United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations, Committee on Government Reform, House of Representatives

For Release
on Delivery
Expected at 10 a.m., PDT
Wednesday
August 29, 2001

INFORMATION SECURITY

Code Red, Code Red II, and SirCam Attacks Highlight Need for Proactive Measures

Statement of Keith A. Rhodes
Chief Technologist

Mr. Chairman and Members of the Subcommittee:

Thank you for inviting me to participate in today's hearing on the most recent rash of computer attacks. This is the third time I've testified before Congress over the past several years on specific viruses—first, the "Melissa" virus in April 1999 and second, the "ILOVEYOU" virus in May 2000. At both hearings, I stressed that the next attack would likely propagate faster, do more damage, and be more difficult to detect and counter.

Again, we are having to deal with destructive attacks that are reportedly costing billions. In the past 2 months, organizations and individuals have had to contend with several particularly vexing attacks. The most notable, of course, is Code Red but potentially more damaging are Code Red II and SirCam. Together, these attacks have infected millions of computer users, shut down Web sites, slowed Internet service, and disrupted business and government operations. They have already caused billions of dollars of damage and their full effects have yet to be completely assessed.

Today, I would like to discuss the makeup and potential threat that each of these viruses pose as well as reported damages. I would also like to talk about progress being made to protect federal operations and assets from these types of attacks and the substantial challenges still ahead.

The Attacks

Despite some similarities, each of the recent attacks is very different in its makeup, method of attack, and potential damage. Generally, Code Red and Code Red II are both "worms," which are attacks that propagate themselves through networks without any user intervention or interaction. They both take advantage of a flaw in a component of versions 4.0 and 5.0 of Microsoft's Internet Information Services (IIS) Web server software.

Code Red originally sought to do damage by defacing Web pages and by denying access to a specific Web site by sending it massive amounts of data, which essentially would shut it down. This is known as a denial-of-service (DoS) attack. Code Red II is much more discreet and potentially more damaging. Other than sharing the name of the original worm, the only similarity Code Red II has with Code Red is that it exploits the same IIS vulnerability to propagate itself. Code Red II installs "backdoors" on infected Web servers, making them vulnerable to hijacking by any attacker who knows how to exploit the backdoor. It also spreads faster than Code Red. Both attacks have the potential to decrease the speed of the Internet and cause service disruptions. More importantly, these worms broadcast

to the Internet the servers that are vulnerable to this flaw, which allows others to attack the servers and perform other actions that are not related to Code Red.

SirCam is a malicious computer virus that spreads primarily through E-mail. Once activated on an infected computer, the virus searches through a select folder and mails user files acting as a "Trojan horse" to E-mail addresses in the user's address book. A Trojan horse, or Trojan, is a program containing hidden code allowing the unauthorized collection, falsification, or destruction of information. If the user's files are sensitive in nature, then SirCam not only succeeds in compromising the user's computer, but also succeeds in breaching the data's confidentiality. In addition to spreading, the virus can attempt to delete a victim's hard drive or fill the remaining free space on the hard drive making it impossible to perform common tasks such as saving files or printing. This form of attack is extremely serious since it is one from which it is very difficult to recover.

SirCam is much more stealthy than the Melissa and ILOVEYOU viruses because it does not need to use the victim's E-mail program to replicate. It has its own internal capabilities to mail itself to other computers. SirCam also can spread through another method. It can copy itself to other unsuspecting computers connected through a Windows network (commonly referred to as Windows network computers) that has granted read/write access to the infected computer. Like Code Red and Code Red II, SirCam can slow the Internet. However, SirCam poses a greater threat to the home PC user than that of the Code Red worms.

Table 1 provides a high-level comparison of the attacks. The attachment to this testimony answers the questions in the table in greater detail.

Table 1: High-level Comparison of the Attacks

	What is it?	How does it spread?	Who is at risk?	What damage can it do?
Code Red	Code Red is a worm, which is a computer attack that propagates through networks without user intervention. This particular worm makes use of a vulnerability in Microsoft's Internet Information Services (IIS) Web server software—specifically, a buffer overflow.	The worm scans the Internet, identifies vulnerable systems, and infects these systems by installing itself. Each newly installed worm joins all the others, causing the rate of scanning to grow rapidly.	Users with Microsoft IIS server installed with Windows NT version 4.0 or Windows 2000.	The program can deface Web sites, and was designed to perform a DoS attack against the www.whitehouse.gov Web site. It can also decrease the speed of the Internet.
Code Red II	Code Red II is also a worm that exploits the same IIS vulnerability. However, the worm also opens a backdoor on an infected server that allows any follow-on remote attacker to execute arbitrary commands.	Code Red II spreads like Code Red; however, in doing so, it selects Internet addresses that are in the same network range as the infected computer to increase the likelihood of finding susceptible victims.	Users with Microsoft IIS Web server software installed with Windows 2000.	Like Code Red, Code Red II can decrease the speed of the Internet. Unlike Code Red, it also leaves the infected system open to any attacker who can alter or destroy files and create a denial of service. It does not deface Web pages.
SirCam	SirCam is a malicious computer virus that spreads through E-mail and potentially through unprotected network connections. Once the malicious code has been executed on a system, it may reveal or delete sensitive information.	This mass-mailing virus attempts to send itself to E-mail addresses found in the Windows Address Book and addresses found in cached browser files. It also attempts to copy itself to specific Windows networked computers.	Any E-mail user or user of a computer with unprotected Windows network connections to the infected computer.	SirCam can publicly release sensitive information and delete files and folders. It can also fill the remaining free space on the computer's hard drive. Furthermore, it can lead to a decrease in the speed of the Internet.

Systems infected by Code Red and SirCam can be fixed relatively easily. A patch made available by Microsoft can remove the vulnerability exploited by Code Red and rebooting the infected computer removes the worm itself. Updating and using antivirus software can help detect and partially recover from SirCam. Patching and rebooting an infected server is not enough when a system is hit by Code Red II. Instead, the system's hard drive should be reformatted, and all software should be reinstalled to ensure that the system is free of other backdoor vulnerabilities.

Of course, there are a number of other immediate actions organizations can take to ward off attacks. These include:

- using strong passwords,
- verifying software security settings,

- installing firewalls,
- backing up files early and often,
- ensuring that known software vulnerabilities are reduced by promptly implementing software patches available from vendors,
- ensuring that policies and controls already implemented are operating as intended,
- using scanners that automatically search for system vulnerabilities,
- using password-cracking tools to assess the password strength of the audited users,
- using network monitoring tools to identify suspicious network activity, and
- developing and distributing lists of the most common types of vulnerabilities and suggested corrective actions.

Impact of the Attacks

Reports from various media and computer security experts indicate that the impact of these viruses has been extensive. On July 19, the Code Red worm infected more than 250,000 systems in just 9 hours, according to the National Infrastructure Protection Center (NIPC). An estimated 975,000 servers have been infected in total, according to Computer Economics, Inc. Code Red and Code Red II have also reportedly disrupted both government and business operations, principally by slowing Internet service and forcing some organizations to disconnect themselves from the Internet.

For example, reports have noted that (1) the White House had to change the numerical Internet address that identifies its Web site to the public, and (2) the Department of Defense was forced to briefly shut down its public Web sites. Treasury's Financial Management Service was infected and also had to disconnect itself from the Internet. Code Red worms also reportedly hit Microsoft's popular free E-mail service, Hotmail; caused outages for users of Qwest's high-speed Internet service nationwide; and caused delays in package deliveries by infecting systems belonging to FedEx Corp. There are also numerous reports of infections in other countries.

The economic costs resulting from Code Red attacks are already estimated to be over $2.4 billion.[1] These involve costs associated with cleaning infected systems and returning them to normal service, inspecting servers

[1] Estimate was developed by Computer Economics Inc.

to determine the need for software patches, patching and testing services as well as the negative impact on the productivity of system users and technical staff.

Although Code Red's reported costs have not yet surpassed damages estimated for last year's ILOVEYOU virus, which is now estimated to be more than $8 billion[2], the Code Red attacks are reportedly more costly than 1988's Morris worm. This particular worm exploited a flaw in the Unix operating system and affected VAX computers from Digital Equipment Corp. and Sun 3 computers from Sun Microsystems, Inc. It was intended to only infect each computer once, but a bug allowed it to replicate hundreds of times, crashing computers in the process. Approximately 10 percent of the U.S. computers connected to the Internet effectively stopped at the same time. At that time, the network had grown to more than 88,000 computers and was a primary means of communication among computer security experts.[3]

SirCam has also reportedly caused some havoc. It is allegedly responsible for the leaking of secret documents from the government of Ukraine. And it reportedly infected a computer at the Federal Bureau of Investigation (FBI) late last month and sent some private, but not sensitive or classified, documents out in an E-mail. There are reports that SirCam has surfaced in more than 100 countries.

Attacks Underscore Challenges Involved in Protecting Systems

GAO has identified information security as a governmentwide high risk issue since 1997. As these incidents continue, the federal government continues to face formidable challenges in protecting its information systems assets and sensitive data. These include not only an ever changing and growing sophistication in the nature of attacks but also an urgent need to strengthen agency security controls as well as a need for a more concerted and effective governmentwide coordination, guidance, and oversight. Today, I would like to briefly discuss these challenges. I would also like to discuss progress that has been made in addressing them, including improvements in agency controls, actions to strengthen warning and crisis management capabilities, and new legislation to provide a comprehensive framework for establishing and ensuring effectiveness of information security controls over information resources that support

[2] Computer Economics, Inc.

[3] http://www.cert.org/encyc_article/tocencyc.html.

federal government operations and assets. These are positive steps toward taking a proactive stand in protecting sensitive data and assets.

First, these latest incidents again show that computer attack tools and techniques are becoming increasingly sophisticated. The Code Red attack was more sophisticated than those experienced in the past because the attack combined a worm with a denial-of-service attack. Further, with some reprogramming, each variant of Code Red got smarter in terms of identifying vulnerable systems. Code Red II exploited the same vulnerability to spread itself as the original Code Red. However instead of launching a DoS attack against a specific victim, it gives an attacker complete control over the infected system, thereby letting the attacker perform any number of undesirable actions. SirCam was a more sophisticated version of the ILOVEYOU virus, no longer needing the victim's E-mail program to spread.

In the long run, it is likely that hackers will find ways to attack more critical components of the Internet, such as routers and network equipment, rather than just Web site servers or individual computers. Further, it is likely that viruses will continue to spread faster as a result of the increasing connectivity of today's networks and the growing use of commercial-off-the-shelf (COTS) products, which, once a vulnerability is discovered, can be easily exploited for attack by all their users because of the widespread use of the products.

Second, the recent attacks foreshadow much more devastating Internet threats to come. According to official estimates, over 100 countries already have or are developing computer attack capabilities. Further, the National Security Agency has determined that potential adversaries are developing a body of knowledge about U.S. systems and methods to attack them. Meanwhile, our government and our nation have become increasingly reliant on interconnected computer systems to support critical operations and infrastructures, including telecommunications, finance, power distribution, emergency services, law enforcement, national defense, and other government services. As a result, there is a growing risk that terrorists or hostile foreign states could severely damage or disrupt national defense or vital public operations through computer-based attacks on the nation's critical infrastructures.

Third, agencies do not have an effective information security program to prevent and respond to attacks—both external attacks, like Code Red, Code Red II, and SirCam, and internal attempts to manipulate or damage systems and data. More specifically, we continue to find that poor security

planning and management are the rule rather than the exception. Most agencies do not develop security plans for major systems based on risk, have not formally documented security policies, and have not implemented programs for testing and evaluating the effectiveness of the controls they rely on.

Agencies also often lack effective access controls to their computer resources and consequently cannot protect these assets against unauthorized modification, loss, and disclosure. Moreover, application software development and change controls are weak; policies and procedures governing segregation of duties are ineffective; and access to the powerful programs and sensitive files associated with a computer systems operation is not well-protected. In fact, over the past several years, our analyses as well as those of the Inspectors General have found that virtually all of the largest federal agencies have significant computer security weaknesses that place critical federal operations and assets at risk to computer-based attacks.

In recognition of these serious security weaknesses, we and the Inspectors General have made recommendations to agencies regarding specific steps they should take to make their security programs effective.[4] Also, in 2001, we again reported information security as a high-risk area across government, as we did in our 1997 and 1999 high-risk series.[5]

Fourth, the government still lacks robust analysis, warning, and response capabilities. Often, for instance, reporting on incidents has been ineffective—with information coming too late for agencies to take proactive measures to mitigate damage. This was especially evident in the Melissa and ILOVEYOU attacks. There is also a lack of strategic analysis to determine the potential broader implications of individual incidents. Such analysis looks beyond one specific incident to consider a broader set of incidents or implications that may indicate a potential threat of national importance.

[4] See, for example, *Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies* (GAO/AIMD-00-295, September 6, 2000).

[5] *High-Risk Series: An Update* (GAO-01-263, January 2001).

Further, as we recently reported,[6] the ability to issue prompt warnings about attacks is impeded because of (1) a lack of a comprehensive governmentwide or nationwide framework for promptly obtaining and analyzing information on imminent attacks, (2) a shortage of skilled staff, (3) the need to ensure that undue alarm is not raised for insignificant incidents, and (4) the need to ensure that sensitive information is protected, especially when such information pertains to law enforcement investigations underway. Lastly, government entities have not developed fully productive information-sharing and cooperative relationships. We recently made a variety of recommendations to the Assistant to the President for National Security Affairs and the Attorney General regarding the need to more fully define the role and responsibilities of the NIPC, develop plans for establishing analysis and warning capabilities, and formalize information-sharing relationships with the private sector and federal entities.[7]

Fifth, most of the nation's critical infrastructure is owned by the private sector. Solutions, therefore, need to be developed and implemented in concert with the private sector, and they must be tailored sector by sector, through consultation about vulnerabilities, threats, and possible response strategies. Putting together effective partnerships with the private sector is difficult, however. Disparate interests between the private sector and the government can lead to profoundly different views and perceptions about threats, vulnerabilities, and risks, and they can affect the level of risk each party is willing to accept and the costs each is willing to bear. Moreover, industry has raised concerns that it could potential face antitrust violations for sharing information. Lastly, there is a concern that an inadvertent release of confidential business material, such as trade secrets or proprietary information, could damage reputations, lower consumer confidence, hurt competitiveness, and decrease market shares of firms.

[6] *Critical Infrastructure Protection: Significant Challenges in Developing Analysis, Warning, and Response Capabilities* (GAO-01-1005T, July 25, 2001).

[7] The NIPC agreed with generally agreed with our findings and stated that the NIPC considers it of the utmost urgency to address the shortcomings we identified. However, the NIPC did not comment on several key recommendations, including the need to improve cooperative relationships with other federal entities, such as Defense and the Secret Service. See *Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities* (GAO-01-323, April 25, 2001).

Fortunately, we are beginning to see improvements that should help agencies ward off attacks. We reported earlier this year[8] that several agencies have taken significant steps to redesign and strengthen their information security programs. For example, the Internal Revenue Service (IRS) has made notable progress in improving computer security at its facilities, corrected a significant number of identified weaknesses, and established a service-wide computer security management program. Similarly, the Environmental Protection Agency has moved aggressively to reduce the exposure of its systems and data and to correct weaknesses we identified in February 2000.

Moreover, the Federal Computer Incident Response Center (FedCIRC) and the NIPC have both expanded their efforts to issue warnings of potential computer intrusions and to assist in responding to computer security incidents. In responding to the Code Red and Code Red II attacks, FedCIRC and NIPC worked together with Carnegie Mellon's CERT Coordination Center, the Internet Security Alliance, the National Coordinating Center for Telecommunications, the Systems Administrators and Network Security (SANS) Institute, and other private companies and security organizations to warn the public and encourage system administrators and home users to voluntarily update their software.

We also recently reported on a number of other positive actions taken by NIPC to develop analysis, warning, and response capabilities. For example, since its establishment, the NIPC has issued a variety of analytical products to support computer security investigations. It has established a Watch and Warning Unit that monitors the Internet and other media 24 hours a day to identify reports of computer-based attacks. It has developed crisis management capabilities to support a multi-agency response to the most serious incidents from FBI's Washington, D.C., Strategic Information Operations Center.

The administration is currently reviewing the federal strategy for critical infrastructure protection that was originally outlined in Presidential Decision Directive (PDD) 63, including provisions related to developing analytical and warning capabilities that are currently assigned to the NIPC. On May 9, 2001, the White House issued a statement saying that it was working with federal agencies and private industry to prepare a new version of the "national plan for cyberspace security and critical

[8] *High-Risk Series: An Update* (GAO-01-263, January 2001).

infrastructure protection" and reviewing how the government is organized to deal with information security issues.

Lastly, the Congress recently enacted legislation to provide a comprehensive framework for establishing and ensuring the effectiveness of information security controls over information resources that support federal government operations and assets. This legislation[9]—known as Government Information Security Reform (GISR)—requires agencies to implement an agencywide information security program that is founded on a continuing risk management cycle. GISR also added an important new requirement by calling for an independent evaluation of the information security program and practices of an agency. These evaluations are to be used by OMB as the primary basis for its summary report to the Congress on governmentwide information security.

In conclusion, the attacks we are dealing with now are smarter and more threatening than the ones we were dealing with last year and the year before. But I believe we are still just witnessing warning shots of potentially much more damaging and devastating attacks on the nation's critical infrastructures. To that end, it's vital that federal agencies and the government as a whole become proactive rather than reactive in their efforts to protect sensitive data and assets. In particular, as we have recommended in many reports and testimonies,[10] agencies need more robust security planning, training, and oversight. The government as a whole needs to fully develop the capability to strategically analyze cyber threats and warn agencies in time for them to avert damage. It also needs to continue building on private-public partnerships—not just to detect and warn about attacks—but to prevent them in the first place. Most of all, trust needs to be established among a broad range of stakeholders, roles and responsibilities need to be clarified, and technical expertise needs to be developed. Lastly, becoming truly proactive will require stronger

[9] Floyd D. Spence, National Defense Authorization Act for Fiscal Year 2001, P.L. 106-398, Title X, Subtitle G, 114 Stat. 1654, 1654A-265 (2000).

[10] See, for example, *Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies* (GAO/AIMD-00-295, September 6, 2000); *Critical Infrastructure Protection: Comprehensive Strategy Can Draw on Year 2000 Experiences* (GAO/AIMD-00-1, October 1, 1999); *Critical Infrastructure Protection: Comments on the National Plan for Information Systems Protection* (GAO/T-AIMD-00-72, February 1, 2000) and *Critical Infrastructure Protection: Challenges to Building A Comprehensive Strategy for Information Sharing and Coordination* (GAO/T-AIMD-00-268, July 26, 2000).

leadership by the federal government to develop a comprehensive strategy for critical infrastructure protection, work through concerns and barriers to sharing information, and institute the basic management framework needed to make the federal government a model of critical infrastructure protection.

Mr. Chairman and Members of the Subcommittee, this concludes my statement. I would be pleased to answer any questions that you or Members of the Subcommittee may have.

Contacts and Acknowledgment

For further information, please contact Keith Rhodes at (202) 512-6412. Individuals making key contributions to this testimony included Cristina Chaplain, Edward Alexander, Jr., Tracy Pierson, Penny Pickett, and Chris Martin.

Attachment I: Details on the Attacks

Code Red

Question	Answer
What is it?	Code Red is a worm, which is a computer attack that propagates through networks without user intervention. This particular worm makes use of a vulnerability in Microsoft's Internet Information Services (IIS) Web server software—specifically, a buffer overflow.[a] The worm looks for systems running IIS (versions 4.0 and 5.0) that have not patched the unchecked vulnerability, and exploits the vulnerability to infect those systems. Code Red was initially written to deface the infected computer's Web site and to perform a distributed denial of service (DDoS) attack against the numerical Internet address used by www.whitehouse.gov. Two subsequent versions of Code Red do not deface Web pages but still launch the DDoS attack. Code Red was first reported on July 17, 2001. The worm is believed to have started at a university in Guangdong, China.
How does it spread?	The worm scans the Internet, identifies vulnerable systems, and infects these systems by installing itself. Each newly installed worm joins all the others causing the rate of scanning to grow rapidly. The first version of Code Red created a randomly generated list of Internet addresses to infect. However, the algorithm used to generate the list was flawed, and infected systems ended up reinfecting each other. The subsequent versions target victims a bit differently, increasing the rate of infection.
Who is at risk?	Users with a Microsoft IIS server installed with Windows NT version 4.0 and Windows 2000.
What damage can it do?	The original variant of Code Red (CRv1) can deface the infected computer's Web site and used the infected computer to perform a DDoS attack against the Internet address of the www.whitehouse.gov Web site. Subsequent variants of Code Red (CRv2a and CRv2b) no longer defaced the infected computer's Web site making detection of the worm harder. These subsequent variants continued to target the www.whitehouse.gov Web site and used smarter methods to target new computers for infection. The uncontrolled growth in scanning can also decrease the speed of the Internet and cause sporadic but widespread outages among all types of systems. Specifically, Although the initial version, CRv1, defaces the Web site, the primary impact to the server is performance degradation as a result of the scanning activity of this worm. This degradation can become quite severe since it is possible for a worm to infect the same machine multiple times. Other entities, even those that are not vulnerable to Code Red, are impacted because servers infected by Code Red scan their systems and networks. Depending on the number of servers performing this scan, these entities may experience network denial of service. This was especially true with the implementation of CRv1 since a "flaw" in the random number generator essentially targeted the same servers. As noted above, this behavior is not found in the later variants. However, the end result may be the same since CRv2a and CRv2b use improved randomization techniques that facilitate more prolific scanning.
What can you do if you're infected?	Install a patch made available by Microsoft and reboot the system. (The patch should also be installed as a preventative measure).

Question	Answer
Technical Details on How the Code Red Worm Operates	
The Code Red worm has three phases – discovery and propagation, attack, and dormancy. Execution of these phases is based upon the day of the month.	
Phase 1: Discovery and Propagation	Between day 1 and day 19 of any month, Code Red performs its discovery and propagation function. It does this by generating 100 subprograms on an infected server. All but one of these subprograms has the task of identifying and infecting other vulnerable Web servers by scanning a generated list of Internet addresses. Once a target system is identified, Code Red uses standard Web server communication to exploit the flaw and send itself to the vulnerable server. Once a new server is infected, the process continues. CRv1 created a randomly generated list of Internet addresses to infect. However, the algorithm used to generate the random number list was "flawed", and infected systems ended up re-infecting each other because the random list that each computer generated was the same. CRv2a and CRv2b were modified to generate actual random lists of Internet addresses that were more effective at identifying potential servers that had not already been attacked. Therefore, these versions can ultimately infect greater numbers of unprotected servers. CRv1 also defaced the target system's Web site. This was done by replacing site's actual Web page with the message, "HELLO! Welcome to http://www.worm.com! Hacked by Chinese!"[b] This message enabled system administrators to easily identify when their servers had been infected. CRv2a and CRv2b modified the functionality so it would no longer deface Web pages, forcing system administrators to be proactive in determining infection. Descriptions of the variants are listed below. • CRv1: Web site defacement and "random" target selection for additional attacks. • CRv2a: No Web defacement and modified random target selection • CRv2b: No Web defacement and better target selection by optimizing the random number generation process, i.e., better target addresses are generated. Due to the target optimization, systems infected with version 2b are able to infect new systems at a faster rate than version 2a.
Phase 2: Attack	Between day 20 and day 27 of any month is Code Red's attack phase. Once Code Red determines the date to be within this designated attack date range, each infected server participates in a DDoS attack by sending massive amounts of data to its intended target, the numeric Internet address of the White House Web site. Since all infected servers are set to attack the same target on the same set of dates, the large amount of Internet traffic is expected to flood the Internet with data and bombard a numeric address used by www.whitehouse.gov with more data than it can handle. This flooding of data would cause the Web server to stop responding to all Web server requests, including legitimate users surfing the White House Web site.
Phase 3: Dormancy	From day 28 to the end of the month, the Code Red worm lays dormant, going into an infinite sleep phase. Although the worm remains in the computer's memory until the system is rebooted, Code Red will not propagate or initiate any attacks once it enters dormancy. According to testing performed by Internet Security Systems, Carnegie Mellon's CERT Coordination Center (CERT/CC), and the Federal Bureau of Investigation's (FBI) National Infrastructure Protection Center (NIPC), the dormant worm cannot be awakened to restart the process.

Code Red II

Question	Answer
What is it?	Code Red II is also a worm that makes use of a buffer overflow vulnerability in Microsoft's IIS Web server software. Except for using the buffer overflow injection mechanism, the worm is very different than the original Code Red and its variants. In fact, it is more dangerous because it opens backdoors on infected servers that allow any follow-on remote attackers to execute arbitrary commands. There is no DDoS attack function in Code Red II. Code Red II was reported on August 4, 2001, by industry analysts.
How does it spread?	Like Code Red, the worm scans the Internet, identifies vulnerable systems, and infects these systems by installing itself. Each newly installed worm joins all the others causing the rate of scanning to grow. Code Red II, however, mostly selects Internet addresses in the same range as the infected computer to increase the likelihood of finding susceptible victims.
Who is at risk?	Users with Microsoft IIS Web server software (versions 4.0 and 5.0) installed with Windows 2000.
What damage can it do?	Like Code Red, Code Red II can decrease the speed of the Internet and service disruptions. Unlike Code Red, it also leaves the infected system open to any attacker who can alter or destroy files and create a denial of service attack. Specifically, • Because of the worm's preference to target its closest neighbors, combined with the enormous amount of scanning traffic generated by the numerous subprograms running in parallel, a large amount of broadcast request traffic is generated on the infected system's network. If several machines on a local network segment are infected, then the resulting attempt to propagate the infection to their neighbors simultaneously can generate broadcast requests at "flooding" rates. Systems on the receiving end of an effective "broadcast flood" may experience the effects of a DoS attack. • Code Red II allows remote attackers and intruders to execute arbitrary commands on infected Windows 2000 systems. Compromised systems are then subject to files being altered or destroyed. This adversely entities that may be relying on the altered or destroyed files. Furthermore, compromised systems are also at high risk for being exploited to generate other types of attacks against other servers.
What do you do if you're infected?	Several anti-virus software vendors have created tools that remove the harmful effects of the worm and reverse the changes made by the worm. This fix, however, is useless if the infected computer had been accessed by an attacker who installed other backdoors on the system that would be unaffected by the Code Red II patch tool. According to FedCIRC (Federal Computer Incident Response Center), due to the malicious actions of this worm, patching and rebooting an infected server will not solve the problem. The system's hard drive should be reformatted and all software should be reinstalled.
Technical Details of the Code Red II Worm	
The Code Red II worm also has three phases – preparation, propagation, and Trojan insertion. Based upon current analysis, Code Red II only affects Web servers running on the Microsoft Windows 2000 operating system platform**.**	
Phase 1: Preparation	During the preparation phase, the worm checks the current date to determine whether it will run at all. If the date is later than October 1, 2001, then the worm will cease to function and will remain infinitely dormant. If the date is before October 1, 2001, then all functions will be

Question	Answer
	performed. Although this discovery may bring hope that after October 1, 2001, this worm will no longer be a threat, this date constraint can be easily changed in a variant. The other activities conducted during the preparation phase include: • The functionality of Code Red II is dependent on both the system's environment and the current date. Code Red II checks the default system's language, e.g., English, Chinese, etc., and stores that information. • The worm also checks if the system has been previously infected, by searching for the existence of a specific file. If the file exists, then Code Red II becomes dormant and does not re-infect the system.[c] If the file does not exist, Code Red II creates the file and continues the process. • Preparation is finalized when the worm disables the capability of the Windows 2000 operating system to repair itself if it discovers that one of its required system files has been modified in any way. This becomes important during the Trojan Insertion function. Once the worm has completed the preparation phase, it immediately starts the propagation and Trojan insertion phases to complete infection.
Phase 2: Propagation	Code Red II creates hundreds of subprograms to propagate itself. The number of subprograms created depends upon the default language that the worm identified in the Preparation phsse. If the system's default language is Chinese, then 600 subprograms are created. If the default language is not Chinese, then 300 subprograms are generated. The propagation phase is unique because Code Red II seeks to copy itself to computers that are mostly near the infected system. The algorithm uses the infected system's own Internet address to generate a list of random Internet addresses. The generated list is comprised of Internet addresses that are closely related to the infected system. The rationale is that similar systems should reside in the "neighborhood" of the infected system, resulting in an increased chance of infection. Each of the subprograms is tasked with scanning one of the randomly generated Internet addresses to identify and infect another vulnerable system. Like Code Red, this worm uses the buffer overflow vulnerability to infect its target. Once a new target is infected, the process continues.
Phase 3: Trojan Insertion	Code Red II is more malicious than the Code Red worm discussed earlier, due to the existence of the Trojan horse backdoor programs that Code Red II leaves behind on the infected computer. The basic process follows: • Initially, executable files are copied to specific locations on the Web server, which by necessity, are accessible by any remote user. These executable files can run commands sent by a remote attacker to the server through the use of well-crafted Web commands. • A Trojan horse program is planted on the server that allows further exploit of the infected computer. The Trojan horse program is named after a required system program that executes when the next user logs into the system. It is also placed in a location that ensures that the Trojan horse program will be run instead of the required system program. Upon execution, the Trojan horse changes certain system settings that grant remote attackers read, write, and execute privileges on the Web server. • Twenty-four to forty-eight hours after the preparation function is initiated, Code Red II forces the infected system to reboot itself. Although the reboot eliminates the memory resident worm, the backdoor and the Trojan horse programs are left in place since they are stored on the system's disks. The reboot also restarts the IIS software, which, in turn, ensures that the Web server uses the newly compromised system settings.

Question	Answer
	Since the Trojan horse will always be executed each time a user logs on, Code Red II guarantees that remote attackers will always have access to the infected system. This is important, since even if the executable files copied at the beginning of the Trojan Insertion phase are deleted, the excessive privileges the Trojan sets at reboot are still in place. Therefore, the Trojan enables a remote attacker to perform similar exploits using these excessive privileges.

SirCam

Question	Answer
What is it?	SirCam is a malicious computer virus that spreads through E-mail and potentially through unprotected Windows network connections. What makes SirCam stealthy is that it does not rely on the E-mail capabilities of the infected system to replicate. Other viruses, such as Melissa and ILOVEYOU, used the host machine's E-mail program while SirCam contains its own mailing capability. Once the malicious code has been executed on a system, it may reveal or delete sensitive information. SirCam was first detected on July 17, 2001.
How does it spread?	This mass-mailing virus attempts to send itself to E-mail addresses found in the Windows Address Book and addresses found in cached files. It may be received in an E-mail message saying "Hi! How are you?" and requesting help with an attached file. The same message could be received in Spanish. Since the file is sent from a computer whose owner is familiar enough with the recipient to have their E-mail address in their address book, there is a high probability that the recipient will trust the attachment as coming from a known sender. This helps ensure the virus's success in the wild and is similar to the social engineering approach used by Melissa and ILOVEYOU. The E-mail message will contain an attachment that will launch the code when opened. When installed on a victim machine, SirCam installs a copy of itself in two files. It then "steals" one of the target system's files and attempts to mail that file with itself as a Trojan, that is, a file with desirable features, to every recipient in the affected system's address book. It can also get E-mail addresses from the Web browser. SirCam can also spread to other computers on the same Windows network without the use of E-mail. If the infected computer has read/write access to specific Windows network computers, SirCam copies itself to those computers, infecting the other computer.
Who is at risk?	Any E-mail user or any user of a PC with unprotected Windows network connections that is on the same Windows network as an infected computer.
What damage can it do?	SirCam can publicly release sensitive information and delete files and folders. It can also completely fill the hard drive of the infected computer. Furthermore, it can also lead to a decrease in the speed of the Internet. Specifically, It can cause security breaches by attaching randomly chosen documents to itself and then E-mailing them to other parties. This allows the worm to cause unauthorized disclosure of

Question	Answer
	confidential information. It can also delete files and folders. There is a one in twenty chance that an infected computer will have its hard drive erased or a one in fifty chance that the hard drive will be completely filled with garbage on October 16. It can create a file named C:\Recycled\sircam.sys which consumes all free space on the C: drive. A full hard drive prevents users from saving files to that drive, and in certain configurations impedes system-level tasks, such as saving files and printing. It can result in a denial of service attack by flooding E-mail systems with useless E-mail containing attachments of various sizes.
What do you do if you're infected?	Most anti-virus software vendors have released updated information, tools, or virus databases to help detect and partially recover from SirCam.
Technical Details of the SirCam Virus	
Actions performed once the user executes the attachment	• SirCam detaches itself from the E-mail attachment and attempts to execute its program file on the target machine. • It copies itself to several directories on the target system. • It then "steals" one of the target system's files and attempts to mail that file with itself as a Trojan to every recipient in the affected system's address book. It can also get E-mail addresses from the Web browser. The subject line and the attachment's name differ from E-mail to E-mail. The attached file is where the virus' malice lies: the infected E-mail's attachment has a name that matches the subject line and two extensions, the second being .exe, .bat, .com, .pif, or .lnk. For example, a Word file called SAMPLE.DOC could be attached to the E-mail as SAMPLE.DOC.EXE. • It can also delete files and folders. There's a one in twenty chance that an infected computer will have its hard drive erased and a on in fifty chance that its hard drive will be completely filled with garbage on October 16. In addition to E-mail propagation, SirCam can copy itself to other systems on the Windows network that have write-able access. SirCam will copy itself to those systems and rename itself to be a system file that will be executed upon the next system reboot.

[a]Buffer overflows occur when programs do not adequately check input for appropriate length. Thus, any unexpected input "overflows" onto another portion of the central processing unit's executions stack. If this input is chosen judiciously by a rogue programmer, it can be used to launch code of the programmer's choice.

[b]http://www.cert.org/advisories/CA-2001-19.html.

[c]A reported variant of Code Red II does reinfect the server.