Volume V, Published March 2004

symantec™

Symantec Internet Security Threat Report

Trends for July 1, 2003 – December 31, 2003

Contents

Executive Summary

EXECUTIVE EDITOR
Oliver Friedrichs
Symantec Security Response

EDITOR
Stephen Entwisle
Symantec Security Response

DEEPSIGHT THREAT ANALYST
Daniel Hanson
Symantec Security Response

MANAGER, DEVELOPMENT
Dave Ahmad
Symantec Security Response

SENIOR RESEARCH FELLOW
Sarah Gordon
Symantec Security Response

DEEPSIGHT THREAT ANALYST
Marc Fossi
Symantec Security Response

SECURITY ARCHITECT
Peter Szor
Symantec Security Response

SECURITY RESEARCHER
Eric Chien
Symantec Security Response

The Symantec *Internet Security Threat Report* provides a six-month update of Internet threat activity. This issue includes an analysis of network-based attacks, known vulnerabilities, and malicious code for the period of July 1 to December 31, 2003. It also examines how and why attacks have affected some organizations more severely than others and how current trends are expected to shape future Internet security threats. Symantec's recommendations for best security practices can be found in Appendix A at the end of this report.

One of the most significant events of 2003 occurred in August when the Internet experienced three new Category 4 worms in only 12 days.[1] Blaster, Welchia, and Sobig.F infected millions of computers worldwide. These threats alone may have resulted in as much as $2 billion in damages.[2]

Other *Internet Security Threat Report* highlights include:

- In the first half of 2003, only one-sixth of the companies analyzed reported a serious breach. In the second half of the year, half of the companies reported a serious breach.
- Seven new vulnerabilities a day were announced in 2003.
- More vulnerabilities are being published with tools to exploit them, forcing administrators to react more quickly.
- Malicious code that exposes confidential data increased significantly in 2003.
- Blended threats targeting Windows® operating systems increased significantly in 2003.
- Attackers and blended threats are increasingly utilizing previously compromised systems to launch attacks.

Attack Trend Highlights

- Worms remained the most common source of attack activity.
- Almost one-third of all attacking systems targeted the vulnerability exploited by Blaster.
- Attackers increasingly targeted backdoors left by other attackers and worms.
- Attacking systems tended to target geographic regions close to them.
- Financial services, healthcare, and power and energy were among the industries hardest hit by severe events.
- Increased client tenure continues to result in a decrease of severe events. Over 70% of clients with tenure of more than six months successfully avoided a severe event.

[1] The Symantec Security Response Threat Severity Assessment evaluates computer threats (viruses, worms, Trojan horses, and macros) and classifies them into one of five categories, with Category 5 being the most severe, and Category 1 the least severe.

[2] Computer Economics estimates the economic impact of these outbreaks: www.computereconomics.com/article.cfm?id=867. These numbers may not include costs such as stock value decline, customer confidence, and negative publicity.

Vulnerability Trend Highlights

- Symantec documented 2,636 new vulnerabilities in 2003, an average of seven per day.
- Symantec data indicates that the rate of vulnerability disclosure has leveled off.
- Newly discovered vulnerabilities are increasingly severe.
- Newly discovered vulnerabilities are increasingly easy to exploit.
- In 2003, 70% of vulnerabilities were classified as easy to exploit.
- The percentage of vulnerabilities for which exploit code was publicly available increased by 5% in 2003.
- The percentage of vulnerabilities that do not require specialized tools to exploit them increased by 6% in 2003.

Malicious Code Trend Highlights

- Blended threats make up 54% of the top ten submissions over the past six months.
- Two and a half times the number of Win32 viruses and worms were observed by Symantec than over the same period in 2002.
- Within the top ten malicious code submissions, the number of mass-mailer worms with their own mail engine increased by 61% over the first half of 2003.
- Threats to privacy and confidentiality were the fastest growing threat, with 519% growth in volume of submissions within the top ten.

Current Issues

- In January 2004, MyDoom began spreading at rates similar to Sobig.F, exposing infected systems through a backdoor and carrying out a targeted attack.
- Two new worms, Doomjuice and Deadhat, followed MyDoom, both propagating via the backdoor left by MyDoom.
- Blended threats continue to serve as vehicles to launch large-scale denial-of-service attacks, including Blaster in August and MyDoom and its successors (DeadHat and DoomJuice) in the first two months of 2004.

ATTACKERS LEVERAGING EXISTING BACKDOORS

A large number of sensors observed activity that was targeting backdoors left behind by previous attacks and blended threats. By leveraging existing backdoors to gain control of a target system, attackers can install their own backdoor or use the compromised system to participate in a distributed denial-of-service attack (DDoS).

As of the first quarter of 2004, attackers and new blended threats are scanning networks seeking the backdoor contained in the MyDoom worm. This backdoor allows attackers to install new malicious code, such as key logging software, and compromise confidential data on infected systems. It also allows new blended threats to infect these systems.

VULNERABILITIES INCREASINGLY SEVERE AND EASY TO EXPLOIT

On average, over the past six months, 99 new high-severity vulnerabilities a month were announced. High-severity threats give attackers increased privileges and access to more prominent targets, thereby offering greater potential rewards. Researchers seek out severe vulnerabilities because they attract more public and media attention. Vulnerabilities are becoming increasingly easy to exploit. This either means that

Vulnerabilities are becoming increasingly easy to exploit. This either means that no specialized knowledge is required to gain unauthorized access to a network or that tools are readily available to help attackers do so. This increases the likelihood of damaging intrusions. In 2003, 70% of vulnerabilities announced were considered easy to exploit, up from 60% the previous year.

MALICIOUS CODE SUBMISSIONS CONTINUING TO INCREASE

Submissions of malicious code threats to Symantec™ Security Response have increased steadily over the past six months. Blended threats continue to be a major concern, representing 54% of the top ten submissions. Blaster, Welchia, Sobig.F, and Dumaru are four blended threats that have spread rapidly over the past six months.

Malicious code that can expose confidential data such as passwords, decryption keys, and keystrokes has increased dramatically over the past six months. The most prominent example of this is Bugbear.B, a blended threat that was designed to extract confidential data. Other such threats include backdoors and spyware, both of which may expose vital, confidential data.

LOOKING TO THE FUTURE

Symantec analysts are closely monitoring several trends. Firstly, many Windows operating systems use components that are common to both corporate and consumer environments. Due to their extensive use, vulnerabilities in these components may make rapid, widespread severe events more likely.

Secondly, client-side vulnerabilities in Microsoft® Internet Explorer are on the rise. These may allow attackers to compromise the systems of client users who unwittingly visit malicious Web sites. In the past six months, researchers discovered 34 vulnerabilities in Internet Explorer.

Finally, the time between the disclosure and widespread exploitation of a vulnerability continues to shrink. In the time between the announcement of a new vulnerability and the development and deployment of a patch, companies are open to attack. As exploits are developed and released more quickly, companies are increasingly vulnerable. The likelihood of blended threats that exploit unpublished vulnerabilities (otherwise known as “zero-day” blended threats) is increasing. Symantec believes that “zero-day” threats are imminent. A “zero-day” blended threat could target such a vulnerability before that vulnerability is announced and a patch made available. If such an outbreak occurs, widespread damage could occur before users are able to effectively patch their systems.

Attack Trends

Symantec has established one of the most comprehensive sources of Internet threat data in the world. Over 20,000 sensors deployed in over 180 countries by Symantec DeepSight™ Threat Management System and Symantec Managed Security Services gather this data. With analysts located in five Security Operations Centers throughout the world, Symantec has an unparalleled ability to identify, report on, and respond to emerging threats.

This section of the Symantec *Internet Security Threat Report* provides an analysis of Internet attack activity for the six months ending December 31, 2003. This activity will be compared to data presented in the two previous *Internet Security Threat Reports* covering July 1, 2002–June 30, 2003. Symantec's recommendations for best security practices can be found in Appendix A at the end of this report.

For the purpose of this report, attack activity has been divided into two categories: worm-related activity and non-worm-related activity. This allows Symantec analysts to differentiate between autonomously propagating attacks and attacks that require human intervention. In some cases, it is difficult to discern whether attack activity is worm-related. In these cases, attacks that are commonly associated with worms have been classified as worm attacks.

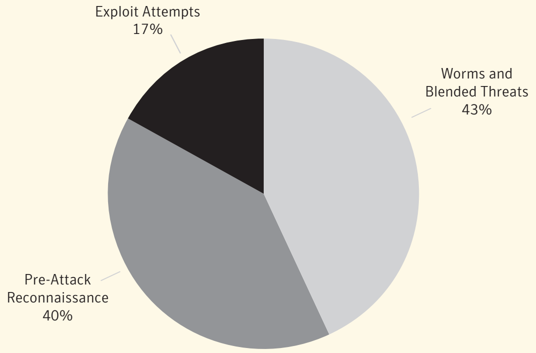
This section of the *Internet Security Threat Report* will discuss:

- Attack activity by type
- The top Internet attacks
- The top attacked ports
- The top originating countries
- The top industries experiencing severe events
- The top targeted industries
- The impact of client tenure on severe event incidence
- Patterns of attack activity by time of day
- Patterns of attack activity by day of the week

ATTACK ACTIVITY BY TYPE

Attacks detected by network security devices can generally be broken down into three categories: pre-attack reconnaissance, exploit attempts, and worms and blended threats. In comparison to the same six-month period in 2002, the percentage of worm events declined dramatically in the second half of 2003 **(Figure 1).** In the second half of 2002, worm activity accounted for 78% of total activity. During this period, worm activity dropped to 43% of the total, with the remaining 57% split: 17% representing exploit attempts and 40% reconnaissance. For the same period in 2002, exploit attempts accounted for only 3.3%, and reconnaissance 18% of the total.

Figure 1. Attack activity by type



Source: Symantec Corporation TMS and MSS data

TOP INTERNET ATTACKS

The top attacks seen by both Symantec Managed Security Services and Symantec DeepSight Threat Management System reflect those that administrators are likely to observe on their own networks. Worm attacks are included for this metric, as they make up a significant portion of Internet attacks for this period.

The most dominant attack, as measured by volume of events **(Table 1)** was related to the SQLExp worm, also known as Slammer. It accounted for over one-quarter of the total attacks. SQLExp was launched on January 24, 2003, and was already over five months old at the beginning of the current reporting period. This illustrates that old threats continue to affect organizations long after they surface.

SQLExp's rapid propagation led to the high number of attacks. In an attempt to spread, the worm will send out UDP packets from an infected system at such a rate that it will frequently saturate the bandwidth of connected networks. As a result, a single SQLExp infection can result in a high volume of attacks. Accordingly, a small number of infected systems could account for its high ranking.

The SQLExp worm is notably absent from the top ten attacks according to the number of sensors detecting the activity **(Table 2).** This indicates that a large number of networks may be filtering traffic to Microsoft SQL Server, the target of this worm, at the network perimeter. On the other hand, attacks related to the older, but still successful, CodeRed and Nimda worms rank highly in both volume and number of detecting sensors. These worms utilize Directory Traversal Attacks, Indexing Server Attacks, and Cmd.exe Attacks, all of which target Microsoft's IIS Web server.

Sensors frequently detected three attacks targeting email infrastructure during this period. The Generic SMTP HELO Buffer Overflow Attack and the Generic SMTP Rcpt To Command Attack, third and fourth in attack volume respectively, are both attempts to compromise SMTP (Simple Mail Transport Protocol) email servers. These attacks may be related to the increase of SPAM email that Internet users are receiving.

The Matt Wright FormMail attack, which uses a faulty Web script to perform malicious activity, occupies fifth spot in attacks by percentage of detecting sensors. The FormMail script, used to submit feedback from a Web page, can allow delivery of email to arbitrary locations and has, therefore, been associated with the relaying of SPAM. Many automated scanners and penetration testing tools include this attack and perform it against any Web server they find. It should be noted that the tendency for many intrusion detection systems to falsely identify this attack may artificially increase the numbers being reported.

Over the past six months, both the Blaster and Welchia worms spread successfully.[3] These two threats were responsible for the presence of the DCOM RPC (Remote Procedure Call) Attack and the Generic WebDAV/Source Attack in these rankings. Both worms caused widespread disruption for organizations, even those with strong perimeter filtering. This highlights the risk that a single unpatched internal system can pose to the security of a network.

In the two previous *Internet Security Threat Report*s, the top attacks were associated with the SQLExp, CodeRed, and Nimda worms. The current period saw a similar trend, with Indexing Server Attacks, HTTP Directory Traversal Attacks, and Cmd.exe Attacks all appearing prominently in the top attacks.

Web-based attacks, occurring over HTTP, accounted for a significant number of the top attacks. When ranked by the volume of attacks, six of the top ten attacks occur over the Web. When ranked by the number of sensors detecting attacks, eight of the top ten are associated with Web applications. As a publicly available service, Web traffic is not filtered as frequently at the network perimeter as many other services.

[3] Please refer to the "Malicious Code Trends" section of this report for a more in-depth discussion of these worms.

Table 1. Top Internet attacks by percentage of total volume

Rank	Attack	Percent of Total Attacks by Volume
1	SQLExp Incoming Worm Attack	26.2%
2	Muhammad A. Muquit Count.cgi Attack	9.0%
3	Generic SMTP HELO Buffer Overflow Attack	8.3%
4	Generic SMTP Rcpt To Command Attack	6.2%
5	Generic WebDAV/Source Disclosure “Translate: f” HTTP Header Request Attack	4.2%
6	Microsoft Indexing Server/Indexing Services ISAPI Buffer Overflow Attack	3.8%
7	Generic UTF8 Encoding in URL Attack	2.1%
8	Generic HTTP Directory Traversal Attack	2.1%
9	Generic HTTP ‘cmd.exe’ Request Attack	2.0%
10	Microsoft Windows DCOM RPC Interface Buffer Overrun Attack	1.8%

Source: Symantec Corporation
TMS and MSS data

Table 2. Top Internet attacks by percentage of reporting sensors

Rank	Attack	Percentage of Sensors Detecting Attack
1	Microsoft Indexing Server/Indexing Services ISAPI Buffer Overflow Attack	18.5%
2	Generic WebDAV/Source Disclosure “Translate: f” HTTP Header Request Attack	16.3%
3	Microsoft FrontPage® Sensitive Page Attack	14.8%
4	Microsoft IIS 4.0/5.0 Extended UNICODE Directory Traversal Attack	14.7%
5	Matt Wright FormMail Attacks	13.5%
6	Microsoft IIS 5.0 .printer ISAPI Extension Buffer Overflow Attack	13.5%
7	Generic HTTP Directory Traversal Attack	13.1%
8	Generic UNIX Portmapper Set RPC Attack	13.1%
9	Microsoft UPnP NOTIFY Buffer Overflow Attack	13.1%
10	Generic HTTP ‘cmd.exe’ Request Attack	12.1%

Source: Symantec Corporation
TMS and MSS data

TOP ATTACKED PORTS

Symantec analyzes the top attacked ports by two metrics: the percentage of attackers that target each port and the number of sensors that detect attacks against a given port. These two metrics give very different views of attack patterns. The first measures how many different attacking systems are targeting a particular port. The second is a measure of how widespread attacks are (that is, how many security devices have seen activity on this port).

Worm activity is included in this list, as it reflects activity that administrators will observe on their own networks. Some ports frequently attacked by worms may be under-represented due to administrators turning off firewall logging for those ports. TCP/80, TCP/445, TCP/139, and UDP/137 are all examples of this.

In the second half of 2003, almost one third of all attackers targeted TCP/135 **(Table 3).** This is the target port for the Blaster worm and a series of automated threats, including the Gaobot family of malicious code. The Welchia worm, released in the wake of Blaster, also targets TCP/135 as well as TCP/80. The interest from worms and other automated tools marks a change from previous *Internet Security Threat Report*s. During those reporting periods, TCP/135 was the target of much less threatening operations, primarily the delivery of “pop-up SPAM.”

Table 3. Top attacked ports by percentage of attackers

Rank	Port	Description	Percentage of Attackers
1	TCP/135	Microsoft/DCE-Remote Procedure Call (Blaster)	32.9%
2	TCP/80	HTTP/Web	19.7%
3	TCP/4662	E-donkey/Peer-to-peer file sharing	9.8%
4	TCP/6346	Gnutella/Peer-to-peer file sharing	8.9%
5	TCP/445	Microsoft CIFS Filesharing	6.9%
6	UDP/53	DNS	5.9%
7	UDP/137	Microsoft CIFS Filesharing	4.7%
8	UDP/41170	Blubster/Peer-to-peer Filesharing	3.2%
9	TCP/7122	Unknown	2.5%
10	UDP/1434	Microsoft SQL Server (Slammer)	2.4%

Source: Symantec Corporation
TMS data

Table 4. Top attacked ports by percentage of reporting sensors[4]

Rank	Port	Description	Percentage of Sensors
1	TCP/80	HTTP/Web	59.6%
2	TCP/17300	Kuang2 backdoor	59.0%
3	TCP/445	Microsoft CIFS Filesharing	57.7%
4	TCP/27374	SubSeven backdoor	51.7%
5	TCP/135	Microsoft/DCE-Remote Procedure Call	51.3%
6	TCP/1433	Microsoft SQL Server	51.2%
7	TCP/21	FTP	50.4%
8	TCP/139	Microsoft CIFS File Sharing	45.2%
9	TCP/443	HTTPS/Web	44.6%
10	TCP/1080	Socks Proxy	42.7%

Source: Symantec Corporation
TMS data

A large number of attackers targeted common peer-to-peer file sharing ports, including TCP/4662, TCP/6346, and UDP/41170. The presence of these ports in the ranking reflects the popularity of peer-to-peer file sharing and the tendency for organizations to filter this traffic. In addition, new companies have emerged, scanning and cataloging peer-to-peer clients in an effort to enforce copyright laws. These companies may also be contributing to the rise in traffic on these ports.

Attackers also heavily targeted TCP/445 and UDP/137, both of which are associated with Windows file sharing. This is primarily due to the availability of many automated tools used to attack these ports. In the second half of 2002, Symantec analysts noted a similar rise in scanning for Window systems with open shares and weak passwords.

UDP/1434 is the final entry in the top ten ports targeted by attackers for this period. It was the most frequently attacked port during the first half of 2003 due in large part to the SQLExp worm. This change indicates that many systems have been patched but that worms and attackers are still targeting vulnerabilities in Microsoft SQL Server and Microsoft Desktop Engine environments. The lower percentage of attackers also confirms

[4] Footnote copy needed.

that the presence of the SQLExp worm in the top Internet attacks table **(Table 1)** is due to high volume, not necessarily a large number of attackers.

Over half of the Symantec DeepSight Threat Management System sensors detected activity on TCP/80 **(Table 4).** This makes TCP/80 the most widely targeted port during this period.

The presence of TCP/17300, ranked second in **Table 4,** is significant. In fact, TCP/17300 alone almost displaces TCP/80 in the ranking. This port, almost unseen prior to 2003, was the target of an increasing number of scans throughout the year. Investigation revealed that it hosted an old, out-of-date backdoor Trojan named Kuang2. Attackers targeted this port in an effort to find systems running this backdoor.

The presence of TCP/27374, another common backdoor port (SubSeven), ranked fourth on this list, is also related to this trend. Attackers scan for systems with SubSeven installed. They subsequently compromise them via the backdoor and then install their own backdoor in order to build a network of remotely controlled zombies. Sensors have detected a larger number of scans targeting these ports. However, the absence of the ports in **Table 3** indicates that they have been scanned by a relatively small number of attackers.

TOP ORIGINATING COUNTRIES

This section will discuss the top countries of attack origin. It is important to note that the country of origin may not necessarily reflect the actual location of the attacker. It is simple to trace an attack back to the last IP address from which the attack was launched. However, the computer used to launch the attack may not be the attacker's own system. Because of this, attackers frequently hop through numerous systems or use previously compromised systems to hide their location prior to launching the actual attack. For example, an attacker in China could launch an attack from a compromised system located in South Korea against a corporate Web server in New York. International jurisdictional issues often prevent proper investigation of an attacker's real location.

Over the two previous six-month periods, computer systems within the United States have consistently been the most common source of attack activity. This trend continued for this period. **Table 5** identifies the top originating countries, excluding worm attacks, and includes their ranking over the two previous six-month periods. (Entries listed as "NR" were not ranked in the top ten for that reporting period.)

Table 5. Top originating countries, excluding worms

Rank	Country	Percent of Total	Position January 1 – June 30, 2003	Position July 1 – December 31, 2002
1	United States	58%	1	1
2	Canada	8%	5	7
3	China	3%	2	3
4	Japan	3%	9	10
5	Australia	3%	NR	NR
6	Germany	2%	3	4
7	South Korea	2%	4	2
8	Taiwan	2%	NR	6
9	France	1%	6	5
10	Italy	1%	10	8

Source: Symantec Corporation TMS and MSS data

The ranking of top originating countries is similar to those noted over the two previous six-month periods. Australia is the only new entry. Over the past six months, both Canada (from fifth to second place) and Japan (from ninth to third place) have climbed in the rankings. While Canada has been steadily climbing over the past 18 months, Japan's movement has occurred primarily over the past six months.

Attacks originating in South Korea declined over this reporting period. In the second half of 2002, South Korea was responsible for four times more attacks than Canada and was ranked second in the top ten. For this period, attacks originating in South Korea represented only 2% of the total.

For many threats, the attack rate from a country is a function of the number of vulnerable systems in that country. A reduction in the number of vulnerable machines will therefore result in a reduction of the attack rate. For instance, South Korea was one of the countries hit hardest by the SQLExp worm in January 2003. Attacks originating from South Korea at that time significantly disrupted Internet connectivity.[5] In November 2003, Microsoft announced plans to work with the Korean Information Security Agency in an effort to improve computer security awareness.[6] The drop in attacks originating from South Korea may indicate that Internet users in that country are becoming more diligent in patch management.

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. However, it does not have the highest number of attacks per Internet user, a measure of the number of attacks launched from that country per 100,000 Internet users. Instead, of countries with over 100,000 Internet users, Canada is the top originating country per Internet user **(Table 6).** The United States is the fourth highest country of attack origin according to attacks per Internet user.

Table 6. Top originating countries per Internet capita

Rank	Country	Attacks per 100,000 Users
1	Canada	8,285
2	Kuwait	6,957
3	Ireland	6,397
4	United States	5,966
5	Nigeria	5,662
6	Cyprus	5,508
7	Finland	5,287
8	Iceland	5,028
9	Israel	4,922
10	Australia	4,251

Source: Symantec Corporation TMS and MSS data

REGION OF ATTACK TARGETS FOR TOP ORIGINATING COUNTRIES

To determine whom attacking systems in the top originating countries targeted, attacks originating in each country were examined and their target locations grouped by region. The resulting regional distributions of attacks were then compared with the global regional distribution seen by Symantec DeepSight Threat Management System and Symantec Managed Security Services sensors. The resulting ratio of attacks **(Table 7)** shows, at least in part, that attacking systems prefer to target countries that are geographically close to their own.

The "ratio of attacks" table is not indicative of overall attack rates for each of the countries. Rather, it indicates whether the distribution of attacks from a country targets some regions more than others. For many of these countries, there is a tendency to target certain regions at a significantly higher rate than other regions. In most cases—especially France, Italy, Germany and Australia—attacking systems prefer to attack targets that are located in the same geographic region.

[5] Source: www.computerworld.com/securitytopics/security/holes/story/0,10801,77898,00.html
[6] Source: www.microsoft.com/presspass/press/2003/nov03/11-04KoreaInfoSecurityPR.asp

Table 7. Ratio of attacks by originating country according to target region[7]

Rank	Source Country	Target Region					
		South America	North America	Africa	Europe	Asia	Australia
1	United States	1.1	1.4	1.0	0.6	0.6	0.8
2	Canada	1.0	1.7	0.9	0.3	0.7	1.0
3	China	1.0	1.2	0.4	0.7	1.9	1.1
4	Japan	0.7	1.9	0.6	0.4	1.9	1.0
5	Australia	0.8	1.0	0.4	0.6	1.0	6.8
6	Germany	0.0	0.6	2.5	3.6	0.4	0.0
7	South Korea	0.9	1.5	0.6	0.7	1.2	2.0
8	Taiwan	0.8	1.1	0.5	0.8	2.6	1.6
9	France	0.0	2.1	0.0	4.4	0.0	0.0
10	Italy	0.2	0.8	0.3	5.2	0.6	0.0

Source: Symantec Corporation
TMS and MSS data

Many factors may contribute to this tendency. The first is the visibility of potential target organizations in the daily life of citizens. Attackers target what they know. The second factor is contiguous IP address allocation. Sequential scans will cluster in networks numerically close to the source. The third factor may be language issues. Attackers may have more difficulty compromising a system that uses a language with which they are unfamiliar.

South Korea was the only country in the top ten that did not show a preference for targets in its own region. Instead, attacks from there seemed to prefer Australian and North American targets.

South America received less interest from the top ten originating countries than any other region. This may be because no South American countries are represented in the top ten source countries, possibly lending weight to the hypothesis that source countries generally target their own regions more than others.

ATTACK ACTIVITY BY INDUSTRY

Attackers choose their targets for many reasons. In some cases, they may target a single company or a group of companies from a single industry. In other cases, an attacker may compromise a system regardless of its owner. Attacks targeting specific industries can be examined in two ways: first, by comparing the number of severe events experienced by an industry to the number of non-severe events and, second, by the number of attacks specifically targeting that industry. Each can result in different conclusions. This section will look at both perspectives.

TOP INDUSTRIES EXPERIENCING SEVERE EVENTS

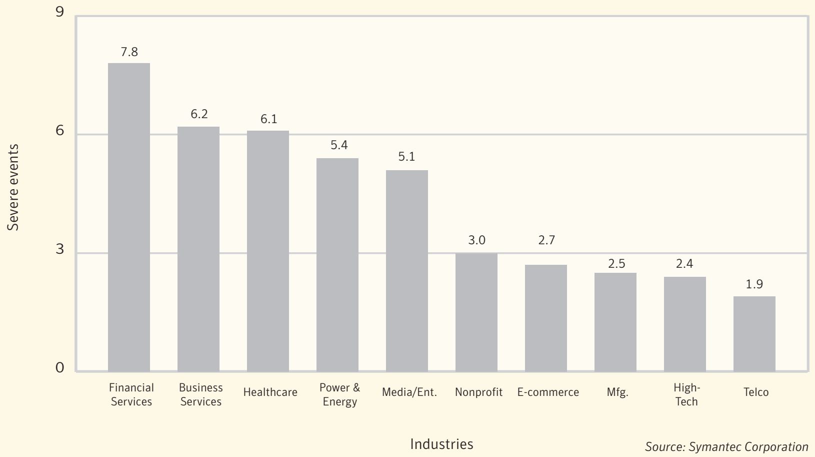
Symantec determines the severity of an event based on the characteristics of the attack, the defensive controls of the client, the value of the assets at risk, and the success of the attack. Severe events pose the greatest threat to organizations. The number of severe events that an industry experiences is one indicator of the amount of risk to which that industry is exposed. Symantec ranks those industries that have received the highest number of severe events per 10,000 events **(Figure 2).** Many factors contribute to the industry ranking, including the interest from attackers, the skill level of attackers, and the technologies deployed in that industry.

[7] In the ratio of attacks table, a value of 1 indicates that the regional attack distribution for that country is the same as the global regional attack distribution. If the country's attack distribution targeting a region is double the global average, this ratio would be 2. If a country's attack distribution were half the global average, this ratio would be 0.5.

The rate of severe attacks experienced by the top industries varies tremendously. The financial services sector, which is ranked first, experienced just over four times the severe attack rate of the telecommunications sector, which is ranked tenth. Businesses with significant financial resources tend to experience a relatively high severe attack rate. Critical infrastructure industries also experience high attack rates.

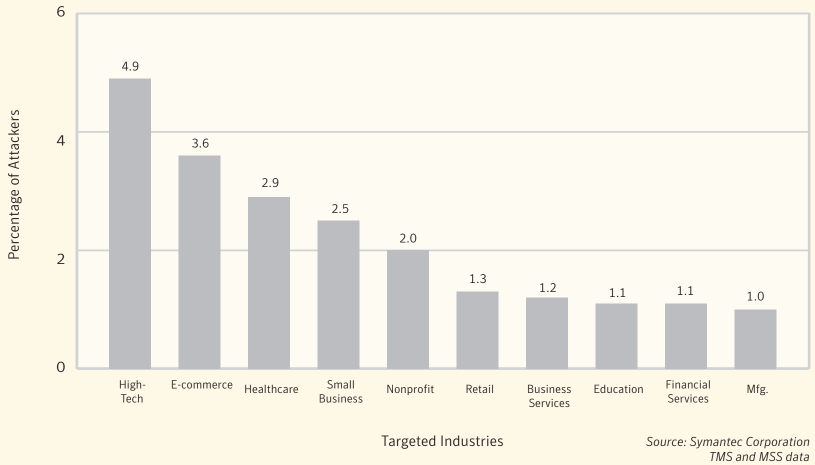
The nonprofit sector, ranked in sixth place, is an interesting entry. Although it likely has little appeal for attackers interested in financial rewards, the nonprofit industry may attract attention for political and social reasons. For instance, nonprofits are often involved in high-profile, controversial issues. This may provoke severe attacks.

Figure 2. Severe events experienced by industries per 10,000 events



Source: Symantec Corporation MSS data

Figure 3. Targeted industry attack rate



Source: Symantec Corporation TMS and MSS data

TOP TARGETED INDUSTRIES BY RATE OF ATTACK

The percentage of total attackers targeting only a specific industry indicates which industries are more frequently the targets of directed, purposeful attacks **(Figure 3).** According to this ranking, organizations with a more prominent Internet presence seem to experience a greater rate of targeted attacks. For instance, the high-tech and e-commerce industries (ranked first and second respectively) experience a much higher attack rate than the remaining industries.

CLIENT TENURE AND SEVERE EVENT INCIDENCE

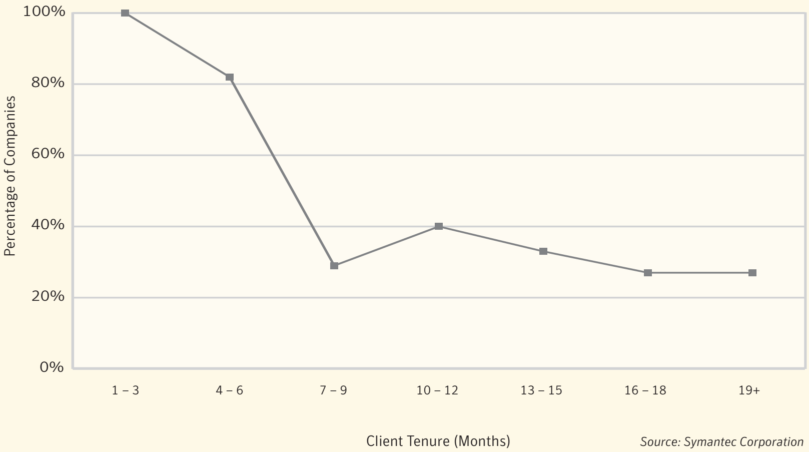
Client tenure is the length of time that an organization has used Symantec Managed Security Services. This metric allows Symantec analysts to assess the result of an organization's investment in security. In 2003, as in 2002, the rate of severe events decreased as client tenure increased. Over 70% of clients with a tenure of more than six months successfully avoided experiencing a severe attack, while all new clients (less than three months tenure) did experience such an attack. This indicates that organizations that have made a commitment to securing their environment show a decrease in severe events over time.

The relationship between client tenure and attack activity for the second half of 2003 is shown in **Figure 4.** It should be noted that, compared to previous reporting periods, the number of total organizations experiencing severe events increased over the past six months, regardless of tenure. The most significant increases occurred in companies with one to three months of tenure. This rise is largely the result of increasingly successful worms. More worms have been targeting vulnerabilities in core Windows components. These components are more widespread than the server software targeted by previous network-based worms, resulting in a much higher density of vulnerable systems. These worms also benefit from two other factors: the decrease in time between vulnerability disclosure and release of exploit code, and the overall increase in exploit code development.

PATTERNS OF ATTACK ACTIVITY BY TIME

Internet attacks can occur at any time of the day, any day of the week. The global nature of the Internet transcends local time patterns. As a result, an attacker may launch an attack at 12:00 in the local time zone that is observed by the target system at 04:00 local time. This section of the *Internet Security Threat Report* will discuss some of the patterns of attack activity according to the time of day and the day of week.

Figure 4. Percentage of companies detecting severe events by client tenure



Source: Symantec Corporation MSS data

WORM ACTIVITY BY DAY OF THE WEEK

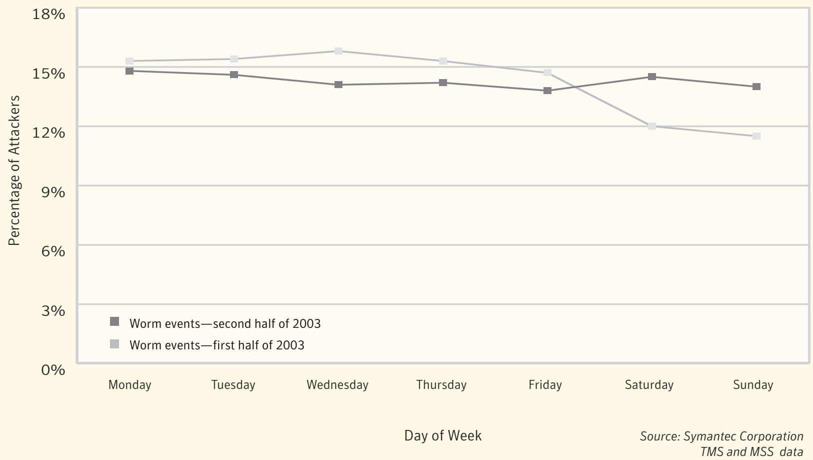
Symantec has noted a significant change in the daily distribution of worm-related attacks for this reporting period compared to the first half of 2003 **(Figure 5).** During that time, worm activity was more common on weekdays (Monday–Friday) than on weekends. However, in the second half of 2003, attack activity was more evenly distributed: roughly the same percentage of worm-related attacks occurred each day. This may be due to the predominant worm in each period.

In the first six months of 2003, the SQLExp (Slammer) worm infected many computers running Microsoft SQL Server or the Microsoft Desktop Engine. These applications are usually found on workstations in corporate environments and are less likely to be deployed on personal desktop systems. As most work-related computers are not used outside of business hours, propagation activity for worms targeting these systems would generally be limited to business hours.

The volume of attacks that infected systems are able to sustain may also influence this trend. SQLExp utilized a highly efficient method for propagation. As a result, it could send infection packets at a far greater rate than previous worms.

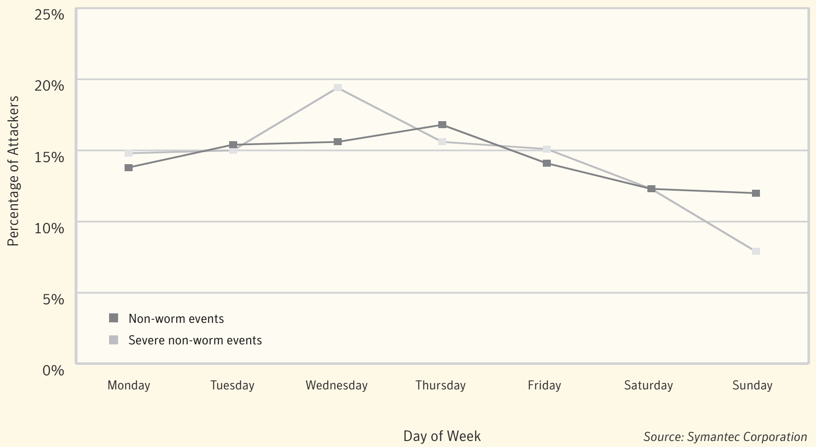
During the second half of 2003, major outbreaks included Blaster and Welchia, which affected all recent versions of Windows. As a result, propagation of these worms could be expected to continue outside normal work hours, including weekends. Additionally, systems that remain infected by SQLExp are those that are not rebooted on a daily basis, as the worm is memory resident and cleaned by such reboots. Although SQLExp is significant in terms of the volume of attacks, when gauged by the number of infected systems, it is far less significant and can be expected to have less impact on day-of-week variability.

Figure 5. Daily distribution of worm-associated attacks



Source: Symantec Corporation TMS and MSS data

Figure 6. Daily distribution of events and severe events



Source: Symantec Corporation TMS and MSS data

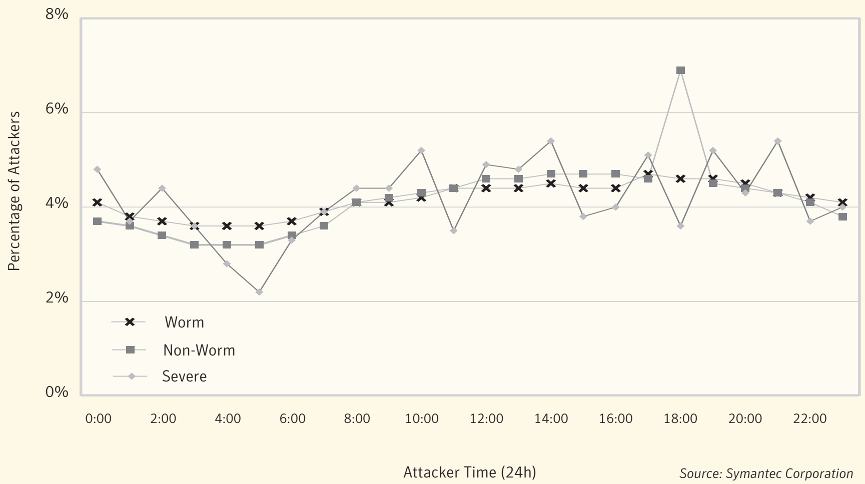
NON-WORM ACTIVITY BY DAY OF THE WEEK

Worms require little human intervention to spread. On the other hand, non-worm attacks are normally initiated by humans, even those performed by a bot network. The fact that these attacks are not automated will likely affect the times at which they are launched. As a result, the time pattern for non-worm attacks is likely to be different from that of worms.

The daily distribution of non-worm attacks and severe attacks **(Figure 6)** shows a decrease in non-worm activity on Fridays, Saturdays, and Sundays. These events seem more likely to occur during the workweek. Severe event activity also shows a definite decrease on the weekend, especially on Sunday. A rise in activity occurs on Wednesday. Regardless of what conclusions may be drawn from this, attacks can still occur on any day of the week. Organizations must be prepared to monitor and respond to these events at all times.

[8] For countries that have multiple time zones such as the United States and Canada, the median time zone was chosen.

Figure 7. Time of day distribution of Internet attacks according to attacker's local time



Source: Symantec Corporation TMS and MSS data

ATTACK ACTIVITY BY TIME OF DAY

The time of day at which attacks take place may affect an organization's security strategy. Symantec analysts have analyzed and plotted Internet attack activity according to the time of day at which it occurred.[8] Attacks from three groups—worms and blended threats, non-worm-associated attacks, and severe events—were analyzed. Overall, the time of attack launch indicates that attacking systems are generally more active between the hours of 07:00 and 20:00 local time.

The time distribution of worm activity **(Figure 7)** appears to be cyclical. The peak of activity occurs at 17:00 local time and the low point occurs at 05:00. This pattern is consistent with computers being turned on and off. Non-worm events are distributed in a similar wave-like fashion, with a greater drop-off in the very early morning hours. The similarity between the worm and non-worm distributions is interesting. It indicates that the systems performing the non-worm attacks may also be influenced by whether or not systems are turned on.

Severe events are important because they are a serious risk to organizations. These show a low incidence in the early morning, followed by a rise through the business day, and a high in the afternoon and early evening. However, compared to other attack events, severe events show a greater variation from hour to hour and a more significant drop from the late evening to early morning of each day. This variability is likely the result of the relatively low numbers of severe attacks. Because of the small sample size, a minor variance in the number of attacks can result in a higher variance in the percentage of attacks.

Vulnerability Trends

The ongoing discovery of new vulnerabilities in information systems continues to pose serious threats to organizations. Without warning, a single critical vulnerability can result in the exposure of systems that were previously considered secure. The fact that latent vulnerabilities can surface at any time is a frustrating fact of life for administrators. It seems that vulnerabilities are being discovered as quickly as they are being remedied.

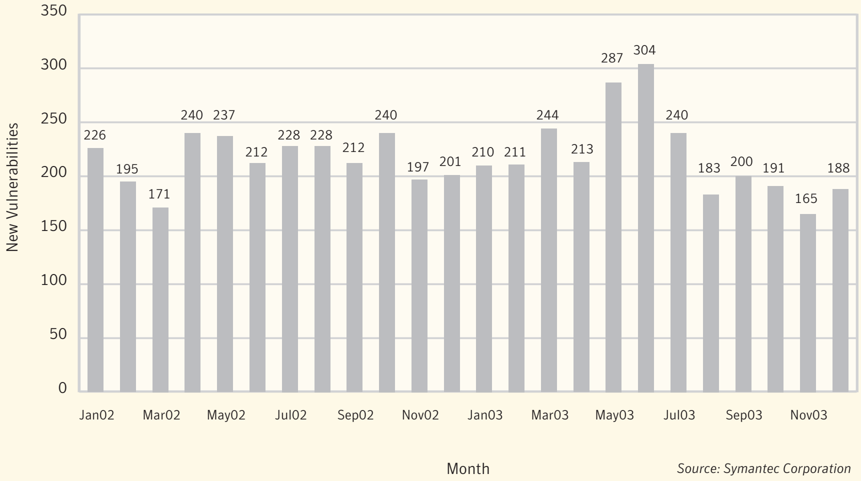
This section of the Symantec *Internet Security Threat Report* discusses developments in vulnerabilities disclosed over the past six months. The intent of this section is to (1) examine the characteristics of vulnerabilities disclosed during the second half of 2003, and (2) discuss potential future threats. It will also analyze and compare vulnerability trends observed in 2003 with those observed in 2002. Symantec's recommendations for best security practices can be found in Appendix A at the end of this report.

Symantec operates BugTraq, the most popular forum for the disclosure and discussion of vulnerabilities on the Internet. The BugTraq mailing list has approximately 50,000 individual subscribers who receive, discuss, and contribute vulnerability information on a daily basis.[9] Symantec also maintains one of the world's most comprehensive databases of security vulnerabilities, covering vulnerabilities affecting over 20,000 technologies from over 2,000 vendors. This discussion of vulnerability trends is based on a thorough analysis of that data.

OVERALL VOLUME

The Symantec vulnerability database documented 2,636 new vulnerabilities in 2003, compared to 2,587 new instances in 2002.[10] This equates to 220 new vulnerabilities published per month, or an average of 7.22 new vulnerabilities every day. This represents a less than 2% increase in total volume over 2002. Compared to the 81% increase from 2001 to 2002, this marginal level of growth suggests that a plateau has been reached. A number of factors may be influencing this, including a leveling off in the number of new vulnerability researchers, a shift toward keeping vulnerability details private, and the number of easily discovered vulnerabilities being exhausted. **Figure 8** depicts the volume of vulnerabilities published monthly since January 2002.

Figure 8. Volume of new vulnerabilities per month



Source: Symantec Corporation

[9] The BugTraq mailing list is hosted by SecurityFocus at www.securityfocus.com. Archives are available at www.securityfocus.com/archive/1

[10] It should be noted that not all vulnerabilities that are discovered are disclosed publicly. The data referred to in the Symantec *Internet Security Threat Report* includes only those vulnerabilities that have been made public.

There was a significant difference between the number of vulnerabilities announced in the first half of 2003 and the second half. Researchers disclosed 21% more vulnerabilities in the first half of 2003 than in the second half. In raw numbers, this equates to 1,469 in the first half, compared to 1,167 in the second. In 2002, the opposite was true, although the difference was smaller: 1,281 vulnerabilities were announced in the first half and 1,306 in the second half.

The total number of vulnerabilities published each month has increased only slightly since 2002 (it has, in fact, decreased in the most recent six months). However, there are some noteworthy changes in the types of vulnerabilities being discovered and the urgency of those new issues. Vulnerabilities discovered in 2003 were increasingly severe and easier to exploit. These trends will be discussed in the following sections.

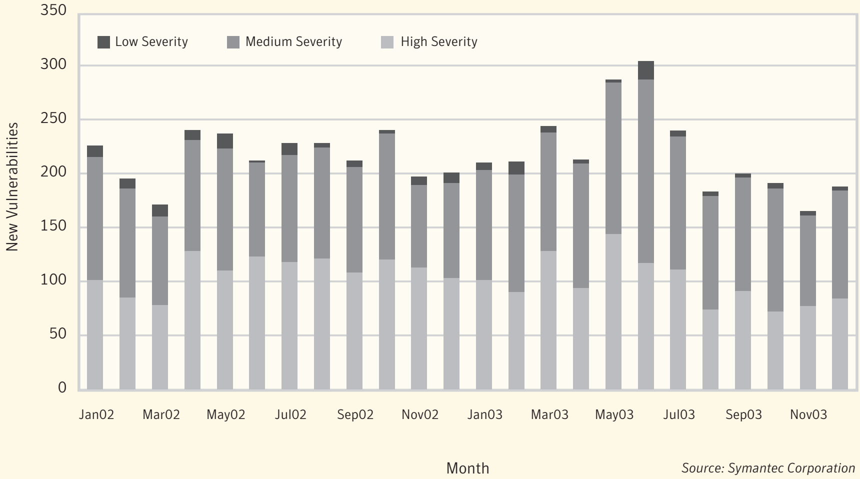
SEVERITY

Symantec analysts rate vulnerabilities according to their potential severity. Severity is defined as the impact of a vulnerability on the confidentiality, integrity, and availability of the affected information system. It is determined by the accessibility of the target system to attackers, and the objects within the system that may be affected.

For the purposes of the Symantec *Internet Security Threat Report,* each entry in the vulnerability database is categorized as 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 also 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.

Figure 9. Breakdown of volume by severity



Source: Symantec Corporation

- **High severity**—vulnerabilities that result in a compromise of the entire system if exploited. In almost all cases, attackers can exploit high-severity vulnerabilities across a network without authentication.

Based on these criteria, the majority of security vulnerabilities published in 2003 were classified as moderate- to high-severity threats **(Figure 9).** Accordingly, the number of low-severity threats appears to be decreasing. In the second half of 2003, Symantec classified approximately five vulnerabilities per month as low-severity threats. This is down from the approximately eight low-severity vulnerabilities published per month in the first half of 2003.

On a year-by-year basis, the number of low-severity vulnerabilities has also decreased. The previous two Symantec *Internet Security Threat Report*s indicated that researchers were focusing on more severe vulnerabilities, with the number of low-severity vulnerabilities declining from July 2002 to June 2003. This trend continued through the remainder of 2003. In 2002, eight vulnerabilities per month, on average, were classified as low severity. In 2003, Symantec considered six vulnerabilities per month as low severity on average.

The continuing decline of low-severity vulnerabilities may be driven by two factors:

- Vulnerabilities that are classified as remotely exploitable are almost always rated at least moderately severe. This is because the vulnerable component may be accessible to a larger number of attackers, making the vulnerability more of a threat. In 2003, 79% of vulnerabilities published were classified as remotely exploitable, 80% in the first half of the year and 78% in the second half. This is nearly the same as the percentage for 2002, 81%. Security researchers increasingly pursue remotely exploitable vulnerabilities due to the larger number of targets accessible by interconnected networks. Furthermore, applications are increasingly network-capable and, as a result, remotely exploitable vulnerabilities naturally follow.
- More researchers want to find high-severity threats and more attackers want to exploit them. The potential for damage caused by high-severity attacks is greater than lower-severity ones. As a result, they often generate more attention when published, both among their peers in the research community as well as in the media. More importantly, higher-severity vulnerabilities also allow attackers to gain higher access privileges on target systems.

Despite the fact that security researchers prize them, the average number of high-severity vulnerabilities published per month dropped slightly over the past year, from 109 per month in 2002 to 99 per month in 2003. Conversely, the number of moderately severe vulnerabilities increased, from an average of 98 per month in 2002 to an average of 115 per month in 2003. This trend is relatively consistent throughout 2003, with an average of 51% of vulnerabilities per month rated as moderately severe in the first half and 54% in the second half.

The increase may be due to the number of vulnerabilities affecting Web-based applications. Many of these vulnerabilities tend to be low impact but, in almost every instance, remotely exploitable. As a result, they are rated as moderately severe or higher. The increase in vulnerabilities affecting Web-based applications is also driving the rising ease of exploitation. This will be discussed in the following section.

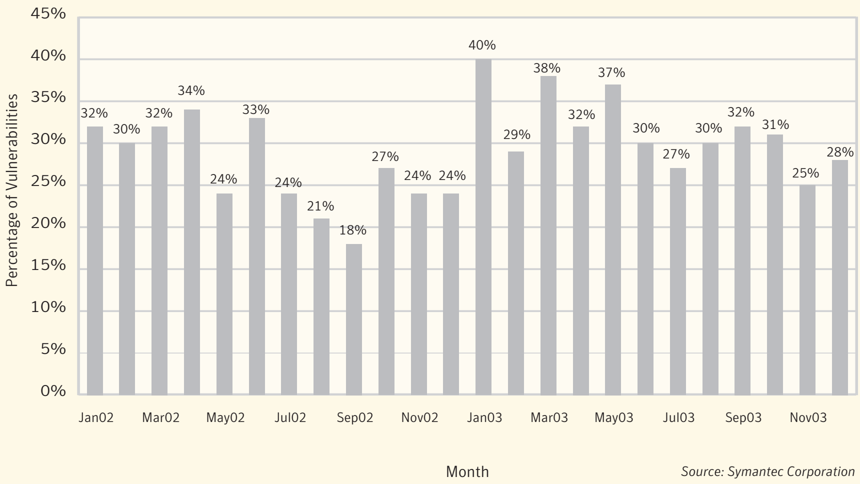
EASE OF EXPLOITATION

Ease of exploitation indicates how difficult it is for an attacker to exploit a vulnerability to compromise a target system. Symantec rates each vulnerability as either “Easily Exploitable” or “No Exploit Available” according to three criteria:

- **No exploit required**—exploit code is not required. With a reasonable amount of technical knowledge, the attacker can exploit the vulnerability without any exploit code.
- **Exploit available**—exploit code has been developed and is publicly available.
- **No exploit available**—exploit code would be required to exploit the vulnerability but, to the best of Symantec’s knowledge, none is known to exist.

Vulnerabilities that require no exploit or that have a required exploit available are classified as “Easily Exploitable.” Generally, these vulnerabilities do not

Figure 10. Percentage of new vulnerabilities affecting web-based applications



Source: Symantec Corporation

require sophisticated skills or knowledge to exploit. Anyone with sufficient general technical knowledge or with publicly available tools can exploit them. Examples of these are Web server vulnerabilities that can be exploited by simply entering an appropriate URL into a Web browser.

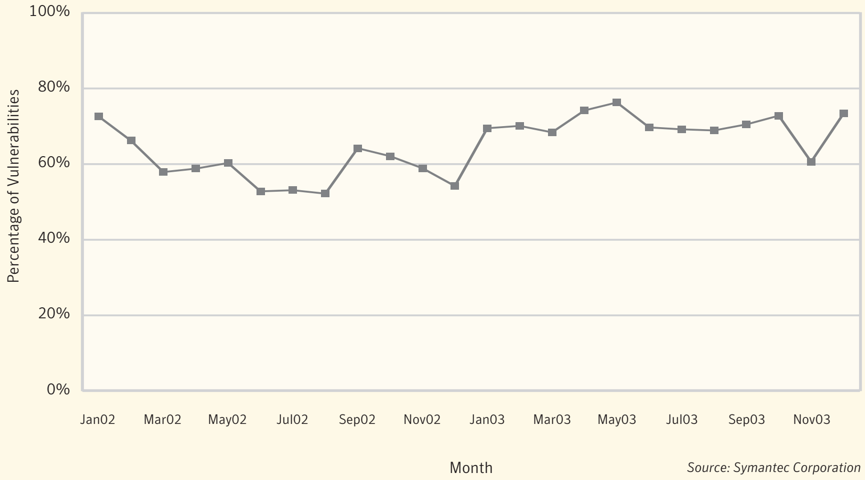
Vulnerabilities that are classified as "No Exploit Available" are more difficult to exploit. This is because attackers cannot exploit them using basic knowledge alone and because no known tools to exploit them have been written or made publicly available. To exploit these vulnerabilities, an attacker would be required to write custom exploit code (assuming that there is none circulating in the underground). This significantly raises the level of knowledge, expertise, and effort required for a successful attack, thus 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 won't likely be widely exploited.

Vulnerabilities are becoming easier to exploit. The percentage of total vulnerabilities that are considered "Easily Exploitable" rose by 10% over 2003. That increase was consistent for both the first and second half of the year. In 2001 and 2002, the percentage of all vulnerabilities classified as "Easily Exploitable" was approximately 60%. In 2003, it was approximately 70%. Two factors emerge as likely reasons behind this increase:

1. More vulnerabilities require no exploit code. The percentage of vulnerabilities that do not require an exploit rose 6% in 2003 over 2002. This is largely due to an increase in vulnerabilities that affect Web-based applications **(Figure 10).** Web-based vulnerabilities tend to be easily exploited input-validation errors such as cross-site scripting and SQL injection attacks. They are frequently rated "No Exploit Required." The number of vulnerabilities that affect Web-based applications increased by 4% in 2003. This increase corresponds closely to the increase in vulnerabilities requiring no exploit code.
2. More exploit code is being published. In 2003, 15% of documented vulnerabilities had exploit code associated with them, compared with 10% in 2002.

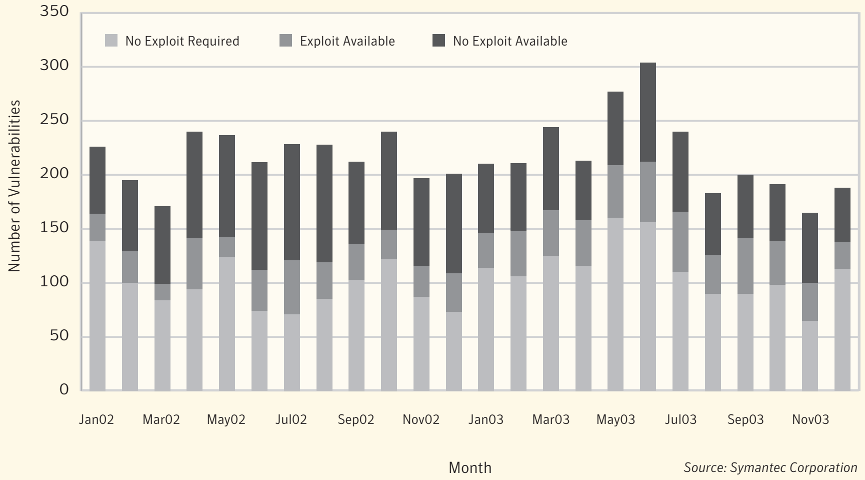
In 2003, the percentage of vulnerabilities that did not require exploit code increased by 6%. This was driven by a similar increase in the number of Web application vulnerabilities. Exploit development also increased by 5%. These two increases

Figure 11. Percentage of easily exploitable new vulnerabilities



Source: Symantec Corporation

Figure 12. Volume of vulnerabilities by ease of exploit



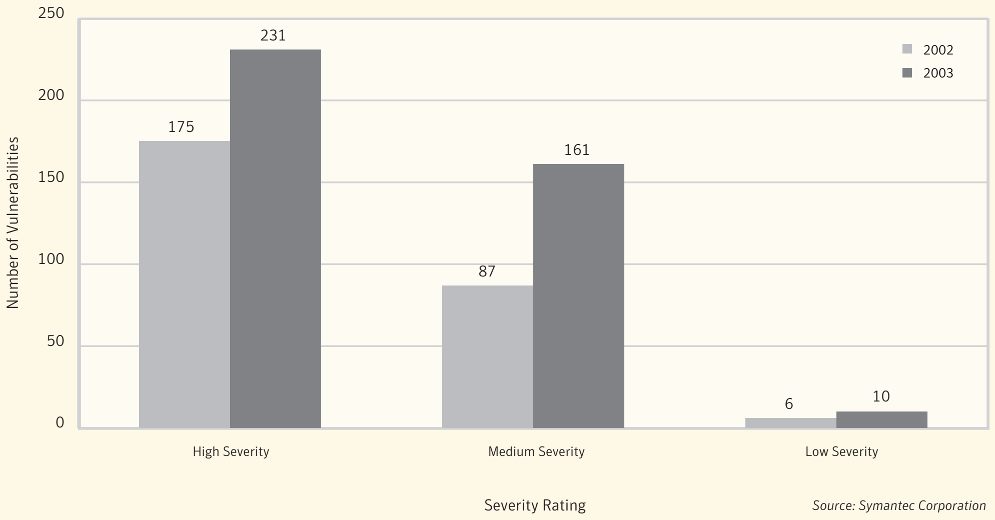
Source: Symantec Corporation

largely account for the 10% increase in easily exploitable vulnerabilities. A small amount of overlap is attributable to exploit development for vulnerabilities requiring no exploit code (1.38% in 2003). **Figure 11** depicts the rise in easily exploitable vulnerabilities. **Figure 12** shows the number of vulnerabilities according to ease of exploitation categories.

EXPLOITS BY VULNERABILITY SEVERITY

To understand the threat posed by the increased development of exploit code, it is important to look at what types of vulnerabilities are being exploited. The majority of vulnerabilities with associated exploit code in 2002 and 2003 are classified as high-severity **(Figure 13).** Most of the remaining vulnerabilities with exploits are moderately severe.

Figure 13. Vulnerabilities with exploit code, By severity



Source: Symantec Corporation

A relatively small number of exploits are developed for low-severity vulnerabilities. This is because researchers and attackers will likely develop exploit code only when the potential reward justifies the effort.

FUTURE CONCERNS

In reality, few of the approximately 220 vulnerabilities per month documented by Symantec pose a serious threat to organizations. Unfortunately, attackers need only one critical vulnerability to completely expose a network. The two major worms that appeared in the summer of 2003—Blaster and Welchia—demonstrated this.

Symantec has identified three particular areas of future concern: (1) blended threats exploiting so-called “zero-day” vulnerabilities, (2) vulnerabilities in core Windows operating system components in both corporate and consumer environments, and (3) the continued threat of client-side vulnerabilities in Microsoft Internet Explorer.

“ZERO-DAY” VULNERABILITY BLENDED THREATS

All blended threats to date have exploited vulnerabilities that were known to the public. In many cases, patches were already available by the time the blended threat surfaced. For example, 26 days elapsed between the announcement of the Microsoft DCOM RPC vulnerability and the appearance of the Blaster worm.[11] The application of patches and other mitigating techniques, such as port filtering, reduces the number of potential victims. However, the likelihood of blended threats that exploit unpublished vulnerabilities (otherwise known as “zero-day” blended threats) is increasing.

It is almost certain that there are still unknown, remotely exploitable vulnerabilities lurking in widely used technologies. A “zero-day” blended threat could target such a vulnerability. If a “zero-day” outbreak occurs, patches are unlikely to be available for many days. Even identifying the means by which such a worm is propagating may take longer than the time required for it to compromise all vulnerable systems.

It is surprising that this has not happened already. The nearest miss thus far occurred when CodeRed appeared in July 2001, exploiting a vulnerability for which no functional exploit code had yet been published. The near certainty of this threat should highlight the need for administrators to always employ effective, preventive security measures.

[11] Source: www.securityfocus.com/bid/8205

VULNERABILITIES IN CORE WINDOWS OPERATING SYSTEM COMPONENTS

The presence of vulnerabilities in components that are used in both corporate and consumer environments is worrisome. Between July 1, 2003, and December 31, 2003, Symantec reported 13 vulnerabilities that affect both corporate and consumer versions of Microsoft Windows.

Today, Microsoft operating systems that are designed for both corporate and consumer environments share common features and code. This makes development, maintenance, and support for these systems more efficient. Unfortunately, it also means that vulnerabilities in shared components will affect all environments that use those components. A good example of this is the Microsoft DCOM RPC Interface Buffer Overflow Vulnerability. Both Windows 2000 and Windows XP are vulnerable to this threat.

Exploitation of both corporate and consumer environments contributed to the successful proliferation of Blaster and Welchia.[12] Even though corporate environments tend to be more immune to infection, due to the use of firewalls, infections in home environments may still affect them because of bandwidth consumption and other consequences. Vulnerabilities in shared components may also allow blended threats that infect consumer systems to “piggyback” their way into otherwise secure corporate networks through laptops, VPNs, and other mobile technologies.

MICROSOFT INTERNET EXPLORER

Client-side vulnerabilities in Microsoft Internet Explorer continue to pose potential threats to organizations. Vulnerabilities in Internet Explorer have been mentioned as possible future threats in the two previous Symantec *Internet Security Threat Report*s. The primary reason for concern is the huge market dominance that Internet Explorer enjoys. It is currently a widely used tool for business and personal communications, particularly with the increasingly commonplace use of Web-based applications.

Researchers continue to discover vulnerabilities in Internet Explorer. The Symantec vulnerability database contains 20 distinct vulnerabilities affecting Internet Explorer that were published in the first half of 2003. In the second half of 2003, 34 Internet Explorer vulnerabilities were published, a 70% increase. Many of these vulnerabilities allow attackers to compromise the systems of client users who unwittingly visit malicious Web sites or Web sites hosting malicious content, intentionally or not.

This risk is further complicated by applications that use the modular nature of Internet Explorer components to render and display Web content received through other applications. One type of application that frequently does this is an email client. The situation is compounded by the fact that many organizations struggle to keep up with patch management on critical servers, not to mention the thousands of desktops and laptops that make up the enterprise network.

It is important to note, however, that because of the highly composite nature of Internet Explorer and the complexity of its security model, it is sometimes difficult to pinpoint the location of each distinct vulnerability. What is reported as a single vulnerability can be the result of multiple security weaknesses linked together to form a more complex exploit. These factors compound the difficulty in managing the risk associated with Web browsers.

Further aggravating the problem is that it is extremely difficult for firewalls, intrusion detection systems, and other security mechanisms to prevent exploitation. Most firewalls allow unrestricted access to the Internet for HTTP traffic over standard ports. It is not possible to enforce content policy at the network level. It may not be possible to differentiate between “good” and “bad” HTML content. As a result, for many of the vulnerabilities, a victim need only visit a malicious Web site in order to be compromised. Finally, parts of Internet Explorer are used in many applications, such as Microsoft Outlook.® It is common for vulnerabilities in these components to affect applications that use them.

Microsoft has acknowledged many security issues associated with Internet Explorer.[13] A document published by Microsoft, listed changes to be made in Windows XP SP2, including several security enhancements for Internet Explorer and related components.[14]

[12] W32.Welchia.Worm, which exploited BID 8205, managed to infect a network of Diebold ATMs running Microsoft Windows XP Embedded: www.securityfocus.com/news/7517

[13] For more information, see the article at news.zdnet.co.uk/internet/security/0,39020375,39117067,00.htm

[14] For more information, go to www.microsoft.com/downloads/details.aspx?FamilyID=7bd948d7-b791-40b6-8364-685b84158c78&DisplayLang=en

Malicious Code Trends

This section of the Symantec *Internet Security Threat Report* will analyze current and future malicious code threats. The trends in this report 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. This report analyzes and discusses the submissions in two ways: first, according to the number of specific examples of malicious code, such as Blaster, Sobig.F, and Bugbear.B; and second, according to the volume of all malicious code, such as viruses and worms, combined.

While the number of unique individual threats has not changed significantly in the past six months, the overall volume of malicious code submissions to Symantec Security Response has steadily increased. Based on the type and volume of the samples submitted, threats to privacy and confidentiality appear to be the most rapidly increasing threats. Additionally, the risk from blended threats continues to escalate, as many companies continue to fail to patch known vulnerabilities in a timely manner. Finally, Win32 threats continue to increase, with four severe Win32 threats appearing during the past six months.

Increased propagation speed, aided in part by increased bandwidth and decreased latency, means that any of these threats has the potential to cause widespread damage more quickly than ever before. Organizations can greatly limit exposure to malicious code by patching known vulnerabilities and adhering to good security policies. Symantec's recommendations for protecting against malicious code attacks can be found in Appendix A at the end of this report.

BLENDED THREATS

Blended threats use multiple methods and techniques to spread. They combine the characteristics of malicious code (such as viruses, worms, and Trojan horse programs) with the ability to exploit vulnerabilities. As a result, blended threats can spread to large numbers of systems in a very short time, causing widespread damage very quickly. The multiple propagation mechanisms of blended threats enable them to compromise a company's security posture and to simultaneously overload system resources and saturate network bandwidth. Examples of blended threats include, but are not limited to, Blaster, Sobig.F, and Bugbear.B.

In the previous issue of the *Internet Security Threat Report,* Symantec emphasized the growing danger of blended threats. This assessment was based on increased numbers of distinct blended threats reported, overall prevalence of blended threats in malicious code submission volume, and analysis of actual damage incurred as a result of several high-profile threats, such as Klez and Sobig.F. In the past six months, Symantec analysts have not seen a statistically significant increase in the number of individual blended threats submitted to Symantec. However, the volume of all blended threats combined has increased. Within the top ten submissions to Symantec **(Table 8)** the volume of blended threats has increased 59%.

Table 8. Top ten submissions received by Symantec

Rank	Sample	Submissions
1	Bugbear.B	80,961
2	Trojan.ByteVerify	51,232
3	Download.Adware.Lop	24,265
4	IRC Trojan	24,092
5	Sobig.F	21,955
6	Blaster	21,166
7	Redlof.A	20,941
8	Swen.A	19,332
9	Klez.H	16,518
10	Download.Trojan	12,458

Source: Symantec Corporation

Thus, while there has been no significant increase in the number of specific blended threats reported, the volume of blended threats as a whole has increased. This trend indicates that blended threats are affecting a larger number of systems and the impact continues to be severe.

The severity of the impact is illustrated by one of the top ten most reported submissions, Blaster, which accounted for approximately 7% of the top ten submissions during the second half of 2003 **(see Table 9)**.[15] According to Symantec DeepSight Threat Management data, the worm infected an average of 2,500 computers per hour. Once an attack was launched, the worm attempted to carry out a denial-of-service attack against the Microsoft Windows update site, in an attempt to keep users from obtaining the patch necessary to secure their system. Fortunately, this attack was unsuccessful.

Symantec analysts have noticed that for some high profile vulnerabilities the time between announcement and widespread exploitation has been decreasing. Blaster is an example of this phenomenon. Unlike previous threats, which emerged months or even years after initial announcement of a vulnerability, Blaster exploited the DCOM RPC vulnerability less than a month after the vulnerability was publicly announced. Multiple vendors were affected[16] and offered workarounds.[17]

Blaster was quickly followed by the release of Welchia. This worm exploited the same vulnerability in an attempt to “fix” Blaster infected computers. If the Blaster worm was found on a system, Welchia would install the Microsoft DCOM RPC patch.

Another of the top ten reported submissions, Sobig.F, also appeared in this reporting period. Using its own SMTP engine (also known as an email engine) to propagate via email, the worm swamped mailboxes of both corporations and consumers. The Sobig.F family of viruses demonstrated greater sophistication than earlier malicious code in several ways. Not only did it make use of social engineering techniques, it was also programmed to act as a command and control center, downloading a biweekly update. Furthermore, it was designed to exploit open SMTP proxies to enhance its spread rate. Sobig.F was able to exploit users’ trust successfully, gaining a global foothold extremely quickly.

Blended threats are increasing in complexity as well as in scope and speed. This complexity not only mandates a strong corporate security policy, it also dictates a comprehensive approach that makes use of strong heuristics, content filtering, and worm-blocking techniques. Patch management, antivirus, IDS, and firewall components all serve to protect against blended threats such as Blaster and Sobig.F.

Table 9. Top ten blended threats submitted

Rank	Blended Threat
1	Bugbear.B
2	Blaster
3	Sobig.F
4	Redlof.A
5	Swen.A
6	Klez.H
7	Welchia
8	Dumaru
9	Exception.Exploit
10	Spybot

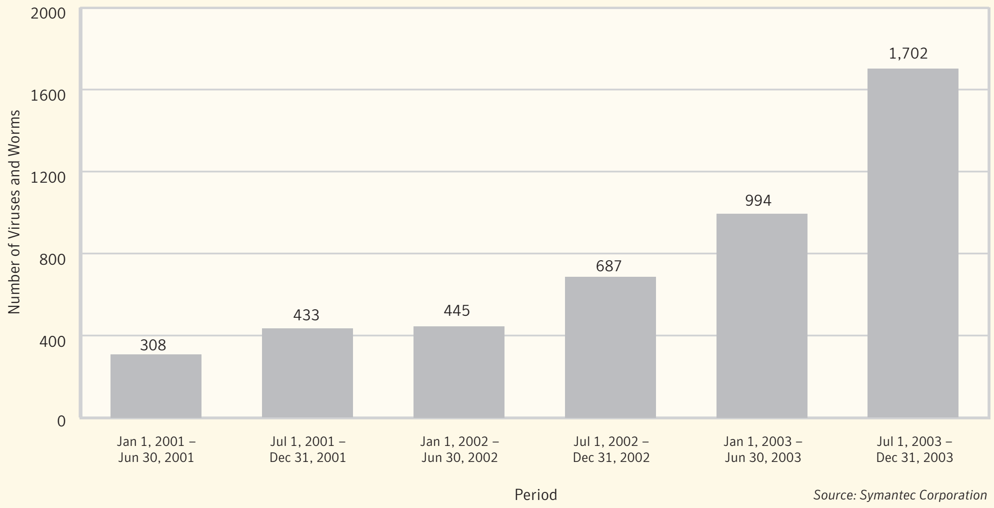
Source: Symantec Corporation

Win32 VIRUSES/WORMS

The Win32 API provides a standard for the development of software on the Windows platform, so it should come as no surprise that malicious code authors are also benefiting by using it. Win32 threats are executable files that operate by using the Win32 API. These forms of malicious code work on at least one Win32 platform. As Microsoft Windows continues to be ubiquitous, instances of Win32 threats have shown a rise in volume. This rise was first noted in the second half of 2002, and it continued to accelerate in the second half of 2003.

[15] See the Worm Lifecycle Speed of Propagation sub-section of this report for additional information on Blaster.
[16] For a list of affected vendors, see www.securityfocus.com/bid/8371
[17] For a list of workarounds, see www.securityfocus.com/bid/8205/solution/

Figure 14. New Win32 viruses and worms



Source: Symantec Corporation

Symantec observed two and a half times the number of Win32 viruses and worms in this period than over the same period in 2002. Over the second half of 2003, Symantec documented more than 1702 new Win32 viruses and worms compared to the 687 documented in the second half of 2002. During that period, Win32 viruses in the top 50 Symantec malicious code submissions decreased by 33%. However, over the past six months, they have increased by 64%. As of December 31, 2003, the total number of Win32 variants was approaching 5,500.

The number of unique Win32 viruses and worms submitted to Symantec has remained relatively stable. However, the volume of submissions of all Win32 malicious code threats combined has increased approximately 64%. The increased volume and impact of these threats is cause for concern. There were four Category 4 outbreaks (Blaster, Welchia, Sobig.F and Dumaru) during the second half of 2003.[18]

Symantec researchers have noted two particularly disturbing trends. First, as has been noted elsewhere in this report, the time between the announcement and widespread exploitation of a vulnerability is decreasing. Whereas in the past, months or even years could elapse between the announcement of a vulnerability and the release of a worm, the Gaobot worm exploited the Workstation Service Vulnerability less than two weeks after it was first published on November 11.[19]

The second disturbing trend is the use of packers to obfuscate malicious code.[20] The Spybot worm family has more than 500 documented variants, over 75% of which are packed with UPX or ASPack packers. Antivirus products must make use of robust binary unpackers to protect systems from this type of malicious code.

Provided that antivirus solutions are implemented proactively and well maintained on all platforms and across all tiers of a corporate network, companies should be well protected from the majority of these threats.

[18] The Symantec Security Response Threat Severity Assessment evaluates computer threats (viruses, worms, Trojan horses, and macros) and classifies them into one of five categories, with Category 5 being the most severe, and Category 1 the least severe.
[19] For more information, see http://securityresponse.symantec.com/avcenter/threat.severity.html
www.securityfocus.com/bid/9011
[20] 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. UPX and ASPack are specific types of packers.

WORM LIFECYCLE AND SPEED OF PROPAGATION

As soon as a worm is released into the wild, it spreads by infecting new systems. The worm may attack computers in specific locations (for instance, designated network blocks, domains, or computers residing in certain countries) or it may indiscriminately attack the entire Internet. If successful, the worm then uses the infected system as a platform from which to target new potential victims.

Each successful penetration follows this pattern, and the number of infected systems grows until either all potential victims are infected or until countermeasures (such as antivirus software) begin to halt the spread. Over time, as effective protection becomes ubiquitous and existing infections are remedied, the rate of propagation slows and suppressive factors begin to chip away at the overall worm population. This pattern of release, growth, and gradual decline is the lifecycle of a worm.

The speed at which a worm propagates is a critical factor in its lifecycle. Propagation speed is governed by a variety of influences, such as the algorithms used by the worm writer, the infection vectors used by the worm, and the number of available viable systems. Other factors that can influence speed of propagation include greater homogeneity of Internet-connected systems, increased bandwidth capacity, and computing speed of target systems.

LIFECYCLE OF BLASTER

The Blaster worm, one of the top submissions to Symantec Security Response, used a propagation strategy based on the exploitation of a well-known buffer overflow vulnerability in the widely deployed Microsoft Windows NT®, 2000, XP and 2003 operating systems.[21] The worm was released less than a month after the vulnerability was announced and the patch made publicly available. However, many systems remained unpatched, enabling the worm to spread rapidly among the vulnerable population.

Earlier worms, such as CodeRed and Slammer, depended on special services such as those run by Web or database servers running on their targets. Blaster, on the other hand, enjoyed the advantage that the vulnerability involved the DCOM RPC (Remote Procedure Call) service, a service active by default on all computers running Windows NT, 2000, XP, and 2003. This vulnerable component is common to both corporate and consumer systems.

The worm's ability to enter corporate networks directly from the Internet was limited, as firewalls typically block RPC traffic at the boundary between the corporate intranet and the Internet. However, Blaster found its way inside intranets through other vectors. Vulnerable machines that had become infected through direct exposure to the Internet or other infected networks were connected to clean company networks either directly or via a VPN connection. Once inside an intranet, the worm could spread freely due to the common nature of its targets.

Blaster produced disruption within affected environments by saturating local networks with the volume of RPC traffic it generated. It also caused the RPC service to crash on some systems that were not susceptible to infection, effectively shutting down the service on some targets and triggering immediate reboots on others.

LIFECYCLE OF WELCHIA

Welchia followed Blaster by less than a week. The Welchia worm spread to Windows XP machines using the same RPC vulnerability. However, it could also spread via HTTP traffic to Windows 2000 systems running Microsoft's IIS 5.0 Web server by using an older buffer overflow vulnerability.[22] The use of HTTP traffic allowed Welchia to sneak through firewalls that block RPC traffic, thus spreading more easily from the Internet to intranets and vice versa. It is worth noting that the Welchia worm normally only propagates until January. Thus, assuming machines are rebooted, this worm should experience a natural decline in the field after January 2004.

Although Blaster and Welchia caused temporary network disruptions on corporate networks, neither carried a destructive payload. If this had not been the case, damage from the outbreaks would have been greater. Symantec expects to see greater worm propagation, resulting in overloads to network hardware. This may cripple network traffic, diminish network availability, and disrupt business continuity, as well as impairing the Internet-based communication ability of both corporate and end users.

[21] The worm itself could spread only to hosts running Windows 2000 and XP.
[22] For a list of vulnerabilities, go to www.securityfocus.com/bid/7116

Although it is hard to defend against swiftly propagating worms, one way to limit damage is to deploy more effective processes for identifying and promptly patching system vulnerabilities. Unfortunately, this is not yet happening. Patches and security updates are usually implemented after the fact, once the damage is already done. Fortunately, virus protection has become more prevalent, helping to inhibit proliferation. However, as viruses move faster, the importance of thoroughly securing machines cannot be overemphasized.

MASS MAILERS WITH INTERNAL EMAIL ENGINES

Mass-mailing viruses and worms spread by harvesting and using email addresses from infected systems. There are two basic types of mass-mailing viruses: those that use an existing email system to propagate and those that use a distinct email engine built into the malicious code itself.

Until recently, viruses and worms relied almost exclusively on a user's existing email engine to replicate and send copies to potential victims. Once infected, however, users could often detect the virus, as copies of bounced viral email would appear in their inboxes. Once alerted, they could take countermeasures to limit its spread.

To bypass this limitation, virus writers create their own email engines, known as SMTP engines, in an attempt to foster propagation that is both more efficient and harder to detect. The number of unique viruses and worms in Symantec's top ten submissions that contain their own email engines experienced little fluctuation over the past six months. However, the volume of all such threats combined increased at a rate that was consistent with the increase of overall submissions. Within the top ten submissions to Symantec, the volume of malicious code utilizing its own SMTP engine increased by approximately 61%.

Because emails generated by the self-contained engine of malicious code do not interact with the user's email system, there are few telltale signs of an active infection. Furthermore, since most of these threats spoof their origin, victims cannot easily identify the true originator. This makes tracking the sources of infection difficult and enables the virus to survive longer.

Filtering of attachments, which can be done by most antivirus SMTP gateway implementations, can help control initial spread until signatures are released. Fortunately, most market-leading antivirus products with effective heuristics-based detection can resist these types of threats.

ADDITIONAL INFECTION VECTORS: INSTANT MESSAGING, PEER-TO-PEER, CIFS

Several infection vectors merit discussion in this six-month update: instant messaging (IM), Internet relay chat (IRC), peer-to-peer (P2P) services, and Windows file sharing (CIFS). Instant messaging worms use a variety of methods to spread, including:

- Utilizing APIs documented by the vendor. For example, using an instant messaging application's file transmission API to send itself out to contacts.
- Enumerating Windows via the Windows OS APIs to interactively send a file, simulating the user.
- Sending a URL link instead of a file.
- Patching client DLLs to send itself along with the original message.

Each of these methods exploits existing program functionality or trust relationships.

Several applications are available that allow Internet users to communicate synchronously in real time, particularly IM and IRC. A review of the top 50 submissions to Symantec finds no instances of threats to IM in the past six months. However, there were two reports of worms that used IRC to spread: Swen and Spybot.

Interestingly, both Swen and Spybot used P2P and IRC to spread. Overall, the volume of P2P threats within Symantec's top 50 submissions has increased 46% over the previous six-month period. Most of these P2P threats spread without any knowledge of the P2P file-sharing protocol; rather, they simply copy themselves to directories that are shared to others with enticing filenames.

One example of this type of threat is the Spybot worm. This worm searches the Windows Registry for the Kazaa configuration keys. Once it has located these, it adds a new key that configures Kazaa to share out an additional directory. The worm then copies itself to this directory using a number of filenames intended to entice users looking for pornography, software cracks, or other illicit content into downloading it.

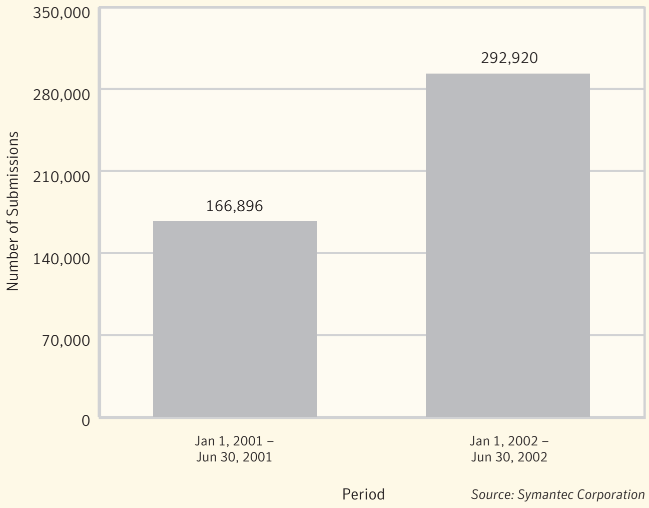
When other users on the Kazaa file-sharing network search for files matching these names, they will connect to the infected user via the Kazaa network and download the worm, believing (because of the filename) that it is another program. New variants of Spybot are discovered daily, with over 600 known variants currently in existence. Another P2P threat, Swen, works the same way. Swen is the eighth-ranked threat in Symantec's top 50, with nearly 20,000 submissions in the past six months.

Worms using Windows file sharing (CIFS) to propagate continued to appear in the past six months.[23] Malicious code often uses Windows file sharing to copy itself onto other network-accessible systems in order to propagate. Three of the submissions within Symantec's top ten reports made use of CIFS, including the most frequent submission, Bugbear.B.

Overall, the volume of submissions using IM, P2P, and CIFS within Symantec's top ten increased 57% in the past six months **(Figure 15).** As both legitimate and unapproved use of IM, IRC, P2P networking, and CIFS continue to increase, Symantec expects to see more new worms and viruses use these mechanisms to spread. Unlike other avenues for propagation, such as email, these vectors often have little corporate oversight, making management difficult.

Fortunately, organizations can take steps to protect users. A simple solution is for organizations to prohibit employees from using insecure versions of these services. Finally, policies regarding proper usage must be defined and enforced.

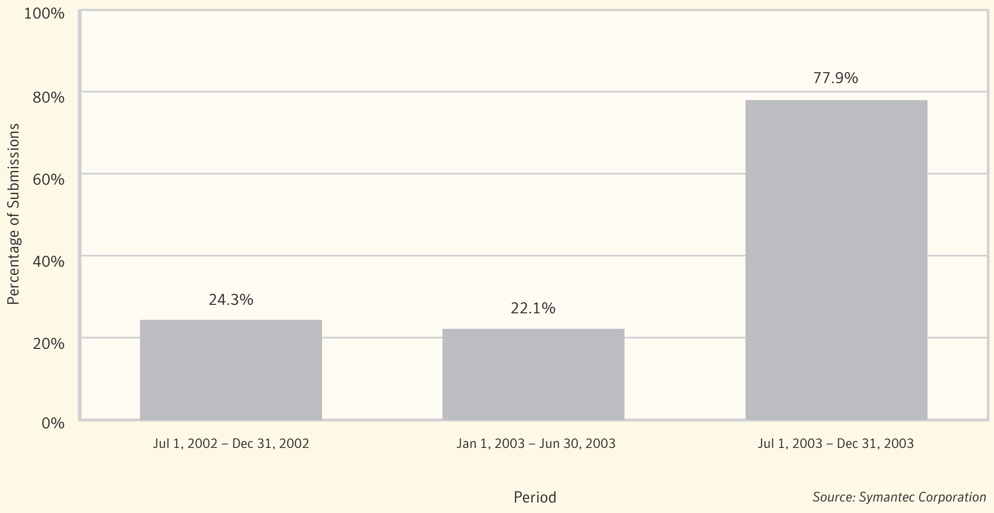
Figure 15. Volume of submissions using IM, P2P, IRC, and CIFS



Source: Symantec Corporation

[23] CIFS is not unique to Windows; however, most, if not all of the threats apply only to Windows systems.

Figure 16. Threats to confidential data as percentage of top ten submissions



Source: Symantec Corporation

THEFT OF CONFIDENTIAL DATA

Over the past six months, Symantec observed a rise in malicious code that can expose confidential data. Older threats compromised confidentiality by exporting random documents. However, more recent viruses and blended threats extract not only documents but also information such as passwords, decryption keys, and logged keystrokes. Analysis of the data from this six-month period shows that the impact of these threats has escalated. Previously, 22% of Symantec's top ten malicious code submissions were a threat to privacy and confidentiality **(Figure 16).** During the past six months this rose to 78%. Likewise, the total volume of top ten submissions threatening privacy and confidentiality has also increased by 519%.

BUGBEAR.B

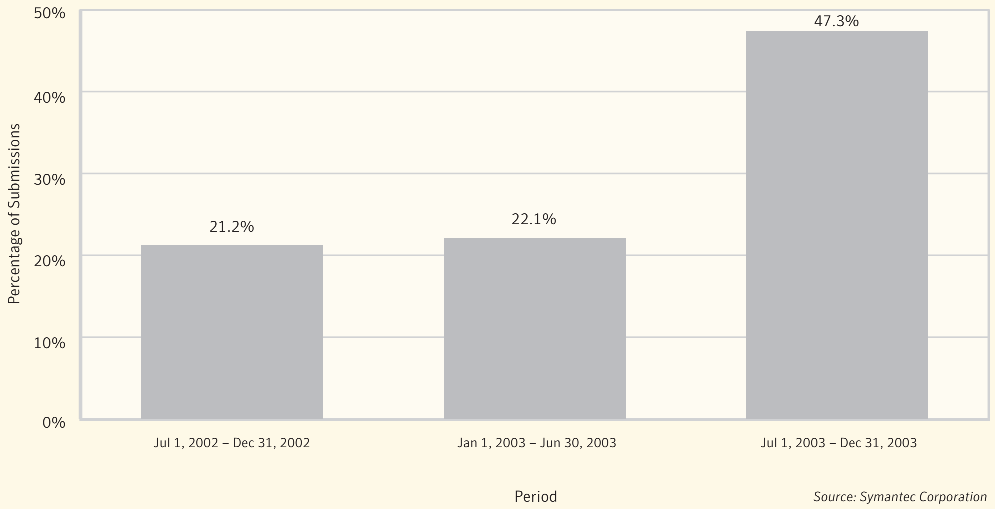
Bugbear.B accounted for approximately 18% of Symantec's top 50 submission volume over the past six months. This blended threat was designed to extract confidential data, such as lists of file names, lists of processes, user names, processor type, OS version, memory information, local drives, and network resource and type. Additionally, Bugbear.B can also deliver logged keystrokes to a third party, compromising important information such as passwords and decryption keys. The creator of this threat appears to have targeted banking institutions in an attempt to export financial data or gain future access to accounts by stealing users' account details and passwords.

BACKDOORS

Submissions to Symantec indicate a continued focus on malicious backdoors. The volume of submissions in Symantec's top ten reports shows an increase of 276% in this category **(Figure 17).** Of entries in Symantec's top 50 submissions, backdoors increased by 123%.

Backdoors can facilitate the unauthorized export of any type of data contained in or processed by the compromised system by providing remote access to it. Once a machine is compromised, intruders can install keystroke loggers and the keystrokes of all users can be exported to the attacker in an easy-to-read file. Entire sessions can be logged and passwords for any systems or applications accessed, recorded, and exported. Once a system is compromised, it can be used to mail out confidential information automatically or as a launching point for attacks against other systems.

Figure 17. Backdoors as percentage of top ten malicious code submissions



Source: Symantec Corporation

SPYWARE

Spyware programs track Internet browser usage, jeopardizing user privacy and confidentiality. These programs typically operate via Port 80; thus, they are often able to slip past firewalls without arousing suspicion. Spyware can deliver information about browser habits and user behavior to a third party.

The implications of spyware are inherently difficult to quantify. However, Symantec's research has shown that even though good technical solutions exist and many companies have security policies in place, users often knowingly engage in activities that risk exposure of confidential information.[24] Corporate and home users alike need to strengthen both technical and operational policies and procedures in order to preserve privacy and confidentiality. For instance, correctly implemented browser and firewall policies can help reduce the risks from spyware, particularly when combined with software that automatically deletes unwanted cookies.

FUTURE CONCERNS: PERVASIVE COMPUTING AND MOBILE DEVICES

Currently, the number of downloadable third-party applications for wireless computing is limited; thus, malicious code threats that can be directed at the devices are minimal. However, as pervasive computing increases, users will adopt wireless devices that are not only connected to the Internet, but that also have email and instant messaging capabilities. As that happens, the potential for these types of threats will increase. Symantec analysts continue to monitor the pervasive computing landscape.

FUTURE CONCERNS: LINUX

In 1998, Symantec observed the first example of a successful Linux worm, the Linux.ADM.Worm, which exploited a widely known vulnerability and compromised many systems. Following this outbreak, there was a period of inactivity. This ended with the appearance of the Slapper worm in September 2002. Although a major outbreak of a Linux worm has not been observed since Slapper, Symantec analysts continue to monitor the potential for Linux-based malicious code.

[24] Preliminary research findings are available at http://securityresponse.symantec.com/avcenter/reference/privacy.attitudes.behaviors.pdf

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.
7. All types of computer users need to know how to recognize computer hoaxes, which typically include a bogus email warning to “send this to everyone you know” and improper technical jargon to frighten or mislead users. 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 cyber crime by tracking and reporting intruders. With the Symantec Security Check tracing service, users can quickly identify the location of potential hackers and forward the information to the attacker’s Internet service provider or local police.

Appendix B—Attack Trends Methodology

Attack trends in this report are based on the analysis of data derived from Symantec DeepSight Threat Management System and Symantec Managed Security Services. Both services use a common naming convention for types of attacks, enabling analysts to combine and analyze attacks together or separately.

Symantec combines these two data sources for analysis when appropriate—that is, when they both contain the attributes required for the particular analysis. In some cases, only one data source is used if attributes required for a particular analysis are not available in the other.

Table 10 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 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 below is a high-level summary of the distinctions used in the report.

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

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

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

Table 10. 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. Due to the nature of monitoring activity, some statistics, such as event severity, client tenure, and attacks per company only apply to data received from Symantec Managed Security Services customers.	49%

Source: Symantec Corporation

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 **(Table 11)**. The primary purpose of this rating system is to prioritize client responses to malicious activity based on the relative level of danger that the event presents to their environment. A determination of severity is based on characteristics of an attack, defensive controls of the client, value of the assets at risk, and the relative success of the attack.

These four severity levels are further grouped into two classifications: severe and non-severe events. Severe events include activity classified as either “emergency” or “critical,” while non-severe events include activity classified as either “informational” or “warning.” For example, a severe event requires immediate countermeasures from an organization, while a non-severe event is mainly informative.

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 TEN 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.

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.

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

Table 11. Event severity classifications

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. *Example:* 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. Example: 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. *Examples:* (1) Continuous attacks by a single IP address against the client network or a significant vulnerability on the client’s network that was identified by either an attacker or the Security Operations Center (SOC). For example, a Web exploit is observed and appears to be successful, but there is no observed follow-up activity to take advantage of the vulnerability. (2) Unknown suspicious traffic that warrants an investigation by the client to track or eliminate the traffic flow.
	Emergency	These events indicate that a security breach has occurred on the client’s protected network. An emergency event requires the client to initiate some form of recovery procedure. Example: Successful exploit of a vulnerable Web server.

Source: Symantec Corporation

error. Currently, Symantec cross-references source IP addresses of attacks against every country in the world.

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

ATTACKS PER INTERNET CAPITA

The number of Internet users was obtained from the CIA *World Factbook*.[25] The CIA *World Factbook* provides a breakdown of the number of Internet users per country.

REGION OF ATTACK TARGETS FOR TOP ORIGINATING COUNTRIES

Symantec developed this metric as a representation of how the attack distribution of each top country compares to the global average attack distribution highlighted in the location of attack targets. For example, if the global distribution of attacks is 30% destined for North America, and only 15% of distribution from a given country was destined for North America, this would be represented as 0.50; whereas if 60% of the traffic was destined for North America, this would be represented as a 2.0. **Table 12** reflects the meaning of the numbers used in these distributions.

It should be noted that this metric is intended solely to represent the degree to which a country deviates from the global distribution, and is not an indication of overall attack rates.

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.

Figures 18 and **19** represent the industry breakdown of the sample set in percentage terms. Industries with less than ten sensors have been excluded from the resulting totals.

ATTACK SEVERITY BY INDUSTRY

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

TARGETED INDUSTRY ATTACK RATE

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

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.

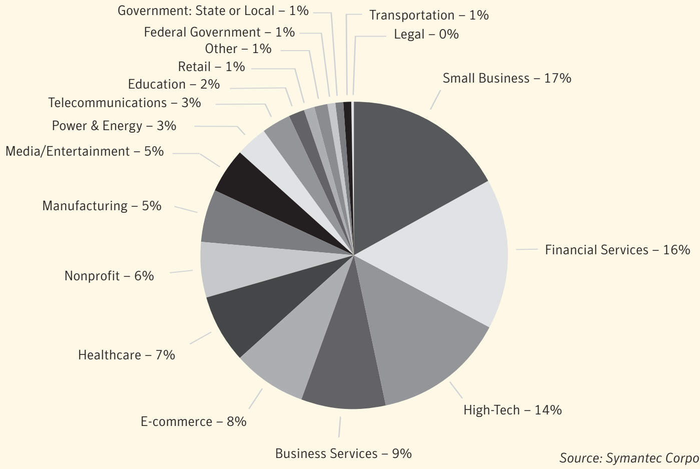
Table 12. Measurement of attack targets for top originating countries

Rank	Heading
0	No attacks destined for that region
<1	Less than the global average destined for that region
1	Same distribution as global average
>1	Greater than the global average destined for that region

Source: Symantec Corporation

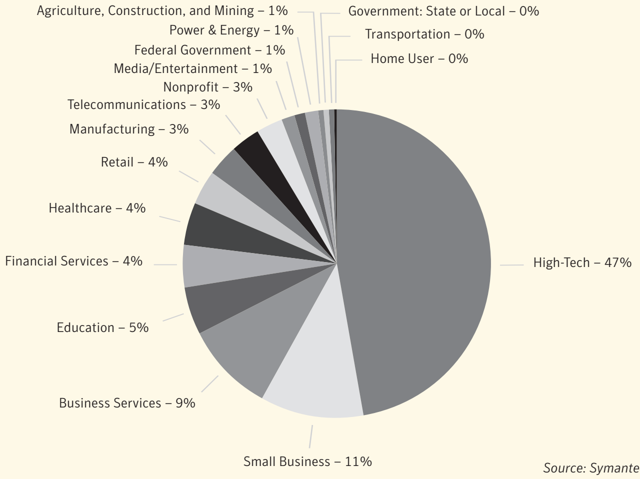
[25] Source: www.cia.gov/cia/publications/factbook

Figure 18. Symantec Managed Security Services sensor distribution by industry



Source: Symantec Corporation MSS data

Figure 19. Symantec DeepSight Threat Management System Sensor Distribution By Industry



Source: Symantec Corporation TMS data

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.

Appendix C—Vulnerability Trends Methodology

The "Vulnerability Trends" section of the Symantec *Internet Security Threat Report* discusses developments in the discovery and exploitation of vulnerabilities over the past six months. This methodology section will discuss how the data was gathered and how it was analyzed to come to the conclusions that are presented in the "Vulnerability Trends" section.

Symantec maintains one of the world's most comprehensive databases of security vulnerabilities, consisting of over 9,000 distinct entries. The information presented in the "Vulnerability Trends" section is based on the analysis of that data by Symantec researchers.

VULNERABILITY CLASSIFICATIONS

Following the discovery and/or announcement of a new vulnerability, Symantec analysts gather all relevant characteristics of the new vulnerability and create an alert. This alert describes important traits of the vulnerability, such as the severity, ease of exploitation, and a list of affected products. These traits are subsequently used both directly and indirectly for this analysis.

VULNERABILITY TYPE

After discovering a new vulnerability, Symantec threat analysts classify the vulnerability into one of 12 possible categories. The classification system is based on Taimur Aslam et al (1996), who define the taxonomy used to classify vulnerabilities.[26] Possible values are indicated below, and the previously mentioned white paper provides a full description of the meaning behind each classification:

- Boundary condition error
- Access validation error
- Origin validation error
- Input validation error
- Failure to handle exceptional conditions
- Race condition error
- Serialization error
- Atomicity error
- Environment error
- Configuration error
- Design error

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 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.

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

Table 13. Measurement of severity level

Severity Level	Severity Score Range
High	X ≥ 7
Moderate	4 ≤ X < 7
Low	X < 4

Source: Symantec Corporation

After gathering information on these four attributes, analysts use a pre-established algorithm to generate a severity score that ranges from one to ten. For the purposes of this report, vulnerabilities are rated as high, moderate, or low severity based on the scores presented in **Table 13.**

EASE OF EXPLOITATION

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

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

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

Appendix D—Malicious Code Trends Methodology

The trends in the “Malicious Code” 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 and individual consumers located throughout the world. Symantec then analyzes these suspect files, matching them with virus definitions. An analysis of this aggregate data set provides statistics on infection rates for different types of malicious code.

MALICIOUS CODE DATABASE

In addition to infection data, Symantec Security Response analyzes and documents attributes for each new form of malicious code that emerges both in the wild and in a "zoo" (or controlled laboratory) environment. Descriptive records of new forms of malicious code are then entered into a database for future reference. For this report, historical trend analysis was performed on this database to reveal trends, such as the use of different infection vectors and the frequency of various types of payloads.

Appendix E—Glossary

ASPack packers

ASPack is a particular type of packer that compresses Win32 executable files.

Blended threat

Blended threats combine the characteristics of viruses, worms, Trojan horses, and malicious code with server and Internet vulnerabilities to initiate, transmit, and spread an attack. By using multiple methods and techniques, blended threats can rapidly spread and cause widespread damage.

Buffer overflow

A buffer overflow is a type of programmatic flaw that is caused by a programmer allowing for an unbounded operation on data. Buffer overflow conditions commonly occur during memory copy operations. In these cases, a lack of bounds checking can allow for memory to be written beyond the buffer, corrupting potentially sensitive values in adjacent memory. Buffer overflow conditions have typically been exploited to hijack program execution flow (i.e., execute arbitrary instructions) by overwriting activation records in stack memory. Buffer overflows in the heap have also proven exploitable, allowing for attackers to have their own instructions executed in the process space of the affected program.

CIFS

Common Internet File System (known previously as SMB) is the file-sharing protocol used natively by Windows-based operating systems. Now supported by many other operating systems, CIFS has become a standard by which files are transferred over a network.

Client-side vulnerability

A vulnerability that is present in a computer or device that requests and receives services from another computer known as a server. Common clients are Web browsers, such as Internet Explorer, and email clients, such as Outlook.

Exploit

A software program, hardware device, or technique that takes advantage of a vulnerability in software and that can be used for breaking security or otherwise attacking a computer.

Heuristics-based detection

Heuristics-based detection is an antivirus technique that detects viruses by scanning files for anomalous actions. A rule-based method, heuristic scanning searches files for certain instructions or commands that are not found in typical application programs. This allows a heuristic engine to detect previously unknown malicious code.

Infection vector

The method by which malicious code gains access to a computer system. The most common infection vector today is email. Other vectors of infection include network shares with weak or no password protection, floppy disks, vulnerabilities in software, peer-to-peer software, and instant messaging.

Internet Relay Chat (IRC)

An Internet-based system for multiple parties to communicate synchronously or asynchronously, often on a specific topic of interest. IRC is a concern for security personnel because it offers a potential infection vector for the proliferation of malicious code.

Kazaa

A popular, free, peer-to-peer file-sharing network that is often used to exchange audio and video files.

Malicious payload

Typically referred to as "payload" because it is assumed to be malicious. Malicious activities performed by a threat in addition to the self-replication routine of a virus. The majority of viruses do not contain a payload, but simply replicate. Payloads include denial-of-service attacks, destruction or modification of data, changes to system settings, and information disclosure.

Mass mailer

A threat that self-replicates by sending itself out by email. Typically, the threat obtains email addresses by searching files on the system or responding to messages found in the email client inbox.

Netblock

A netblock is the "block" of IP addresses that have been assigned to a network. The network may be assigned an entire address range; for example, a Class C network that would have a maximum of 256 IP addresses. Individual IP addresses can be assigned from within the netblock, or it can be segregated into smaller "subnets" within that overall netblock for use.

Packers

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.

Pervasive computing

The integration of computing and communications technology into non-traditional contexts and applications, particularly small mobile devices that can allow for ubiquitous connectivity to the Internet and other communications networks.

Remotely exploitable

Remotely exploitable vulnerabilities are those that can be exploited by attackers across a network. For example, vulnerabilities in Web servers that can be exploited by Web clients are remotely exploitable vulnerabilities.

SQL injection attack

An Internet-based database attack in which an attacker obtains unauthorized access to information systems by manipulating SQL (structured query language) code.

UPX packers

A specific type of packer that is free, publicly available, and compresses files for several different executable formats.

Virus

A self-replicating computer program.

Vulnerability

A security vulnerability is a condition affecting an information system that can cause it to function outside of its documented design such that it violates its documented security policy. Vulnerabilities can be the result of implementation errors, design oversights, and insecure default configurations. A vulnerability can be fixed with a patch or update.

Worm

A program that makes copies of itself on the network: for example, from one network disk drive to another, or by using email or another transport mechanism.

SYMANTEC, THE WORLD LEADER IN INTERNET SECURITY TECHNOLOGY, PROVIDES A BROAD RANGE OF CONTENT AND NETWORK SECURITY SOFTWARE AND APPLIANCE SOLUTIONS TO INDIVIDUALS, ENTERPRISES, AND SERVICE PROVIDERS. THE COMPANY IS A LEADING PROVIDER OF CLIENT, GATEWAY, AND SERVER SECURITY SOLUTIONS FOR VIRUS PROTECTION, FIREWALL AND VIRTUAL PRIVATE NETWORK, VULNERABILITY MANAGEMENT, INTRUSION DETECTION, INTERNET CONTENT AND EMAIL FILTERING, AND REMOTE MANAGEMENT TECHNOLOGIES AND SECURITY SERVICES TO ENTERPRISES AND SERVICE PROVIDERS AROUND THE WORLD. SYMANTEC'S NORTON BRAND OF CONSUMER SECURITY PRODUCTS IS A LEADER IN WORLDWIDE RETAIL SALES AND INDUSTRY AWARDS. HEADQUARTERED IN CUPERTINO, CALIF., SYMANTEC HAS WORLDWIDE OPERATIONS IN 38 COUNTRIES.

FOR MORE INFORMATION, PLEASE VISIT WWW.SYMANTEC.COM

symantec™

WORLD HEADQUARTERS

20330 Stevens Creek Blvd.
Cupertino, CA 95014 U.S.A.
408.517.8000
800.721.3934

www.symantec.com

For Product Information

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

Symantec has worldwide operations in 38 countries. For specific country offices and contact numbers please visit our Web site.