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 Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

Code Red: A New Threat

Tim Hughes

GSEC Practical Assignment 1.2e

August 28, 2001

Introduction

Since the death of Chinese fighter pilot Wang Wei, U.S. websites have been under an increased threat of attack from Chinese hackers. In early May, numerous U.S. Government and Corporate websites were defaced in retaliation for the pilot's death. The U.S. Geological Survey, Federal Emergency Management Agency, and the U.S. Department of Labor are just a few of the sites that have been defaced in this apparent cyberwar. Most of these sites were defaced with messages denouncing the U.S. Government and have been linked to hacker groups within China. [1] Additionally, federal investigators have linked the Lion Worm to China. This worm propagates by attacking the BIND DNS service on vulnerable servers and sending the systems password files to an E-mail address in China. [2]

Worms, like the Lion worm, differ from viruses in that they propagate without user intervention, and do not infect individual files on a system. [3] Viruses, on the other hand, typically infect executable files and require the user to pass the infection to additional systems. [4] The worm style of compromise can spread rapidly, and be exceedingly effective in infecting multiple computer systems depending upon the vulnerability being exploited. This type of infection is demonstrated quite well with the Code Red and Code Red II worms.

Seeing Red?

According to CERT/CC ®[1], the first Code Red infections are believed to have appeared around July 13, 2001. There are believed to be at least two variants of the Code Red worm actively attacking systems on the internet by exploiting a known vulnerability in Microsoft's IIS Webservers. This is a rapidly moving virus that has been recorded as infecting more than 250,000 systems in just over 8 hours. [4]

On July 20, 2001, the Symantec Antivirus Research Center upgraded the Code Red worm to a level 3 virus threat due to the number of reported submissions of system compromise.[2] SARC categorizes the threat from this worm to be a high rate of infection with moderate damage to the system. The virus is known to degrade system performance, utilize network bandwidth, and can cause system instability. [5]

Additionally, at the beginning of August 2001, a new variant of the Code Red worm appeared for the first time. According to Symantec, on August 4, 2001, the worm Code Red II was discovered. This variant of the Code Red worm is considered to be a high threat. This worm is considered to be a variant of the Code Red worm as it uses the same exploit to infect new systems. However, the payload of the worm has

© SANS Institute 2000 - 2005 Author retains full rights.

been modified. This new worm infects the target systems with a rootkit giving a remote attacker the ability to remotely control the server. [7]

The Vulnerability

The Code Red worm utilizes a known vulnerability in the Microsoft IIS Indexing service to infect remote machines. On June 18, 2001, Microsoft release a security advisory detailing the vulnerability used by the Code Red worm. According to Microsoft, as long as the mappings for the .ida and .idq extensions used by the Microsoft Indexing services are present on a system with a vulnerable idq.dll file, the indexing service does not even need to be running for the server to be exploited. The cause of this is a buffer overflow that is executed before the server receives any indexing commands.

A buffer overflow is one of the most widely seen vulnerabilities. They typically result from programs not checking the size of the data being placed into variables in the program. These variables are usually of a predetermined size, and store their values in memory buffers. If the program does not check the size of the data being placed into these variables, it is possible for the data to “overflow” the predetermined size and write the data to adjacent areas of the computer buffer. This buffer overflow can possibly allow malicious users to run arbitrary commands on the remote system. [8]

The result of this unchecked boundary condition is an exploitable hole that can be used by attackers to compromise the system. This condition exists in Microsoft IIS 4.0, 5.0, and the IIS Server found in Windows XP. Microsoft has had a patch for this issue since June 18, 2001. [9]

Code Red utilizes the vulnerability by connecting to web servers and making an HTTP request. This request exploits the Indexing Service buffer overflow and allows the worm to compromise the system. Once the worm exploits this hole, it does not modify any files, but it does recreate itself and run in the system’s memory. [5] However, Code Red II does modify the file and operating system of the infected systems. It modifies the Windows Registry and installs a "trojaned" explorer.exe executable file. [10]

Worm Propagation

According to both CERT and SARC, once the Code Red worm infects a system, it spawns multiple threads. These threads first check for the file “C:\notworm”. If this file exists, the threads are placed into an infinite sleep state. If this file does not exist, these threads begin the process of propagation. [11] [5]

Once activated, the threads are programmed to perform different actions depending upon the day of the month. At the beginning of the month (Day 1-19), the

© SANS Institute 2000 - 2005 Author retains full rights.

worm threads randomly attempt to connect to web servers on the Internet and exploit additional hosts. On Days 20-27, the worm threads actively attack 198.137.240.91. This was the former location of www.whitehouse.gov. This site has been moved to a new IP address, and the old IP address is inactive at the moment. At the end of the month, (Days 28- End of Month) the worm's threads go into a sleep state and are inactive. [11]

Additionally, when the threads of one of the two known variants of Code Red run, they will "hook" into the web server and return web page requests with its own HTML code. This code responds to request with the display of:

"Welcome to http://www.worm.com !
Hacked by Chinese!" [5]

This defacement lasts for 10 hours; however, other threads can attach to this web server hook and reinitiate the defacement of the webserver.

In contrast, Code Red II attempts to infect other computer for only 24-48 hours after infection. If the infected system has the language set to Chinese, the worm spawns 600 threads that it uses for the next 48 hours to aggressively scan for vulnerable systems. For other languages, the worm only spawns 300 threads that only scan for vulnerable hosts for 24 hours. After the scanning time period, the infected host will reboot. Additionally, the Code Red II worm contains code that sets a time limit on the spread of the worm. This limit will stop the worm from spreading after October 1, 2001. However, any infected systems will continue to be infected by the Trojan payload carried by the Code Red II worm. [10]

The Trojan Horse payload of the Code Red II worm performs multiple actions affecting the file system and windows registry of an infected system. First, it disables the Windows System File Checker (SFC). It then modifies multiple registry keys to install new Virtual Root directories into the Web Server as well as setting the user group to "217". At this time the Trojan copies the file "cmd.exe" to the scripts and MSADC folders of the web server. It also puts a "trojaned" copy of "explorer.exe" in the root directory of the server. At this point, the Web Server has been compromised, and a remote attacker can issue arbitrary commands to the server. [7][10]

Detection and Removal

The Code Red worm can only be detected by scanning the system in question's memory, as the worm does not directly modify any files. The best method of removal for this virus is to download and install the security patch from Microsoft and reboot the infected system. According to Symantec, this is the recommended method for removing the worm. [5] The patch can be obtained from Microsoft at the following URL: [9]

For Windows NT 4:
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=30833
For Windows 2000 Professional, Server, and Advanced Server:
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=30800

© SANS Institute 2000 - 2005 Author retains full rights.

In addition to the patches from Microsoft to fix the buffer overflow vulnerability, the Code Red II worm requires registry and file system changes to completely remove the Trojan. The following files must be removed from the infected system: [10]

"\inetpub\scripts\root.exe"
"\program files\common files\system\MSADC\root.exe"
"\explorer.exe"

Subsequently, the following registry entries must be modified to remove the "217" user group from the web server. The added ",217" string must be removed from the following registry locations: [10]

Hive: HKEY_LOCAL_MACHINE
Key: SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots\Scripts
-and-
SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots\MSADC

Finally, the following registry keys must be completely removed: [10]

Hive: HKEY_LOCAL_MACHINE
Key: SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots\C
-and-
SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots\D

Dangers

As the Code Red worm has shown, leaving system vulnerabilities un-patched is potentially catastrophic for system administrators. Code Red has been shown to be highly effective in propagating across the Internet. Consider the impact of the Code Red and Code Red II worms. Both worms have managed to infect hundreds of thousands of systems worldwide. With many of these systems remaining un-patched and infected, attackers have access to thousands of systems from which they can launch additional attacks and/or steal data.

Also, through it's behavior, Code Red II has created a new reason for System Administrators to maintain adequate security countermeasures. Prior to Code Red's release, worms and viruses had typically propagated through scripting and programming languages found on the target operating systems. With the release of Code Red into the wild, administrators were exposed to the first worm that used a hacking technique to propagate between systems. With the release of Code Red II, the public was exposed to a worm that used the same propagation method, but installed a backdoor program to compromise the security and integrity of the infected system. Code Red II effectively became an automated hacking tool that could be used to compromise any vulnerable system.

Additionally, these worms have shown once again the need for system administrators to continually keep abreast of the security patches available for their systems. Microsoft was aware of the problem, and promptly created a security patch to this vulnerability. They also, in good faith, attempted to warn their users through the posting and sending of a security bulletin detailing the vulnerability with instructions on receiving and installing their security patch. This vulnerability and patch were both

© SANS Institute 2000 - 2005 Author retains full rights.

known and published for approximately one month before Code Red exploited this hole. The widespread infection of this worm only underlines the need for system administrators to maintain their security awareness. [9]

Also, the burden of security awareness cannot only be solely placed upon Windows system administrators. The Lion worm highlighted the same informal security attitude common among all system administrators, including Unix administrators. Many of the systems compromised by the Lion worm were running versions of Bind that were months out of date. Operating system and network service security need to be pro-actively monitored to avoid widespread compromise of host systems.

Protecting your systems

As an organization or individual, there are many different ways that you can increase the security of the systems under your control. An effective methodology to protect operating systems and services makes use of the Defense in Depth paradigm. This strategy involves layering your security so that multiple defenses are used in protecting points on your network. [12]

In regards to virus and worm protection, a Defense in Depth strategy could involve multiple different facets of the problem. An important first step in defining a defensive strategy is to formulate a personal or corporate policy to cover the topic. A good Anti-Virus policy will cover the non-technical details regarding virus protection in your environment. This policy should cover which systems require specific software to ensure protection. Also, it should outline the responsibilities for providing updates to the software. Additionally, this policy will cover the responsibilities for incident handling and response. Finally, auditing your anti-virus installation is a needed step to ensure compliance with the policy.

From this policy, technical guidelines for proper installation and configuration of the Anti-Virus software should be created. These guidelines should provide the detailed instructions on managing the Anti-virus software. As most of the major Anti-virus vendors publish free virus database updates regularly, the scheduling of these updates should be covered in these documents. This is a major step in preventing the spread and infection systems by common viruses and worms. Additionally, technical details on how to conduct and document audits of the anti-virus system are crucial to maintaining a secure virus free environment. Guidelines should also be prepared for incident handling and response. This provides a framework of steps that can be practiced to ensure proper response to a worm or virus incident.

Consequently, there should also be a policy put into place regarding general network security. This document should cover the responsibilities for maintaining the operating systems and network services from a security perspective. It should provide non-technical details regarding the responsibilities for system security, and incident handling and response.

© SANS Institute 2000 - 2005 Author retains full rights.

Again, there should be technical guidelines drawn from this policy to provide details on how to properly secure systems and services within the operating environment. Detailed installation checklists that cover hardening the operating system and services should be created to provide a standardized operating environment. Periodic audits of systems and services need to be performed to ensure compliance with the created standards. Security incident handling and response procedures should be created and practiced to ensure proper handling of security violations.

Additionally, system administrators need to keep up to date on the latest anti-virus and security information. Lists of sites to be regularly checked for new information should be created. The latest virus and worm information can be found at the following sites:

Symantec Antivirus Research Center (SARC)
http://www.symantec.com/avcenter/index.html
McAfee Virus Information Library
http://vil.mcafee.com/
Trend Micro Virus Information Center
http://www.antivirus.com/vinfo/
F-Secure Security Information Center
http://www.f-secure.com/virus-info/

Also, the following security mailing lists regularly provide information regarding exploits and patches to operating systems and services. Information regarding the following mailing lists can be found at the following links:

Bugtraq
http://www.securityfocus.com/forums/bugtraq/intro.html
NTBugtraq
http://www.ntbugtraq.com/
Microsoft Security Bulletins
http://www.microsoft.com/technet/security/
RedHat Linux Mailing List Archives
http://www.redhat.com/mailing-lists/

Conclusion

The Code Red worms provided another example of a known security hole being widely exploited after fixes to the vulnerability had been made available. Due to many unknown reasons, available patches were not applied to vulnerable systems. This allowed the worm to propagate more than a month after fixes to this vulnerability were made publicly available. However, people and organizations can minimize their risk of being affected by similar vulnerabilities by following an in-depth defensive strategy. Through education and vigilance, the impact of viruses and worms like Code Red can be contained and the damage kept to a minimum.

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

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

© SANS Institute 2000 - 2005 Author retains full rights.

References

1. Costello, Sam. "U.S., Chinese hackers continue Web defacements." CNN.com/Sci-tech. May 2, 2001. URL: http://www.cnn.com/2001/TECH/internet/05/02/china.hacks.idg/index.html (7/28/01)

2. Kasadra, Austin. "The Lion Worm: King of the Jungle?" SANS Information Security Reading Room. April 5, 2001. URL: http://www.sans.org/infosecFAQ/malicious/lion.htm (7/28/01)

3. "Worm – a searchSecurity definition." SearchSecurity.com Dictionary. URL: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci213386,00.html (7/28/01)

4. "CERT® Advisory CA-2001-23 Continued Threat of the "Code Red" Worm." CERT Advisories. URL: http://www.cert.org/advisories/CA-2001-23.html (7/28/01)

5. "SARC Write-up – CodeRed Worm" Symantec Antivirus Research Center. URL: http://www.symantec.com/avcenter/venc/data/codered.worm.html (7/28/01)

6. "Symantec Security Updates – Threat Severity Assessment Page" Symantec Antivirus Research Center. URL: http://www.symantec.com/avcenter/threat.severity.html#category (7/28/01)

7. "SARC Write-up – CodeRed II" Symantec Antivirus Research Center. URL: http://www.symantec.com/avcenter/venc/data/codered.ii.html (8/28/01)

8. "Glossary" Security Focus URL: http://www.securityfocus.com/templates/glossary.html?let=b (8/28/01)

9. "Microsoft Security Bulletin MS01-033." Microsoft Technet Security. URL: http://www.microsoft.com/technet/security/bulletin/MS01-033.asp (7/28/01)

10. "F-Secure Computer Virus Information Pages: Code Red" F-Secure Corporation URL: http://www.europe.f-secure.com/v-descs/bady.shtml (8/28/01)

11. "CERT® Advisory CA-2001-19 "Code Red" Worm Exploiting Buffer Overflow in IIS Indexing Service DLL." CERT Advisories. URL: http://www.cert.org/advisories/CA-2001-19.html (7/28/01)

12. McIntyre, William A. "Defense in Depth – A Critical Case Study of a Large Enterprise." SANS Information Security Reading Room. May 31, 2001. URL: http://www.sans.org/infosecFAQ/casestudies/large_enterprise.htm (7/28/01)

© SANS Institute 2000 - 2005 Author retains full rights.

[1] While the initials "CERT" do not stand for any acronym, the group based out of Carnegie Mellon University was originally known as the Computer Emergency Response Team. CERT/CC stands for the CERT Coordination Center. CERT and CERT/CC are registered trademarks of the Software Engineering Institute operated by Carnegie Mellon University for the Department of Defense.

[2] SARC, the Symantec Antivirus Research Center, categorizes viruses and worms on a threat scale of 1-5. This categorization is an approximate risk level with Level 1 being "very low" and Level 5 being "very severe". These risk levels are based upon how active the virus is in the wild, and how much of a threat to individual systems the virus or worm corresponds. [6]

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

Last Updated: May 1st, 2017

Upcoming Training

Click Here to
{Get CERTIFIED!}

SANS Riyadh 2017	Riyadh, Saudi Arabia	May 06, 2017 - May 11, 2017	Live Event
SANS Security West 2017	San Diego, CA	May 09, 2017 - May 18, 2017	Live Event
SANS Northern Virginia - Reston 2017	Reston, VA	May 21, 2017 - May 26, 2017	Live Event
SANS Melbourne 2017	Melbourne, Australia	May 22, 2017 - May 27, 2017	Live Event
SANS London May 2017	London, United Kingdom	May 22, 2017 - May 27, 2017	Live Event
SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
Community SANS Philadelphia SEC401	Philadelphia, PA	Jun 19, 2017 - Jun 24, 2017	Community SANS
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS