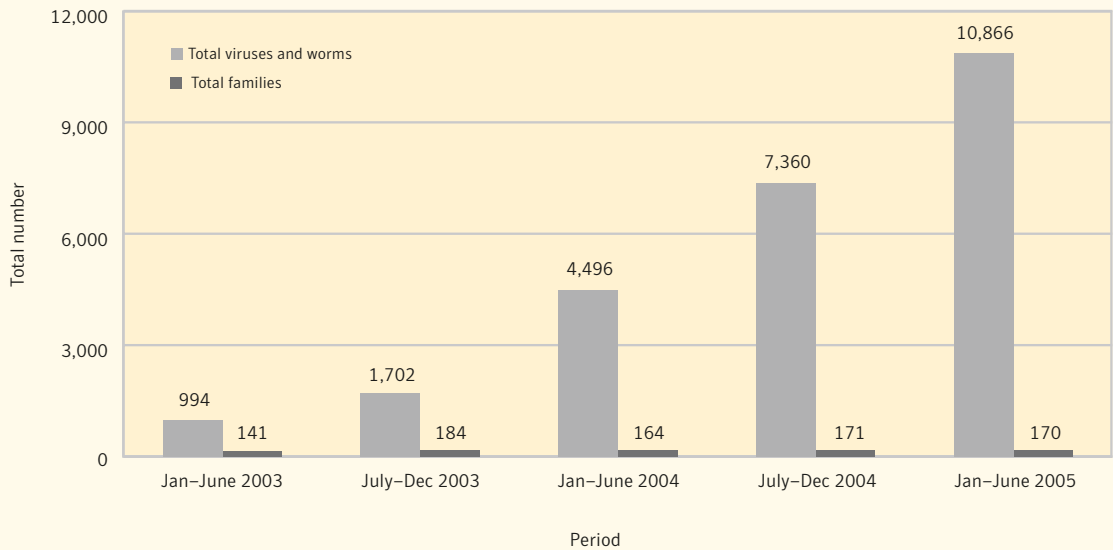
Figure 21. New Win32 virus and worm variants, 2003–2005
Source: Symantec Corporation

With the significant growth in Win32 viruses and worms, the number of new Win32 families could be expected to also show a notable increase, but this has not been the case. The number of new families reported has remained relatively level for the past five reporting periods (figure 21), indicating that the vast majority of the new viruses and worms reported are variants of existing families.

In many cases, a successful worm is modified slightly in an effort to reproduce the success of the original, thus creating a new variant. In other cases, the source code for a piece of malicious code may be readily available, allowing even novices to create new malicious code variants. The rapid rise in variants is important because each variant represents a new, distinct threat against which administrators must protect their systems.

Despite the fact that only two individual mass-mailing worms were present in the top ten malicious code during this period, this class of worm continues to be successful. In the first half of 2005, mass-mailing worms such as Sober.O and the Mytob family were amongst the most significant outbreaks.

It appears that development of classic virus code—that is, viruses that infect files in order to propagate—is slowing. This may due to the increased success of criminal prosecutions against attackers. For example, the German author of the Sasser and Netsky worms, which accounted for 20% of all malicious code samples reported to Symantec in 2004,[66] was recently prosecuted,[67] along with several other high-profile virus writers. The decline of the classic virus is also likely due to the high levels of Internet connectivity, which has increased the effectiveness of direct propagation techniques, such as host-to-host propagation, thereby diminishing the reliance on files as the infection vector.

[66] Please see the "Appendix D" of this report for details on how this figure was obtained.
[67] http://www.securityfocus.com/news/11238

Attackers continuously look for easy targets, those that will provide them with the maximum return on the time they invest in writing malicious code. Since there have been fewer easily exploitable, remote code-execution vulnerabilities in Windows recently, attackers are moving towards applications and services provided by third parties. At the same time, a number of Windows XP Service Pack 2 vulnerabilities have been reported. Interestingly, some of these vulnerabilities apply to the 64-bit Windows platforms, thus raising the possibility of exploitation of 64-bit Windows. For example, the Microsoft Windows Shell Remote Code Execution Vulnerability[68] affects Windows XP computers with Service Pack 2 as well as 64-bit versions of Windows XP. This vulnerability can be exploited in a way that would bypass the unsigned content execution warning[69] that was introduced as a security feature of Windows XP Service Pack 2.

Recent Win32 attacks have been specific to the Windows Security Center, a part of Windows XP Service Pack 2. Such attacks perform a variety of tasks, including silently switching off the firewall and adding application-specific exclusions that allow an application to contact the Internet without producing warnings. For example, the Reitrec[70] Trojan turns off the Windows XP Service Pack 2 firewall in order to allow it to download remote files related to adware programs on a compromised computer.

To protect against threats that disable software firewalls, additional layers of security are needed. Administrators can prevent these threats from accessing remote resources by using egress filtering and deploying firewalls on host systems. This is particularly important in enterprise settings, in which a single compromise can result in additional compromises within the local network.

Exposure of confidential information

Threats that expose confidential information from a compromised computer are a concern to all users, in the home and enterprise environment alike. These threats may expose system information, sensitive files and documents, or cached logon credentials. Some threats, such as back doors, may give a remote attacker complete control over a compromised computer. 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.[71]

During the first six months of 2005, threats with the potential to expose confidential information continued to increase, as they have for the past three reporting periods (figure 22). Between January 1 and June 30, 2005, malicious code that exposes confidential information represented 74% of the top 50 malicious code samples reported to Symantec. This is an increase of 37% over the previous reporting period in which 54% of the top 50 malicious code samples exposed confidential information. It is a 68% increase over the 44% reported in the same period in 2004.

[68] http://www.securityfocus.com/bid/13132
[69] This feature warns the user that they may be executing unsigned code that could potentially be harmful to their computer.
[70] http://securityresponse.symantec.com/avcenter/venc/data/downloader.reitrec.html
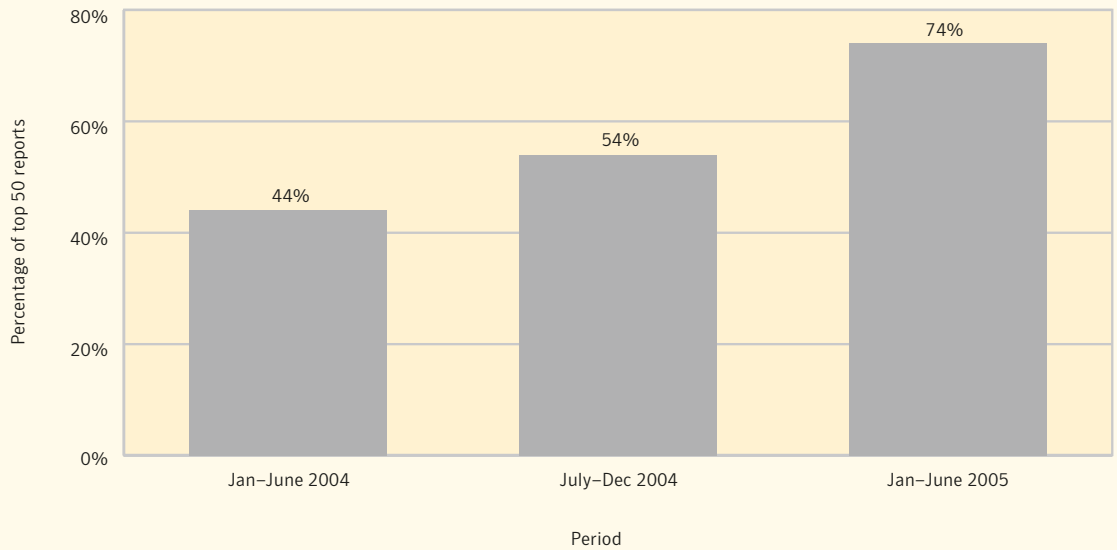[71] http://www.securityfocus.com/news/11219

Figure 22. Threats to confidential information
Source: Symantec Corporation

As noted in the previous *Internet Security Threat Report*, the rise in confidential information threats may be due, at least in part, to the increase in bots; however, other new threats also helped contribute to this trend. For example, the Mytob[72] family of mass-mailing worms also includes remote access capabilities. During the month of June 2005, 97 variants of Mytob were reported to Symantec. This family of worms was produced in extremely rapid succession, with multiple new variants of the family being observed in the wild on the same day. Such rapid production of variants is likely intended to overwhelm security administrators who are trying to keep their systems up-to-date. In such a case, protective technology such as behavior-blocking technologies can be used to help secure users against these threats.

Mobile devices

Malicious code writers continue to create proof-of-concept malicious code for mobile devices, particularly 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 MMS and other telephony protocols.

In the second half of 2004, multiple variants of Cabir,[73] the first mobile device worm, which spreads via Bluetooth, were detected due to the release of source code. However, the beginning of 2005 saw a decline in new variants with only two released in early January. Cabir was originally created as a proof of concept, but has now been reported in the wild in 17 countries.

[72] http://securityresponse.symantec.com/avcenter/venc/data/w32.mytob.db@mm.html
[73] http://securityresponse.symantec.com/avcenter/venc/data/symbos.cabir.html

In the second half of 2004, two newly documented malicious code samples for the Windows CE operating system—Duts[74] and Brador[75]—were documented. In the first half of 2005, Symantec did not document any additional threats for this platform. This does not mean that research in this area has ceased entirely. However, because smart phones are widely used and offer high connectivity, they will likely constitute a more appealing target than Windows CE. Malicious code authors may be focusing their efforts on these platforms instead.

This suspicion was borne out in March when the first MMS worm, Commwarrior,[76] was discovered. While previous malicious code for Symbian devices used only Bluetooth as a propagation vector, Commwarrior also uses MMS. This is significant because Bluetooth requires physical proximity between an infected device and a target in order to propagate. MMS only requires a connection between a phone and the network in order to send messages and files to other phones. This has the potential to expand the scope of an outbreak from the local to the global level.

Commwarrior randomly chooses a phone number from the compromised device's phonebook. It then sends an MMS message that contains the worm itself to that number as an attachment named commw.sis, which the recipient has to run for it to propagate. The MMS message contains one of a variety of subject headers and message bodies purporting to be a legitimate free software application. Within four months of initial discovery, Commwarrior had been detected in 15 countries.[77]

The first half of 2005 saw a rise in the number of Skulls[78] variants. Skulls is a simple Symbian Trojan that overlays existing applications, rendering the device inoperable by overwriting critical operating system files. Six new variants of Skulls appeared in the first half of 2005, tripling the number of known variants. A few users have reported being affected by Skulls but none of these reports have been confirmed. The inability of Skulls to replicate on its own means that it poses less of a threat than a worm or virus. However, it has been released on message boards as a program to bypass product activation keys for legitimate software applications.

While the number of threats to mobile devices, particularly Symbian Series 60 smart phones, continues to increase, the number reported in the wild is still small. To this point, most have been proof-of-concept threats that have found their way into the wild. Nevertheless, the types of threats created demonstrate some of the robust capabilities of these devices.

As is the case for most malicious code, users can protect themselves against these threats by practicing safe computing practices. For instance, they can help prevent infection from these programs by not installing unknown programs or accepting connections from unknown sources. It is somewhat surprising that no automatically propagating malicious code has yet been developed and released into the wild, particularly as platform complexity and connectivity have risen to sufficient levels for a widespread outbreak.

[74] http://securityresponse.symantec.com/avcenter/venc/data/wince.duts.a.html
[75] http://securityresponse.symantec.com/avcenter/venc/data/backdoor.brador.a.html
[76] http://securityresponse.symantec.com/avcenter/venc/data/symbos.commwarrior.a.html
[77] http://www.virus.org/modules.php?op=modload&name=News&file=article&sid=118
[78] http://securityresponse.symantec.com/avcenter/venc/data/symbos.skulls.html

P2P/IM/IRC/CIFS

While peer-to-peer services (P2P), instant messaging (IM), Internet relay chat (IRC), and network file sharing (CIFS) continue to be used as propagation vectors for the top threats, their effectiveness appears to be on the decline. In the first half of 2005, only 19% of the top 50 malicious code reported to Symantec used one of these replication vectors, compared with 50% in the previous six months and 36% one year ago (figure 23).

In the final six months of 2004, Mydoom,[79] Netsky, and Beagle variants dominated the top ten malicious code reports and all possessed the ability to spread via P2P. However, in the first half of 2005, of those three, only Netsky appeared in the top ten. As a result, the primary infection vector has shifted from P2P applications to a combination of P2P applications and Windows CIFS. Nevertheless, a downward trend in the use of these replication vectors continues.
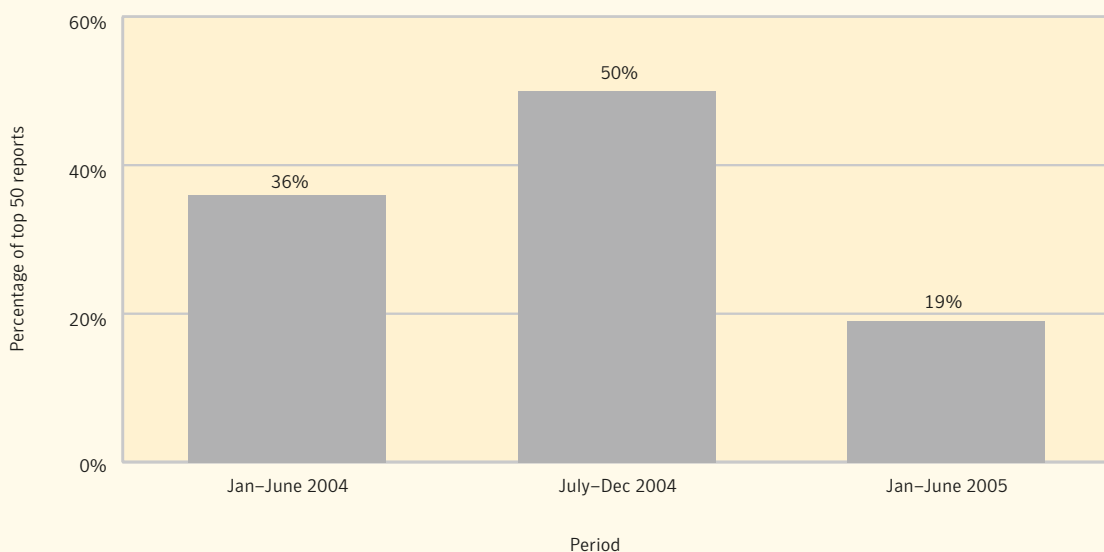

Figure 23. P2P, IM, IRC, and CIFS threats
Source: Symantec Corporation

None of the top 50 reported malicious code samples this period used IM as a propagation mechanism. However, the number of threats in the overall count of malicious code samples that used IM as a propagation vector did increase. This was mainly due to multiple variants of the Bropia[80] and Kelvir[81] families. Both are worms that send URL links via MSN Messenger to people on a compromised computer's contact list. The URL link is either a link to the worm itself or to a variant of Spybot.

The first variant of Bropia was detected in January 2005, and 39 variants have been discovered since. Kelvir was first spotted in March 2005; by the end of June, 130 variants had been discovered. However, neither worm has appeared in the top 50, demonstrating the general ineffectiveness of the propagation

vector compared to other common vectors, such as email. One likely reason for this is that the actual executable file was not transferred through the instant messages but was hosted in a separate location instead. This means that once authorities removed access to the executable file from the hosting server, the worm could no longer propagate.

In addition, a buffer overflow in the image–processing component of Microsoft Messenger[82] was made public in February and led to speculation that it may be the next step in threats such as Bropia. However, days after the vulnerability was patched, Microsoft required all their MSN messenger clients to be updated before users could join the network. This eliminated the possibility of the vulnerability being used as a replication vector. This mitigation strategy will likely prevent malicious threats from exploiting such vulnerabilities in instant messaging systems.

Because these vectors continue to appear in the top ten threats, organizations should still audit networks for rogue usage of peer-to-peer applications and protocols. In addition, any approved applications should be regularly updated with all necessary security-related patches.

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.

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. Additionally, bots can be used to perform DoS attacks against the enterprise's Web site, which can disrupt revenue for ecommerce companies, or against other organizations' Web sites, which can have serious legal consequences.

In the first half of 2005, the percentage of bot-related malicious code reported to Symantec increased, accounting for 14% of the top 50 (figure 24). This represents a 17% increase since the last half of 2004, when bots accounted for 12% of the top 50 malicious code reports. It is also a 40% increase over the 10% from the six-month period prior to that.
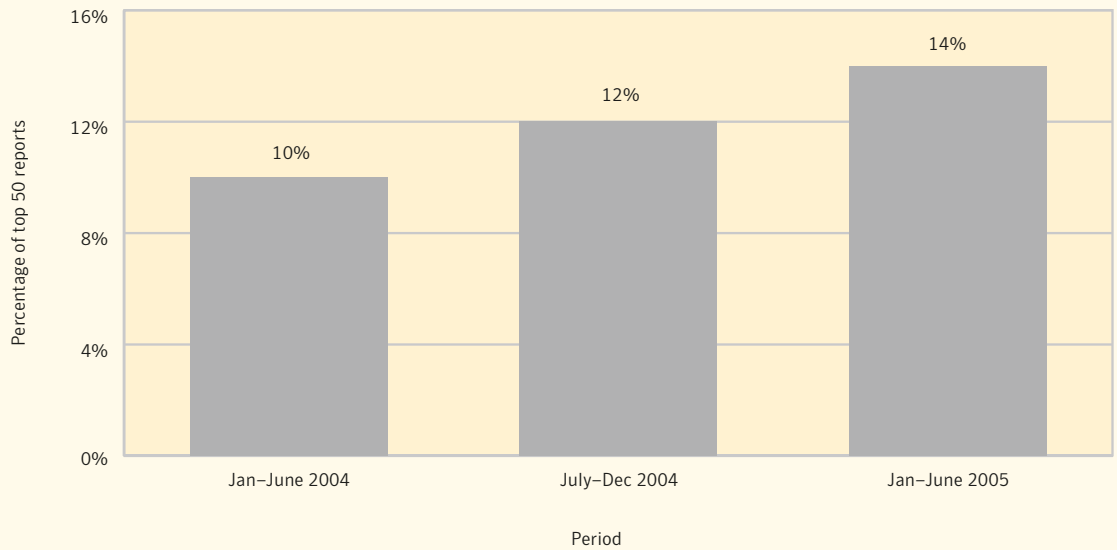
82 http://www.securityfocus.com/bid/12506

Figure 24. Bots in top 50 malicious code reports
Source: Symantec Corporation

Bots often employ multiple propagation mechanisms to compromise other computers. They may copy themselves to shared network drives with weak password protection. They may also spread through P2P networks by copying themselves to the shared folders of the P2P client application. Most bots, such as Randex,[83] Spybot, and Gaobot, employ multiple propagation mechanisms that also include exploiting vulnerabilities in remotely accessible services, such as the Microsoft Windows LSASS Buffer Overrun Vulnerability.[84]

The most significant new development in bot technology over the first six months of 2005 was the addition of a new propagation mechanism. In addition to propagating by traditional methods such as those mentioned above, Spybot.IVQ,[85] propagated through Microsoft SQL and MySQL servers with weak password protection. Symantec believes this is significant since it indicates that bot authors may be looking to increase the number of potential systems they can control.

83 http://securityresponse.symantec.com/avcenter/venc/data/w32.randex.gen.html
84 http://www.securityfocus.com/bid/10108
85 http://securityresponse.symantec.com/avcenter/venc/data/w32.spybot.ivq.html

Bot variants

During the first six months of 2005, the number of new bot variants continued to climb, particularly the number of new Spybot variants. In the current period 6,361 new variants of Spybot were reported to Symantec, a 48% increase over the 4,288 variants documented in the second half of 2004.

While the number of new Gaobot and Randex variants decreased slightly between the first and second half of 2004, they rose again in the first half of 2005, although not to the same degree as Spybot. In the first half of 2005, there were 1,412 new Randex variants and 1,121 new Gaobot variants, 54% and 47% increases over the previous six-month period respectively (figure 25).

While more variants of Spybot were created in the last two periods than Gaobot variants, Gaobot was reported more often to Symantec. This is likely because Gaobot variants typically contain more propagation mechanisms than Spybot variants. While a Spybot variant typically only propagates through a few vulnerabilities, a Gaobot variant may propagate through several different vulnerabilities as well as network shares. Therefore, a single Gaobot variant can be used to spread to a large number of different systems, while a Spybot variant has a much more limited scope of potential targets. As a result, an attacker using Spybot is more likely to employ multiple variants, each of which exploits a different set of vulnerabilities. This results in a large number of Spybot variants, each of which affects a smaller range of vulnerable computers.
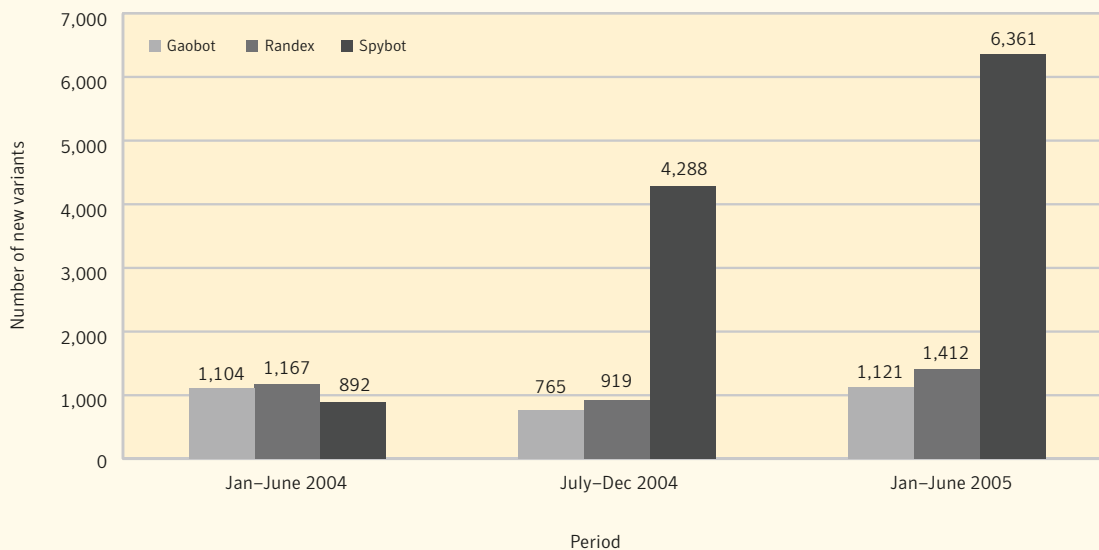

Figure 25. Number of new bot variants
Source: Symantec Corporation

Symantec Internet Security Threat Report

Malicious code for profit

In the previous edition of the *Internet Security Threat Report*,[86] Symantec stated that malicious code that can be used to generate profit appears to be on the rise. That discussion focused mainly on the growing use of malicious code to relay bulk unsolicited email (spam) for profit. This trend continues. In the first half of 2005, 64% of the top 50 malicious code samples reported to Symantec allowed email relaying, compared to 53% in the last six months of 2004 and 37% in the first half of the year (figure 26).
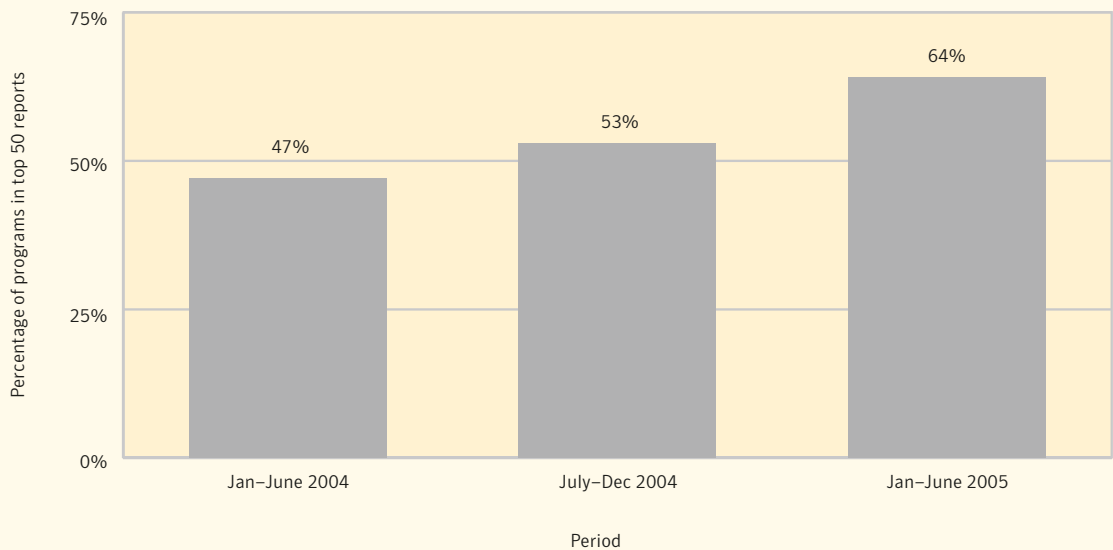

Figure 26. Malicious code that allows email relaying
Source: Symantec Corporation

During the first six months of 2005, new methods of using malicious code for financial gain were observed with increasing frequency. One example is the development of bot networks for financial gain. In the "Future Watch" section of the previous *Internet Security Threat Report*, Symantec stated that it was realistic to "expect more growth in bot owners who modify their bot networks and rent them out for these purposes, amongst others."[87] The Symantec DeepSight threat analyst team has uncovered evidence indicating that this is already happening.

The Symantec DeepSight Threat analyst team has uncovered evidence indicating that bot networks that can be used for malicious purposes are available for hire. In July 2005, in an IRC conversation that the DeepSight team was monitoring, a self-proclaimed bot network owner revealed the size, capacity, and price of a bot network that he was making available.

These discussions revealed that it is not uncommon for those who maintain control of these networks to provide full or partial access to the compromised systems for a nominal fee. Users who desire the functionality of bot networks but who lack the skill or resources to develop their own can solicit those services from bot network owners. These services are typically solicited for purposes of profit or general malicious activity.

Prices negotiated between these individuals will vary. The Symantec DeepSight investigation discovered, however, that the use of a network as large as 150,000 bot computers can carry a cost as low as approximately U.S.$300. This price may be influenced by the number of hosts within the bot network, as well as the duration and level of access granted to the compromised hosts. Other factors may include the collective bandwidth, the functionality of the actual bots deployed, and the stability of the network.

In addition to offering access to an existing bot network, conversations were observed in which unique customized versions of a bot binary could reportedly be purchased. Claims were made that because such binaries are unique, they would not be detected by current antivirus definitions. While it is possible to create a unique binary to avoid detection by previous antivirus definitions, most antivirus products will be able to identify the threat using a generic definition or a heuristic signature. The cost associated with this service was reportedly between U.S.$200 and U.S.$300.

Another method of using malicious code for profit is the use of Trojans. One such case that was reported to Symantec in the first half of 2005 was the Gpcoder[88] Trojan. This Trojan encrypts data files such as documents, spreadsheets, and database files on the compromised computer. It then creates a file in each folder containing information on how the user can obtain a decoder for the encrypted files. Reportedly, if the user emails an address that is provided, he or she is instructed to pay $200 for the decoder application.

For enterprise systems, this Trojan can cause serious data loss if proper backup plans are not in place. Effective disaster recovery strategies should always be part of security planning in order to protect against attacks that are capable of destroying or modifying critical data.

Another example of malicious code for profit is malicious code that downloads adware onto a compromised computer. For example, the Lazar Trojan[89] downloads and installs adware that displays pop-up advertisements in the user's Web browser. The malicious code author earns a fee each time the adware is installed on a computer. Over the first six months of 2005, seven distinct malicious code samples that downloaded adware were present in the top 50 malicious code reports, including two variants of the Vundo[90] Trojan and the Desktophijack[91] virus. There was only one in the second half of 2004 and none in the first six months of the year (figure 27).

[88] http://securityresponse.symantec.com/avcenter/venc/data/trojan.gpcoder.html
[89] http://securityresponse.symantec.com/avcenter/venc/data/trojan.lazar.html
[90] http://securityresponse.symantec.com/avcenter/venc/data/trojan.vundo.html and http://securityresponse.symantec.com/avcenter/venc/data/trojan.vundo.b.html
[91] http://securityresponse.symantec.com/avcenter/venc/data/w32.desktophijack.html
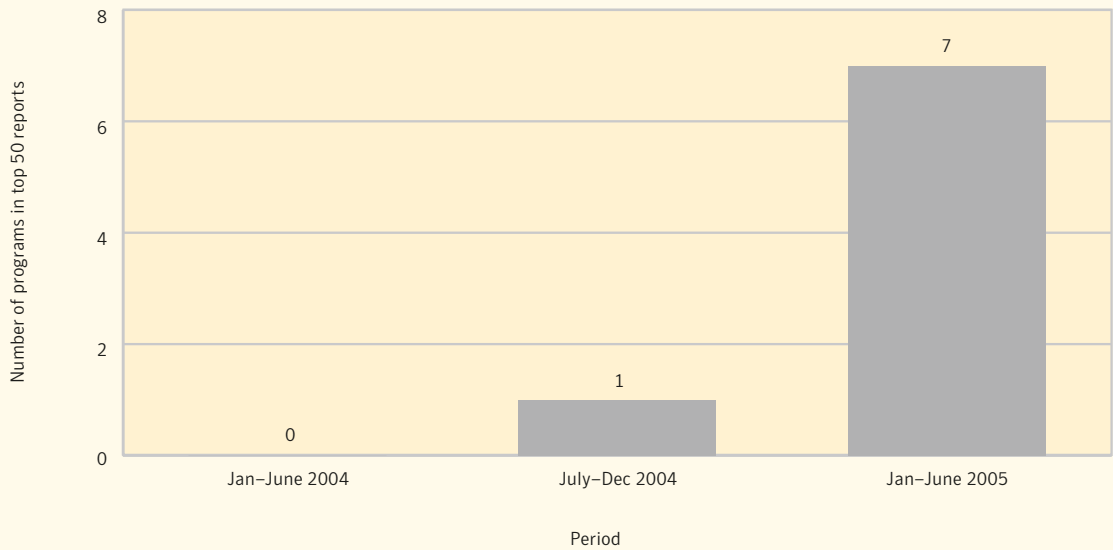
Figure 27. Malicious code that downloads adware

A more worrisome trend in the use of malicious code for profit has been observed in the form of targeted Trojan attacks. At the end of May, several executives at large companies in Israel were arrested for allegedly using Trojans to monitor their competitors.[92] A private investigation firm was reported to have written a custom Trojan program[93] that was then sent to users at the competing companies to entice them to execute the application. Once installed, this Trojan would log keystrokes and allow remote access to the compromised computer, allowing the authors to illicitly obtain sensitive information from their competitors.

Another targeted Trojan attack that was observed over the last six months was aimed at U.S. and U.K. government agencies.[94] These attacks are specific to the agency being targeted and may arrive as email attachments or be installed by exploiting a vulnerability in Microsoft Word.[95] Once installed, these Trojans[96] have the ability to download other applications and open back doors on the compromised computers.

The threat of targeted Trojan attacks is one that Symantec will continue to monitor closely. Since attacks are usually targeted to a specific user or group of users, it is likely that social engineering will be used to persuade users to run the Trojan application. To protect against these threats, users should always verify the authenticity of any application before running it on critical computers. Administrators should deploy defense in-depth strategies such as firewalls and email gateway protection to stop these threats from reaching end users. Additionally, updated antivirus applications should be installed on every desktop to protect users if the malicious code is able to get past external security layers.

[92] http://www.wired.com/news/privacy/0,1848,67684,00.html?tw=rss.PRV
[93] http://securityresponse.symantec.com/avcenter/venc/data/trojan.hotword.b.html
[94] http://www.securityfocus.com/news/11222
[95] http://www.securityfocus.com/bid/8835
[96] http://securityresponse.symantec.com/avcenter/venc/data/trojan.mdropper.b.html and http://securityresponse.symantec.com/avcenter/venc/data/trojan.riler.c.html

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 first six months of 2005. In particular, it will examine trends in adware, spyware, phishing, and spam.

Adware and spyware

While adware and spyware are not categorized as malicious code, Symantec monitors them using many of the same 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,[97] 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. Steps for the protection against and mitigation of these security risks are presented at the end of this discussion.

Adware

Adware programs are programs that facilitate the delivery and display of advertising content onto the user's display device.[98] This may be done without the user's prior consent or knowledge. It 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—such as information related to Internet browser usage or other computing habits—and relay this information back to a remote computer.

Adware is not always a security risk. In some cases, it simply delivers an advertising message that appears on the user's screen. However, this is not always the case. Depending upon its functionality and the context in which it is deployed, adware can constitute a security risk. If attributes of a security risk include the compromise of the confidentiality, availability, or integrity of data on a computing system, some forms of adware qualify. For example, they may do so by:

• Tracking user Web use and compiling a profile on the user's browsing habits.
• Occupying bandwidth, thereby diminishing the functionality and availability of a computing system.
• Modifying the Winsock.dll[99] in order to monitor the user's Web browsing habits, thereby affecting the integrity of the computer.

Volume of adware

During the first six months of 2005, the percentage of adware in the top 50 programs reports to Symantec increased dramatically over the two previous reporting periods (figure 28). Between January 1 and June 30, 2004, adware made up 4% of the top 50 programs reported. In the second half of 2004, it made up 5% of the top 50 reports. Between January 1 and June 30, 2005, however, it made up 8% of the top 50 reports. This increase is likely due to a combination of three factors: increased anti-adware capability in security products, resulting in improved detection; an increase in adware itself; and increased use of products designed to deal with unwanted adware.
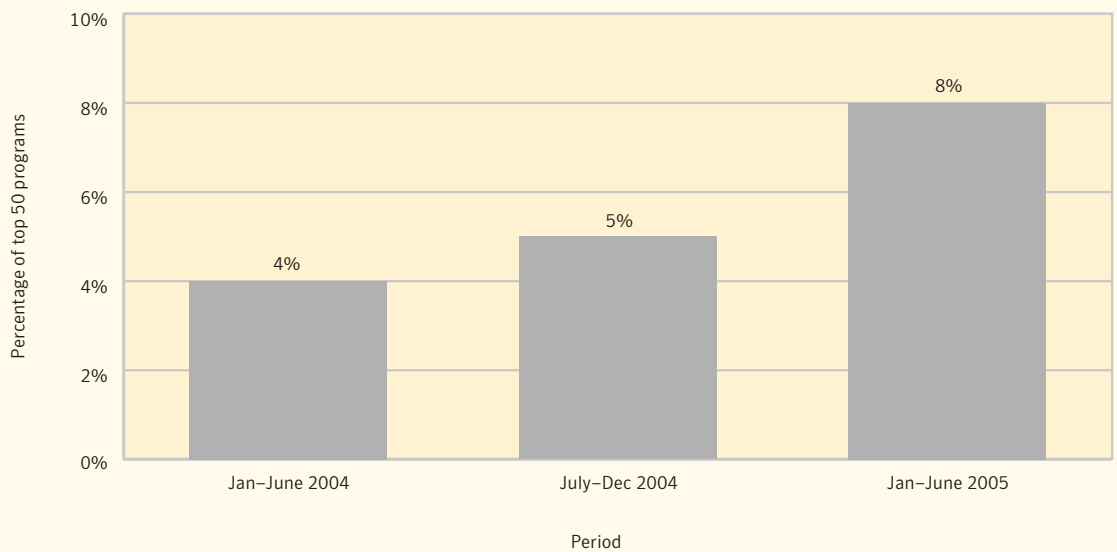

Figure 28. Percentage of adware in top 50 reports
Source: Symantec Corporation

Top ten reported adware

The most reported adware program between January 1 and June 30, 2005, was ShopAtHomeAgent,[100] which accounted for 19% of the top ten adware programs reported (table 6). This program is a new addition to the *Internet Security Threat Report*. It downloads and displays advertisements; however, it may also redirect access to certain Web sites through www.shopathomeselect.com, depending on whether or not the target site is affiliated with ShopAtHomeSelect.com. This redirection may result in insecure transactions, putting the user's confidential data at risk.

Rank	Program name
1	ShopAtHomeAgent
2	Istbar
3	CoolWebSearch
4	SearchAssistant
5	Iefeats
6	Gain
7	BetterInternet
8	VirtuMonde
9	EliteBar
10	NdotNet

Table 6. Top ten adware
Source: Symantec Corporation

The second most common adware program over the first six months of 2005 was Istbar,[101] a program that makes up 14% of the top ten reports. This program was previously ranked fourth. Istbar is a family of adware programs that install via an Internet Explorer toolbar, often using aggressive, persistent techniques. Some versions of ISTbar hijack Internet Explorer home pages and search results as well as displaying pop-up advertisements. Depending on the version, the pop-up advertisements may be pornographic in nature.

CoolWebSearch[102] was the third most commonly reported adware for the first half of 2005, making up just over 13% of the top ten adware reports. This program is new to the top ten. CoolWebSearch is a large family of security risk programs that may be manually installed or bundled with another program. The programs in the CoolWebSearch family exhibit a variety of different behaviors, but have been observed hijacking searches, which are then redirected to their Web site or an affiliate. Programs in the CoolWebSearch family have used stealth behavior to remain undetected and installed on a system.

[100] http://securityresponse.symantec.com/avcenter/venc/data/adware.sahagent.html
[101] http://securityresponse.symantec.com/avcenter/venc/data/adware.istbar.html
[102] http://securityresponse.symantec.com/avcenter/venc/data/adware.coolwebsearch.html

Adware installation

There are numerous different ways by which adware can be installed on a user's computer (table 7). The following sections will discuss some of those installation methods and offer suggestions for the prevention of unauthorized installation. It should be noted that some additional security risks use more than one method of installation.

End user license agreements (EULAs)

Many companies use adware as a way of providing services while lowering costs to customers. This is particularly true of software that is made available for users to download for free (popularly known as freeware). These programs usually require the user to agree to an EULA.

A EULA is a legal contract between the manufacturer and/or the author, producer and/or vendor of an application and the end user that stipulates the conditions under which the software may be obtained and used, and lists any restrictions that the author, producer and/or vendor may impose on the end user. EULAs can be complicated and confusing. While some adware presents the user with a EULA that is easy to read, advising specifically and clearly what actions the program will take, this is not always the case. The user may unknowingly consent to the installation of this adware by accepting the EULA because the agreement is so complex that the user is unable or unwilling to read and understand the terms and conditions before agreeing to them.[103] Assuming that the information in the EULA is correct and acceptable to the user, the risk presented by an introduction of this type of adware is minimal.

Adware can also be installed by a third-party software provider after the user has accepted the software EULA and installed the program. During the first six months of 2005, five of the top ten adware programs reported to Symantec were installed as a result of accepting a third-party EULA (table 7): Betterinternet, ISTBar, GAIN, ShopAtHomeAgent and 180Search. This is an increase over the last six months of 2004, during which three of the top ten adware programs were installed as a result of the user accepting a EULA.

It should be noted that the presence of the EULA can be dependent upon the configuration of the adware program (for instance, turning on registry keys, etc.), as well as upon the preferences and practices of third party affiliates. As a result, different users are likely to have different experience with adware programs.

Bundling

As was discussed in the previous section, some companies increase the distribution of their software by offering it to users for free download. In order to generate revenue from this software, the producers often "bundle" the free software with adware. This is particularly true of peer-to-peer file sharing programs. In some cases, the user may be notified of this bundling in the EULA but not always. When the software is run on the user's system, the adware is also installed, either with the user's knowledge and consent or without it. In the first six months of 2005, seven of the top ten adware programs were bundled with other programs (table 7). In the last six months of 2004, nine of the top ten programs installed by bundling.

---

[103] It should be noted that users often accept the terms of a EULA as an acceptable cost to pay to obtain the software with which the EULA is associated. As such, these end users must accept the consequences of accepting the EULA.

Web browsing

Adware is often installed through the user's Web browser. This can be done through pop-up ads offering free software to download. The pop-up sometimes offers the user a choice of clicking "Yes" or "No" to accept or reject the offer. In reality, though, clicking anywhere on the ad often results in the download of adware. Browser-installed adware may also be installed through ActiveX[104] controls or browser helper objects (BHOs).[105] Eight of the top ten adware programs reported to Symantec in the first six months of 2005 were installed through Web browsers (table 7). This is an increase over the five reported in the last six months of 2004.

Symantec has conducted an internal study designed to determine the relationship between the types of sites visited and the adware or spyware downloaded on the user's machine. Symantec security researchers spent one hour surfing well known Web sites and found that after one hour of navigating children's Web sites, 359 adware programs had been installed on the user's computer. Of all the categories of Web sites visited, this was far and away the highest number of adware programs installed.[106] This indicates that sites targeting children may have a disproportionately high rate of adware installation. This could be because children are more likely to click on prompts or buttons in order to quickly get to the activities they wish to explore. It is possible that machines used predominately by children may not be regularly updated.

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 require ActiveX, in which case they should configure their browser 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.

Program name	Displays EULA	Bundled	Uses BHO
180Search	Yes	Yes	Sometimes
BetterInternet	Yes	Yes	Yes
CoolWebSearch	No	No	Yes
EliteBar	No	No	Yes
Gain	Yes	Yes	Sometimes
Iefeats	No	Yes	Yes
Istbar	Yes	No	Yes
NdotNet	No	Yes	Yes
ShopAtHomeAgent	Yes	Yes	No
VirtuMonde	No	Yes	No

Table 7. Adware installation methods
Source: Symantec Corporation

---

[104] ActiveX is set of Microsoft technologies that allows users to share information among different programs. For more information on ActiveX, please visit: http://msdn.microsoft.com/library/default.asp?url=/workshop/components/activex/intro.asp

[105] Browser helper objects (BHOs) are add-on programs that can add legitimate features to a user's browser (Internet Explorer 4.X and up). For example, document readers that used to read programs within the browser do so through BHOs.

[106] Other categories of Web sites include: sports, gaming, news, reseller (auction), shopping, and travel.

Spyware

Spyware programs are stand-alone programs that can secretly 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 utilized by organizations to monitor 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 usernames, passwords, banking information, and credit card details. This can be done through keystroke logging and by capturing email and instant messaging traffic. Because spyware can capture sensitive information before it is encrypted for transmission, it can bypass security measures such as firewalls, secure connections, and VPNs. Spyware is a particular concern because of its potential for use in identity theft and fraud.

Top ten reported spyware

In the first six months of 2005, Webhancer[107] was the top spyware program, accounting for 29% of the top ten spyware programs reported overall (table 8). It was also the most reported spyware program during both reporting periods of 2004. Webhancer monitors the user's browsing habits, sending the information back to its centralized servers. The program has a EULA; however, it is also capable of updating itself from the servers. This means that updated versions may contain additional functionality that the user may not have agreed to as part of the original EULA. For example, the additional functionality may disable antivirus software or allow remote access of the machine.

Rank	Program name
1	Webhancer
2	Apropos
3	Marketscore
4	CometCursor
5	e2give
6	Perfect
7	ISearch
8	Goidr
9	ISpynow
10	KeyTick

Table 8. Top ten spyware reports
Source: Symantec Corporation

Apropos,[108] was the second most reported spyware program in the first six months of 2005, making up 27% of the top ten spyware reports. It was ranked third in the second half of 2004. An Internet Explorer browser helper object (BHO) installed by an ActiveX control, Apropos installs a toolbar that links to Web sites and sends information back to its server. Additionally, the application may download and install other files on the user's computer. In some cases these files 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.

[107] http://securityresponse.symantec.com/avcenter/venc/data/spyware.webhancer.html
[108] http://securityresponse.symantec.com/avcenter/venc/data/spyware.apropos.html

The third most reported spyware program, Marketscore,[109] is a new addition to the top ten most reported spyware programs, making up 19% of the top ten reported spyware programs. When Marketscore is installed on a computer, it starts a proxy service. Once this service has executed, all the systems' Internet connections will be routed through the Marketscore's proxy, called OSSProxy. The publisher states that the program is designed to improve the speed of the Internet connection by using OSSProxy. However, because all of the system's Internet connections will go through the Marketscore proxy, Internet usage information may be logged and submitted to Marketscore's customer companies. This could introduce a security risk, depending upon customer preferences and policies.

Spyware installation

As is the case with adware, there are numerous different ways by which spyware programs can be installed on a user's system. The following sections will discuss some of those installation methods and offer suggestions for the prevention of unauthorized installation. It should be noted that some additional security risks use more than one method of installation.

Spyware and EULAs

Commercial spyware programs tend to have EULAs. However, as some spyware may be designed to be installed and work without the user's knowledge, the programs may contain an option that will allow for remote installation without the presence of the EULA. In other cases, the software's EULA may contain terms that permit future installation of spyware programs onto the end user's computer without notification. Spyware has the capacity to log keystrokes, IM conversations, email, and other communications that can contain personal identification information. As such, it can facilitate not only monitoring by legitimate sources, but fraud and identity theft as well. In the spyware category, the most reported program, Webhancer, was consistently reported to have a EULA. Other programs may display EULAs depending on configuration by third-party affiliates.

Bundling

Similar to adware, spyware programs are sometimes bundled with other programs, such as freeware downloaded from the Internet; however, rather than being bundled intentionally by the program producer or distributor, spyware is likely to be inserted into a "desirable" program archive by someone who wishes to use it to obtain confidential data. The software package is then placed on a public download site or sent to a newsgroup for maximum exposure. The spyware is then executed when the user runs the desired program. Of the top ten spyware programs reported to Symantec over the first six months of 2005, six came bundled with other software, including the top reported spyware program, Webhancer.

Web Browsers

Like adware, spyware can also be installed through a Web browser using ActiveX controls or BHOs. However, some adware programs also install BHOs onto a user's system for less legitimate purposes. Amongst other things, BHOs can monitor Web sites visited by the user, detect events, replace ads, change home pages, and create windows to display information. BHOs can provide spyware with a wide range of functionality including, for example, the ability to download program updates, or log and export confidential data. During this reporting period, six of the top ten reported spyware programs used BHOs to install themselves, including the most reported program, Webhancer.

[109] http://securityresponse.symantec.com/avcenter/venc/data/spyware.marketscore.html

To reduce the risk from spyware that is installed through a Web browser, users should consider disabling ActiveX. It is important to note, however, that disabling ActiveX may also affect the functionality of the Web browser and may prevent certain Web sites and pages from rendering correctly. Some users require ActiveX, in which case they should configure their browser 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.

Program name	Displays EULA	Bundled	Uses BHO
Apropos	No	Yes	Yes
CometCursor	No	Yes	Yes
e2give	No	No	Yes
Goidr	No	Yes	No
Isearch	No	Yes	Yes
Ispynow	No	No	No
KeyTick	No	Yes	No
Marketscore	No	No	No
Perfect	Sometimes	No	Yes
Webhancer	Yes	Yes	Yes

Table 9. Spyware installation methods
Source: Symantec Corporation

Adware and spyware functionality—browser hijackers

If a user is browsing the Internet, an adware program may initiate search redirection. For example, the program may redirect a search by replacing the user's default search engine or by replacing "404 page not found" messages with internal search queries. This is not only misleading for the end user but also represents a security risk, as the redirection may steer the user's browser to a malicious Web site. For instance, a user might be redirected to a spoofed site[110] and then be prompted for personal information such as passwords, authentication credentials, financial information, or other confidential data. The data may then be used to commit identity theft or fraud. For example, users of Wells Fargo Bank were recently targeted with emails suggesting the user go to the bank's home page through a link that was conveniently provided. Clicking on the link took users not to the bank's home page but to a look-alike site where any personal information they provided was stolen.[111]

Of the top ten adware programs reported in the first six months of 2005, five hijacked browsers. Spyware can also hijack browsers. During the first six months of 2005, two spyware programs performed this function.

Users should follow security best practices as outlined in "Appendix A" of this report. Furthermore, as spyware can be placed on a user's computer by exploiting vulnerabilities, operating system patches should be kept updated. Users should also avoid visiting unknown, untrustworthy, or otherwise potentially malicious Web sites.

---

[110] A spoofed Web site is an illegitimate Web site that is made to look like a legitimate site, usually for malicious purposes. For instance, people engaged in online fraud may create a Web site to look like a bank's Web site, prompting the user to enter authentication credentials or account information that can subsequently be used for illicit purposes.
[111] http://www.antiphishing.org/phishing_archive/Wells_3-9-04.htm

Program Name	Hijacks Browser
180Search	No
BetterInternet	Yes
CoolWebSearch	Yes
EliteBar	Yes
Gain	No
Iefeats	Yes
Istbar	Yes
NdotNet	No
ShopAtHomeAgent	No
VirtuMonde	No

Program Name	Hijacks Browser
Apropos	No
CometCursor	Yes
e2give	No
Goidr	No
Isearch	Yes
Ispynow	No
KeyTick	No
Marketscore	No
Perfect	No
Webhancer	No

Table 10. Adware functionality
Source: Symantec Corporation

Table 11. Spyware functionality
Source: Symantec Corporation

Adware and spyware—prevention and mitigation

Symantec recommends that all users continue to update their antivirus software regularly. Security administrators 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, an integrated antivirus and intrusion detection systems. 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 has been established in the preceding discussion, some spyware and adware programs are installed using ActiveX controls, Symantec recommends that users consider disabling ActiveX altogether. However, as was also stated earlier, some users may require ActiveX for some applications, in which case they should configure their browser to require a prompt for ActiveX controls to execute.

In addition to the deployment of defense in-depth, Symantec recommends that acceptable usage policies are put in place and enforced. 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.

Phishing

This section of the Symantec *Internet Security Threat Report* will assess phishing activity that Symantec has detected between January 1 and June 30, 2005. 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.

The data provided in this section is based on statistics returned from the Symantec Probe Network, which consists of over two million decoy accounts that attract email messages from 20 different countries around the world. The network encompasses more than 600 participating enterprises in the Americas, Europe, Asia, Africa, and Australia/Oceania and attracts e-mail 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 online 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. A single message, or lure, can be used many times in phishing attacks.

A phishing attempt can be defined as an instance of a phishing message being sent to a single user. Phishing attempts are email messages that have been sent by the same phisher to one or more targets. This means that an attempt may consist of one or more different unique email messages. For instance, different phishing attempts may consist of the same phishing message being sent to different targets, different phishing messages being sent to the same target, or a combination of the two. Extending the fishing analogy, an attack can be considered a single cast of the lure or one instance of a phisher using a phishing message, or lure, to try to ensnare a target.

It should be noted that variations in accounting methods for phishing attempts exist amongst different monitoring organizations. Some groups may identify and count unique phishing messages based solely on specific content items such as subject headers or URLs. These differing methods can often lead to differences in the number of phishing attacks being reported by different organizations.

Symantec detects and confirms messages in a two-step process. First, all messages in the Symantec Probe Network are scanned with a set of low-level heuristics,[112] which search for key triggers such as domain names that are known to be frequently phished entities. Symantec analysts then confirm that the suspicious messages are in fact phishing messages.

This confirmation is important, as the goal of phishing attempts is to deceive the end user. Many phishing messages closely resemble email messages sent by the entities that are being phished. In many cases only careful scrutiny of multiple message parts such as headers and body content can confirm that suspicious email does in fact constitute a phishing attempt.

---

[112] Heuristics are a set of simple filters that analyze email messages for common characteristics that appear in phishing messages.

This section will discuss the following:

• Six-month growth in phishing messages
• Number of blocked phishing attempts
• Phishing as a percent of email scanned

Six-month growth in 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 first six months of 2005, the Symantec Probe Network detected 97,592 unique phishing messages (figure 29). This is an increase of 40% over the 69,906 unique phishing messages that were detected in the second half of 2004. This increase may be attributed to several factors. First as the Symantec Probe Network grows, the number of total messages detected by the network also grows, which would likely increase the number of phishing messages detected. However, the Symantec Probe Network grew less than 3% during the current reporting period, so this factor is not likely the cause for the current increase in phishing messages.
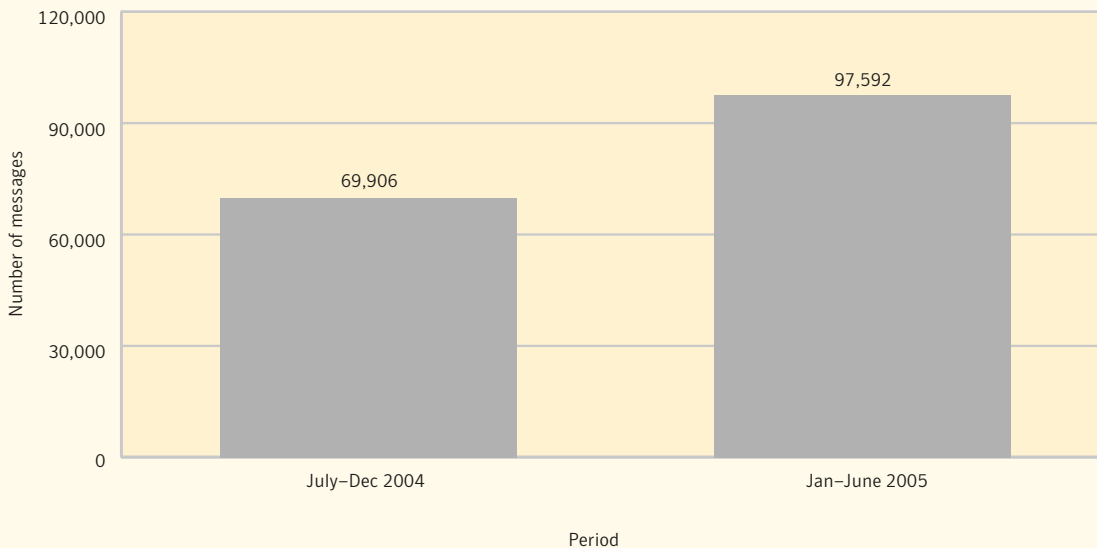

Figure 29. Unique phishing messages detected
Source: Symantec Corporation

A more likely contributing factor is that as the number of companies identified by Symantec as phishing targets grows, so does the number of phishing messages detected. Targeted companies can be divided into two groups: those targets that were previously being phished but were undetected, and those targets that had not previously been phished. The discovery of new targets aids in strengthening detection heuristics, which in turn assists in detecting more phishing attempts.

The third factor contributing to the growth in detected phishing messages is an increase in highly randomized phishing attacks. There is some evidence that certain phishers are narrowing the focus of their email campaigns. This means that they are customizing phishing attempts to their targets, even going so far as to include valid account information in messages. This would likely shrink the size of these more targeted phishing spam campaigns. If all phishers were moving to this tactic there would be a discernable decrease in the amount of phishing. However large scale spam blasting[113] is still occurring. As a result, phishers are still able to continue to send out large numbers of email messages that have been highly randomized, especially in areas that are somewhat invisible to the average end user, such as pixels in attachments, URLs, and other HTML code. Much of this randomization is implemented for the purpose of bypassing antispam and antifraud filters. The result is that larger numbers of unique phishing messages are being sent out, which likely means that more end users are at risk of being phished.

Blocked phishing attempts

The number of blocked phishing is derived from the total number of phishing email messages sent to users that were blocked in the field by Symantec Brightmail AntiSpam antifraud filters. 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 to the customer base where they prohibit the phishing email messages from reaching end users.

The number of phishing attempts blocked by Symantec Brightmail AntiSpam in the first six months of 2005 indicates a significant increase in phishing activity (figure 30). In the first half of 2005, Symantec blocked 1.04 billion phishing attempts, compared to 546 million in the last six months of 2004; this is a 90% increase in attempts blocked between the two periods.

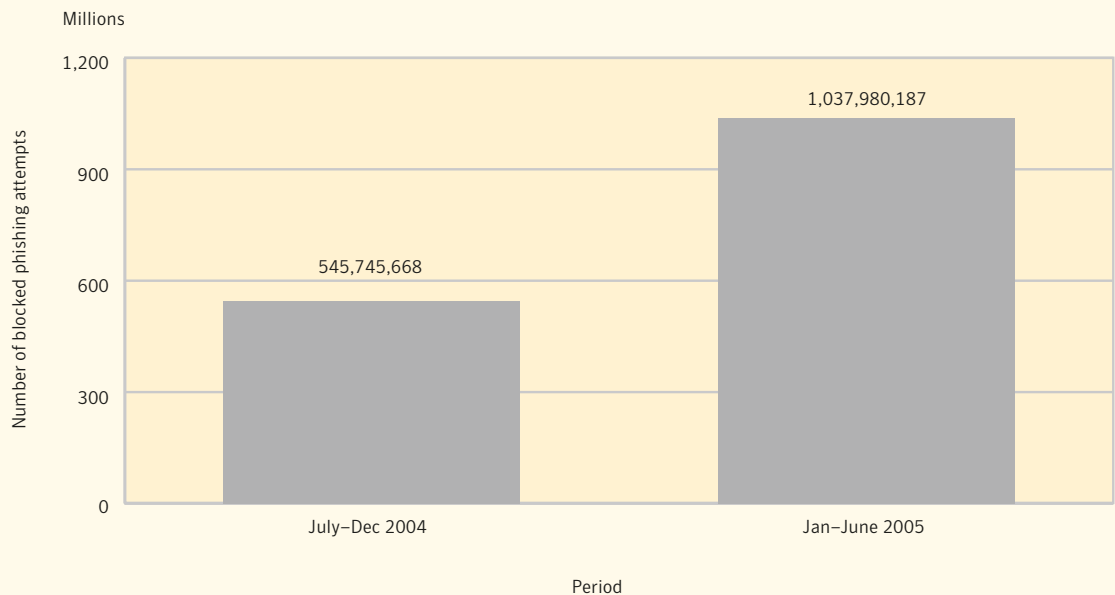**Figure 30. Blocked phishing attempts**
Source: Symantec Corporation

[113] Spam blasting is a term used to describe widespread unsolicited spam email attacks. A spammer will send thousands upon thousands of messages in a single burst or blast.

This increase is also evident in the weekly average of messages blocked. Between July 1 and December 31, 2004, Symantec blocked an average of 21 million phishing attempts a week. Between January 1 and June 30, 2005, the weekly average was 40 million phishing attempts blocked, a 90% increase.

This growth can be attributed in part to growth of the Symantec Brightmail AntiSpam customer base. As the number of customers increases, so do the number of phishing attempts caught by antifraud filters. The number of Symantec Brightmail AntiSpam customers increased over 12% during the six-month period of January 1 to June 30, 2005; as a result, it is not surprising that detected phishing attempts also increased. However, the phishing attempt data is also based on a dynamic set of antifraud filters. As phishing changes and new phishing targets are discovered, the composition and volume of antifraud filters increases. The fact that new antifraud filters are continually being developed supports the notion that phishing is still growing.

Phishing likely continues to grow because phishing attempts continue to succeed and to be lucrative. In 2004, the average loss to consumers who reported Internet-related fraud to the Internet Crime Complaint Center[114] was U.S.$240.00 for credit card fraud and U.S.$907.30 for identity theft.[115] According to the FBI, in one specific case, an identity theft ring was able to net over U.S.$2 million.[116]

For phishers, the amount of time required to send out phishing emails is negligible. However, for consumers who must re-establish credit histories and other personal records after identity theft has occurred, the cost in time and effort is considerable.

Phishing as a percent of email scanned

This section will discuss the volume of phishing attempts as a percentage of the total email scanned by the Symantec Brightmail AntiSpam solution. This number is determined by dividing the total number of email messages scanned by the number of email messages that trigger antifraud filters. These filters are distributed across the Symantec customer base.

Between January 1 and June 30, 2005, the percentage of email messages that constitute phishing attempts increased from 0.4% of the messages processed, or an average of 2.99 million attempts per day, to 0.8% of the messages processed, an average of approximately 5.70 million phishing attempts per day (figure 31). Peak days during this period experienced numbers well in excess of 13 million phishing attempts per day.

[114] The Internet Crime Complaint Center or IC3 is a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center see
http://www.ic3.gov/ for more information.
[115] http://www.ifccfbi.gov/strategy/2004_IC3Report.pdf
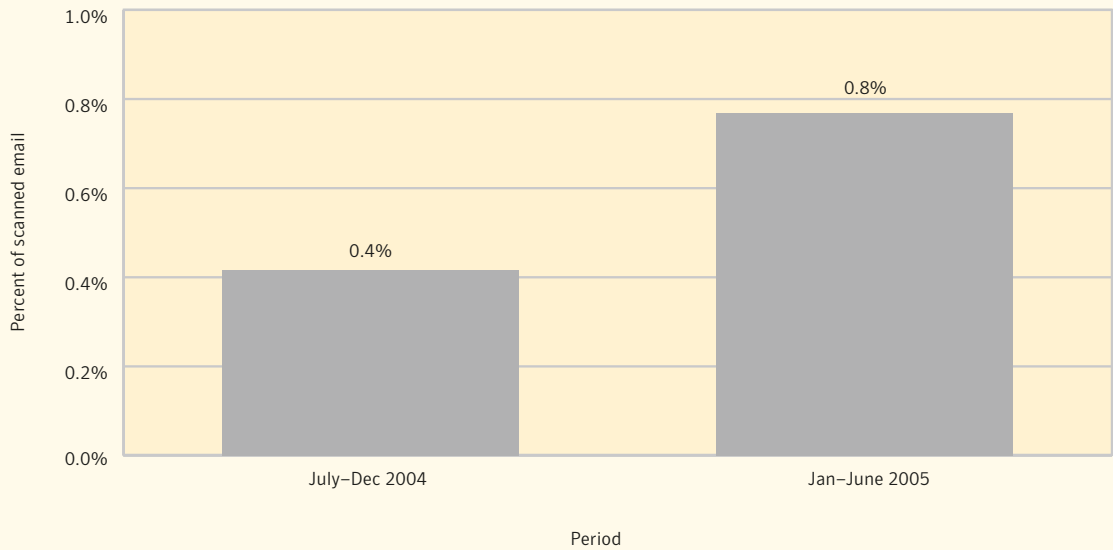[116] http://www.fbi.gov/congress/congress05/swecker041305.htm

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

The 0.8 % of email scanned that made up phishing attempts may appear small in terms of percentages; however, it translates into significant numbers. What it means is that roughly one out of every 125 email messages scanned was a found to be a phishing attempt. This is an increase from roughly one out of every 250 email messages that constituted phishing attempts in the second half of 2004. In reality, what this means is that if an end user were to receive an average of 25 email messages per day, that user would then be receiving at least one phishing message every week.

Prevention and mitigation of phishing

Symantec recommends that enterprise users protect themselves against phishing threats through the detection and filtering of email at the server level via the mail transfer agent (MTA).[117] Although this will likely remain the primary point of filtering for phishing, IP-based filtering can be used upstream as well as providing HTTP filtering. DNS block lists (DNSBLs),[118] which offer more general protection and may mitigate some of the risk of phishing emails, offer another preventative option. Domain level authentication, the process of verifying the actual origin of an email message, should provide some protection from phishers who are spoofing mail domains.[119]

In countering the threat posed by phishing, administrators should always follow Symantec best practices as outlined in "Appendix A" of this report. Symantec also recommends that organizations ensure that their end users are educated about phishing in general,[120] and are advised about the latest phishing scams and how to avoid falling victim to them.[121]

---

[117] Message transfer agents are programs that are responsible for routing email messages to the proper destination.
[118] A DNSBL is simply a list of IP addresses or blocks of IP addresses that are known to send unwanted email traffic. The DNSBL is used by email software to either allow or reject mail coming from IP addresses on the list.
[119] 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.
[120] For instance, the FTC has published some basic guidelines on how to avoid phishing. They are available at:
http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm
[121] A good resource for information on the latest phishing threats can be found at http://www.antiphishing.org

Organizations can also employ Web-log monitoring to track if complete Web site downloads are occurring. This may indicate that someone is using the legitimate site to create an illegitimate phishing Web site. Organizations can also be alerted to phishing attacks that use spoofing by monitoring non-deliverable email addresses, or bounced email returned to non-existent users. They should also monitor cousin domain[122] purchasing by other entities. Tracking the registration of new cousin domains allows for companies to identify purchases that could be used to spoof their corporate domain. This can be done with the help of companies that specialize in domain monitoring, some registrars are even beginning to provide this service as well.[123]

End users should also follow best security practices. As some phishing attacks may utilize spyware and keystroke loggers, Symantec advises end users to use antivirus software, firewalls, 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. Bank and credit card information should be reviewed frequently. This can provide information on any irregular activities. For further information, the Internet Fraud Complaint Center[124] has also released a list of guidelines on how to avoid Internet-related scams.[125]

Spam

Spam is usually defined as junk email 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. Furthermore, high volumes of spam can create denial of service conditions wherein email systems are so overloaded that legitimate email and network traffic are unable to get through. This section of the Symantec *Internet Security Threat Report* will discuss developments in spam activity between January 1 and June 30, 2005.

This analysis is based on data returned from the Symantec Probe Network as well as data derived from a statistical sampling of the Symantec Brightmail AntiSpam customer base. Specifically, statistics were gathered from the Symantec Brightmail AntiSpam servers of enterprise customers that received more than 1,000 total email messages per day. This normalization allows for a more accurate representation of data by removing extremely small data samples, such as smaller customers and test servers. The proportion of email that is spam is calculated by dividing the total inbound email messages received by the sample customer base the total spam filtered by Symantec Brightmail AntiSpam.

The Symantec Probe Network comprises millions of decoy email addresses that are configured to attract a large stream of spam attacks. These attacks are representative of the spam that is being received by the Probe Network's partner's domain. An attack can consist of one or more messages, or a group of similar messages. All attacks are received and analyzed by Symantec Brightmail analysts, who produce antispam filters based on the characteristics of the attacks.

The goal of the Symantec Probe Network is to simulate a wide variety of Internet email users, thereby attracting a true representation of the spam messages that are circulating on the Internet at any given time. For this reason, it is continuously optimized in order to attract new varieties of spam attacks. This is accomplished through internal production changes made to the Probe Network, which thus affect the number of new spam attacks it receives.

---

[122] "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.
[123] See http://www.markmonitor.com/brandmanagement/index.html for instance.
[124] The IFCC (http://www.ifccfbi.gov/) is a partnership between the FBI and the National White Collar Crime Center:
[125] http://www.fbi.gov/cyberinvest/inetschemes.htm

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 explore the following:

• Spam as a percentage of email
• Top 10 countries of spam origin

Spam as a percentage of email

Between January 1 and June 30, 2005, spam made up approximately 61% of all email traffic. This is a very slight increase over the last six months of 2004 when just over 60% of email was classified as spam.

While the six-month average remains above 60%, analysis of the spam data reveals a month-to-month decline in the percentage of email that is spam between January 1 and June 30, 2005 (figure 32). In January 2005, 67% of email was categorized as spam. By the end of June, this number had declined to 53%. In absolute terms this represents a decline of 14 percentage points; however, in proportionate terms, it is a 21% decrease.
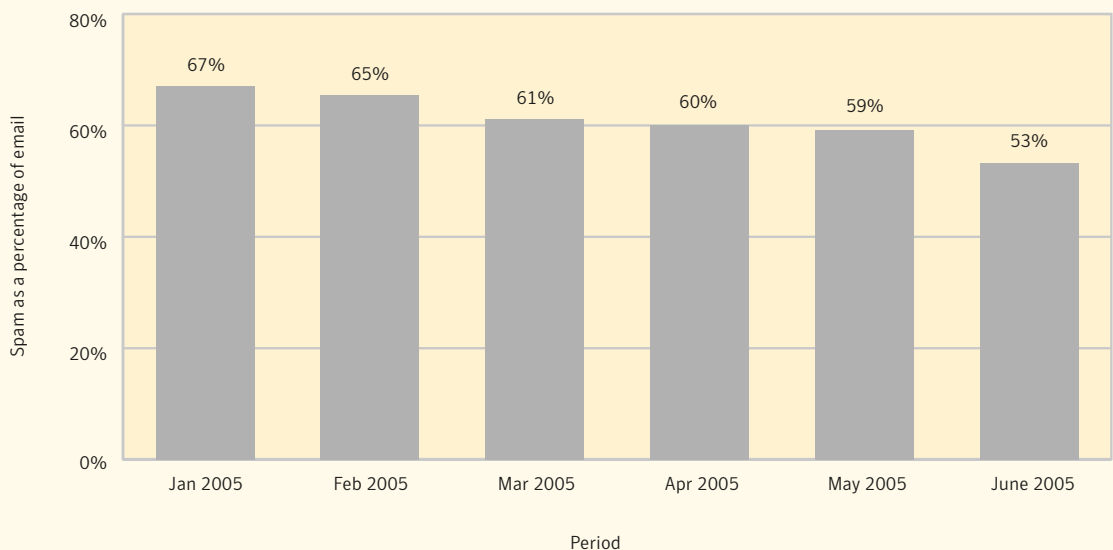

Figure 32. Spam as percentage of email
Source: Symantec Corporation

Much of this decline is due to the fact that network and security administrators are using IP filtering and traffic shaping to control spam. 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—such as an originating IP address that is a known source of spam—to selectively determine what connections to allow, deny, or throttle (slow down).

Compared with other antispam techniques, the benefit of router-based IP filtering and traffic shaping is that spam messages are filtered upstream from the MTA. This reduces the burden on the MTA, thus allowing it to better handle the transfer of legitimate email through its network of end users. This gain is especially valuable for large enterprises and ISPs that manage large volumes of email traffic. It also allows for the implementation of more resource-intensive antispam filtering techniques, resulting in a reduction of the spam experienced by email users.

It is important to note that, due to IP filtering and traffic shaping, a denied email message is more likely to be invisible to the network; therefore, it will not contribute to the data that is gathered. As a result, Symantec believes that the six-month decline in the percentage of email is due, at least in part, to the successful implementation of these technologies. This does not necessarily signify any decrease in spam attack attempts to Internet email users. However, it does indicate that these attempts are meeting with decreasing success.

Another factor contributing to the decline in spam over the first six months of 2005 was the implementation of outbound filtering by major ISPs. Given the large volumes of spam that have historically originated from compromised ISP accounts, many ISPs are working with their vendors to implement measures to filter their outbound email traffic. This is partly because of the success of IP-filtering. As third party blacklists[126] grow in usage and popularity, ISPs that are unable to prevent their email servers from being used to send spam risk being blacklisted. This would subsequently limit their end users' ability to successfully send email. Outbound filtering by ISPs will not end spam on the Internet. However, it could significantly reduce the distribution of spam from compromised ISP accounts and bot networks.

Top 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 when attempting to identify the geographic location of spammers. Many spammers try to obscure their actual location. In an attempt to bypass blacklists, they build coordinated networks of compromised computers known as bot networks,[127] allowing them to send spam from sites that are distant from their physical location. 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 the data gathered and returned by customer installations of Symantec Brightmail Anti Spam, including the IP addresses of the originating servers, 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 originating from a particular country, then that country would less likely be represented in this metric.

During the first six months of 2005, 51% of all spam received worldwide originated in the United States (table 12). South Korea was the second highest country of origin, accounting for 14% of all spam in the first half of 2005. Canada, with over 7% of Internet spam, was the third-ranked country during this reporting period followed by China providing over 5%.

With the rapid deployment of high-speed Internet in even the smallest of countries, it is reasonable to assume that the number of countries from which spam originates can be expected to increase. This is evident when comparing the first six months of 2005 with the last six months of 2004. For example, spam originating in the United States decreased from 60% in the last six months of 2004 to 51% in the first six months of 2005. Spam originating in nearly all other top ten countries increased over the same period. This growth, coupled with newly emerging spam-producing countries, accounts for the United States' reduced percentage of total spam. Symantec predicts that as broadband connectivity continues to expand around the world, spam will originate in even more countries than it currently does.

Country	Jan–June 2005	July–Dec 2004
United States	51%	60%
Korea	14%	9%
Canada	7%	6%
China	5%	4%
Belgium	3%	2%
Great Britain	2%	2%
France	2%	n/a
Japan	2%	2%
Spain	1%	n/a
Brazil	1%	1%

Table 12. Monthly growth of top ten countries of spam origin
Source: Symantec Corporation

Future Watch

The previous sections of this report have discussed Internet security developments between January 1 and June 30, 2005. This section of the *Internet Security Threat Report* will discuss emerging trends and issues that Symantec believes will become prominent over the next 12 to 18 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.

Modular malicious code

Traditional malicious code usually incorporates a wide range of functions in one executable program or file. However, as security vendors have learned to protect against those attacks, malicious code authors have developed increasingly more sophisticated methods.

Over the past 18 months, Symantec has observed a disturbing trend in malicious code. Malicious code authors have been deploying modular malicious code. Modular malicious code is malicious code—such as worms, viruses and Trojans—that initially possesses limited functionality.[128] However, once installed on a target computer, it downloads other pieces (or modules) of malicious code with different functionalities and further compromises the infected computer.

The Tooso.I[129] Trojan is an example of modular malicious code that, once installed, attempts to disable antivirus solutions and then download further functionality from different sources. Because of its modular structure, the majority of this additional functionality is hosted on machines distributed across the Internet. Attackers can easily modify extant malicious code into new variants in order to bypass antivirus detection signatures or to add new or additional functionality. As a result, security administrators may have to deploy stricter access rules and limit sites that host machines are able to connect to.

In addition to following recommended best practices outlined in "Appendix A" of this report, Symantec continues to advise all administrators and end users to ensure that their antivirus definitions are updated regularly. Furthermore, administrators and end users should apply operating system patches as soon as they become available.

Bot networks increase in number, diversity, and sophistication

As discussed in the "Attack Trends" section of this report, bot activity increased considerably in the first six months of 2005. The number of DoS attack attacks also increased during this period—by more than 680% over the last six months of 2004.

Using statistical regression testing, Symantec has determined that there is strong correlation between the number of bot computers and the number of DoS attacks.[130] Due to this observation Symantec believes that bot network activity is driving the number of DoS attacks. As a consequence, Symantec feels that other bot-related activity—such as spam relaying and Internet-based extortion[131]—may also be on the rise, as this activity is also likely being driven by bot network activity.

---

[128] Initial functionalities can include disabling antivirus and firewalls.
[129] http://securityresponse.symantec.com/avcenter/venc/data/trojan.tooso.i.html
[130] Regression testing yielded a coefficient of determination of 85%.
[131] See http://www.newscientist.com/channel/info-tech/mg18725125.900 and http://www.theregister.co.uk/2004/07/21/cyber_shakedown_taken_down/ for instance.

Symantec speculates that over the next year there will be a more coordinated community of bot network computers carrying out more sophisticated, targeted attacks. This may include the use of bot networks as a method of seeding compromised networks with other types of malicious code, which could be used for spam, phishing, and theft of confidential information. Symantec also expects that as bot networks continue to mature they will begin to employ more sophisticated methods to avoid detection, such as encryption, packing, and rootkits.

Users and security administrators should employ defense in-depth strategies to reduce the likelihood that their computer infrastructure will become compromised. Furthermore, users should be educated to never view, open, or execute any email attachment unless it is expected and comes from a known and trusted source, and the purpose of the attachment is known. Administrators and end users should also ensure that antivirus definitions are current and up-to-date.

Due to the increase in bot networks, the United States Federal Trade Commission has been urging ISPs to take more action against bot networks in their subscriber bases.[132] It is reasonable to believe that legislative action may not be far behind.

Phishing targets and methods continue to grow

In the "Additional Security Risks" section of this *Internet Security Threat Report*, Symantec observed that the threat of phishing continues to grow as attackers take advantage of new targets. Due to the fact that there are far more smaller targets (such as regional banks) than large ones (like credit card companies) and that smaller targets generally present fewer challenges for attackers, the number of phishing targets will most likely continue to grow.

Phishing messages are continually being altered in order to evade antispam and antiphishing filters. This is driving new innovation in methods of evasion, particularly in the use of randomized changes in phishing messages.[133] This can take the form of randomized pixels in attached images, as well as URL obfuscation techniques such as the use of cousin domains,[134] and Web site redirection.

Many of these new attacks target personal information and there is ample reason to believe that this practice will continue to flourish. Any method that is successful in fooling end users into providing valid information or simply validating information will continue to be used. For instance, some targeted phishing attacks will include the user's account number and ask the intended victim to click on it in order to verify that it is the correct account information for that user. If the user does this, these numbers may subsequently be used for fraudulent purposes.[135]

Symantec urges security administrators to monitor the registration of cousin domain names and to educate users on the increased sophistication of these types of attacks. Industries that are often targeted by these attacks—such as financial services—need to pay particular attention and stay informed of emerging techniques and threats.

132 http://www.ftc.gov/bcp/conline/edcams/spam/zombie/index.htm
133 http://discussions.virtualdr.com/archive/index.php/t-174119.html
134 Cousin domains are domains created to appear as if they are part of a target's legitimate domain. For example, if the target has a domain registered as biz.com, an attacker may register security-biz.com and attempt to trick users into responding to email coming from the illegitimate domain.
135 http://news.zdnet.com/2100-1009_22-5706305.html

Symantec recommends that enterprises deploy an antiphishing solution that blocks these types of threats. Symantec also recommends that organizations ensure that their end users are educated about phishing.[136] They should also monitor phishing activity and keep their users informed of the latest phishing scams and how to avoid falling victim to them.[137] End users should be educated about the types of threats they are likely to encounter and to not respond to any requests for confidential or financial information without confirming the source and validity of the request.

Adware/spyware future developments

During the first half of 2005, media attention on both adware and spyware programs continued to increase. Ongoing efforts to create legislation continue and working groups to address these issues have been formed. Symantec predicts these types of efforts will continue as other stakeholders invest time and resources in research related to spyware and adware.

As cellular telephones, PDAs, and hybrid devices become more prevalent, it is reasonable to assume that security risks, such as spyware and adware, will increasingly target them. However, the risks will vary depending on the operating system, application, and how the devices are configured and used.[138] Furthermore, Symantec expects to see an increase in spam targeting these devices.

Symantec expects to see more targeted spyware utilizing a variety of sophisticated techniques in an attempt to avoid detection. As was discussed in the "Malicious code for profit" section of the "Malicious Code" report, these programs may be related to corporate espionage with the delivery and installation of the spyware programs being achieved through social engineering. For example, prominent employees in an organization may be easily identified, and their areas of interest determined using readily available search engines. Information about those interests can be used to design and deliver social engineering bait that is likely to be executed by the recipient.

Wireless security threats

Over the past couple of years, the number of wireless local area networks (WLAN) in enterprises and other locations has increased noticeably. It is now common to find WLAN connections in such places as coffee shops, airports, and hotels. Furthermore, many home users are enjoying the increased convenience wireless connectivity offers. There have even been proposals for municipalities to implement low-cost or free wireless access in public places such as parks and libraries.[139] While these sorts of initiatives provide an alternative method for users to connect to the Internet, they often neglect important security implications of wireless deployment.[140] The growing number of people using wireless connectivity has brought a corresponding increase in the number of concerns posed by insecure wireless access points.[141]

Symantec continues to monitor reports of attacks and vulnerabilities in wireless devices. Attackers are able to monitor, capture, and hijack sessions taking place over wireless networks. These illegitimate uses are made easier by poor configuration of these devices, a lack of encryption, and inadequate authentication requirements. These weaknesses are inherent in the fact that wireless access points often act as *de facto* public terminals.

---

[136] For instance, the FTC has published some basic guidelines on how to avoid phishing. They are available at:
http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm
[137] A good resource for information on the latest phishing threats can be found at http://www.antiphishing.org
[138] Bluetooth-enabled devices, for example, appear to have greater potential to allow exploitation than a non-Bluetooth-enabled device.
[139] See http://www.wirelessphiladelphia.org for instance.
[140] http://www.eweek.com/article2/0,1895,1830998,00.asp
[141] Wireless access points are devices that allow laptops, mobile devices, and desktops to connect to a local area network without the need for network cabling.

In some cases, attackers will impersonate the wireless access point itself in order to capture sensitive or useful information from machines attempting to connect to it. This has led to a reported increase in the number of war drivers[142] who use those connections to launch attacks and steal confidential information. Malicious users may also surf other users' Internet connections and, in the process, impersonate a legitimate user or anonymize their online activities.[143]

Enterprises that deploy wireless networks are particularly at risk. Attackers can gain access to these networks by bypassing the traditional perimeter security measures, such as IDS systems and firewalls, which are normally in place on wired networks. Symantec recommends that enterprises that use wireless networks implement authentication and strong encryption such as 128-bit WEP[144] or WPA.[145] Additionally, enterprises should ensure that wireless networks operate over a VPN and that connections be placed in a DMZ,[146] in which inbound and outbound connections are required to pass through a firewall. Mobile users should ensure that they connect only to secure wireless access points and that, when not in use, wireless network devices are turned off or disabled.

VoIP threats expected to emerge

Voice over Internet Protocol (VoIP)[147] is quickly becoming a widely adopted alternative to traditional analogue phone systems. There are currently 23 million users of Skype VoIP alone with users expected to surpass 160 million by the end of 2006.[148] By that time, it is expected that two-thirds of the Global 2000 companies[149] will have adopted VoIP as their primary means of voice communication.[150] Designed to carry voice and data over the same network connection, VoIP is subject to quality-of-service concerns when security measures are implemented. Current standards such as Session Initiation Protocol (SIP)[151] could be vulnerable to general protocol threats and cross platform vulnerabilities.

VoIP may be vulnerable to a wide range of possible attacks, including (but not necessarily limited to):

• Attempts to discover legitimate IP phone addresses through directory harvesting.[152]
• Clogging voicemail systems with voice spam sent as audio files.
• Voice phishing, in which voicemails urge users to return calls and leave personal financial information.
• DoS attacks against voice servers.
• Vulnerabilities in VoIP products[153] that may be exploited for malicious purposes.

VoIP can also be subject to attacks that result in call redirection to another phone, the hijacking of ongoing calls, and the ability to turn on other phones so they act as receivers of conversations. The introduction of VoIP on enterprise networks in the absence of appropriate security measures could introduce another entry point for attackers to exploit.

[142] War drivers are people who scan for available wireless networks and often hijack or join those networks without permission.
[143] An anonymized attack allows a person to launch an attack without being traced.
[144] Wireless equivalent protocol (WEP) is a security protocol for wireless local area networks that encrypts data over radio waves. While initially developed for security, a number of flaws have been identified in WEP and it has since been superseded as a means of securing wireless computing.
[145] Wi-fi protected access (WPA) is a system to secure wireless networks that was designed to improve upon the security shortcomings of WEP.
[146] A DMZ is subnetwork that is situated between a trusted internal network and an external public network such as the Internet. Web, email, and FTP servers are often placed in DMZs.
[147] Voice over Internet Protocol (VoIP) is technology for transmitting ordinary telephone calls over the Internet.
[148] Evalueserve "The Impact of SKYPE on Telecom Industry(PDF)(Study by Evalueserve) http://www.evalueserve.com/Media_Center/mediacenternew.asp#
[149] The Global 2000 is a composite ranking of the world's biggest companies as ranked by Forbes. http://www.forbes.com
[150] eWeek.com "VOIP: A New Day is Dawning" (December 6, 2004): http://www.eweek.com/article2/0,1759,1735347,00.asp
[151] Session Initiation Protocol (SIP), is a signaling protocol for Internet conferencing, telephony, presence, events notification, and instant messaging.
[152] Directory harvesting attacks occur when an attacker uses known email addresses to generate other valid addresses from corporate or ISP servers. Often used by spammers, this technique allows attackers to send emails to randomly generated email addresses. Some of these email addresses are real users in the organization; however, many of them are bogus addresses that flood the victim's mail server.
[153] http://www.securityfocus.com/bid/14174/info

While there are currently few reported attacks directed at VoIP systems, Symantec feels that as this new communications technology gains widespread acceptance and deployment, it is only a matter of time before attackers target it more intensely. One possible scenario is the ability of IP-based attackers to gain access to tradition phone systems through IP-PSTN gateways.[154]

Symantec advises that enterprises that are considering the adoption of VoIP perform a risk analysis prior to implementation. They should also put in place appropriate security measures, such as an SIP firewall on all systems that connect through VoIP. Organizations are also advised to consider separating VoIP and data networks in order to address performance issues that security measures might introduce.

Continued security concerns for Mac OS®

In the "Future Watch" section of the previous *Internet Security Threat Report*,[155] Symantec advised readers that Apple's Mac OS X was an emerging target for attacks. During the current reporting period, Symantec documented a noteworthy number of vulnerabilities and attacks directed at Mac OS X.

An ever-increasing number of users are adopting Mac OS X. Many of these users believe that this operating system and the applications that run on it are immune to traditional security concerns. However, evidence suggests that, increasingly, they may be operating under a false sense of security.[156]

Mac OS X is based on a Berkeley Systems Design (BSD) UNIX-like environment. Many of the security concerns that UNIX users face are now shared by those who have adopted Mac OS X.[157] As Mac OS X users demand more features and implement more ports[158] of popular UNIX applications, vulnerabilities and exploits targeting this operating system and its underlying code base are likely to increase.

Over the past two reporting periods, the number of vendor-confirmed vulnerabilities in Mac OS X has remained relatively constant. None of these have been widely exploited. However, this could change in the near future. During the writing of this report, an analysis was performed on a rootkit[159] designed to take advantage of Mac OS X.[160] Mac OS X/Weapox[161] is a rootkit based on the AdoreBSD rootkit. While there have been no reports of widespread infection to date, this Trojan serves to demonstrate that as Mac OS X increases in popularity so too will the scrutiny it receives from potential attackers.

The discovery of Mac OS X/Weapox indicates that Mac OS X may no longer be immune from widespread attack. As such, system administrators, security administrators, and end users should employ defense in-depth. Though vulnerabilities and malicious code targeting other operating systems continue to outnumber those on Mac OS X, Symantec recommends that users continue to apply security patches as they become available and continue to educate themselves on security issues affecting Mac OS X.

---

[154] An IP-PSTN gateway translates voice and data carried over a VOIP network to conventional telephone signaling so that calls can be routed over a conventional telephone network.

[155] Symantec *Internet Security Threat Report*, Volume VII (March 2005): http://enterprisesecurity.symantec.com/content.cfm?articleid=1539

[156] See the following URL, for instance:
http://www.securityfocus.com/swsearch?query=OS+X&sbm=bid&submit=Search%21&metaname=swishtitle&sort=swishlastmodified

[157] A recent announcement surrounding an audit of the underlying source code in Darwin, the implementation of UNIX that underlies Apple Computer Inc.'s Mac OS X operating system, revealed kernel level vulnerabilities that could be exploited by remote attackers. (For more details, see:
http://www.eweek.com/article2/0,1759,1752632,00.asp)

[158] A port is application or piece of code written on one platform that is then modified to run on another.

[159] A rootkit is a collection of tools that allows an attacker to provide a back door into a system, collect information on other systems on the network, mask the fact that the system is compromised, and perform other activities as desired by the attacker.

[160] Virus Bulletin July 2005: http://www.virusbtn.com

[161] http://pferrie.tripod.com/vb/weapox.pdf

Advanced tools make finding vulnerabilities easier

Recent advances in technologies that analyze software code have made the discovery of vulnerabilities and the creation of code designed to exploit those vulnerabilities easier than ever before. Traditionally, vulnerability research has been a time-intensive process requiring, in most cases, above average programming and reverse engineering skills. Advances in software analysis tools[162] have made decompiling software and binary patches quicker and easier than previous methods, particularly manual techniques. Specifically, advanced analysis tools are now available to help researchers to find vulnerabilities in software. These tools have abstracted program flow from machine code, providing researchers with a visual representation of program structure that may be even simpler, in some instances, than looking at source code.

As is the case with many security tools, these programs can be deployed for legitimate purposes by security administrators. Some high-profile security researchers have been able to demonstrate how these tools and new methods have made the discovery of vulnerabilities and the design of exploit code easier.[163]

As the "Exploit development time" discussion in the "Vulnerability Trends" report of this paper points out, the average time for exploit development was 6.0 days. Advanced analysis tools may allow potential attackers to narrow this window. The widespread availability of an exploit means that vulnerabilities are exposed to potential exploitation. By making the development of exploit code faster and easier, advanced analysis tools increase the probability that vulnerabilities will be exploited before appropriate patches are made available and applied.

Just as advances in programming techniques have opened the door to more programmers, Symantec believes that advances in code debugging and analysis tools will increase the number of people who are able to discover and exploit vulnerabilities. It will also likely mean an increase in both the number and the severity of vulnerabilities and the likelihood of zero-day exploits.[164]

---

[162] Sabre Security's (http://www.sabre-security.com) BinDiff and BinNavi are examples of advanced analysis tools used by some researchers to find vulnerabilities in software.
[163] Sabre Security demonstrates the use of its tool to quickly identify a vulnerability corrected by Microsoft via a binary-only patch: http://www.sabre-security.com/products/flash_bindiff_png.html
[164] A zero-day exploit is a set of code that is developed to exploit a vulnerability before the vulnerability is disclosed publicly. Zero-day exploits are particularly dangerous. Since the attack is completely unknown to the public it is impossible for administrators to protect their systems against it.

Appendix A—Symantec Best Practices

Enterprise Best Practices

1. Employ defense-in-depth practices, which emphasize multiple, overlapping, and mutually supportive defensive systems to guard against single-point failures in any specific technology or protection methodology. This should include the deployment of antivirus, firewalls, intrusion detection and intrusion protection systems on client systems. Enterprises should also ensure that they are actively monitoring their environments 24x7 against attack.

2. Turn off and remove unneeded services.

3. If a blended 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—such as HTTP, FTP, SMTP, and DNS servers—and are accessible through a firewall.

5. Enforce a password policy.

6. Configure email 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 further compromise within the organization. Perform a forensic analysis and restore the computers using trusted media.

8. Train employees not to open attachments unless they are expecting them. Also, do 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 systems along with file-sharing programs, free downloads, and freeware and shareware versions of software, or by clicking on links or attachments in email messages, or via instant messaging clients. Ensure that only applications approved by your 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 blended threats.

2. Ensure that security patches are up-to-date.

3. Ensure that passwords include a mix of symbols, letters, and numbers. Do not use dictionary words. Change passwords often.

4. Never view, open, or execute any email attachment unless the purpose of the attachment is known.

5. Keep virus definitions updated. By deploying the latest virus definitions, corporations and consumers are protected 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 types of 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 improper technical jargon 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 Web site designed to look like that of the legitimate organization. Consumers and business professionals also need to consider who is sending the information and determine if it is a reliable source. The best course of action is to simply delete these types of emails.

8. Consumers can get involved in fighting Internet crime 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 Internet service provider or local police.

9. Be aware of the differences between spyware and adware. Spyware has been used for malicious purposes, including identity theft, while adware is often used to gather data for marketing purposes and has a valid, generally benign purpose.

10. Both spyware and adware can be automatically installed on your system along with file-sharing programs, free downloads, and freeware and shareware versions of software, or by clicking on links or attachments in email messages, or via instant messaging clients. Therefore, be informed and selective about what you install on your computer.

11. Don't just click those "Yes, I accept" buttons on EULAs. Some spyware and adware applications can be installed after, or as a by-product of, accepting the EULA. Read each EULA carefully to examine what it means 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 you respond to these ads. When you see ads in a program's user interface, you 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 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.

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:

• The proportion of sensors that detect a given attack.
• The proportion of attacking IP addresses that perform a given attack.
• 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.[165]

---

[165] In previous editions of the Symantec *Internet Security Threat Report*, both the attack volume and number of attackers were cited and compared.

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:

• The proportion of sensors that detect a given attack.
• The proportion of attacking IP addresses that perform a given attack.
• 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 sample periods.

Previous volumes of the *Internet Security Threat Report* have used the median number of attack events determined by analyzing Symantec Managed Security Services and Symantec DeepSight Threat Management System sensors. Symantec analysts identified attack events formerly represented in this metric such that a single attack event could be made up of multiple attacks conducted by a single source IP against a single company. However, this method had the affect of under-representing the number of individual attacks observed.

For this volume of the Symantec *Internet Security Threat Report*, this metric has been redesigned to include all unauthorized access attempts denied[166] at the firewall and the network intrusion detection system level. This new method of determining the daily number of attacks is more representative of the rate of attack activity experienced by networks connected to the Internet than the method previously used. Furthermore, the number of attacks used for this analysis is that of the company that observed the median number of attacks in the sample set. Using the median organization assures 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.[167]

Bot networks

Symantec identifies certain scanning patterns and observed network traffic and cross-references this traffic with rules that define specific coordinated scanning behavior. For an originating computer to be flagged as participating in this coordinated scanning, which would indicate bot network activity, 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.

---

[166] 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.
[167] The mean average number of attacks per day for the companies observed was approximately 2,012 with a standard deviation of approximately 27,311 while the median was 57. This illustrates the large positive skew represented in the data.

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.[168] 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 referred to 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.

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.

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.

---

[168] 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.

Targeted attack activity by industry

For the purposes of the 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 33 represents the industry breakdown of 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 directed 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.
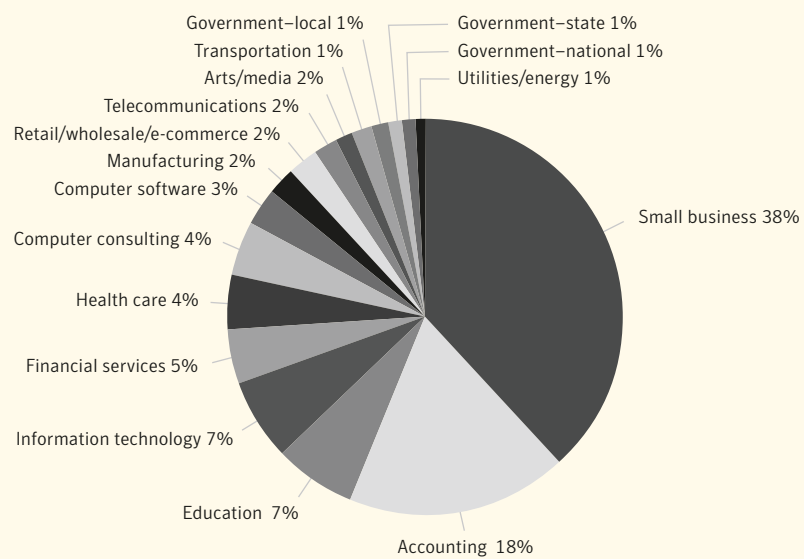
Government–local 1%
Transportation 1%
Arts/media 2%
Telecommunications 2%
Retail/wholesale/e-commerce 2%
Manufacturing 2%
Computer software 3%
Computer consulting 4%
Health care 4%
Financial services 5%
Information technology 7%
Education 7%
Accounting 18%
Government–state 1%
Government–national 1%
Utilities/energy 1%
Small business 38%

Figure 33. 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 13,000 distinct entries. 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

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. The classification system is based on Taimur Aslam *et al* (1996),[169] who define the taxonomy used to classify 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
• Atomicity error
• Environment error
• Configuration error
• Design error

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

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, or availability of the affected system. Symantec analysts calculate a severity score on a scale of 1 to 10 for each new vulnerability discovery. 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 credentials 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 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. For the purposes of this report, vulnerabilities are rated as high, moderate, or low severity based on the scores presented in table 13 below. For the purposes of the *Internet Security Threat Report*, each vulnerability is categorized as 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. As well, 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 (4–7)—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 (8–10)—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 ≥ 8
Moderate	4 ≤ X≤ 7
Low	X ≤ 3

Table 13. Measurement of severity level

Remotely exploitable vulnerabilities, adjusted severity

Because the majority of vulnerabilities are remotely exploitable, and remote exploitability raises severity, the overall severity composition of vulnerabilities is skewed towards having a higher severity. This metric attempts to compensate for this. The metric is computed using the severity rating formula with the remote exploitability criteria (as a weighted factor in the formula) removed. This metric only includes remotely exploitable vulnerabilities.

Ease of exploitation

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

- **Exploit available**—exploit code to enable the exploitation of the vulnerability is publicly available to all would-be attackers.

- **No exploit 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 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 development time

The ability to measure exploit development time is limited and applies only to the vulnerabilities that would normally require exploit code. Therefore, the metric is based on vulnerabilities that Symantec considers to be of sufficient complexity,[170] 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 associated with 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 publication is the date of the first reference to the exploit code found.

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

Patch development and availability time

The time to patch metric measures the time lapse between the disclosure date of a vulnerability and the release date of a patch. 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
- EMC
- IBM®
- Cisco®
- Oracle®

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

---

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

Browser vulnerability comparisons

This metric will offer a comparison of vulnerability data for numerous browsers, namely: Microsoft Internet Explorer, the Mozilla browsers (which includes 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:

• Because of the difficulty in comparing verifiable, confirmed, unique vulnerabilities, only those that were confirmed by the vendor were taken into consideration.

• 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.

• 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 form of malicious code that emerges both in the wild and in a "zoo" (or controlled laboratory) environment. Descriptive records of new forms of malicious code are then entered into a database for future reference. For this report, 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.

Sasser and Netsky calculation

In order to determine the percentage of malicious code for which the author of the Sasser and Netsky worms was responsible, the total reports of all Sasser and Netsky variants received by Symantec in 2004 was calculated. This number was then compared against the total malicious code reports received by Symantec for the same period. While the original author was not directly responsible for all variants of Sasser and Netsky, he is still considered to be indirectly responsible for their creation. Additionally, the author made the source code for Netsky publicly available, thus facilitating the creation of additional variants due to his actions.

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 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 impact 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,[171] 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 attracts 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.

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, sent to unique users. The messages attempt to gain confidential and personal information from online users.

Symantec Brightmail AntiSpam software reports statistics to Security Response 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 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 warranted 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 upon similarities in the message bodies and headers. Sample messages are then passed through general fraud heuristics to identify messages as 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.

[171] Systems deploying Symantec AntiVirus security solutions

The data presented in this section is based on 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 customer base 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 sent to users 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 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.

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 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 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 the host country of origin and the percentage of spam originating in each country is derived from the total volume of 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 networks 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 spammers are located.

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