

# Symantec Internet Security Threat Report

Trends for January 1, 2004 – June 30, 2004

**EXECUTIVE EDITOR**

Dean Turner

*Symantec Security Response*

**EDITOR**

Stephen Entwisle

*Symantec Security Response*

**TECHNICAL ADVISOR**

Oliver Friedrichs

*Symantec Security Response*

**DEEPSIGHT THREAT ANALYST**

Daniel Hanson

*Symantec Security Response*

**DEEPSIGHT THREAT ANALYST**

Marc Fossi

*Symantec Security Response*

**MANAGER, DEVELOPMENT**

David Ahmad

*Symantec Security Response*

**SENIOR RESEARCH FELLOW**

Sarah Gordon

*Symantec Security Response*

**SECURITY ARCHITECT**

Peter Szor

*Symantec Security Response*

**SECURITY RESEARCHER**

Eric Chien

*Symantec Security Response*

**SECURITY RESEARCHER**

Frederic Perriot

*Symantec Security Response*

**SECURITY RESEARCHER**

Peter Ferrie

*Symantec Security Response*

# Contents

|   |    |
|---|----|
| <b>Executive Summary</b> .....                            | 2  |
| <b>Attack Trends</b> .....                                | 6  |
| <b>Vulnerability Trends</b> .....                         | 24 |
| <b>Malicious Code Trends</b> .....                        | 32 |
| <b>Future Watch</b> .....                                 | 42 |
| <b>Appendix A—Symantec Best Practices</b> .....           | 47 |
| <b>Appendix B—Attack Trends Methodology</b> .....         | 48 |
| <b>Appendix C—Vulnerability Trends Methodology</b> .....  | 53 |
| <b>Appendix D—Malicious Code Trends Methodology</b> ..... | 54 |

## 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. This summary of the current *Internet Security Threat Report* can alert executives to current trends and impending threats. In addition, it will offer some recommendations for protection against and mitigation of these concerns. This edition of the *Internet Security Threat Report* covers the six-month period from January 1, 2004, to June 30, 2004.

With over 20,000 sensors monitoring network activity in over 180 countries by Symantec DeepSight™ Threat Management System and Symantec Managed Security Services, Symantec has established one of the most comprehensive sources of Internet threat data in the world. In addition, Symantec gathers malicious code data from over 120 million client, server, and gateway systems that have deployed Symantec's antivirus products in consumer and corporate environments. Combined with Symantec's vulnerability database of over 10,000 entries, these resources give Symantec analysts an unparalleled source of data with which to identify emerging trends in attacks and malicious code activity.

### TIME TO PATCH VULNERABLE SYSTEMS IS SHORT

Over the past six months, the average time between the announcement of a vulnerability and the appearance of associated exploit code was 5.8 days.<sup>1</sup> Once exploit code is made available, a new vulnerability can be widely scanned for and exploited quickly. This danger is made worse if the application in which the vulnerability is found is widely deployed, such as a Web server or database application.

Recent widespread worms have illustrated the dangers of the narrow vulnerability-to-exploit window. For example, the Witty worm was discovered only two days after the vulnerability it exploited was made public. The ability of malicious code writers to rapidly upgrade bot networks (discussed in the next section) compounds the dangers posed by the brief vulnerability-to-exploitation window. Furthermore, as these worms are becoming more sophisticated and, in many cases, remotely controlled by attackers, the potential impact on an enterprise is significant.

Once a vulnerability is made public, organizations must introduce security countermeasures before an exploit is made available or risk having their systems exploited. This means that, on average, organizations have less than a week to patch all their systems on which the vulnerable application is running. However, without significant investment in enterprise tools, this may not be practical.

System administrators must become aware of new threats and implement the appropriate countermeasures in time to prevent successful attacks. This is particularly challenging in large organizations, for which applying enterprise-wide patching in a matter of days is nearly impossible, especially when the necessity of patching individual workstations and laptops is taken into account.

Symantec recognizes the difficulties that most security administrators face in tracking and patching 48 new vulnerabilities a week and recommends that enterprises devote sufficient resources to alerting and patch remediation solutions. They should also consider engaging a managed security service provider to assist them in monitoring their networks.

## REMOTELY CONTROLLED BOT NETWORKS ARE GROWING

Bots (short for “robots”) are programs that are covertly installed on a targeted system. They allow an unauthorized user to remotely control the compromised computer for a wide variety of malicious purposes. Attackers often coordinate large groups of bot-controlled systems known as bot networks. These networks can be used to perform distributed attacks, including denial-of-service (DoS) attacks, against organizations’ systems.

Over the first six months of 2004, the number of monitored bots rose from well under 2,000 computers to more than 30,000. The short vulnerability-to-exploit window makes these bots particularly dangerous. Once an exploit is released, the owner of the bot network can quickly and easily upgrade the bots, which can then scan target systems for the vulnerability in question. This vastly increases the speed and breadth of potential attacks. This makes a risk assessment of a compromise very uncertain, as the capabilities of the tool may change at a moment’s notice. It also makes it very difficult to patch organization systems in time to prevent widespread compromise.

Symantec recognizes the increasing risk that bots pose and recommends that organizations implement vulnerability alerting, centralized logging, and security event management—steps that can quickly identify and investigate potential attacks. This will lead to a quicker and more accurate response, an important component of a successful mitigation.

## IP SPACE OF 40% OF FORTUNE 100 COMPANIES COMPROMISED BY WORMS

Over the first six months of 2004, Symantec observed worm traffic originating from Fortune 100 corporations. This data was gathered not by monitoring the Fortune 100 companies themselves, but by analyzing attack data that revealed the source IP addresses of attack activity. The purpose of this analysis was to determine how many of these systems were infected by worms and actively being used to propagate worms. More than 40% of Fortune 100 companies controlled IP addresses from which worm-related attacks propagated.

The propagation of worms from these systems does not mean that anyone within or affiliated with the organization is necessarily involved with attack activity. Rather, the systems that are being used to launch attacks are themselves likely to have been compromised by external attackers. This indicates that, despite the measures taken by organizations, their systems are still becoming infected. Continued worm traffic coming from these networks indicates to potential attackers that the network is still susceptible to exploitation.

Due to their high profile, Fortune 100 companies are often attractive targets for attackers. They can be seen as representative of corporate networks as a whole. Symantec recommends that all companies actively audit their critical systems. Increased vigilance at the network perimeter, coupled with best practices, can help protect against and mitigate attacks.

## E-COMMERCE MOST FREQUENTLY TARGETED INDUSTRY

During the first six months of 2004, e-commerce received more targeted attacks than any other industry. During this period, 16% of attackers attacking e-commerce organizations were considered targeted. This is up dramatically from the last six months of 2003, during which only 4% of attackers against e-commerce were considered targeted.

The rise in targeted attackers for e-commerce is worrisome, as these businesses often depend entirely on the Internet for their revenue. This rise may indicate that the motivation of attackers may be shifting from looking for notoriety toward seeking illicit financial rewards. Whether attackers intend to obtain customers’ personal data, steal money, or blackmail the company, organizations that depend heavily on their Internet presence may be vulnerable to a financially motivated attack.

## ATTACKS AGAINST WEB APPLICATION TECHNOLOGIES INCREASING

Web applications are becoming increasingly popular targets of attacks. As many organizations deploy hundreds of custom Web applications throughout their enterprise, the security of all of these applications, should be confirmed. It is not uncommon to find critical human resources functions, business services, and accounting applications that are accessible via the World Wide Web.

In the first half of 2004, 39% of disclosed vulnerabilities were associated with Web application technologies. Web application vulnerabilities can allow an attacker to access confidential information from databases without having to compromise any servers. They allow attackers to gain access to the target system simply by penetrating one end user's computer, bypassing traditional perimeter security measures.

These vulnerabilities are often straightforward. For example, in the first six months of 2004, 82% of Web application vulnerabilities were considered easy to exploit. As such, they represent a significant problem for organizations. Traditional security devices are not generally configured to monitor custom Web applications. This makes monitoring for and protecting against these threats difficult. Adding to the problem is the fact that many Web applications are not rigorously audited for security prior to deployment. Symantec recommends that organizations perform thorough security audits before any Web application is deployed.

## INTERNET SECURITY THREAT REPORT HIGHLIGHTS

### Attack Trend Highlights

- Overall, daily volume of attacks decreased, likely due to a decline in Internet-based worm attack activity over the first six months of 2004.
- The Slammer worm was the most common attack over the past six months, with 15% of attacking IP addresses performing an attack related to it.
- Gaobot and its variants were the second most common attack, increasing by over 600% over the past six months.
- The number of bot-infected computers rose substantially over the past six months, from less than 2,000 to more than 30,000.
- E-commerce received the most targeted attacks of any industry during this period. Small business received the second most.
- United States was the top attack source country with 37%, down from 58% in the previous six months. Other countries rose accordingly, indicating that attack activity is becoming more international.
- During this period, 87% of Managed Security Service's clients with tenure of more than six months successfully avoided experiencing a severe attack.

### Vulnerability Trend Highlights

- The average time between the public disclosure of a vulnerability and the release of an associated exploit was 5.8 days.
- The Symantec Vulnerability Database documented 1,237 new vulnerabilities between January 1 and June 30, 2004.
- On average, 48 new vulnerabilities per week were disclosed between January 1 and June 30, 2004.
- During this period, 96% of disclosed documented vulnerabilities were rated as moderately or highly severe.
- In the first six months of 2004, 70% of disclosed vulnerabilities were considered easy to exploit.
- During this period, 64% of vulnerabilities for which exploit code is available were considered high severity.
- In the first half of 2004, 479 vulnerabilities, or 39% of the total volume, were associated with Web application technologies.

### Malicious Code Trend Highlights

- Over the past six months, Symantec documented more than 4,496 new Windows® (particularly Win32) viruses and worms, over four and a half times the number as the same period in 2003.
- The number of distinct variants of bots is rising dramatically, increasing by 600% over the past six months.
- Peer-to-peer services (P2P), Internet relay chat (IRC), and network file sharing continue to be popular propagation vectors for worms and other malicious code.
- Adware is becoming more problematic for users: 6 of the top 50 malicious code submissions were adware.
- The first malicious worm for mobile devices, Cabir, was developed.

### Future Trends and Emerging Threats

- Client-side and Web application attacks are expected to increase in the near future.
- Targeted attacks on firewalls, routers, and other security devices protecting users' systems are a growing security concern.
- Symantec expects bot networks to employ increasingly sophisticated methods of control and attack synchronization that are difficult to detect and locate.
- Symantec expects to see instances of port knocking, a method attackers may use to create direct connections to potential target systems.
- Symantec expects that recent Linux® and BSD vulnerabilities that have been discovered and used in proof-of-concept exploits will be used as exploit-based worms in the near future.
- Symantec expects to see more attempts to exploit mobile devices.

## Attack Trends

This section of the *Symantec Internet Security Threat Report* provides an analysis of Internet attack activity for the six months ending June 30, 2004. This activity will be compared to Internet attack activity from the two previous six-month periods: January 1–June 30, 2003, and July 1–December 31, 2003. Where applicable, suggestions on attack remediation have been made, including Symantec’s recommendations for best security practices, which can be found in Appendix A at the end of this report.

Symantec has established one of the most comprehensive sources of Internet threat data in the world. Over 20,000 sensors deployed by Symantec DeepSight Threat Management System and Symantec Managed Security Services in more than 180 countries gather this data. This section will be based on that data.

For the purposes of this report, attack activity is divided into three categories: 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 information-gathering attacks (probes).

In some cases, it is 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. Readers should note that backdoors and remote control software to create networks of zombie<sup>2</sup> hosts called bot networks are classified as worm-related attacks for the purposes of this report.

Over the last few years, there has been a convergence of previously distinct security devices. This convergence means that the traditional distinction between intrusion detection, firewalls, antivirus, and other security devices has begun to blur. One of the consequences of this is that, in addition to the traditional antivirus products, non-antivirus devices have also begun to detect specific malicious code infections.

This shift may affect the way that data is presented in this report. Attack trends data is ranked based on infected sources attempting to spread, whereas antivirus data is ranked according to the number of samples that are submitted by antivirus engines. Assessing threats according to attack trends data can lead to different results than analyzing malicious code data. This may lead to different ranking of data between the “Attack Trends” section and the “Malicious Code Trends” section 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
- Top originating countries
- Top originating countries per Internet capita
- Targeted attack activity by industry
- Attack activity by time of day
- Attack activity by day of week
- Fortune 100 infection exposure
- Client tenure and severe event incidence

## TOP INTERNET ATTACKS

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

The top attacks can be considered in three ways:

1. By the percentage of total attacking IP addresses that performed a given attack
2. By the percentage of total events that a given attack constituted
3. By the percentage of total sensors that detected an attack

Each way of looking at the data can reveal different trends. In Volume V of the *Internet Security Threat Report* (March 2004), both the percentage of total sensors and percentage of total events were used to

<sup>2</sup> A zombie is a compromised computer that is remotely controlled by an attacker who can use it to launch attacks such as DoS attacks. The legitimate user of the compromised computer may not be aware that an attacker has control over his or her computer.

Table 1. Top attacks January 1–June 30, 2004

| Rank<br>Jan–June 2004 | Rank<br>July–Dec 2003 | Attack   | Percent of<br>Attackers |
|-----------------------|-----------------------|--|-------------------------|
| 1                     | 1                     | Slammer Attack   | 15%                     |
| 2                     | Not Ranked (NR)       | W32.HLLW.Gaobot Attack   | 4%                      |
| 3                     | 6                     | Generic WebDAV/Source Disclosure "Translate: f" HTTP Header Request Attack | 4%                      |
| 4                     | 5                     | Microsoft® IIS 5.0 .printer ISAPI Extension Buffer Overflow Attack         | 3%                      |
| 5                     | NR                    | MyDoom Incoming Worm Attack  | 3%                      |
| 6                     | NR                    | Generic SMTP Malformed Command/Header Attack                               | 2%                      |
| 7                     | 2                     | Generic ICMP Flood Attack  | 2%                      |
| 8                     | NR                    | Generic IP SRC=127.x.x.x (localhost) Spoofing Attack                       | 2%                      |
| 9                     | NR                    | Generic HTTP Directory Traversal Attack                                    | 1%                      |
| 10                    | NR                    | Microsoft Windows DCOM RPC Interface Buffer Overrun Attack                 | 1%                      |

Source: Symantec Corporation  
TMS and MSS data

highlight the prevalence of Slammer and the Blaster worm. However, for this report, Symantec analyzed attack data according to the percentage of total attacking IP addresses.

The top attacks (**Table 1**) for the first six months of 2004 are largely new. Six of the attacks were not ranked in the top ten attacks for the second half of 2003. This volatility highlights the constantly evolving nature of Internet attacks and illustrates the fact that no organization can remain complacent in its security measures.

Slammer was the most common attack in the first six months of 2004. Fifteen percent of attacking IP addresses performed a Slammer-related attack. Since its outbreak in January 2003, Slammer has remained a constant problem for organizations. It is often able to bypass firewalls when infected computers are connected to the corporate network either directly, as with a laptop, or through a VPN.

The prominence of Slammer as a top attack is related to two factors. First, it uses a single UDP packet to proliferate. This means that intrusion detection systems will interpret every infection attempt by Slammer as an actual attack. Worms that spread over services that use TCP will only see attacks when the targeted port is open (that is, when a service is installed and listening). However, UDP allows Slammer to send a whole attack to every IP

address, regardless of whether Microsoft SQL Server is installed. If Slammer propagated over a TCP service, most of the "attacks" would be regarded as scans for the service rather than attacks.

The second factor contributing to the high numbers of Slammer is the widespread use of the Microsoft Desktop Engine (MSDE). MSDE is deployed in many third-party applications. As it is a variant of the SQL Server engine, it is also vulnerable to Slammer. This makes patching for the worm harder because it is difficult to identify and patch applications that use MSDE. This may leave a significant number of systems inside a network vulnerable to Slammer.

Gaobot was the second most common attack over the first six months of 2004. Four percent of detected attackers were compromised by Gaobot, which was not ranked in previous reporting periods. The current prominence of the attack reflects the sudden appearance of numerous Gaobot variants over this reporting period. Gaobot, a type of bot,<sup>3</sup> 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. (For more on the Gaobot family of worms, please see the "Malicious Code Trends" section of this report.)

The WebDAV Translate: f Attack was ranked third in the top attacks during this reporting period. It is often detected when any of several worms and

<sup>3</sup> Short for "robot," a computer program that runs automatically. For more detailed discussion, please see the "Bot Networks" discussion on page 13.

viruses propagates via the Microsoft Windows ntdll.dll Buffer Overflow vulnerability.<sup>4</sup> Many intrusion detection systems generate an alert on this attack when this vulnerability is exploited remotely via WebDAV, a file-sharing protocol that allows modification of documents over the HTTP (Web) protocol. This attack was widely associated with the Welchia worm that began spreading in August 2003, shortly following the outbreak of Blaster. Since that time, other malicious code, including Gaobot and other bot network software, have exploited this vulnerability.

MyDoom, a new worm entrant, is ranked fifth in the top ten attacks for the first half of 2004. It was launched by 3% of attacking IP addresses. This mass-mailing worm was discussed in the “Current Issues” section of the previous *Internet Security Threat Report* (March 2004) after it broke out in January 2004. (It is important to note that for the purposes of this discussion, the many variants of MyDoom are treated as one type of attack; however, in the “Malicious Code Trends” section of this report, variants of MyDoom are considered as separate attacks.)

The large number of Gaobot and Mydoom detections, representing 4% and 3% of attacking IP addresses respectively, highlights the fact that network protection systems are dealing with malicious code that in previous years would be considered the

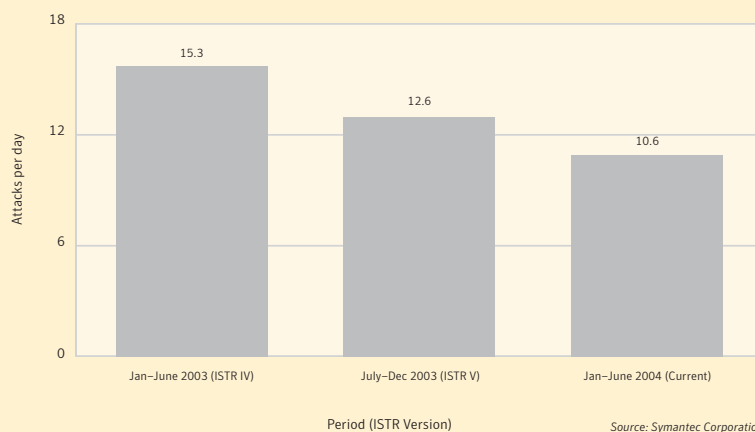
domain of antivirus protection. This highlights the convergence of security devices that was discussed in the overview to this section.

The 127.x.x.x spoofing attack is ranked eighth in the top ten attacks of the past six months. It was performed by 2% of detected attackers. The presence of this attack indicates that packets with a source IP address in the 127.x.x.x range were detected on the network. This range of IP addresses is reserved as a localhost address and, as such, should never be detected as valid network traffic on a properly configured network. This attack is often used as part of a DoS attack. Shortly after the outbreak of the Blaster worm, it was seen on some networks following a discussion on security mailing lists regarding an inappropriate mitigation strategy for the DoS routine contained in Blaster.<sup>5</sup>

#### ATTACK ACTIVITY PER DAY

This section will discuss the average number of attacks seen each day by organizations that are connected to the Internet. The number of attack attempts that an organization experiences in a given period of time can be a good indication 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.

**Figure 1. Daily attack rate**



Source: Symantec Corporation  
TMS and MSS Data

<sup>4</sup> <http://www.securityfocus.com/bid/7116>

<sup>5</sup> A post summarizing the resulting activity and the reasons for it can be found on the SecurityFocus Incidents mailing list at <http://www.securityfocus.com/archive/75/342726>

On average, organizations received 11 attacks per day, continuing a decrease that was observed over the two previous reporting periods (**Figure 1**).

Specifically, this represents a 15% decrease from the average of 13 attacks between July 1 and December 31, 2003, and a 27% drop from the 15 attacks in the January 1–June 30, 2003, reporting period. The major contributor to the decline is a drop in attack rates due to worms. This change in the proportion of attacks is further noted in the “Attack Activity by Type” discussion below.

## 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 types of attacks are taking place. This section will discuss attack activity according to 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 2**).

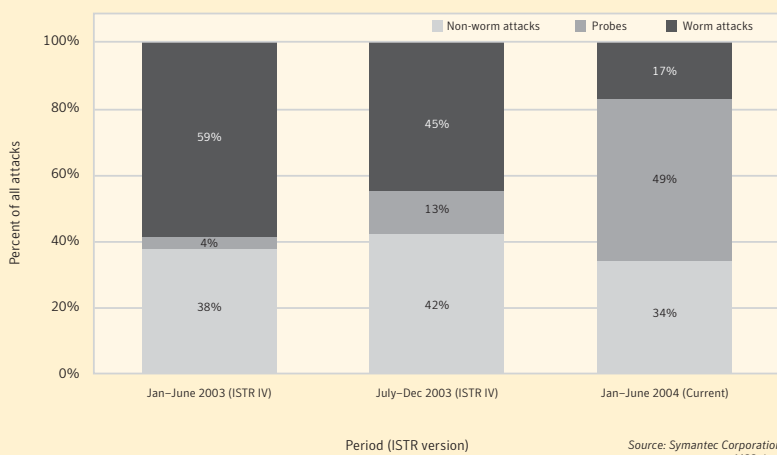
From January 1 to June 30, 2004, 49% of detected activity was classified as probes. This is a substantial rise from the 13% in the second half of 2003, and a further increase over the 4% detected in the first half of that year. One explanation for this increase is that Symantec often reclassifies attack activity as additional information about the attacks

becomes available. Probes are often the first indication of an attack. However, as the initial probe is investigated and new intrusion detection signatures are released, the probe may be reclassified as a worm-related or non-worm related attack.

The effect of this is evident in the impact that Sasser had on attack statistics.<sup>6</sup> The Sasser worm, first discovered in April, probes TCP port 445 to determine if a remote computer is online. While activity targeting port 445 increased during this reporting period because of Sasser, attacks related to Sasser were absent from the top attack list. This is because port 445 probing was not classified as Sasser-related activity because there are so many exploit tools and examples of malicious code that also scan for this port. The fact that the majority of the detected activity attributed to Sasser consisted of scanning also helps to explain the large increase in probes. This effect is largely related to strong perimeter filtering of TCP port 445 that occurs on most corporate networks.

In the first six months of 2004, worms accounted for 17% of attack activity. This is a significant decrease from the two previous reporting periods. In the second half of 2003, worm activity accounted for 45% of attack activity. In the first half of that year, they made up 59% of attack activity. This decrease is due to a decline in significant worm-related attack activity detected by Threat Management System (TMS)

**Figure 2. Breakdown of attack type**



<sup>6</sup> <http://securityresponse.symantec.com/avcenter/venc/data/w32.sasser.worm.html>

and Managed Security Services (MSS) sensors during the first half of 2004. However, readers should note that this does not represent a decrease in overall worm infections, only a decrease in worm-related attacks.

There were two reasons for the lower number of detected worm attacks. The first was the fact that Sasser was largely seen in probing rather than attack attempts, as was discussed previously. The second factor was that the traditional division between network security devices, such as intrusion detection systems and antivirus, meant that it was difficult to configure sensors to detect the MyDoom and Netsky mass-mailing worms. The sensors that did detect these email worms detected a significant number of infected systems. This is evident in the presence of MyDoom in the top ten Internet attacks.

While worm activity has decreased over the past three reporting periods, non-worm attack activity does not appear to be following any consistent long-term pattern. During the first six months of 2004, 34% of attack activity was classified as non-worm attacks. This represents a decrease from the 42% of activity in the second half of 2003, which was in turn an increase over the 38% of activity in the first half of that year.

The lack of a significant long-term trend is not surprising given the variety of vulnerabilities that attackers may use and the different motives for attack. Many vulnerabilities are not conducive to worm exploitation; however, they can be scanned for and manually exploited to achieve some end other than compromise of a system. For example, a Web application vulnerability can allow unauthorized disclosure of information without necessarily compromising a destination server. Because of the constant discovery of medium-security vulnerabilities with a low barrier to entry,<sup>7</sup> non-worm attacks can be expected to remain fairly steady.

Because this trend is a proportion of total attack activity, any significant increase or decrease in one type of activity will result in changes in the other. Symantec found that the raw numbers of attacks show similar trends to the proportional percentages: Large declines in worm-related attacks were matched by large increases in probes.

This shift is likely related to the recent increase in remote-controlled bots and other malicious code applications that do not fit the traditional definition of a worm. As discussed in the “Malicious Code Trends” section of this report, the past six months have seen a significant increase in the number of variants of three popular bot network applications: Gaobot, Spybot, and Randex. The increasing number of variants of these bots is apparent in the growth of IP addresses associated with bot network activity (see the “Bot Networks” section on page 13). The resulting activity, which largely consists of scanning for older vulnerabilities, helps to explain this shift from worm activity to probe activity.

The increasing risk from these numerous bot networks and the speed at which they can be upgraded for additional functionality make them potentially more dangerous than traditional viruses and worms. For instance, Gaobot and Spybot are able to propagate through numerous vulnerabilities. Their architecture is such that new propagation vectors can be added to a large number of hosts very rapidly. This flexibility and speed of deployment makes it difficult to categorize attacks as coming from a certain tool or variant of malicious code. As a result, organizations that rely on attack identification to prioritize incident response face a more difficult task in protecting their systems.

Despite the decline in the number of attacks per day discussed earlier, the threat that large bot networks pose to systems connected to the Internet is making the job of security administrators that much more difficult. Sorting out automated attacks from targeted attacks and giving response priority to certain events is becoming a far more complex task. Symantec recommends that organizations consider procedures and solutions that can expedite the rapid identification and complete investigation of attacks. Centralized logging and security event management, in addition to vulnerability alerting, can significantly hasten threat identification. This will lead to a quicker and more accurate response, an important component of successful management of a security incident.

Table 2. Top attacked ports January 1–June 30, 2004

| Rank<br>Jan–June 2004 | Rank<br>July–Dec 2003 | Port     | Service Description                 | Percent of<br>Attackers |
|-----------------------|-----------------------|----------|-------------------------------------|-------------------------|
| 1                     | 2                     | TCP/80   | HTTP/Web                            | 30%                     |
| 2                     | 5                     | TCP/445  | Microsoft CIFS file sharing         | 17%                     |
| 3                     | 1                     | TCP/135  | Microsoft DCE Remote Procedure Call | 15%                     |
| 4                     | 3                     | TCP/4662 | E-donkey/P2P file sharing           | 7%                      |
| 5                     | 4                     | TCP/6346 | Gnutella/P2P file sharing           | 5%                      |
| 6                     | NR                    | TCP/22   | Secure shell/remote access          | 4%                      |
| 7                     | NR                    | UDP/1026 | Various dynamic services            | 3%                      |
| 8                     | NR                    | TCP/113  | Ident service                       | 3%                      |
| 9                     | NR                    | TCP/2745 | Beagle                              | 3%                      |
| 10                    | NR                    | TCP/1025 | Various dynamic services            | 3%                      |

Source: Symantec Corporation  
TMS data

## 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. Nor does it attempt to provide any attack information. The lack of attack information means that it is impossible to separate worm-related activity from information-gathering activity or potential exploit attempts.

Over the first half of 2004, attackers most frequently targeted port 80, the HTTP service. It was targeted by 30% of attackers during this period. This represents a significant increase over the previous reporting period. From July 1–December 31, 2003, port 80 was the second most frequently attacked port, receiving attention from 20% of attackers. The current standing represents a return to a previously established norm. TCP port 80 has historically been the top attacked port; however, in the second half of 2003, it was displaced due to the Blaster worm of August 2003.

Port 80 hosts Web servers, which are popular targets for worms such as Code Red and Nimda. It also hosts Web applications. Attackers frequently target

Web applications in order to compromise information hosted on a Web site. With the ubiquity of the Web as a method of publishing information and giving clients and partners access to select internal resources, port 80 is the most commonly opened service for incoming connections. Administrators can limit the exposure of their system to attackers by auditing and filtering incoming requests.

TCP port 445 was the second most frequently targeted port over the past six months, with 17% of attackers targeting it. Port 445 is associated with the Sasser worm. Like the Blaster worm, Sasser targeted the Microsoft Windows LSASS Buffer Overrun vulnerability<sup>8</sup> in the default install of Microsoft Windows NT®-based systems, including Windows 2000, Windows XP, and Windows Server™ 2003 editions. As was described in the “Attack Activity by Type” discussion, the spread of the Sasser worm was largely responsible for the rise in TCP port 445 activity during this reporting period.

TCP port 445 is commonly well controlled at the network perimeter. This filtering may help explain the absence of Sasser-related attack data in other metrics despite widespread Sasser infections. However, worms targeting vulnerabilities over this port may be able to bypass the network perimeter. As a result, if an infection takes place, perimeter blocking should be accompanied by stronger filtering at logical network segments to limit propagation. Strong system

<sup>8</sup> <http://www.securityfocus.com/bid/10108>

configuration policy and audit control for all computers that do not remain behind a firewall can significantly decrease chances of infection.

During the first half of 2004, TCP port 135 was targeted by 15% of attackers, making it the third most commonly attacked port. This is a dramatic drop from the second half of 2003, when it was the top port with 32% of attackers targeting it. 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 Blaster and Welchia worms, which were propagating at that time.

The drop in TCP port 135 activity over the last six months likely reflects the decline in Blaster and Welchia activity. The high degree of publicity that these worms generated and a significant push by Microsoft to raise awareness of patch availability has likely resulted in increased patching of potentially vulnerable systems. As with TCP port 445, this port is also generally well filtered at the network perimeter. However, Symantec recommends that additional client-side protections also be used in order to guard against problems if the worm should bypass the perimeter.

The presence of TCP port 22 in sixth place in the top ten targeted ports is noteworthy, as there have been no recent vulnerabilities in the SSH protocol that is found on this port. There are two possible explanations for this. First, speculation about the possibility of a new vulnerability may have triggered increased scanning. Second, a new tool may have been targeting an old vulnerability. Regarding the first possibility, mailing list discussions through July 2004 identified a compromised network of systems that appeared to be scanning for SSH systems with weak username/password combinations.<sup>9</sup> As these systems compromised additional systems, the scanning activity continued to rise. This activity is known as username/password grinding and has been seen on other ports that require authentication, including Microsoft CIFS file sharing (TCP ports 139 and 445) and FTP (TCP port 21).

To guard against this activity, administrators are advised to audit all Internet-exposed systems for strong passwords and to disable all unnecessary default accounts. Robust log aggregation and analysis on a secure host can help to determine the extent of a breach should one occur. Because SSH connections are encrypted crossing the network, effective logging policies on all systems running SSH are required to identify and investigate suspicious activity. Furthermore, logging of successful and unsuccessful login attempts can be critical to determine whether password grinding attacks have been successful.

The scanning for ports 1026 and 1025, ranked seventh and tenth respectively, are new entries in the list of top attacked ports. 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 viewed cautiously. Without any indication of whether or not the addresses are spoofed, the true nature and source of this activity cannot be determined.

As for TCP port 1025, the RPC DCOM buffer overflow vulnerabilities are known to be exploitable over this port. In addition to possible RPC DCOM exploitation, there are Trojan applications that can be configured to utilize this port. With the interest in other backdoor ports, 17300 and 27374, noted in the previous *Internet Security Threat Report*, as well as port 2745, which is associated with the Beagle mass-mailer worm, the nature of this activity cannot be easily determined.

TCP ports 4662 and 6346, present in fourth and fifth place among the top targeted ports respectively, are both used for P2P file sharing. There is no indication whether activity on these ports is malicious or if it simply reflects the use of these P2P applications by end users within organizations. Regardless of this uncertainty, organizations would be well advised to audit all incoming and outgoing traffic for unauthorized use of these applications. The use of P2P applications by employees may place the organization at legal risk due to potential copyright infringement. Furthermore, P2P clients may be susceptible to vulnerabilities that may allow remote compromise of the clients involved in the network. Finally, files

exchanged through P2P applications may contain malicious code that will not be detected by the organization's antivirus scanner.

Many of the top targeted ports are already well controlled at the network perimeter, but services that exist on these ports can still pose risks to corporations. As laptops, virtual private networks (VPNs), and personal information management devices allow employees and other computer users to become more mobile, the traditional network perimeter continues to be degraded. Additionally, unauthorized services installed by users continue to present threats to the network.

Organizations can take several steps to minimize the risk posed by these threats. They should install perimeter security devices that inspect and proxy requests. They should also enforce configuration policy and audit control for all computers connecting to the network, including mobile and VPN-connected systems. All mobile computers should require the mandatory use of up-to-date antivirus and personal firewalls. Finally, all systems connecting to the network should be monitored for unauthorized applications.

## BOT NETWORKS

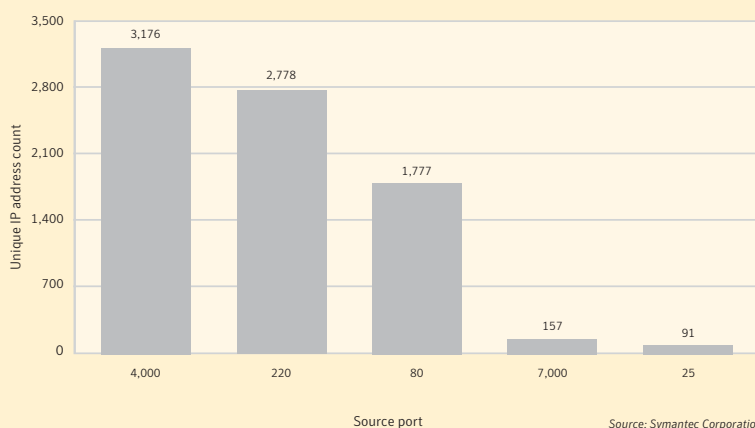
Bot networks are groups of systems that have been compromised and had software installed on them that allows simple remote control. The software can

easily be upgraded to include new exploits targeting new vulnerabilities. Bot networks are often better able to exploit new vulnerabilities than worms, as propagation code is not needed to use the exploits in a bot network. This simplifies the incorporation into the bot network of exploits written by third parties. Additionally, any number of exploits can be included, making differentiation of bot network attacks from targeted attacks by a single attacker difficult.

During the first six months of 2004, Symantec began identifying groups of compromised hosts performing coordinated scanning patterns. Identifying these coordinated groups allows Symantec to identify bot networks that are engaging in concerted activity. It also allows the detection of some types of worms that would likely go undetected by other methods. Identification of these hosts cannot produce an exhaustive list of all systems participating in a bot network. This is because, in order to limit the number of false positive identifications, multiple behavioral requirements have to be met by each host. As a result, some hosts that may qualify will not be identified.

One of the variables that Symantec uses to identify these groups of compromised systems is scanning with fixed source ports (**Figure 3**). This activity is highly unusual in normal network communications. The top source port, TCP port 4000, is associated

Figure 3. Bot network size (identified by source port)



Source: Symantec Corporation  
TMS data

with exploitation of Internet Security Systems Protocol Analysis Module ICQ Parsing Buffer Overflow vulnerability.<sup>10</sup> The Witty worm, which appeared in the past six months, propagated through this vulnerability.<sup>11</sup> A more complete discussion of the Witty worm and its effects can be found in the “Malicious Code Trends” section of this report.

TCP port 80 was the top source port detected during this reporting period. However, this was not because of coordinated scanning or attempts to bypass firewalls, as one might expect; rather, it was a consequence of spoofed-source DoS attempts. Called “backscatter,” this type of traffic occurs when an attacker spoofs an IP address for a DoS attack and the target replies to the spoofed host from the port that is targeted for attack. Many DoS attacks target TCP port 80 (HTTP); therefore, it is not surprising to detect back-scatter that looks like scans from that source port.

TCP port 220 was the second highest source port. This was a surprising entry in the top source ports and provoked further investigation. Symantec analysts determined that it was used by 2,170 unique IP addresses, almost the same number of hosts identified as associated with port 4000. Symantec remains unaware of any particular attack tool or worm that utilizes port 220 as a source port. Further investigation of the port 220 traffic resulted in an interesting trend (**Figure 4**).

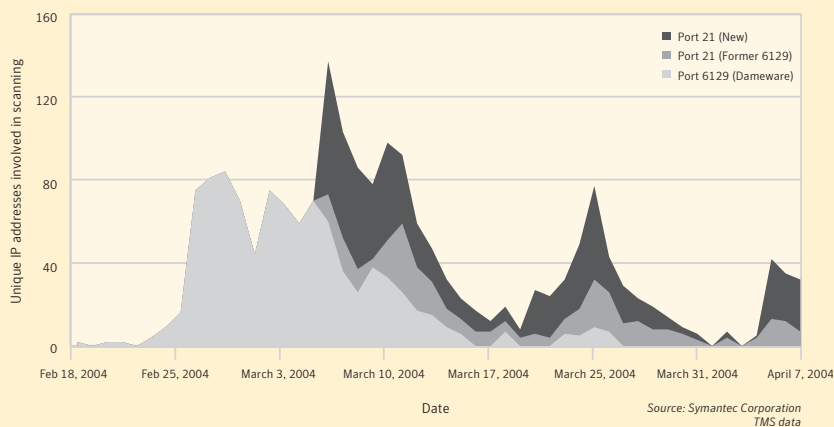
This trend highlights the evolution of scanning patterns that occur with these bot networks. In February, at the beginning of the monitoring period, the scanning originating from TCP port 220 targeted TCP port 6129. Attackers often scan for this port because the Dameware remote access tool operates on it. Both attackers and administrators use Dameware to allow remote access; it can thus be a security risk even though it is also a legitimate tool.

Through March and April, the scanning pattern began to change. Initially, attacking systems scanned for port 6129 and TCP port 21 (FTP). By April, systems were scanning exclusively for port 21. The shift toward TCP port 21 is not likely related to a specific vulnerable FTP server; rather, it is likely related to scanning for systems with badly secured FTP servers, which could be used to distribute illegally copied software, music, and video.

Throughout this period, new attacking systems joined this network. While this particular network is relatively small, reaching a maximum daily size of 140 systems, it shows how bot networks are being used in a coordinated fashion. Even a seemingly minor network of 140 systems can be a significant threat if used as an attack base for a DoS attack or as a launching pad for a new exploit or worm.

As they evolve, identification and detection of bot networks is expected to become more difficult.

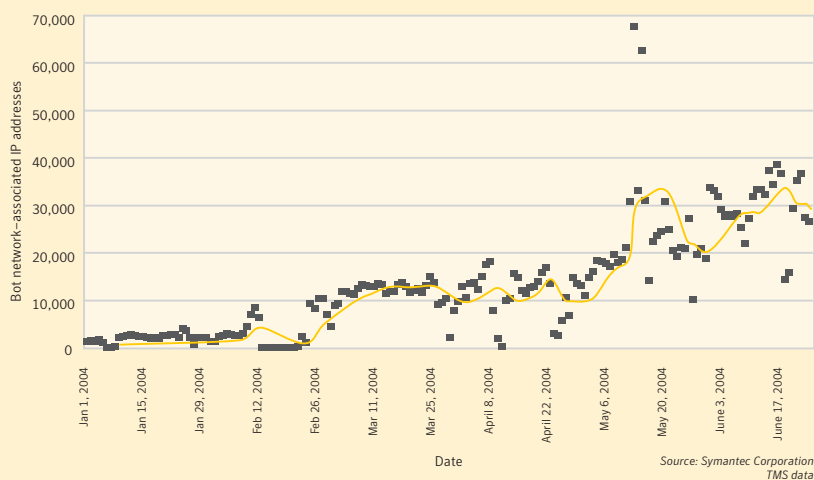
**Figure 4. Source port 220 scan pattern changes**



<sup>10</sup> <http://www.securityfocus.com/bid/9913>

<sup>11</sup> There are other requirements that must be met by each host identified as part of a bot network. This explains why not every host that may have been infected by Witty is identified in this source port analysis.

Figure 5. Daily number of bot network–associated IP addresses



The window of opportunity to protect systems prior to widespread scanning is also likely to decrease. The decreasing time between vulnerability disclosure and the availability of an associated public exploit, which is discussed in the “Vulnerability Trends” section in this report, is likely to be compounded by bot networks that easily incorporate new exploits. The more rapidly upgradeable these bot networks are, the more quickly a public exploit can be integrated into the network, and the sooner widespread scanning for the associated vulnerability can begin.

### INCREASING NUMBER OF BOT NETWORK SYSTEMS

From January 1 through June 30, 2004, Symantec tracked bot network–associated hosts on a daily basis. The number of identified hosts appears to be increasing (**Figure 5**). In January, less than 2,000 systems were identified each day. By late June, this number had risen to over 30,000 systems.

Two significant increases make up a large part of this trend. The first occurred in early March, after the number of identified systems appeared to plateau for a period. The second rise occurred in mid-May, during which there were two days—May 17 and 19—when over 60,000 compromised hosts were identified. These two spikes are related

to scanning for TCP port 5000, Universal Plug and Play (UPnP). Multiple worms and bots are known to scan for this vulnerability, including the W32.Kibuv.B worm,<sup>12</sup> which began spreading shortly before this rise in activity, as well as many variants of Gaobot. The sudden increase in this scanning pattern precludes definitive classification of the tool used.

### TOP ORIGINATING COUNTRIES

This section will discuss the top countries of attack origin (**Table 3**). It is important to note that the country of origin may not necessarily reflect the actual location of the attacker. While it is simple to trace an attack back to the last IP address from which the attack was launched, the computer used to launch the attack 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 an 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.

The United States continues to be the top source country of attacks. However, the percentage of

<sup>12</sup> <http://securityresponse.symantec.com/avcenter/venc/data/w32.kibuv.b.html>

Table 3. Top source countries January 1–June 30, 2004

| Rank<br>Jan–June 2004 | Rank<br>July–Dec 2003 | Country       | Percent of Events<br>Jan–June 2004 | Percent of Events<br>July–Dec 2003 |
|-----------------------|-----------------------|---------------|------------------------------------|------------------------------------|
| 1                     | 1                     | United States | 37%                                | 58%                                |
| 2                     | 3                     | China         | 6%                                 | 3%                                 |
| 3                     | 2                     | Canada        | 6%                                 | 8%                                 |
| 4                     | 5                     | Australia     | 5%                                 | 3%                                 |
| 5                     | 6                     | Germany       | 5%                                 | 2%                                 |
| 6                     | NR                    | Great Britain | 4%                                 | NR                                 |
| 7                     | 9                     | France        | 4%                                 | 1%                                 |
| 8                     | NR                    | Spain         | 3%                                 | NR                                 |
| 9                     | 7                     | South Korea   | 3%                                 | 2%                                 |
| 10                    | NR                    | Netherlands   | 2%                                 | NR                                 |

Source: Symantec Corporation  
TMS and MSS data

attacks that originated from within networks located in the United States dropped substantially over the past six months: from 58% during the last six months of 2003, to just 37% in the first half of 2004. Great Britain, ranked sixth in this reporting period, has returned to the top ten attacking countries after a six-month hiatus.

South Korea, which was ranked second in the second half of 2002 and fourth in the first half of 2003, was ranked ninth in the first half of 2004. This is a notable decline given the high rate of computer penetration and high-speed Internet in that country. Most of the entries in the top five are relatively static compared to the last six-month reporting period. However, Japan, which was ranked fourth in the last half of 2003, is noticeably absent from the top ten source countries.

The drop in the rankings of Korea and Japan from the top attack source countries would seem to indicate that attempts to encourage security awareness in those countries are succeeding. In Volume V of the *Internet Security Threat Report* (March 2004), Symantec stated that authorities in those countries had embarked on an information security education campaign. The attack ratios appear to indicate that this approach is working.

As would be expected, while the percentage of events originating in the United States has decreased, the percentages for many of the other

countries have risen accordingly. In some cases, like that of China, they have doubled. This trend is strongly correlated to the significant change in the rankings of top originating countries by Internet capita, which will be discussed in the next section.

#### 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 4**). This discussion includes all countries with over 100,000 Internet users. (The data on number of Internet users in each country is gathered from the 2003 CIA World Factbook.)

Whereas the United States is the originating country for the most attacks in aggregate, it is not in the top ten originating countries weighted by Internet capita. Canada, which was the source of the most attacks per Internet capita in the last half of 2003, dropped to number nine in the first half of 2004.

Along with Canada, only Israel, Australia, Nigeria, and Finland are holdovers from the second half of 2003. The remaining five countries, including the top country, Latvia, are new entrants in the top ten source countries by Internet capita. Over the last year, reports in the media have linked attacks for profit to former Eastern bloc countries.<sup>13</sup> The fact that Latvia is the source of the highest rate of attacks per Internet capita may support these theories. Symantec will continue to monitor attack activity to determine if there is merit to this claim.

The presence of Macau is surprising. Of the countries included in this analysis, Macau has the lowest number of Internet users. Because of the small sample size, a limited number of attacks may cause a rapid rise in the attacks-per-user ratio. Countries with relatively low Internet populations show greater variability between periods in the per capita analysis, and as such, Macau is unlikely to remain as a top country in future periods.

The downward trend seen in North America and parts of Asia is not as strong as in other parts of the world. Europe has two new entrants—Spain and Turkey—while Israel, Australia, and Finland have all climbed significantly in the ranking. One potential reason for this may be a lack of widespread awareness of information security issues in those countries. Only ongoing analysis of attack activity will indicate if the attack-per-user ratio decreases in regions with widespread computer security education.

#### TARGETED ATTACK ACTIVITY BY INDUSTRY

Attackers choose their targets for many reasons. In some cases, an attack may target 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 6**). 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.

**Table 4. Top source countries per Internet capita**

| Rank<br>Jan-June 2004 | Rank<br>July-Dec 2003 | Country   |
|-----------------------|-----------------------|-----------|
| 1                     | NR                    | Latvia    |
| 2                     | NR                    | Macau     |
| 3                     | 9                     | Israel    |
| 4                     | 10                    | Australia |
| 5                     | 7                     | Finland   |
| 6                     | NR                    | Egypt     |
| 7                     | NR                    | Turkey    |
| 8                     | NR                    | Spain     |
| 9                     | 1                     | Canada    |
| 10                    | 5                     | Nigeria   |

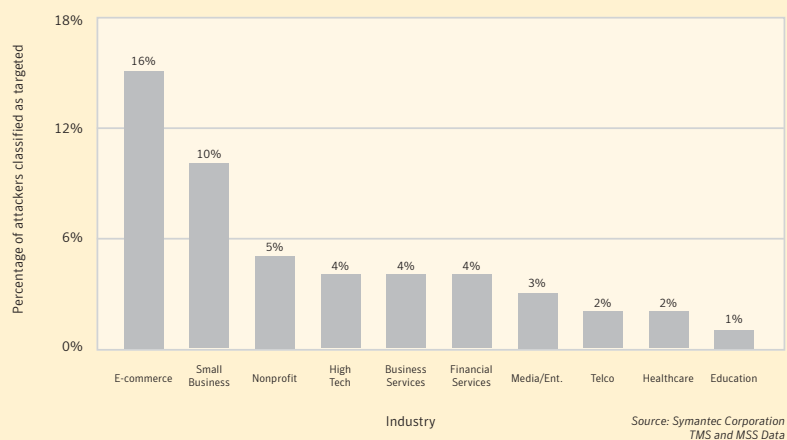
Source: Symantec Corporation  
TMS and MSS data

Over the first half of 2004, e-commerce was the most highly targeted industry. During this period, 16% of attackers attacking e-commerce organizations were considered targeted attackers. This is up dramatically from the last six months of 2003, during which only 4% of attackers against e-commerce were considered targeted.

The rise in targeted attacker rate for e-commerce is worrisome, as these businesses often depend entirely on the Internet for their revenue. This rise may indicate that attackers may be shifting from individuals looking for notoriety toward individuals seeking illicit economic rewards. Whether the attacker intends to obtain customers' personal data, steal money, or blackmail the company, organizations that depend heavily on their Internet presence may be vulnerable to a financially motivated attack.

As with e-commerce, small business has a significantly higher targeted attack rate than other industries. Over the first half of 2004, 10% of attacks against small business were classified as targeted. This is a significant increase over the 3% of targeted attacks observed over the last six months of 2003. One reason for the high ranking may be the increased chance of having multiple businesses within a range of cable or DSL IP addresses. This may mean that some attackers of small business who are considered targeted are simply attacking a range of IP addresses within which multiple small businesses are located.

<sup>13</sup> <http://www.informationweek.securitypipeline.com/22104197>

**Figure 6. Percentage of attackers classified as targeted**

Targeted attacks against the high tech industry dropped by 1% over the first half of 2004. Over the last six months of 2003, high tech was the most highly targeted industry, with a 5% targeted attack rate. However, from January 1–June 30, 2004, only 4% of attacks against high tech organizations appeared to be targeted. Targeted attacks against the healthcare industry also dropped during the current reporting period. This is particularly noteworthy given the rise experienced by most other industries. This may be related to a higher level of security that may be deployed in the health and high tech industries. For instance, Health Insurance Portability and Accountability Act (HIPAA) regulations in the United States require that healthcare organizations meet certain high network security standards.

#### PATTERNS OF ATTACK ACTIVITY BY TIME

Attacks can occur at any hour of the day, any day of the year. Furthermore, the global nature of the Internet transcends local time zones. As a result, an attacker may launch an attack at 12:00 in the attacking system's time zone that is observed by the target system at 04:00 local time. This section will discuss the distribution of attack activity over time during the past six months, both by the time of day and the day of week in which it was observed. Specifically, it will discuss attack activity by attacker's

time of day, worm activity by day of the week, and non-worm activity by day of the week.

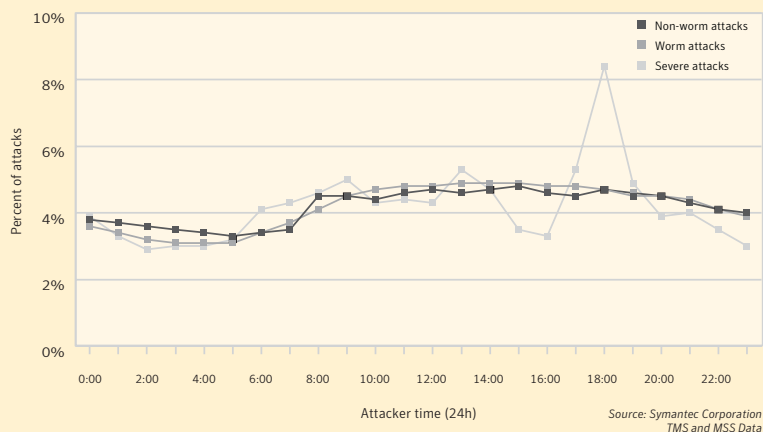
The data does not appear to indicate a significant correlation between target time of day and attack activity; rather, attack activity seems to correlate to the time of day of the attacking systems. Regardless of what conclusions may be drawn from this analysis, attacks can still occur at any time of day and on any day of the week. Organizations must be prepared to monitor and respond to attack activity at all times.

#### Attack activity by attacker's time of day

For the purposes of this report, the local time of the attacking computer was computed from the median time zone of the country in which the IP address is registered. A substantial daily fluctuation can be seen in the time of attack, with a low occurring during the early morning hours for the attacking computer and a high occurring in the afternoon (**Figure 7**). This is similar to the distribution of time observed in the last six months of 2003.

This wave-like pattern corresponds largely with the waking hours of the source countries of the attacks. This is likely related to corporate computers being turned off at certain hours of the day, which would make them unavailable to be used as an attack base by remote attackers. Most experienced attackers

Figure 7. Attacks according to attacker's time of day



will not use their own PCs to attack others; rather, they tunnel their attacks through previously compromised computers. In order for those systems to be used to launch attacks, they must obviously be turned on. This situation is the same for both worm-related attacks and non-worm-related attacks.

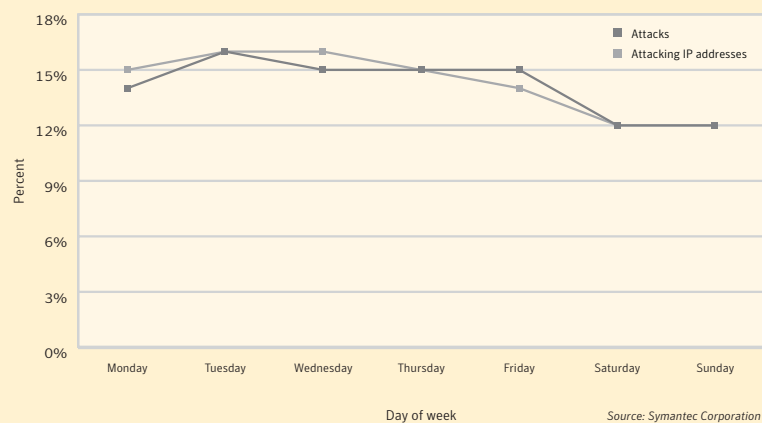
In the first half of 2004, of the three types of attacks, worms tended to exhibit the most stable daily time distribution with the least variability. This pattern is similar to that identified in Volume V of the *Internet Security Threat Report*. Compared to non-worm events, a higher percentage of worm activity occurs in the high-activity hours. The attack rate is consistent over the entire period that a worm-infected computer is turned on. In contrast, a computer that is used as part of a bot network or as a tunnel for a non-worm attack may sit idle for a long period of time, even if it is on, because the attacks are not automated.

The timing of the rise for both worm- and non-worm-related attacks, beginning at 07:00, indicates that a significant number of the computers implicated in this activity are turned on and used during local business hours. This would imply that corporate networks are being used to launch attacks—both automated and manual. The trend shows some

weakening of activity at the end of the business day, around 16:00, but does not begin to significantly decline until late evening, around 23:00. This indicates that home computers, used largely in the evening hours, are also infected at a fairly high rate.

The time distribution of severe attacks displays a similar pattern as the worm and non-worm attacks, with low rates of attack in the early morning hours between 02:00 and 05:00. However, there is a noticeable anomaly between the hours of 15:00 and 20:00. After a significant drop for the hours of 15:00 and 16:00, a significant rise was seen with a peak at 18:00. Initially, it was thought that this was likely the result of a very specific attack. Further investigation has revealed that only a small number of companies experienced an elevated level of attack at 18:00 and that this spike in severe events is not consistent across the sample set.

The very low number of severe attacks means that a relatively small concentrated attack can significantly affect the time distribution of severe events. As noted in the previous version of this report (March 2004), the significantly lower number of severe events, compared to worm and non-worm attacks, results in much greater variability in the distribution of severe events over time.

**Figure 8. Daily distribution of worm attacks**

## ATTACK ACTIVITY BY DAY OF WEEK

Tracking attack activity by the day of the week serves two purposes. First, it allows administrators to see when attacks may be likely to occur. Second, the time distribution of attacks may help security analysts understand what type of attacks are taking place. As was previously stated, regardless of what conclusions may be drawn, organizations must be prepared to monitor and respond to attack activity at all times.

There are two possible ways of measuring attack activity by day of the week. In previous volumes of the *Internet Security Threat Report*, the discussion of attack activity by day of the week was based solely on event counts. For this report, the day of the week distribution of worm and non-worm attacks includes an attack count and IP address count breakdown. Symantec believes that the more automated nature of worms should create a situation in which the daily IP address/attack ratio remains constant while the non-worm IP address/attack ratio will change depending on the attack being performed.

The daily distribution of worm-related events (**Figure 8**) shows a very strong correlation of attack counts and IP counts across all days of the week. This suggests that each worm infection sends out a relatively stable number of events. The percentage of total events and total IP addresses remains within one

percentage point each day. Activity on Saturday and Sunday declines from over 14% of the total attacks to just over 12% of the total attacks. This is consistent for both IP address and event count.

The decline in activity over Saturday and Sunday (non-work days for significant parts of the Internet population) was evident in the first half of 2003 but not in the second half of the year. At that time, Symantec postulated that the reason was related to the Blaster worm. Blaster targeted any unprotected Windows system, including home systems. This means that propagation activity was not likely to be influenced by the workweek. This contrasts with Slammer, the most significant worm in the first half of 2003. Slammer exploited Microsoft SQL Servers, which is almost exclusively a business application. As a result, Slammer activity would have been influenced strongly by corporate activity and would, therefore, have declined during non-working hours. As was discussed in the “Top Internet Attacks” and “Top Attacked Ports” sections, the decrease in Blaster-related attacks and TCP port 135 traffic indicates that Blaster has declined significantly, which may help to explain the return to predominantly business week worm activity.

The non-worm attack breakdown by day of the week (**Figure 9**) shows different behavior for non-worm attackers than for the worm attackers just

discussed. The day of the week distribution of attacking IP addresses shows a similar pattern to non-worm attackers, with decreases in the percentage of IP addresses that attack on weekend days. This behavior is not surprising as attackers often proxy attacks through intermediate computers that have previously been compromised. As with worm attacks, for attacks to originate from these computer systems, they must be turned on. The lower number of IP addresses attacking on weekend days would indicate that some of the systems used to proxy attacks are workplace computers that are turned off during non-work days.

The biggest difference between worm and non-worm attacks is evident in the correlation between attack numbers and attacking IP addresses. Unlike the worm attacks, which saw a very strong correlation between the two, non-worm attacks rise throughout the week, hitting a peak on Saturday before declining slightly on Sunday. This rise in events occurs despite the lower number of individual systems performing the attacks. This would indicate that each attacking system is performing a greater number of average attacks during weekend days.

This relation between attacks and IP addresses would indicate that attackers are more active on the weekends but that there are more limited systems through which to proxy their attacks. The rise in non-worm attacks indicates that attackers are more

active when the organization's staffing levels are likely to be lowest. This supports the need for constant monitoring of security devices in many organizations.

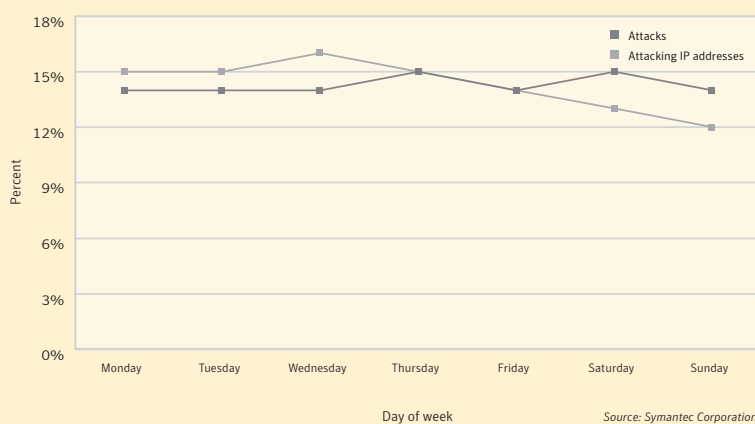
## FORTUNE 100 WORM EXPOSURE

Over the past six months, Symantec observed worm traffic originating from Fortune 100 corporations. This data is gathered not by monitoring the Fortune 100 companies themselves, but by analyzing attack data that reveals the source IP addresses of attack activity. The purpose of this analysis was to determine how many of these systems were infected by worms and actively being used to propagate worms.

Of the address space registered to Fortune 100-ranked corporations, seven companies were identified as Internet service providers (ISPs) and were removed from the sample set. This was done to ensure accuracy in determining infection rates for the largest companies. Many IP addresses registered to ISPs are used by home users with limited security processes in place. As a result, including them in the sample set could skew the result of corporate infection rates. The remaining 93 companies were identified as controlling over 198 million allocated IP addresses.

This discussion includes three caveats. First, security devices can be prone to false positives. Thus, the possibility exists that some of the events identified

Figure 9. Daily distribution of non-worm attacks



**Table 5. Percent of worms detected from Fortune 100 companies**

| Attack   | Percentage of Fortune 100 seen as source |
|--|--|
| Generic WebDAV/Source Disclosure "Translate: f" HTTP Header Request Attack | 27%                                      |
| Slammer Attack   | 20%                                      |
| Microsoft Windows DCOM RPC Interface Buffer Overrun Attack                 | 11%                                      |
| Microsoft Indexing Server/Indexing Services ISAPI Buffer Overflow Attack   | 3%                                       |
| Microsoft IIS 4.0/5.0 Extended UNICODE Directory Traversal Attack          | 3%                                       |

Source: Symantec Corporation  
TMS and MSS data

**Table 6. Attacks originating from Fortune 100-registered IP addresses**

| Attack  | Percentage of Fortune 100 seen as source |
|---|--|
| Generic HTTP POST Containing Script Code Attack                   | 80%                                      |
| Generic TCP Syn Flood DoS Attack                                  | 80%                                      |
| Muhammad A. Muquit Count.cgi Attack                               | 78%                                      |
| Generic HTTP Directory Traversal Attack                           | 77%                                      |
| Microsoft IIS 5.0 .printer ISAPI Extension Buffer Overflow Attack | 73%                                      |
| Generic SMTP Malformed Command/Header Attack                      | 72%                                      |
| Microsoft FrontPage Sensitive Page Attack                         | 70%                                      |
| Typot Trojan Attack   | 68%                                      |
| Generic HTTP 'campus' CGI Attack                                  | 67%                                      |
| Generic Invalid HTTP Version String                               | 61%                                      |

Source: Symantec Corporation  
TMS and MSS data

in this section may not actually represent attacks. Second, it is important to note that the data regarding IP space was gathered from regional registries and may not take into account IP space that contains third-party-administered machines. Third, the list of IP addresses registered to these companies should not be considered exhaustive, as subsidiary companies may register IP space separately from the parent corporation.

It is important to state that while systems associated with these organizations may be used to launch attacks, this does not mean that anyone within or affiliated with the organization is necessarily involved with the attack. Rather, systems that are being used to launch attacks are themselves likely to have been compromised by external attackers. This metric is thus a measurement of the susceptibility of corporate networks to compromise.

Between January 1 and June 30, 2004, 40 of the 93 eligible Fortune 100 companies controlled IP space from which worm-related attacks propagated (**Table 5**). The most common such activity was related to Welchia and was propagated via the WebDAV vulnerability. This attack is strongly associated with Welchia but has been seen in many other forms, including variants of popular bot network software.

Slammer was seen originating from 20% of Fortune 100 registered networks. The Blaster-related DCOM RPC Interface Buffer Overrun Attack was seen coming from 11% of registered networks. Code Red and Nimda still appear to affect a small number of organizations, as the presence of the Microsoft Indexing Server attack and the IIS Extended Unicode Directory Traversal Attack indicate.

The HTTP POST Script Code Attack and the TCP Syn Flood DoS Attack were the top attacks originating from Fortune 100–owned IP addresses, regardless of worm association or potential false positives (**Table 6**). The HTTP POST Script Code Attack is triggered when an HTTP request that contains suspicious strings of characters is detected. This is a generic signature that will be triggered when various types of Web application attacks are attempted.

The TCP Syn Flood DoS attack relies largely on timing of incoming TCP connections. If numerous connection attempts to a popular service from one location are seen, it may be triggered. The Muhammad A. Muquit Count.cgi vulnerability is widely scanned for by various malicious toolkits, but most detections of this attack rely on matching the string “count.cgi” in a Web site’s URL. All three of these attacks can be prone to false positives, which may explain their prominence in this list.

The Microsoft IIS.printer Overflow and the HTTP Directory Traversal Attack are associated with the compromise of improperly secured HTTP servers. Both of these attacks are seen widely across the Internet. The HTTP Directory Traversal Attack is a relatively generic signature to detect an attempt to traverse outside of a known location on a Web server by using a “../” string of code.

The Typot Trojan attack, which originated from 63 organizations, is interesting because the signature is largely based around a static window size of 55808 in a spoofed IP packet. The use of a spoofed packet means that these attacks are unlikely to originate from a Fortune 100 company. Instead, the attack tool is likely picking an address in a range registered by the companies in question. When this 55808 activity was first noted in 2003, the origin of the activity was unknown and thus received significant attention from the security community. Since its peak in 2003, 55808 activity has abated. This may be due to the evolution of the attack tool or because the strategy was ineffective for its purpose.

## CLIENT TENURE AND SEVERE EVENT INCIDENCE

Client tenure is the length of time that an organization has used Symantec Managed Security Services. This metric allows Symantec analysts to assess the result of an organization’s investment in security. Consistent with past reports, this metric revealed that companies with greater tenure were less likely to suffer severe events. Approximately 87% of clients with tenure of more than six months successfully avoided experiencing a severe attack. This is a marked improvement over the previous report, in which over 70% of clients with tenure of more than six months successfully avoided experiencing a severe attack.

Newer clients fared better in the first six months of 2004 than in the last six months of 2003. Nevertheless, companies with less than six months tenure were still four times more likely to experience a severe incident. What this metric does not reveal is that, in addition to an increased incidence rate, newer clients also experienced larger incidents. Only as a client’s tenure increased did both rate and magnitude of attacks decrease.

Aggressive network-based worms such as Sasser continue to be the primary cause of severe events for companies. As the time between the disclosure of vulnerabilities and the release of aggressive worms is very short, companies must have procedures and tools in place to rapidly react before a security incident becomes a severe event.

## Vulnerability Trends

This section of the Symantec *Internet Security Threat Report* will discuss vulnerabilities that have been disclosed over the past six months. The intent of this section is to examine those vulnerabilities and to compare them with vulnerabilities disclosed in the two previous six-month periods. Symantec's recommendations for best security practices can be found in Appendix A at the end of this report. Where appropriate, specific recommendations for the vulnerabilities discussed in this section will be included.

Symantec operates the most popular forum for the disclosure and discussion of vulnerabilities on the Internet. The BugTraq<sup>14</sup> mailing list has approximately 50,000 individual subscribers who receive, discuss, and contribute vulnerability information on a daily basis. Symantec also maintains one of the world's most comprehensive databases of security vulnerabilities, currently consisting of over 10,000 vulnerabilities (spanning more than a decade) affecting over 20,000 technologies from more than 2,000 vendors. This discussion is based on a thorough analysis of that data.

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

- Overall volume of vulnerabilities disclosed in the first six months of 2004

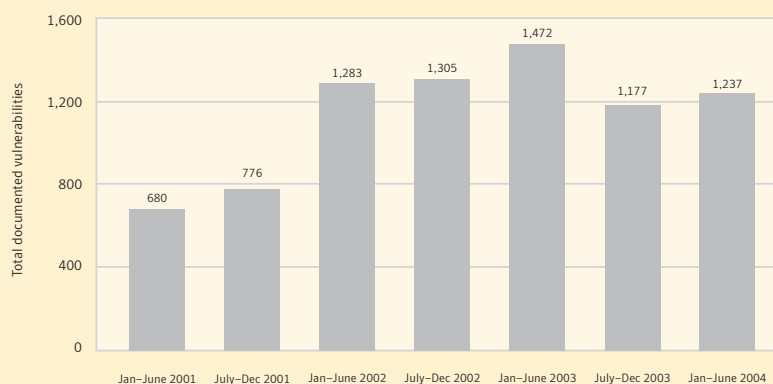
- Severity of vulnerabilities
- Ease of exploitation
- Vulnerabilities with exploit code
- Exploits by severity of vulnerability
- Web application vulnerabilities
- Exploit development time

## OVERALL VOLUME

During the first six months of 2004, 1,237 new vulnerabilities were disclosed (**Figure 10**). This is a 5% increase over the 1,177 new vulnerabilities published during the previous six-month reporting period.<sup>15</sup> On the other hand, this figure represents 16% fewer than the 1,472 vulnerabilities that were disclosed from January–June 2003. However, this decrease is likely an anomaly in a steady long-term increase in the discovery and disclosure of vulnerabilities. As the current composition of the total vulnerability volume is similar to what was observed in prior periods, the decrease from two reporting periods ago does not appear to be anything other than a lull in researcher activity.

The number of new vulnerabilities published each week remains high. On average, during the first half of 2004, 48 new vulnerabilities were published per week. This means that security administrators face the task of reviewing, evaluating, prioritizing, and securing against an average of nearly seven new vulnerabilities every day.

**Figure 10. Total vulnerability volume**



Source: Symantec Corporation

<sup>14</sup> The BugTraq mailing list is hosted by SecurityFocus (<http://www.securityfocus.com>). BugTraq archives are available at <http://www.securityfocus.com/archive/1>

<sup>15</sup> The number of vulnerabilities documented as published during the six-month periods in the *Internet Security Threat Report* will change as vulnerabilities are added and removed after publication.

These numbers indicate that vulnerability research remains a popular pursuit. There is no reason to believe that this will change in the near future. As was stated in the previous *Internet Security Threat Report*, Symantec believes that while worrisome numbers of vulnerabilities continue to be discovered, the rate of discovery has reached a plateau. However, the number of vulnerabilities being discovered is not likely to diminish in the near future. On the contrary, it is likely that the rate of discovery will remain steady for some time.

## SEVERITY OF VULNERABILITIES

Symantec analysts rate vulnerabilities according to their potential severity. Severity is determined by the degree to which the vulnerability gives an attacker access to the targeted system. It is also determined by the potential loss of confidentiality, integrity, or availability of information stored or transmitted upon the system.

For the purposes of the Symantec *Internet Security Threat Report*, each entry in the vulnerability database is categorized according to one of three severity levels. These levels are:

- **Low severity**—Vulnerabilities that constitute a minor threat. Attackers cannot exploit such vulnerabilities across a network. In addition, the impact on the affected system's confidentiality, integrity, or availability is not a complete compromise. 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**—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**—Vulnerabilities that result in a complete compromise of the entire system if exploited. In almost all cases, attackers can exploit high-severity vulnerabilities across a network without authentication.

Of the vulnerabilities disclosed during the six-month period from January to June 2004, 568, or 46% of the total volume, were classified as high-severity threats (**Figures 11 and 12**). This represents an increase of more than 2% over the second half of 2003. It is the same percentage observed in the first six months of 2003, when 513 vulnerabilities were classified as high-severity threats.

If successfully exploited, high-severity vulnerabilities may result in a substantial compromise of the target system. As such, they are more interesting for researchers to discover than less severe vulnerabilities. Discovery of high-severity vulnerabilities can mean more recognition from peers in the research community and, increasingly, media exposure in the case of higher profile high-severity vulnerabilities.

Moderately severe vulnerabilities make up exactly 50% of the new vulnerabilities documented between January and June 2004. This is a slight decrease from the previous six-month period (54%) and is almost equal to the proportion of moderately severe vulnerabilities documented between January and June 2003 (51%). The significant percentage of total vulnerabilities that affect Web-based applications (39%) is driving this trend.<sup>16</sup> Because they are remotely exploitable, Web application vulnerabilities are at least moderately severe.

Low-severity vulnerabilities make up 4% of all vulnerabilities published during this reporting period, up from 2% in the second half of 2003. The percentage of low-severity vulnerabilities documented in the first half of 2003 was 3%. Because their impact on affected systems is minimal, low-severity vulnerabilities tend to be the least interesting to researchers. They also draw the least attention from the security community and the media. This is likely one reason that researchers seek and report relatively few low-severity vulnerabilities.

<sup>16</sup> Web-based applications are those with Web-based interfaces. The applications can often reside on Web servers and rely on a Web browser to provide the user-interface.

Figure 11. Monthly volume by vulnerability severity

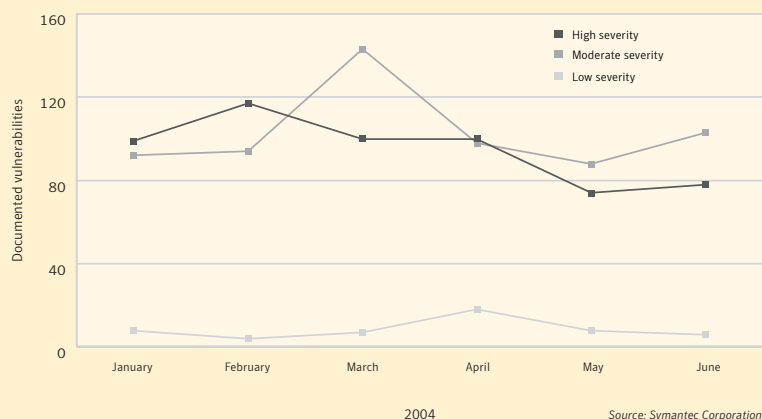
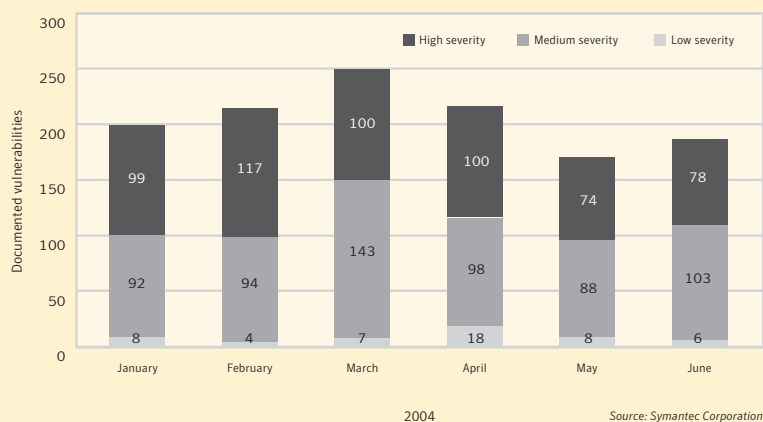


Figure 12. Breakdown of total volume by severity



As these numbers indicate, during the six-month period from January to June 2004, 96% of new vulnerabilities were rated as high or moderate severity. This continues the trend toward more severe vulnerabilities that was reported in the two previous volumes of the *Internet Security Threat Report*. This seems to confirm that researchers continue to focus their efforts on identifying vulnerabilities that will have a substantial impact on affected systems. It further reinforces the notion that researchers are less likely to search for low-severity vulnerabilities.

## EASE OF EXPLOITATION

Symantec rates each vulnerability according to how difficult it is for an attacker to exploit it to compromise a targeted system. This rating assumes a base level of attacker sophistication. That is, it assumes that the attacker possesses 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” or “no exploit available” according to three criteria:

- **No Exploit Required**—With a reasonable amount of technical knowledge, the attacker can exploit the vulnerability without any exploit code.
- **Exploit Available**—This rating is set when publicly available exploit code has been developed.
- **No Exploit Available**—This value is assigned when there is no exploit code yet available but would be required in order to exploit the vulnerability.

Vulnerabilities that require no exploit or that have a required exploit available are classified as “easily exploitable.” Generally, these 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 simply by entering an appropriate URL into a Web browser.

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 made publicly available. To exploit these vulnerabilities, an attacker would be required to write custom exploit code (assuming

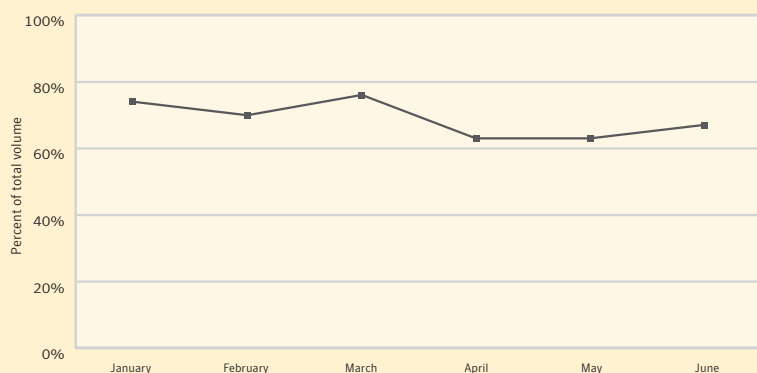
that there is none circulating in the underground). This significantly raises the level of knowledge, expertise, and effort required for a successful attack, thus increasing the difficulty and lowering the probability of such an attack. It should be pointed out that while no tools may be publicly available, private exploits might exist. However, without a public exploit, these vulnerabilities are unlikely to be widely exploited.

During the first six months of 2004, Symantec classified 858 vulnerabilities, or 69% of all new vulnerabilities, as easy to exploit (**Figure 13**). This is similar to the percentages that were reported in 2003. In the first half of that year, 72% of total vulnerabilities were easy to exploit, as were 70% in the second half of 2003.

By comparison, 379, or 31% of the total volume, of the vulnerabilities disclosed in the current reporting period were classified as difficult to exploit. This number is consistent with the two previous reporting periods. In the second half of 2003, 29% of all vulnerabilities discovered were classified as being difficult to exploit, as were 30% in the first half of that year.

Between January and June 2004, 52% of vulnerabilities disclosed require no custom code to exploit (**Figure 14**). This is roughly the same number as was discovered in the two previous reporting periods. Between July and December of 2003,

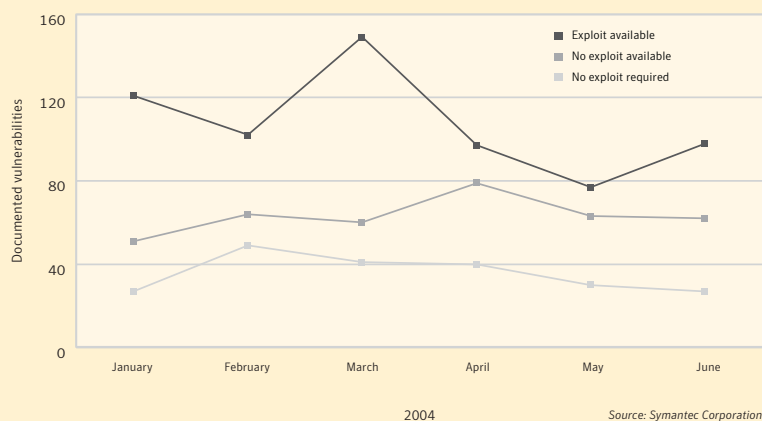
Figure 13. Easily exploitable vulnerabilities



2004

Source: Symantec Corporation

Figure 14. Ease of exploit breakdown



49% of vulnerabilities did not require exploit code compared to 53% in the first half of the same year. The increasing percentage of vulnerabilities that affect Web-based technologies contributes to this trend.

Many of these were cross-site scripting and HTML/SQL injection vulnerabilities, which can be exploited by manipulating fields through a Web browser without exploit code. One example of such a vulnerability is a cross-site scripting vulnerability that affected Microsoft Outlook® Web Access.<sup>17</sup> This vulnerability allowed attackers to execute script code in another user's browser. It was addressed in Microsoft Security Bulletin MS03-047. The high number of vulnerabilities in this ease of exploit category in the first half of 2004 corresponds to an increase in vulnerabilities affecting Web-based applications (see the "Web Application Vulnerabilities" discussion on the next page).

#### VULNERABILITIES WITH EXPLOIT CODE

For vulnerabilities that require exploit code, there were slightly fewer associated exploits disclosed in the first half of 2004 than in the two previous six-month reporting periods, both in number and as a proportion of total vulnerability volume (Figure 15).<sup>18</sup> From January 1 to June 30, 2004, 165 vulnerabilities were published for which associated exploit code

was available, or 13% of the total volume of vulnerabilities. This is lower than the previous six-month period when exploit code was available for 207 vulnerabilities, or 18% of the total volume. It is also lower than the first half of 2003, when exploit code was available for 209 vulnerabilities, or 14% of all vulnerabilities disclosed.

#### EXPLOITS BY SEVERITY OF VULNERABILITY

In the two previous volumes of the *Internet Security Threat Report*, Symantec observed that exploit developers were focusing their efforts on writing exploit code almost exclusively for moderately and highly severe vulnerabilities. This trend has continued in the first six months of 2004 (Figure 16), although the proportions have changed slightly.

In the first half of 2004, 64% of the vulnerabilities for which exploit code is available were classified as highly severe. This is an increase of 7% compared to the period of July–December, 2003. In the first half of 2003, the percentage was 58%.

In the first half of 2004, 36% of the vulnerabilities with associated exploit code published were classified as moderately severe. This is a decrease of 5% from the second half of 2003, during which a percentage of 41% was observed. The percentage seen during the first half of 2003 was 39%. This signals a decline

<sup>17</sup> Microsoft Exchange Server 5.5 Outlook Web Access Cross-Site Scripting vulnerability: <http://www.securityfocus.com/bid/8832>

<sup>18</sup> Due to the methodology by which dates are assigned to exploits, the number of exploits that are listed as available during a reporting period may change from one issue of the ISTR to the next. When ISTR V was written (January 2004) exploit code was available for 17% of vulnerabilities disclosed in the second half of 2003. This is still higher than the proportion for the first half of 2004.

Figure 15. Vulnerabilities with exploit code

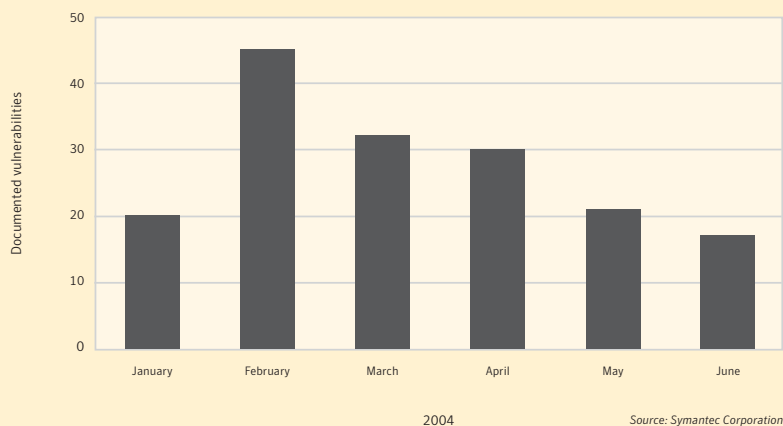
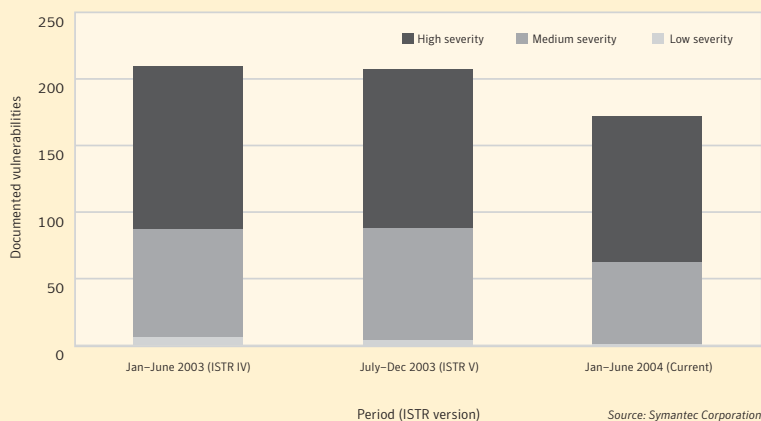


Figure 16. Vulnerabilities with exploit code by severity



in publication of exploit code for moderately severe vulnerabilities. This may be because researchers have shifted their focus to high-severity vulnerabilities or have less desire to write exploit code for vulnerabilities with a moderate impact.

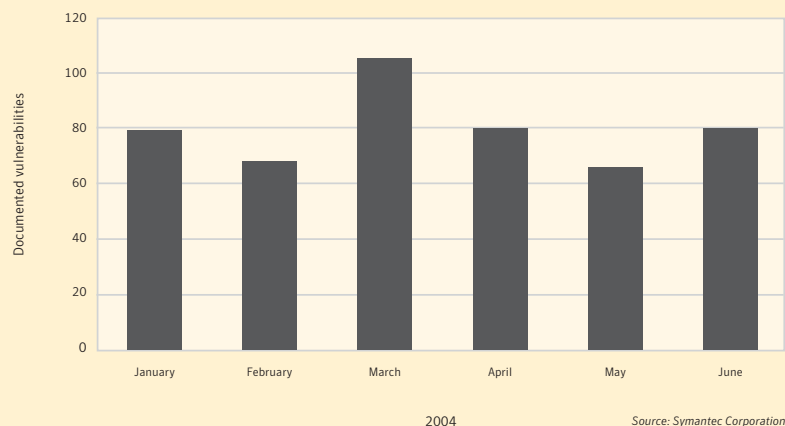
During the current reporting period, only one vulnerability with associated exploit code was classified as low severity.<sup>19</sup> This represents less than 1% of the total number of vulnerabilities with exploit code documented during this period. This is a drop from the 2% seen in the second half of 2003 and

3% in the first half. The tendency to develop exploits for more severe vulnerabilities has been consistent since the start of 2003. Researchers clearly favor expending the time and energy required to develop exploit code for vulnerabilities that are more severe; that is, when they have the most to gain (in terms of level of compromise) from a successful attack.

## WEB APPLICATION VULNERABILITIES

Web application vulnerabilities affect technologies that rely on a browser for their user interface and are often hosted on Web servers. Web application

<sup>19</sup> It is likely that exploit code will be added to vulnerabilities documented during this period after the time of writing. These may be represented in future volumes of the *Internet Security Threat Report*.

**Figure 17. Web application vulnerabilities**

vulnerabilities typically include attacks such as cross-site scripting, SQL injection, HTML injection, and so on.

These vulnerabilities, which are often easily exploited, continue to make up a substantial portion of the total vulnerability volume. As noted in the earlier “Ease of Exploitation” discussion, vulnerabilities targeting Web applications are considered easily exploitable and contribute significantly to the fact that the number of easily exploitable vulnerabilities is as high as it is. Their prevalence is likely due to the increasing use of the World Wide Web as a tool for building and delivering applications.

Many security researchers consider Web application vulnerabilities to be generally straightforward. As such, they represent a significant problem for organizations worried about information theft. This is because they can allow an attacker to access confidential information from databases without having to compromise any servers. Furthermore, because they can be sent through open anonymous proxies, they are often difficult to track.

In the first half of 2004, 479 vulnerabilities, or 39% of the total volume, were associated with a Web application technology (**Figure 17**). This is an increase of 8% over the 31% seen in the second half of 2003, and is also higher than the 35% observed in the first half of the same year.

## EXPLOIT DEVELOPMENT TIME

In the first half of 2004, worms such as Sasser and Witty appeared remarkably soon after the disclosure of the vulnerability that they targeted. Previous *Internet Security Threat Reports* (specifically Volume V) have reported that the time between vulnerability announcement and release of an associated exploit is short. This indicates that exploit writers are becoming increasingly sophisticated; that is, they are writing more effective exploit code more quickly, while at the same time requiring fewer publicly available vulnerability details to develop exploit code.

Over the past six months, Symantec has analyzed the average time between the publication of vulnerability details and the initial appearance of functional or semifunctional exploit code associated with that vulnerability. The objective of this analysis is to obtain an approximate average period of time required for development of exploit code for a certain subset of vulnerabilities. It is hoped that this will provide organizations with a measure of the response time they have once a vulnerability is published.

These vulnerabilities are assumed to be reasonably complex and require a reasonable level of skill to exploit. This analysis also assumes that the attacker began working on the exploit code after disclosure

of the vulnerability, and that he or she had no prior knowledge of the details of the vulnerability. Therefore, the criteria for exploits that were considered in this analysis were as follows:

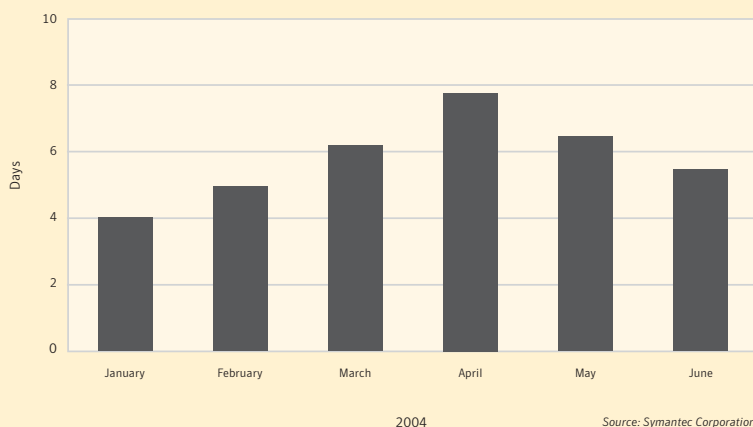
- The exploit must apply to a vulnerability that is not trivially exploitable; that is, one that requires exploit code.
- The exploit must be functional or able to be made functional with relative ease; that is, totally non-functional proof-of-concept code programs are excluded. For example, proof-of-concept exploits that simply cause an application to crash when the vulnerability allows code execution would be excluded.
- The exploit must appear to be authored by an individual or group that is independent of the party who discovered the vulnerability.
- The exploit must appear to have been developed after the disclosure of the vulnerability and as a result of the disclosure. The intent is to measure how long it takes, on average, for an individual or group (third party) to author exploit code once the details of the vulnerability are available. It is impossible to tell what the development time for exploit code was in instances where either the

discoverer of the vulnerability wrote the exploit code or where the code appeared before disclosure of the vulnerability. For this reason, such instances have been excluded from the sample set.

The results of this analysis have shown that between January and June 2004 third-party functional exploit code was developed and published, on average, 5.8 days after the announcement of the associated vulnerability (**Figure 18**).<sup>20</sup> The fact that functional exploit code can be assembled by independent researchers and published in under a week is worrisome but not surprising.

Many of the vulnerabilities included in this count were reasonably complex,<sup>21</sup> yet exploit code was published almost immediately. These observations highlight the need for administrators to either patch, if possible, or implement other measures to protect against new threats as soon as possible. This is particularly challenging for large organizations, for which applying enterprise-wide patching in a matter of days is nearly impossible, especially when patching individual workstations and laptops is required.

Figure 18. Average number of days for exploit development



<sup>20</sup> It should be noted that there were two instances in 2004 where exploit code appeared more than 30 days after disclosure of the vulnerability. Those instances were excluded after comparing the complexity of the associated vulnerability to others and concluding that the author of the exploit had likely not started development immediately after announcement.

<sup>21</sup> The Witty worm is a good example. Another example is the Symantec™ Client Firewall Remote DNS Response DoS vulnerability (<http://www.security-focus.com/bid/10336>), the exploit for which was published two days after the vulnerability was announced.

## Malicious Code Trends

This section of the *Symantec Internet Security Threat Report* will analyze developments in malicious code over the first six months of 2004. Symantec gathers data from over 120 million client, server, and gateway systems 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 submission process. This discussion is based on malicious code samples submitted to Symantec for analysis between January 1 and June 30, 2004.

This report analyzes and discusses submissions in three ways: (1) according to unique instances of malicious code, such as MyDoom and Netsky; (2) according to the category or type of malicious code in question, such as viruses, worms, and Trojans; (3) according to the overall volume of all malicious code combined. For example, the overall volume of malicious code submissions to Symantec™ Security Response continues to grow. However, the distribution of the various types of malicious code has changed over the past six months, with submissions of bots and adware increasing significantly (**Table 7**).

### DOMINANCE OF WIN32 THREATS

Win32 threats are executable files that operate by using the Win32 API (application program interface), which provides a standard for the development of software on the Windows platform.

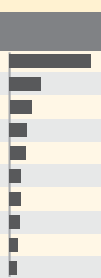
These forms of malicious code all work on at least one Win32 platform. Given the Windows current market dominance, Win32 threats will likely be the predominant type of malicious code for the foreseeable future. In addition to this, other types of malicious code will also continue to affect Win32 systems.

Symantec first reported an increase in Win32 threats in the second half of 2002. The volume of these attacks is still increasing. During the first six months of 2004, Symantec documented more than 4,496 new Win32 viruses and worms (**Figure 19**). This compares to 994 in the first six months of 2003 and 1,702 in the second half of that year.

Since they were first discovered on August 18, 1998, Win32 viruses and worms have become more common than script- and macro-based threats. As of June 30, 2004, the total number of documented Win32 threats and their variants exceeded 10,000. By comparison, there are approximately 8,200 known macro viruses. In fact, Win32-based threats now make up the majority of new unique submissions received by Symantec. During the first six months of 2004, Symantec documented almost twice as many Win32 threats as had been reported from the discovery of the first Win32 threat until December 31, 2003. In the month of June 2004 alone, the number of Win32 threats increased by over 1,000—more than the number reported in the first six months of 2003.

MyDoom<sup>22</sup> and Netsky<sup>23</sup> were the most significant and high-profile Win32 worm outbreaks in the first half of 2004. MyDoom.A was the top submission received by Symantec during this period. First discovered on January 26, MyDoom.A was responsible for one of the worst mass-mailer worm outbreaks ever seen. The worm carried a backdoor that allowed anyone to control a compromised system remotely. It also performed a DoS attack against several targets,<sup>24</sup> using Web browser requests to bombard the target hosts to prevent easy filtering, a simple strategy that has traditionally been used to mitigate worm-brokered DoS attacks.

**Table 7. Top ten malicious code submissions received by Symantec**

| Rank | Sample     | Submissions |   |
|------|------------|-------------|---|
| 1    | MyDoom.A   | 247,615     |  |
| 2    | Netsky.P   | 95,230      |   |
| 3    | Gaobot.gen | 66,782      |   |
| 4    | Netsky.B   | 51,629      |   |
| 5    | Netsky.D   | 47,813      |   |
| 6    | Netsky.C   | 35,483      |   |
| 7    | Beagle.M   | 33,886      |   |
| 8    | Bugbear.B  | 32,225      |   |
| 9    | Sasser.C   | 26,217      |   |
| 10   | Redlof.A   | 21,573      |   |

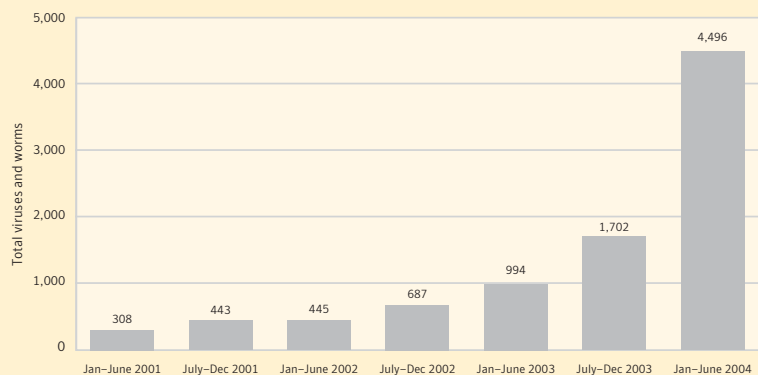
Source: Symantec Corporation

<sup>22</sup> <http://securityresponse.symantec.com/avcenter/venc/data/w32.mydoom.a@mm.html>

<sup>23</sup> <http://securityresponse.symantec.com/avcenter/venc/data/w32.netsky.d@mm.html>

<sup>24</sup> This is discussed in more detail in the "Blended Threats" discussion in this section.

Figure 19. Newly documented Win32 viruses and worms



Source: Symantec Corporation

The outbreak occurred extremely quickly. According to the data gathered by Symantec, over 12,000 instances of MyDoom.A were seen during the initial outbreak period, although this is a small fraction of the total number of systems affected. The DoS component of MyDoom variants targeted numerous high-profile targets, including the Recording Industry Association of America (RIAA) and Microsoft. As a result, two of the targeted companies—SCO and Microsoft—offered rewards for information leading to the arrest of the worm’s author.

Netsky was discovered on March 28, shortly after the release of MyDoom. Variants of Netsky make up four of the top ten malicious code submissions during this reporting period. Netsky subverted some gateway scanners by occasionally sending itself in an archive using a seemingly innocuous .ZIP extension. Users would unzip the file, then inadvertently run the virus. This strategy was particularly effective because, in general, .ZIP files have been treated as safe and most common attachment filtering configurations would permit them.

In addition to this innovative proliferation method, Netsky was noteworthy because it attempted to disable variants of the Mimail<sup>25</sup> and MyDoom worms

on systems it infected. This proceeded to spark a competition between the authors of MyDoom and Netsky, which is discussed later in this report.

The Beagle mass-mailer worm was the eighth-ranked submission in the first six months of 2004. Beagle is notable because it used a propagation technique similar to that of Netsky. However, it took the technique one step further by occasionally password-protecting the Zip-file archive,<sup>26</sup> relying on the fact that people are more likely to trust password-protected files. This allowed the message attachment to bypass many email gateways and scanners, since they are unable to scan inside a password-protected archive file. This represents two disturbing new trends. First, the creators of mass-mailing worms are becoming more creative in the techniques they employ. Second, it is troubling that even with the extra effort required on the part of the user to open a password-protected archive and execute the file contained within, a significant number of users are still being infected with these worms. Fortunately, these Beagle variants do not require any more complex removal methods than the previous variants.<sup>27</sup>

<sup>25</sup> <http://securityresponse.symantec.com/avcenter/venc/data/w32.mimail.t@mm.html>

<sup>26</sup> The password required to open the archive was included in the email message body or as a JPEG file attached to the message. See <http://securityresponse.symantec.com/avcenter/venc/data/w32.beagle@mm!zip.html> for details.

<sup>27</sup> <http://securityresponse.symantec.com/avcenter/venc/data/w32.beagle@mm.removal.tool.html>

## BLENDED THREATS

Blended threats can use multiple methods and techniques to spread. They may also 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.<sup>28</sup> As a result, blended threats can infect large numbers of systems in a very short time with little or no human intervention, causing widespread damage very quickly. The multiple propagation mechanisms often used in blended threats allow them the versatility to circumvent an organization's security in a variety of ways. They can then simultaneously overload system resources and saturate network bandwidth.

In the first six months of 2004, the overall volume of blended threat submissions to Symantec increased by 58% over the last half of 2003 (**Table 8**). However, while the total number of blended threat submissions increased, the number of individual blended threat submissions as a proportion of all malicious code submissions actually declined slightly compared to the previous six-month period. In the first half of 2003, blended threats made up 51% of the top 50 submissions. In the second half of that year, 61% of the top 50 submissions were blended threats. In the first half of 2004, 60% of the top 50 submissions were blended threats, a decrease of 1% over the previous six months.

MyDoom, at over 247,000 submissions, and Netsky, at over 95,000 submissions, were the two most prolific blended threats in the first half of 2004. The third most common blended threat was Gaobot.<sup>29</sup> The number of blended threats was greatly enhanced by the many variants of Gaobot. Over the past six months, 1,104 variants of Gaobot were published—almost nine times the 127 documented in the last six months of 2003. Gaobot variants now have the ability to exploit a wide range of vulnerabilities, including (but not limited to):

- The Microsoft Universal Plug and Play (UPnP) NOTIFY Buffer Overflow<sup>30</sup>
- The Windows Locator Service Buffer Overflow<sup>31</sup>
- Two DCOM RPC Buffer Overrun vulnerabilities<sup>32</sup>
- The “WebDav”/NTDLL vulnerability<sup>33</sup>

It is also important to note that Gaobot allows a malicious attacker to easily create a new variant that exploits different vulnerabilities. This is because the Gaobot code allows new exploits to simply be “plugged into” the bot. They can also propagate via backdoors installed by other worms.

MyDoom and Netsky propagated primarily through email. However, Sasser<sup>34</sup> was a reminder that email is not the only way to infect machines on a large scale, exploiting the LSASS vulnerability<sup>35</sup> to propagate. This method was effective enough that

**Table 8. Top ten blended threats submitted**

| Rank | Blended Threats | Vulnerability   |
|------|-----------------|---|
| 1    | MyDoom.A        | No vulnerability exploited  |
| 2    | Netsky.P        | Microsoft IE MIME Header Attachment Execution Vulnerability       |
| 3    | Gaobot.gen      | Numerous vulnerabilities  |
| 4    | Beagle.M        | No vulnerability exploited  |
| 5    | Bugbear.B       | Microsoft IE MIME Header Attachment Execution Vulnerability       |
| 6    | Sasser.C        | Microsoft Windows LSASS Buffer Overrun Vulnerability              |
| 7    | Beagle.X        | No vulnerability exploited  |
| 8    | Blaster.F       | Microsoft Windows DCOM RPC Interface Buffer Overrun Vulnerability |
| 9    | MyDoom.F        | No vulnerability exploited  |
| 10   | Netsky.Q        | Microsoft IE MIME Header Attachment Execution Vulnerability       |

Source: Symantec Corporation

<sup>28</sup> By contrast, a worm simply creates new copies of itself.

<sup>29</sup> <http://securityresponse.symantec.com/avcenter/venc/data/w32.hllw.gaobot.gen.html>

<sup>30</sup> <http://www.securityfocus.com/bid/3723>

<sup>31</sup> <http://www.securityfocus.com/bid/6666>

<sup>32</sup> <http://www.securityfocus.com/bid/8205> and <http://www.securityfocus.com/bid/8459>

<sup>33</sup> <http://www.securityfocus.com/bid/7116>

<sup>34</sup> <http://securityresponse.symantec.com/avcenter/venc/data/w32.sasser.worm.html>

<sup>35</sup> <http://www.securityfocus.com/bid/10108>

Symantec DeepSight Threat Management System observed approximately 160,000 unique hosts generating activity associated with Sasser variants during the first weekend of their outbreak.

Blended threats are exhibiting increasingly destructive payloads. For example, the Witty<sup>36</sup> worm was injected into memory on hosts that it exploited. It featured a very destructive payload that corrupted the content of the hard drives of compromised systems. This is unusual, since destroying the host potentially prevents the worm from propagating further. However, Witty's payload would slowly corrupt small areas of the hard drives to maximize the length of time for which it could propagate before the host would fail. Since the vulnerability Witty exploited was in an intrusion detection system (IDS) product, it could send its payload to variable destination ports. Because an IDS must examine all packets entering a network, the vulnerability could be exploited regardless of the destination port.

Witty also illustrated another worrisome trend: the rapidly diminishing time between the announcement of a vulnerability and the release of an associated exploit. Witty exploited a buffer overflow vulnerability in the ICQ parsing routines of the protocol analysis module in ISS BlackICE™ in order to propagate.<sup>37</sup> The worm appeared in the wild only two days after the vulnerability was disclosed, leaving many unpatched systems for it to target. The danger of this small window of exploitation was demonstrated by the fact that the Symantec DeepSight Threat Management System sensors detected more than 26,500 unique instances of Witty in its first four days in the wild.

## MALICIOUS CODE COMPETITION

Malicious code authors sometimes create programs that compete or conflict with one another, either intentionally or unintentionally. Authors of worms that install backdoors on systems may not want any other malicious code to run on the system, as it might interfere with the initial worm's activities or

alert the user to the presence of the worm. To prevent this from happening, the author may build code into the worm that removes other worms from an infected system.

The first half of 2004 saw interesting developments in the competition between computer worm authors. Previously, some worms would uninstall other malicious code from a compromised host. For example, the Welchia<sup>38</sup> worm would terminate the process of the Blaster<sup>39</sup> worm and delete its executable file. In the current reporting period, this competition appeared to become more overt and hostile. As mentioned earlier in this report, Netsky attempted to disable variants of the Mimail and MyDoom worms on systems it infected. Other examples of this competition include the following:

- Beagle attacked Netsky and vice versa. The code for some variants of these worms contained a "war of words," in which the authors included messages to each other within the code. Additionally, different variants of each worm would remove the other from infected computers.
- The B variant of Welchia attacked MyDoom, removing some variants of the MyDoom worm from any computers it infected.<sup>40</sup>
- Dabber exploited a vulnerability in the FTP server of Sasser. It used this vulnerability to propagate to computers already infected with Sasser. It then deleted registry entries created by other worms.
- Gaobot committed a vampire attack against Sasser. A vampire attack refers to a worm that injects itself into the process space of another worm that is already running on a system. The existing worm's routines are then subjugated to perform the actions of the attacking worm. This caused systems infected by Sasser to continue to scan for vulnerable systems, but instead of sending Sasser to these vulnerable systems, the infected systems sent Gaobot.

<sup>36</sup> <http://securityresponse.symantec.com/avcenter/venc/data/w32.witty.worm.html>

<sup>37</sup> <http://www.securityfocus.com/bid/9913/discussion>

<sup>38</sup> <http://securityresponse.symantec.com/avcenter/venc/data/w32.welchia.worm.html>

<sup>39</sup> <http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.worm.html>

<sup>40</sup> Welchia.B deleted files and registry keys created by the A and B variants of the MyDoom worm.

- Doomjuice used the backdoor of MyDoom to propagate.<sup>41</sup> This provided a propagation vector almost as effective as exploiting an unpatched vulnerability.

In some of these cases, the worm's author may simply be taking advantage of flaws or backdoors in other malicious code to aid in the propagation of their own creations. In other cases, one worm may attack another due to a conflict or vendetta between the authors themselves. In other cases, the competition may be the result of the professionalization of hacking, and may signal a battle for control of zombie systems that can be leased to spammers.<sup>42</sup> Whatever the motivation in any individual instance, the damage to end users has been greater than damage to the opposing author.

### P2P/IM/IRC/CIFS

Instant messaging (IM), peer-to-peer services (P2P), and Internet relay chat (IRC) are all applications that support file sharing. However, in the workplace they are often used with little or no corporate oversight. As they allow users to share files that may include potentially malicious code, this makes them a fertile infection vector. In fact, seven of the top ten threats over the first half of 2004 used one or more of these services to propagate. This is an increase over the first half of 2003 when three of the top ten submissions propagated via these vectors. In the second half of 2003, four of the top ten submissions used these vectors to propagate.

MyDoom and Netsky, which dominate the top ten submissions, both use P2P as a secondary mechanism to propagate. MyDoom searches the registry to locate the Kazaa-shared folder and simply copies itself to that directory using a variety of enticing filenames. Netsky performs a similar action, searching the hard drive for any directories that appear to be a P2P-shared folder. It then copies itself to these directories using a preconfigured list of file names that are commonly searched for. When users search the Kazaa file-sharing network for files matching these file names, they will inadvertently download and possibly execute the worm.

Worms that use Windows file sharing (CIFS)<sup>43</sup> to propagate made up three of the top ten submissions

in each of the last three reporting periods. The prime example of this is Bugbear.B,<sup>44</sup> which has been in the top ten submissions for all three periods.

Some malicious code threats, such as Gaobot, are able to use Windows file sharing to exploit weak passwords in order to copy and execute themselves on remote machines. Gaobot was submitted to Symantec close to 67,000 times in the current reporting period, accounting for almost 6% of the top 50 submissions. It attempts to connect to available Windows network shares by using a dictionary of commonly used passwords. Once connected to a remote machine with a weak password, Gaobot copies itself to the machine and executes itself remotely.

Overall, the volume of threats using P2P, IM, IRC, and CIFS within Symantec's top 50 submissions increased more than 100% over the previous six-month period (**Figure 20**). However, similar to the last six-month period, no IM threats were listed in the top 50 submissions to Symantec. One of the reasons that IM threats are sparse could be that since most of these applications rely on a central server to relay messages between users, it would be easy for the provider to filter messages carrying malicious code. Spybot and Swen, both of which use IRC, remain in the top 50 submissions for this six-month period.

Data transferred via IM, IRC, P2P, and CIFS often bypasses corporate access control measures and thus may be difficult to manage. Organizations should determine the business necessity for these file-sharing mechanisms and limit employees' usage of these services accordingly. In addition, insecure versions of these services should be prohibited and organizations should ensure that strong password policies are met. Finally, organizations must define and enforce policies outlining proper usage of these services.

### MOBILE DEVICES/PDAS

Many popular mobile devices, such as PDAs and smart phones, run full-fledged operating systems, such as Pocket PC™, Symbian™, and Palm™, among others. Each operating system provides a standard API for development of applications. This API can

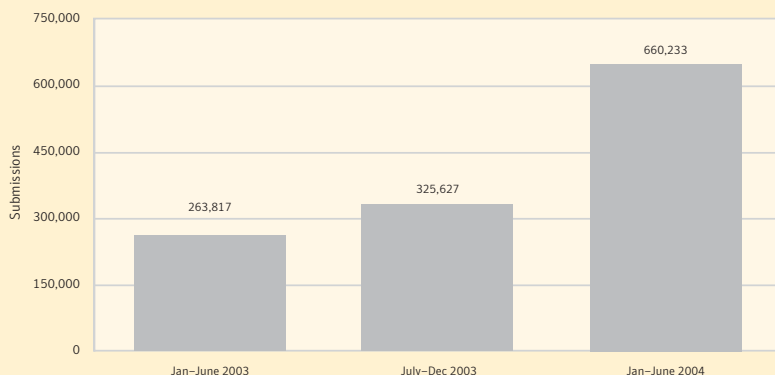
<sup>41</sup> At the time that Doomjuice was discovered, only the A and B variants of MyDoom were in the wild. The A, B, D, E, and K variants of MyDoom all use the same backdoor port, meaning that Doomjuice would be capable of propagating through any of these.

<sup>42</sup> [http://www.theregister.co.uk/2004/04/30/spam\\_biz/](http://www.theregister.co.uk/2004/04/30/spam_biz/)

<sup>43</sup> CIFS is not unique to Windows; however, most, if not all of the threats apply only to Windows systems.

<sup>44</sup> <http://securityresponse.symantec.com/avcenter/venc/data/w32.bugbear.b@mm.html>

Figure 20. P2P, IM, IRC, and CIFS in top 50 by volume



Source: Symantec Corporation

also be used in the development of malicious software. However, these operating systems and devices are relatively new and still limited in distribution.

In June 2004, the first mobile device worm was developed. Named Cabir, the worm has not yet been reported in the wild. It spreads via Bluetooth on Symbian Series 60 devices such as smart phones, cellular telephones with computer-enabled features such as LAN connectivity and full Internet connectivity. Cabir repeatedly sends itself to the first Bluetooth-enabled device that it can find, regardless of the type of device. It will even send itself to a Bluetooth-enabled printer if it is within range. (Of course, the printer will not become infected, as it is unlikely to be running the Symbian Series 60 operating system.) In addition, Cabir installs a small program known as a recognizer, which will allow the worm to start itself whenever the smart phone is turned on.

Cabir spreads as a Symbian install package (a .SIS file) and will generate multiple warning dialogues before actually being installed. These warnings are standard Symbian-implemented dialogues. They include a prompt to accept the Bluetooth connection and another to authorize the installation of an

unsigned application. Only after the user has accepted multiple prompts will the worm install itself onto the system and begin executing.

Even if Cabir were to be released in the wild, the worm would not spread very quickly due to the multiple dialogues the user would be required to accept and the fact that Bluetooth is not running by default on most devices. Furthermore, Bluetooth devices typically must be within ten meters for effective communication; thus, a worldwide outbreak would be highly unlikely. However, this would not preclude the possibility of small, localized outbreaks in high traffic areas such as airports, convention centers, or even shopping centers.

Cabir does not contain a deliberate payload, apart from the vastly shortened battery life caused by the constant scanning for Bluetooth-enabled devices.<sup>45</sup> It now joins the few other malicious code threats for mobile devices including two Trojans—Vapor<sup>46</sup> and Liberty<sup>47</sup>—and one overwriting virus, Phage,<sup>48</sup> for the Palm operating system.

The low number of threats for mobile devices is due to the limited number of mobile devices and the relatively new developer environment. Nevertheless, Multimedia Messaging Service (MMS) worms, classic viruses, and backdoor Trojans are all

<sup>45</sup> Some malicious code commentators believe that shortened battery life constitutes a "power virus," a form of DoS attack. Power viruses of a different type can also attack and damage desktops and servers by overheating the processor. Intel has added clockrate throttling logic to some of their higher powered Xeon processors to guard against power viruses. For added discussion, see [http://www.theregister.co.uk/2001/03/23/intel\\_moves\\_to\\_throttle\\_throttlebottle/](http://www.theregister.co.uk/2001/03/23/intel_moves_to_throttle_throttlebottle/)

<sup>46</sup> <http://securityresponse.symantec.com/avcenter/venc/data/palm.vapor.html>

<sup>47</sup> <http://securityresponse.symantec.com/avcenter/venc/data/palm.liberty.a.html>

<sup>48</sup> <http://securityresponse.symantec.com/avcenter/venc/data/palm.phage.dropper.html>

technically feasible on these devices. As mobile computing becomes more common and mobile devices like cellular phones become more complex, it is likely that other avenues of attack will be discovered.

### TROJAN HORSES

A Trojan horse (also known as a Trojan) is a program that neither replicates nor copies itself but may cause damage to or compromise the security of a host in some way. Trojans appear to serve some useful purpose, which encourages users to download and run them, but actually carry a destructive program. They may masquerade as legitimate applications available for download from various sources or be sent to an unsuspecting user as an email attachment. Since Trojans do not replicate like viruses and worms (although they may be delivered by worms), they typically do not receive as much media attention. However, if they are executed on a computer they can be extremely destructive, with payloads ranging from unauthorized export of confidential data to surreptitious reformatting of hard drives.

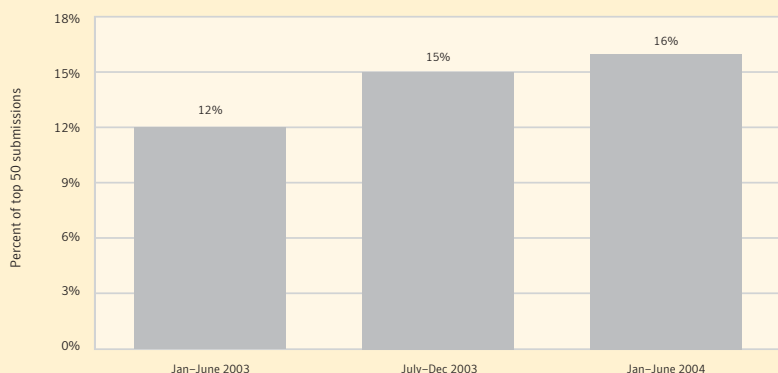
From January 1 to June 30, 2004, over 16% of the top 50 submissions received were Trojans (**Figure 21**). More than 1,000 new Trojans were submitted to Symantec during each of the last three reporting

periods, reflecting the wide variety of Trojans currently found in the wild.

Trojans are increasingly being installed via malicious Web sites. They exploit browser vulnerabilities that allow malicious code authors to download and execute the Trojans with little or no user interaction. This was recently illustrated by a series of system compromises involving Microsoft Internet Information services servers. The IIS servers were compromised so that exploit code was attached to all the Web pages they served.<sup>49</sup> When a user viewed one of these pages using Microsoft Internet Explorer, a Trojan was installed on the user's system through multiple client-side vulnerabilities in the browser. The Trojan was then used to record authentication credentials for certain Web sites and send them to a remote attacker.

Such attacks may also target specific users or organizations.<sup>50</sup> In these cases, a simple keystroke-logging Trojan may be used to compromise a corporate VPN and gain access to internal servers. Many newer Trojans are also written to steal specific information from compromised systems. For example, the Bancos<sup>51</sup> family of keylogging Trojans monitors Microsoft Internet Explorer title bars for specific strings that will appear when a user visits the online

**Figure 21. Trojan horses**



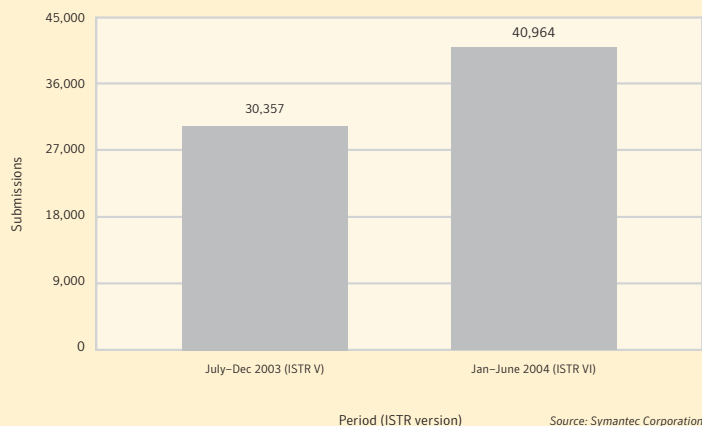
Source: Symantec Corporation

<sup>49</sup> <http://tms.symantec.com/documents/040624-Alert-CompromisedIIServerReports.pdf>

<sup>50</sup> <http://tms.symantec.com/documents/040617-Analysis-FinancialInstitutionCompromise.pdf>

<sup>51</sup> <http://securityresponse.symantec.com/avcenter/venc/data/pwsteal.bancos.html>

Figure 22. Adware submissions in top 50



banking sites of certain Brazilian banks. When a matching string is found, the Trojan displays a login window that mimics that of the bank. Any information the user enters into this window is then sent to a remote FTP server. In addition to online banks, PayPal, eBay, and other online services are popular targets of password-stealing Trojans.

Trojans incorporate a wide variety of functionality ranging from exposure of information to file deletion and DoS attacks. While in the past, many Trojans simply provided unauthorized remote access to compromised computers, newer Trojans are becoming more complex and purpose-driven. Several recent Trojans, such as the Mitglieder<sup>52</sup> family, install covert proxies on compromised computers. These proxies allow the system to be used to relay various network protocols such as the Simple Mail Transfer Protocol (SMTP). Because this allows attackers to use the system to relay spam, these Trojans may cause a significant increase in network and system load.

#### Expanded Threats: Adware and Bots

Expanded threats exist outside the traditional definitions of worms, Trojans, and viruses. They can encompass adware and spyware (although adware and spyware often perform similar functions) that typically represent some violation of user privacy or

confidentiality. According to the number of submissions to Symantec in the first six months of 2004, expanded threats appear to be becoming more common (**Figure 22**).

Overall, adware dominates the expanded threats category, accounting for about 80% of expanded threats. Spyware represents about 20%. The top 50 list of threats submitted by Symantec customers in the last six months contains six widespread adware packages (Adware.InstantAccess, Adware.lefeats, Adware.MainSearch, Adware.Gator, Adware.NetOptimizer, and Adware.Binet) but no spyware packages.

Adware packages perform numerous operations, including displaying pop-up ads (Adware.InstantAccess, Adware.NetOptimizer), dialing to high-cost numbers through the system's modem if one is present (Adware.InstantAccess), modifying browser settings such as the default home page (Adware.lefeats, Adware.MainSearch), and monitoring the user's surfing activity to display targeted advertisements (Adware.Binet, Adware.Gator). The effects range from mere user annoyance to privacy violations to monetary loss (in the case of dialers<sup>53</sup>).

<sup>52</sup> <http://securityresponse.symantec.com/avcenter/venoc/data/trojan.mitglieder.html>

<sup>53</sup> Dialers are programs that use a system's modem without the user's permission to dial to toll numbers, typically to accrue charges.

Threats in the adware category are becoming more common. In the last six months, the most frequently submitted piece of adware was Adware.InstantAccess, a combination of pop-up adware and dialer. It was submitted to Symantec over 19,000 times between January 1 and June 30, 2004. In contrast, Symantec received only 27 submissions of it in July–December 2003 and none in January–June 2003. In the previous six-month period, the top adware was Adware.Binet. It was submitted only 2,000 times, although some adware downloaders were massively reported independent of the adware programs themselves.<sup>54</sup>

Expanded threats can be installed in numerous ways: as self-contained packages, with network applications like P2P clients, or on vulnerable machines through exploits. For instance, the second and third most reported adware packages—Adware.Iefeats<sup>55</sup> and Adware.MainSearch<sup>56</sup>—belong to the CoolWebSearch family. This group is installed through an exploit for the Microsoft Java Virtual Machine Bytecode Verifier vulnerability.<sup>57</sup> This vulnerability allows specially crafted Web pages to surreptitiously run arbitrary code on vulnerable machines, thus making “drive-by downloading”<sup>58</sup> possible.

Another example of the use of an exploit to install adware packages is the much-publicized 180 Solutions Trojan.<sup>59</sup> This Trojan installed Adware.Ncase,<sup>60</sup> which exploited the previously unpublished Modal Dialog Zone Bypass vulnerability<sup>61</sup> to coerce Microsoft Internet Explorer clients into installing the adware package.

The implications of adware are inherently difficult to quantify. However, this does not mean that they are not a security concern. The most significant implication may be the potential for widespread loss of integrity in individual end-user systems. In addition, because adware is unauthorized, surreptitiously installed software, administrators have no knowledge of or control over what the adware may be running. For instance, they could be used to monitor users' browsing habits (in order to display directed advertisements), constituting a loss of

privacy. Most adware packages are also capable of dynamically updating themselves, often with new functionality that the user is unaware of.

Symantec's research has shown that there are good technical countermeasures to adware, such as implementing more restrictive Web browser settings. In addition, many companies have security policies in place that prohibit users from downloading or installing unauthorized software on corporate computers. Despite this, users often knowingly engage in activities that risk exposure of confidential information.<sup>62</sup>

## BOTS

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. Bots are used for a wide variety of malicious purposes, such as information theft, stealing application serial numbers, or stealing user passwords. They are also used to establish networks of “zombie” machines to be used in distributed denial-of-service (DDoS) attacks.

The most prevalent bots, such as Gaobot, Randex, and Spybot, have the ability to replicate by conventional means, such as copying themselves to network shares with weak password protection and to the shared folders of P2P network clients. They may also replicate by exploiting remote vulnerabilities.

The number of bots has been steadily increasing over the first six months of 2004. During this period, variants of the Gaobot family alone accounted for 67,000 submissions received by Symantec. The Randex and Spybot families of bots were also very widespread, accounting for 10,000 and 8,000 customer submissions, respectively.

<sup>54</sup> Once the downloader component is detected by antivirus software, it will not be able to download and execute the adware on the system.

<sup>55</sup> <http://securityresponse.symantec.com/avcenter/venc/data/adware.iefeats.html>

<sup>56</sup> <http://securityresponse.symantec.com/avcenter/venc/data/adware.mainsearch.html>

<sup>57</sup> <http://www.securityfocus.com/bid/6221>

<sup>58</sup> Drive-by downloading is a process by which a program is downloaded and installed on a user's system without the user's knowledge, intervention, or permission.

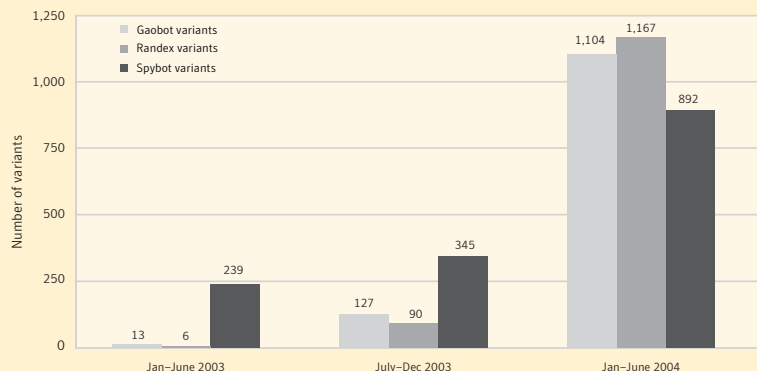
<sup>59</sup> <http://www.securityfocus.com/archive/1/365695>

<sup>60</sup> <http://securityresponse.symantec.com/avcenter/venc/data/adware.ncase.html>

<sup>61</sup> <http://www.securityfocus.com/bid/10473>

<sup>62</sup> <http://securityresponse.symantec.com/avcenter/reference/privacy.attitudes.behaviors.pdf>

Figure 23. Bot variants



Source: Symantec Corporation

The number of distinct variants of these bots is increasing dramatically. Documented variants of Spybot increased by almost 200%, from over 300 to almost 900 in the last six months. The number of Gaobot variants increased by 600%, from over 100 to over 1,100. And the number of Randex variants rose by 1,100%, from almost 100 variants to nearly 1,200 (Figure 23). Variants of Gaobot in particular present an array of original features, including polymorphism, stealth techniques, exploits for newly discovered vulnerabilities, and the use of multiple layers of run-time packers.<sup>63</sup>

Similarities in code and the usage of common master IRC servers suggest that some families of bots are closely related. Some evolved from a common ancestor. For instance, the Sdbot backdoor was reused in Randex and Kwbot, for which worm functionality was added by spreading through shares or P2P networks. Multiple bots often inherit the same exploit modules from a single source. The occasional publication of the source code for a bot variant also makes it easier to swap modules between worm families.

The trend of merging Trojan, backdoor, and worm functionalities into single threats is becoming apparent in bots (further illustrating the tendency toward blended threats that was discussed earlier

in this “Malicious Code Trends” discussion). As is the case with some Win32 worms, there are signs of cooperation and competition between worm and bot families. For instance, some variants of the Dumaru worm install Spybot on infected machines. Conversely, it is likely that some bot authors are competing for territory, trying to get the largest zombie networks under their command.

One way to establish such a territory is to establish a “seed” network. The high initial numbers of Witty may have been aided by the use of a seed network to propagate the worm. This seed network was likely a network of computers compromised by IRC bots. The Witty author probably owned this network and used the compromised hosts to send out the Witty payload, even though the systems on this network were not running the vulnerable software. It is also possible that the author may have mapped vulnerable systems prior to releasing Witty into the wild and had the initial payload packets sent to these vulnerable hosts first, rather than targeting random systems.

Systematic use of unpatched Windows vulnerabilities partially accounts for the success of exploit-based bots such as Gaobot. Since the publication of the Windows RPC DCOM vulnerability in the summer of 2003 and the ensuing success of the Blaster worm,

<sup>63</sup> Packers are tools that compress and encrypt Windows executable files. This is a concern for security personnel because it makes detection by antivirus engines more difficult.

many more worms and bots have used exploits to spread, including Spybot. As demonstrated by the success of Gaobot, whose recent variants commonly exploit up to a dozen vulnerabilities, many unpatched systems remain on the Internet. These systems represent easy targets for attackers.

There are several steps that security administrators can take to protect against the proliferation of bots. These include hardening systems and keeping machines patched against new vulnerabilities. In addition, administrators should use strong outbound filtering and proxies, and should configure firewalls to control external network connections. These steps can prevent bots from contacting their master IRC servers. However, as the recent growth in bots has demonstrated, this can be difficult to achieve.

## Future Watch

The previous sections of this report have discussed Internet security developments over the past six months. In this section of the *Internet Security Threat Report* we will discuss emerging trends and issues that Symantec believes will become more prominent over the next six months. These forecasts are based on emerging data that Symantec has collected during the current reporting period. In anticipating future trends, Symantec hopes to provide organizations with an opportunity to prepare for the rapidly evolving and complex security environment in which they find themselves.

## PHISHING

Phishing is an attempt by a third party to solicit confidential information from an individual, group, or organization, often for financial gain. Perpetrators attempt to trick users into disclosing credit card numbers, online banking information, or other sensitive information that is then used to commit fraudulent acts. Symantec has identified phishing as one of the top threats to watch for in the coming months. Over the past year alone, it is estimated that phishing cost U.S. banks and credit card issuers nearly US\$1.2 billion in damages. It is further estimated that over 1.78 million people have fallen victim to online fraud as a result of phishing.<sup>64</sup>

Phishing may be conducted through email, spam, spyware, and blended threats. Perpetrators have used spoofed<sup>65</sup> email to trick users into entering confidential information into fraudulent Web sites or forms.<sup>66</sup> Often, the email appears to be from a legitimate source such as eBay or PayPal, but it directs the victim to a malicious Web site. These sites often look exactly like the authentic ones and thereby trick users into thinking that they are providing their confidential information to the legitimate site. This information is collected by fraudulent parties and used for credit card fraud and identity theft.

<sup>64</sup> <http://enterprisesecurity.symantec.com/article.cfm?articleid=4445&EID=0>

<sup>65</sup> "Spoofed" refers to altered email headers, IP addresses, and other identifying characteristics that convince a user that the source of the soliciting email is trusted and valid.

<sup>66</sup> <http://www.securityfocus.com/infocus/1745>

Symantec continues to monitor this situation and recommends that administrators and users employ caution when opening email attachments. Enterprises and ISPs should update their security policies to alert users to these threats and inform them how to avoid being victimized. Individuals are also advised to thoroughly verify any requests for confidential information before disclosing any potentially sensitive information via email or through an online form or Web site.

## SPAM

Over the next six months, Symantec believes that spam and threats associated with it will continue to rise. In particular, Symantec forecasts a rise in the use of spam as a propagation vector for more traditional threats and as a tool in phishing.

During the current reporting period, Symantec noticed a marked increase in the amount of spam being distributed across the Internet. Spam, usually defined as junk or unsolicited email from a third party, made up over 60% of all email traffic during this reporting period. What was once merely an annoyance is now a serious security concern as Trojans, viruses, and phishing attempts continue to spread through spam. For example, the Mimap.B<sup>67</sup> downloader used spam to propagate the Mimap.P<sup>68</sup> worm, which in turn used a phishing attack to entice users to install the payload on their systems. Once it was installed, users were presented with fake PayPal dialogue boxes that could then send captured information to the original attackers.

In addition to threats contained in spam messages themselves, 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. The volume of email generated by spammers<sup>69</sup> forces administrators and users to expend already overextended resources filtering suspect messages and scanning for malicious code. As such, the costs associated with preventive and mitigating strategies are increasing.

Symantec recommends that enterprises deploy effective antispam measures in their organizations and filter email messages at the gateway. Additionally, users should follow accepted best practices and continue to be cautious in opening all email messages.

Symantec continues to monitor this situation and recommends that administrators and users employ caution when clicking on URLs, responding to emails, and opening email attachments. They should also deploy antispam technologies wherever possible. As was stated in the previous section, organizations and ISPs should update their security policies to alert users to these threats and inform them how to avoid being victimized. Individuals are also advised to thoroughly verify any requests for confidential information before disclosing any potentially sensitive information.

## CLIENT-SIDE ATTACKS

Previous volumes of the *Symantec Internet Security Threat Report* have cited browser vulnerabilities as potentially serious emerging threats. Because of its market dominance, it was expected that such threats would particularly affect Microsoft Internet Explorer. Recent events have borne out those concerns.<sup>70</sup>

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, P2P networks, IM 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.

Active exploitation of browser vulnerabilities<sup>71</sup> has shown that client-side vulnerabilities are very attractive to attackers. This is because it is much easier to exploit a single vulnerable workstation through a universally exploitable client-side vulnerability than to penetrate the target organization from outside the perimeter defenses. Compounding this risk is the fact that the users on client systems may not be as security conscious as security administrators, whose primary role is to secure networks and servers.

<sup>67</sup> <http://securityresponse.symantec.com/avcenter/venc/data/downloader.mimail.b.html>

<sup>68</sup> <http://securityresponse.symantec.com/avcenter/venc/data/w32.mimail.p@mm.html>

<sup>69</sup> "Spammers" is a colloquial term used to refer to people who send spam.

<sup>70</sup> This refers to recent active exploitation of several Microsoft Internet Explorer vulnerabilities. Another apparently targeted attack is described at

<http://tms.symantec.com/documents/040617-Analysis-FinancialInstitutionCompromise.pdf>

<sup>71</sup> <http://www.securityfocus.com/bid/10517>

Browser vulnerabilities are partially caused by errors in the way that data—almost all of which is external in origin and considered untrustworthy—is processed. Other client-side applications are also vulnerable, as is security software such as VPN clients and personal firewalls. Many of these applications will accept data from any source, even with firewall and other security measures in place. As such, they are perfect targets for effective client-side exploits.

The success of recent vulnerabilities such as the Adobe Acrobat/Reader File Name Handler Buffer Overflow Vulnerability<sup>72</sup> in attacking individual hosts, suggests that we will likely see more targeted attacks against other client-side applications in the near future. Additionally, the risk posed by these threats is enhanced by the shrinking window of time between the announcement of a vulnerability and the release of an associated exploit (as discussed in the “Vulnerability Trends” section in this report). Symantec recommends that administrators and users continue to monitor their environments and apply patches as soon as possible on affected systems and applications.

## BROADBAND ROUTER AND FIREWALL DEVICES

To guard against direct, unprotected exposure to the Internet, many home, small office, and mobile computer users opt for a firewall or router device to serve as a physical barrier between their systems and the Internet. While these devices are relatively inexpensive and easy to configure, they are also becoming increasingly popular targets for vulnerability researchers.

The Symantec vulnerability database documented over 20 vulnerabilities in these perimeter devices in 2004. The vulnerabilities ranged from remote crashes and resets to a full compromise of the device, which allowed administrative access to remote attackers. For example, as technical details of these devices have become public,<sup>73</sup> attackers have modified the firmware<sup>74</sup> to provide internal access and even allow attackers to monitor traffic on the network.

Additionally, with hardware devices, the patching process may be difficult for many end users. Patching often requires users to download updated software and install it on the device. This can be an issue if users are not aware of the vulnerability or are unfamiliar with the patching process. Furthermore, there is often no easy way for a vendor to notify users that a patch must be installed. As a result, it is highly likely that most of these devices are using outdated and vulnerable firmware.

As more and more employees connect remotely to corporate networks through these devices, security administrators must now deal with additional risks such as the potential for DDoS attacks that compromised machines may launch. Also, improperly configured devices could lead to compromised hosts transmitting confidential company information such as documents and passwords.

While these devices are critical components in preventing successful attacks against hosts connected to the Internet, many of them appear to be fragile and vulnerable. Successful exploitation of these flaws can expose an organization’s network to attack. Symantec recommends that users check vendor Web sites for updated firmware and patches on a regular basis and that users connecting to corporate networks should use a secure virtual private network (VPN) in order to assist in protecting confidential information.

## REMOTELY CONTROLLED BOT NETWORK ACTIVITY

As mentioned in both the “Attack Trends” and “Malicious Code Trends” sections of this report, remotely controlled bot networks are a growing security threat. Bot networks are an effective way of compromising and controlling large networks of systems, with new tools and exploits continuously being developed. The short vulnerability-to-exploit window makes these bots even more dangerous. They can quickly be upgraded with new exploits. The bots can then widely scan and attack a new vulnerability very quickly without the additional

<sup>72</sup> <http://www.securityfocus.com/bid/10696>

<sup>73</sup> <http://www.seattlewireless.net/index.cgi/LinksysWrt54g>

<sup>74</sup> Firmware is the combination of software and hardware that provides the functionality of the application.

coding that would be required for a successful worm. This makes it difficult to patch systems in a timely manner.

Bot networks are employing increasingly sophisticated methods of control and synchronization that are hard to detect, are decentralized, and obscure the network's communication channels.<sup>75</sup> Symantec continues to watch developments in bot networks and believes that malicious code that implements this concept in some format will be developed in the near future. In order to protect against this possibility, Symantec recommends that administrators implement strong firewall rules in addition to logging and auditing of incoming and outgoing connections.<sup>76</sup>

## PORT KNOCKING

Port knocking is a method to broker direct connections to compromised hosts. It involves observing all traffic on a network for a specific key. When this key is detected, a port is opened on the host, allowing communication. Originally developed as a tool to make network communications more secure, port knocking can be used by an attacker to compromise a remote host. Discussed and presented in various forums,<sup>77</sup> it is simply awaiting a workable implementation in a backdoor application.

Port knocking presents a serious concern because it can defeat common port scanning techniques—used both by administrators and attackers—that audit networks and compromise older backdoors. Should this functionality be included in compromise tools, it will become critical for organizations to constantly monitor their network connections and develop new methods to detect suspiciously coordinated network events.<sup>78</sup>

Though Symantec has not yet detected any implementations of port knocking, that does not mean they do not exist. Attackers will often keep new methods of compromise to themselves for as long as possible in order to maximize their ability to control systems. Administrators should continue to audit their network connections and take note of any suspicious or anomalous activity.

## MALICIOUS CODE FOR LINUX

Malicious code in all forms continues to be a significant issue for administrators and users.<sup>79</sup> Over the past six months, Symantec has seen limited malicious code activity in the Linux community. Due to numerous base package and code variations between Linux platforms, worms and other forms of malicious code have had a difficult time propagating between different Linux operating systems.

This does not mean, however, that consumer and enterprise users of Linux should be any less vigilant. Some techniques originally observed in DOS and Win32 file infectors continue to be adapted to the Linux environment, an indication that efforts to develop malicious code across Linux platforms continue. The file header infection in Linux.Thebe and host data compression in Linux.Cassini are two examples of this type of activity.

Even though no significant worm outbreaks have plagued Linux (or BSD) systems in the last six months, a steady flow of vulnerabilities has been discovered and used in proof-of-concept exploits. Symantec expects that these may be used as exploit-based worms in the near future. As such, Symantec will continue to monitor the development of malicious code directed at Linux-based systems.

Administrators and users of Linux systems are cautioned that even though their systems are not currently targeted by as much malicious code activity as the Win32 environment, this does not mean that Linux is immune to exploitation. Symantec recommends that administrators and users continue to monitor new developments in the Linux community and follow recommended best practices.

## SPYWARE

Many adware packages already bear similarities to spyware by monitoring a user's Web-browsing habits. Spyware is often installed surreptitiously on a user's computer when the user downloads free software from the Internet. It may be downloaded in conjunction with legitimate applications or through illegitimate means, such as exploitation of client-side vulnerabilities in Web browsers. In addition to

<sup>75</sup> One of the first attempts at this type of control was found in the Typot Trojan first discussed in ISTR IV.

<sup>76</sup> Bot networks usually use port 6667 for their communications; disallowing outgoing connections to this port can help control some of these issues.

<sup>77</sup> <http://www.securityfocus.com/archive/105/355843/2004-07-29/2004-08-04/1>

<sup>78</sup> For example, the port knock followed by the connection.

<sup>79</sup> The forms include viruses, Trojans, worms, and blended threats.

privacy and confidentiality issues, this software often will redirect users to adult Web sites, provide unwanted pop-up ads, and even update itself dynamically.<sup>80</sup>

In both the home and enterprise environments, spyware is rapidly becoming a serious security concern, particularly as most corporate networks allow HTTP traffic, the means by which spyware is propagated. Employees browsing a Web site could inadvertently install spyware on their corporate desktop that could expose the enterprise to malicious code such as password-stealing programs.<sup>81</sup>

Symantec continues to view spyware as a significant threat and recommends that both enterprise and home users continue to update their antivirus software. Security administrators should take extra measures to maintain a strong security posture on client systems. They should also ensure that client system patch levels are up-to-date and that acceptable usage policies are in place and enforced.

#### MALICIOUS CODE MUTATIONS— FIRST-GENERATION POLYMORPHISM

During the first six months of 2004, Symantec observed a number of developments that indicate that malicious code continues to evolve to keep pace with changes in computing technologies. For example, malicious code mutations otherwise known as first-generation polymorphism<sup>82</sup> continued to appear in worms like Gaobot and Beagle.

Advanced virus infection strategies that render previous antivirus scanning techniques obsolete appeared for the Microsoft .NET Framework. For example, Impanate, the first parasitic, entry-point obscuring (EPO) appending virus was created. Unlike traditional viruses, an EPO virus does not place its code near the beginning or end of an infected file but in an unknown location. Impanate was followed by Gastropod, the first metamorphic virus. Metamorphism changes the body of the virus between replications, resulting in significantly different patterns between generations.

These advanced infection mechanisms may render many traditional antivirus scanning techniques

ineffective. EPO viruses require larger chunks of files to be scanned in order to locate and remove an infection. Metamorphic infectors require an antivirus scanner to pick the useful pieces of code from an infected file one by one. Scanning for these types of viruses may place a large burden on system resources, significantly affecting performance.

As malicious code is developed for new platforms and devices, network administrators must continue to adopt protection technologies and policies to cope with this evolving landscape. Symantec recommends that users and security administrators continue to update their antivirus products regularly, as new, effective algorithms have been developed that scan for these new types of threats.

#### PORTABLE DEVICES

Symantec continues to monitor the development of malicious code on portable devices. Examples include the Rugrat virus,<sup>83</sup> which is the first virus known to infect portable executable files on the 64-bit Windows on IA-64 platforms, Cabir,<sup>84</sup> the first worm to infect Symbian OS smart phones using Bluetooth technology to replicate, and Duts.A,<sup>85</sup> the first parasitic infector of portable executable files on the Windows CE platform. Also, Brador.A,<sup>86</sup> the first backdoor Trojan to target Windows Mobile™ operating systems, was discovered on August 5, 2004.

Duts.A demonstrates that virus techniques that appeared on PC viruses can be reused to infect files on mobile devices. While the infection method that Duts uses is simplistic and requires user intervention, it is likely that advanced techniques will appear on mobile platforms in the future, more closely mirroring the evolution of PC viruses.

All of these examples demonstrate the ability of malicious code authors to adapt new technologies for their own purposes. They also reflect an increased sophistication in the development and propagation of malicious code. Symantec recommends following accepted best practices. Security administrators should continue to follow developments in this area.

<sup>80</sup> <http://www.securityfocus.com/columnists/250>

<sup>81</sup> <http://securityresponse.symantec.com/avcenter/venc/data/spyware.rempsteal.html>

<sup>82</sup> A polymorphic virus is one that can change its byte pattern when it replicates, thereby avoiding detection by simple string-scanning techniques.

Worms have recently started employing polymorphism.

<sup>83</sup> <http://securityresponse.symantec.com/avcenter/venc/data/w64.rugrat.3344.html>

<sup>84</sup> <http://securityresponse.symantec.com/avcenter/venc/data/epoc.cabir.html>

<sup>85</sup> <http://securityresponse.symantec.com/avcenter/venc/data/wince.duts.a.html>

<sup>86</sup> <http://securityresponse.symantec.com/avcenter/venc/data/backdoor.brador.a.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 that emergency response procedures are in place.
9. Educate management on security budgeting needs.
10. Test security to ensure that adequate controls are in place.

### Consumer Best Practices

1. Use an Internet security solution that combines antivirus, firewall, intrusion detection, and vulnerability management for maximum protection against blended threats.
2. Ensure that security patches are up-to-date.
3. Ensure that passwords 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](http://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 ISP or local police.

## 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. Symantec has selected a sample set of customers from each service that have uploaded data throughout the complete period.

**Table 9** provides high-level details of the methods used by each service.

### ATTACK DEFINITIONS

In order to avoid ambiguity with our findings, Symantec’s methodology for identifying various forms of attack activity is outlined clearly in the table 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. Presented in the following copy is a high-level summary of the distinctions used in the report.

**Attacks**—Attacks are individual signs of potential 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 as to 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.”

**Table 9. Data collection methods used by Symantec services**

| 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.  | 51%                                |
| Symantec Managed Security Services          | Symantec Managed Security Services provides real-time monitoring and analysis of attack activity launched against more than 500 companies worldwide. The interactive monitoring that MSS analysts perform is required for some statistics, such as event severity, client tenure, and attacks per company; therefore, these statistics only apply to data received from Symantec Managed Security Services customers. | 49%                                |

Table 10. Event severity classification

| Severity Classifications | Severity Level | Description   |
|--------------------------|----------------|---|
| 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.<br><i>Example:</i><br>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.<br><i>Example:</i><br>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.<br><i>Examples:</i><br>Continuous attacks by a single IP address against the client network. <ul style="list-style-type: none"> <li>A significant vulnerability on the client's network that was identified by either an attacker or the 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.</li> <li>Unknown suspicious traffic that warrants an investigation by the client to track or eliminate the traffic flow.</li> </ul> |
|                          | 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.<br><i>Example:</i><br>Successful exploit of a vulnerable Web server.   |

## EVENT SEVERITY

Event severity is only applicable to data generated by Symantec Managed Security Service. Every event validated by Symantec security analysts is assigned to one of four severity classifications: informational, warning, critical, and emergency. 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, security measures protecting the targeted system, 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, while a non-severe event is mainly informative (Table 10).

## 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.

### 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 and, instead, 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.

#### ATTACK ACTIVITY PER DAY

Symantec uses a daily attack rate as a rough estimate of the rate of attack activity experienced by networks connected to the Internet. While this attack rate is determined by a large number of factors, it is generally a reliable indicator of whether the attack rates are rising or falling from one reporting period to the next.

Previous volumes of the *Internet Security Threat Report* have used the mean average number of attacks detected by Symantec Managed Security Services and DeepSight Threat Management System sensors to determine the daily rate of attack. However, this figure 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 for this report. This approach more accurately represents the variations in attack volume over time that a typical network (in size and defensive deployment) may see.

#### 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

This report uses the proportion of attacking IP addresses that perform a given attack.

#### BOT NETWORKS

Symantec DeepSight Threat Management System tracks source IP addresses for identifiable patterns of attacks and probes. This automated tracking allows Symantec to identify groups of systems involved in coordinated attack activity. The systems that are participating in this activity to the exclusion of other activity that day are considered to be zombie hosts, part of a bot network.

The numbers of zombie systems identified each day should not be considered inclusive of all bot networks, as in order to be identified as a zombie system, the source IP address must participate in an attack or scanning pattern to the exclusion of other activity. Symantec expects the identified numbers to be a very small subset of the total number of remotely controlled systems, and that the growth in these identified systems is indicative of a similar increase in the total number of compromised, remotely controlled hosts.

#### Top Originating Countries

Symantec identified the national sources of attacks by automatically cross-referencing source IP addresses of every attack with several third-party, subscription-based databases that link the geographic location of systems to source IP addresses. While these databases are generally reliable, there is a small margin of error. Currently, Symantec cross-references source IP addresses of attacks against every country in the world.

It is important to note that while Symantec has a reliable process for identifying the source IP address of the host that is directly responsible for launching an attack, it is impossible to verify where the attacker is physically located. It is probable that many of the sources of attack are intermediary systems used to disguise the attacker's true identity and location.

### Top Originating Countries per Internet Capita

The number of Internet users was obtained from the CIA World Factbook.<sup>87</sup> The CIA World Factbook provides a breakdown of the number of Internet users per country.

### Targeted Attack Activity by Industry

For the purposes of the report, a targeted attacker is one that is detected attacking at least three companies in a specific industry, to the exclusion of all other industries. 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.

**Figures 24** and **25** represent the industry breakdown of the sample set in percentage terms. Industries with less than ten sensors have been excluded from the resulting totals.

### Patterns of Attack Activity by Time

Symantec analysts have analyzed and plotted Internet attack activity according to the time of day. Taking into account the global nature of the Internet, this data has been adjusted to the median time zone of the originating country of the attack. The attacks analyzed were from three groups: worm-associated attacks, non-worm associated attacks, and severe attacks.

Each attack detected by Symantec has a corresponding time stamp (expressed in Greenwich Mean Time), which describes the precise time that the attack was detected. This time is extracted from the log data (for example, firewall or IDS) produced by the device that Symantec is monitoring. However, in order to evaluate what time of day attackers are most active within specific locations throughout the world, Symantec adapted these time stamps by the offset of the local time zone in which the attacking system was located.

### Fortune 100 Infection Exposure

Symantec identifies each attacking system as part of a netblock that is registered to an organization in the regional Internet address registrars. The list of Fortune 100 companies ranked by *Fortune* magazine was cross-referenced to the netblock registration from the regional registries to identify netblocks owned by Fortune 100 organizations. Manual correlation was used to account for subsidiary companies and to detect netblocks that were registered to companies that have since been acquired by Fortune 100 companies. While not inclusive of every netblock used by Fortune 100 corporations, this list is representative of the netblocks used by these corporations.

### Client Tenure and Severe Event Incidence

Symantec analysts have analyzed the average number of severe attacks experienced per Symantec Managed Security Service customer in each of the tenure brackets. The tenure is the amount of time the company has been a customer of Symantec Managed Security Service, and is an indication of the effect that can be seen when Symantec is driving security improvements in the organization.

<sup>87</sup> <http://www.cia.gov/cia/publications/factbook>

Figure 24. Symantec Managed Security Services sensor distribution by industry

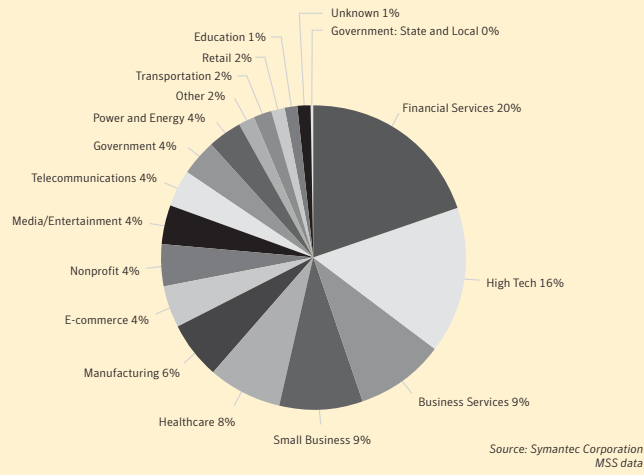
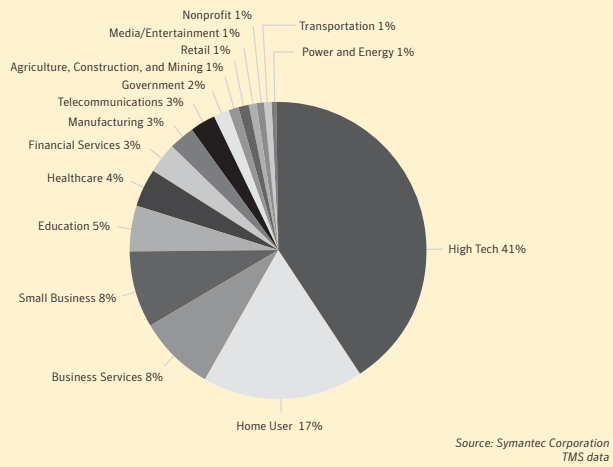


Figure 25. Symantec DeepSight Threat Management System sensor distribution by industry



## 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 10,000 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),<sup>88</sup> who define the taxonomy used to classify vulnerabilities. Possible values are indicated below. This mentioned white paper also 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

### SEVERITY

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.

<sup>88</sup> “Use of a Taxonomy of Security Faults,” <http://ftp.cerias.purdue.edu/pub/papers/taimur-aslam/aslam-krsul-spaf-taxonomy.pdf>

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 11**.

#### 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.

- **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.
- **Exploit Available**—sophisticated exploit code to enable the exploitation of the vulnerability is publicly available to all would-be attackers.
- **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 or her own exploit code to make use of the vulnerability.

**Table 11. Measurement of severity level**

| Severity Level | Severity Score Range |
|----------------|----------------------|
| High           | $X \geq 7$           |
| Moderate       | $4 \leq X < 7$       |
| Low            | $X < 4$              |

## Appendix D—Malicious Code Trends Methodology

The trends in the “Malicious Code Trends” section are based on statistics from malicious code samples submitted 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 submission 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 customers 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.<sup>89</sup> 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.

<sup>89</sup> “In the wild” viruses are those that have been observed propagating on, through, or between computers of users as they go about their daily activities. The “zoo” is not necessarily a laboratory environment. Zoo viruses are those that have been created and made available (on the Internet, BBS, FTP sites) but which are not actually spreading on the computers of users in the course of their daily activity—thus, they have not been seen “in the wild.”

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](http://WWW.SYMANTEC.COM).



**WORLD HEADQUARTERS**

20330 Stevens Creek Blvd.  
Cupertino, CA 95014 U.S.A.  
(408) 517 8000  
(800) 721 3934

[www.symantec.com](http://www.symantec.com)

**For Product Information**

In the U.S., call toll-free  
(800) 745 6054.

Symantec has worldwide operations  
in more than 35 countries. For  
specific country offices and contact  
numbers please visit our Web site.