



# Symantec Internet Security Threat Report

## Trends for July 05–December 05

Volume IX, Published March 2006

### Executive Summary

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

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

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

**Dean Turner**  
Executive Editor  
Symantec Security Response

**Marc Fossi**  
DeepSight Threat Analyst  
Symantec Security Response

**David Cowings**  
Sr. Business Intelligence Manager  
Symantec Business Intelligence

**Eric Chien**  
Security Researcher  
Symantec Security Response

**Stephen Entwisle**  
Editor  
Symantec Security Response

**Daniel Hanson**  
DeepSight Threat Analyst  
Symantec Security Response

**Dylan Morss**  
Principal Business Intelligence Analyst  
Symantec Business Intelligence

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

**Oliver Friedrichs**  
Technical Advisor  
Symantec Security Response

**Sarah Gordon**  
Sr. Principal Research Engineer  
Symantec Security Response

**Brad Bradley**  
Sr. Business Intelligence Analyst  
Symantec Business Intelligence

**Jesse Gough**  
DeepSight Threat Analyst  
Symantec Security Response

**David Ahmad**  
Manager, Development  
Symantec Security Response

**David Cole**  
Director, Product Management  
Symantec Security Response

**Peter Szor**  
Security Architect  
Symantec Security Response

**Josh Talbot**  
DeepSight Threat Analyst  
Symantec Security Response

**Joseph Blackbird**  
Assoc. Software Engineer  
Symantec Security Response

## Symantec Internet Security Threat Report

### ***Attack Trends Highlights***

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

### ***Vulnerability Trends Highlights***

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

### **Malicious Code Trends Highlights**

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

### **Additional Security Risks Highlights**

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

<sup>1</sup> See <http://www.newscientist.com/channel/info-tech/mg18725125.900> and [http://www.theregister.co.uk/2004/07/21/cyber\\_shakedown\\_taken\\_down/](http://www.theregister.co.uk/2004/07/21/cyber_shakedown_taken_down/) for instance.

## **Symantec Internet Security Threat Report Overview**

The *Symantec Internet Security Threat Report* provides a six-month update of Internet threat activity. It includes analysis of network-based attacks, a review of known vulnerabilities, and highlights of malicious code and additional security risks. This summary of the current report will alert readers to current trends and impending threats. In addition, it will offer recommendations for protection against and mitigation of these concerns. This volume of the *Internet Security Threat Report* covers the six-month period from July 1 to December 31, 2005.

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

Symantec also maintains one of the world's most comprehensive databases of security vulnerabilities, covering over 13,000 vulnerabilities affecting more than 30,000 technologies from over 4,000 vendors. In addition to the vulnerability database, Symantec operates BugTraq,™ one of the most popular forums for the disclosure and discussion of vulnerabilities on the Internet. Finally, the Symantec Probe Network, a system of over two million decoy accounts, attracts email messages from 20 different countries around the world, allowing Symantec to gauge global spam and phishing activity.

These resources give Symantec analysts unparalleled sources of data with which to identify emerging trends in attacks and malicious code activity. The *Symantec Internet Security Threat Report* is grounded principally on the expert analysis of this data. Based on Symantec's expertise and experience, this analysis yields a highly informed commentary on current Internet threat activity. By publishing the analysis of Internet security activity in the *Symantec Internet Security Threat Report*, Symantec intends to provide enterprises and consumers with the information they need to help effectively secure their systems now and in the future.

### **Threats to confidential information**

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

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

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

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

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

### **Web application vulnerabilities**

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

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

As the number of Web application vulnerabilities grows, Symantec believes that they may serve as an increasingly attractive target for potential attackers to exploit. Organizations should manage their Web-based assets carefully. If they are developing Web applications in-house, developers should be educated about secure development and the use of secure shared components. If possible, all Web applications should be audited for security prior to deployment. Web application security solutions and a number of products and services are available to detect and prevent attacks against these applications.<sup>4</sup>

### **Web browser vulnerabilities**

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

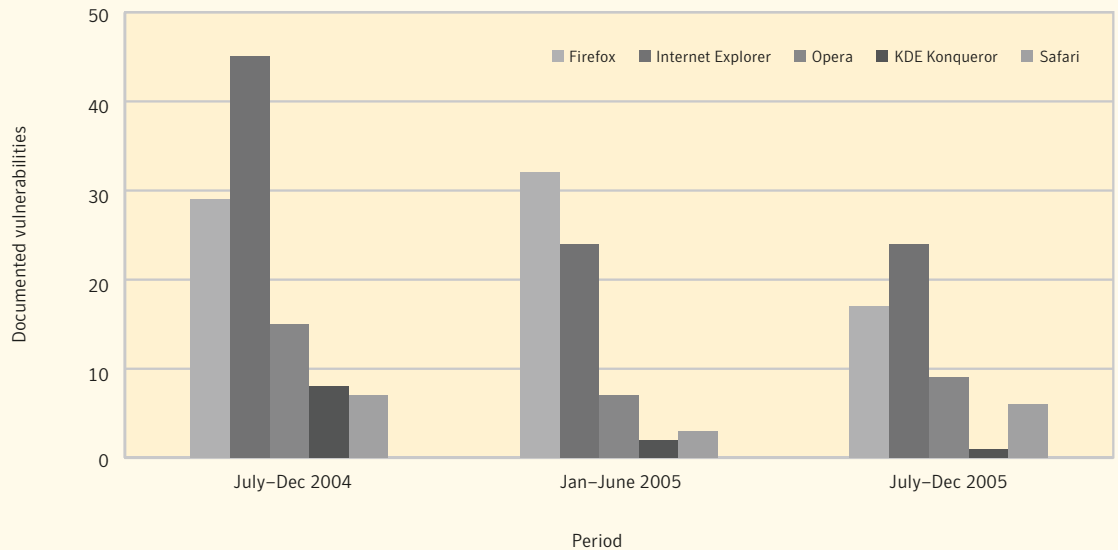
<sup>2</sup> <http://securityresponse.symantec.com/avcenter/venc/data/pwsteal.bancos.html>

<sup>3</sup> <http://securityresponse.symantec.com/avcenter/venc/data/pwsteal.banpaes.html>

<sup>4</sup> <http://www.owasp.org>

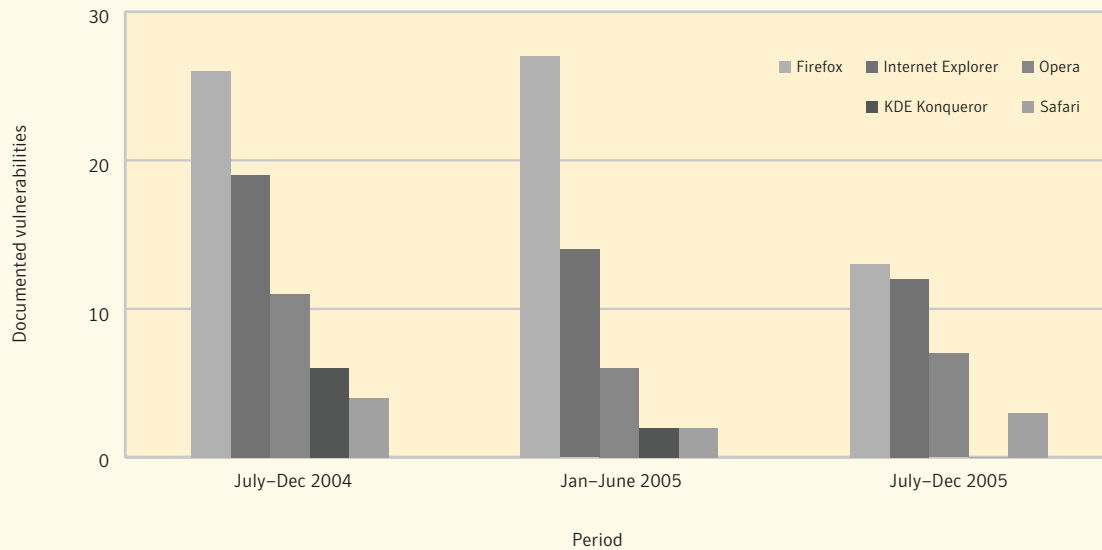
## Symantec Internet Security Threat Report

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



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

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



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

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

**Total volume of vulnerabilities**

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

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

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

## Symantec Internet Security Threat Report

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

Symantec also recommends that security administrators follow the best practices outlined in Appendix A of the *Symantec Internet Security Threat Report*, March 2006 edition. Administrators should audit their systems to ensure that no vulnerable Web applications or scripts are being hosted on them. Administrators should also thoroughly review the need for and use of all Web applications. Only those Web applications that are required for enterprise operations should be deployed.

### **Time to compromise for Internet-connected computers**

For the first time, the March 2006 volume of the *Internet Security Threat Report* is assessing the amount of time it takes for attackers to compromise a newly installed operating system once it has been connected to the Internet. This metric has been developed to give insight into how quickly an Internet-connected computer may become compromised. This will help administrators and users to understand the immediacy of potential threats against Internet-facing computers.

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

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

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

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

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

<sup>5</sup> Symantec performs automated heuristic analysis on the computer to determine when it is considered to be compromised. It should be noted that multiple failed compromise attempts are often observed prior to a successful compromise.

<sup>6</sup> For a complete listing of operating systems and their time to compromise statistics, please see the “Attack Trends” section of this report.

<sup>7</sup> The testing period for the time to compromise was from November 16 to December 31, 2005.

## Window of exposure

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

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

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

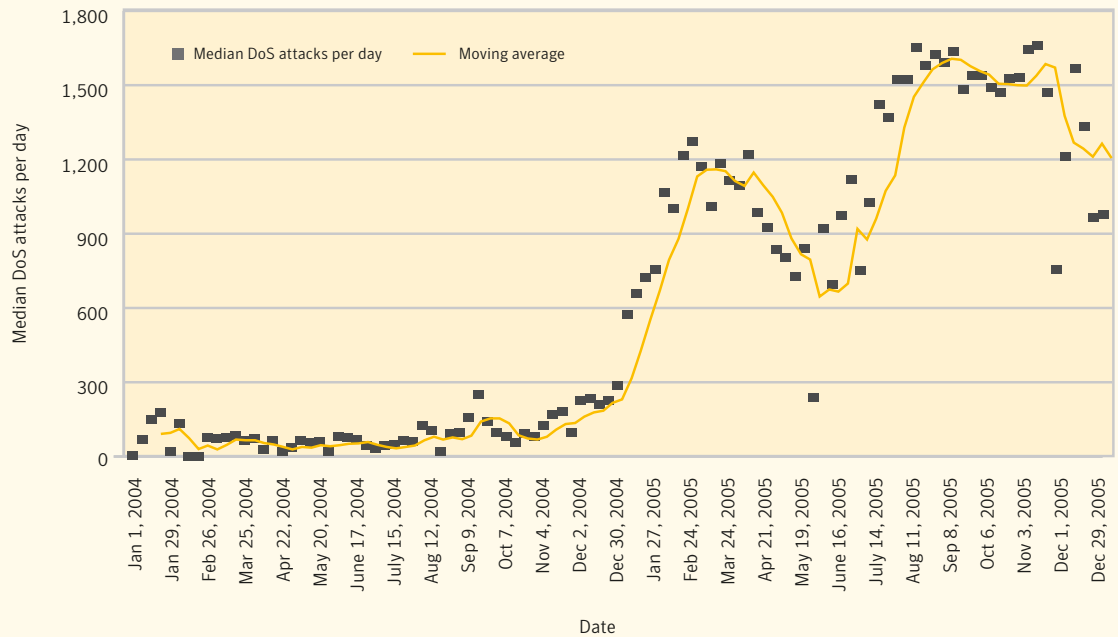
In the time between the availability of exploit code and the application of a patch, computers hosting the vulnerable applications will be exposed to potential compromise. Symantec refers to this time as the "window of exposure." During the last six months of 2005, 42 days elapsed on average between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

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

## Denial of service attacks

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

revenue. They are particularly dangerous because they are very difficult to defend against. Over the last six months of 2005, Symantec detected an average of 1,402 DoS attacks per day (figure 3). This is an increase of 51% from the first half of 2005, when Symantec detected an average of 927 DoS attacks per day.



**Figure 3. DoS attacks per day**  
Source: Symantec Corporation

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

Organizations should ensure that a documented procedure exists for responding to DoS events. Symantec also recommends that organizations perform egress filtering on all outbound traffic. One the best ways to mitigate a DoS attack is to filter upstream of the target. For most organizations this filtering will involve working in conjunction with their Internet service provider (ISP). Further, once a DoS attack is identified, the targeted organization will likely need to engage its ISP to help filter the traffic to minimize the impact of the attack.

<sup>8</sup> Bots (short for "robots") are programs that are covertly installed on a user's machine in order to allow an unauthorized user to control the computer remotely through a communication channel such as IRC. These communication channels are used to allow the remote attacker to control a large number of compromised computers over a single, reliable channel in a bot network, which can then be used to launch coordinated attacks.  
<sup>9</sup> Symantec *Internet Security Threat Report* Volume VIII (September 2005) <http://enterprisesecurity.symantec.com/content.cfm?articleid=1539>; p. 11  
<sup>10</sup> <http://www.networkworld.com/news/2005/051605-ddos-extortion.html>

**Top bot-infected countries**

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

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

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

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

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

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

<sup>11</sup> Bot command-and-control servers are computers that bot network owners use to relay commands and instructions to other computers on their bot networks.

### Instant messaging threats

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

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

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

### Phishing activity

Phishing is an attempt by a third party to solicit confidential information from an individual, group, or organization, often for financial gain. Phishers are groups or individuals who attempt to trick users into disclosing personal data such as credit card numbers, online banking credentials, and other sensitive information. They may then use the information to conduct cybercrime activities for profit.

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

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

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

<sup>12</sup> <http://tc.imlogic.com/threatcenterportal/pubThreatDetail.aspx?ThreatID=3505>

<sup>13</sup> <http://www.securityfocus.com/bid/16074>

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

Administrators should always follow Symantec best practices as outlined in Appendix A of the Symantec *Internet Security Threat Report*, March 2006 edition. Symantec also recommends that organizations educate their end users about phishing.<sup>16</sup> Organizations should also keep their employees notified of the latest phishing attacks and how to avoid falling victim to them.<sup>17</sup>

### Spam activity

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

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

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

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

### Adware and spyware

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

<sup>14</sup> Message transfer agents are programs that are responsible for routing email messages to the proper destination.

<sup>15</sup> A DNSBL is simply a list of IP addresses that are known to send unwanted email traffic. The DNSBL is used by email software to either allow or reject email coming from IP addresses on the list.

<sup>16</sup> For instance, the United States Federal Trade Commission has published some basic guidelines on how to avoid phishing. They are available at: <http://www.ftc.gov/bcp/online/pubs/alerts/phishingalrt.htm>

<sup>17</sup> A good resource for information on the latest phishing threats can be found at <http://www.antiphishing.org>

<sup>18</sup> IP filtering simply involves comparing inbound connection attempts against a preconfigured list of bad or suspicious IP addresses. Traffic shaping is the use of different IP characteristics—for instance, if an originating IP is determined to be a known source of spam—to selectively determine what connections to allow, deny, or throttle (slow down).

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

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

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

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

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

### Modular malicious code

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

<sup>19</sup> <http://securityresponse.symantec.com/avcenter/venc/data/adware.websearch.html>

<sup>20</sup> <http://securityresponse.symantec.com/avcenter/venc/data/spyware.cometcursor.html>

<sup>21</sup> Browser helper objects (BHOs) are add-on programs that can add legitimate features to a user’s browser (IE 4.X and up). For example, document readers used to read programs within the browser do so via BHOs. BHOs can also be used to install security risks on a user’s Web browser using ActiveX controls

<sup>22</sup> <http://securityresponse.symantec.com/avcenter/venc/data/adware.aurora.html>

<sup>23</sup> <http://securityresponse.symantec.com/avcenter/venc/data/spyware.apropos.html>

<sup>24</sup> For more details on Symantec’s risk levels, please see: [http://securityresponse.symantec.com/avcenter/enterprise/security\\_risks/#riskAssessment](http://securityresponse.symantec.com/avcenter/enterprise/security_risks/#riskAssessment)

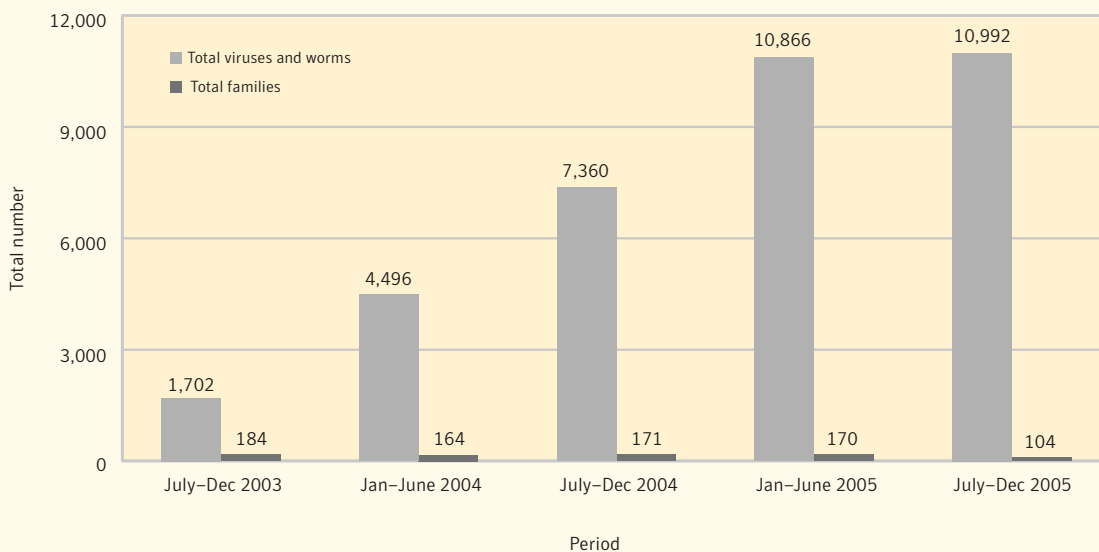
In the previous volume of the *Internet Security Threat Report*, Symantec stated that modular malicious code would likely be an issue of concern in the near future.<sup>25</sup> This appears to be the case. Between July and December of 2005, modular malicious code accounted for 88% of the top 50 malicious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

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

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

### Win32 virus and worm variants

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



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

<sup>25</sup> Symantec *Internet Security Threat Report*, Volume VIII (September 2005) <http://enterprisesecurity.symantec.com/content.cfm?articleid=1539>; p. 83

<sup>26</sup> *Crimeware* is an application that aids in the commission of cybercrime activity.

<sup>27</sup> Egress traffic refers to traffic that is leaving a network, bound for the Internet or another network.

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

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

### **Malicious code propagation vectors**

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

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

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

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

<sup>28</sup> SMTP is the protocol by which email is transmitted between mail servers.  
<sup>29</sup> CIFS is used for file sharing.

## Future Watch

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

## Cybercrime expected to rise

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

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

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

## Increase in malicious code utilizing stealth capabilities

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

<sup>30</sup> Symantec *Internet Security Threat Report*, Volume VIII (September 2005) <http://enterprisecurity.symantec.com/content.cfm?articleid=1539>, p. 4  
<sup>31</sup> [http://www.symantec.com/avcenter/cybercrime/index\\_page5.html](http://www.symantec.com/avcenter/cybercrime/index_page5.html)

<sup>32</sup> This figure excludes from consideration reports of Sober.X, which was the most prominent malicious code report during this period. Please see the "Threats to confidential information" section in the "Malicious Code Trends" report in this document

<sup>33</sup> Definitions of the term "rootkit" vary but for the purposes of this discussion, a rootkit is defined as a set of tools designed to hide the presence of a running process and avoid detection and removal of that process.

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

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

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

### **Increased commercialization of vulnerability research**

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

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

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

<sup>34</sup> <https://www-secure.symantec.com/avcenter/venc/data/w32.fanbot.a@mm.html>

<sup>35</sup> <http://www.symantec.com/avcenter/reference/when.malware.meets.rootkits.pdf>

<sup>36</sup> <http://www.securityfocus.com/news/11372>

<sup>37</sup> Non-disclosed vulnerabilities are often referred to in a process known as closed disclosure, which refers to the practice of disclosing vulnerabilities to only a commercial vulnerability vendor or the affected vendor without notifying other reporting organizations.

<sup>38</sup> <http://www.securityfocus.com/news/11363>

<sup>39</sup> <http://www.security-express.com/archives/dailydave/2005-q2/0308.html>

<sup>40</sup> <http://www.securityfocus.com/news/11364>

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

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

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

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

### **Non-traditional platform threats expected to emerge**

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

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

Voice and data devices such as Research in Motion's (RIM) Blackberry<sup>™</sup> and Palm's Treo<sup>™</sup> 700w have

<sup>41</sup> A zero-day attack is one that attacks a vulnerability for which there is no available patch. It also generally means an attack against a vulnerability that is not yet public knowledge or even known of by the vendor of the affected technology.

<sup>42</sup> <http://www.dhs.gov/interweb/assetlibrary/vdwgreport.pdf>

<sup>43</sup> <http://www.sarc.com/avcenter/venc/data/trojan.pspbrick.html>

<sup>44</sup> [http://www.xbox-linux.org/wiki/Main\\_Page](http://www.xbox-linux.org/wiki/Main_Page)

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

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

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

### **A "boom" cycle for bots and bot networks**

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

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

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

<sup>45</sup> <http://www.geekzone.co.nz/content.asp?contentid=2972>

<sup>46</sup> <http://search.securityfocus.com/swsearch?query=Blackberry&sbm=bid&submit=Search%21&metaname=alldoc&sort=swishrank>

<sup>47</sup> <http://securityresponse.symantec.com/avcenter/venc/data/pwsteal.lineage.html>

<sup>48</sup> [http://www.theregister.co.uk/2005/08/24/fantasy\\_role\\_play\\_worm/](http://www.theregister.co.uk/2005/08/24/fantasy_role_play_worm/)

<sup>49</sup> [http://news.com.com/Bots+may+get+cloak+of+encryption/2100-7349\\_3-5952102.html](http://news.com.com/Bots+may+get+cloak+of+encryption/2100-7349_3-5952102.html)

<sup>50</sup> For further discussion of this trend please see the "Attacks Trends" section of this report.

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

### **Increase in phishing messages and malicious code distributed through instant messaging**

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

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

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





## **About Symantec**

Symantec is the world leader in providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information.

Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries.

More information is available at [www.symantec.com](http://www.symantec.com).

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

Symantec Corporation  
World Headquarters  
20330 Stevens Creek  
Boulevard  
Cupertino, CA 95014 USA  
+1 (408) 517 8000  
1 (800) 721 3934  
[www.symantec.com](http://www.symantec.com)

Copyright © 2006 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. 03/06 10553081