

# Botnet Communications and Detection

- Presented by HKCERT – 27-August-2009

HK Clean PC Day 2009 . Fighting against Botnet

## 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 “**



HK Clean PC Day 2009 . Fighting against 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



HK Clean PC Day 2009 . Fighting against Botnet

# Use of Botnets

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

HK Clean PC Day 2009 . Fighting against Botnet

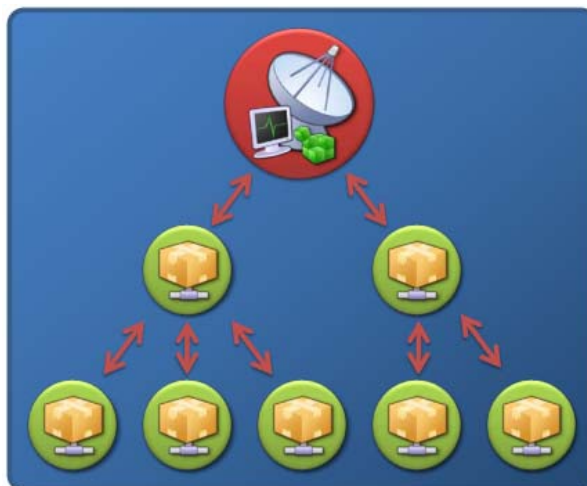
# Infection channel

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

HK Clean PC Day 2009 . Fighting against Botnet

# Communication Topology

- Centralized
  - Star
  - Multi-server
  - Hierarchical

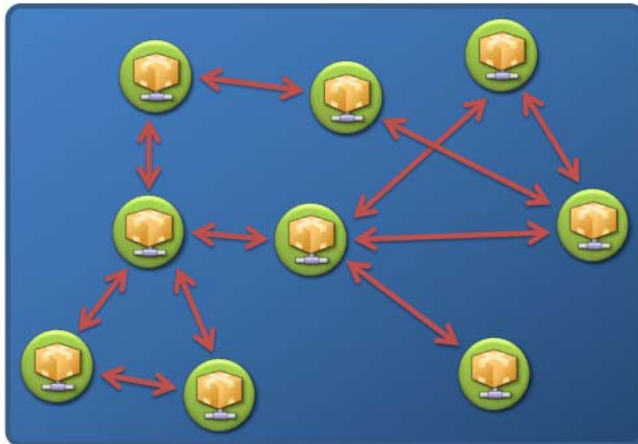


[image source from damballa.com]

HK Clean PC Day 2009 . Fighting against Botnet

# Communication Topology

- Decentralized
  - Random



[image source from damballa.com]

HK Clean PC Day 2009 . Fighting against Botnet

# Communication Channels

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

HK Clean PC Day 2009 . Fighting against Botnet

# IRC

- Port 6667 or custom port

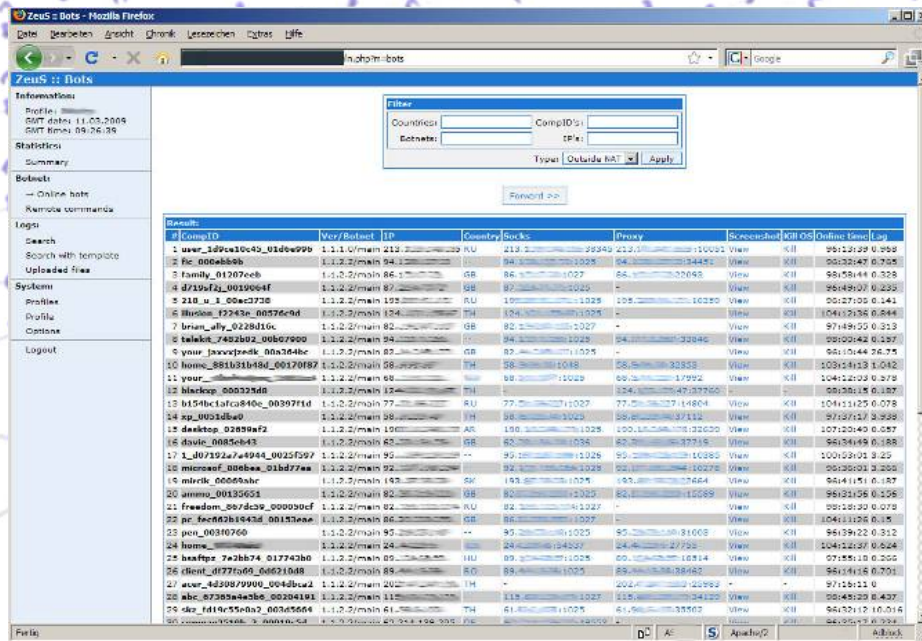
```
-----tCl--'
Configuration File: psybnc.conf
Language File: psyBNC Language File - English
No logfile specified, logging to log/psybnc.log
Listening on: 0.0.0.0 port 31337
psyBNC2.3.2-4-cBtITLdDMSNp started (PID 29855)
```

- 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



The screenshot shows the Zeus Bot Manager interface in Mozilla Firefox. The main window displays a list of botnet members with columns for CompID, Ver/Botnet, IP, Country, Socks, Proxy, Screenshot, Kill OS, and Online Time. A filter dialog is open, allowing users to search by Country, CompID, and IP. The table lists various bots with their respective IDs and IP addresses.

CompID	Ver/Botnet	IP	Country	Socks	Proxy	Screenshot	Kill OS	Online Time
1 user_1d9c10c40_01d0w999	1.1.2.0/main	213.213.213.213	KU	213.213.213.213	213.213.213.213	View	Kill	00:01:29 0.298
2 fc_000abb0b	1.1.2.0/main	94.104.104.104	GB	94.104.104.104	94.104.104.104	View	Kill	00:02:47 0.705
3 family_01207ecb	1.1.2.0/main	86.104.104.104	GB	86.104.104.104	86.104.104.104	View	Kill	00:05:44 0.328
4 82197d_0019064f	1.1.2.0/main	87.104.104.104	GB	87.104.104.104	87.104.104.104	View	Kill	00:06:00 0.235
5 210_u_00ac3730	1.1.2.0/main	193.104.104.104	KU	193.104.104.104	193.104.104.104	View	Kill	00:07:05 0.441
6 Husion_12243e_00576c0d	1.1.2.0/main	124.104.104.104	TH	124.104.104.104	124.104.104.104	View	Kill	00:07:56 0.644
7 briam_wly_0228d10c	1.1.2.0/main	82.104.104.104	GB	82.104.104.104	82.104.104.104	View	Kill	00:08:50 0.313
8 teiska_7402b02_00b79900	1.1.2.0/main	94.104.104.104	GB	94.104.104.104	94.104.104.104	View	Kill	00:09:42 0.197
9 your_javajspok_00c264be	1.1.2.0/main	87.104.104.104	GB	87.104.104.104	87.104.104.104	View	Kill	00:10:44 0.715
10 home_88121b1494_00120f87	1.1.2.0/main	193.104.104.104	TH	193.104.104.104	193.104.104.104	View	Kill	00:11:13 1.012
11 your_000323d8	1.1.2.0/main	68.104.104.104	US	68.104.104.104	68.104.104.104	View	Kill	00:12:03 0.378
12 blackop_000323d8	1.1.2.0/main	124.104.104.104	TH	124.104.104.104	124.104.104.104	View	Kill	00:12:15 0.187
13 b154bca840c_00397f1d	1.1.2.0/main	77.104.104.104	KU	77.104.104.104	77.104.104.104	View	Kill	00:11:25 0.078
14 ay_009385d0	1.1.2.0/main	98.104.104.104	TH	98.104.104.104	98.104.104.104	View	Kill	00:12:52 0.308
15 blackop_02899af2	1.1.2.0/main	193.104.104.104	AS	193.104.104.104	193.104.104.104	View	Kill	00:12:40 0.087
16 dovic_0085eb43	1.1.2.0/main	82.104.104.104	GB	82.104.104.104	82.104.104.104	View	Kill	00:13:49 0.188
17 l_d0192a7a4944_0025f097	1.1.2.0/main	92.104.104.104	--	92.104.104.104	92.104.104.104	View	Kill	00:13:01 0.320
18 microsoft_0085ea_01bd77ea	1.1.2.0/main	92.104.104.104	GB	92.104.104.104	92.104.104.104	View	Kill	00:13:01 0.200
19 miric_000606be	1.1.2.0/main	193.104.104.104	GB	193.104.104.104	193.104.104.104	View	Kill	00:14:11 0.187
20 home_00135651	1.1.2.0/main	82.104.104.104	GB	82.104.104.104	82.104.104.104	View	Kill	00:13:16 0.126
21 freedom_807dc39_000090cf	1.1.2.0/main	82.104.104.104	KU	82.104.104.104	82.104.104.104	View	Kill	00:13:30 0.079
22 pr_fec80b1643d_001530ee	1.1.2.0/main	86.104.104.104	GB	86.104.104.104	86.104.104.104	View	Kill	00:11:26 0.135
23 pen_003f0760	1.1.2.0/main	92.104.104.104	--	92.104.104.104	92.104.104.104	View	Kill	00:13:22 0.312
24 home_000606be	1.1.2.0/main	193.104.104.104	GB	193.104.104.104	193.104.104.104	View	Kill	00:12:59 0.244
25 blackop_7a2bb74_017743b0	1.1.2.0/main	68.104.104.104	HU	68.104.104.104	68.104.104.104	View	Kill	00:14:18 0.200
26 iRent_0f77fa69_00621048	1.1.2.0/main	85.104.104.104	RO	85.104.104.104	85.104.104.104	View	Kill	00:14:16 0.701
27 acer_4d30879900_004db2e2	1.1.2.0/main	202.104.104.104	TH	202.104.104.104	202.104.104.104	View	Kill	00:13:11 0.0
28 abc_873894a388_00204191	1.1.2.0/main	115.104.104.104	TH	115.104.104.104	115.104.104.104	View	Kill	00:05:29 0.437
29 daz_1d107954b2_00265664	1.1.2.0/main	61.104.104.104	TH	61.104.104.104	61.104.104.104	View	Kill	00:12:17 10.214
30 ...	1.1.2.0/main	87.104.104.104	GB	87.104.104.104	87.104.104.104	View	Kill	00:05:43 0.394

HK Clean PC Day 2009 . Fighting against Botnet

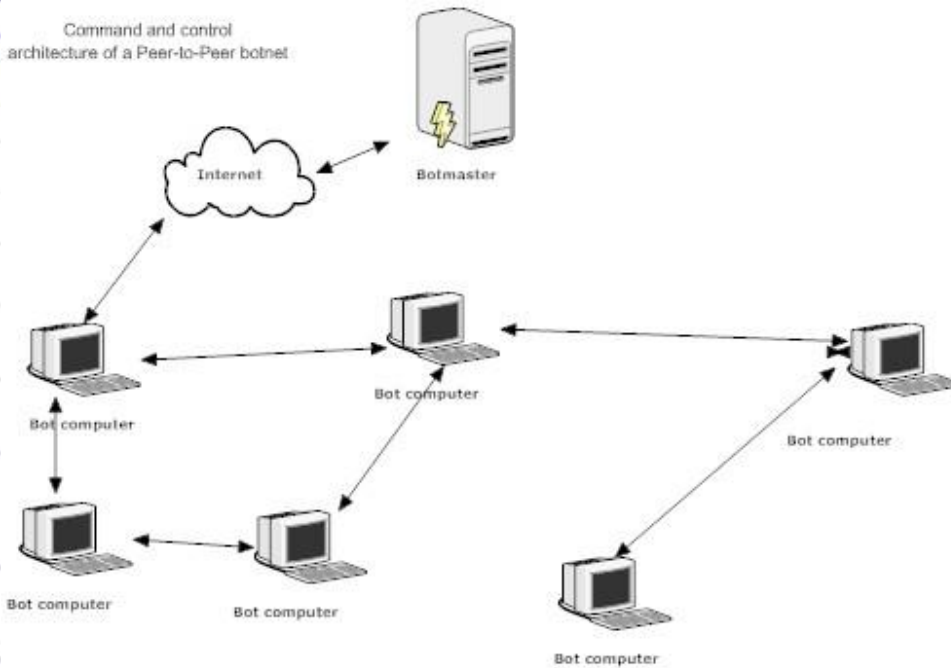
# P2P

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

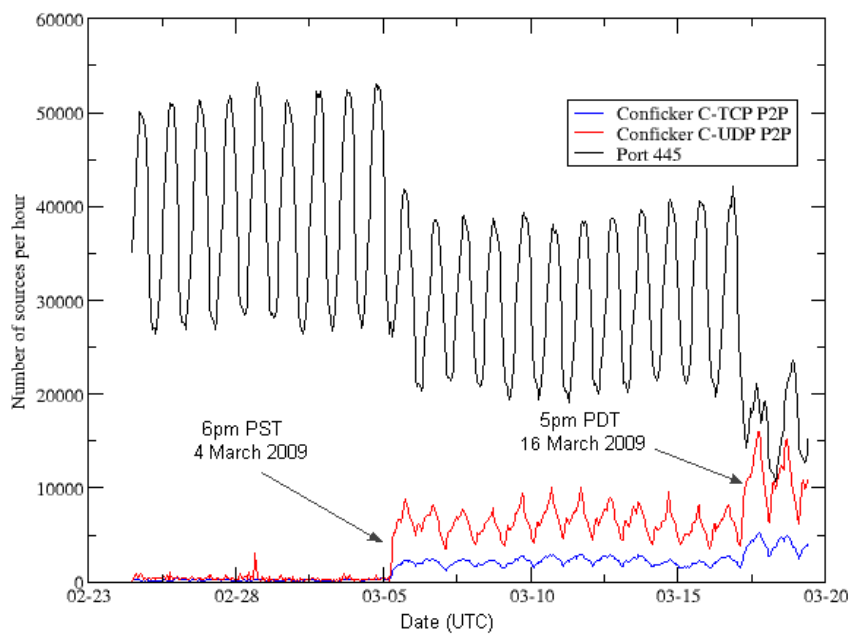
HK Clean PC Day 2009 . Fighting against Botnet

# P2P

Command and control architecture of a Peer-to-Peer botnet



# P2P



[Image source from SRI]

# Demo 1

HK Clean PC Day 2009 . Fighting against Botnet

# Botnet Detection

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

HK Clean PC Day 2009 . Fighting against Botnet



# Challenges for Botnet Detection

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

**Any Solution?**

HK Clean PC Day 2009 . Fighting against Botnet

# 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.

HK Clean PC Day 2009 . Fighting against Botnet

# 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.

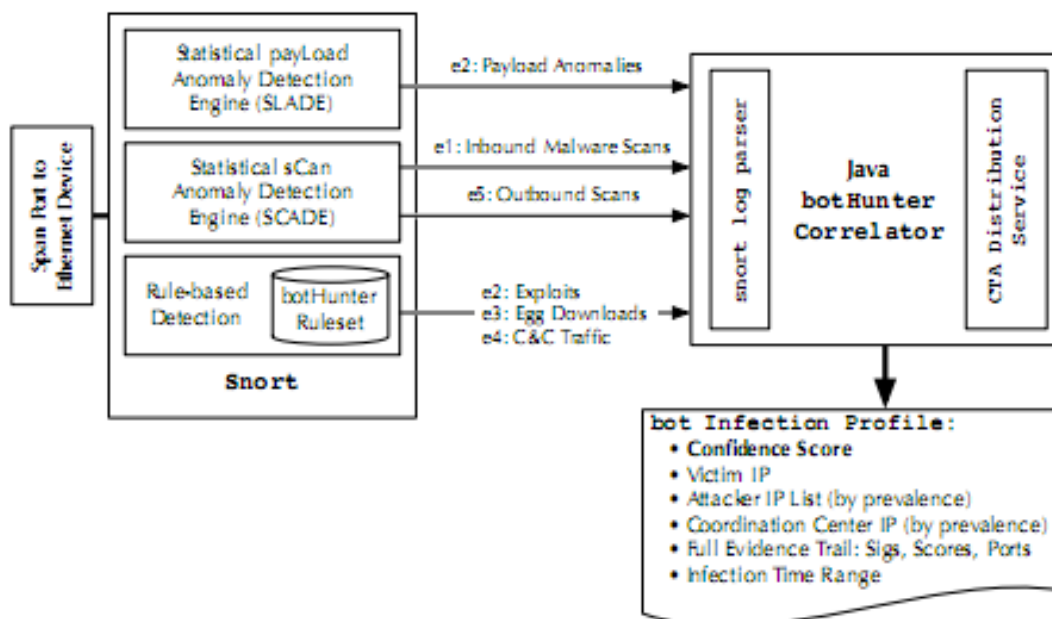
HK Clean PC Day 2009 . Fighting against Botnet

# Structure

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

HK Clean PC Day 2009 . Fighting against Botnet

# Structure



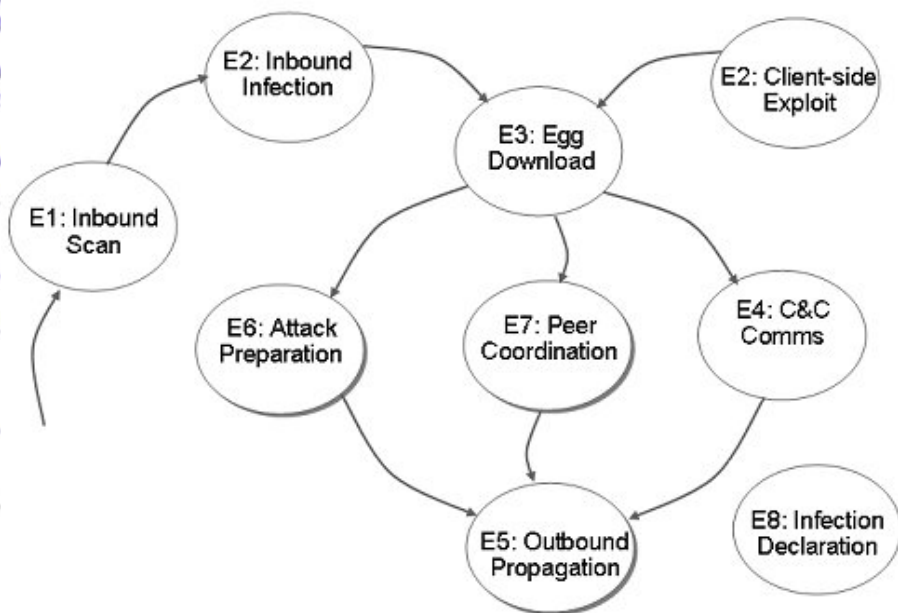
HK Clean PC Day 2009 . Fighting against Botnet

# Botnet Model

- Models an infection sequence
- Infection  $I = \langle A, V, E, C, P, V', \{D\} \rangle$
- 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.

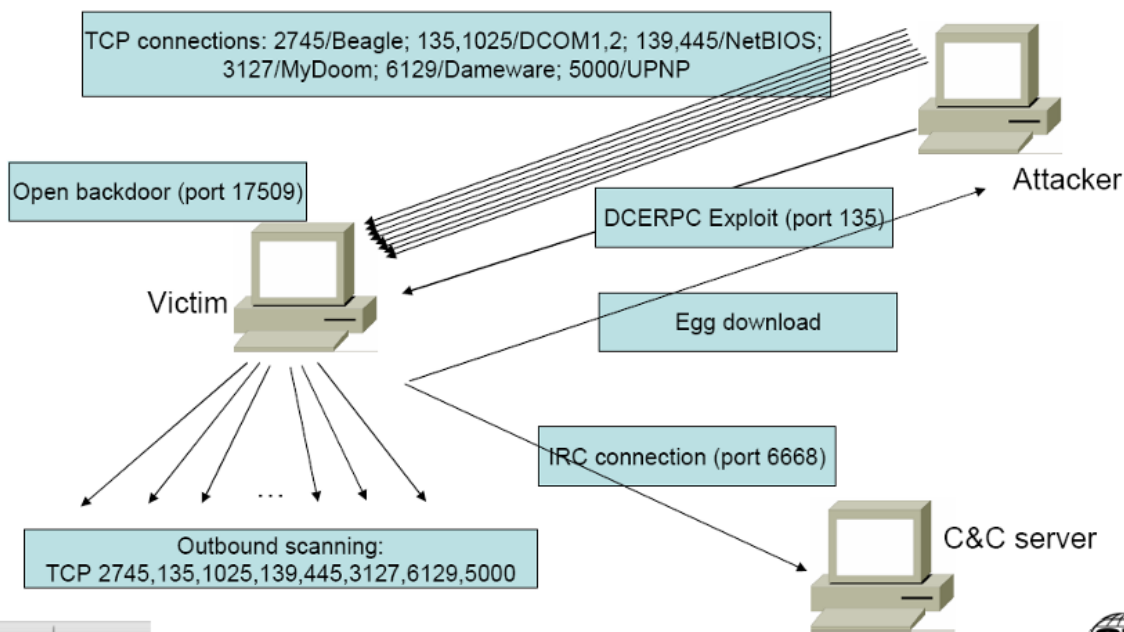
HK Clean PC Day 2009 . Fighting against Botnet

# Botnet infection life cycle



HK Clean PC Day 2009 . Fighting against Botnet

# Botnet infection life cycle



HK Clean PC Day 2009 . Fighting against Botnet

# Dialog 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

HK Clean PC Day 2009 . Fighting against Botnet

# 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

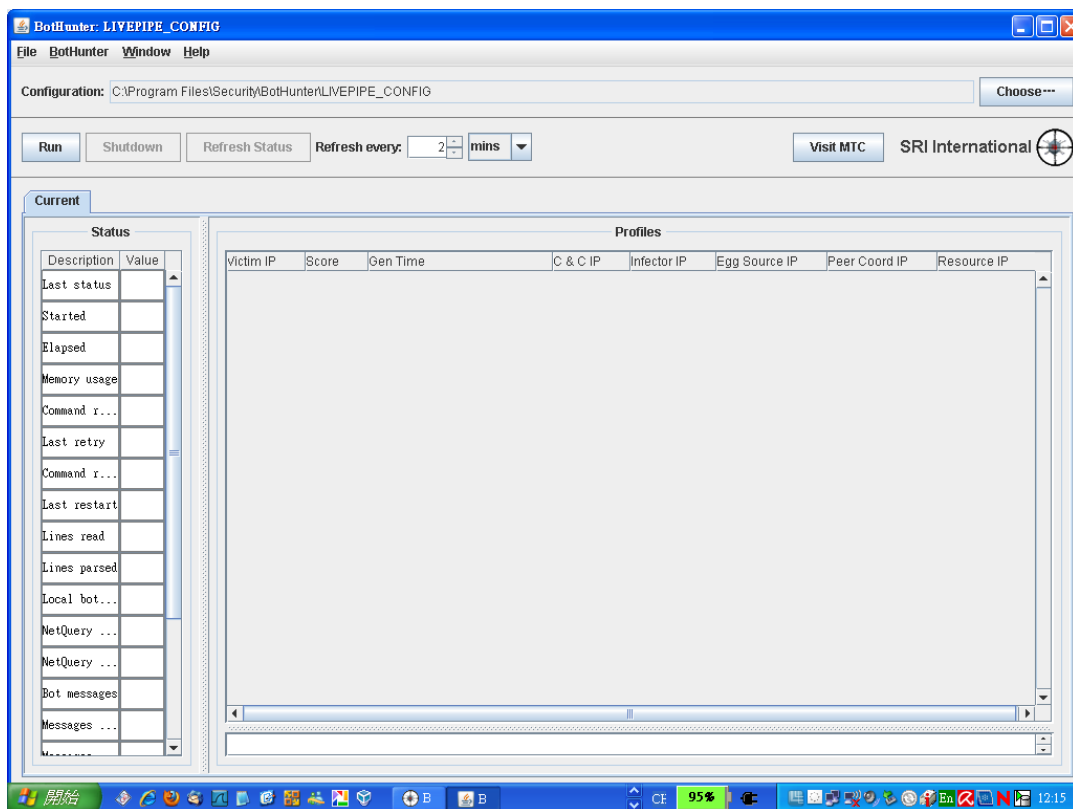
- Infection sequence score

HK Clean PC Day 2009 . Fighting against Botnet

# Dialog Correlation

- Network dialog correlation matrix

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



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	Patch Trace	Detection Signatures	Infection Charter	Bot/Hunter 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	human http 28 lines	Yeah : 0.8 profile	none	summary tabball	2 of 38	e1a2c3990d (Firefox 2.5 hits: 12-05 to 01-11)	none [2]	none none	UEFI
T:00:13:00	Win2K-f	123.204.145.66 (SEED.NET.TW); DIGITAL UNITED INC, TAIPEI, TAI-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 tabball	3 of 37	d8cb288f31 (Firefox 1.6921 hits: 11-20 to 01-12)	45603a001c [3]	ASM-Graph	UEFI
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 tabball	3 of 37	d8cb288f31 (Firefox 1.6921 hits: 11-20 to 01-12)	45603a001c [3]	ASM-Graph	UEFI

Done

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

HK Clean PC Day 2009 . Fighting against Botnet

# Demo 2

HK Clean PC Day 2009 . Fighting against Botnet



# Q & A

● **Thank You**

HK Clean PC Day 2009 . Fighting against Botnet