Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

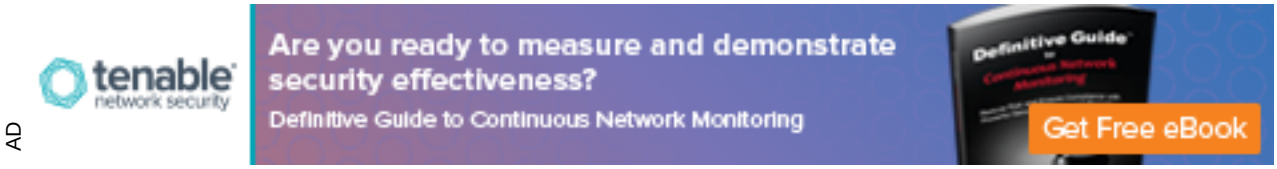
This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Code Red and Code Red II: Double Dragons

This paper describes the mechanisms of the Code Red and Code Red II worms and the software vulnerabilities that went unpatched allowing the worms to propagate.

Copyright SANS Institute
Author Retains Full Rights

AD



Code Red and Code Red II: Double dragons

SANS GSEC Practical Assignment Version 1.2f
Kittipong Teeraruangchaisri
September 15, 2001

Before July 2001, if you ask people about Code Red, you may hear they say about pop rock artist from England whose songs had been in the music charts years ago. However, in July 2001 people recognize the name "Code Red" as one of the harmful worm that spread through the Internet.

This year, many worms have been discovered on various platforms. In January, Ramen worm is the one that use vulnerability of wu-ftpd software on Linux platform to spread. Another one called Lion worm, which exploits vulnerability of BIND DNS server on Unix system, has been discovered in March. The sadmind/IIS worm attack both Sun Solaris and Windows plat form by using exploitation on Solaris to propagate and then attack Microsoft IIS web server.

On 16 July, 2001 eEye digital security found the worm that use IIS Index Server ISAPI Extension vulnerability, also known as ".ida vulnerability", to propagate. This is the one called "Code Red" worm.

This worm has become more familiar when NIPC(National Infrastructure Protection Center) issued an alert regarding the threat from worm propagation on July 29.

At first sight

In my opinion, Windows platform is likely to be the better place for worm to stay and propagate compare to Unix system because Windows always use by less skill users (i.e. home users) who have less sense of security. In addition, there is large number of machines running Windows all around the world and default installation of Windows system contains many serious vulnerabilities.

When I first saw the news about Code Red worm in security mailing list, I didn't think it would be a serious threat because it exploits .ida vulnerability, which had been found months ago, all of machines under my administration had been patched. Also, this vulnerability is on Window NT and 2000 that open web server service, so it should not affect home users who use Windows 98 and Windows ME. However, when I read more information about this worm, I could realize that I should prepare to deal with its effect.

The Vulnerability

Vulnerability used by this worm was also discovered by eEye digital security on June 18. Microsoft issued security bulletin MS01-033 to state this vulnerability. It is caused by unchecked buffer in idq.dll, which is part of Microsoft Indexing Service. The attacker can use buffer overflow technique to run code in the context of local SYSTEM account on target machine.

This is a serious vulnerability. The attacker can compromised target machine by insert malicious code to HTTP request and send them to an affected machine. The similar vulnerability, IIS Unicode vulnerability (MS00-078), had been discovered months ago and it had been used to create sadmind/IIS worm, which I have mentioned earlier in

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

this paper. However, comparing to IIS Unicode vulnerability, this vulnerability looks better than Unicode vulnerability for use as mechanism in creating Internet worm. These two vulnerabilities can be exploited easily just sending special form of HTTP request. However, Unicode vulnerability allows code to be running in limited privilege while .ida vulnerability allows worm to execute code in high privilege context that will facilitate staying, propagating and attacking function of the worm. This may explain why sadmind/IIS worm need both Solaris and IIS to function while Code Red can work with IIS alone.

Default installation of IIS 4 and IIS 5 contain idq.dll and the vulnerability as well. However, the ISAPI extension .ida and .idq is rarely used by typical web application. It can be removed from IIS configuration. This is one of the tasks recommended in Microsoft IIS security checklist. The web servers which .ida and .idq extension was removed are not vulnerable.

Code Red worm

Code Red worm infect target machine by sending special form of HTTP request which contains code of worm. The request may look like:

```
http://www.target.web/default.ida?NNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN NNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNN%u9090%u6858%ucbd3%u7801%u9
090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090
%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a
```

When vulnerable web server processes the request, the worm code is activated and it starts working. After successful infection, Code Red will perform many activities:

- If the system is running Windows English version, it will change starting page of web site to display a message "Welcome to http://www.worm.com, Hacked By Chinese".
- It use infected machine to scan and spread through other machines. The scanning process waste much of system resources especially network bandwidth.
- Its activity is also based on system date of infected machine that is:
  - During day 1st to 19th of each month it will try to scan other system to find more machine to propagate
  - During day 20th to 27th of each month it will send large amount of data to port 80 of www.whitehouse.gov.
  - During day 28th to end of month it will hibernate, no activity is performed.
- The worm is memory resident, all its code include starting page, which it will change, are resident in memory. It does not generate any file or data on hard disk of infected machine. Therefore, simply reboot the infected machine can clear the worm out of the system.

From the information above, you may notice that:

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

- Even though it can spread very fast, the recovery process is so simple. There is no files or backdoor leave on the infected system. Thus, you can recover from the worm by installing patch to make sure that the system will not be infected again then reboot the machine to clear the worm out of the system.
- The system administrator, whose system has limited network bandwidth, will be automatically alerted on the infection of the worm by the worm itself because network bandwidth will be depleted that will cause problem to other network application.

On August 6, while Code Red were spreading all around the world, CERT issued incident note stated that there were another worm call Code Red II which used the same .ida vulnerability spreading through out the Internet.

Code Red II: The real threat

Actually, Code Red II is another worm that does not seems to be mutated from original version of Code Red. The only similar activity is that both of them will heavily scan other machines on Internet to propagate. All other activities of Code Red II are different from original Code Red.

Code Red II: Attacking function

Code Red II itself does not have any attacking function like Code Red. Instead of that it install additional backdoor to allow attacker to use the infected machine as one of the troop to make further attack. It will copy the cmd.exe, which is command shell, to be root.exe in default executable IIS virtual directory (i.e. /scripts and /msadc). This will allow anyone to remotely run programs or commands on the infected machines that could allow further compromise of the system.

In addition, Code Red II will make it self more tolerant by installing trojan version of explorer.exe on c:\ for it will be run every time users log on to system. Its version of explorer.exe is designed to open more backdoor on the system. It will modify following system registries:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots\Scripts
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots\msadc
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots\c
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots\d
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\SFCDisable

The first two registries will be modify to allow program execution in IIS virtual directory /scripts and /msadc. Other two entries are added to create new virtual directory /c and /d that will be link to physical path c:\ and d:\ and also allow program execution on both of them. These registries modification is designed to make sure that attacker can be always access cmd.exe in the system partition in addition to Trojan root.exe, which have copied to executable virtual directory. The last one is modified to disable file system checker feature of Windows 2000.

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

The file explorer.exe make worm hard to kill. As long as worm explorer process is running, virtual directories that used as backdoor are always active. Restart the infected machine cannot stop explorer.exe from running because it will be started automatically when user log on.

Code Red II: Propagating function

Code Red II scanning function is much different from original Code Red in many ways.

1. Number of threads used: While original Code Red will create not more than 100 threads to scan others and propagate, Code Red II use at least 300 threads (up to 600 threads) to do the scanning. Obviously, Code Red II will use much more network resources than original Code Red.
2. Scanning pattern: Original Code Red use random algorithm to select target that makes its target more scattered through out the Internet but Code Red II use the different algorithm.

   Code Red II will select its target IP address based on local IP address of the infected machines. Most of which will have the same first and second octet as infected host. Only small number of target IP are random and not related to IP of infected machines. That means Code Red II target to machine near its current host first. However, some random target IP are still be use to spread more worm to Internet.

The scanning method of Code Red II makes its behavior much different than original Code Red. Code Red II use more threads than Code Red that make it spread faster. The way it select its next target may lead to more chance of finding vulnerable host, base on the assumption that adjacent IP address is likely to be owned by the same owner and if one machine is vulnerable, other machines are believe to be vulnerable too.

The impact: Traffic Congestion and denial of service

The main impact of these two worms is traffic congestion that is denial of service attack especially on the organization that has limited Internet connection bandwidth. Code Red II makes more severe impact than Code Red.

1. If the worm infects the machines in your own network, outbound traffic will be used to scan other hosts. For the network with low bandwidth (i.e 128 Kbps), only one infected machine can saturate all outbound bandwidth.
2. Other infected machines try to scan your network; inbound traffic will be increased due to the scan.

   For original Code Red, because of its random target selection the scanning will be originated from different sources and only small number of scanning from each source. The more number of total infections will lead to higher scanning rate you will receive. Fortunately, public awareness on this issue make number of infection under control before scanning function fully activated in August.

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

For Code Red II, the scanning traffic might be very high even though total number of infection is low. If the infected hosts use IP address adjacent to your network, you may receive many scanning attempts because Code Red II aim to infect nearby IP address first and it selects its target as a group.

For instance, if you network use IP 10.2.0.0/16 and Code Red II has infected the machine that use IP 10.2.3.4, the infected host will mostly scan IP address that begin with 10.2.x.x so your network will be hit heavily.

3. Many products of Cisco network equipments may stop working when receive some number of traffic. Cisco 600 series DSL router will stop forwarding packet and need a restart after receive Code Red scanning.
4. Dial-up Internet users may suffer from being scanned that will consume most of modem bandwidth.

The impact: Backdoor/Trojan

Code Red II leave backdoor on your system even though it had been cleared. This is another dangerous action of this worm because it can lead to further compromise of the infected system that is very hard to detect and recover.

For instance, one of hacker is familiar with this worm so he know about the backdoor that the worm leave on the system. Then he scans Internet IP to find the backdoor leaved by the worm. After that he may compromise the host and install another trojan to the infected machine. The trojan might be the one that widely used or the brand new one which is very hard to detect. Now even though machine owner clean the Code Red II and close the backdoor, the hacker are still able to access to the compromised system.

Defensive Action

The protection can be done at both perimeter/network and system security level.

1. Perimeter/network level

   Firewall or router with high-level filtering can filter out the request send by worm. Checkpoint Firewall-1 can stop both Code Red inbound and outbound request by defining rules to block Code Red HTTP request (i.e. HTTP request containing ".ida"):
   http://support.checkpoint.com/public/publisher.asp?id=a0ff902e-7d65-11d5-97ed-080020a7af00&resource=&number=0&isExternal=0

   Cisco has also provided step to configure Cisco router to block Code Red HTTP request:
   http://www.cisco.com/warp/public/63/nbar_acl_codered.shtml

   For network that never need inbound HTTP traffic, block all inbound traffic on port 80 using basic router access list or firewall rule should be the best solution. For dial-up users, typically they do not need any inbound HTTP request; ISP may block all inbound HTTP traffic at access server to protect them from problems and mitigate the propagation of the worm.

2. System security level

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

Install patch that fix this vulnerability is the best solution. Remember that you should install all patch before connect the machine to network. When the worm is spreading around, affected machine can be infected immediately after connecting to network.

Microsoft has released the cumulative patch that fixes all IIS vulnerabilities include .ida vulnerability. Details can be found in Microsoft security bulletin MS01-044: http://www.microsoft.com/technet/security/bulletin/ms01-044.asp

Worm Detection

Security scanning software can be used to search for vulnerable host in your network In addition, eEye Digital Security provide free tool to scan range of IP address for .ida vulnerable machines:
http://www.eeye.com/html/Research/Tools/CodeRedScanner.exe

Most of intrusion detection system can detect the exploitation of .ida vulnerability that indicates the worm scanning. From www.snort.org, following Snort rule can be used to detect this type of attack:

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 80 (msg:"WEB-IIS ISAPI
.ida attempt"; uricontent:".ida?"; nocase;
dsize:>239; flags:A+; reference:arachnids,552; classtype:attempted -
admin; reference:cve,CAN-2000-0071; sid:1243
; rev:1;)
```

Worm Cleaning

Original Code Red do not need special step for cleaning. Simply install patch and restart the machine to clear the worm.

For Code Red II, you need to verify that your system had been compromised or not. If you are sure that only Code Red II is infected and no other backdoor/trojan in the system you can use automatic cleaning tools release by many vendors include Microsoft to clean your system.

However, if you suspect that your system has been compromised, you need more action than just cleaning the worm. Recovering from compromised system need many steps include re-install the whole system and restore data from backup. You may consult CERT guideline at the following link:
http://www.cert.org/tech_tips/win-UNIX-system_compromise.html

The light side

Although the worm may cause much damage to computer system, the protection measures against worm sometimes improve security protection system. It raises users awareness of system security. Great number of machines had been patched so they safe from many security issues not only Code Red because cumulative patch from Microsoft will correct all known security issues of IIS include other serious vulnerabilities such as Unicode vulnerability.

References:

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

CERT. "CERT Advisory CA-2001-11 sadmind-IIS Worm". May 10, 2001.
URL: http://www.cert.org/advisories/CA-2001-11.html.

CERT. "Advisory CA-2001-19 "Code Red" Worm Exploiting Buffer Overflow In IIS Indexing Service DLL". August 23, 2001.
URL: http://www.cert.org/advisories/CA-2001-19.html.

CERT. "Incident Note IN-2001-09". August 6, 2001.
URL: http://www.cert.org/advisories/CA-2001-19.html.

eEye Digital Security. ".ida "Code Red" Worm". July 17, 2001.
URL: http://www.eeye.com/html/Research/Advisories/AL20010717.html.

eEye Digital Security. "CodeRedII Worm Analysis". August 4, 2001.
URL: http://www.eeye.com/html/Research/Advisories/AL20010804.html.

eEye Digital Security. "CodeRed Scanner from eEye Digital Security".
URL: http://www.eeye.com/html/Research/Tools/codered.html.

Microsoft Corp. "Microsoft Security Bulletin MS01-033 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.

Microsoft Corp. "Microsoft Security Bulletin MS01-044 Cumulative Patch for IIS". August 15, 2001.
URL: http://www.microsoft.com/technet/security/bulletin/MS01-044.asp.

National Infrastructure Protection Center. "ALERT 01--016 Code Red Worm". July 29, 2001.
URL: http://www.nipc.gov/warnings/alerts/2001/01-016.htm.

Symantec Corp. "CodeRed II" Symantec Security Response. September 5, 2001.
URL: http://www.symantec.com/avcenter/venc/data/codered.ii.html.

Snort Web site. "Snort Current Rules Official Release". August 13, 2001.
URL: http://www.snort.org/downloads/snortrules.tar.gz.

Cisco System Inc. "Cisco Security Advisory: "Code Red" Worm - Customer Impact". August 11, 2001.
URL: http://www.cisco.com/warp/public/707/cisco-code-red-worm-pub.shtml.

Cisco System Inc. "Using Network-Based Application Recognition and Access Control Lists for Blocking the "Code Red" Worm at Network Ingress Points".
URL: http://www.cisco.com/warp/public/63/nbar_acl_codered.shtml.

Checkpoint Software Technologies Ltd. "Solution: How to use the VPN-1/FireWall-1 HTTP Security Server to protect against the Code Red worm" Secure Knowledge Database.
URL: http://support.checkpoint.com/public/publisher.asp?hotid=a0ff902e-7d65-11d5-97ed-080020a7af00.

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

Richman, Dan. "State pressing Qwest for refunds after 'Code Red II' DSL breakdowns" MSNBC News. August 22, 2001.
URL: http://www.msnbc.com/local/pisea/m82670.asp.

Junnarkar, Sandeep. and Fried, Ian. "Code Red II: A double whammy" ZDNet News. August 6, 2001.
URL: http://www.zdnet.com/zdnn/stories/news/0,4586,5095260,00.html.

Annanova Ltd. "Code Red attack to be less damaging than thought". August 17, 2001.
URL: http://www.ananova.com/news/story/sm_376461.html.

© SANS Institute 2001, Author retains full rights.

Last Updated: February 11th, 2016

Upcoming SANS Training

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

SANS Northern Virginia - McLean 2016	McLean, VAUS	Feb 15, 2016 - Feb 20, 2016	Live Event
SANS Munich Winter 2016	Munich, DE	Feb 15, 2016 - Feb 20, 2016	Live Event
ICS Security Summit & Training - Orlando	Orlando, FLUS	Feb 16, 2016 - Feb 23, 2016	Live Event
SANS Southern California - Anaheim 2016	Anaheim, CAUS	Feb 22, 2016 - Feb 27, 2016	Live Event
SANS Secure India 2016	Bangalore, IN	Feb 22, 2016 - Mar 05, 2016	Live Event
RSA Conference 2016	San Francisco, CAUS	Feb 28, 2016 - Feb 29, 2016	Live Event
SANS London Spring 2016	London, GB	Feb 29, 2016 - Mar 05, 2016	Live Event
SANS Philadelphia 2016	Philadelphia, PAUS	Feb 29, 2016 - Mar 05, 2016	Live Event
SANS Abu Dhabi 2016	Abu Dhabi, AE	Mar 05, 2016 - Mar 10, 2016	Live Event
SANS 2016	Orlando, FLUS	Mar 12, 2016 - Mar 21, 2016	Live Event
ICS410 Dubai 2016	Dubai, AE	Mar 13, 2016 - Mar 17, 2016	Live Event
SANS Secure Singapore 2016	Singapore, SG	Mar 28, 2016 - Apr 09, 2016	Live Event
SANS Secure Europe 2016	Amsterdam, NL	Apr 04, 2016 - Apr 16, 2016	Live Event
SANS Northern Virginia - Reston 2016	Reston, VAUS	Apr 04, 2016 - Apr 09, 2016	Live Event
SANS Atlanta 2016	Atlanta, GAUS	Apr 04, 2016 - Apr 09, 2016	Live Event
Threat Hunting and Incident Response Summit	New Orleans, LAUS	Apr 12, 2016 - Apr 19, 2016	Live Event
ICS Amsterdam 2016	Amsterdam, NL	Apr 18, 2016 - Apr 23, 2016	Live Event
SANS Secure Canberra 2016	Canberra, AU	Apr 18, 2016 - Apr 23, 2016	Live Event
SANS Pen Test Austin	Austin, TXUS	Apr 18, 2016 - Apr 23, 2016	Live Event
SANS Copenhagen 2016	Copenhagen, DK	Apr 25, 2016 - Apr 30, 2016	Live Event
SANS Security West 2016	San Diego, CAUS	Apr 29, 2016 - May 06, 2016	Live Event
SANS Baltimore Spring 2016	Baltimore, MDUS	May 09, 2016 - May 14, 2016	Live Event
SANS Houston 2016	Houston, TXUS	May 09, 2016 - May 14, 2016	Live Event
SANS Stockholm 2016	Stockholm, SE	May 09, 2016 - May 14, 2016	Live Event
SANS Prague 2016	Prague, CZ	May 09, 2016 - May 14, 2016	Live Event
SANS Secure Japan 2016	OnlineJP	Feb 15, 2016 - Feb 20, 2016	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced