Timeline of Major Events in Internet Security

1946 John William Mauchly designs the first all-electronic computer, the ENIAC.

1951 The Remington Rand Corporation unveils the UNIVAC (Universal Automatic Computer).

1962 The ARPAnet begins life as a paper architecture and, under the leadership of the Department of Defense's Advanced Research Project Agency (ARPA), grows into a small network intended to promote the sharing of supercomputers among researchers in the United States.

1963 International Business Machines (IBM) introduces the System 360 Computer. The 360, which is a second-generation computer based on transistors, is a huge success and becomes the mainstay computer of many businesses for many years.

1968 The first generation of networking hardware and software is designed.

1971 John Draper, a.k.a. "Captain Crunch," discovers that a toy whistle from a cereal box can product the precise tone (2600 hertz) needed to make free long distance phone calls. "Phreaking" is born.

1974 Bolt, Beranek & Newman opens Telenet, the first commercial version of the ARPAnet.

1975 The era of the personal computer begins with the release of the Altair 8800, which uses the 8080 microprocessor. The following year, the Apple I is released by Steve Wozniak and Steve Jobs; the Apple I is built on a 6502 processor. One year later, the Apple II is released. The Apple II is the first serious home computer and results in a desktop computer revolution throughout the world.

Queen Elizabeth goes online with the first royal email message, announcing that The Royal Signals and Radio Establishment in Malvern is available on the ARPAnet system.

1976 Data Encryption Standard is approved for the first time.

1982 Apple computer viruses versions 1, 2, and 3 are found in-the-wild.

Xerox PARC's Jon Hepps and John Shock create internal worms for distributed computation. The worms get out of control and force the shutdown of multiple systems.

Bob Kahn and Vint Cerf are key members of a team that creates TCP/IP, the common language of all Internet computers. For the first time, the loose collection of networks that made up the ARPAnet is seen as an "internet," and the Internet as we know it today is born.

1983 Fred Cohen, known as the father of contemporary computer virology, demonstrates a virus-like program at a computer security seminar at Lehigh University; a year later, he formally introduces the term "computer virus" to the world.

The mid-80s marks a boom in the personal computer and super-minicomputer industries and corporations begin to use the Internet to communicate with each other and with their customers.

1984 British hackers Robert Schifreen and Steve Gold are arrested for hacking into Prince Philip's Prestel mailbox. Their actions will later inspire the writing of the UK's Computer Misuse Act.

1985 The first PC virus is created. Named Brain, the virus is a boot viruses and, for the first time, uses stealth techniques. Brain originated in Pakistan.

1988 By 1988, the Internet is an essential tool for communications, but it begins to create concerns about privacy and security in the digital world. New words such as "hacker," "cracker," and "electronic break-in" are created.

Robert Morris, 22, launches the Internet Worm. It spreads to 6,000 computers, 1/10 of all computers on the Internet. He is sentenced to three years' probation, 400 hours of community service, and a $10,000 fine.

1993 Traffic on the Internet expands at an annual growth rate of 341,634 percent.

1994 A virus writer utilizes the Internet to spread malicious code when the Kaos virus is posted to a newsgroup.

1995 Hackers alter the Web sites of the U.S. Justice Department, the CIA, and the U.S. Air Force.

1998 **March:** NASA, the U.S. Navy, and university campuses across the United States are targets of denial of service (DoS) attacks on computers running MS Windows NT and Windows 95.

Carl-Fredrik Neikter releases the Netbus Trojan tool, which allows hackers to obtain remote access to infected machines.

May: CERT announces that intruders are increasingly scanning port 1 to locate IRIX machines. Upon locating the machines, intruders then try to exploit known weaknesses in default accounts that do not have passwords.

July: AOL Trojans appear. The first of many Trojans designed to steal information from America Online users is unleashed by the spamming of AOL email addresses with "trojanized" attachments.

August: Back Orifice is released by Cult of the Dead Cow. The group writes a stealth remote control tool Trojan that allows execution and monitoring on an infected computer system. The media brings attention to the previously unknown Netbus program, which is similar in function.

September: A hacker group defaces the Web site of The New York Times.

December: Intruders automate attacks by using scripted tools to control data-collection and exploitation tools.

1999 **January:** Hackers make "sscan" publicly available. The sscan tool enables hackers to probe hosts to identify services that might be exploited.

March: The Melissa virus is released and spreads rapidly worldwide. The virus infects Word documents and emails itself to everyone in the MS Outlook address book, shutting down email servers.

June: The SubSeven Trojan is discovered. SubSeven is a malicious remote administration program. Once installed and executed, the SubSeven Trojan enables attackers to connect to,

control, and monitor the activity on other networked computers. The SubSeven Trojan uses several default ports for communication.

July: An updated version of Back Orifice is released by Cult of the Dead Cow. The remote control Trojan now works on Windows NT.

October: Hackers use scripts to automate attacks involving RPC service vulnerabilities.

Hackers use distributed network sniffers to capture usernames and passwords. Linux hosts are exclusively compromised by the sniffer client.

November: CERT announces they have received reports of intruders installing distributed DoS tools. According to CERT, the tools utilize distributed technology to create large networks of hosts capable of launching large coordinated packet-flooding DoS attacks.

2000 **February:** DoS attacks shut down Yahoo!, Buy.com, Amazon, eBay, and CNN. Yahoo! estimates that its three-hour outage cost the company as much as 5 percent of its weekly ad revenue. In January 2001, a 16-year-old hacker from Canada pleads guilty to launching the attacks.

May: GTE “secure” computers are damaged by a rogue employee who uses his security privileges to break into GTE’s Network Service Support Center and erase information, configuring the malicious code to prevent anyone from halting the deletion process and causing approximately $200,000 in damages. The worker pleads guilty March 2001.

The LoveLetter worm is released, sending itself to email addresses in the MS Outlook address book and spreading to Internet chatrooms using mIRC. The worms overwrites files on local and remote drives. The contents of most of these files are replaced with the source code of the worm, destroying the original contents. The worm also tries to download a password-stealing Trojan horse from a Web site.

August: MTX is discovered. It has a virus component and a worm component. It propagates by email and also infects some Win32 executables in specific folders. The virus can block access to certain Web sites, thereby preventing users from downloading new virus definitions.

Palm.Liberty.A is discovered. This is the first known Trojan horse for the Palm OS.

October: Microsoft announces that their internal network was compromised and that the attackers gained access to confidential Microsoft source code. The attack was initiated using a worm.

The Bymer worm is discovered. This worm, written in a high-level language, spreads over shared network drives. It searches for shared folders on the network, then copies itself to the Windows\System folder. The paylod copies the Dnetc.client and modifies the Win.ini file.

Widespread exploitation of common Linux vulnerabilities is reported. Attackers are searching the Internet for hosts with vulnerable rpc.statd and wu-ftpd services. In many cases, scans are followed by attempts to exploit both services. By successfully exploiting these flaws, a hacker can execute arbitrary instructions on the host with the privileges of the exploited process—typically root privileges.

December: The NIPC issues a security advisory regarding increased illegal hacker activity against U.S. e-commerce and Internet-hosted systems, primarily affecting sites running Microsoft applications and operating systems. Intruders are exploiting publicly known vulnerabilities to gain access to sensitive customer information on targeted sites. The NIPC later re-issues the advisory, saying attackers are using stolen information from customer and credit card databases to extort money from the affected companies and, in some cases, are selling that information to organized crime groups.

2001 **January:** The Ramen worm is discovered. It exploits well-known Linux vulnerabilities to propagate and to compromise privileged access on the systems it infects.

The U.S. Department of Energy system is compromised when a hacker breaks into the Sandia National Laboratories in Albuquerque, N.M.

February: The NASA Web site is vandalized when a 15-year-old student breaks into it and posts images related to a hacking group.

A buffer overflow vulnerability is discovered in the Lotus Domino R5 Server HTML parser. The buffer overflow can be exploited for denial of service or unauthorized access.

March: Microsoft announces vulnerabilities in MS IIS 5.0 and Exchange 2000 that could allow a hacker to launch DoS attacks and bring down systems.

Police in New York discover that a restaurant worker breached the bank, brokerage, and credit card accounts of Microsoft co-founder Paul Allen as well ask of movie director Steven Spielberg, financier Warren Buffet, CNN founder Ted Turner, and others on the Forbes "Richest Americans" list.

Microsoft issues a security bulletin concerning an incident in which Verisign, Inc. erroneously issued two digital certificates to an imposter claiming to be a Microsoft employee. These certificates can be used to digitally sign any program containing malicious code of any type under the name of Microsoft Corp.

The Lion worm is discovered. It is a blended threat. The Lion worm exploits a well-known vulnerability in BIND to gain privileged access to Linux systems. Once it has obtained access, it runs a rootkit to hide its presence, then searches for other vulnerable systems.

April: CERT reports that a distributed DoS tool named Carko is being installed on compromised hosts. The compromised hosts are at high risk for being used to attack other Internet sites, having system binaries and configuration files altered, and exposing sensitive information to external parties. Additionally, the tool is capable of reducing the availability of services through packet flooding attacks and other attacks that consume resources.

Hackers deface Web sites operated by the departments of Labor and of Health and Human Services. Hackers post a picture of a Chinese pilot, killed in a collision with a U.S. Navy spy plane early in the month, on the department of Labor's Web site.

May: Hackers attack the White House Web site, causing a DoS attack that lasts for several hours. No information on the site is altered or destroyed.

CERT is hit by a distributed DoS attack that limits access to its site for more than a day.

The official Web site of the Weather Channel goes down for the first time in its six-year history as a result of a DoS attack. Access to the site is blocked, but weather information is not compromised.

The Sadmind worm is discovered. The worm gains root access on Solaris systems and, in turn, uses the system to launch attacks against unpatched versions of MS IIS Web servers to modify the Web pages with harsh language against the U.S. government and against the U.S. hacker group PoizonBOx.

July: The Sircam worm is discovered. The worm contains its own SMTP engine and is network-aware. It does a large-scale mailing, using email addresses from the Windows Address Book and Outlook Express Sent Items folder. It also causes system instability by overwriting hard drives, erasing CMOS, and flashing the BIOS. In addition, it can send confidential Microsoft Word documents to others.

The Code Red worm is discovered. It is a blended threat. The worm is written to spread until the 20th of the month, attack whitehouse.gov until the 28th of the month, then sleep until the end of the month. It exists only in memory, which makes it uniquely able to remain undetected by many security technologies. The Code Red worm uses a known buffer overflow vulnerability contained in Microsoft Index Server and Windows 2000 Indexing Service.

August: The Code Red II worm, also a blended threat, is discovered. The worms uses the same attack and propagation methods as Code Red but carries a more malicious payload, installing a back door that enables future unauthorized administrative access. Computer Economics estimates that Code Red and Code Red II caused more than $2.6 billion in damages.

Web sites that use MS DNS Server report to CERT that they are experiencing cache corruption. Clients resolving hostnames against the corrupted cache are redirected, without authorization, to illegitimate sites. Further, applications that rely on DNS information are potentially manipulated by incorrect information stored in the cache.

September: The Nimda worm is discovered. It is a blended threat. The worm spreads through email, Web servers, Web browsing code, and open network shares by using known vulnerabilities in MS IIIS, MS IE, and MS Office. Computer Economics estimates that Nimda infected more than 2.2 million servers and PCs in a 24-hour period and caused more than half a billion dollars in damages.

A vulnerability is discovered that affects some intrusion detection systems. The vulnerability stems from a non-HTTP standard Unicode encoding format known as %u encoding that Microsoft IIS Web Server recognizes. This non-standard encoding could potentially obfuscate an attack similar to Code Red and variants, and potentially allow intruders to launch attacks against IIS Web servers that might go undetected by intrusion detection systems with signatures that only check for RFC-compliant encoding methods.

October: It is discovered that unauthorized macro files, potentially containing malicious code, can run without warning in MS Excel or PowerPoint documents, successfully bypassing Microsoft's security features. An attacker, therefore, could run arbitrary code with user privileges.

November: The BadTrans worm is discovered. BadTrans is a malicious Windows program that is distributed as an email file attachment. BadTrans exploits known vulnerabilities in Internet Explorer and some email programs and executes as soon as the user views the message. The worm can execute arbitrary commands with the same privileges as the user who triggered it.

December: The Goner worm is discovered. Goner is malicious Windows code distributed as an email file attachment and via ICQ file transfers. It appears to the user as a Windows screen saver, then infects when the user executes the file. The worm can disable antivirus and other security software installed on the system.

2002

February: The JS.Menger worm appears. This worm exploits a patched vulnerability in MSN Messenger. Code in JavaScript, the worm directs the user to one of a number of Web sites that contain the code.

A remote access buffer overflow condition is reported to exist in versions of ISS BlackICE and RealSecure firewall/IDS products that can potentially allow a remote attacker to execute arbitrary code with kernel-level access on targeted systems.

Multiple SNMP vulnerabilities are reported in multiple products. According to CERT, the products of more than 100 vendors may be at risk.

Microsoft Commerce Server 2000 is found to contain a buffer overflow vulnerability in the code that handles certain authentication requests. By exploiting this vulnerability, a remote intruder can potentially run arbitrary code with System privileges on the server and gain complete control over the targeted system.

Multiple buffer overflows are found in PHP that allow remote access to servers.

The Sharpei virus is discovered. It targets .exe files under the Microsoft .NET framework. The virus also mass emails itself to all contacts in the MS Outlook address book by using a VBS component. The virus arrives as an email message; when executed, it makes a copy of itself, then performs the mass-mailing routing, sending the previously described message.

The Kitro worm is discovered. Written in Delphi, Kitro uses SMTP to send itself to email addresses it finds in the MSN Messenger Service list.

March: The Gibe worm is discovered. Written for Windows, Gibe spreads via email disguised as a Microsoft security bulletin and patch. The payload is not destructive; however, Gibe installs a back door that might allow unauthorized access to the infected system.

A programming error is discovered in the zlib compression library used by many versions of software. Under the proper circumstances, an attacker can manipulate a system call in such a manner as to create a DoS condition or potentially allow arbitrary code to be run on the targeted system. Such code would run with the permissions of the affected program, to include root.

Microsoft announces that MS SQL Server 7.0 and 2000 extended stored procedures contain buffer overflow vulnerabilities that can be exploited to crash the SQL server, resulting in a DoS or potentially permit arbitrary code execution.

CERT reports that users of IRC and Instant Messaging (IM) are being tricked into downloading and executing malicious software; this software enables the intruders to use the infected systems to launch distributed DoS attacks.

April: Multiple vulnerabilities are discovered in MS IIS. The more critical of the vulnerabilities are buffer overflow conditions that can allow an attacker to overwrite system memory on the targeted system. Generally, these will result in the IIS service crashing and a DoS. In the worst cases, an attacker can run arbitrary code on the targeted system.

The Klez worm is discovered. It spreads by sending itself as an attachment to email addresses found in the Windows address book, the ICQ database, and local files. The email arrives with a random subject line. The worm randomly chooses a file from the infected machine to send along with the worm to recipients. It spreads through network share drives and is capable of infecting files. In addition, the Klez worm exploits an old vulnerability in MS Outlook and Outlook Express in an attempt to execute itself when the user opens or even previews the message.

Hackers break into the personnel database of the State of California and attempt to access financial information about all State employees, including judges and the governor. The security breach is discovered the following month.

The CIA releases a report warning that Chinese hackers, possibly backed by the Chinese government, might launch widespread cyber attacks on U.S. computer networks.

A hacking group calling itself the Dynamic Duo breaks into the computer systems of the U.S. Navy's Space and Naval Warfare Systems Command, the Federal Aviation Administration, and commuter airline company Midwest Express systems. The hackers deface the U.S. Navy and FAA sites and take customer information from the airline's Web site. The group claims they did it to expose security weaknesses.

A defense contractor developing a public Web site for the U.S. Navy shuts down its network after hackers gain access to employee passwords and other information. Web pages are defaced, public information is disclosed, and unauthorized messages claim responsibility by the Dynamic Duo.

May: The Microsoft MSN Chat Control input parameter handling functionality is found to contain an unchecked buffer that can allow remote code execution. This can enable an attacker to run arbitrary code on the targeted system with user-level privileges.

The Benjamin worm appears. The worm targets peer-to-peer systems. It comes disguised as popular music, movie, or software files. It spreads across KaZaA file-sharing networks by tricking KaZaA users into downloading the program and opening it. The worm displays a fake message and waits in the background for other KaZaA users to download the worm file. The Benjamin worm is the first of several worms to appear each month targeting KaZaA and/or similar networks.

The Digispid worm is discovered. It is a self-propagating malicious worm. It spreads to computers that are running MS SQL Server and that have a blank SQL administrator password. It copies files to the infected computer and changes the SQL administrator password to a string of four random characters.

June: Companies in Northern Ireland report that computer hackers are illicitly tapping into their Private Automatic Branch Exchange (PABX) systems and placing calls to places as far away as Kuwait and Hong Kong, running up bills in the tens of thousands of pounds in a single month.

Sun Solaris SNMP components are found to allow remote execution of code with root access.

The Apache Software Foundation announces that the Apache 1.3 and several versions of the Apache 2 Web servers contain a security flaw that can help a hacker launch a DoS attack or, in some cases, run his or her own code on the server.

The challenge response handling code in specific versions of OpenSSH is found to contain two related vulnerabilities. These vulnerabilities may allow a remote malicious user to execute arbitrary code as the user running sshd, which is often root.

The Remote Access Service (RAS) MS Windows phonebook is found to contain a buffer overflow that can allow malicious users to cause a DoS or to execute code.

The Scalper worm is discovered. This worm uses the Apache HTTP Server chunk encoding stack overflow vulnerability to spread itself. It targets the FreeBSD platform, derived from BSD UNIX.

The Sunday Star-Times in Auckland, New Zealand, reports that its investigative team identified more than 50 at-risk wireless networks in the city's business district. The article says its team and a computer security expert found 79 networks broadcasting signals in a 45-minute drive in central Auckland. Of those, 70 appeared unprotected and some had not even changed basic settings installed by the manufacturer.

USA Today reports that Microsoft is on track this year to match or exceed the number of security bulletins it used the previous year. According to the source, Microsoft issued 60 advisories in 2001 and by early June 2002 had issued 30 advisories outlining fixes for 40 vulnerabilities.

Computer Economics estimates that in 2001, software code attacks cost companies and others $13.2 billion.

July: The Symantec Internet Security Threat Report for January 1, 2002 through June 30, 2002 indicates that the average attacks per company per week was 28 percent higher than the previous period.

Three vulnerabilities are identified in MS Content Management Server. The effects of exploitation range from a DoS attack to gaining root access.

A vulnerability is found in the PHP parsing code that handles file uploads. By sending a specially crafted POST request to the Web server that corrupts the internal data structures used by PHP, a remote attacker can run arbitrary code with privileges of the Web server and potentially gain privileged access.

Multiple vulnerabilities are identified in MS SQL Server that can allow remote attackers to access to modify data, compromise SQL servers, and, in some configurations, compromise the server hosts.

A new exploit is discovered for an OpenSSL vulnerabilities, targeting Apache Web servers hosted on various Linux platforms. This also includes peer-to-peer capabilities, which allow it to communicate with other clients and participate in a distributed DoS. The exploit further exhibits worm behavior; once it is set up, it scans and attempts to propagate by infecting other vulnerable systems.

The Houston Chronicle reports that members of the international hacker group Hacktivismo released a program called CameraShy that allows Internet users to conceal messages inside photos posted on the Web, bypassing most known police monitoring methods. In addition, the group announces that it will soon launch technology that would allow anyone to set up his or her own anonymous, untraceable VPN.

August: The MS File Transfer Manager ActiveX control is found to contain a buffer overflow vulnerability and allows arbitrary file upload and download.

The ActiveX component of MS Terminal Services Advanced Client are found to contain a parameter with a buffer overflow vulnerability that allows arbitrary code execution. The vulnerability can be exploited from a Web page or through the use of HTML email.

The Charleston, S.C., Division of Motor Vehicles Web site is shut down after being hacked. According to The Charleston Gazette, although the unauthorized activity was recently discovered, it actually started in October 2001 when the DMV installed a new Internet server. The hacked Web site was created for Internet users to buy NASCAR license plates online.

MSNBC reports that hackers broke into the online files of a Florida company that provides surveillance technology to the U.S. military, federal agencies, and local police forces, and posted confidential information, including the names and email addresses of undercover police offers, on a public Web site. The hacker was reportedly able to get into the system through a Web order form on the company's site.

Microsoft announces a security flaw in its IE Web browser that can undermine the Secure Sockets Layer standard for securing online transactions and e-commerce.

A security hole is announced that affects Sun and IBM UNIX systems, Red Hat Linux systems, MacOS X Server software, and possibly Microsoft and HP operating systems. It also affects Kerberos authentication software. The vulnerabilities involves a communication protocol developed by Sun and based on its SunRPC remote procedure call technology. The flaw is in a program function distributed as part of an XDR library used by Sun and others to provide platform-independent methods for sending data between disparate systems.

September: A Canadian man accidentally hacks into the network of the City of Aspen, Colo., which enables him to access login names and passwords of the Aspen Police Department, among other details. The man, who immediately reported the accident, said he found himself viewing the entire contents of a city employee's computer hard drive when he was searching the KaZaA file-sharing network and it linked him to the computer of the City's network administrator, who had just installed the same peer-to-peer program onto his system.

Cisco Systems advises users that its VPN 3000 series concentrators contain vulnerabilities—13 in all—that can make it easier for hackers to get into secured networks or carry out DoS attacks.

President George W. Bush establishes the National Infrastructure Advisory Council (NIAC) and, with Special Advisor for Cyberspace Security Richard Clarke, announces the National Strategy for Securing Cyberspace. The Council includes Symantec Chairman and CEO John Thompson. The Council and Strategy aim to foster a better relationship between the public and private sectors in order to fortify homeland cybersecurity.

2003 **January:** The Slammer worm is discovered. It is the most major worm to hit SQL servers, in effect taking the entire Internet offline. In addition, unlike many worms, Slammer is not file-based, which enables it to spread quickly. The worm targets systems running MS SQL Server 2000 as well as MS Desktop Engine 2000. Slammer spreads with amazing speed. It has the unintended payload of performing a DoS attack due to the large number of packets it sends.

The SoBig worm is discovered. SoBig is a mass-mailing, network-aware worm that sends itself to all the email addresses it finds in the files with specific extensions. Subsequent variants of SoBig also spoof the From: field. SoBig also releases confidential information, in some cases stealing system information such as passwords. SoBig is unique in that it and its variants had hard-coded deactivation dates set so that when one variant deactivated, the next variant launched.

June: The BugBear.B worm is discovered. A variant of BugBear.A, the worm is polymorphic and also infects a select list of executable files. It possess keystroke-logging and back door capabilities and attempts to terminate the processes of various antivirus and firewall programs. The worm uses the Incorrect MIME Header Can Cause IE to Execute Email Attachment vulnerability to cause unpatched systems to auto-execute the worm when reading or previewing an infected message.

In addition, BugBear.B contains routines that specifically affect financial institutions. This functionality causes the worm to send sensitive data to one of 10 hard-coded, public Internet email addresses. The send information includes cached passwords and keystroke-logging data. Although BugBear.B is not the first worm to target a specific industry, it is unusually successful because it combines a targeted industry with mass-mailing capabilities as well as the ability to spread through network shares.

August: The Mimail worm is discovered. Mimail is a worm that spreads by email and steals information form a user's machine. The threat captures information from certain windows on a user's desktop and emails it to specific addresses. The worm is also packed with UPX. Mimail is unusual in that is spreads in the form of a zip archive, which would typically require effort to spread as users are required to double-click to open and then extract content. However, this worm is successful because the vulnerabilities it exploits allow it to autoexecute. In addition, the worm is noteworthy because it uses effective social engineering tactics to spread, pretending to be a message regarding the user's email account sent from the user's domain administrator.

The Blaster worm is discovered. W32.Blaster.Worm is a worm that exploits the DCOM RPC vulnerabilities using TCP port 135. The worm targets only Windows 2000 and Windows XP machines. While Windows NT and Windows 2003 Server machines are vulnerable to the exploit if not properly patched, the worm is not coded to replicate to those systems. More than two years later, Microsoft would announce that Blaster spread to more systems than any other piece of malicious software to date, with more than 25 million computers infected.

The Welchia worm is discovered. It is unique because it attempts to protect systems against Blaster by downloading a legitimate patch from the Microsoft Web site. Until Welchia, when a worm downloaded code, the download was typically an update to the worm itself.

September: Symantec releases its fourth *Internet Security Threat Report*, which covers Internet activity for the period of Jan. 1, 2003 to June 30, 2003. Symantec reports that one of the most significant security issues companies face comes from blended threats, which accounted for 60 percent of malicious code submissions in the first half of 2003. Symantec also notes that the speed of propagation of blended threats is increasing; the Blaster worm would be found to have infected as many as 2,500 computers per hour in its initial stage. For the first time, Symantec provides analysis of attacker vulnerability preferences in its report; 64 percent of all new attacks were found to have targeted vulnerabilities less than one year old. This information will become critical as the vulnerability-to-exploit window shrinks by the next period.

December: The Can-Spam Act is passed in the United States. The law prohibits the use of false header information in bulk commercial email and requires unsolicited messages to include opt-out instructions. Penalties for violations include fines of up to $250 per email, capped at up to $6 million.

2004

January: MyDoom.A, a Win32 worm, is discovered and is responsible for one of the worst mass-mailer worm outbreaks ever seen. The worm carries a back door that allows anyone to control a compromised system remotely. It also performs a DoS attack against several targets, using Web browser requests to bombard the target hosts to prevent easy filtering.

The Beagle mass-mailing worm is discovered. A Win32 worm, Beagle accesses remote Web sites and sends email to any addresses it finds using its own SMTP engine.

March: The Netsky worm is discovered. A Win32 worm, Netsky subverts some gateway scanners by occasionally sending itself in an archive using a seemingly innocuous .zip extension. Users unzip the file, then inadvertently run the virus. In addition to this innovative proliferation method, Netsky is noteworthy because it attempts to disable variants of the Mimail and MyDoom worms on systems it infected. This proceeds to spark a competition between the authors of MyDoom and Netsky.

The Witty worm is discovered. A Win32 worm, Witty uses a vulnerability in ICQ parsing by ISS products. The worm sends itself to multiple IP addresses using UDP source port 4000 and a random destination port. The worm resides in memory only, and does not create files on an infected computer. The worm also has a payload that overwrites random sectors of a random hard disk. Witty illustrates a worrisome trend: the rapidly diminishing time between the announcement of a vulnerability and the release of an associated exploit. The Witty worm appears in the wild only two days after the buffer overflow vulnerability it exploited is disclosed.

Symantec releases its fifth *Internet Security Threat Report*, which covers the period of July 1, 2003 to Dec. 31, 2003. Blended threats continue to remain a significant security concern, making up 54 percent of the top 10 malicious code submissions to Symantec during the reporting period. The vulnerability-to-threat window continues to shrink from months to days—for example, the Blaster worm emerged just 26 days after the announcement of the vulnerability it would exploit. Consequently, Symantec warns of the possibility of future "zero-day" threats that could exploit a vulnerability before that vulnerability was announced or a patch was made available for it. Symantec also notes an increase in malicious code that

can expose confidential information, pointing to Bugbear, backdoors, and spyware as examples.

April: The Sasser worm is discovered. A Win32 worm, Sasser attempts to exploit the LSASS vulnerability described in Microsoft Security Bulletin MS04-011. It spreads by scanning the randomly selected IP addresses for vulnerable systems. Sasser is a reminder that email is not the only way to infect machines on a large scale.

IDG.net reports that in recent weeks, malicious hackers have infiltrated computer systems at universities in the United States and worldwide. The systems were located at universities and research facilities that operate high-performance computer centers, including facilities that are part of a project funded by the U.S. National Science Foundation. Attackers gained access to systems by cracking or sniffing passwords from insecure network traffic such as Telnet remote communications sessions or from password files on other compromised systems. Attackers were also able to gain access to many systems because of loose security configuration for NFS.

June: Cabir, the first mobile device worm, is developed. Cabir spreads via Bluetooth on Symbian Series 60 devices such as smart phones, cellular telephones with computer-enabled features such as LAN connectivity and full Internet connectivity. Cabir repeatedly sends itself to the first Bluetooth-enabled device that it can find, regardless of the type of device. It also installs a small program known as a recognizer, which allows the worm to start itself whenever the smart phone is turned on. By the end of 2004, 11 new variants of Cabir will have been discovered.

Symantec captures an example of what is believed to be the first virus that targets 64-bit MS Windows systems. W64.Rugrat.3344 is believed to be a “proof of concept” virus that infects Windows Portable Executable files.

July: Duts.A is discovered; it is the first parasitic infector of portable executable files on Windows CE. Duts.A. shows that virus techniques appearing on PC viruses can be reused to infect files on mobile devices.

August: Brador.A is discovered. It is it the first back door Trojan to target Windows Mobile operating systems.

A Trojan named Mos is discovered in a Symbian game that sends an SMS message to a toll-charge phone number. The code in the game was purposely included by the developer as a copy protection scheme in January 2004. While the developer removed the code shortly thereafter, cracked versions of the game with the SMS code are found on some popular software piracy sites several months later.

September: Symantec releases its sixth *Internet Security Threat Report*, which covers the period of Jan. 1, 2004 to June 30, 2004. One of the most significant findings bears out Symantec’s earlier analysis, as the vulnerability-to-exploit window shrinks to an average of just 5.8 days. This is a serious concern for organizations as it allows them less than a week to patch vulnerable systems. Adding to this concern is the growth in bots; over the first six months of 2004, the number of monitored bots rose from under 1,000 to more than 30,000.

Symantec also notes that more vulnerabilities are being documented every week and that the majority of them are severe or moderately severe and easy to exploit. The Report also finds that e-commerce is the most targeted industry, with nearly 16 percent of attacks against it, a

significant increase from 4 percent reported during the previous period; Symantec theorizes that this rise may indicate a shift from attacks motivated by notoriety to attacks motivated by economic gain. This theory would be proven by the next reporting period.

December: The Santy worm is discovered. Santy is a worm written in Perl script that attempts to spread to Web servers running versions of the phpBB 2.x bulletin board software prior to 2.0.11, which are vulnerable to the PHPBB Viewtopic.PHP PHP Script Injection Vulnerability. Other systems are not affected. If successful, the worm copies itself to the server and overwrites certain files. The worm uses the Google search engine to find potential new infection targets, which prompts Google to block such requests.

2005

February: The Lazar Trojan is discovered. Trojan.Lazar is a Trojan horse that downloads other programs. It contacts a remote computer for instructions on files to download and configuration changes to make to the infected computer. Trojan.Lazar is one of the first examples of a growing trend in Internet threat activity—malicious code for financial gain. The Lazar Trojan downloads and installs adware that displays pop-up advertisements in the user's Web browser. The malicious code author receives a fee each time the adware is installed on a computer.

March: The first Multimedia Messaging Service (MMS) worm is discovered. SymbOS.Commwarrior.A is a worm that replicates on Series 60 phones. While previous malicious code for Symbian devices used only Bluetooth as a propagation vector, Commwarrior also uses MMS. This is significant because Bluetooth requires physical proximity between an infected device and a target in order to propagate. MMS requires only a connection between a phone and the network in order to send messages and files to other phones. This has the potential to expand the scope of an outbreak from the local to the global level. By the end of 2005, 57 wireless threat variants in Symbian device families will be discovered; only 17 were discovered in 2004.

Symantec releases its seventh *Internet Security Threat Report*, which covers the period of July 1, 2004 to Dec. 31, 2004. Symantec reports that threats to confidential information have continued to increase over the last three reporting periods—from 36 percent of the top 50 malicious code samples in the second half of 2003 to 44 percent in the first half of 2004 and 54 percent in the second half of 2004. Phishing is one such threat; 10 million phishing attempts were blocked, a ten-fold increase in the number of messages blocked since July 2004.

The report also showed that the volume of Windows 32 viruses and worms increased dramatically, from 4,496 in the first half of 2004 to more than 7,360 in the second half of the year. Also, for the first time, more vulnerabilities were found in an alternative browser than in Microsoft Internet Explorer; 21 vulnerabilities were found in Mozilla browsers, while 13 vulnerabilities in Internet Explorer were documented.

April: W32.Mytob.AA@mm is discovered. The worm is a mass-mailer that uses its own SMTP engine to send an email to addresses that it gathers from files on the compromised computer. The email has a variable subject and attachment name. The worm also has the ability to open a back door and spreads through the network by exploiting common system vulnerabilities. The Mytob family of worms will continue to proliferate quickly throughout 2005. Such rapid production of new variants is likely intended to attempt to bypass existing antivirus definitions and, by extension, to overwhelm security administrators trying to keep their systems up-to-date.

May: The trend in malicious code for profit continues with the discovery of Trojan.Gpcoder. This Trojan encrypts data files such as documents, spreadsheets, and database files on the compromised computer. It then creates a file in each folder containing information on how the user can obtain a decoder for the files. Reportedly, the user must pay $200 for the decoder software.

A more worrisome trend in the use of malicious code for profit was observed in the form of targeted Trojan attacks. At the end of May 2005, several executives at large companies in Israel were arrested for allegedly using Trojans to monitor their competitors. A private investigation firm was reported to have written a custom Trojan program that was then sent to users at the competing companies to entice them to execute the application. Once installed, this Trojan would log keystrokes and allow remote access to the compromised computer, allowing the authors to illicitly obtain sensitive information from their competitors.

The Tooso.I Trojan is discovered. It is an example of another disturbing trend in malicious code as hackers begin deploying modular malicious code. Modular malicious code is malicious code such as worms, viruses, and Trojans that initially possess limited functionality; however, once installed on a target computer, it downloads other pieces (or modules) of malicious code with different functionalities and further compromises the infected computer. With the Tooso.I Trojan, once installed, it attempts to disable antivirus solutions and then download further functionality from different sources. Because of its modular structure, the majority of this additional functionality is hosted on machines distributed across the Internet.

August: Zotob.E is discovered. Zotob was one of only a handful of Level 3 threats discovered in 2005. The worm exploited a Microsoft Windows Plug and Play Service Vulnerability in Windows 2000 described in Microsoft Security Bulletin MS04-039 issued on August 9, 2005. Although the proliferation of Zotob was not as great as other high-profile threats, those who were hit by it felt a significant impact. Zotob attacked older platforms, which many companies didn't have the bandwidth to deal with.

A group of European wireless security experts develop Car Whisperer to demonstrate the shortcomings of some Bluetooth systems. Car Whisperer takes advantage of the fact that many of these hands-free systems require only a simple four-digit security key in order to grant a device access to the system. Many car manufacturers use the same code for all of their Bluetooth systems, making it easy for Car Whisperer to send and receive audio from the car.

September: Symantec releases its eighth *Internet Security Threat Report*. Traditionally the Report has broken security threats down into three general categories: attacks, vulnerabilities, and malicious code. However, as Internet-based services and applications have expanded and diversified, the potential for computer programs to introduce other types of security risks has increased. The emergence of new risks—particularly spam, phishing, spyware, and adware—necessitates an expansion of the traditional security taxonomy.

Consequently, Symantec adds a new section to its Report for concerns its classifies as "additional security risks." Between January 1 and June 30, 2005, adware makes up 8 percent of the top 50 programs reported to Symantec. During the same period, the Symantec Probe Network detected 40 percent more unique phishing messages than were detected in the previous six-month period; it also calculated that spam made up approximately 61 percent of all email traffic.

October: Trojan.PSPBrick is discovered—the first Trojan horse targeting Sony PlayStation Portable (PSP) that has been discovered in the wild. Users download the file, which is described as an application that allows the PSP to run non-Sony games, and transfer it to the PSP via memory stick. Once installed on the PSP, the malicious code wipes out system files that render the game unit useless. Symantec predicts that such threats on non-traditional platforms are expected to increase.

December: Symantec security experts pursue several research projects focusing on cybercrime and crimeware. They find that the development of malicious code is likely a full-time endeavor rather than something done "on the side"; fraudsters use the Internet not only to find victims but also to communicate with other fraudsters; unskilled novices can enter the world of cybercrime and use the many online tools, forums, and tutorials that walk them through the steps and techniques needed to defraud others.