



Complex malware & forensic investigation

Hackito Ergo Sum 2015 – Paul Rascagneres & Sebastien Larinier

Me: Paul Rascagnères

Twitter account: @r00tbsd

Senior threat researcher at CERT SEKOIA

Author of the French book

"Malwares - Identification, analyse et eradication"
(ISBN: 978-2746079656)

Co-Organizer of Botconf (2-4 December – Paris)

Located in our offices in Luxembourg & Paris

Complex malware & forensics investigation | about us

Me: Sebastien Larinier

Twitter account: @sebdraven

Digital Forensics and Incidence Response at
CERT SEKOIA

Member of the Honeyynet Project

Co-Organizer of Botconf (2-4 December – Paris)

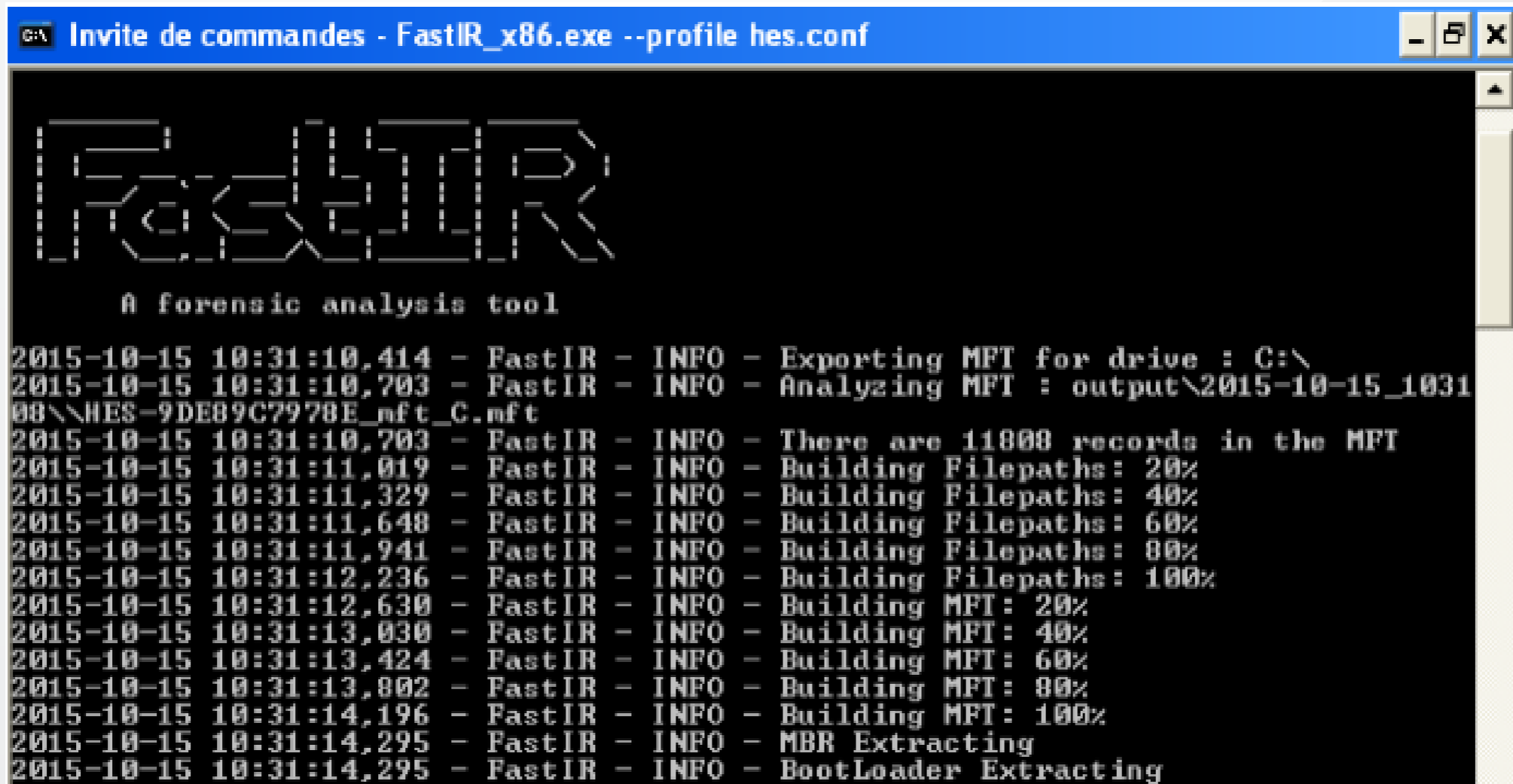
Located in Paris

What is FastIR Collector?

FastIR Collector:

- Open Source project sponsored by SEKOIA
- http://github.com/SekoiaLab/Fastir_Collector
- release du HES 2015
- configurable forensic collector
- standalone
- 32/64b
- Windows XP -> 8.1 (Workstation & Server)

FastIR Collector:



```
Invite de commandes - FastIR_x86.exe --profile hes.conf

FastIR
A forensic analysis tool

2015-10-15 10:31:10,414 - FastIR - INFO - Exporting MFT for drive : C:\
2015-10-15 10:31:10,703 - FastIR - INFO - Analyzing MFT : output\2015-10-15_1031
00\HES-9DEB9C7978E_mft_C.mft
2015-10-15 10:31:10,703 - FastIR - INFO - There are 11800 records in the MFT
2015-10-15 10:31:11,019 - FastIR - INFO - Building Filepaths: 20%
2015-10-15 10:31:11,329 - FastIR - INFO - Building Filepaths: 40%
2015-10-15 10:31:11,648 - FastIR - INFO - Building Filepaths: 60%
2015-10-15 10:31:11,941 - FastIR - INFO - Building Filepaths: 80%
2015-10-15 10:31:12,236 - FastIR - INFO - Building Filepaths: 100%
2015-10-15 10:31:12,630 - FastIR - INFO - Building MFT: 20%
2015-10-15 10:31:13,030 - FastIR - INFO - Building MFT: 40%
2015-10-15 10:31:13,424 - FastIR - INFO - Building MFT: 60%
2015-10-15 10:31:13,802 - FastIR - INFO - Building MFT: 80%
2015-10-15 10:31:14,196 - FastIR - INFO - Building MFT: 100%
2015-10-15 10:31:14,295 - FastIR - INFO - MBR Extracting
2015-10-15 10:31:14,295 - FastIR - INFO - BootLoader Extracting
```

Collected artefacts:

- MFT
- MBR
- RAM
- HDD
- processes
- named pipes
- MRU
- recent docs
- event logs
- prefetch
- drives
- browsers history
- recycle bin
- startups
- shellbags
- + FileCatcher
 - files collect
 - hashes
 - ...
- ...

Filecatcher description

```
[filecatcher]
  recursively=True
  path=c:\tmp|*,c:\temp|*,c:\recycler|*,%WINDIR%|*,%USERPROFILE%|*
  mime_filter=application/msword;application/octet-stream;application/xarchive;application/x-ms-pe;application/x-ms-dosexecutable;application/x-lha;application/x-dosexec;application/xelc;application/x-executable, statically linked, stripped;application/x-gzip;application/x-object, not stripped;application/x-zip;
  mime_zip=application/x-ms-pe;application/x-ms-dosexecutable;application/x-dosexec;application/x-executable, statically linked, stripped
  compare=AND
  size_min=6k
  size_max=100M
  ext_file=*
  zip_ext_file=*
  zip=True
```


Filecatcher description + signature filter
Yara support



What is the goal of this talk?

Use on real cases such as:

- rootkit
- bootkit
- userland RAT
- ...

Provide a document with a detailed description of each case studies on our blog:

<http://sekoia.fr/blog/fastir-collector-on-advanced-threats/>



Case studies

Case 1: Uroburos/Turla/Snake

Malware description:

- rootkit publicly released in 02/2014
- probably state sponsored
- it uses 2 Virtual File Systems
- hides itself (driver file .sys + registry)

Live forensics collect on this kind of case is always complicated: we cannot trust the system behavior

FastIR Collector:

Driver identification via the filecatcher (.zip + _Filecatcher.csv):

```
paul@lab:~$ unzip -l HES-demo_files_.zip
```

```
Archive:  HES-demo_files_.zip
```

Length	Date	Time	Name
210944	2015-10-08	11:07	WINDOWS/\$NtuninstallQ817473\$/fdisk.sys
224768	2007-11-06	19:23	WINDOWS/WinSxS/x86_Microsoft.VC90/msvcm90.dll
59904	2007-11-06	21:51	WINDOWS/WinSxS/x86_Microsoft.VC90/mfc90.dll
59904	2007-11-06	21:51	WINDOWS/WinSxS/x86_Microsoft.VC90/mfc90u.dll
555520			4 files

```
"HES-demo", "Filecatcher", "2015-10-08 11:07:40.763156",  
"C:\WINDOWS\NtuninstallQ817473$\fdisk.sys",  
"50edc955a6e8e431f5eceb5b1d3617d3606b8296f838f0f986a929653d289ed ",  
"application/x-ms-dosexecutable", "True", "False",  
http://www.virustotal.com/en/file/50edc955a6e8e431\[...\]929653d289ed/analysis
```

FastIR Collector:

Persistence identification (_startup.csv):

```
"HES-demo", "registry_services", "2015-10-15 10:28:32",  
"HKEY_LOCAL_MACHINE",  
"System\CurrentControlSet\Services\Ultra3", "ImagePath",  
"VALUE", "REG_SZ",  
"\SystemRoot\$\Ntuninstall1Q817473$\fdisk.sys"
```

FastIR Collector:

Named pipe identification (_named_pipes.csv):

```
"HES-demo", "named_pipes", "\\.\pipe\isapi_http2"  
"HES-demo", "named_pipes", "\\.\pipe\isapi_dg2"  
"HES-demo", "named_pipes", "\\.\pipe\isapi_http"  
"HES-demo", "named_pipes", "\\.\pipe\isapi_dg"
```

FastIR Collector:

VFS identification (_prefetch.csv):

```
\DEVICE\RAWDISK1\KLOG  
\DEVICE\RAWDISK1\$_MFT  
\DEVICE\RAWDISK1\QUEUE
```


Case 2: ComRAT

Malware description:

- user land RAT
- developed by the same author than Uroburos
- uncommon persistence (COM Object hijack)

FastIR Collector:

Malware identification (.zip):

```
paul@lab:~$ unzip -l HES-demo_files.zip
  Length      Date    Time    Name
-----
 260096  2008-04-14 14:00  Documents and Settings/demo
/Application Data/Microsoft/credprov.tlb
  51200  2008-04-14 14:00  Documents and Settings/demo
/Application Data/Microsoft/shdocvw.tlb
 224768  2007-11-06 19:23  WINDOWS/WinSxS/x86_Microsoft
.VC90/msvcm90.dll
  59904  2007-11-06 21:51  WINDOWS/WinSxS/x86_Microsoft
.VC90/mfcm90.dll
  59904  2007-11-06 21:51  WINDOWS/WinSxS/x86_Microsoft
.VC90/mfcm90u.dll
```

FastIR Collector:

Persistence identification not visible...

```
HKCU\Software\CLSID\{42aedc87-2188-41fd-b9a30c966feabec1}\InprocServer32
```

FastIR Collector:

Library injection (_processes_dll.csv):

```
"HES-demo", "processes_dll", "1420", "C:\WINDOWS\Explorer.EXE"  
,"C:\Documents and Settings\demo\Application Data\Microsoft  
\shdocvw.tlb"
```

```
"HES-demo", "processes_dll", "1420", "C:\WINDOWS\Explorer.EXE"  
,"C:\Documents and Settings\demo\Application Data\Microsoft  
\credprov.tlb"
```


Case 3: Babar

Malware description:

- user land RAT
- probably developed by a French intel agency

FastIR Collector:

Persistence identification (_startup.csv)

```
"HES-demo", "startup", "2015-10-08 11:20:21",  
"HKEY_LOCAL_MACHINE", "Software\Microsoft\Windows  
\CurrentVersion\Run ", "MSSecurity", "VALUE", "REG_SZ",  
""regsvr32.exe" /s /n /i "C:\Documents and Settings  
\All Users\Application Data\perf_585.dll""
```

FastIR Collector:

Process identification (_processes.csv)

```
"HES-demo", "processes", "1828", "regsvr32.exe",  
"" "C:\WINDOWS\system32\regsvr32.exe" /s /n /i  
"" "C:\Documents and Settings\All Users\Application Data  
\perf_585.dll""", "C:\WINDOWS\system32\regsvr32.exe"
```

FastIR Collector:

Library injection (_processes_dll.csv)

```
"HES-demo", "processes_dll", "1440", "C:\WINDOWS\Explorer.EXE",  
"C:\Documents and Settings\All Users\Application Data\  
perf_585.dll"
```

```
"HESdemo", "processes_dll", "1788", "C:\WINDOWS\system32\  
VBoxTray.exe", "C:\Documents and Settings\All Users\  
Application Data\perf_585.dll"
```

```
"HESdemo", "processes_dll", "1848", "C:\WINDOWS\system32\  
ctfmon.exe", "C:\Documents and Settings\All Users\  
Application Data\perf_585.dll"
```


Case 4: Casper

Malware description:

- user land RAT
- probably developed by the same team than Babar

FastIR Collector:

Persistence identification (_startup.csv)

```
"HES-demo", "startup", "2015-10-08 11:30:07",  
"HKEY_LOCAL_MACHINE", "Software\Microsoft\Windows  
\CurrentVersion\Run ", "VBOX Audio Interface Device  
Manager", "VALUE", "REG_SZ", "" "C:\Program Files\  
Fichiers communs\VBOX Audio Interface Device Manager  
\aiomgr.exe"" 3071006457"
```

FastIR Collector:

Filecatcher doesn't detect the file because it is stored in "Program Files" and this directory is not scanned by default.

Case 5: Poweliks

Malware description:

- user land RAT
- first file less malware
- entirely in registry
- uses non-ASCII characters

FastIR Collector:

Persistence identification (_startup.csv)

```
"PC-demo", "startup", "2015-10-08 14:28:18", "HKEY_USERS",  
"S-1-5-21-2108495583517838646-14091684911000\Software\  
Microsoft\Windows\CurrentVersion\Run", "\x01\x00\x01",  
"VALUE", "REG_SZ", "rundll32.exe javascript:""\..\mshtml,  
RunHTMLApplication "";document.write("""\74script language=  
jscript.encode>""+(new%20ActiveXObject("""WScript.Shell""))  
.RegRead(" HKCU\\software\\microsoft\\windows\  
currentversion\\run\\"""")+"""\74/script>"" )"
```

```
"PC-demo", "startup", "2015-10-08 14:28:18", "HKEY_USERS",  
"S-1-5-21-2108495583517838646-14091684911000\Software\  
Microsoft\Windows\CurrentVersion\Run", "", "VALUE", "REG_SZ",  
"#@~^ kXcAAA==W!x^DkKxP^WTcV* ODH ax +h,)mDkp64N+1YcJ\dX:s  
SEKOIA  
Cj+M\n.oHSuP:n vcTr#IXRKw+ `r!2:JSJ4Y02=zz6C+(NGc^G:JVKo35
```

Case 6: HDRoot

Malware description:

- bootkit (infects the MBR)
- not “really” a malware

FastIR Collector:

MBR collect in raw or with the ASM code:
`bootloaderAssemblyCode.txt`

FastIR Collector:

MBR compromise identification

Before:

```
00: 33c0    XOR AX, AX
02: 8ed0    MOV SS, AX
04: bc007c MOV SP, 0x7c00
07: 8ec0    MOV ES, AX
09: 8ed8    MOV DS, AX
0b: be007c MOV SI, 0x7c00
0e: bf0006 MOV DI, 0x600
11: b90002 MOV CX, 0x200
14: fc     CLD
```

After:

```
00: 33c0    XOR AX, AX
02: 8ed0    MOV SS, AX
04: bc007c MOV SP, 0x7c00
07: eb69    JMP 0x72
09: 8ed8    MOV DS, AX
0b: be007c MOV SI, 0x7c00
0e: bf0006 MOV DI, 0x600
11: b90002 MOV CX, 0x200
14: fc     CLD
```



Conclusion

FastIR Collector:

- is not perfect
- some artifacts are missing

But:

- it's open source: feel free to open issues, requests...
- it's maintained
- it's really use during incident response

**We would like to thank the
members of the SEKOIA's CERT**



Thank you for your attention.

Questions or awkward silence?