Analisi del Malware

```
remnux@remnux:/media/C8D5-495F/TorrentLocker$ volatility -f xpsp3-before-infection.dmp --profile=WinXPSP3x86 pstree
Volatility Foundation Volatility Framework 2.3.1
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x823c8830:System                                      4      0     56    256 1970-01-01 00:00:00 UTC+0000
. 0x81f877c0:smss.exe                                 536      4      3     19 2014-12-19 20:24:47 UTC+0000
.. 0x822a1020:csrss.exe                               600    536     10    346 2014-12-19 20:24:48 UTC+0000
.. 0x81f16da0:winlogon.exe                            624    536     20    509 2014-12-19 20:24:49 UTC+0000
... 0x822f64f0:wpabaln.exe                           1940    624      1     58 2014-12-19 20:26:51 UTC+0000
... 0x81df5020:lsass.exe                              680    624     20    330 2014-12-19 20:24:49 UTC+0000
... 0x81f0c850:services.exe                           668    624     16    253 2014-12-19 20:24:49 UTC+0000
.... 0x81de5da0:svchost.exe                          1024    668     66   1162 2014-12-19 20:24:49 UTC+0000
..... 0x81d98020:wscntfy.exe                          260   1024      1     28 2014-12-19 20:26:06 UTC+0000
..... 0x81dd68c0:wmiadap.exe                          772   1024      5    150 2015-02-28 16:12:52 UTC+0000
..... 0x82123148:wuauclt.exe                          220   1024      8    180 2014-12-19 20:26:49 UTC+0000
.... 0x822a3708:spoolsv.exe                          1444    668     13    136 2014-12-19 20:24:51 UTC+0000
.... 0x81efb750:svchost.exe                          1072    668      6     76 2014-12-19 20:24:49 UTC+0000
.... 0x81f08380:vmacthlp.exe                          836    668      1     25 2014-12-19 20:24:49 UTC+0000
.... 0x822ef020:alg.exe                               328    668      6    107 2014-12-19 20:26:04 UTC+0000
.... 0x82279780:svchost.exe                           852    668     18    195 2014-12-19 20:24:49 UTC+0000
.... 0x82192d08:svchost.exe                           932    668     11    254 2014-12-19 20:24:49 UTC+0000
.... 0x82185360:svchost.exe                          1140    668     15    201 2014-12-19 20:24:50 UTC+0000
.... 0x82190020:vmtoolsd.exe                         1020    668      7    262 2014-12-19 20:26:00 UTC+0000
 0x821711a0:explorer.exe                             1564   1548     13    490 2014-12-19 20:24:51 UTC+0000
. 0x8216b590:vmtoolsd.exe                            1668   1564      7    229 2014-12-19 20:24:52 UTC+0000
. 0x81f544f8:VMwareTray.exe                          1660   1564      1     52 2014-12-19 20:24:52 UTC+0000
remnux@remnux:/media/C8D5-495F/TorrentLocker$ volatility -f xpsp3-after-infection.dmp --profile=WinXPSP3x86 pstree
Volatility Foundation Volatility Framework 2.3.1
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x823c8830:System                                      4      0     56    263 1970-01-01 00:00:00 UTC+0000
. 0x81f877c0:smss.exe                                 536      4      3     19 2014-12-19 20:24:47 UTC+0000
.. 0x822a1020:csrss.exe                               600    536     11    338 2014-12-19 20:24:48 UTC+0000
.. 0x81f16da0:winlogon.exe                            624    536     17    502 2014-12-19 20:24:49 UTC+0000
... 0x822f64f0:wpabaln.exe                           1940    624      1     58 2014-12-19 20:26:51 UTC+0000
... 0x81df5020:lsass.exe                              680    624     20    344 2014-12-19 20:24:49 UTC+0000
... 0x81f0c850:services.exe                           668    624     16    255 2014-12-19 20:24:49 UTC+0000
.... 0x81de5da0:svchost.exe                          1024    668     59   1159 2014-12-19 20:24:49 UTC+0000
..... 0x81d98020:wscntfy.exe                          260   1024      1     28 2014-12-19 20:26:06 UTC+0000
.... 0x822a3708:spoolsv.exe                          1444    668     10    130 2014-12-19 20:24:51 UTC+0000
.... 0x81efb750:svchost.exe                          1072    668      6     83 2014-12-19 20:24:49 UTC+0000
.... 0x81f08380:vmacthlp.exe                          836    668      1     25 2014-12-19 20:24:49 UTC+0000
.... 0x822ef020:alg.exe                               328    668      6    107 2014-12-19 20:26:04 UTC+0000
.... 0x82279780:svchost.exe                           852    668     15    189 2014-12-19 20:24:49 UTC+0000
..... 0x81e8eb28:wmiprvse.exe                         868    852      5    136 2015-02-28 17:07:59 UTC+0000
.... 0x82192d08:svchost.exe                           932    668      9    257 2014-12-19 20:24:49 UTC+0000
.... 0x82185360:svchost.exe                          1140    668     11    199 2014-12-19 20:24:50 UTC+0000
.... 0x82190020:vmtoolsd.exe                         1020    668      6    259 2014-12-19 20:26:00 UTC+0000
 0x8225e020:explorer.exe                             1872   1380      8    328 2015-02-28 17:06:16 UTC+0000
  0x822f2020:vssadmin.exe                            1168   1872      0 ------ 2015-02-28 17:06:16 UTC+0000
  0x8214a8e0:IEXPLORE.EXE                            1224   1872      5    194 2015-02-28 17:14:54 UTC+0000
 0x821711a0:explorer.exe                             1564   1548     15    569 2014-12-19 20:24:51 UTC+0000
. 0x8216b590:vmtoolsd.exe                            1668   1564      5    213 2014-12-19 20:24:52 UTC+0000
. 0x81f544f8:VMwareTray.exe                          1660   1564      1     52 2014-12-19 20:24:52 UTC+0000
```

Run list of process from known good machine and then compare it with infected machine

The parent process of explorer.exe does not exist. This is rather suspicious!

Explorer.exe launched Volume Shadow Copies util?

Analisi del Malware

- Statica
- Dinamica
- Analisi della memoria
- Estrazione di codice malevolo da file

- Un esempio: FinFisher

Analisi Statica

- Header PE
- Import Address Table (IAT)

```
Resource entries
================================================================================
Name                RVA      Size     Lang         Sublang
--------------------------------------------------------------------------------
BIN                 0x19100  0x4a63   LANG_CHINESE SUBLANG_CHINESE_SIMPL
BINSYS              0x1db68  0x727    LANG_CHINESE SUBLANG_CHINESE_SIMPL
RT_VERSION          0x1e290  0x3ec    LANG_CHINESE SUBLANG_CHINESE_SIMPL

Suspicious IAT alerts
================================================================================
OpenProcess
VirtualAllocEx
WriteProcessMemory
CreateRemoteThread
CreateProcessA
StartServiceA
OpenProcessToken
InternetReadFile
```

Analisi statica

- Disassembler
- Debugger

```
OllyDbg - PEB.exe - [CPU - main thread, module PEB]
File View Debug Plugins Options Window Help

00401231  $ 55              PUSH    EBP
00401232  . 8BEC            MOV     EBP,ESP
00401234  . 83C4 F8         ADD     ESP,-8
00401237  . 60              PUSHAD
00401238  . 8B75 08         MOV     ESI,DWORD PTR SS:[EBP+8]
0040123B  . 8D3D 70334000   LEA     EDI,DWORD PTR DS:[403370]
00401241  . 33C0            XOR     EAX,EAX
00401243  > 8A06            MOV     AL,BYTE PTR DS:[ESI]
00401245  . 8807            MOV     BYTE PTR DS:[EDI],AL
00401247  . 47              INC     EDI
00401248  . 83C6 02         ADD     ESI,2
0040124B  . 803E 00         CMP     BYTE PTR DS:[ESI],0
0040124E  .^ 75 F3          JNZ     SHORT PEB.00401243
00401250  . 66:C707 0D0A    MOV     WORD PTR DS:[EDI],0A0D
00401255  . 83C7 02         ADD     EDI,2
00401258  . 66:C707 0D0A    MOV     WORD PTR DS:[EDI],0A0D
0040125D  . 33C0            XOR     EAX,EAX
0040125F  . 8D3D 70334000   LEA     EDI,DWORD PTR DS:[403370]
00401265  . B9 FFFFFFFF     MOV     ECX,-1
0040126A  . F2:AE           REPNE   SCAS BYTE PTR ES:[EDI]
0040126C  . F7D1            NOT     ECX
0040126E  . 49              DEC     ECX
0040126F  . 894D FC         MOV     DWORD PTR SS:[EBP-4],ECX
00401272  . 6A 02           PUSH    2                          Origin = FILE_END
00401274  . 6A 00           PUSH    0                          pOffsetHi = NULL
00401276  . 6A 00           PUSH    0                          OffsetLo = 0
00401278  . FF35 6D324000   PUSH    DWORD PTR DS:[40326D]      hFile = 00000080 (window)
0040127E  . E8 4B000000     CALL    <JMP.&kernel32.SetFilePointer>  SetFilePointer
00401283  . 6A 00           PUSH    0                          pOverlapped = NULL
00401285  . 8D45 F8         LEA     EAX,DWORD PTR SS:[EBP-8]
00401288  . 50              PUSH    EAX                        pBytesWritten
00401289  . FF75 FC         PUSH    DWORD PTR SS:[EBP-4]       nBytesToWrite
0040128C  . 68 70334000     PUSH    PEB.00403370               Buffer = PEB.00403370
00401291  . FF35 6D324000   PUSH    DWORD PTR DS:[40326D]      hFile = 00000080 (window)
00401297  . E8 38000000     CALL    <JMP.&kernel32.WriteFile>  WriteFile
0040129C  . 68 FF000000     PUSH    0FF                        Length = FF (255.)
004012A1  . 68 70334000     PUSH    PEB.00403370               Destination = PEB.00403370
004012A6  . E8 1D000000     CALL    <JMP.&kernel32.RtlZeroMemory>  RtlZeroMemory
004012AB  . 61              POPAD
004012AC  . C9              LEAVE
004012AD  . C2 0400         RETN    4
004012B0  $- FF25 00204000  JMP     DWORD PTR DS:[<&kernel32.CloseHandle>]   kernel32.CloseHandle
004012B6  $- FF25 04204000  JMP     DWORD PTR DS:[<&kernel32.CreateFileA>]   kernel32.CreateFileA
004012BC  .- FF25 08204000  JMP     DWORD PTR DS:[<&kernel32.ExitProcess>]   kernel32.ExitProcess
004012C2  $- FF25 0C204000  JMP     DWORD PTR DS:[<&kernel32.GetCommandLineA>]   kernel32.GetCommandLineA
004012C8  $- FF25 10204000  JMP     DWORD PTR DS:[<&kernel32.RtlZeroMemory>]   ntdll.RtlZeroMemory
004012CE  $- FF25 14204000  JMP     DWORD PTR DS:[<&kernel32.SetFilePointer>]   kernel32.SetFilePointer
004012D4  $- FF25 18204000  JMP     DWORD PTR DS:[<&kernel32.WriteFile>]   kernel32.WriteFile
004012DA  $- FF25 1C204000  JMP     DWORD PTR DS:[<&kernel32.lstrcatA>]   kernel32.lstrcatA
004012E0  $- FF25 20204000  JMP     DWORD PTR DS:[<&kernel32.lstrcpyA>]   kernel32.lstrcpyA
004012E6  $- FF25 34204000  JMP     DWORD PTR DS:[<&user32.wsprintfA>]   user32.wsprintfA
004012EC  $- FF25 30204000  JMP     DWORD PTR DS:[<&user32.MessageBoxA>]   user32.MessageBoxA
004012F2  $- FF25 28204000  JMP     DWORD PTR DS:[<&shell32.ShellExecuteA>]   shell32.ShellExecuteA
004012F8    00              DB      00
004012F9    00              DB      00
```

Analisi statica

- Ricerca di stringhe e url

```
remnux@remnux:~$ xorsearch -s hubert.dll http:
Found XOR 05 position 2E18: http://%s/readdatagateway.php?type=stats
remnux@remnux:~$ strings hubert.dll.XOR.05 > out.txt
```

```
remnux@remnux:~$ xorstrings Windows\ Live\ Messenger.exe
Opr   Key  Count Avg   Max
  XOR 0xf7     1   6.0     6
  XOR 0xfb     1  12.0    12
  XOR 0xe3     2   7.5     9
  XOR 0xe6     2   8.0     9
  XOR 0xf9     2   5.0     5
  XOR 0x1a     4   8.5    16
  XOR 0xc9     4   7.0     9
  XOR 0xe5     4   9.2    15
  XOR 0xe7     4   9.8    21
  XOR 0xef     4  10.5    12
  XOR 0xf5     4   6.0     6
  XOR 0xfa     4   5.5     6
  XOR 0xfe     4  13.5    39
  XOR 0x1d     5   7.0     9
  XOR 0xec     5   7.2     8
  XOR 0x1b     6   6.5     7
  XOR 0xcd     6   7.2    11
  XOR 0xce     6  56.2   293
```

Analisi statica

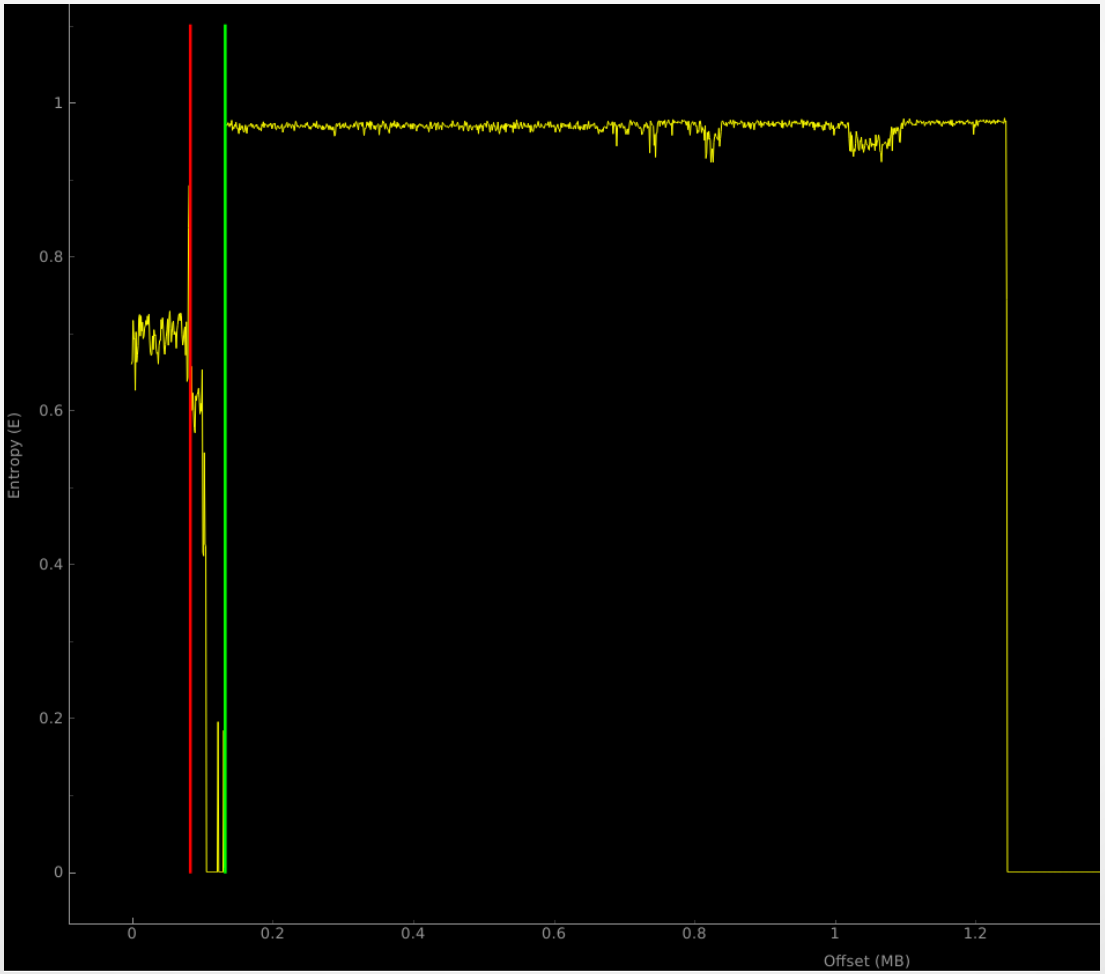
- Packer

```
remnux@remnux:~$ pescanner lamarr.dll
#################################################################
Record 0
#################################################################

Meta-data
=================================================================
File:     lamarr.dll
Size:     120355 bytes
Type:     PE32 executable for MS Windows (DLL) (GUI) Intel 80386
MD5:      9a7a3ed7e9fa238c3314e579a4dc192b
SHA1:     6b7e2a6d72fd938485701897f4a3b2c6b5a93bde
ssdeep:   3072:Nf32CzOZEZrFu2ZPNBReAiAP0Ck8Ig3gqoFC256:92SOZg0WN
Date:     0x4B9F339D [Tue Mar 16 07:30:37 2010 UTC]
EP:       0x100119ba .text 0/5
CRC:      Claimed: 0x0, Actual: 0x2a415 [SUSPICIOUS]
Packers:  Armadillo v1.xx - v2.xx
```

Analisi statica

- Analisi entropia



Le contromisure del malware

- Codice antiVM, antisandbox e antidebugging

Branch: **master** ▾ **soldier-win** / Soldier / **antivm.cpp**

Ivan new VMWare check, Facebook photo and location scheduling moved into s…

0 contributors

165 lines (127 sloc) | 4.05 KB

```
1  #include <Windows.h>
2  #include "utils.h"
3  #include "crypt.h"
4  #include "antivm.h"
5  #include "utils.h"
6
7  BOOL AntiVM()
8  {
9          AntiCuckoo();
10         BOOL bVMWare = AntiVMWare();
11         BOOL bVBox = AntiVBox();
12
13         if (bVMWare || bVBox)
14                 return TRUE;
15
16         return FALSE;
17 }
```

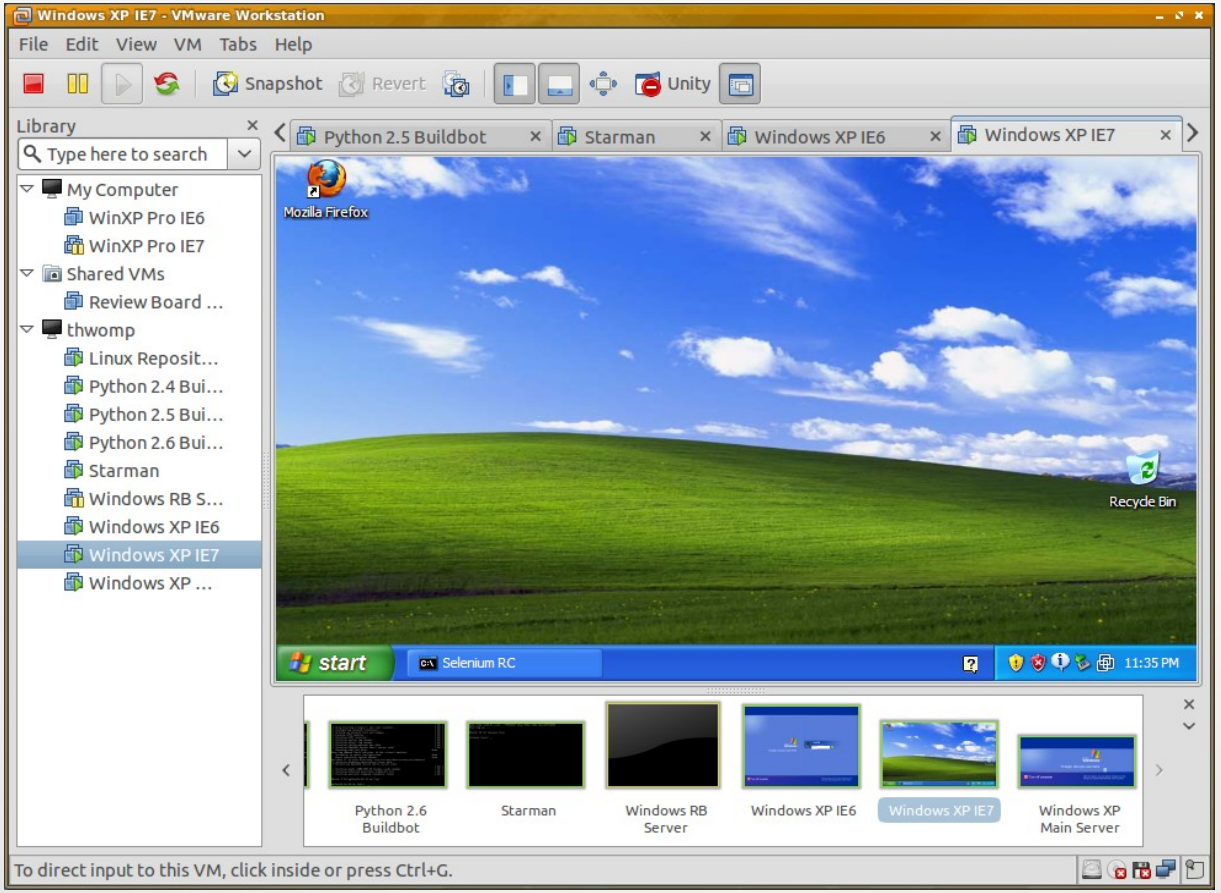
Le contromisure del malware

- Sfruttare vulnerabilità dei software di analisi

CVE-ID	
CVE-2014-8485	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
The setup_group function in bfd/elf.c in libbfd in GNU binutils 2.24 and earlier allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via crafted section group headers in an ELF file.	

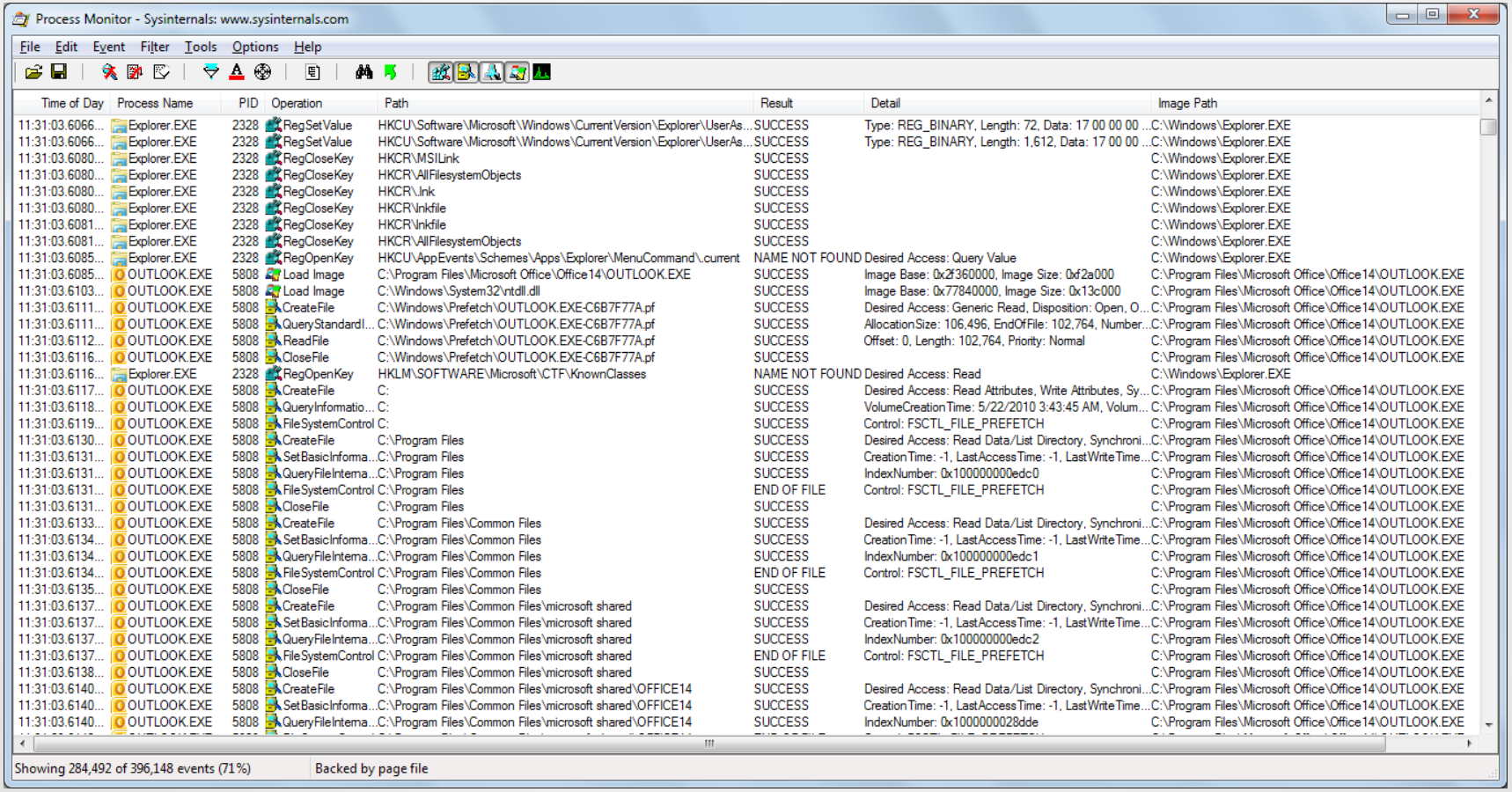
Analisi dinamica

- Esecuzione del malware in ambiente isolato e analisi degli artefatti



Analisi dinamica

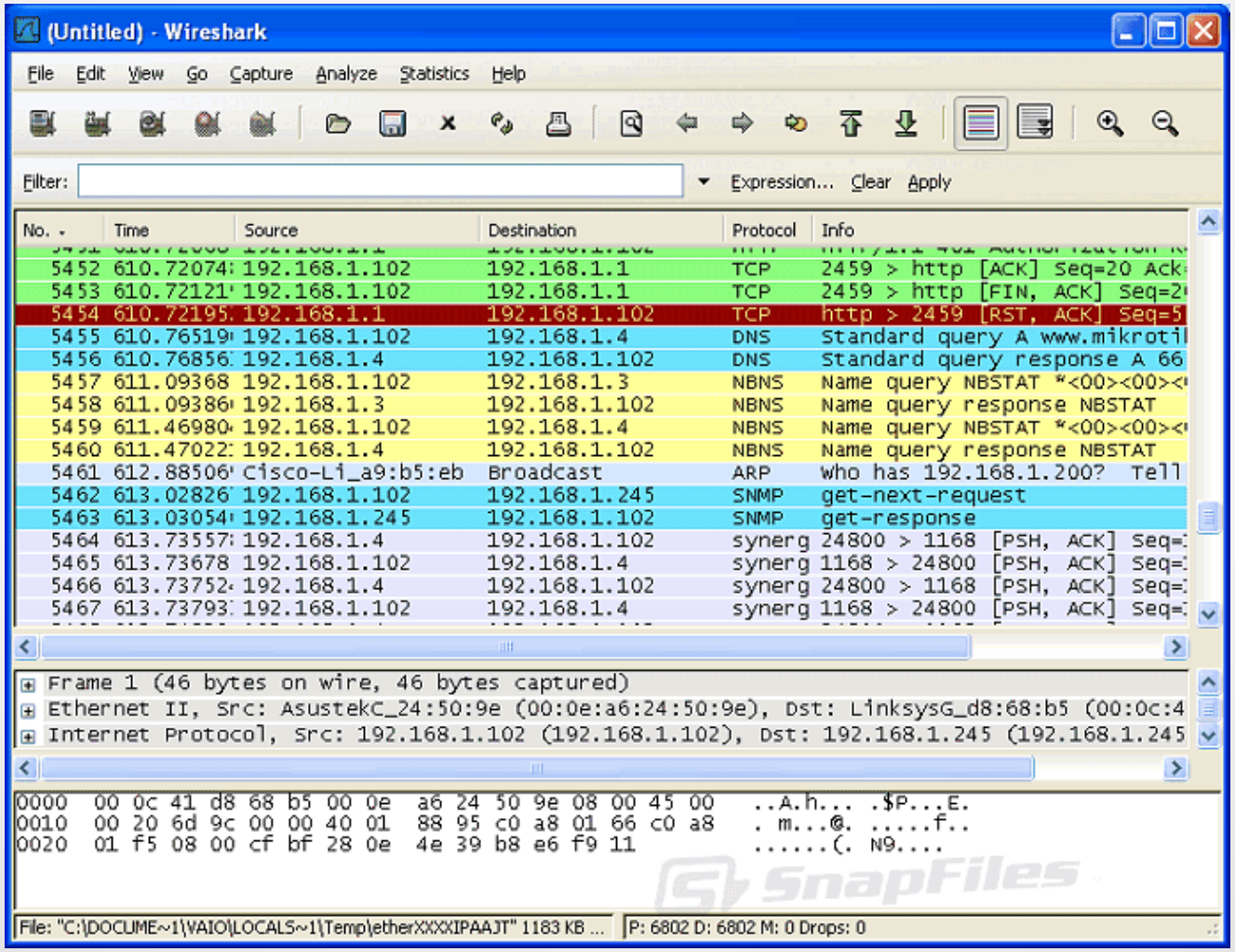
- Confronto dello stato del sistema prima e dopo l'esecuzione del malware (files, chiavi di registro...)



Time of Day	Process Name	PID	Operation	Path	Result	Detail	Image Path
11:31:03.6066...	Explorer.EXE	2328	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAs...	SUCCESS	Type: REG_BINARY, Length: 72, Data: 17 00 00 00 ...	C:\Windows\Explorer.EXE
11:31:03.6066...	Explorer.EXE	2328	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAs...	SUCCESS	Type: REG_BINARY, Length: 1,612, Data: 17 00 00 ...	C:\Windows\Explorer.EXE
11:31:03.6080...	Explorer.EXE	2328	RegCloseKey	HKCR\MSILink	SUCCESS		C:\Windows\Explorer.EXE
11:31:03.6080...	Explorer.EXE	2328	RegCloseKey	HKCR\AllFilesystemObjects	SUCCESS		C:\Windows\Explorer.EXE
11:31:03.6080...	Explorer.EXE	2328	RegCloseKey	HKCR\.lnk	SUCCESS		C:\Windows\Explorer.EXE
11:31:03.6080...	Explorer.EXE	2328	RegCloseKey	HKCR\lnkfile	SUCCESS		C:\Windows\Explorer.EXE
11:31:03.6081...	Explorer.EXE	2328	RegCloseKey	HKCR\lnkfile	SUCCESS		C:\Windows\Explorer.EXE
11:31:03.6081...	Explorer.EXE	2328	RegCloseKey	HKCR\AllFilesystemObjects	SUCCESS		C:\Windows\Explorer.EXE
11:31:03.6085...	Explorer.EXE	2328	RegOpenKey	HKCU\AppEvents\Schemes\Apps\Explorer\MenuCommand\.current	NAME NOT FOUND	Desired Access: Query Value	C:\Windows\Explorer.EXE
11:31:03.6085...	OUTLOOK.EXE	5808	Load Image	C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE	SUCCESS	Image Base: 0x2f360000, Image Size: 0xf2a000	C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6103...	OUTLOOK.EXE	5808	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x77840000, Image Size: 0x13c000	C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6111...	OUTLOOK.EXE	5808	CreateFile	C:\Windows\Prefetch\OUTLOOK.EXE-C6B7F77A.pf	SUCCESS	Desired Access: Generic Read, Disposition: Open, O...	C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6111...	OUTLOOK.EXE	5808	QueryStandardI...	C:\Windows\Prefetch\OUTLOOK.EXE-C6B7F77A.pf	SUCCESS	AllocationSize: 106,496, EndOfFile: 102,764, Number...	C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6112...	OUTLOOK.EXE	5808	ReadFile	C:\Windows\Prefetch\OUTLOOK.EXE-C6B7F77A.pf	SUCCESS	Offset: 0, Length: 102,764, Priority: Normal	C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6116...	OUTLOOK.EXE	5808	CloseFile	C:\Windows\Prefetch\OUTLOOK.EXE-C6B7F77A.pf	SUCCESS		C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6116...	Explorer.EXE	2328	RegOpenKey	HKLM\SOFTWARE\Microsoft\CTF\KnownClasses	NAME NOT FOUND	Desired Access: Read	C:\Windows\Explorer.EXE
11:31:03.6117...	OUTLOOK.EXE	5808	CreateFile	C:	SUCCESS	Desired Access: Read Attributes, Write Attributes, Sy...	C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6118...	OUTLOOK.EXE	5808	QueryInformatio...	C:	SUCCESS	VolumeCreationTime: 5/22/2010 3:43:45 AM, Volum...	C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6119...	OUTLOOK.EXE	5808	FileSystemControl	C:	SUCCESS	Control: FSCTL_FILE_PREFETCH	C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6130...	OUTLOOK.EXE	5808	CreateFile	C:\Program Files	SUCCESS	Desired Access: Read Data/List Directory, Synchroni...	C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6131...	OUTLOOK.EXE	5808	SetBasicInforma...	C:\Program Files	SUCCESS	CreationTime: -1, LastAccessTime: -1, LastWriteTime...	C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6131...	OUTLOOK.EXE	5808	QueryFileInterna...	C:\Program Files	SUCCESS	IndexNumber: 0x100000000edc0	C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6131...	OUTLOOK.EXE	5808	FileSystemControl	C:\Program Files	END OF FILE	Control: FSCTL_FILE_PREFETCH	C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6131...	OUTLOOK.EXE	5808	CloseFile	C:\Program Files	SUCCESS		C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6133...	OUTLOOK.EXE	5808	CreateFile	C:\Program Files\Common Files	SUCCESS	Desired Access: Read Data/List Directory, Synchroni...	C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6134...	OUTLOOK.EXE	5808	SetBasicInforma...	C:\Program Files\Common Files	SUCCESS	CreationTime: -1, LastAccessTime: -1, LastWriteTime...	C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6134...	OUTLOOK.EXE	5808	QueryFileInterna...	C:\Program Files\Common Files	SUCCESS	IndexNumber: 0x100000000edc1	C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6134...	OUTLOOK.EXE	5808	FileSystemControl	C:\Program Files\Common Files	END OF FILE	Control: FSCTL_FILE_PREFETCH	C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6135...	OUTLOOK.EXE	5808	CloseFile	C:\Program Files\Common Files	SUCCESS		C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6137...	OUTLOOK.EXE	5808	CreateFile	C:\Program Files\Common Files\microsoft shared	SUCCESS	Desired Access: Read Data/List Directory, Synchroni...	C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6137...	OUTLOOK.EXE	5808	SetBasicInforma...	C:\Program Files\Common Files\microsoft shared	SUCCESS	CreationTime: -1, LastAccessTime: -1, LastWriteTime...	C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6137...	OUTLOOK.EXE	5808	QueryFileInterna...	C:\Program Files\Common Files\microsoft shared	SUCCESS	IndexNumber: 0x100000000edc2	C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6137...	OUTLOOK.EXE	5808	FileSystemControl	C:\Program Files\Common Files\microsoft shared	END OF FILE	Control: FSCTL_FILE_PREFETCH	C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6138...	OUTLOOK.EXE	5808	CloseFile	C:\Program Files\Common Files\microsoft shared	SUCCESS		C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6140...	OUTLOOK.EXE	5808	CreateFile	C:\Program Files\Common Files\microsoft shared\OFFICE14	SUCCESS	Desired Access: Read Data/List Directory, Synchroni...	C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6140...	OUTLOOK.EXE	5808	SetBasicInforma...	C:\Program Files\Common Files\microsoft shared\OFFICE14	SUCCESS	CreationTime: -1, LastAccessTime: -1, LastWriteTime...	C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6140...	OUTLOOK.EXE	5808	QueryFileInterna...	C:\Program Files\Common Files\microsoft shared\OFFICE14	SUCCESS	IndexNumber: 0x1000000028dde	C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE

Analisi dinamica

- Analisi del traffico di rete



Analisi dinamica

- Interagire con il malware per scoprire nuove caratteristiche
- Usare honeypot per DNS, SMTP, HTTP e qualunque altro servizio il malware cerchi di raggiungere

Closed

Connected At	Rcpt To	Bytes	File Name	Remote IP	Subject	Attachment
6/27/2007 1:13:42 PM	<proagent2.1@gmail.com>	6493	1736031209.txt	192.168.1.26	RISHIVMXPP is Online	
6/27/2007 3:29:03 PM	<proagent2.1@gmail.com>	6318	437640621.txt	192.168.1.24	VM-2KPRO is Online	
6/27/2007 3:48:09 PM	<hostmaster@aiin.net>	3565	241873872.txt	192.168.1.71	Secure Mail from MSN.com user.	msg.zip
6/27/2007 3:48:11 PM	<robert2004@yahoo.com>	3608	736420135.txt	192.168.1.71	Encrypted Message from MSN.com user.	mail.zip
6/27/2007 6:13:17 PM	<bill2002@msn.com>	3635	1622644734.txt	192.168.1.77	Secure Message from Yahoo.com user.	message.zip
6/27/2007 6:18:46 PM	<pamela2001@hotmail.com>	5193	1191991604.txt	192.168.1.77	Secure E-mail from Gmail.com user.	data.zip
6/27/2007 6:27:58 PM	<austria@msdirectservices.com>	5160	1951468189.txt	192.168.1.77	Secure Message	mail.zip
6/27/2007 6:27:59 PM	<mts@lebanon-online.com.lb>	5145	1072017617.txt	192.168.1.77	Protected Message	message.zip
6/27/2007 6:49:02 PM	<eo5ha@funb.com>	2626	1144140450.txt	192.168.1.71	You've received a postcard from a family	
6/27/2007 6:49:02 PM	<envy730@funb.com>	2603	1550201278.txt	192.168.1.71	You've received a postcard from a family	
6/27/2007 6:49:02 PM	<bullard@jnli.com>	5471	245871049.txt	192.168.1.71	You've received a postcard from a family	
6/27/2007 6:49:02 PM	<brysonnn@jnli.com>	5421	1909203634.txt	192.168.1.71	You've received a postcard from a family	
6/27/2007 6:49:02 PM	<calvelonn@jtax.com>	5438	199303371.txt	192.168.1.71	You've received a postcard from a family	
6/27/2007 6:49:02 PM	<caldwell@jtax.com>	5447	1986980167.txt	192.168.1.71	You've received a postcard from a family	
6/27/2007 6:49:02 PM	<engupta@csplc.com>	8322	831852132.txt	192.168.1.71	You've received a postcard from a family	
6/27/2007 6:49:02 PM	<enrique.bernaldez@csplc.com>	5538	3187635.txt	192.168.1.71	You've received a postcard from a family	
6/27/2007 6:49:02 PM	<devoll.dougdd@con-way.com>	5396	1145617454.txt	192.168.1.71	You've received a postcard from a family	
6/27/2007 6:49:02 PM	<dewittd@con-way.com>	5490	1737950965.txt	192.168.1.71	You've received a postcard from a family	

Trojan victim email notification

Mass Mailer

Spam

Log Dir = C:\mailpot\ Listen Port = 25 Server Banner Maillennium ESMTP/MULTIBOX Listen

Analisi della memoria

- Estrazione di artefatti dalla RAM
- Tecnica completamente indipendente dal sistema sotto indagine
- Volatility Framework

```
C:\Users\Haider\Downloads\volatility>volatility.exe -f H-HP-20121209-120703.raw --profile=Win7SP1x64 pslist
Volatile Systems Volatility Framework 2.1
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                 Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------- ----
0xfffffa8003606740 System                    4      0    170     3039 ------      0 2012-12-07 11:42:15
0xfffffa8006939b30 smss.exe                440      4      2       32 ------      0 2012-12-07 11:42:15
0xfffffa8007581b30 csrss.exe               564    544     11      929      0      0 2012-12-07 11:42:21
0xfffffa8007816b30 wininit.exe             760    544      3       78      0      0 2012-12-07 11:42:24
0xfffffa800781ab30 csrss.exe               780    768     13      849      1      0 2012-12-07 11:42:24
0xfffffa8007839b30 services.exe            824    760      9      311      0      0 2012-12-07 11:42:24
0xfffffa8008162b30 lsass.exe               840    760      8      825      0      0 2012-12-07 11:42:24
0xfffffa80081891e0 lsm.exe                 848    760     10      204      0      0 2012-12-07 11:42:24
0xfffffa800816ab30 winlogon.exe            900    768      3      117      1      0 2012-12-07 11:42:24
0xfffffa800820e060 svchost.exe             984    824     11      415      0      0 2012-12-07 11:42:25
0xfffffa8008249060 svchost.exe             484    824      9      425      0      0 2012-12-07 11:42:25
0xfffffa800824cb30 atiesrxx.exe            648    824      6      118      0      0 2012-12-07 11:42:25
0xfffffa8008358750 svchost.exe             784    824     21      643      0      0 2012-12-07 11:42:25
0xfffffa8008369350 svchost.exe            1000    824     18      542      0      0 2012-12-07 11:42:26
0xfffffa80083ff8a0 svchost.exe            1040    824     43     1605      0      0 2012-12-07 11:42:26
0xfffffa800839b580 stacsv64.exe           1124    824     10      325      0      0 2012-12-07 11:42:27
0xfffffa800849cb30 svchost.exe            1328    824     18      597      0      0 2012-12-07 11:42:29
0xfffffa8008508060 hpservice.exe          1432    824      4       76      0      0 2012-12-07 11:42:29
0xfffffa8008537b30 svchost.exe            1480    824     13      449      0      0 2012-12-07 11:42:30
```

Analisi della memoria

- Estrarre file PE dalla memoria per eseguire analisi statica dopo l'esecuzione del packer
- Trovare zone di memoria che contengono codice malevolo
- Trovare processi nascosti o infettati

```
Volatile Systems Volatility Framework 2.1_alpha
Name                 Pid    Start      End        Tag      Hits   Protect
svchost.exe          856    0x00b70000 0xb95fff00 VadS     0      PAGE_EXECUTE_READWRITE
Dumped to: /home/evild3ad/Volatility/dump-files/svchost.exe.115b8d8.00b70000-00b95fff.dmp
0x00b70000   4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00    MZ..............
0x00b70010   b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00    ........@.......
0x00b70020   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
0x00b70030   00 00 00 00 00 00 00 00 00 00 00 00 d0 00 00 00
0x00b70040   0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68    ........!..L.!Th
0x00b70050   69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f    is program canno
0x00b70060   74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20    t be run in DOS
0x00b70070   6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00    mode....$.......
```

Estrarre codice malevolo da file

- xxxswf: Estrarre sfw da altri formati
- swfdump: Disassembly Adobe Flash
- pdfid e pdfextract: Estrarre contenuti da pdf (JS, media...)

```
PDFiD 0.0.11 conrad.pdf
 PDF Header: %PDF-1.4
 obj                    15
 endobj                 15
 stream                  2
 endstream               2
 xref                    1
 trailer                 1
 startxref               1
 /Page                   1
 /Encrypt                0
 /ObjStm                 0
 /JS                     2
 /JavaScript             3
 /AA                     0
 /OpenAction             1
 /AcroForm               1
```

FinFisher

- Una suite di malware “legale” destinato a forze dell’ordine
- Venduto a regimi non democratici in tutto il mondo

Security

FinFisher spyware used to snoop on Bahraini activists, police told

Gamma International on the end of UK criminal complaint

FinFisher spyware seen targeting victims in Vietnam, Ethiopia

New research finds the surveillance spyware is spreading but may be used to spy on activists

FinFisher: funzionalità

FinSpy

- Features:
  - Custom Executables
  - Bypasses Anti-Virus/ Anti-Spyware Software
  - Location Tracing
  - Scheduled Operations
  - Key Logging
  - Password Gathering
  - Webcam/ Microphone Access
  - Communication Sniffing:
    - Skype
    - Instant Messengers (ICQ, Yahoo, ..)
  - Other

elaman

FinFisher: il caso del Bahrain

- Attacchi mirati ad attivisti e oppositori politici
- Social engineering tramite mail e social network

----- Forwarded Message -----
From: Melissa Chan <melissa.aljazeera@gmail.com>
To:
Sent: Tuesday, 8 May 2012, 8:52
Subject: Torture reports on Nabeel Rajab

Acting president Zainab Al Khawaja for Human Rights Bahrain reports of torture on Mr. Nabeel Rajab after his recent arrest.

Please check the attached detailed report along with torture images.

Finfisher: vettore di infezione

- File rar contenenti eseguibili mascherati da jpg o doc
- Uso del carattere RLO per non destare sospetti

Finfisher: infezione

- Cancella il file originale e si sposta in una cartella temporanea
- Crea la cartella destinata ai file da inviare al C&C

C:\DOCUME~1\%USER%\LOCALS~1\Temp\delete.bat

C:\DOCUME~1\%USER%\LOCALS~1\Temp\driverw.sys

```
Thu Jun 14 2012 11:50:59    35875 m..b r/rrwxrwxrwx 0        0        22469-128-4 C:/Documents and Settings/XPMUser/Desktop/Arrested Suspects.jpg
                               48 ...b d/drwxrwxrwx 0        0        25931-144-1 C:/Documents and Settings/XPMUser/Local Settings/Temp/TMP51B7AFEF
                           909824 ...b r/rrwxrwxrwx 0        0        25932-128-4 C:/Documents and Settings/XPMUser/Local Settings/Temp/tmpD.tmp
Thu Jun 14 2012 11:51:01    35875 .ac. r/rrwxrwxrwx 0        0        22469-128-4 C:/Documents and Settings/XPMUser/Desktop/Arrested Suspects.jpg
                              807 ...b r/rrwxrwxrwx 0        0        25934-128-4 C:/Documents and Settings/XPMUser/Recent/Arrested Suspects.lnk
                           438272 .a.. r/rrwxrwxrwx 0        0        3011-128-3 C:/WINDOWS/system32/shimgvw.dll
Thu Jun 14 2012 11:51:02   389120 .a.. r/rrwxrwxrwx 0        0        2114-128-3 C:/WINDOWS/system32/cmd.exe
                              807 mac. r/rrwxrwxrwx 0        0        25934-128-4 C:/Documents and Settings/XPMUser/Recent/Arrested Suspects.lnk
Thu Jun 14 2012 11:51:03   389120 ..c. r/rrwxrwxrwx 0        0        2114-128-3 C:/WINDOWS/system32/cmd.exe
Thu Jun 14 2012 11:51:08       48 m.c. d/drwxrwxrwx 0        0        25931-144-1 C:/Documents and Settings/XPMUser/Local Settings/Temp/TMP51B7AFEF
                           909824 .ac. r/rrwxrwxrwx 0        0        25932-128-4 C:/Documents and Settings/XPMUser/Local Settings/Temp/tmpD.tmp
Thu Jun 14 2012 11:51:09    37024 mac. r/rrwxrwxrwx 0        0        10351-128-4 C:/WINDOWS/Prefetch/CMD.EXE-087B4001.pf
                               56 m.c. d/drwxrwxrwx 0        0        10992-144-6 C:/Documents and Settings/XPMUser/Application Data/Microsoft
                              312 m.cb d/drwxrwxrwx 0        0        25933-144-1 C:/Documents and Settings/XPMUser/Application Data/Microsoft/Installer
                               48 ..c. d/drwxrwxrwx 0        0        25935-144-1 C:/Documents and Settings/XPMUser/Application Data/Microsoft/Installer/{5AAB219B-1B2B-4404-2F96-57347FF27294}
                            11008 .ac. r/rrwxrwxrwx 0        0        25936-128-3 C:/Documents and Settings/XPMUser/Local Settings/Temp/driverw.sys
```

FinFisher: infezione

- Infetta processi di sistema tra cui winlogon e svchost
- L'analisi delle stringhe contenute in memoria permette l'attribuzione

```
Process: winlogon.exe Pid: 424 Address: 0x1af0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 19, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x01af0000  4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00   MZ..............
0x01af0010  b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00   ........@.......
0x01af0020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x01af0030  00 00 00 00 00 00 00 00 00 00 00 00 f0 00 00 00   ................
```

```
00003960  47 4e 55 20 4d 50 3a 20  43 61 6e 6e 6f 74 20 61  |GNU MP: Cannot a|
00003970  6c 6c 6f 63 61 74 65 20  6d 65 6d 6f 72 79 20 28  |llocate memory (|
00003980  73 69 7a 65 3d 25 75 29  0a 00 00 00 47 4e 55 20  |size=%u)....GNU |
00003990  4d 50 3a 20 43 61 6e 6e  6f 74 20 72 65 61 6c 6c  |MP: Cannot reall|
000039a0  6f 63 61 74 65 20 6d 65  6d 6f 72 79 20 28 6f 6c  |ocate memory (ol|
000039b0  64 5f 73 69 7a 65 3d 25  75 20 6e 65 77 5f 73 69  |d_size=%u new_si|
000039c0  7a 65 3d 25 75 29 0a 00  79 3a 5c 6c 73 76 6e 5f  |ze=%u)..y:\lsvn_|
000039d0  62 72 61 6e 63 68 65 73  5c 66 69 6e 73 70 79 76  |branches\finspyv|
000039e0  34 2e 30 31 5c 66 69 6e  73 70 79 76 32 5c 73 72  |4.01\finspyv2\sr|
000039f0  63 5c 6c 69 62 73 5c 6c  69 62 67 6d 70 5c 6d 70  |c\libs\libgmp\mp|
00003a00  6e 2d 74 64 69 76 5f 71  72 2e 63 00 63 20 3d 3d  |n-tdiv_qr.c.c ==|
00003a10  20 30 00 00 00 00 00 00  01 02 03 03 04 04 04 04  | 0..............|
```

Persistenza

- Il malware modifica il MBR per rimanere persistente

y:\lsvn_branches\finspyv4.01\finspyv2\src\target\bootkit_x32driver\objfre_w2k_x86\i386\bootkit_x32driver.pdb

hackedteam / **vector-edk**

Watch 12 | Star 35 | Fork 145

Code | Issues 0 | Pull requests 0 | Projects 0 | Insights

Branch: master | vector-edk / vector-uefi / | Create new file | Find file | History

cod replaced "chipsec" Intel with "chipsec.efi" ... Latest commit 1ad0980 on 19 Mar 2015

..		
UEFITool-master	vector-uefi tools and source code	4 years ago
fd	replaced "chipsec" Intel with "chipsec.efi"	3 years ago
insyde	vector-uefi tools and source code	4 years ago
GenFfs.exe	vector-uefi tools and source code	4 years ago
Qt5Core.dll	vector-uefi tools and source code	4 years ago
UEFIExtract.exe	vector-uefi tools and source code	4 years ago
dropper.mod	first release based on chipsec/*python*	4 years ago

Antidebugging

- Utilizzo di diverse tecniche per eludere e rallentare l'analisi
- Se individua un debugger salta ad un indirizzo casuale
- Virtualized Packer

```
.text:00401683 finit
.text:00401686 fld ds:tbyte_40168E
.text:0040168C jmp short locret_401698
---------------------------
.text:0040168E tbyte_40168E dt 9.2233720368547758075e18
---------------------------
.text:00401698 locret_401698:
.text:00401698 retn
```

Raccolta dati

- Nella cartella C:\Windows\Installer\[random]\ , protetti da cifratura
- Screenshot, tasti premuti, conversazioni, password…

winlogon.exe	420	CreateFile	C:\WINDOWS\Installer\{49FD463C-18F1-63C4-8F12-49F518F127}\t111o00000000.dat	SUCCESS	Desired Access: Generic Write,
winlogon.exe	420	SetEndOfFileInformationFile	C:\WINDOWS\Installer\{49FD463C-18F1-63C4-8F12-49F518F127}\t111o00000000.dat	SUCCESS	EndOfFile: 0
winlogon.exe	420	SetAllocationInformationFile	C:\WINDOWS\Installer\{49FD463C-18F1-63C4-8F12-49F518F127}\t111o00000000.dat	SUCCESS	AllocationSize: 0
winlogon.exe	420	WriteFile	C:\WINDOWS\Installer\{49FD463C-18F1-63C4-8F12-49F518F127}\t111o00000000.dat	SUCCESS	Offset: 0, Length: 4,096
winlogon.exe	420	WriteFile	C:\WINDOWS\Installer\{49FD463C-18F1-63C4-8F12-49F518F127}\t111o00000000.dat	SUCCESS	Offset: 4,096, Length: 4,096
winlogon.exe	420	WriteFile	C:\WINDOWS\Installer\{49FD463C-18F1-63C4-8F12-49F518F127}\t111o00000000.dat	SUCCESS	Offset: 8,192, Length: 4,096
winlogon.exe	420	WriteFile	C:\WINDOWS\Installer\{49FD463C-18F1-63C4-8F12-49F518F127}\t111o00000000.dat	SUCCESS	Offset: 12,288, Length: 4,096
winlogon.exe	420	WriteFile	C:\WINDOWS\Installer\{49FD463C-18F1-63C4-8F12-49F518F127}\t111o00000000.dat	SUCCESS	Offset: 16,384, Length: 4,096
winlogon.exe	420	WriteFile	C:\WINDOWS\Installer\{49FD463C-18F1-63C4-8F12-49F518F127}\t111o00000000.dat	SUCCESS	Offset: 20,480, Length: 4,096
winlogon.exe	420	WriteFile	C:\WINDOWS\Installer\{49FD463C-18F1-63C4-8F12-49F518F127}\t111o00000000.dat	SUCCESS	Offset: 24,576, Length: 4,096
winlogon.exe	420	WriteFile	C:\WINDOWS\Installer\{49FD463C-18F1-63C4-8F12-49F518F127}\t111o00000000.dat	SUCCESS	Offset: 28,672, Length: 4,096
winlogon.exe	420	WriteFile	C:\WINDOWS\Installer\{49FD463C-18F1-63C4-8F12-49F518F127}\t111o00000000.dat	SUCCESS	Offset: 32,768, Length: 4,096
winlogon.exe	420	WriteFile	C:\WINDOWS\Installer\{49FD463C-18F1-63C4-8F12-49F518F127}\t111o00000000.dat	SUCCESS	Offset: 36,864, Length: 4,096
winlogon.exe	420	WriteFile	C:\WINDOWS\Installer\{49FD463C-18F1-63C4-8F12-49F518F127}\t111o00000000.dat	SUCCESS	Offset: 40,960, Length: 4,096
winlogon.exe	420	WriteFile	C:\WINDOWS\Installer\{49FD463C-18F1-63C4-8F12-49F518F127}\t111o00000000.dat	SUCCESS	Offset: 45,056, Length: 4,096
winlogon.exe	420	WriteFile	C:\WINDOWS\Installer\{49FD463C-18F1-63C4-8F12-49F518F127}\t111o00000000.dat	SUCCESS	Offset: 49,152, Length: 4,096
winlogon.exe	420	WriteFile	C:\WINDOWS\Installer\{49FD463C-18F1-63C4-8F12-49F518F127}\t111o00000000.dat	SUCCESS	Offset: 53,248, Length: 4,096
winlogon.exe	420	WriteFile	C:\WINDOWS\Installer\{49FD463C-18F1-63C4-8F12-49F518F127}\t111o00000000.dat	SUCCESS	Offset: 57,344, Length: 4,096
winlogon.exe	420	WriteFile	C:\WINDOWS\Installer\{49FD463C-18F1-63C4-8F12-49F518F127}\t111o00000000.dat	SUCCESS	Offset: 61,440, Length: 4,096
winlogon.exe	420	WriteFile	C:\WINDOWS\Installer\{49FD463C-18F1-63C4-8F12-49F518F127}\t111o00000000.dat	SUCCESS	Offset: 65,536, Length: 4,096

I problemi della cifratura

- La chiave è composta da 8 letture consecutive dell’indirizzo 0x7ffe0014 (orologio Windows Time Service)
- La risoluzione dell'orologio non è alta: ~15.6 millisecondi
- Non è implementato padding

```
00000200  ed ff c5 7e 0e 8e 17 4b  33 80 2f 9a 74 92 b6 50  |...~...K3./.t..P|
00000210  41 ba fc 1d 7f ce ff 52  cf 68 1f d1 ea 8a 3b 5d  |A......R.h....;]|
00000220  b5 1a fe eb eb 54 e2 4a  12 d1 24 33 60 cd 2e f6  |.....T.J..$3`...|
00000230  da dc 86 6a 56 c6 df 6d  b5 18 5c 96 14 a3 84 13  |...jV..m..\.....|
00000240  3e 27 25 dd 33 72 56 e8  be 5c e5 54 3a dc 96 e2  |>'%.3rV..\.T:...|
00000250  4f cc 3f e9 16 76 8b 6e  bf 61 73 40 2e 15 11 d7  |O.?..v.n.as@....|
00000260  73 a1 c6 12 c2 c6 7f 56  08 bb 37 50 5f 55 54 99  |s......V..7P_UT.|
00000270  d3 21 2c 59 2a 27 48 01  54 b5 45 a7 d7 b5 32 62  |.!,Y*'H.T.E...2b|
00000280  dd 15 fc 46 00 00 00 90  03 fe 00 ea e9 e8 ff 38  |...F...........8|
00000290  01 3a 64 e2 98 58 c7 e6  b7 96 7f 68 8d 1f 4e 09  |.:d..X.....h..N.|
000002a0  b1 9f 29 7f e4 dd e2 9f  b9 4b eb 3d 4b 4a 8b 42  |..).......K.=KJ.B|
000002b0  81 b5 6a 76 db d8 1c 36  ad a9 25 1f 40 b5 ef 69  |..jv...6..%.@..i|
000002c0  00 6e 00 53 00 70 00 79  00                      |.n.S.p.y.|
```

C&C

- Il sample contatta un IP del Bahrain
- Comunica sulle porte 22, 53, 80, 443, 4111

TCP Conversations - Filter: ip.addr == 77.69.140.194

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A->B	Bytes A->B	Packets A<-B	Bytes A<-B	Rel Start	Duration	bps A->B	bps A<-B
192.168.131.65	1200	77.69.140.194	53	3	186	3	186	0	0	46.533336000	8.9749	165.80	N/A
192.168.131.65	1212	77.69.140.194	53	3	186	3	186	0	0	229.148416000	8.9776	165.75	N/A
192.168.131.65	1217	77.69.140.194	53	3	186	3	186	0	0	447.436820000	8.9725	165.84	N/A
192.168.131.65	1204	77.69.140.194	80	15	1767	8	1273	7	494	101.999621000	2.0481	4972.45	1929.61
192.168.131.65	1205	77.69.140.194	80	15	1767	8	1273	7	494	134.195659000	2.0208	5039.53	1955.64
192.168.131.65	1181	77.69.140.194	22	25	5489	13	4387	12	1102	15.101931000	2.5512	13756.79	3455.66
192.168.131.65	1202	77.69.140.194	80	25	5225	13	4387	12	838	68.840833000	2.7173	12915.95	2467.19
192.168.131.65	1207	77.69.140.194	80	56	7266	27	4312	29	2954	166.481391000	32.9779	1046.04	716.60
192.168.131.65	1213	77.69.140.194	443	1710	1270075	597	59063	1113	1211012	251.429902000	193.7304	2438.98	50008.13
77.69.140.194	4111	192.168.131.65	1219	15660	4766223	8258	498554	7402	4267669	469.714476000	196.8652	20259.71	173425.05

Fonti

- The Citizen Lab, University of Toronto, Morgan Marquis Boire, From Bahrain With Love: FinFisher's Spy Kit Exposed?

  https://citizenlab.ca/2012/07/from-bahrain-with-love-finfishers-spy-kit-exposed/
- https://www.sans.org/event/san-francisco-summer-2018/course/reverse-engineering-malware-malware-analysis-tools-techniques
- https://zeltser.com/introductory-malware-analysis-webcasts/
- https://countuponsecurity.com/2015/03/16/memory-forensics-with-volatility-on-remnux-v5-part-1/