symantec™

Symantec Internet Security Threat Report

September 2003

EXECUTIVE EDITOR
Linda McCarthy
Symantec Office of the CTO

MANAGER, DEVELOPMENT
David Ahmad
Symantec Security Response

SENIOR THREAT ANALYST
Cori Lynn Arnold
Symantec Managed Security Services

SENIOR MANAGER, ANALYSIS OPERATIONS
Brian Dunphy
Symantec Managed Security Services

SENIOR MANAGER, DEVELOPMENT
Oliver Friedrichs
Symantec Security Response

RESEARCH FELLOW
Sarah Gordon
Symantec Security Response

SECURITY ARCHITECT
Peter Szor
Symantec Security Response

PRINCIPAL TREND ANALYST
Mike Prosser
Symantec Security Services

SENIOR DIRECTOR, DEVELOPMENT
Vincent Weafer
Symantec Security Response

Executive Summary

The Symantec *Internet Security Threat Report* provides a six-month update about Internet threat activity[1]. It includes analysis of network-based attacks, a review of known vulnerabilities, and highlights of malicious code. This summary of that report can alert executives to impending threats and current trends.

With over 20,000 sensors monitoring network activity in over 180 countries, Symantec has established one of the most comprehensive sources of Internet threat data in the world, giving Symantec's analysts a superior source of attack data from which to spot important trends. These trends educate executives about potential threats and exposures, and using the data can help them identify weaknesses in their own security architecture or policies.

In August 2003, the Win32.Blaster blended threat rapidly spread worldwide, and several other highly severe worms followed. In only eight days the pace and frequency of these threats created havoc for systems administrators as well as for PC home users, with an estimated cost of damages running up to $2 billion[2]. This report clearly shows why some corporations were prepared and not affected by these threats while others were unprepared. Threat Report highlights:

ATTACK HIGHLIGHTS:

- Systems in the United States are still the primary source of attacks
- Increased scanning of non-public services, such as Microsoft SQL Server
- Severe events for managed security service customers decreased 52%
- Remote execution of commands

MALICIOUS CODE HIGHLIGHTS:

- Blended threats have increased 20%
- Increased threat to confidential data
- Speed of propagation has increased
- Linux systems may be targeted for future attacks
- Windows 32—increased sophistication of malicious code
- New infection vectors:
  – Instant messaging
  – Peer-to-peer service

VULNERABILITY HIGHLIGHTS:

- 80% of all vulnerabilities discovered are remotely exploitable
- Web application vulnerabilities up 12%
- Attacks are being released faster
- Areas to watch for new vulnerabilities:
  – Integer error
  – Timing analysis
  – Microsoft Internet Explorer
  – Microsoft IIS

CURRENT ISSUES:

- In August 2003, Blaster worm exploits a vulnerability 26 days after it was discovered
- The cost of eight days of massive worm attacks in August may be up to USD$2 billion
- Corporate systems and PC home users remain at risk

[1] All data analyzed in this report reflect data captured between January 1, 2003, and June 30, 2003, and are compared to data captured between January 1, 2002, and June 30, 2002, unless noted otherwise.
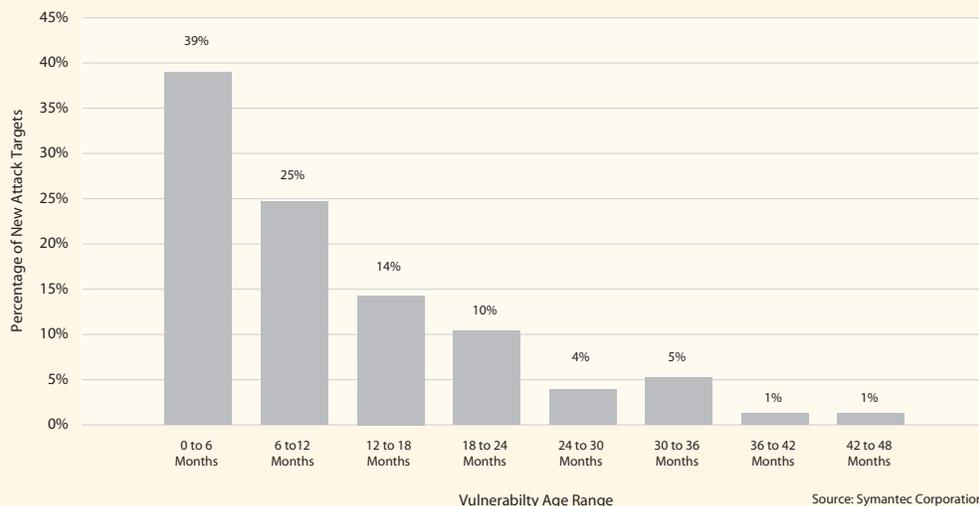[2] Computer Economics estimates the economic impact of the recent wave of outbreaks: http://www.computereconomics.com/article.cfm?id=867

The Window of Time to Patch Systems is Closing

ATTACKS ARE BEING RELEASED QUICKER

Blaster used a well-known Microsoft security flaw that had been announced only 26 days before Blaster was released. This fact supports our analysis that the time from discovery to outbreak has shortened greatly. During the first half of 2003, our analysis shows that attackers focused on the newer vulnerabilities; of all new attacks observed, 64% targeted vulnerabilities less than one year old. Furthermore, attackers focused on highly severe vulnerabilities that could cause serious harm to corporations; we found that 66% targeted highly severe vulnerabilities. That attackers are quickly focusing on the attacks that will cause the most harm or give them the most visibility should be a warning to executives. Corporations must enforce patch-management policies to ensure that systems are protected from newly found flaws and must deploy adequate defenses in advance to protect their data against new threats on the horizon.

Figure 1
Vulnerabilities Targeted for New Attacks by Vulnerabilty Age
(January 1, 2003–June 30, 2003)

Percentage of New Attack Targets

Vulnerabilty Age Range	Percentage
0 to 6 Months	39%
6 to 12 Months	25%
12 to 18 Months	14%
18 to 24 Months	10%
24 to 30 Months	4%
30 to 36 Months	5%
36 to 42 Months	1%
42 to 48 Months	1%

Source: Symantec Corporation

Blended Threats

BLENDED THREATS INCREASING IN SPEED AND FREQUENCY

Blended threats, which use combinations of malicious code to begin, transmit, and spread attacks, are increasing and are among the most important trends to watch and guard against this year. By using multiple techniques, blended threats can spread to large numbers of hosts, causing rapid and widespread damage. During the first half of 2003, blended threats increased nearly 20% over the last half of 2002. One blended threat alone, Slammer, disrupted systems worldwide in less than a few hours. Slammer's speed of propagation, combined with poor configuration management on many corporate sites, enabled it to spread rapidly across the Internet and cause outages for many corporations. Companies hit by Slammer were not harmed as badly as they might have been, because it was designed to propagate quickly, degrade networks, and to compromise vulnerable systems rather than cause destruction or steal confidential data. Corporations that had updated firewalls, updated patches, and virus protection throughout the enterprise were prepared for this attack.

Blended-Threat Targets

MICROSOFT IIS VULNERABILITIES

Microsoft IIS is one of the most widely deployed Web servers throughout the world. Symantec has documented several high-severity vulnerabilities affecting it. Their characteristics render these vulnerabilities attractive targets for future blended threats. Given Microsoft IIS's susceptibility to past blended threats such as Code Red and Nimda, Symantec believes that it may again be hit by highly destructive malicious-code attacks.

MICROSOFT INTERNET EXPLORER VULNERABILITIES

Several vulnerabilities allow attackers to compromise client systems through Web pages containing embedded malicious code. Others can enable the easy and almost undetectable installation of spyware, which allows attackers to extract confidential data.

THEFT OF CONFIDENTIAL DATA

The release of Bugbear and its variant Bugbear.B (discovered in early June 2003) were good examples of theft of confidential data. Once systems were infected, confidential data was extracted such as file names, processes, usernames, keystrokes, and other critical system information, and delivered to a third party, potentially compromising passwords and decryption keys. Furthermore, it appears that the creator of Bugbear specifically targeted banks.

During the first half of 2003, Symantec saw a 50% increase in confidential data attacks using backdoors. By granting access to compromised systems, backdoors allow data to be exported to unauthorized individuals. For example, entire sessions can be logged, and passwords for systems and applications can be taken. Companies need to implement controls that make it difficult for malicious code to steal confidential data, such as updated firewalls, patch management policies, intrusion detection, virus protection, and so on.

ATTACKERS EXECUTING COMMANDS FROM THOUSANDS OF INFECTED SYSTEMS

Once a system is compromised, an attacker can install malicious code known as a "bot" that allows the attacker to use the system for future scanning or as a launching point for future attacks (such as planned, distributed denial-of-service attacks). Once a system has become infected, the attacker can maintain a running list of the entire botnet (network of infected systems) by simply issuing commands through Internet Relay Channel (IRC is a common communication channel used by bots). Afterwards, all listening bots (sometimes numbering in the thousands) will execute any command issued by the attacker. Symantec examined an automated tool like this, which accounted for supposable Nimda (blended threat) traffic, after it was captured in a Honeypot network[3].

CONCLUSION

The evidence in this report clearly shows that the risk of blended threats and attacks is rising. Understanding how to budget for security and what products and services are needed will involve some of the most important decisions that every corporation faces in the 21st century. The trends that we discuss in this report help executives understand some of the threats faced by their systems administrators every day.

Symantec carefully monitors other potential threats such as the rise in peer-to-peer attacks (including instant messaging), mass mailers (like SoBig), the general trend toward theft of confidential information, and the rapid increase in the number of Windows 32 (Win32) threats. These issues and others are discussed further in each section of Symantec's *Internet Security Threat Report*, available for download at *www.ses.symantec.com/ITR*.

---

[3] For details about this tool see, https://tms.symantec.com/members/AnalystReports/030627-IllpatientAnalysis.pdf

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 36 COUNTRIES.

FOR MORE INFORMATION, PLEASE VISIT WWW.SYMANTEC.COM

![Symantec logo]

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 36 countries. For specific country
offices and contact numbers please
visit our Web site.

Symantec Internet Security Threat Report

Trends for January 1, 2003 – June 30, 2003

EXECUTIVE EDITOR
Linda McCarthy
Symantec Office of the CTO

SENIOR THREAT ANALYST
Cori Lynn Arnold
*Symantec Managed Security
Services*

**SENIOR MANAGER, ANALYSIS
OPERATIONS**
Brian Dunphy
*Symantec Managed Security
Services*

**SENIOR MANAGER,
DEVELOPMENT**
Oliver Friedrichs
Symantec Security Response

PRINCIPAL TREND ANALYST
Mike Prosser
Symantec Security Services

Contents

Report Highlights

Overall threats remained significant during the first half of 2003. Companies without adequate controls risk having their networks and applications compromised. This report discusses in depth some specific findings that support this observation.[1]

HIGHLIGHTS: ATTACK TRENDS

- The top ten attack sources account for nearly 80% of all attack activity
- Systems in the United States are still a primary source of attacks
- Increased scanning of non-public services, such as Microsoft SQL Server
- Network-based attacks were 19% higher
- The severe event incidence rate declined by 52% among managed security service customers
- 11% of companies suffered from at least one severe event, down from 23% in 2002
- Most attacks occurred between 1 p.m. and 10 p.m. GMT (from 8 a.m. to 5 p.m. EST)
- Remote execution of commands

Types of Attacks

OVERVIEW

Attack trends noted here are based on data from two sources: Symantec DeepSight Threat Management System and Symantec Managed Security Services. This first section of the report provides insights into major trends in actual attack activity based on statistical analysis of real-time attacks. With the ability to select data from 20,000 sensors in over 180 countries around the world, the sample size has doubled over the previous six-month period. (See *The Threat Report Methodology* document for the methodology used.)

The statistics presented in this section, with the exception of the top ten attacks and scans, exclude activity associated with major worms and blended threats, such as SQL Slammer, Code Red, and Nimda.[2] This was done because a small number of worms and blended threats accounted for the vast majority of attack activity (78% during this time period). Filtering out this type of activity enables Symantec to identify underlying, important attack trends that would otherwise be obscured or completely hidden by the sheer volume of activity from major worms and blended threats.

This section highlights:

- Attack sources by location
- Attacks by day of the week
- Attacks by time of day
- Severity of attacks
- Top ten attack types

---

[1] All data analyzed in this report were captured between January 1, 2003, and June 30, 2003, and are compared with data captured between January 1, 2002, and June 30, 2002, unless noted otherwise.
[2] The top ten attacks and scans include worm and blended threat activity in order to show what systems administrators are seeing every day. Unless otherwise stated, all other statistics presented in the attack section exclude worms and blended threats. Worms and blended threats are covered in detail under the Malicious Code section of this report.

ATTACK SOURCES
Top Ten Attack Sources

Symantec's analysis of the origins of attacks showed that 80% of all attacks were launched from systems located in just 10 countries. As noted in past reports, systems in the United States were the main source of attack, and in the first half of 2003, 51% of all attacks were launched from systems located within the United States. The top ten countries identified as attack sources were virtually the same as those reported in the same six-month period of 2002. The only exception was the Netherlands, which replaced Taiwan (even though the data set now includes the Symantec DeepSight Threat Management System data). See **Figure 1**.

It is simple to trace an attack back to the last IP address from which the attack was launched, but this location is seldom the attacker's own system. Attackers normally hop through multiple unsecured 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.

Top Ten Attack Sources per Internet Capita

In addition to identifying the top ten attack sources in terms of overall volume, Symantec analyzed attacks by country in relation to the number of Internet users within each country. This metric is intended to identify geographic locations with relatively high concentrations of attacking systems. For example, a country such as Israel does not show a high overall volume of attack activity mainly because the country has a small Internet user base. But when attacks from Israel are expressed on a per–Internet user basis, it becomes clear that this country consistently shows a high "concentration" of attacking systems relative to the size of its Internet user base.

Figure 1:
Top Ten Attack Sources
Six Months Ending June 2003

Rank	Country	Percent of Total
1	United States	51%
2	China	5%
3	Germany	5%
4	South Korea	4%
5	Canada	4%
6	France	3%
7	Great Britain	2%
8	Netherlands	2%
9	Japan	2%
10	Italy	2%

Source: Symantec Corporation

Figure 2: Top Ten Attack Sources per Internet Capita
Countries with Greater than 1 Million Users
Six Months Ending June 2003

Rank	Country
1	Israel
2	United States
3	Belgium
4	New Zealand
5	Canada
6	Chile
7	France
8	Netherlands
9	Norway
10	Mexico

Source: Symantec Corporation

Figure 3: Top Ten Attack Countries per Internet Capita
Countries with between 100,000 and 1 Million Internet Users
Six Months Ending June 2003

| Rank	Country
1	Peru
2	Iran
3	Kuwait
4	United Arab Emirates
5	Nigeria
6	Saudi Arabia
7	Croatia
8	Vietnam
9	Egypt
10	Romania

Source: Symantec Corporation

Figures 2 and **3** show the top attack sources per 10,000 Internet users in two different classes. The first includes countries with more than 1 million Internet users; this group represents countries with a relatively large, developed Internet infrastructure. The second includes countries with between 100,000 and 1 million Internet users; this group represents countries with smaller and less-developed Internet infrastructures. Countries with fewer than 100,000 Internet users were excluded from this analysis.

ATTACKS BY DAY OF WEEK
Symantec has noted in past reports that certain hours of the day and days of the week are more or less prone to attack activity. During the first half of 2003, Symantec noted decreased attack activity on weekends, echoing the trends of past reports. Although only 20% of attackers were active over the weekend, possibly taking advantage of reduced support staff and the less likelihood of detection, this reinforces the need for continuous security monitoring.

Symantec also compared attack activity related to worm propagation versus all other attack activity. While worms don't care what day of the week it is, there are many other factors that affect their propagation rate, for example, the number of computers turned on. As a result, attacks associated with worm propagation are not perfectly distributed across the week, and there is a minor dip in activity over the weekend (though much less of a dip compared with non-worm attack activity). **Figure 4** shows the percentage of worm and non-worm attackers detected by day of week during the first half of 2003.

Figure 4: Attacker Activity by Day of Week
(January 1, 2003 – June 30, 2003)

Source: Symantec Corporation
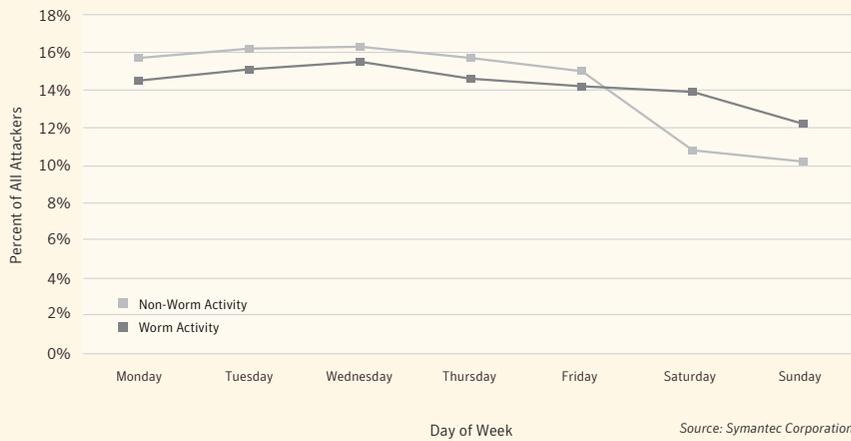
ATTACKS BY TIME OF DAY

Attack activity for the entire Internet community consistently peaks at predictable times during the day. For all Internet-connected organizations (regardless of geographic location), attack activity against a target peaks between 1:00 p.m. GMT and 10:00 p.m. GMT.[3]

Since attacks originate globally, an individual organization's normal work hours will not correlate directly with the peak attack activity. However, depending on the location of the organization, the local time for this peak attack activity will vary. For example, a corporate network in Washington, D.C., will see peak activity between the hours of 8:00 a.m. and 5:00 p.m. EST. However, an organization in Tokyo, Japan, will see peak activity between the hours of 10:00 p.m. and 7:00 a.m. the next day.

Without effective detection and monitoring in conjunction with strong security awareness programs and policies, such attacks would be a challenge to notice at any hour of the day or night.

[3] The Greenwich Meridian (Prime Meridian or Longitude Zero degrees) marks the starting point of every time zone in the world. GMT is the average (mean) time it takes the earth to make a complete rotation. GMT has been measured from Greenwich, England, since 1884 (http://greenwich2000.com/).

INTERNET ATTACKS PER COMPANY

The overall rate of attack activity during the past six months was 19% higher than the rate for the same six-month period in 2002. On average, companies experienced approximately 38 attacks per company per week, as compared with 32 attacks per company per week during the same six-month period in 2002.[4] **Figure 5** illustrates this trend.

Despite the rise in attack volume, Symantec saw a decline in the number of severe debilitating attacks.

SEVERITY OF ATTACKS
Sharp Decline in Severe-Event Incidence

On average, companies were substantially less likely to experience a severe event during the past six months, as compared with the prior six-month period.[5] Only 11% of companies suffered from one or more severe events during the first six months of 2003, versus 23% during the same period in 2002. **Figure 6** shows the reduction of severe event incidence rates in the last year. While it is difficult to isolate the cause of this trend, Symantec believes it reflects the overall strengthening of the security policies among customers.

Figure 5: Attacks per Company per Week
(First Six Months of 2002 vs. First Six Months of 2003)

Source: Symantec Corporation
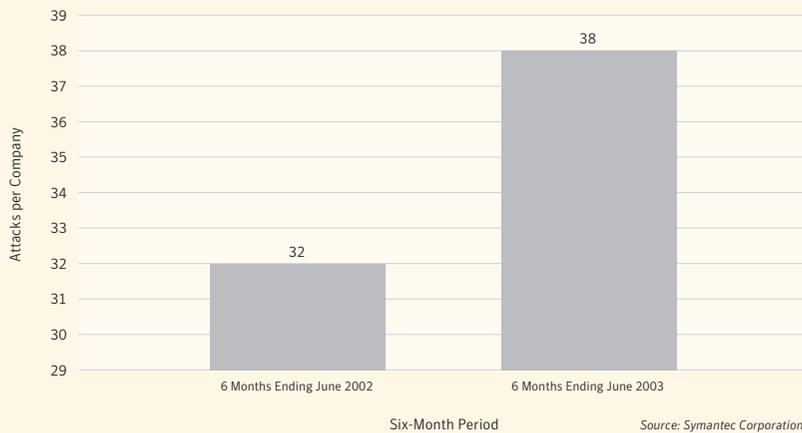
Figure 6: Severe Event Incidence by Six-Month Period

Source: Symantec Corporation

---
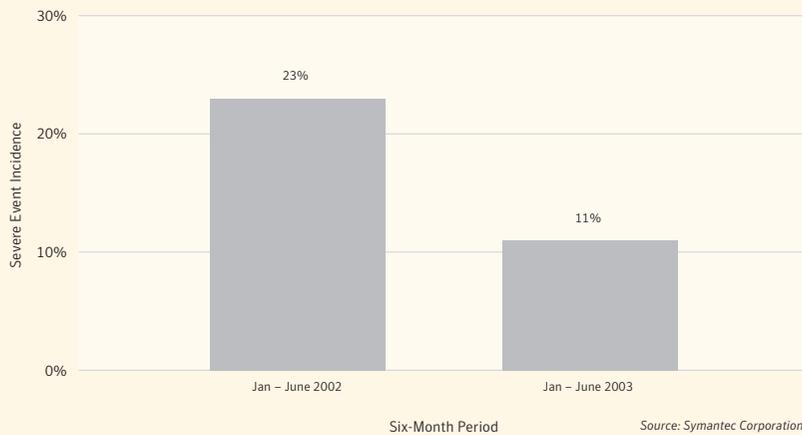
[4] Total number of attacks came from Managed Security Service data.
[5] Only companies that subscribe to the Symantec Managed Security Service were evaluated in terms of event severity. This is because attacks detected by the DeepSight Threat Management systems are not currently classified according to severity. For more details on event severity, see Appendix A.

Figure 7: Severe Event Incidence by Client Tenure
(January 1, 2003 – June 30, 2003)

Bar chart with vertical axis "Severe Event Incidence" ranging 0% to 25% and horizontal axis "Months of Tenure":
- 1–3 Months: 20%
- 4–6 Months: 19 %
- 7–9 Months: 10%
- 10–12 Months: 9%
- 13–15 Months: 12 %
- 16–18 Months: 12 %
- 19+ Months: 11 %

Source: Symantec Corporation
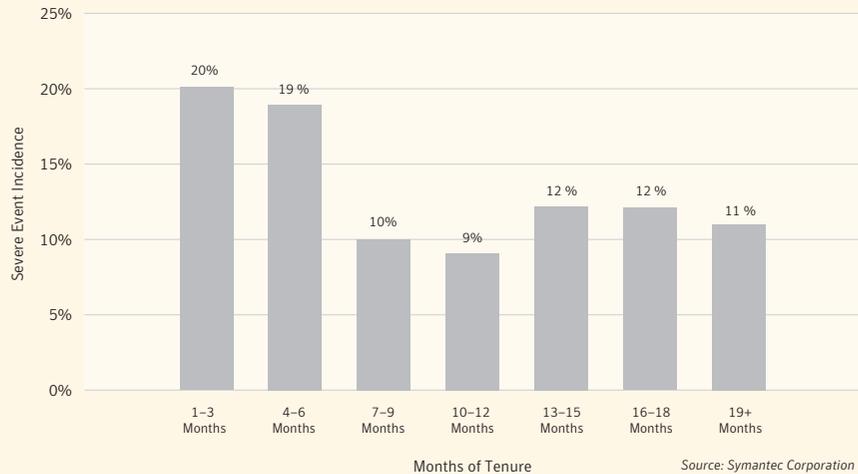
Prevalence of Non-Severe Events

More than 99% of all events detected by Symantec during the first six months of 2003 were classified as non-severe and did not represent an immediate threat to the companies in the sample set. It is probable that this type of "noise" constitutes the vast majority of attacks detected by companies throughout the Internet, which explains why companies often experience such difficulty isolating "real threats" from the vast amounts of attack data.

Positive Results with Symantec Managed Security Service Client Tenure

Symantec uses a metric, called client tenure, to assess how the effectiveness of a company's attack defenses evolve as Symantec drives improvements to their security posture over time. In the past, this metric revealed that companies with greater tenure as security monitoring clients were less likely to suffer severe events. The hypothesis was that tenured clients tended to have stronger security postures, which made severe events less likely.

For this issue of the *Threat Report,* Symantec retested this hypothesis, and the results suggest that the trend has continued. The one difference, however, is the level of tenure at which severe event incidence drops. During the first half of 2003, companies with less than six months of tenure were nearly twice as likely to suffer a severe event as companies with greater than six months of tenure. In the previous report, the likelihood of suffering a severe event dropped sharply at the 12-month point. **Figure 7** shows the severe event incidence rates by client tenure.

Top Ten Attacks and Network Scans

In past reports, Symantec analyzed the top 10 network scans launched against companies in order to provide a better understanding of the types of services attackers most often seek to exploit. For the current issue of the *Threat Report,* Symantec repeated this investigation and added our analysis of the top 10 attacks. This new measurement reveals the specific attacks that were most commonly detected against companies. In sum, the top 10 scans can be thought of as a measurement of reconnaissance activity, while the top 10 attacks

measure the specific attacks that are actually launched. **Figures 8** and **9** list the top 10 attacks and the top 10 scans (worm and blended threat attacks were included in this analysis).

While the top ten scans measure reconnaissance activity, they do not correlate to the top ten attacks. Most of the attacks detected for the first half of 2003 were associated with worm activity (**Figure 8**).

Figure 8: Top Ten Attack Types
(January 1, 2003 – June 30, 2003)

Rank	Signature	Percent of All Attacks
1	Microsoft SQL Server 2000 Resolution Service Stack Overflow Attack	27%
2	Microsoft Indexing Server/Indexing Services ISAPI Buffer Overflow Attack	17%
3	Muhammad A. Muquit Count.cgi Attack	6%
4	Generic HTTP Directory Traversal Attack	3%
5	Generic WebDAV/Source disclosure "Translate: f" HTTP Header Request Attack	2%
6	Microsoft IIS Escaped Character Parsing Attack	2%
7	SMB-NETBIOS Default Administrative Share Attack	2%
8	Microsoft IIS/PWS Escaped Characters Decoding Command Execution Attack	2%
9	Microsoft FrontPage Sensitive Page Attack	2%
10	Microsoft IIS 4.0/5.0 Extended UNICODE Directory Traversal Attack	1%

Source: Symantec Corporation

Figure 9: Top Ten Network Scans
(January 1, 2003 – June 30, 2003)

Rank	Scan Type	Port	Percent of All Attacks
1	Common Internet File System (CIFS)	445/tcp	24%
2	NetBIOS Name Service	137/udp	16%
3	Microsoft SQL Monitor	1434/udp	11%
4	HTTP	80/tcp	10%
5	FTP	21/tcp	6%
6	Microsoft SQL Server	1433/tcp	6%
7	17300/tcp	17300/tcp	4%
8	HTTPS	443/tcp	4%
9	NetBIOS Session Service	139/tcp	4%
10	NetBIOS RPC	135/tcp	2%

Source: Symantec Corporation

Blended Threat Targets

A total of 51% of all network scans targeted the top three services. When compared to the same time period last year, these same three services accounted for only 2% of network scans. For example, prior to Slammer, scanning activity related to Microsoft SQL Monitor (1434/udp) was almost non-existent. This shows that a worm can easily turn an obscure vulnerability into the number one attack within minutes.

Systems administrators must be aware of a sudden shift or increase in activity over ports. Knowing that a possible attack is on the horizon can make the difference between being attacked or being prepared to adequately defend against an attack. To guard against attacks, systems administrators can benefit from early warning and intrusion detection for both known and unknown attacks.[7]

Increased Threat to Non-Public Services

Out of the top scanned ports, only three services are commonly made available as public services: FTP, HTTP, and HTTPS. Of these three services, only HTTPS was scanned at a much higher rate than during the same time period last year. Most of the top ten scans targeted non-public services such as Microsoft SQL Server and file sharing (services that are commonly available on both home computers and internal corporate networks). When non-public services are exploited, the number of potential victims is substantially higher than in systems that only host public services. Although companies do not typically allow these non-public services to enter their networks directly from the Internet, internal systems are still at risk because of unsecured and unpatched laptops and home computers connecting via VPNs. This trend reinforces the importance of extending security policies and controls beyond public-facing systems.

Misconfigured Proxies

During this time period, three common proxy services were routinely targeted: SOCKS, Alt SOCKS, and Squid.

A proxy server acts as an intermediary between a private network and the Internet. To increase performance, many proxy servers cache Web content. Misconfigured proxy servers are frequently used by spammers to relay anonymous unsolicited email and may also allow an attacker to gain unauthorized access to networks. Many unsophisticated home computer users are setting up proxy servers to share a single cable modem or DSL line with multiple home computers. This increases the risk of unauthorized use and access.

Attacks Disguised as Worm Activity

Most of the top-ranking attacks were attributed to blended threats (such as Nimda and Code Red). Once released these worms continue to thrive on vulnerable networks long after their first appearance. Attackers often use the same vulnerabilities as worms to build large networks of compromised systems. By blending in with worm activity, attackers can go unnoticed by systems administrators.

An area of concern is that once a system is compromised, an attacker can install malicious code known as a bot that allows the attacker to use the system for future scanning or as a launching point for future attacks (such as planned distributed denial-of-service attacks). A bot (short for robot) is a small application that serves as an agent for another program or user. There are good (legal) bots such as Web crawlers or bad bots that are installed without the user's knowledge. These bad bots, or "zombies" as they are sometimes called, will listen on a designated port for commands from their master.

One common communication channel often used by bots is Internet Relay Chat (IRC). By having each individual bot connected to an IRC server once a system has become infected, the attacker can maintain a running list of the entire botnet by simply issuing commands through IRC. Then all listening bots (sometimes numbering in the thousands) will execute any command issued by the attacker. Symantec examined an automated tool like this, which accounted for supposable Nimda (blended threat) traffic after it was captured in a Honeypot network.[8]

---

[7] Unknown attacks are often referred to as zero-day attacks. Threats at this point in their life cycles are also called *zero-day* attacks. Because they are not publicly known, they are not yet reflected in detection signatures and can sidestep existing defenses.
[8] For details about this tool see, https://tms.symantec.com/members/AnalystReports/030627-IllpatientAnalysis.pdf

FTP Scans

Although FTP scans decreased from the same time period last year, systems administrators should not let down their guard. While FTP servers were not affected by blended threat activity (the only service in the top ten list not affected), unauthorized individuals continue to exploit misconfigured FTP servers with writable directories to share a variety of copyrighted content (such as movies, music, software, and pornography). Systems administrators should test their FTP servers to ensure that they are configured correctly. Routine testing for misconfigured systems can help ensure that systems are secure and have not been compromised.

Glossary

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 due to 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.

Class A Network

A Class A network is the largest IP address class of the three public use "classes" (Class A, Class B, and Class C) in the IP address space. There are 127 Class A networks with each supporting around 16 million hosts or individual IP addresses. Classless Inter-Domain Routing (CIDR) is an updated addressing scheme that provides more effective use of IP addresses than the old Class A, B, and C scheme. You will now see Class A networks called a /8 (slash eight) network, so called for the 8-bit network prefix assigned under CIDR.

Exploit

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

Infection Vector

The method in which malicious code gains access to a computer system. The most common infection vector today is email. Other vectors of infection include floppy disks, vulnerabilities in software, peer-to-peer software, and instant messaging.

Integer Error

Integer errors are a type of programmatic flaw caused by a failure to properly handle variables of the integer data type. Integer errors can result in unexpected/unanticipated behavior in affected programs and can sometimes allow attackers to hijack the execution flow of the affected program.

Malicious Payload

Typically referred to as "Payload" because "malicious" is a major part of the definition. 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 for email addresses in 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, e.g., 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.

Remotely Exploitable

Remotely exploitable vulnerabilities are those which 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.

Side-Channel Attack

An attack that typically targets a weakness in the implementation of a system rather than its design. Errors in implementations of systems can cause a leak of important information in the timing of specific events. By observing the amounts of time that a system takes to perform certain behavior, attackers can sometimes obtain or infer valuable information. For example, knowledge of crucial timing information can possibly allow an attacker to compromise SSL/TLS sessions. Other reported timing-analysis attacks allowed attackers to guess valid usernames or determine the existence of confidential files. To a sophisticated attacker, timing-analysis and side-channel vulnerabilities offer powerful new methods to penetrate highly secure systems.

Virus

A self-replicating computer program.

Vulnerability

A security vulnerability is a coding error within a software system that can cause it to function outside of its documented design, violating its documented security policy. 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 copying itself 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 36 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 36 countries. For specific country
offices and contact numbers please
visit our Web site.

Symantec Internet Security Threat Report

Trends for January 1, 2003 – June 30, 2003

Contents

Report Highlights

Overall threats remained significant during the first half of 2003. Companies without adequate controls risk having their networks and applications compromised. This report discusses in depth some specific findings that support this observation.[1]

HIGHLIGHTS: VULNERABILITY TRENDS

- 80% of all vulnerabilities are exploited remotely
- Web application vulnerabilities are up 12%
- New vulnerabilities with a high severity rating are being exploited faster
- Areas to watch for new vulnerabilities:
  - Integer errors—introduced in routine programming
  - Timing analysis—subtle weaknesses that may compromise cryptosystems
  - Microsoft Internet Explorer—widespread client systems continue to be affected by serious vulnerabilities
  - Microsoft IIS—susceptible to blended threats

Vulnerability Discovery

OVERVIEW

As attackers persist in finding new vulnerabilities, the risk to the Internet community continues to intensify. Unfortunately, just a single vulnerability opens the door to a successful attack. Systems thought to be secure are left vulnerable unless proper controls are in place to fix new found flaws. To address these issues, organizations need proactive, early warning systems that alert IT organizations to new vulnerabilities and active attacks.

This section describes major trends seen during the first half of 2003.

This section highlights:

- Severity of vulnerabilities
- Ease of exploitation
- Attack prioritization
- Globalization
- Trends in vulnerabilities

[1] All data analyzed in this report were captured between January 1, 2003, and June 30, 2003, and are compared with data captured between January 1, 2002, and June 30, 2002, unless noted otherwise.

GENERAL TRENDS
Overall Volume

For the six-month period ending June 30, 2003, Symantec documented 1,432 new vulnerabilities, a 12% increase over the number found in the same period the previous year **(Figure 1)**.

The rate of discovery for new vulnerabilities continues to escalate—albeit at a slower rate than in the previous six months. In the February 2003 *Threat Report,* Symantec observed an 82% increase in new vulnerability discoveries for 2002 compared with 2001. The high rate of growth resulted from a convergence of several trends, such as increased media exposure for vulnerabilities, gathering momentum of the responsible-disclosure,[2] and a dramatic rise in Web vulnerabilities. Symantec sees these trends continuing to drive new discoveries in 2003, but their influence is simply less pronounced than during the same time period in 2002. As of today potential attackers are aware of 8,000 vulnerabilities affecting over 4,000 different technology products. This is why it is critical for enterprises that need to ensure the continuity of their operations to be protected are protected.

SEVERITY OF VULNERABILITIES

For the first six months of 2003, moderate- and high-severity vulnerabilities were the most common. The number of new moderately severe vulnerabilities increased 21% and high severity vulnerabilities increased 6% as compared with the same period in 2002, while the volume of low-severity vulnerabilities actually decreased by 11% **(Figure 2)**.

This trend was first identified in the February 2003 *Threat Report* and is driven by the following:

Remote Exploitability—80% of vulnerabilities discovered in the first half of 2003 can be exploited remotely. Since global access is a mandate in today's business environment, companies have created numerous Internet-enabled applications. Because of the severity of attacks that can occur across the network, Symantec rates the severity of remotely exploitable vulnerabilities between moderate and high.

Figure 1: Vulnerability Volume by Six-Month Period
(6 Months Ending June 2002 vs. 6 Months Ending June 2003)

Six-Month Period   *Source: Symantec Corporation*

---
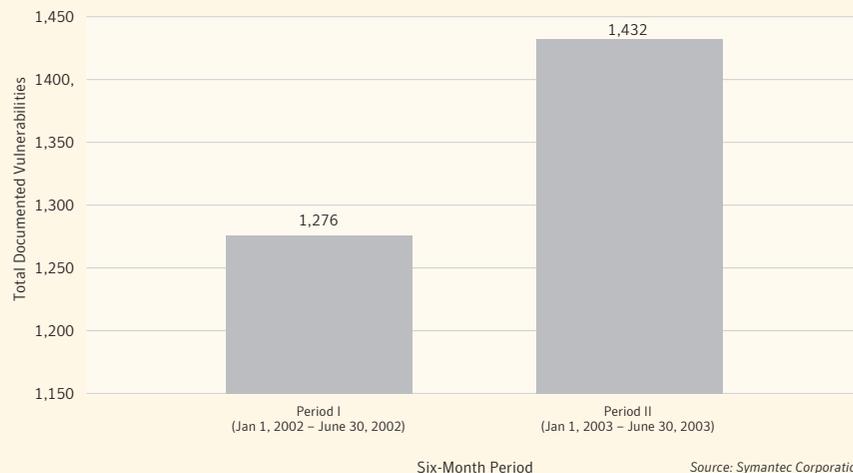
[2] Responsible-Disclosure refers to a policy of working with the vendor to ensure that patches are made available before or at the same time as the announcement of the vulnerability. Adherents to responsible disclosure do not typically publish any exploit code.

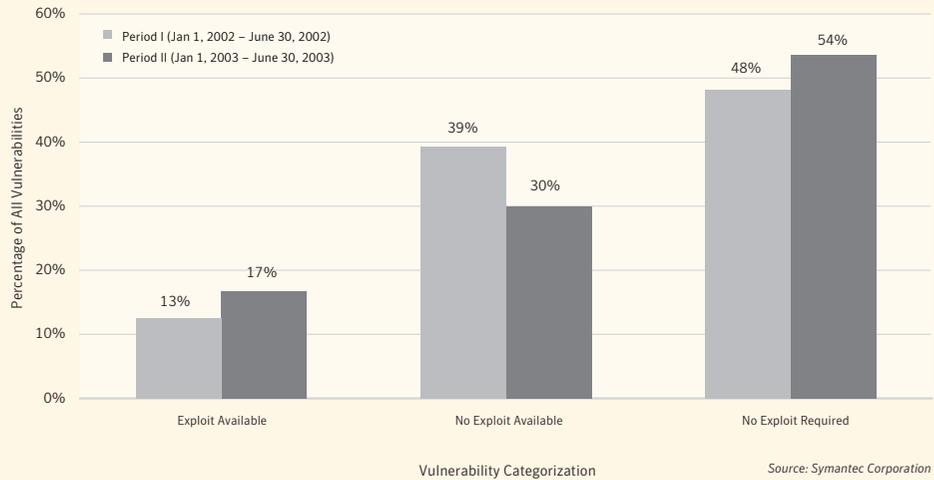**Figure 2: Percent Increase/Decrease in New Vulnerabilities by Severity**

Source: Symantec Corporation
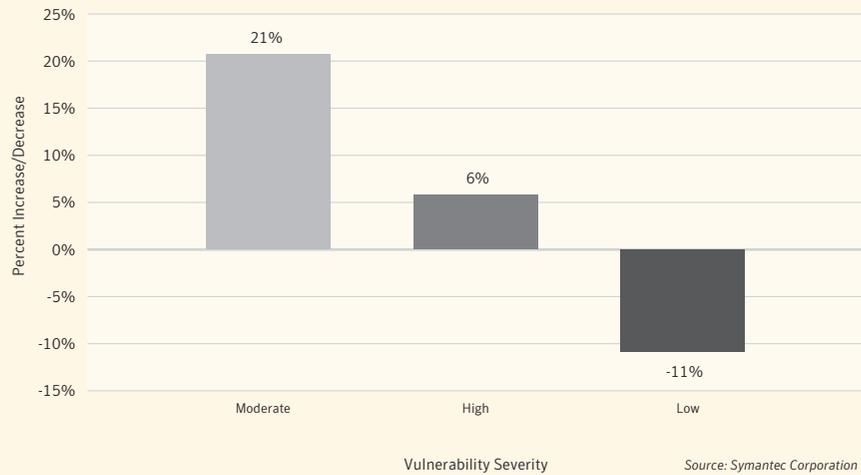
Researcher Interest—The relative "news-worthiness" of severe vulnerabilities contributes to the rise in severity. Symantec is constantly monitoring the work of vulnerability researchers, who appear to have shown a decrease in interest in vulnerabilities that pose little threat. The seeming decline in low-severity vulnerabilities may simply reflect the reluctance of researchers to announce their existence when they are found.

EASE OF EXPLOITATION

Vulnerabilities found during the first half of 2003 tended to be easier to exploit than those discovered during the first half of 2002.

Symantec documented a rise in vulnerabilities that do not require an exploit, as well as a rise in those for which exploits are publicly available **(Figure 3)**.

Figure 3: Percent of Vulnerabilities by Ease of Exploitation
(6 Months Ending June 2002 vs. 6 Months Ending June 2003)

Legend:
- Period I (Jan 1, 2002 – June 30, 2002)
- Period II (Jan 1, 2003 – June 30, 2003)

Y-axis: Percentage of All Vulnerabilities (0% to 60%)

Exploit Available: 13%, 17%
No Exploit Available: 39%, 30%
No Exploit Required: 48%, 54%

X-axis: Vulnerability Categorization

Source: Symantec Corporation

The increased ease of exploitation contrasts with observations made during the second half of 2002, when Symantec reported vulnerabilities were harder to exploit. Symantec's analysis determined this change might result in part from the following factors:

Globalization of Vulnerability Research—Over the past six months, Symantec has noted a dramatic rise in the number of exploits discovered by researchers from outside North America and Western Europe. Unfortunately, many independent vulnerability researchers (particularly those from Asia, Latin America, and Eastern Europe), because of language constraints or an unfamiliarity with concepts of responsible disclosure, do not communicate security issues to vendors. Symantec recognizes that the globalization of vulnerability research will potentially increase the development of exploit code.

Continued Increase of Web Application Vulnerabilities—As mentioned earlier, Symantec has documented a 12% increase since 2002 in the discovery of vulnerabilities in Web applications, (678 in the first half of 2003). These are particularly dangerous because attackers need only modest skills, as these vulnerabilities are derived from input validation or configuration errors. Since no exploit is often required, attacks become easier and the danger to the enterprise rises.

Vulnerability Preferences

Symantec analyzed attacker vulnerability preferences for the first time in this issue of the *Threat Report,* by evaluating the characteristics of vulnerabilities that were targeted by new attacks found in the first half of 2003. Understanding the preferences of adversaries is important to assessing the relative risks created by different types of vulnerabilities. Security administrators must ask themselves several questions in order to prioritize vulnerabilities and their organization's risk. For instance, which systems are at the most risk based on the exploits in existence? Are attackers targeting new or old vulnerabilities? Are they targeting high- or low-severity ones? Or are they selecting vulnerabilities at random? Symantec has answered these questions based on the analysis of data generated by our vulnerability database.

Analysis shows that attackers focused on the newer vulnerabilities during the first half of 2003. Of all new attacks observed, 64% targeted vulnerabilities less than one year old **(Figure 4)**.

Attackers have also been focusing on vulnerabilities with a higher severity rating that were relatively easy to exploit—an explosive combination designed to have high impact and damage potential. Of all new attacks documented in the first half of 2003, 66% targeted highly severe vulnerabilities and 79% focused on those that either had an exploit or did not require one.

Attackers who are sophisticated enough to develop new attacks are attracted by the newest, most exciting vulnerabilities. Security teams must therefore be proactive in taking steps to patch new vulnerabilities, and must set priorities to address existing vulnerabilities based on severity.

Figure 4: Vulnerabilities Targeted for New Attacks by Vulnerabilty Age
(January 1, 2003 – June 30, 2003)

Percentage of New Attack Targets

Vulnerabilty Age Range

Source: Symantec Corporation
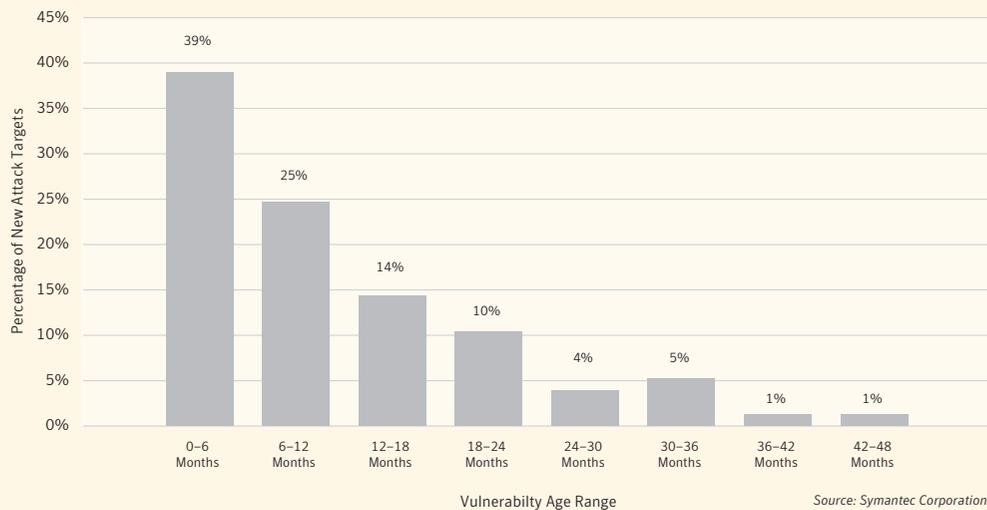
TRENDS IN VULNERABILITIES
Integer-Error Vulnerabilities

Apache, Sendmail, and OpenSSH have all been affected by vulnerabilities introduced by errors in the handling of integers. In the first half of 2003, Symantec analysts saw an increase in the number of vulnerabilities due to integer errors, a relatively simple type of programming flaw often made by developers. Symantec documented 19 integer-error vulnerabilities during the first half of 2003, as compared to only 3 in the first half of 2002. Since vulnerabilities based on integer errors have only recently emerged, many programmers may not check their code for this type of error before releasing product. As a result, many applications, ranging from manufacturing to games, may silently house such vulnerabilities without the knowledge of their developers.

The sharp rise in integer-error vulnerabilities poses a significant future threat to medium and large organizations due to the prevalence of such errors and their high severity ratings.

Symantec's analysis of integer-error vulnerabilities shows that unforeseen behavior can be introduced in affected programs. For example, an integer overflow may result in an incorrect calculation that could lead to a buffer overflow. Errors in the comparison of integers can result in the bypass of crucial security checks. Many such errors have created disastrous consequences within organizations.

TIMING ANALYSIS AND SIDE-CHANNEL VULNERABILITIES

Symantec analysts saw timing-analysis vulnerabilities, a relatively rare type, suddenly increase in number during the first half of 2003. The sudden appearance of these vulnerabilities coincided with the release of two papers discussing timing-analysis attacks against implementations of SSL/TLS. Although these weaknesses are still uncommon (Symantec documented only four in the first half of 2003), their high severity makes them a noteworthy future concern.

Timing analysis is a side-channel attack that typically targets a weakness in the implementation of a system rather than its design. Errors in system implementations may cause a leak of important information in the timing of specific events. By measuring the length of time that a system takes to perform certain functions, attackers can sometimes obtain or infer valuable information. For example, timing-analysis attacks have allowed attackers to guess valid usernames or determine the existence of confidential files. To a sophisticated attacker, timing-analysis and side-channel vulnerabilities offer powerful new methods to penetrate highly secure systems.

Microsoft Internet Explorer Vulnerabilities

During the first half of 2003, Symantec documented more than a dozen new vulnerabilities affecting various versions of Microsoft® Internet Explorer. More important than the sheer volume of these vulnerabilities is their potential impact. Several enable attackers to compromise client systems through Web pages containing embedded malicious code. Others can enable the easy (and virtually undetectable) installation of spyware.

The high market penetration of Microsoft Internet Explorer, combined with the emergence of many high-severity vulnerabilities, renders it increasingly prone to attack. Vulnerable Internet Explorer applications could easily become effective tools to launch distributed denial-of-service attacks, install new Trojan horse and spyware applications, and disperse blended threats.

Microsoft IIS Vulnerabilities

Microsoft IIS is one of the most widely deployed Web servers throughout the world. Symantec has documented several high-severity vulnerabilities during the first half of 2003 (in addition to many found in the second half of 2002). At least a few of these have characteristics that render them very attractive targets for future blended threats. Given Microsoft IIS's susceptibility to past blended threats such as Code Red and Nimda, Symantec believes that this application may again be the target of a highly destructive malicious code.

Glossary

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 due to 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 check-ing 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 over-writing 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.

Class A Network

A Class A network is the largest IP address class of the three public use "classes" (Class A, Class B, and Class C) in the IP address space. There are 127 Class A networks with each supporting around 16 million hosts or individual IP addresses. Classless Inter-Domain Routing (CIDR) is an updated address-ing scheme that provides more effective use of IP addresses than the old Class A, B, and C scheme. You will now see Class A networks called a /8 (slash eight) network, so called for the 8-bit network prefix assigned under CIDR.

Exploit

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

Infection Vector

The method in which malicious code gains access to a computer system. The most common infection vector today is email. Other vectors of infection include floppy disks, vulnerabilities in software, peer-to-peer software, and instant messaging.

Integer Error

Integer errors are a type of programmatic flaw caused by a failure to properly handle variables of the integer data type. Integer errors can result in unexpected/unanticipated behavior in affected programs and can sometimes allow attackers to hijack the execution flow of the affected program.

Malicious Payload

Typically referred to as "Payload" because "mali-cious" is a major part of the definition. 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 for email addresses in 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, e.g., 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.

Remotely Exploitable

Remotely exploitable vulnerabilities are those which 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.

Side-Channel Attack

An attack that typically targets a weakness in the implementation of a system rather than its design. Errors in implementations of systems can cause a leak of important information in the timing of specific events. By observing the amounts of time that a system takes to perform certain behavior, attackers can sometimes obtain or infer valuable information. For example, knowledge of crucial timing information can possibly allow an attacker to compromise SSL/TLS sessions. Other reported timing-analysis attacks allowed attackers to guess valid usernames or determine the existence of confidential files. To a sophisticated attacker, timing-analysis and side-channel vulnerabilities offer powerful new methods to penetrate highly secure systems.

Virus

A self-replicating computer program.

Vulnerability

A security vulnerability is a coding error within a software system that can cause it to function outside of its documented design, violating its documented security policy. 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 copying itself 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 36 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 36 countries. For specific country offices and contact numbers please visit our Web site.

Symantec Internet Security Threat Report

Trends for January 1, 2003 – June 30, 2003

EXECUTIVE EDITOR
Linda McCarthy
Symantec Office of the CTO

RESEARCH FELLOW
Sarah Gordon
Symantec Security Response

PRINCIPAL TREND ANALYST
Mike Prosser
Symantec Security Services

SECURITY ARCHITECT
Peter Szor
Symantec Security Response

SENIOR DIRECTOR, DEVELOPMENT
Vincent Weafer
Symantec Security Response

Contents

Report Highlights

Overall threats remained significant during the first half of 2003. Companies without adequate controls risk having their networks and applications compromised. This report discusses in depth some specific findings that support this observation.[1]

HIGHLIGHTS: MALICIOUS CODE TRENDS

- Blended threats increased 20%
- 60% of malicious code submissions were blended threats
- Speed of propagation has increased
- Linux systems may be targeted for future attacks
- Increased theft of confidential data
- Windows 32—increased sophistication of malicious code
- New infection vectors:
  – Instant messaging
  – Peer-to-peer services—19 new attacks identified (up from four in 2002)

Emergence of Malicious Code

OVERVIEW

The increasing prevalence of blended threats remains the most pressing issue for companies that lack effective intrusion protection and patch management policies. Blended threats use combinations of malicious code such as viruses, worms, and Trojan horses to exploit known vulnerabilities in application or system code. Other high-ranking concerns are the rapid increase in the number of Windows 32 (Win32) threats, the growing number of threats targeting peer-to-peer services and instant messaging clients, and the propagation speed of new worms.

These combined trends suggest that malicious code is becoming an increasingly significant danger to organizations and individuals. Managers and home users alike must now implement security practices for maintaining antivirus and patch management solutions. Only by recognizing and patching system vulnerabilities can managers and users truly defend against the next major outbreak of a blended threat.

This section of the *Internet Security Threat Report* analyzes current and future threats posed by malicious code and offers a comprehensive picture of the current and future threat environment. Observations are based on trend data, qualitative intelligence gathering, behavioral analysis, and adversary profiling.

Many trends seen in the first half of 2003, such as the increasing danger of blended threats, build on observations discussed in the *February 2003 Threat Report*. Such trends are based on statistical analysis from the Symantec AntiVirus™ Research Automation (SARA) system. For a detailed description of research methods, see *Threat Report Methodology* document.

---

[1] All data analyzed in this report were captured between January 1, 2003, and June 30, 2003, and are compared with data captured between January 1, 2002, and June 30, 2002, unless noted otherwise.

This section highlights:

- Blended threats
- Speed of propagation
- Windows 32 viruses and worms
- Theft of confidential information
- Mass mailers with internal email engines
- New infection vectors

BLENDED THREATS

Symantec has determined that blended threats are among the most significant trends to watch and guard against this year. In the first six months of 2003 blended threats increased nearly 20% over the previous six-month period. One blended threat alone, SQL Slammer, impacted systems worldwide in less than an hour. Blended threats use combinations of malicious code to begin, transmit, and spread attacks. By using multiple types and techniques, blended threats can spread to large numbers of hosts, causing rapid and widespread damage.

Blended threats impact personal productivity and a company's ability to do business. The multiple propagation mechanisms of blended threats allow them not only to compromise a company's security, but also to overload system resources and saturate network bandwidth. Examples of blended threats include Klez, Bugbear, Slammer, SoBig, SQL Spida, and Code Red.

Symantec's assessment of the growing danger of blended threats in the February 2003 issue of the *Threat Report* was based on their predominance in malicious code submission data, as well as on a review of the actual damage caused by several high-profile threats. Unfortunately, in the first half of 2003, the danger from blended threats increased. Analysis shows that 31 of the top 50 submissions were classed as blended threats, up from 26 in the prior six months—an increase of nearly 20%.[2] One of the most rapidly spreading blended threats on record, SQL Slammer, hit the Internet dramatically

Figure 1: Blended Threats and Targeted Vulnerabilities

Blended Threat	Bugtraq ID of Targeted Vulnerability	Vulnerability Name	CVE Reference Number	Date of Vulnerability Discovery	Date of Blended Threat Outbreak	Time Delay from Discovery to Outbreak
W32.Klez	2524	Microsoft IE MIME Header Attachment Execution Vulnerability	CVE-2001-0154	29 Mar 2001	25 Oct 2001	210 days
W32.Sobig	2524	Microsoft IE MIME Header Attachment Execution Vulnerability	CVE2001-0154	29 Mar 2001	9 Jan 2003	651 days
W32.Bugbear	2524	Microsoft IE MIME Header Attachment Execution Vulnerability	CVE-2001-0154	29 Mar 2001	30 Sep 2002	550 days
W32.Yaha	2524	Microsoft IE MIME Header Attachment Execution Vulnerability	CVE-2001-0154	29 Mar 2001	15 Feb 2002	349 days
W32.Nimda	2524	Microsoft IE MIME Header Attachment Execution Vulnerability	CVE-2001-0154	29 Mar 2001	18 Sep 2001	538 days
	2708	Microsoft IIS/PWS Escaped Characters Decoding Command Execution Vulnerability	CVE-2001-0333	15 May 2001	18 Sep 2001	126 days
	1806	Microsoft IIS and PWS Extended Unicode Directory Traversal Vulnerability	CVE-2000-0884	17 Oct 2000	18 Sep 2001	336 days
W32.Opaserv	1780	Microsoft Windows 9x / Me Share Level Password Bypass Vulnerability	CVE-2000-0979	10 Oct 2000	30 Sep 2002	710 days
W32.Lirva	2524	Microsoft IE MIME Header Attachment Execution Vulnerability	CVE-2001-0154	29 Mar 2001	7 Jan 2003	649 days
W32.SQLExp.Worm	5311	Microsoft SQL Server Resolution Service buffer overflows allow arbitrary code execution	CAN-2002-0649	25 Jul 2002	24 Jan 2003	208 days
CodeRed.Worm	2880	Microsoft Index Server and Indexing Service ISAPI Extension Buffer Overflow Vulnerability	CVE-2001-0500	18 Jun 2001	16 Jul 2001	28 days

Source: Symantec Corporation

[2] Data were compared with the last half of 2002 (rather than the first half) because comparative data was not available for the first half of 2002.

on January 25, 2003. Slammer was the fastest worm in history. Slammer's speed of propagation, combined with poor configuration management on many corporate sites, enabled it to dramatically interrupt performance across the Internet.

Blended threats present three reasons for heightened concern. First, there are more of them. Second, the most effective blended threats spread by exploiting numerous application and system vulnerabilities. Third, even when a vulnerability is found, companies often fail to patch their systems promptly which points to a lack of established patch management policies by companies. Evidence of this failure is the length of time between the discovery of vulnerabilities and their exploitation by a blended threat. **Figure 2** shows this trend by detailing the top blended threats reported during the past 12 months. Recently, vulnerabilities that have been well known for several months have had numerous versions of attack code written against them. For example, Klez, SoBig, Bugbear, Yaha, and Nimda repeatedly exploit the *same* vulnerability.

While blended threats increase, corporate patch management policies (a key defense against blended threats) continue to lag. To defend against future blended threats, companies must identify and patch

vulnerabilities on their networks quickly. The cost of doing so will be far less than the lost productivity experienced later.
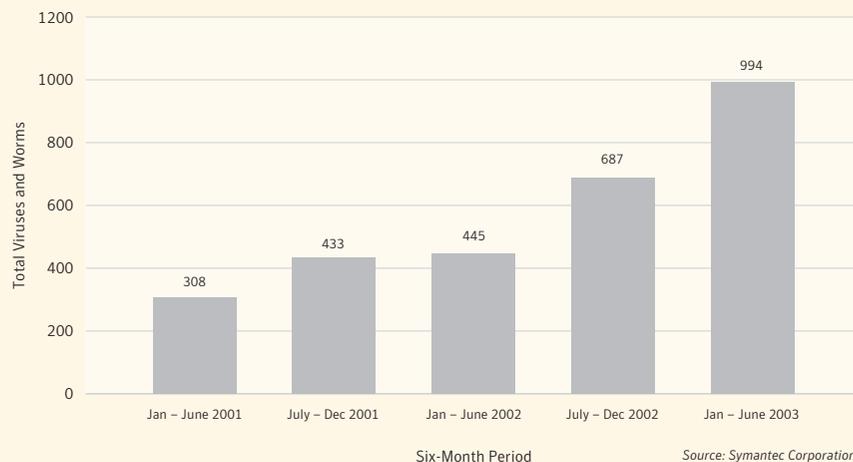
Win32 Viruses and Worms

As Microsoft Windows expands its installed base, Win32 threats have increased correspondingly. These threats are executable files that operate by using the Win32 application program interface (API), and work on at least one Win32 platform.

Over the past six months, Symantec has documented more than 994 new Win32 viruses and worms, more than double the 445 documented in the first half of 2002. The total number of Win32 variants now approaches 4,000. **Figure 2** shows the number of new Win32 viruses and worms by six-month period from January 1, 2001, through June 30, 2003.

Over a short period, Win32 attacks are more common than script and macro-based threats. In addition to their rising volume, the complexity of the malicious code in Win32 attacks is increasing. For example, several recent attacks exploit complex Win32 buffer-overflow vulnerabilities, while others demonstrate advanced evasion and sophisticated anti-detection techniques. Several Win32 attacks leverage multiple exploits to maximize the potential for infection.

Figure 2: New Documented Win32 Viruses and Worms
(January 1, 2001 – June 30, 2003)

Source: Symantec Corporation

[3] Zoo-based threats are those that exist only in virus and antivirus labs, not in the wild. Most zoo threats never get released into the wild and, as a result, rarely threaten users.

Even with the growing number and complexity of Win32 viruses and worms, most market-leading, antivirus products like Symantec's maintain robust detection. When these solutions are deployed proactively and are well maintained on all platforms and across all tiers of a corporate network, companies are protected from most threats.

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. However, after this outbreak, there were few successful malicious-code attacks on Linux. This period of inactivity suddenly changed with the emergence of the Linux.Slapper worm in September 2002. The infection vector of Slapper and its variants was based on a remote buffer overflow vulnerability in the OpenSSL implementation of the SSL protocol, and the worm targeted Apache Web servers on various versions of the Linux operating environment.

Although Symantec has not seen a major outbreak of a Linux worm since Slapper, Symantec analysts remain concerned about several highly sophisticated zoo-based Linux viruses and worms that have been developed recently.[3] Such threats are cause for concern, as they show that malicious-code writers are developing a greater sophistication in programming and more familiarity with the Linux operating system and its applications.

Symantec will monitor the evolution of Linux attacks during the next 12 months. Such threats are worrisome as Linux-based solutions become more popular among consumers.[4] Unlike people already familiar with various flavors of the Unix operating system, new Linux users may be unaware of appropriate security practices.

Lifecycle of a Worm and Speed of Propagation

As soon as a computer worm, such as SQL Slammer, is released into the wild, it spreads by infecting new systems. The worm may attack computers in specific locations (for instance, designated netblocks, domains, or computers resid-

ing in certain countries), or it may indiscriminately attack the entire computing population at random.

If successful, the worm then uses the infected system as a platform from which to identify potential new victims. Each successful penetration follows this pattern, and the number of infected systems grows until either all potential victims are infected or countermeasures such as antivirus software begin to halt the spread. Over time, as protection becomes more effective and ubiquitous, the rate of propagation slows, new infections decrease, and existing infections are remedied. This pattern of release, growth, and gradual decline is the lifecycle of a worm.

A critical factor shaping a worm's lifecycle is the speed at which it propagates. Propagation speed is governed by a variety of influences, such as the writer's algorithm, the infection vectors used, and the available number of targeted systems. As worm writers improve their techniques, the speed of propagation can rise dramatically. Greater homogeneity of Internet-connected systems, increased bandwidth capacity, and computing speed of target systems have all assisted in improving speed of propagation.

The recent SQL Slammer worm used a propagation strategy based on the exploitation of a well-known buffer-overflow vulnerability in Microsoft's popular SQL Server. In part the speed of propagation was so high because the worm spread via UDP, a connectionless protocol. By relying on UDP, the worm used little bandwidth and few system resources, enabling an extremely short time delay between new generations of the worm.

In addition, the buffer-overflow vulnerability that Slammer exploited was fairly short, so that Slammer could probe many machines without consuming much bandwidth. Fortunately, despite the speed of propagation, many companies were able to stop Slammer at the firewall by closing a single port. Systems administrators could thus contain Slammer relatively quickly. Companies hit by Slammer benefited by the fact the worm was designed only to propagate and be a nuisance. It

---

did not carry a malicious payload. If this had been the case, damage from the outbreak might have been catastrophic.

Symantec expects to see greater worm propagation resulting in overloads to network hardware, crippling network traffic and seriously preventing both individuals and businesses from using the Internet.

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. However, virus protection has become more prevalent.

NEW INFECTION VECTORS
Instant Messaging and Peer-to-Peer Applications

As both legitimate and unapproved use of instant messaging (IM) clients and peer-to-peer (P2P) networking increases, new worms and viruses use these mechanisms to spread. A review of the top 50 virus and worms over the past six months shows 19 malicious code submissions used P2P and IM applications. This is an increase of almost 400% in only one year.

The two main reasons for this dramatic increase are that these applications have become more popular among corporate and home users and these services are relatively insecure. Unlike other avenues for propagation such as email, IM and P2P often have little to no security in place. For example, many IM products transmit unencrypted data outside of the firewall, making it easy to intercept this traffic on a network. The minimal security associated with P2P and IM invites malicious code propagation.

Fortunately, organizations can take steps to protect IM and P2P users. The simplest is for organizations to prohibit employees from using insecure versions of these services. Companies should acquire IM applications that are specifically developed for commercial use and include security. Finally, policies must be defined and enforced regarding restrictions on usage.[5]

Mass Mailers with Internal Email Engines

Mass-mailing viruses and worms spread by harvesting and using email addresses from infected systems. The two basic types of mass-mailing viruses are 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 suspicious mail would appear in their email inbox. They could then take countermeasures to limit its spread.

To bypass this limitation, virus writers create their own email engines in an attempt to foster propagation that is both efficient and harder to detect. The number of viruses and worms with their own email engines grew by more than 100% in the first half of this year, increasing from 8 to 19 in the six months ending June 30, 2003.

Because emails generated by the self-contained engine of malicious code do not interact with the user's email system, few users are able to detect the code. Since the threats spoof the "From:" address on emails, victims cannot easily identify the true originator of the infected email. This makes tracking the sources of infection difficult and enables the virus to survive longer. Fortunately, most market-leading antivirus products with effective heuristics-based detection can resist these types of threats.

THEFT OF CONFIDENTIAL DATA

The best example of theft of confidential data is the release of a new Bugbear variant, Bugbear.B, discovered in early June 2003. Once systems were infected, Bugbear.B began extracting confidential data, such as lists of file names, processes, user names, and other critical system information. Bugbear.B also delivered logged keystrokes to a third party, potentially compromising important information such as passwords and decryption keys. The discovery of this new variant of Bugbear raises serious concerns, since it appears that the creator specifically targeted banking institutions.

[5] For a more complete description of the security risks of using instant messaging and guidelines for securing this technology, see http://securityresponse.symantec.com/avcenter/reference/secure.instant.messaging.pdf

Although the creator's motivation is unknown, he or she may have been specifically interested in obtaining either financial data or information, such as client usernames and passwords, that would allow future access to customer accounts.

Confidential data attacks increasingly use backdoors. Submissions of malicious code with backdoors has risen nearly 50%, increasing from 11 submissions to 17 for the first half of 2003. By granting remote access to compromised systems, backdoors allow the unauthorized export of any type of data that those systems contain. For example, keystroke loggers can be installed and the keystrokes of infected systems can be sent to the attacker in an easy-to-read file. Entire sessions can be logged, and passwords for systems or applications can be extracted. Attackers then use compromised systems as launching points for future attacks.

Finally, the confidentiality of data is increasingly threatened by malicious code that tracks Internet browser usage. Such programs, commonly known as spyware, are placed surreptitiously on a user's computer. As the data-export functions of spyware typically operate using Web traffic (over Port 80), firewalls usually fail to catch the intrusion. Spyware applications can track and deliver to its creator the critical browsing habits and other behavioral information of infected users.

In response to the potential danger of compromised confidential data, corporate and home users must develop stronger policies and procedures to preserve confidentiality. Browser and firewall policies need to be established and implemented to mitigate the effects of spyware applications. Companies should install software that automatically deletes unwanted cookies, and implement security controls that make it more difficult for malicious code to compromise confidential data.

BLASTER

As this report goes to press, the Win32.Blaster, W32.SoBig.F, @mm, and Win32.Welchia worms are rapidly spreading worldwide. While Blaster appeared too late for analysis of its impact to be included in this report, the message is nevertheless clear: It is vital to ensure that all machines, both personal and corporate, are patched up to date—especially in areas related to security. Symantec's current data indicates that the threat posed by malicious code continues to grow; this is especially true in the areas of blended threats and Win32 threats.

Other areas, which Symantec continues to carefully monitor, include the rise in P2P threats, mass mailers, and the theft or export of confidential information. Despite the risks, the maintenance of a viable defensive stance is achievable: A good combination of procedural and technical prophylactics is able to stave off and even reverse the rising tide of malicious code. Good, correctly maintained antivirus software and solid firewall/IDS solutions combined with an aggressive yet calculated response to security-related patches greatly mitigate the risks. Furthermore, human factors, such as education and awareness, backed up by policy and procedure, can go a long way to minimize losses.

Appendix—Closing Comments: Blaster, SoBig, and Welchia

As this report goes to press, three new threats—W32.Blaster.worm, W32.SoBig.F@mm, and W32.Welchia.worm were responsible for the swift and large-scale compromise of academic, corporate, and home user systems worldwide.

HISTORY

Blaster exploited a single vulnerability: the Microsoft Windows DCOM RPC Interface Overrun. Microsoft announced the vulnerability on July 16, 2003. In less than a month, Blaster appeared. In some cases, automated scripts appear to have been used in deployment of the exploit code, dramatically increasing the number of hosts that could be attacked in a given time period. Reports of infection of over a 1,000 hosts per network were not uncommon, and for a short time, Symantec data showed as many as 2,500 computers per hour becoming infected.

Academic networks were particularly hard hit by the worm. Infected users were advised to patch their systems and utilize firewall rules to stop the worm from spreading further. However, their efforts were complicated by the fact that, in addition to exploiting the vulnerability, Blaster also contained code written to keep infected users from obtaining the necessary patch. The worm attempted to perform a denial-of-service attack upon the Microsoft Windows update site. As of August 15, 2003, Microsoft removed the DNS record for the specific update site used by the worm.

Shortly thereafter, SoBig appeared, using its own SMTP engine to propagate via email. Like previous worms, it made use of a rudimentary social engineering technique: choosing the "to" and "from" addresses from an infected user's address book. Coupled with realistic "Subject:" lines, SoBig was able to exploit users' trust and thus gain a global foothold extremely quickly. However, in addition to utilizing these basic social engineering techniques, SoBig was programmed to act as both a command and control center on infected machines. Carrying a payload that would, when successfully deployed, download an update twice weekly, SoBig was ideally positioned to obtain further instructions from the remote locations.

Finally, Welchia appeared. Welchia displayed yet even more complexity. It exploited two vulnerabilities as it attempted to clean Blaster.A infected computers.

CONCLUSION

Whereas previous threats might not appear in the wild until several months to a year or more after the disclosure of a vulnerability, Blaster and Welchia each appeared within approximately one month of the vulnerability disclosure. Additionally, attacks are occurring with greater frequency and increasingly larger target space. To ensure that systems are continuously protected, it is imperative that all machines—corporate, academic, home user—be patched up to date.

The threat posed by malicious code is increasing not only in rapidity of infection, but in complexity as well. This complexity not only mandates a strong corporate security policy but 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 provide the comprehensive layered approach needed to reduce the risk from blended threats such as Blaster, SoBig, and Welchia.

Glossary

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 due to 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.

Class A Network

A Class A network is the largest IP address class of the three public use "classes" (Class A, Class B, and Class C) in the IP address space. There are 127 Class A networks with each supporting around 16 million hosts or individual IP addresses. Classless Inter-Domain Routing (CIDR) is an updated addressing scheme that provides more effective use of IP addresses than the old Class A, B, and C scheme. You will now see Class A networks called a /8 (slash eight) network, so called for the 8-bit network prefix assigned under CIDR.

Exploit

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

Infection Vector

The method in which malicious code gains access to a computer system. The most common infection vector today is email. Other vectors of infection include floppy disks, vulnerabilities in software, peer-to-peer software, and instant messaging.

Integer Error

Integer errors are a type of programmatic flaw caused by a failure to properly handle variables of the integer data type. Integer errors can result in unexpected/unanticipated behavior in affected programs and can sometimes allow attackers to hijack the execution flow of the affected program.

Malicious Payload

Typically referred to as "Payload" because "malicious" is a major part of the definition. 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 for email addresses in 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, e.g., 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.

Remotely Exploitable

Remotely exploitable vulnerabilities are those which 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.

Side-Channel Attack

An attack that typically targets a weakness in the implementation of a system rather than its design. Errors in implementations of systems can cause a leak of important information in the timing of specific events. By observing the amounts of time that a system takes to perform certain behavior, attackers can sometimes obtain or infer valuable information. For example, knowledge of crucial timing information can possibly allow an attacker to compromise SSL/TLS sessions. Other reported timing-analysis attacks allowed attackers to guess valid usernames or determine the existence of confidential files. To a sophisticated attacker, timing-analysis and side-channel vulnerabilities offer powerful new methods to penetrate highly secure systems.

Virus

A self-replicating computer program.

Vulnerability

A security vulnerability is a coding error within a software system that can cause it to function outside of its documented design, violating its documented security policy. 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 copying itself 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 36 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 36 countries. For specific country
offices and contact numbers please
visit our Web site.

Symantec Internet Security Threat Report

Trends January 1, 2003 – June 30, 2003

EXECUTIVE EDITOR
Linda McCarthy
Symantec Office of the CTO

MANAGER, DEVELOPMENT
David Ahmad
Symantec Security Response

SENIOR THREAT ANALYST
Cori Lynn Arnold
*Symantec Managed Security
Services*

**SENIOR MANAGER, ANALYSIS
OPERATIONS**
Brian Dunphy
*Symantec Managed Security
Services*

**SENIOR MANAGER,
DEVELOPMENT**
Oliver Friedrichs
Symantec Security Response

RESEARCH FELLOW
Sarah Gordon
Symantec Security Response

SECURITY ARCHITECT
Peter Szor
Symantec Security Response

PRINCIPAL TREND ANALYST
Mike Prosser
Symantec Security Services

**SENIOR DIRECTOR,
DEVELOPMENT**
Vincent Weafer
Symantec Security Response

Contents

Appendix A—Network-Based Attack Methodology

OVERVIEW

Attack trends in this report are based on the analysis from Symantec DeepSight Threat Management Service (TMS) and Symantec Managed Security Service (MSS). TMS and MSS have created a common language to name specific types of attacks, enabling analysts to combine and analyze attacks in one database, as well as separately.

Symantec combines the TMS and MSS data sources for analysis when appropriate—that is, when they represent similar findings and trends. Symantec analysts use the data source that is appropriate;

with consideration to the level of review of the data and the demographic makeup of the sources (both in terms of vertical and geographic distribution).

By combining TMS and MSS data, Symantec doubled the size of previous sample sets used in this report. The table below provides high-level details of the methods used by each service.

The remainder of this section explains the following attributes of the sample set and research inquiries.

Data Source	Data Collection Methodology	Percent of Companies in Sample Set
Threat Management System	The DeepSight Threat Management System collects IDS alerts and firewall logs on a voluntary basis from more than 20,000 security devices deployed in more than 180 countries. For this report, a sample of data from more than 1,000 devices was studied.	59%
Managed Security Service	Symantec's Managed Security Service provides real-time monitoring and analysis of cyber attack activity launched against more than 400 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 Managed Security Service customers.	41%

COMPANY DEMOGRAPHICS

In addition to the sheer size of the sample set, Symantec maintains a diverse mix of companies. Specifically, the sample set includes a broad array of organizations as measured by criteria such as industry, ownership type, and company size. A selection of these company characteristics is outlined in greater detail below.

INDUSTRY

The industry breakdown for TMS and MSS is listed by percentage. Industry groups are based on the review of a variety of public and private references, as well as direct client interactions. It is important to note that several classifications were altered since the February 2003 issue of the report. These changes were necessary to further refine the standardized classification methodology that is now employed throughout Symantec.

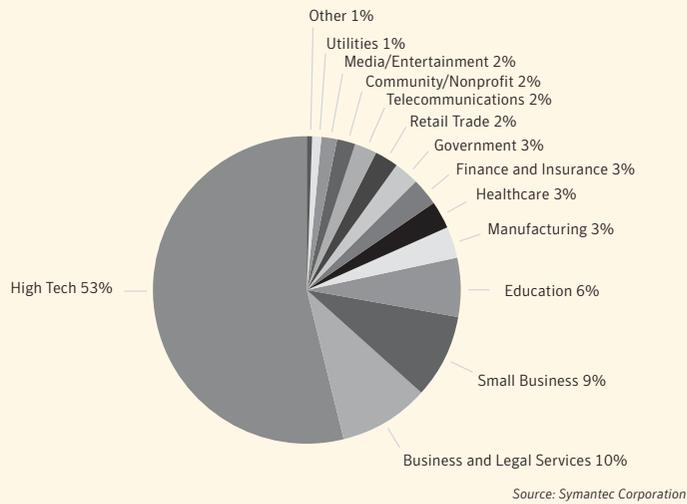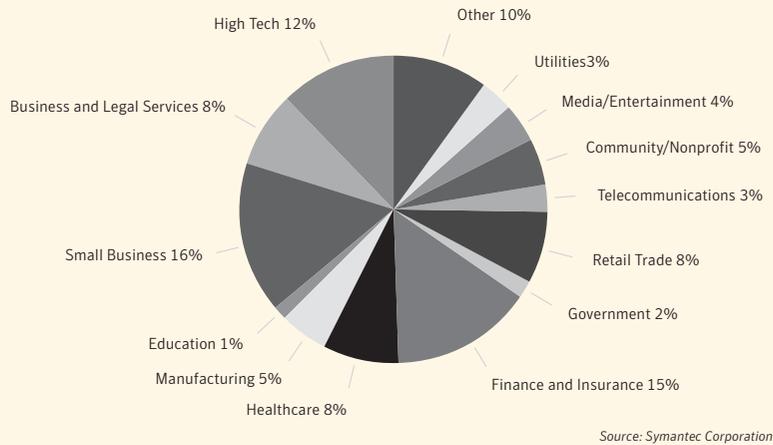**Figure 1: Breakdown of Companies by Industry—TMS Data**

Other 1%
Utilities 1%
Media/Entertainment 2%
Community/Nonprofit 2%
Telecommunications 2%
Retail Trade 2%
Government 3%
Finance and Insurance 3%
Healthcare 3%
Manufacturing 3%
Education 6%
High Tech 53%
Small Business 9%
Business and Legal Services 10%

Source: Symantec Corporation

Figure 2: Breakdown of Companies by Industry—MSS Data

High Tech 12%
Other 10%
Utilities 3%
Media/Entertainment 4%
Business and Legal Services 8%
Community/Nonprofit 5%
Telecommunications 3%
Small Business 16%
Retail Trade 8%
Government 2%
Education 1%
Manufacturing 5%
Finance and Insurance 15%
Healthcare 8%
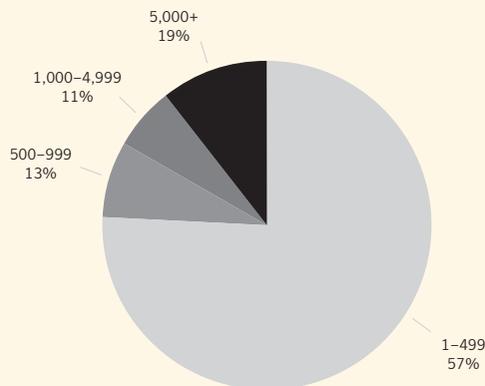
Source: Symantec Corporation

COMPANY SIZE

Symantec used employee count as a proxy to measure company size. This metric was selected as the best proxy for company size because the number of employees typically correlates best to the relative size of a company's network. Employee counts were gathered from public sources, as well as engaging in direct client interaction.

Figure 3: Breakdown of Companies by Size—TMS Data

5,000+
7%

1,000–4,999
6%

500–999
0%

1–499
87%
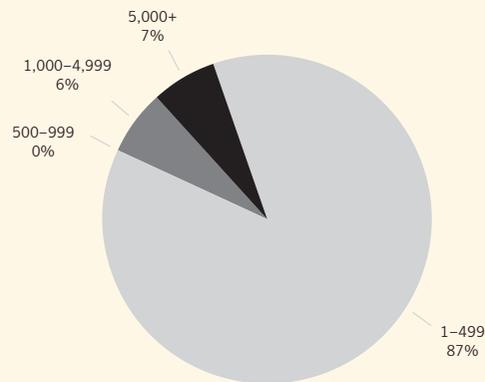
Source: Symantec Corporation

Figure 4: Breakdown of Companies by Size—MSS Data

5,000+
19%

1,000–4,999
11%

500–999
13%

1–499
57%

Source: Symantec Corporation

ATTACK DEFINITIONS

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 uniquely appropriate under a certain set of circumstances. Presented below is a high-level summary of the three metrics that are commonly used in the report.

Attacks—Attacks are individual signs of malicious network activity. Attacks can consist of one or more IDS alerts and/or firewall logs 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.

Events—Security events are logical groupings of multiple attacks. A security event may include a group of similar, but non-threatening, signs of attack activity 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), or a security event may 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."

EXPLANATION OF RESEARCH INQUIRIES

The intent of this subsection is to provide more detail on specific methodologies used to produce the data and statistics used in this report. While most methodologies are adequately explained in the analysis section of the report, the following investigations warranted additional detail.

Event Severity

Event severity is only applicable to data generated by MSS. Every event validated by Symantec security analysts is assigned to one of four severity classifications: informational, warning, critical, and emergency. The primary purpose of this rating system is to prioritize client responses to malicious activity based on the relative level of danger that the event presents to their environment. A determination of severity is based on characteristics of an attack, 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.

Table 2: Event Severity Metrics

Severity Classification	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:* Continuous attacks by a single IP address against the client network. • 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. • 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.

ATTACK SOURCE
Country

Symantec identified the national and regional 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 hosts to source IP addresses. While these databases are generally reliable, there is a small margin of error. Currently, Symantec cross-references source IP addresses of attacks against every country in the world and also analyzes attack trends according to the following regions:

- Africa
- Asia
- Caribbean
- Eastern Europe
- Latin America
- Middle East
- North America
- Oceania
- South America
- Western Europe

It is important to note that while Symantec has a reliable process for identifying the source IP of the host that is directly responsible for launching an attack, it is impossible to verify (from the network) whether the attacker is actually physically present at this location. It is probable that many (if not most) of the apparent sources of attacks are, in fact, systems that were used by attackers as a platform to disguise their identity and true location.

Appendix B—Vulnerability Methodology

OVERVIEW

Symantec threat analysts continually search hundreds of security vendor, industry, underground Web sites, and mailing lists to document new security vulnerabilities.

After the discovery of a new vulnerability, analysts gather all information related to it and issue an alert. Fields within the alert describe characteristics of the vulnerability, such as severity, ease of exploitation, and products affected. Symantec Security Response Service maintains a database that contains detailed reports describing more than 8,000 distinct vulnerabilities.

This section explains several characteristics of vulnerabilities stored in the Symantec database, and clarifies in greater detail several specific queries used in our investigations.

CHARACTERISTICS OF VULNERABILITIES

After discovering a new vulnerability, threat analysts put it into one of 12 possible categories. The Symantec classification is based on Taimur Aslam's white paper, "A Taxonomy of Security Faults in the Unix Operating System." This paper fully describes the meaning of each classification listed here.

- 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. This score is based on the following:

Impact—This measures the relative impact on the affected systems if the vulnerability is exploited. For example, if the vulnerability enables the attacker to gain root access to the system, it is classed as "high impact." A higher impact rating contributes to a higher severity score.

Remote Exploitability—This measure indicates whether or not the vulnerability can be exploited remotely, in other words, using at least one method to exploit the vulnerability from a host, distinct from the vulnerable system, via some type of communication protocol such as TCP/IP, IPX, or dial-up. Remotely exploitable vulnerabilities contribute to a higher severity score.

Ease of Exploitation—How easily can a vulnerability be exploited? Vulnerabilities for which an exploit is widely available or for which an exploit is not required contribute to a higher severity score. We describe this metric at the end of this section.

Authentication Requirements—This metric indicates whether the vulnerability can be exploited only after some sort of credentials are provided to the vulnerable system, or whether one can exploit it without supplying any authentication credentials. Vulnerabilities that require no authentication from the attacker contribute to a higher severity score. After gathering information on these four attributes, analysts use a pre-established algorithm to generate a severity score that ranges from 1 to 10. Vulnerabilities are rated as being of high, moderate, or low severity according to the following scores.

Table 3: Vulnerability Severity Scale

Severity Level	Severity Score Range
High	$X \geqq 7$
Moderate	$4 \leqq X < 7$
Low	$X < 4$

Ease of Exploitation

The vulnerability analyst assigns the ease of exploitation rating after thoroughly researching both the need for and the availability of exploits for the vulnerability. All vulnerabilities are classed into one of three possible categories, listed next.

Exploit Available—Sophisticated exploit code that enables 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.

No Exploit Available—Although would-be attackers must use exploit code to make use of the vulnerability, no such exploit code is publicly available. In this report, the first two types of vulnerability are considered "easily exploitable" because the attacker needs only limited sophistication. The last type of vulnerability is considered "difficult to exploit" because the attacker must develop the exploit code required to make use of the vulnerability.

Appendix C—Malicious Code Methodology

Observations in this section were 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. In an average month SARA receives hundred of thousands of suspect files daily from both enterprise and individual consumers located throughout the world. These suspect files are then analyzed by Symantec and matched with virus definitions. An analysis of this aggregate data set provides Symantec with 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 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.

CONCLUSION

Whereas previous threats might not appear in the wild until several months to a year or more after the disclosure of a vulnerability, Blaster and Welchia each appeared within approximately one month of the vulnerability disclosure. Additionally, attacks are occurring with greater frequency and increasingly larger target space. To ensure that systems are continuously protected, it is imperative that all machines—corporate, academic, home user—be patched up to date.

The threat posed by malicious code is increasing not only in rapidity of infection, but in complexity as well. This complexity not only mandates a strong corporate security policy but 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 provide the comprehensive layered approach needed to reduce the risk from blended threats such as Blaster, SoBig, and Welchia.

Glossary

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 due to 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 check-ing 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 over-writing 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.

Class A Network

A Class A network is the largest IP address class of the three public use "classes" (Class A, Class B, and Class C) in the IP address space. There are 127 Class A networks with each supporting around 16 million hosts or individual IP addresses. Classless Inter-Domain Routing (CIDR) is an updated address-ing scheme that provides more effective use of IP addresses than the old Class A, B, and C scheme. You will now see Class A networks called a /8 (slash eight) network, so called for the 8-bit network prefix assigned under CIDR.

Exploit

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

Infection Vector

The method in which malicious code gains access to a computer system. The most common infection vector today is email. Other vectors of infection include floppy disks, vulnerabilities in software, peer-to-peer software, and instant messaging.

Integer Error

Integer errors are a type of programmatic flaw caused by a failure to properly handle variables of the integer data type. Integer errors can result in unexpected/unanticipated behavior in affected programs and can sometimes allow attackers to hijack the execution flow of the affected program.

Malicious Payload

Typically referred to as "Payload" because "mali-cious" is a major part of the definition. 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 for email addresses in 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, e.g., 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.

Remotely Exploitable

Remotely exploitable vulnerabilities are those which 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.

Side-Channel Attack

An attack that typically targets a weakness in the implementation of a system rather than its design. Errors in implementations of systems can cause a leak of important information in the timing of specific events. By observing the amounts of time that a system takes to perform certain behavior, attackers can sometimes obtain or infer valuable information. For example, knowledge of crucial timing information can possibly allow an attacker to compromise SSL/TLS sessions. Other reported timing-analysis attacks allowed attackers to guess valid usernames or determine the existence of confidential files. To a sophisticated attacker, timing-analysis and side-channel vulnerabilities offer powerful new methods to penetrate highly secure systems.

Virus

A self-replicating computer program.

Vulnerability

A security vulnerability is a coding error within a software system that can cause it to function outside of its documented design, violating its documented security policy. 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 copying itself 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 36 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 36 countries. For specific country offices and contact numbers please visit our Web site.