

Information Security Summit 2006

Unconventional Malware Detection

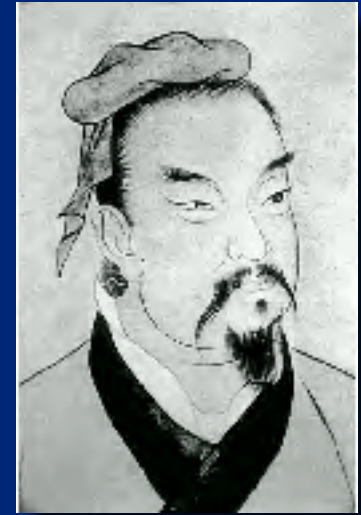
October 4th, 2006

Ron Dilley
Principal Information Security Architect
IS Security
Enterprise Architecture and Security

This is not an original idea

“To secure ourselves against defeat lies in our own hands, but the opportunity of defeating the enemy is provided by the enemy himself.”

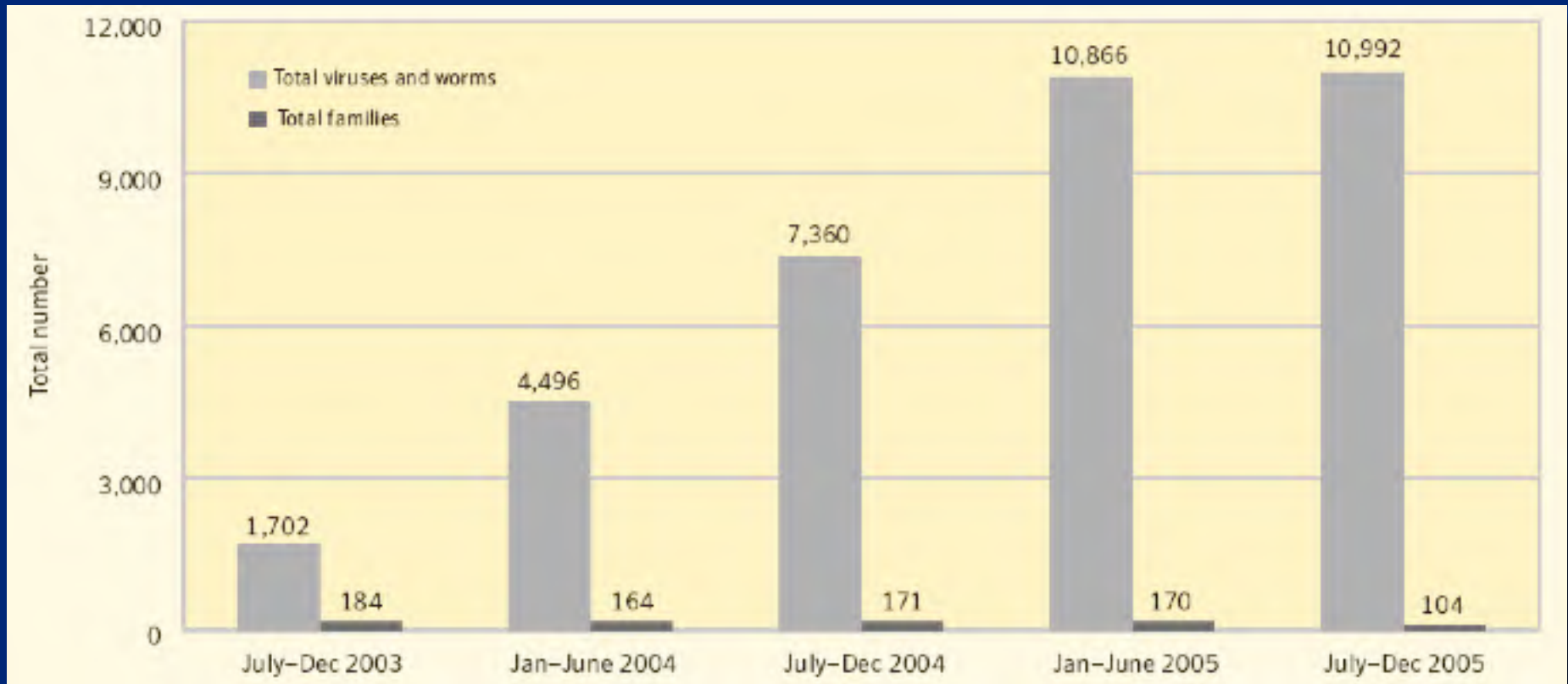
- Sun Tzu, 544-496 BC



Why is this important?

- Zero-day malware is not detected by our conventional security infrastructure
- The faster we identify an outbreak, the smaller the impact
- Identifying patient zero helps us reduce our attack surface

It's a dangerous world out there!



Source: Symantec Threat Report, March 2006

The numbers don't lie

- 1,402 Denial of Service (DoS) attacks p/day (up 51%)
- 9,163 New Infected Bots per day
- 1,896 New vulnerabilities (up 40%)
- 10,992 New WIN32 viruses and worms
- 80% of malware threatens confidential data
- 6 Days from vulnerability announcement to appearance of an exploit

Source: Symantec Threat Report, March 2006

Viruses, Worms, Trojans OH MY!

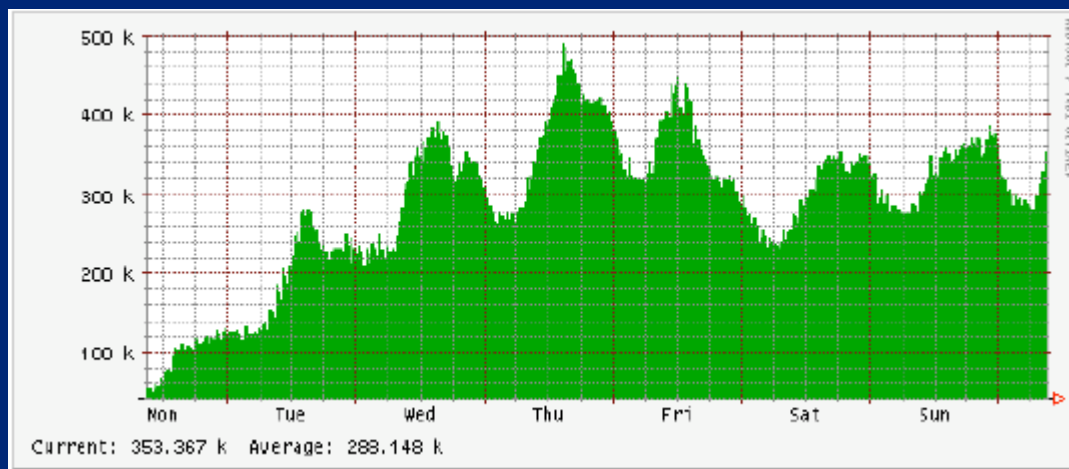
- Viruses replicate with the aid of a user or system
- Worms replicate without intervention
- Trojans are executed by fooling users
- Rootkits are tools that hide malware on a computer
- Spyware are trojans that usually send user data to a third party

How a worm works (Welchia/Nachi)

1. Pings random network ranges
2. Sends RPCDCOM Attack to responsive hosts
3. If the Attack succeeds, uses TFTP to download the worm from the attacking hosts
4. Executes the worm
5. The worm downloads patches from Microsoft
6. Patches system
7. Starts scanning for more victims

Detecting Welchia/Nachi

- Anti-Virus
- Detect the PING and RCPDCOM packets
- Volume of network traffic



- HTTP download of patches

Source: Nachi worm ICMP traffic on Internet2

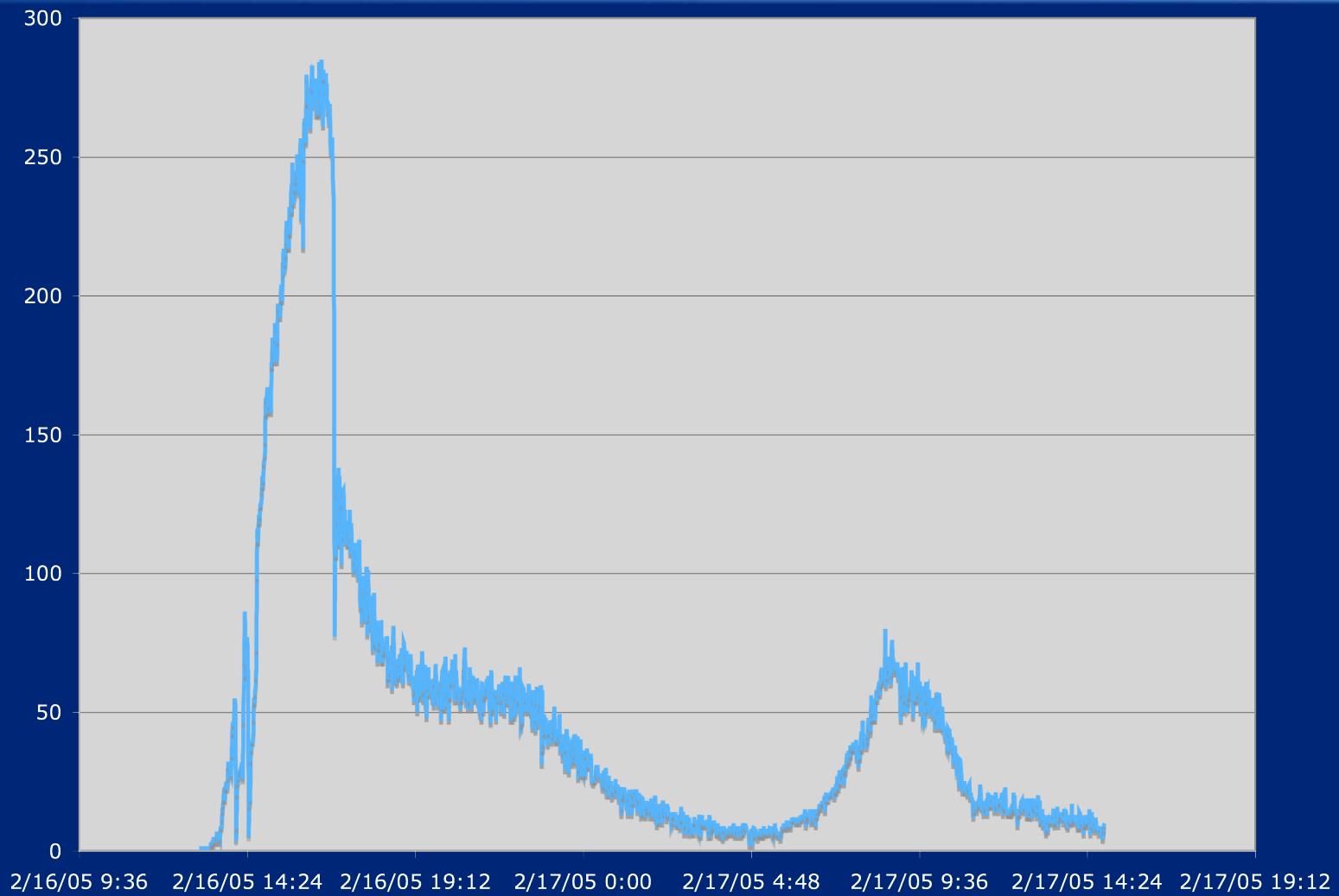
What makes malware tick?

- Network propagation
 - E-mail, Scanning, Instant Messaging (IM), Shares
- Control channels
 - IRC, IM, HTTP/HTTPS
- Intellectual Property (IP) Leakage
 - HTTP, FTP

Detecting scanning malware

- LaBrea: A low interaction honeypot
 - *Written by Tom Liston (<http://labrea.sourceforge.net>)*
- When placed on an unused subnet, will respond to ping and TCP requests as though the subnet is fully populated
- Can dampen the propagation of network based malware
- Logs all traffic via syslog
- Extremely simple configuration
 - A few lines in one text file

IT WORKS!



Detecting e-mail worms

- No network scanning
- Every infected system needs to send e-mail to propagate
- Only authorized mail relays can send e-mail
- Egress filters and logging RULE!
- Simple script to find outbound E-Mailers

```
% cat fwlogs | grep 'src zone=Trust' | grep 'action=Deny' | grep  
  'dst_port=25'
```

Detecting spyware

- User Agent Strings, every browser has one
- Tcpflow is an open source TCP stream reassembler
 - *Written by Jeremy Elson (<http://www.circlemud.org/~jelson/software/tcpflow>)*
- Combine tcpflow with a little perl and you have a User Agent String sniffer

User agents tell tales

```
175  MOZILLA/4.0 (COMPATIBLE; MSIE 6.0; WINDOWS NT 5.0; Q312461; FOO.V1B; FUNWEBPRODUCTS; .NET CLR
1.1.4322)
75   MOZILLA/4.0 (COMPATIBLE; MSIE 6.0; WINDOWS NT 5.0; Q312461; FUNWEBPRODUCTS; .NET CLR 1.1.4322)
65   MOZILLA/4.0 (COMPATIBLE; MSIE 6.0; WINDOWS NT 5.0; Q312461; FUNWEBPRODUCTS; FOO.V1B; .NET CLR
1.1.4322)
65   MOZILLA/4.0 (COMPATIBLE; MSIE 6.0; WINDOWS NT 5.0; Q312461; YPC 3.2.0; FUNWEBPRODUCTS;
AMGEN.V1B; .NET CLR 1.1.4322)
34   MOZILLA/4.0 (COMPATIBLE; MSIE 6.0; WINDOWS NT 5.0; Q312461; FOO.V1B; .NET CLR 1.1.4322;
SPAMBLOCKERUTILITY 4.8.0)
33   MOZILLA/4.0 (COMPATIBLE; MSIE 6.0; WINDOWS NT 5.1; SV1; FUNWEBPRODUCTS; INFOPATH.1; .NET CLR
1.1.4322; .NET CLR 2.0.50727)
11   MOZILLA/4.0 (COMPATIBLE; MSIE 6.0; WINDOWS NT 5.1; SV1; FUNWEBPRODUCTS; .NET CLR 1.1.4322;
.NET CLR 2.0.50727; INFOPATH.1)
5    MOZILLA/4.0 (COMPATIBLE; MSIE 6.0; WINDOWS NT 5.0; Q312461; YPC 3.0.1; FOO.V1B; .NET CLR
1.1.4322)
4    MOZILLA/4.0 (COMPATIBLE; MSIE 6.0; WINDOWS NT 5.0; Q312461; SBCYDSL 3.12; YCOMP 5.0.0.0;
AMGEN.V1B; .NET CLR 1.1.4322)
2    MOZILLA/5.0 (COMPATIBLE; GNOTIFY 1.0.25.0)
2    MOZILLA/4.0 (COMPATIBLE; GOOGLETOLBAR 3.0.131.0-BIG; WINDOWS 2000 5.0; GOOGLE-TR-3)
1    MOZILLA/4.0 (COMPATIBLE; MSIE 6.0; PLAXO_2.8.1.2)
1    MOZILLA/4.0 (COMPATIBLE; MONEYCENTRAL; VERSION 15.0.0.513)
```

Detecting control channels

- Internet Relay Cat (IRC)
- Instant Messenger
- HTTP/HTTPS
- Egress filtering and logs to the rescue again!

Scripts a-go-go

- Simple script to find outbound IRC

```
% cat fwlogs | grep 'src zone=Trust' | grep  
'action=Deny' | egrep 'dst_port=666[0-9] '
```

```
Sep  8 05:44:09 csec1-fw: src=10.10.131.60 dst=195.56.29.202 src_port=30076  
dst_port=6664  
Sep  8 11:40:43 tsec1-fw: src=10.10.29.167 dst=207.38.11.136 src_port=2252  
dst_port=6667  
Sep  8 11:40:46 tsec1-fw: src=10.10.29.167 dst=207.38.11.136 src_port=2252  
dst_port=6667  
Sep  8 11:40:52 tsec1-fw: src=10.10.29.167 dst=207.38.11.136 src_port=2252  
dst_port=6667  
Sep  8 11:41:04 tsec1-fw: src=10.10.29.167 dst=207.38.11.136 src_port=2264  
dst_port=6667  
Sep  8 11:41:07 tsec1-fw: src=10.10.29.167 dst=207.38.11.136 src_port=2264  
dst_port=6667  
Sep  8 11:41:13 tsec1-fw: src=10.10.29.167 dst=207.38.11.136 src_port=2264  
dst_port=6667  
Sep  8 11:41:27 tsec1-fw: src=10.10.29.167 dst=207.38.11.136 src_port=2267  
dst_port=6667  
Sep  8 11:41:30 tsec1-fw: src=10.10.29.167 dst=207.38.11.136 src_port=2267  
dst_port=6667  
Sep  8 11:41:36 tsec1-fw: src=10.10.29.167 dst=207.38.11.136 src_port=2267  
dst_port=6667  
Sep  8 11:41:48 tsec1-fw: src=10.10.29.167 dst=207.38.11.136 src_port=2276  
dst_port=6667
```


More scripts a-go-go

- A not-so-simple script to find clients with DNS issues

% OutBoundDNS.pl fwlogs

```
10.21.54.119 = 4576
10.21.54.34 = 2522
10.10.215.127 = 2175
it-206-dhcp-104 = 1797
ausy-dns01 = 106
dhcp61-194 = 55
dhcp147-236 = 40
dhcp101-46 = 30
uk1-192-ssr = 14
toast = 4
ZT075057.ppp.dion.ne.jp = 1
```

Detecting new websites that have never been visited before

- Never before seen (nbs)
 - *Written by Marcus Ranum (http://www.ranum.com/security/computer_security/index.html)*
- Creates and manages a simple and fast database of strings that have been seen before
- Create a database

```
% nbsmk -d /var/tmp/neverseen
```
- Now it is time to get to parsing

Test your perl-fu

- Our web proxies store all the info we need

```
% cat proxylog | /usr/bin/perl -e  
  'while($line=<stdin>){if($line=~m/^\.*\s(http\:\V[\w\d\.\-  
  \_]+)\.*$/){print "$1\n";}}' > urilog
```

- Don't panic, we are just getting rid of cruft
- Now lets start training nbs

```
% cat urilog | nbs -d /var/tmp/neverseen
```

One month later . . .

- Now that NBS is trained, we can scrutinize new URI's

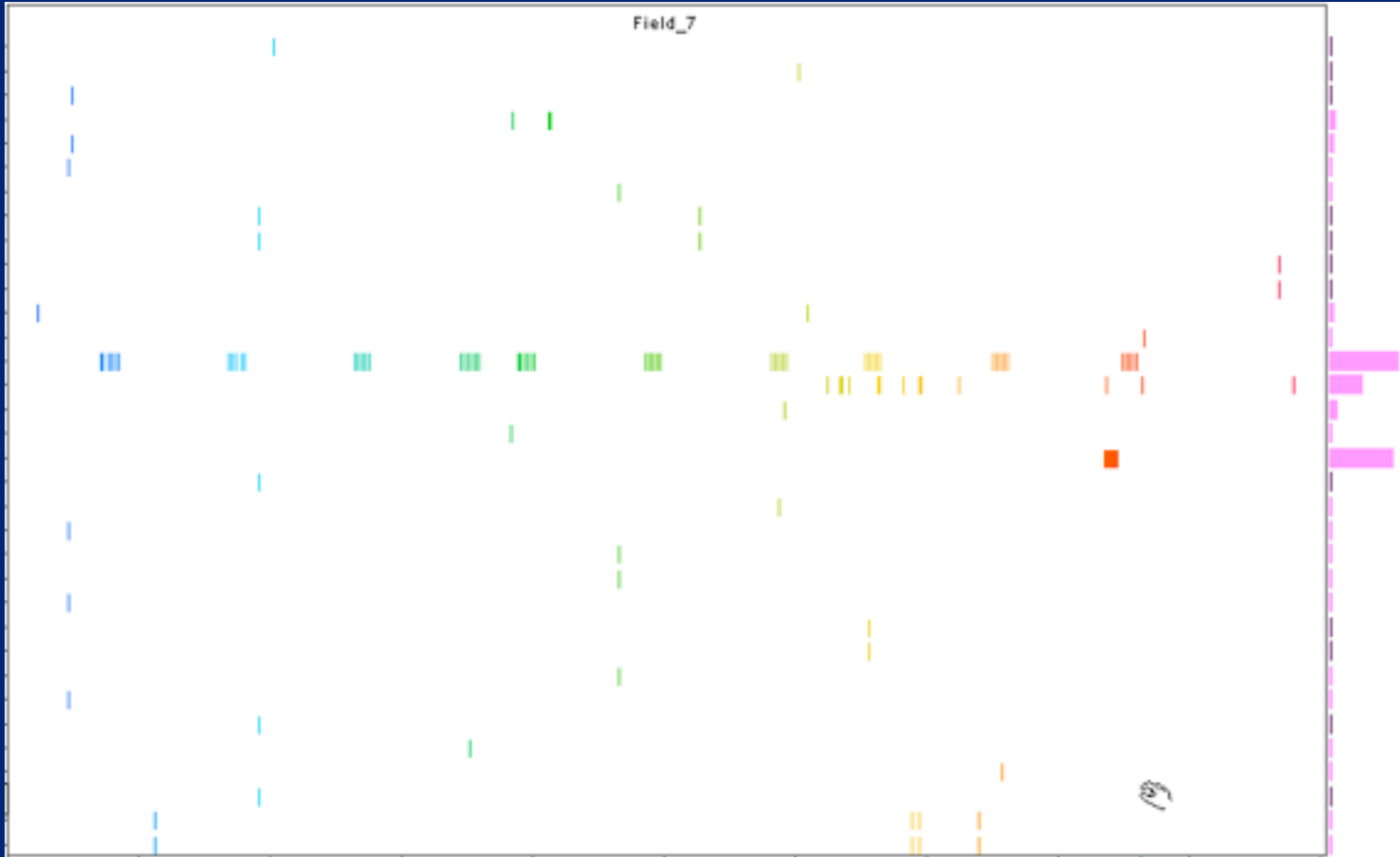
```
% cat proxylog | /usr/bin/perl -e  
'while($line=<stdin>){if($line=~m/^\.*\s(http\:\V\[\w\d\.\-\_]+\).*$/){print "$1\n";}}'  
| nbs -d /var/tmp/neverseen  
http://www.sun-herald.com  
http://www.saraevans.com  
http://www.comiczone.com  
http://www.physics.ubc.ca  
http://www.nieforth.com
```

Network traffic trends

- Remember Welchia/Nachi?
- Firewalls logs can be monitored/mined for trending
- Who is pinging what, when, how much and how long?

On an empty network you can ping forever

Destination IP Addresses

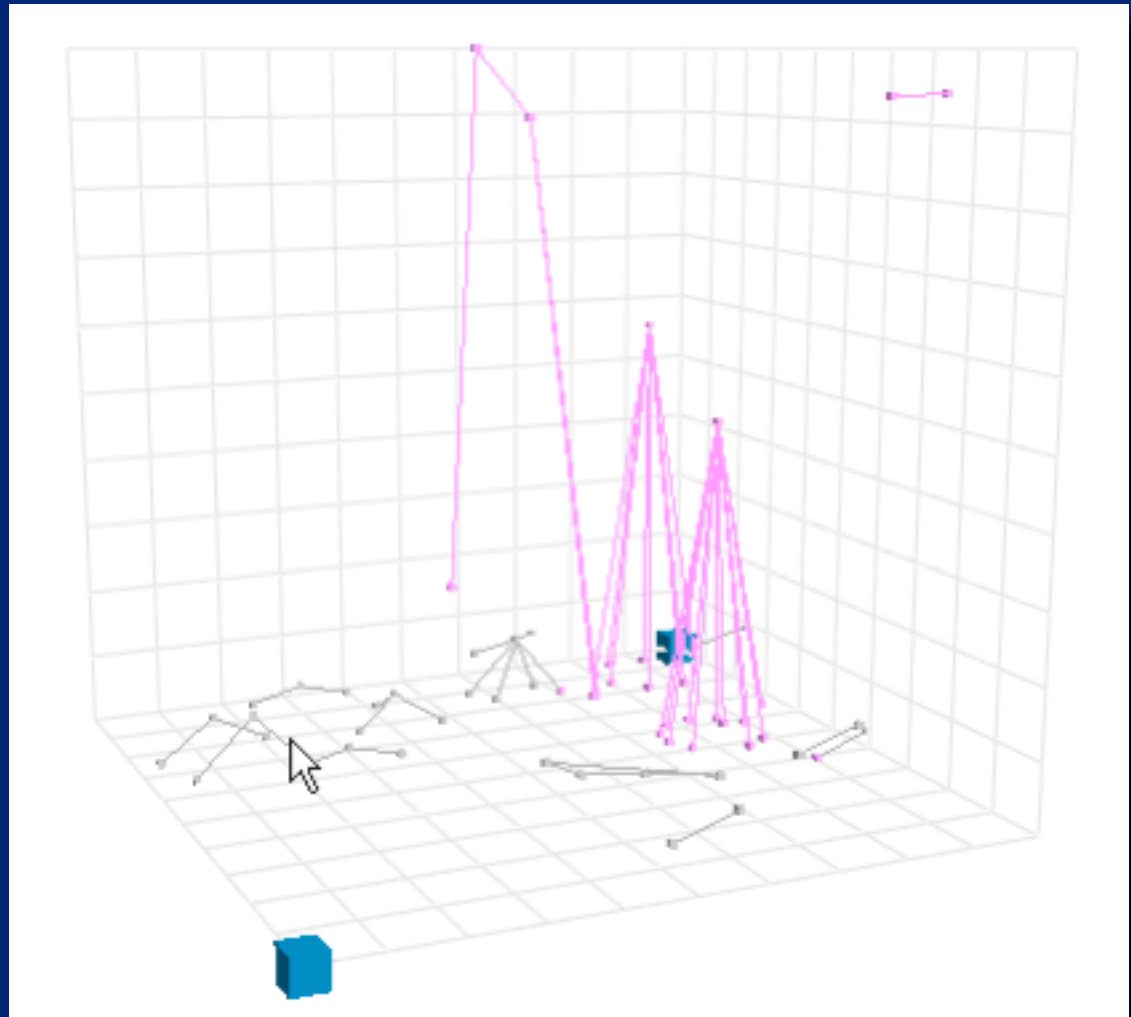


24 Hour Time Span

Every good presentation needs a pretty graph

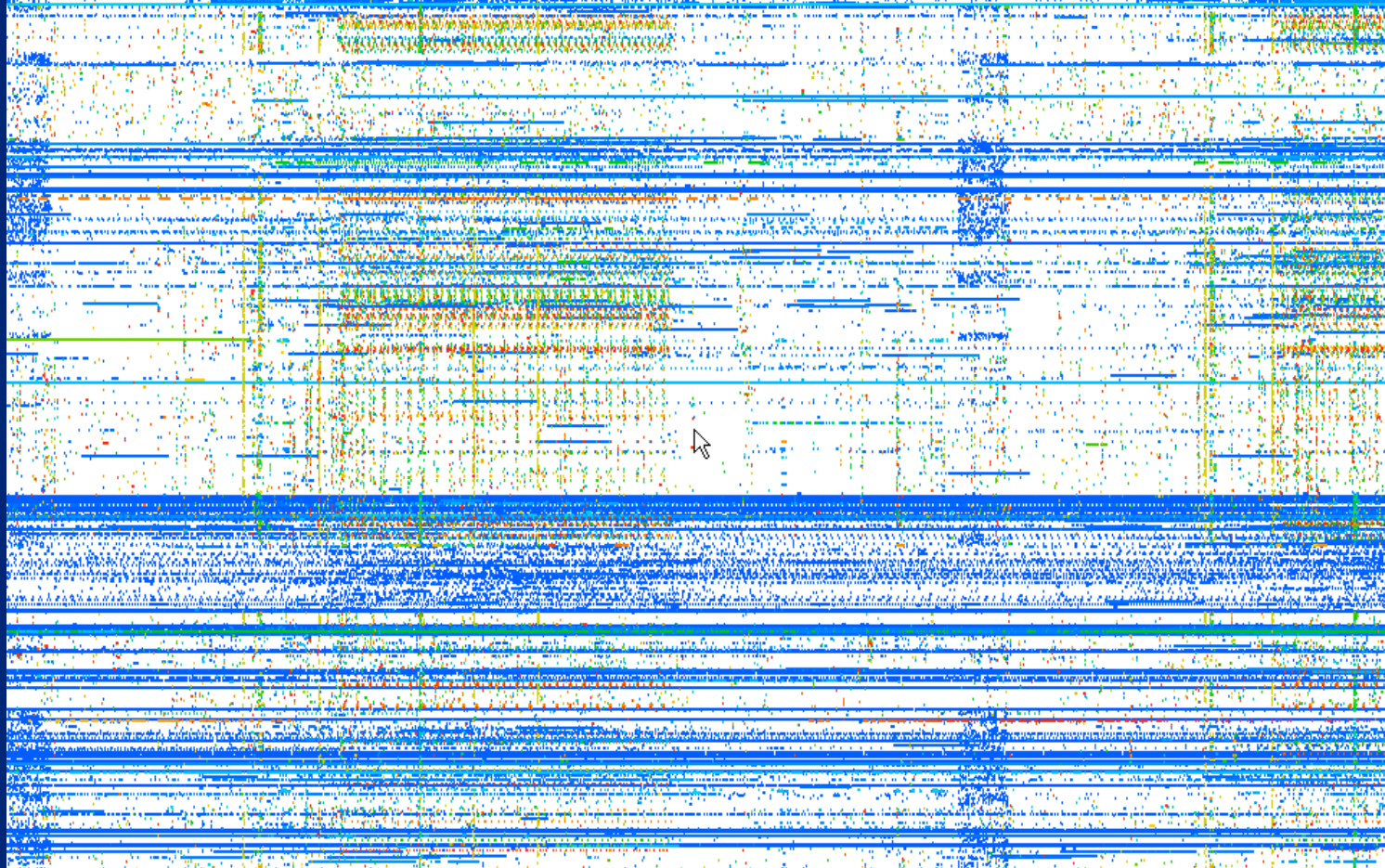
“The frequency and relation of uninteresting events are interesting.”

-Marcus Ranum



Firewall Log Analysis

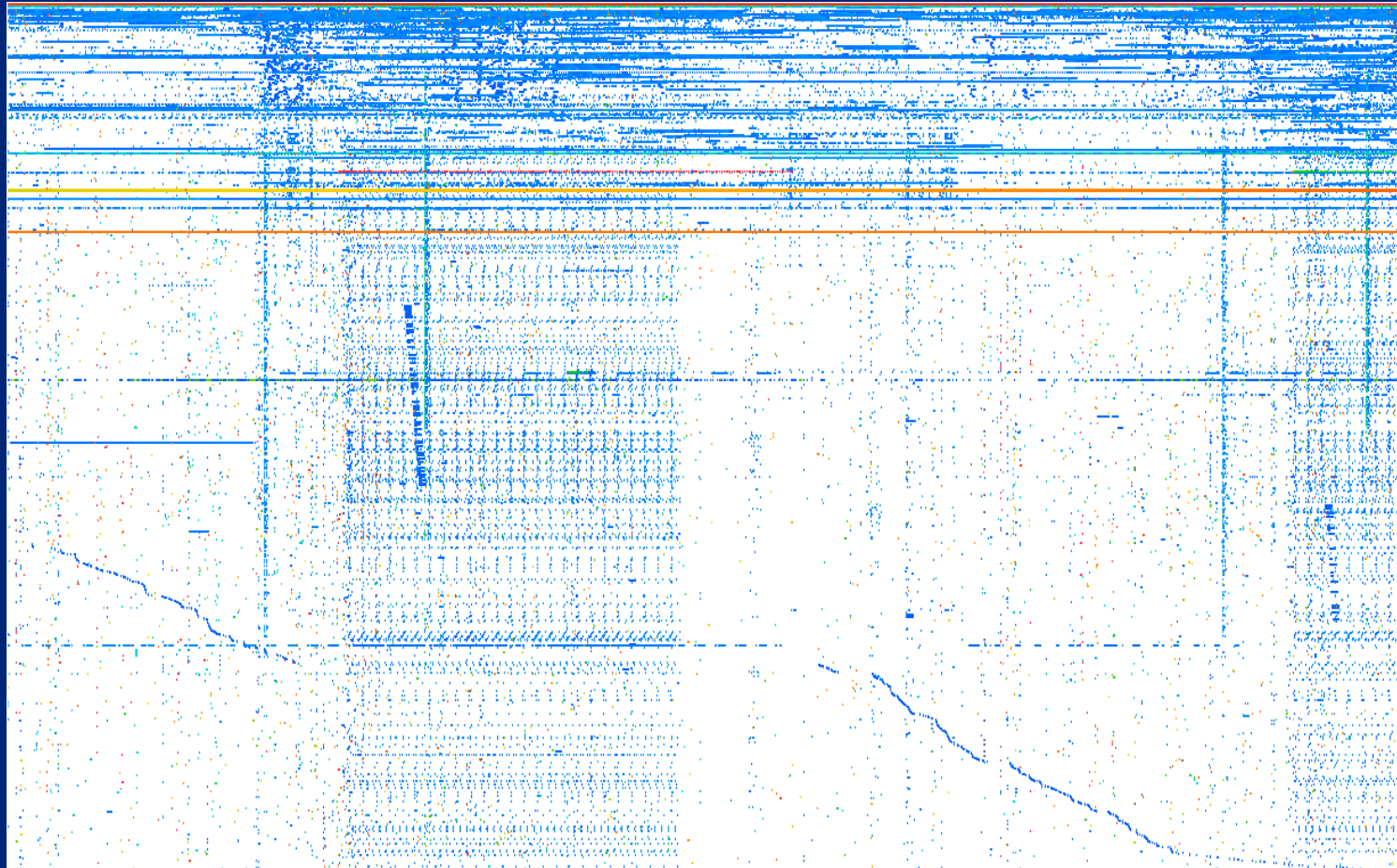
Destination IP Addresses



24 Hour Time Span

Firewall Log Analysis (cont)

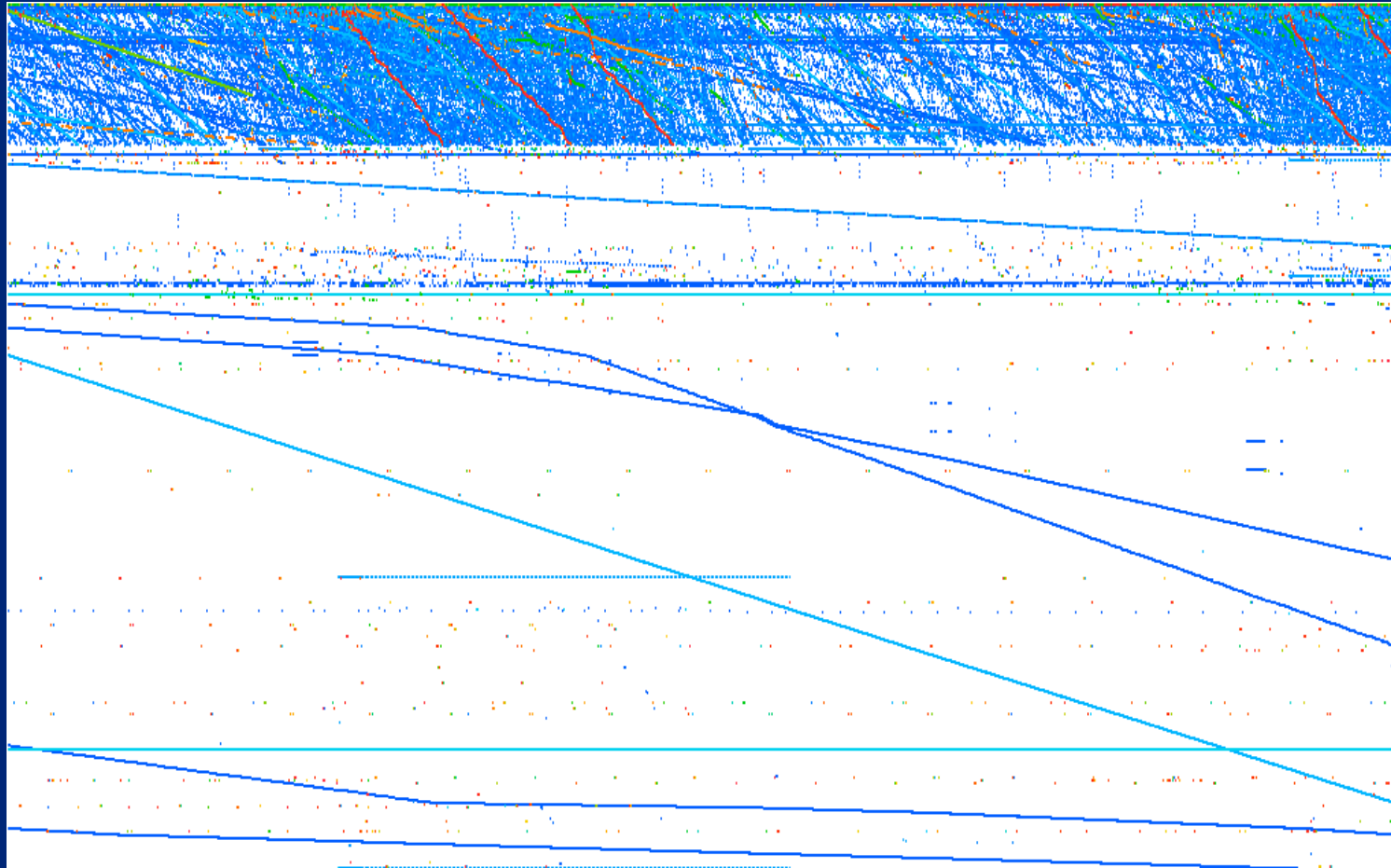
Destination Port



24 Hour Time Span

Firewall Log Analysis (cont)

Source Port



24 Hour Time Span

Current/future research

- The wire spy (wsd)
 - This utility sniffs the network, building access control lists based on the traffic that is seen on the wire.
 - After training wsd, any added ACLs must be traffic that has not been seen before
- DNS statistical analysis to detect traffic blooms
 - Many systems searching for one(or few) new names
 - One(or few) systems searching for many new names

Questions?