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...
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.
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, reformating 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


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?

   %u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=*

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
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.
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
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:
Windows 2000 Professional, Server and Advanced Server:
Step-by-step instructions for these actions are posted at URL:
http://www.digitalisland.net/codeder

Additional information about the patch, its installation, and the vulnerability is available at follow URL:

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:
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.
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](http://www.ciac.org/ciac/CIACHome.html)

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

Microsoft Security Notification Service  

SANS Institute NewsBites  
URL: [http://www.sans.org/newlook/digests/newsbites.htm](http://www.sans.org/newlook/digests/newsbites.htm)

SANS Emergency Incident Handler – Incident.org  
URL: [http://www.incidents.org/](http://www.incidents.org/)

Security Portal  
URL: [http://www.securityportal.com](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](http://www.ciac.org/ciac/bulletins/l-098.shtml)


URL: [http://www.digitalisland.net/codered/](http://www.digitalisland.net/codered/)
URL: http://www.eeye.com/html/advisories/coderedII.zip

URL: http://www.eeye.com/html/Research/Advisories/AL20010717.html

URL: http://www.eeye.com/html/Research/Advisories/AD20010618.html

URL: http://www.incidents.org/react/code_redII.php

URL: http://www.harshtruth.com/warnings.html

URL: http://www.microsoft.com/technet/security/bulletin/MS01-033.asp

[12] Microsoft, Hotfix for Windows NT 4.0


[14] Sullivan, Bob, MSNBC "Remembering the Net Crash of ‘88"

URL: http://www.worm.net/rfc1135.txt

URL: http://www.nipc.gov/warnings/alerts/2001/01-016.htm

URL: http://www.securityportal.com/research/virus/profiles/codered.html

URL: http://www.digitalisland.net/codered/

URL: http://www.sarc.com/avcenter/venc/data/codered.worm.html


## Upcoming SANS Training

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

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Location</th>
<th>Dates</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Munich March 2018</td>
<td>Munich, DE</td>
<td>Mar 19, 2018 - Mar 24, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Pen Test Austin 2018</td>
<td>Austin, TXUS</td>
<td>Mar 19, 2018 - Mar 24, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure Canberra 2018</td>
<td>Canberra, AU</td>
<td>Mar 19, 2018 - Mar 24, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Boston Spring 2018</td>
<td>Boston, MAUS</td>
<td>Mar 25, 2018 - Mar 30, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS 2018</td>
<td>Orlando, FLUS</td>
<td>Apr 03, 2018 - Apr 10, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Abu Dhabi 2018</td>
<td>Abu Dhabi, AE</td>
<td>Apr 07, 2018 - Apr 12, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>Pre-RSA® Conference Training</td>
<td>San Francisco, CAUS</td>
<td>Apr 11, 2018 - Apr 16, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Zurich 2018</td>
<td>Zurich, CH</td>
<td>Apr 16, 2018 - Apr 21, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS London April 2018</td>
<td>London, GB</td>
<td>Apr 16, 2018 - Apr 21, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Baltimore Spring 2018</td>
<td>Baltimore, MDUS</td>
<td>Apr 21, 2018 - Apr 28, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>Blue Team Summit &amp; Training 2018</td>
<td>Louisville, KYUS</td>
<td>Apr 23, 2018 - Apr 30, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Seattle Spring 2018</td>
<td>Seattle, WAUS</td>
<td>Apr 23, 2018 - Apr 28, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Riyadh April 2018</td>
<td>Riyadh, SA</td>
<td>Apr 28, 2018 - May 03, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Doha 2018</td>
<td>Doha, QA</td>
<td>Apr 28, 2018 - May 03, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS SEC460: Enterprise Threat Beta Two</td>
<td>Crystal City, VAUS</td>
<td>Apr 30, 2018 - May 05, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>Automotive Cybersecurity Summit &amp; Training 2018</td>
<td>Chicago, ILUS</td>
<td>May 01, 2018 - May 08, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS SEC504 in Thai 2018</td>
<td>Bangkok, TH</td>
<td>May 07, 2018 - May 12, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Security West 2018</td>
<td>San Diego, CAUS</td>
<td>May 11, 2018 - May 18, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Melbourne 2018</td>
<td>Melbourne, AU</td>
<td>May 14, 2018 - May 26, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Northern VA Reston Spring 2018</td>
<td>Reston, VAUS</td>
<td>May 20, 2018 - May 25, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Amsterdam May 2018</td>
<td>Amsterdam, NL</td>
<td>May 28, 2018 - Jun 02, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Atlanta 2018</td>
<td>Atlanta, GAUS</td>
<td>May 29, 2018 - Jun 03, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Rocky Mountain 2018</td>
<td>Denver, COUS</td>
<td>Jun 04, 2018 - Jun 09, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>DFIR Summit &amp; Training 2018</td>
<td>Austin, TXUS</td>
<td>Jun 07, 2018 - Jun 14, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Milan June 2018</td>
<td>Milan, IT</td>
<td>Jun 11, 2018 - Jun 16, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SEC487: Open-Source Intel Beta One</td>
<td>OnlineVAUS</td>
<td>Mar 19, 2018 - Mar 24, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Books &amp; MP3s Only US</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>