Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

What is Code Red Worm?

Code Red worm can be viewed as a new generation of Internet worm that took the Internet and security community by surprise. Now there exist a few versions of Code Red worm and each new version proofs to be more malicious then the original Code Red worm. This should serve as a strong motivation for businesses and corporations alike to beef up their system's defense. Prevention is much more cost effective than cure, especially for mission critical systems. A flexible, defense-in-depth strategy that allows adaptation to t...

Copyright SANS Institute
Author Retains Full Rights

AD
ONLY ONE INDEPENDENT TEST
MEASURES REAL-WORLD,
ENDPOINT MALWARE PROTECTION.
TREND MICRO SMART PROTECTION NETWORK

What is Code Red Worm?

Adrian Tham

Aug 4, 2001

Internet Worm

The term Internet worm brings to mind the first notorious worm, Morris Worm. A fast self-replicating worm that crippled almost 10 percent of the computer connected to the Internet in Nov 1988[14]. This worm took advantage of exploits in Unix's sendmail, and finger daemon to propagate over the Internet. Though Morris worm could only successfully attack Sun and VAX system which run on Berkeley Unix code, it has caused great damage because these machines made up a large percentage of the Internet.

These days, most of the headlines on security breaches focus on viruses, for example Love Letter and SirCam viruses. What is a virus? A virus is a program that requires human interaction to spread itself around. A virus is usually introduced to a computer through an e-mail attachment, or from a disk inserted into a computer. A virus is different from a worm. According to RFC 1135: A worm is a program that can run independently, will consume the resources of its host from within in order to maintain itself, and can propagate a complete working version of itself on to other machines [15].

On July 13 2001, the administrators and the computer security community were given a loud wakeup call. A new worm was detected and was spreading rapidly to systems connected to the Internet. This fast replicating worm known as the 'Code Red Worm' took advantage of a flaw in Microsoft Internet Information Server (IIS) to manifest itself. This vulnerability was reported a month before Code Red worm was discovered on the Internet. Many administrators were either not aware of the vulnerabilities' existence or were not prepared for the attack. This gave rise to the mass disruption on the Internet traffic. According to CERT/CC, an estimate of more than 250,000 systems were infected in just 9 hours [2].

What is Code Red Worm?

"Code Red Worm", also known as I-Worm.Bady and W32/Bady.worm from Symantec Antivirus Research Center [19], is a self-replicating malicious code that exploits a known vulnerability in IIS servers. Once it has infected a system, it multiplies itself and it begins scanning random IP addresses at TCP port 80 looking for other IIS servers to infect. At the same time, the home page of infected machines will also be defaced. In addition, it does a denial of service attack on a particular IP address, previously was www.whitehouse.gov within certain timeframe, but later a variant were discovered that does not deface webpage on the infected host.

Quoted in Information Assurance Foundations discussion, vulnerabilities are the gateways by which threats manifest. Let's look at the vulnerability discovered in the IIS server, follow by the worm operation.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Vulnerability in Microsoft Windows IIS Index Server ISAPI extension
On June 18, 2001 eEye Digital Security [8] reported that the existence of a remote buffer overflow vulnerability in all version of IIS Web server software.

Using the default Internet Information Server installation process, several Internet Service API (ISAPI) extensions or dynamic linked libraries were included. One of extension mapping, idq.dll is a component of Index Server (known as Indexing Service in Windows 2000) and it provides support for administrative scripts (.ida files) and Internet Data Queries (.idq files). The indexing server 2.0 and indexing services provide full-text search and indexing service to search data on a web server or site.

Security vulnerability was discovered in “idq.dll” (Indexing service). The ISAPI filter does not perform proper “bounds checking” on user inputted buffers. A remote attacker connecting to the server can initiate an attack that will overflow the buffer. This will cause either a Denial of Service on the server, or introduce a code to run on the targeted server. Such code running in the Local System security context would give the attacker completes control of the server, thus enabling them to take virtually any action on the target server they chose, including changing web pages, reformatting the hard drive or adding new users to the local administrators group.

The vulnerable index service ISAPI are the affecting the following systems:

- Microsoft Windows NT 4.0 IIS Services 4.0,
- Microsoft Windows 2000 IIS Services 5.0,
- Microsoft Windows XP beta IIS Services 6.0 beta

Extensive reports can be obtained in CIAC Bulletin L-098, Microsoft Index Server ISAPI Extension buffer Overflow [1] and Microsoft Security Bulletin MS01-033, Unchecked Buffer in Index Server ISAPI Extension Could Enable Web Server Compromise [11].

Code Red Worm Operation

The following lists the first version of Code Red worm operation:

1. The worm attempts to connect to TCP port 80 on a randomly selected host assuming that web server will be found. Upon successfully connected, the attacking host sends a HTTP GET request to the victim. That request exploits the buffer overflow vulnerability causing the worm to be executed on the system. The worm is not written to disk but injected and executed directly from memory. The beginning of the worm's attack packet looks like the following:

```
GET/default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNN%u9090%u6858%ucbd3%u7801%u9090%u6858%ucb
d3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003%u
8b00%u531b%u53ff%u0078%u0000%u00=a
```

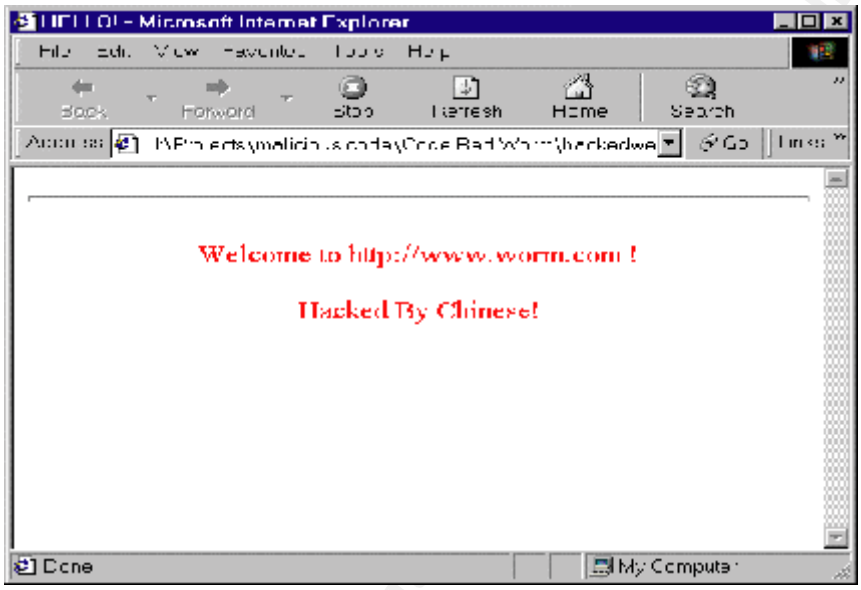
2. Once executed, the worm checks for the file c:\notworm. If the file exists, the thread goes into an infinite sleep. If the c:\notworm file does not exit, new threads are then

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

created. Each thread may cause another thread to be spawned causing continually thread creation to a number of 100.

3. The next 99 threads attempt to exploit more systems by targeting random IP addresses, if the date is before 20th of the month.

4. The 100th thread of the worm code defaces the web server's homepage if the system's default language is US English. Firstly, the thread sleeps for 2 hours and then hooks a function which response to HTTP requests. That link is then pointed to worm code that produces the web page as shown below. The changes in the home page is not done by changing the home page in the physical disk files, but is done by the code in the memory. This hook lasts for 10 hours and is then removed.



5. If the date is between the 20th and 28th, the active threads then attempt a Denial of Service attack on a particular IP address 198.137.240.91 (once was www.whitehouse.gov) by sending a large amount of junk data, 98,304 packets.

6. If the date is greater than 28th, the worm's threads are directed into an infinite sleep.

Detail analysis of the worm can be found in the following locations:

- URL: http://www.eeye.com/html/Research/Advisories/AL20010717.html
- URL: http://www.securityportal.com/research/virus/profiles/codered.html

Reported in Handler's Diary [9], second variant of the CODE RED worm has been captured within a short period after the first was released in the Internet. The differences are:

1. It uses Time-based randomness to select a list of target IP addresses;
2. Web page defacement has been disabled.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

These changes have made the worm more effective in spreading since it does not restrict itself to a set of IP addresses. And also target user might not be aware that its IIS is under attack because there is no physical view on the infected IIS server that the worm is present.

A new version of Code Red worm known as Code Red II was discovered on 4 Aug 2001, uses the same "buffer overflow" exploit to propagate to other web servers. According to eEye Digest Security, Code Red II has a different payload than the original worm [6].

1. It creates a back door process on the infected machine by copying a command shell 'CMD.exe' to a externally accessible location,
2. It also leaves a trojan 'explorer.exe' on the root directory,
3. Its propagation rate has also increased tremendously. If the system is a Chinese IIS server, the worm creates 600 threads and attempts to spread for 48 hours. If the system is a non-Chinese IIS, the worm creates 300 threads and attempts to spread for 24 hours. After the infection-spreading interval, the system is forcibly rebooted. The reboot flushes the memory resident worm, and leaves the backdoors and the explorer.exe trojan in place.

Mitigations

Online advises on how to remove the vulnerability are available in many security sources such as Digital Island, National Infrastructure Protection Center, Symantec, CERT® Advisory, SecurityPortal.com.

Generally using a standard anti-virus program may not be an effective solution to detect and remove this worm because the worm exists only in memory on a system and it does not write to disk. There are some free tools available on the Internet to check if the IIS is vulnerable. Such examples would be the program called "FixCodeRed" from Symantec that warns of vulnerable systems and scan memory to detect traces of the Code Red worm. Another such program "CodeRed Scanner" from eEye Digital Security .

A normal system reboot will remove the worm and restore the system. However, due to the large number of infected systems and the fact that they may attack the same list of IP addresses again, there is a high chance that a system will be re-infected as soon as it reboots. An effective way of removing the threat is to locate the causes of the vulnerability. The following is a suggestion to protect the system

1. Disable .ida, .idq, and for all other script mappings that are not explicitly required by IIS and
2. Patch the .ida processor.

If the system does not require the index server, .ida processing should be disabled. CIAC Bulletin L-117 has defined the steps to test a server on whether the .ida processing is enabled [2]. TruSecure, Alert- TSA-01-020 [22] lists the steps to remove the script mapping for .ida, .idq, and for all other script mappings that are not explicitly required in IIS. One must aware that disabling .ida should be a temporary solution until the patch can

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

be installed. This is because future additional Windows's component installation could possibly reactivate the .ida.

Apply the MS IIS patch to remove the Code Red problem -
Windows NT version 4.0:
URL: http://www.microsoft.com/Downloads/Release.asp?ReleaseID=30800
Windows 2000 Professional, Server and Advanced Server:
URL: http://www.microsoft.com/Downloads/Release.asp?ReleaseID=30833
Step-by-step instructions for these actions are posted at URL:
http://www.digitalisland.net/codered

Additional information about the patch, its installation, and the vulnerability is available at follow URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-033.asp.

Some of the Internet devices listen on port 80 may be vulnerable to the attack or denial of services due to port scan. Cisco has made patches available to remedy this vulnerability at URL: http://www.cisco.com/warp/public/707/cisco-code-red-worm-pub.shtml

Conclusion

Code Red worm can be viewed as a new generation of Internet worm that took the Internet and security community by surprise. The last such attention-grabbing worm was detected 13 years back, known as the Morris worm. Now there exist a few versions of Code Red worm and each new version proofs to be more malicious then the original Code Red worm. This should serve as a strong motivation for businesses and corporations alike to beef up their system's defense. Prevention is much more cost effective than cure, especially for mission critical systems. In order to build up a bullet proof system, I would look into 3 basic concern:1) Corporate security policies 2) Security professionals practices 3) Tools to enforce security protection.

When a company adopts certain software, it is unlikely to have a 100% guarantee that the software is free of flaws. Reason being that the software may contain inherent flaws that were not identified at the time it is released to the market. Proactively identifying security loopholes and enforcing the effective and timely patching of the flaws is a prerequisite to ensure the security of the system. Microsoft provides Internet Information Services checklist for the IIS users to find the available security fixes available at following location:
IIS4.0 – URL: http://www.microsoft.com/technet/itsolutions/security/tools/iischk.asp
IIS5.0 – URL: http://www.microsoft.com/technet/itsolutions/security/tools/iis5chk.asp

It is important for security professional to keep themselves abreast of the latest information on new available patches released by the vendors, and what is happenings on in the security community. One way to stay current is to subscribe to security bulletins and newsletters to obtain the latest information and issues faced by other professionals on the field.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Patching this IIS vulnerability is definitely not good enough, as new worms would seek out different ways to access systems and networks. A flexible, defense-in-depth strategy that allows adaptation to the dynamic environment plus well-defined policies and procedures are required to keep the system secured. It is helpful to devise a continuous lifecycle security plan that will update security policy, practices and supporting tools to secure systems and information against future attacks.

Security Bulletins

Computer Incidents Advisory Center
URL: http://www.ciac.org/ciac/CIACHome.html

CERT® Coordination Center (CERT/CC)
URL: http://www.cert.org/nav/index.html

Microsoft Security Notification Service
URL: http://www.microsoft.com/security/

SANS Institute NewsBites
URL: http://www.sans.org/newlook/digests/newsbites.htm

SANS Emergency Incident Handler – Incident.org
URL: http://www.incidents.org/

Security Portal
URL: http://www.securityportal.com

References

[1] Computer Incident Advisory Center, L-098: Microsoft Index Server ISAPI Extension buffer Overflow
URL: http://www.ciac.org/ciac/bulletins/l-098.shtml

[2] Computer Incident Advisory Center, L-117: The Code Red Worm, July 19, 2001.
URL: http://www.ciac.org/ciac/bulletins/l-117.shtml

[3] CERT Advisory, CA-2001-19 "Code Red" Worm Exploiting Buffer Overfolw In IIS Indexing Service DLL, July 20, 2001.
URL: http://www.cert.org/advisories/CA-2001-19.html

[4] Cisco, Cisco Security Advisory: "Code Red" Worm – Customer Impact, July 20, 2001.
URL: http://www.cisco.com/warp/public/707/cisco-code-red-worm-pub.shtml

[5] Digital Island, Code Red Worm InfoSec Bulletin
URL: http://www.digitalisland.net/codered/

© SANS Institute 2001, Author retains full rights

[6] eEye Digital Security, CodeRedII Worm Analysis, Aug 4, 2001
URL: http://www.eeye.com/html/advisories/coderedII.zip

[7] eEye Digital Security, .ida "Code Red" Worm, July 19, 2001.
URL: http://www.eeye.com/html/Research/Advisories/AL20010717.html

[8] eEye Digital Security, MS IIS Remote buffer overflow (SYSTEM Level Access), June 18, 2001.
URL: http://www.eeye.com/html/Research/Advisories/AD20010618.html

[9] Handler's Diary, CodeRed II, Aug 6, 2001
URL: http://www.incidents.org/react/code_redII.php

[10] HarshTruth, Major Alert!!! Code Red Worm, June 18, 2001
URL: http://www.harshtruth.com/warnings.html

[11] Microsoft, Unchecked Buffer in Index Server ISAPI Extension Could Enable Web Server Compromise, June 18, 2001.
URL: http://www.microsoft.com/technet/security/bulletin/MS01-033.asp

[12] Microsoft, Hotfix for Windows NT 4.0
URL: http://www.microsoft.com/Downloads/Release.asp?ReleaseID=30833

[13] Microsoft, Windows 2000 Professional, Server and Advanced Server patch:
URL: http://www.microsoft.com/Downloads/Release.asp?ReleaseID=30800

[14] Sullivan, Bob, MSNBC "Remembering the Net Crash of '88"
URL: http://www.msnbc.com/news/209745.asp

[15] Network Working Group, The Helminthisasis of the Internet, December 1989
URL: http://www.worm.net/rfc1135.txt

[16] National Infrastructure Protection Center, Ida Code Red Worm, 17 July 2001
URL: http://www.nipc.gov/warnings/alerts/2001/01-016.htm

[17] SecurityPortal
URL: http://www.securityportal.com/research/virus/profiles/codered.html

[18] SANS, Securing IIS Against Code Red, Jason Fossen.
URL: http://www.digitalisland.net/codered/

[19] Symantec, CodeRed Worm, July 31, 2001.
URL: http://www.sarc.com/avcenter/venc/data/codered.worm.html

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

[20] Symantec, Symantec Enterprise Security Solutions protect against the Microsoft Windows IIS Index Server ISAPI System-level Remote Access Buffer Overflow, June 20, 2001.
URL: http://www.sarc.com/avcenter/security/Content/2001_06_20a.html

[21] Symantec, CodeRed.v3, Aug7, 2001.
URL: http://www.sarc.com/avcenter/venc/data/codered.v3.html

[22] TruSecure Alert- TSA-01-020 IIS Index Server Worm, 17 July 2001.
URL: http://www.trusecure.com/html/tspub/hypeorhot/rxalerts/tsa01020_cid115.shtml

© SANS Institute 2001, Author retains full rights.

Last Updated: June 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**