



# **SANS Institute**

## Information Security Reading Room

### **Code Red and Code Red II: Double Dragons**

---

Kittipong Teeraruangchaisri

Copyright SANS Institute 2019. Author Retains Full Rights.

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**

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 platform 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



- 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.

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.

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](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

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](http://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](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:**

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](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>.



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>.

Ananova Ltd. "Code Red attack to be less damaging than thought". August 17, 2001.

URL: [http://www.ananova.com/news/story/sm\\_376461.html](http://www.ananova.com/news/story/sm_376461.html).

© SANS Institute 2001, Author retains full rights.



# Upcoming SANS Training

[Click here to view a list of all SANS Courses](#)

SANS Reno Tahoe 2019	Reno, NVUS	Feb 25, 2019 - Mar 02, 2019	Live Event
SANS Brussels February 2019	Brussels, BE	Feb 25, 2019 - Mar 02, 2019	Live Event
Open-Source Intelligence Summit & Training 2019	Alexandria, VAUS	Feb 25, 2019 - Mar 03, 2019	Live Event
SANS Baltimore Spring 2019	Baltimore, MDUS	Mar 02, 2019 - Mar 09, 2019	Live Event
SANS Training at RSA Conference 2019	San Francisco, CAUS	Mar 03, 2019 - Mar 04, 2019	Live Event
SANS Secure India 2019	Bangalore, IN	Mar 04, 2019 - Mar 09, 2019	Live Event
SANS London March 2019	London, GB	Mar 11, 2019 - Mar 16, 2019	Live Event
SANS St. Louis 2019	St. Louis, MOUS	Mar 11, 2019 - Mar 16, 2019	Live Event
SANS Secure Singapore 2019	Singapore, SG	Mar 11, 2019 - Mar 23, 2019	Live Event
SANS San Francisco Spring 2019	San Francisco, CAUS	Mar 11, 2019 - Mar 16, 2019	Live Event
SANS Secure Canberra 2019	Canberra, AU	Mar 18, 2019 - Mar 29, 2019	Live Event
ICS Security Summit & Training 2019	Orlando, FLUS	Mar 18, 2019 - Mar 25, 2019	Live Event
SANS SEC504 Paris March 2019 (in French)	Paris, FR	Mar 18, 2019 - Mar 23, 2019	Live Event
SANS Norfolk 2019	Norfolk, VAUS	Mar 18, 2019 - Mar 23, 2019	Live Event
SANS Munich March 2019	Munich, DE	Mar 18, 2019 - Mar 23, 2019	Live Event
SANS Doha March 2019	Doha, QA	Mar 23, 2019 - Mar 28, 2019	Live Event
SANS Jeddah March 2019	Jeddah, SA	Mar 23, 2019 - Mar 28, 2019	Live Event
SANS SEC560 Paris March 2019 (in French)	Paris, FR	Mar 25, 2019 - Mar 30, 2019	Live Event
SANS Madrid March 2019	Madrid, ES	Mar 25, 2019 - Mar 30, 2019	Live Event
SANS 2019	Orlando, FLUS	Apr 01, 2019 - Apr 08, 2019	Live Event
SANS Cyber Security Middle East Summit	Abu Dhabi, AE	Apr 04, 2019 - Apr 11, 2019	Live Event
SANS London April 2019	London, GB	Apr 08, 2019 - Apr 13, 2019	Live Event
Blue Team Summit & Training 2019	Louisville, KYUS	Apr 11, 2019 - Apr 18, 2019	Live Event
SANS Riyadh April 2019	Riyadh, SA	Apr 13, 2019 - Apr 18, 2019	Live Event
SANS Seattle Spring 2019	Seattle, WAUS	Apr 14, 2019 - Apr 19, 2019	Live Event
SANS Boston Spring 2019	Boston, MAUS	Apr 14, 2019 - Apr 19, 2019	Live Event
FOR498 Battlefield Forensics Beta 1	Arlington, VAUS	Apr 15, 2019 - Apr 20, 2019	Live Event
SANS FOR585 Madrid April 2019 (in Spanish)	Madrid, ES	Apr 22, 2019 - Apr 27, 2019	Live Event
SANS Northern Virginia- Alexandria 2019	Alexandria, VAUS	Apr 23, 2019 - Apr 28, 2019	Live Event
SANS Muscat April 2019	Muscat, OM	Apr 27, 2019 - May 02, 2019	Live Event
Cloud Security Summit & Training 2019	San Jose, CAUS	Apr 29, 2019 - May 06, 2019	Live Event
SANS Pen Test Austin 2019	Austin, TXUS	Apr 29, 2019 - May 04, 2019	Live Event
SANS Riyadh February 2019	OnlineSA	Feb 23, 2019 - Feb 28, 2019	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced