# Complex malware & forensic investigation

CoRI&IN 2016 – 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

Located in our offices in Luxembourg & Paris

Me: Sebastien Larinier
Twitter account: @sebdraven

Digital Forensics and Incidence Response at CERT SEKOIA

Member of the Honeynet Project

Co-Organizer of Botconf

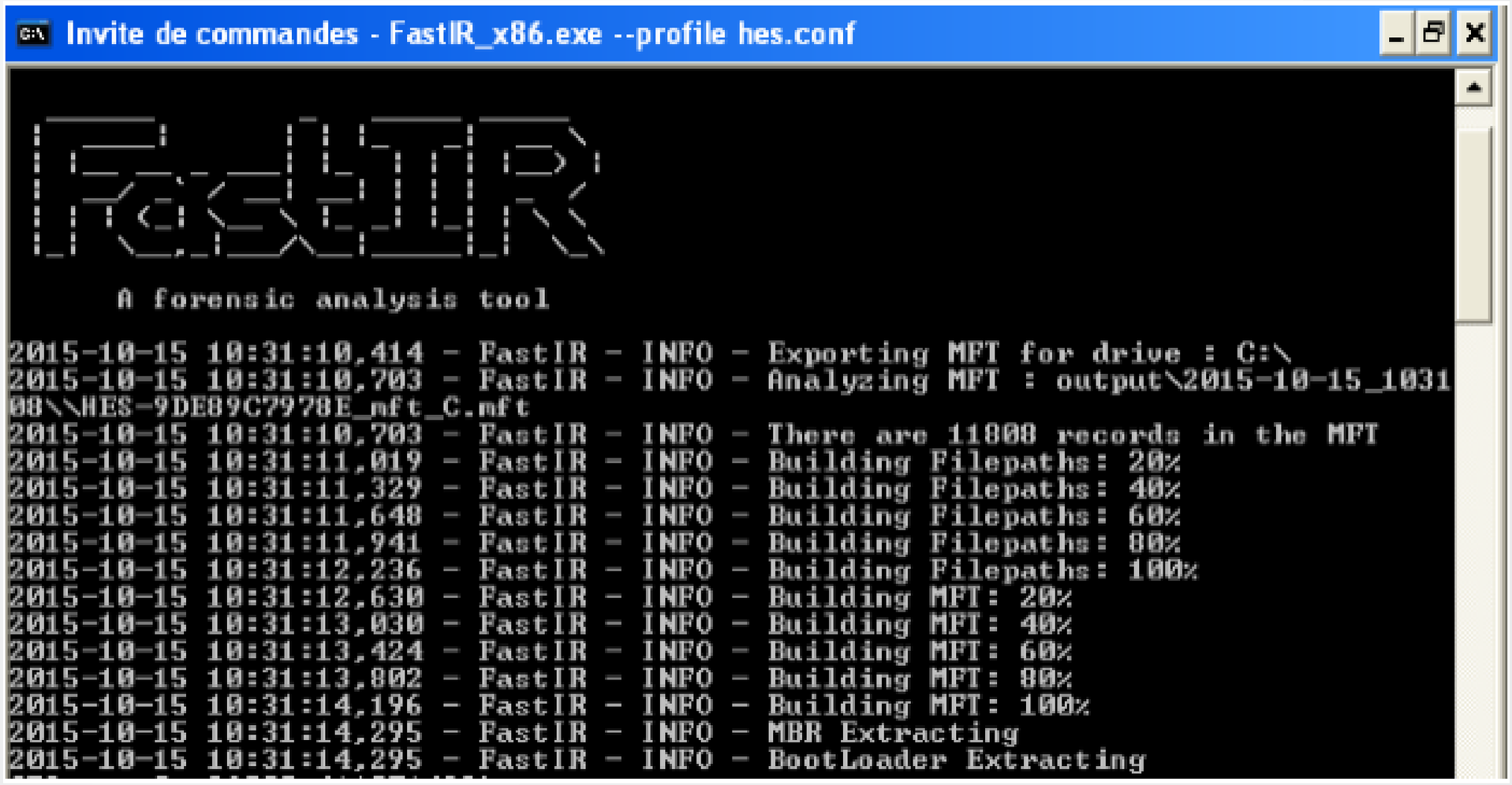
Located in Paris

# What is FastIR Collector?

FastIR Collector:

- Open Source project sponsored by SEKOIA
- http://github.com/SekoiaLab/FastIR_Collector
- configurable forensic collector
- standalone
- 32/64b
- Windows XP -> 10 (Workstation & Server)

# FastIR Collector:



# 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;applica
tion/x-lha;application/x-dosexec;application/xelc;application/x-exec
utable, statically linked, stripped;application/x-gzip;application/x
-object, not stripped;application/x-zip;
 mime_zip=application/x-ms-pe;application/x-ms-dosexecutable;applica
tion/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

# 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://www.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/mfcm90.dll
    59904  2007-11-06 21:51   WINDOWS/WinSxS/x86_Microsoft.VC90/mfcm90u.dll
---------                     -------
   555520                     4 files
```

```
"HES-demo","Filecatcher","2015-10-08 11:07:40.763156",
"C:\WINDOWS\$NtuninstallQ817473$\fdisk.sys",
"50edc955a6e8e431f5ecebb5b1d3617d3606b8296f838f0f986a929653d289ed ",
"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\$NtuninstallQ817473$\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-1-5-21-2108495583517838646-1409168491l000\Software\
Microsoft\Windows\CurrentVersion\Run","\x01\x00\x01",
"VALUE","R EG_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-1-5-21-2108495583517838646-1409168491l000\Software\
Microsoft\Windows\CurrentVersion\Run","","VALUE","REG_SZ",
"#@~^ kXcAAA==W!x^DkKxP^WTcV* ODH ax +h,)mDkp64N+1YcJ\dX:s
cj+M\n.oHSuP:n vcTr#IXRKw+ `r!2:JSJ4YO2=zz6C+(NGc^G:JVKo_
```

# 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
```

# CoRI&IN release…

# CoRI&IN release…

# Linux collector

FastIR Collector Linux:

- Open Source project sponsored by SEKOIA
- https://github.com/SekoiaLab/Fastir_Collector_Linux
- standalone
- 32/64b
- it works probably on MacOS

# Collected artefacts:

- Kernel version
- Network interfaces
- hostname
- Distribution version
- Last Logins
- Connections
- Handles
- Hidden files
- SSH know_host
- /tmp
- Autoruns (*.d+cron)
- List of partitions
- MBR
- File information
- ...

# 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 thanks the members of the SEKOIA CERT who use/correct/comment/… our collector since years now!!

# Thank you for your attention.

# Questions or awkward silence?