

Novel Worm Attack Detection

*3rd MyCERT Special Interest Group (MyCERT-SIG)
Knowledge Sharing Session*

By

R.Azrina R.Othman GCIA

MIMOS Berhad

17th January 2005

Table of Contents

- Introduction
- Anomaly Detection
- Snort NIDS Detection
- Correlation
- Countermeasures
- Challenges

Introduction

Definition

Computer worm is *an independently replicating and autonomous infection agent, capable of seeking out new host systems and infecting them **via network***

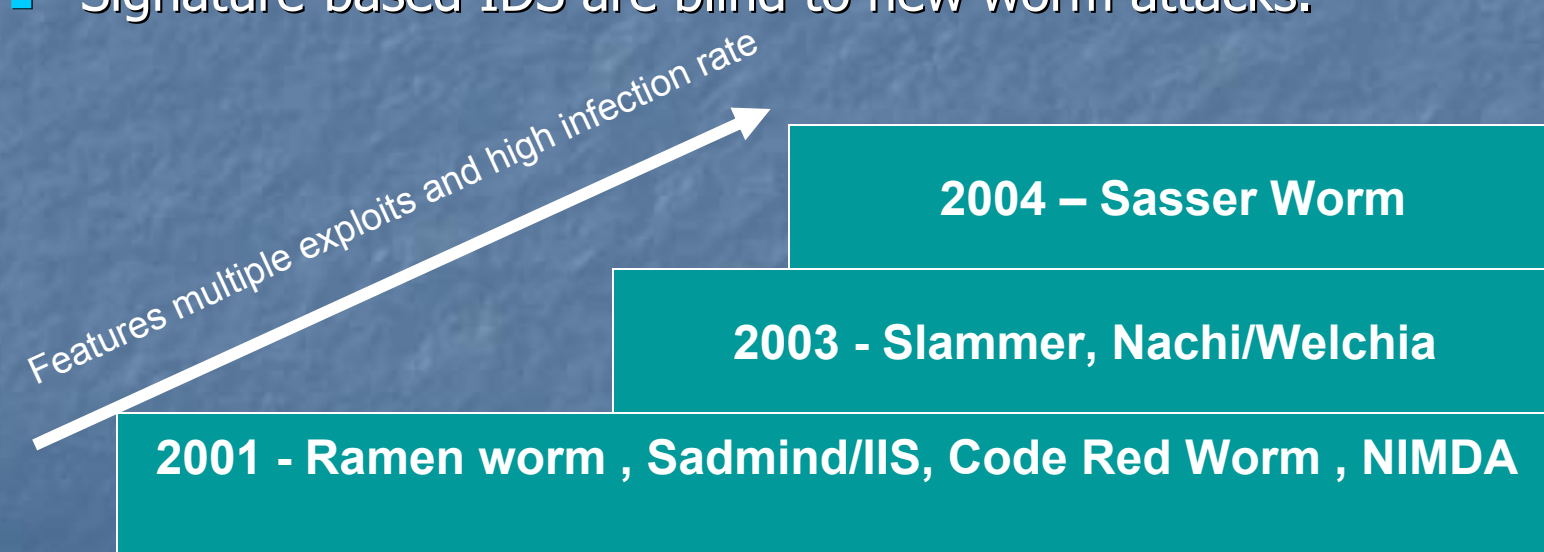
Ref: Nazario, Jose. (2004). Defense and detection strategies against Internet worms. Artech House, Inc. MA, US. pp.12.

Worm Trends

Worm	Ports Scanned	Impact	Exploit Vuln	Payload
Code Red 2001 July 19, 2001	80/tcp	i) deface webpages ii) Denial of Service attack on US gov website	MS04-033-MSDAC	Memory resident
Slammer Jan 2003	1434/udp	Denial of Service attack on Internet.	MSSQL Buffer overrun MS02-039	Memory resident
MSBlaster 12 Aug 2003	135/tcp	Denial of Service attack on windowsupdate.com	MS DCOM RPC MS03-026	rsh 4444 (tftp)
Nachi 19 Aug 2003	135/tcp and 80/tcp	Critical payload includes: - Remove msblast.exe where found. - system instability - cyberkit ping.	Exploits MS DCOM RPC and webdav MS03-007	Open 707/TCP
Sasser1 May 2004	445/tcp	Denial of Service attack	LSA Remote Buffer Overflow MS04-011	Open 9996/tcp 5554/tcp

Issues

- Worms are affecting critical networks around the globe primarily financial, health and government networks.
- Incurring high financial loss.
- Resulting breach in confidentiality, integrity and availability of information
- Signature-based IDS are blind to new worm attacks.



*Note: non comprehensive list of recent worms

Previous Work

- packet matching [\[i\]](#),
- traffic concentration analysis and inductive learning [\[ii\]](#),
- connection history-based anomaly detection [\[iii\]](#) and
- Kalman filter [\[iv\]](#)

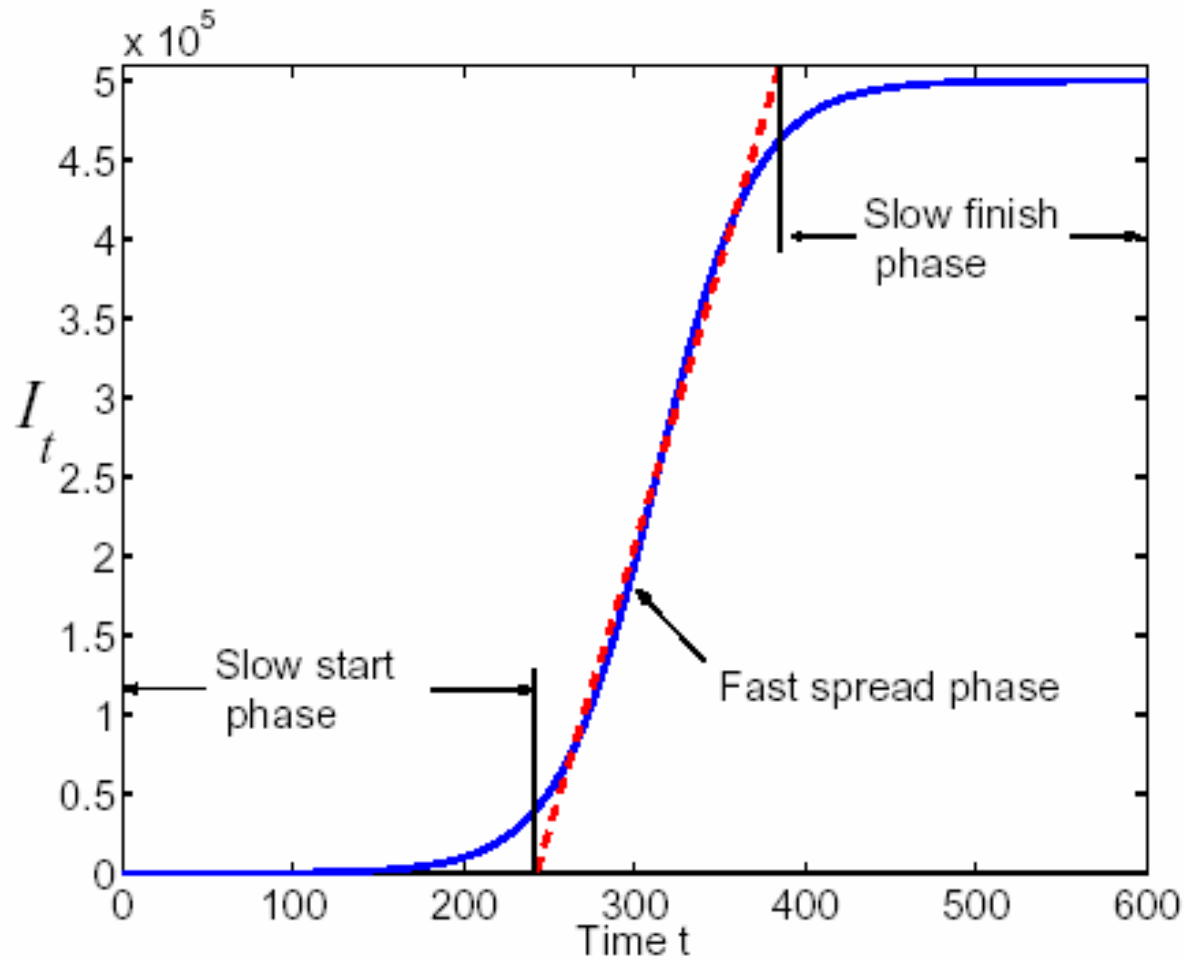
[i] Chen, Xuan & Heidemann, John. (2004). Detecting Early Worm Propagation through Packet Matching. Technical Report ISI-TR-2004-585, USC/Information Sciences Institute, February, 2004. [Internet] Available from: <http://www.isi.edu/~johnh/PAPERS/Chen04a.html>. [Last accessed 14/9/04]

[ii] Noh, Sanguk. Lee, Cheolho. Ryu, Kaywon. Choi, Kyunghee & Jung, Gihyun. (2004). Detecting Worm Propagation Using Traffic Concentration Analysis and Inductive Learning. Proceedings of IDEAL04 University of Exeter, on 27th August 2004. [Internet] Available from: <http://songsim.catholic.ac.kr/~sunoh/webdata/idealWorm04.pdf> [Last accessed 14/9/04]

[iii] Toth, T & Kruegel, C. (2002). Connection-history Based Anomaly Detection. Proceedings of the 3rd IEEE Workshop on Information Assurance and Security, West Point, NY, June 2002. IEEE Computer Society Press, USA.

[iv] Zou, Cliff Changchun. Gao, Lixin. Gong, Weibo & Towsley, Don. (2003). Monitoring and early warning for internet worms. Proceedings of the 10th ACM Conference on Computer and Communication Security 2003, Washington D.C., USA on October 27 - 30, 2003. ACM Press, New York, NY, USA. pp: 190 - 199

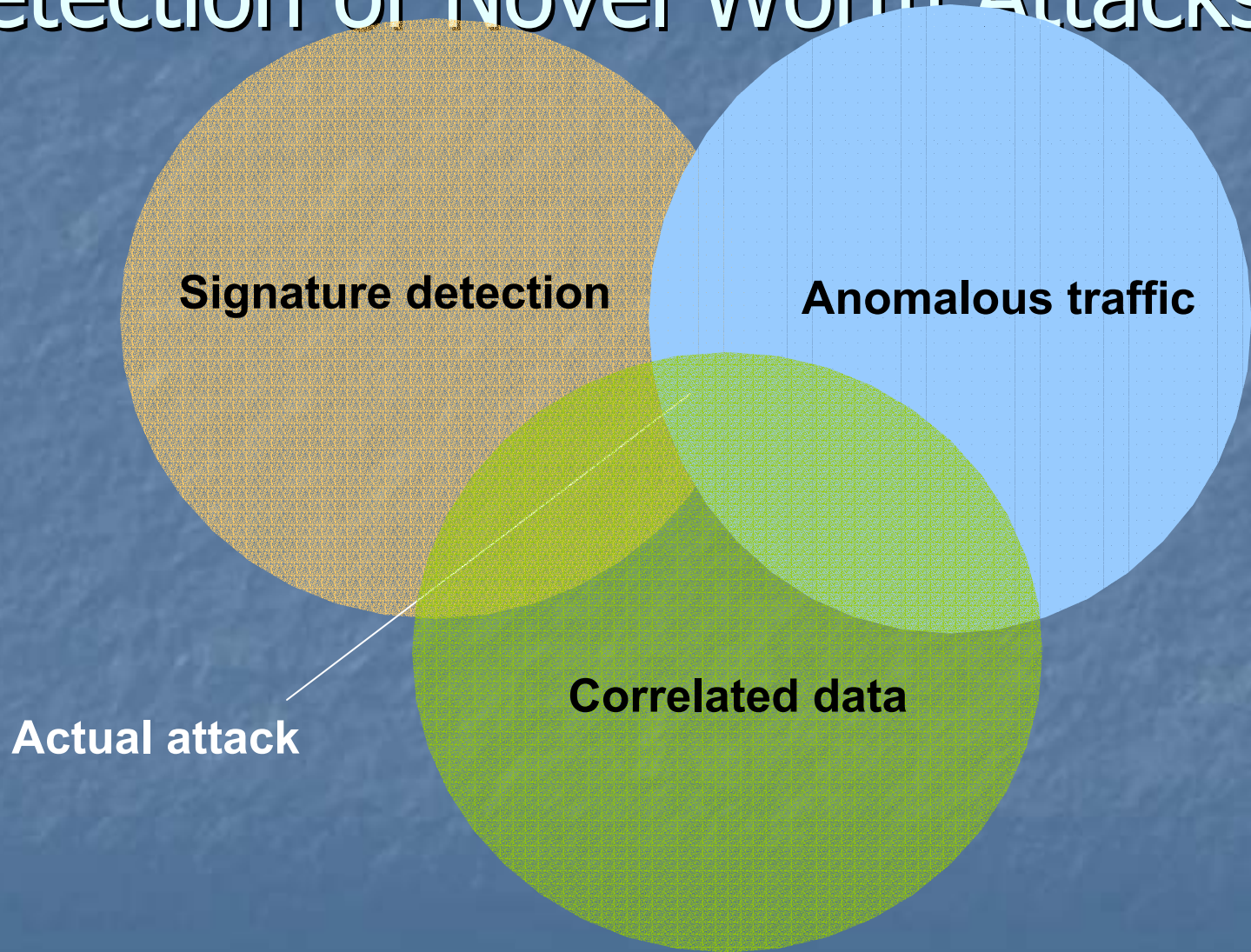
Worm propagation Model



Source: Zou et al. Zou, Guo, Changshun, Cao, Lixin, Song, Weiss & Powers, Don. (2003). Monitoring and early warning for internet worms. Proceedings of the 10th ACM Conference on Computer and Communication Security 2003, Washington D.C.,

USA on October 27 - 30, 2003. ACM Press, New York, NY, USA. pp: 190 - 199

Detection of Novel Worm Attacks

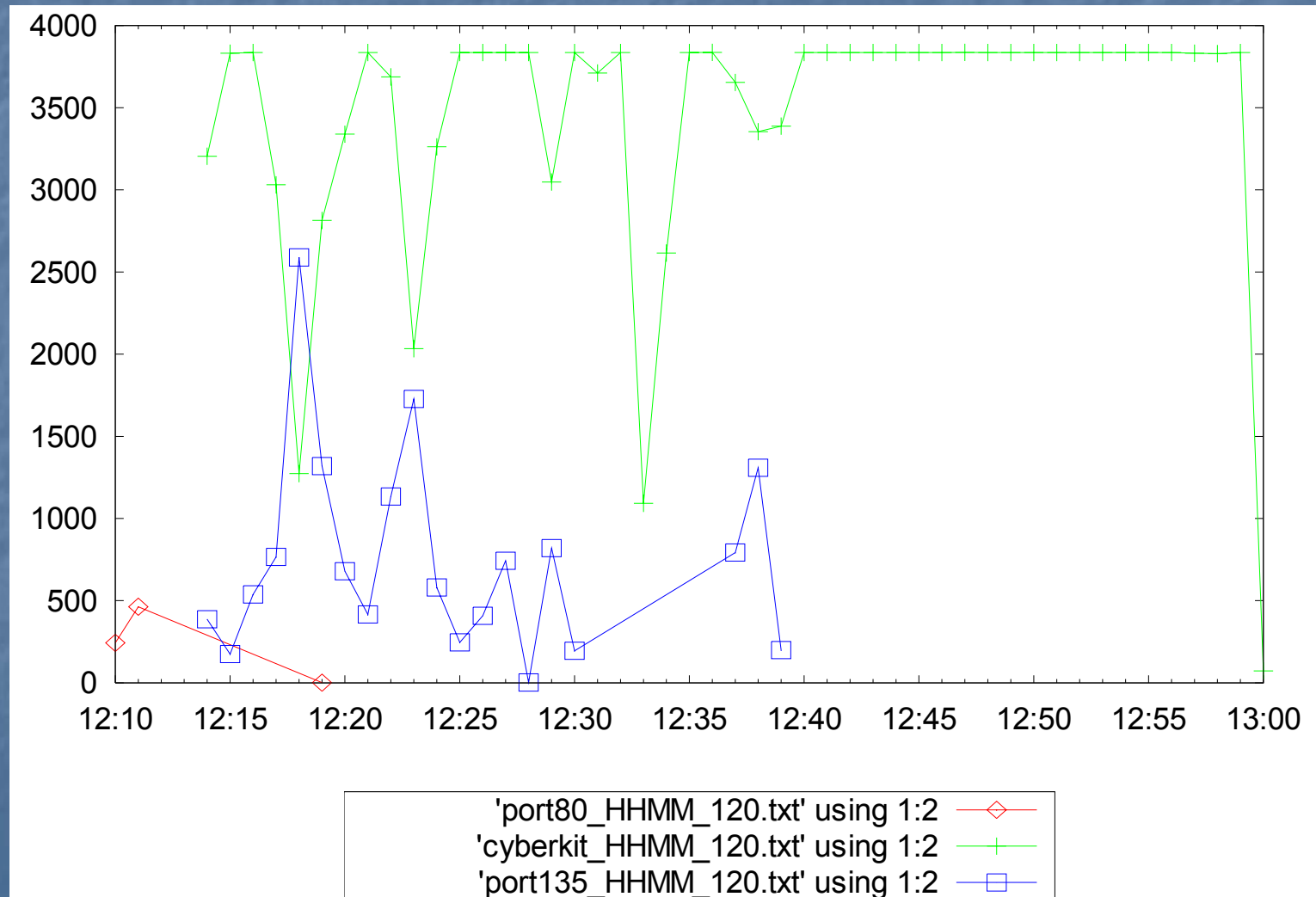


Data Sets

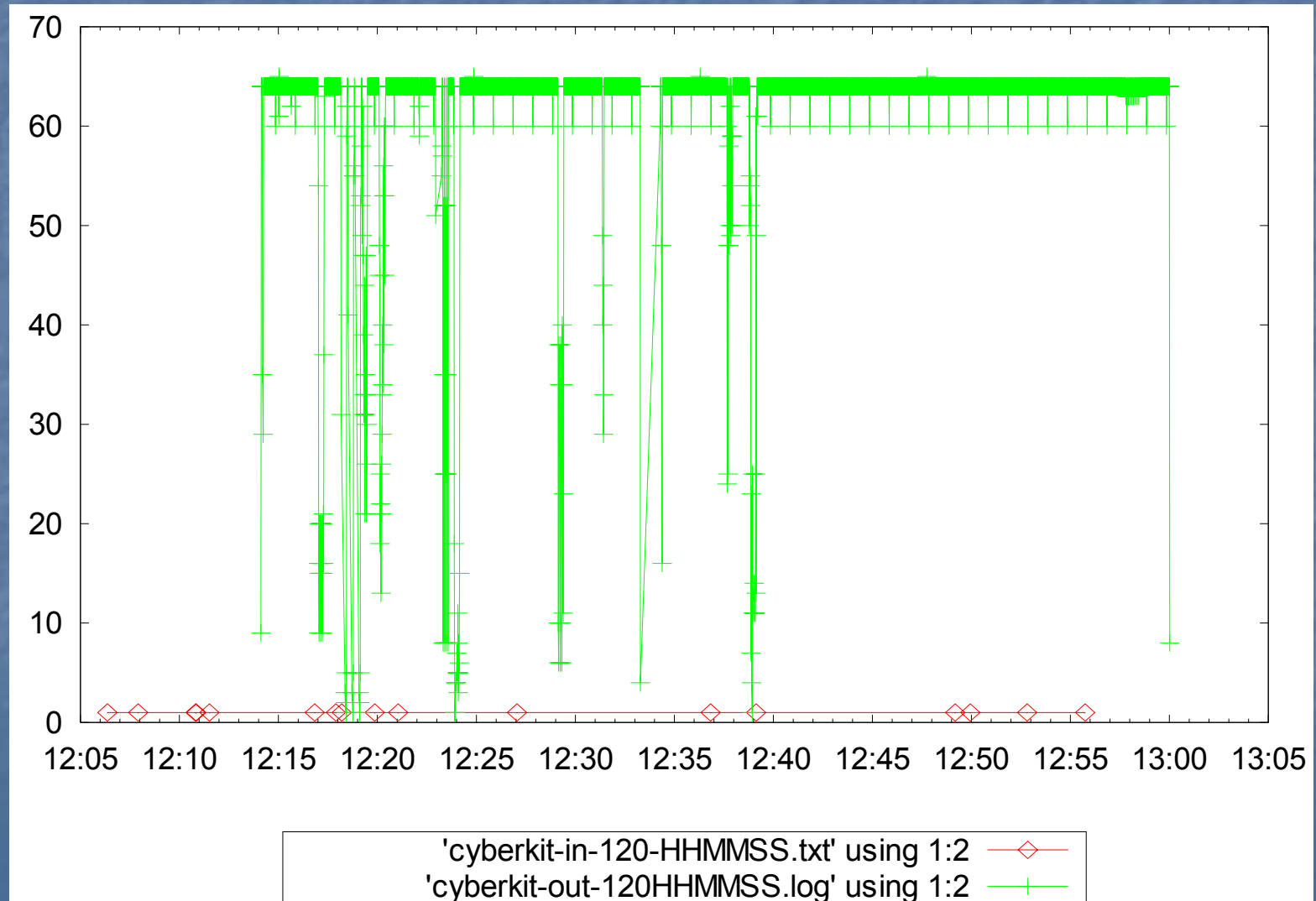
- Two honeypots – Target 1 & Target 2 were infected with the following worms:
 - Nachi – 20th August 2003 (ICMP-based)
 - Sasser – 2nd June 2004 (TCP-based)
- pcap binary logs

Anomaly Detection

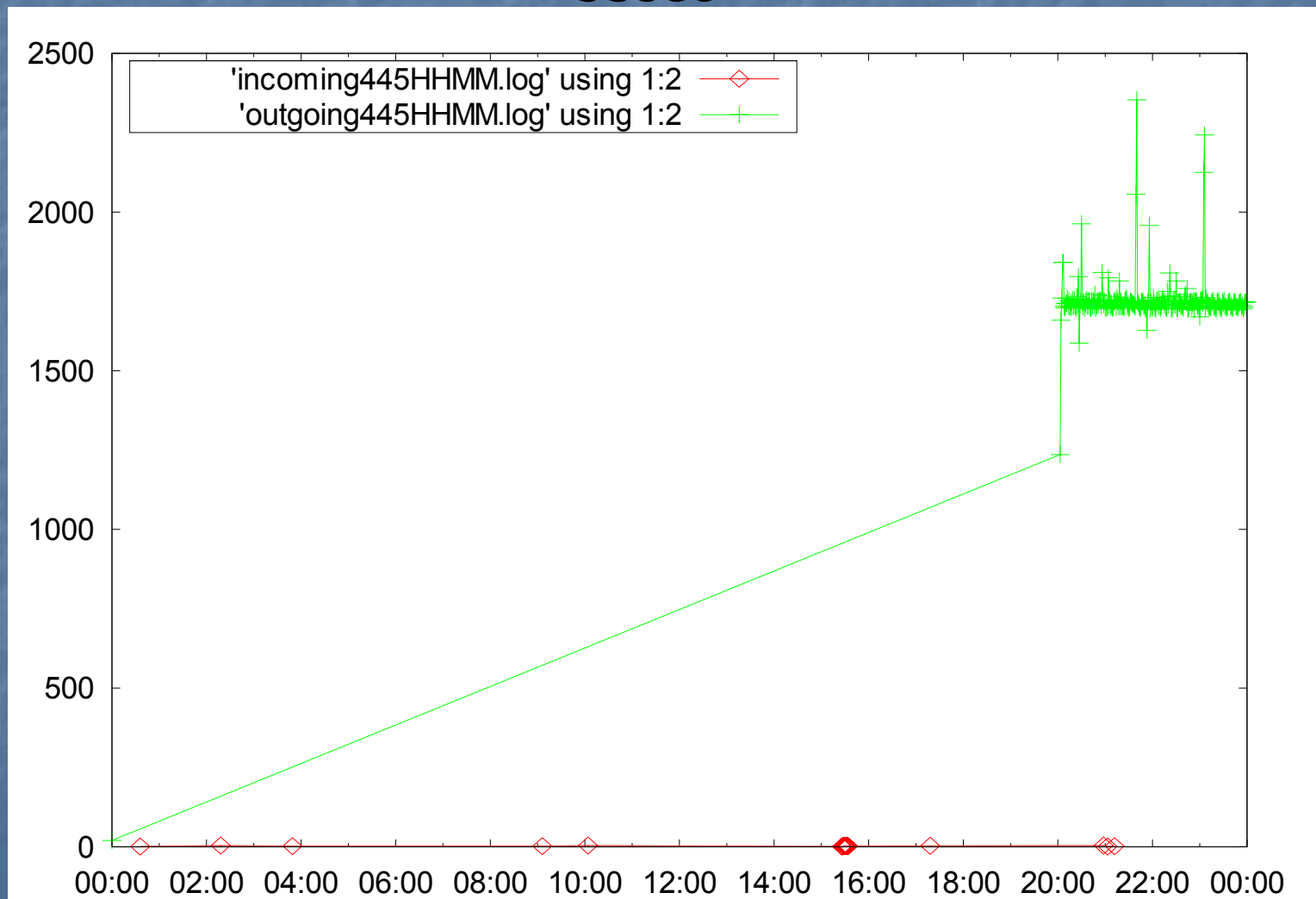
Nachi Worm on Target 1 only began generating cyberkit scans 3min 18sec after infection, after downloading the relevant Microsoft patches.



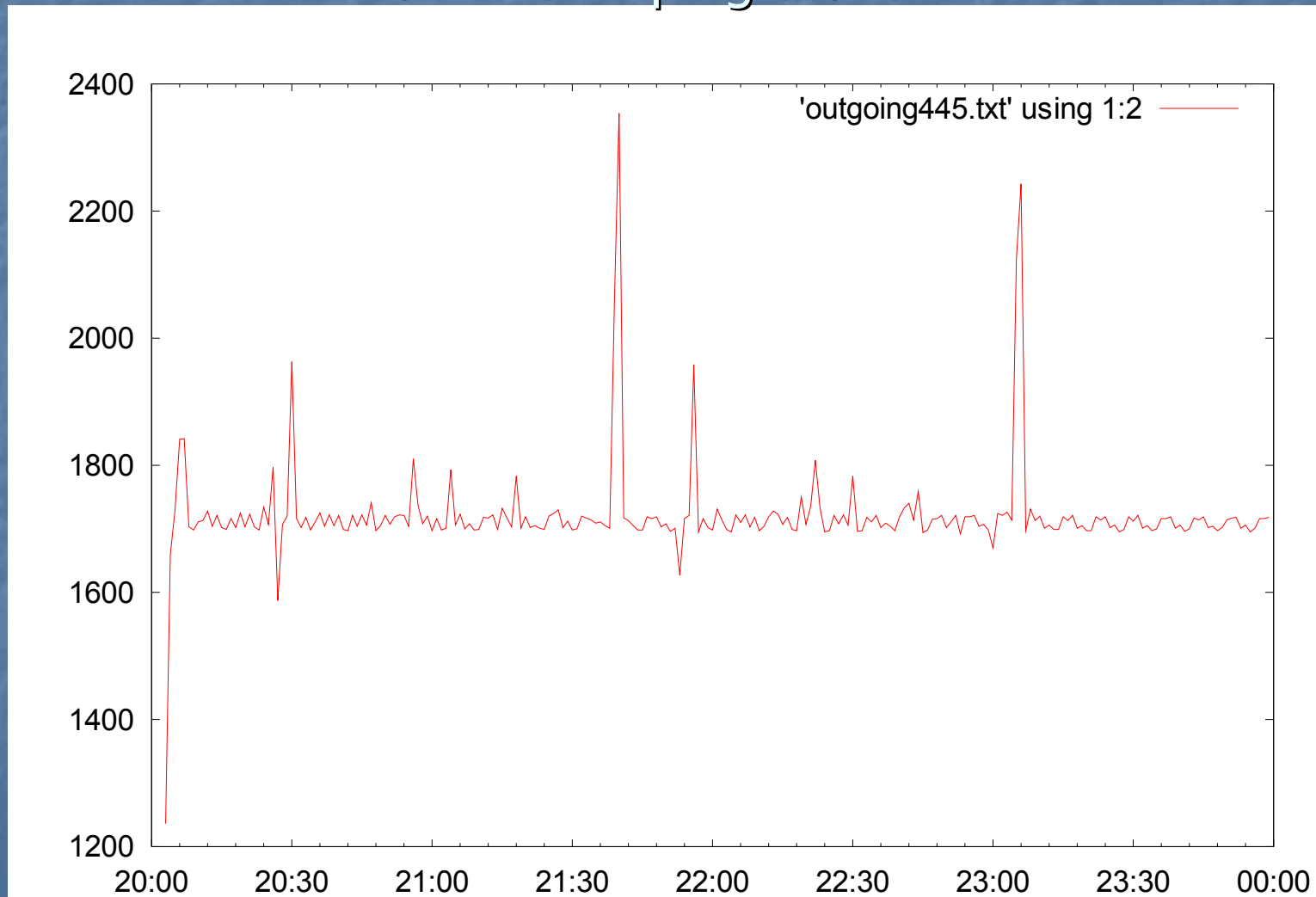
Nachi, average of 59 and 61 pings per-second within the first minute for Target 2 and Target 1 respectively. Both targets reached 64 pings per-second at its plateau.



Sasser Worm, time lapse of the last incoming scans and the time when host began to scan network was 2hrs 44min 33sec



Sasser on Target 1 produced 1723 scans per minute, which is about 28 SYN scans per second, almost half the rate of nachi ICMP ping scans.



Snort (NIDS) Detection

Applying Snort PreProcessor

Nachi

- preprocessor portscan: \$HOME_NET 4 3
/data/log/fastScanLog/fastscan.log
- filter failed to detect the source of the infection of Target 2 host (the incoming cyberkit scan that hit Target 2).
- Snort Pre-processor data cannot be used for correlation.

Applying Snort PreProcessor

Sasser

- preprocessor portscan: \$HOME_NET 4 3 /data/log/fastScanLog/fastscan.log
- several incoming scans were detected targeting Target 1 host. The scans targeted several ports other than 445, such as ports 135, 139 and Sasser's backdoor port 5554.

```
Jun  2 03:49:19 210.x.238.176:3046 -> 202.190.target1-host:445 SYN *****S*  
Jun  2 09:06:24 202.x.3.209:4696 -> 202.190.target1-host:445 SYN *****S*  
Jun  2 17:18:41 206.x.12.9:2133 -> 202.190.target1-host:445 SYN *****S*
```

Snort Signature-based Detection of Nachi's Cyberkit Ping

Rules

- "NETBIOS DCERPC ISystemActivator path overflow attempt little endian" with snort sid # 2351 and "ICMP PING CyberKit 2.2 Windows" with snort sid #483.

Results:

- Cyberkit Ping from the infected host (Target 1) was at approximately 12:14:07.875193 which was exactly the same time as the actual scan.

Signature-based detection of Sasser Worm

Rules

- LSASS exploits (worm.rules- appendix 1a) were included in the *snort.conf* files and snort was run against the June 2004 logs.

Results

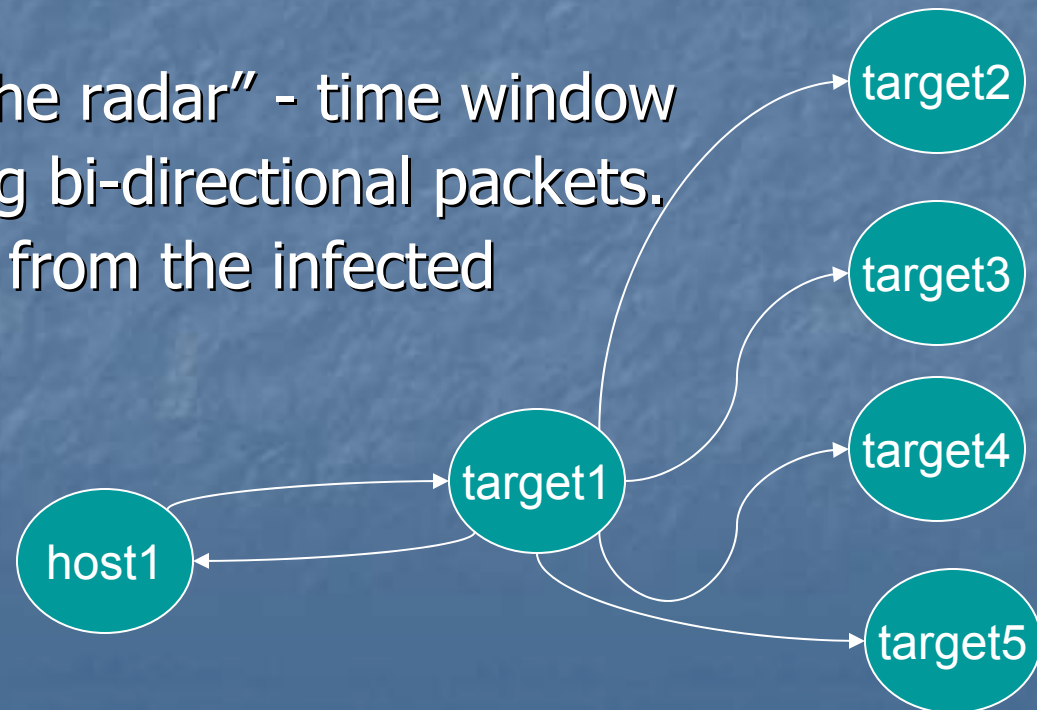
- first snort detection of the Netbios-LSASS exploit (Sasser worm) had a delay of about 8 minutes after the first scan was initiated from the infected Target 1 host which appeared approximately at 20:03:14.035580

Correlation

Correlation

Correlating traffic time-based and multi-host:

- Detect bi-directional traffic of the incoming scan from other infected system, followed by identical outgoing scan initiated from the host.
- Match the ports/protocols corresponding to the matched IP.
- Decide “footprint of the radar” - time window between the matching bi-directional packets.
- Measure rate of scan from the infected host.



Countermeasures

- To reduce the impact, following options may be considered depending on the type of worm traffic (port, protocol and payload):
 - Filtering at router (ACL)
 - Application layer Firewall/Cache
 - Packet scrubber
 - Sinkholes or Blackholes
 - Intrusion Prevention System

Challenges

- But the challenges are,
 - fast scanning worms that congest before the perimeter defence device can kick-in.
 - Worms that scans without unique payload/ports.
- Improved methods of detection and mitigation are constantly being developed.

Thank you