

Dissecting Distributed Malware Networks

Dave Dittrich

University of Washington

<dittrich @ cac.washington.edu>

Overview

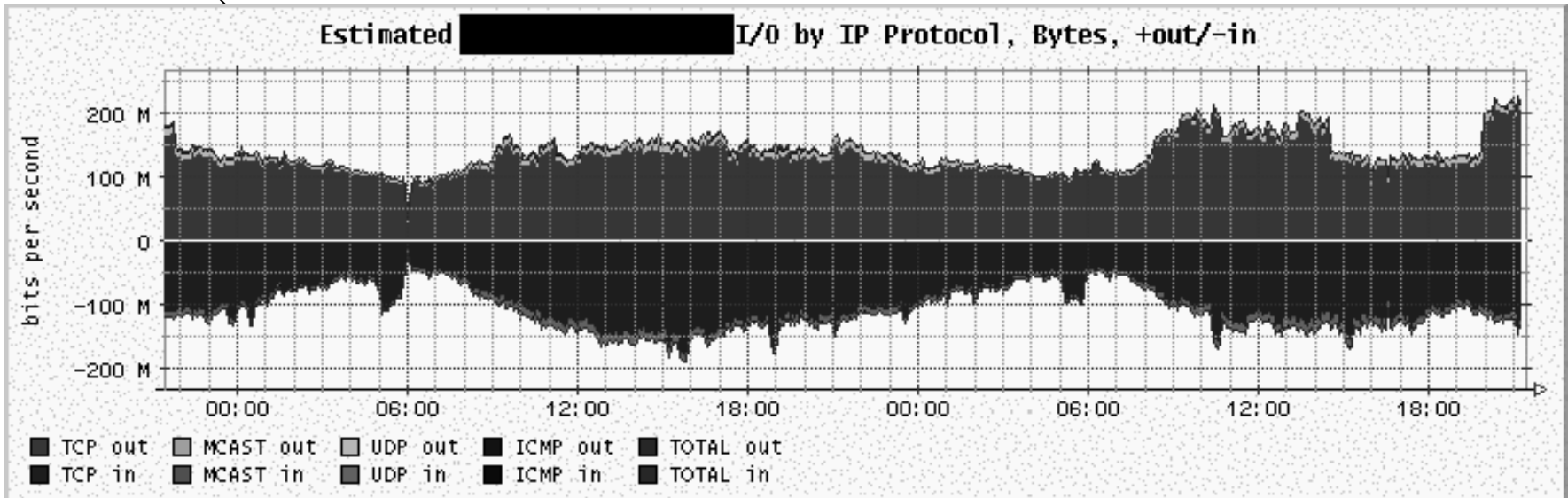
- Introduction
 - Why this talk?
 - Review of DDoS
 - Response Strategy
- Tools
 - Network Forensics
 - Host Forensics
- Attack scenario (tactics)
- Conclusion

Why this talk?

- This is *not* a new problem
- D{DoS|warez|BNC|scanning} very much alive
(Power, knight.exe, GTbot, X-DCC)
- **Bandwidth** vs. **Access** vs. *Security*
- Broadband, DSL, .edu = = MESS!
- Chaos is the norm

Why this talk?

- Some networking tools aren't keeping up with attack tools



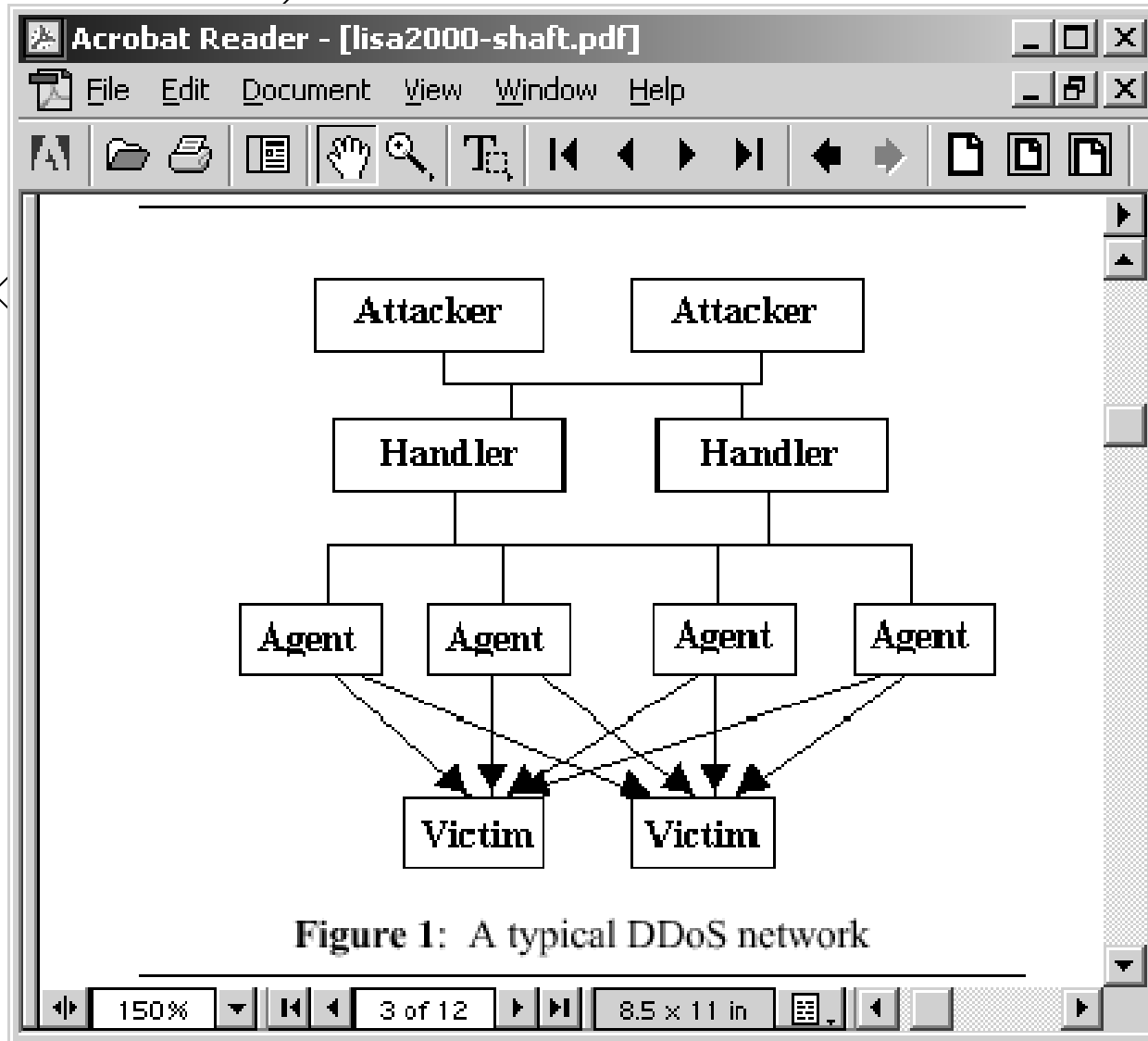
Why this talk?

- To improve the state of network analysis

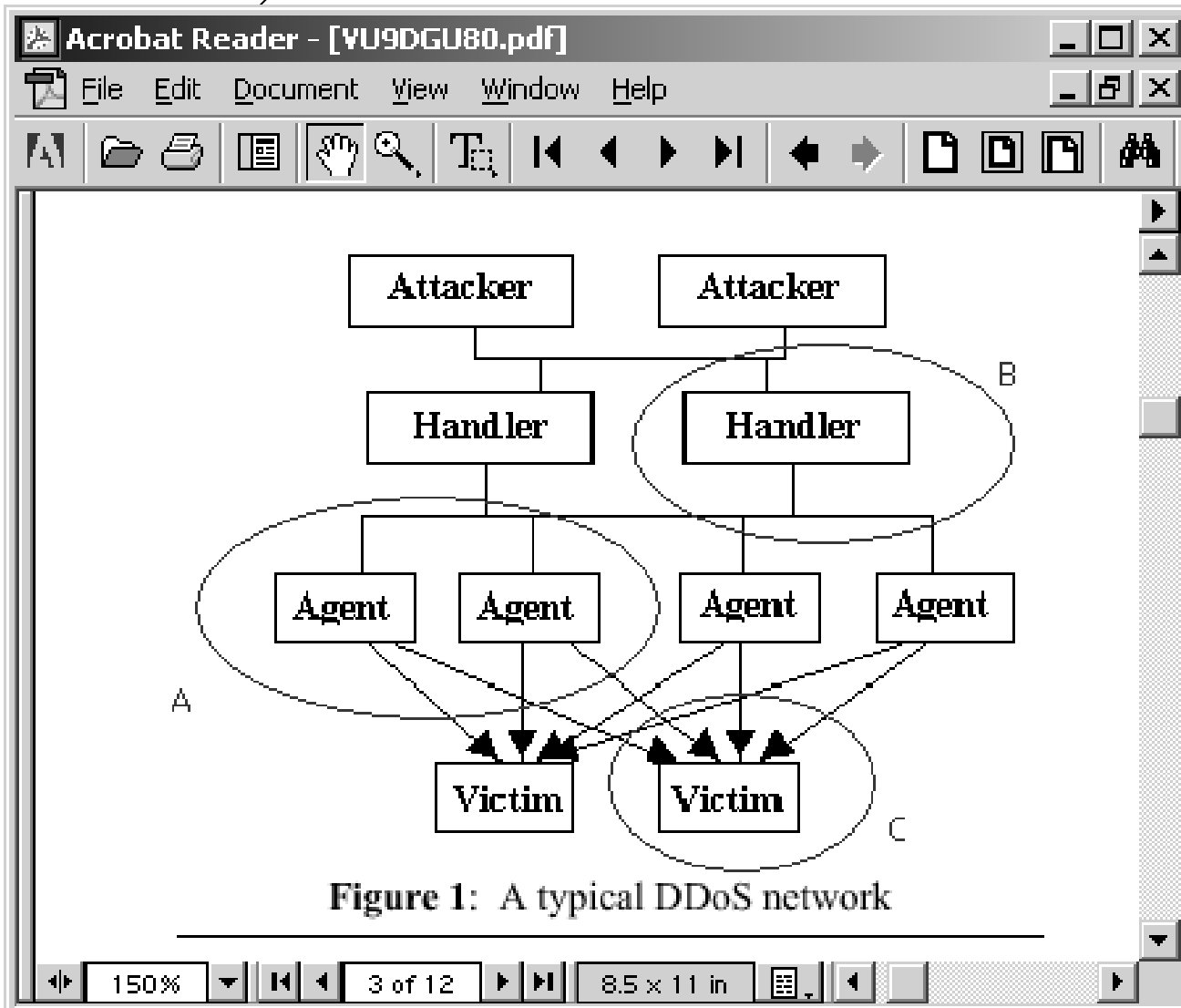
These networks CAN be taken down, if response is disciplined, coordinated, and efficient

*[http://www.cert.org/reports/
dsit_workshop.pdf](http://www.cert.org/reports/dsit_workshop.pdf)*

Review of DDoS



Review of DDoS



Strategies

- Analyze attack traffic (*find agents*)
- Analyze command/control traffic (*find agents & handlers, identify victims & attackers, etc.*)
- Identify signatures of tool (*find artifacts, define cleanup procedures*)
- Pass along intelligence to other sites (*take down entire network, not just 1%*)
- ***RESPECT PRIVACY RIGHTS!!!***
- Remember for future reference! (*They're BA-ACK!*)

Preparation

- Assemble tools
- Negotiate procedures
- Practice
- Execute
 - Coordinate
 - Communicate

Tools

Data Collection Tools

- libpcap/tcpdump
- Support scripts
- Snort, Ethereal also useful
(these are not covered here)

libpcap / tcpdump

- Standard packet capture interface
- Common dump format
- Basic packet decoding features
- Filters packets various ways

<http://www.tcpdump.org/>

tcpdump examples

```
# tcpdump -s 64 -w dos-04282002.dump
```

```
# tcpdump -r dos-04282002.dump ip proto 255
```

```
# tcpdump -s 0 -w irc-04282002.dump \  
tcp port 6667 or tcp port 7000
```

```
# tcpdump -r irc-04282002.dump \  
-w suspect-irc.dump "(ip host 192.168.0.1 \  
and port 1234) or ip net 10.1.1.0/24"
```

[http://www.eas.asu.edu/~ieeecs/pages/
springCalendar_99/resource/intro.ppt](http://www.eas.asu.edu/~ieeecs/pages/springCalendar_99/resource/intro.ppt)

Data Analysis Tools

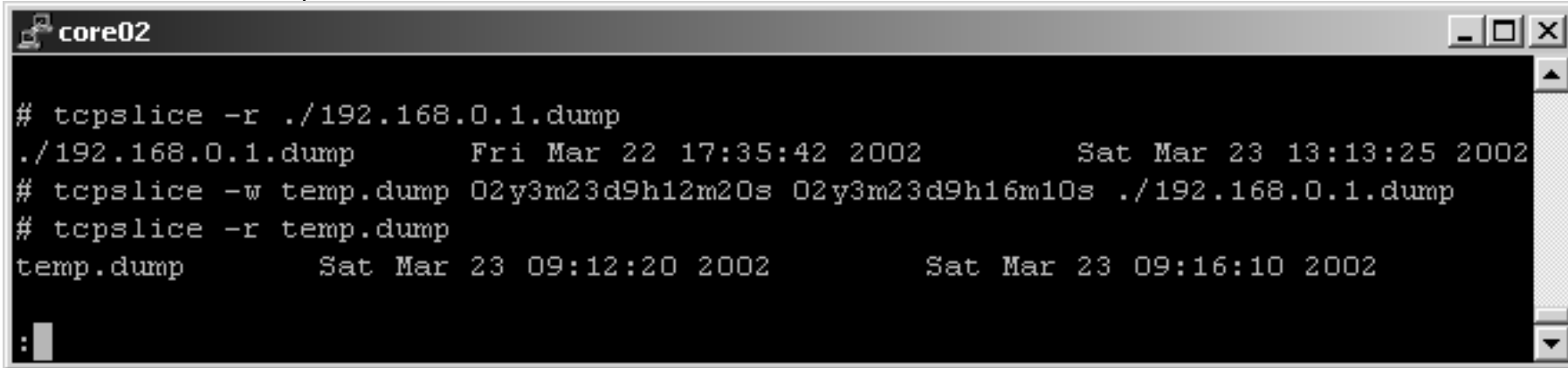
- tcpslice
- tcpdstat
- tcptrace
- ngrep
- ipgrep
- Graphing utilities

tcpslice

- Slices tcpdump files by start/end time
- Shows start/end times
- Merges tcpdump files

<ftp://ftp.ee.lbl.gov/tcpslice.tar.gz>

tcpslice example



```
core02
# tcpslice -r ./192.168.0.1.dump
./192.168.0.1.dump      Fri Mar 22 17:35:42 2002      Sat Mar 23 13:13:25 2002
# tcpslice -w temp.dump 02y3m23d9h12m20s 02y3m23d9h16m10s ./192.168.0.1.dump
# tcpslice -r temp.dump
temp.dump              Sat Mar 23 09:12:20 2002      Sat Mar 23 09:16:10 2002
```


tcpdstat

- Traffic Statistics
- Protocol breakdown
- My simple mods
 - More protocols
 - Peak flow rate
 - Compile on Linux

<http://staff.washington.edu/dittrich/misc/core02/tcpdstat-uw.tgz>

tcpdstat example

```
core02
PINE 4.44  MESSAGE TEXT  Folder: INBOX  Message 13,900 of 13,910 65%

DumpFile: /log/core02-02.dump
FileSize: 386.15MB
Id: 200204292150
StartTime: Mon Apr 29 21:50:44 2002
EndTime: Mon Apr 29 21:54:45 2002
TotalTime: 240.57 seconds
TotalCapSize: 312.60MB  CapLen: 68 bytes
# of packets: 4820393 (418.34MB)
AvgRate: 28.12Mbps  stddev:8.00M  PeakRate: 40.08Mbps

### IP flow (unique src/dst pair) Information ###
# of flows: 15 (avg. 321359.53 pkts/flow)
Top 10 big flow size (bytes/total in %):
100.0% 0.0% 0.0% 0.0% 0.0% 0.0% 0.0% 0.0% 0.0% 0.0%

### IP address Information ###
# of IPv4 addresses: 15
Top 10 bandwidth usage (bytes/total in %):
100.0% 100.0% 0.0% 0.0% 0.0% 0.0% 0.0% 0.0% 0.0% 0.0%

? Help      < MsgIndex  P PrevMsg   - PrevPage  D Delete    R Reply
C OTHER CMDS > ViewAttch W NextMsg   Spc NextPage  U Undelete  F Forward
```

tcpdstat example (cont)

```
core02
PINE 4.44 MESSAGE TEXT Folder: INBOX Message 13,900 of 13,912 95%
<<<<
[ 32- 63]: 36
[ 64- 127]: 4820357
>>>>

### Protocol Breakdown ###
<<<<
      protocol          packets          bytes          bytes/pkt
-----
[0] total                4820393 (100.00%)    438656698 (100.00%)    91.00
[1] ip                   4820393 (100.00%)    438656698 (100.00%)    91.00
[2] tcp                   36 ( 0.00%)         2160 ( 0.00%)         60.00
[3] other                 36 ( 0.00%)         2160 ( 0.00%)         60.00
[2] udp                  4820261 (100.00%)    438643751 (100.00%)    91.00
[3] other                 4820261 (100.00%)    438643751 (100.00%)    91.00
[2] icmp                 96 ( 0.00%)         10787 ( 0.00%)        112.36
>>>>

[New mail to you! From thegnome with regard to A special good tool]
? Help < MsgIndex P PrevMsg - PrevPage D Delete R Reply
C OTHER CMDS > ViewAttch N NextMsg Spc NextPage U Undelete F Forward
```

tcptrace

- Reports on streams
- Produces flow graphs
- Reconstructs streams

<http://jarok.cs.ohiou.edu/software/tcptrace/tcptrace.html>

tcptrace example

```
core02
# tcptrace -b test.dump
1 arg remaining, starting with 'test.dump'
Ostermann's tcptrace -- version 6.0.1 -- Mon Dec  3, 2001

718 packets seen, 689 TCP packets traced
elapsed wallclock time: 0:00:08.977980, 79 pkts/sec analyzed
trace file elapsed time: 0:00:33.971287
TCP connection info:
1: 192.168.8.128:1428 - 62.73.7.40:80 (a2b)          68> 126<
2: 192.168.8.128:1429 - 62.73.7.40:80 (c2d)          47>  87<
3: 192.168.8.128:1431 - 216.52.245.204:80 (e2f)           6>   5< (reset)
4: 192.168.8.128:1433 - adj31.thruport.com:80 (g2h)       5>   6< (complete)
5: 192.168.8.128:1435 - 208.249.124.247:80 (i2j)         5>   5< (complete)
6: 192.168.8.128:1436 - adj31.thruport.com:80 (k2l)       5>   5< (complete)
7: 192.168.8.128:1438 - 216.52.245.204:80 (m2n)           6>   5< (reset)
8: 192.168.8.128:1439 - 208.249.124.247:80 (o2p)         5>   5< (complete)
9: 192.168.8.128:1441 - 216.52.245.201:8000 (q2r)        5>   5< (complete)
10: 192.168.8.128:1442 - 216.52.245.201:8000 (s2t)        6>   7< (complete)
11: 192.168.8.128:1443 - 216.52.245.201:8000 (u2v)       7>   9< (complete)
12: 192.168.8.128:1444 - 216.52.245.201:8000 (w2x)       5>   5< (complete)
13: 192.168.8.128:1446 - 209.132.120.171:80 (y2z)        9>  14<
14: 192.168.8.128:1447 - 216.52.245.201:8000 (ba2bb)     5>   5< (complete)
15: 192.168.8.128:1448 - 216.52.245.201:8000 (bc2bd)     6>   7< (complete)
```

tcptrace example

```
core02
# tcptrace -e -o1 test.dump
1 arg remaining, starting with 'test.dump'
Ostermann's tcptrace -- version 6.0.1 -- Mon Dec  3, 2001

718 packets seen, 689 TCP packets traced
elapsed wallclock time: 0:00:01.819971, 394 pkts/sec analyzed
trace file elapsed time: 0:00:33.971287
TCP connection info:
  1: 192.168.8.128:1428 - 62.73.7.40:80 (a2b)   68> 126<

# cat a2b_contents.dat
GET / HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-
powerpoint, application/vnd.ms-excel, application/msword, /*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)
Host: www.desktopgirls.com
Connection: Keep-Alive

GET /frame-intro.htm HTTP/1.1
Accept: /*
Referer: http://www.desktopgirls.com/
```

ngrep

- Identifies strings in network traffic
- Supports RE and byte arrays (hex)
- Only clear text (of course)

<http://www.packetfactory.net/ngrep/>

ngrep example

```
core02
# ngrep -q -t -I 192.168.0.1.dump "*" tcp port 6423
input: 192.168.0.1.dump

T 2002/03/22 17:36:36.273828 10.87.100.214:2863 -> 192.168.0.1:6423 [AP]
  TYPE I..

T 2002/03/22 17:36:36.274430 192.168.0.1:6423 -> 10.87.100.214:2863 [AP]
  200 Type set to I..

T 2002/03/22 17:36:36.402443 10.87.100.214:2863 -> 192.168.0.1:6423 [AP]
  SIZE Marry.A.Rich.Man.VCD.Retail.A.R07..

T 2002/03/22 17:36:36.407593 192.168.0.1:6423 -> 10.87.100.214:2863 [AP]
  213 15000000..

T 2002/03/22 17:36:36.549508 10.87.100.214:2863 -> 192.168.0.1:6423 [AP]
  PASV..

T 2002/03/22 17:36:36.550710 192.168.0.1:6423 -> 10.87.100.214:2863 [AP]
  227 Entering Passive Mode (192.168.0.1,5,241)..

T 2002/03/22 17:36:36.828602 10.87.100.214:2863 -> 192.168.0.1:6423 [AP]
  RETR Marry.A.Rich.Man.VCD.Retail.A.R07..

T 2002/03/22 17:36:36.839161 192.168.0.1:6423 -> 10.87.100.214:2863 [AP]
```


Host Analysis Tools

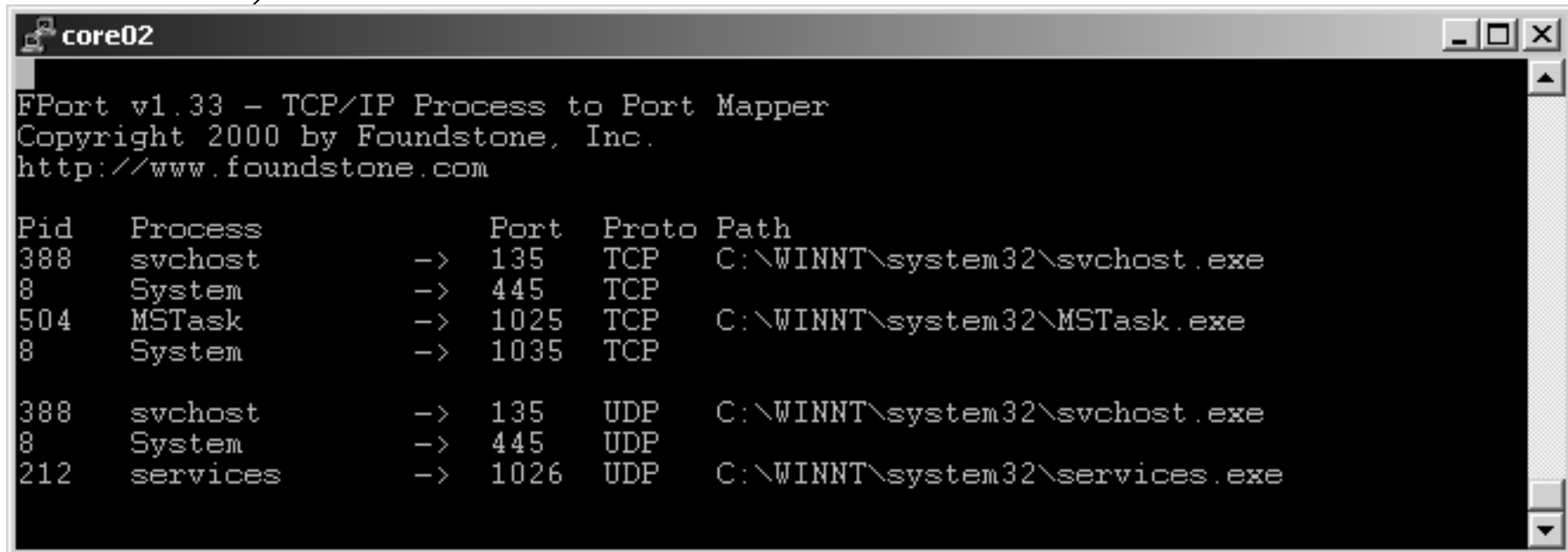
- Foundstone's Fport
- Anti Virus software (if used properly)
- @Stake's TASK
- Farmer/Venema's TCT

FPort

- Shows open ports
- ...and processes that hold them
- Windows tool (use “lsof” on Unix)

<http://www.foundstone.com/knowledge/proddesc/fport.html>

FPort example



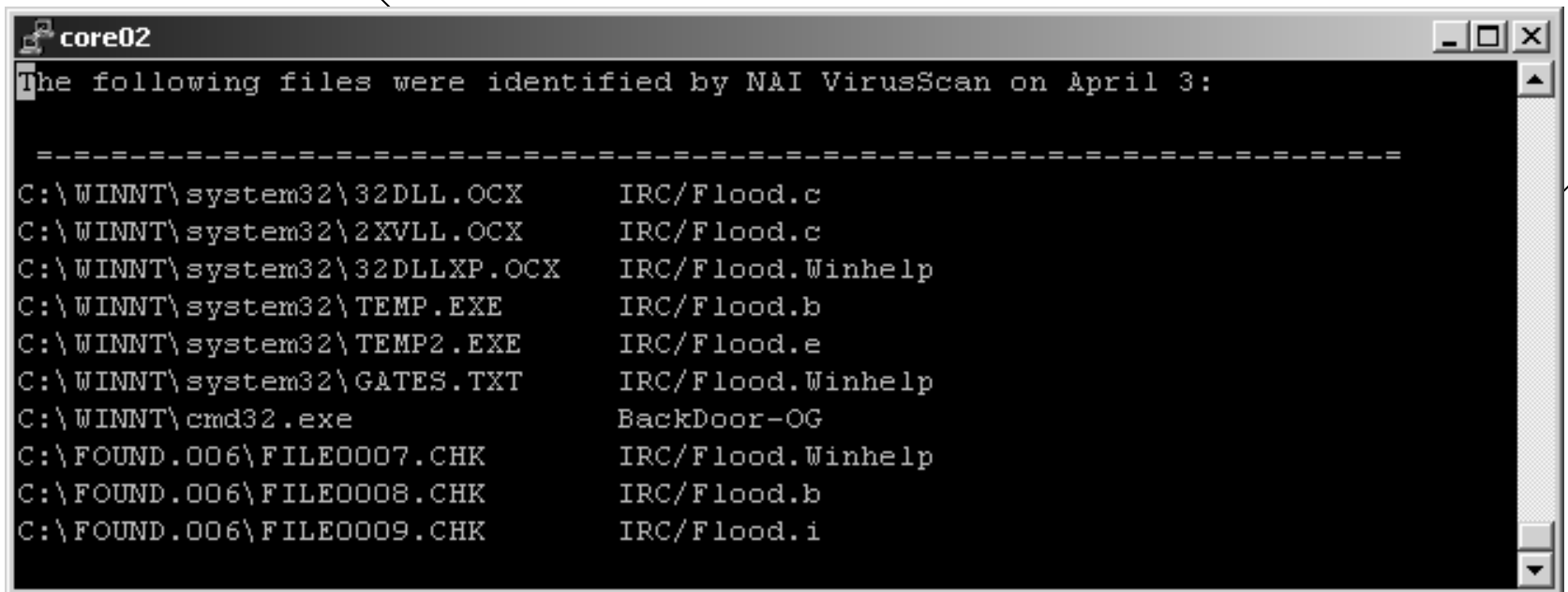
The screenshot shows a window titled 'core02' with the following text:

```
FPort v1.33 - TCP/IP Process to Port Mapper  
Copyright 2000 by Foundstone, Inc.  
http://www.foundstone.com
```

Pid	Process	Port	Proto	Path
388	svchost	-> 135	TCP	C:\WINNT\system32\svchost.exe
8	System	-> 445	TCP	
504	MSTask	-> 1025	TCP	C:\WINNT\system32\MSTask.exe
8	System	-> 1035	TCP	
388	svchost	-> 135	UDP	C:\WINNT\system32\svchost.exe
8	System	-> 445	UDP	
212	services	-> 1026	UDP	C:\WINNT\system32\services.exe

Anti-Virus Software

- Disable auto-delete before scan
- Use latest virus signature files
- Not 100% reliable analyses



```
core02
The following files were identified by NAI VirusScan on April 3:

-----
C:\WINNT\system32\32DLL.OCX      IRC/Flood.c
C:\WINNT\system32\2XVLL.OCX     IRC/Flood.c
C:\WINNT\system32\32DLLXP.OCX   IRC/Flood.Winhelp
C:\WINNT\system32\TEMP.EXE      IRC/Flood.b
C:\WINNT\system32\TEMP2.EXE     IRC/Flood.e
C:\WINNT\system32\GATES.TXT     IRC/Flood.Winhelp
C:\WINNT\cmd32.exe              BackDoor-OG
C:\FOUND.006\FILE0007.CHK      IRC/Flood.Winhelp
C:\FOUND.006\FILE0008.CHK      IRC/Flood.b
C:\FOUND.006\FILE0009.CHK      IRC/Flood.i
```

McAfee - AVERT - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites History Print Mail

Address http://vil.nai.com/vil/content/v_98936.htm Go Links

program infects your machine. The Visual Basic 6 runtime files are required for this worm to function. The following files are extracted into the Windows System directory upon running IRC/Flood:

GATES.TXT	Contains a list of IP addresses
MIRC.INI	Contains BOT instructions for mIRC
MIRC2.INI MIRC3.INI	Contains BOT & flooding instructions for mIRC
PR.INI	Cleanup instructions
TEMP.EXE	UPX packed mIRC client program
TEMP.SCR	List of usernames
TEMP2.EXE	Program that keeps other programs from appearing in the taskbar
WHVLXD.DAT	Configuration file
WHVLXD.EXE	Loader Program

The following key value is created in some variants to launch the trojan at system start:
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\
Run\WHVLXD="C:\WINDOWS\SYSTEM\WHVLXD.exe"

The WIN.INI file may also be modified to run the worm at system startup.

[Top of Page](#)

Symptoms

- Presence of the files previously mentioned
- Prompt to locate the file "C:\WINDOWS\SYSTEM\MIRC.HLP"
- DOS windows appearing running PING.EXE

[Top of Page](#)

Internet



[Buy Products](#) [Try Products](#) [Download Updates](#)



[Products](#) [Downloads](#) [Support](#) [Services](#) [AVERT](#) [Partners](#) [About McAfee](#)

[Virus Alerts](#)

[Anti-Virus Updates](#)

[Virus Information Library](#)

- [Overview](#)
- [Newly Discovered Viruses](#)
- [Recently Updated Viruses](#)
- [Hoaxes](#)
- [Virus Calendar](#)
- [White Papers](#)

[AVERT Research Center](#)

[AVERT WebImmune](#)

Virus Information Library

[Search again](#)

Search Results:

- | | |
|------------------------------------|---|
| Backdoor-K.sfx | BackDoor-G |
| Armaqeddon | W95/Kuang.GR |
| VBS/Fool | BackDoor-AB |
| Trojan Sockets.svr | BackDoor-Sub7 |
| BackDoor-J | BackDoor-AQ |
| JS/Judgement | IRC/Bat |
| Wincrash.svr | BackDoor-DB.svr |
| BackDoor-EP.svr | W97M/Reploq.a |
| Downloader | Fake First Aid 6.03 Upgrade |
| W32/QAZ.worm | New BackDoor |
| BackDoor-CI | W95/MTX.gen@M |
| BackDoor-GZ | BackDoor-HC |
| Erap Estrada | Backdoor-HJ |
| Backdoor-CT | Backdoor-IW |

TASK

- Graphical interface (autopsy)
- Direct file system processing
- Supports FAT16/FAT32 (NTFS in development)

<http://www.atstake.com/research/tools/task/>

The Coroner's Toolkit

- Not just for Unix
- Image Windows FAT16/FAT32, mount on Linux
- Perform MAC time analysis

<http://project.honeynet.org/challenge/>

<http://staff.washington.edu/dittrich/misc/forensics/>

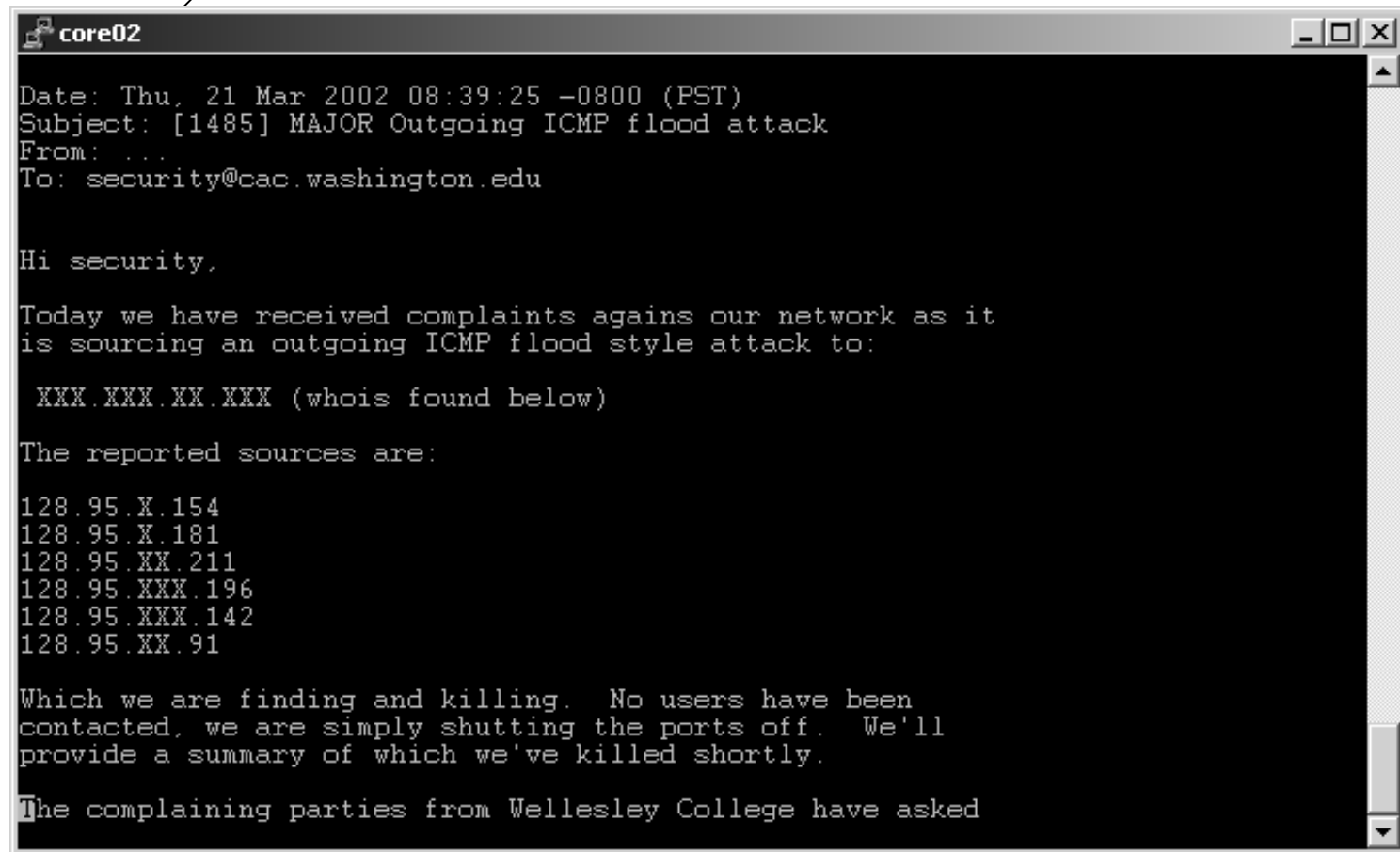
TCT (mactime) example

```
core02
Mar 09 02 07:09:54 293685 ma. -rwxr-xr-x root root /t/winnt/system32/XXXX/asp/cygwin1.dll
Mar 09 02 07:09:58 1220 ma. -rwxr-xr-x root root /t/winnt/system32/XXXX/asp/ir.con
Mar 09 02 07:10:46 226689 ma. -rwxr-xr-x root root /t/winnt/system32/XXXX/asp/svhost.exe
226689 ma. -rwxr-xr-x root root /t/winnt/system32/XXXX/aspc/svhost.exe
Mar 09 02 07:11:00 78848 ma. -rwxr-xr-x root root /t/winnt/system32/XXXX/asp/tar.exe
Mar 09 02 07:11:38 293685 ma. -rwxr-xr-x root root /t/winnt/system32/XXXX/aspc/cygwin1.dll
Mar 09 02 07:11:42 1396 ma. -rwxr-xr-x root root /t/winnt/system32/XXXX/aspc/ir.con
Mar 09 02 07:11:56 981 ma. -rwxr-xr-x root root /t/winnt/system32/XXXX/32dllemu.txt
Mar 09 02 07:12:12 81920 ma. -rwxr-xr-x root root /t/winnt/system32/XXXX/firedaemon.exe
Mar 09 02 07:12:20 31232 ma. -rwxr-xr-x root root /t/winnt/system32/XXXX/inetserv.exe
Mar 09 02 07:12:28 35600 ma. -rwxr-xr-x root root /t/winnt/system32/XXXX/kill.exe
Mar 09 02 07:12:34 34304 ma. -rwxr-xr-x root root /t/winnt/system32/XXXX/pulist.exe
Mar 09 02 07:12:46 73216 ma. -rwxr-xr-x root root /t/winnt/system32/XXXX/services.exe
```

Attack scenario (Tactics)

Responding to an Attack

- How it starts



```
core02
Date: Thu, 21 Mar 2002 08:39:25 -0800 (PST)
Subject: [1485] MAJOR Outgoing ICMP flood attack
From: ...
To: security@cac.washington.edu

Hi security,

Today we have received complaints agains our network as it
is sourcing an outgoing ICMP flood style attack to:

  XXX.XXX.XX.XXX (whois found below)

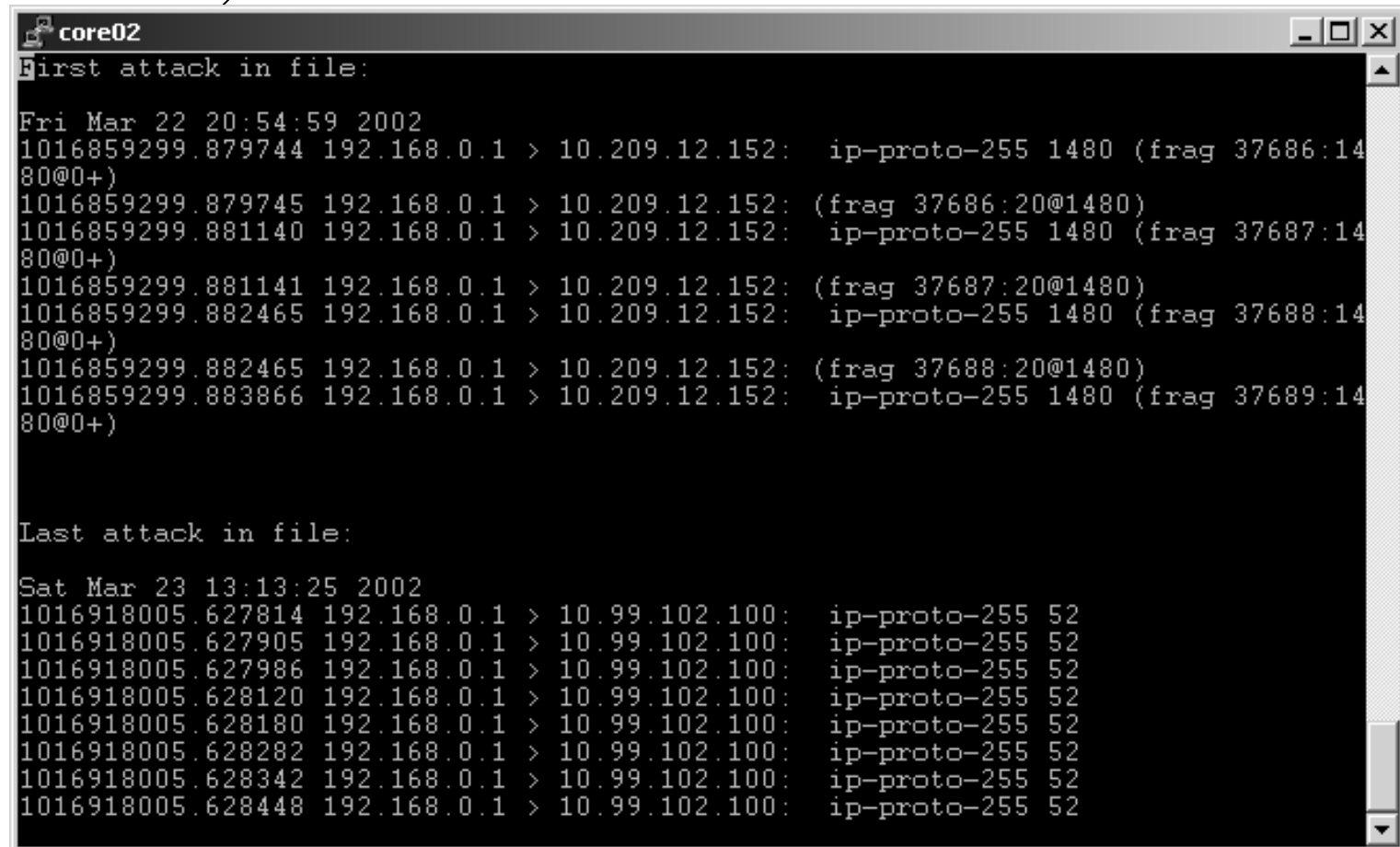
The reported sources are:

128.95.X.154
128.95.X.181
128.95.XX.211
128.95.XXX.196
128.95.XXX.142
128.95.XX.91

Which we are finding and killing.  No users have been
contacted, we are simply shutting the ports off.  We'll
provide a summary of which we've killed shortly.

The complaining parties from Wellesley College have asked
```

Using tcpdump to analyze attack traffic



```
core02
First attack in file:

Fri Mar 22 20:54:59 2002
1016859299.879744 192.168.0.1 > 10.209.12.152: ip-proto-255 1480 (frag 37686:1480@0+)
1016859299.879745 192.168.0.1 > 10.209.12.152: (frag 37686:20@1480)
1016859299.881140 192.168.0.1 > 10.209.12.152: ip-proto-255 1480 (frag 37687:1480@0+)
1016859299.881141 192.168.0.1 > 10.209.12.152: (frag 37687:20@1480)
1016859299.882465 192.168.0.1 > 10.209.12.152: ip-proto-255 1480 (frag 37688:1480@0+)
1016859299.882465 192.168.0.1 > 10.209.12.152: (frag 37688:20@1480)
1016859299.883866 192.168.0.1 > 10.209.12.152: ip-proto-255 1480 (frag 37689:1480@0+)

Last attack in file:

Sat Mar 23 13:13:25 2002
1016918005.627814 192.168.0.1 > 10.99.102.100: ip-proto-255 52
1016918005.627905 192.168.0.1 > 10.99.102.100: ip-proto-255 52
1016918005.627986 192.168.0.1 > 10.99.102.100: ip-proto-255 52
1016918005.628120 192.168.0.1 > 10.99.102.100: ip-proto-255 52
1016918005.628180 192.168.0.1 > 10.99.102.100: ip-proto-255 52
1016918005.628282 192.168.0.1 > 10.99.102.100: ip-proto-255 52
1016918005.628342 192.168.0.1 > 10.99.102.100: ip-proto-255 52
1016918005.628448 192.168.0.1 > 10.99.102.100: ip-proto-255 52
```

Use tcpdstat to analyze attack traffic

```
core02
DumpFile: 192.168.0.1.dump
Id: 200203221735
StartTime: Fri Mar 22 17:35:42 2002
EndTime: Sat Mar 23 13:13:25 2002
TotalTime: 70663.53 seconds
TotalCapSize: -681.87MB CapLen: 1514 bytes
# of packets: 167707807 (15702.13MB)
AvgRate: 2.07Mbps stddev:2.89M PeakRate: 12.16Mbps
. . .
### Protocol Breakdown ###
<<<<

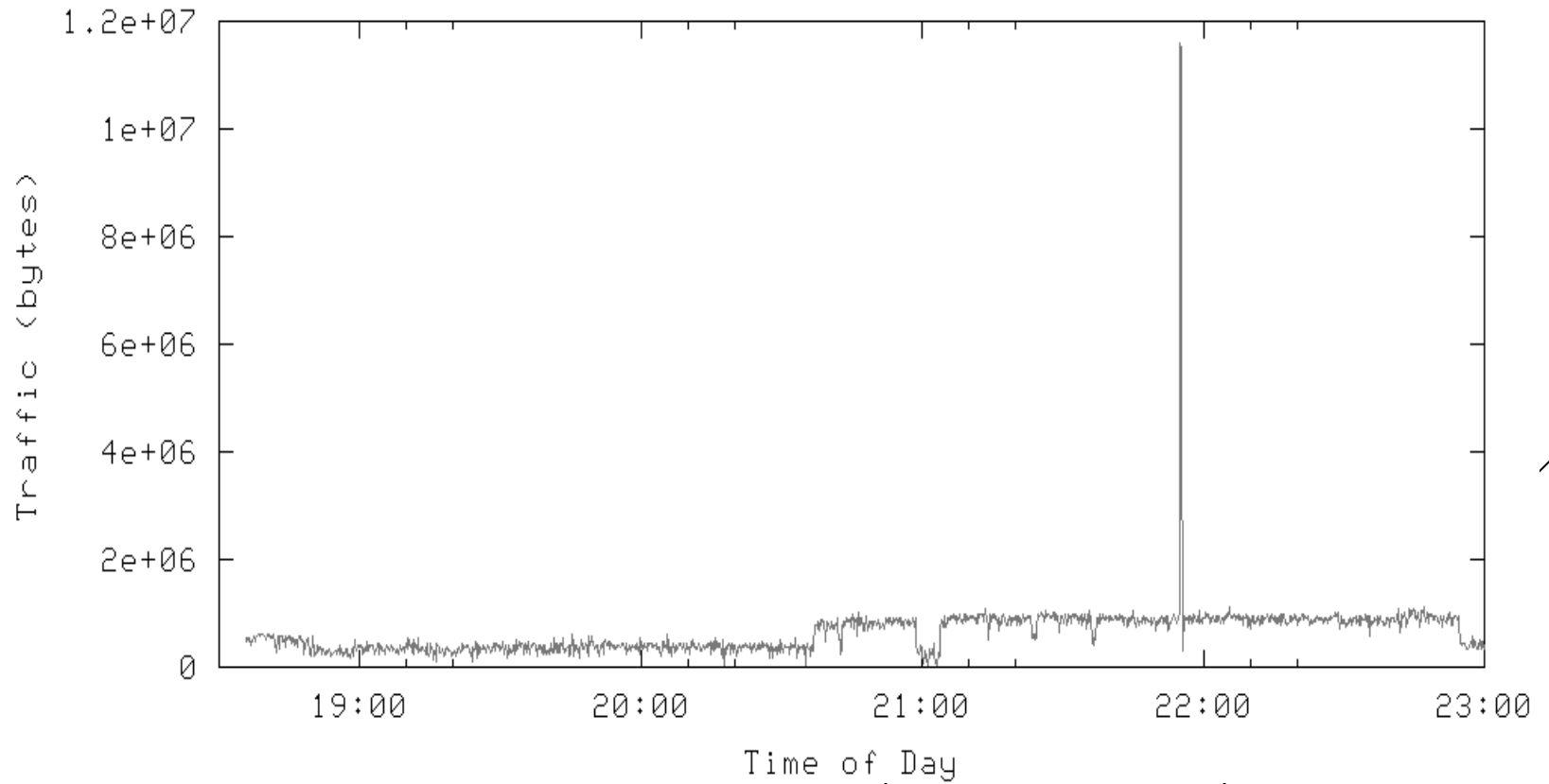
```

	protocol	packets	bytes	bytes/pkt
[0]	total	167707807 (100.00%)	16464877084 (100.00%)	98.18
[1]	ip	167707807 (100.00%)	16464877084 (100.00%)	98.18
[2]	tcp	2312006 (1.38%)	2223505740 (13.50%)	961.72
[3]	ftp	12 (0.00%)	742 (0.00%)	61.83
[3]	irc6667	6303 (0.00%)	669118 (0.00%)	106.16
[3]	http-a	2 (0.00%)	134 (0.00%)	67.00
[3]	other	2305620 (1.37%)	2222831025 (13.50%)	964.09
[2]	icmp	398486 (0.24%)	27952528 (0.17%)	70.15
[2]	res_255	164997315 (98.38%)	14213418816 (86.33%)	86.14

```
>>>>
```

First Attack

Bandwidth Utilization Stats



Statistics of first attack

```
core02
DumpFile:  dos1.dump
FileSize:  25.88MB
StartTime: Fri Mar 22 20:54:59 2002
EndTime:   Fri Mar 22 20:55:24 2002
TotalTime: 24.42 seconds
TotalCapSize: 25.36MB  CapLen: 1514 bytes
# of packets: 34153 (25.36MB)
AvgRate: 8.71Mbps  stddev:0.22M  PeakRate: 9.04Mbps

### Packet Size Distribution (including MAC headers) ###
<<<<
[  32-  63]:      17277
[ 1024- 2047]:   16876
>>>>

### Protocol Breakdown ###
<<<<

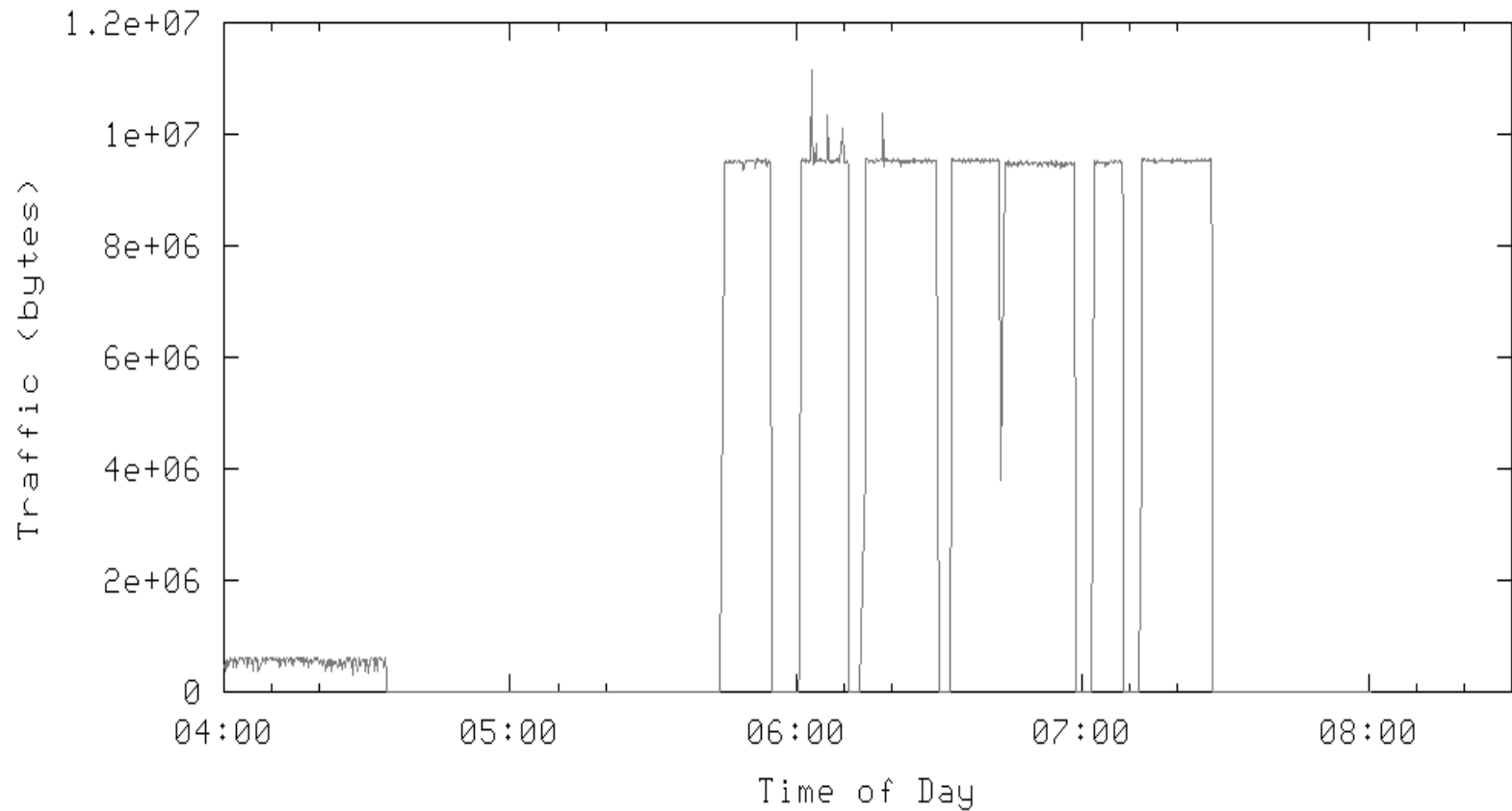
```

protocol	packets	bytes	bytes/pkt
[0] total	34153 (100.00%)	26586884 (100.00%)	778.46
[1] ip	34153 (100.00%)	26586884 (100.00%)	778.46
[2] res_255	34153 (100.00%)	26586884 (100.00%)	778.46

```
>>>>
```

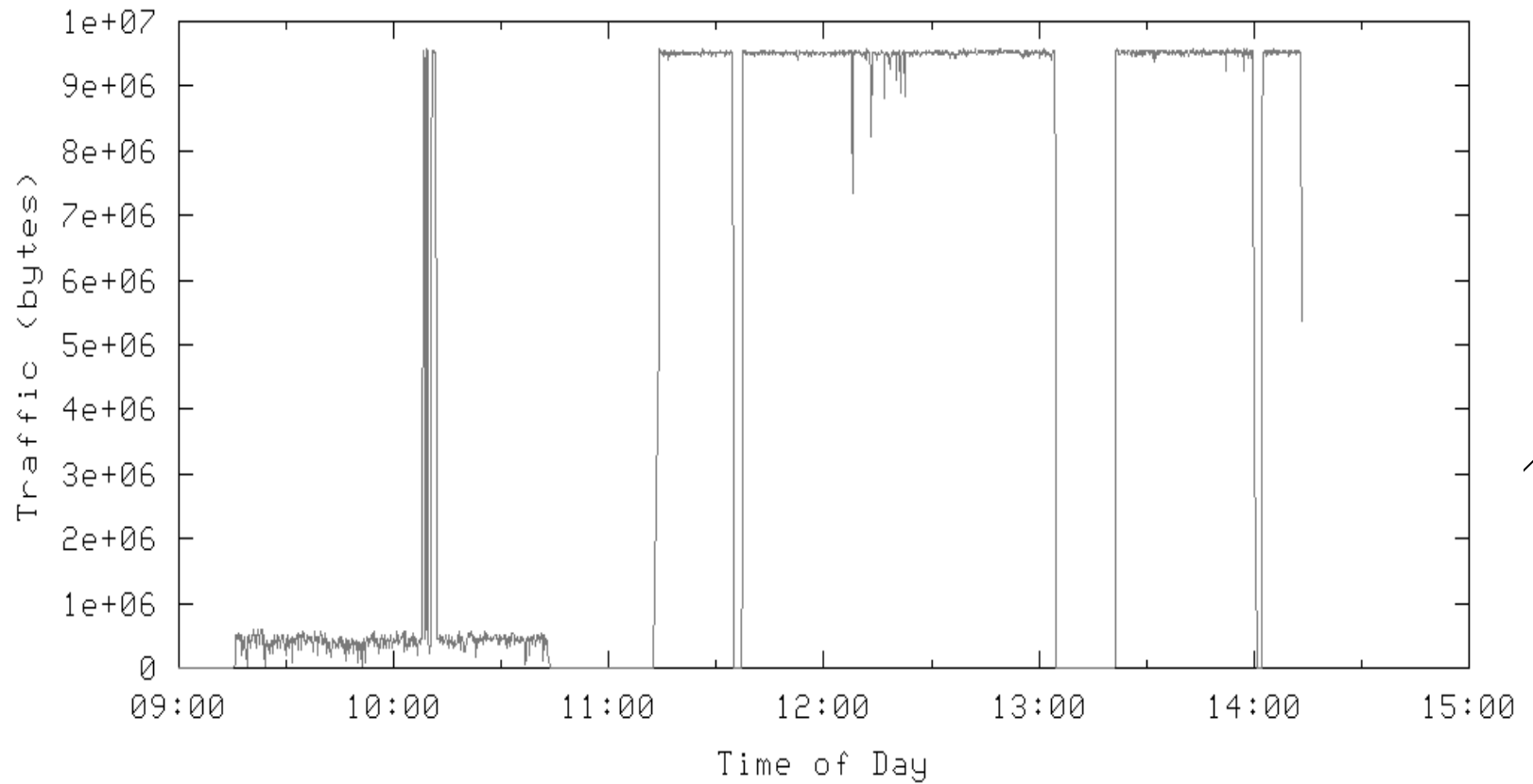
More Attacks

Bandwidth Utilization Stats



More Attacks

Bandwidth Utilization Stats



Using ngrep to find control traffic

```
core02
% ngrep -q -t -I 192.168.0.1.dump "10.209.12.152" | less
input: 192.168.0.1.dump

T 2002/03/22 20:54:59.858777 10.0.1.1:6667 -> 192.168.0.1:4895 [AP]
:foobarCKV!~XXXXXX@ns1.XXXXXX.XXXXXX.net PRIVMSG #%g :.@UDP 10
.209.12.152 38 500...

T 2002/03/22 20:54:59.860632 192.168.0.1:4895 -> 10.0.1.1:6667 [AP]
PRIVMSG #%g :*** [foobarJKV] UDP 10.209.12.152 38 500.

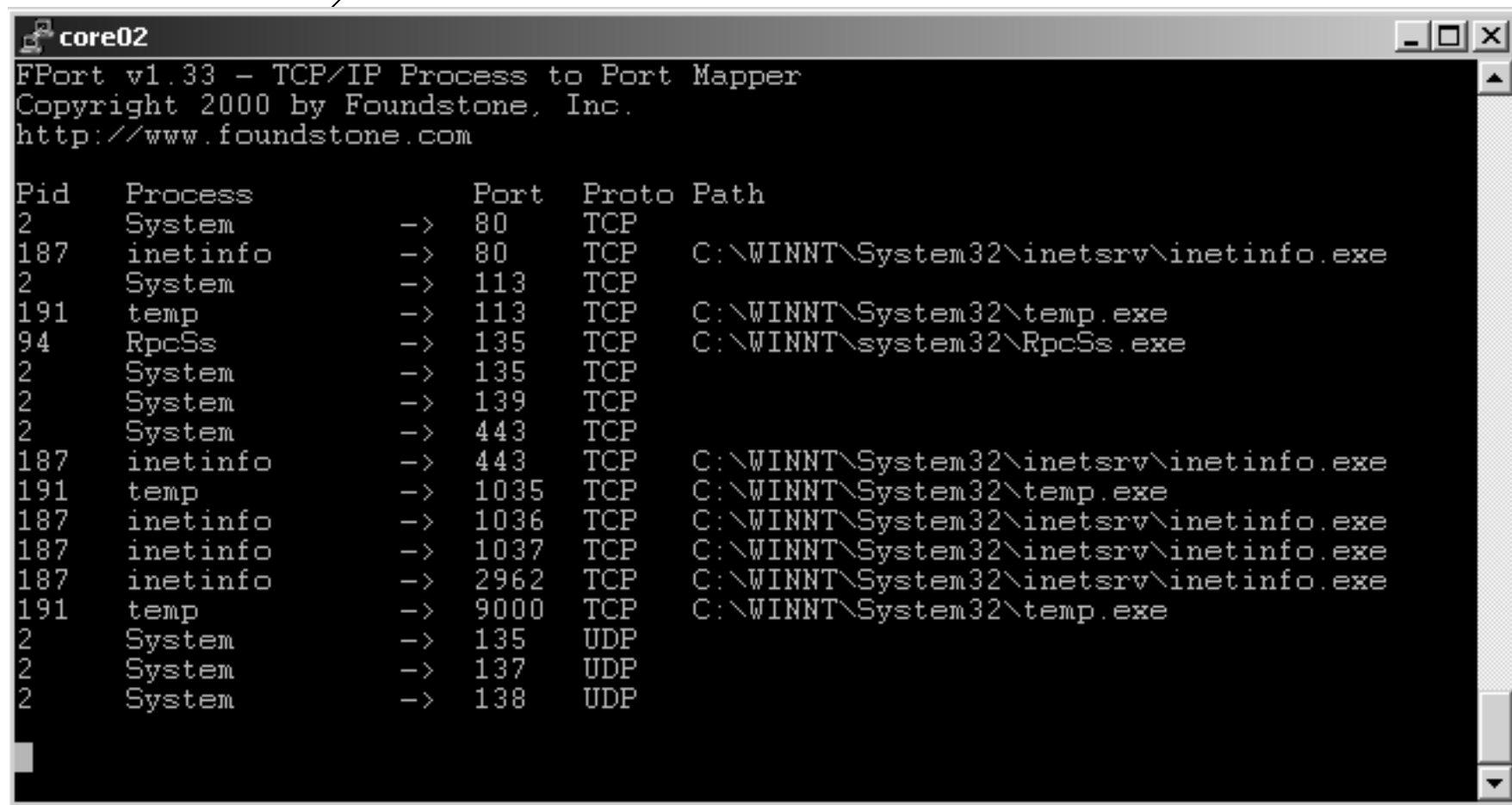
T 2002/03/22 20:54:59.926743 10.0.1.1:6667 -> 192.168.0.1:4895 [AP]
:foobarXRN!~XRN@XXXXXX-XXX-XXX.reshall.umich.edu PRIVMSG #%g :
*** [foobarJKV] UDP 10.209.12.152 38 500..

T 2002/03/22 20:54:59.930080 192.168.0.1:4895 -> 10.0.1.1:6667 [AP]
NOTICE foobarCRV :Packeting 10.209.12.152..

T 2002/03/22 20:54:59.982601 10.0.2.2:6667 -> 192.168.0.1:4869 [AP]
:foobarMTP!~MTP@XXXXXXXX-XXX.rh.rit.edu PRIVMSG #%g :*** [fooba
rJKV] UDP 10.209.12.152 38 500..

T 2002/03/22 20:54:59.996410 10.0.1.1:6667 -> 192.168.0.1:4895 [AP]
:foobarFYM!~FYM@XXXXXXXX-XXX-XX.reshall.umich.edu PRIVMSG #%g :*
```

Using Fport to correlate ports and programs



```
core02
FPort v1.33 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com

Pid    Process          Port  Proto Path
2      System           -> 80   TCP   C:\WINNT\System32\inetinfo.exe
187    inetinfo         -> 80   TCP   C:\WINNT\System32\inetinfo.exe
2      System           -> 113  TCP   C:\WINNT\System32\temp.exe
191    temp             -> 113  TCP   C:\WINNT\System32\temp.exe
94     RpcSs            -> 135  TCP   C:\WINNT\system32\RpcSs.exe
2      System           -> 135  TCP
2      System           -> 139  TCP
2      System           -> 443  TCP
187    inetinfo         -> 443  TCP   C:\WINNT\System32\inetinfo.exe
191    temp             -> 1035 TCP   C:\WINNT\System32\temp.exe
187    inetinfo         -> 1036 TCP   C:\WINNT\System32\inetinfo.exe
187    inetinfo         -> 1037 TCP   C:\WINNT\System32\inetinfo.exe
187    inetinfo         -> 2962 TCP   C:\WINNT\System32\inetinfo.exe
191    temp             -> 9000 TCP   C:\WINNT\System32\temp.exe
2      System           -> 135  UDP
2      System           -> 137  UDP
2      System           -> 138  UDP
```

Feedback from system owner

```
core02
Date: 21 Mar 2002 09:10 PST
Subject: Re: [1485] UW ICMP Attack Against Wellesley (fwd)
From: XXXXXXXXXXXX <XXXXXX@XXXX.washington.edu>
To: XXXXX@cac.washington.edu
Cc: XXXX@XXXXX.washington.edu, XXXXXXXX@XXXXX.washington.edu,
    netops@cac.washington.edu, security@cac.washington.edu

> We'd like 192.168.0.1 (XXXXX.XXXXX) removed from the network
> and looked at.

Our indications are this machine is no longer participating in the
attack.  The circumstances are approximately as follows:

    1) The machine's owner came in about an hour ago and found the
       CPU meter pegged.
    2) He discovered a program called "knight.exe" running.
    3) He killed the program, deleted the file (sigh!) and rebooted Windows.

We will attempt to find out how this occurred.
```

Identification of attack tool

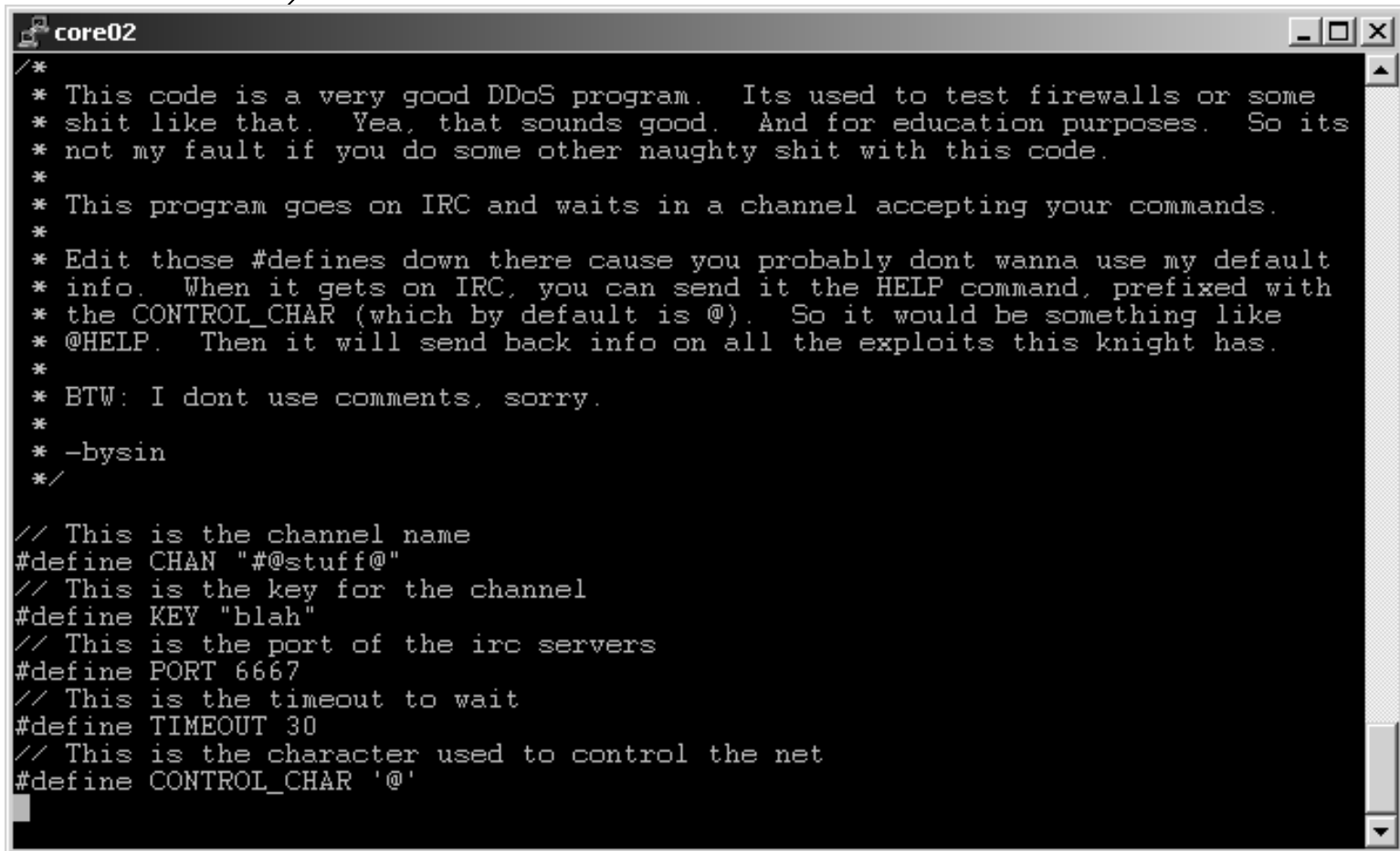


Find analysis/code

Microsoft Internet Explorer window showing the URL: <http://packetstormsecurity.nl/distributed/>

kaiten.c	39019	Dec 27 15:26:26 2001	74fe3d86afcbf6c801d1cc3c4d6e357d
Kaitan.c is an IRC based DDoS client. By contem.			
knight.c	34822	Jul 11 22:36:50 2001	30aded215fadd9c85bfc92da55f8fd4
Knight.c Knight is a distributed denial of service client that is very light weight and is very powerful. It goes on IRC and joins a channel, then accepts commands via IRC (to prevent from getting caught). It has features like, an automatic updater via http or ftp, a checksum generator, a syn flooder, a tcp flooder, a udp flooder, slice2, spoofing to subnets, and more. This program has been used to create DDoS nets of over 1000 clients. By Bysin.			
mio-star.tgz	9961	Apr 25 10:08:42 2000	38125314bcf691a20a4acf5974f43e02
The mio-star distributed multihosted unix password cracker v0.1 runs on all platforms where perl is installed. Comments and documentation is in German. By Drunken Monkey Style			
mstream.analysis.txt	97850	May 14 03:56:00 2000	82dd67ecacb8ff5731279209d4b70342
Analysis of the "mstream" distributed denial of service attack tool, based on the source code of "stream2.c", a classic point-to-point DoS attack tool. mstream is more primitive than any of the other DDoS tools. Homepage here . By Dave Dittrich			
mstream.txt	26473	May 1 12:52:04 2000	08ec36853347b7b88b5ac0f7f3f15685
mstream, a DDoS tool. It's been alleged that this source code, once compiled, was used by persons unknown in the distributed denial of service (DDoS) attacks earlier this year. Obviously such a thing cannot be confirmed aside from through a process of targeted sites making an appropriate comparison between the traffic this software would generate and the traffic they actually received. Submitted Anonymously.			
Mstream_Analysis.txt	98002	May 1 14:19:09 2000	d99d36bb136ad1b329fab03870d478df
Mstream, the newest of DDoS tools to be circulated, has been analyzed and has been found to be more primitive than any of			

Identify keys to control



```
core02
/*
 * This code is a very good DDoS program. Its used to test firewalls or some
 * shit like that. Yea, that sounds good. And for education purposes. So its
 * not my fault if you do some other naughty shit with this code.
 *
 * This program goes on IRC and waits in a channel accepting your commands.
 *
 * Edit those #defines down there cause you probably dont wanna use my default
 * info. When it gets on IRC, you can send it the HELP command, prefixed with
 * the CONTROL_CHAR (which by default is @). So it would be something like
 * @HELP. Then it will send back info on all the exploits this knight has.
 *
 * BTW: I dont use comments, sorry.
 *
 * -bysin
 */

// This is the channel name
#define CHAN "#@stuff@"
// This is the key for the channel
#define KEY "blah"
// This is the port of the irc servers
#define PORT 6667
// This is the timeout to wait
#define TIMEOUT 30
// This is the character used to control the net
#define CONTROL_CHAR '@'
```

Identify commands in source

```
core02
}
struct FMessages { char *cmd; void (* func)(int,char *,int,char **); } flooders[
] = {
    { "NICK", nickc },
    { "UPDATEHTTP", updatehttp },
    { "UPDATE", update },
    { "CHECKSUM", checksum },
    { "PAN", pan },
    { "MAJIN", majin },
    { "UDP", bysin },
    { "SLICE2", slice2 },
    { "GETSPOOFS", getspoofs },
    { "SPOOFS", spooft },
    { "DISABLE", disable },
    { "ENABLE", enable },
    { "DNS", dns },
    { "VERSION", version },
    { "KILLALL", killall },
    { "HELP", help },
    { "KILL", killdis },
    { (char *)0, (void (*)(int,char *,int,char **))0 } };
void _PRIVMSG(int sock, char *sender, char *str) {
    int i;
    char *to, *message;
    for (i=0;i<strlen(str) && str[i] != ' ';i++);
    str[i]=0;
    to=sender;
    message=sender+i+2;
}
```


Use tcptrace to isolate TCP stream

```
core02
1 arg remaining, starting with '192.168.0.1.dump'
Ostermann's tcptrace -- version 6.0.1 -- Mon Dec  3, 2001

167707807 packets seen, 2312006 TCP packets traced
elapsed wallclock time: 0:10:40.840262, 261699 pkts/sec analyzed
trace file elapsed time: 19:37:43.529375
TCP connection info:
 1: . . . .
 2: . . . .
 3: 10.0.1.1:6667 - 192.168.0.1:4895      (e2f)      2124> 1230<
 4: . . . .
 5: . . . .
 6: . . . .
 7: . . . .
 8: . . . .
 9: . . . .
10: . . . .
11: . . . .

# tcptrace -o3 -e 192.168.0.1.dump
# ls -l *_contents.dat
-rw-r--r--  1 root    daemon   98697 Apr 20 18:50 e2f_contents.dat
-rw-r--r--  1 root    daemon   31786 Apr 20 18:50 f2e_contents.dat
```

Identify attack victims

```
core02
# egrep "SLICE|UDP|MAJIN" f2e_contents.dat
PRIVMSG #%controlchan :*** [XXXXXX] SLICE2 128.208.XX.X 1 200 380
PRIVMSG #%controlchan :*** [XXXXXX] UDP 128.208.XX.X 38 400
PRIVMSG #%controlchan :*** [foobarJKV] UDP 10.209.12.152 38 500
PRIVMSG #%controlchan :*** [foobarJKV] SLICE2 10.89.192.250 1 200 600
PRIVMSG #%controlchan :*** [foobarJKV] SLICE2 10.83.176.20 1 200 600
PRIVMSG #%controlchan :*** [foobarJKV] SLICE2 10.83.176.20 1 200 900
PRIVMSG #%controlchan :*** [foobarJKV] SLICE2 10.170.226.2 1 200 900
PRIVMSG #%controlchan :*** [foobarJKV] SLICE2 10.26.242.104 1 200 900
PRIVMSG #%controlchan :*** [foobarJKV] SLICE2 10.226.209.42 1 200 900
PRIVMSG #%controlchan :*** [foobarJKV] SLICE2 10.231.1.180 1 200 900
PRIVMSG #%controlchan :*** [foobarJKV] SLICE2 10.231.1.180 1 200 900
PRIVMSG #%controlchan :*** [foobarJKV] SLICE2 10.231.1.180 1 200 900
PRIVMSG #%controlchan :*** [foobarJKV] SLICE2 10.83.176.20 1 200 450
PRIVMSG #%controlchan :*** [foobarJKV] SLICE2 10.63.82.26 1 200 450
PRIVMSG #%controlchan :*** [foobarJKV] SLICE2 10.99.102.100 1 200 450
PRIVMSG #%controlchan :*** [foobarJKV] SLICE2 10.126.96.163 1 200 450
PRIVMSG #%controlchan :*** [foobarJKV] SLICE2 10.116.202.58 1 200 450
PRIVMSG #%controlchan :*** [foobarJKV] SLICE2 10.99.102.100 1 200 1250
PRIVMSG #%controlchan :*** [foobarJKV] SLICE2 10.99.102.100 1 200 5250
PRIVMSG #%controlchan :*** [foobarJKV] SLICE2 10.99.102.100 1 200 9250
```

What's this?

```
core02
PRIVMSG #XXXXXXX :@find rogue
PRIVMSG #XXXXXXX :** 6 packs ** 0 of 20 slots open, Queue: 11/20, Min: 5.0KB/s, Record: 283.5KB/s
PRIVMSG #XXXXXXX :** Bandwidth Usage ** Current: 885.0KB/s, Cap: 3000.0KB/s, Record: 1087.7KB/s
PRIVMSG #XXXXXXX :** To request a file type: "/msg [XDCC]BOT-E340 xdcc send #x" **
PRIVMSG #XXXXXXX :#1 172x [433M] Scorpion King TS - CENTROPY - CD1
PRIVMSG #XXXXXXX :#2 120x [431M] Scorpion King TS - CENTROPY - CD2
PRIVMSG #XXXXXXX :#3 43x [286M] SIMON THE SORCERER 3D - DEVIANCE - CD1
PRIVMSG #XXXXXXX :#4 46x [332M] SIMON THE SORCERER 3D - DEVIANCE - CD2
PRIVMSG #XXXXXXX :#5 69x [298M] Bandits DVD DivX [1of3]
PRIVMSG #XXXXXXX :#6 10x [278M] Bandits DVD DivX [2of3]
PRIVMSG #XXXXXXX :#7 11x [298M] Bandits DVD DivX [3of3]
PRIVMSG #XXXXXXX :Total Offered: 2705.4 MB Total Transferred: 447.27 GB
```

networks of the Internet Relay Chat



specials: current channel charts



netsplit.de
 the summary
 the charts
 top 10 graphs
 links
 specials
 notes

- current channel charts
- servers by *reverse domain*
- list of daemons
- current network charts
- servers by *network*

channel	users	network	topic
1. #XDCC	2418	criten.net	[#XDCC] The Sweetest Thing. Subbed. TS-NEWiSO Panic. F
2. #warez-central	1542	Undernet	Most of the XDCC bots have been moved.. Type /server
3. #isoz	1152	criten.net	[#iSOZ] NOW SERVING : (04/26/2002) Project Earth, (
4. #warez-central	1090	AlphaNine	[WC] Newest Packs On XDCCz : Jason.X.Proper. Screen
5. #X-DCC	912	criten.net	[X-DCC] NEW: Tactical.Ops.Assault.On.Terror.REPACK-
6. #kampung	805	WebChat	- USE /server linkline.webchat.org ops applicati
7. #mp3passion	778	Undernet	#Mp3Passion Left Eye Trib-The Toasters-Mighty Might
8. #manaus	708	BRASnet	Bem vindos ao #manaus. Divirta-se ;-) Para ver as f
9. #bandung	703	DALnet	http://www.makaimedia.com/swf/games/juggling.asp
10. #brasil	672	BRASnet	Lançada a lista de discussão do #Brasil - brasilbra
11. #jakarta	604	DALnet	New Topic in FORUM : "Menyembunyikan Pasangan ? Mer
12. #movies-first	595	criten.net	[MF] We Have It All Asf-DivX-VCD-SVCD + Games/Warez
13. #recife	592	BRASnet	Confirmam o site do #Recife em www.canalrecife.net C
14. #tmd-moviez	573	criten.net	Welcome to TMD-MOVIEZ (NO Requests,Trading or FTP's
15. #manila	550	DALnet	Welcome To Manila <>Wud u agree if i say that<>Ther
16. #mp3z	544	DALnet	Welcome to #mp3z : To search for a song type: @loc
17. #iso-xdcc	534	DALnet	[iX] new movies.. everywhere... !! :) xXx@13; xX
18. #montreal	514	Undernet	Vive la neige! <- yen a pas a quebec nia nia :P
19. #rio	513	BRASnet	Bem-vindo ao #Rio! :: Respeite as regras do canal.
20. #belem	513	BrasIRC	Seja bem vindo(a) ao #belem Dúvidas? Procure um (
21. #bawel	503	DALnet	our newest homepage http://www.dalnetbawel.com * a

XDCC traffic report

```
core02
=====
Report on IRC audit for XDCC traffic
=====

Date/timezone:   Mon Apr 29 13:13:06 PDT 2002
Dump file:       xdcc-0429-1213.dump
Start/End date:  Mon Apr 29 12:13:34 2002      Mon Apr 29 13:13:00 2002

Channel: # _____
Bot             Host                               Offered   Transf'd
=====
[XXXX] XXXX-E341 10.240.218.238                        2.71 GB  333.07 GB
[XXXX] XXXX-E156 10.94.249.154                          1.08 GB  15.38 GB
[XXXX] XXXX-E158 10.206.119.198                         2.74 GB  231.85 GB
[XXXX] XXXX-E303 10.53.210.239                          364.50 MB 40.10 GB
. . .
[XXXX] XXXX-102  XXXX.XXXXXXXXXX.polymtl.ca            3.86 GB  248.85 GB
[XXXX] XXXX-324 dup-192-168-224-16.prodigy.net.mx      8.00 MB   9.40 GB
[XXXX] XXXX-814 dynXXX.XXX.oakland.edu                 1.36 GB  34.52 GB
[XXXX] XXXX-03  res-192-168-0-14.dorm.duke.edu         3.04 GB   1.37 TB
[XXXX] XXXX-E17 res0000-000.rh.rit.edu                   1.76 GB  301.45 GB
[XXXX] XXXX-454 resnet0-00.resnet.umbc.edu          11.30 MB 17.98 GB
[XXXX] XXXX-E102 ucsf-00-000.ucsf.edu                   781.50 MB 52.74 GB

Bots in # _____
Total Offered in #XXXX: 89.29 GB
Total Transferred in #XXXX: 12.34 TB
. . .

Grand Total Channels: 20
Grand Total Bots: 382
Grand Total Offered: 521.79 GB
Grand Total Transferred: 50.66 TB
```

XDCC traffic report (cont)

```
core02
Files served by host
=====

10.71.17.176:
#1: Big Trouble [TS-AVI]-[MM²] [275M]
#2: Kung Pow [TC-AVI]-[MM²] [296M]
#3: Fear And Loathing In Las Vegas [DvD-AVI]-[MM²] [421M]
#4: Fluff [XXX-AVI]-[MM²] [256M]
#5: PI [DvD-AVI]-[MM²] [332M]
#6: Thir13en Ghosts [DvD-AVI]-[MM²] [318M]

10.36.119.65:
#1: Soldier_of_Fortune_Gold_FINAL_Usa_Dvd_Rip_Ps2-GeNiuS-CD1 [562M]
#11: VA-Dj_Whoo_Kid-Hydro_Part_2_(Smoking_Day)-2002-WCR [105M]
#12: Scorpion.King.TS-CENTROPY-CD1 [426M]
#13: Scorpion.King.TS-CENTROPY-CD2 [431M]
#14: Deep.Inside.Tia.Bella-NovaVCD-CD1 [672M]
#15: Deep.Inside.Tia.Bella-NovaVCD-CD2 [673M]
#16: Devon.Up.Close.And.Personal.DVDRip.XXX-SPiCE [619M]
#2: Soldier_of_Fortune_Gold_FINAL_Usa_Dvd_Rip_Ps2-GeNiuS-CD2 [596M]
#3: Deep.Inside.Jill.Kelly.XXX-DVNVCD [CD1] [447M]
#4: Deep.Inside.Jill.Kelly.XXX-DVNVCD [CD2] [397M]
#5: Shine_JAP_PS2-MiRACLE [685M]
#6: Puss.N.Boots.XXX.DVDRip.DivX-xDMVx [694M]
#7: ADOBE.PHOTOSHOP.v7.0.FULL.RETAIL-FooZiSo [462M]
#8: Tactical_Ops_Assault_On_Terror_REPACK-FLT [483M]

10.89.23.10:
#1: Corel Pro Photo Yellowstone National Park - RORiSO [368M]
#2: IBM DB2 ONLINE ANALYSIS PROCESSING SERVER V8.0 - MKiSO [189M]
#3: MULTIGEN PARADIGM CREATOR V2.5.1 - ISO [208M]
```

Review what you know

- Attacks from: 128.95.X.154,
128.95.X.181...
- Traffic mostly Protocol 255, IRC, “other”
- Lots of FTP traffic (“warez”)
- Firedaemon/knight.c/GTbot installed
- IRC ports/channels known (“warez” bots)

Communication/Cooperation

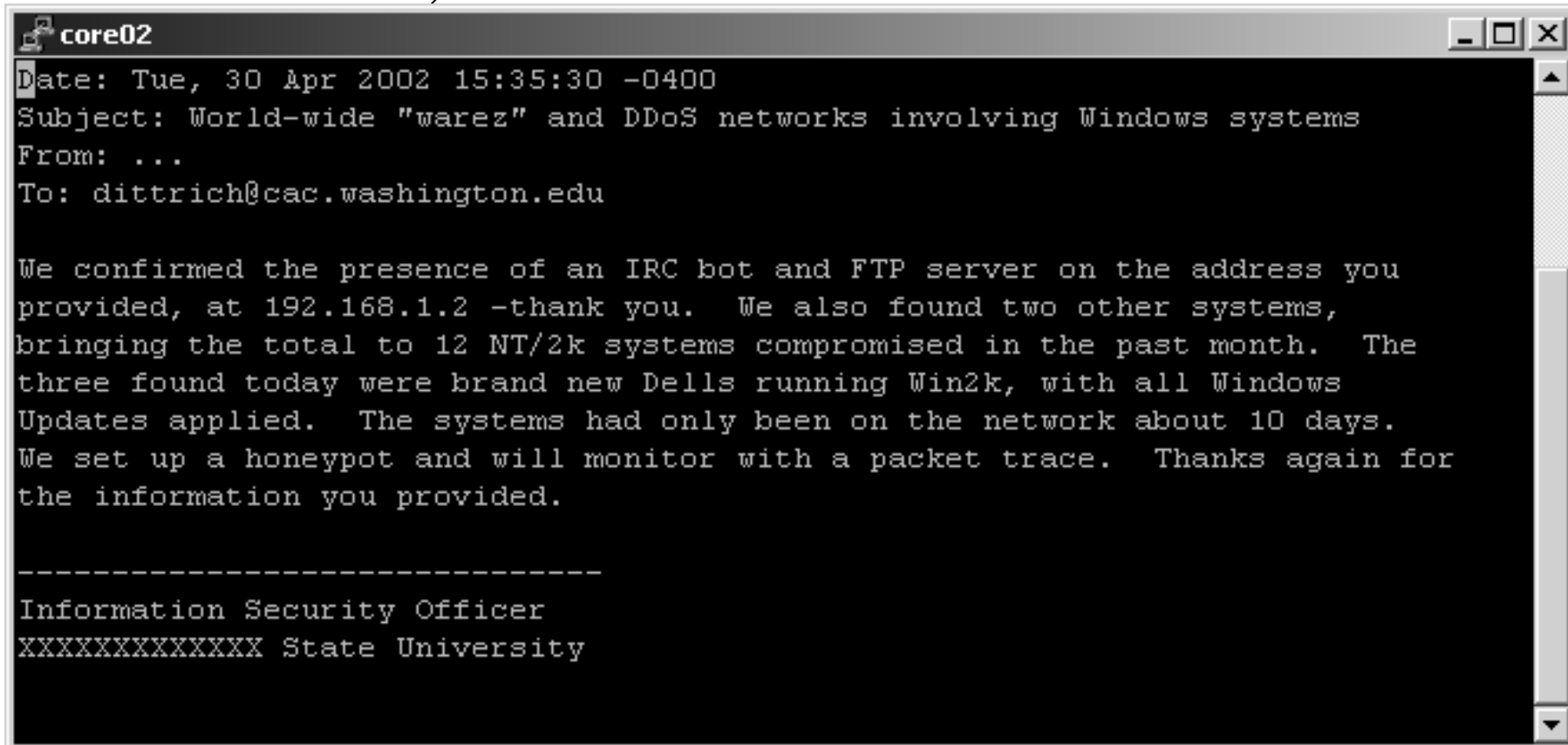
```
core02
Over the months of March through late April of 2002, the University of
Washington has seen multiple incidents of distributed "warez" (pirated
software) and denial of service (DDoS) attacks, coming from
Windows 2000 and NT systems.  These systems all have several things in
common:

o They appeared to be found with no password on the
  Administrator account, and control taken over.
o They had various IRC bots installed on them, including
  knight.exe, GTbot, and X-DCC (a distributed "warez"
  serving bot.)
o They had the ServUFTP daemon running on them for incoming
  file transfer (to load the "warez".)
o They had Firedaemon (a program that registers programs for
  execution to serve incoming connections, similar to the Unix
  "inetd" daemon.)

Forensic analysis of hard drive contents and IRC traffic has revealed
the methods and signatures of the malware installed on the compromised
systems.  To date we are not 100% sure of the initial intrusion
method, but once the intruder is able to run a program on the system,
the "tftp" (trivial file transfer protocol) client is run to download
a bootstrap program, which then goes out and installs all the other
software above on the system, making various changes to the system
settings and directory/file permissions to hide the presence of
files on the system and ensure programs will continue running after
a reboot.  This is accomplished by the following script:

=====
@echo off
c:
cd c:\winnt\system32\vmn32
mkdir \RECYCLER\S-1-5-21-2686636377-1107193052-384560437-1000
attrib +s +r +h \RECYCLER\S-1-5-21-2686636377-1107193052-384560437-1000
kill sxe*
kill temp.exe
:
```


Communication/Cooperation



```
core02
Date: Tue, 30 Apr 2002 15:35:30 -0400
Subject: World-wide "warez" and DDoS networks involving Windows systems
From: ...
To: dittrich@cac.washington.edu

We confirmed the presence of an IRC bot and FTP server on the address you
provided, at 192.168.1.2 -thank you. We also found two other systems,
bringing the total to 12 NT/2k systems compromised in the past month. The
three found today were brand new Dells running Win2k, with all Windows
Updates applied. The systems had only been on the network about 10 days.
We set up a honeypot and will monitor with a packet trace. Thanks again for
the information you provided.

-----
Information Security Officer
XXXXXXXXXXXXXXXX State University
```

Conclusion

- This was moderately complex
- Encryption makes things much harder (Eggdrop w/Blowfish, burneye, etc.)
- Today its guerilla warfare (on both sides)
- Discipline and skill wins
- Products from Arbor or Niksun help

Questions?

Website:

<http://staff.washington.edu/dittrich/>
(add [misc/ddos/](http://staff.washington.edu/dittrich/misc/ddos/) for DDoS page,
[misc/core02/](http://staff.washington.edu/dittrich/misc/core02/) for files)

Email:

dittrich@cac.washington.edu