



# Lutte Informatique Défensive

## SOC, CERT et CTI

Georges Bossert - SEKOIA  
Frédéric Guihéry - AMOSSYS

*15 janvier 2019 - Université Rennes 1*



# L'analyse forensique

---



# Introduction

- Le périmètre de l'analyse forensique
  - L'analyse des logs
  - L'analyse des disques
  - L'analyse de mémoires
  - L'analyse de flux réseau
  - L'analyse de malwares



# Remote live forensic vs Forensic post-mortem

Question : quels avantages et inconvénients pour ces deux méthodes ?



# Remote live forensic vs Forensic post-mortem

- **Forensic post mortem** : poste éteint, copie de disques et mémoires
  - Avantages : altération impossible, carving possible (fichiers supprimés / accès RAW disque), toutes les données sont disponibles
  - Inconvénients : débranchement du poste (sauf en cas de ransomware), lent, passage à l'échelle difficile
- **Remote live forensic** : accès distant sur poste en cours de fonctionnement
  - Avantages : pas d'interruption du poste, rapide, déployable sur un parc
  - Inconvénients : altération possible (pendant l'acquisition / après), données incomplètes
- A adapter en fonction du contexte
  - Incident terminé / en cours
  - But recherché



# Remote live forensic

- Automatisation du déploiement (exemple : GPO sous Windows)
- Automatisation de l'extraction/la recherche d'information sur un ensemble de machines
- Recherche d'IOC en mémoire
  - Inconvénient : l'IOC est transmis à une cible potentiellement infectée
- Outils : Mozilla MIG, Google Grr, les produits de type EDR, etc.

# Remote Live Forensic : Google GRR

Récupération de données à distance sur un parc de machines

GRR Response Rig User: admin

WIN-JTWK71ONUX4  
Status: ● 9 minutes ago.  
ip-10-204-62-88.ec2.internal  
Host Information

**Start new flows**

Browse Virtual Filesystem  
Manage launched flows  
Advanced ▾  
Client Performance Stats  
Crashes  
Debug Client Requests

MANAGEMENT

Automated flows  
Cron Job Viewer  
Hunt Manager  
Show Statistics  
Start Global Flows  
Advanced ▾

CONFIGURATION

Manage Binaries  
Settings

- Administrative
- Browser
  - CacheGrep
  - ChromeHistory
  - ChromePlugins
  - FirefoxHistory
- Collectors
  - ArtifactCollectorFlow**
  - KnowledgeBaseInitiali
- FileTypes
- Filesystem
  - Fetch Files
  - Find Files
  - FingerprintFile
  - GetFile
  - GetMBR
  - ListDirectory
  - ListVolumeShadowCo
  - RecursiveListDirector
  - Search In Files
  - SendFile
  - SlowGetFile
- Memory
- Misc
- Network
- Processes
  - GetProcessesBinaries
  - GetProcessesBinaries
  - ListProcesses
- Registry
- Services
- Timeline

Artifact list

Search

Windows

- TerminalServicesEventLogEvtx
- UserShellFolders
- VolatilityPsList
- WMIProcessList
- WinCodePage
- WinDirEnvironmentVariable
- WinDomainName
- WinHostsFile
- WinPathEnvironmentVariable
- WinTimeZone
- WindowsAdminUsers
- WindowsDrivers**
- WindowsHotFixes
- WindowsLoginUsers
- WindowsPersistenceMechanism
- WindowsRegistryProfiles
- WindowsRunKeys

Add Add all Clear Remove

**SecurityEventLogEvtx**

SophosWinQuarantineFiles  
WindowsDrivers

Windows Security Event Log for Vista or newer systems.

Labels	Logs
Platforms	Windows
Conditions	VistaOrNewer
Dependencies	environ_systemroot
Links	<a href="http://www.forensicswiki.org/wiki/Window">http://www.forensicswiki.org/wiki/Window</a>
Output Type	StatEntry

**Artifact Collectors**

Action	GetFile
arg:path	%%environ_systemroot%%\System3

**Artifact Processors**

None

Flow Information Current Running Flows

**ArtifactCollectorFlow**

Flow that takes a list of artifacts and collects them.

# Remote Live Forensic : Google GRR

Accès aux systèmes de  
fichiers à distance

GRR Response Rig

User: admin

WIN-JTWK71ONUX4

Status: ● 1 seconds ago.

 ip-10-204-62-

88.ec2.internal

[Host Information](#)

[Start new flows](#)

[Browse Virtual Filesystem](#)

[Manage launched flows](#)

[Advanced ▾](#)

[Client Performance  
Stats](#)

[Crashes](#)

[Debug Client Requests](#)

**MANAGEMENT**

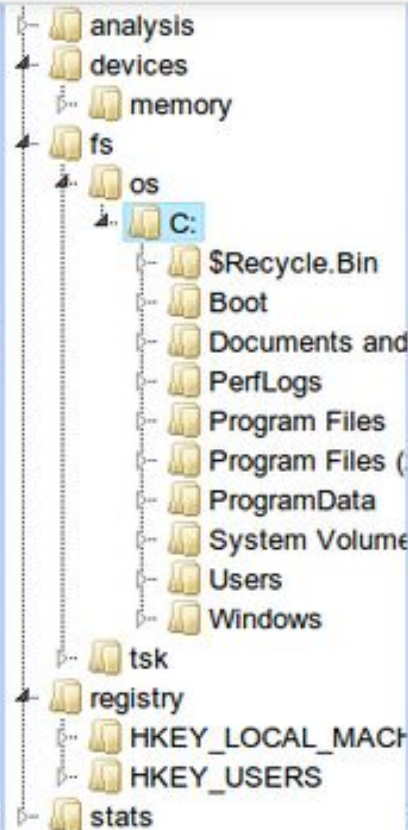
[Automated flows](#)

[Cron Job Viewer](#)














[Hunt Manager](#)

[Show Statistics](#)

[Start Global Flows](#)



/ > fs > os > C:

Icon	Name	type	size	stat.st_size	stat.st_mtime
	\$Recycle.Bin	VFSDirectory	0	0	2013-11-14 07:12:36
	BOOTSECT.BAK	VFSBlobImage	8192	8192	2009-11-13 12:23:33
	Boot	VFSDirectory	0	4096	2009-11-13 12:23:33
	Documents and Settings	VFSDirectory	0	0	2012-02-26 02:42:25
	PerfLogs	VFSDirectory	0	0	2008-01-19 10:11:20
	Program Files	VFSDirectory	0	4096	2012-12-08 18:33:14
	Program Files (x86)	VFSDirectory	0	4096	2013-09-10 22:43:30
	ProgramData	VFSDirectory	0	4096	2012-12-08 18:36:21
	System Volume Information	VFSDirectory	0	0	2012-02-26 02:44:46
	Users	VFSDirectory	0	4096	2013-11-14 07:12:15
	Windows	VFSDirectory	0	16384	2013-11-14 07:06:18
	bootmgr	VFSFile	0	333257	2009-04-11 16:13:10
	hiberfil.sys	VFSFile	0	644472832	2013-11-14 07:04:20



# Remote Live Forensic : Google GRR

Recherche d'IOC  
en mémoire sur  
un parc

GRR Response Rig

User: admin

WIN-JTWK71ONUX4

Status: ● 1 minutes ago.

ip-10-204-62-88.ec2.internal

Host Information

Start new flows

Browse Virtual Filesystem

Manage launched flows

Advanced ▾

Client Performance Stats

Crashes

Debug Client Requests

MANAGEMENT

Automated flows

Cron Job Viewer

Hunt Manager

Show Statistics

Start Global Flows

Advanced ▾

CONFIGURATION

Manage Binaries

Settings

+

▶

⏸

⚙

Status	Hunt ID	Name	Start Time	Expires	Client Limit	Creator	Description
⏪	hunts/W:602FA2FD	GenericHunt	2013-11-18 07:39:08	2013-12-19 07:39:12	0	admin	Scan memory for bad string 1
⏸	hunts/W:E2890D	GenericHunt	2013-11-18 07:38:09	2013-11-18 07:38:09	0	admin	This is a hunt to start any flow on multiple clients.

View hunt details

Name

Hunt ID

Hunt URN

Creator

Client Limit

Client Count

Outstanding

Completed

Total CPU seconds used

Total network traffic

Arguments

GenericHunt

W:602FA2FD

aff4:/hunts/W:602FA2FD

admin

0

0

0

0

0.00

0 bytes

args	Flow args	Grep	Literal	testtesttest
	Flow runner args	Flow name	ScanMemory	
		Hunt name	GenericHunt	
		Description	Scan memory for bad string 1	
		Regex rules	Attribute regex	Windows
			Attribute name	System
			Username	admin
			Reason	
		Token	Expiry	294247-01-10 04:00:54
			Source ips	::ffff:74.125.56.17
			Process	GRRAdminUI
	backtrace	None		



# Analyse des logs

- Les étapes
  - Collecte des logs sur les équipements (si aucun SIEM/collecteur en place)
    - C:\Windows\System32\winevt\Logs\\*.evtx
  - Filtrage sur les événements importants (création de processus, tentatives de connexion, créations de service, etc.)
  - Identification des événements suspects
  - Qualification des événements suspects
  - Reconstruction de la chronologie (*timeline*) des événements suspects qualifiés



# Analyse des logs : détection de mouvements latéraux

- Techniques d'attaques et éléments d'investigation
  - psExec (version Metasploit)
    - Fonctionnement
      - Création d'un exécutable malveillant
      - Connexion sur le partage caché ADMIN\$ sur le système distant via SMB
      - Dépôt de l'exécutable sur le partage
      - Utilisation du mécanisme Service Control Manager (SCM) pour lancer un service
      - Chargement en mémoire de l'exécutable par le service, puis exécution
      - Mécanisme de communication possible avec la source
    - Détectable avec l'Event ID 7045 (service install)



# Analyse des logs : détection de mouvements latéraux

- Techniques d'attaques et éléments d'investigation
  - WMI (Windows Management Instrumentation)
    - Fonctionnement
      - Exécution de commandes à distance avec utilitaire wmic
      - Pas de dépôt de fichier sur le disque ni création d'un nouveau service (donc plus difficile à détecter qu'un psExec)
    - Détectable avec Sysmon (ID WmiEvent 19, 20 et 21)



# Analyse des logs : détection de mouvements latéraux

- Techniques d'attaques et éléments d'investigation
  - WinRM (Windows Remote Management)
    - Event ID 4656 et 4658 (création d'un handle sur une ressource spécifique)
  - Powershell
    - Event ID 1 et 5 avec exécution du processus "wsmpvhost.exe"
  - Copie de malwares sur point de montage distant
    - Event ID 4624 / 4672 (successful network logon as admin)
    - Event ID 5140 (share mount)

Ressource très complète sur les mécanismes de mouvements latéraux, et les moyens de détection : [https://www.jpccert.or.jp/english/pub/sr/20170612ac-ir\\_research\\_en.pdf](https://www.jpccert.or.jp/english/pub/sr/20170612ac-ir_research_en.pdf)

# Analyse des logs : détection de mouvements latéraux

Event ID 4624 en détails



**Timestamp = 2015-02-14 12:00:00**

**Event ID = 4624**

SubjectUserSid = S-1-0-0

SubjectUserName = -

SubjectDomainName = -

SubjectLogonId = 0x0000000000000000

TargetUserSid = S-1-5-21-2723264887-207281631-482592677-2984

**TargetUserName = imowned**

**TargetDomainName = MYDOM**

TargetLogonId = 0x000000021457dbab

**LogonType = 3**

LogonProcessName = Kerberos

AuthenticationPackageName = Kerberos

WorkstationName =

LogonGuid = {726F6B9E-C1BE-4EC1-BB95-3B0B6238BE56}

TransmittedServices = -

LmPackageName = -

KeyLength = 0

ProcessId = 0x0000000000000000

ProcessName = -

**IpAddress = 10.1.1.10**

IpPort = 3005

Heure de  
connexion

Compte utilisé

Domaine ciblé

IP source

# Analyse de supports de stockage

- Les étapes
  - Copie de disque
    - Copie parfaite, sans altérer le disque initial (mécanisme WriteProtect)
  - Analyse des partitions
    - Identification et accès aux partitions (FAT, NTFS, ext2/3/4, ...)
  - Analyse des fichiers
    - Si partition connue, parcours du système de fichiers
    - Sinon, reconstruction des fichiers à partir des données brutes (*file carving*)
    - Identification de fichiers cachés
  - Identification de fichiers supprimés





# Analyse de supports de stockage

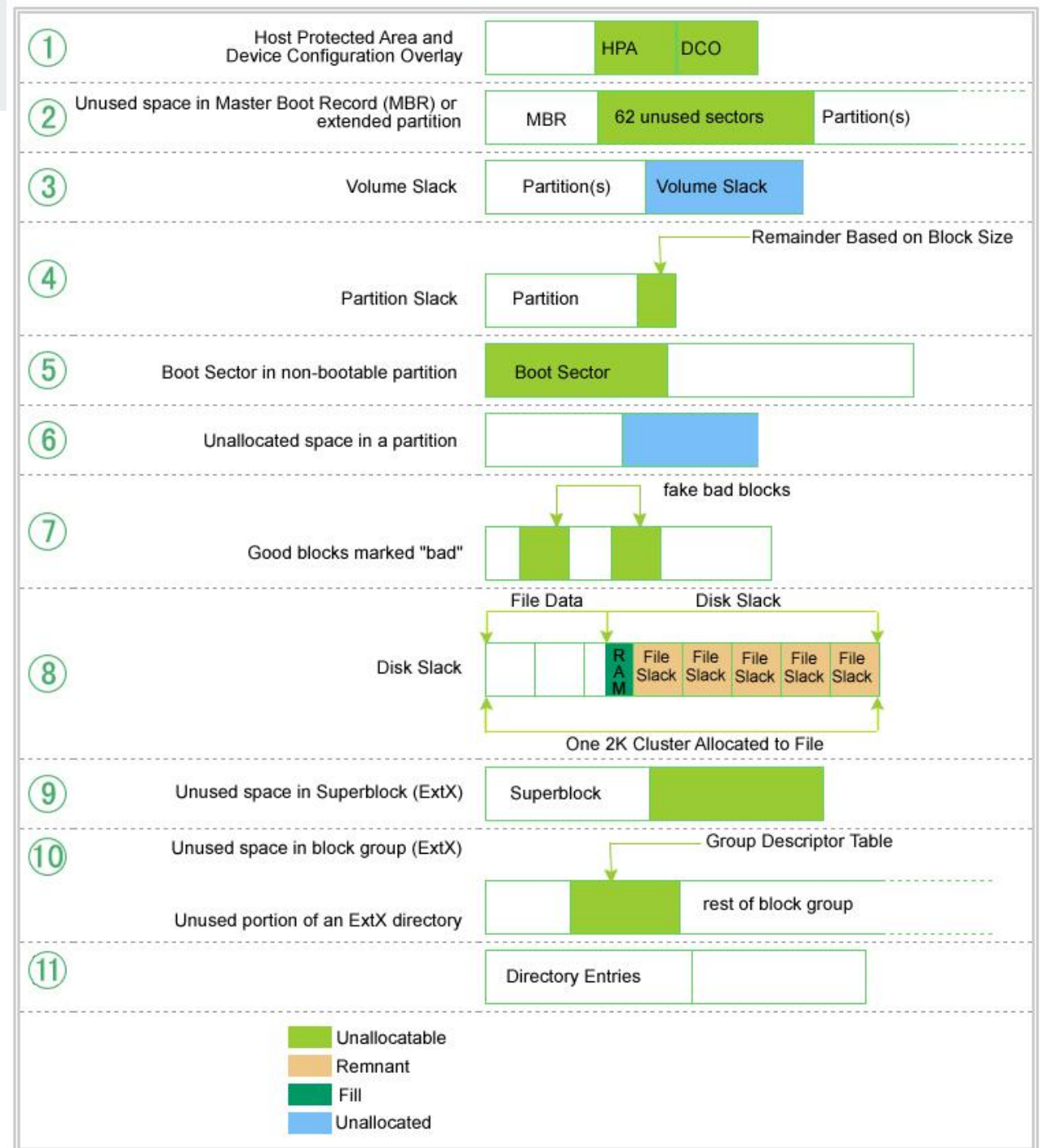
Point d'attention : il existe de nombreux  
moyens de cacher de l'information sur un  
disque

**Question : lesquels ?**



# Analyse de supports de stockage

Point d'attention : il existe de nombreux moyens de cacher de l'information sur un disque



# Analyse de supports de stockage

## Reconstruction de la chronologie de l'activité sur un poste (outil Autopsy)

Display Times In: ☒ Local Time Zone ☐ GMT / UTC

Mode: ☒ Counts ☒ Details ☐ snapshot

Layout Options: ☐ Band by Type ☐ One Event Per Row

Truncate Descriptions to (px):

Zoom History:

Time Units:

Event Type:

Description Detail:

Filters Events

☐ Hide Known Files

☒ Text Filter

☒ Event Type Filter

☒ File System ☐ Web Activity

Start: Mar 10, 2012 2:00:00 PM End: Mar 11, 2012 12:00:00 AM

1970-01-16 04:50:24 to 1970-01-16 04:50:25

Icon	Date/Time	Event ID	File ID	Result ID	Base Type	Sub Type	Known	Desc
	2012-03-10 19:19:23	39681	13409		File System	File Accessed	KNOWN	/img_...
	2012-03-10 19:23:39	44289	14759		File System	File Accessed	KNOWN	/img_...
	2012-03-10 19:23:25	57347	18428		File System	File Changed	KNOWN	/img_...
	2012-03-10 19:23:37	44165	14720		File System	File Accessed	KNOWN	/img_...
	2012-03-10 19:23:39	44169	14721		File System	File Accessed	KNOWN	/img_...

img\_xp-sp3-v3.001/vol\_vol2/Documents and Settings (432)

img\_xp-sp3-v3.001...vol2/WINDOWS (78)

img\_xp-sp3-v3.001/vol\_vol2/Documents and Settings (1576)

C:\Documents and Settings\John (5)

C:\Documents and Settings\John\My Documents (6)

img\_xp-sp3-v3.001/vol\_vol2/Program Files (135)

doubleclick.net (1)

78

Hex Strings Metadata Results Text Media



# Analyse de supports de stockage

## Reconstruction de la chronologie d'une attaque à partir d'une analyse disque (outil log2timeline)

# Spearphishing Attack SuperTimeline

Spear Phish Email Received w/Java Applet attack  
w/PDF and link (Email was about IRS w-2 tax forms)  
The victim clicked on the link <http://bit.ly/GEUMQQ>

4/2/2012	20:32:52	MACB	Firefox 3 history	http://bit.ly/GEUMQQ ( [count: 2] Host: bit.ly (URL not typed directly) type: LINK
4/2/2012	20:32:52	MACB	Firefox 3 history	http://207.58.245.179/ (Internal Revenue Service) [count: 2] visited from: http://bit.ly/GEUMQQ (URL not typed directly) type: REDIRECT_PERMANENT
4/2/2012	20:32:57	M.CB	NTFS \$MFT	C:/WINDOWS/Sun/Java/Deployment
4/2/2012	20:32:57	M.CB	NTFS \$MFT	C:/WINDOWS/Sun
4/2/2012	20:32:57	M.CB	NTFS \$MFT	C:/WINDOWS/Sun/Java
4/2/2012	20:32:58	MACB	NTUSER key	Key name: HKEY_USER/Software/JavaSoft
4/2/2012	20:32:58	MACB	NTUSER key	Key name: HKEY_USER/Software/JavaSoft/JavaRuntimeEnvironment
4/2/2012	20:32:58	MACB	NTUSER key	Key name: HKEY_USER/Software/JavaSoft/JavaRuntimeEnvironment/1.6.0_31
4/2/2012	20:32:58	M.C.	NTFS \$MFT	C:/Documents and Settings/tdungan/Application Data/Sun/Java/Deployment/deployment.properties
4/2/2012	20:33:06	...B	NTFS \$MFT	C:/Documents and Settings/tdungan/Application Data/Sun/Java/Deployment/cache/6.0/62/63075a3e-77699f39.idx
4/2/2012	20:33:07	...B	NTFS \$MFT	C:/Documents and Settings/tdungan/Application Data/Sun/Java/Deployment/cache/6.0/lastAccessed
4/2/2012	20:33:15	M.CB	NTFS \$MFT	C:/Documents and Settings/tdungan/Local Settings/Temp/pkxezy1tji98.exe
4/2/2012	20:33:15	...B	NTFS \$MFT	C:/Documents and Settings/tdungan/Application Data/Sun/Java/Deployment/cache/6.0/4/6f13884-712bc739.idx
4/2/2012	20:33:16	M.C.	NTFS \$MFT	C:/Documents and Settings/tdungan/Application Data/Sun/Java/Deployment/
4/2/2012	20:33:16	...C.	NTFS \$MFT	C:/Documents and Settings/tdungan/Application Data/Sun/Java/Deployment/
4/2/2012	20:33:17	MACB	XP Prefetch	PKXEZY1TJI98.EXE-0BCBF29B.pf - [PKXEZY1TJI98.EXE] was executed - on col
4/2/2012	20:33:17	MACB	Firefox 3 history	http://www.irs.gov/ (Internal Revenue Service) [count: 1] Host: www.irs.gov visited from: http://207.58.245.179/ (URL not typed directly) type: LINK
4/2/2012	20:33:27	M.CB	NTFS \$MFT	C:/WINDOWS/Prefetch/PKXEZY1TJI98.EXE-0BCBF29B.pf
4/2/2012	20:34:26	...B	NTFS \$MFT	C:/WINDOWS/system32/dllhost
4/2/2012	20:35:10	M.CB	NTFS \$MFT	C:/WINDOWS/system32/dllhost/svchost.exe
4/2/2012	20:35:10	M.CB	NTFS \$MFT	C:/WINDOWS/system32/dllhost/winclient.reg
4/2/2012	20:35:49	M.C.	NTFS \$MFT	C:/WINDOWS/system32/dllhost
4/2/2012	20:36:03	...B	NTFS \$MFT	C:/WINDOWS/Prefetch/REG.EXE-0D2A95F7.pf
4/2/2012	20:37:14	MACB	SYSTEM key	Key name: HKLM/System/ControlSet002/Services/Netman/domain
4/2/2012	20:37:14	MACB	SYSTEM key	Key name: HKLM/System/ControlSet001/Services/Netman/domain
4/2/2012	20:39:24	MACB	SOFTWARE key	Key name: HKLM/Software/Microsoft/Windows/CurrentVersion/Run

## Java Applet attack hits – Download of malware into /temp folder

## Malware run from /temp folder

## Files Dropped – svchost.exe is beacon malware

## Beacon Interval Set and Persistence Achieved via "RUN" Key



# Analyse de supports de stockage

- Possibilité d'identifier des comportements suspects au travers des mécanismes prefetch/superfetch
- Pré-chargement en mémoire de .exe/.dll souvent utilisés
- Prefetchs
  - Fichiers « .pf » indiquant les processus lancés couramment
    - %windir%\Prefetch
  - Indique quels fichiers il a l'habitude de loader
- Superfetchs
  - Apprentissage des habitudes de l'utilisateur
    - Fichiers « Ag\*.db »
  - Prémapping des fichiers en fonction de ses habitudes
  - Exemple : « firefox.exe exécuté généralement à 18h »



# Analyse de supports de stockage

- Éléments d'investigation de techniques d'attaque de **persistance**
  - Altération de la chaîne de boot (MBR, UEFI, Grub, ...)
    - Comparaison de hash avec liste blanche
  - Utilisation de certaines clés de registre
    - Ex : chargement d'une DLL spécifique dans tous les processus exécutés  
HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\Session Manager\AppCertDLLs
  - Fichiers de login altérés (.bash\_profile, .bashrc, ...)
    - Analyse manuelle de ces fichiers et/ou des dates de modification
  - Attaque "sethc.exe" (démarrage en mode réparation, accès à un terminal, remplacement du binaire "sethc.exe" par "cmd.exe", redémarrage normal et appui 5 fois sur la touche Shift)
    - Comparaison de hash avec liste blanche



# Analyse de supports de stockage

- Éléments d'investigation de techniques d'attaque d'élévation de privilèges
  - “DLL search order hijacking” sous Windows
    - Fonctionnement
      - Profiter d'un processus privilégié chargeant ses DLL depuis un chemin de recherche accessible en écriture par tout le monde
    - Investigation
      - Analyser les prefetchs pour identifier le chargement de DLLs suspectes



# Analyse de supports de stockage

- Éléments d'investigation de techniques d'attaque d'élévation de privilèges
  - “API hooking”
    - Fonctionnement sous Linux
      - Exploitation de la variable d'environnement LD\_PRELOAD
      - Permet de charger une bibliothèque automatiquement au lancement d'un processus
      - Si positionné sur un binaire *setuid*, cela permet une élévation de privilèges
      - => ne fonctionne que sur d'anciennes versions de Linux
    - Investigation
      - Dump mémoire des processus (outils ProcessDumper)
      - Analyse des variables d'environnement (plugin Volatility)



# Analyse de supports de stockage

- Éléments d'investigation de techniques d'attaque d'élévation de privilèges
  - "Application Shimming"
    - Fonctionnement
      - Exploitation du mécanisme de rétro-compatibilité de Windows
      - Positionnement de faux hooks de rétro-compatibilité sur l'exécution de certaines API
      - Possibilité de contourner certains mécanismes (UAC, SEH, ...)
    - Investigation
      - Analyse des bases de données des "Shims"
        - %WINDIR%\AppPatch\sysmain.sdb
        - %WINDIR%\AppPatch\custom
        - %WINDIR%\AppPatch\AppPatch64\Custom
      - Outil ShimCacheParser.py (Mandiant)





# Analyse de mémoires

- Constat
  - Certaines activités suspectes restent entièrement en mémoire volatile (meterpreter, ...)
  - Aucune écriture sur disque, donc aucune trace détectable par les précédents outils de forensic
- Approches d'analyse
  - Dump de mémoires volatiles
  - Listing
    - des processus en cours d'exécution
    - des connexions en cours
    - des utilisateurs connectés
    - des drivers chargés
    - ...
  - Recherche d'indicateurs de compromission en mémoire
  - Analyse des fichiers d'échange, d'hibernation et des dump de crash d'exécution (*core dump*)



# Analyse de mémoires

Identification des processus en cours d'exécution au moment du dump (outil Rekall, plugin pslist)

```
$ rekall -f disk_copy.img pslist
```

Offset (V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start	Exit
-----									
0x823c87c0	System	4	0	61	1140	-----	False	-	-
0x81fdf020	smss.exe	448	4	3	21	-----	False	2015-06-25 16:47:28	-
0x81f5a3b8	csrss.exe	504	448	12	596	0	False	2015-06-25 16:47:30	-
0x81f8eb10	winlogon.exe	528	448	21	508	0	False	2015-06-25 16:47:31	-
0x820e0da0	services.exe	580	528	18	401	0	False	2015-06-25 16:47:31	-
...									



# Analyse de mémoires

Identification des connexions réseau en cours d'exécution au moment du dump (outil Volatility, plugin connscan)

```
$ vol.py -f Win2K3SP0x64.vmem --profile=Win2003SP2x64 connscan
```

Offset(P)	Local Address	Remote Address	Pid
-----	-----	-----	-----
0x0ea7a610	172.16.237.150:1419	74.125.229.187:80	2136
0x179099e0	172.16.237.150:1115	66.150.117.33:80	2856
0x2cdb1bf0	172.16.237.150:139	172.16.237.1:63369	4
0x339c2c00	172.16.237.150:1138	23.45.66.43:80	1332
0x39b10010	172.16.237.150:1148	172.16.237.138:139	0
...			

# Analyse de mémoires

Identification des zones mémoire suspectes au moment du dump (outil Volatility, plugin malfind)

```
$ python vol.py -f stuxnet.vmem --profile=WinXPSP2x86 malfind -D stuxout/
```

```
Process: services.exe Pid: 668 Address: 0x13f0000
```

```
Vad Tag: Vad Protection: PAGE_EXECUTE_READWRITE
```

```
Flags: Protection: 6
```

```
0x013f0000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00  MZ.....
0x013f0010 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  .....@.....
0x013f0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
```

```
0x013f0000 4d      DEC EBP
0x013f0001 5a      POP EDX
0x013f0002 90      NOP
0x013f0003 0003     ADD [EBX], AL
0x013f0005 0000     ADD [EAX], AL
0x013f0007 000400   ADD [EAX+EAX], AL
```

Le plugin malfind s'appuie sur différentes heuristiques suspectes. Ici, suspect car page mémoire en W+X

# Analyse de mémoires

Identification des DLLs suspectes en mémoire au moment du dump (outil Volatility, plugin ldrmodules)

```
$ ./vol.py ldrmodules -p 1928
```

Pid	Process	Base	InLoad	InInit	InMem Path
1928	lsass.exe	0x00080000	0	0	0 -
1928	lsass.exe	0x7C900000	1	1	1 \WINDOWS\system32\ntdll.dll
1928	lsass.exe	0x773D0000	1	1	1 \WINDOWS\WinSxS\x86_Microsoft.Windows...\comctl32.dll
1928	lsass.exe	0x77F60000	1	1	1 \WINDOWS\system32\shlwapi.dll
1928	lsass.exe	0x771B0000	1	1	1 \WINDOWS\system32\wininet.dll
1928	lsass.exe	0x77A80000	1	1	1 \WINDOWS\system32\crypt32.dll
1928	lsass.exe	0x77FE0000	1	1	1 \WINDOWS\system32\secur32.dll
1928	lsass.exe	0x77C00000	1	1	1 \WINDOWS\system32\version.dll
1928	lsass.exe	0x01000000	1	0	1 -
1928	lsass.exe	0x5B860000	1	1	1 \WINDOWS\system32\netapi32.dll

Suspect car aucun  
fichier correspondant  
sur le disque

# Analyse de mémoires

Identification des zones de mémoire suspectes (outil Volatility, plugin hollowfind)

```
root@kratos:~/Volatility# python vol.py -f stuxnet.vmem hollowfind
Volatility Foundation Volatility Framework 2.5
Hollowed Process Information:
  Process: lsass.exe PID: 1928 PPID: 668
  Process Base Name(PEB): lsass.exe
  Hollow Type: Invalid EXE Memory Protection and Process Path Discrepancy

VAD and PEB Comparison:
  Base Address(VAD): 0x1000000
  Process Path(VAD):
  Vad Protection: PAGE_EXECUTE_READWRITE
  Vad Tag: Vad

  Base Address(PEB): 0x1000000
  Process Path(PEB): C:\WINDOWS\system32\lsass.exe
  Memory Protection: PAGE_EXECUTE_READWRITE
  Memory Tag: Vad

Disassembly(Entry Point):
  0x010014bd e95f1c0000 JMP 0x1003121
  0x010014c2 0000 ADD [EAX], AL
  0x010014c4 0000 ADD [EAX], AL
  0x010014c6 0000 ADD [EAX], AL
```

Attaque de type  
“Process hollowing”  
(remplacement de  
processus) potentielle

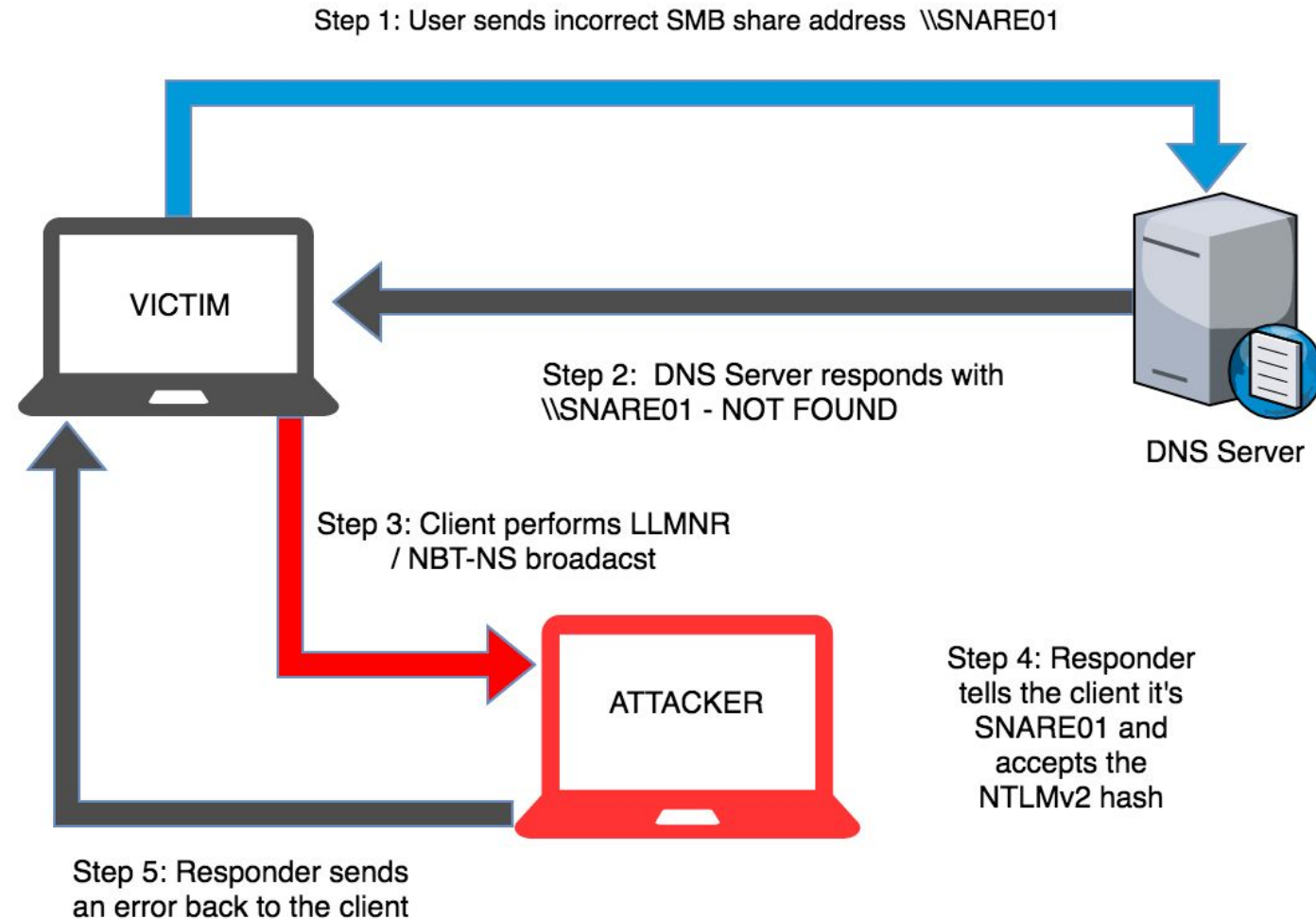


# Récupération de credentials

- Techniques d'attaques et éléments d'investigation
  - Pré-requis des attaques
    - Capture de credentials en mémoire, dans la base SAM, base de registre ou sur le réseau
    - Privilèges administrateur local la plupart du temps
  - Objectif : acquérir les droits administrateur du domaine
  - Techniques
    - Pass the hash : authentification avec hash du mot de passe plutôt que par le mot de passe lui même
    - Pass the ticket : rejeu d'un ticket Kerberos légitime afin d'obtenir un TS (Ticket Service) ou TGT (Ticket Granting Ticket)
    - Golden ticket : capacité à générer un ticket valide sans limitation de durée et pour tous les comptes
    - ...
  - Détection :
    - Difficile mais possible avec la combinaison de l'Event ID 4624 (authentification réussi) et d'un nom de processus suspect sur la machine source

# Récupération de credentials

- Techniques d'attaques et éléments d'investigation
  - Attaquer "Responder" sur le protocole LLMNR/Netbios
    - Capture d'un hash NTLMv2 potentiellement crackable





# L'analyse de malwares

---



# L'analyse de malwares

Question : quels peuvent être les objectifs de l'analyse de malware ?



# Objectifs de l'analyse de malwares

- Comprendre l'impact d'un malware : destruction, compromission, vol, espionnage, ...
- Comprendre le fonctionnement d'un malware
- Produire une signature pour détecter des compromissions passées et futures
- Partager l'information à d'autres entités, et récupérer des renseignements sur la menace
- Difficulté
  - Les malwares peuvent se protéger contre l'analyse (packing, machine virtuelle, anti-débug, détection de sandbox, etc.)



# Approches et outillage pour une analyse manuelle

- Analyse statique
  - IDA Pro / Hex rays decompiler
  - Objdump / readelf / strings
  - Radare2
- Analyse dynamique
  - Cuckoo sandbox
  - Ollydbg
  - Windbg
  - Gdb
- Analyse réseau / rétro-ingénierie de protocoles
  - Wireshark
  - Tcpdump
  - Netzob

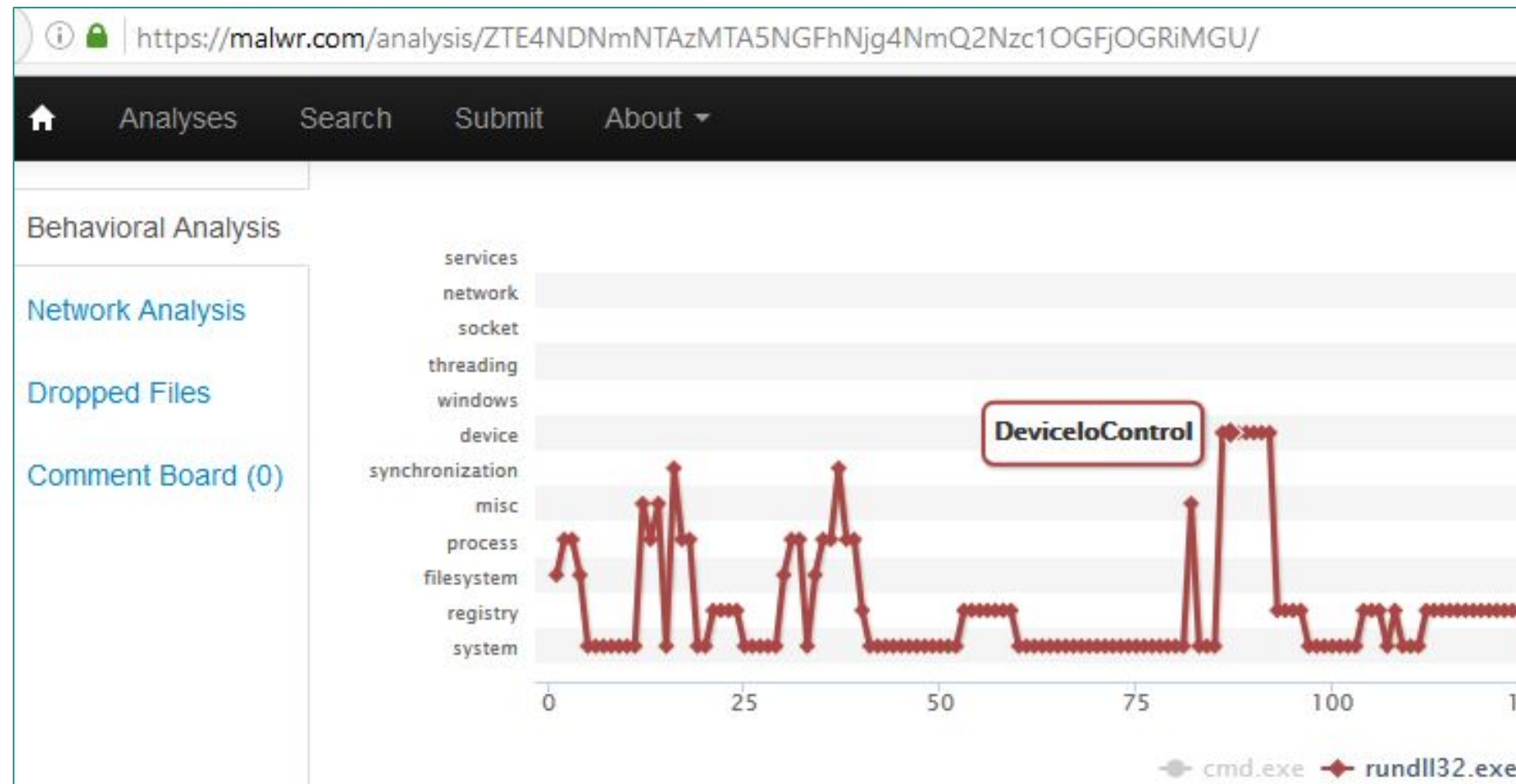


# Plateformes d'analyse

- Open source
  - Cuckoo
- En ligne
  - Anubis
  - VirusTotal
  - Malwr
- Commercial
  - Lastline
  - FireEye

# Exemple d'un rapport d'analyse automatique

Résultat d'une  
analyse  
comportementale  
avec la plateforme  
malwr.com





# Exemple d'un rapport d'analyse de malware

Analyse du malware GREENCAT à priori conçu par le groupe APT1, par la société Mandiant/FireEye

## Persistence Mechanism

- The malware sets the following value to the path of the GREENCAT DLL:
  - `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\<service_name>\Parameters\ServiceDll`
- The malware creates the following value to the path of the original ServiceDLL value:
  - `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\<service_name>\Parameters\DllPath`
- The malware sets
  - `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\<service_name>\Start`
    - Value: 2 (SERVICE\_AUTO\_START)

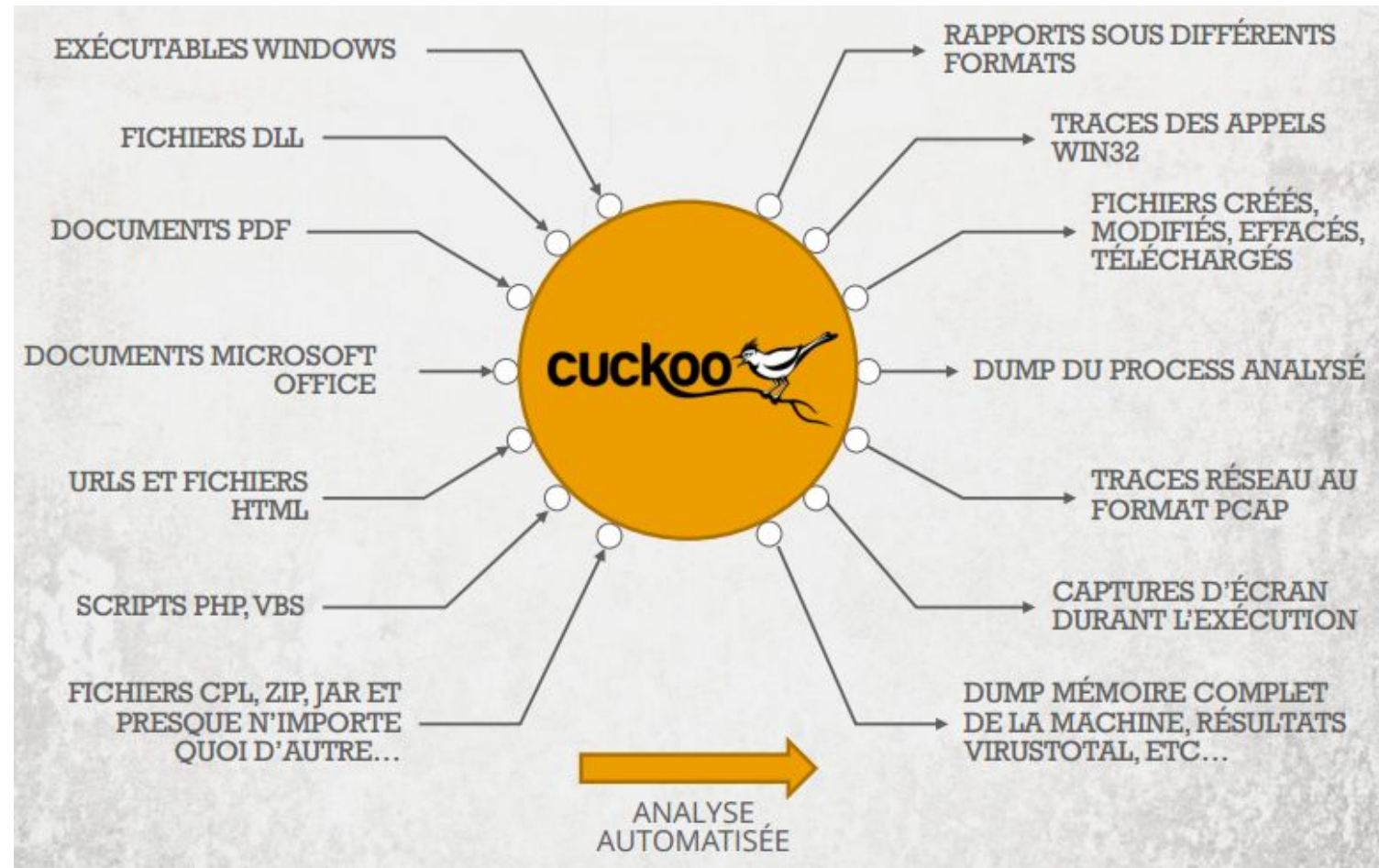
## Host-Based Signatures

- The malware may write BMP files to a directory on the system identified as `<number>.bmp`, such as `1.bmp` or `17.bmp`.

## Network-Based Signatures

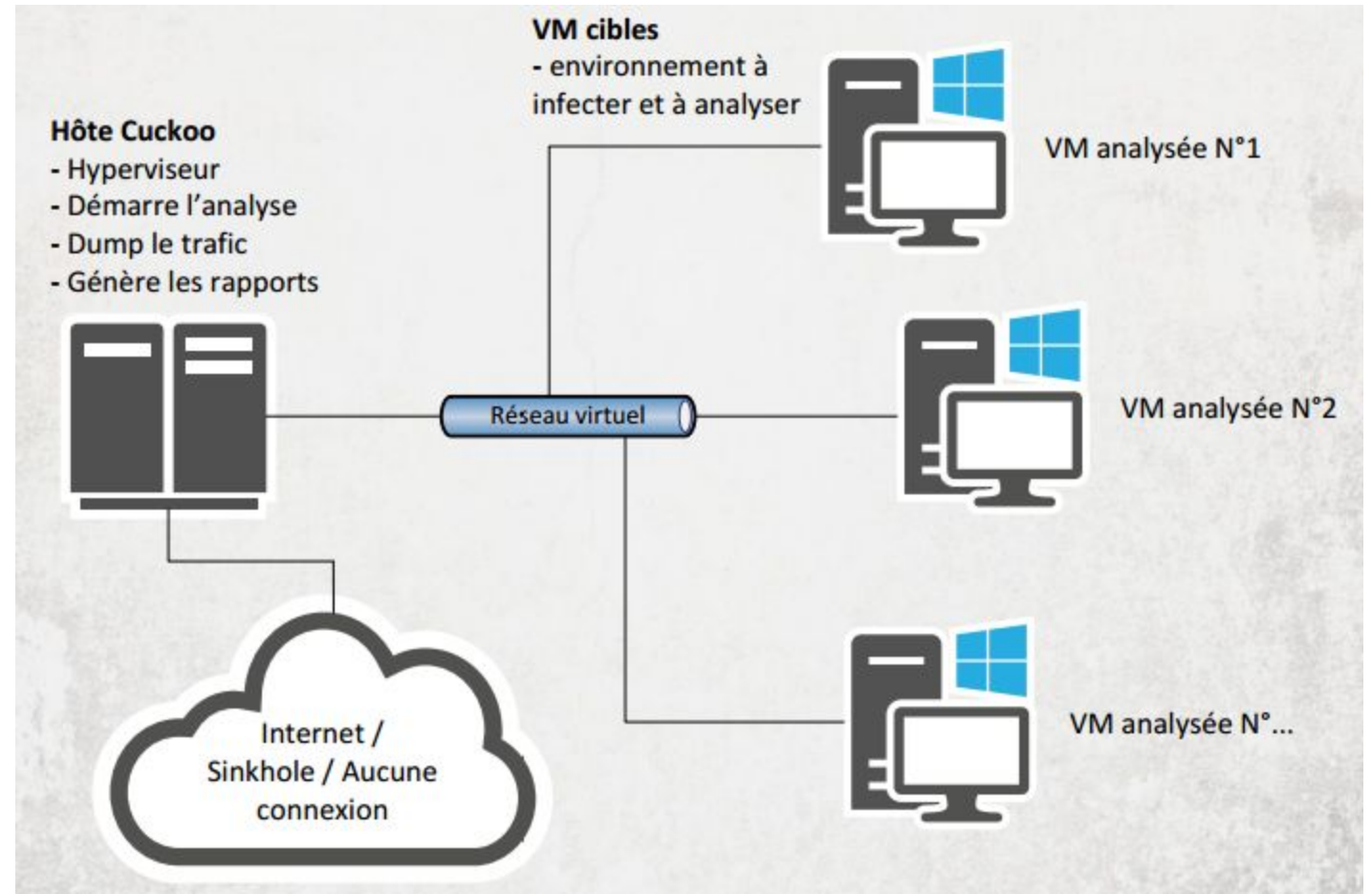
- The malware has been observed with the following User-Agent strings:
  - `Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; SV1)`
  - `Mozilla/5.0`
  - `Mozilla/4.0`
- Reference Appendix F for known APT1-generated certificates used in conjunction with this malware.

# La plateforme Cuckoo





# Architecture de la plateforme Cuckoo



# Les données produites par Cuckoo

```
guru@dell: ~/Desktop/cuckoo/storage/analyses
guru@dell:~/Desktop/cuckoo/storage/analyses$ tree 43
43
├── analysis.log
├── binary -> /home/guru/Desktop/cuckoo/storage/binaries/c065e5325c7eee100fb65429b2b9200153eb6ec0d7185
├── c5d
├── dump.pcap
├── files
│   ├── 1429217182
│   │   └── ohbya.exe
│   ├── 214884399
│   │   └── tmpcae09bba.bat
│   ├── 3486094655
│   │   └── MPS1.tmp
│   ├── 4979675364
│   │   └── zalando.exe
│   ├── 6360346017
│   │   └── lege.tmp
│   ├── 6469544114
│   │   └── lege.lia
│   ├── 7055760738
│   │   └── wbemprox.log
│   └── 9669662366
│       └── Inbox.dbx
├── logs
│   ├── 1232.bson
│   ├── 1508.bson
│   ├── 1652.bson
│   ├── 1784.bson
│   ├── 1828.bson
│   ├── 1848.bson
│   ├── 1880.bson
│   └── 1916.bson
├── memory.dmp
├── reports
│   ├── report.html
│   ├── report.json
│   └── report.maec-4.0.1.xml
├── shots
│   ├── 0001.jpg
│   └── 0002.jpg
```

La capture réseau

Les fichiers créés / droppés

Le dump mémoire

Le reporting

Les captures d'écran

---

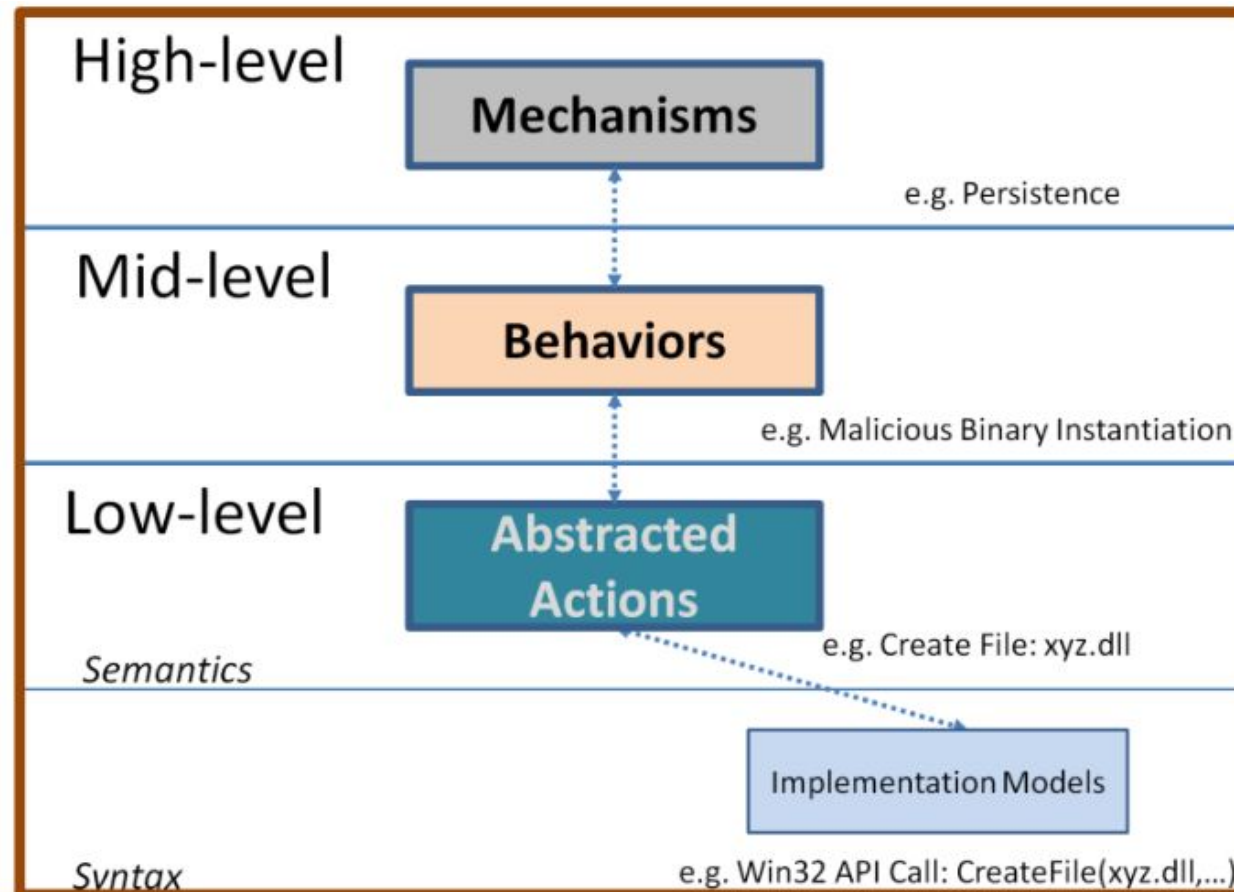
# Productions d'indicateurs de compromission et de règles de détection



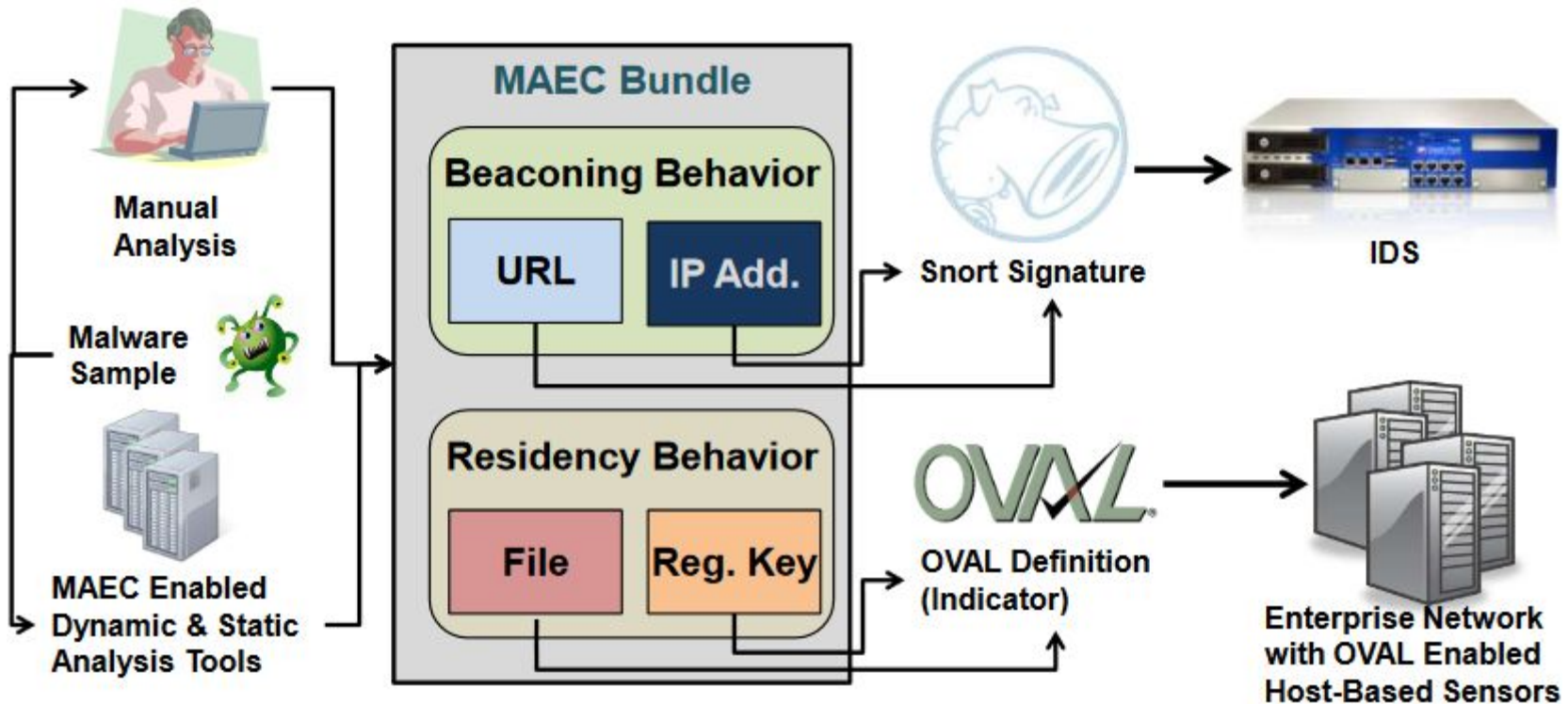
# MAEC – Malware Attribute Enumeration and Characterization

- Standard du MITRE
- Objectif : Structuration de la caractérisation d'un malware
- Sous la forme d'un langage (grammaire et vocabulaire) et d'une collection
- Compatible avec CybOX (depuis la version 2.0) pour la structuration des observables

# MAEC : Structure



# MAEC : Cas d'applications



# Création de règles de détection

## Création d'un IoC avec l'outil RedLine de Mandiant

Add:	Definition:
<input type="button" value="Item"/>	<input type="checkbox"/> OR
<input type="button" value="AND"/>	File MD5 is 672e0e296a58e31107c3d779953eaaa9
<input type="button" value="OR"/>	<input type="checkbox"/> AND
	Process Name contains svchost.exe
	Process arguments contains not -k
	<input type="checkbox"/> AND
	File Name contains svchost.exe
	<input type="checkbox"/> OR
	File Full Path contains not system32
	File Import Name contains mscoree.dll
	File Digital Signature Verified contains False
	File Compile Time contains 2010-09-09T12:04:21Z
	<input type="checkbox"/> AND
	File Size is [8000 TO 10000]
	File PE Subsystem contains Windows_GUI
	File Import Name contains mscoree.dll
	File PE Type contains Executable
	<input type="checkbox"/> OR
	File Path is WINDOWS
	File Path is WINNT
	<input type="checkbox"/> AND
	File Section Name contains .rsrc
	File Section Name contains .txt
	File Section Name contains .reloc



# Extraction d'IOC de rapports d'analyse

Extraction d'IOC et production de données structurées (exemple avec Yara en sortie de l'outil IOC Parser)

```
$ ./iocp.py -p patterns.ini -i html -l requests -d -o yara
http://blog.malwaremustdie.org/2015/09/mmd-0042-2015-hunting-mr-black-ids-via.html

rule mmd_0042_2015_hunting_mr_black_ids_via
{
    strings:
        $URL1 = "http://www.blogger.com/go/cookiechoices"
        $IP1 = "210.92.18.118"
        $IP2 = "106.120.167.25«
        ...
        $Host23 = "libworker.so"
        $Host24 = "www.blogger.com"
        $Email1 = "ppyy@astpbx.com"
    condition:
        ...
}
```



# Outillage pour l'investigation

---

---

# Plateformes de réponse à incident



# La plateforme FIR

- FIR : Fast Incident Response
- Origine : CERT Société Générale
- Objectif : permet le suivi des tickets d'incidents

# La plateforme FIR

## STARRED INCIDENTS

Date ▼		Category	Subject	Business Lines	Severity	Status	Detection	Leader	Last Action	Plan	Lvl	IH	Edit
2015-03-10	★	Phishing	<a href="http://phishingsite.com/url/">http://phishingsite.com/url/</a>	Sub BL 1	2	Open	CERT	CERT	Abuse 16 hours ago	B	C1	dev	

Open

Blocked

Old

Tasks

Date ▼		Category	Subject	Business Lines	Severity	Status	Detection	Leader	Last Action	Plan	Lvl	IH	Edit
2015-03-10	★	Phishing	<a href="http://phishingsite.com/url/">http://phishingsite.com/url/</a>	Sub BL 1	2	Open	CERT	CERT	Abuse 16 hours ago	B	C1	dev	
2015-01-15	☆	Phishing	test	Demo BusinessLine 1	1	Open	CERT	None	Opened 2 months ago	None	C1	dev	
2015-01-05	☆	Phishing	test	Demo BusinessLine 1, Demo BusinessLine 2	2	Open	Pôle	None	Alerting 2 months ago	None	C1	dev	
2015-01-05	☆	Phishing	test	Demo BusinessLine 1, Demo BusinessLine 2	2	Open	Pôle	None	Opened 2 months ago	None	C1	dev	
2014-12-17	☆	IS integrity	Alerte Jokeware	Demo BusinessLine 1	1	Open	SOC	None	Opened 3 months ago	None	C1	dev	
2014-12-17	☆	Phishing	phishing	Demo BusinessLine 1, Demo BusinessLine 2	2	Open	CERT	CERT	Info 3 months ago	B	C1	dev	

(page 1 of 1)

# La plateforme FIR

FIR

New event

Dashboard

Incidents

Events

Stats

search...

Currently logged in as dev [logout] [Admin]

Incident Leader

None

Plan

None

Severity

1

Category

Phishing

Status

Closed

Detection

CERT

B/L

Demo BusinessLine 1

## Incident / Phishing / test

Opened on Jan. 15, 2015, 5:47 p.m. by dev

DESCRIPTION

phishing copying our brand website on http://evilwebsite.com/evilurl  
detected by one of our clients

TO-DO LIST

Action	Accountable
<input checked="" type="checkbox"/> Contact registrar	CERT

+ Add To-Do Item

CORRELATED ARTIFACTS

Type	Values
Hostnames	<a href="#">evilwebsite.com</a> (2) ✕

RELATED FILES

Date	File	Description
Feb. 5, 2015, 5:20 p.m.	<a href="#">MongoHub.zip</a>	
Feb. 5, 2015, 5:50 p.m.	<a href="#">YARA_User_s_Manual_1.6__1_.pdf</a>	yara

Browse...

Upload files

Download archive

ATTRIBUTES

Name	Value
loss	2784

+ Add attribute

Comments (3)

Artifacts (2)

		Comment	Action
2015-02-09 14:32	dev	new test	Monitor ✎ ✕
2015-01-30 19:10	dev	Changed "status" from "Closed" to "Open"; Changed "is_starred" from "True" to "False";	Info ✎ ✕
2015-01-15 17:47	dev	Incident opened	Opened ✎ ✕

+ Add

Comment

Edit

Open

Block

Incident followup

Alert

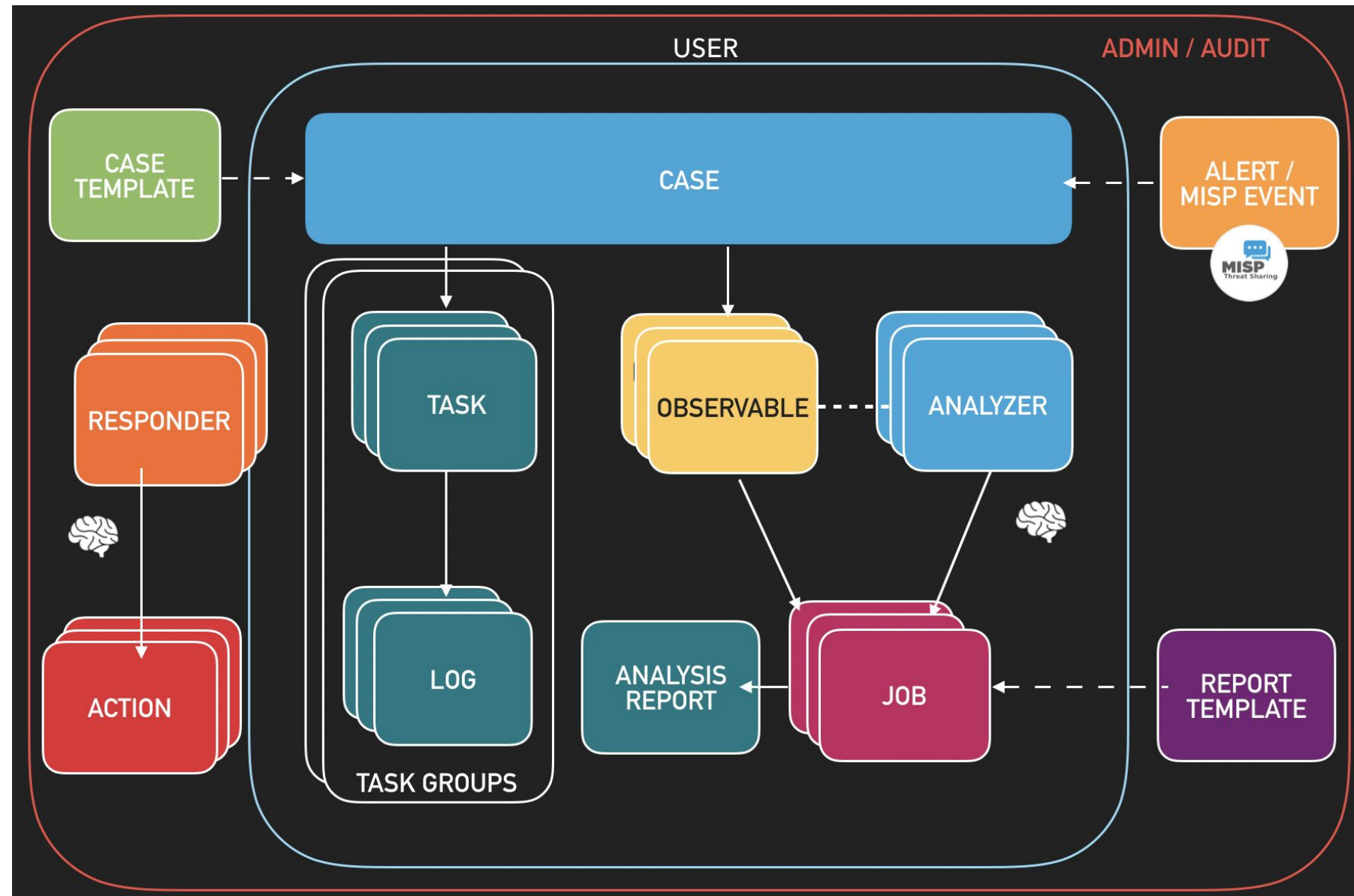
Takedown



# The Hive

- Plateforme de réponse à incidents
- Origine : CERT Banque de France
- Principales fonctionnalités
  - Management des incidents
  - Analyse automatisée d'observables
  - Intégration avec MISP

# The Hive





# The Hive

## Liste des cas d'analyse

List of cases (3 of 3) Show live stream

Quick Filters ▾

Sort by ▾

Stats

Filters

15 per page

1 filter(s) applied: status: Open Clear filters

Title	Severity	Tasks	Observables	Assignee	Date
#3 - Investigation alerte antivirus None	M	6 Tasks	1	A	01/12/19 17:33
#2 - Investigation sur phishing None	M	2 Tasks	3	A	11/09/17 13:38
#1 - test None	L	1 Task	1	A	11/09/17 1:00



# The Hive

Tâches  
associées à un  
cas d'analyse

M

Case # 3 - Investigation alerte antivirus

Created by admin

Sat, Jan 12th, 2019 17:33 +01:00

2 Related cases

Details

Tasks 6

Observables 1

Analyser les logs système 8[.]8[.]8[.]8

+ Add Task

Filter

Task	Date	Assignee
<div><div></div>Analyser les logs système</div>	Sat, Jan 12th, 2019 17:34 +01:00	<div>A</div> admin
Analyser forensique du disque		Not assigned
Analyser les logs réseau		Not assigned
Analyser logs antivirus		Not assigned
Produire éléments d'amélioration continue		Not assigned
Produire rapport d'analyse		Not assigned

[Details](#)[Tasks](#) **6**[Observables](#) **1**[Analyser les logs système](#) **×**[8\[.\]8\[.\]8\[.\]8](#) **×**

### Basic Information

[Flag](#) [Close](#)

### Task logs

**Title** Analyser les logs système

**Owner** admin


**Date** Sat, Jan 12th, 2019 17:34 +01:00

**Status** InProgress


**Description** *Not specified*

[+ Add new task log](#)[Sort by: Newest first](#)

10 per page

 adminSat, Jan 12th, 2019 17:35 +01:00 **×**

l'élément suspect est en fait un faux positif : il s'agit d'un outil utilisé par l'administrateur système

 adminSat, Jan 12th, 2019 17:35 +01:00 **×**

j'ai observé tel élément suspect : fichier c:/rat.exe

# The Hive


Liste des observables  
liés à l'analyse

List of observables (3 of 3)

<input type="checkbox"/>	Type ▲▼	Data/Filename ▲▼
<input type="checkbox"/>	domain	rusian-bank[.]ru 🔖 domain name ⚙️ No reports available
<input type="checkbox"/>	filename	c:/rat[.]exe 🔖 fichier ⚙️ No reports available
<input type="checkbox"/>	ip	8[.]8[.]8[.]8 🔖 ip ⚙️ PT:PassiveDNS="6904 records" MaxMind:Location="United States/North America"

# The Hive

Moteurs d'analyse des observables  
(liés au composant Cortex)

 <b>TheHive</b>	<a href="#">+ New Case</a> ▾	<a href="#">My tasks</a> <b>1</b>	<a href="#">Waiting tasks</a> <b>7</b>	<a href="#">Alerts</a> <b>0</b>	<a href="#">Statistics</a>	<input type="text" value="Case, user, URL, hash, IP, dom"/>
<h2>Observable Analyzers</h2>						
Analyzer		Cortex Server		Last analysis		
Abuse_Finder_2_0 Find abuse contacts associated with domain names, URLs, IPs and email addresses		LOCAL CORTEX		None		
CIRCLPassiveSSL_2_0 Check CIRCL's Passive SSL for a given IP address or a X509 certificate hash		LOCAL CORTEX		None		
DNSDB_IPHistory_2_0 Provide history records for an IP address using DNSDB Passive DNS service		LOCAL CORTEX		None		
DomainTools_ReverseIP_2_0 Use DomainTools Reverse IP service to provide a list of domain names sharing the same IP address		LOCAL CORTEX		None		



# The Hive

**Nouvelle analyse d'un  
observable (composant  
Cortex)**

## Run new analysis

TLP

AMBER

Data Type

ip

Data

8.8.8.8

Analyzers

☐ FireHOLBlocklists\_2\_0

☐ Nessus\_2\_0

☒ Abuse\_Finder\_2\_0

☐ PassiveTotal\_Ssl\_Certificate\_History\_2\_0

☐ PassiveTotal\_Passive\_Dns\_2\_0

☒ PassiveTotal\_Malware\_2\_0

☒ PassiveTotal\_Osint\_2\_0

☐ PassiveTotal\_Unique\_Resolutions\_2\_0

☐ PassiveTotal\_Whois\_Details\_2\_0

☐ PassiveTotal\_Enrichment\_2\_0

☐ PassiveTotal\_Ssl\_Certificate\_Details\_2\_0

☐ CIRCLPassiveSSL\_2\_0

☐ HippoMore\_2\_0

---

# Partage du renseignement



# La plateforme MISP






- Plateforme de partage d'IOC et d'indicateurs de menaces
- Fonctionnalités
  - Partage
  - Collaboration autour d'évènements
  - Corrélation d'indicateurs
  - Import
  - Export
- 320 organisations et 800 utilisateurs à ce jour



# La plateforme MISP : les événements

## Events

« previous 1 2 3 4 5 6 7 next »

Published	Org	Id	Tags	#Attr.	#Corr.	Date	Threat Level	Analysis	Info	Distribution	Actions
✓		231	<div>circl:incident-classification="malware"</div> <div>tlp:white</div>	22	1	2016-08-29	Low	Completed	Bitcoinminer installed by malware	All	
✓		275	<div>tlp:white</div> <div>circl:incident-classification="malware"</div> <div>ms-caro-malware:malware-type="Ransom"</div> <div>malware_classification:malware-category="Ransomware"</div>	9	1	2016-08-29	Low	Completed	Ransomware - Xorist	All	
✓		351	<div>circl:incident-classification="malware"</div> <div>ms-caro-malware:malware-type="RemoteAccess"</div> <div>tlp:white</div> <div>Type:OSINT</div>	14		2016-08-30	Low	Completed	OSINT - German Speakers Targeted by SPAM Leading to Ozone RAT	All	
✓		252	<div>tlp:white</div> <div>circl:incident-classification="malware"</div>	80	17	2016-08-29	Low	Initial	Malspam 2016-08-29 (.wsf in .zip) - campaign: "Please find attached invoice no"	All	
✓		328	<div>tlp:white</div> <div>circl:incident-classification="malware"</div>	150	18	2016-08-29	Low	Initial	Malspam 2016-08-26 (.js in .zip) - campaign: "monthly report"	All	



# La plateforme MISP : un évènement

## Bitcoinminer installed by malware

Event ID	231
Uuid	57c4400e-1420-46f0-8837-41d7950d210f
Org	<a href="#">CIRCL</a>
Contributors	
Tags	<span>circl:incident-classification="malware" x</span> <span>tlp:white x</span> <span>+</span>
Date	2016-08-29
Threat Level	Low
Analysis	Completed
Distribution	All communities
Info	Bitcoinminer installed by malware
Published	Yes

### Related Events

2016-08-29 (275)

— Pivots — Attributes — Discussion

# La plateforme MISP : les attributs des évènements

## Attributes

« previous 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17

Event	Org	Category	Type	Value
412		External analysis	comment	At first I thought I could be dealing with someone trying to get the latest version available at the 'Orcus RAT' website
412		External analysis	link	<a href="http://blog.deniable.org/blog/2016/08/09/cracking-orcus-rat/">http://blog.deniable.org/blog/2016/08/09/cracking-orcus-rat/</a>
412		External analysis	link	<a href="https://www.virustotal.com/file/4056ee5b23e47d172b48c84ceb5b6eca5ee68cf839c0a1a039c8bc97f973b6780f07/analysis/4056ee5b23e47d172b48c84ceb5b6eca5ee68cf839c0a1a039c8bc97f973b6780f07/">https://www.virustotal.com/file/4056ee5b23e47d172b48c84ceb5b6eca5ee68cf839c0a1a039c8bc97f973b6780f07/analysis/4056ee5b23e47d172b48c84ceb5b6eca5ee68cf839c0a1a039c8bc97f973b6780f07/</a>
412		External analysis	link	<a href="http://researchcenter.paloaltonetworks.com/2016/08/09/cracking-orcus-rat/">http://researchcenter.paloaltonetworks.com/2016/08/09/cracking-orcus-rat/</a>
412		Payload installation	filename sha1	4056ee5b23e47d172b48c84ceb5b6eca5ee68cf839c0a1a039c8bc97f973b6780f07
412		Payload installation	filename sha256	4056ee5b23e47d172b48c84ceb5b6eca5ee68cf839c0a1a039c8bc97f973b6780f07
412		Payload installation	md5	d2140d8c9eb3889dee164f09014380d7
412		Payload installation	sha1	ea6d05abfce77d01a1a039c8bc97f973b6780f07

## Add Proposal

Category

Artifacts dropped

(choose one)

categories

Internal reference  
Targeting data  
Antivirus detection  
Payload delivery  
**Artifacts dropped**  
Payload installation  
Persistence mechanism  
Network activity  
Payload type  
Attribution  
External analysis  
Financial fraud  
Other

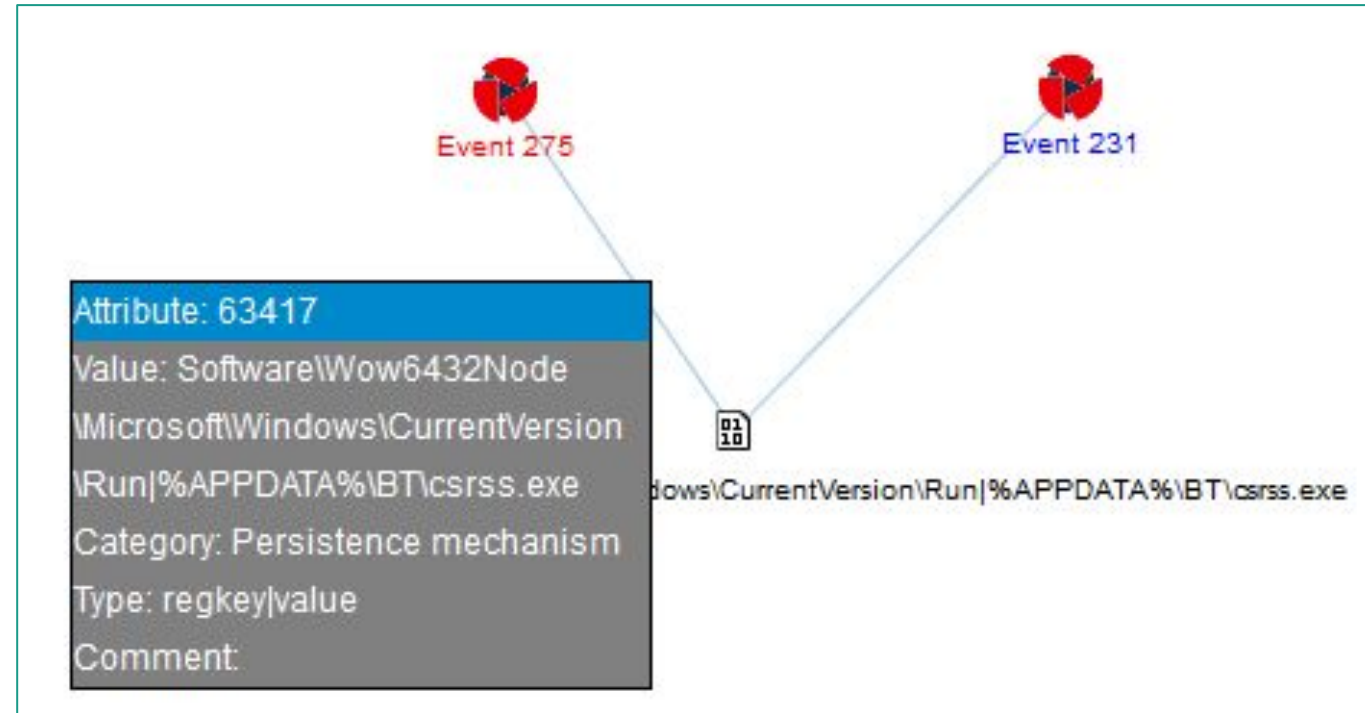
Any artifact (files, registry keys etc.) dropped by the malware or other modifications to the system

Veuillez compléter ce champ.

☐ Batch Import

# La plateforme MISP : la corrélation d'évènements

- Corrélation d'évènements
  - Partage d'au moins un attribut en commun
- Intérêts :
  - Pouvoir corréler des campagnes s'appuyant sur les mêmes outils / vecteurs d'attaques.
  - Faciliter l'attribution



# La plateforme MISP : les tags

23	✓	circ:topic="malware"
24	✓	circ:topic="industry"
25	✓	circ:topic="medical"
26	✓	circ:topic="services"
27	✓	circ:topic="undefined"
31	✓	ecsirt:malicious-code="malware"
10	✓	ecsirt:malicious-code="ransomware"
35	✓	estimative-language:likelihood-probability="almost-certain"
43	✓	estimative-language:likelihood-probability="very-likely"
38	✓	expansion:whois-registrant-email
4	✓	malware_classification:malware-category="Ransomware"
40	✓	ms-caro-malware:malware-type="Ransom"
41	✓	ms-caro-malware:malware-type="RemoteAccess"
44	✓	tlp:amber
46	✓	tlp:ex:chr
11	✓	tlp:green
45	✓	tlp:red
2	✓	tlp:white
42	✓	veris:action:malware:variety="Ransomware"



# La plateforme MISP : les tags

Liste des  
événements  
ayant un tag  
spécifique

Events

« previous

next »

Q

Tag : malware\_classification:malware-category="Ransomware" X

My Events

Org Events

Filter

Published	Org	Id	Tags	#Attr.	#Corr.	Date	Threat Level	Analysis	Info	Distrib
✓		275	<div>tlp:white</div> <div>circl:incident-classification="malware"</div> <div>ms-caro-malware:malware-type="Ransom"</div> <div>malware_classification:malware-category="Ransomware"</div>	9	1	2016-08-29	Low	Completed	Ransomware - Xorist	All
✓		232	<div>tlp:white</div> <div>circl:incident-classification="malware"</div> <div>malware_classification:malware-category="Ransomware"</div> <div>estimative-language:likelihood-probability="almost-certain"</div>	18		2016-07-22	Low	Initial	Malspam 2016-07-22 .js in .zip with embedded Locky (campaign: "Financial statement")	All
✓		271	<div>Type:OSINT</div> <div>tlp:white</div> <div>ecsirt:malicious-code="ransomware"</div> <div>malware_classification:malware-category="Ransomware"</div> <div>circl:incident-classification="malware"</div>	11		2016-06-30	Low	Completed	OSINT - Apocalypse: Ransomware which targets companies through insecure RDP	All
✓		367	<div>Type:OSINT</div> <div>circl:incident-classification="malware"</div>	10		2016-06-30	Low	Completed	OSINT - Satana ransomware – threat coming soon?	All



# La plateforme MISP : les taxonomies

- Objectif : supporter différents standards de classification
- Exemples de standards
  - NATO - Admiralty Scale
  - CIRCL Taxonomy - Schemes of Classification in Incident Response and Detection
  - EU classified information marking
  - Information Security Marking Metadata from DNI (Director of National Intelligence - US)
  - NATO Classification Marking
  - TLP - Trac Light Protocol
  - VERIS - Vocabulary for Event Recording and Incident Sharing
  - ...