

Adaptive Network Intelligence

netDeFlect

Protecting DR and BCP

Esphion
March 2005

ESPHION

1

Esphion Limited Copyright © 2004 - Proprietary & Confidential

Agenda

- Static security
- Anomalies and rules
- Neural technology (ANN)
- Esphion's Solution
- Anomalous Traffic
- Signature generation
- Deployment
- Existing Technology
- Reporting

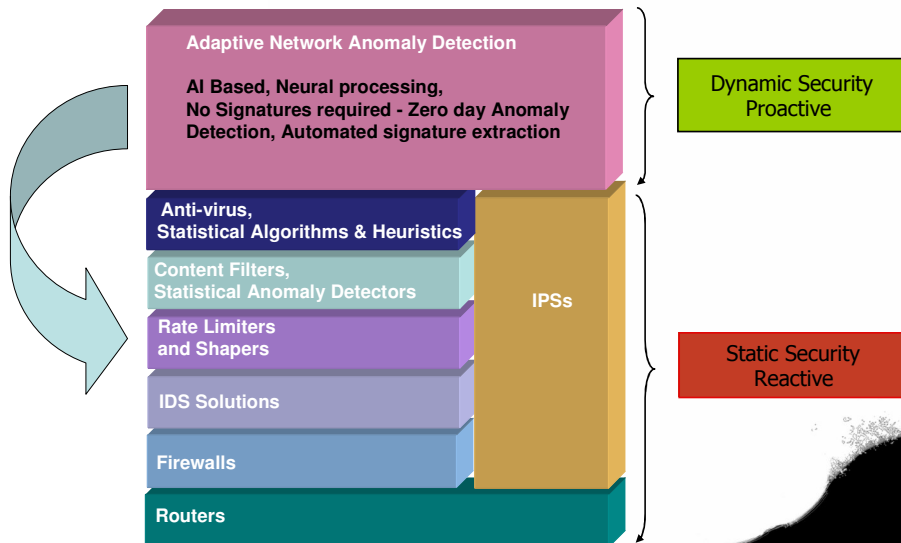
ESPHION

Router's, Firewalls, IDS, IPS Static Technology

- Current technologies rely on known factors
- Rule based
- Filter based
- Signatures
- In Line
- Protect Networks from known events

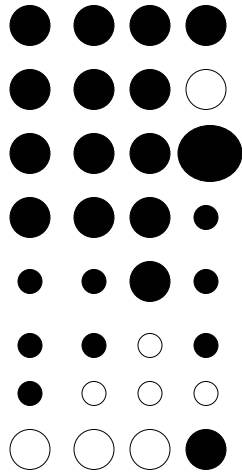
ESPHION

Dynamic Security Overlay



ESPHION

Anomalies and Rules !



•Rules

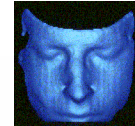
- IF one is WHITE
- IF one is BIG
- IF one is SMALL
- IF three are SMALL
- IF all are SMALL and one is WHITE
- IF all are SMALL and one is BLACK
- IF one is BLACK
- IF.....
- ..



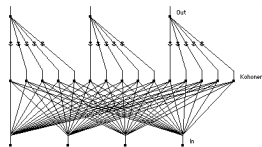
What is the Rule for this ?

ESPION

What is a Neural Network?



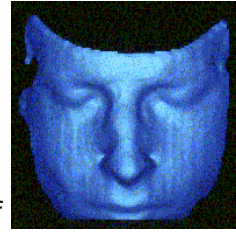
- Neural networks are based on the processing ability and memory abstraction of the human brain to identify patterns of behavior of interest.
- Neural networks are used where:
 - We can not use fixed mathematical solutions to complex evolving problems
 - We can get lots of examples of the behavior we require
 - Where we need to pick out structure from existing data and patterns of behaviors
 - Where huge volumes of data need to be processed in real, or near-real time.



ESPION

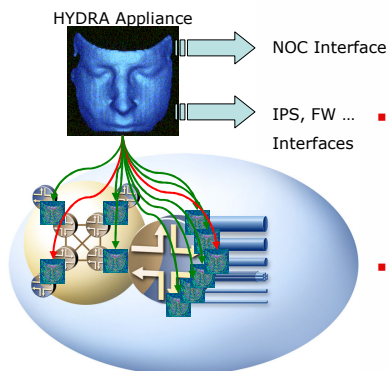
Neural networks

- **1940's** first neural network model
- **1950's** Rosenblatt's "perceptron" capable of learning
- **1980's** renewed interest – faster machines, self generating NN's - competitive learning models, multilayer networks.
- **1990's** Commercial, Banks – OCR –Image compression, Data mining speech recognition, Weather forecast.
- **2000's** ???



ESPHION

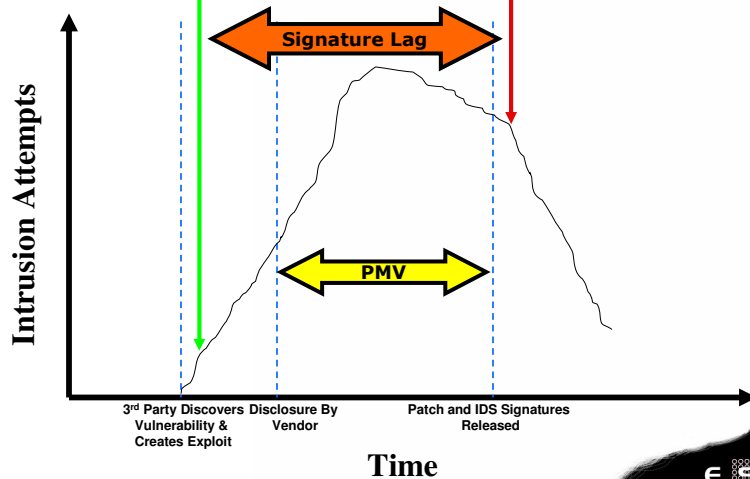
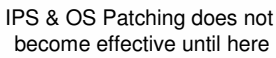
Esphion's Solutions netDeFlect – adaptive Security



- Distributed adaptive solution that automatically detects and diagnoses unknown threats in real-time without **signatures**
- Self learning **neural networks**: maximize the ability to adapt to changing network conditions without ongoing re-configuration and maintenance
- Creates - *within seconds* - 'signatures' from anomalous network traffic for use by in-line IPS tailored to the traffic on a specific network.
- Compliments existing reactive security solutions (IPS) – delivers layered 'best practice' security solution

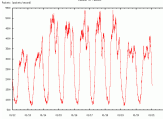
ESPHION

netDeflect effective
from day Zero

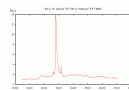
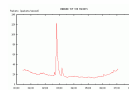
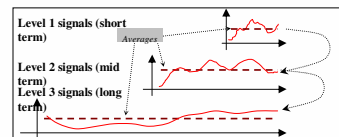


ESPHION

- Extensive data collected directly from the network, e.g.
 - Number of packets of particular types
 - Ratio of particular packet types compared to each other



Patent Pending Neural Network
analysis used to detect anomalous
deviations in traffic profiles

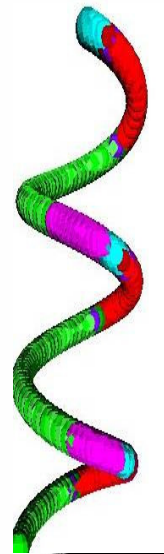
[illegible]

- Patented Anomaly diagnosis technology produces
- Automated Capture of anomalous traffic
 - Standardized signature of anomaly created
 - Worm scanning activity revealed
 - Critical Information output to network operation for action

ESPHION

Anomalous Traffic: Worms

- Designed to Intrude by Stealth
 - Objective is to Secure Unlawful Access, Theft, Vandalism, Extortion
- Worms attack the hosts / computers on a network
 - Take advantage of vulnerability's in OS's and/or application's.
 - The network is typically NOT the target.
 - Do NOT need intervention to perform the infection or replication.
 - Automatically looks for new systems to infect (Self Propagating)
- Worms are most often identified through Symptoms of infection
 - instability of infected host, increased CPU load
 - Network Scanning activity seeking - new hosts to infect
 - Well written Worms are not detected!!!!
- Networks are impacted as a 'side-effect'
 - rapidly spreading worms may cause huge traffic increases
 - overload billing systems

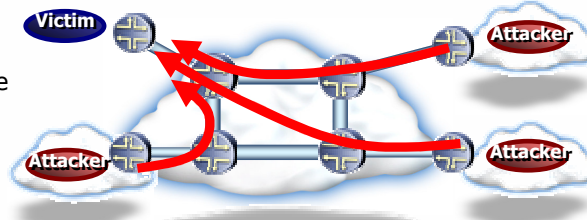


ESPION

Anomalous Traffic: DDoS (Distributed Denial of Services)

- Extortionate activity NOT aimed to 'intrude', but only to 'deny access'

- For most enterprises and individuals, defense is not possible



- Often Tens of ,000's of compromised PC's used to send network traffic (Flood) to a targeted company.

- DDoS may affect multiple levels of network infrastructure
- filling the network links
- exhausting router forwarding capability
- overloading Ethernet switches
- Exhausting IDS / Firewall memory and resources overloading of servers

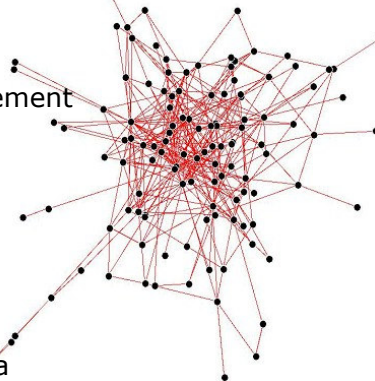
- Traditional (Firewall/IDS) Methods of Detection and Filtering are Limited

- Target typically notices only when services cease to function.
- Providers notice when their customers (The targets) call and complain
- Flood Traffic may look like 'normal' network traffic

ESPION

Anomalous Traffic: Network Abuse (MISUSE)

- Not-used for-business / Peer to Peer (P2P) applications
 - Traffic Volumes
 - Content Liability
 - Work and private data management
- Web and Game Servers
 - UDP traffic.
 - Streaming Content
- Non-sanctioned Applications
 - Chat Relay's
 - Re-mailers, Spam hosts
 - Non-sanctioned storage of data
- Non-sanctioned Network Access
 - Wireless Networking
 - Internally configured Firewall Bypass dial-in



ESPHION

netDeFlect Visualisation Portal

ESPHION Traffic Hosts Ports Anomaly Help Logout

Anomaly List

XENsors: Esphion Group(s): Adelaide, Brisbane, Catch_All, Chippendale Type(s): sick-in, ack-out, frag-in, frag-out

Time Range (Eastern Summer Time (New South Wales))

Preset: Custom From: 2005 Feb 22 08 To: 2005 Feb 26 12 43

Minimum Duration: 5 mins Minimum Rank: 3 Minimum Packetrate Deviation: 50 pkt/s 15 % Minimum Bitrate Deviation: 40 kbit/s 100 % Result Limit: 100 records Go

ID	Timestamp	XENsors	Group	Type	Duration	Rank	Deviation (pkt/s)	% pktrate	Deviation (kbit/s)	% bitrate
98508	2005-Feb-25 17:55:18	Esphion	Catch_All	tcp-out	14m 35s	3	193.99	235.80 %	1,653.60	248.21 %
98062	2005-Feb-23 09:57:16	Esphion	Catch_All	tcp-out	05m 36s	3	208.93	195.76 %	1,662.04	240.48 %
97985	2005-Feb-22 18:48:24	Esphion	Catch_All	tcp-out	09m 44s	3	113.09	283.81 %	377.74	306.44 %
97891	2005-Feb-22 09:50:16	Esphion	Catch_All	syn-in	05m 36s	3	82.35	238.31 %	42.14	238.35 %

authorised access only

Printer Friendly Version

Esphion Visualisation Portal v2.4

Copyright 2003-2004 Esphion Ltd.

ESPHION

ANALYTICS

Activity Report

Traffic

Hosts

Ports

Accounts

Info

Tools

Activity ID: 97391

Exploit: Exploit

Group: CME_0

Time Detected: 2015-04-22 10:50:28 (10:51:37)

Time Used: 2015-04-22 10:50:28 (10:51:37)

Duration: 05m 36s

Location: Localhost

Activity ID: 97391

Summary

Rank	3
Type	0/0/0
Packetrate Deviation	230.31%
Bitrate Deviation	230.31%
Bytes Deviation	15.5
Patterns Detected	20

Traffic Statistics

Direction	Mean Packetrate (pkts/s)	Mean Bitrate (kB/s)	Total Packets (Packets)	Total Bytes (Bytes)
Download	34.6	42.1	14,117	7,766
Upload	92.35	52.4	297,458	15,565
Observed	116.95	68.12	442,273	28,375

Traffic Charts

Increasing TCP SYN packet rate

Traffic Charts

Increasing TCP SYN / outgoing TCP FIN ratio

Detected Patterns

Pattern ID	Matches	Hosts	Last Seen	Short Description
97391-0	314/1000	1/100	09:50 192.49.132.92 x 192.49.145.60	
97391-1	205/1000	1/100	09:51 192.49.132.92 x 192.49.145.60	
97391-2	188/1000	1/100	09:51 192.49.132.92 x 192.49.145.60	
97391-3	103/1000	1/100	09:51 192.49.132.92 x 192.49.145.60	
97391-4	79/1000	1/100	09:51 192.49.132.92 x 192.49.145.60	
97391-5	613/1000	1/100	09:50 192.49.132.92 x 192.49.145.60	
97391-6	188/1000	1/100	10:08 192.49.132.92 x 192.49.145.60	
97391-7	188/1000	1/100	10:11 192.49.132.92 x 192.49.145.60	
97391-8	287/1000	1/100	10:14 192.49.132.92 x 192.49.145.60	
97391-9	185/1000	1/100	10:17 192.49.132.92 x 192.49.145.60	
97391-10	398/1000	1/100	10:23 192.49.132.92 x 192.49.145.60	
97391-11	317/1000	1/100	10:23 192.49.132.92 x 192.49.145.60	
97391-12	344/1000	1/100	10:29 192.49.132.92 x 192.49.145.60	
97391-13	342/1000	1/100	10:29 192.49.132.92 x 192.49.145.60	
97391-14	175/1000	1/100	10:30 192.49.132.92 x 192.49.145.60	
97391-15	282/1000	1/100	10:35 192.49.132.92 x 192.49.145.60	
97391-16	204/1000	1/100	10:41 192.49.132.92 x 192.49.145.60	
97391-17	329/1000	1/100	10:41 192.49.132.92 x 192.49.145.60	
97391-18	399/1000	1/100	10:47 192.49.132.92 x 192.49.145.60	

authorised access only

Printer Friendly Version

Epsilon Visualisation Portal

v2.4

ESPION

[illegible]

ESPION

netDeFlect ACL Generation

The screenshot shows the 'Anomaly Filter' configuration page in the Esphion Visualisation Portal. The 'Pattern ID' is 97891-0. The 'Type' is set to 'Cisco_ACL'. The 'Options' section has checkboxes for 'No Extended' and 'No Flags', both of which are unchecked. The 'Name' field contains 'Esphion-Pattern-Filter-97891-0'. Below this, the 'Packet Filter' section displays the following rules:

```
ip access-list extended esphion_pattern_filter_97891_0
deny tcp 162.48.130.82 0.0.0.0 162.48.0.0 0.0.255.255 eq 445 match-all *syn *fin *rst *push *ack *urg
```

The 'Filter Details' section shows:

Pattern ID	97891-0
Filter Type	Cisco_ACL
Filter Options	None
Filter Name	Esphion-Pattern-Filter-97891-0

At the bottom, it says 'authorised access only' and 'Printer Friendly Version'. The portal version is v2.4.

netDeFlect produces automatic ACL's and Rules that can be directly applied to complimentary security devices.....

Now:-

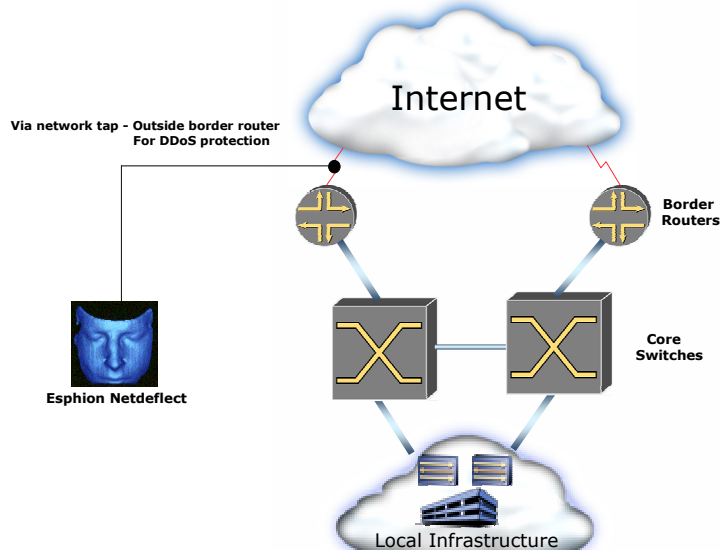
Cisco ACL's, Fortinet, SNORT

Near Deliverables:-

PIX, CheckPoint, Symantec...

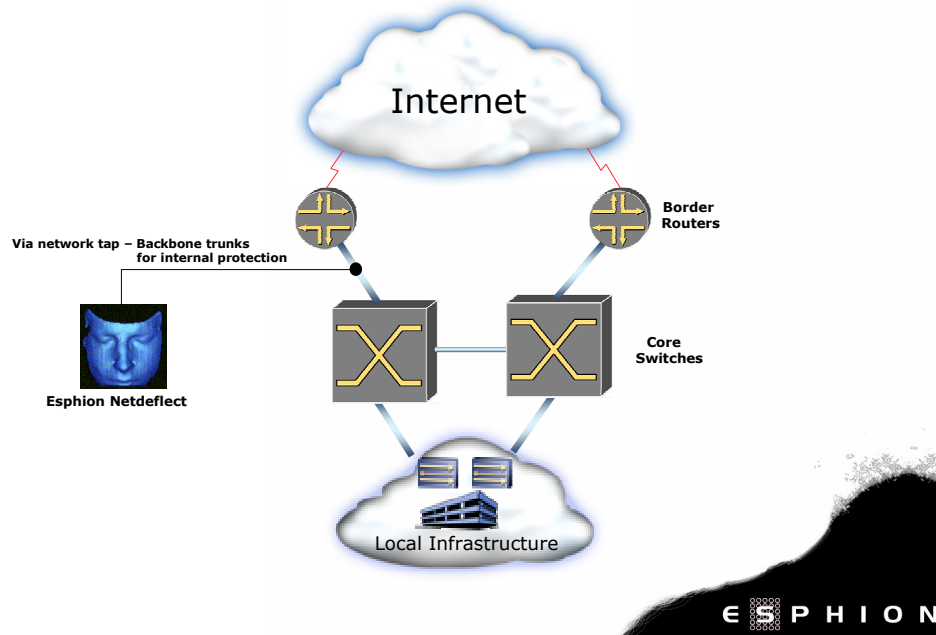
ESPHION

Standalone Deployments

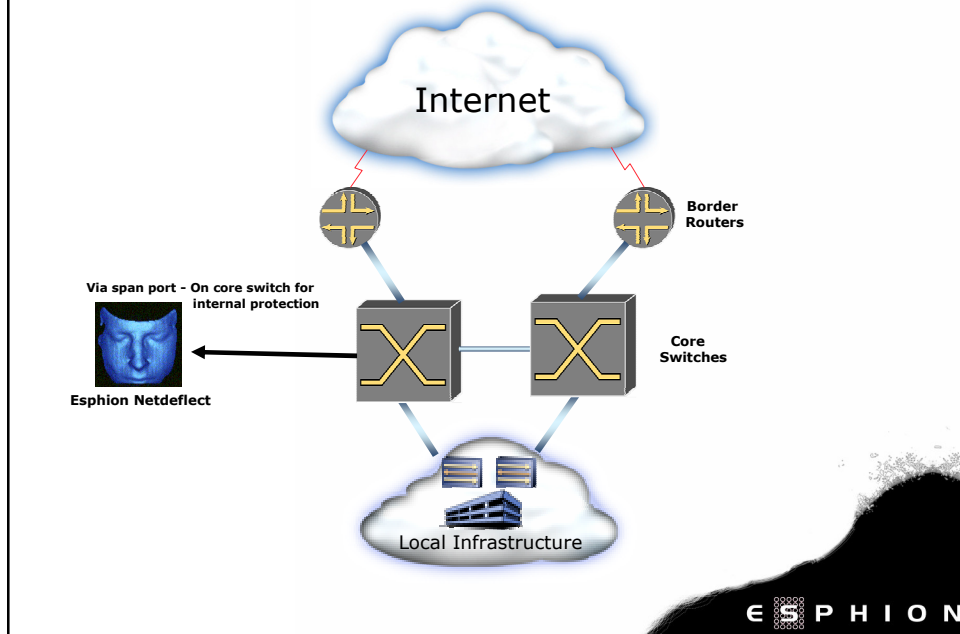


ESPHION

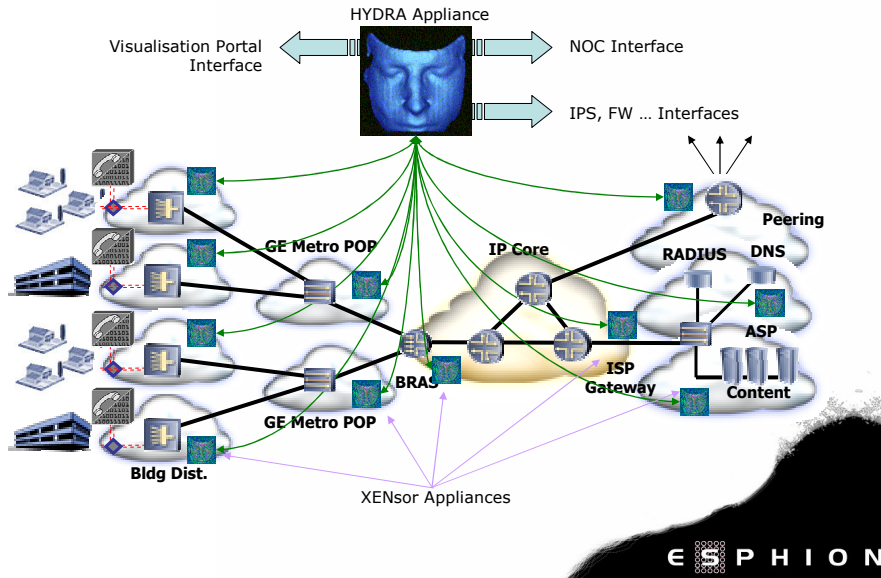
Standalone Deployments



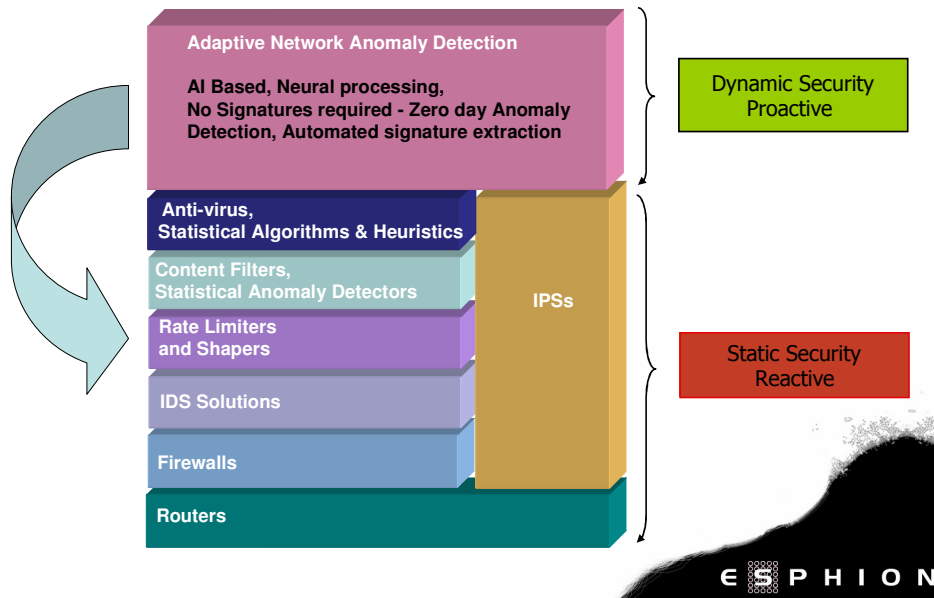
Standalone Deployment



Typical distributed deployment



Dynamic Security Overlay

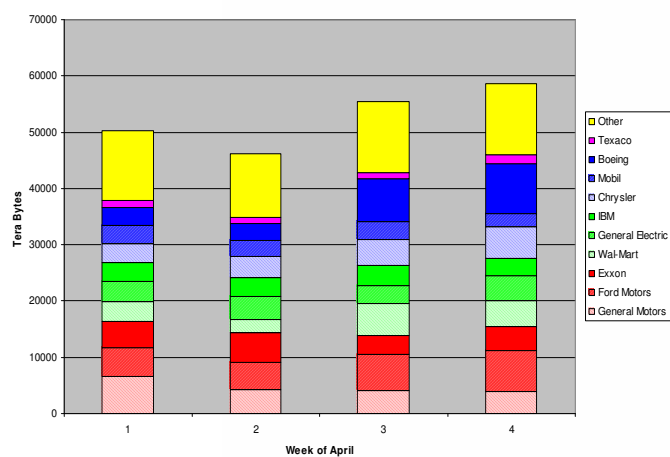


Real Time Traffic views from netDetail



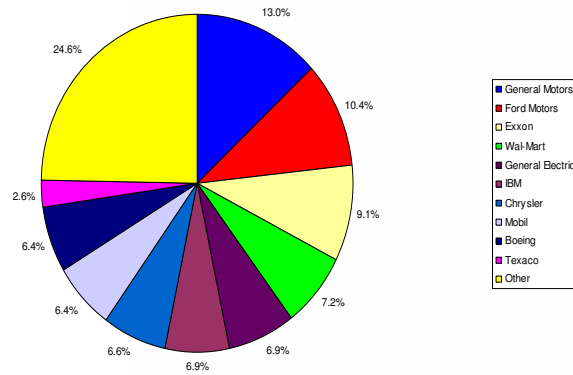
Top 10 Users – Total Usage by week

Top 10 Companies (April 2004)



Top 10 Users by % used

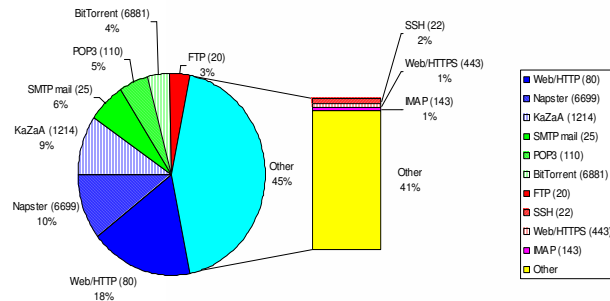
Percentage Total Usage by Top 10 Customers (12 - 18 April 2004)



ESPION

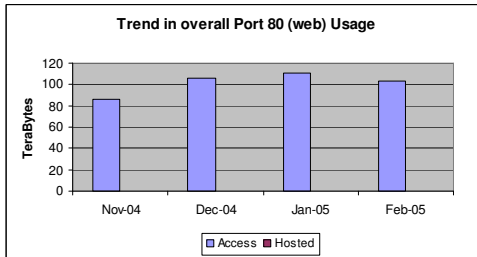
Top 10 Applications and % of Network used

Company Percentage Total Usage by Top 10 Applications by TCP Port (12-18 April 2004)



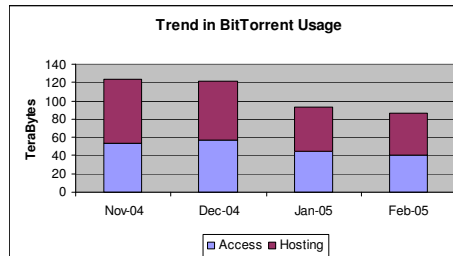
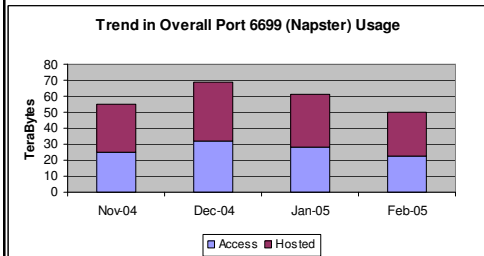
ESPION

Sample Reports – Usage Trends Web, P2P



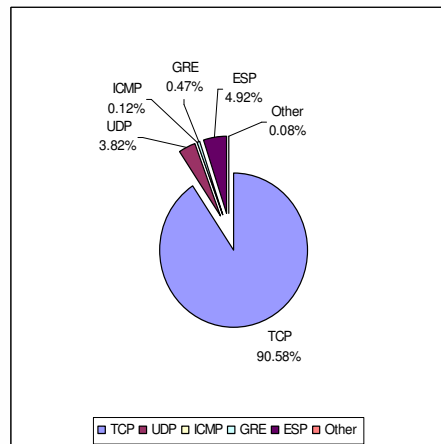
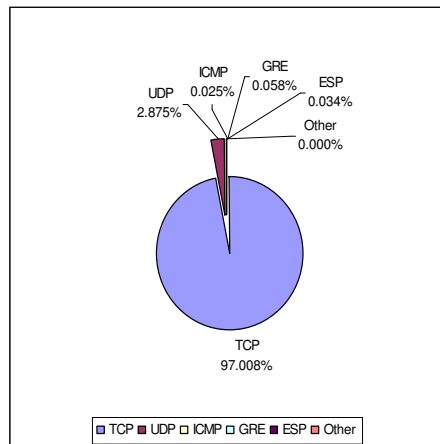
Notes:

• Port 6881, 16881, 1881 and 6882 are used to represent BitTorrent. These ports contribute 95.5% of overall BitTorrent volume.



ESPHION

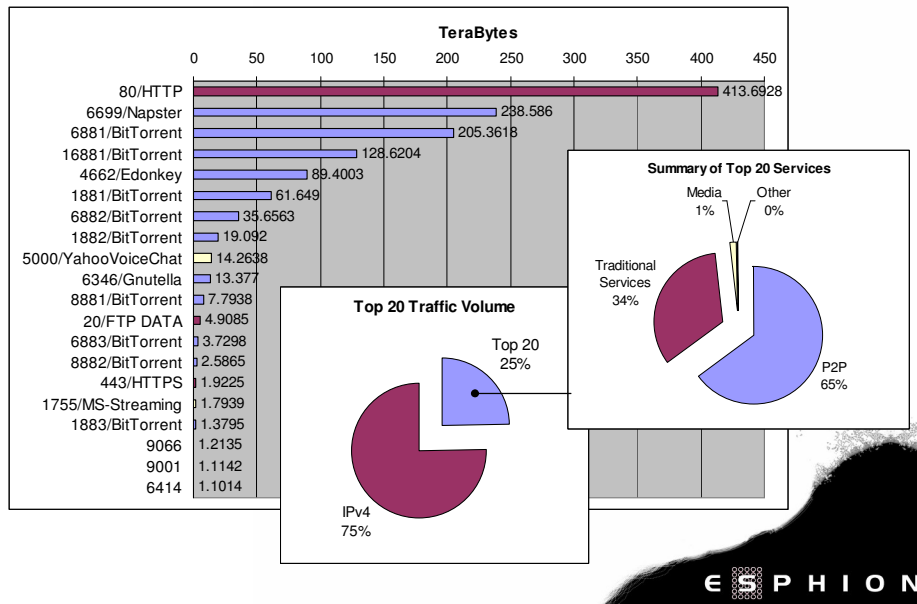
Sample Reports – Overall Traffic Usage



90-97% of traffic is TCP

ESPHION

Sample Reports – Traffic Volumes



Anomaly Report for period: 12-18 April 2004

Total number of anomalous events	200
Inbound	60%
Outbound	40%
Total number critical events >15 minutes >30% degrade/total usage	90
Critical anomalous events alerted and mitigated	90

Anomalies by Classified Event

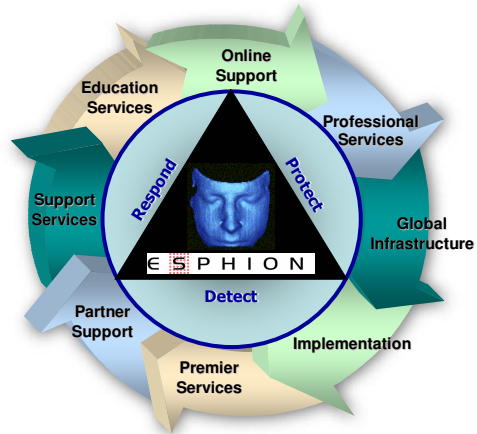
Total anomalies attributed to worm scanning	90
Anomalies due to worm scanning into your network	70%
Anomalies due to worm scanning originating from your network	30%
Total anomalies attributed to Denial of Service attacks	40
Denial of Service attack into your network	90%
Denial of Service attack out of your network	10%
Total anomalies attributed to P2P traffic	50
Inbound P2P traffic	40%
Outbound P2P traffic	60%
Total other/unattributed/unclassified anomalies	20
Inbound	40%
Outbound	60%

Estimated Bandwidth Consumed by Classified Anomalies

Worm scanning	3GB
Denial of Service attacks	1GB
P2P traffic	30GB
Total other/unattributed/unclassified anomalies	70GB
Percentage of TOTAL consumption for the period	51.75%

ESPHION

Esphion Life-Cycle Services



ESPHION

THANK YOU

ESPHION

ESPHION