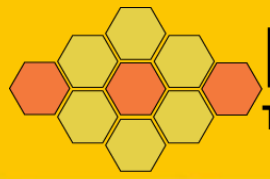


Honeynet Project
Taiwan Chapter

Botnet and Malware behavior analysis

蔡一郎

Google Me.

Taiwan Chapter

- 蔡一郎 Steven
- 學歷：國立成功大學電機工程研究所碩士
- 現任：國家高速網路與計算中心 副工程師
- 重要經歷：
  - 國立成功大學研究發展基金會助理研究員
  - 崑山科技大學兼任講師
  - 台南科學園區產學協會理事
  - Honeynet Project Taiwan Chapter負責人
  - 自由作家
    - 電腦圖書著作33本
    - Information Security(資安人)、Linux Guide、NetAdmin專欄，計60餘篇
- 專業證照：
  - RHCE、CCNA、CCAI、CEH、CHFI、ACIA、ITIL Foundation、ISO 27001 LAC、ISO 20000 LAC

TWHP TaiWan Honeynet Project

The Honeynet PROJECT®

redhat. CERTIFIED ENGINEER

CCNA CISCO CERTIFIED

C|EH™ Certified Ethical Hacker

C|HFI™ Computer Hacking Forensic INVESTIGATOR

ITIL foundation

Outline

- Honeynet and Botnet
- Honeynet Project introduction
- Taiwan Chapter introduction
- What is Honeypot and Honeynet
- Honeynet Project Tools
- TWMAN

Honeynet and Botnet

Taiwan Chapter

- Where can find Malware sample?
  - User、provider、Honeynet…
- What is the behavior about Botnet?
  - Network connection、system modify…
  - Multi Function
  - bots

Honeynet Project introduction

Taiwan Chapter

- Non-profit (501c3) organization with Board of Directors.
- Funded by sponsors
- Global set of diverse skills and experiences.
- Open Source, share all of our research and findings at no cost to the public.
- Deploy networks around the world to be hacked.
- Everything we capture is happening in the wild.
- We have nothing to sell.

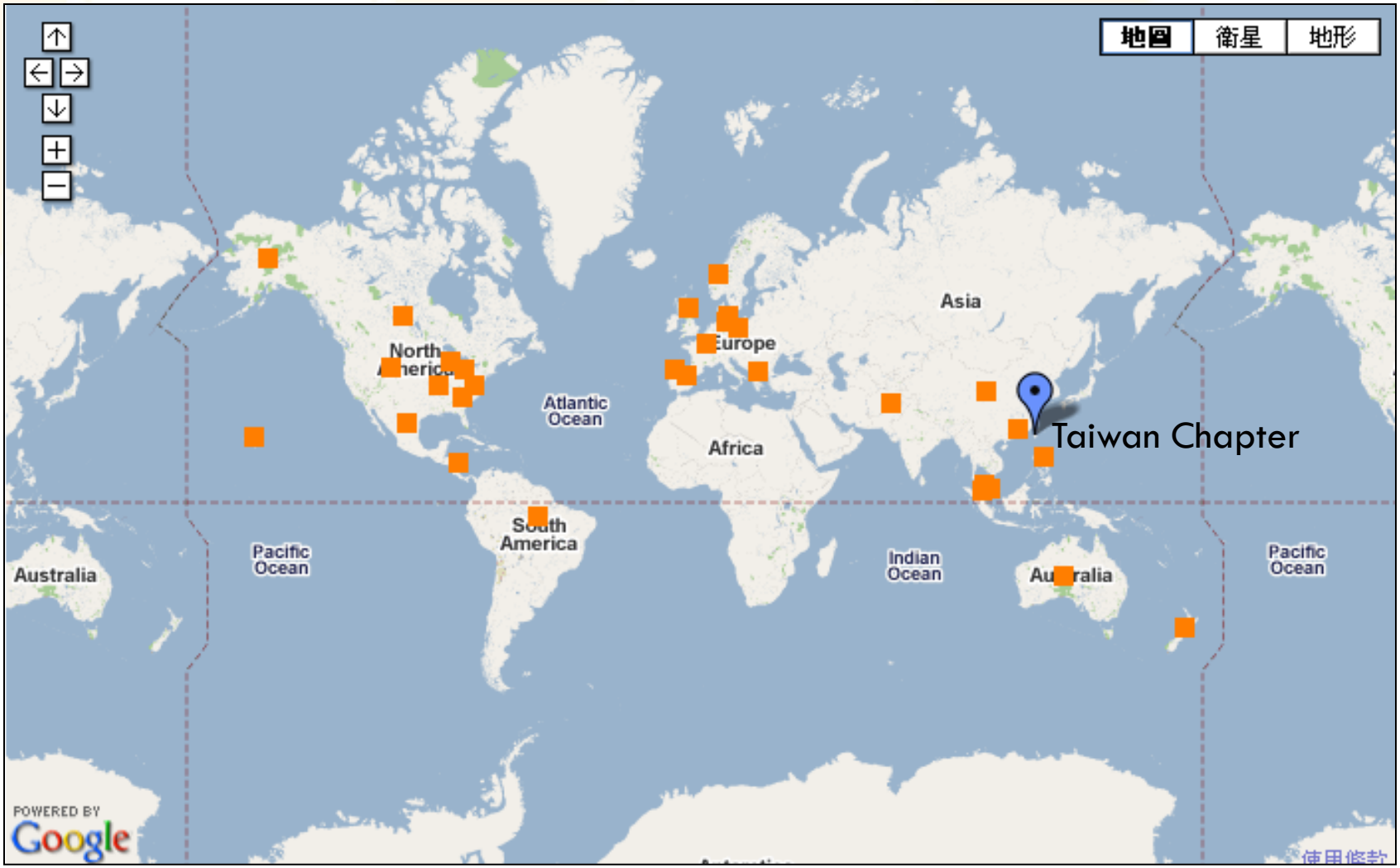
Honeynet Project Mission

Taiwan Chapter

- A community of organizations actively researching, developing and deploying Honeynets and sharing the lessons learned.
  - **Awareness:** 增進企業與組織對存在於現行網路上的威脅與弱點之了解，進一步思考如何去減輕威脅的方法
  - **Information:** 除了提供基本的攻擊活動外，進一步提供更關鍵性的資料，如: 攻擊動機，駭客間如何聯絡，駭客攻破主機後下一步的攻擊動作
  - **Tools:** Honeynet Project 致力於發展 Open Source Tools，藉由這些Tools，我們可以更有效率的佈建誘捕系統了解網路環境攻擊威脅現況

Honeynet Project 全球支會分布

Taiwan Chapter



Honeypot/Honeynet Technology

Taiwan Chapter

- What is a Honeynet ?
  - High-interaction Honeypot
  - It is an architecture, not a product or software
  - Populate with live systems
  - Once compromised, data is collected to learn the tools, tactics, and motives of the Blackhat community
- Value of Honeynet
  - Research : Identify new tools and new tactics, Profiling Blackhats
  - Early warning and prediction
  - Incident Response / Forensics
  - Self-defense

The Threat

- Hundreds of scans a day.
- Fastest time honeypot manually compromised, 15 minutes (worm, under 60 seconds).
- Life expectancies: vulnerable Win32 system is under three hours, vulnerable Linux system is three months.
- Primarily cyber-crime, focus on Win32 systems and their users.
- Attackers can control thousands of systems (Botnets).

Botnets

- Large networks of hacked systems.
- Often thousands, if not tens of thousands, of hacked systems under the control of a single user.
- Automated commands used to control the ‘zombies’.

How They Work

Taiwan Chapter

- After successful exploitation, a bot uses TFTP, FTP, or HTTP to download itself to the compromised host.
- The binary is started, and connects to the hard-coded master IRC server.
- Often a dynamic DNS name is provided rather than a hard coded IP address, so the bot can be easily relocated.
- Using a special crafted nickname like USA|743634 the bot joins the master's channel, sometimes using a password to keep strangers out of the channel

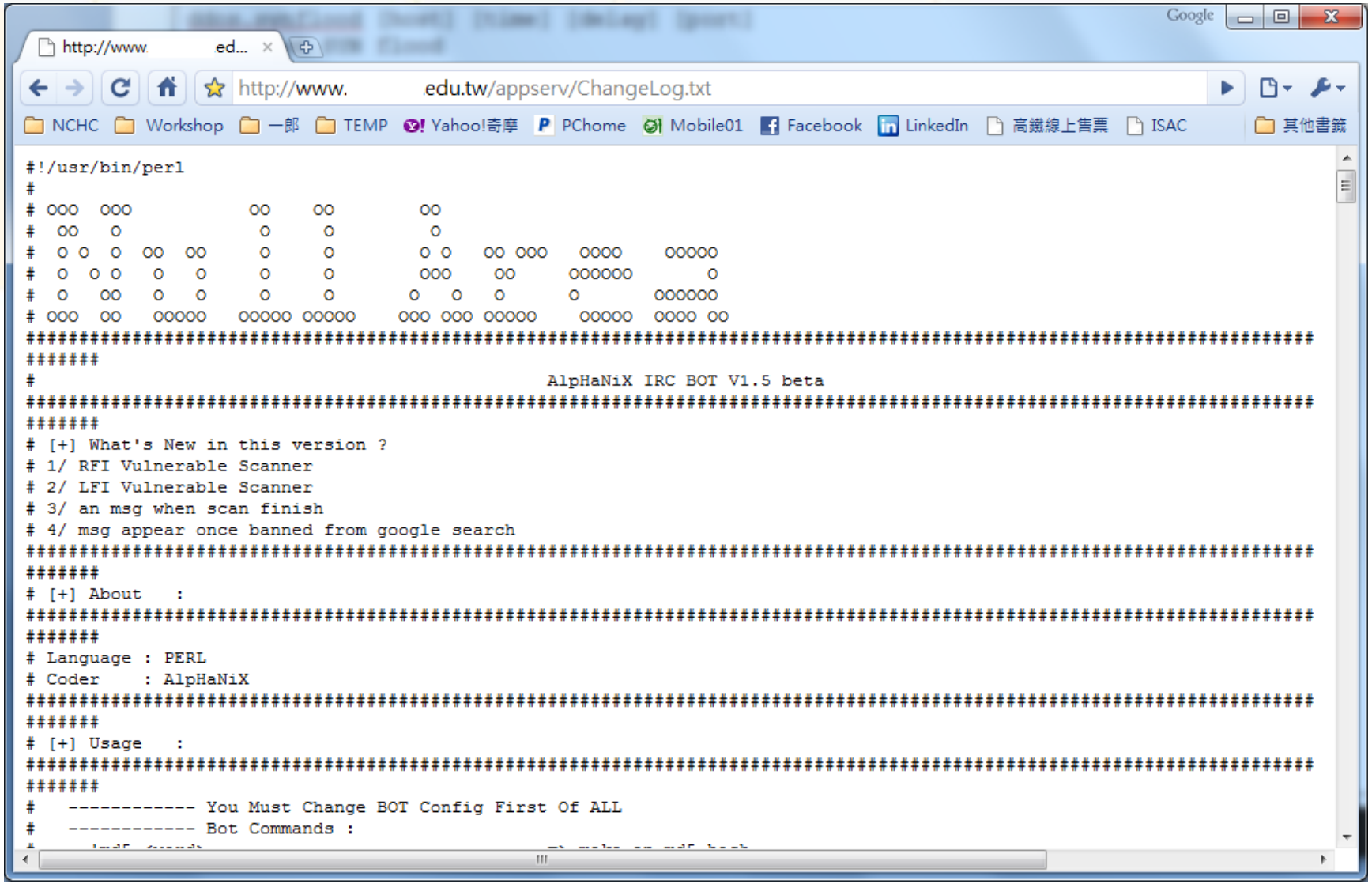
Bots

Taiwan Chapter

```
ddos.synflood [host] [time] [delay] [port]
starts an SYN flood

ddos.httpflood [url] [number] [referrer] [recursive = true||false]
starts a HTTP flood

scan.listnetranges
list scanned netranges

scan.start
starts all enabled scanners

scan.stop
stops all scanners

http.download
download a file via HTTP

http.execute
updates the bot via the given HTTP URL

http.update
executes a file from a given HTTP URL

cvar.set spam_aol_channel [channel]
AOL Spam - Channel name

cvar.set spam_aol_enabled [1/0]
AOL Spam - Enabled?
```

IRC BOT

Taiwan Chapter



Botnet Economy

- Botnets sold or for rent.
- Saw Botnets being stolen from each other.
- Observed harvesting of information from all compromised machines. For example, the operator of the botnet can request a list of CD-keys (e.g. for Windows or games) from all bots. These CD-keys can be sold or used for other purposes since they are considered valuable information.

How it works

A highly controlled network where every packet entering or leaving is monitored, captured, and analyzed.

- Data Control
- Data Capture
- Data Analysis

http://www.honeynet.org/papers/honeynet/

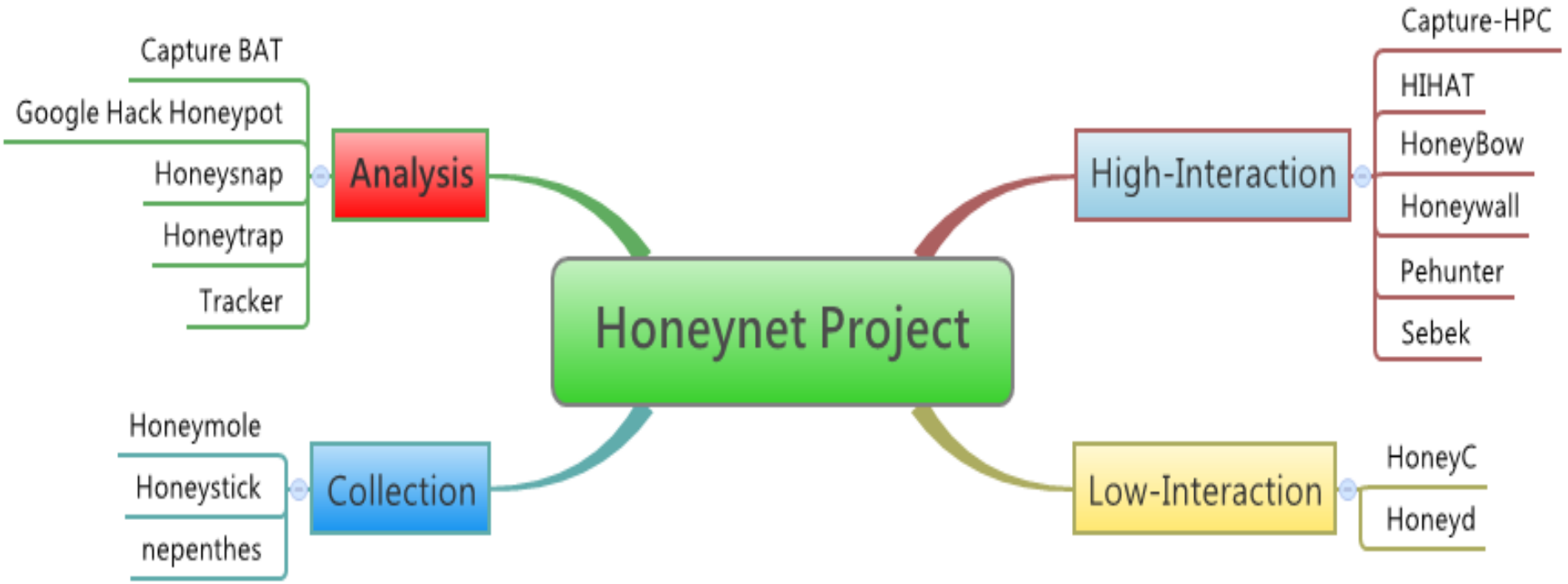
Honeynet Project Tools

Taiwan Chapter

- Capture BAT
- Capture-HPC
- Google Hack Honeypot
- HIHAT(High Interaction Honeypot Analysis Toolkit
- HoneyBow
- HoneyC
- Honeyd
- Honeymole
- Honeysnap
- Honeystick
- Honeytrap
- Honeywall CDROM
- nepenthes
- Pehunter
- Sebek
- Tracker

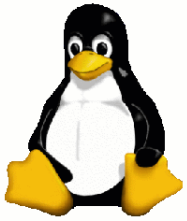
Honeynet Project Tools

Taiwan Chapter



Our Environment

Taiwan Chapter

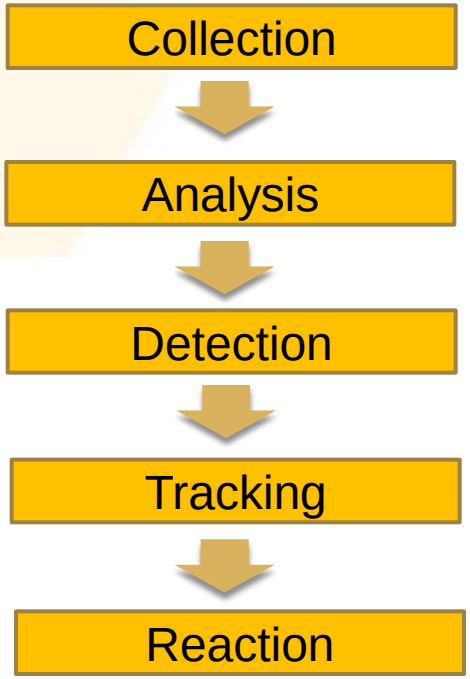


- Virtual Machine Honeynet
  - Advanced Server(128GB Memory)
  - Blade Server(SAS or SSD HDD)
  - VMWare ESX/vSphare
  - 1200+ Servers, Windows XP/Vista, Linux, FreeBSD
  - High Interaction and Low Interaction Honeypots
- Distribution Honeynet/Honeypot
  - Taiwan Education Network
  - Taiwan Chapter members
  - GDH Project

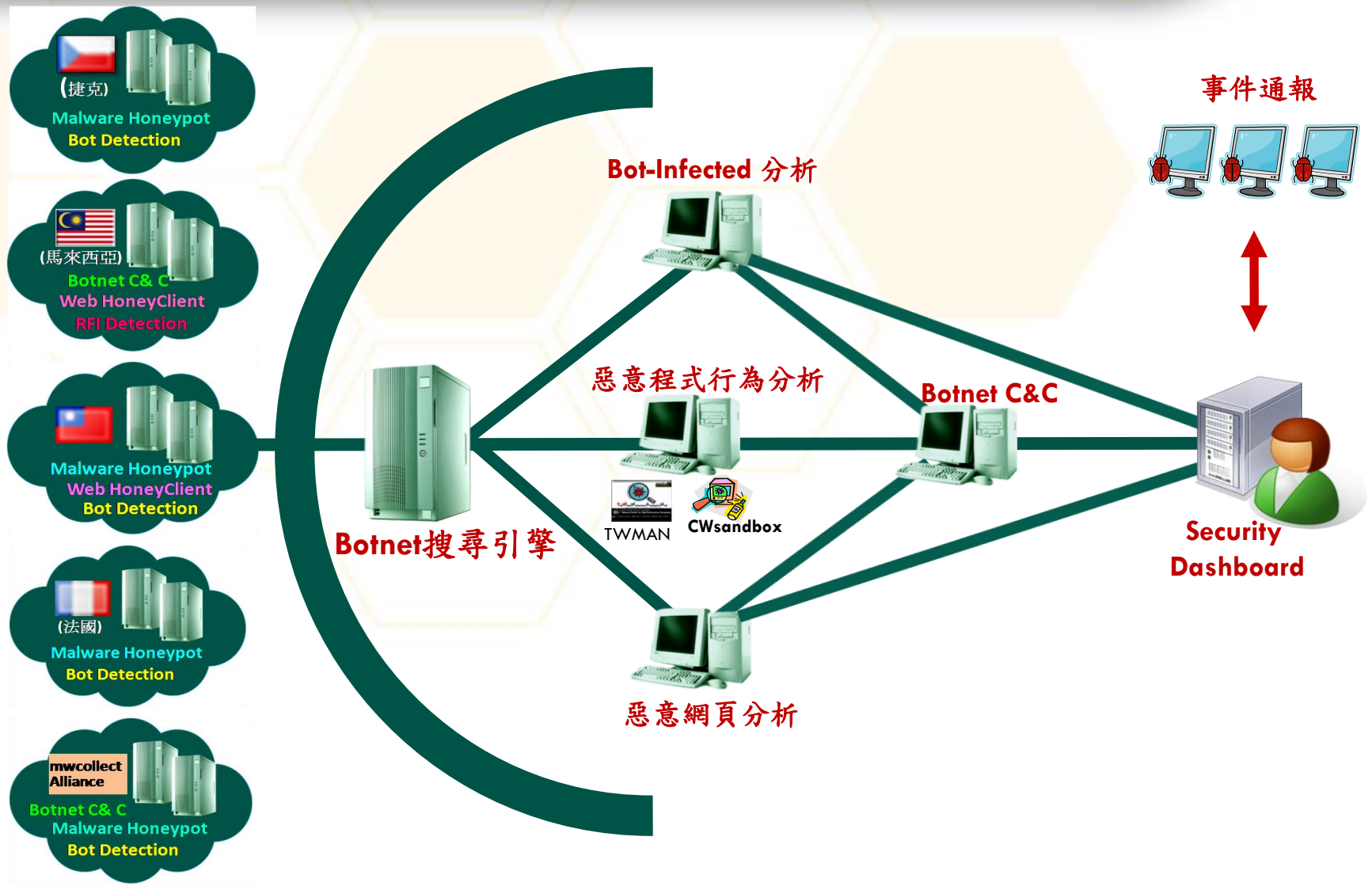
Research Project & Achievements

Taiwan Chapter

- Large-Scale VM-based Honeynet Deployment
- Malware Collection and Analysis
- Honey-Driven Botnet Detection
- Client-Side Attack
  - Malicious Web Server Exploring
  - RFI Scripts Detection
- Fast-Flux Domain Service Tracking
- Research Alliance
  - Distributed Search and Analysis on Honeynet Data



Botnet Detection

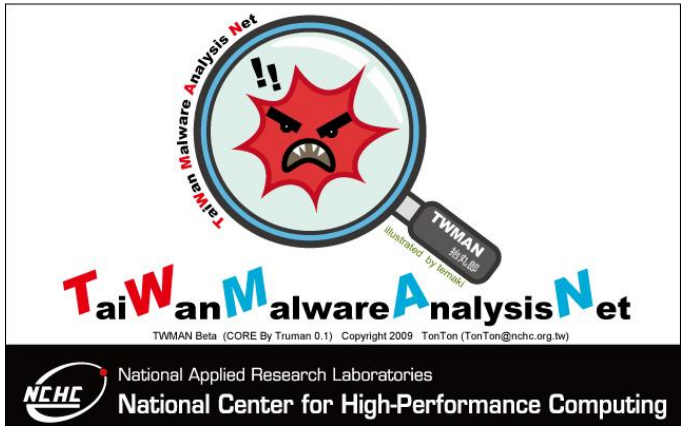


Botnet analysis in global

Taiwan Chapter

Why is TWMAN

- TaiWan Malware Analysis Net
- Open Source malware analysis Net
- Project
  - http://twman.sourceforge.net/
  - http://twman.openfoundry.org/
- Behavior analysis
- Multi-Platform(OS)



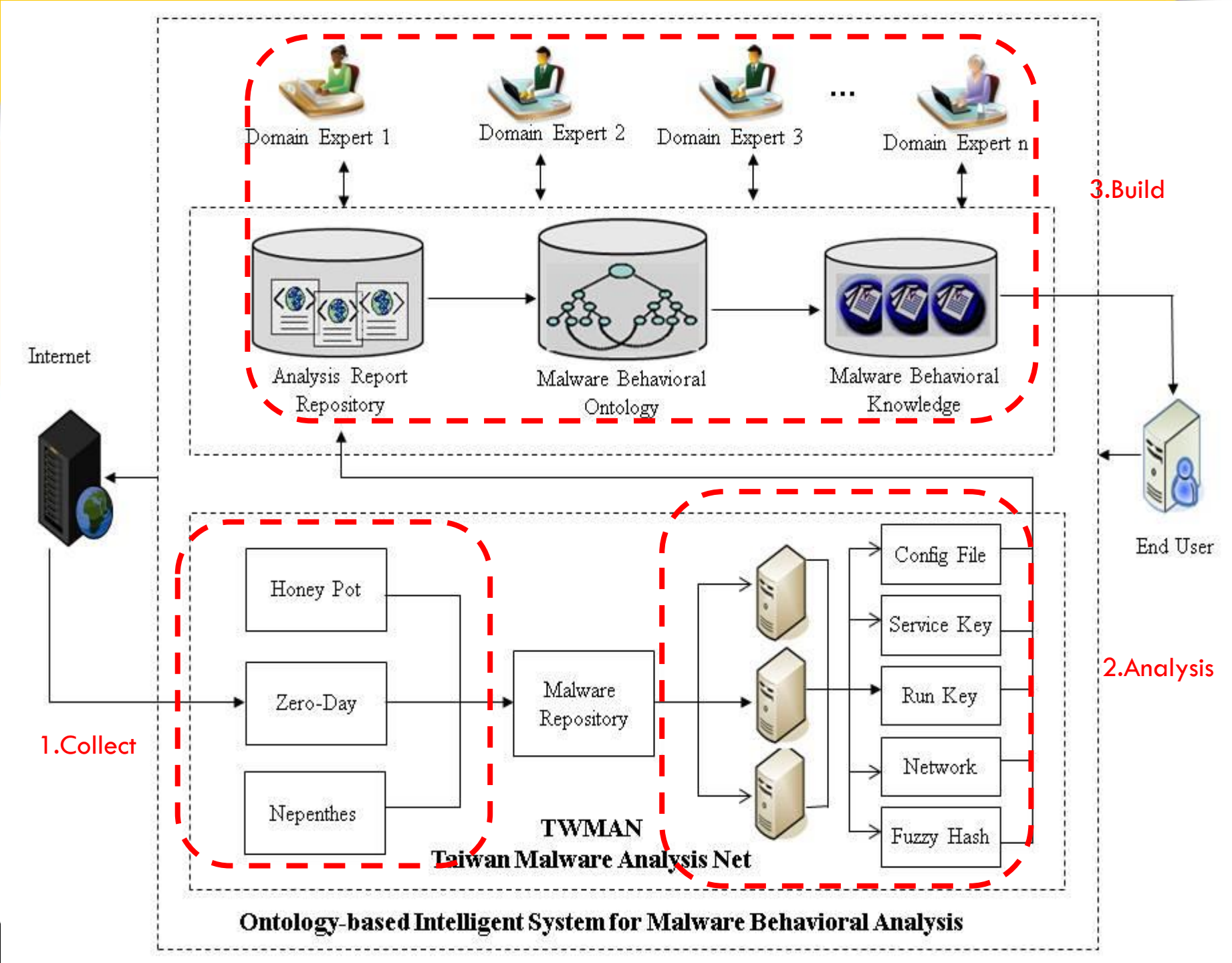
Taiwan Malware Analysis Net (TWMAN)

Taiwan Chapter

- Two composed：
  - Malware behavioral analysis agent
  - Ontology agent
- Collects the malware behavioral information to build：
  - malware behavioral ontology
  - malware behavioral rules.
- Malware behavioral ontology, which is store in an ontology repository.
- TWMAN will protect the computers from the attack of malware, computer viruses and Trojans etc...

TWMAN

- Development
  - Truman, The Reusable Unknown Malware Analysis Net
  - NCHC Clonezilla
  - INetSim, Internet Services Simulation Suite
- Co-operation
  - Honeynet
    - Nepenthes
    - Dionaea
  - Search engine
    - Splunk
  - Virus Scanner
    - Virus Total


Domain Expert 1
Domain Expert 2
Domain Expert 3
...
Domain Expert n
3.Build
Analysis Report Repository
Malware Behavioral Ontology
Malware Behavioral Knowledge
Internet
End User
Honey Pot
Zero-Day
Nepenthes
Malware Repository
Config File
Service Key
Run Key
Network
Fuzzy Hash
2.Analysis
1.Collect
TWMAN
Taiwan Malware Analysis Net
Ontology-based Intelligent System for Malware Behavioral Analysis

Taiwan Malware Analysis Net, TWMAN - Analysis Report
臺灣惡意程式分析網，抬丸郎 - 分析報告 Last Update : 2010-06-20
http://twman.sourceforge.net
>> Summary report for 81ae20781a0fb227ad17952aec5c4493 created at Tue Apr 20 19:02:44 CST 2010 <<

1.MD5 Info

>> Host file changes - Host File 被修改處 <<
>> Registry Run Key changes - Registry Run Key 被修改處 <<
>> Registry Service Key changes - Registry Service Key 被修改處 <<
-WZCSVC|Wireless Zero Configuration|%SystemRoot%\System32\svchost.exe -k netsvcs|Share_Process|Auto Start|TDI
+{33F3B709-064F-4FF7-95BD-434D50D67CCC}|||

2.Config File Change

>> 網路連線記錄 <<
IP 192.168.0.110.57982 > 168.95.1.1.53: UDP, length 34
IP 168.95.1.1.53 > 192.168.0.110.57982: UDP, length 473
IP 192.168.0.110.123 > 207.46.197.32.123: UDP, length 48
IP 192.168.0.110.123 > 207.46.197.32.123: UDP, length 48
IP 192.168.0.110.1034 > 203.69.113.26.80: tcp 0
IP 192.168.0.110.1034 > 203.69.113.26.80: tcp 204
IP 203.69.113.26.80 > 192.168.0.110.1034: tcp 0
IP 203.69.113.26.80 > 192.168.0.110.1034: tcp 983
IP 192.168.0.110.1034 > 203.69.113.26.80: tcp 0
IP 192.168.0.110.1034 > 203.69.113.26.80: tcp 0

3. Network Connect

>> NPASCAN - 警政署惡意程式偵測工具 <<
-==<<警政署惡意程式偵測工具 NPASCAN v1.7 >>==-
Current User : TWMAN-SINGLE-01\Administrator
Current IP : 192.168.0.110
Start Time : 20 April 2010 18:51:23
----------Start Scan----------
掃瞄完成!!未偵測到相關惡意程式!
----------End Scan----------
>> CWSandBox VirusScan Report <<
VSCAN Version:3.2.1861.2 (Feb 22 2009 19:30:04);run at:: Apr 20 10:54:01 2010
defs version: 5444 (2009-10-12T17:47:12)
command line: c:\SBScanV3\vscan /l c:\virus.txt /def c:\SBDefsV3 C:\WINDOWS\system32\sandnet.exe
[15], No threat , , , ,C:\WINDOWS\system32\sandnet.exe
1 objects processed in 0 secs, 0 fps
0 threats detected, 0 suspicious files

4.Virus Scan

>> Advanced Intrusion Detection Environment-檔案異動偵測 <<
Start timestamp: 2010-04-20 19:02:15
Summary:
Total number of files: 29933
Added files: 20
Removed files: 0
Changed files: 19

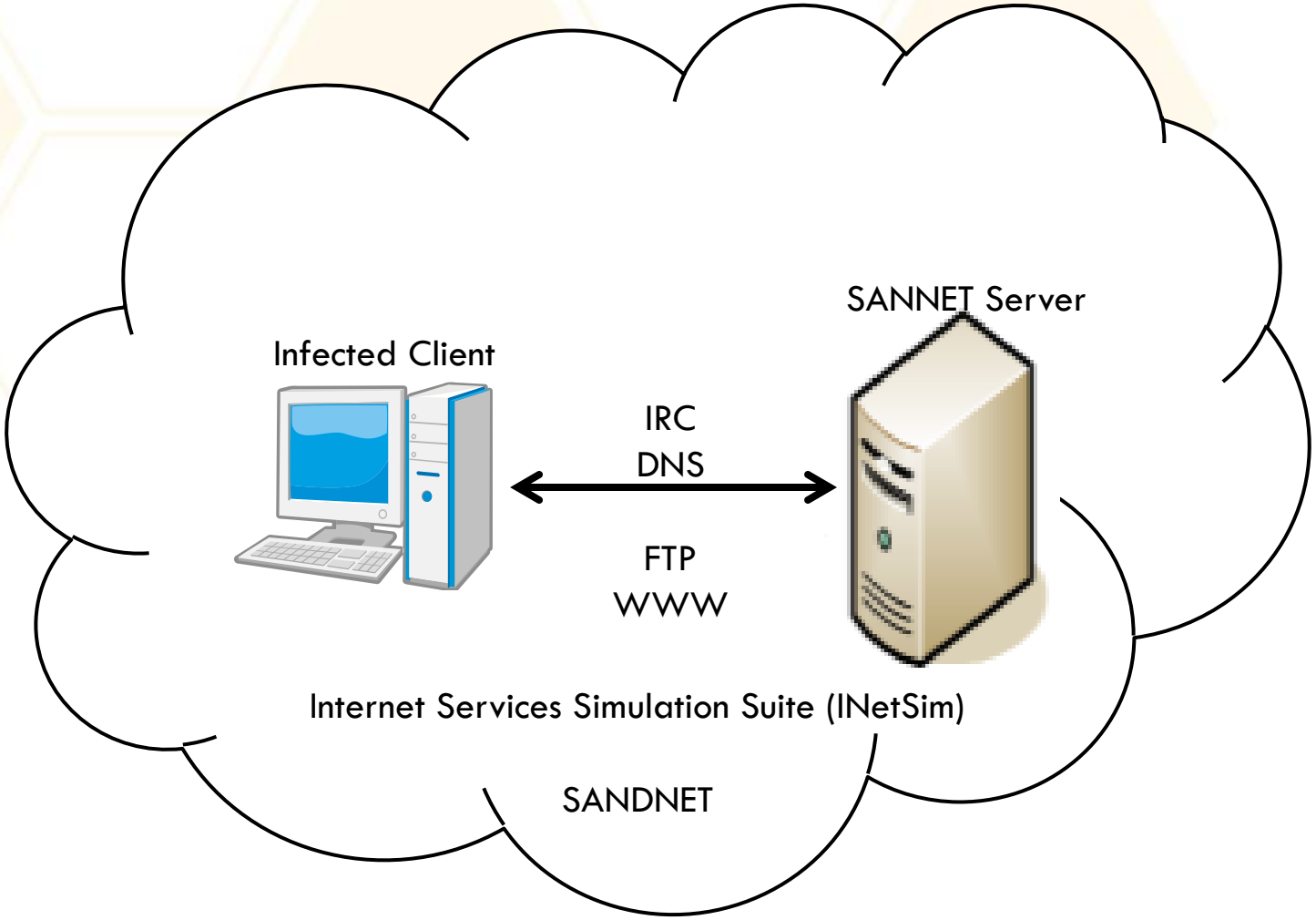
Added files:
---
added: /mnt/images/Documents and Settings/Administrator/twman.cgi@res=startfauxserver.2
added: /mnt/images/Documents and Settings/Administrator/wget-log.5
added: /mnt/images/Documents and Settings/Administrator/wget-log.6
added: /mnt/images/System Volume Information/_restore{399113A8-6E6F-4DCA-A398-D03564F81D09}/RP24/A0003606.ini
added: /mnt/images/System Volume Information/_restore{399113A8-6E6F-4DCA-
---
Changed files:
---
changed: /mnt/images/Documents and Settings/Administrator/Local Settings/Temp/AdobeARM.log
changed: /mnt/images/Documents and Settings/Administrator/Local Settings/Temp/jusched.log
changed: /mnt/images/System Volume Information/_restore{399113A8-6E6F-4DCA-A398-D03564F81D09}/RP24/change.log
changed: /mnt/images/WINDOWS/Prefetch/NOTEPAD.EXE-336351A9.pf
changed: /mnt/images/WINDOWS/Prefetch/NPASCAN.EXE-1F4DCEFB.pf
changed: /mnt/images/WINDOWS/Prefetch/NTOSBOOT-B00DFAAD.pf
changed: /mnt/images/WINDOWS/system32/wbem/Logs/FrameWork.log
changed: /mnt/images/WINDOWS/system32/wbem/Logs/wbemcore.log
changed: /mnt/images/WINDOWS/system32/wbem/Logs/wbemess.log
changed: /mnt/images/WINDOWS/system32/wbem/Logs/wmiprov.log

臺灣惡意程式分析網，抬丸郎 - 分析報告 2010-06-20 版

5.File Change

Taiwan Chapter

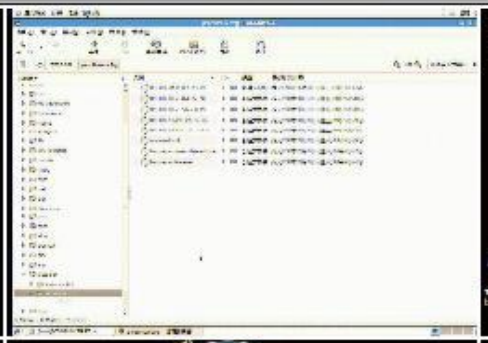
Sandnet


SANNET Server
Infected Client
IRC
DNS
FTP
WWW
Internet Services Simulation Suite (INetSim)
SANDNET

Remote View

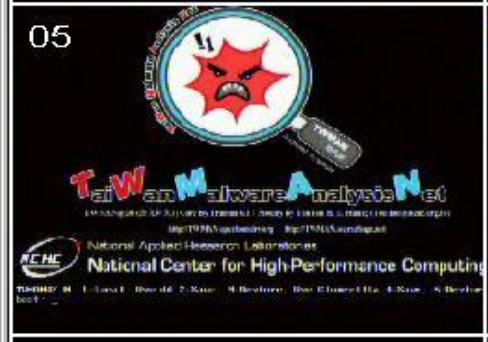
01

02



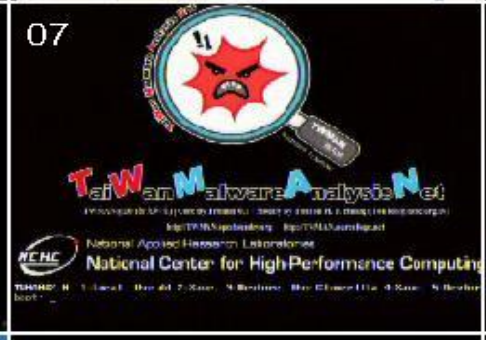
04

05

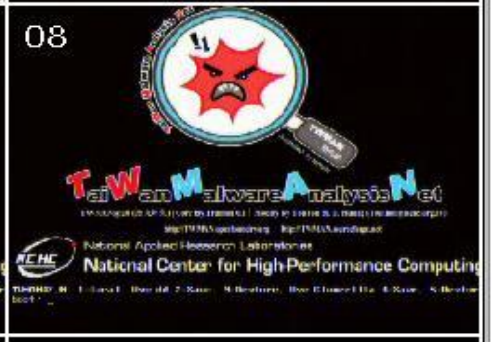


06

07



08



09

10

11

12

13

14

15

16-01

Port 13: [13] Child Edu, 1024X768@60, Power on, Full access.

Ahead 4 ports.

Conclusions and Future work

Taiwan Chapter

- Malware and malware behavioral ontology can be solve the problems.
- It will be develop by Protégé API, OWL API, SWRL API and FML.
- TWMAN can integrate with a human thinking semantic model.
- TWMAN@2.0
  - Multi OS
  - Multi Clients
  - Green Computing
  - Cloud Computing

Q & A

yilang@honeynet.org.tw

事件通報
security@honeynet.org.tw
csirt@honeynet.org.tw