



Symantec Internet Security Threat Report

Trends for July 04–December 04

Volume VII, Published March 2005

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

Daniel Hanson

DeepSight Threat Analyst
Symantec Security Response

Marc Fossi

DeepSight Threat Analyst
Symantec Security Response

Sarah Gordon

Sr. Principal Research Engineer
Symantec Security Response

Peter Szor

Security Architect
Symantec Security Response

Eric Chien

Security Researcher
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

Symantec Internet Security Threat Report

Contents

Executive Summary	4
Attack Trends	13
Vulnerability Trends	33
Malicious Code Trends	46
Additional Security Risks Report	60
Future Watch	75
Appendix A—Symantec Best Practices	80
Appendix B—Attack Trends Methodology	82
Appendix C—Vulnerability Trends Methodology	87
Appendix D—Malicious Code Trends Methodology	91
Appendix E—Additional Security Risks Methodology	92

Executive Summary

The Symantec *Internet Security Threat Report* provides a six-month update of Internet threat activity. It includes analysis of network-based attacks, a review of known vulnerabilities, and highlights of malicious code and additional security risks. This summary of the current *Internet Security Threat Report* will alert readers to current trends and impending threats. In addition, it will offer recommendations for protection against and mitigation of these concerns. This volume covers the six-month period from July 1, 2004 to December 31, 2004.

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 over 20,000 sensors monitoring network activity in over 180 countries. Symantec also 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. In addition, Symantec maintains one of the world's most comprehensive databases of security vulnerabilities, covering over 11,000 vulnerabilities affecting more than 20,000 technologies from over 2,000 vendors. Furthermore, Symantec operates BugTraq™, one of the most popular forums for the disclosure and discussion of vulnerabilities on the Internet. Finally, the Symantec Probe Network, a system of over two million decoy accounts, attracts email messages from 20 different countries around the world, allowing Symantec to gauge global spam and phishing activity. These resources give Symantec analysts unparalleled sources of data with which to identify emerging trends in attacks and malicious code activity.

The Symantec *Internet Security Threat Report* is grounded principally on the expert analysis of this data. Based on Symantec's expertise and experience, this analysis yields a highly informed commentary on current Internet threat activity. By publishing the analysis of Internet security activity in the *Internet Security Threat Report*, Symantec hopes to provide the computer security community with the information they need to help effectively secure their systems now and in the future.

Phishing a growing threat

In the last volume of the *Internet Security Threat Report*, Symantec identified phishing as an emerging security threat.¹ Phishing is an attempt by a third party to solicit confidential information from an individual, group, or organization, often for illicit financial gain or other fraudulent purposes. These attempts are often conducted through a Web browser and involve social engineering.

Phishing is a serious threat, not only to consumers but also to e-commerce companies, financial institutions, and other organizations that conduct transactions over the Internet. Phishers often use spoofed email, malicious Web sites, or Trojans delivered surreptitiously through a Web browser to trick users into disclosing sensitive data, such as credit card numbers, online banking information and other confidential information. If consumers lose confidence in the security of transactions conducted over the Internet, businesses and organizations that rely on such transactions could suffer serious financial losses.

Illustrating the prevalence of these threats is the increase in the number of phishing attempts being blocked. In mid-July 2004, Symantec Brightmail AntiSpam™ antifraud filters were blocking 9 million phishing attempts per week. By the end of December this number had increased to a weekly average of over 33 million messages being blocked per week.

¹ The Symantec *Internet Security Threat Report*, Volume VI (September 2004): p. 44
<http://enterprisecurity.symantec.com/content.cfm?articleid=1539>

Symantec expects that phishing will continue to be a very serious concern over the next year. Phishing attacks are difficult to defend against. As the sophistication of spoofed email and Internet sites increases, it will become more difficult for users to determine what is legitimate and what is not. Symantec recommends that in addition to following best practices, organizations ensure that end users are educated about phishing in general, and about the latest phishing scams in particular.² Symantec advises that end users never disclose any confidential personal or financial information if they have any doubts about the authenticity of any email or Web site.

Web application security threats increasing

In the previous volume of the *Internet Security Threat Report*, Symantec noted that vulnerabilities in Web applications were becoming more common.³ This raised concerns that attackers would increasingly target Web applications in the near future. Security activity over the past six months appears to have borne out those concerns.

Web applications are technologies that rely on a browser for their user interface and are often hosted on Web servers. They are a convenient way for users to share, create, or modify content through a Web browser. Web application vulnerabilities are particularly worrisome because they can expose information publicly over the Internet. They may allow an attacker to access confidential information from databases without having to compromise any servers. They may also allow an attacker to circumvent traditional perimeter security measures, such as firewalls, and are particularly dangerous because they could allow an attacker to compromise an entire network by gaining access through a single local system.

Typically, Web application vulnerabilities are targeted by attacks that take advantage of input validation errors and the improper handling of submitted requests. This could allow an attacker to execute malicious code on the target system. For instance, a worm targeting a Web application was detected in December 2004. Dubbed Perl.Santy,⁴ it targeted the popular Web application phpBB.

² A good resource for information on the latest threats can be found at <http://www.antiphishing.org>

³ The Symantec *Internet Security Threat Report*, Volume VI (September 2004): p. 30
<http://enterprisesecurity.symantec.com/content.cfm?articleid=1539>

⁴ <http://securityresponse.symantec.com/avcenter/venc/data/perl.santy.html>

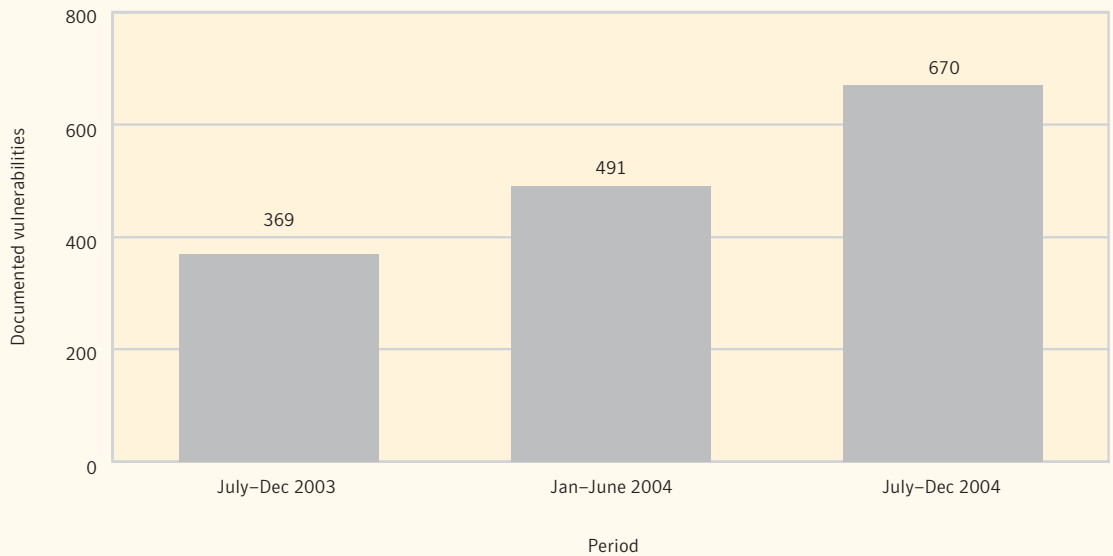


Figure 1. The increase in Web application vulnerabilities over 18 months
 Source: Symantec Corporation

Between July 1 and December 31, 2004, Symantec catalogued 670 vulnerabilities affecting Web applications, nearly half (48%) of the total vulnerabilities disclosed during this period (figure 1). This is substantially higher than the 39% documented in the first six months of 2004. This indicates that Web applications will likely continue to be a target of attack activity in the near future.

Symantec recommends that security administrators follow the best practices outlined in “Appendix A” of this report. They should also continually audit their Web applications for possible vulnerabilities and patch them as soon as possible. Finally, administrators should thoroughly review policy relevant to the deployment and usage of Web applications, restricting deployment only to Web applications that are absolutely necessary for organizational purposes.

Vulnerabilities continue to increase in number and severity

Between July 1 and December 31, 2004, Symantec documented 1,403 new vulnerabilities. This is an increase of 13% over the 1,237 vulnerabilities disclosed in the first six months of 2004. This indicates that vulnerability research remains a popular activity and that enterprises need to stay informed of the latest vulnerabilities that may affect their environments.

During the second half of 2004 nearly 97% of all reported vulnerabilities were rated as moderate or high severity, which could result in the complete or partial compromise of a system. In addition, over 70% of all the vulnerabilities reported during this period were easy to exploit. This means that no exploit code was needed or that exploit code was readily available, making the compromise of systems relatively easy. Compounding this problem is that nearly 80% of all the documented vulnerabilities in this reporting period are remotely exploitable, which can increase the number of possible attackers.

Symantec recommends that in addition to following best practices, enterprises continue to monitor their systems for known vulnerabilities and to patch them as soon as possible. Symantec also recommends that enterprises consider subscribing to a vulnerability alerting service that will provide them with early notification of new vulnerabilities.

Malicious code and exposure of confidential information

Some malicious code is created with the intent of stealing confidential information from a compromised computer. Information exposure threats can be present in almost any type of malicious code, including Trojan horses, worms, viruses, and back door server programs. Once a computer has been compromised by malicious code, information such as email addresses, cached logon credentials, proprietary data, and financial information may be accessed, disclosed, or altered without authorization.

Threats with the potential to expose confidential information have continued to increase over the past three reporting periods. Between July 1 and December 31, 2004, these threats represented 54% of the top 50 malicious code samples received by Symantec, up from 44% in the first half of 2004, and 36% in the second half of 2003. This represents a 23% increase between the current period and the first half of 2004, and a 50% increase over the same period the previous year (figure 2). This rise in information-exposure threats is partially due to the presence of bots and bot networks,⁵ which can expose confidential information on compromised computers because of their remote access capabilities.

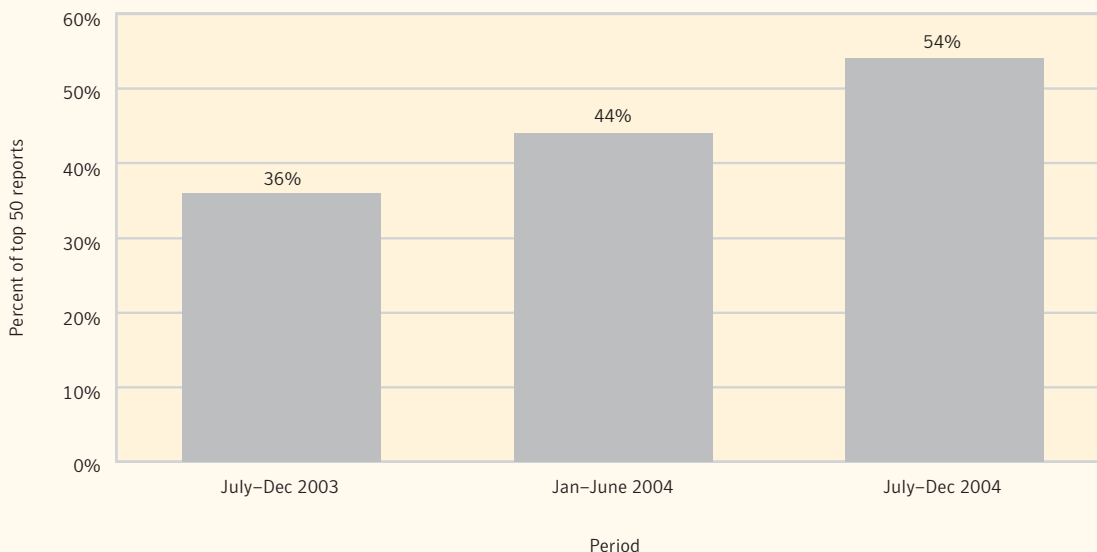


Figure 2. Malicious code threats to confidential information

Source: Symantec Corporation

⁵ 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. They allow an attacker to remotely control the targeted system 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.

Trojans continue to be a particular threat to confidential information, representing 33% of the top 50 malicious code reported to Symantec between July 1 and December 31, 2004. This is a significant increase over the first six months of the year when Trojans made up 17% of the top 50 malicious code reports. The rise in reported Trojans may be partially attributed to the increase in client-side exploits for Web browsers.⁶ The Trojan program may be hosted on a malicious Web site that attempts to exploit a specific Web browser vulnerability to deliver the Trojan.

Users can protect themselves from these threats by never executing unknown applications, especially those received in email or downloaded from sources that are not known to be trustworthy. Users should also avoid using public computer terminals to logon to Web-based email or online banking sites, as the integrity of these systems cannot be verified. Users should also avoid using single passwords for authentication in multiple applications, as the compromise of a single password may subsequently allow an attacker access to numerous sources of confidential data. Changing passwords frequently can also help protect against a password compromise. Finally, Symantec advises users not to allow Web browsers to cache logon credentials for Web sites.

Vulnerabilities affecting new alternative browser distributions

Historically, most of the exploits targeting Web browser vulnerabilities have been directed at Microsoft® Internet Explorer, the most widely used Web browser. In response to this, many people in the Internet community have turned to browsers such as Mozilla, Mozilla Firefox, Opera, and Safari as more secure alternatives. However, as security-conscious users have migrated away from Internet Explorer, attackers have followed suit. In response to the changing browser landscape, this volume of the *Internet Security Threat Report* Symantec is including an analysis of vulnerabilities in different browsers.

The discovery of vulnerabilities affecting browsers appears to be on the rise (figure 3), with more Mozilla vulnerabilities documented in this period than those affecting Microsoft Internet Explorer. This runs contrary to a trend seen in previous periods where nearly all browser vulnerabilities affected Microsoft Internet Explorer exclusively.

Between July 1 and December 31, 2004, Symantec documented 13 vulnerabilities affecting Microsoft Internet Explorer. This is notably lower than the 21 vulnerabilities affecting each of the Mozilla browsers that were documented during the same period. Six vulnerabilities were reported in Opera and none in Safari.

Though the share of vulnerabilities affecting the Mozilla browsers has increased, Microsoft Internet Explorer still has a greater proportion of high-severity vulnerabilities. Of the 13 vulnerabilities affecting Microsoft Internet Explorer documented by Symantec this period, nine were considered high severity. Of the 21 vulnerabilities affecting the Mozilla browsers, 11 were classified as high severity, while only seven affecting Firefox were highly severe. While there have been few, if any credible reports of attacks against Mozilla, Mozilla Firefox, Opera, or Safari in the wild, it remains to be seen whether these browsers will live up to the expectations that many have for them.

⁶ Client-side vulnerabilities target the computer systems of individual users rather than servers of an organization. They target applications such as Web browsers, email clients, peer-to-peer networks, instant messaging clients, and media players. They are often, but not always, the result of logic errors or flaws in access-control systems, and they are often easily exploitable, particularly in browsers.

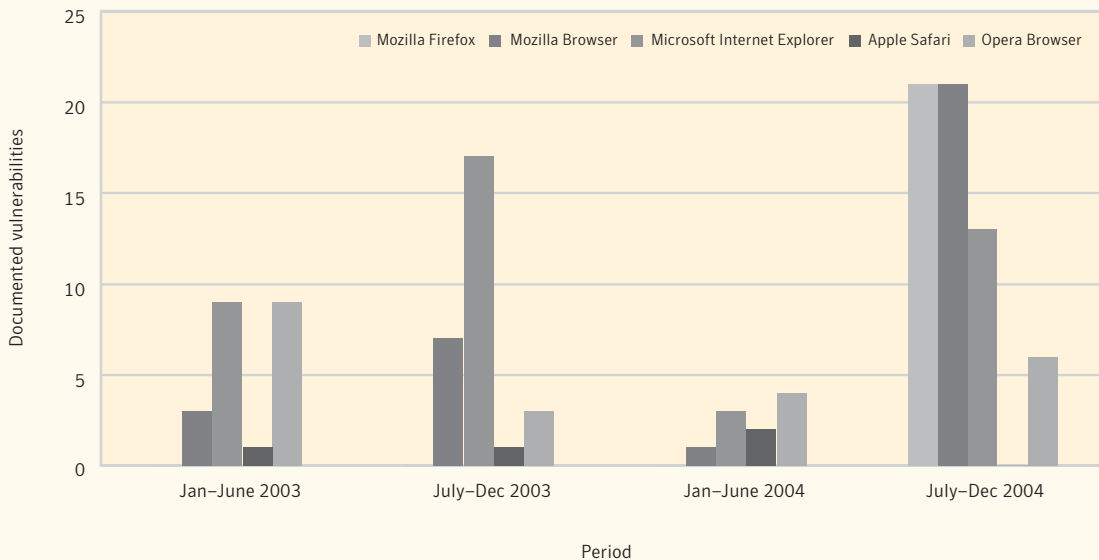


Figure 3. Documented browser vulnerabilities, Jan. 2003–Dec. 2004
 Source: Symantec Corporation

This data indicates that the attention of researchers may be shifting. In the rush to find more secure alternatives to Microsoft’s Internet Explorer, organizations and end users should be cautious about choosing an alternative, as all browsers appear to be susceptible to vulnerabilities. Symantec recommends that enterprise security administrators and consumers take the time to research browser alternatives and to evaluate their level of security before deploying them on the desktop. Furthermore, administrators are advised to subscribe to a vulnerability notification service, and to apply necessary patches across the enterprise in a timely manner.

U.K. has highest percentage of bot-infected computers in world

For this edition of the *Internet Security Threat Report*, Symantec has assessed the distribution of bot-infected computers across the Internet. In order to do this, Symantec calculated the number of computers worldwide that are known to be infected with bots, and assessed what percentage are situated in each country. The identification of bot-infected computers is important, as a high percentage of infected machines could indicate an increased likelihood of bot-related attacks. It could also indicate the level of patching and security awareness amongst computer users in a given region.

For the second half of 2004, 25.2% of the identified bots worldwide were located in the United Kingdom, making it the highest ranked country. Bots, as observed by Symantec, tend to compromise computers that are connected to the Internet by high-speed broadband connectivity. One factor that is likely to contribute to the rise of bot-infected computers in the United Kingdom is the rapid growth in broadband that is occurring there.⁷ Symantec believes that new broadband customers may not be aware of the additional security

⁷ <http://news.bbc.co.uk/1/hi/technology/4065047.stm>

precautions that need to be taken when using an always-on high-speed Internet connection. Furthermore, the addition of many new customers, with the corresponding increase in infrastructure and support costs may slow the response of Internet Service Providers (ISP) to reports of network abuse and infection.

Symantec recommends that organizations employ defense in-depth,⁸ including firewalls and adequate perimeter filtering. Furthermore, administrators are advised to subscribe to a vulnerability notification service, and to apply necessary patches across the enterprise in a timely manner. End users should always deploy antivirus software and a firewall. They should also ensure that antivirus definitions are updated regularly.

Win32 viruses and worms continue to rise

Win32 threats are executable programs that operate by using the Win32 application program interface (API), which provides the basis for all software development on the Microsoft Windows® platforms. Due to the widespread deployment of Microsoft Windows operating systems in enterprise and consumer environments, Win32 viruses and worms pose a serious threat to the security and integrity of those systems. A failure to prevent, detect, or remove these threats could result in severe financial losses, the disclosure of confidential information, and or the loss of data.

Throughout 2004, Win32 virus and worm variants showed a significant increase in volume (figure 4).⁹ Between July 1 and December 31, 2004, Symantec documented more than 7,360 new Win32 viruses and worms. This is an increase of 64% over the 4,496 reported in the first half of the year, and 332% over the 1,702 documented in the second half of 2003. As of December 31, 2004, the total number of Win32 variants was approaching 17,500. They are now more common than script- and macro-based threats combined.

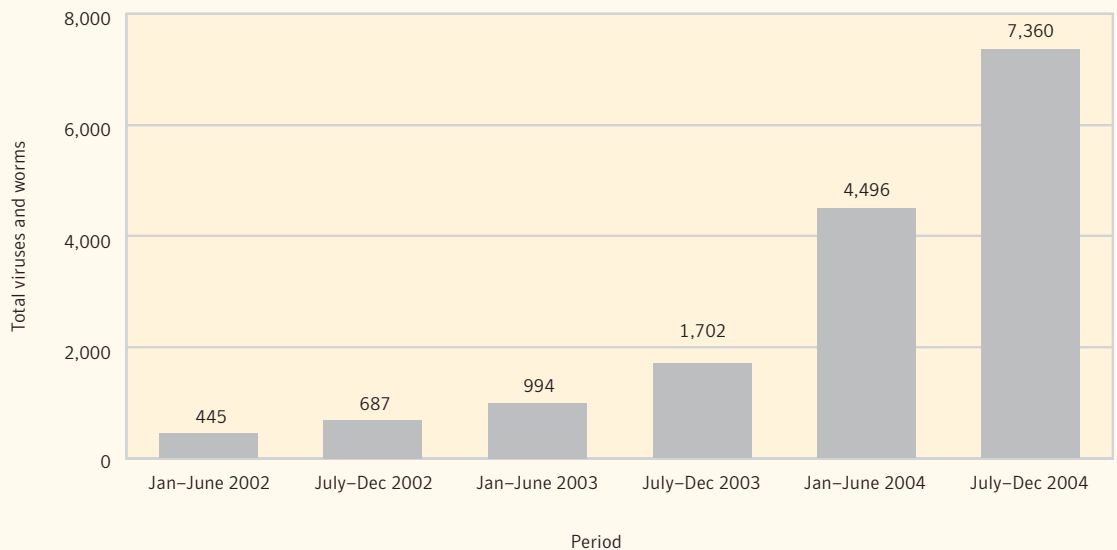


Figure 4. New Win32 viruses and worms by six-month period 2002–2004

Source: Symantec Corporation

⁸ The security approach in which each system on the network is secured to the greatest possible degree. This should include the deployment of antivirus, firewalls, and intrusion detection systems, amongst other measures.

⁹ In some cases, a particular family of malicious code, such as the Mydoom and Netsky families, may have multiple variants. A variant is a new iteration of the same family that may have minor differences but is still based on the original. In this report, variants of a family are counted as separate samples due to the variations in functionality.

Symantec Internet Security Threat Report

The continued upward trend of these Win32 variants suggests that despite the rapid response to these types of threats, malicious code authors continue to publish new variants—sometimes several in a day. Symantec recommends that security administrators and users update their antivirus solutions frequently and ensure that recommend best practices are followed at all times.

Financial services receives highest ratio of severe attacks

As part of its analysis of Internet attack activity, Symantec compares industry segments based on the ratio of severe events originating from external attackers detected by sensors deployed in each industry. Symantec determines severity of an attack based on the characteristics of the attack, the defensive controls of the client, the value of the assets at risk, and the success of the attack. Severe attacks pose the greatest threat to organizations, as they can result in serious damage and compromise of the target network. As such, they may indicate the risk to which an industry is exposed.

During the second half of 2004, the financial services sector experienced the highest number of severe events of any industry, 16 per 10,000 security events. This sector is likely an attractive target for attackers because of its high profile and association with financial transactions. It is clear that financial organizations must take appropriate steps to identify and mitigate risks of attack.

Due to the sensitive nature of the data in the financial services sector, Symantec recommends that security administrators consistently audit their networks for vulnerabilities and patch as soon as possible. Security administrators should also restrict access only to those services deemed absolutely necessary and enforce strong connectivity policies and procedures.

Internet Security Threat Report Highlights

Vulnerability Trend Highlights

- The time between the disclosure of a vulnerability and the release of an associated exploit increased from 5.8 to 6.4 days.
- Symantec documented 1,403 new vulnerabilities, a 13% increase over the previous six-month period.
- Web application vulnerabilities made up 48% of all vulnerabilities disclosed, up from 39% in the first half of 2004.
- 97% of vulnerabilities disclosed were rated as moderately or highly severe.
- 21 vulnerabilities affecting Mozilla browsers were disclosed during the last six months of 2004, compared to 13 vulnerabilities affecting Microsoft Internet Explorer.
- 70% of reported vulnerabilities were considered easy to exploit.

Attack Trend Highlights

- For the third straight reporting period, the Microsoft SQL Server Resolution Service Stack Overflow Attack (formerly referred to as the Slammer Attack) was the most common attack, used by 22% of all attackers.
- Organizations received 13.6 attacks per day, up from 10.6 in the previous six months.
- Known bot network computers declined from over 30,000 per day in late July to an average of below 5,000 per day by the end of the year.
- The United Kingdom had a higher percentage of bot-infected computers than any other country.
- The United States continues to be the top country of attack origin, followed by China and Germany.
- The financial services sector experienced 16 severe events per 10,000 security events, the highest ratio of any industry.

Internet Security Threat Report Highlights *continued*

Malicious Code Trend Highlights

- Variants of Netsky, MyDoom, and Beagle, dominated the top ten malicious code samples in the second half of 2004.
- Symantec documented more than 7,360 new Win32 viruses and worms, an increase of 64% over the first half of the year.
- Malicious code that exposed confidential information made up 54% of the top 50 malicious code samples, up from 44% in the previous reporting period.
- At the end of this reporting period there were 21 known samples of malicious code for mobile applications, up from one in June 2004.
- Two bots were present in the top ten malicious code samples, compared to just one in the previous reporting period.
- 4,300 new distinct variants of Spybot were reported, an increase of 180% over the previous six months.

Additional Security Risks Highlights

- In the last six months of 2004, adware programs made up 5% of the top 50 Symantec customer reports, up from 4% in the previous report.
- Five of the top ten reported adware samples were installed via a Web browser. Nine of the top ten reported spyware programs were bundled with other software.
- Iefeats was the most commonly reported adware program, accounting for 36% of the top ten reports.
- Webhancer was the most frequently reported spyware program during the second half of 2004, representing 38% of the top ten spyware reported.
- Between July 1 and December 31, 2004, Symantec detected 10,310 new phishing attacks.
- By the end of December, Symantec antifraud filters were blocking over 33 million phishing attempts per week on average, up from approximately 9 million per week at the beginning of July.
- Symantec reported a 77% growth in spam for companies whose systems were monitored for spam.

Attack Trends

This section of the Symantec *Internet Security Threat Report* will provide an analysis of Internet attack activity for the six months ending December 31, 2004. An attack may be defined as any malicious activity crossing a network that has been detected by an intrusion detection system or firewall. These attacks are usually an attempt to exploit a vulnerability in software or hardware. Attack activity for this period will be compared to data presented in the two previous *Internet Security Threat Reports*.¹⁰ Where applicable, suggestions on attack remediation will be made, including references to Symantec's best practices contained in "Appendix A" of this report.

Symantec has established one of the most comprehensive sources of Internet attack data in the world. Over 20,000 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 system¹¹ that is used to identify, observe, and study complete instances of worm and non-worm attack activity. It provides qualitative data 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.

For the purposes of this report, attack activity is divided into three categories: reconnaissance (probes), worm-related attacks, and non-worm related attacks (exploit activity). This allows Symantec analysts to differentiate between attacks that propagate autonomously (worms), attacks that are launched manually (non-worm-related), and attacks that are intended to gather information.

It is sometimes difficult to discern whether attack activity is worm-related or not. In these cases, attacks that are commonly associated with worms have been classified as worm-related. The use of back doors and remote-control software to create networks of zombie hosts called bot networks are classified as worm-related attacks for the purposes of this report.

Security devices can monitor for attacks and suspicious behavior at many different levels in the network. Devices such as intrusion detection systems, intrusion protection systems, 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 attacks, but view them in different ways. For instance, attack trends data is ranked based on the number of infected sources attempting to spread, whereas malicious code data is based on a number of sources, 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
- Attack activity per day
- Attack activity by type
- Top attacked ports
- Bot networks and denial of service attacks
- Denial of service attacks

¹⁰ The Symantec *Internet Security Threat Report* Volumes V (March 2004) and VI (September 2004), both available at: <http://enterprisesecurity.symantec.com/content.cfm?articleid=1539>

¹¹ A honeypot is an Internet-connected system that acts as a decoy, allowing attackers to enter the system in order to observe the attacker's behavior once he or she is inside it.

Symantec Internet Security Threat Report

- Top countries by bot-infected computers
- Top originating countries
- Top originating countries per Internet capita
- Targeted attack activity by industry
- Severe event ratio by industry

Top Internet attacks

The top attacks detected by Symantec Managed Security Services and Symantec DeepSight Threat Management System largely reflect attacks that security administrators are likely to observe on their own networks. Worm attacks are included in this metric, as they make up an important component of the risk that organizations must continue to defend against.

The analysis of top attacks is based on the percentage of total attacking IP addresses performing a given attack. In the first six months of 2004, six of the top ten attacks were new entries, indicating that significant changes were occurring in the threat landscape. Over the last six months of the year, there were only three new entrants in the top ten attacks (table 1), suggesting that a more stable information security threat environment may be prevailing.

Jul-Dec 2004 Current rank	Jan-Jun 2004 Previous rank	Attack	Jul-Dec 2004 Current percent of attackers	Jan-Jun 2004 Previous percent of attackers
1	1	Microsoft SQL Server Resolution Service Stack Overflow Attack	22%	15%
2	Not ranked (NR)	Generic TCP Syn Flood Denial of Service Attack	12%	NA
3	10	Microsoft Windows DCOM RPC Interface Buffer Overrun Attack	7%	1%
4	6	Generic SMTP Malformed Command/Header Attack	5%	2%
5	2	W32.HLLW.Gaobot Attack Version	4%	4%
6	NR	Generic Invalid HTTP String Attack	4%	NA
7	7	Generic ICMP Flood Attack	3%	2%
8	3	Generic WebDAV/Source Disclosure "Translate: f" HTTP Header Request Attack	2%	4%
9	9	Generic HTTP Directory Attack	2%	1%
10	NR	Generic UTF8 Encoding in URL Attack	2%	NA

Table 1. Top attacks
Source: Symantec Corporation

Between July 1 and December 31, 2004, the Microsoft SQL Server Resolution Service Stack Overflow Attack was the most common attack, accounting for 22% of attacking IP addresses. This continues the trend seen during the first six months of 2004, during which this attack was also the most common. It should be noted that in the previous reporting period, this attack was identified as the Slammer attack, as the majority of the attack activity was associated with the original Slammer worm. However, other malicious code threats are now also known to be using this attack. As a result, Symantec has reverted to the original nomenclature of this attack.

This is the third consecutive reporting period for which the Microsoft SQL Server Overflow Attack has been the most common attack. The continued prominence is related to three factors. First, many threats, including the original Slammer worm, use a single UDP packet to exploit this vulnerability. The use of UDP allows this attack to come from a spoofed¹² source address, which may inflate the number of observed source IP addresses. Spoofing source addresses increases the ability to obscure the source location of the attack, making investigation and response significantly more difficult. While Slammer did not spoof its source, other mechanisms that use this attack may do so. Analysis of the source addresses indicates that up to 10% of these attacks originate from spoofed addresses that do not exist.

Secondly, the use of UDP also allows an attacker to send a complete attack¹³ to every IP address, regardless of whether SQL Server is installed or running. This means that intrusion detection systems will often interpret every attack attempt as a full attack.

The third factor that can affect the number of systems vulnerable to this attack, and therefore the number of attacking systems, is the deployment of MSDE, the Microsoft Desktop Engine. MSDE is included and deployed by many third-party applications. It is a variant of the SQL Server engine, which means it is also vulnerable to Slammer or Slammer-related attacks. Identifying and patching these systems is challenging, and the ongoing installation of software running vulnerable versions of MSDE can turn a previously secure computer into a potential victim.

The second most common attack during the second half of 2004 was the TCP SYN Flood Denial of Service Attack, which was launched by 12% of attackers. It should be noted that some IDS signatures associated with this attack may be prone to false positives, which may inflate the number of attacks detected. Despite this, Symantec still believes that this attack is occurring at a significant rate. A generic denial of service (DoS) strategy, this attack has not previously been ranked as a top attack. It is characterized by an overwhelming flood of requests to an Internet service running on a computer. A SYN packet initiates each TCP session. By overwhelming a target with SYN requests and not completing the initial request, the attack prevents other valid requests from being processed. This attack often relies on an attacker spoofing the source of the packets for maximum effect, a characteristic that is likely to have increased the number of source attackers.

The appearance of this more traditional DoS attack is intriguing. It indicates that while attackers have been experimenting with new forms of DoS attacks (primarily using bot networks), they may be migrating back to more traditional DoS methods.¹⁴ With the spread of bot networks, and the easy availability of victim hosts (due to vulnerabilities in DCOM RPC, LSASS and other default Windows services), it had become relatively easy for an attacker to marshal hundreds or thousands of bots to overwhelm a victim with valid

¹² The term "spoofed" refers to the practice of establishing a connection with a forged sender address. This normally involves exploiting a trust relationship that exists between source and destination addresses or systems. The IP address that is used as the source address when spoofed may be a valid address used elsewhere on the Internet. It may also be from unallocated IP space and, therefore, unused.

¹³ UDP does not require that any form of synchronization be done before data is sent and accepted by the target service. By contrast, an attack that uses TCP must go through the three-way handshake to synchronize the systems prior to data being sent; therefore, a TCP-based attack will only be seen if the service being targeted is accepting connections. In the case of UDP, the attacking system can simply send the complete attack without regard for whether the service is listening.

¹⁴ This conclusion is further supported by the "Bot networks and denial of service" discussion, which is included below.

Symantec Internet Security Threat Report

requests. However, the introduction of Windows XP Service Pack 2¹⁵ and other mitigating measures appears to have limited the number of computers available for compromise. This may have resulted in a corresponding decline in the number of computers available for use in bot network scanning. With less bots available, attackers are again relying on older techniques to attack victims. (For a more in-depth discussion, please see the “Bot networks and denial of services” section below.)

To protect against the threat of DoS attacks, different procedures can be used. In the case of a SYN flood attack, computer operating systems and firewalls often have internal configuration parameters to ensure that the resources necessary to service valid requests are available. Administrators should familiarize themselves with proper tuning of their systems and ensure that they can engage their upstream Internet service provider to help filter incoming DoS traffic.

Between July 1 and December 31, 2004, the Microsoft Windows DCOM RPC Interface Buffer Overflow Attack was the third most common attack. It has regained prominence as a top attack after ranking tenth in the first six months of the year. This attack, most famously used by Blaster¹⁶ to spread in 2003, has more recently been used by the different bot network applications, including Gaobot, Spybot and Randex.¹⁷ The prevalence of this attack indicates that attackers are continuing to use this vulnerability to target systems. Analysis of data from the Symantec honeypot system indicates that a majority of the attack attempts occur from systems infected with variants of Gaobot, Spybot, and other bot network applications.

Systems administrators can mitigate the threat of exploitation by ensuring that TCP ports 135 and 445 are filtered at the network perimeter. However, worms and other malicious code targeting vulnerabilities over this port may be able to bypass the network perimeter using a VPN or a mobile computer such as a laptop. As a result, to prevent further damage if an infection takes place, perimeter blocking should be implemented accompanied by strong filtering between logical network segments to limit propagation. Strong system configuration policy and audit control for all computers that do not remain behind a firewall can significantly decrease chances of infection.

Gaobot has fallen from being the second most common attack over the first six months of 2004 to fifth in the second half of the year. Gaobot, a type of bot, can allow an attacker to maintain control over a large number of discrete systems and instruct those systems to scan for, exploit, and control new systems. It can also be rapidly updated with exploits targeting new vulnerabilities, allowing widespread compromise of unpatched systems shortly after an exploit is available publicly. As a result, it remains a significant threat for any organization with Windows systems that are not rapidly patched for new vulnerabilities. In addition to timely deployment of critical patches, the use of a personal or desktop firewall can significantly reduce the risk of compromise by bot applications. (For more on bot network activity please see the “Malicious Code Trends” section of this report.)

¹⁵ Microsoft released Windows XP Service Pack 2 in August 2004. The actual release date varied depending on the version and language of Windows XP. XP Home first received SP2 via Windows Update on August 16, 2004. The service pack included vulnerability fixes, activation of the XP firewall, the ability to monitor the status of third-party antivirus and firewall applications, and rate limiting to control the volume of outgoing connections each computer can make. Each of these steps lessens the ability of attackers to use a computer as a participant in a distributed bot network.

¹⁶ <http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.worm.html>

¹⁷ A full discussion of the rise in bot variants can be found in the “Malicious Code Trends” section of this report.

Attack activity per day

This section will discuss the number of attacks per day seen by organizations connected to the Internet. The number of attack attempts an average organization experiences in a given period of time is taken to be representative of the overall attack rate on the Internet as a whole. The attack activity per day is determined by the number of attacks detected against the median organization in the sample set.

Between July 1 and December 31, 2004, the average attack rate for an organization in the sample set was 13.6 attacks per day (figure 5). In the previous six-month period, the average attack rate for an organization was 10.6 attacks per day. By comparison, during the last six months of 2003, the average organization experienced 12.6 attacks per day.

The increase of three attacks per day is due to increases in the volume of probes and non-worm-based attacks. Previously, in periods with an elevated daily attack rate, worm activity was the most significant contributor to this increase. By contrast, in the current period, worm activity continued to decline from previous levels and the bulk of the rise in activity was related to non-worm attack activity. The changes in the attack breakdown are further detailed in the “Attack activity by type” section below.

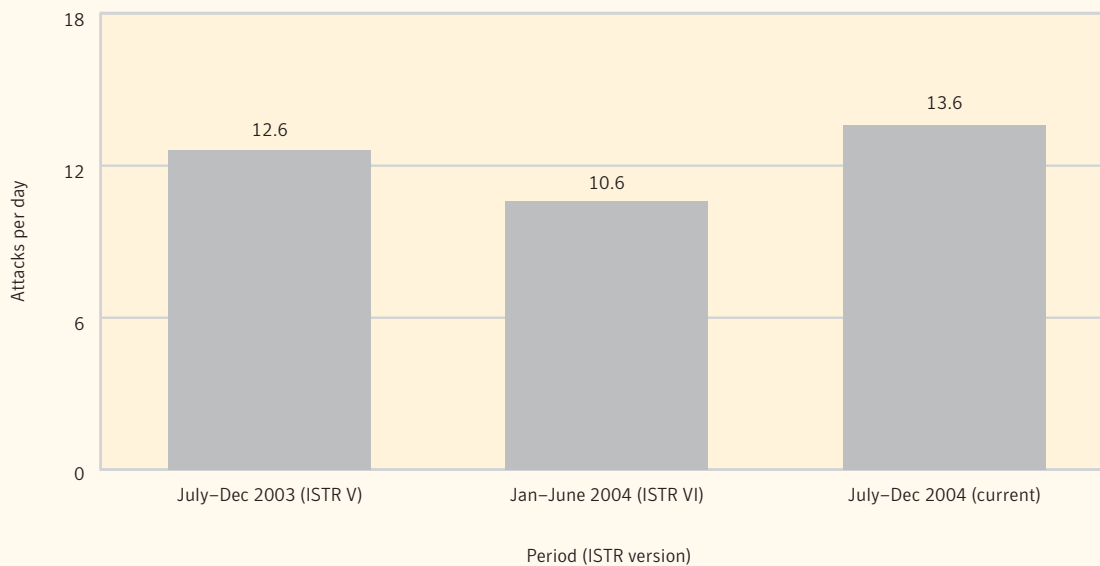


Figure 5. Daily attack rate over the last three six-month periods

Source: Symantec Corporation

Attack activity by type

In order to better understand current Internet attack activity and how to best protect against it, it is helpful to understand specifically what type of attacks are taking place. This section will discuss the attack activity that has occurred over the past six months broken down by three types of attack: probes, worm-related attacks, and non-worm-related attacks. The type of attack is analyzed as a percentage of the total volume of detected attacks (figure 6).

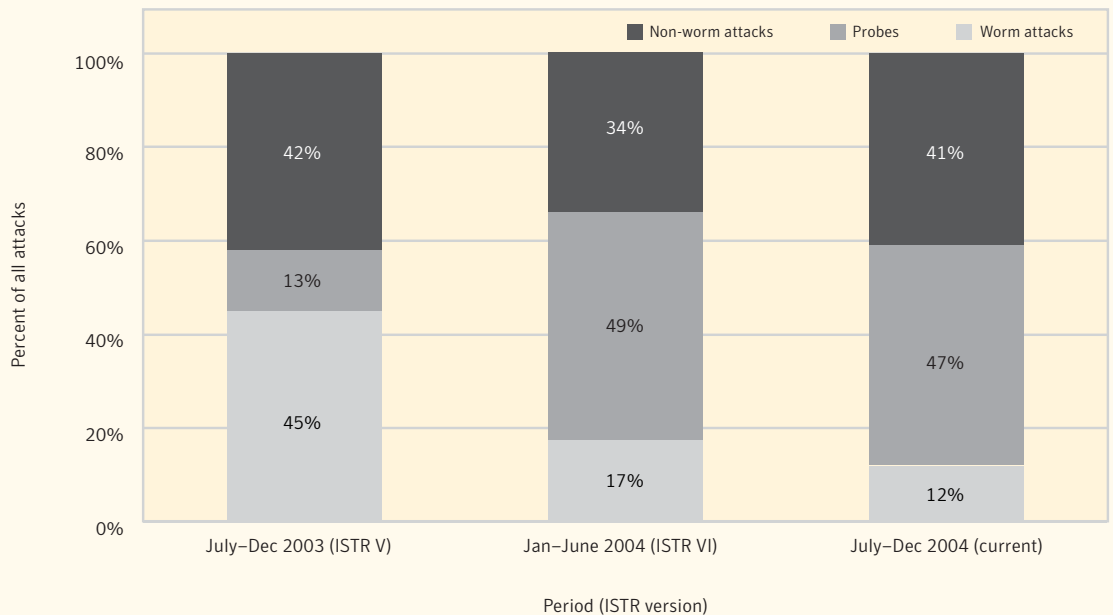


Figure 6. Breakdown of attack type July 1–December 31, 2004

Source: Symantec Corporation

From July 1 to December 31, 2004, 47% of detected attacks were classified as probes. This is similar to the 49% of activity that was classified as probe activity in the first six months of the year. Scanning for back door services on high-level ports (that is, ports numbered higher than 1023) continues to contribute to the probe total. Widespread scanning for these back door services has been increasing over the past three report periods and is expected to continue.

Several mitigation measures should be put in place to ensure that these scans don't find a viable target. Administrators should ensure that systems are running antivirus software with up-to-date definitions. Symantec also recommends that strong perimeter filtering and connection logging be put in place. Finally, administrators should log outgoing connections to find internal machines that may have been compromised.

Symantec Internet Security Threat Report

In the final six months of 2004, worms accounted for only 12% of attack activity (figure 6), the lowest level in the last four six-month reporting periods. Worm attack activity has declined steadily from 59% in the first half of 2003. The most significant drop occurred between the last six months of 2003 and the first six months of 2004, when worm attacks dropped from 45% to 17%.

The low rate of worm activity can be explained by the fact that no traditional worms were discovered to be propagating widely during this period. In fact, the prevalence and popularity of bot networks and semi-autonomous exploitation tools is making the distinction between worm attacks and non-worm attacks more difficult. As this trend continues, it may be necessary to stop attempting to distinguish between worm and non-worm activity.

While worm activity has decreased over the past three reporting periods, non-worm attack activity does not appear to be following any long-term trend, as was noted in the previous volume of the *Internet Security Threat Report*.¹⁸ Non-worm attacks have varied from a high of 42% of activity in the last half of 2003, to a low of 34% in the first half of 2004. In the second half of 2004, they rose again to make up 41% of activity. Symantec believes that exploits for older vulnerabilities and emerging Web application and client-side vulnerabilities are being included in non-worm toolkits, which contributes to the static nature of non-worm attack trends.

Traditionally, network intrusion detection systems have provided adequate coverage of network-borne threats. However, the increasing use of Web application attacks and client-side exploitation, particularly through browser attacks and through malformed files such as images, are proving problematic for traditional intrusion detection systems. They are also making the classification of probes, attacks, and worm-related attacks increasingly difficult. As these trends evolve, particularly Web application attacks and client-side attacks, new classification and detection systems will need to be developed to meet this need. By extension, this section of the *Internet Security Threat Report* will likely have to expand its traditional typology to include the emerging class of Web application attacks.

Top attacked ports

Symantec DeepSight Threat Management System tracks the top attacked ports as detected by all contributing firewall sensors (table 2). The best criterion for judging the top attacked ports is the number of unique IP addresses that are targeting each port. This metric only reflects attacker interest in a given port; it does not assume that there is necessarily an attack associated with it, such as the specific service being targeted. Nor does it attempt to provide any attack information. The lack of definitive attack information means that it is impossible to separate out worm-related activity from information-gathering attacks or exploit attempts. This metric only identifies and measures rejected or denied connection attempts; therefore, legitimate port activity should not be represented in the data.

¹⁸ Symantec *Internet Security Threat Report* Version VI, September 2004: p. 10
<http://enterprisesecurity.symantec.com/content.cfm?articleid=1539>

Jul-Dec 2004 rank	Jan-Jun 2004 rank	Port	Service description	Jul-Dec 2004 Percent of total attackers	Jan-Jun 2004 Percent of total attackers
1	2	445 TCP	CIF (Microsoft file sharing)	35%	17%
2	3	135 TCP	DCE-RPC (remote Microsoft Windows communication)	17%	15%
3	7	1026 UDP	Various dynamic services	8%	3%
4	4	4662 TCP	Edonkey (file sharing)	6%	7%
5	NR	1027 UDP	Various dynamic services	5%	NA
6	5	6346 TCP	Gnutella (file sharing)	5%	5%
7	NR	139 TCP	SMB (Microsoft file sharing)	4%	NA
8	10	1025 TCP	Various backdoors and dynamic services	2%	3%
9	NR	1434 UDP	Microsoft SQL services	2%	NA
10	NR	25 TCP	SMTP services	2%	NA

Table 2. Top attacked ports

Source: Symantec Corporation

From July 1 to December 31, 2004, port 445 was the most frequently targeted port, with 35% of attackers targeting it. Port 445 is the common port for Microsoft File and Printer Sharing (often referred to as SMB or CIFS). In addition to being used for file sharing, other remote management functionality is accessible through this port, including some remote procedure call (RPC) functionality, which likely explains its widespread appeal for attackers. In the first half of 2004, 445 was the second most attacked port. A significant portion of that attack activity was attributed to the continued activity of the Sasser worm.¹⁹

Analysis of the Symantec honeypot system has shown that bot network applications, including variants of Spybot and Gaobot, are heavy attackers of 445. Primarily, they target the Microsoft Windows LSASS Buffer Overrun Vulnerability²⁰ and the Microsoft Windows DCOM RPC Interface Buffer Overflow vulnerability²¹ through this port. In addition to exploitation of these vulnerabilities, some attacks are performed when an easily guessable user name and password combination allows an attacker to access the file share directly.

TCP port 445 is usually well controlled at the network perimeter. However, worms and other malicious code targeting vulnerabilities over this port may be able to bypass the network perimeter through a VPN or via a mobile computer such as a laptop. As a result, to prevent further damage if an infection takes place, perimeter blocking should be implemented accompanied by stronger filtering between logical network segments to limit propagation. Strong system configuration policy and audit control for all computers that do not remain behind a firewall can significantly decrease chances of infection.

TCP port 135 was the second most frequently targeted port between July 1 and December 31, 2004. It had been the third most attacked port in the first half of the year. There was a small rise in the percentage of attackers targeting the port, from 15% in the first six months of 2004 to 17% the second half of the year.

¹⁹ <http://securityresponse.symantec.com/avcenter/venc/data/w32.sasser.worm.html>

²⁰ <http://www.securityfocus.com/bid/10108>

²¹ <http://www.securityfocus.com/bid/8205>

Symantec Internet Security Threat Report

Port 135 is associated with the Microsoft RPC service on computers running Microsoft Windows. Most of the activity detected between July and December 2003 was related to the highly successful Blaster²² and Welchia²³ worms, which were propagating successfully at that time. In 2003, activity targeting TCP port 135 achieved its peak when almost a third of attacking hosts were targeting it. Since the outbreak of those worms, this port, along with TCP port 445, has been popular with attackers looking to build bot networks. Both ports are heavily targeted by Spybot and Gaobot.

Like TCP port 445, TCP port 135 is usually well controlled at the network perimeter; however, worms and other malicious code can bypass perimeter protections by VPN connections and mobile laptop computers. To limit the potential damage incurred by attacks against this port, Symantec recommends the deployment of desktop or personal firewalls, and strong system configuration and policy controls, especially for computers that do not remain behind a firewall.

UDP port 1026 was the third most frequently targeted port during the last six months of 2004, with 8% of attackers targeting it. This is up from 3% for the first half of 2004, when it was the seventh most commonly targeted port. UDP port 1026 has been used in the past as a method of delivering RPC Messenger pop-up spam to Microsoft Windows hosts. The spoofable nature of UDP means that the ranking of this port should be treated cautiously. Without any indication of whether or not the addresses are spoofed, the true nature and source of this activity cannot be determined. Analysis of Symantec honeypot system activity indicates that pop-up spam continues to plague UDP 1026. While exploitation of the RPC DCOM overflow is possible by this route, Symantec has not yet observed any widespread attack activity of this type on this port.

TCP port 80 has historically been the top attacked port. It hosts Web servers, which are popular targets for worms such as Code Red and Nimda. It also hosts Web applications, which are an emerging target for malicious code. However, over the last six months of 2004, port 80 did not rank as a top targeted port. This is quite a change from the first six months of 2004, when it was the top scanned port, accounting for 30% of the scanning IP addresses. The biggest reason for this decline was that Welchia.B stopped propagating in June, at the end of the previous sample period. Welchia.B was written with an expiry date, beyond which it would not attempt to spread.

Attacks targeting Web servers and Web applications continue to be feasible methods of compromising information; however, as noted by the significant presence of TCP ports 445 and 135, the majority of attacks remain attempts to compromise and control both desktop computers and servers alike. The Perl.Santy²⁴ worm shows that widespread scanning for a port is not necessary for a worm to successfully target a Web technology.

Santy targeted the PHPBB Viewtopic.PHP PHP Script Injection Vulnerability²⁵ in the phpBB Web bulletin board application. This worm chose its targets with a Google search rather than by scanning networks for Web servers, as many traditional Web-based worms (such as Code Red and Nimda) have done. The lack of scanning for targets ensured that activity associated with this worm would not appear in port 80 traffic activity. Further, only those organizations that were running a potentially vulnerable application would be targeted, making a rise in scanning activity much more difficult to detect. (Santy is discussed in greater depth in the "Malicious Code Trends" section of this report.)

²² <http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.worm.html>

²³ <http://securityresponse.symantec.com/avcenter/venc/data/w32.welchia.worm.html>

²⁴ <http://securityresponse.symantec.com/avcenter/venc/data/perl.santy.html>

²⁵ <http://www.securityfocus.com/bid/10701>

Symantec Internet Security Threat Report

UDP port 1434, the ninth most widely targeted port, is the port affected by the Microsoft SQL Server Resolution Service Stack Overflow Attack. The low rank that this port displays is likely due to security administrators deciding to disable the logging of infection attempts on this port for performance reasons or to simplify log auditing.

Bot networks and denial of service attacks

Beginning with Volume VI of the *Internet Security Threat Report* (September 2004), Symantec has been identifying groups of computers performing coordinated scanning or attack patterns. This allows Symantec to identify bot networks that are engaged in coordinated activity. This has the added advantage of detecting some types of worms that would go undetected by other methods. Identification of these computers should not be considered exhaustive: in order to limit the number of false positive identifications, multiple behavioral requirements have to be met by each computer.

Bot networks are groups of compromised computers on which attackers have installed software that listens for and responds to commands (usually via 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. Bot networks are often more dangerous to new vulnerabilities than worms are, as they don't require an attacker to write propagation code in order to exploit the vulnerability. This vastly simplifies the inclusion of new exploits. Additionally, any number of exploits can be included, making it difficult to differentiate between a bot network attack and a targeted attack by a single attacker.

Over the first six months of 2004, Symantec analysts observed a persistent increase in the number of computers identified as belonging to bot networks. During this period, the average number of computers identified in daily bot network scanning increased to over 30,000 systems a day. This trend was expected to continue as additional systems were added to these bot networks; however, as shown in figure 7, this increasing trend did not continue through the second half of the year.

Between July 1 and December 31, 2004, observed bot network computers actively scanning declined from a peak of over 30,000 per day in late July to below 5,000 per day by the end of the year. The bulk of this decrease occurred in mid-August with a significant drop on August 19. The timing of this drop corresponds closely with the availability of Windows XP Service Pack 2. It is reasonable to assume that this service pack is responsible, along with other mitigation measures, for the decline in identified bot network computers.

It should be noted that this discussion is based on coordinated and focused bot network activity. Any significant shift by attackers, particularly one towards smaller groups of computers scanning for a shorter period of time might reduce the effectiveness of this method of bot network identification and analysis. The analysis of bot network trends included in the "Malicious Code Trends" section of this report shows a significant rise in the number of variants and a rise in the number of reports of these bot applications. One possible explanation for these apparently divergent trends is the emergence of smaller bot networks. Smaller network sizes would make detection based on coordinated scanning more difficult.

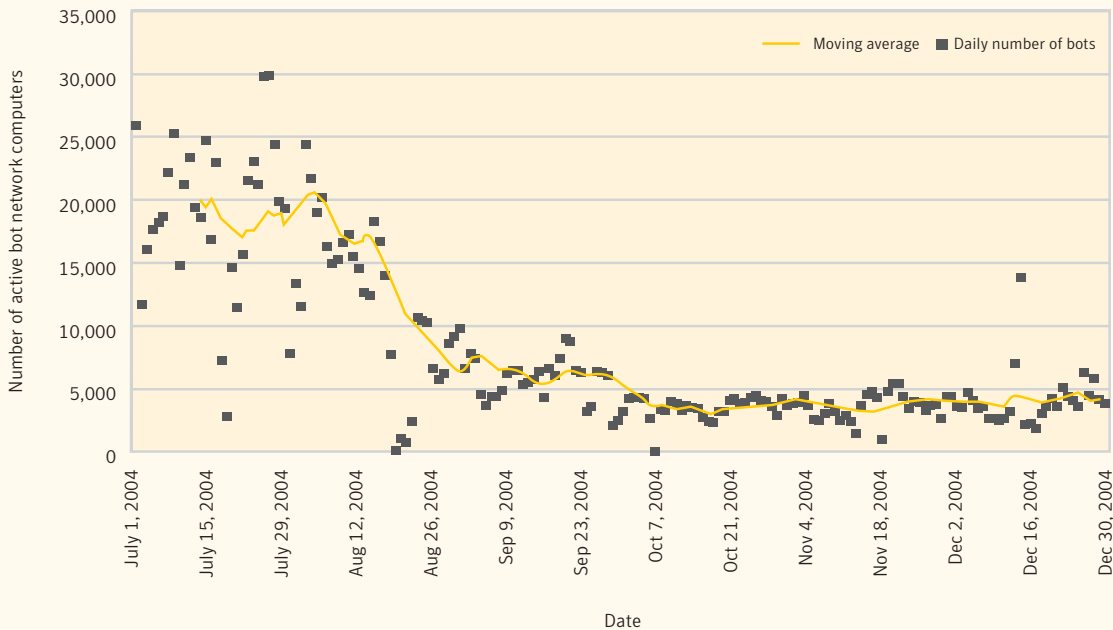


Figure 7. Known bot network computers, July 1–December 31, 2004
 Source: Symantec Corporation

Symantec investigated the declining bot network scanning patterns (figure 8). This investigation showed that the significant drop in bot network computers is largely associated with very large drops in the number of computers performing coordinated scanning for and attacking TCP port 445 and TCP port 135. The drop in computers participating in coordinated bot network scanning on these two ports largely accounts for the decrease in identified bot systems. Both ports are common paths for bot networks to spread onto computer systems, either through unpatched vulnerabilities or bad user name and password choices.

Many common bot network applications, including Gaobot, target vulnerabilities that are accessible through these Windows ports as a method of infecting new systems. The sudden drop in bot network scanning indicates that Service Pack 2, in addition to cumulative patches, may have been successful at reducing the number vulnerabilities in Windows XP systems that are subject to remote compromise.

The inclusion of default firewall rules that block TCP port 135 and confine TCP port 445 activity to only the local subnet may have helped to reduce the chances of compromising a badly secured machine for participation in a bot network. These bot networks are a significant threat to many Internet-connected systems, as they can easily be used to perform denial of service attacks. The loss of potential victim computers to serve in bot networks appears to also have changed denial of service attack patterns, which will be discussed in the following section.

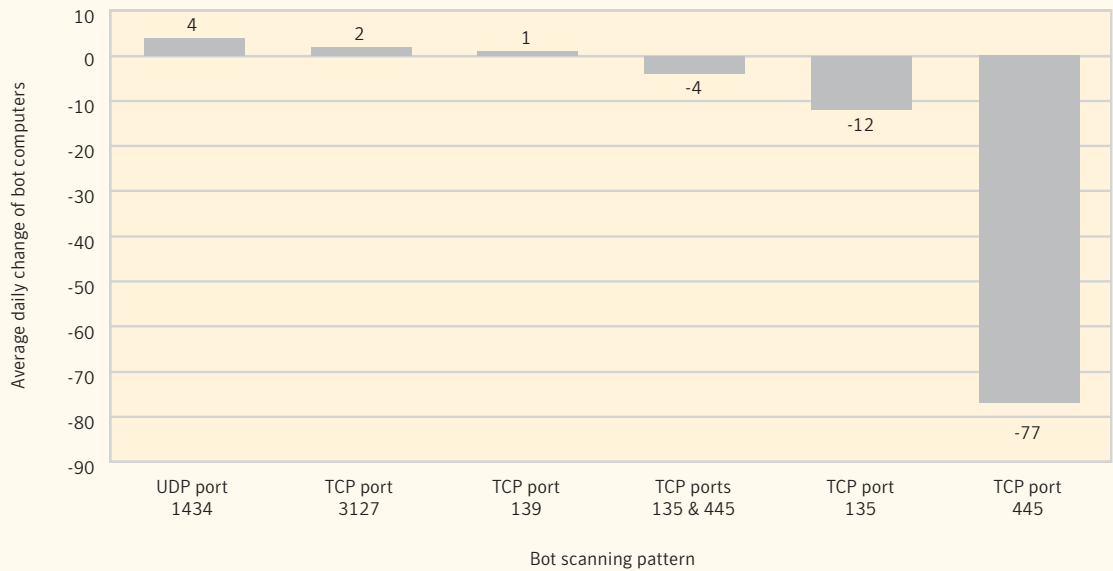


Figure 8. Changes in bot network scanning of ports
 Source: Symantec Corporation

Denial of service attacks

Denial of service (DoS) attacks are a significant threat to organizations that depend on the Internet, particularly those that depend on Internet connectivity to generate a significant portion of their revenue. The term denial of service is a generic description and simply defines an event that blocks or slows legitimate access to a service provided by a computer.

As was noted previously in the “Top Internet Attacks” discussion, the second most common attack was the Generic TCP SYN Flood Denial of Service Attack. This type of attack relies on overwhelming an Internet service with connection attempts without completing the connection negotiation.²⁶ Often, this type of attack is performed by spoofing the source IP address, which results in unsolicited traffic called backscatter being sent to other systems on the Internet. Figure 9 shows DoS attack targets as determined by analyzing the backscatter of attacks.

²⁶ The TCP protocol requires a three-way exchange before any data can be sent. The SYN packet is the initiation of this exchange. Once a SYN is received, the destination system sends a SYN-ACK packet back and waits to receive an ACK, which completes the three-way exchange. By spoofing the source of the initial SYN packet, an attack can cause the responding system to sit waiting indefinitely for the ACK after sending out the SYN-ACK. This enables the attacker to keep a finite number of sessions open, thereby creating the conditions for a DoS attack.

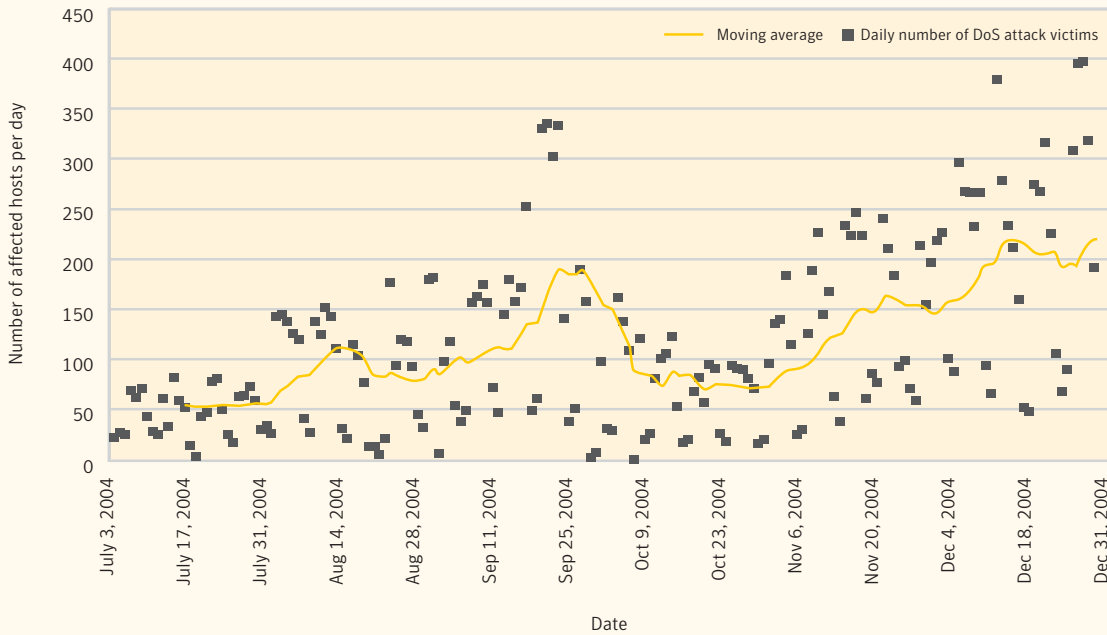


Figure 9. Number of DoS victims per day
 Source: Symantec Corporation

DoS attacks depending on spoofed source traffic increased notably in early August, 2004. This coincided with the release of Windows XP Service Pack 2, which has been previously noted for its possible impact on the number of active computers involved in coordinated bot network scanning. Symantec believes there may be a correlation in the drop in active bot-infected computers and the rise in the practice of attacking Internet servers with spoofed hosts.

Symantec believes that there is good reason to believe that as attackers are losing the ability to perform DoS attacks that rely on large numbers of bot computers, they are reverting back to older methods, including spoofing the source address as part of a SYN flood attack. The use of spoofed source addresses can allow an attacker to overwhelm a victim by using fewer attacking computers, an important consideration when the supply of computers that can be used for an attack is dwindling.

Defending against spoofed-source DoS attacks is difficult, as the spoofing of the addresses makes filtering based on the IP address much more complicated. Some systems have configuration options to make the system less prone to resource exhaustion.²⁷ DoS victims will frequently need to engage their upstream Internet service provider to help filter the traffic.

²⁷ Computers have finite resources that are related to the amount of memory, CPU power and network bandwidth available. Other limits can be imposed by the operating system. When one of these limits is reached, or the memory, CPU or network bandwidth is saturated, it is referred to as resource exhaustion.

Top countries by bot-infected computers

For this edition of the *Internet Security Threat Report*, Symantec has assessed the distribution of bot-infected computers across the Internet. In order to do this, Symantec calculated the number of computers worldwide that are known to be infected with bots, and assessed 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 users in a given region.

During the last six months of 2004, the highest percentage of identified worldwide bots was located in the United Kingdom, with 25.2% (table 3). Bot networks, as observed by Symantec, tend to be dominated by computers on large Internet service providers, often providing high-speed broadband Internet connectivity. The rapid growth in broadband that is occurring in the United Kingdom is likely one factor to contributing to the bot network penetration.²⁸ Symantec believes that new broadband customers may not be aware of the additional security precautions that need to be taken when using an always-on high-speed Internet connection. Furthermore, the addition of many new customers, with the corresponding increase in infrastructure and support costs may slow Internet service providers' responses to reports of network abuse and infection.

Rank	Country	Percent of bot infected computers
1	United Kingdom	25.2%
2	United States	24.6%
3	China	7.8%
4	Canada	4.9%
5	Spain	3.8%
6	France	3.6%
7	Germany	3.5%
8	Taiwan	3.1%
9	South Korea	3.0%
10	Japan	2.6%

Table 3. Top countries by percentage of bot-infected computers

Source: Symantec Corporation

The United States accounts for 24.6% of the bot-infected computers worldwide. The large number of Internet users and high-speed broadband users in the United States—over 30 million users, the largest of any country—helps to explain the prominence of the United States in this metric.²⁹

China accounts for 7.8% of the bot-infected computers. China like many countries, is experiencing rapid growth in the population connecting to the Internet by high-speed broadband.³⁰ This growth has not pushed China into the prominent positions held by the United States and United Kingdom, but has positioned it in advance of regional neighbors, such as South Korea and Japan. Symantec believes that the proportion of bot-infected computers will continue to rise in China until the rate of broadband growth slows.

²⁸ <http://news.bbc.co.uk/1/hi/technology/4065047.stm>

²⁹ <http://www.point-topic.com/content/dslanalysis/Q304+BB+analysis+041215.htm> (note that access to this site requires registration.)

³⁰ <http://news.bbc.co.uk/2/hi/technology/3699820.stm>

Top originating countries

This section will discuss the top countries of attack origin (table 4). This metric only discusses the location of the computer from which the attack originated and not the actual location of the attacker. While, it is simple to trace an attack back to the last computer from which the attack 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.

Jul-Dec 2004 rank	Jan-Jun 2004 rank	Country	Jul-Dec 2004 percent of events	Jan-Jun 2004 percent of events
1	1	United States	30%	37%
2	2	China	8%	6%
3	5	Germany	8%	5%
4	9	South Korea	4%	3%
5	3	Canada	4%	6%
6	6	Great Britain	4%	4%
7	7	France	3%	4%
8	NR	Japan	3%	NA
9	8	Spain	3%	3%
10	NR	Italy	2%	NA

Table 4. Top originating countries

Source: Symantec Corporation

The United States continues to be the top source country of attacks; however, the percentage of attacks originating in the United States declined for the third consecutive six-month reporting period. During the second half of 2004, 30% of attacks originated in the United States, down from 37% in the first half of the year and 58% in the second half of 2003. As other countries continue to add to their Internet infrastructure, particularly their high-speed connections, attacks originating from those countries can be expected to rise, and the percentage of attacks originating in the United States to fall accordingly.

China was the second-ranked country of attack origin for the first six months of 2004, the same position that it occupied in the first half of the year. The percentage of total worldwide events originating in China increased slightly from 6% in the first six months of 2004 to 8% in the second. Germany has moved up to third position in the countries of attack origin for the second half of 2004. 8% of Internet attack activity occurred there, compared to 5% in the first half of the year, when it was the fifth-ranked source country.

Top originating countries by Internet capita

The measurement of attack rates according to the country of origin does not take into account the number of Internet users in each country. For example, as the United States has one of the highest populations of Internet users, it is not surprising that it occupies a significant position in overall attack rates. This section will discuss the top originating countries according to the number of attacks launched from that country per 10,000 Internet users (table 5). This discussion includes all countries with over 100,000 Internet users.³¹

Rank	Country	ISTR VI rank
1	Panama	NR
2	Hong Kong SAR	NR
3	Macau	2
4	Qatar	NR
5	Israel	3
6	Turkey	7
7	Bosnia and Herzegovina	NR
8	Canada	9
9	Luxembourg	NR
10	Spain	8

Table 5. Top source countries per Internet capita

Source: Symantec Corporation

Except for Canada and Spain, none of the top countries of attack per Internet capita are present in the top countries of attack origin for this period. Additionally, five of the top ten were not present on the list for the previous six-month reporting period. This indicates significant changes in attack rates when adjusted for Internet users.

When examining the top originating countries on a per-capita basis, one pattern seems to emerge. Although, there are some countries that remain relatively static in their attack-per-10,000-user ratio—namely Turkey, Israel, Spain and Canada—other countries are far more variable. One factor leading to this variability may be the rapid increase of Internet use in these countries. One consequence of this is that the end users may not have been adequately educated about best security practices. As a result, computers in countries experiencing rapid Internet growth may be less rigorously secured than in countries with experienced end users.

Another consequence of this rapid rise in Internet usage is that it challenges the reporting of that Internet use. Until the rate of Internet adoption slows in these countries, it is likely that considerable variability in the ranking from year to year will be found. Countries with smaller base populations are likely to experience the more significant changes, some doubling or tripling in Internet usage and, therefore, Internet attack activity, in a year.

³¹ The data on number of Internet users in each country is gathered from the *CIA World Factbook 2004* (<http://www.cia.gov/cia/publications/factbook/>).

Many of the new entrants to the top ten of per-capita attack rates are countries with an Internet user base between 100,000 and 200,000 Internet users. These countries would likely not have had the minimum 100,000 Internet users required for consideration in previous reporting periods. This indicates that each of these countries is experiencing significant growth, in many cases doubling or tripling the reported Internet population. The growth of the Internet user base in these countries (including Panama, Qatar, Bosnia, and Herzegovina) is reflected in their positioning as a top per-capita attack source.

This metric is also affected by the lag between the actual growth in Internet usage and the documentation of that growth in reference sources. One example of this was the presence in the last reporting period of Latvia. The cited Internet user population of Latvia increased from 312,000 in the 2003 version to 936,000 in the *CIA World Factbook 2004*. While the attack activity would have been affected by the rapid increase in Internet usage, the numbers would not have been reflected in the sources on which this analysis is based. As a result, the ratio would have been skewed. The displacement of Latvia from the top-per-capita attacking country metric is more likely due to the fact that the numbers of documented Internet users has increased (to reflect the rapid growth of Internet usage) while the number of attacks has remained relatively steady. As a result, the ratio of attack activity to known Internet users has dropped.

Targeted attack activity by industry

Attackers choose their targets for a number of reasons. In some cases, an attack may be targeted against a single company or a group of companies from a single industry. In other cases, attacks may simply be opportunistic: the attacker may be interested in compromising a system regardless of its owner. This section will discuss attackers who target a specific industry (figure 10). A targeted attacker is defined as an attacking IP address that has attacked at least three sensors in a given industry to the exclusion of all other industries in the sample period.

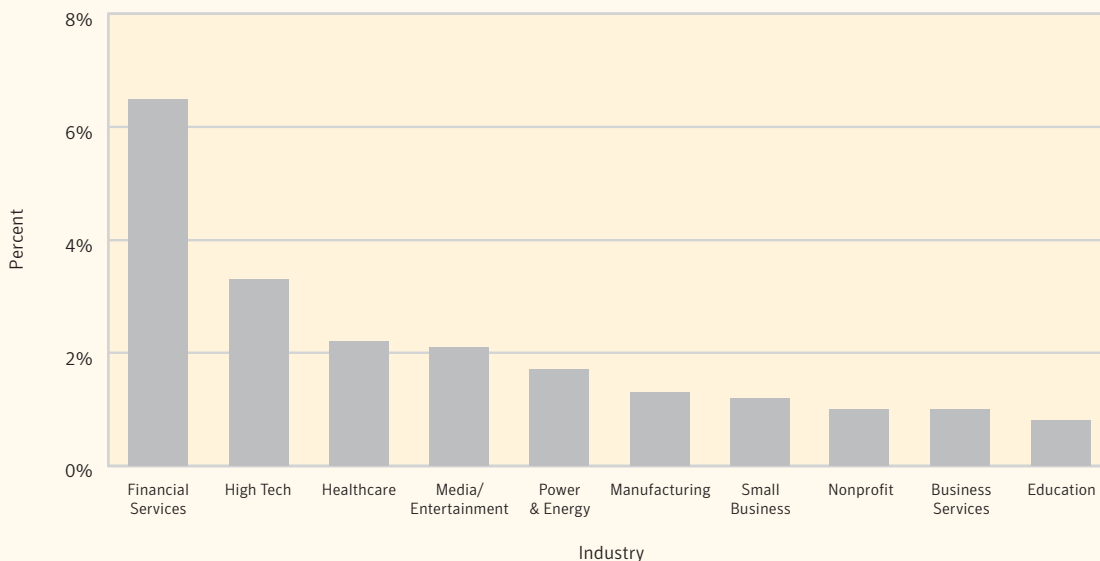


Figure 10. Targeted attacks by industry
Source: Symantec Corporation

Symantec Internet Security Threat Report

Between July 1 and December 31, 2004, the financial services industry was the most frequently targeted industry. It experienced an increase from 4% to over 6% in targeted attacks. This increase continues the pattern seen during the previous six-month period, during which the targeted attacker rate rose from 1% to 4%. This increase was the most significant increase in targeted attack rates for any industry. Financial services is generally regarded to be an attractive target for attackers hoping to profit from the attack, and the continued increase in targeted attacker rates indicates that attackers are probing more financial organizations for weaknesses.

The high tech industry was the second most frequently targeted industry between July 1 and December 31, 2004. It was the fourth most frequently targeted in the previous period. However, while the high tech industry rose in the rankings, the percentage of attacks targeting high tech organizations actually declined, from slightly under 4% in the first half of 2004 to just over 3% in the second half. In the second half of 2003, the targeted attacker rate was slightly under 5%. It is possible that organizations in the high tech industry are more likely to have robust security systems in place; therefore, the attractiveness of those organizations to targeted attackers is waning, as targeting other industries may lead to greater rewards.

As with high tech, the healthcare industry also rose in the ranking from ninth place in the first half of 2004 to third place in the second half of the year. Despite this significant jump, health care organizations experienced a marginal increase in targeted attack rates, with the percentage remaining very close to 2%.

The most significant decline from the first half of 2004 occurred in the small business industry. The second most targeted industry in the first six months of 2004, it was the seventh most targeted industry in the second half of the year, with just over 1% of targeted attackers.

In the previous version of the *Internet Security Threat Report*, Symantec posited that the high ranking of small businesses was related to the way small businesses access the Internet. Small organizations are more likely to use DSL or cable for Internet access and comparatively smaller address spaces are allocated to each company. As a result, Symantec suggested that a concerted attack targeting a range of IP addresses belonging to a DSL or cable Internet provider would be noted as a targeted attack, despite the opportunistic nature of that attack.

Symantec still maintains that this clustering will amplify any intense scanning directed at these Internet segments, because of the amplification of certain classes of network scanning. It is likely that a spate of targeted scanning on these ranges can upwardly skew the targeted attack numbers in some sample periods, leading to tremendous variability in this industry.

The e-commerce industry, the top targeted industry in the first half of 2004 is notably absent from the top attacked industries in the current period. During this period, the number of sensors required to ensure statistical validity was not maintained. As a result, Symantec has excluded this industry from this discussion.

It is possible that changes in industry classifications, specifically relating to a distinction between e-commerce and so-called traditional bricks-and-mortar businesses is causing this decline in contributing sensor base of the e-commerce industry. As traditional companies continue to expand into the online world with e-offerings, the distinction between an e-commerce company and a traditional company may not be an appropriate separation.

Severe event ratio by industry

This metric compares industry segments based on the ratio of severe events originating from external attackers that are detected by sensors based in each industry. Symantec determines severity of an attack based on the characteristics of the attack, the defensive controls of the client, the value of the assets at risk, and the success of the attack. Severe attacks pose the greatest threat to organizations. The number of severe events that an industry experiences may indicate the risk to which it is exposed. This metric will discuss the industries that have received the highest number of severe events per 10,000 events (figure 11).

The financial services sector experienced the highest number of severe events per 10,000 regular events. This sector, with its high profile and involvement in financial transactions, is an attractive target for attackers. When considering the high placement of this industry in both the “severe event ratio” and the “targeted attacker” metrics, it is clear that organizations involved in this industry must take appropriate steps to identify and mitigate risks of attack.

Other industries are also heavily affected by a high severe event rate, including manufacturing, transportation, and the media/entertainment industries. The high severe event rate of these industries compared to other core infrastructure industries, such as power and energy or healthcare, may indicate that extra security measures have been deployed in the power and energy and healthcare industries to better mitigate against successful attacks.

The presence of the media and entertainment industry in fourth place may be noteworthy, particularly in light of successful instances of media manipulation by Internet attackers. Because of their high visibility to the public, these sites are often targeted by “hacktivists”, who may deface the sites in order to convey their message.

Adrian Lamo performed some of the most high-profile examples of Web site manipulation. In one case, he manipulated a story on the Yahoo news site³² in August 2001, subtly changing the facts reported. Lamo has since been charged and has pleaded guilty for his behavior.³³ The possibility of high-profile manipulation of events reported by news organizations should not be discounted given the high visibility of Web sites associated with them.

³² <http://www.securityfocus.com/news/254>
³³ <http://www.securityfocus.com/news/9520>

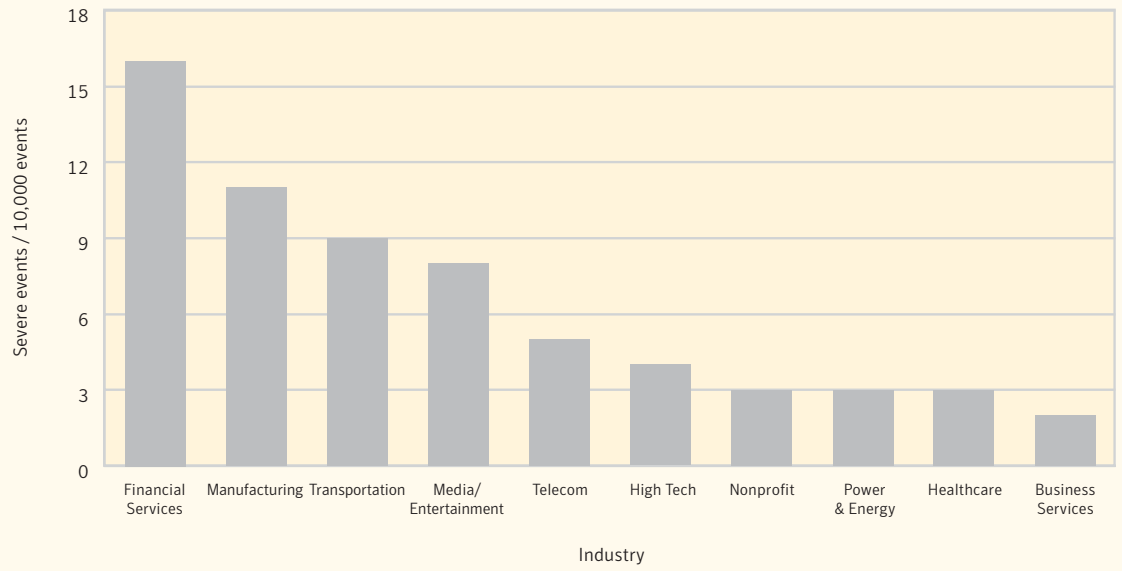


Figure 11. Severe event ratio by industry
Source: Symantec Corporation

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 by 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 exploited actively, either by malicious users or automated malicious code, or triggered passively during system operation. New vulnerabilities are discovered and disclosed regularly by a sizeable community of end users, researchers, hackers, and security vendors. The 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 discussion to the issuance of a patch or other remediation measure. This section of the Symantec *Internet Security Threat Report* will discuss vulnerabilities that have been disclosed between July 1 and December 31, 2004. It will compare them with those disclosed in the two previous six-month periods and discuss how current vulnerability trends may affect potential future threats. 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.³⁴

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

- Total number of vulnerabilities disclosed
- Severity of vulnerabilities
- Ease of exploitation
- Exploit development time
- Web application vulnerabilities
- Web browser vulnerabilities
- Web browser vulnerabilities by severity

Symantec operates one of the most popular forums for the disclosure and discussion of vulnerabilities on the Internet. The BugTraq mailing list³⁵ has approximately 50,000 individual subscribers, who receive, discuss, and contribute vulnerability research on a daily basis. Symantec also maintains one of the world's most comprehensive databases of security vulnerabilities, currently consisting of over 11,000 vulnerabilities (spanning more than a decade) affecting more than 20,000 technologies from over 2,000 vendors. This discussion of vulnerability trends is based on a thorough analysis of that data.

Total number of vulnerabilities disclosed

Symantec documented 1,403 new vulnerabilities during the six-month period between July 1 and December 31, 2004 (figure 12). This represents growth of 13% in total volume over the 1,237 vulnerabilities disclosed in the first six months of 2004. It is also a 19% increase over the 1,180 vulnerabilities disclosed between July 1 and December 31, 2003.

The second half of 2004 was the second consecutive period during which an increase in total volume was observed. As figure 12 shows, disclosure activity rose continually between the first half of 2001 and the first half of 2003. After a drop-off in disclosure activity in the second half of 2003, it has risen again for the past two six-month periods and is now near the peak established in the middle of 2003.

³⁴ Please note that all numbers presented in this discussion have been rounded off to the nearest whole number. As a result, some cumulative percentages may exceed 100%.
³⁵ The BugTraq mailing list is hosted by SecurityFocus (<http://www.securityfocus.com>). Archives are available at <http://www.securityfocus.com/archive/1>

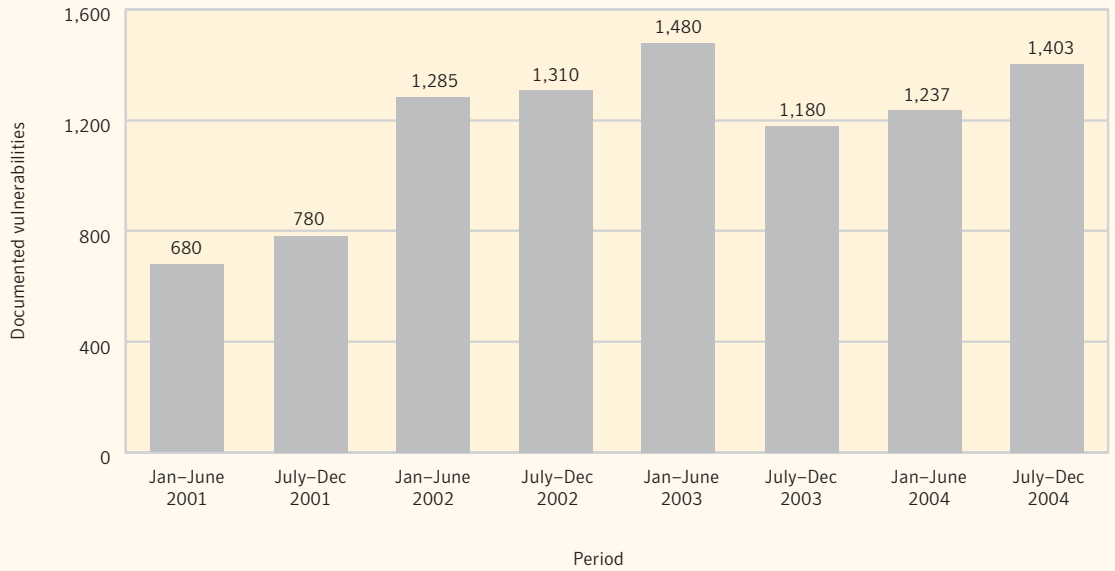


Figure 12. Total volume of vulnerabilities documented by Symantec, 2001-04
Source: Symantec Corporation

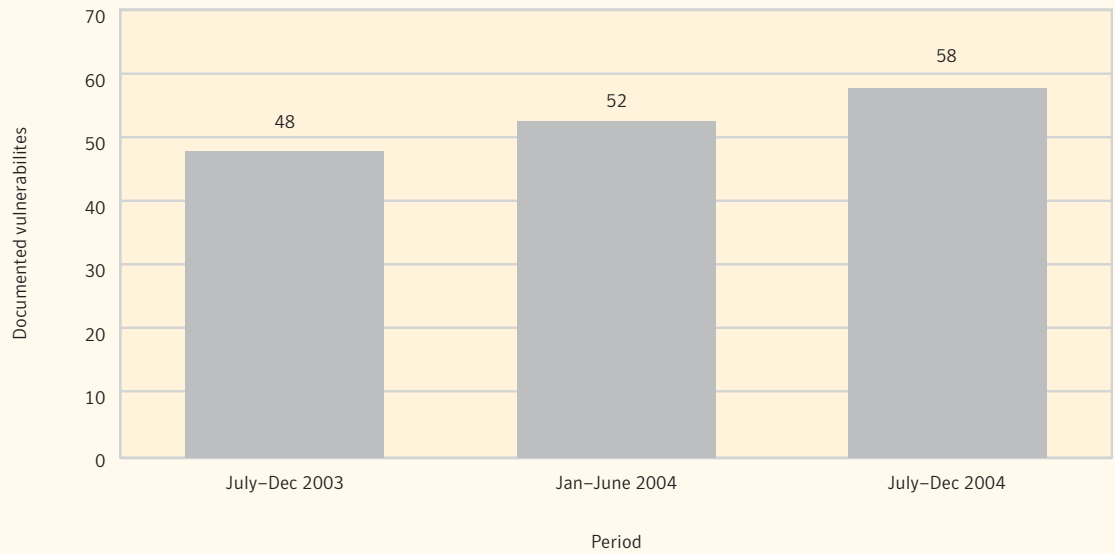


Figure 13. Vulnerabilities per week over the past 18 months
Source: Symantec Corporation

The increase in vulnerability disclosure over the past two reporting periods is also apparent when assessed on a weekly basis. Over the second half of 2004, an average of 58 new vulnerabilities per week were disclosed, an increase from 52 per week in the previous six-month period, or nearly one additional vulnerability a day (figure 13). Between July 1 and December 31, 2003, 48 new vulnerabilities were published per week. This means that security administrators must currently protect against ten additional vulnerabilities per week, on average, than one year ago.

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 on the confidentiality, integrity, and or availability of the affected system. For the purposes of the *Internet Security Threat Report*, each vulnerability is categorized as one of three severity levels. These levels are:

Low severity—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.

Moderate severity—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.

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.

For the period of July 1 through December 31, 2004, 696 of the vulnerabilities documented by Symantec, or 50% of the total volume, were rated high severity (figure 14). This is a 4% increase over the first six months of 2004, when 46% of all vulnerabilities were rated high severity. The number of high-severity vulnerabilities has increased by 6% over the same period one year ago.

Of the vulnerabilities that Symantec documented during the last six months of 2004, 667, or 48% of the total volume, were considered moderately severe. This is a small decrease from the 50% rated as moderately severe in the first half of the year. It is lower still than the 54% rated as moderately severe between July 1 and December 31, 2003.

In the last six months of 2004, Symantec classified only 40 disclosed vulnerabilities as low severity, amounting to 3% of the total volume. This is a smaller proportion than the previous reporting period during which 4% were rated low severity. However, it is a slight increase over the number of low-severity vulnerabilities noted during the same period a year ago, 2%.

The current reporting period continued an increase in moderate and high-severity vulnerabilities that was observed in the two previous six-month periods. In the last six months of 2004, 97% of vulnerabilities were rated as moderate or high severity. This is up from 95% in the previous period.

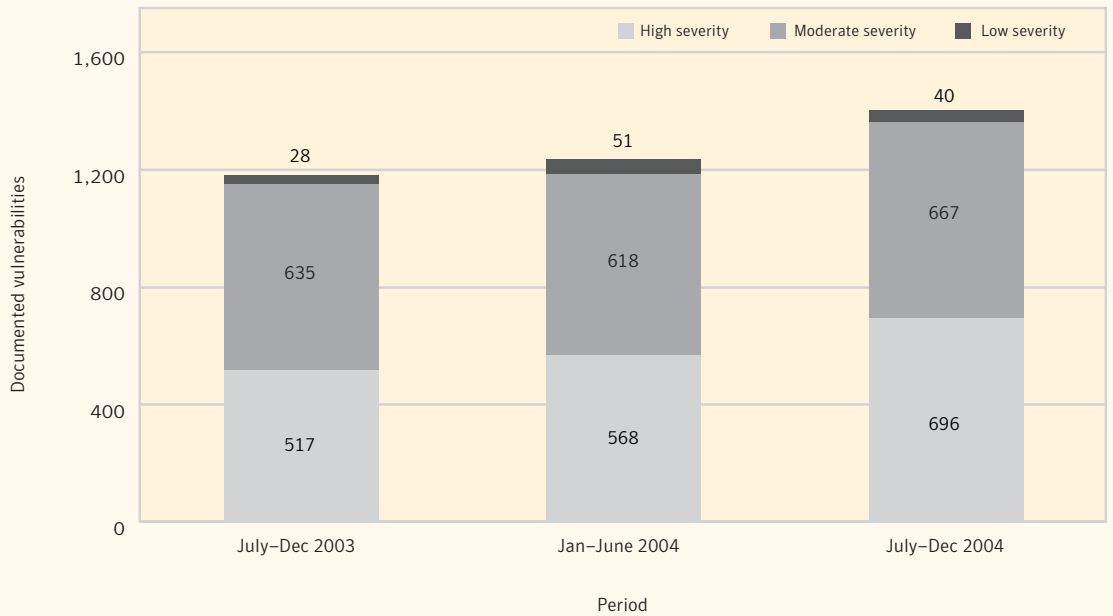


Figure 14. Severity breakdown over the past 18 months
 Source: Symantec Corporation

The increasing proportion of higher severity vulnerabilities is likely due to two factors. First, researchers are more interested in finding and reporting high-severity vulnerabilities. The severity rating of a vulnerability reflects, among other things, the potential impact that an exploit may have on a compromised system. Researchers are not likely to expend the time and effort involved in researching and exploiting vulnerabilities unless the “reward” is worth it. Furthermore, Symantec believes it is reasonable to conclude that there is a correlation between the potential impact of a vulnerability on the system and the recognition of the researcher among peers in the research community.

The second reason for the increase in more severe vulnerabilities is that over 80% of vulnerabilities documented this period are remotely exploitable. Nearly 50% affect technologies associated with the World Wide Web. Most modern information technology systems either require or support network access, which is increasingly accessed through Web interfaces or technologies associated with the World Wide Web. The changing composition of the vulnerability database reflects these developments. Because vulnerabilities that can be exploited by attackers across a network are, by definition, at least moderately severe, the increase in remotely exploitable vulnerabilities has resulted in an increase in moderately to highly severe classifications.

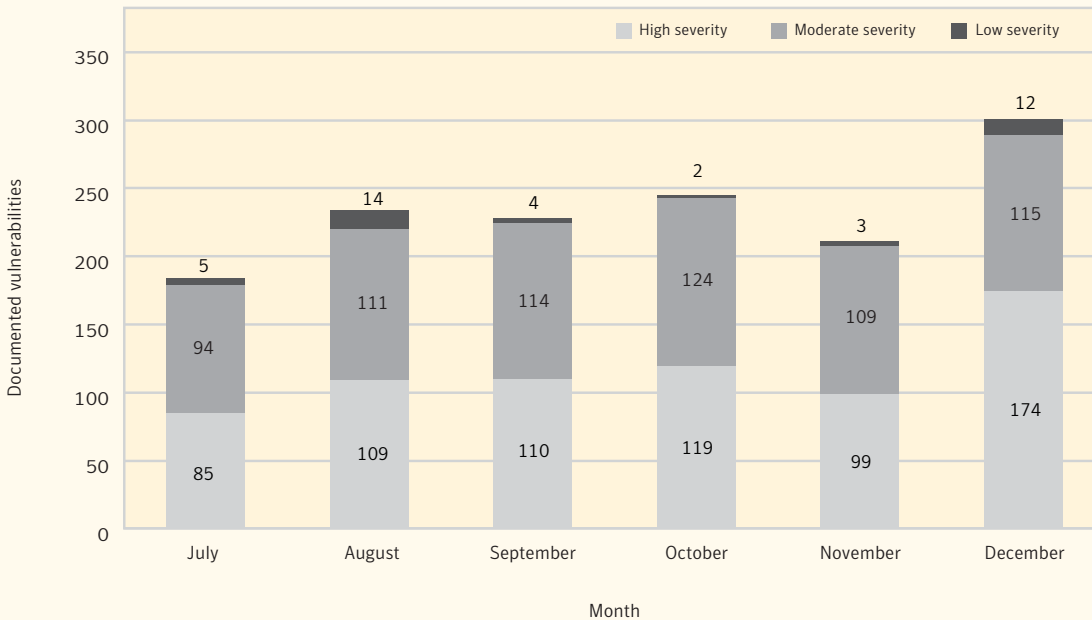


Figure 15. Monthly volume, by severity
 Source: Symantec Corporation

Ease of exploitation

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

Generally speaking, “easily exploitable” vulnerabilities do not require sophisticated skills or knowledge to exploit. Anyone with sufficient general technical knowledge or with publicly available tools can exploit them. Examples of these are 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 exploit. 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 (assuming that there is none circulating in the underground). This significantly raises the level of knowledge, expertise, and effort required for a successful attack, thus lowering the probability of such an attack. It should be pointed out that while no tools may be publicly available, private exploits might exist. However, without a public exploit, these vulnerabilities won’t likely be widely exploited.

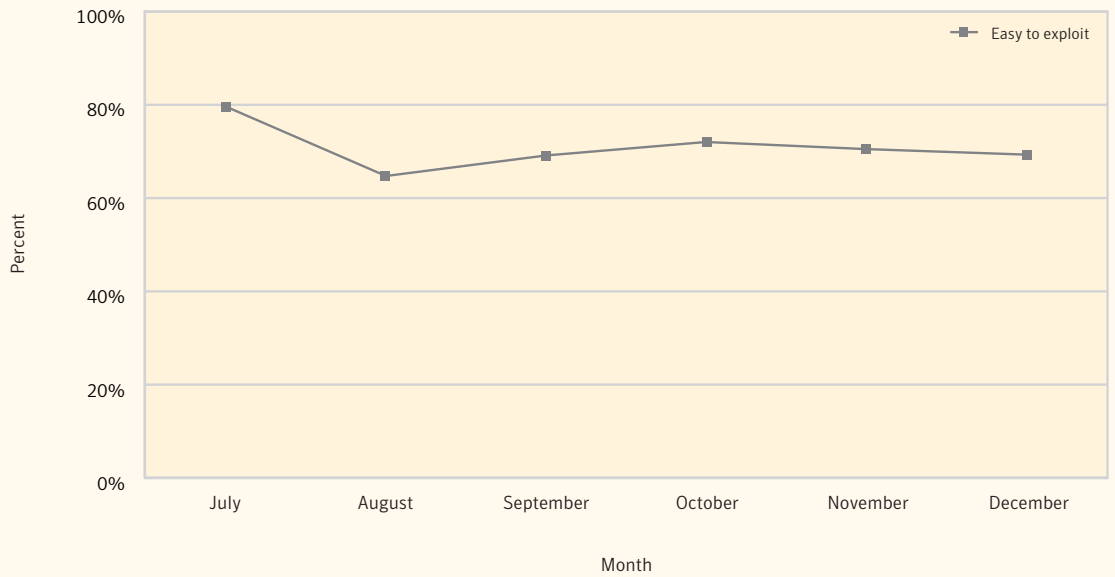


Figure 16. Vulnerabilities rated easy to exploit
 Source: Symantec Corporation

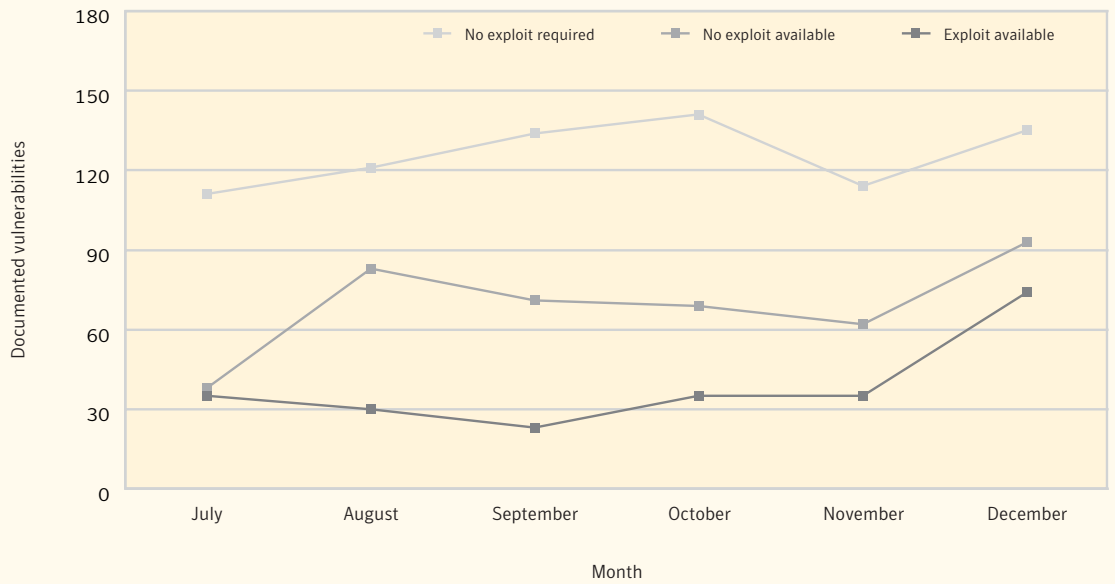


Figure 17. Ease of exploit breakdown
 Source: Symantec Corporation

Between July 1 and December 31, 2004, Symantec classified 987 vulnerabilities as easily exploitable (figure 16). This means that 70% of all vulnerabilities disclosed during this period require no exploit code or had some type of exploit code available. 69% of the vulnerabilities documented in the first half of 2004 were classified easy to exploit, as were 72% of the total in the second half of 2003. The proportion of easily exploitable vulnerabilities in this period remains virtually unchanged from what was noted in the two previous periods. A possible explanation for this is that the same researchers are finding the same types of vulnerabilities. There are many researchers who post to mailing lists such as BugTraq who only ever find easy-to-exploit Web application vulnerabilities.

The majority of the vulnerabilities classified as easy to exploit—53% between July 1 and December 31, 2004—do not require any exploit code at all. This is a small increase from the 52% noted in the previous period and 5% higher than in the same period one year ago. The apparent decline in easy-to-exploit vulnerabilities during the month of July, which is evident in figure 17, is due to the low volume of vulnerabilities during that month.

The vulnerabilities classified as easy to exploit are nearly all input validation errors in Web-based applications. This includes cross-site scripting, HTML injection, and SQL injection. The proportion of vulnerabilities for which no exploit is required has been steadily increasing with the proportion of Web application vulnerabilities. (For more detail, please see the discussion on Web application vulnerabilities below.) This reflects the fact that many applications are now being delivered to users online via the Web. These remotely accessible applications are frequently susceptible to easy-to-find vulnerabilities.

Vulnerabilities with exploit code

Over the last six months of 2004, Symantec documented 201 vulnerabilities for which associated exploit code was widely available (figure 18). Because of the availability of exploit code, these vulnerabilities are considered easy to exploit. The percentage of the total volume of vulnerabilities with exploit code, 14%, is slightly higher than what was observed between January 1 and June 30, 2004 (13%). The percentage seen during the same period one year ago was 18%, which is substantially higher. The decrease in the proportion of vulnerabilities with exploit code is likely attributed to the fact that a larger portion of vulnerabilities disclosed over the second half of 2004 affect Web applications, as these vulnerabilities typically do not require exploit code.

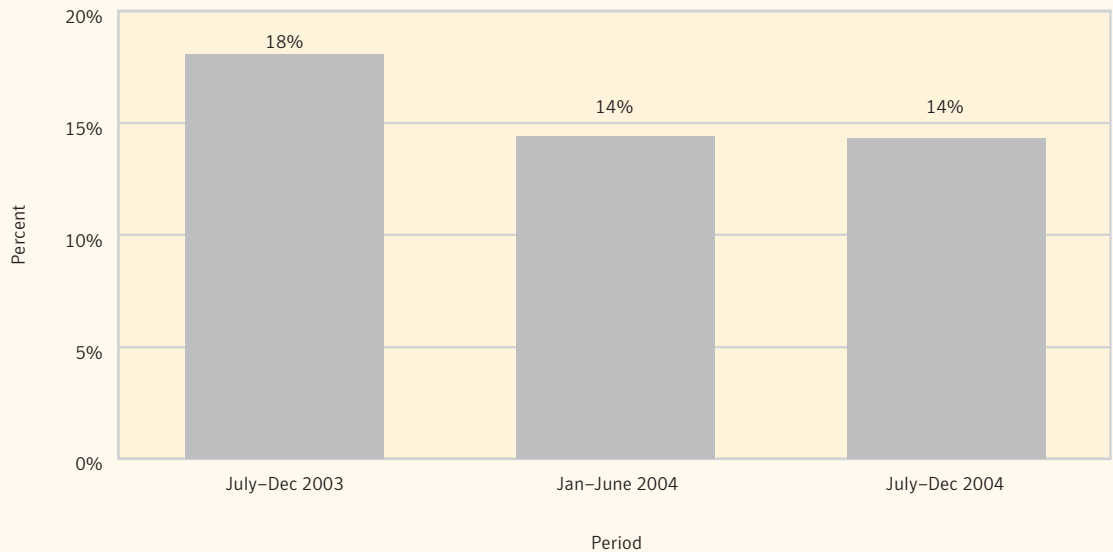


Figure 18. Percentage of vulnerabilities with associated exploit code over 18 months

Source: Symantec Corporation

Of the 202 vulnerabilities documented in this period with associated exploit code, 76% were classified as high-severity threats (figure 19). This is a substantial increase over the previous period, during which 64% of documented vulnerabilities were considered highly severe.

It is not surprising that the majority of vulnerabilities with associated exploit code are classified as high severity; however, it is noteworthy that this proportion appears to be increasing. This reflects a desire on the part of exploit authors to expend the effort required to create exploit code only when the potential impact is the greatest. This is a worrisome trend, as the availability of exploit code shortens the window that administrators have to patch their systems before the risk of compromise rises significantly. (For a more in-depth discussion of the disclosure-to-exploit window, please see the “Exploit development time” discussion, which follows.)

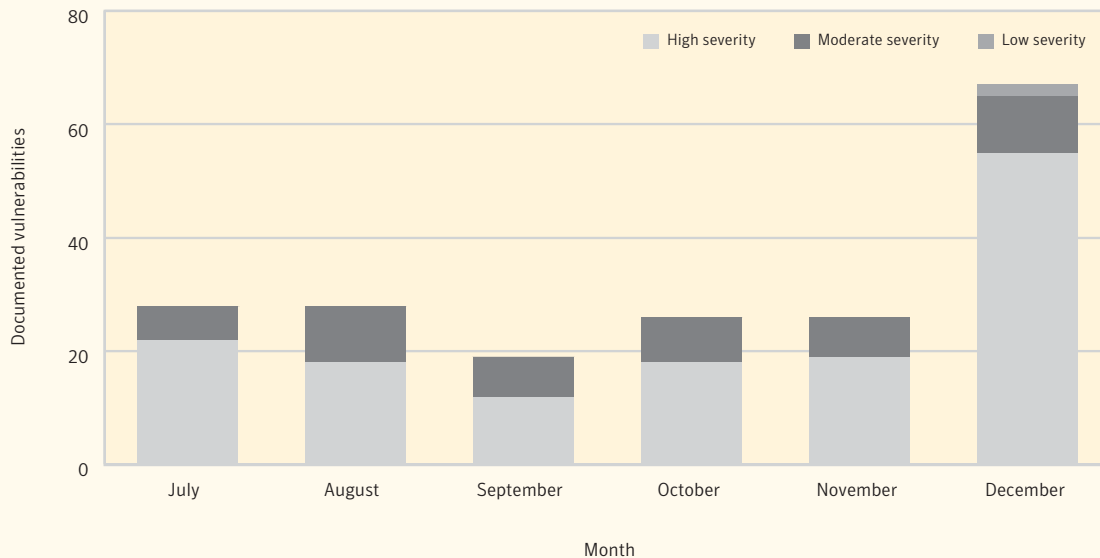


Figure 19. Monthly breakdown of vulnerabilities with associated exploit code, by severity

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 more hosts are vulnerable to attack, until patches become available.

Between July 1 and December 31, 2004, the average time between the disclosure of a vulnerability and the publication of its associated exploit was 6.4 days (figure 20). This is an increase of just over half a day over the previous six months. Between January and June 2004, the time to exploit was 5.8 days after the announcement of the associated vulnerability. Compared to the previous reporting, the average exploit development time increased by less than a day.

Continuing from the first half of 2004, the average amount of time between vulnerability publication and the appearance of a third-party functional exploit remains less than one week. This 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 an 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, and relevant mitigation or patching information, as well as an understanding of the potential risk of the vulnerability.

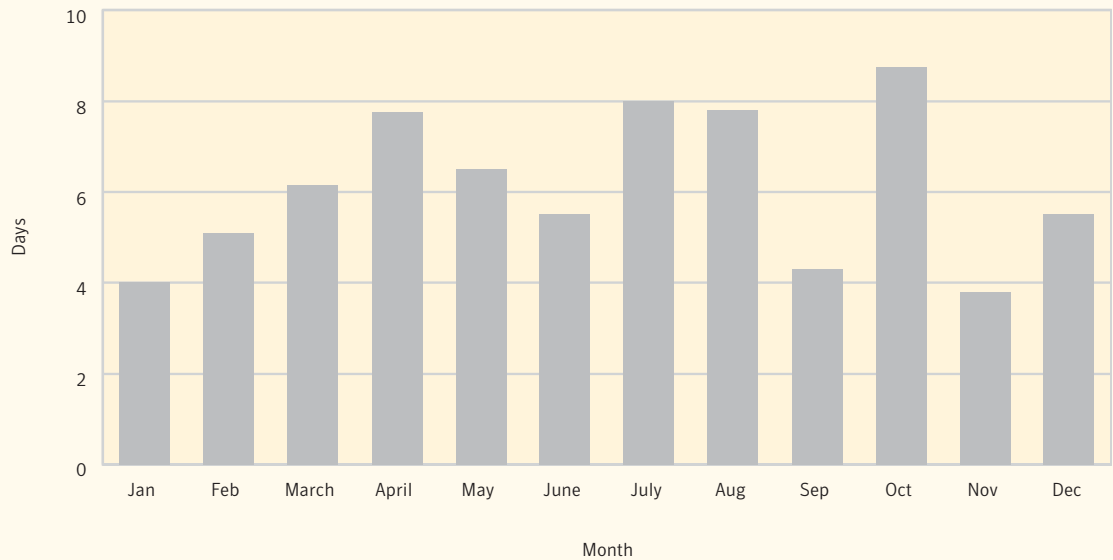


Figure 20. Average number of days for exploit development, by month, in 2004

Source: Symantec Corporation

Web application vulnerabilities

Web applications are technologies that rely on a browser for their user interface. They are often hosted on Web servers. Vulnerabilities in Web applications are typically exploited by attacks such as cross-site scripting, SQL injection, and HTML injection, and can allow an attacker to access confidential information from databases without having to compromise any servers.

Between July 1 and December 31, 2004, Symantec catalogued 670 vulnerabilities affecting Web applications, nearly half (48%) of the total vulnerabilities disclosed during this reporting period (figure 21). This is substantially higher than the 39% documented in the first six months of 2004 and the 32% documented between July 1 and December 31, 2003.

As noted in the “ease of exploitation” discussion, vulnerabilities targeting Web applications are often classified as easily exploitable, and their increase has contributed significantly to the high number of easily exploitable vulnerabilities. This is likely due to the increasing use of the World Wide Web as a tool for building and delivering applications. As Web applications are becoming more prevalent, vulnerabilities associated with them are becoming a greater concern. As a case in point, the first worm based on a Web application, Perl.Santy,³⁶ which targeted the popular phpBB application, was detected in December 2004. This highlights the need for security personnel to keep abreast of new vulnerabilities, to deploy only Web applications that are necessary for organizational purposes, and to audit all deployed Web applications for security.

³⁶ <http://securityresponse.symantec.com/avcenter/venc/data/perl.santy.html>
For an in-depth discussion of the Santy worm, please see the “Malicious Code Trends” section of this report.

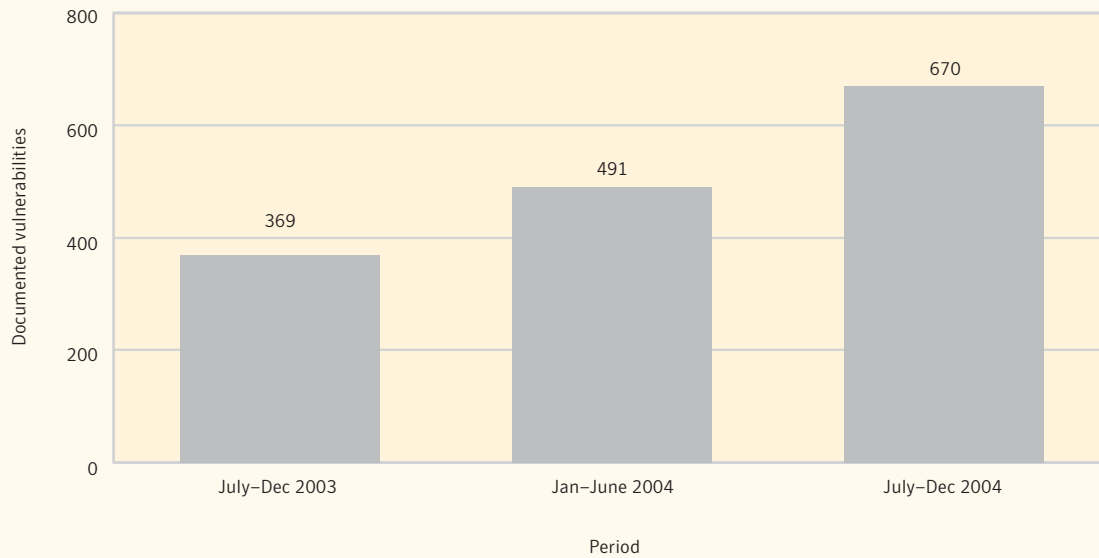


Figure 21. The increase in Web application vulnerabilities over 18 months
Source: Symantec Corporation

Web browser vulnerabilities

The Web browser is a critical and ubiquitous application that has increasingly made security headlines over the past few years. Traditionally, the focus of security strategies has been on the network perimeter: servers, firewalls, and other assets with outward-facing exposure. However, a notable shift has occurred, with security of client-side systems, primarily end-user desktop hosts, becoming increasingly important. The Symantec *Internet Security Threat Report* has anticipated and followed this trend over the past several reporting periods.

Almost exclusively, vulnerabilities affecting Microsoft Internet Explorer, one of the most widely used client-side applications, have brought client-side security to the forefront. Criticism of Microsoft's Internet Explorer in response to many high profile vulnerabilities led to the popular promotion of other browsers—particularly Mozilla, Firefox, and Opera—as safe alternatives.

For the first time, the Symantec *Internet Security Threat Report* is including a comparison of vulnerability data for different browsers, specifically Microsoft Internet Explorer, Mozilla, Mozilla Firefox, Opera, and Apple's Safari. The methodology section for this analysis, included in "Appendix C" of this report, includes some important caveats that should be noted before any conclusions are drawn from this discussion. In addition to those points, the following should be kept in mind while considering this data:

- 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 involved in identifying individual vulnerabilities in often-complex browser exploits.

- Not every vulnerability discovered is exploited. As of this writing, there has been no widespread exploitation of any browser except Microsoft Internet Explorer. This is something that Symantec expects to change as alternative browsers become more widely deployed.

Between July 1 and December 31, 2004, Symantec documented 13 vulnerabilities affecting Microsoft Internet Explorer (figure 22). This is sharply higher than the three vulnerabilities documented by Symantec in the first half of 2004, during which reports of all browser vulnerabilities were lower. However, it is down from the peak of 17 vulnerabilities seen in the second half of 2003. This is likely due to two factors: the effort that Microsoft has undertaken to secure Internet Explorer and patch latent vulnerabilities, and the shift of vulnerability researcher interest towards alternative browsers that are being marketed or promoted as secure.

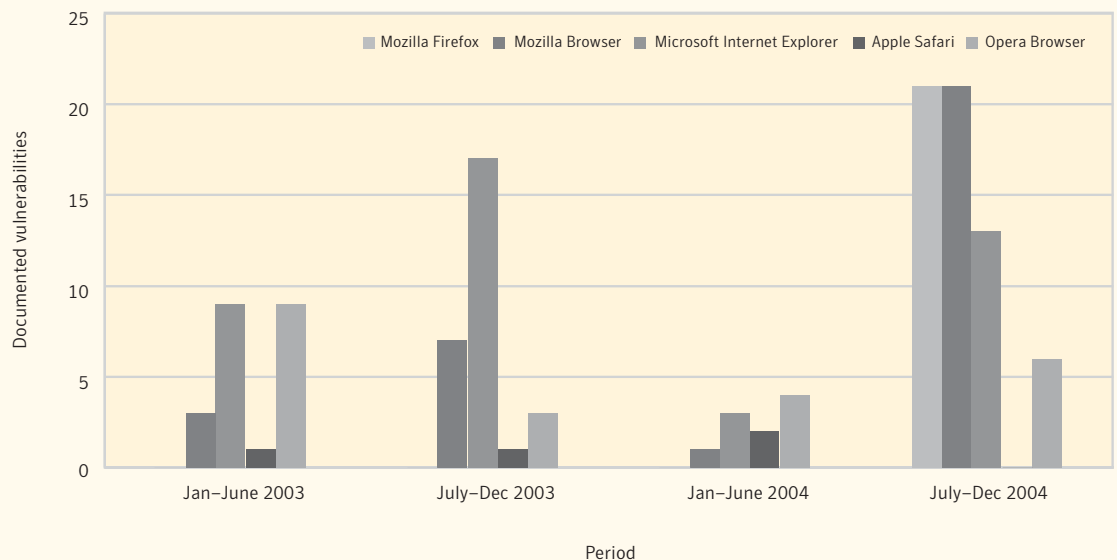


Figure 22. Vulnerabilities affecting browsers, 2003–2004
 Source: Symantec Corporation

During the last six months of 2004, 21 vulnerabilities affecting the Mozilla browsers were disclosed. This is a massive increase over the single Mozilla vulnerability documented in the previous period and the seven noted in the same reporting period one year ago. Notably, for the first time, there were more vulnerabilities disclosed for Mozilla than for Microsoft Internet Explorer. Research into the security of Mozilla browsers is directly the result of the increased popularity and deployment of the browser, which is itself a reaction to the widespread abuse of several high-profile vulnerabilities in Internet Explorer.

During the first six months of 2004, six Opera vulnerabilities were documented, an increase from the four seen in the first six months of the year. In the last six months of 2003, Symantec documented three vulnerabilities affecting Opera. This apparently steady increase over the past 18 months reflects growing researcher interest in the alternative browser, though there has been interest in the browser for some time: the largest number of Opera vulnerabilities recorded in a six-month period was in the first half of 2003

(nine vulnerabilities). Interestingly, vulnerabilities affecting Opera have been reported regularly for at least two years. The Opera browser has been popular with a niche group of dedicated users since its appearance. It is likely that continued security research comes from this base of users.

Over the last six months of 2004, there were no vendor-confirmed Safari vulnerabilities. This is somewhat surprising given the increasing popularity of Mac OS® X, which is in turn associated with the success of the iPod. In the first half of 2004, there were two vulnerabilities affecting Safari compared to a single vulnerability in the second half of 2003.

The number of Safari vulnerabilities reported so far is too low to suggest any trends. This may be due to an inability of researchers to find vulnerabilities, or it may simply be due to a lack of interest in the browser because of its recent entry into the market and subsequent limited deployment. However, Symantec believes that as the browser becomes more entrenched in the market and as more users deploy it, researchers will continue to find security vulnerabilities in Safari.

The overall decline in Internet Explorer vulnerabilities seen during 2004 is likely due to a combination of the security efforts of Microsoft and the shift of researchers' attention to the increasingly popular alternative browsers. So far, nearly all reports of vulnerabilities exploited in the wild against browsers are associated with Microsoft Internet Explorer. While there have been few, if any, credible reports of attacks against Mozilla, Mozilla Firefox, Opera, or Safari in the wild, it remains to be seen whether these browsers will live up to the expectations that many have for them.

Web browser vulnerabilities by severity

Of the 13 vulnerabilities affecting Microsoft Internet Explorer documented by Symantec between July 1 and December 31, 2004, nine were classified as high severity. The three vulnerabilities noted in the first half of the year were all classified as highly severe. In the second half of 2003, 16 out of the total of 17 were considered high severity. In all periods, the majority of vendor-confirmed vulnerabilities affecting Microsoft Internet Explorer were high severity. The average severity of vendor-confirmed vulnerabilities affecting Microsoft Internet Explorer falls just above the lower bound of the high severity classification range.

In the second half of 2004, 11 out of 21 vulnerabilities affecting the Mozilla browsers were classified as high severity. In the first half of 2004, the single Mozilla vulnerability was considered high severity. Of the seven Mozilla vulnerabilities documented in the second half of 2003, four were rated as highly severe. On average, Mozilla vulnerabilities are moderately severe; however, the average severity rating nears the upper bound of the "moderately severe" severity range.

Only one of the six Opera vulnerabilities noted in the current period was classified as highly severe. In the previous six-month period, none of the four vulnerabilities documented were high severity threats. In the second half of 2003, two of the three vulnerabilities affecting Opera that were catalogued by Symantec were classified as highly severe. The average Opera vulnerability is moderately severe.

As was stated in the previous section, there were no Safari vulnerabilities disclosed between July 1 and December 31, 2004. Furthermore, there were no high-severity vulnerabilities found in Safari in the previous six-month period. In the last six months of 2003, the lone Safari vulnerability was rated high severity. The average severity of Safari vulnerabilities (of which there are only four in the entire vulnerability database) is within the high severity range, though it is skewed by the small sample set and the presence of a single high-severity vulnerability.³⁷

³⁷ <http://www.securityfocus.com/bid/7518>

Malicious Code Trends

This section of the Symantec *Internet Security Threat Report* will analyze developments in malicious code over the second half of 2004. 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 July 1 and December 31, 2004.

This section analyzes and discusses malicious code in two ways: firstly, according to specific examples of malicious code, such as MyDoom and Netsky, and secondly, according to the category or type of malicious code in question, such as viruses and worms. In some cases, a particular family of malicious code, such as the aforementioned MyDoom and Netsky families, may have multiple variants. A variant is a new iteration of the same family that may have minor differences but is still based on the original. In this report, variants of a family are counted as separate samples due to the variations in functionality.

In past editions of the *Internet Security Threat Report*, adware and spyware reported to Symantec was included within this section. However, as these security risks continue to grow, they have been assigned a separate section for discussion. The "Malicious Code Trends" section will discuss:

- Top ten malicious code samples
- Win32 viruses and worms
- Malicious code for Linux®
- Exposure of confidential information
- Trojan horses
- Malicious code for mobile devices
- Malicious code for P2P (peer to peer), IM (instant messaging), IRC, and CIFS
- Bots
- New bot trends
- Malicious code for profit

While this discussion will include any prevention and mitigation information that might be relevant to the particular threats being discussed, Symantec recommends that certain best security practices always be followed to protect against malicious code attacks in general. In order to prevent malicious code infection, it is crucial to employ best security practices. Administrators should keep patch levels up-to-date, especially on computers that host public services and are accessible through a firewall or placed in a DMZ, such as HTTP, FTP, SMTP, and DNS servers. Email servers should be configured to only allow file types that are required for business needs. Alternatively, other means can be used to transfer files such as file servers, FTP, or SSH. Security administrators should also remind employees to never run software that has not been authorized by the organization.

End users should employ defense in-depth,³⁸ including antivirus software and a 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 known and trusted source, and the purpose of the attachment is known.

³⁸ Defense in-depth is the security approach in which each system on the network is secured to the greatest possible degree. This should include the deployment of antivirus, firewalls, and intrusion detection systems, among other security measures.

Top ten malicious code samples

As in previous volumes of the *Internet Security Threat Report*, mass-mailing worms³⁹ dominated the top malicious code reported to Symantec over the last six months of 2004. Eight of the top ten samples reported to Symantec during this period were variants of mass-mailer worms that have been seen in previous reports: Netsky,⁴⁰ Sober,⁴¹ Beagle,⁴² and MyDoom.⁴³

Mass-mailing worms have the capacity to affect a large number of users because they proliferate via email, one of the most widely used applications on the Internet. However, they have had to become more sophisticated in response to the increasing security savvy of end users. As a result, successful mass-mailers now employ additional propagation mechanisms, such as peer-to-peer networks, and are more difficult to eradicate. Four of the eight mass-mailing worms in the top ten reports used additional propagation mechanisms. An example of this is Beagle.AV,⁴⁴ which used email and peer-to-peer networks to propagate, and disabled antivirus products in order to hinder disinfection.

While several of the top ten samples in this reporting period were listed in previous *Internet Security Threat Reports*, others, such as Beagle.AV, are new additions to the list (table 6). When a particular piece of malicious code proves itself to be successful by infecting a large number of users, new variants are often created since similar techniques will likely work again. For instance, the use of P2P networks in combination with mass-mailing worms has become such a common practice that four of the eight mass-mailing worms in the top ten malicious code—all of which were variants of Netsky, Beagle or MyDoom—reported this period employed this propagation mechanism.

Rank	Sample
1	Netsky.P
2	Sober.I
3	Gaobot
4	Spybot
5	Beagle.AV
6	Beagle.X
7	Mydoom.M
8	Netsky.Z
9	Netsky.D
10	Beagle.AW

Table 6. Top ten malicious code reported to Symantec

Source: Symantec Corporation

³⁹ A mass-mailing worm is an application that propagates primarily by attaching a copy of its executable to email messages that it sends to other users.

⁴⁰ <http://securityresponse.symantec.com/avcenter/venc/data/w32.netsky@mm.html>

⁴¹ <http://securityresponse.symantec.com/avcenter/venc/data/w32.sober@mm.html>

⁴² <http://securityresponse.symantec.com/avcenter/venc/data/w32.beagle.a@mm.html>

⁴³ <http://securityresponse.symantec.com/avcenter/venc/data/w32.novarg.a@mm.html>

⁴⁴ <http://securityresponse.symantec.com/avcenter/venc/data/w32.beagle.av@mm.html>

Netsky.P⁴⁵ was the most common malicious code sample reported to Symantec between July 1 and December 31, 2004. Variants of Netsky, which was first seen on February 16, 2004, make up three of the top ten malicious code submissions during this reporting period. Netsky sends itself in an archive using a .zip extension that allows it to bypass filtering measures. Because files with a .zip extension are generally trusted, end users are likely to unzip the file and then inadvertently run the virus.

The second-ranked malicious code sample for this reporting period, Sober.I,⁴⁶ is new to the top ten this reporting period. A new variant of the Sober worm, Sober.I was initially reported on November 19, 2004 and propagated rapidly. The original Sober worm was first reported on October 24, 2003. It was a mass-mailing worm that used its own SMTP engine to spread, sending itself as an email attachment to the addresses gathered from the infected computer. Previous variants of the Sober family have also been successful, with four other variants present in the top 50 reported malicious code samples over the previous two reporting periods.

Bots continue to make inroads during the last six months of 2004, accounting for two of the top ten reported samples, compared to just one in the previous reporting period. Gaobot was the third most frequently reported sample over the past six months, followed in fourth spot by Spybot. Gaobot also occupied the third ranking in the previous reporting period, whereas Spybot was not included in the top ten at that time.

The presence of these two bots in the top ten may indicate that the use of bots is continuing to increase, as was noted in the previous volume of the *Internet Security Threat Report*. This may be due to the variety of functions they can perform on compromised computers. These are discussed in greater depth in the “Bots” discussion below.

The fifth and sixth most common malicious code samples during the second half of 2004 were variants of the Beagle mass-mailer worm. In the previous reporting period, Beagle.M was the eighth most reported sample. Beagle uses a similar propagation technique to that of Netsky. However, it took this technique one step further by applying password protection to the .zip file.⁴⁷ This tactic exploited the fact that users are more likely to trust password-protected files. It also enabled the attachment to bypass many email gateways and scanners, which are unable to scan password-protected files.

Win32 viruses and worms

Win32 threats are executable programs that operate by using the Win32 API (application program interface),⁴⁸ which provides a standard for the development of software on the Windows platform. These forms of malicious code work on at least one Win32 platform. Win32 threats have shown a major rise in volume during 2004 (figure 23). This rise was first noted in the second half of 2002 and it is clear that it continues, although the rate of increase has decreased over the second half of 2004.

Between July 1 and December 31, 2004, Symantec documented more than 7,360 new Win32 virus and worm variants. This is an increase of 64% over the 4,496 reported in the first half of the year and an increase of more than 332% over the 1,702 documented in the second half of 2003. As of December 31, 2004, the total number of Win32 variants is approaching 17,500.

⁴⁵ <http://securityresponse.symantec.com/avcenter/venc/data/w32.netsky.p@mm.html>

⁴⁶ <http://securityresponse.symantec.com/sarc/sarc.nsf/html/w32.sober.i@mm.html>

⁴⁷ The password required to open the archive was included in the email message body or as a JPEG file attached to the message.

For details, please see: <http://securityresponse.symantec.com/avcenter/venc/data/w32.beagle@mm!zip.html>.

⁴⁸ An API (application program interface) is a set of tools that are specific to an operating system that allows programmers to write software within that system. The Win32 API provides a standard for the development of software on the Windows platform.

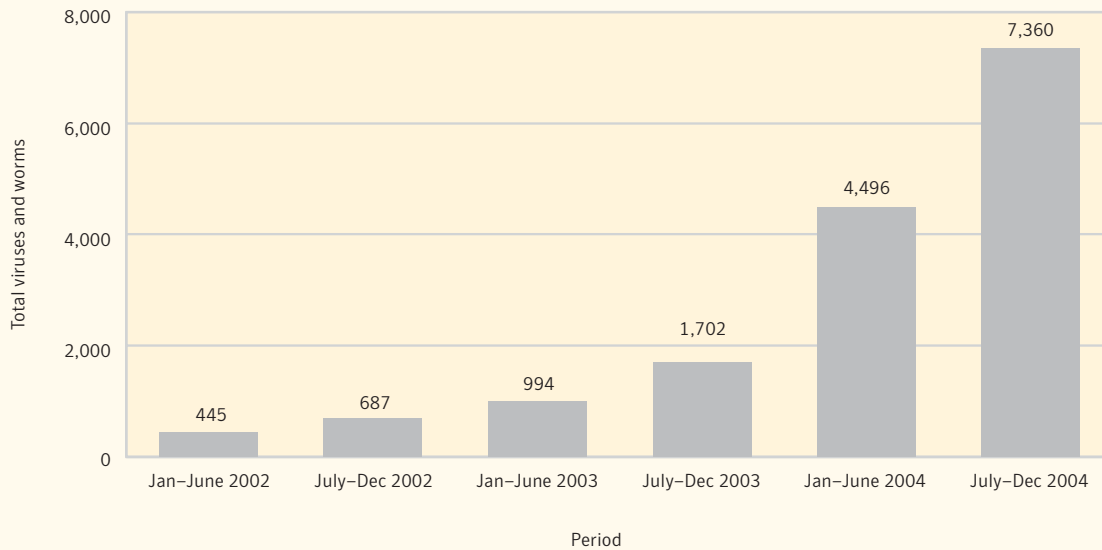


Figure 23. New Win32 viruses and worms by six-month period 2002–2004

Source: Symantec Corporation

With their massive accumulation over the past few years, Win32 threats are now more common than script- and macro-based threats combined. Initially, script- and macro-based threats were more prolific; however, this has quickly changed. This may be due to the ease of creating script and macro threats for new technology. When a new technology is released, scripting languages are easier to learn and use than more complex compiled languages.

As malicious code authors become more familiar with the new technology and its APIs, it becomes more beneficial for them to create compiled threats using native code. Script- or macro-based threats rely upon the presence of an appropriate scripting host to interpret and execute it. If the interpreter is not present on the computer or if it has been disabled through policies, the script will not run. This is not the case with native code, which does not require any specialized interpreter. Since script and macro threats are easier for antivirus software to detect than a compiled application, there is greater incentive for malicious code writers to use compiled languages in order to increase the effective lifespan of the malicious code.

During 2004 alone, Symantec documented over 11,800 unique samples of Win32 threats, a greater number than the cumulative 10,000 DOS viruses⁴⁹ documented between 1986–1996. In October of 2004 alone, Symantec documented 1,500 Win32 samples, almost as many as the 1,702 documented in the entire last six months of 2003.

⁴⁹ Prior to the release of Windows 95, DOS (Disk Operating System) was the primary operating system used by most personal computers. Early versions of Windows simply ran as an application within DOS. Therefore, most malicious code written prior to 1995 was intended to run on DOS just as most current malicious code is intended to run on Windows.

Malicious code for Linux

In the previous *Internet Security Threat Report*, Symantec cautioned that an exploit-based worm for Linux and Linux-based applications could soon appear.⁵⁰ This warning appears to have been well founded. On December 21, 2004, the Santy worm⁵¹ was the first reported Web application worm to be detected propagating in the wild. While other worms have exploited Web servers and their related components, this was the first time a worm exploited a vulnerability in a separate application running on the Web server. Specifically, it exploited a script injection vulnerability in phpBB.⁵²

Santy is interesting for a number of reasons. For one, while it affected primarily Linux systems, it could also affect computers running phpBB on Windows and other operating systems. Santy used the Google search engine to locate vulnerable systems to exploit. It was also the first worm in the wild to exploit a vulnerability in a Web application rather than the underlying operating system or the Web server itself. Symantec expects that Santy is likely just the first in a new trend of worms exploiting these types of vulnerabilities.

Santy was implemented as a Perl script, making it easy to modify the worm and implement new functionality. The first version of Santy would simply propagate to a vulnerable system and overwrite certain Web pages in order to deface the site. Two later versions, Santy.B and Santy.C, were modified to also install a back door server and an IRC bot on infected systems and to use different search engines to locate vulnerable systems. This was made necessary because Google began filtering search requests made by the worm. Additionally, these Santy variants would exploit similar injection vulnerabilities in multiple Web application scripts, not only phpBB.

The vulnerability exploited by Santy had been announced on the BugTraq mailing list on July 11, 2004. On November 18, 2004, the vendor of phpBB confirmed the existence of this vulnerability and released a fix for it the following day. Slightly more than a month passed before the Santy worm was initially reported, adequate time for most users to test and apply the patch to vulnerable systems. Still, an abundance of vulnerable systems remained available for Santy to infect. This may reflect the fact that patching Linux systems involves a more complicated process than patching Microsoft systems.

When Santy overwrote Web pages on a compromised computer, it replaced them with a page containing the text "This site is defaced!!! NeverEverNoSanity WebWorm generation X," where X was the number of sites defaced by that strain of the worm. At the time of writing, a Google search for this text returned over 30,000 results.⁵³ This demonstrates the need for users to remain informed of new vulnerabilities, as well as the availability of patches, workarounds, and mitigation strategies.

In cases where a vulnerability affects an application or service that must be available to the public, such as Web applications, patches should be applied as soon as possible. Vulnerabilities in Web services usually cannot be mitigated using the common strategies normally recommended for other remote services, such as using a firewall to block or filter traffic to a port, because they are critical enterprise services that must exchange data with external users.

⁵⁰ Symantec *Internet Security Threat Report*, Volume VI, September 2004: p. 45
<http://enterprisesecurity.symantec.com/content.cfm?articleid=1539>

⁵¹ <http://securityresponse.symantec.com/avcenter/venc/data/perl.santy.html>

⁵² <http://www.securityfocus.com/bid/10701>

⁵³ This number may include Web pages that discuss the Santy worm, such as antivirus vendor sites.

Exposure of confidential information

Almost every computer is likely to contain information that its owner would prefer to keep private. Information such as email addresses, confidential documents, cached logon credentials, and financial information may all be found on the drives of corporate and home users alike. Once a computer has been compromised by malicious code, all of this information may potentially be accessed, disclosed, and or altered without authorization. In fact, some malicious code is created with the intent of purposely stealing confidential information from a compromised computer.

Threats with the potential to expose confidential information have continued to increase over the past three reporting periods. Between July 1 and December 31, 2004, malicious code that exposed confidential information represented 54% of the top 50 malicious code samples received by Symantec, up from 44% in the first half of 2004, and 36% in the second half of 2003. This represents a 23% increase between the current period and the first half of 2004, and a 50% increase over the same period the previous year (figure 24). This is partially due to the increasing proliferation of bots, which expose all information on the compromised computer due to their remote access capabilities. (For a more detailed discussion, see the “Bots” discussion below.)

Information exposure threats can be present in almost any type of malicious code, including Trojan horses, worms, viruses, and back door server programs. Many worms and Trojans contain keystroke-logging and back door functionality in addition to their other components. For example, variants of the MyDoom worm contained keystroke-logging functionality in addition to their propagation routines and other payloads.

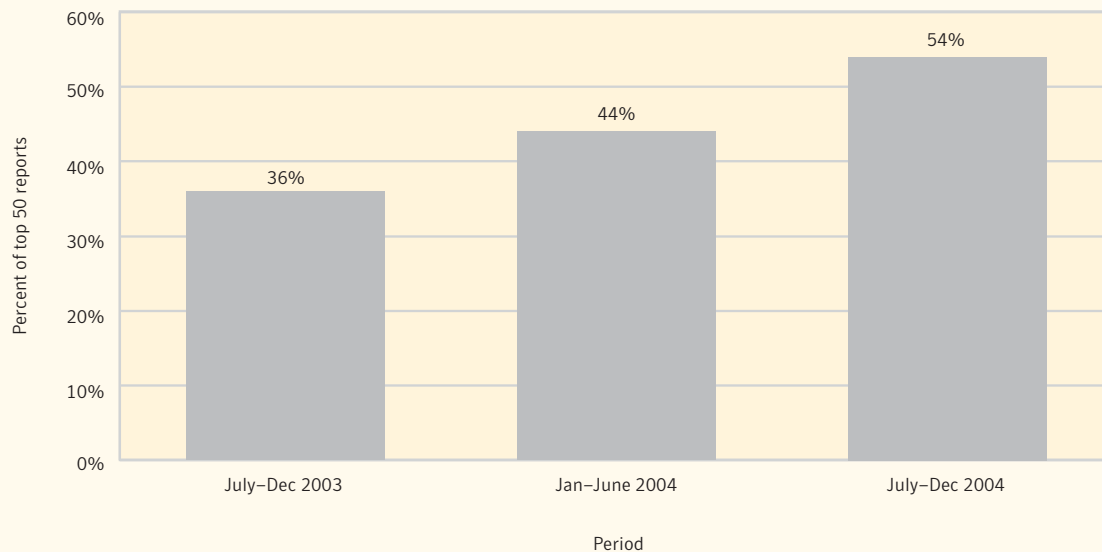


Figure 24. Malicious code threats to confidential information
Source: Symantec Corporation

Some malicious code that has keystroke-logging functionality, such as some variants of Spybot, may simply log all keystrokes on the compromised computer. Others may perform more sophisticated information-exposure functions. For instance, the Banker Trojan,⁵⁴ waits for a user to open a Web browser to an online banking site and records the user's authentication information. Others, such as the Bancos family,⁵⁵ will wait for the user to visit certain online banking sites and mimic the bank's online interface in order to capture the user's confidential information. This information is then sent to a remote attacker and can be used for identity theft purposes or to simply logon as the user and transfer account funds. This technique is similar to phishing, which is discussed in the "Additional Security Risks" section of this report. However, whereas phishing consists of emails that attempt to lure users to a false Web site, these examples are actually Trojans that mimic the user interface.

Back door server programs, or simply back doors, allow a remote attacker nearly unfettered access to the compromised computer. The attacker can use the back door to install other programs on the computer, such as keystroke-logging Trojans or other monitoring software. Additionally, the back door could allow the remote attacker to view the contents of files saved on the computer or to retrieve cached passwords. The password cache could potentially contain logon information for online banking Web sites if the user has chosen to have their Web browser store their credentials for the site. Some back doors even allow a remote attacker to turn on any Web cams attached to the computer and view the video stream without the user's knowledge.⁵⁶

Users can protect themselves from these threats by never executing unknown applications, especially those received in email or downloaded from sources that are not certain to be trustworthy. Users should also avoid using public computer terminals to logon to Web-based email or online banking sites, as the integrity of these systems cannot be verified. They should also avoid using single passwords for authentication in multiple applications, as the compromise of a single password may subsequently allow an attacker access to numerous sources of confidential data. Changing passwords frequently can also help protect against a password compromise. Finally, Symantec advises users not to allow Web browsers to cache logon credentials for Web sites

Trojan horses

Trojan horses are a major source of information exposure. A Trojan horse (also referred to as a Trojan) is a program that intentionally misrepresents its functionality through a filename, location, or appearance. A Trojan neither replicates nor copies itself, but may cause damage to or compromise the security of a computer in some way. During the first six months of 2004, these programs were second only to the MyDoom worm in numbers reported by Symantec customers. During the last six months of the year, Trojans have become the most reported threat, representing 33% of the top 50 malicious code reported to Symantec (figure 25).

⁵⁴ <http://securityresponse.symantec.com/avcenter/venc/data/pwsteal.banker.b.html>

⁵⁵ <http://securityresponse.symantec.com/avcenter/venc/data/pwsteal.bancos.html>

⁵⁶ <http://www.securityfocus.com/news/8893>

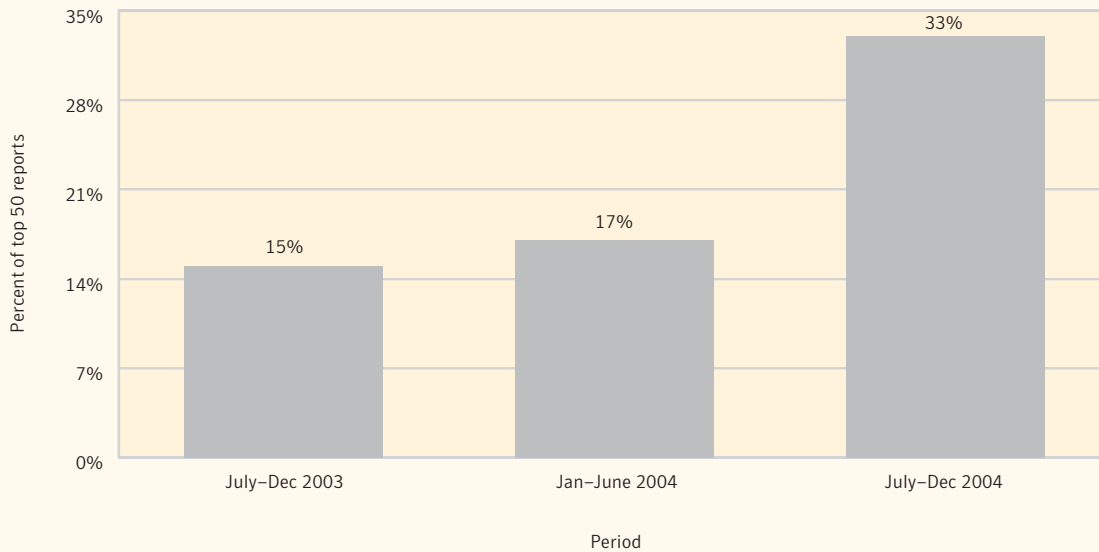


Figure 25. Trojans as percentage of top 50 malicious code submissions

Source: Symantec Corporation

The increase in reported Trojans may be partially attributed to the increase in client-side exploits for Web browsers.⁵⁷ These exploits can allow a Trojan to be installed on a computer without the knowledge of the user. Since Trojans do not have the means to propagate (if they did, they would be reclassified as worms or viruses), exploitation of these client-side vulnerabilities provides an effective mechanism for their delivery.

The Trojan program may be hosted on a malicious Web site that attempts to exploit a specific Web browser vulnerability. The attacker then entices users to visit this Web page, possibly by including a link to the page in spam emails. When a user of a vulnerable Web browser views the page, the exploit code is executed and the Trojan is installed on the user's computer. For example, the Phel Trojan⁵⁸ is typically installed on a computer by exploiting a vulnerability in Internet Explorer⁵⁹ that was unpatched at the time the Trojan was initially released. Once this Trojan is running on a computer, it downloads and installs a back door program⁶⁰ from a remote Web site.

Users can take several steps to prevent applications from being installed on computers through client-side vulnerabilities in Web browsers. Disabling the execution of script code and active content by the browser will reduce the ability of malicious Web pages to download and execute code. Also, running the Web browser as an unprivileged user will limit the consequences of successful compromises.

⁵⁷ Client-side vulnerabilities target the computer systems of individual users rather than servers of an organization. They target applications such as Web browsers, email clients, peer-to-peer networks, instant messaging clients, and media players. They are often, but not always, the result of logic errors or flaws in access-control systems, and they are often easily exploitable, particularly in browsers.

⁵⁸ <http://securityresponse.symantec.com/avcenter/venc/data/trojan.phel.a.html>

⁵⁹ <http://www.securityfocus.com/bid/11467>

⁶⁰ <http://securityresponse.symantec.com/avcenter/venc/data/backdoor.coreflood.html>

Malicious code for mobile devices

Smart phones are mobile phones that contain a full-fledged operating system with a wide variety of user-installable software. Combined with increasingly common PDAs, these phones have created a new class of mobile computing devices. The popularity of these devices has been matched by an increased interest among malicious code writers in producing creations for these platforms, particularly PocketPC, Symbian,[®] and Palm.[™]

As was reported in the previous *Internet Security Threat Report*, the first worm to target these mobile devices, Cabir,⁶¹ was released in June 2004.⁶² Multiple variants of the worm followed shortly thereafter. Initially, these variants were simply created by using a hex code editor to change visible strings, such as the filenames in the binary file of the original Cabir. However, in December 2004, the source code was publicly released and a variety of new variants were updated, recompiled, and released.

By the end of December 2004, 11 new variants of Cabir had been discovered. Many of these new variants were actually included in a new Trojan, known as Skulls,⁶³ which not only installed Cabir but also replaced many of the system applications, thereby disrupting the targeted device's functionality. While most of these variants have not been observed in the wild, some reports of Cabir in the wild have been fielded from a variety of Southeast Asian countries, including Singapore and the Philippines.⁶⁴

On July 17, 2004, the first threat to Windows CE was reported, a simple appending virus known as Duts.⁶⁵ Duts would only infect ARM-based devices, such as Pocket PCs, and would merely append itself to all the .exe files in the root folder. Closely on the heels of Duts, the second Windows CE threat appeared on August 5, 2004, a back door Trojan known as Brador.⁶⁶ Brador opens a listening port on TCP 2989 and waits for instructions from an attacker to perform a number of tasks, including: listing directory contents, uploading files, displaying message boxes, downloading files, and executing commands.

Finally, a Trojan was discovered in a Symbian game⁶⁷ that would actually send an SMS (Simple Message Service) message to a toll-charge phone number. This Trojan was named Mos.⁶⁸ The code in the game was purposely included by the developer as a copy protection scheme in January 2004. While the developer removed the code shortly thereafter, cracked versions of the game with the SMS code were found on some popular software piracy sites in August 2004.

The absolute number of threats to mobile devices remains low; however, due to the discovery of multiple variants of Cabir, it has increased dramatically over the past six months. In June 2004, the sum total of malicious code threats targeting mobile devices was four: one worm (Cabir), one virus, and two Trojans. By the end of the year, there were thirteen worms (Cabir and Duts and their variants), one virus, and seven Trojans.

The number of mobile device threats reported in the wild is still extremely small. Most are proof-of-concept threats that have not been released in the wild. Nevertheless, the types of threats created demonstrate some of the robust capabilities of these devices. For example, Mos demonstrates that mobile devices may well serve as delivery vectors for spyware or adware in the near future.

⁶¹ <http://securityresponse.symantec.com/avcenter/venc/data/epoc.cabir.html>

⁶² Symantec *Internet Security Threat Report*, Volume VI (September 2004): p. 37
<http://enterprisesecurity.symantec.com/content.cfm?articleid=1539>

⁶³ <http://securityresponse.symantec.com/avcenter/venc/data/symbos.skulls.html>

⁶⁴ <http://www.cellular-news.com/story/11546.shtml>

⁶⁵ <http://securityresponse.symantec.com/avcenter/venc/data/wince.duts.a.html>

⁶⁶ <http://securityresponse.symantec.com/avcenter/venc/data/backdoor.brador.a.html>

⁶⁷ This game was called Mosquitos. Only early official versions of this game contained the code to dial the toll-charge numbers. The developer terminated the premium-rate contracts for the toll-charge numbers shortly after the Trojan was reported.

⁶⁸ <http://securityresponse.symantec.com/avcenter/venc/data/trojan.mos.html>

Security products that can detect malicious code exist for most mobile device operating systems. In addition, common safe computing practices such as not installing unknown programs or accepting connections from unknown sources will help prevent infection by these threats.

Malicious code for P2P, IM, IRC, and CIFS

Peer-to-peer services (P2P) and Windows file sharing (CIFS) continue to be propagation vectors used by the top malicious code threats. However, contrary to widespread expectations, instant messaging (IM) has not become a widely used propagation mechanism. Furthermore, while IRC is a commonly used mechanism for bot communication, none of the top 50 malicious code reported to Symantec in the last six months of 2004 use IRC as a propagation mechanism (although some bots do use IRC as a communication channel). Overall, the number of threats using P2P, IM, IRC, and CIFS within Symantec's top 50 malicious code reports has increased by 39% over the previous six-month period (figure 26).

As was evident in the top ten malicious code samples discussed earlier in this section, variants of Netsky, Beagle, and MyDoom continued to be predominant threats in the last six months of 2004. This was similar to the previous six-month reporting period. All three worms use P2P to spread. MyDoom simply copies itself to the Kazaa-shared folder using enticing filenames. Netsky and Beagle search the hard drive for any directories that appear to be P2P-shared folders and copy themselves to these shared directories using one of a number of commonly searched for filenames. When users search a P2P file-sharing network for files matching these filenames, they will download and execute the worm, allowing it to propagate further.

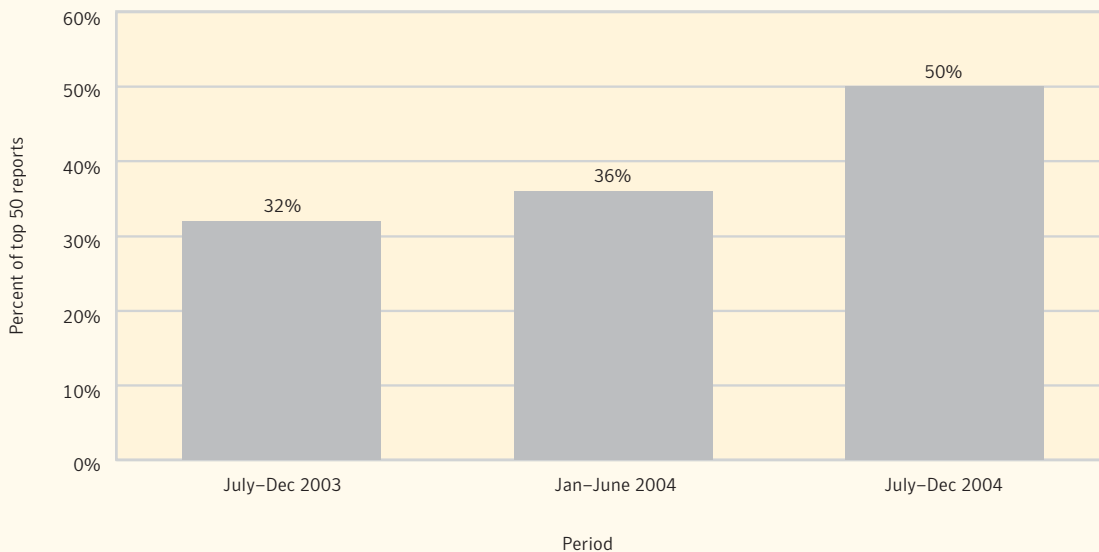


Figure 26. P2P, IM, IRC, and CIFS threats
Source: Symantec Corporation

Windows file sharing (CIFS) continues to be a popular propagation vector for Windows bots. Threats such as Gaobot and Spybot, both of which are in the top ten reports for this period, exploit weak passwords on Windows systems. Both threats use a dictionary of commonly used passwords to connect to a remote Windows machine. Once connected, they copy themselves over to the machine and remotely execute themselves. 30% of the top fifty threats reported between July 1 and December 31, 2004, use CIFS as a propagation vector.

There has long been speculation, particularly in the media, that IM would at some point in time provide a fertile infection vector for malicious code. Thus far, this has not been realized. As was the case in the first six months of 2004, there were no IM threats in the top 50 malicious code reports during the second half of the year. Symantec believes that this is probably because these applications rely on a central server to relay messages between users; it would therefore be easy for the Internet service provider or the IM provider to filter messages carrying malicious code.

P2P and CIFS are commonly used on a daily basis for business and personal purposes. Symantec expects to continue to see malicious code developed that will propagate through these services. In addition, mechanisms such as IRC are being used for command and control in bot networks. Organizations should ensure that systems are audited for unauthorized usage of such applications and protocols. In addition, insecure versions of these services and their client applications should be avoided and organizations should ensure that strong password policies are followed.

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. They are distinct from similar types of malicious code because of their unique networking functionality. Bots are designed to let an attacker create a network of compromised hosts (a bot network), which can then be remotely controlled to conduct malicious activities collectively. Once the bot network is established, the attacker can issue commands through broadcast communication channels, such as IRC. Bots can be used for a wide variety of malicious purposes, such as information theft, proxying network traffic such as SMTP and HTTP, and performing distributed denial of service (DDoS) attacks.

Bots often employ multiple propagation mechanisms to compromise other computers. They may copy themselves to shared network drives with weak password protection or through P2P networks by copying themselves to the shared folders of the P2P client application. Most bots, such as Randex, 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.⁶⁹

Bots are steadily becoming more prevalent in malicious code reported to Symantec. During the last six months of 2004, they accounted for 12% of the top 50 malicious code samples reported to Symantec. This is a significant increase over the 10% from the first six months of 2004 and the 9% of the last six months of 2003 (figure 27).

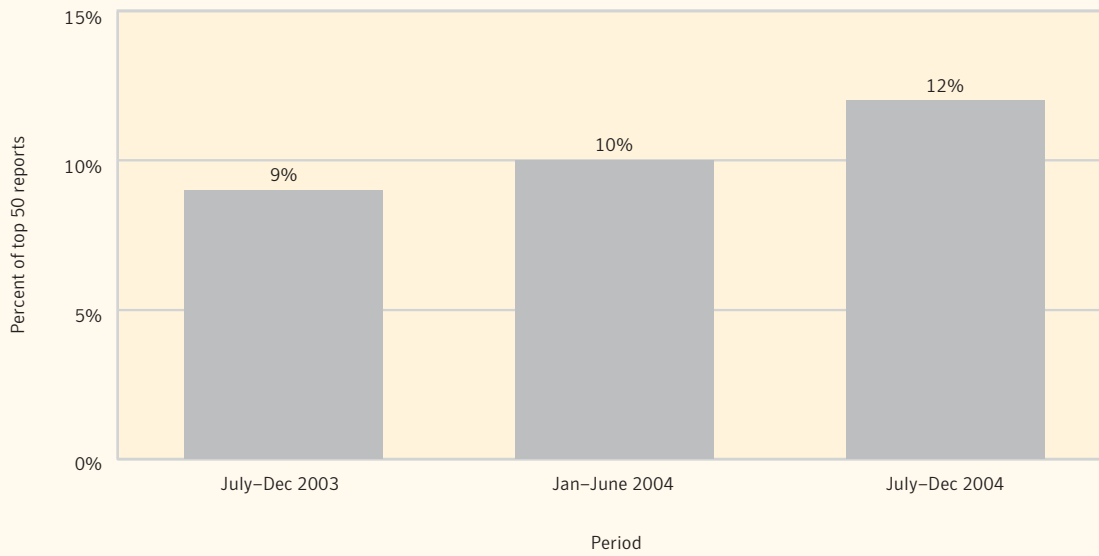


Figure 27. Bots in top 50 malicious code reports
Source: Symantec Corporation

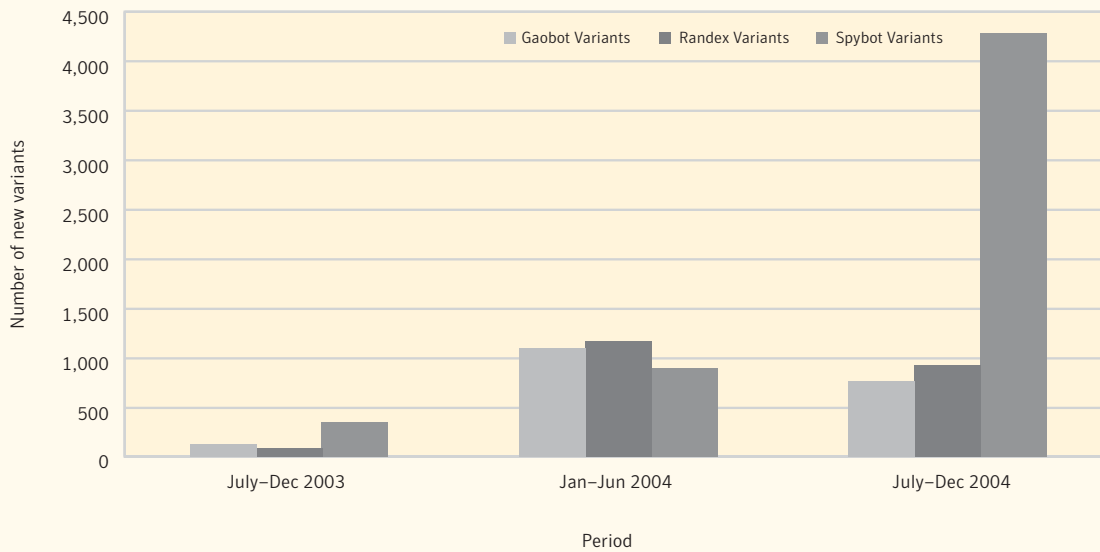


Figure 28. Number of new bot variants
Source: Symantec Corporation

As noted in the previous edition of the Symantec *Internet Security Threat Report*, the number of documented variants of the major bots continues to increase. In the last six months, the three major bots—Randex, Gaobot, and Spybot—represented a combined total of close to 6,000 new variants. This represents a 189% increase over the previous six-month period in which there were just over 3,100 new variants. Further, it is a 1063% increase over the same period last year, during which there were just over 550 new variants.

While the total number of variants increased between July 1 and December 31, 2004, only the number of variants of Spybot increased, while the number of new Gaobot and Randex variants decreased slightly. Spybot showed a dramatic increase in new variants, adding close to 4,300 new distinct variants to its numbers (figure 28), a 180% increase over the previous six months. Randex and Gaobot added over 900 and 700 variants respectively. These variants may incorporate different characteristics, such as employing runtime packers,⁷⁰ leveraging different exploits, or performing different functionalities.

This does not necessarily imply that malicious code authors have abandoned Randex and Gaobot in favor of Spybot. Rather, since the source code for all three of these bots is readily available on the Internet, malicious code authors are likely combining features from each to create new variants. In some cases, the finished product may more closely resemble Spybot than the other two, leading them to be classified as a new Spybot variant. Additionally, the wide usage of run-time packers continues to create an increasing number of new variants.

New bot trends

Over the past six months, Symantec analysts have observed disturbing new trends in the evolution and development of bots. Most bots use IRC as a control channel. A bot will typically be programmed to connect to a predetermined IRC server and a specific channel to join. Once the bot joins the channel, it can receive commands from a remote attacker. The dependence on a centralized communication channel makes the bot network fragile, since taking down the IRC server will effectively disable communication between the bots and their master.

In response to this, bots that utilize new communication methods are emerging. In particular, two bots that were captured by Symantec DeepSight Honeypots™, Moonlit⁷¹ and Zincite,⁷² were observed using their own peer-to-peer networks for communication. This communication was encrypted and used random network ports in order to evade detection. Rather than connecting to a central server to receive commands, these bots maintained a list of IP addresses that were also compromised. This way, the removal of any one peer from the network would have no impact on the rest, making it more difficult to shut down the network.

Another new development in bot communication is the use of POP3⁷³ to send commands. This was seen in Sconato,⁷⁴ a bot that also contained keystroke-logging functionality. The bot would connect to a predefined mail server to retrieve email messages containing attachments. Embedded within the attachments were commands that were able to direct the bot to manipulate various aspects of the compromised computer. Additionally, Sconato is able to respond to commands by sending email messages to the mail server. Since POP3 communication is not uncommon on most networks, this traffic would be more likely to go undetected than a connection to an IRC server. Additionally, ports used for POP3 communication are less likely to be filtered or blocked at the network perimeter.

⁷⁰ Packers are tools that compress and encrypt Windows executable files. This is a concern for security personnel because it makes detection by antivirus engineers more difficult.

⁷¹ <https://tms.symantec.com/downloads/040809-Analysis-Backdoor.Moonlit.pdf>

⁷² <https://tms.symantec.com/downloads/040727-Analysis-Mydoom.M.pdf>

⁷³ POP3 is a version of the post office protocol used to retrieve email from a server.

⁷⁴ <https://tms.symantec.com/downloads/040821-Analysis-Trojan.SconatoPOP3CommunicationChannel.pdf>

Malicious code for profit

The use of malicious code for profit appears to be an increasing concern and bots are expected to be a big part of this trend. A bot captured by the Symantec DeepSight Honeypot system appeared to be intended as a relay for bulk unsolicited email (spam). This bot, named Spammerbot,⁷⁵ contains an SMTP proxy that is used to send spam from computers controlled by a remote attacker.

It has long been rumored that networks of bots such as these have been traded or sold on IRC channels. Due to blacklisting,⁷⁶ spammers are in constant need of new IP addresses from which to relay messages; compromised home and corporate computers serve this purpose ideally. The top 50 malicious code reported to Symantec saw an increase in malicious code containing SMTP relays, which seems to confirm that this activity is increasing. In the last six months of 2003, only 37% of the volume of the top 50 samples of malicious code reported to Symantec contained SMTP-relaying functionality. This rose to 47% in the first six months of 2004 and 53% in the last six months of the year (figure 29).

Beagle.AV was another example of malicious code being developed for profit. This variant of the Beagle worm installed an SMTP relay, which was observed by Symantec DeepSight Honeypots being used to relay phishing email.

The inclusion of revenue generation mechanisms within malicious code is worrisome. Symantec expects the trend towards monetization of malicious code to continue and extend into other forms, such as worms. As such, Symantec will continue to monitor this activity closely.

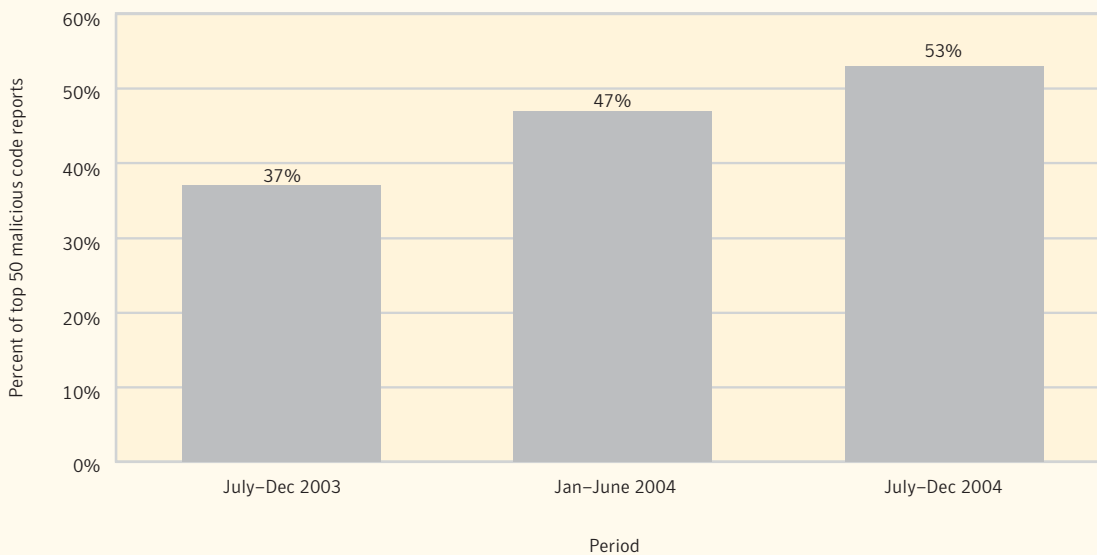


Figure 29. Malicious code that allows SMTP relaying
Source: Symantec Corporation

⁷⁵ <https://tms.symantec.com/downloads/041203-Analysis-HarnessingBotNetworksForSpam.pdf>

⁷⁶ Blacklisting is the practice of recording IP addresses of computers and networks that send spam. When an address is used consistently to send spam, that address may be blacklisted and mail servers configured to ignore connections from those addresses.

Additional Security Risks Report

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 threats, particularly spam, phishing, spyware, and adware, has necessitated an expansion of the traditional security taxonomy.

Symantec has monitored these new emerging security risks as they have developed, classifying them as “additional security risks.” This section will examine developments in additional security risks over the last six months of 2004. In particular, it will examine trends in spyware and adware, phishing, and spam.

Adware and spyware

Adware consists of programs that display advertising content on a user’s monitor, often without the user’s prior consent or explicit knowledge. It is usually, but not always, presented in the form of pop-up windows or bars that appear on the screen. 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.

While much adware is benign, depending upon its functionality, some forms of adware are not. 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. It does 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.
- In some cases the adware may also modify the Winsock.dll⁷⁷ in order to monitor the user’s Web browsing habits, affecting the integrity of the computer.

Spyware refers to stand-alone programs that can secretly monitor system activity and relay the information back to another computer. In some cases, spyware may be legitimate programs that are employed by corporations to monitor employee Internet usage or by parents to monitor their children’s Internet usage. However, it may also represent less legitimate applications.

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. Because spyware can capture sensitive information before it is encrypted for transmission, it can bypass security measures such as firewalls, secure connections, and VPNs that may be in place. Spyware is a particular concern because of its potential use in identity theft and fraud.

Volume of adware and spyware

Even though spyware and adware are not classified as malicious code, Symantec monitors and analyzes them using the same methods as for malicious code. This involves an ongoing analysis of customer reports and data delivered from over 120 million client, server, and gateway email systems,⁷⁸ as well as filtration of 25 million email messages per day. Symantec then compiles the most common reports and analyzes them to determine whether the activity they identify is related to adware and spyware as opposed to malicious code.

⁷⁷ Winsock, short for Windows Socket, is an API that allows Windows computers to communicate using the TCP/IP protocol.
⁷⁸ Systems deploying Symantec antivirus security solutions

Top ten adware reported

As was mentioned in the previous volume of the *Internet Security Threat Report*, adware is a growing concern.⁷⁹ Over the past six months, the percentage of adware in the top 50 malicious code reports to Symantec has increased over the first six months of 2004. Between January 1 and June 30, adware made up 4% of the top 50 malicious code reported. Between July 1 and Dec 31, it made up 5% of the top 50 reports.

The top reported adware program between July 1 and December 31, 2004, was lefeats (table 7), which accounted for 36% of the top ten reports. lefeats can be installed manually, but is sometimes bundled with other software. It possesses a variety of functionalities. When installed via the user's browser, it registers itself as a browser help object (BHO),⁸⁰ and modifies registry keys to ensure its survival.

lefeats also hijacks the browser start page to display its own search engine page. This can be used to track any search terms the user enters, possibly to display only results that link to pages of paying advertisers. Not only does the program utilize system resources, it hijacks the browser start page and downloads a number of other programs to help it perform Web searches.

The second most common adware of the past six months was InstantAccess. Accounting for almost 11% of the top ten reported adware, this program downloads pop-up ads onto the user's computer. It is most likely bundled with software, so that the user downloads it when installing the desired software.

Gator was the third most commonly reported adware for the second half of 2004. During this period, it made up just over 9% of the top ten adware reports. Gator downloads and displays advertisements. It also tracks the user's Web browsing habits and online purchasing and sends them to its centralized servers.

This adware program must be manually installed. However, there are several known programs that have Gator bundled with them and that install it as the program itself is installed. This can happen in two ways. First, a program may tell the user in a complex end user license agreement (EULA) that Gator will be installed, and ask for consent to permit Gator's installation. By accepting the EULA, the user (either knowingly or, due to the complexity of the EULA, unknowingly) agrees to have the adware installed on his or her computer. Second, some programs are bundled with Gator and install it without the user's knowledge or consent.

Rank	Adware name
1	lefeats
2	InstantAccess
3	Gator
4	Istbar
5	VirtuMonde
6	Binet
7	CDT
8	MainSearch
9	180Search
10	NetOptimizer

Table 7. Top ten adware reports
Source: Symantec Corporation

Rank	Spyware name
1	Webhancer
2	e2Give
3	Apropos
4	Look2Me
5	2020search
6	Dotcomtoolbar
7	Iwantsearch
8	ClientMan
9	Perfect
10	Shopnav

Table 8. Top ten spyware reports
Source: Symantec Corporation

⁷⁹ The Symantec *Internet Security Threat Report*, Volume VI (September 2004): p. 41
<http://enterprisesecurity.symantec.com/content.cfm?articleid=1539>

⁸⁰ Browser helper objects (BHOs) are add-on programs that can add legitimate features to a user's browser (IE 4.X and up). For example, document readers used to read programs within the browser do so via BHOs.

Top ten reported spyware

Webhancer was the most frequently reported spyware program during the second half of 2004, representing 38% of the top ten spyware reported (table 8). It is a program that monitors the user's browsing habits, sending the information back to its centralized servers. The program is 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 EULA. It is typically bundled with other programs, particularly certain peer-to-peer file sharing programs.

The second most common spyware reported between July 1 and December 31, 2004, was e2give, an Internet Explorer browser helper object (BHO). This program accounted for over 30% of the top ten spyware reported to Symantec during this period. It tracks which Web sites the user visits and monitors the length of time a user spends at each site. e2give may also track the user's country, zip code, and first name as well as information about the user's computer. e2give can be installed manually or by an ActiveX downloader.

The third most common spyware program reported during the last six months of 2004 was Apropos, which accounted for just under 10% of the top ten spyware reports. An Internet Explorer BHO, Apropos installs a toolbar that links to Web sites and sends information back to its server. It is installed via an ActiveX control. Additionally, this 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.

Installation of adware and spyware

There are numerous different ways by which adware and 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.

End user license agreements (EULAs)

Some companies justify the use of 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 a EULA.

Some 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. Assuming the information in the EULA is correct and acceptable to the user, the risk presented by the introduction of this type of adware is minimal. However, other adware may be bundled with the desired software without the users' knowledge. The user often unknowingly consents 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 it. Adware can also be installed by a third party after the user has accepted the EULA and installed the original software.

Commercial spyware programs tend to have EULAs. However, as spyware is designed to be installed and work without the target's knowledge, the programs may contain an option that will allow for remote installation without the presence of the EULA. Spyware has the capacity to log keystrokes, IM conversations, email, and other communications that can contain personally identifiable information. As such, it can facilitate not only monitoring by legitimate sources, but fraud and identity theft as well. Thus, security solutions that deal with spyware programs should detect spyware regardless of the presence of a EULA.

During the last six months of 2004, three of the top ten adware programs reported to Symantec —Gator, NetOptimizer, and Binet—had EULAs. In the spyware category, one reported program, Webhancer, came with a EULA.

Bundled with other software

As discussed in the previous section, some companies increase the distribution of their software by offering it to users for free download. In order to monetize 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.

Spyware programs are sometimes bundled with other programs as well; 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 obtain confidential data. The software package is then placed on a public download site, or sent to a newsgroup for maximum exposure.⁸¹ The spyware is then executed when the user runs the desired program.

Of the top ten adware programs reported to Symantec over the last six months of 2004, nine came bundled with other software, including lefeats. Five of the top ten spyware were bundled, including Webhancer.

Web browsers

Adware is often installed through the user's Web browser. Often this is done through pop-up ads offering free software to download. The pop-up offers the user a choice of clicking “Yes” or “No” to accept or reject the offer. In reality, though, clicking anywhere on the ad results in the download of adware. Browser-installed adware may also be installed through ActiveX controls or browser helper objects (BHOs). (For a full description of browser help objects, see “Functionality of adware and spyware” below.)

Five of the top ten adware programs reported to Symantec in the last six months of 2004 were installed through Web browsers, including Istar, the most common adware with this functionality. Spyware can also be installed through a Web browser using ActiveX controls or BHOs. However, in this reporting period none of the top ten reported spyware were installed in this way.

To reduce the risk from adware or spyware that is installed through a Web browser, users should disable 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. Finally, the user may also choose to disable the acceptance of third-party cookies.

⁸¹ Spyware is often downloaded along with hacking tools or sexually explicit programs.

Functionality of adware and spyware

Within the broad categories of adware and spyware are many programs that accomplish similar objectives in different ways. This section will discuss some of the functions by which adware and spyware identify potential targets and attain their objectives.

Hijacked browsers

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 users' 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 result in the user downloading malicious code from the new page. Furthermore, a user might be redirected to a spoofed site and then prompted for personal information such as passwords, login IDs, financial information, or other confidential data. The data may then be used to commit identity theft or fraud.

Five of the top ten adware programs reported in the last six months of 2004 hijacked browsers, with Istbar being the most common. Spyware can also hijack browsers. The most commonly reported example of this functionality during the last six months of 2004 was Shopnay.

Users should deploy security software that intercepts attempted browser hijacking. Furthermore, as spyware can be placed on a user's computer by exploiting vulnerabilities, operating system patches should be kept updated.

Browser helper objects

BHOs are add-on programs that can add legitimate features to a user's browser;⁸² for example, document readers used to read files within the browser do so through 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. Between July 1 and December 31, 2004, three of the top ten adware programs, such as lefeats, used BHOs.

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, three of the top ten reported spyware programs, including Apropos, used BHOs.

Commercial monitoring tools

As has been established, spyware gathers information by logging keystrokes to obtain personal information, such as user names, passwords, instant messaging transactions, and emails. Many spyware programs are commercially produced and distributed monitoring programs, such as those employed in workplaces and public institutions to monitor users' Internet use. However, much of the spyware reported is not commercially produced.

Only one of the top ten spyware programs reported between July 1 and December 31, 2004, Perfect, was a commercial tool. As previously discussed, legitimate tools can often be used for malicious activities, such as keystroke logging, unauthorized viewing of email, and so on. As a result of those malicious activities, commercial programs may occasionally be included amongst spyware programs reported by customers to Symantec.

⁸² For instance, in Microsoft Internet Explorer versions 4.0 and higher.

As discussed previously, adware is used to gather information about browsing habits and preferences, to create targeted advertising. As such, most adware programs are commercially produced. Thus, it is not surprising that of the top ten adware programs reported during the last six months of 2004, all were commercially produced.

Adware and spyware—prevention and mitigation

Symantec recommends that users continue to update their antivirus software. Security administrators should also take extra measures to ensure that client system patch levels are up-to-date. Symantec also recommends that users and administrators employ defense in-depth, including the use of a properly configured firewall, as well as integrated antivirus and intrusion detection systems. Finally, Symantec advises users to exercise caution when installing any software via a Web browser and to not download software from sources that are not known and trusted.

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.

Finally, as some spyware is installed using ActiveX controls, Symantec recommends that users consider disabling ActiveX altogether. However, as was stated earlier in this discussion, 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. Finally, users should also consider disabling the acceptance of third party cookies.

One final note of caution should be raised. When removing spyware, Symantec recommends that users be extremely cautious. 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* looks at phishing attacks that have been conducted between July 1 and December 31, 2004. Phishing is an attempt by a third party to solicit confidential information from an individual, group, or organization, often for financial gain. Phishers attempt to trick users into disclosing personal data, such as credit card numbers, online banking credentials, and other sensitive information. They may then use it to commit fraudulent acts. In the last volume of the *Internet Security Threat Report*, Symantec identified phishing as one of the top threats to watch for in the coming months.⁸³

⁸³ Symantec *Internet Security Threat Report*, Volume VI (September 2004): p. 44
<http://enterprisesecurity.symantec.com/content.cfm?articleid=1539>

Phishing has evolved from simple attempts to obtain small items of information like gaming passwords to all-out identity theft. It may be conducted through email, spyware, and blended threats.⁸⁴ An example would be an attack that is propagated through an email that appears to come from a legitimate source (such as a bank), or a malicious Web site that has spoofed a legitimate site. When the email is viewed or the Web site visited, an executable (.exe) file is inserted onto the user's computer. The .exe file remains dormant until the user's browser attempts to access certain financial Web sites. It then begins saving data, such as user names and passwords, and transmitting it to the phisher's server.

Phishing attacks may also use spoofed email to trick users into entering confidential information into fraudulent Web sites or forms. Such phishing email often consists simply of a form that the user is requested to fill out and return. The email may appear to be from a legitimate source but it actually directs the victim to a malicious Web site. Browser vulnerabilities are often exploited so that a legitimate URL appears in the browser window when in fact the user is accessing a malicious Web site. The Web site may also be manipulated to make the lock icon appear in the lower right-hand side of the browser window, thereby misleading the user into believing that the Web site is secure when it is not. These Web sites often look exactly like the real ones, thereby tricking users into thinking that they are providing their confidential information to the legitimate site.

Among other tactics that phishers use are: schemes asking users to submit information via fax and phone; Java script that use legitimate Web sites to install pop-up windows, which are intended to trick users into submitting personal information; and injecting legitimate Web sites with malicious code that will load spyware onto an end users' system. Vulnerabilities in legitimate Web sites also allow phishers to serve spoofed phishing Web pages through the legitimate Web site or server.

This section discusses both phishing email messages as well as phishing attacks. A phishing email message is any single email message that is sent to a single, unique user that attempts to gain confidential and or personal information from online users. An attack is defined as a group of email messages that have been sent by the same user, with similar basic properties, in a single batch.

The data provided in this section is based on the statistics returned from the Symantec Probe Network, a system of over two million decoy accounts that attracts email messages from 20 different countries around the world. The Symantec Probe Network attracts spam samples that are representative of over 250 million mailboxes. Symantec's Probe Network has over 600 participating enterprises and ISPs in the Americas, Europe, Asia, and Australia. It consists of both formerly active email addresses as well as email accounts that have been generated solely for the purpose of attracting spam to the Symantec Probe Network.

This section will discuss the following:

- Six-month growth in phishing
- Blocked phishing attempts
- Volume of phishing messages
- Phishing prevention and mitigation

⁸⁴ A blended threat is a type of malicious code that uses multiple methods and techniques to propagate. Blended threats typically combine the characteristics of different types of malicious code (such as viruses, worms, and Trojan horse programs) as well as having the ability to exploit vulnerabilities.

Six-month growth in phishing

Because this is the first time that Symantec has analyzed phishing activity in the *Internet Security Threat Report*, it is not possible to offer a comparison between six-month periods. However, Symantec has analyzed the patterns of phishing behavior for the last six months of 2004.

Between July 1 and Dec. 31, 2004, 10,310 new phishing attacks were detected. While phishing activity was somewhat erratic on a week-to-week basis during this period, new phishing attacks increased consistently over the six-month reporting period (figure 30). (A moving average⁸⁵ was added to figure 30 to more clearly depict the growth in phishing attacks during this period.) During the first week of July, the Symantec Probe Network detected 193 new phishing attacks. This number rose fairly rapidly, reaching a peak of 584 new attacks during the week of October 7 to 13. The rate then slowed somewhat before climbing again in the final weeks of December, when 558 new phishing attacks were detected.

Within the security community, there has been a lot of discussion as to whether phishing is a fad or whether it will continue to grow. Looking at the numbers observed in the Symantec Probe Network, it would appear that phishing is not going away; rather, it will likely continue to increase. Symantec believes that this activity will continue to grow as phishers continue to spread their target base.

Blocked phishing attempts

The most effective measure of the rise of phishing is the total number of phishing attempts (that is, phishing email messages sent to end users) blocked in the field by Symantec Brightmail AntiSpam™ antifraud filters. (Antifraud filters are rules that are created by the Brightmail Logistics and Operations Center that target and block phishing email messages.) In mid-July 2004, antifraud filters were blocking 9 million phishing attempts per week. By the end of December this number had increased to a weekly average of over 33 million blocked messages (figure 31). (A moving average was added to figure 31 to make identification of the trends more apparent.)

The peaks in the weekly phishing attempts blocked (figure 31) are closely correlated to the peaks seen in new phishing attacks (figure 30). This is because as new phishing attacks are detected, Symantec is able to develop antifraud filters for those attacks, which in turn results in an increase in phishing attempts being blocked.

⁸⁵ A moving average is a technique used to allow trending analysis of highly volatile and dynamic data. Data that has a lot of fluctuations sometimes becomes difficult to assess and analyze visually. Each new day's or week's data are added to the average while the oldest data are removed, thereby moving the average over time. The amount of time used to calculate the moving average will directly affect how volatile the trend-line appears (shorter timeframes equate to greater volatility).

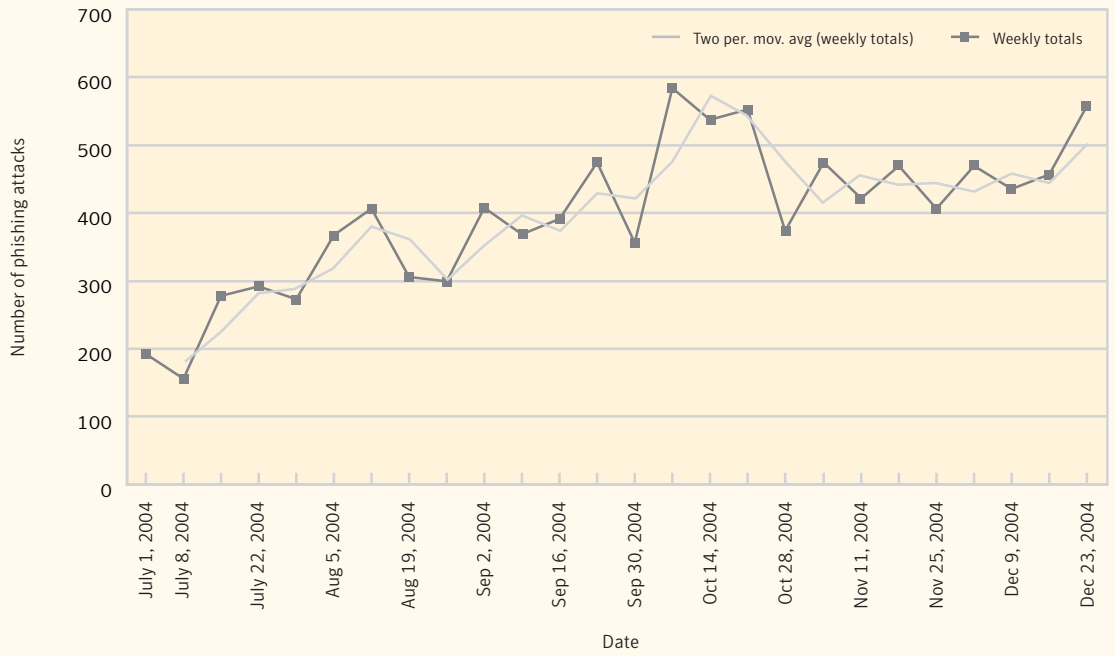


Figure 30. Weekly growth in phishing attacks
Source: Symantec Corporation

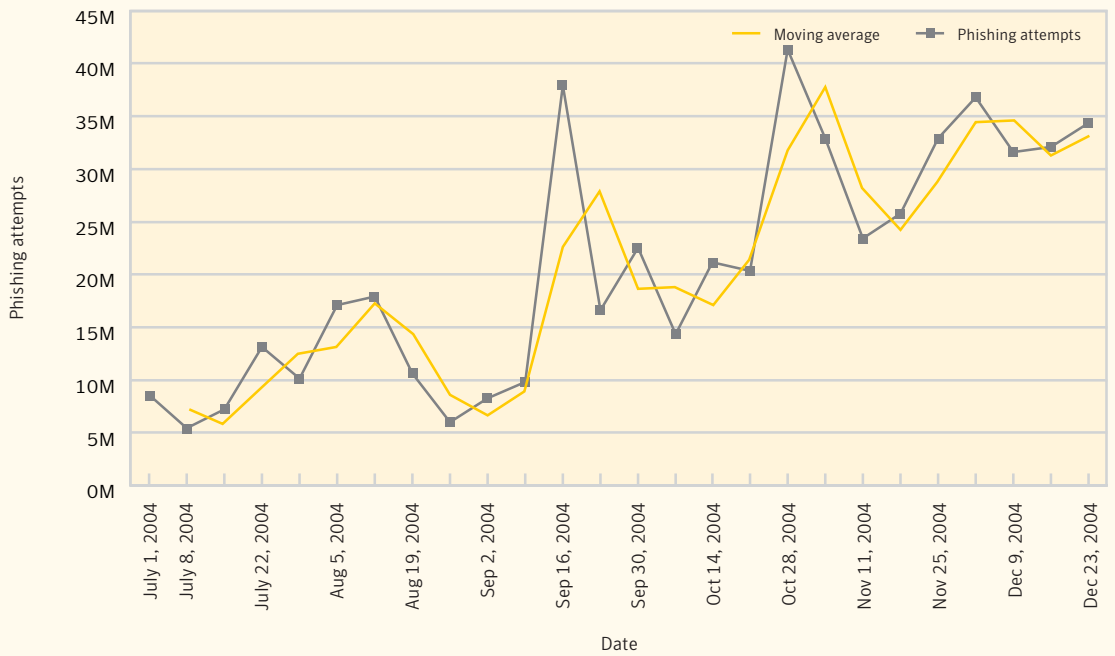


Figure 31. Blocked phishing attempts
Source: Symantec Corporation

Volume of phishing messages

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

Between July 1 and December 31, 2004, the percentage of messages that constitute phishing attempts increased. The volume of phishing messages rose from 0.1 % of the messages processed, or an average of 1 million fraud messages per day, to 0.6 % of the messages processed, an average of approximately 4.5 million fraud messages per day (figure 32). Peak days during this period experienced numbers well in excess of 9 million phishing messages per day.

Over this period the average percentage of phishing messages appearing in mail processed was 0.4%. While this figure may appear small, it means that 1 out of every 250 email messages received was a phishing attack. At the peak of activity recorded this was as high as 1 in 100 messages. This is quite a large jump, particularly considering that phishing was not considered a significant security threat as recently as two years ago.

This data supports the notion that phishing continues to grow, and will continue to grow in the foreseeable future. It is reasonable to conclude that phishers are actively seeking out and adding new targets for phishing attacks. The addition of new phishing targets (companies being phished) is a contributor to many of the spikes in this data, since there seems to be a slight lag in time from the point where a new target is phished to when that target is properly monitored for phishing attacks.

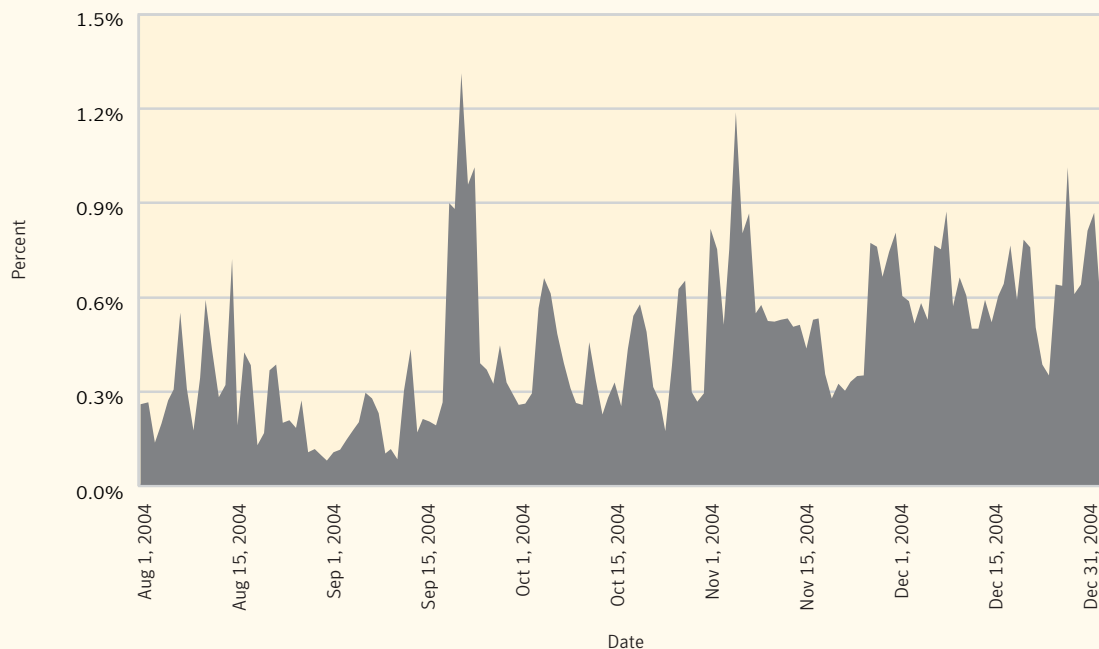


Figure 32. Phishing as a percent of messages scanned
Source: Symantec Corporation

Prevention and mitigation of phishing

Symantec recommends that enterprise users protect themselves against phishing threats primarily through the detection and filtering of email at the server level via the MTA (mail transfer agent). Although this level of filtering will likely remain one of the primary points at which filtering is performed for phishing, other attempts will be filtered utilizing upstream IP-based filtering, as well as providing filtering for HTTP. DNS block lists (DNSBLs) offer more general protection and may mitigate some of the risk of phishing emails; however, they frequently run the risk of false positives. Sender policy frameworks (SPFs), domain keys, and other similar solutions will not provide useful protection. Phishers can easily purchase domains that contain names similar to the targeted company and configure them to SPF and other standards to allow for their messages to be processed as SPF valid email.

General corporate best practices should also be followed, including Web log monitoring to make sure that complete Web site downloads are not occurring. Organizations may want to monitor cousin domain⁸⁶ 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. Symantec recommends that organizations ensure that their end users are educated about phishing in general, and are advised about the latest phishing scams.⁸⁷

End users should also follow best security practices. As some phishing attacks may utilize spyware and key loggers, Symantec advises end users to seek out software detection methods. Symantec also advises that end users never disclose any confidential personal or financial information if they have any doubts about the authenticity of an email or Web site requesting such information. They should never disclose sensitive information unless they can confirm that the request is legitimate.

Spam

In the last volume of the *Internet Security Threat Report*, Symantec projected that spam and risks associated with it would continue to rise.⁸⁸ Spam, usually defined as junk or unsolicited email from a third party, made up over 60% of all email traffic during this reporting period. 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 DoS 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 July 1 and December 31, 2004.

The data used in this analysis is based on data returned from the Symantec Probe Network. The Symantec Probe Network comprises millions of decoy email addresses that are configured to attract a large stream of spam attacks that are representative of spam 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 at Symantec Brightmail Logistics and Operation Centers (BLOCs) where anti-spam filters are produced.

⁸⁶ Cousin domains refers to domain names that include some of the key words of an organization's domain name. For example, for corporate domain "bigbank.com," cousin domains could include "bigbank-alerts.com," "big-bank-security.com", and so on.

⁸⁷ A good resource for information on the latest threats can be found at <http://www.antiphishing.org>

⁸⁸ Symantec *Internet Security Threat Report*, Volume VI (September 2004): p. 45
<http://enterprisesecurity.symantec.com/content.cfm?articleid=1539>

Symantec Internet Security Threat Report

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, the Probe Network is continuously optimized in order to attract new varieties of spam attacks. This is accomplished through internal production changes made to the Probe Network that affect the number of new spam attacks received by the Probe Network as a whole. All daily time periods are reported in Greenwich Median Time.

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

- Spam activity and growth projections
- Total messages from new attacks per day of the week
- Total messages versus existing spam attacks per day

Spam activity and growth projections

The data used in this analysis is based upon statistics reported from customers in the field. There are a large number of variables affecting email infrastructure and although best practices are frequently shared, the manner in which companies implement email security solutions is often unique to their particular situation. Different levels of email security will be deployed at the router, mail exchange (MX), or mail server levels. The point at which an antispam solution is deployed will have a direct impact on the statistics the system returns.

This section will assess spam activity and growth projections by categorizing the severity of a company's spam problem. Figure 33 identifies the spam growth of 20 companies that were experiencing extremely high percentages of spam for the month of July. The selected companies also had the largest total mail volumes (total mail volumes include the sum of all spam and non-spam email) during the month of July. The data represents this sampling of companies over a six-month period. There was little deviation in the email not filtered as spam (which includes legitimate email and a small percentage of undetected spam messages). Therefore the volume of legitimate email stayed fairly constant during the six-month period.

The purpose for selecting these companies is that the companies with the largest mail volumes have the lowest deviation in daily mail volumes. These companies also have more stringent change control policies on their email infrastructures, so there are fewer variables affecting the volume of mail being processed at the MTA level.

Between July 1 and December 31, 2004, there was a 77% growth in spam for these companies (figure 33). Companies experiencing significant spam problems continued to see a sharp increase in the amount of spam they received. The weekly totals of spam rose from an average of 800 million spam messages per week to well over 1.2 billion spam messages per week by the end of the six-month period.

Total messages from new attacks per day of the week

Between July 1 and December 31, 2004, the Symantec Probe Network received an average of 4,696,122 messages from new attacks (new groupings of probe email that are not currently tracked in the BLOC database) per day. Mondays brought a larger quantity of new attacks to the Probe Network than any other day of the week (figure 34). It could be speculated that spammers launch new tactics and subsequently send more attacks on Mondays. The number of total messages received by the Symantec Probe Network levels off during the remainder of the week, with another slight increase seen on Fridays.

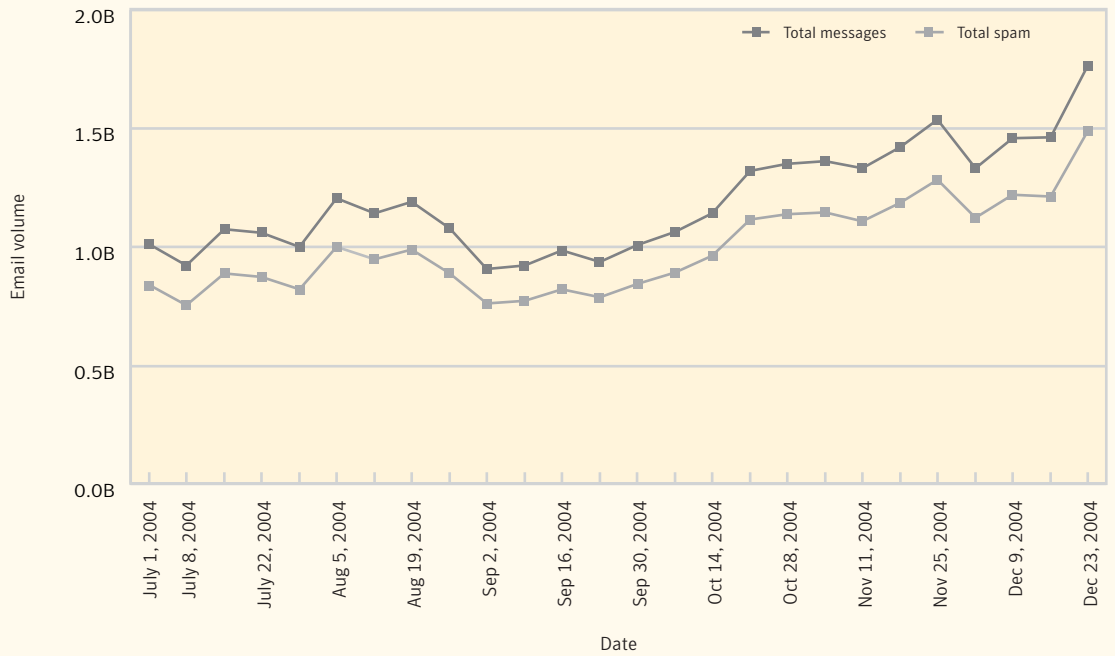


Figure 33. Weekly total spam for selected companies
 Source: Symantec Corporation

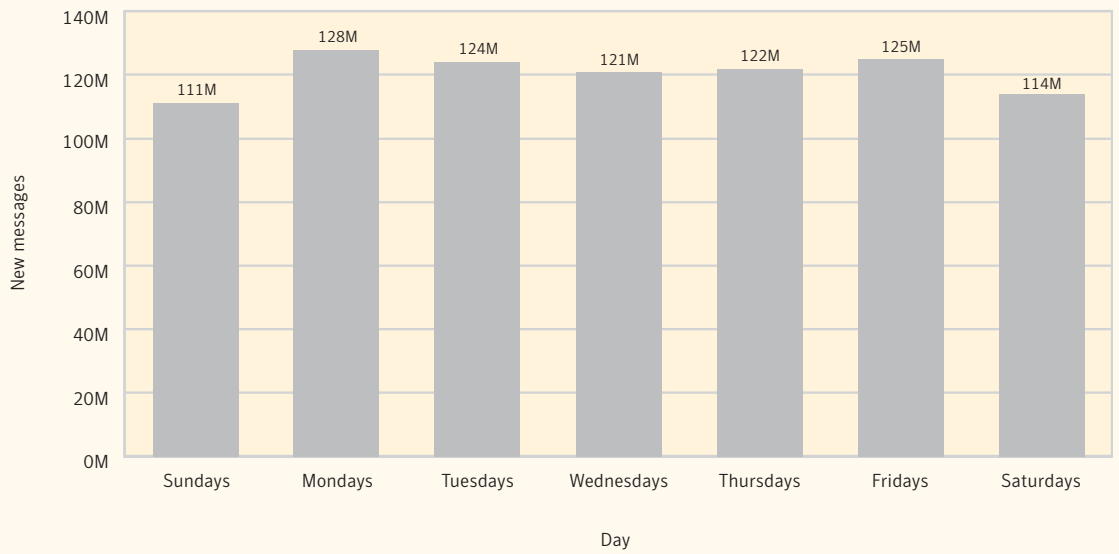


Figure 34. Total message from new attacks per day of week
 Source: Symantec Corporation

While Mondays brought more new spam attacks, the amount of change was small compared with total messages. The quantity of existing spam attacks—that is, attacks for which antispam filters have already been detected—remained relatively static throughout the week, with Wednesdays seeing a slight slump. Saturdays and Sundays account for the least spam quantities of the week.

Total messages versus existing spam attacks per day

Between July 1 and December 31, 2004, the Symantec Probe Network received an average of 11,069,154 total messages per day, including messages that may contain new, unknown spam messages (figure 35). (Unknown spam messages are synonymous with new spam attacks, or attacks that have not previously been tracked in the BLOC database). This compares with an average 6,373,032 messages from existing spam attacks.

Internal changes and optimizations to the Symantec Probe Network are apparent in this metric. As spam is continuously evolving, production changes to the Probe Network are necessary to keep pace. These changes consist of retiring poor spam-producing probes, as well as developing and activating new probes. These actions result in increased or decreased total quantity of email received by the Probe Network. This quantity is represented in dark gray in figure 35. The quantity of messages in existing spam attacks, protected with existing filters, is represented in light gray.

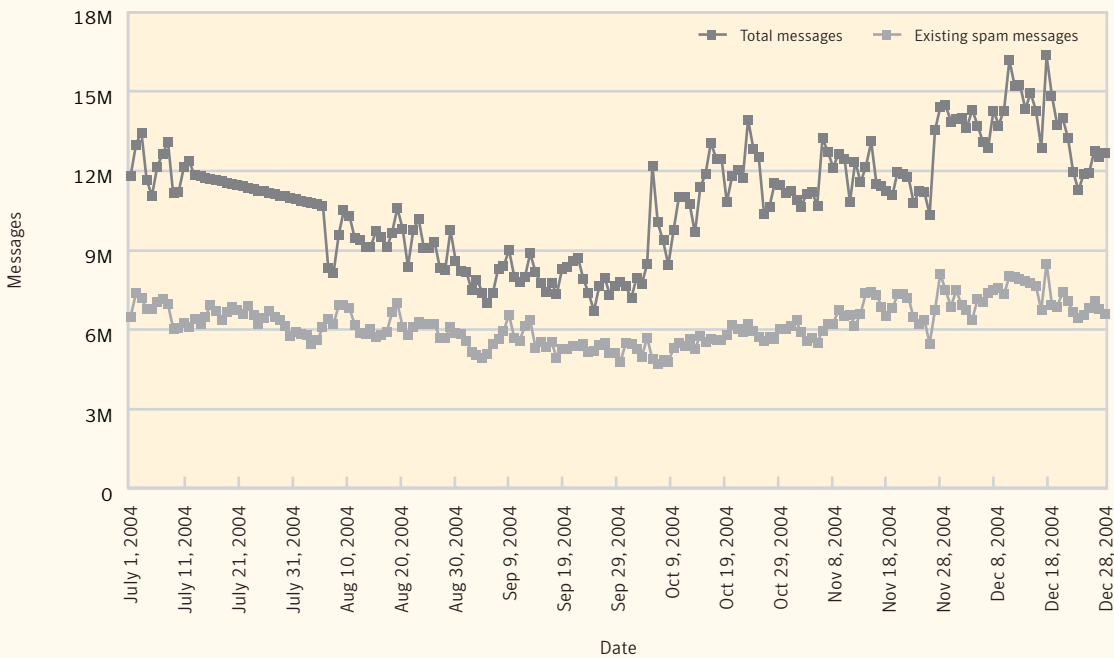


Figure 35. Total messages, including new spam attacks, compared with known spam messages
Source: Symantec Corporation

Symantec Internet Security Threat Report

Changes to the quantity of existing spam attacks were less dramatic than the changes in total messages received. These changes involve both acquiring more messages from new spam attacks and subsequently producing antispam filters against them. For this reason, this analysis can be used to gauge productivity associated with the Probe Network's quantity of email received, as well as filter production against new spam attacks. Additionally, the changes in volume of messages received by the Probe Network do not necessarily reflect growth trends of spam on the Internet, only to the new attacks being attracted by the Symantec Probe Network for the purpose of filter development.

The increasing number of new attacks detected over the last three months of this reporting period is also reflective of Symantec's expansion of the Probe Network into new geographic regions and increasing the Probe Network's coverage in specific countries. New probe accounts were initiated in early October 2004, consisting of many international and foreign language-attracting probes. The October activation of probes restored the total quantity of inbound probe messages to July levels, and another activation in late November increased the Probe Network's total messages again.

The drastic increase in total messages brought with it a wider variety of spam. Filter production against this new stream of spam attacks brought with it a gradual increase in messages filtered, or existing spam attacks, for the second half of the six-month period (October 1 to December 31, 2004).

The daily average of total messages and messages from existing attacks experienced very little growth over the six-month period (July 1 to December 31, 2004). The messages seen on July 1, 2004 totaled 11,822,284, compared to 12,671,366 total messages received on December 31, 2004. However, a 43% decline in total messages per day was experienced from July 1 to its lowest point of 6,704,900 total messages received on September 26.

One reason contributing to the decline in Probe Network messages during this six-month period was the refinement and deactivation of probes that were attracting a low volume of spam (or unacceptable volumes of inadvertent legitimate email). Initially, deactivating probes provides the Symantec BLOC more resources to focus filter production against a leaner collection of spam email received. The deactivation of poor probes, however, must be complemented by the activation of newly created probes in order to increase the trend of inbound spam attacks.

Future Watch

The previous sections of this report have discussed Internet security developments between July 1 and December 31, 2004. This section of the *Internet Security Threat Report* will discuss emerging trends and issues that Symantec believes will become prominent over the next year. These forecasts are based on emerging data that Symantec has collected during the current reporting period. In discussing potential future trends, Symantec hopes to provide organizations with an opportunity to prepare themselves for rapidly evolving and complex security issues.

Viruses and worms targeting client-side exploits

Over the past two reporting periods, Symantec has cautioned users to be wary of vulnerabilities in client software installed on both consumer and corporate desktops. As noted in the “Future Watch” section of the previous *Internet Security Threat Report* and discussed in greater detail in the “Vulnerability Trends” and “Malicious Code Trends” sections of this report, client-side exploits are becoming an increasing security concern.

Traditionally, the focus of security strategies has been on the network perimeter: servers, firewalls, and other assets with outward-facing exposure. However, a notable shift has occurred, with the security of client-side systems, primarily end-user desktop hosts, becoming increasingly important. This is because as administrators have become more effective in securing network perimeters, attackers have had to search for alternative entry points into targeted computing systems. As a result, vulnerability researchers and attackers are focusing more on client software installed on individual systems rather than on the underlying operating systems themselves. The Microsoft GDI+ Library JPEG Segment Length Integer Underflow Vulnerability⁸⁹ is a good example of this.

Symantec feels that the current shift towards client-side attacks will result in the use of worms as an initial propagation mechanism for attacks targeting specific vulnerabilities in client-side software. Viruses and worms are excellent ways for client-side attacks to propagate initially and Symantec believes that worms propagating by this method will become more common.⁹⁰ This could mean that traditional security mechanisms and procedures will become less effective at protecting networks as a whole. Administrators and end users alike will have to exercise extra vigilance to ensure that these new infection vectors are adequately secured.

Bots and bot networks for financial gain

As was discussed in the “Attack Trends” section of this report, although Symantec has observed a drop in the number of bot networks over the past six months, bot activity continues to be a source of concern. Symantec feels that the security threat from this form of attack will only get worse, especially in financial terms. In conjunction with a rise in the number of more sophisticated phishing and malicious code attacks, this edition of the *Internet Security Threat Report* noted that bots are increasingly used for financial gain. Symantec expects this trend to escalate, as the diverse means of acquiring new bots and developing bot networks become more prevalent.

⁸⁹ <http://www.securityfocus.com/bid/11173>

⁹⁰ <http://tms.symantec.com/ClientSideExploitation.asp>

It is very easy for an attacker to create a bot with very specific functions. Since it is also possible for bots to be remotely updated with new functionality, attackers can easily change the capabilities of their bot networks. This could allow the bot creators to modify their bot network for a variety of mercenary purposes. For instance, as was noted in the “Malicious Code Trends” section of this report, bots are frequently used as email relays in order to disseminate spam and phishing messages. In the near future, Symantec believes that it is reasonable to expect growth in the number of bot owners who modify their bot networks and rent them out for these purposes, amongst others.

Bots are frequently used to perform DoS attacks against various organizations.⁹¹ Bot networks have increasingly been used in online extortion schemes.⁹² In such schemes, the attacker contacts the owner of a Web site, usually an e-commerce site or online casino, and demands to be paid a sum of money. If these demands are not met, they threaten to launch a denial of service attack against the site, disrupting any income it may generate. Police reports and anecdotal evidence have suggested that this type of extortion has been known to be successful.⁹³ Because of the increasing sophistication seen in newer bots, these bot networks are becoming more difficult to shut down. Symantec believes that it is reasonable to conclude that this type of activity will increase in the near future.

More damaging mobile device malicious code in the wild

As noted in the previous edition of the *Internet Security Threat Report*, malicious code has been developed for mobile devices, namely a worm called Cabir.⁹⁴ As cellular telephones and PDAs become more sophisticated and mobile connectivity increases, the potential for more malicious code that affects them to be developed increases as well. Symantec feels that over the next six months, more malicious code of this nature will be seen in the wild.

In late December 2004, a Trojan was reported that would install the Cabir worm on mobile phones using the Symbian operating system.⁹⁵ This Trojan masqueraded as an installer for a popular video game in order to entice users into downloading and installing it on their phones. While not devastating in its effects, the Cabir worm demonstrated that more damaging payloads in malicious code of this type may be on the way. The SymbOS.Skulls Trojan,⁹⁶ which was released in November 2004, reinforced this notion. It not only replaced icons on the compromised mobile device but also caused most applications to no longer function.

In support of the theory that more dangerous and damaging exploits are on the horizon, the source code of the Cabir worm was publicly released in late December 2004.⁹⁷ Based on instances of various bots that have had their source code publicly released, Symantec expects to see numerous new variants of Cabir, or other malicious code based on its source code, released in the near future.

Until now, Cabir has been limited in its ability to propagate due to limitations and restrictions imposed by Symbian operating systems. However, the availability of source code could allow others to develop new variants that may be capable of bypassing these restrictions. With many groups researching vulnerabilities in Bluetooth-enabled devices,⁹⁸ the possibility that a worm or some other type of malicious code propagating by exploiting these vulnerabilities increases.

⁹¹ <http://www.securityfocus.com/news/9411>

⁹² http://www.theregister.co.uk/2004/07/21/cyber_shakedown_taken_down/

⁹³ http://www.businessweek.com/magazine/content/04_32/b3895106_mz063.htm

⁹⁴ <http://securityresponse.symantec.com/avcenter/venc/data/epoc.cabir.html>

⁹⁵ <http://www.symantec.com/avcenter/venc/data/symbos.mgdrops.html>

⁹⁶ <http://securityresponse.symantec.com/avcenter/venc/data/symbos.skulls.html>

⁹⁷ http://www.theregister.co.uk/2004/12/29/cabir_code_unleashed/

⁹⁸ <http://www.securityfocus.com/archive/1/371443> and http://trifinite.org/trifinite_stuff.html

Embedded content processing in audio and video images

On September 14, 2004, Microsoft announced a vulnerability⁹⁹ in its implementation of the JFIF (JPEG) image file format. The vulnerability potentially allowed for malicious image files to cause code to be executed on the host displaying the image. Eight days later, functional exploit code for the vulnerability was published. Exploitation of this vulnerability by malicious code in the wild was seen shortly afterwards.¹⁰⁰

Until this time, image files have generally been considered relatively trustworthy, even when embedded in externally originating content such as Web pages and HTML email messages. Image data files, particularly compressed images such as JPEGs, are complex data formats that require complicated code to render. Greater complexity usually means more potential vulnerabilities to be discovered. Several image file format implementations, such as those for PNG and TIFF, contain vulnerabilities.

This is worrisome because image files are ubiquitous, almost universally trusted, and an integral part of modern day computing. For example, users browsing a trusted Web site, such as an online auction site, could be victimized by a maliciously crafted image uploaded to the Web site, which in turn could lead to the user's system being compromised. The exploitable vulnerabilities found in image file format implementations give rise to concern about other embedded or externally originating data, such as audio and video files.

The discovery of these vulnerabilities highlights the shift from perimeter attacks to client-side attacks that is discussed throughout this volume of the *Internet Security Threat Report*. Symantec believes that attackers will continue to harvest the vulnerabilities in code for processing complex data formats, such as audio and video files, in an attempt to find new vectors of attack against client-side systems.

Unauthorized third-party bundling of Trojans with software

With the increase in popularity of open source software packages over the past few years, a disturbing trend has begun to emerge. In 2002, back doors were discovered in several popular open source software packages, such as Sendmail¹⁰¹ and Fragrouter.¹⁰² More recently, in late 2003, an attempt to place a back door in the Linux kernel was discovered.¹⁰³ Since then, there have been very few discoveries of surreptitious Trojans embedded in publicly available software, whether open or closed source.

It is unlikely that all software distribution points have become completely secure and untainted, or that attackers—internal or external—have collectively decided not to back door software. Rather, Symantec feels it is likely that back doors inserted into software at certain (perhaps stale) distribution sites persist and remain undiscovered. The possibility of back door code being slipped into downloadable software bundles continues to remain a very real threat for users of all platforms.

The large number of mirror Web sites¹⁰⁴ and FTP servers hosting copies of applications and packages is especially worrisome. Compounding the problem is that most operating systems rely on regular downloads of updated packages from Web sites or mirror sites. The authenticity of most downloadable software, such as popular shareware applications, often cannot be verified, particularly as very few closed source vendors or authors provide digital signatures¹⁰⁵ of their packages.

⁹⁹ <http://www.microsoft.com/technet/security/bulletin/ms04-028.msp>

¹⁰⁰ <http://securityresponse.symantec.com/avcenter/venc/data/trojan.ducky.html>

¹⁰¹ <http://www.securityfocus.com/bid/5921/info/>

¹⁰² <http://www.securityfocus.com/archive/1/296407>

¹⁰³ <http://www.securityfocus.com/news/7388>

¹⁰⁴ Mirror sites are software repositories that are spread out geographically to balance downloading of software packages. Mirror sites contain exact replicas of software hosted on the primary site.

¹⁰⁵ Digitally signed packages ensure end users that the software they are downloading has not been tampered with or altered.

Open source developers are generally better in providing verification mechanisms such as MD5,¹⁰⁶ although there are concerns that these too are vulnerable to attack.¹⁰⁷ Further, even though some have automated authentication of downloaded updates, many do not. Any of these servers, if compromised, could potentially distribute maliciously modified software and could remain undetected until many networks and individual computers have become compromised.

Symantec is concerned that a major back door will be discovered implanted in a popular application or software repository. This may serve as a wake-up call for consumer and enterprise users to verify both the integrity and authenticity of downloaded software prior to installation.

Emerging security concerns for Mac OS

Generally speaking, the Macintosh® operating system has been relatively immune to malicious activity, particularly compared to other operating systems like Linux and Microsoft. With the introduction and popularity of Mac OS X, however, Apple® Computer has become a target for new attacks and vulnerabilities. With a newly designed operating system based on a BSD-UNIX lineage, Mac OS X has begun to not only capture the attention of users but of vulnerability researchers as well.

Over the past year, Symantec has documented 37 high-severity vulnerabilities in Mac OS X.¹⁰⁸ These vulnerabilities have been confirmed by the vendor, which, in the Apple case, almost always means that the company has released a patch. The appearance of a rootkit¹⁰⁹ called Opener in October 2004,¹¹⁰ serves to illustrate the growth in vulnerability research on the OS X platform. Additionally, multiple remote and local vulnerabilities¹¹¹ have been disclosed that affect both the server and desktop versions of OS X.

Vulnerabilities in the Apple windowing system and development kit and in the Apple default Apache configurations are two of the nine vulnerabilities (not all of which were high severity) for which Apple released patches. The various OS X vulnerabilities allow attackers to carry out information disclosure, authentication bypass, code execution, privilege escalation, and DoS attacks.

Contrary to popular belief, the Macintosh operating system has not always been a safe haven from malicious code.¹¹² Out of the public eye for some time, it is now clear that the Mac OS is increasingly becoming a target for the malicious activity that is more commonly associated with Microsoft and various UNIX-based operating systems. Symantec believes that as the popularity of Apple's new platform continues to grow, so too will the number of attacks directed at it.

The market penetration of Macintosh platforms will be accelerated by the much lower priced Mac® mini, which may be purchased by less security-savvy users. As a result, the number of vulnerabilities can be expected to increase, as will malicious activity that targets them. However, it should be stated that while the number of vulnerabilities in Macintosh operating systems is expected to increase, they will likely be outnumbered by vulnerabilities in other operating systems for some time to come.

¹⁰⁶ <http://userpages.umbc.edu/~mabzug1/cs/md5/md5.html>

¹⁰⁷ <http://www.securityfocus.com/archive/1/383574>

¹⁰⁸ Examples of some of these vulnerabilities can be found at <http://www.securityfocus.com/bid/11802/info/>

¹⁰⁹ A rootkit is a collection of tools designed to allow hackers unfettered access to a computer system, often in a manner that avoids detection by others.

¹¹⁰ <http://www.securityfocus.com/news/9796>

¹¹¹ <http://www.securityfocus.com/bid/11802>

¹¹² <http://www.faqs.org/faqs/computer-virus/macintosh-faq/>

Combating adware and spyware with legislation—the problems

As discussed in the “Additional Security Risks” section of this *Internet Security Threat Report*, adware and spyware represent serious threats to privacy and confidentiality, as well as identity security. Symantec is concerned that as adware and spyware become more prominent, legislation¹¹³ designed to protect against illegitimate usage of these programs will prove to be an insufficient deterrent.

Over the next six months, the functionality and distribution of adware will come under increasing scrutiny by groups concerned with privacy. It is expected that in the near future standards related to adware will evolve that will center on EULAs, product uninstall capabilities, and the level of stealth with which these programs install themselves on a user’s system. Another issue is the fact that some of them stubbornly resist normal removal procedures.

Symantec expects that the bundling of adware with other programs will grow as a viable method of installing adware. The explosion in adware over the past few years would suggest that its return on investment is relatively good. As such, Symantec feels that this will continue to drive the creation and implementation of adware despite legislation aimed at curbing these technologies. Such laws are not expected to be effective. The transboundary nature of the Internet creates serious jurisdictional issues; particularly as distribution activity may take place in locations not subject to jurisdiction of such laws. As such, adware could easily become more problematic for users, as prosecution will rely on jurisdictional cooperation, which is not always forthcoming.

The risks from spyware will also continue to grow, compromising privacy and confidentiality and increasing the risk of identity theft. This can present a challenge to corporations as well as end users. Victims must deal with the aftermath of a compromise not only at the technical, but also at operational levels: for instance, by getting new credit cards, reviewing and correcting credit reports, challenging credit card charges, and tracking other uses of the stolen data.

¹¹³ http://www.leginfo.ca.gov/pub/03-04/bill/sen/sb_1401-1450/sb_1436_bill_20040928_chaptered.html

Appendix A—Symantec Best Practices

Enterprise best practices

1. Turn off and remove unneeded services.
2. If a blended threat exploits one or more network services, disable, or block access to, those services until a patch is applied.
3. Always keep your patch levels up-to-date, especially on computers that host public services and are accessible through the firewall, such as HTTP, FTP, mail, and DNS services.
4. Enforce a password policy.
5. Configure your email server 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.
6. Isolate infected computers quickly to prevent further compromising your organization. Perform a forensic analysis and restore the computers using trusted media.
7. 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.
8. Ensure emergency response procedures are in place.
9. Educate management on security budgeting needs.
10. Test security to ensure adequate controls are in place.
11. Both spyware and adware can be automatically installed on systems along with file-sharing programs, free downloads, and freeware and shareware versions of software, 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 passwords are a mix of letters and numbers. Do not use dictionary words. Change passwords often.
4. Never view, open, or execute any email attachment unless the 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 a Web site designed to look like 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 computer 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 to perform malicious attacks and 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 end user license licensing agreements (EULAs). Some spyware and adware applications can be installed after, or as a by-product of, accepting the EULA. Read them carefully to examine what they mean in terms of privacy. The agreement should clearly explain what the product is doing and provide an uninstaller.
12. Beware of programs that flash ads in the user interface. Many spyware programs track how you respond to these ads, and their presence is a red flag. 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 use a common naming convention for types of attacks, enabling analysts to combine and analyze attacks together or separately. Symantec combines these two data sources for analysis when appropriate—that is, when they both contain the attributes required for the particular analysis. In some cases, only one data source is used if attributes required for a particular analysis are not available in the other. Table 9 provides high-level details of the methods used by each service.

Data source	Data collection methodology	Percent of companies in sample set
Symantec DeepSight Threat Management System	Symantec DeepSight Threat Management System collects IDS and firewall events from more than 20,000 security devices deployed in more than 180 countries.	60%
Symantec Managed Security Services	Symantec Managed Security Services provides real-time monitoring and analysis of attack activity launched against companies worldwide. Due to the nature of monitoring activity, some statistics, such as event severity, client tenure, and attacks per company only apply to data received from Symantec Managed Security Services customers.	40%

Table 9. Data collection methods used by Symantec

Attack definitions

In order to avoid ambiguity with our findings, 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. Rather than limiting the analysis to only one metric of attack activity, Symantec uses several different metrics, each of which is appropriate under a certain set of circumstances. A high-level summary of the distinctions used in the report is used below.

Attacks—Attacks are individual signs of malicious network activity. Attacks can consist of one or more IDS or firewall alerts that are indicative of a single type of attacker action. For example, multiple firewall logs often indicate the occurrence of a single network scan. The attack metric is the best indicator of the overall volume of actual “attacker actions” detected over a specified period of time.

Worm Attacks—In order to better draw conclusions regarding attack trends, activity related to autonomously propagating worms has been identified. An absolute verification of the origin of some activity is often impossible, as certain scans from networks containing a Trojan horse will look identical to a worm attempting to propagate. The decision of whether traffic originates from a worm is a judgment based on the origin of the majority of the traffic.

Events—Security events are logical groupings of multiple attacks. “Event” is a term that is used only by Symantec Managed Security Services. A security event may include a group of similar, but non-threatening individual attacks experienced by companies during the course of a day (for example, all non-threatening HTTP scans experienced during a single day are grouped into an event). A security event may also include multiple attacks against a single company by a single attacker during a specified period of time. Security events are generated only by the Symantec Managed Security Service, and are only used in this report when discussing “Severe Event Incidence.”

Event Severity

Event severity is only applicable to data generated by Symantec Managed Security Services. Every event validated by Symantec security analysts is assigned to one of four severity classifications: informational, warning, critical, and emergency (table 10). The primary purpose of this rating system is to prioritize client responses to malicious activity based on the relative level of danger that the event presents to their environment.

A determination of severity is based on characteristics of an attack, defensive controls of the client, value of the assets at risk, and the relative success of the attack. These four severity levels are further grouped into two classifications: severe and non-severe events. Severe events include activity classified as either “emergency” or “critical,” while non-severe events include activity classified as either “informational” or “warning.” For example, a severe event requires immediate countermeasures from an organization, while a non-severe event is mainly informative.

Severity	Classifications	Definitions
Non-severe	Informational	Events consisting of scans for malicious services and IDS events that do not have a significant impact on the client’s network. <i>Example:</i> Scans for vulnerable services where all connection attempts are dropped by the firewall.
	Warning	Events consisting of malicious attacks that were unsuccessful in bypassing the firewall and did not compromise the intended target systems. <i>Example:</i> Scans and horizontal sweeps where some connections were allowed, but a compromise has not occurred.
Severe	Critical	These events are malicious in nature and require action on the part of Symantec or the client to fix a weakness or actual exploit of the client network or devices. By definition, if a critical event is not addressed with countermeasures, it may result in a successful compromise of a system. <i>Examples:</i> (1) Continuous attacks by a single IP address against the client network or a significant vulnerability on the client’s network that was identified by either an attacker or the Symantec Managed Security Services Security Operations Center (SOC). For example, a Web exploit is observed and appears to be successful, but there is no observed follow-up activity to take advantage of the vulnerability. (2) Unknown suspicious traffic that warrants an investigation by the client to track or eliminate the traffic flow.
	Emergency	These events indicate that a security breach has occurred on the client’s protected network. An emergency event requires the client to initiate some form of recovery procedure. <i>Example:</i> Successful exploit of a vulnerable Web server.

Table 10. Severity classifications

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.

Daily attack rate

Symantec uses a daily attack rate as a rough estimate of the rate of attack activity experienced by networks connected to the Internet. This attack rate will be highly determinative of a large number of factors but is an indicator of whether the attack rates are rising or falling from between sample periods.

Previous volumes of the *Internet Security Threat Report* have used the average number of attacks detected by Symantec Managed Security Services and Symantec DeepSight Threat Management System sensors to gather this data. However, the mean average of this data could potentially be skewed if a small number of organizations received a disproportionately high number of attacks. To mitigate this possibility, the median average for all contributing data sensors was used. This approach more accurately represents the variations in attack volume over time that a typical network (in size and defensive deployment) may see.

Top Internet attacks

Symantec identified and ranked the top attacks seen on networks across the Symantec DeepSight Threat Management System and Symantec Managed Security Services base. This ranking does not differentiate between worm and non-worm-related attacks; instead, it can be seen as indicative of the distribution of attacks that an Internet-connected host can be expected to observe. Where certain attacks are strongly associated with worm activity, it is noted in the text.

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 a given attack.

Included in this report is the proportion of attacking IP addresses that perform a given attack.

Top attacked ports

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

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

- 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 a given attack.

Included in this report is the proportion of attacking IP addresses that perform a given attack.

Bot networks and denial of service activity

Symantec identifies certain scanning patterns and observed network traffic and correlates this traffic to rules that define specific coordinated scanning behavior. For an originating computer to be flagged as participating in this coordinated scanning, indicative of a bot network, it must fit into that scanning pattern to the exclusion of any other activity. This behavioral matching will not catch every bot network infected computer, and may identify other malicious code behaving in a coordinated way as a bot network. Denial of service activity is summarized by analyzing the backscatter from denial of service attacks that utilize spoofed source addresses.

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.

Attacks per Internet capita

The number of Internet users was obtained from the *CIA World Factbook 2004*. The *CIA World Factbook* provides a breakdown of the number of Internet users per country.

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 36 represents the industry breakdown of the sample set in percentage terms. Industries with less than ten sensors have been excluded from the resulting totals.

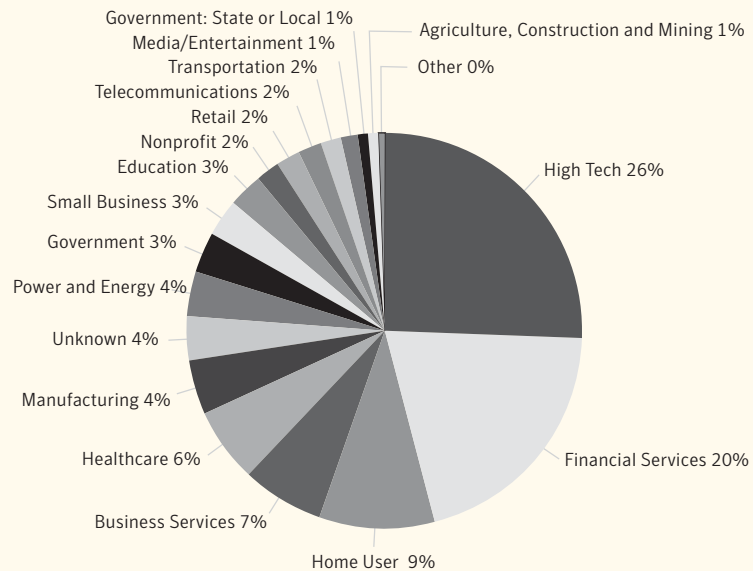


Figure 36. Attack activity by industry
Source: Symantec Corporation

Attack severity by industry

The Symantec Managed Security Services infrastructure allows ranking of attacks based on severity of attacks. Symantec analysts classify attacks for severity according to the attack being performed, exposure of the victim to the attack, and indications as to whether it was successful.

Targeted industry attack rate

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.

Appendix C—Vulnerability Trends Methodology

The “Vulnerability Trends” section 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 9,000 distinct entries. The information presented in the “Vulnerability Trends” section is based on the analysis of that data by Symantec researchers.

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),¹¹⁴ 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

¹¹⁴ “Use of a Taxonomy of Security Faults” <http://ftp.cerias.purdue.edu/pub/papers/taimur-aslam/aslam-krsul-spaf-taxonomy.pdf>

Severity

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 systems 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 via 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 3 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	$X \geq 7$
Moderate	$4 \leq X < 7$
Low	$x < 4$

Table 11. Measurement of severity level
Source: Symantec Corporation

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**—Sophisticated 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 sophisticated 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 the following:

- Vulnerabilities that Symantec considers to be of sufficient complexity,¹¹⁵ and that did not have functional exploit code until it was created by a third party.

Excluded are:

- 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 delta between vulnerability disclosure and appearance of exploit code for each applicable vulnerability is determined and computed into a monthly average.

¹¹⁵Memory 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

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. The following caveats should be kept in mind when interpreting the data:

- 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 their own right. This may distort the total vulnerability count.
- Not every vulnerability discovered is exploited. As of this writing, there has been no widespread exploitation of any browser except Microsoft Internet Explorer. This is expected to change as other browsers become more popular.
- Firefox is a relatively new browser. It is not represented in the data sets prior to the current reporting period.

Appendix D—Malicious Code Trends Methodology

The trends in the “Malicious Code Trends” section are based on statistics from malicious code samples reported to Symantec for analysis. Symantec gathers data from over 120 million client, server, and gateway systems that have deployed Symantec’s antivirus products in both consumer and corporate environments. The Symantec Digital Immune System and Scan and Deliver technologies allow customers to automate this reporting process.

Observations in the “Malicious Code Trends” section are based on empirical data and expert analysis. 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 reveal 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 variances between some reports in the previous edition of the *Internet Security Threat Report* and the current edition.

Appendix E—Additional Security Risks Methodology

Symantec products help users to protect their data not only 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 with another software program and meets the following criteria:

1. Is considered to be non-viral in nature.
2. Meets criteria for programmatic functionality having potential to impact security.
3. Has been submitted to Symantec for detection 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 criterion considers stealth, privacy, performance impact, damage, and removal.

The trends in the "Additional Security Risks" section are based on Symantec's ongoing research, reports from customers, and data from over 120 million client, server, and gateway systems that have deployed Symantec's products,¹¹⁶ as well as filtration of 25 million email messages per day by the Symantec Probe Network. Symantec then analyzes the top reports and analyzes which of these are, in fact, adware and spyware as opposed to malicious code.

In this discussion, adware and spyware are discussed according to samples, or individual cases of adware or spyware. However, in some cases, a particular sample may have multiple variants. A variant is a new iteration of the same family that may have minor differences but is still based on the original. For the purposes of this report, all variants of a sample of adware or spyware are treated as a single sample.

Phishing methodology

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

Attack definition

Symantec Probe Network data is used to track the growth in new attacks. A fraud attack is a group of email messages with similar messages sent to a unique user. The messages attempt to gain confidential and or personal information from online users. Symantec Brightmail AntiSpam field data is used to identify general trends in phishing email messages.

The following table provides high-level details of the methods used by each service.

Data source	Data collection methodology
Symantec Probe Network	The Symantec Probe Network has over 2 million probes with a statistical reach of over 250 million mailboxes. It is a vast array of email addresses (formerly live users as well as email accounts that have been generated solely for this purpose) that attracts junk email. Symantec's Probe Network has over 600 participating enterprises and ISPs. The reach of the Probe Network covers countries in the Americas, Europe, Asia, and Australia.
Symantec Brightmail AntiSpam field data	Symantec Brightmail AntiSpam software reports statistics to the Brightmail Logistics and Operations Center (BLOC) indicating messages processed, messages filtered, and filter specific data. Symantec has classified different filters so that spam statistics as well as phishing statistics can be separately determined.

Table 12. Phishing data collection methods

Source: Symantec Corporation

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.

Growth in phishing rate

Symantec maintains automated systems to identify new potential fraud attacks 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 fraud. The Brightmail Logistics and Operations Center (BLOC) reviews attacks that are identified for confirmation and filter development. The Symantec Brightmail Business Intelligence department reviews phishing attacks in order to develop predictive filters (Symantec Brightmail AntiSpam Heuristics).

The data presented in this section is based on weekly totals in the number of new phishing attacks ruled upon by the BLOC. The BLOC addresses only those phishing attacks not caught by existing antispam and antifraud filters. Existing filters refers 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 the BLOC for the development of filters that are more widely dispersed.

Spam

Spam trends in this report are based on the analysis of data derived from the Symantec Probe Network. Symantec Brightmail AntiSpam field data is utilized to gauge the growth in spam. Symantec Brightmail AntiSpam field data consists of statistics reported back from customer installations providing feedback as to firing characteristics of anti-spam filters as well as overall mail volume being processed.

Sample customer base

Due to the numerous variables influencing a company's spam activity, Symantec focused on identifying spam activity and growth projections based upon categorizing the severity of a company's spam problem. The sample customer base (20 companies) was selected from those companies experiencing spam rates exceeding 75% of their mail volume in the month of July. The selected companies also had the largest mail volume during the month of July. The data represents weekly totals over a six-month period for the combined message traffic of the 20 sample customers. The table below provides high-level details of the methods used by each service.

Data source	Data collection methodology
Symantec Probe Network	The Symantec Probe Network has over 2 million probes with a statistical reach of over 250 million mailboxes. It is a vast array of email addresses (formerly live users as well as email accounts that have been generated solely for this purpose) that attracts junk email. Symantec's Probe Network has over 600 participating enterprises and ISPs. The reach of the Probe Network covers countries in the Americas, Europe, Asia, and Australia.
Symantec Brightmail AntiSpam field data	Symantec Brightmail AntiSpam software reports statistics to the BLOC indicating messages processed, messages filtered, and filter specific data. Symantec has classified different filters so that spam statistics as well as phishing statistics can be separately determined.

Table 13. Spam data collection methods
Source: Symantec Corporation

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

Symantec, the Symantec logo, Brightmail, and DeepSight are U.S. registered trademarks of Symantec Corporation. Brightmail AntiSpam, BugTraq, Digital Immune System, Symantec AntiVirus, Symantec AntiVirus Research Automation (SARA), Symantec Managed Security Services, and Symantec Security Response are trademarks of Symantec Corporation. Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation. Macintosh, Mac, and Mac OS are registered trademarks of Apple Computer, Inc. Linux is a registered trademark of Linus Torvalds. Other brands and products are trademarks of their respective holder/s. Copyright © 2005 Symantec Corporation. All rights reserved. Any technical information that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

About Symantec

Symantec is the global leader in information security, providing a broad range of software, appliances, and services designed to help individuals, small and mid-sized businesses, and large enterprises secure and manage their IT infrastructure.

Symantec's Norton brand of products is the worldwide leader in consumer security and problem-solving solutions.

Headquartered in Cupertino, Calif., Symantec has operations in more than 35 countries.

More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 800 745 6054

Symantec Corporation
World Headquarters
20330 Stevens Creek Blvd.
Cupertino, CA 95014 U.S.A.
1 408 517 8000
1 800 721 3934
www.symantec.com

Copyright © 2005 Symantec Corporation. All rights reserved. Any technical information that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation. 03/05 10395235