

Code Red II Worm

Analysts:
Ryan Russell, Andrew Mackie

Incident Analysis Report
Version 3
November 30, 2001

SecurityFocus

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

Quoting SecurityFocus Information and Data: *Internal Documents and Presentations:* Quoting individual sentences and paragraphs for use in your company's internal communications does not require permission from SecurityFocus. The use of large portions or the reproduction of any SecurityFocus document in its entirety *does* require prior written approval and may involve some financial consideration. *External Publication:* Any SecurityFocus information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the Vice President of Product Marketing of SecurityFocus. A draft of the proposed document should accompany any such request. SecurityFocus reserves the right to deny approval of external usage for any reason.
Copyright © 2001 SecurityFocus. Reproduction is forbidden unless authorized.

Executive Summary

In the wake of the Code Red worm, a new, potentially more malicious worm called Code Red II is using the same means of compromise as the original worm. These worms all target the Microsoft Indexing Server/Indexing Services ISAPI Buffer Overflow vulnerability (http://www.securityfocus.com/bid/2880).

Code Red originally appeared on July 11, followed a few days later by a variant. On July 20, the Code Red worms stopped spreading and directed Denial of Service (DoS) attacks at one of the www.whitehouse.gov servers. On July 28 they worms went dormant, only to reemerge on August 1.

Code Red and its variant compromised hundreds of thousands of systems. It appears that many systems remain vulnerable. The new worm, Code Red II, can reinfect those already infected with Code Red or its variant. More systems in one locality get infected and the speed of the infection technique has been improved. In addition, the observed rate of spread is much higher because both worms are now infecting unpatched systems across the Internet.

Code Red II is more malicious. It inserts a Trojan that enables unauthorized remote access. The Trojan is activated upon login with administrator group privileges. The Recommendations section of this analysis report outlines steps a system administrator can take to recover from Code Red II.

Copyright © 2001 SecurityFocus

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*

Technical 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 exists in the code that handles .ida requests. Code Red and Code Red II use this buffer 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 actions through its Infection, Propagation, and Trojan Insertion phases:

1. **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 reinfection; 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 that reinitiates the Infection phase.
   - Starts the Trojan phase and the worm sleeps for one day for non-Chinese infections, or two days for Chinese infections, before rebooting Windows.

2. **Propagation Phase**
   - Spreads until October 1, 2001; after this the system reboots, 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, according to the following probabilities:
     - 1/8 chance of selecting an IP address unrelated to the local address
     - 4/8 chance of selecting same class A range as local address (first octet of address is unchanged)
     - 3/8 chance of selecting same class B range as local address (first two octets of address are unchanged)
   - Attempts a speedy nonblocking connection to the address selected; if successful, it converts to a blocking connection and attempts to infect.
   - Repeats Propagation phase.

Copyright © 2001 SecurityFocus

3. **Trojan Insertion Phase**
   - Copies cmd.exe into two directories.
   - Creates copies of explorer.exe on C: and D: drives if they exist.
   - Imbeds Trojan code in these copies of explorer.exe
   - Relies on administrative login and lack of patch for a second vulnerability to initiate a copy of Trojan explorer.exe; as long as one of these programs is running, an attacker will be able to execute commands remotely.

Patches

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

Microsoft also has a patch to prevent the Trojan from executing. The registry entry that specifies the Windows Shell executable (explorer.exe) provides a relative, rather than absolute, path name. Code Red II uses this path to run its own copy of explorer.exe before invoking the real copy. You can find the latest Microsoft announcement regarding this patch at http://www.microsoft.com/WINDOWS2000/downloads/critical/q269049/default.asp.

Description of Vulnerabilities

Windows Index Server ships with the 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 of this vulnerability at http://securityfocus.com/bid/2880.

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

```
/default.ida?NNNN
```

inserts its own Trojan copy of explorer.exe in one or both the C: and D: drives if they exist. Microsoft has had patches for this since July 2000.

IDS Updates

By now, all major IDS vendors have rules to catch the overflow attempts. In addition, some of the IDSes are spotting the string “cmd.exe” in the exploit code, and issuing an alarm as a result of this trigger. SecurityFocus recommends that you update to the latest rule set available for your IDS as soon as possible.

Recommendations

You must consider reformatting and rebuilding any compromised system. In this case, the Trojan may not have been initiated if an administrative login has not occurred or if the system has been patched with SP2 or MS00-052. You may consider it an acceptable risk to attempt recovery by following these steps:

1. Download Microsoft’s patch for your IIS Web server from 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[1].
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 reinfection.
9. Reboot before attempting to change registry values.
10. The Trojan modifies registry values. If you find the following values, you must consider the machine compromised and decide whether to reinstall 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 to zero for SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SFCDisable to enable system file protection.

[1] These copies of explorer.exe may be hidden unless you use the “ATTRIB” MS-DOS command. In this case, you will have to change their attributes before you can delete them. Note that a running explorer.exe cannot be removed.

Copyright © 2001 SecurityFocus

13. Code Red II sets registry values for remote Web access. If you have a default installation, you do not need these keys and you may remove them or set them to zero. If you use these keys you will need to reset them to your own values[2]:

    - 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.

Microsoft has developed a tool to assist you in these steps. SecurityFocus has tested this tool and verified that it adjusts the registry values and removes the executables. It does not apply any patches. You still need to do this yourself. You must also be aware that a chance exists that your system may have been compromised and altered in other ways. The safest approach is to reformat and rebuild your system installation. If you are willing to accept the risk then you can find the tool at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/security/tools/redfix.asp.

If you are unsure whether you are at risk from these worms, Symantec has a free tool that you can find at http://www.sarc.com/avcenter/venc/data/codered.v3.html. If you are vulnerable, you should assume that you have been contaminated and therefore follow the preceding steps for recovery.

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

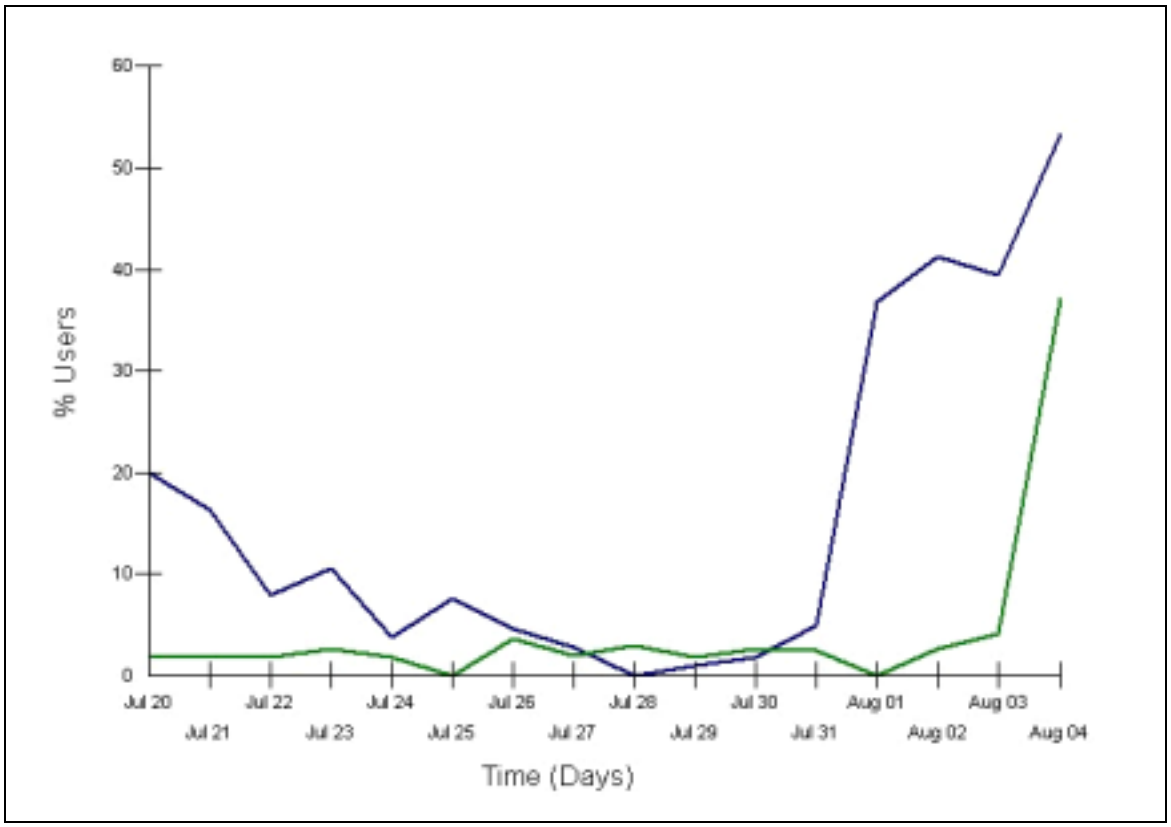
An IIS5 Hotfix Checking Tool also exists that you can use to check for patches that have not been installed. You can get it from Microsoft TechNet at http://www.microsoft.com/Downloads/Release.asp?ReleaseID=24168.

You can configure Cisco IOS to reduce the impact of these worms. You can find their Technical Notes on this topic at http://www.cisco.com/warp/public/63/ts_codred_worm.shtml.

[2] Some have observed that the default values for SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots\Scripts is 204 while SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots\msadc is 205.

Copyright © 2001 SecurityFocus

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

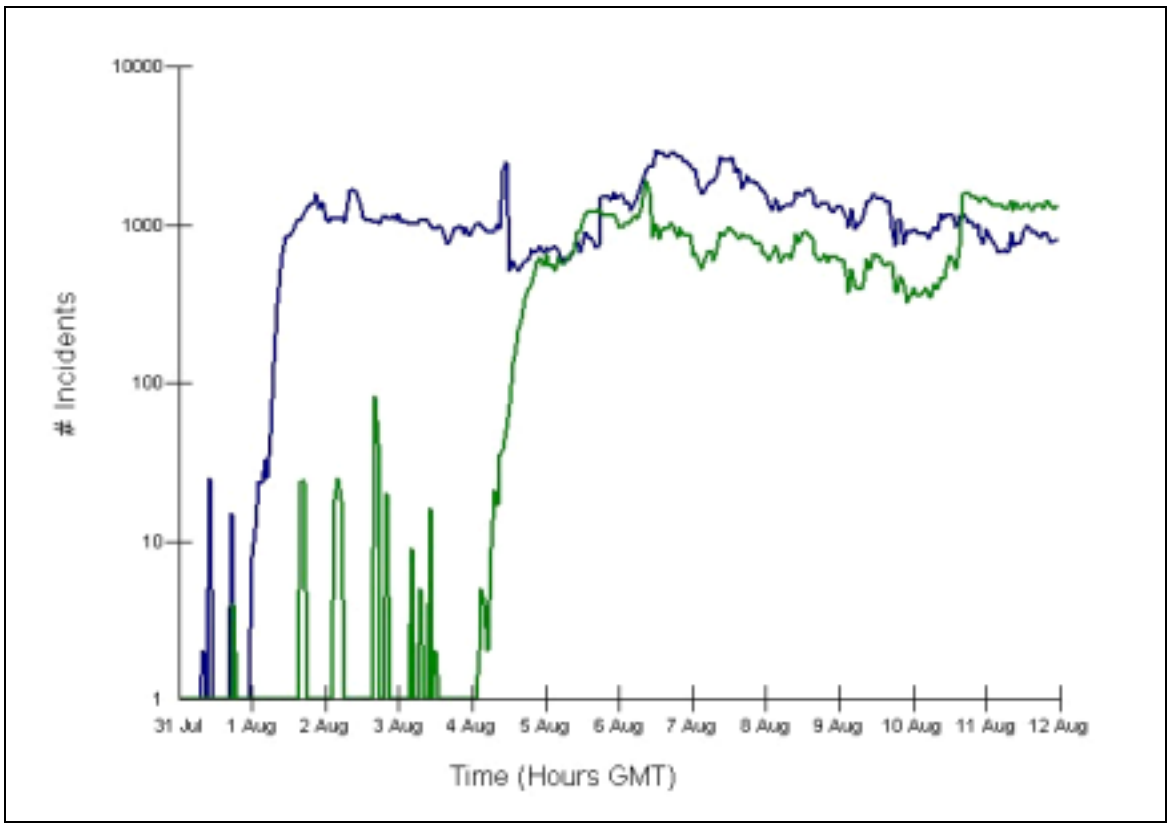
Figure 1 — Worm Tracks

The original Code Red and its variant stopped spreading on July 20 and began attacking a White House Web server. On July 28 these two worms went dormant, only to reemerge on August 1. Their worm tracks were detected as Microsoft Indexing Server/Indexing Services ISAPI Buffer Overflow attacks. Code Red II is detected both by this first 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 percent of ARIS users were detecting this worm. The original Code Red worm became active on August 1, lost some momentum, and then Code Red II became active. This new worm uses an address selection algorithm that increases the worm's rate of successful penetration.

Previous worms have relied on random address selection to cover the Internet. This worm spreads randomly but spends more time seeking out other vulnerable IIS systems on nearby network addresses. This worm is very successful in selecting addresses previously missed by the previous Code Red versions. If one system is vulnerable, others nearby are likely to be vulnerable as well. Once the worm gets to one, it quickly infects them all.

Copyright © 2001 SecurityFocus

Figure 2 indicates the dramatic growth of the Code Red worms starting on August 1. They reached saturation level in only a couple of hours. This is the third worm to target the same vulnerability. A large number of systems with the vulnerability had been patched as a result of previous Code Red worms. Code Red had a limited pool of unpatched systems to reinfect, so it stalled out quickly.



Attacks	% Users	# Attacks
Microsoft Indexing Server/Indexing Services ISAPI Buffer Overflow Attack	0.32	321969
Generic HTTP 'cmd.exe' Request Attack	0.20	151095

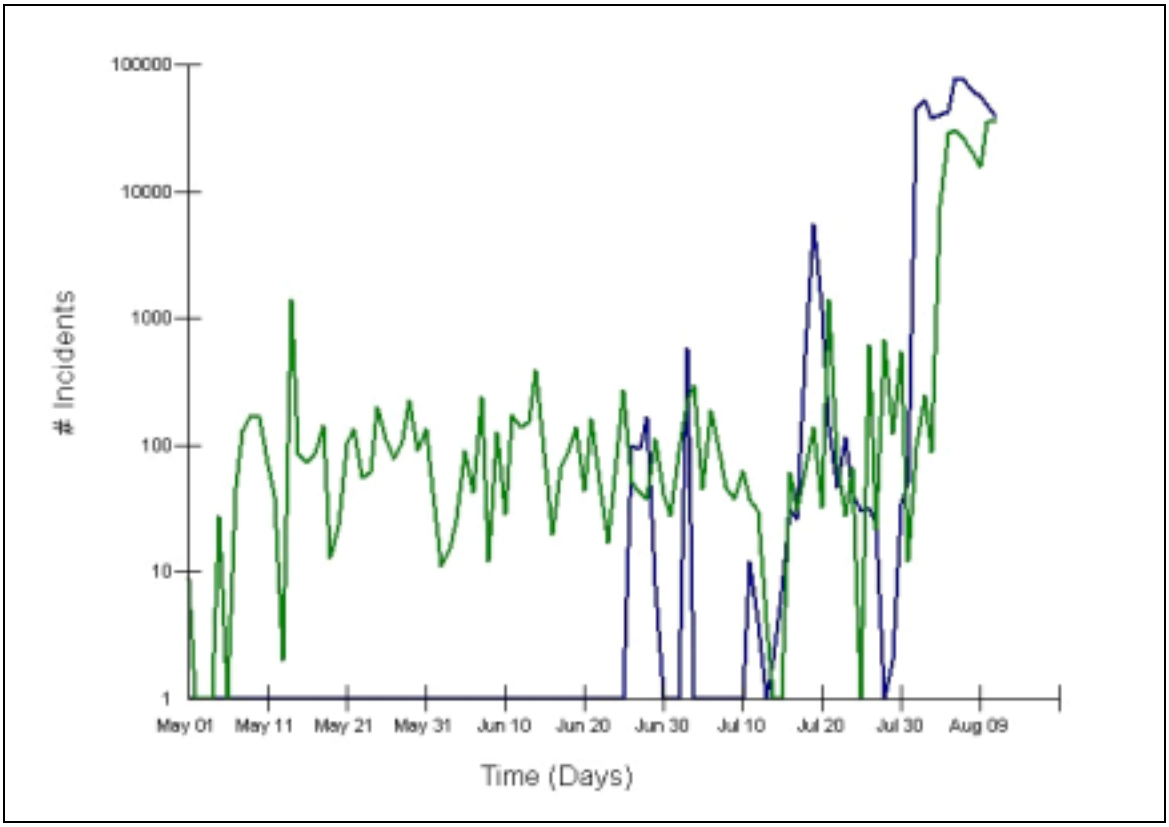
Figure 2 — ISAPI Overflows and cmd.exe Requests

In **Figures 1 and 2**, note that the cmd.exe attacks had a very sharp growth rate on August 4, while the actual overflow attacks remained relatively flat from August 1 to 4. The cmd.exe attacks are new with this worm (they did not appear with Code Red), while Code Red tends to mask the activity of the new worm at present. This worm succeeded in finding more than 300,000 systems that remained vulnerable. Observations indicate that a large majority of these systems appear to be small business or personal systems, often cable users. Default installations of Windows 2000 systems include vulnerable IIS servers.

It is interesting to see the lack of drop off in numbers even as late as August 11. It appears most administrators of these compromised systems are either unaware or tolerant of the worm's presence. Eventually the worm depletes system resources and denies service. Simply rebooting the system removes the worm code but leaves the system vulnerable once the Trojan has been activated. Expect an increase in remote administrative login attempts seeking to activate Trojans lurking on such systems.

Copyright © 2001 SecurityFocus

The original Code Red worms and Code Red II should account for almost all the IIS ISAPI Buffer Overflow attacks reported. Code Red II also triggers the HTTP cmd.exe Request attacks. However, it is not the only source of such attacks. Looking back over several months, **Figure 3** shows a daily level of HTTP cmd.exe Request attacks ranging from the 100s into the low 1000s. The use of the IIS ISAPI Buffer Overflow attack shows itself in three bursts during late June and early July, after it was first announced and before Code Red spread wildly. In **Figure 2**, on August 5, and again since August 10, the numbers of HTTP cmd.exe Request attacks exceeding that of IIS ISAPI Buffer Overflow attacks indicates unusually high levels of HTTP cmd.exe Requests. The difference between the levels indicates thousands more HTTP cmd.exe Requests were being reported than Code Red II was generating. We can assume that attackers are actively attempting to exploit vulnerable systems.

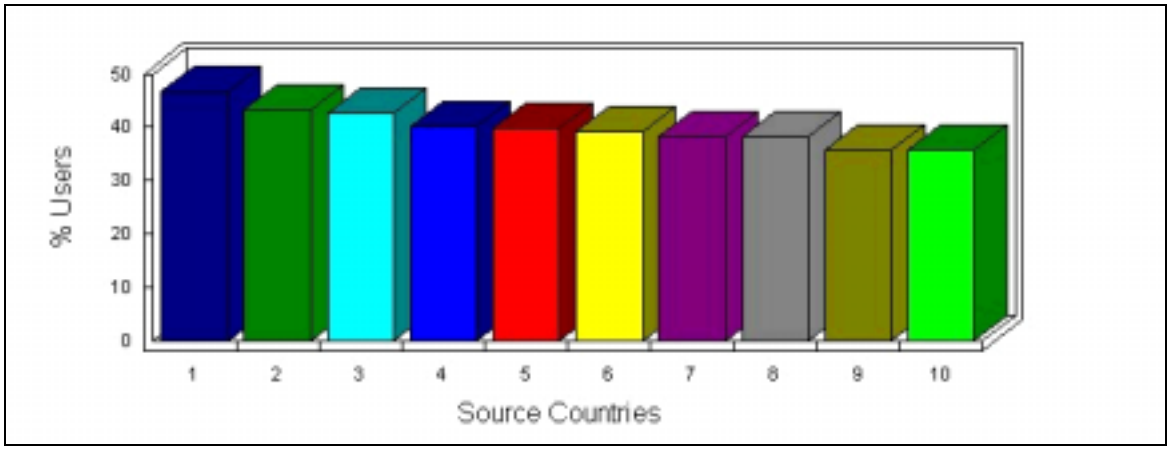


Attacks	% Users	# Attacks
Microsoft Indexing Server/Indexing Services ISAPI Buffer Overflow Attack	1.04	595204
Generic HTTP 'cmd.exe' Request Attack	0.78	214356

Figure 3 — Daily Level of HTTP cmd.exe Request Attacks for the Past Three Months

Figure 4 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. The numbers of ARIS users reporting the attacks fall within a small range, indicating the successful spread of these worms across the Internet. We have found no indication of this worm's source. The code changes its actions slightly if the local system language is Chinese. Otherwise, this worm's intent is not overtly political. Its objective appears to be to provide unauthorized remote access. Such large numbers of compromised systems could be enlisted in large-scale Distributed DoS attacks.

Copyright © 2001 SecurityFocus



	Attacking Country	# Users	% Users	# Attacks
1	United States	93	46.73	248651
2	Korea	86	43.22	143273
3	Netherlands	85	42.71	12606
4	Taiwan	80	40.20	34400
5	China	79	39.70	18816
6	Canada	78	39.20	34361
7	Germany	76	38.19	10224
8	Italy	76	38.19	9655
9	France	71	35.68	8718
10	United Kingdom	71	35.68	17562

Figure 4 — 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. You can find their full analysis and disassembly at 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 the 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 (and 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 then jumps to propagation, because that will no longer be the first execution.
- Calls the Trojan functions.
- Sleeps for one day on a non-Chinese system, or two days on a Chinese system.
- Reboots the system (which removes any memory-resident worms, leaving only the backdoors and explorer.exe Trojan).

Copyright © 2001 SecurityFocus

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

- Checks local time. If the year is before 2002 and the month is before October, then it continues. Otherwise, it reboots. 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. The worm uses nonblocking sockets, which gives a performance advantage.
- If the worm gets a connection, it sends a copy of itself (so far, all copies are identical; no self-modifying code exists).
- Repeat.

The most interesting piece is how Code Red II selects a new victim IP address to try. The worm generates four 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 from 0 through 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
```

This table 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, the address selection stays within the equivalent of a Class B of the attacker; 4 times out of 8, the selection stays within a Class A equivalent; and 1 time out of 8, the selection 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 Code Red II worm favors nearby IP addresses that tend to have similar host types (such as 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 internal network using addresses specified in RFC1918, it would likely be much more damaging to that network than previous worms.

Also note that the worm tests for and rejects addresses in the 127.x.x.x and 224.x.x.x ranges.

Finally, the worm installs backdoors during the Trojan step. The worm takes the following steps during this phase:

- Gets the system directory (usually C:\winnt\system32).
- Appends cmd.exe to the string.

Copyright © 2001 SecurityFocus

- 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.
- Repeats the steps for drive D: instead of C:.

The Trojan explorer.exe is not 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 the MS00-052 patch has not been applied, it executes 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 ten minutes

The Virtual Roots ensure that the scripts and msadc directories stay mapped, and maps C and D virtual roots that do not normally exist. These are mapped to the drive roots, which gives 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 scripts and msadc directories under the IIS Web root. You should delete these files, because they are copies of cmd.exe, and will permit remote access to your Web server. In addition, a file named explorer.exe is created in the root of C: and D: if it exists. See the Recommendations section for steps in recovering from this worm.

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

Copyright © 2001 SecurityFocus

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 we released publicly on the SecurityFocus incidents list early on 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 for Code Red II. These logs have 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 searched through their logs to track down who had specific dynamic IP addresses at certain times, and notified them that they were infected.

Copyright © 2001 SecurityFocus

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

Field Office

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

Copyright © 2001 SecurityFocus