ARIS predictor
Attack Registry & Intelligence Service

Code Red II Worm

Analysts:
Ryan Russell
Andrew Mackie

Incident Analysis Report
August 5, 2001

SecurityFocus
1660 S. Amphlett Boulevard | Suite 128 | San Mateo | CA | 94402 | 650 655 6300 | 650 655 2099 fax

Executive Summary

A new, potentially more malicious worm is using the same means of compromise as the original Code Red. Code Red II targets the Microsoft Indexing Server/Indexing Services ISAPI Buffer Overflow vulnerability (http://www.securityfocus.com/bid/2880.)

Code Red originally appeared on July 11. Just a few days later a Code Red variant appeared. On July 20 the worms stopped spreading and directed Denial of Service attacks at one of the www.whitehouse.gov servers. On July 28 these worms went dormant, only to re-emerge on August 1.

Hundreds of thousands of systems were compromised by Code Red and its variant. It appears that many systems remain vulnerable. This worm, called Code Red II, can re-infect those already infected with Code Red or its variant. The observed rate of spread is much higher since both worms are now infecting unpatched systems across the Internet.

Code Red II inserts a Trojan allowing unauthorized remote access. The Trojan is activated upon login with administrator group privileges. The steps to be taken in recovering from Code Red II are:

1. Download Microsoft's patch for your IIS Web server using this link http://securityfocus.com/vdb/bottom.html?section=solution&vid=2880
2. Disconnect your Internet connection to avoid infection
3. Remove Trojan versions of C:\explorer.exe and D:\explorer.exe if they exist
4. If possible apply MS00-052 if you do not have Service Pack 2 (SP2) installed
5. Reboot your system to clear the worm from memory
6. If you do not have SP2 installed and did not wish to apply MS00-052 in step 4 then you must log in as a user not in the administrative group to prevent activating the Trojan explorer.exe
7. Remove Trojan versions of C:\explorer.exe and D:\explorer.exe if they exist
8. Apply the patch to prevent re-infection
9. Reboot before attempting to change registry values
10. The Trojan modifies registry values. If the following values are found you must consider the machine compromised and decide whether to re-install the system:
    - SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SFCDisable set to 0FFFFFF9Dh
    - SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots\Scripts set to ,,217
    - SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots\msadc set to ,,217
    - SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots\c set to ,,217
    - SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots\d set to ,,217
11. The steps from this point on assume you are attempting to remove the worm. Remove any copies of root.exe from C:\inetpub\scripts\root.exe and D:\inetpub\scripts\root.exe
12. Reset registry values for SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SFCDisable to enable system file protection to zero to enable system file protection
13. Code Red II sets registry values for remote Web access. If you have a default installation you do not require these keys and they may be removed or set to zero. If you use these keys you will need to reset them to your own values:
    - SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots\Scripts
    - SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots\msadc
    - SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots\c
    - SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots\d
14. Reboot your system
15. Reconnect to the Internet

Associated Vulnerability:	*MS Index Server and Indexing Service ISAPI Extension Buffer Overflow Vulnerability*
Associated Bugtraq ID:	*2880*
Urgency:	*High*
Ease of Exploit:	*Automatic*
Associated Operating Systems:	*Windows NT 4.0, Windows 2000, Windows XP Beta*

Overview

On June 18, 2001, eEye Digital Security released an advisory regarding a new security hole in IIS. You can find its advisory at http://www.eeye.com/html/Research/Advisories/AD20010618.html.

In short, a buffer overflow in the code handles .ida requests. Code Red and Code Red II use this to successfully infect only Windows 2000 systems. They crash other Windows systems. Otherwise Code Red II is entirely new and infected systems are vulnerable to remote access by the Trojan code it inserts.

According to the eEye Digital Security code analysis the Code Red II worm carries out the following decisions and action through its Infection, Propagation and Trojan insertion phases:

- Infection Phase
    - Checks local system language for Chinese (both Taiwanese and PRC)
    - Checks to see if this is the first execution; if not it proceeds to Propagation Phase
    - Uses the existence of an "atom" or flag inserted by Code Red II to determine if this is a re-infection; if the atom exists the worm sleeps forever, otherwise the atom is created
    - Sets the number of parallel propagation threads to 300 for non-Chinese systems and 600 for Chinese and the Propagation Phase begins
    - Creates a new copy of its process which re-initiates the Infection Phase
    - Starts the Trojan Phase and the worm sleeps for 1 day for non-Chinese or 2 days for Chinese, before rebooting Windows
- Propagation Phase
    - Spreads until October 1, 2002; after this the system will reboot, effectively clearing the worm from memory
    - Selects the next IP address to attempt to infect; address selection is biased to seek out nearby addresses, thereby speeding the spread
        - 1/7 chance of selecting an IP address unrelated to local address
        - 3/7 chance of selecting same class A range as local address
        - 3/7 chance of selecting same class B range as local address
    - Attempts a speedy non-blocking connection to the address selected; if successful it converts to blocking connection and attempts to infect
    - Repeats Propagation Phase
- Trojan Injection Phase
    - Copies cmd.exe into two directories
    - Creates copies of explorer.exe on C; and D: of they exist
    - Imbeds Trojan code in these copies of explorer.exe; as long as one of these are is running an attacker will be able to execute commands remotely

Patches

Microsoft has its security patch at:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-033.asp

Attack Signatures

Windows Index Server ships with Windows NT 4.0 Option Pack and Windows Indexing Service ships with Windows 2000. An unchecked buffer exists in the idq.dll ISAPI extension associated with each service. A maliciously crafted request could allow the execution of arbitrary code on the host in the Local System context. You can find a more complete description at: http://securityfocus.com/bid/2880

The original Code Red and its variant send the following request during the attack:

```
/default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN%u9090%u6
858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%
u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a HTTP/1.0
```

The new worm sends a very similar header:

```
/default.ida?XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX%u9090%u6
858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%
u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a HTTP/1.0
```

The difference is that it uses X instead of N as its filler character. The machine code that follows is different between the two.

IDS Updates

By now, all the major IDS vendors have rules to catch the overflow attempts. In addition, some of the IDS' are spotting the string "cmd.exe" in the exploit code, and alarming on this. SecurityFocus recommends that you update to the latest rule set available for your IDS as soon as possible.

Recommendations

SecurityFocus recommends that you follow these steps in recovering from Code Red II:

1. Download Microsoft's patch for your IIS Web server using this link http://securityfocus.com/vdb/bottom.html?section=solution&vid=2880
2. Disconnect your Internet connection to avoid infection
3. Remove Trojan versions of C:\explorer.exe and D:\explorer.exe if they exist
4. If possible apply MS00-052 if you do not have Service Pack 2 (SP2) installed
5. Reboot your system to clear the worm from memory
6. If you do not have SP2 installed and did not wish to apply MS00-052 in step 4 then you must log in as a user not in the administrative group to prevent activating the Trojan explorer.exe
7. Remove Trojan versions of C:\explorer.exe and D:\explorer.exe if they exist
8. Apply the patch to prevent re-infection
9. Reboot before attempting to change registry values
10. The Trojan modifies registry values. If the following values are found you must consider the machine compromised and decide whether to re-install the system:
    - SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SFCDisable set to 0FFFFFF9Dh
    - SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots\Scripts set to ,,217
    - SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots\msadc set to ,,217
    - SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots\c set to ,,217
    - SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots\d set to ,,217
11. The steps from this point on assume you are attempting to remove the worm. Remove any copies of root.exe from C:\inetpub\scripts\root.exe and D:\inetpub\scripts\root.exe
12. Reset registry values for SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SFCDisable to enable system file protection to zero to enable system file protection
13. Code Red II sets registry values for remote Web access. If you have a default installation you do not require these keys and they may be removed or set to zero. If you use these keys you will need to reset them to your own values:
    - SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots\Scripts
    - SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots\msadc
    - SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots\c
    - SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots\d
14. Reboot your system
15. Reconnect to the Internet

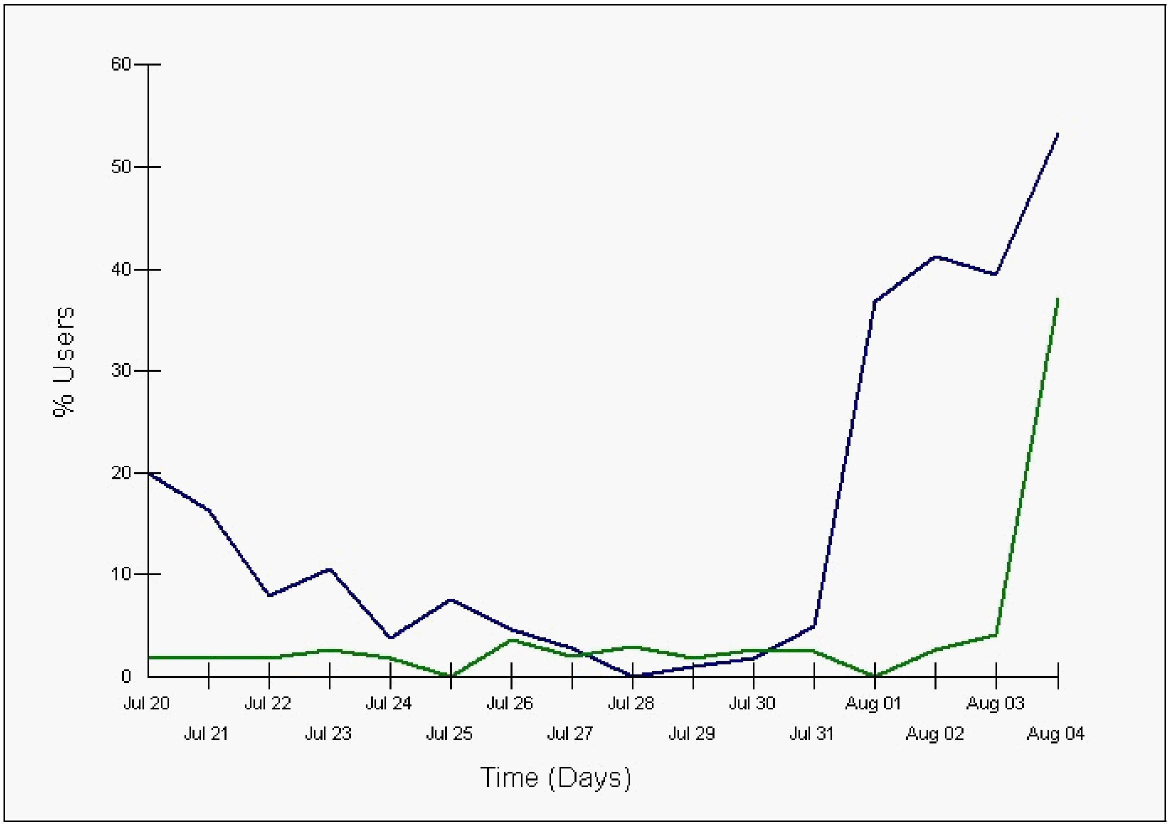
In addition, SecurityFocus analysts recommend that you implement as much of the following hardening/checklist document as possible:

* IIS4:
http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/columns/questions/iischeck.asp

* IIS5:
http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/iis/deploy/depovg/securiis.asp

There is also an IIS5 Hotfix Checking Tool to check for patches that haven't been installed. You can get it from Microsoft Technet at:
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=24168

Attack Data



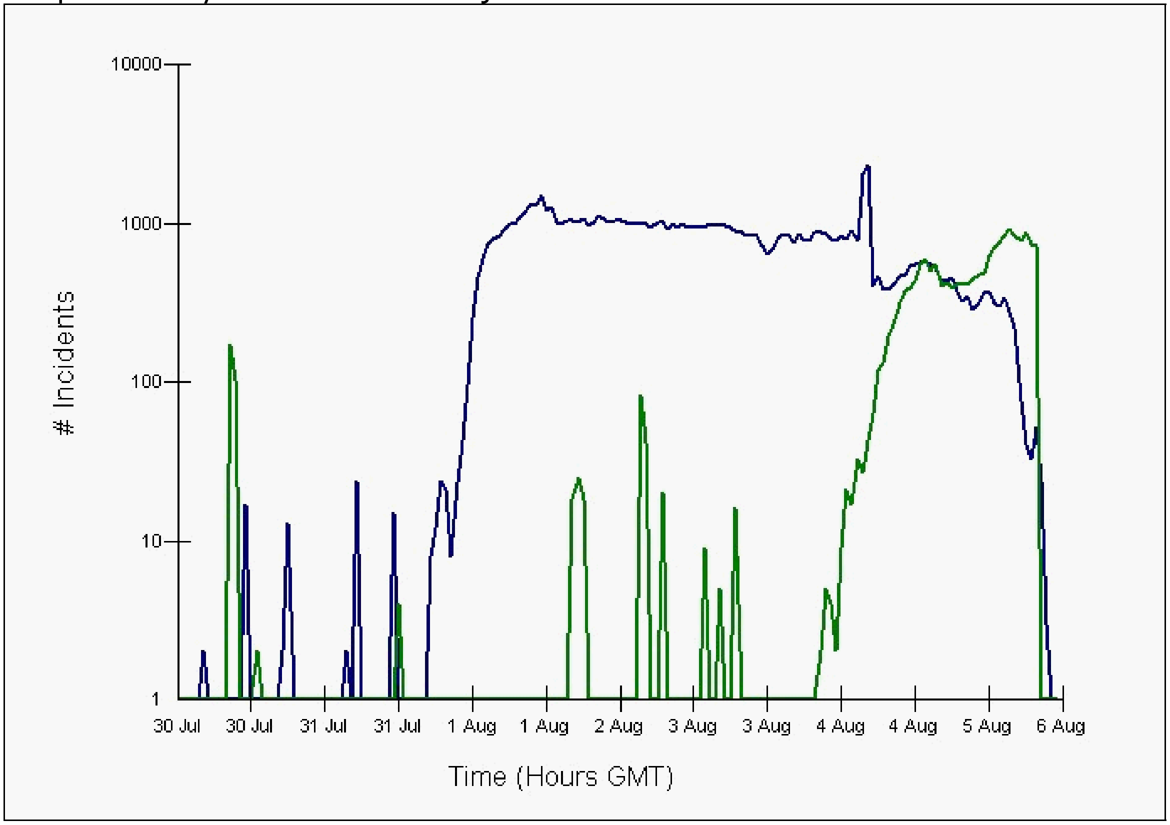
	Attacks	% Users	# Attacks
🟦	Microsoft Indexing Server/Indexing Services ISAPI Buffer Overflow Attack	4.19	90824
🟩	Generic HTTP cmd.exe Request Attack	1.94	8424

Figure 1 — Worm Tracks

The original Code Red and its variant stopped spreading on July 20 and began attacking a White House Web server. On July 28 they went dormant, only to re-emerge on August 1. Their worm tracks were detected as Microsoft Indexing Server/Indexing Services ISAPI Buffer Overflow attacks. The Code Red II will be detected both by this fist buffer overflow signature as well as by a Generic HTTP cmd.exe Request attack signature. **Figure 1** shows the dramatic spread of Code Red II since August 3. In just one day almost 60% of ARIS users were detecting this worm. The original Code Red became active on August 1, lost some momentum, and then was joined by Code Red II.

Figure 1 shows activity early on August 5. **Figure 2** indicates the dramatic change later on the same day. Data for August 5 is incomplete impairing accuracy however the growth in incidents caused by the worm appears to be limited.

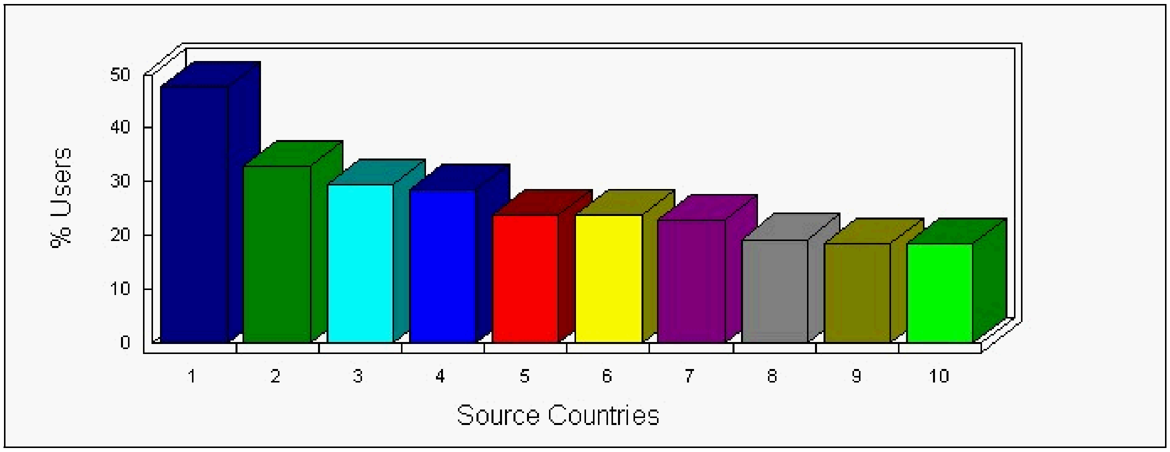
Note that the cmd.exe attacks have a very sharp growth rate, while the actual overflow attacks remain relatively flat. The cmd.exe attacks are new with this worm (they didn't appear with Code Red), while Code Red tends to mask the activity of the new worm at present. It is interesting to see the cmd.exe incidents crossing above the buffer overflow attack trend. There may be attempts to exploit systems compromised by the Code Red II Trojan.



	Attacks	% Users	# Attacks
🟦	Microsoft Indexing Server/Indexing Services ISAPI Buffer Overflow Attack	0.34	84222
🟩	Generic HTTP cmd.exe Request Attack	0.15	15680

Figure 2 - ISAPI Overflows and cmd.exe Requests

Figure 3 shows the top ten attacking countries ranked by the numbers of ARIS users affected. The distribution is likely based on those countries with the most vulnerable IIS Web servers. There is no indication as to source of this worm. The code changes its actions slightly if the local system language is Chinese. Otherwise this worm’s intent is not overtly political. It appears to be intended to provide unauthorized remote access.



		Attacking Country	# Users	% Users	# Attacks
🟦	1	United States	40	36.70	2638
🟩	2	Korea	35	32.11	1768
🟦	3	China	31	28.44	687
🟦	4	Taiwan	30	27.52	743
🟥	5	Netherlands	25	22.94	304
🟨	6	Italy	25	22.94	419
🟪	7	Canada	22	20.18	269
⬛	8	France	19	17.43	381
🟨	9	Germany	19	17.43	327
🟩	10	Japan	18	16.51	177

Figure 3 - Top Attacking Countries

Technical Description

This technical description is based on an analysis and disassembly performed by Marc Maiffret and Ryan Permeh of eEye Digital Security. Their full analysis and disassembly can be found at the following location:
http://www.eeye.com/html/advisories/coderedII.zip

The worm has three sections: The infection mechanism, the propagation mechanism, and Trojan component.

When the worm successfully installs itself on a new victim, it goes through a number of initialization steps:

- Obtains the current victim's IP address (used in propagation step, see below)
- Checks to see if the system language is Chinese (Taiwanese or PRC)
- Checks for previous execution, if so then it jumps to propagation
- Checks to see if the "CodeRedII" atom has been set, if so then sleep forever (kills new arrivals of same worm)
- Adds the "CodeRedII" atom (if previous check failed)
- Sets the number of worker threads to 300, or if it is a Chinese system, 600.

- Spawns a thread back at the first step, which will then jump to propagation, since that will no longer be the first execution
- Calls the Trojan functions
- Sleeps for 1 day on non-Chinese system, 2 on Chinese
- Reboots the system (which will remove any memory resident worms, leaving only the backdoors and explorer.exe Trojan)

The propagation mechanism is the most novel aspect of this particular worm. Here are the steps performed:

- Check local time. If it is less than the year 2002 and is also less than the 10th month, then continue. Otherwise, reboot. This should limit the worm to the end of September 2001 if it lives that long.
- Sets up the sockets needed to connect to other potential victims. Uses non-blocking sockets, which gives a performance advantage.
- If it gets a connect, it sends a copy of itself (so far, all copies are identical, no self-modifying code)
- Repeat

The most interesting piece is how it selects a new victim IP address to try. The worm generates 4 octets in the range 1 through 254, to avoid IP addresses with a 0 or 255. It takes one of these bytes, and binary ANDs it with 7, yielding a random number between 0 and 7. It then consults a table:

```
dd 0FFFFFFFFh            ; 0 - addr masks
dd 0FFFFFF00h            ; 1
dd 0FFFFFF00h            ; 2
dd 0FFFFFF00h            ; 3
dd 0FFFFFF00h            ; 4
dd 0FFFF0000h            ; 5
dd 0FFFF0000h            ; 6
dd 0FFFF0000h            ; 7
```

which determines how much of the randomly generated IP address will be used versus the original address. For example, if it generates a 5, then half will be random, and half will be the old IP address. If the current victim IP address is 192.168.1.1, the new one to try might be 192.168.45.67 (byte order is reversed in the machine code.)

This has the result that 3 times out of 8, it stays within the equivalent of a Class B of the attacker, 4 times out of 8, it stays within a Class A equivalent, and 1 time out of 8, it goes after a completely random IP address.

For the most part, the Internet address space is a sparse matrix. Many of the possible (and assigned) addresses are not reachable from the Internet. Still others have been delegated to a particular ISP or geographic region, but are not yet in use by actual customers. The result is that actual hosts tend to be bunched together in numerically-related netblocks. The CodeRed II worm favors nearby IP addresses which tend to have similar host types (i.e. Windows), so it is exhibiting a much higher rate of growth than previous worms. This also means that if it finds its way onto an RFC1918 network, it would likely be much more damaging to that network than previous worms.

It should also be noted that the worm takes measures to avoid 127.x.x.x and 224.x.x.x.

Finally, during the trojan step is when the backdoors are installed. This portion has the following steps:

- Gets the system directory (usually c:\winnt\system32)
- Appends cmd.exe to the string
- Copies the resulting string (usually c:\winnt\system32\cmd.exe) to
- c:\inetpub\scripts\root.exe and
- c:\progra~1\common~1\system\MSADC\root.exe
- Creates c:\explorer.exe
- Goes back and repeats the steps for drive d: instead of c:

The trojan explorer.exe doesn't get executed until the next time the host is rebooted and someone logs in as a user in the administrative group. If the system does not have SP2 installed and has not had the MS00-052 patch applied it will execute explorer.exe from the root of the drive before it tries its normal location. When it is run, it executes the real explorer, and then does the following in an infinite loop:

- Sets SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SFCDisable to 0FFFFFF9Dh (disables system file protection)
- Sets SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots\Scripts to ,,217
- Sets SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots\msadc to ,,217
- Sets SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots\c to c:\,,217
- Sets SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots\d to d:\,,217
- Sleeps for 10 minutes

The Virtual Roots ensure that the scripts and msadc directories stay mapped, and maps a c and d virtual root which don't normally exist. These are mapped to the drive roots, which will allow an attacker yet another way into the victim web server remotely. Even if the root.exe files are removed and the overflow patched, if explorer.exe is running, an attacker can execute the original cmd.exe, or any other executable, with a command similar to the following:

http://IpAddress/c/winnt/system32/cmd.exe?/c+dir

File Names

The worm itself is memory-resident only. However, it may leave behind files named root.exe, in the script and msadc directories under the IIS webroot. These should of course be deleted, as they are copies of cmd.exe, and will permit remote access to your web server. In addition, a file named explorer.exe will be created in the root of c: and d: if it exists. This needs to be removed, and the host rebooted.

Resources

Securing IIS:
http://securityfocus.com/focus/microsoft/iis/iissecure.html

Free Code Red scanner from eEye:
http://www.eeye.com/html/Research/Tools/index.html

Community Credits

SecurityFocus wishes to thank Ryan Permeh and Marc Maiffret of eEye Digital Security for their analysis. SecurityFocus ARIS Analysts requested their assistance in providing an analysis of the Code Red II assembler code. They worked diligently throughout the night of August 4 to deliver an early analysis that was released publicly on the SecurityFocus incidents list early August 5.

SecurityFocus also wishes to thank the many Internet users who have provided us with logs during the Code Red process, as well as Code Red II. This has enabled us to notify many Code Red victims, who were then able to clean up their affected hosts. We also wish to thank the many ISPs and other providers who had to search through their logs to track down who had the dynamic IP address at that time, and notify them that they were infected.

Glossary

If you are unfamiliar with any term used in this report, please visit the SecurityFocus glossary at http://www.securityfocus.com/glossary/index.html for more details on information security terminology.

Contact Information

Corporate Headquarters

SecurityFocus, Inc.
1660 S. Amphlett Blvd., Suite 128
San Mateo, CA 94402 USA
650-655-6300 (tel)
650-655-2099 (fax)

Field Offices

100-4th Avenue S.W., Suite 710
Calgary, AB, T2P 3N2 Canada
403-213-3939 (tel)
403-233-9179 (fax)

1701 16th Street N.W., Suite 825
Washington, DC 20009 USA
202-232-5200 (tel)
202-232-5200 (fax)

The ARIS *predictor* service provides Incident Alert and Analysis Reports, as well as Weekly and Monthly Summary Reports. These reports draw on IDS log data contributed to the SecurityFocus Incidents Database by ARIS *analyzer* members. This log data is submitted to the Incidents Database voluntarily and often anonymously. While SecurityFocus experts make every effort to inspect this data for validity, SecurityFocus does not guarantee the accuracy of submitted data. The aggregated log information is used to detect trends and is provided AS IS by SecurityFocus. Should you have questions, please contact ARIS-Report@securityfocus.com.