Traffic Monitoring :

MyCERT

Malaysian
Computer
Emergency
Response
Team

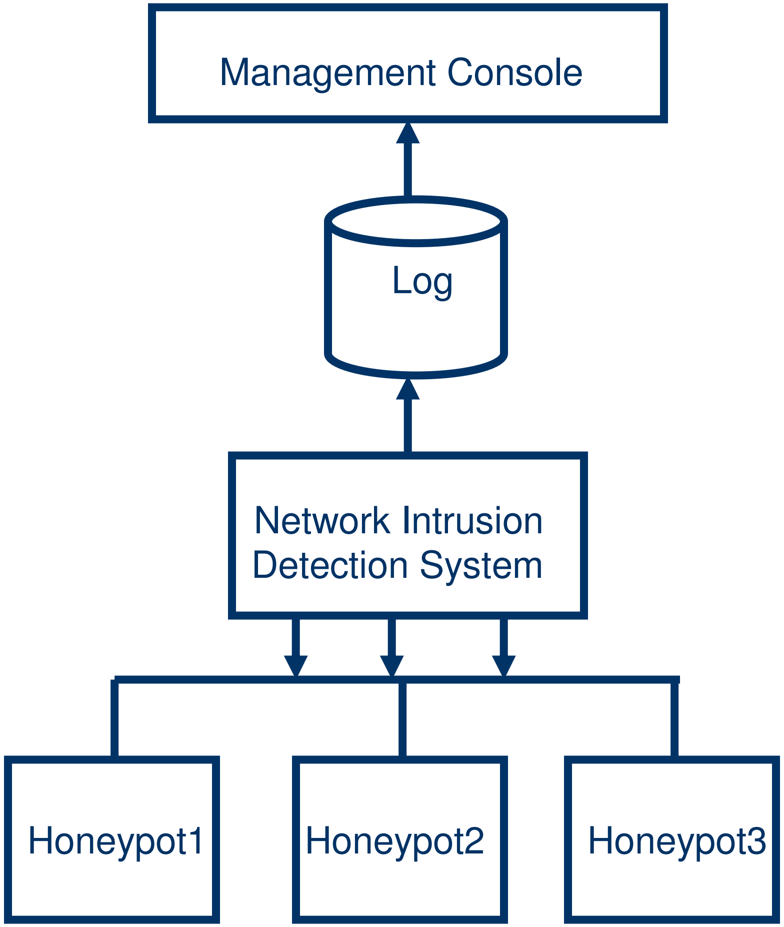
Experience

Solahuddin Shamsuddin
MyCERT Manager

Objectives

- To understand who and/or what the threats are
- To understand “attacker” operation
  - Originating Host
  - Motives (purpose of access)
  - Tools and Techniques
  - Who (personality)
- To be able to capture and predict new attacks – pattern and trend
- To be able to produce new attack identifications

How it Works



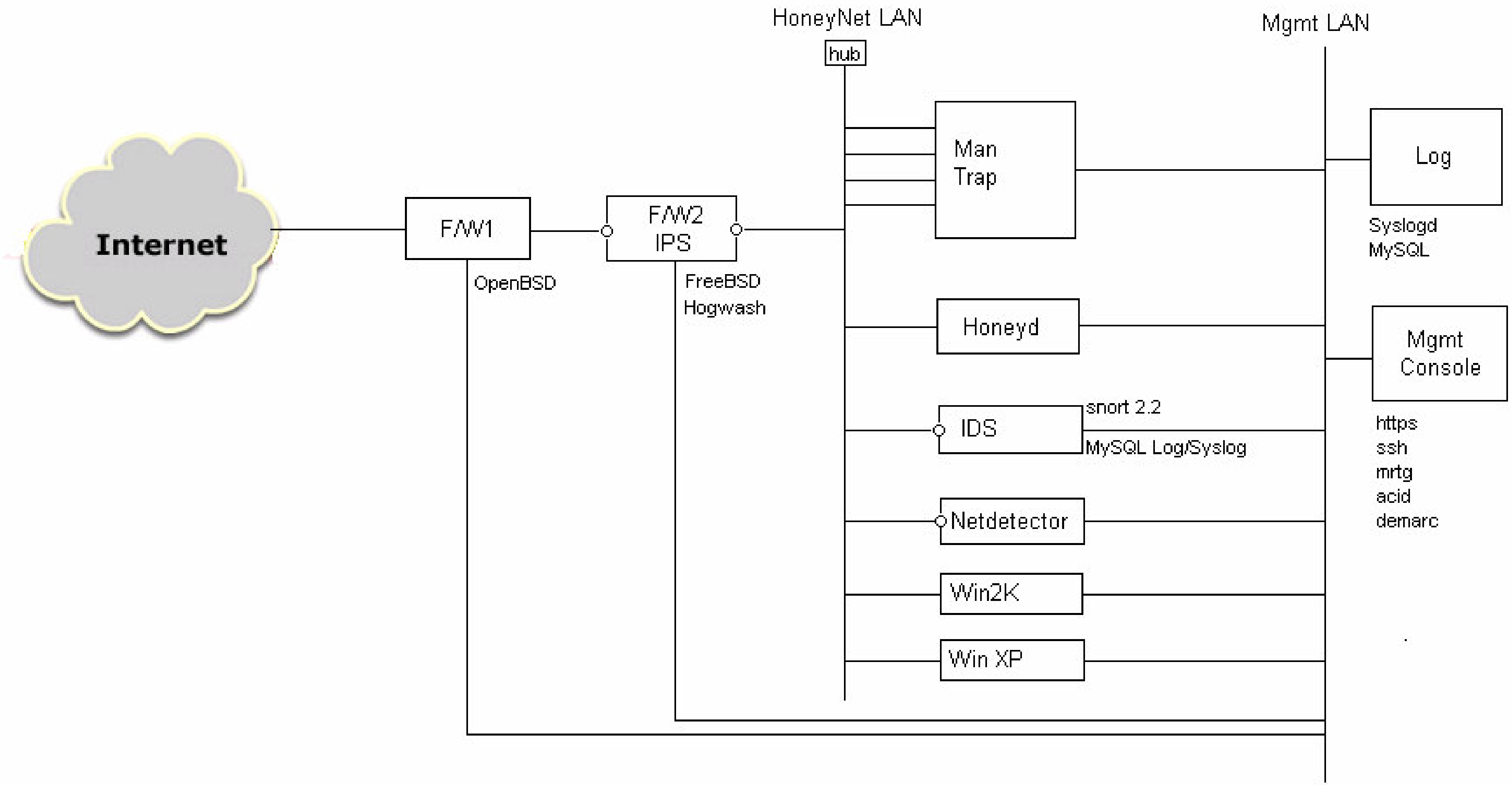
The Management console is used to view the logs to conduct analysis of activities.

The Log Server retains the logs for a certain period of time and backed up to external media periodically.

NIDS listens in promiscuous mode all activities carried out within the network to and from the honeypots. All binaries of the logs are dumped into the Database.

The Honeypots consists of hosts setup with certain vulnerabilities introduced. It emulates various platforms and has mechanisms to contain the perpetrator from launching attacks to other external systems.

Architecture



Network Activity Profiling

- Act of collecting statistics
- Intrusion as deviations from normal behavior
- Checking
  - Service running vs Network traffic
- Look for
  - Activity that has not been seen before
  - Activity level that is greater than normal

Analyzing Data

- Well known network signatures
  - IDS – Snort, Bro
  - Pcap filters
- Look for behavioral changes
  - Quiet system suddenly scanning
  - Trigger on initiated outbound traffic
- Examine captured binaries
  - Disassemble

Traffic Characteristics

- Protocols
- Ports
- Success and Failures
- Peers of communication
- Traffic Volume

Network Behavior

- Volume of Traffic
- Traffic Pattern

Volume of Traffic

- Most worm uses logistic growth model.
- Host is brought into the network with scans and attacks.
- Best measure at router or firewall

Traffic Pattern

- Change of behavior.
- Worm will make host acting ‘abnormal’.
- Look for its presence.

Techniques

- Traffic Analysis
  - Honeypots
  - Black Hole/Sink Hole

Traffic Capture Method

- Tcpdump
- SNMP
- Flow-Based

Correlation

- Correlation – to find connectedness of events within the set.
- Autocorrelation
  - Events of the same type
- Crosscorrelation
  - Interaction of 2 different events

Honeypots and Black Hole Monitoring

- Effectively listen to the network
- Honeypots – functional system
- Black Hole – unused network
- Common is – any activity appear on this domain is in the interest.

Honeypots

- Technology
  - Low Level
  - High Level
- Risk Factor
- Real attack
- Still need compliment technology on the network analysis

Black Hole

- Unused IP space
  - Backscatter
  - Advertise route
  - View to the network

Packet Capture and Analysis

- 2 ways of Black Hole
  - 1. Export flow logs from routing device
  - 2. Passive network monitor

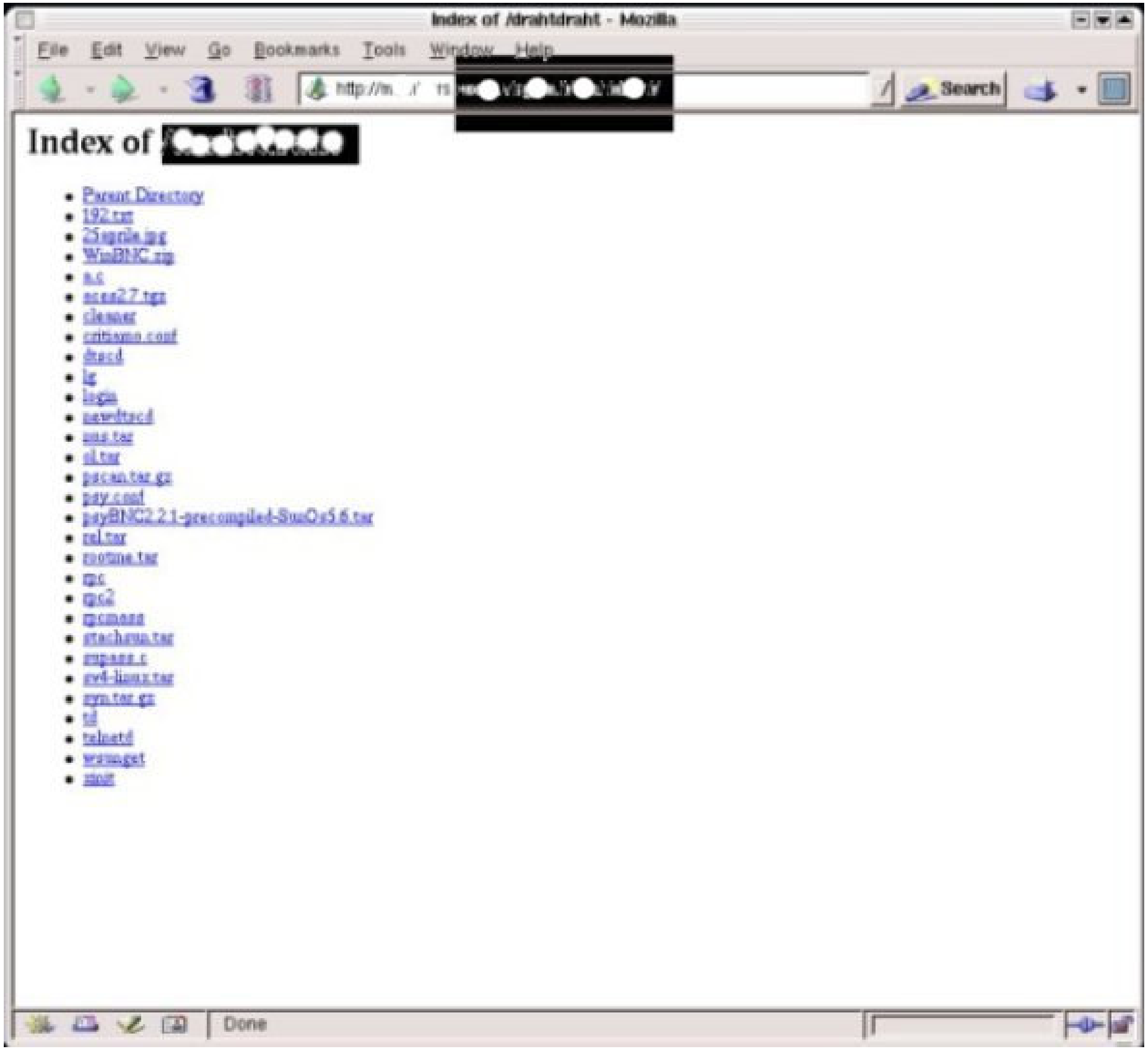
Traffic Analysis Conclusion

- Works against most worm especially those that uses active target and exponential growth.
- Required lengthy period of monitoring and understanding
- Worm that move sufficiently slow will become undetected

After all

- Which is the best ?
- False positive or False negative

Attacker Tools



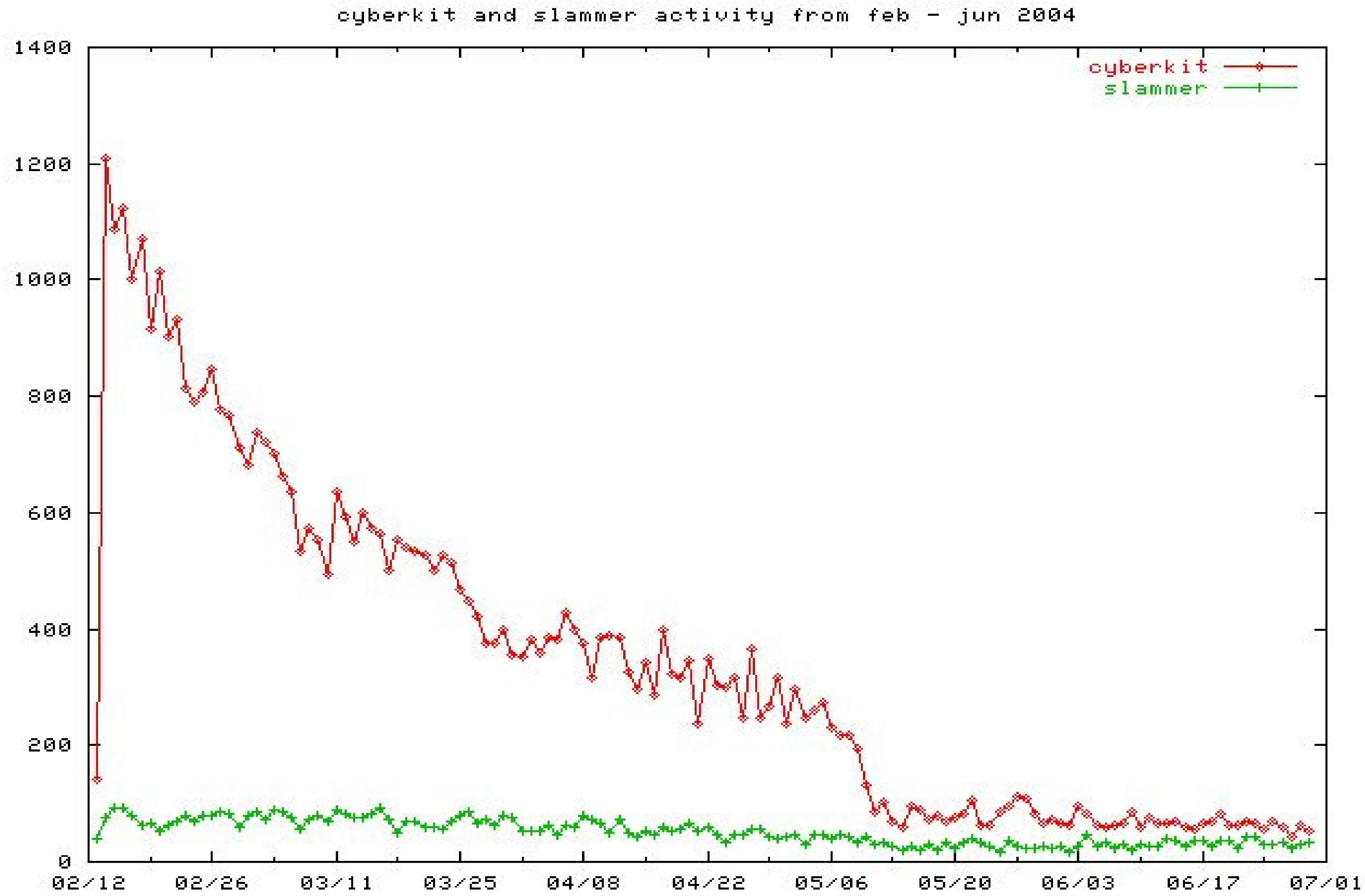
Index of [redacted]

- Parent Directory
- 192.tar
- 25egrule.jpg
- WinBNC.zip
- a.c
- acea2.7.tgz
- cleaner
- crttsamn.conf
- dtecd
- lg
- login
- newdtecd
- nss.tar
- sl.tar
- pscan.tar.gz
- psy.conf
- psyBNC2.2.1-precompiled-SunOs5.6.tar
- rel.tar
- rootme.tar
- rpc
- rpc2
- rpcmass
- stacheum.tar
- snpass.c
- sv4-linux.tar
- syn.tar.gz
- td
- telnetd
- wsmget
- snif

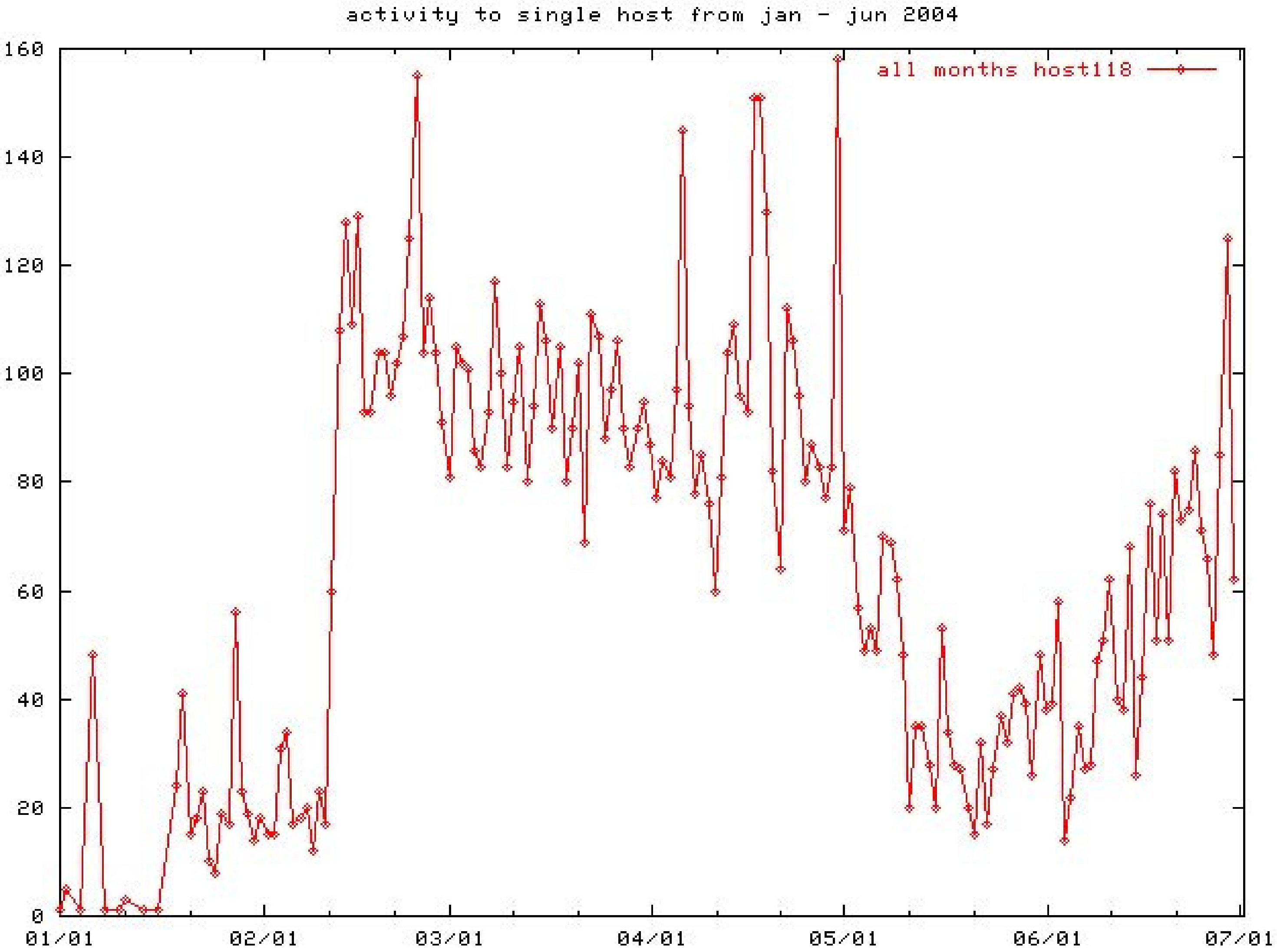
Launching Pad - DDOS

```
Jun 19 03:57:26 ips hogwash: [1:1855:2] Packet Dropped-DDOS Stacheldraht
    agent->handler (skillz) {ICMP} x.y.z.117 - > 151.9.116.99
Jun 19 03:57:31 ips hogwash: [1:1855:2] Packet Dropped-DDOS Stacheldraht
    agent->handler (skillz) {ICMP} x.y.z.117 - > 151.9.116.99
Jun 19 03:57:36 ips hogwash: [1:1855:2] Packet Dropped-DDOS Stacheldraht
    agent->handler (skillz) {ICMP} x.y.z.117 - > 140.112.38.9
Jun 19 03:57:41 ips hogwash: [1:1855:2] Packet Dropped-DDOS Stacheldraht
    agent->handler (skillz) {ICMP} x.y.z.117 - > 140.112.38.9
Jun 19 03:58:37 ips hogwash: [1:1855:2] Packet Dropped-DDOS Stacheldraht
    agent->handler (skillz) {ICMP} x.y.z.117 - > 151.9.116.99
Jun 19 03:58:42 ips hogwash: [1:1855:2] Packet Dropped-DDOS Stacheldraht
    agent->handler (skillz) {ICMP} x.y.z.117 - > 151.9.116.99
```

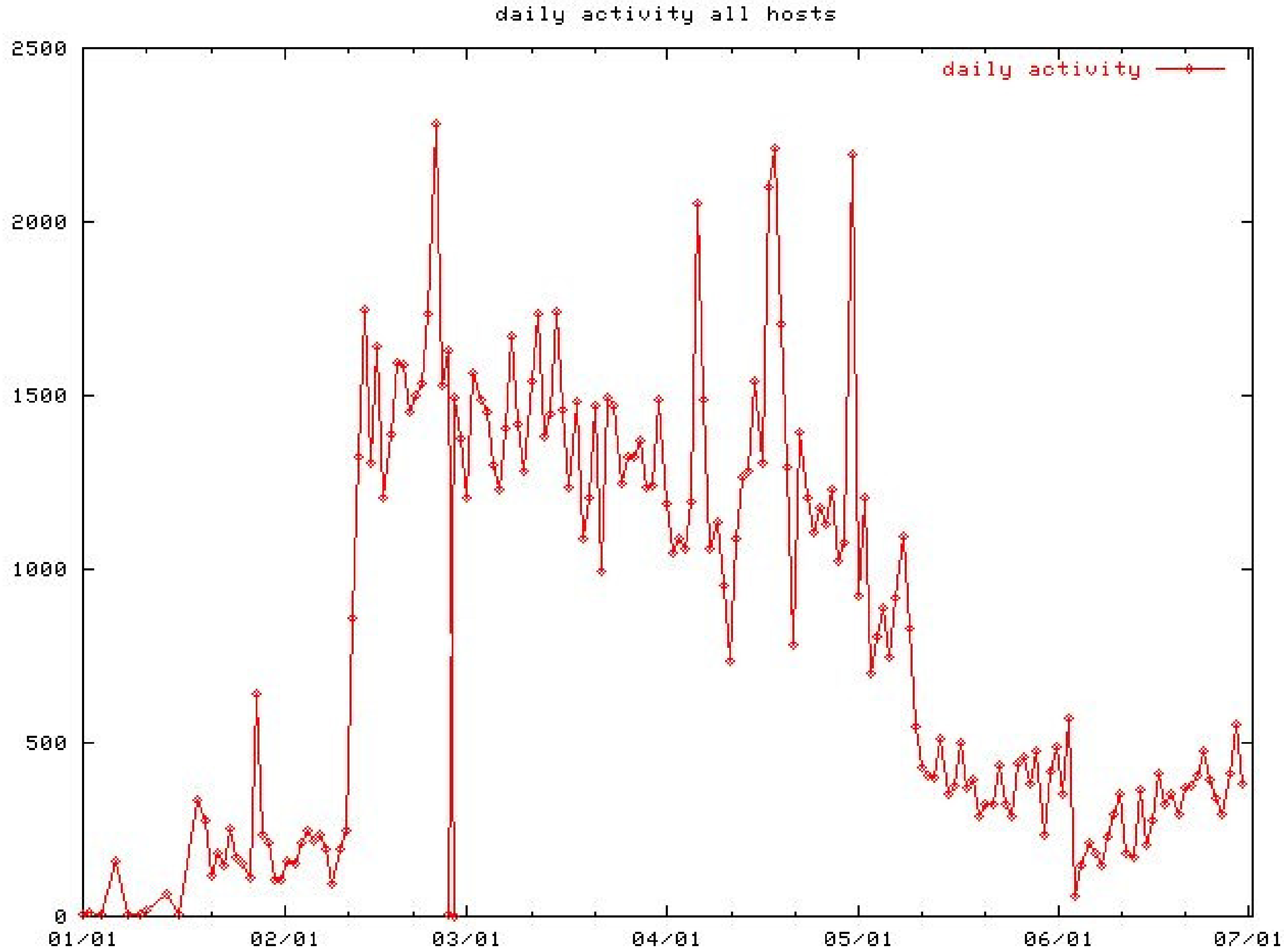
Measuring Worm



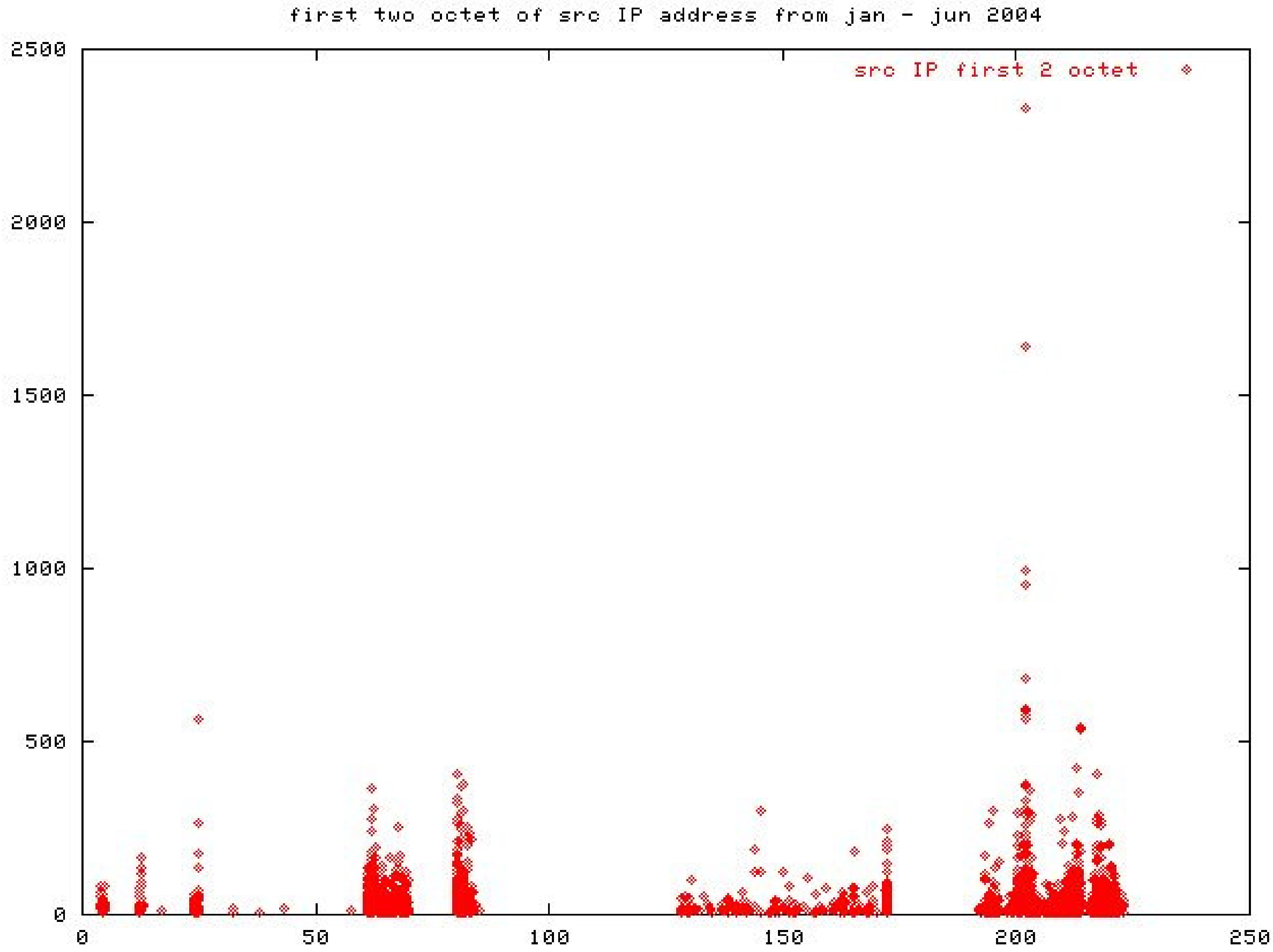
Traffic to 1 Host



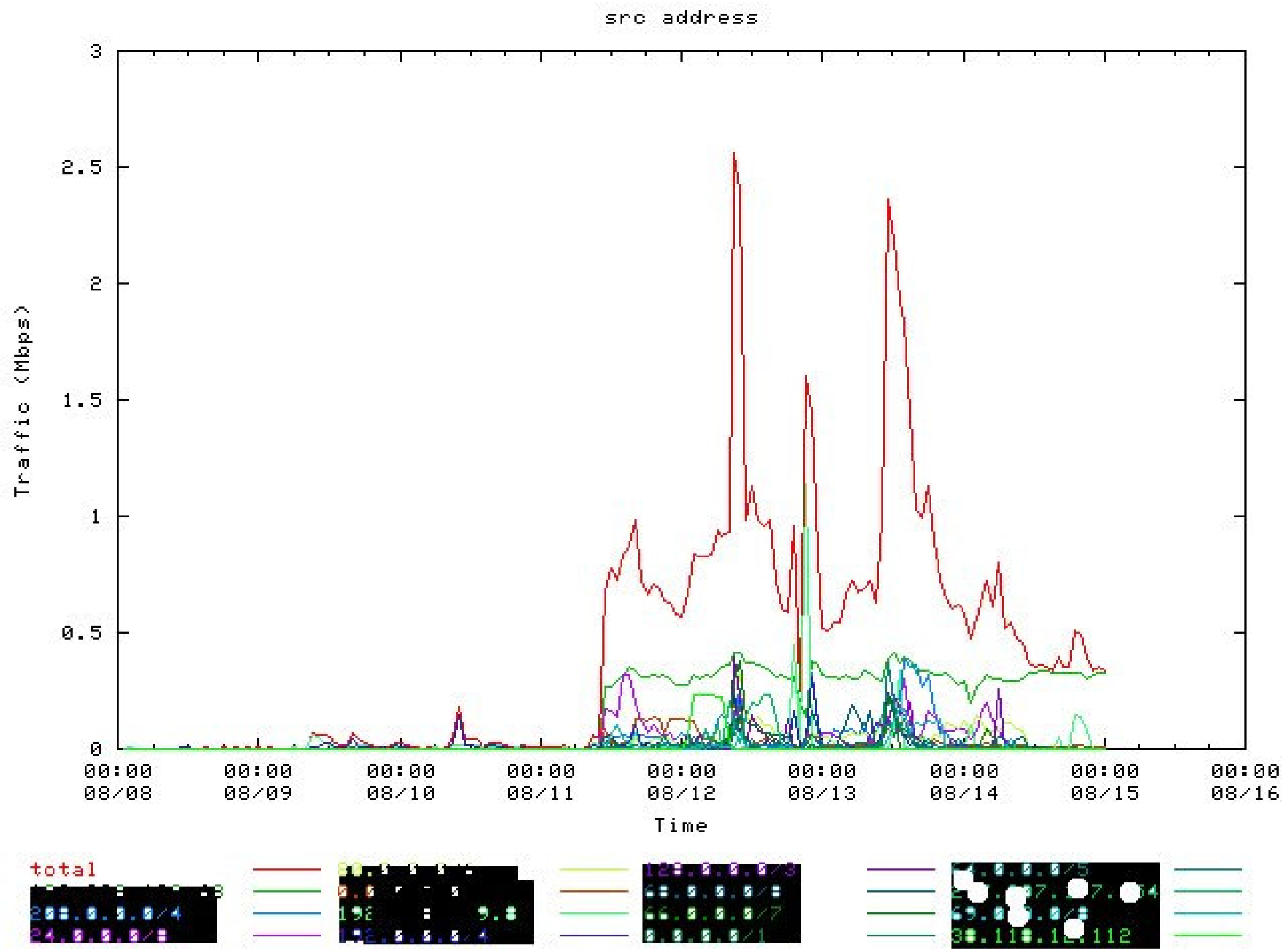
Traffic to Multiple Host



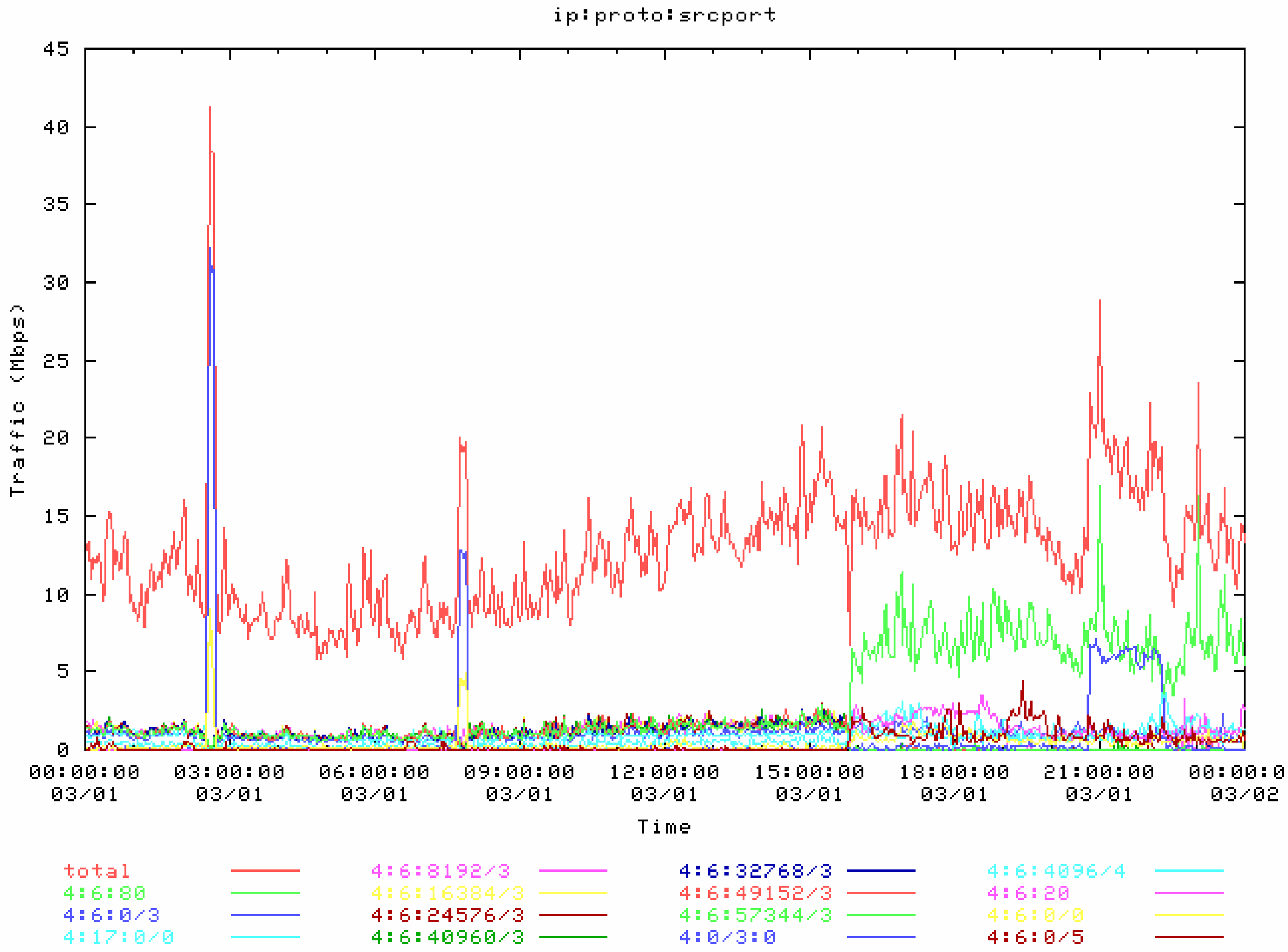
Source IP Address Distribution



Early Warning ?

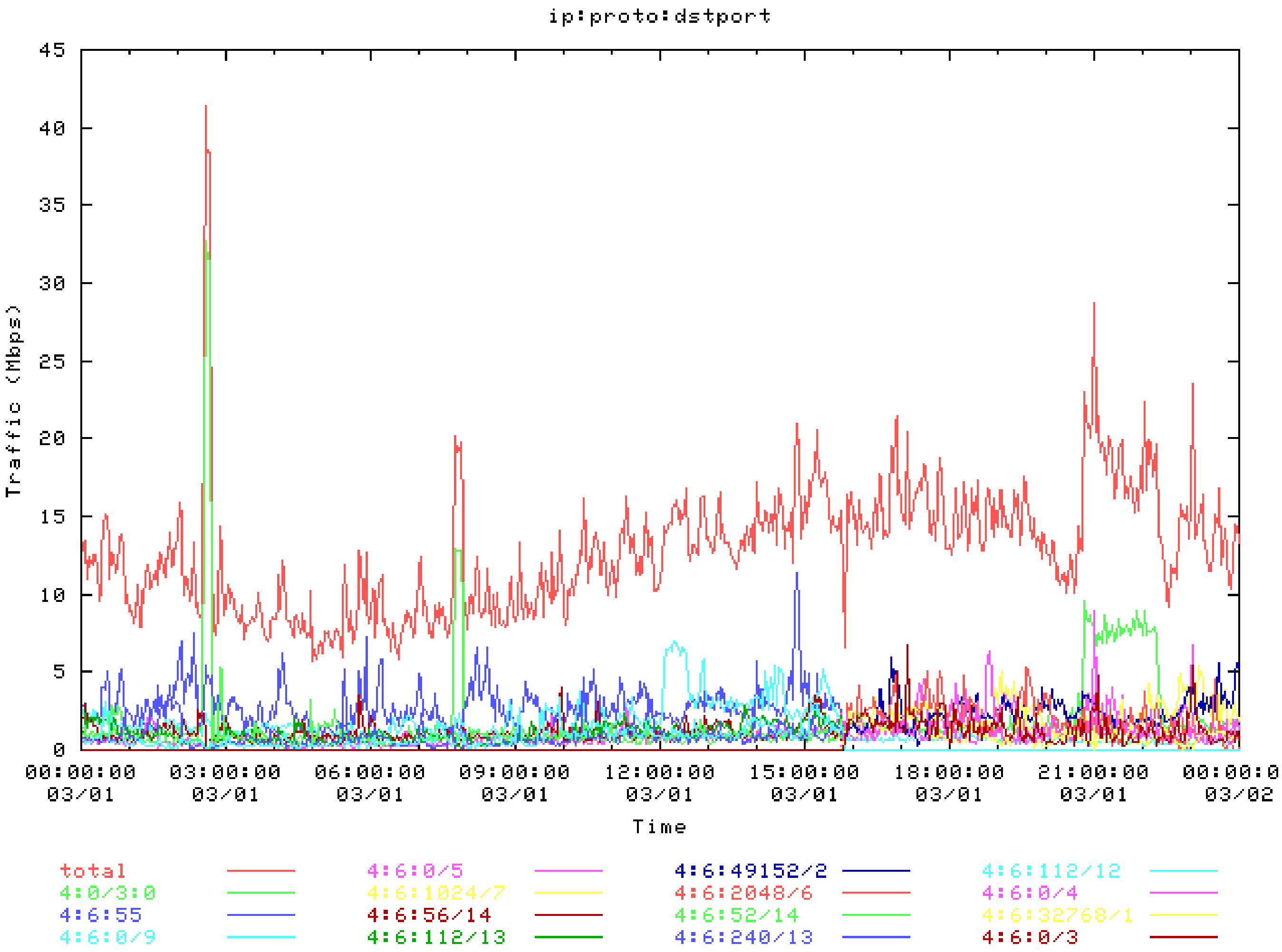


Aguri Data



Source - http://tracer.csl.sony.co.jp/mawi/aguri-ports-B/2001/

Aguri Data



http://tracer.csl.sony.co.jp/mawi/aguri-ports-B/2001/20010301-dst.png

Value of Research Output

Research on tools, tactics, and motives of the attacker.

Development of:

- Incident Response Techniques and Procedures
- Intrusion Analysis
- Forensic Analysis
- Threat Analysis
- Motivation and Profiling
- Perimeter Defense Tools

In Development

- Active Responder
- Active Defense

THANK YOU

For more information, please contact:

NISER
National ICT Security and
Emergency Response Centre

MyCERT
Malaysian
Computer
Emergency
Response
Team

Technology Park Malaysia
57000 Kuala Lumpur
Tel: +60 3 8996 1901
Fax: +60 3 8996 0827
website: http://www.niser.org.my
http://www.mycert.org.my
For General Inquiries: info@niser.org.my
Email Incidents Reporting: mycert@mycert.org.my