Botnet Communications and Detection

- Presented by HKCERT – 27-August-2009

What is bot ?

- Alias : Zombie , Drone
- Autonomously and automatically runs on a compromised computer
- Performing task without owner's consent
- Widely propagated and coordinated group of bots to form a network **"Botnet "**

Botmaster/Bot Herder

- A person/group who control the botnet
- via Command & Control (C&C) channel, Centralized or Decentralized
- keep himself anonymous
- Professionally written, with update and patch
- Profit-driven

Use of Botnets

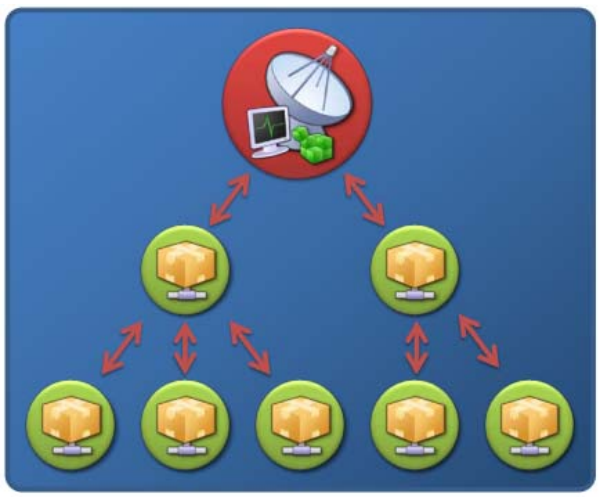
- Service (CasS - Crimeware as a service)
- Performing:
  - Information theft
  - DDoS attack
  - Spam
  - Click fraud
  - Phishing
  - Distribute other malwares

Infection channel

- Email
- Instant Messenger
- Social network
- Drive by download (exploit vulnerability)
  - Malicious site
  - Legitimate website but injected with malicious code
- P2P file sharing

CommunicationTopology

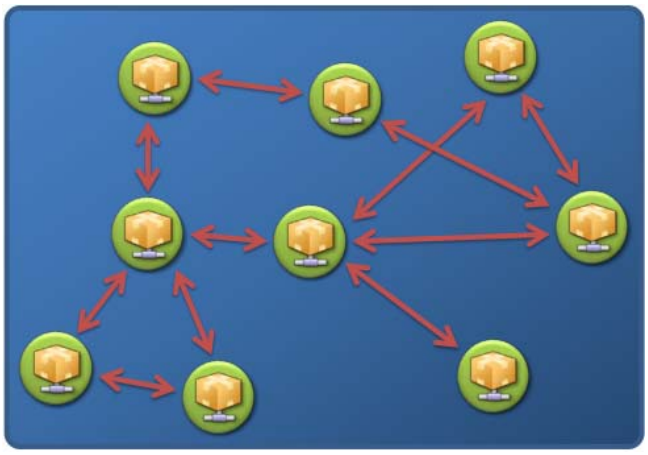
- Centralized
  - Star
  - Multi-server
  - Hierarichial



[image source from damballa.com]

CommunicationTopology

- Decentralized
  - Random



[image source from damballa.com]

Communication Channels

- Internet Relay Chat (IRC)
  - IRCBot
- HTTP/HTTPS
  - Zeus, MPack, FirePack
- Peer to Peer (P2P)
  - Storm, Torpig
- Hybrid
  - Conficker

IRC

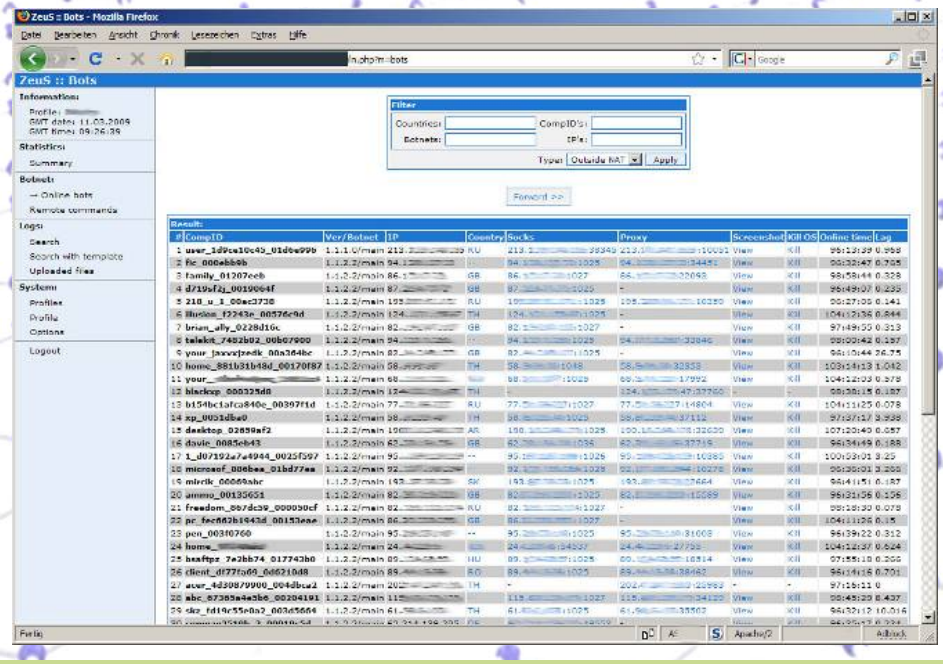
- Port 6667 or custom port

- join hardcoded channel
- send command/instruction via joined channel (PUSH)

HTTP/HTTPS

- Port 80, 443
- Php based system
- Post request (PULL)
- Snd.php (register the botnet)
- Update.php (update the binary file)
- Stat.php (get the command)

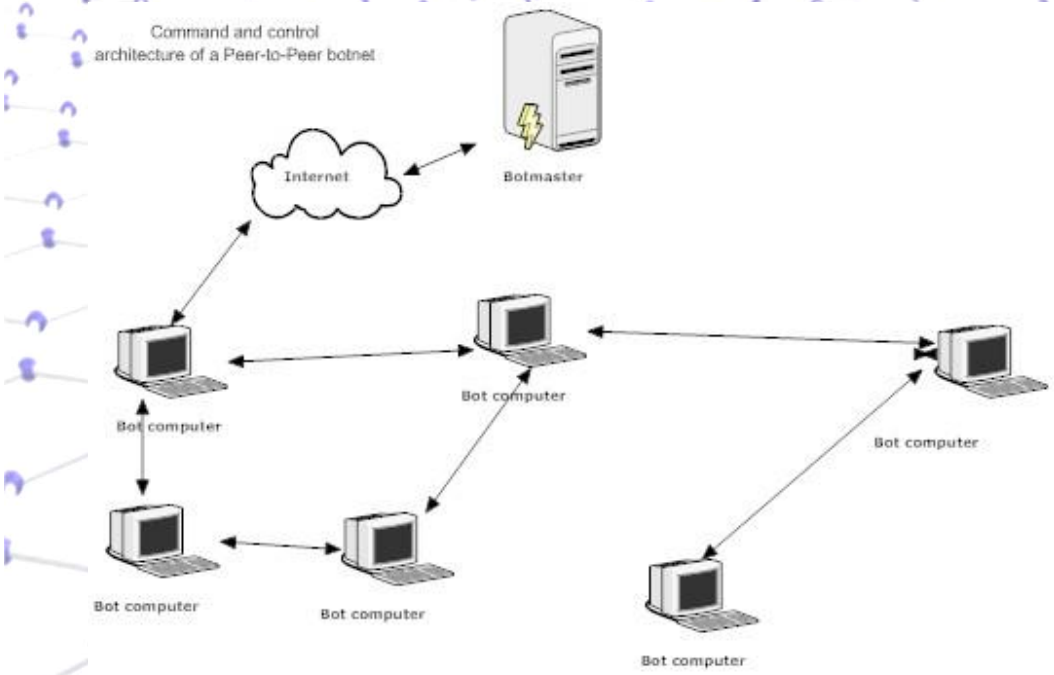
HTTP/HTTPS



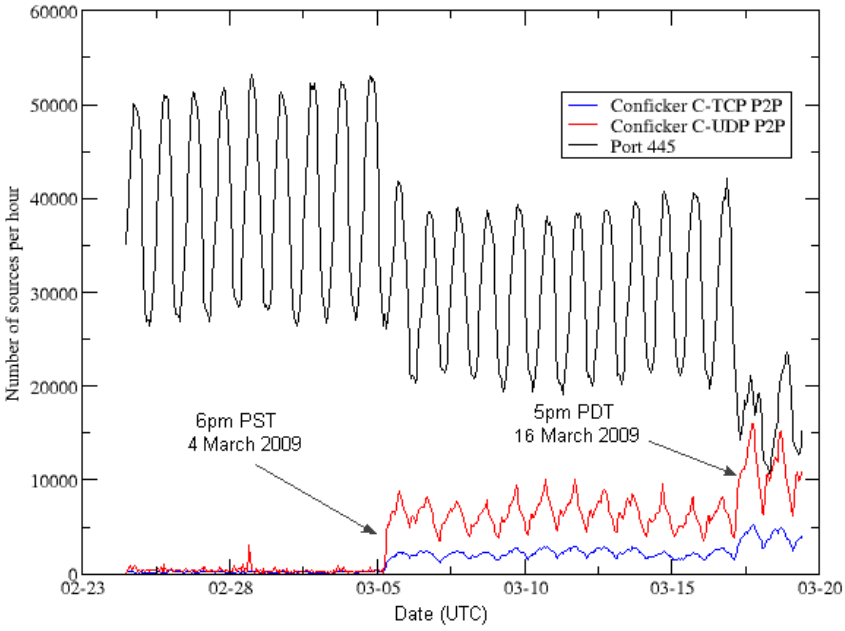
P2P

- UDP
- No fixed port
- Supernode (locate where the C&C server)
- Highly resilient
- Authentication

P2P



P2P



[Image source from SRI]

Demo 1

Botnet Detection

- Antivirus
  - Based on signature
- Firewall
  - Based on defined policy
- IDS/IPS
  - Based on signature and defined policy

Challenges for Botnet Detection

- Dynamic
- Use legitimate communication protocol
  - HTTP/HTTPS
- Inject to General Application Process
- Stealthy
- Multiple communication channel

Any Solution?

Bot Hunter

- A passive network monitoring tool designed to recognize the communication patterns of malware-infected computers within your network perimeter.
- Created by SRI International in 2007
- Freeware, Latest version 1.0.4a
- Supported Windows, Mac, and Linux driven systems.

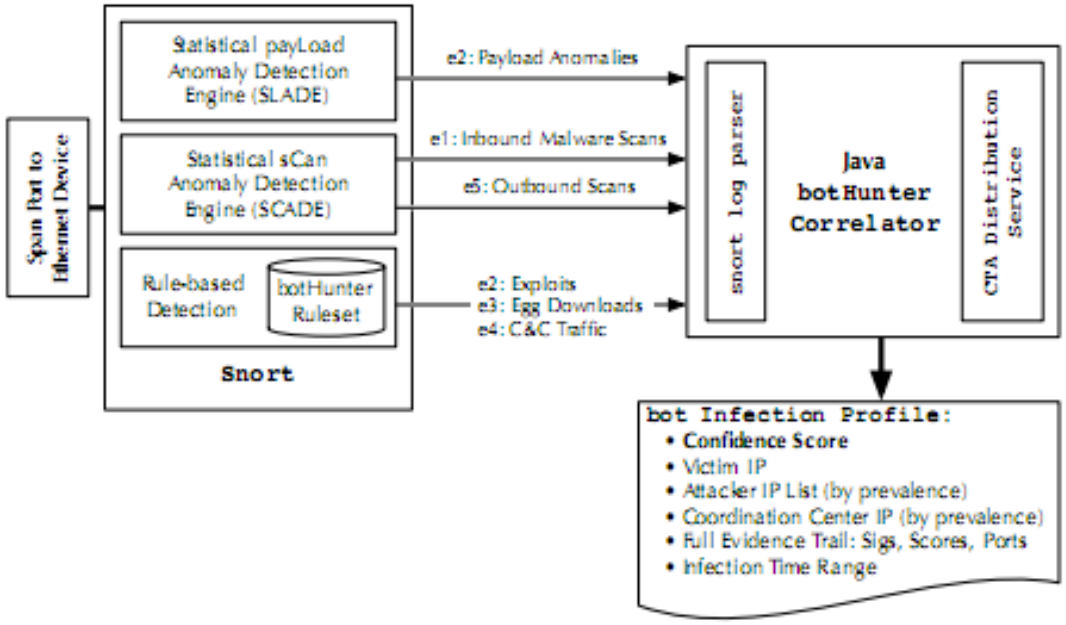
Goal

- Track the two-way communication flows between internal assets and external entities, developing an evidence trail of data exchanges that match a state-based infection sequence model.
- help stimulate research in understanding the life cycle of malware infections.

Structure

- Custom Snort IDS engine
- SLADE – incoming traffic flow
- SCADE – malware focused port scan
- Black List Server
- Dialog correlation engine

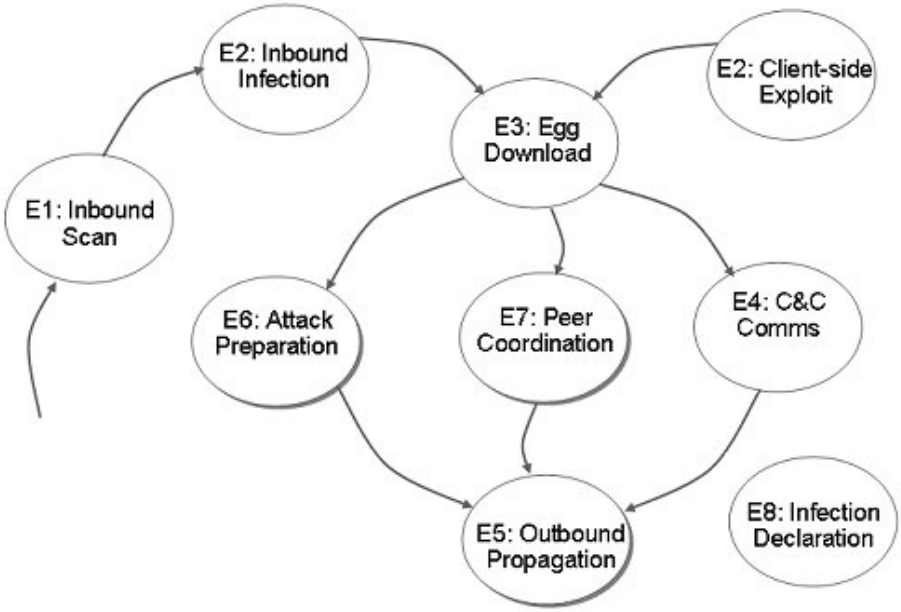
Structure



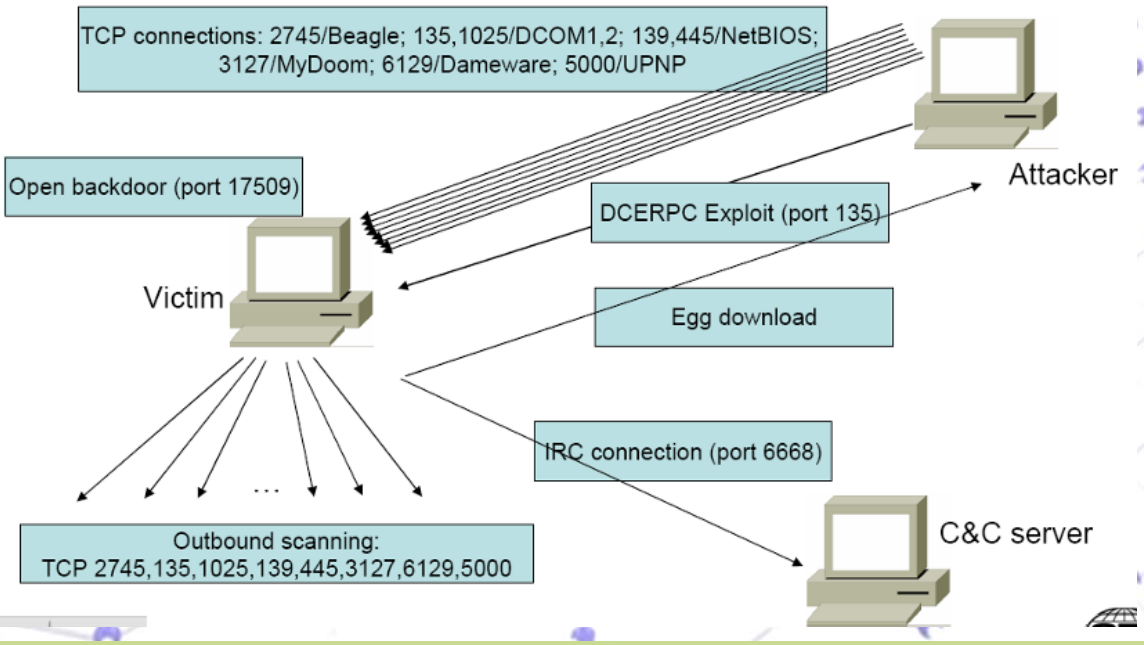
Botnet Model

- Models an infection sequence
- Infection I = <A, V, E, C, P, V', {D}>
- A = attacker
- V = victim
- E = egg download location, (ie Malware binary file)
- C = C&C server
- P = peer to peer coordination points
- V' = the victim's next propagation targets.
- {D} represents a set of dialog sequences composed of bidirectional flows that cross the egress boundary.

Botnet infection life cycle



Botnet infection life cycle



Diaglog Classification

- E1 - Inbound malware port focused scans
- E2 - In and Outbound Exploit Detection
- E3 - Forced Download / Illegal Software Install Detection:
- E4 - C&C Detection
- E5/E6 - Insider Attack / Malware Preparation Activity
- E7 - Peer to Peer Rules
- E8 - Malware Infection Declaration Rules

Dialog Correlation

- Track sequence of IDS dialog warnings between local host and those external entities involved.
- Weight table

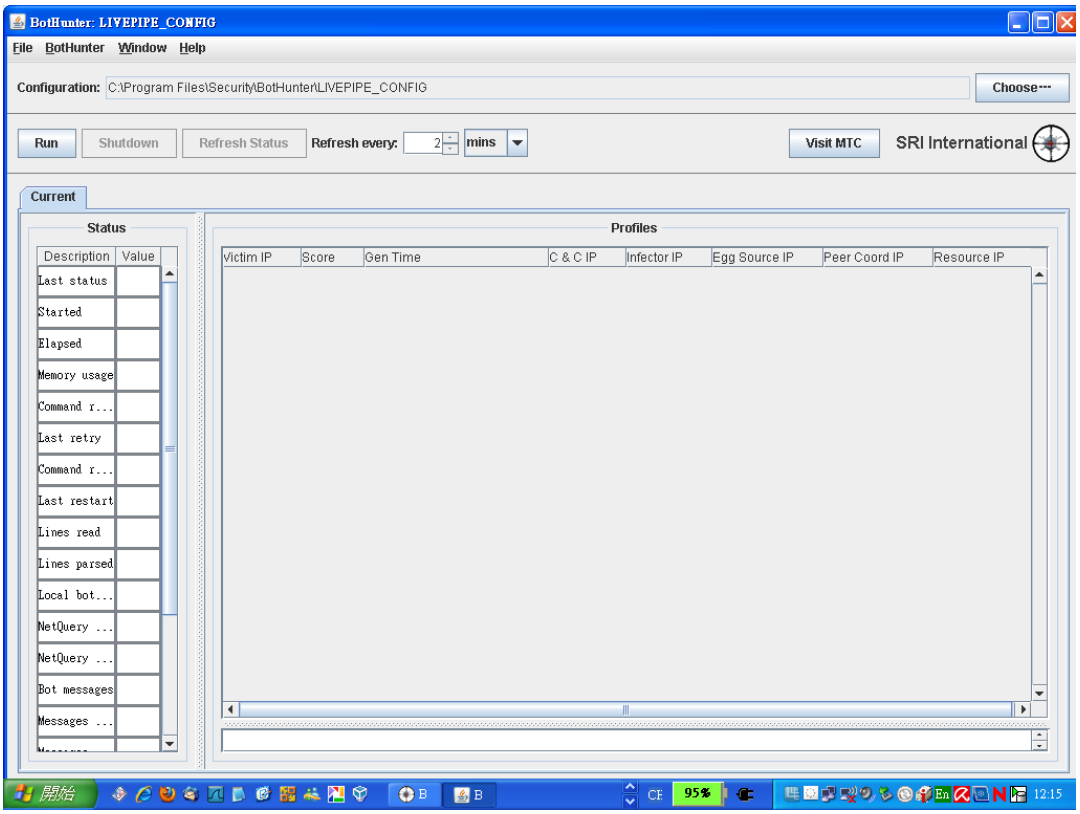
	Coefficients	Standard Error
E1	0.09375	0.100518632
E2 rulebase	0.28125	0.075984943
E2 slade	0.09375	0.075984943
E3	0.34375	0.075984943
E4	0.34375	0.075984943
E5	0.34375	0.075984943

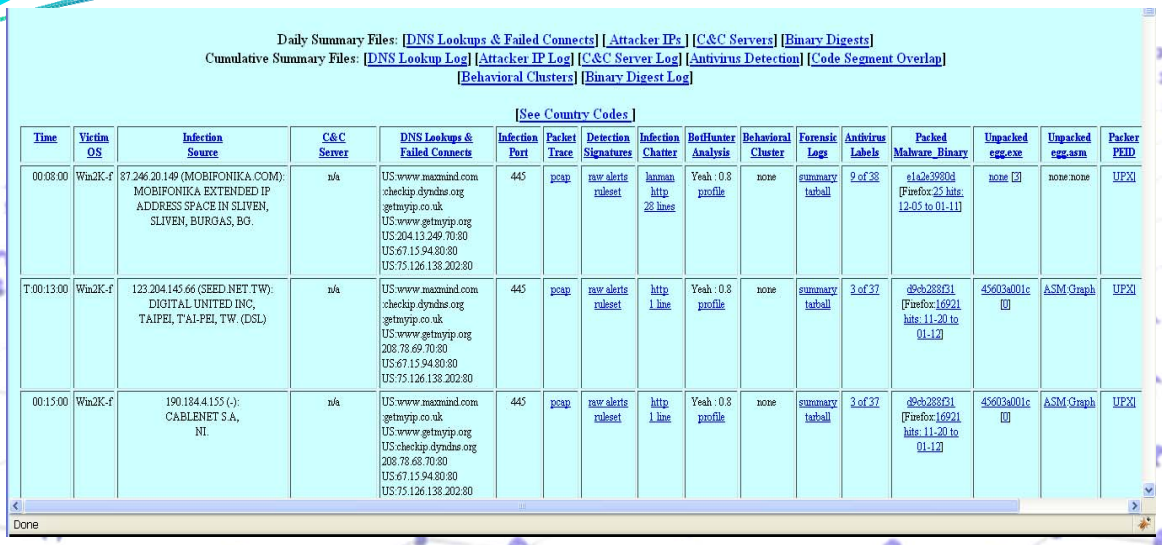
- Infection sequence score

Dialog Correlation

- Network dialog correlation matrix

Int. Host	Timer	E1 ◷	E2	E3	E4	E5
192.168.12.1	◷	$A_a \ldots A_b$				
192.168.10.45	◔		$A_c \ldots A_d$		$A_e \ldots A_f$	
192.168.10.66	◔		A_g			
192.168.12.46	◔				$A_h \ldots A_i$	$A_j \ldots A_k$
:						
192.168.11.123	◷ ◔	A_l	$A_m \ldots A_n$	A_o		





Daily Summary Files: [DNS Lookups & Failed Connects] [Attacker IPs] [C&C Servers] [Binary Digests]
Cumulative Summary Files: [DNS Lookup Log] [Attacker IP Log] [C&C Server Log] [Antivirus Detection] [Code Segment Overlap]
[Behavioral Clusters] [Binary Digest Log]

[See Country Codes]

Time	Victim OS	Infection Source	C&C Server	DNS Lookups & Failed Connects	Infection Port	Packet Trace	Detection Signatures	Infection Chatter	BotHunter Analysis	Behavioral Cluster	Forensic Logs	Antivirus Labels	Packed Malware_Binary	Unpacked egg.exe	Unpacked egg.asm	Packer PEID
00:08:00	Win2K-f	87.246.20.149 (MOBIFONIKA.COM): MOBIFONIKA EXTENDED IP ADDRESS SPACE IN SLIVEN, SLIVEN, BURGAS, BG.	n/a	US:www.maxmind.com :checkip.dyndns.org :getmyip.co.uk US:www.getmyip.org US:204.13.249.70:80 US:67.15.94.80:80 US:75.126.138.202:80	445	pcap	raw alerts ruleset	lanman http 28 lines	Yeah : 0.8 profile	none	summary tarball	9 of 38	e1a2e3980d [Firefox:25 hits: 12-05 to 01-11]	none [3]	none:none	UPXI
T:00:13:00	Win2K-f	123.204.145.66 (SEED.NET.TW): DIGITAL UNITED INC, TAIPEI, T'AI-PEI, TW. (DSL)	n/a	US:www.maxmind.com :checkip.dyndns.org :getmyip.co.uk US:www.getmyip.org 208.78.69.70:80 US:67.15.94.80:80 US:75.126.138.202:80	445	pcap	raw alerts ruleset	http 1 line	Yeah : 0.8 profile	none	summary tarball	3 of 37	d9cb288f31 [Firefox:16921 hits: 11-20 to 01-12]	45603a001c [0]	ASM:Graph	UPXI
00:15:00	Win2K-f	190.184.4.155 (-): CABLENET S.A, NI.	n/a	US:www.maxmind.com :getmyip.co.uk US:www.getmyip.org US:checkip.dyndns.org 208.78.68.70:80 US:67.15.94.80:80 US:75.126.138.202:80	445	pcap	raw alerts ruleset	http 1 line	Yeah : 0.8 profile	none	summary tarball	3 of 37	d9cb288f31 [Firefox:16921 hits: 11-20 to 01-12]	45603a001c [0]	ASM:Graph	UPXI

Done

Source: http://www.cyber-ta.org/releases/malware-analysis/public/

Demo 2

Q & A

- **Thank You**