GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Code Red: The One to Not "Dew"
David Doyle
August 2001 Version 1.2e

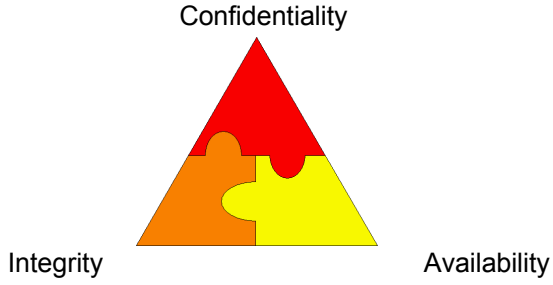
Introduction

On July 19, 2001 a worm propagated itself through the Internet to infect over 250,000 computers in an unheralded nine hours (1), causing a flood of data that slowed the Internet by 40 percent (2). The website Incidents.org, which is run by the SANS Institute and is designated to monitor network threats, jumped from a green to an orange threat level - which is the second highest threat level in their four level ranking system - due to the threat of the worm.

The worm, which was dubbed "Code Red" after the caffeinated cherry flavored Mt. Dew beverage that the members of eEye Digital Security consumed while decompiling the worm's code, is unique because it incorporates hacker techniques for attacking computer systems. Not only does the worm spread to other computers via random IP range scans, but it also has the ability to deface web pages, as well as launch a Distributed Denial of Service (DDoS) attack on an IP address which houses the Whitehouse web page.

C-I-A Model

Why has Code Red caused so much chaos and concern for security professionals and network administrators? The answer is found in the ultimate impact that the worm has had on what is often referred to as the "Three Bedrock Principles" of information security: confidentiality, integrity, and availability (C-I-A) (3).



- Confidentiality: the ability to confirm that data is only accessible by authorized parties or individuals.
- Integrity: the ability to authenticate data and confirm that it has not been corrupted or altered in any way.
- Availability: the ability to access the required information whenever it is needed (4).

When an attack is launched, the end result is to affect at the least one of these principles, although the more successful and damaging attacks are comprised of two or all three. In

© SANS Institute 2000 - 2005 Author retains full rights.

the case of Code Red, only integrity and availability were affected. However, it should be noted that new variants of Code Red have added confidentiality attacks as well.

The Code Red worm violated integrity through the defacement of many web pages. It also attempted to launch a distributed denial of service attack on the website of the Whitehouse, which constituted an availability breach.

Malicious Code

What is Code Red exactly? The Code Red worm is an example of malicious code. Malicious code is a program that is designed to perform some kind of hidden, destructive task on a computer system. While there are several types of malicious code that can infect computer systems, the most prevalent are viruses, worms, and Trojan horses (5).

- Virus: program code that replicates by infecting other innocuous programs. It is important to note that a virus *must* attach itself to something in order to infect and spread.
- Worm: program code that infects other systems through an exploit or flaw in valid code. Unlike a virus, a worm does not attach to anything, allowing it to replicate further and faster than a virus.
- Trojan horse: program code that looks as though it is a valid application, but performs another malicious program in the background without the user's knowledge (6).

Although worms are often mistakenly called viruses, there is a fundamental difference. A virus is only able to replicate if it has a host to attach itself to. On the other hand, a worm is able to replicate and connect to many computer systems through a programming flaw in programs or operating systems. Virus experts Rosenberger and Greenberg make the distinction between a virus and a worm as follows: "If the Trojans had left that wooden horse outside the city, they wouldn't have been attacked from inside the city. Worms, on the other hand, can bypass your defenses without having to deceive you into dropping your guard. (5)"

Another "In"-Famous Worm

Is the Code Red worm the most damaging worm to date? Until recently, the most well publicized Internet worm was the Morris Worm. In November 1988 a twenty-three year old doctoral student from Cornell named Robert Morris created an experimental, self-replicating program that exploited a flaw in the UNIX programs *sendmail* and *finger daemon* (7) that brought approximately sixty thousand university and military computers to a halt (8).

The Internet is filled with more information regarding the Morris worm. If you are interested in learning more, check out the book "Cybepunk: Outlaws and Hackers on the

© SANS Institute 2000 - 2005 Author retains full rights.

Computer Frontier" by Hafner and Markoff which has an interesting case study, (9) or perform a search using your favorite Internet search engine for the Morris Worm.

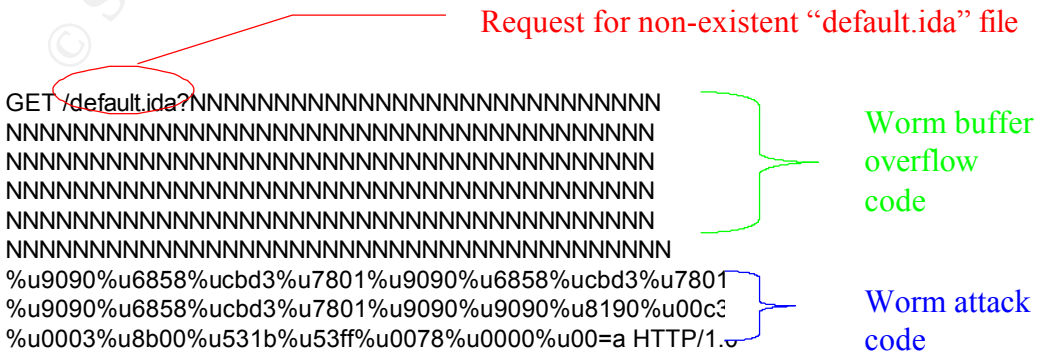
The Exploit

The vulnerability which Code Red exploited was first discovered by eEye Digital Security's security professional Riley Hassell on June 18, 2001, while running some test security scripts on IIS web servers (10). The original report of the findings, the detailed deep analysis, and the complete worm disassembly can be found at eEye's web site.

How does Code Red infect a system? The Code Red worm is able to infect a system though an exploit technique known as a buffer overflow. Buffer overflows are flaws in software program code that are due to poor programming. Files that are vulnerable to such attacks often allow the worm's code to run with elevated privileges. What that means is that files and services run with different privileges, which are defined by the operating system. Through the use of the privileges, the operating system is able to define which tasks are more important than others, and consequently take priority over less privileged services. The highest level a service can run in is known as *system* level. In the case of the Code Red worm, a buffer overflow exists in the IIS indexing service .dll file that allows the worm's code to run with system level privilege, allowing the worm code to do whatever it wants. In the case of this worm, the buffer overflow exists in the idq.dll file, which is one of the Internet/Indexing Service Application Programming Interface (ISAPI) extensions (11).

The Code Red worm consists of two parts, the exploit and the payload. An exploit is defined as "A sequence of actions or a program that enables an individual to take advantage of, or exploit, a vulnerability or security weakness in a program or system" (12). In this case the exploit is executed by performing an HTTP GET request through port 80 to an IIS server looking for a non-existent file named "default.ida" followed by both the code to cause the buffer overflow and the malicious code to perform the attacks.

A sample of part of the worm is listed below. It should be noted that the code actually runs as one continuous line, but was broken down to make it easier to read (13).



© SANS Institute 2000 - 2005 Author retains full rights.

When the system could not find the "default.ida" file explicitly, it instead looked at the file's extension. Due to a file association for .ida files, the system made a call to the flawed idq.dll, which runs as a system level privilege. Once the jump was made to idq.dll, the malicious code was able to execute at will.

The Payload Code

Once the Code Red worm successfully exploits the idq.dll vulnerability by overflowing the buffer, the service crashes, and when it is restarted the remaining worm code is designed to initiate the "payload" and perform three main tasks:

- Propagate over the Internet: scan IP range for systems with the same vulnerability and launch the buffer overflow attack
- Deface web page: if the IIS server is running an English version of the software, then the worm will deface the web page with a message "Hacked by Chinese"
- Launch DDoS attack: at a pre-programmed time and date, launch a flood of data to cause a distributed denial of service attack against an IP address that serves the Whitehouse's home page

Is it just Microsoft?

While much of the hype has centered on Microsoft's IIS servers, the worm has also affected some of Cisco's products that run versions of IIS as well. The advisory is available at http://www.cisco.com/warp/public/707/cisco-code-red-worm-pub.shtml.

Are you Vulnerable?

How do you know if you are vulnerable? Only Microsoft Windows NT 4.0 and Windows 2000 computer systems that are running Internet Information Server (IIS) 4.0 and 5.0 and some Cisco products are vulnerable. In addition, it is possible that there are some systems with XP beta that could also be running the IIS service that can be affected. Systems running Windows 95, 98, and ME, which are mostly operating systems that are used by home users, are not vulnerable to the Code Red worm (14).

Fortunately there is help in determining if an IIS server is vulnerable to this type of attack. A tool has been issued named the CodeRed Scanner that performs a scan of up to 254 IP addresses to determine if there are any servers running the .ida vulnerability. When it finds a system that is vulnerable, it flags it in a report so that an administrator can run the patch. In addition to the CodeRed Scanner, Microsoft is due to release a tool, named Prefix, which will search programs for security holes (15).

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

How to Protect Yourself

What can be done to protect systems against Code Red? The first and most important step that needs to done, after confirming that the system is vulnerable, is to download and install the patch from Microsoft's web site. There are actually two versions that are available, one for the Windows NT operating system and one for Windows 2000.

It is also advisable to un-associate all indexing services for IIS so as to prevent possible future exploits. There are also a number of internet web sites that provide step-by-step guidance on determining if a system is vulnerable, as well as providing a patch installation and system cleansing walkthrough via MP3 audio, PowerPoint, and Adobe PDF formats.

The amount of camaraderie in the community has been outstanding. With the tireless efforts of individuals from The SANS Institute, eEYE Digital Security, NIPC, Digital Island, Microsoft, CERT/CC and many others, information regarding the worm and how to protect vulnerable systems has been widely distributed.

Another way of protecting yourself from exploit attacks and other vulnerabilities is to have the knowledge of them as soon as possible. Fortunately, there are numerous resources that are freely available that can assist in providing up-to-the-minute information and analysis of new exploits and vulnerabilities. By subscribing to these mailing lists and periodically checking these sites, administrators can have the knowledge of what and how to better protect themselves from malicious attacks.

The Variants

At present there are three variants of the Code Red worm. Unfortunately, these new strains have a more efficient algorithm used to scan IP addresses and contain an even more damaging payload (16). In addition to compromising the integrity and availability of the system, these new variants also affect the system confidentiality through the installation of backdoors that allow remote attackers to further compromise the system, as well as launch new attacks against other remote systems.

The best method for protecting yourself from these new variations is to install Microsoft's patch. It is also advisable for system administrators, information technology professionals, and security professionals to make a habit of periodically checking resources such as NIPC's Cybernotes, CERT Advisories, Microsoft Security Bulletins, SANS security newsletters, and countless others that are freely available, to assist in providing information regarding new and current security flaws. In addition, some organizations can update their Intrusion Detection Systems (IDS) signature pattern files to include the initial worm code.

© SANS Institute 2000 - 2005 Author retains full rights.

Lessons Learned

The Code Red worm and its variants are rumored to have infected more than 300,00 systems to date, and it can only be guessed as to how many systems may be affected in the future. Could such a massive propagation of the worm have been prevented? Most security professionals would emphatically agree that "Yes", the spread of the worm could have been significantly reduced to a much smaller number of computer systems being infected if system administrators had installed the Microsoft patch in a timely manner. One of the most simple, and often times overlooked, methods that administrators and network professionals can use to protect themselves from malicious network attacks is to keep up-to-date with software patches and hotfixes. It is through the amazing swiftness of the spread of Code Red that this hits home.

Not only is it imperative to patch systems, but it's equally important to keep abreast of the latest exploits in a real-time manner. Utilizing free newsletters and web sites devoted to providing comprehensive information and helping to fix security flaws are vital resources. There is one caveat; they have to be used to be effective.

References

1. "Code Red Worm." Alert 01—016. 29 July 2001. URL: http://www.nipc.gov/warnings/alerts/2001/01-016.htm. (16 August 2001).

2. Barrett, Randy. "Code Red Expected to Resurface." 30 July 2001. URL: http://www.zdnet.com/filters/printerfriendly/0,6061,2799957-35,00.html. (16 August 2001).

3. Cole, Eric. SANS Security Essentials, Part 1. Baltimore: SANS Institute, May 2001

4. "Overview of Information Security in General." URL: http://uk.geocities.com/picocosm/overview.html. (16 August 2001).

5. Tipton, Harold F. / Krause, Micki. Information Security Management Handbook, 4th Ed. Boca Raton, Florida: CRC Press LLC, 2000. 513-515.

6. Pfleeger, Charles P. Security in Computing, 2nd Ed. Upper Saddle River, New Jersey: Prentice Hall PTR, 2000. 176-179.

7. "The Robert Morris Internet Worm." URL: http://www.swiss.ai.mit.edu/6805/articles/morris-worm.html. (16 August 2001).

8. "The Lessons of the Worm." URL: http://www.software.com.pl/newarchive/misc/Worm/darbyt/pages/lessons.html. (16 August 2001).

© SANS Institute 2000 - 2005 Author retains full rights.

9. “6.805/STS085: Readings on Computer Crime.” URL: http://www.swiss.ai.mit.edu/6805/readings-crime.html. (16 August 2001).

10. “All versions of Microsoft Internet Information Services Remote buffer overflow (SYSTEM Level Access).” 18 June 2001. URL: http://www.eeye.com/html/Research/Advisories/AD20010618.html. (16 August 2001).

11. “Ida Code Red Worm.” Advisory 01-015. 19 July 2001. URL: http://www.nipc.gov/warnings/advisories/2001/01-015.htm. (16 August 2001).

12. Glossary. URL: http://www.securtyfocus.com. (16 August 2001).

13. “.ida Code Red Worm.” 17 July 2001. URL: http://www.eeye.com/html/Research/Advisories/AL20010717.html. (16 August 2001).

14. “Code Red Worm InfoSec Bulletin.” URL: http://www.digitalisland.net/codered. (16 August 2001).

15. Babcock, Charles. “Microsoft Plugs IIS Security Holes.” 26 June 2001. URL: http://www.zdnet.com/filters/printerfriendly/0,6061,2779701-54,00.html. (16 August 2001).

16. Irwin, Vicki. “Handler’s Diary.” 30 July 2001. URL: http://www.incidents.org/diary/diary.php. (16 August 2001).

© SANS Institute 2000 - 2005 Author retains full rights.