Cuckoo Sandbox

Analyse automatisée de code malveillant

Alain Sullam – OWASP – 2 mars 2015

WHO AM I?

Alain Sullam
alain.sullam [at] gmail.com
GPG key id: 0x999EF732
https://ch.linkedin.com/in/alainsullam
https://github.com/sysinsider

- Ingénieur de formation, puis d'autres petites choses…
- Dans l'infosec depuis ~2000 – 2003
    - Consulting (administration publique, groupes industriels)
    - Domaine bancaire
    - Domaine juridique depuis environ 10 ans
- Intervenant à l'Université de Genève - Master Infosec (DFIR)
- Membre de l'ISC², ISACA, OWASP et ISMA

AGENDA

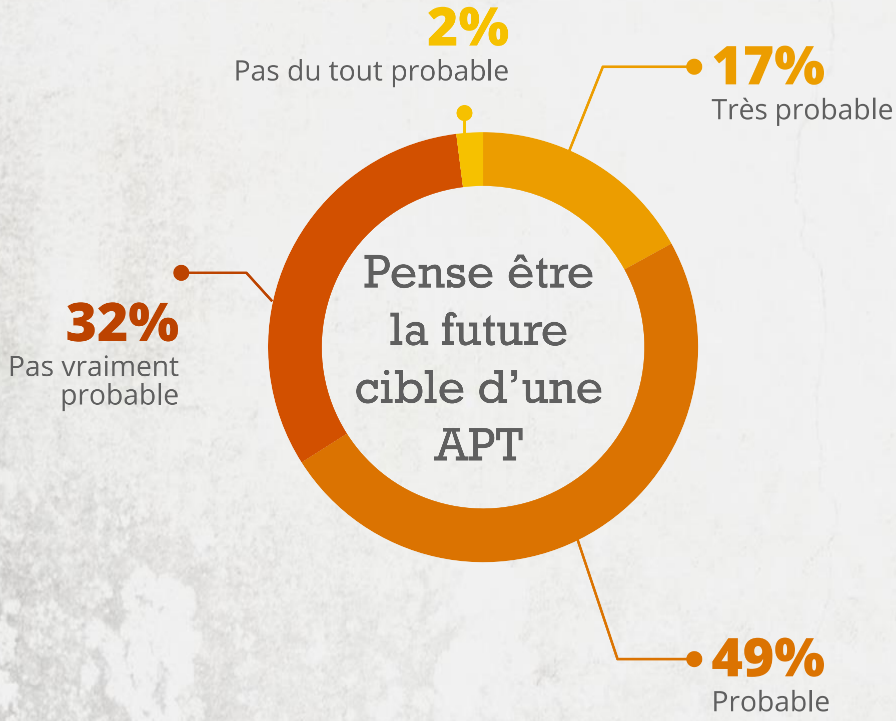
- Les entreprises face aux malwares / APT
- Cuckoo sandbox, c'est quoi?
- Analyse manuelle vs. automatisée
- L'architecture de Cuckoo Sandbox et ses prérequis
- La configuration
- Points importants de la virtualisation et du sandboxing
- Demo et reporting
- Etendre et/ou intégrer Cuckoo Sandbox
- Conclusion
- (Bonus) un peu de visualisation
- (Bonus) Pour aller plus loin…
- Questions

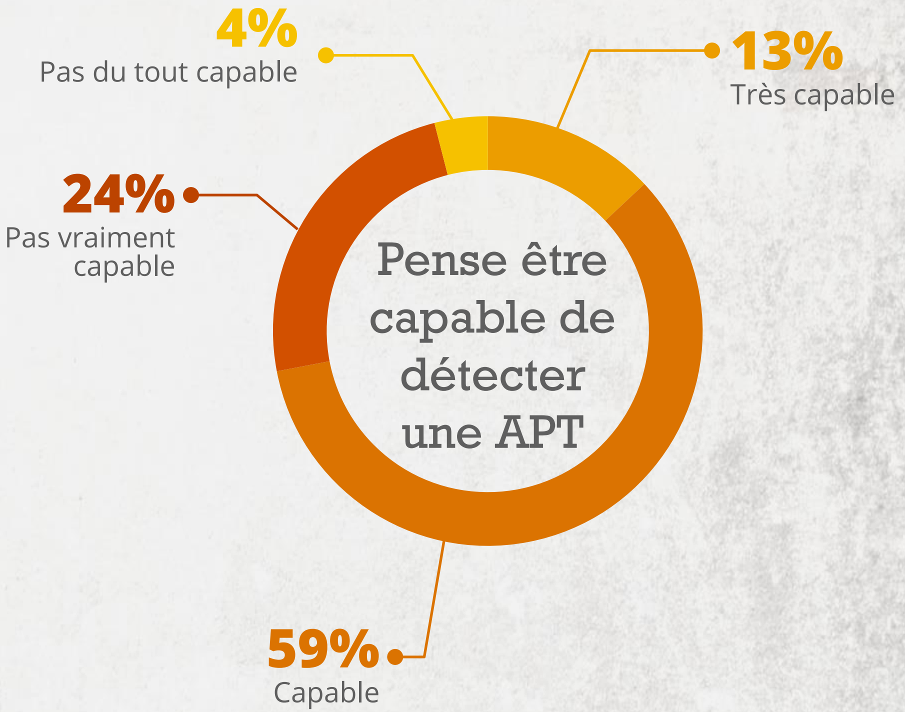
THREAT Toons™
by: Alex Savchuk
THAT'S HIM, OFFICER! THE ONE WHO RAN-SACKED MY NETWORK!
6'
5'
4'
3'
1'

Can your CSO identify a threat?

QUELQUES CHIFFRES…

LA PERCEPTION

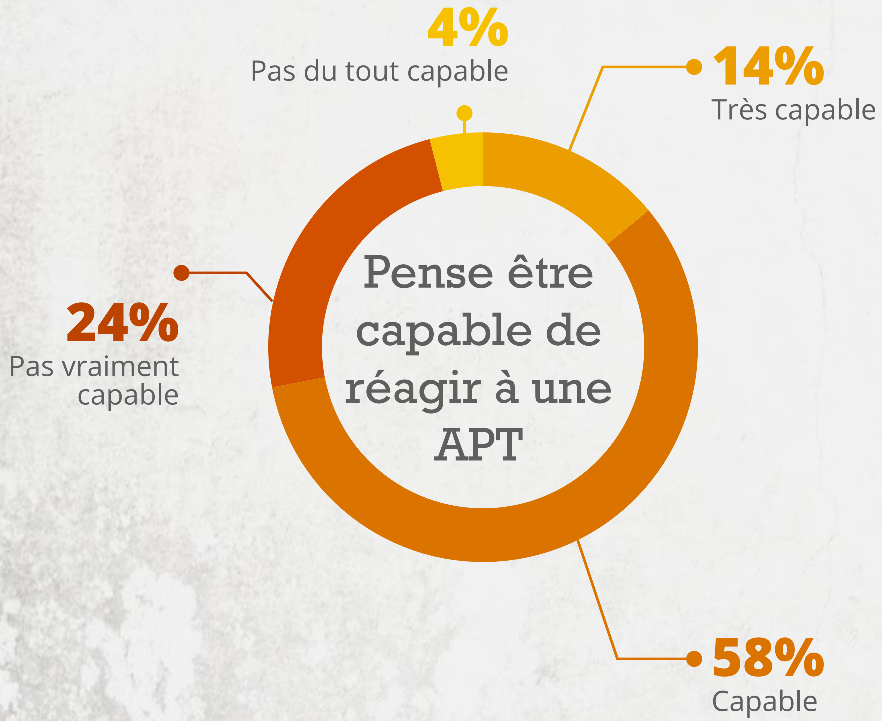


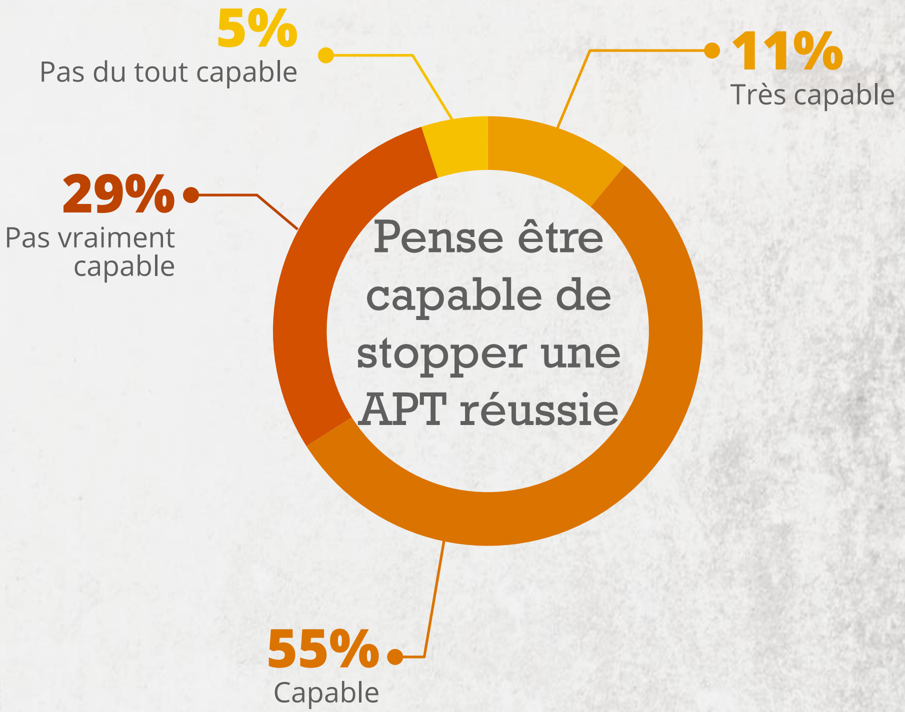


– Isaca APT survey report, 2014

QUELQUES CHIFFRES (CONT'D)…

LA PERCEPTION



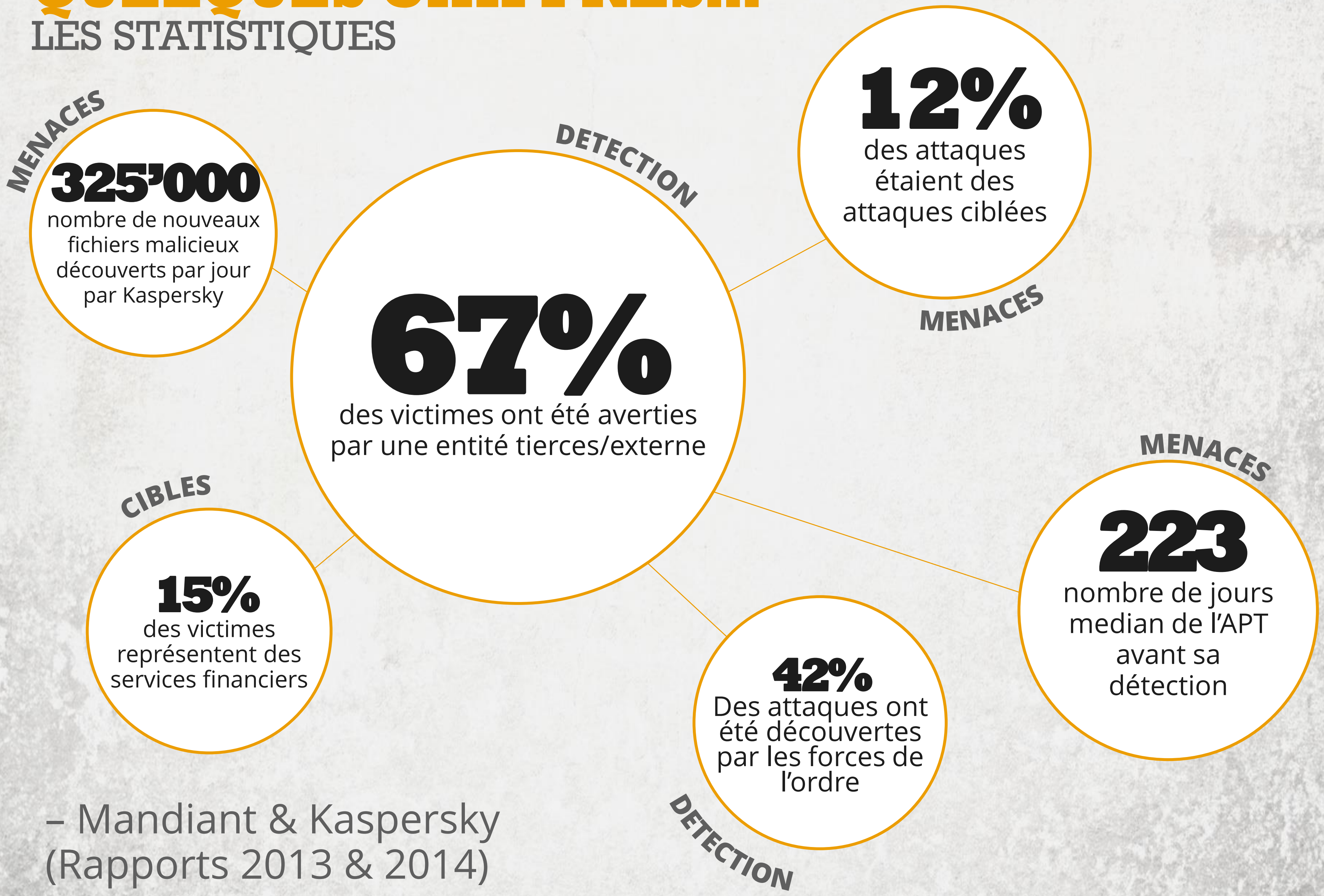


– Isaca APT survey report, 2014

THREAT Toons™
by: Alex Savchuk
2013
~~2012~~
RESOLUTIONS
THIS YEAR I WILL:
• Work to stop more than just malware
• Prevent insider threats
• Stop critical data from leaving the network
DID YOUR CSO ACCOMPLISH THEIR NEW YEAR'S RESOLUTIONS?

QUELQUES CHIFFRES…

LES STATISTIQUES



MENACES

325'000
nombre de nouveaux fichiers malicieux découverts par jour par Kaspersky

DETECTION

67%
des victimes ont été averties par une entité tierces/externe

12%
des attaques étaient des attaques ciblées

MENACES

MENACES

223
nombre de jours median de l'APT avant sa détection

CIBLES

15%
des victimes représentent des services financiers

42%
Des attaques ont été découvertes par les forces de l'ordre

DETECTION

– Mandiant & Kaspersky
(Rapports 2013 & 2014)

LES GRANDES QUESTIONS…

En cas d’incident, on va naturellement se demander :

- Quels fichiers (locaux ou non) ont été accédés, créés, supprimés?
- Y-a-t-il eu des communications réseaux, et si oui, lesquelles (internes, externes, multiples, ponctuelles, permanentes, etc.)?
- En cas de communications réseaux, quels sont leurs buts / contenus (spamming, (D)DOS, exfiltration de données, etc.) et leurs destinations?
- Est-ce une attaque ciblée ou opportuniste?
- Est-ce une attaque persistante ou non?
- Quel est le périmètre de compromission?
- …

CUCKOO SANDBOX, C'EST QUOI?

In three words, Cuckoo Sandbox is a **malware analysis system**.

What does that mean? It simply means that you can throw any **suspicious file** at it and in a matter of seconds Cuckoo will provide you back **some detailed results** outlining what such file did when executed inside an **isolated environment**.

– http://www.cuckoosandbox.org

- Analyse automatique de fichiers suspects
- Génération automatisée de rapports (détaillés)
- Dans un environnement «sandboxé»

OPEN SOURCE VS. PRODUITS COMMERCIAUX

cuckoo

malwr*

ThreatExpert*

Anubis Sandbox*

*online

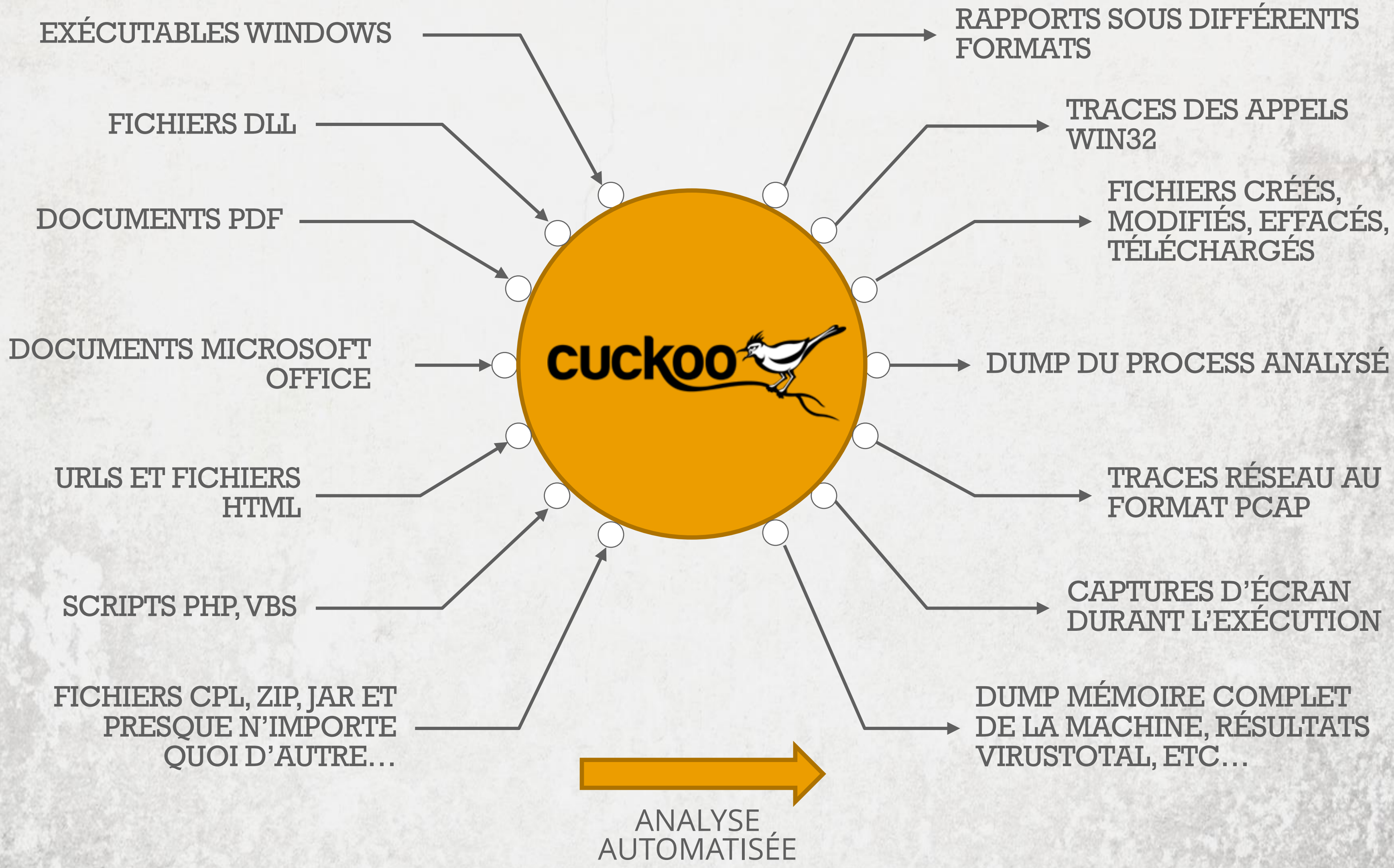
FireEye™

lastline

ThreatTrack™ Security

(paloalto NETWORKS)

COMMENT ÇA FONCTIONNE?



EXÉCUTABLES WINDOWS

FICHIERS DLL

DOCUMENTS PDF

DOCUMENTS MICROSOFT OFFICE

URLS ET FICHIERS HTML

SCRIPTS PHP, VBS

FICHIERS CPL, ZIP, JAR ET PRESQUE N'IMPORTE QUOI D'AUTRE…

RAPPORTS SOUS DIFFÉRENTS FORMATS

TRACES DES APPELS WIN32

FICHIERS CRÉÉS, MODIFIÉS, EFFACÉS, TÉLÉCHARGÉS

DUMP DU PROCESS ANALYSÉ

TRACES RÉSEAU AU FORMAT PCAP

CAPTURES D'ÉCRAN DURANT L'EXÉCUTION

DUMP MÉMOIRE COMPLET DE LA MACHINE, RÉSULTATS VIRUSTOTAL, ETC…

ANALYSE AUTOMATISÉE

L'ANALYSE MANUELLE

LES COMPÉTENCES REQUISES

DESASSEMBLAGE DECOMPILATION

ASSEMBLEUR, C/C++, IDA PRO, HOPPER, OLLYDBG, ETC.

SYSTEMES D'EXPLOITATION

FONCTIONNEMENT BAS NIVEAU, APPELS SYSTÈMES, GESTION MÉMOIRE, SYSTÈMES DE FICHIERS, REGISTRE, API WINDOWS, ETC.

RESEAU

CONNAISSANCES DES PROTOCOLES STANDARDS, FUZZING DE PROTOCOLES, CONCEPTS TCP/IP, ETC.

CRYPTOGRAPHIE

CONNAISSANCES DES ALGOS STANDARDS ET EXOTIQUES, DE LEURS IMPLÉMENTATIONS ETC.

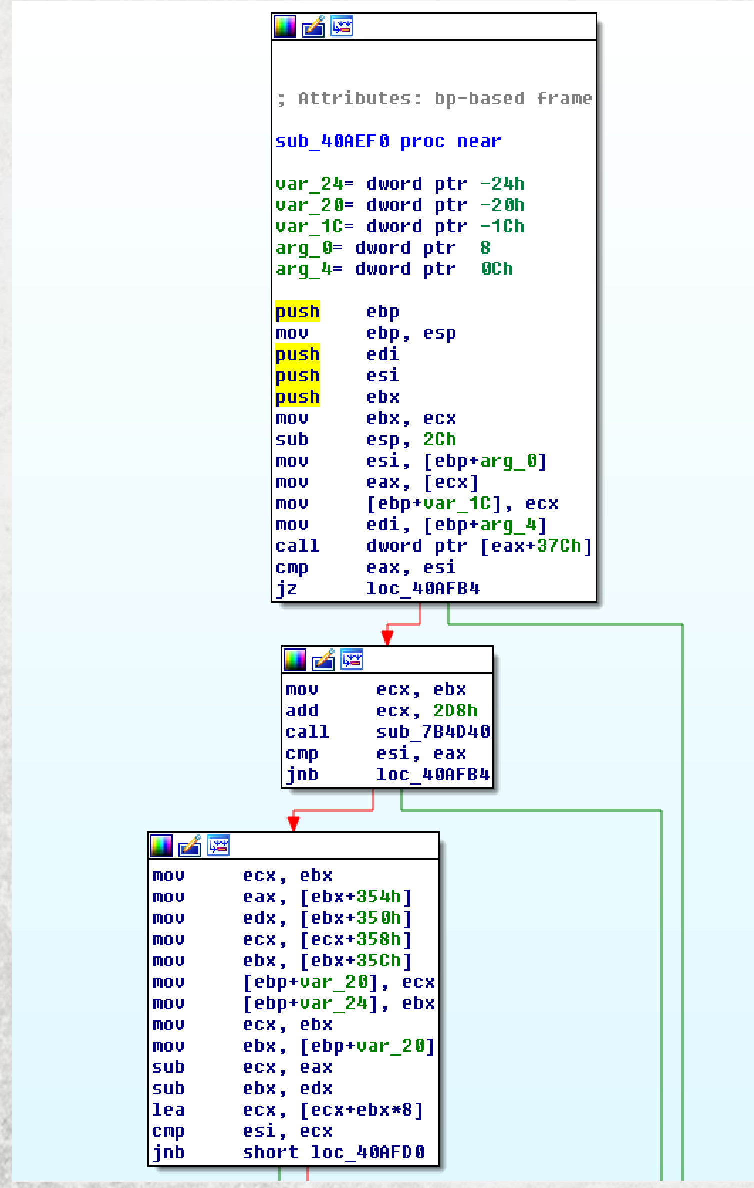
PACKERS OBFUSCATION

DÉTECTION DE PACKER, UNPACKING, DÉSOBFUSCATION, ETC.

ETC...

(ANTI-)DEBBUGING, (ANTI-)FORENSIC, HONEYPOTTING, SANDBOXING, ETC.

ANALYSE MANUELLE VS. AUTOMATISÉE

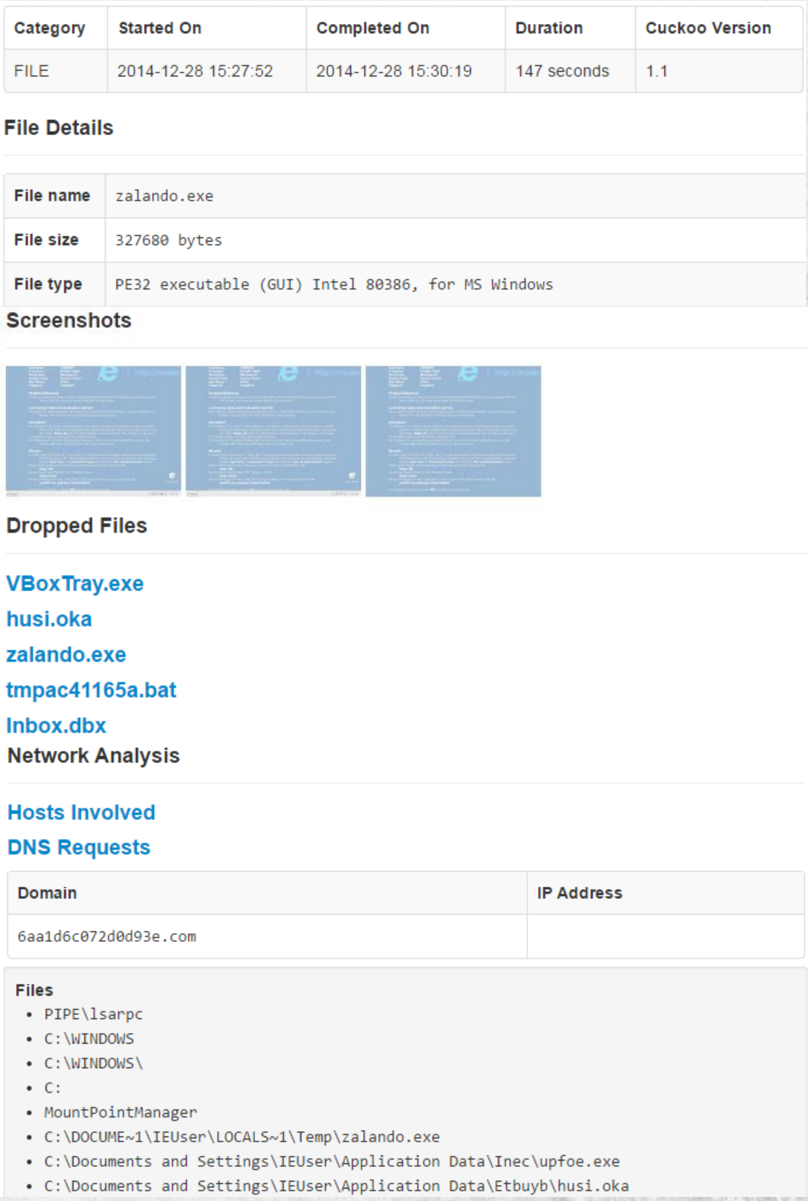


```
; Attributes: bp-based frame

sub_40AEF0 proc near

var_24= dword ptr -24h
var_20= dword ptr -20h
var_1C= dword ptr -1Ch
arg_0= dword ptr  8
arg_4= dword ptr  0Ch

push    ebp
mov     ebp, esp
push    edi
push    esi
push    ebx
mov     ebx, ecx
sub     esp, 2Ch
mov     esi, [ebp+arg_0]
mov     eax, [ecx]
mov     [ebp+var_1C], ecx
mov     edi, [ebp+arg_4]
call    dword ptr [eax+37Ch]
cmp     eax, esi
jz      loc_40AFB4
```

```
mov     ecx, ebx
add     ecx, 2D8h
call    sub_7B4D40
cmp     esi, eax
jnb     loc_40AFB4
```

```
mov     ecx, ebx
mov     eax, [ebx+354h]
mov     edx, [ebx+350h]
mov     ecx, [ecx+358h]
mov     ebx, [ebx+35Ch]
mov     [ebp+var_20], ecx
mov     [ebp+var_24], ebx
mov     ecx, ebx
mov     ebx, [ebp+var_20]
sub     ecx, eax
sub     ebx, edx
lea     ecx, [ecx+ebx*8]
cmp     esi, ecx
jnb     short loc_40AFD0
```

VS.



Category	Started On	Completed On	Duration	Cuckoo Version
FILE	2014-12-28 15:27:52	2014-12-28 15:30:19	147 seconds	1.1

File Details

File name	zalando.exe
File size	327680 bytes
File type	PE32 executable (GUI) Intel 80386, for MS Windows

Screenshots

Dropped Files

- VBoxTray.exe
- husi.oka
- zalando.exe
- tmpac41165a.bat
- Inbox.dbx

Network Analysis

Hosts Involved

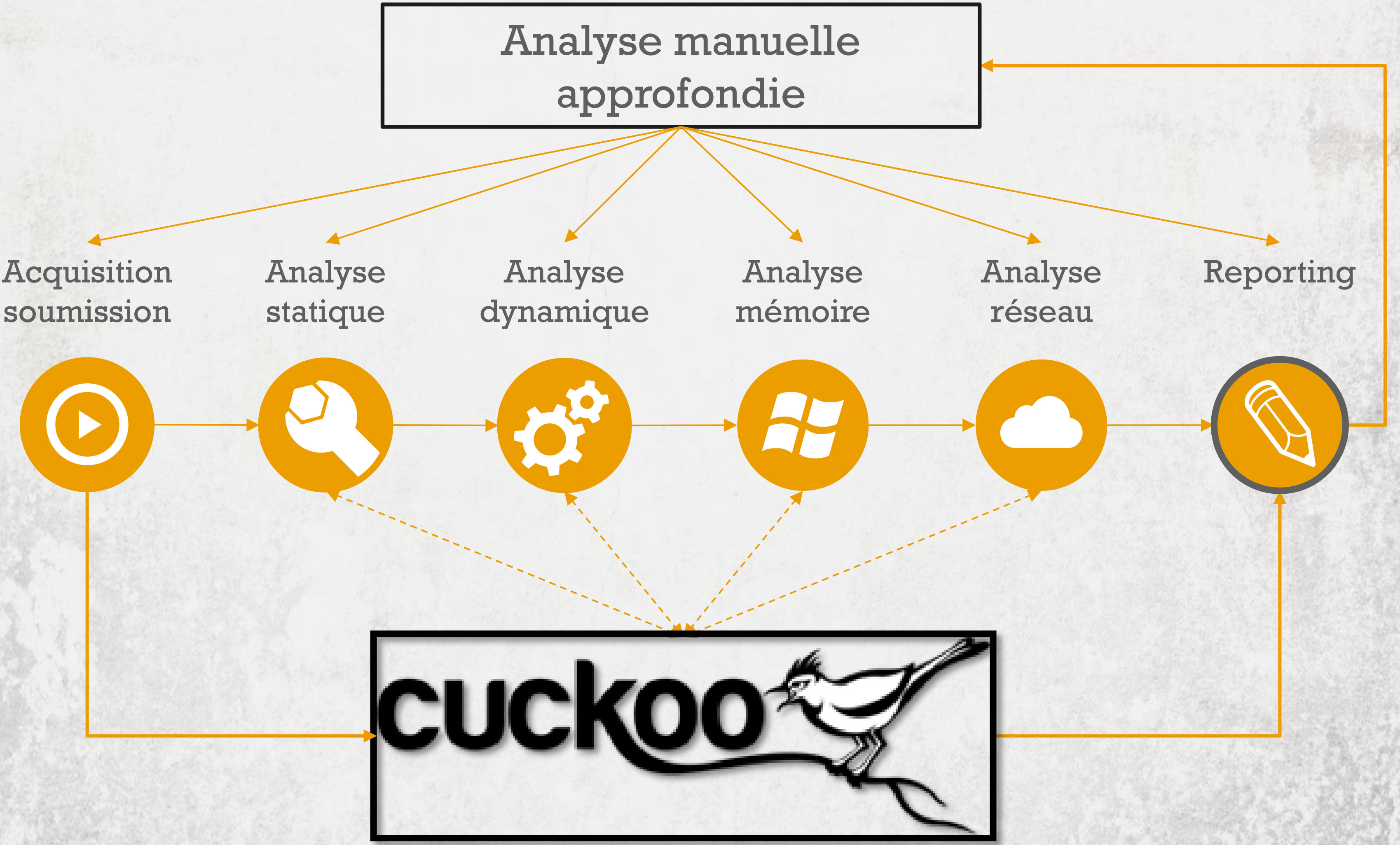
DNS Requests

Domain	IP Address
6aa1d6c072d0d93e.com	

Files

- PIPE\lsarpc
- C:\WINDOWS
- C:\WINDOWS\
- C:
- MountPointManager
- C:\DOCUME~1\IEUser\LOCALS~1\Temp\zalando.exe
- C:\Documents and Settings\IEUser\Application Data\Inec\upfoe.exe
- C:\Documents and Settings\IEUser\Application Data\Etbuyb\husi.oka

ANALYSE MANUELLE VS. AUTOMATISÉE



Analyse manuelle approfondie

Acquisition soumission

Analyse statique

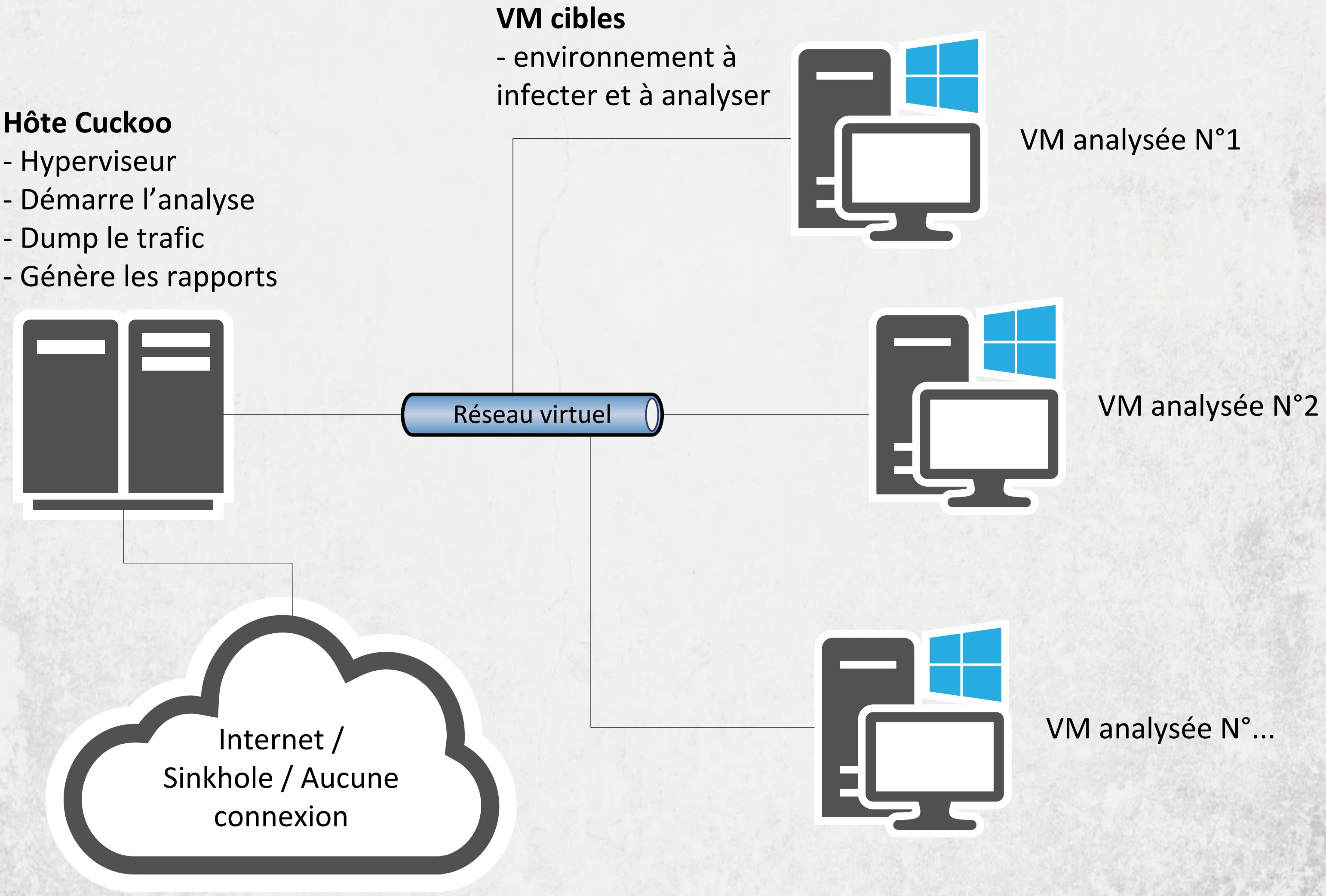
Analyse dynamique

Analyse mémoire

Analyse réseau

Reporting

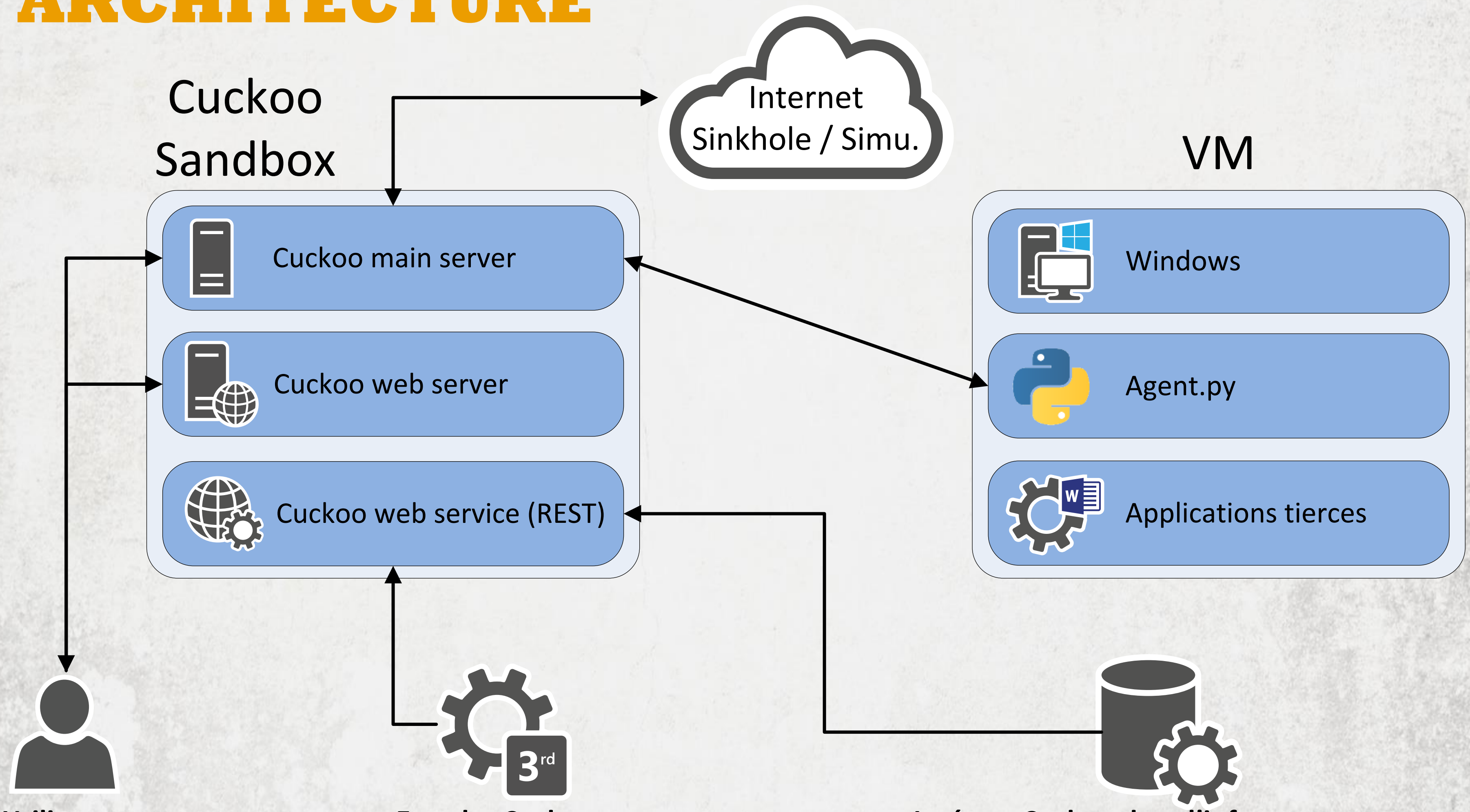
ARCHITECTURE



VM cibles
- environnement à infecter et à analyser

Hôte Cuckoo
- Hyperviseur
- Démarre l'analyse
- Dump le trafic
- Génère les rapports

ARCHITECTURE



Utilisateur

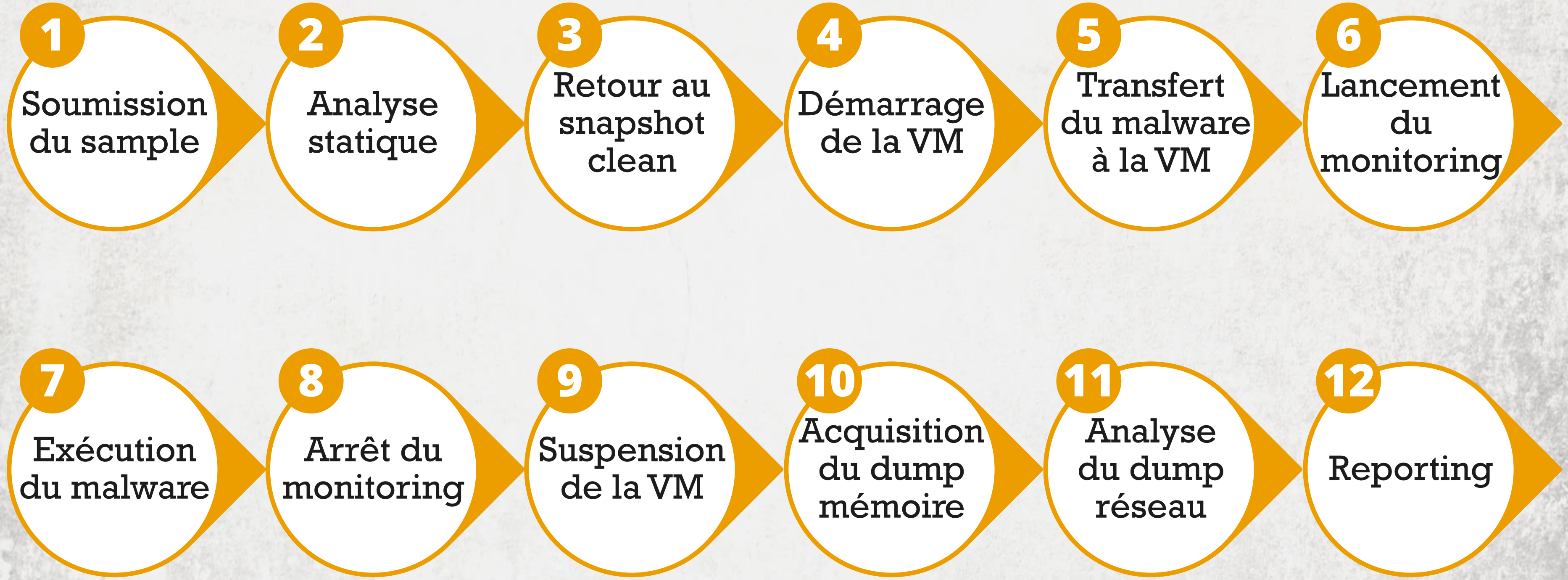
Etendre Cuckoo:

- Maltego
- El Jefe
- Etc...

Intégrer Cuckoo dans l'infrastructure:

- CuckooMX
- El Jefe
- SOC
- CERT, CSIRT
- Etc...

FLUX D’EXÉCUTION



1 Soumission du sample

2 Analyse statique

3 Retour au snapshot clean

4 Démarrage de la VM

5 Transfert du malware à la VM

6 Lancement du monitoring

7 Exécution du malware

8 Arrêt du monitoring

9 Suspension de la VM

10 Acquisition du dump mémoire

11 Analyse du dump réseau

12 Reporting

PRÉREQUIS (HÔTE)

Hardware :

- Les prérequis habituels pour de la virtualisation (CPU's, RAM et HDD)

Software :

- Linux (Debian, Ubuntu, etc.), Windows et MacOsX possibles en théorie.
- Un hyperviseur (Théoriquement ouvert à plusieurs système mais VirtualBox reste fortement conseillé).
- Python (version 2.7 fortement conseillée).
- SQLAlchemy, Python BSON, Tcpdump, Volatility, DPKT, Jinja2, Magic, Pydeep, MongoDB, Pymongo, Yara, Yara Python, Libvirt, Bottlepy, Django, Pefile, MAEC Python bindings, Chardet.

PRÉREQUIS OBLIGATOIRES (GUEST)

vHardware :

- Les prérequis habituels pour de la virtualisation (CPU’s, RAM et HDD).

Software :

- Windows XP SP3 (Windows 7, UAC désactivé).
- Logiciels tiers (Office, Adobe reader, navigateurs, etc.)
- Désactivation du firewall.
- Désactivation des mises à jour automatiques.
- Python 2.7 + PIL for Python.
- Cuckoo agent.py (agent.pyw).
- Paramétrer le réseau.
- Activer le login automatique.
- **SNAPSHOT!**

LA CONFIGURATION

6 fichiers de configuration principaux :

- ***cuckoo.conf*** **:** Configuration générale et options d'analyse.
- ***auxiliary.conf*** **:** Configuration des modules auxiliaires (ex: capture réseau).
- ***<machinery>.conf*** **:** Configuration de la virtualisation.
- ***memory.conf*** **:** Configuration de l'analyse mémoire (Volatility framework).
- ***processing.conf*** **:** Activation / désactivation des étapes d'analyse.
- ***reporting.conf*** **:** Configuration du reporting.

QUELQUES POINTS IMPORTANTS

Un environnement isolé n'est que rarement sûr à 100%:

- Cuckoo Sandbox (Evasion) : http://cuckoosandbox.org/2014-10-07-cuckoo-sandbox-111.html
- Oracle VirtualBox : CVE-2014-4261, CVE-2014-4228, CVE-2014-2489, etc…
- Instructions CPU non virtualisables, offloading (interface réseau)

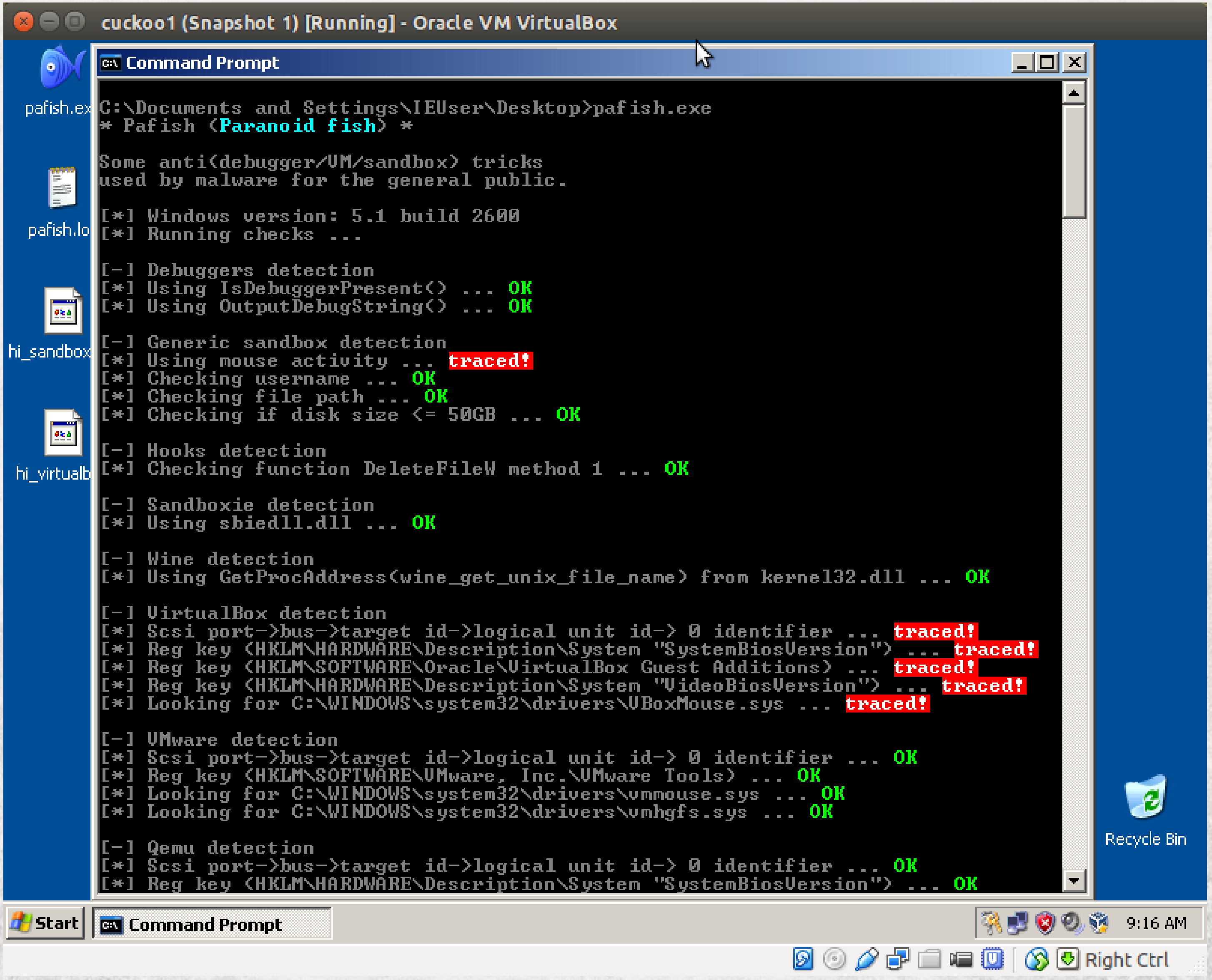
Lors de l'attribution de l'accès internet au malware, attention aux infections sur le LAN:

- Solution (partielle) : Simulation de services réseau (ex : InetSim)

Un environnement sandboxé et/ou virtualisé peut être détecté par certains malwares:

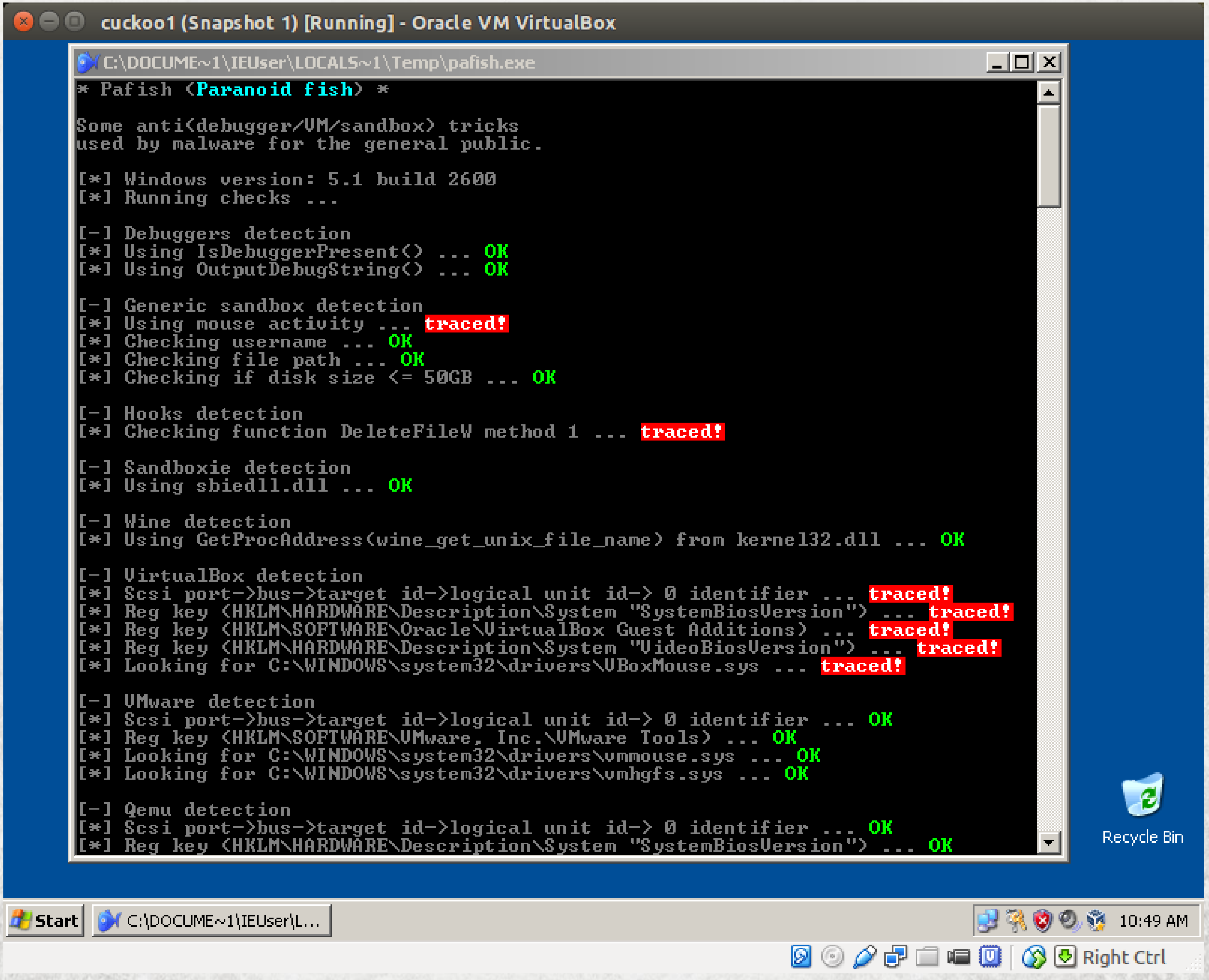
- Test : Pafish https://github.com/a0rtega/pafish
- Solution (partielle) : Zer0m0n ou Markedoe + tweak(s) manuel(s)…

ANTI DÉTECTION : VM



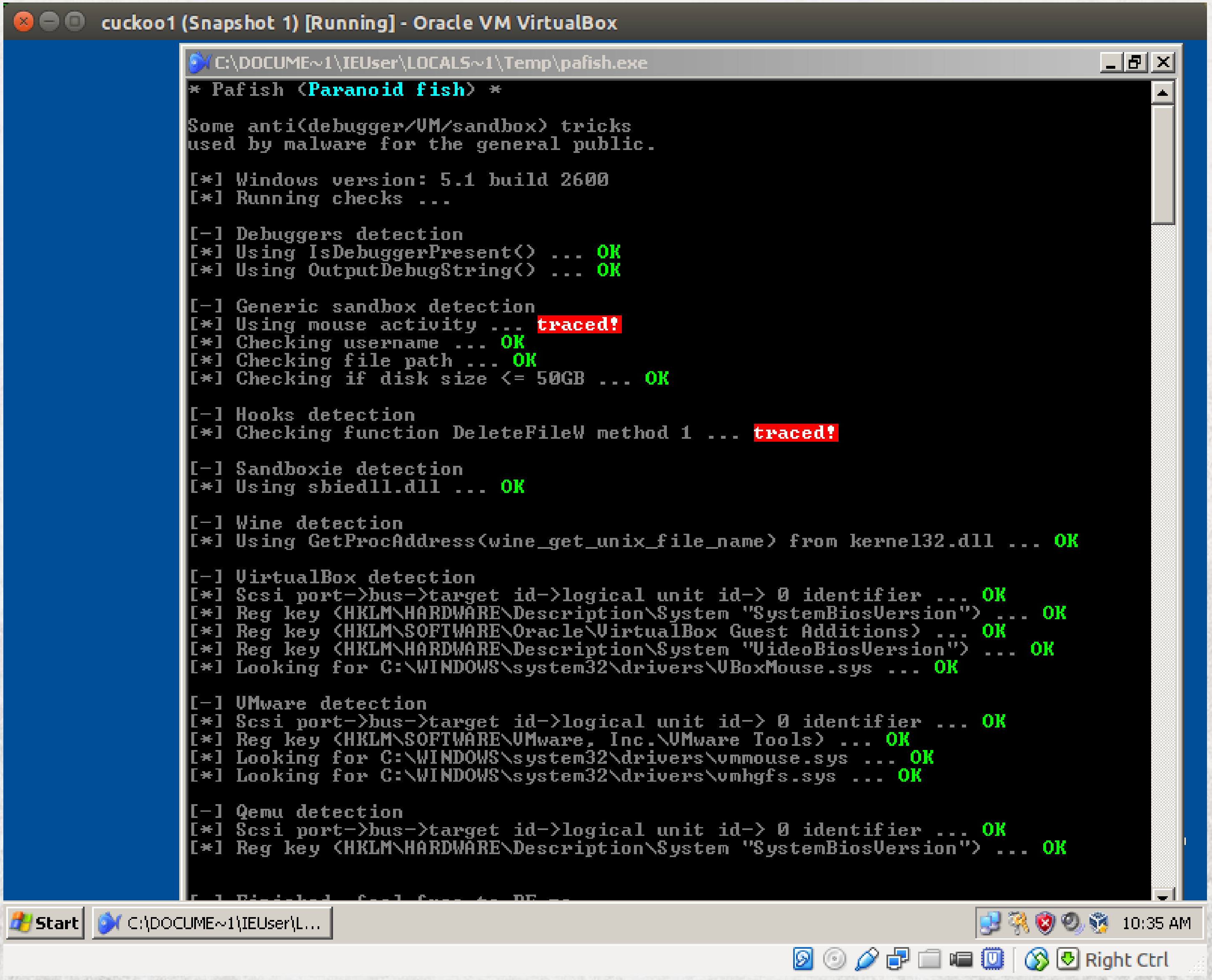
```
C:\Documents and Settings\IEUser\Desktop>pafish.exe
* Pafish (Paranoid fish) *

Some anti(debugger/VM/sandbox) tricks
used by malware for the general public.

[*] Windows version: 5.1 build 2600
[*] Running checks ...

[-] Debuggers detection
[*] Using IsDebuggerPresent() ... OK
[*] Using OutputDebugString() ... OK

[-] Generic sandbox detection
[*] Using mouse activity ... traced!
[*] Checking username ... OK
[*] Checking file path ... OK
[*] Checking if disk size <= 50GB ... OK

[-] Hooks detection
[*] Checking function DeleteFileW method 1 ... OK

[-] Sandboxie detection
[*] Using sbiedll.dll ... OK

[-] Wine detection
[*] Using GetProcAddress(wine_get_unix_file_name) from kernel32.dll ... OK

[-] VirtualBox detection
[*] Scsi port->bus->target id->logical unit id-> 0 identifier ... traced!
[*] Reg key (HKLM\HARDWARE\Description\System "SystemBiosVersion") ... traced!
[*] Reg key (HKLM\SOFTWARE\Oracle\VirtualBox Guest Additions) ... traced!
[*] Reg key (HKLM\HARDWARE\Description\System "VideoBiosVersion") ... traced!
[*] Looking for C:\WINDOWS\system32\drivers\VBoxMouse.sys ... traced!

[-] VMware detection
[*] Scsi port->bus->target id->logical unit id-> 0 identifier ... OK
[*] Reg key (HKLM\SOFTWARE\VMware, Inc.\VMware Tools) ... OK
[*] Looking for C:\WINDOWS\system32\drivers\vmmouse.sys ... OK
[*] Looking for C:\WINDOWS\system32\drivers\vmhgfs.sys ... OK

[-] Qemu detection
[*] Scsi port->bus->target id->logical unit id-> 0 identifier ... OK
[*] Reg key (HKLM\HARDWARE\Description\System "SystemBiosVersion") ... OK
```

ANTI DÉTECTION : VM + CUCKOO


cuckoo1 (Snapshot 1) [Running] - Oracle VM VirtualBox
C:\DOCUME~1\IEUser\LOCALS~1\Temp\pafish.exe
Recycle Bin
Start
C:\DOCUME~1\IEUser\L...
10:49 AM
Right Ctrl

```
* Pafish (Paranoid fish) *

Some anti(debugger/VM/sandbox) tricks
used by malware for the general public.

[*] Windows version: 5.1 build 2600
[*] Running checks ...

[-] Debuggers detection
[*] Using IsDebuggerPresent() ... OK
[*] Using OutputDebugString() ... OK

[-] Generic sandbox detection
[*] Using mouse activity ... traced!
[*] Checking username ... OK
[*] Checking file path ... OK
[*] Checking if disk size <= 50GB ... OK

[-] Hooks detection
[*] Checking function DeleteFileW method 1 ... traced!

[-] Sandboxie detection
[*] Using sbiedll.dll ... OK

[-] Wine detection
[*] Using GetProcAddress(wine_get_unix_file_name) from kernel32.dll ... OK

[-] VirtualBox detection
[*] Scsi port->bus->target id->logical unit id-> 0 identifier ... traced!
[*] Reg key (HKLM\HARDWARE\Description\System "SystemBiosVersion") ... traced!
[*] Reg key (HKLM\SOFTWARE\Oracle\VirtualBox Guest Additions) ... traced!
[*] Reg key (HKLM\HARDWARE\Description\System "VideoBiosVersion") ... traced!
[*] Looking for C:\WINDOWS\system32\drivers\VBoxMouse.sys ... traced!

[-] VMware detection
[*] Scsi port->bus->target id->logical unit id-> 0 identifier ... OK
[*] Reg key (HKLM\SOFTWARE\VMware, Inc.\VMware Tools) ... OK
[*] Looking for C:\WINDOWS\system32\drivers\vmmouse.sys ... OK
[*] Looking for C:\WINDOWS\system32\drivers\vmhgfs.sys ... OK

[-] Qemu detection
[*] Scsi port->bus->target id->logical unit id-> 0 identifier ... OK
[*] Reg key (HKLM\HARDWARE\Description\System "SystemBiosVersion") ... OK
```

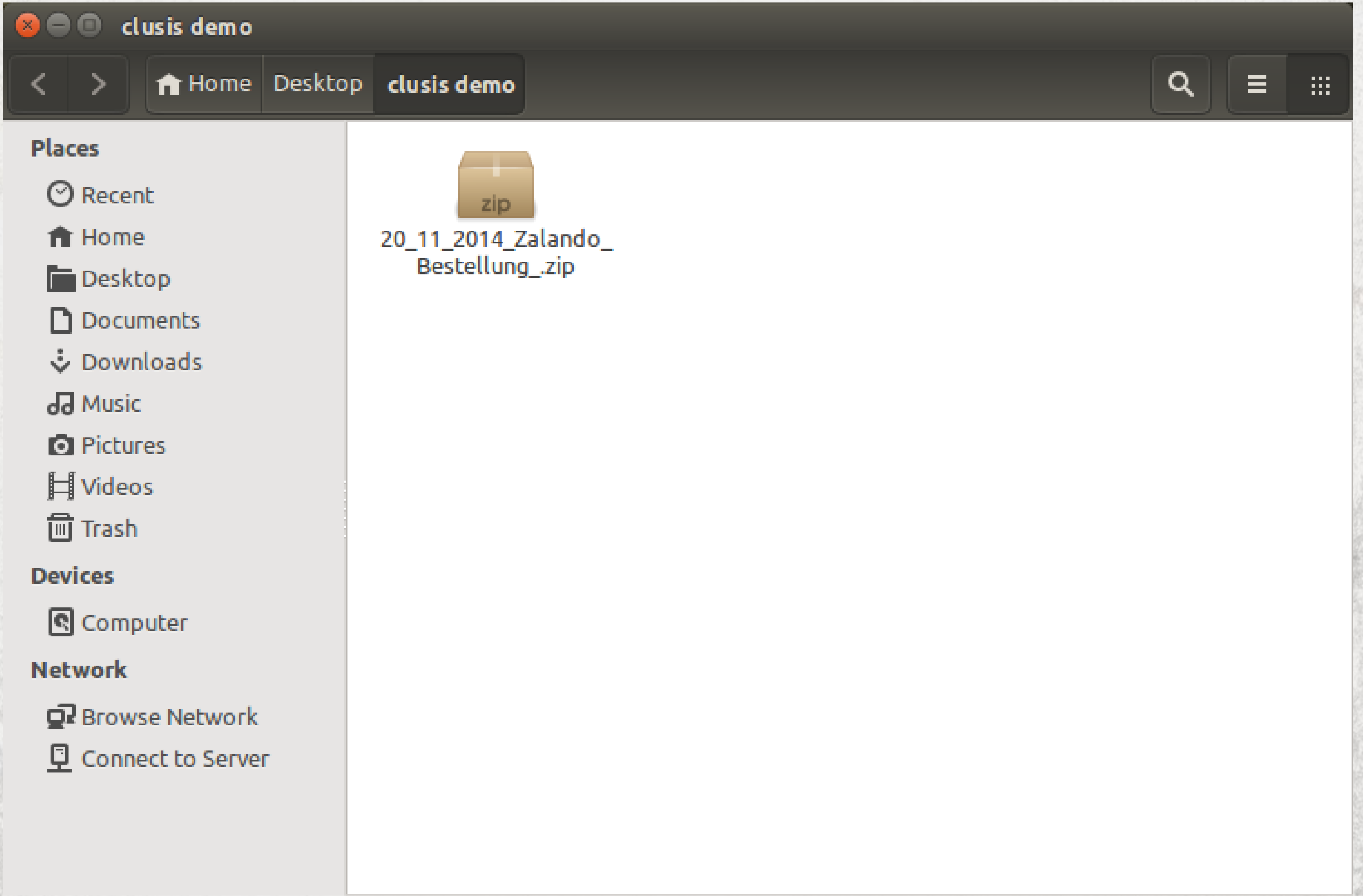
DÉTECTION : VM + CUCKOO + TWEAKING


cuckoo1 (Snapshot 1) [Running] - Oracle VM VirtualBox
C:\DOCUME~1\IEUser\LOCALS~1\Temp\pafish.exe
Start
C:\DOCUME~1\IEUser\L...
10:35 AM
Right Ctrl

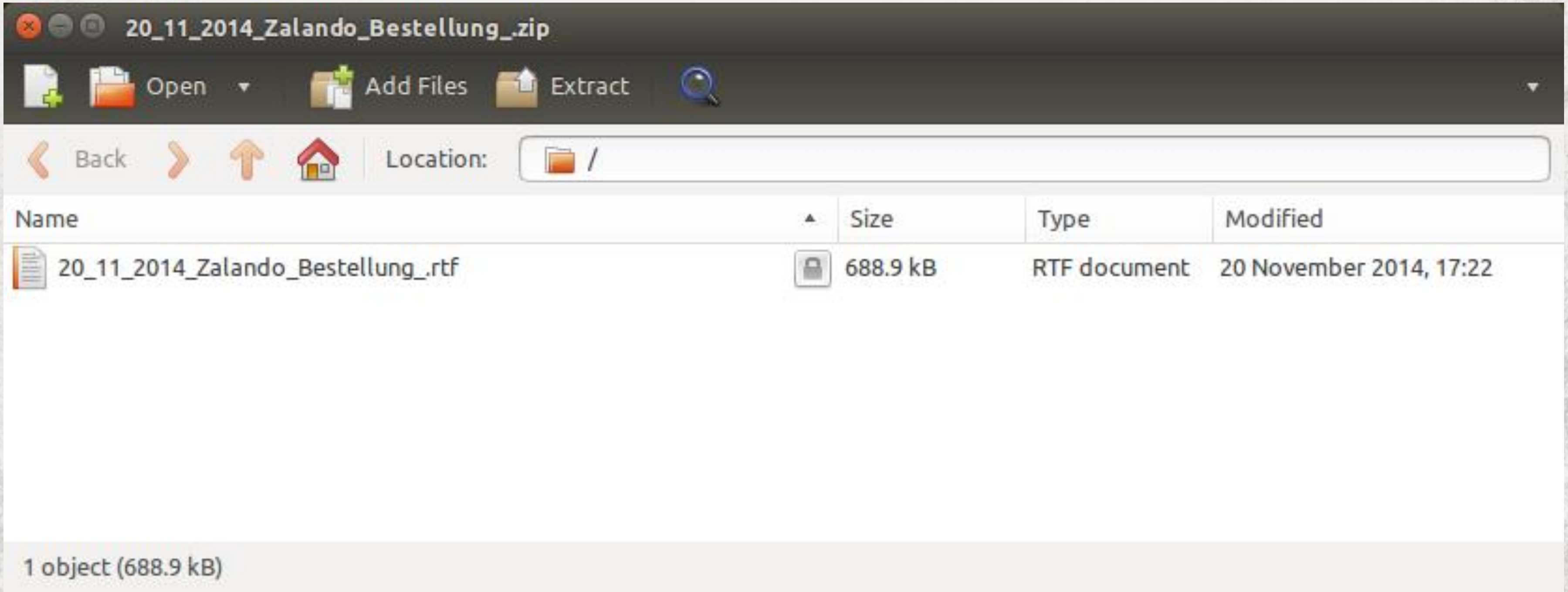
```
* Pafish (Paranoid fish) *

Some anti(debugger/VM/sandbox) tricks
used by malware for the general public.

[*] Windows version: 5.1 build 2600
[*] Running checks ...

[-] Debuggers detection
[*] Using IsDebuggerPresent() ... OK
[*] Using OutputDebugString() ... OK

[-] Generic sandbox detection
[*] Using mouse activity ... traced!
[*] Checking username ... OK
[*] Checking file path ... OK
[*] Checking if disk size <= 50GB ... OK

[-] Hooks detection
[*] Checking function DeleteFileW method 1 ... traced!

[-] Sandboxie detection
[*] Using sbiedll.dll ... OK

[-] Wine detection
[*] Using GetProcAddress(wine_get_unix_file_name) from kernel32.dll ... OK

[-] VirtualBox detection
[*] Scsi port->bus->target id->logical unit id-> 0 identifier ... OK
[*] Reg key (HKLM\HARDWARE\Description\System "SystemBiosVersion") ... OK
[*] Reg key (HKLM\SOFTWARE\Oracle\VirtualBox Guest Additions) ... OK
[*] Reg key (HKLM\HARDWARE\Description\System "VideoBiosVersion") ... OK
[*] Looking for C:\WINDOWS\system32\drivers\VBoxMouse.sys ... OK

[-] VMware detection
[*] Scsi port->bus->target id->logical unit id-> 0 identifier ... OK
[*] Reg key (HKLM\SOFTWARE\VMware, Inc.\VMware Tools) ... OK
[*] Looking for C:\WINDOWS\system32\drivers\vmmouse.sys ... OK
[*] Looking for C:\WINDOWS\system32\drivers\vmhgfs.sys ... OK

[-] Qemu detection
[*] Scsi port->bus->target id->logical unit id-> 0 identifier ... OK
[*] Reg key (HKLM\HARDWARE\Description\System "SystemBiosVersion") ... OK


[-] Finished, feel free to RE me.
```

IT'S DEMO TIME!

La facture Zalando



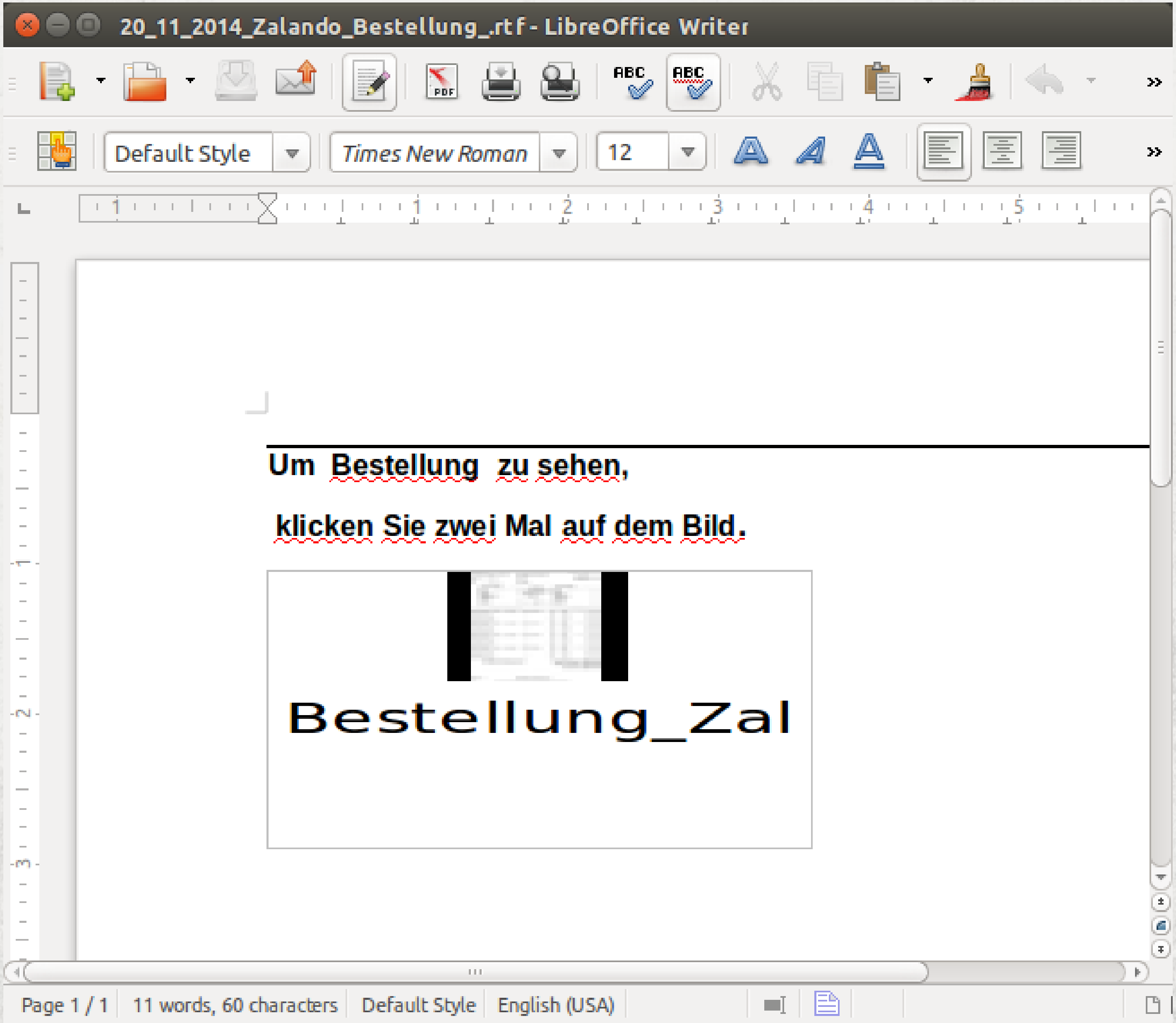
clusis demo
Home
Desktop
clusis demo
Places
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
Devices
Computer
Network
Browse Network
Connect to Server
zip
20_11_2014_Zalando_Bestellung_.zip



20_11_2014_Zalando_Bestellung_.zip

Name	Size	Type	Modified
20_11_2014_Zalando_Bestellung_.rtf	688.9 kB	RTF document	20 November 2014, 17:22

1 object (688.9 kB)

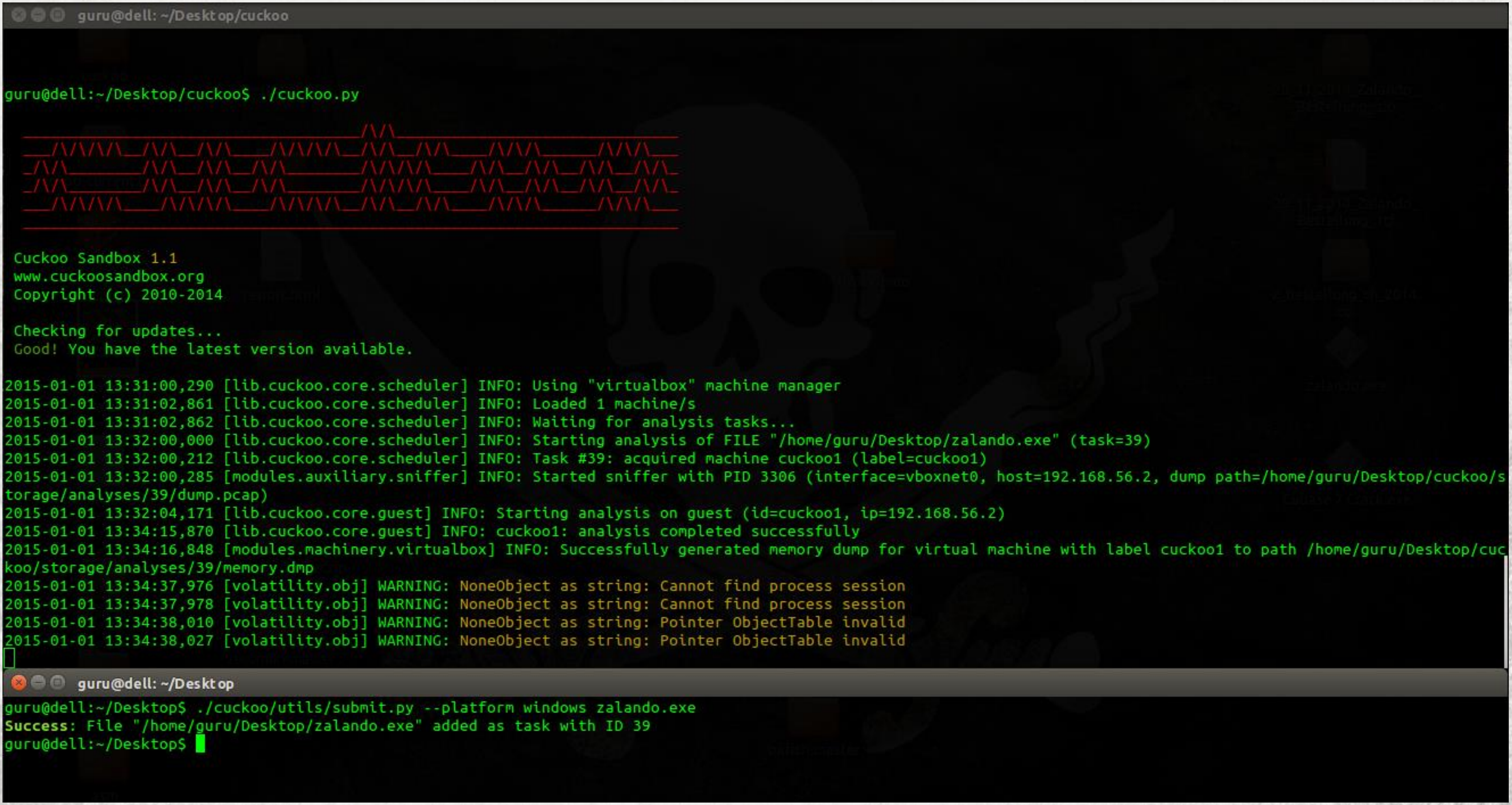


20_11_2014_Zalando_Bestellung_.rtf - LibreOffice Writer

Um Bestellung zu sehen,

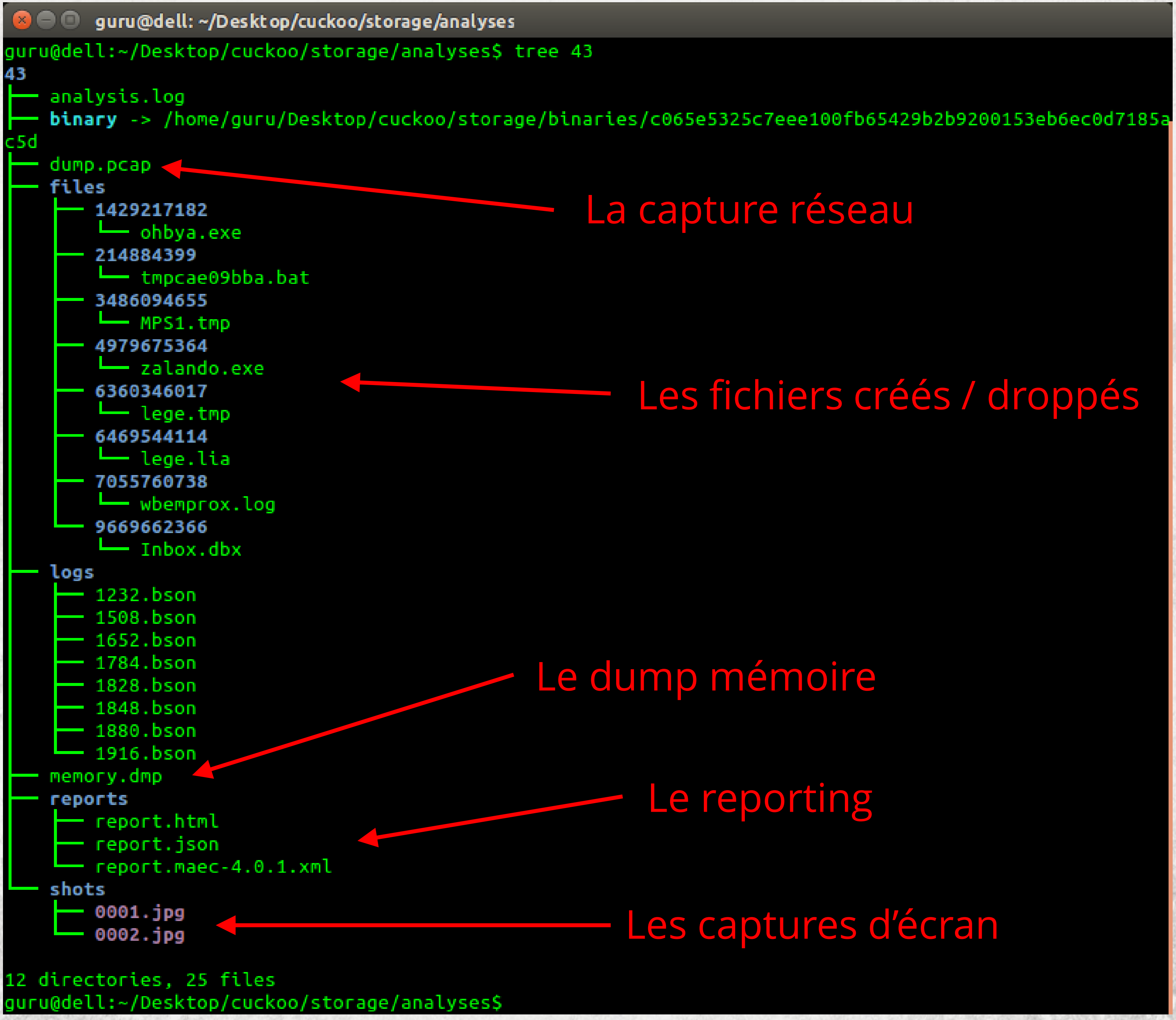
klicken Sie zwei Mal auf dem Bild.

Bestellung_Zal



```
guru@dell:~/Desktop/cuckoo$ ./cuckoo.py

  _____________________________________/\/\________________________________
  ___/\/\/\/\__/\/\__/\/\____/\/\/\/\__/\/\__/\/\____/\/\/\______/\/\/\____
  _/\/\________/\/\__/\/\__/\/\________/\/\/\/\____/\/\__/\/\__/\/\__/\/\_
  _/\/\________/\/\__/\/\__/\/\________/\/\/\/\____/\/\__/\/\__/\/\__/\/\_
  ___/\/\/\/\____/\/\/\/\____/\/\/\/\__/\/\__/\/\____/\/\/\______/\/\/\____
  _________________________________________________________________________

 Cuckoo Sandbox 1.1
 www.cuckoosandbox.org
 Copyright (c) 2010-2014

 Checking for updates...
 Good! You have the latest version available.

2015-01-01 13:31:00,290 [lib.cuckoo.core.scheduler] INFO: Using "virtualbox" machine manager
2015-01-01 13:31:02,861 [lib.cuckoo.core.scheduler] INFO: Loaded 1 machine/s
2015-01-01 13:31:02,862 [lib.cuckoo.core.scheduler] INFO: Waiting for analysis tasks...
2015-01-01 13:32:00,000 [lib.cuckoo.core.scheduler] INFO: Starting analysis of FILE "/home/guru/Desktop/zalando.exe" (task=39)
2015-01-01 13:32:00,212 [lib.cuckoo.core.scheduler] INFO: Task #39: acquired machine cuckoo1 (label=cuckoo1)
2015-01-01 13:32:00,285 [modules.auxiliary.sniffer] INFO: Started sniffer with PID 3306 (interface=vboxnet0, host=192.168.56.2, dump path=/home/guru/Desktop/cuckoo/s
torage/analyses/39/dump.pcap)
2015-01-01 13:32:04,171 [lib.cuckoo.core.guest] INFO: Starting analysis on guest (id=cuckoo1, ip=192.168.56.2)
2015-01-01 13:34:15,870 [lib.cuckoo.core.guest] INFO: cuckoo1: analysis completed successfully
2015-01-01 13:34:16,848 [modules.machinery.virtualbox] INFO: Successfully generated memory dump for virtual machine with label cuckoo1 to path /home/guru/Desktop/cuc
koo/storage/analyses/39/memory.dmp
2015-01-01 13:34:37,976 [volatility.obj] WARNING: NoneObject as string: Cannot find process session
2015-01-01 13:34:37,978 [volatility.obj] WARNING: NoneObject as string: Cannot find process session
2015-01-01 13:34:38,010 [volatility.obj] WARNING: NoneObject as string: Pointer ObjectTable invalid
2015-01-01 13:34:38,027 [volatility.obj] WARNING: NoneObject as string: Pointer ObjectTable invalid
```

```
guru@dell:~/Desktop$ ./cuckoo/utils/submit.py --platform windows zalando.exe
Success: File "/home/guru/Desktop/zalando.exe" added as task with ID 39
guru@dell:~/Desktop$
```



```
guru@dell:~/Desktop/cuckoo/storage/analyses$ tree 43
43
├── analysis.log
├── binary -> /home/guru/Desktop/cuckoo/storage/binaries/c065e5325c7eee100fb65429b2b9200153eb6ec0d7185a
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

12 directories, 25 files
guru@dell:~/Desktop/cuckoo/storage/analyses$
```

La capture réseau

Les fichiers créés / droppés

Le dump mémoire

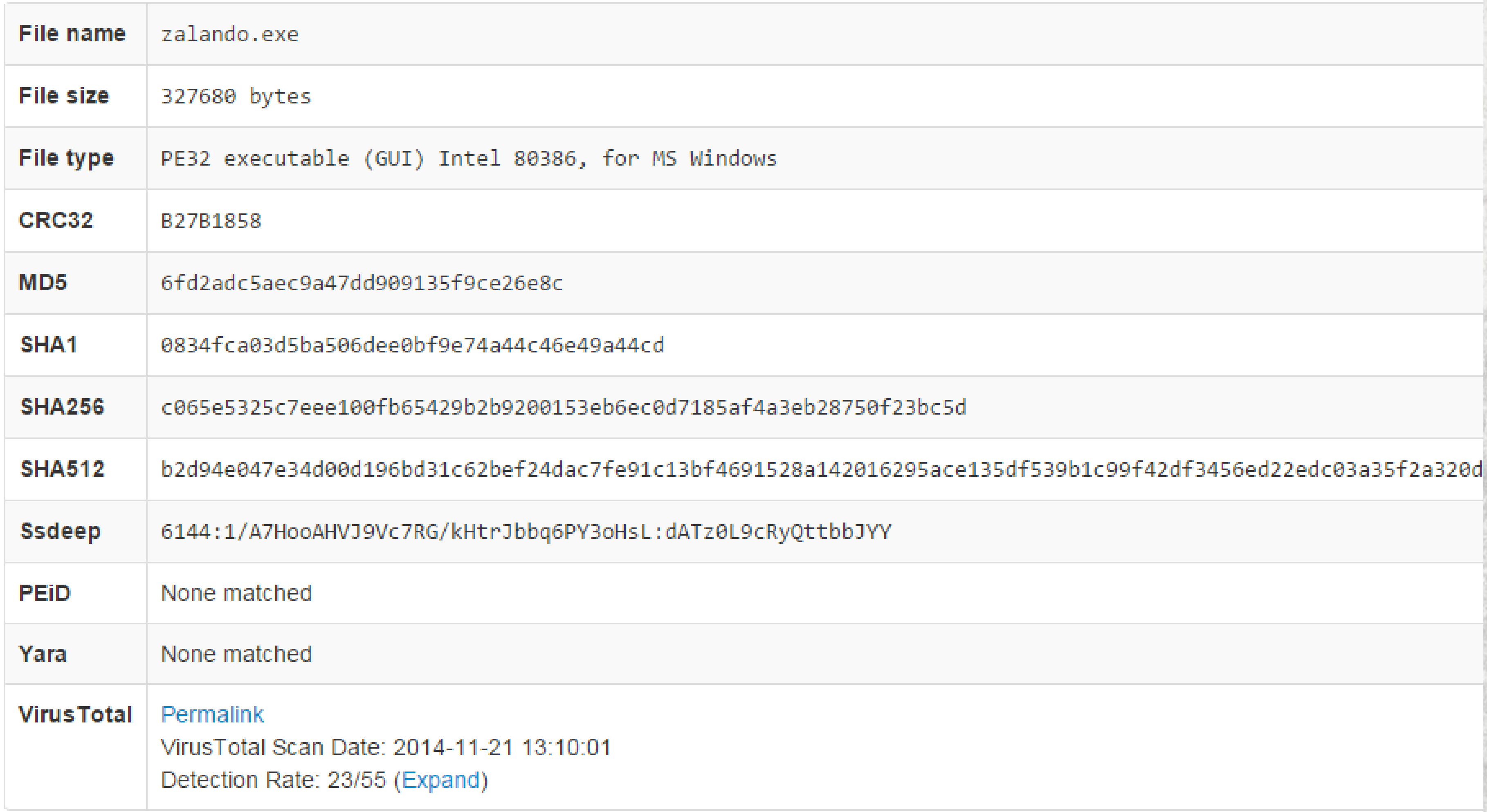
Le reporting

Les captures d'écran

Super, mais j’aime pas les lignes de commandes…

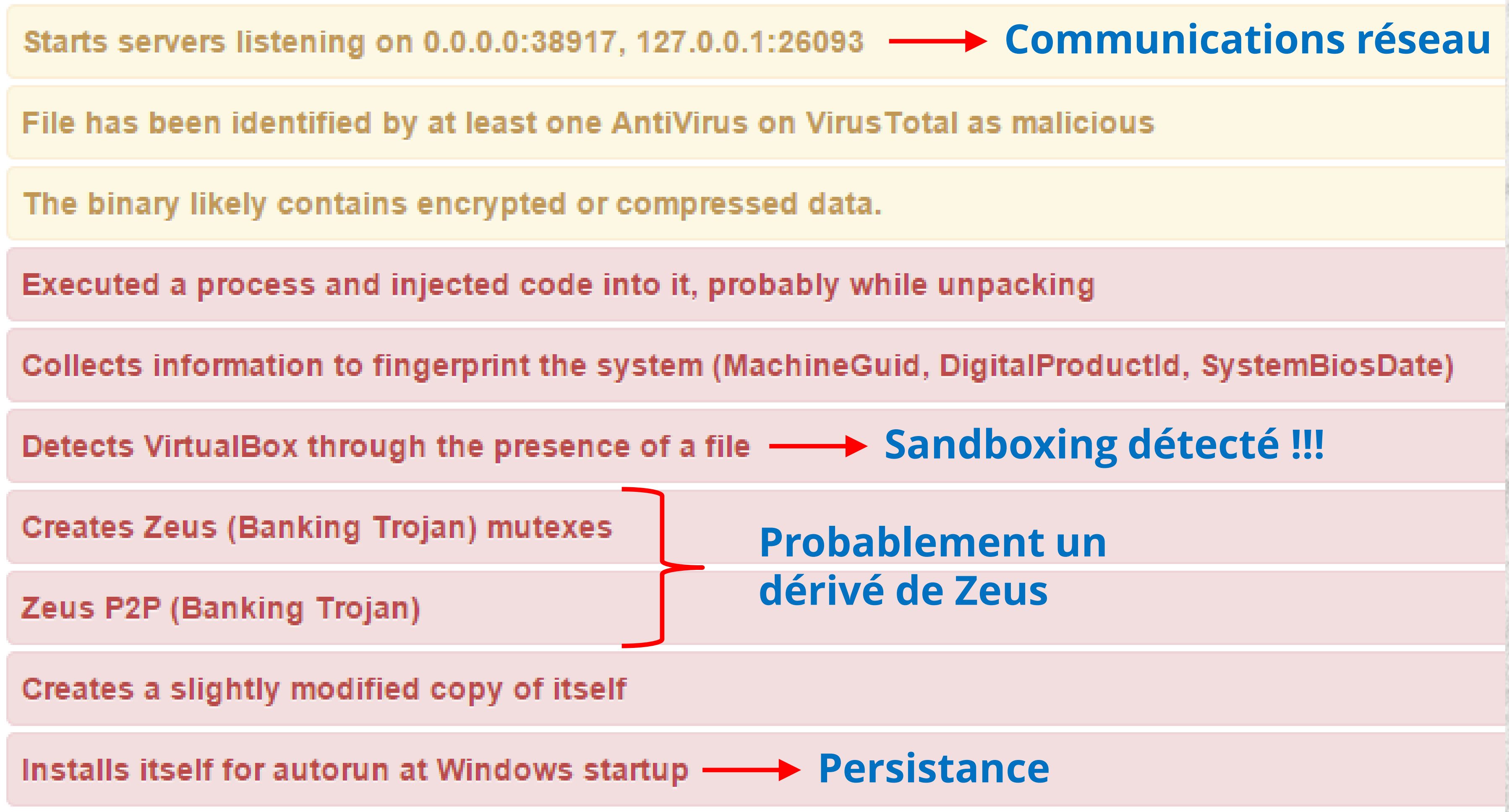
LE REPORTING

CARACTÉRISTIQUES DU FICHIER



File name	zalando.exe
File size	327680 bytes
File type	PE32 executable (GUI) Intel 80386, for MS Windows
CRC32	B27B1858
MD5	6fd2adc5aec9a47dd909135f9ce26e8c
SHA1	0834fca03d5ba506dee0bf9e74a44c46e49a44cd
SHA256	c065e5325c7eee100fb65429b2b9200153eb6ec0d7185af4a3eb28750f23bc5d
SHA512	b2d94e047e34d00d196bd31c62bef24dac7fe91c13bf4691528a142016295ace135df539b1c99f42df3456ed22edc03a35f2a320d
Ssdeep	6144:1/A7HooAHVJ9Vc7RG/kHtrJbbq6PY3oHsL:dATz0L9cRyQttbbJYY
PEiD	None matched
Yara	None matched
VirusTotal	Permalink VirusTotal Scan Date: 2014-11-21 13:10:01 Detection Rate: 23/55 (Expand)

LES SIGNATURES



Starts servers listening on 0.0.0.0:38917, 127.0.0.1:26093 → Communications réseau

File has been identified by at least one AntiVirus on VirusTotal as malicious

The binary likely contains encrypted or compressed data.

Executed a process and injected code into it, probably while unpacking

Collects information to fingerprint the system (MachineGuid, DigitalProductId, SystemBiosDate)

Detects VirtualBox through the presence of a file → Sandboxing détecté !!!

Creates Zeus (Banking Trojan) mutexes

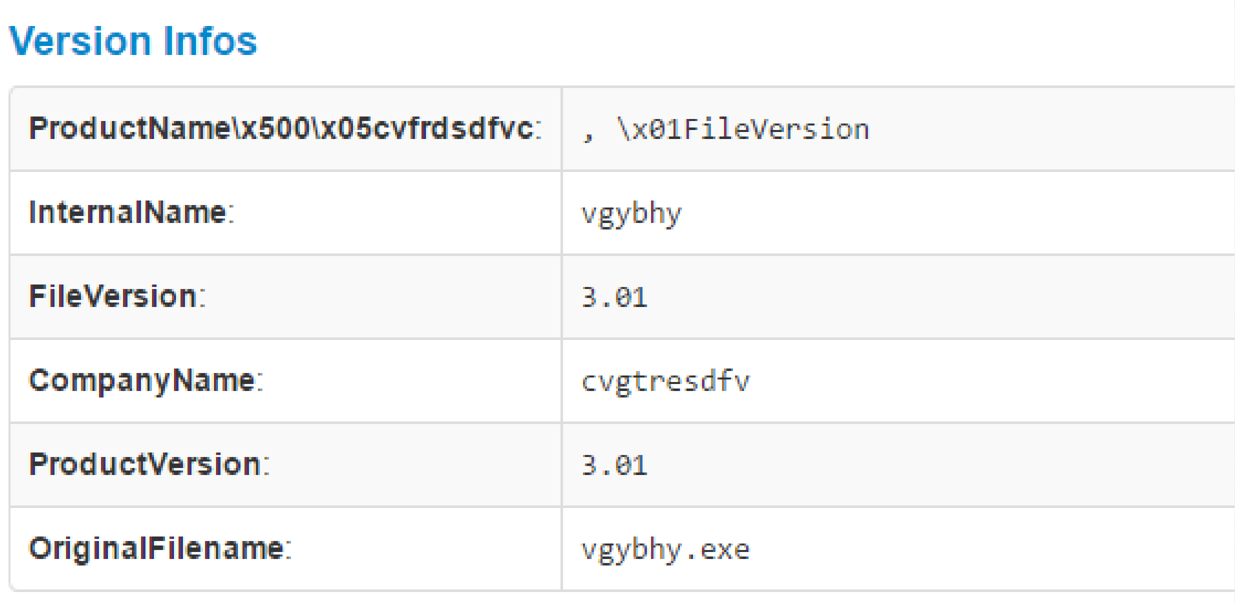
Zeus P2P (Banking Trojan)

Probablement un dérivé de Zeus

Creates a slightly modified copy of itself

Installs itself for autorun at Windows startup → Persistance

L'ANALYSE STATIQUE



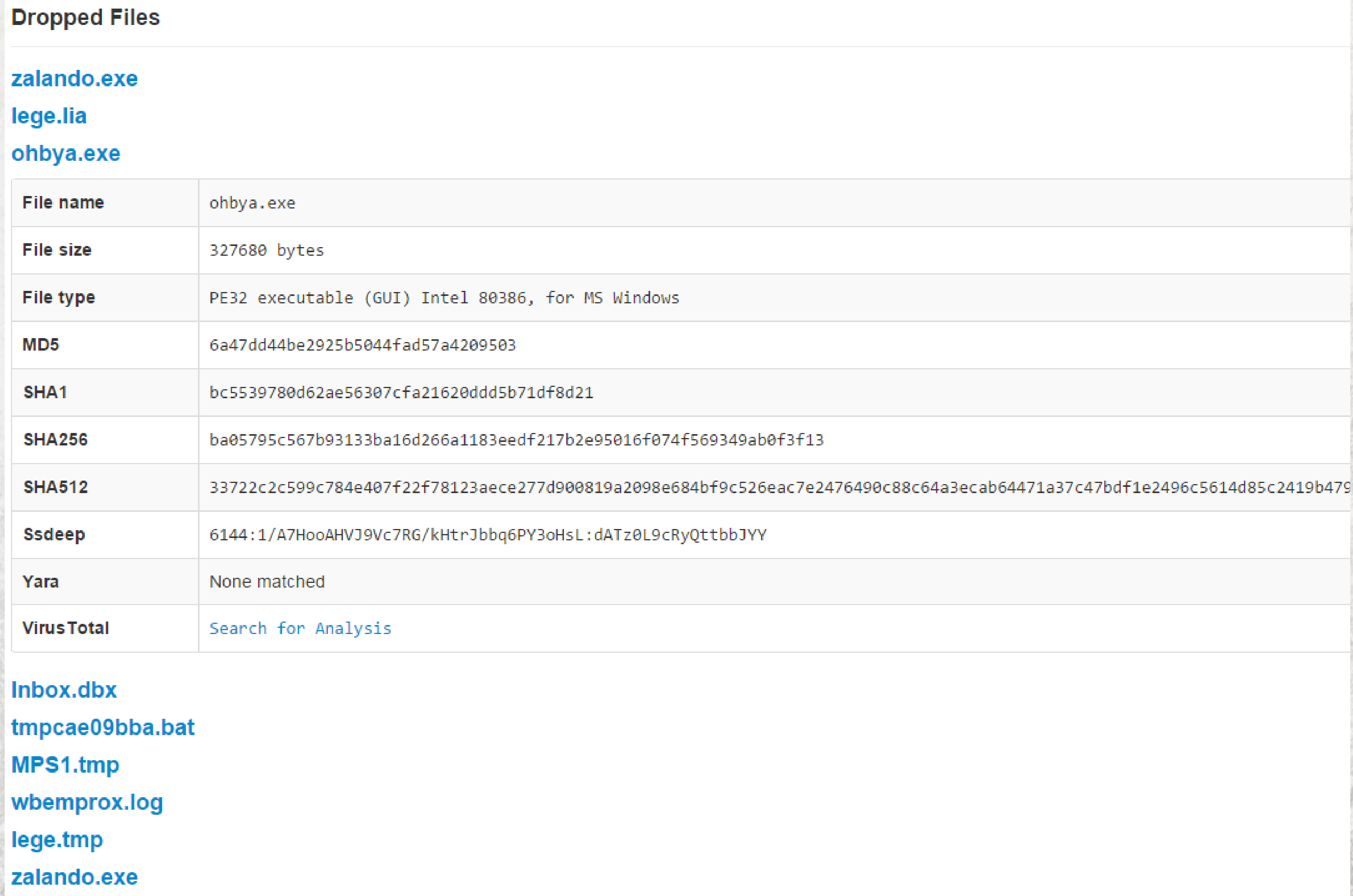
Version Infos

ProductName\x500\x05cvfrdsdfvc:	, \x01FileVersion
InternalName:	vgybhy
FileVersion:	3.01
CompanyName:	cvgtresdfv
ProductVersion:	3.01
OriginalFilename:	vgybhy.exe

Quelques chaînes de caractères intéressantes :

- *\AC:\FA2\C7\YkYW.vbp
- vgybhy, fvgdcf, cvfdezcvg, uhuihiuh, cvfrdsdfvc
- Etc...

LES FICHIERS CRÉÉS / DROPPÉS



Dropped Files

zalando.exe

lege.lia

ohbya.exe

File name	ohbya.exe
File size	327680 bytes
File type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	6a47dd44be2925b5044fad57a4209503
SHA1	bc5539780d62ae56307cfa21620ddd5b71df8d21
SHA256	ba05795c567b93133ba16d266a1183eedf217b2e95016f074f569349ab0f3f13
SHA512	33722c2c599c784e407f22f78123aece277d900819a2098e684bf9c526eac7e2476490c88c64a3ecab64471a37c47bdf1e2496c5614d85c2419b479
Ssdeep	6144:1/A7HooAHVJ9Vc7RG/kHtrJbbq6PY3oHsL:dATz0L9cRyQttbbJYY
Yara	None matched
VirusTotal	Search for Analysis

Inbox.dbx

tmpcae09bba.bat

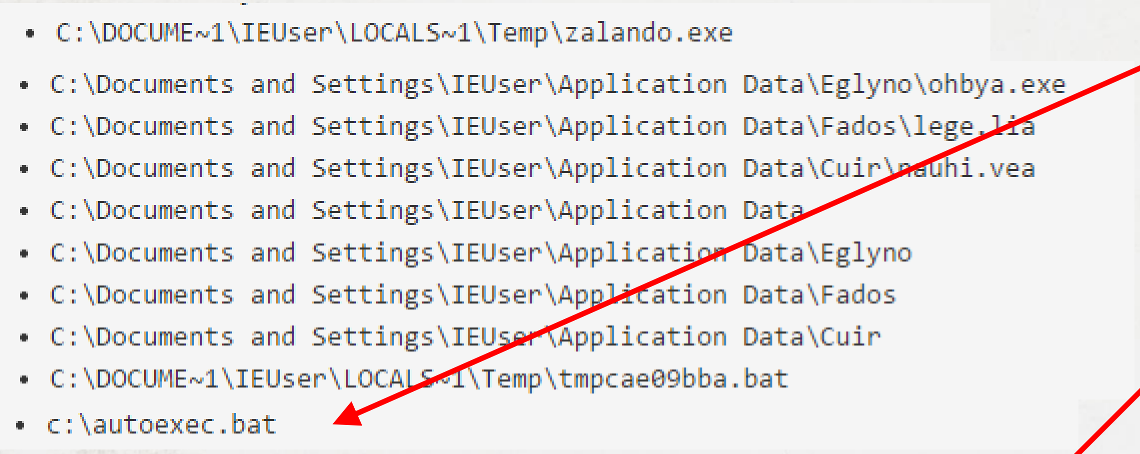
MPS1.tmp

wbemprox.log

lege.tmp

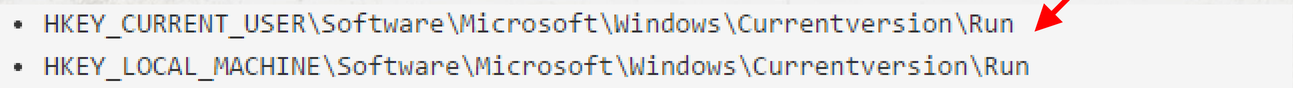
zalando.exe

L’ANALYSE DYNAMIQUE



- C:\DOCUME~1\IEUser\LOCALS~1\Temp\zalando.exe
- C:\Documents and Settings\IEUser\Application Data\Eglyno\ohbya.exe
- C:\Documents and Settings\IEUser\Application Data\Fados\lege.lia
- C:\Documents and Settings\IEUser\Application Data\Cuir\nauhi.vea
- C:\Documents and Settings\IEUser\Application Data
- C:\Documents and Settings\IEUser\Application Data\Eglyno
- C:\Documents and Settings\IEUser\Application Data\Fados
- C:\Documents and Settings\IEUser\Application Data\Cuir
- C:\DOCUME~1\IEUser\LOCALS~1\Temp\tmpcae09bba.bat
- c:\autoexec.bat

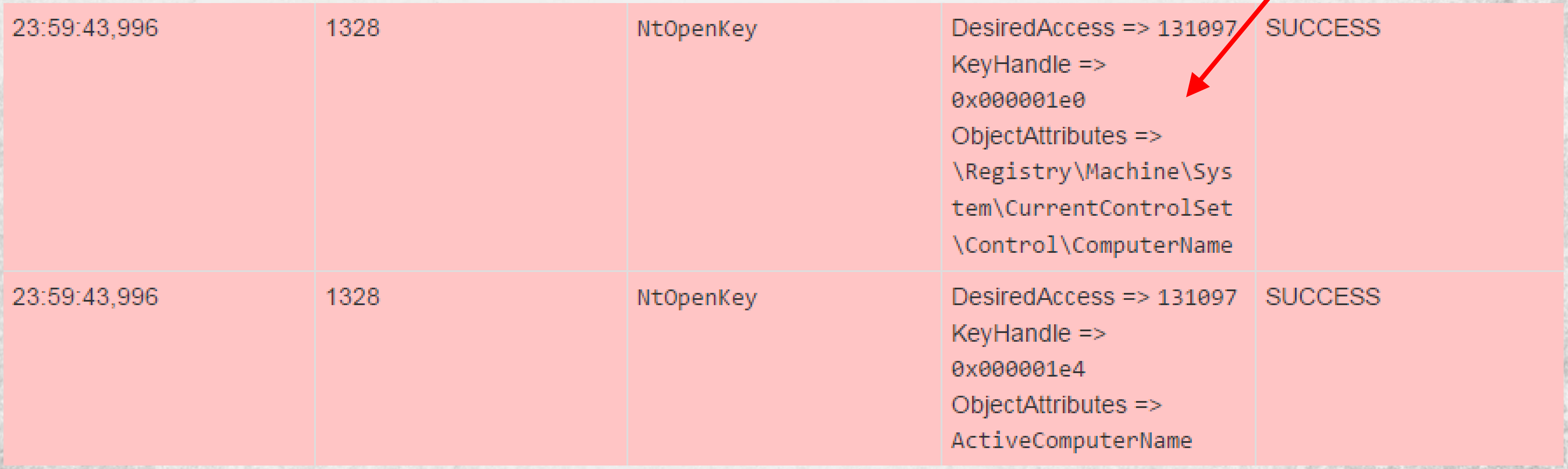
Exécution d’opérations au démarrage et/ou persistance



- HKEY_CURRENT_USER\Software\Microsoft\Windows\Currentversion\Run
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Currentversion\Run

Persistance

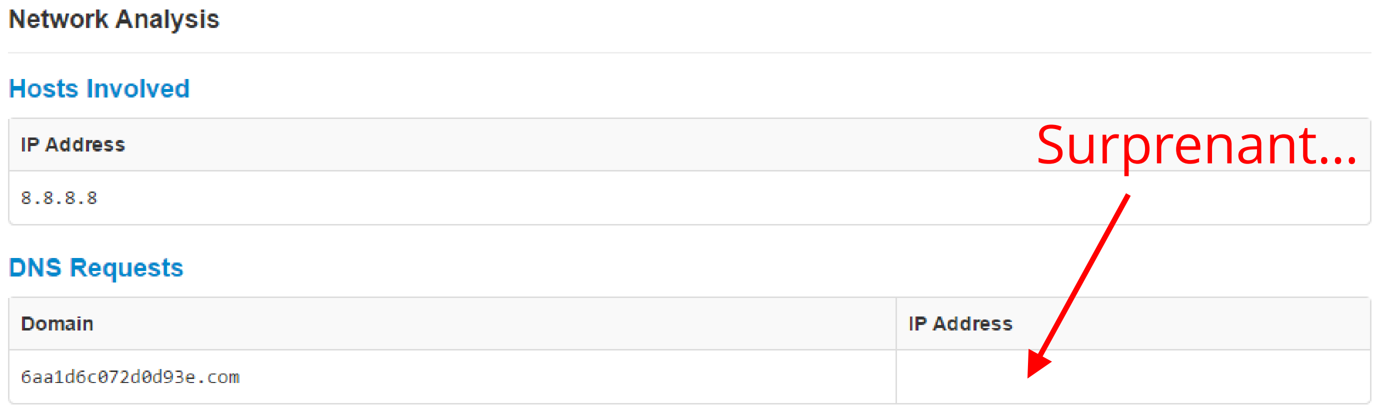
Récupération du nom de la machine



23:59:43,996	1328	NtOpenKey	DesiredAccess => 131097
			KeyHandle => 0x000001e0
			ObjectAttributes => \Registry\Machine\System\CurrentControlSet\Control\ComputerName
				SUCCESS

23:59:43,996	1328	NtOpenKey	DesiredAccess => 131097
			KeyHandle => 0x000001e4
			ObjectAttributes => ActiveComputerName
				SUCCESS

L'ANALYSE RÉSEAU



Network Analysis

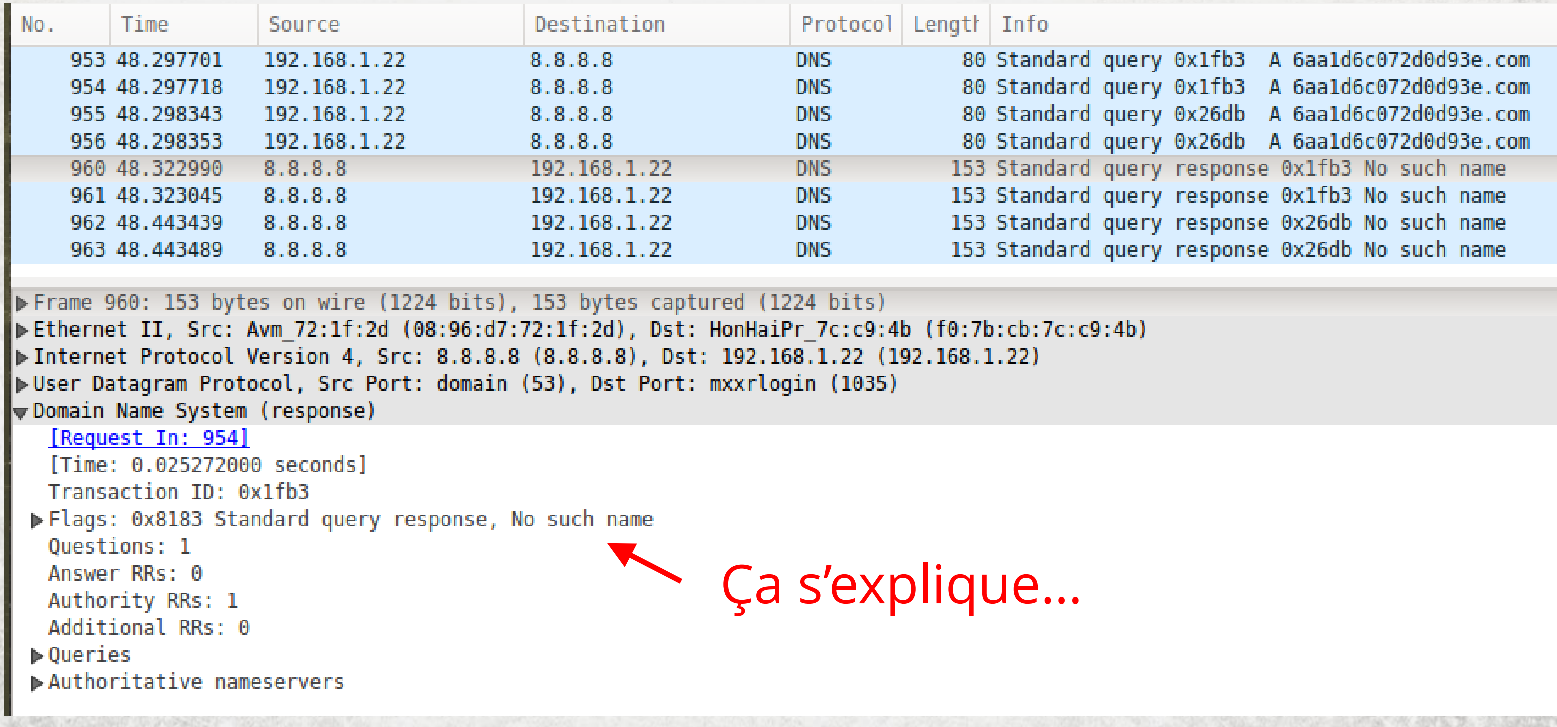
Hosts Involved

IP Address
8.8.8.8

DNS Requests

Domain	IP Address
6aa1d6c072d0d93e.com	

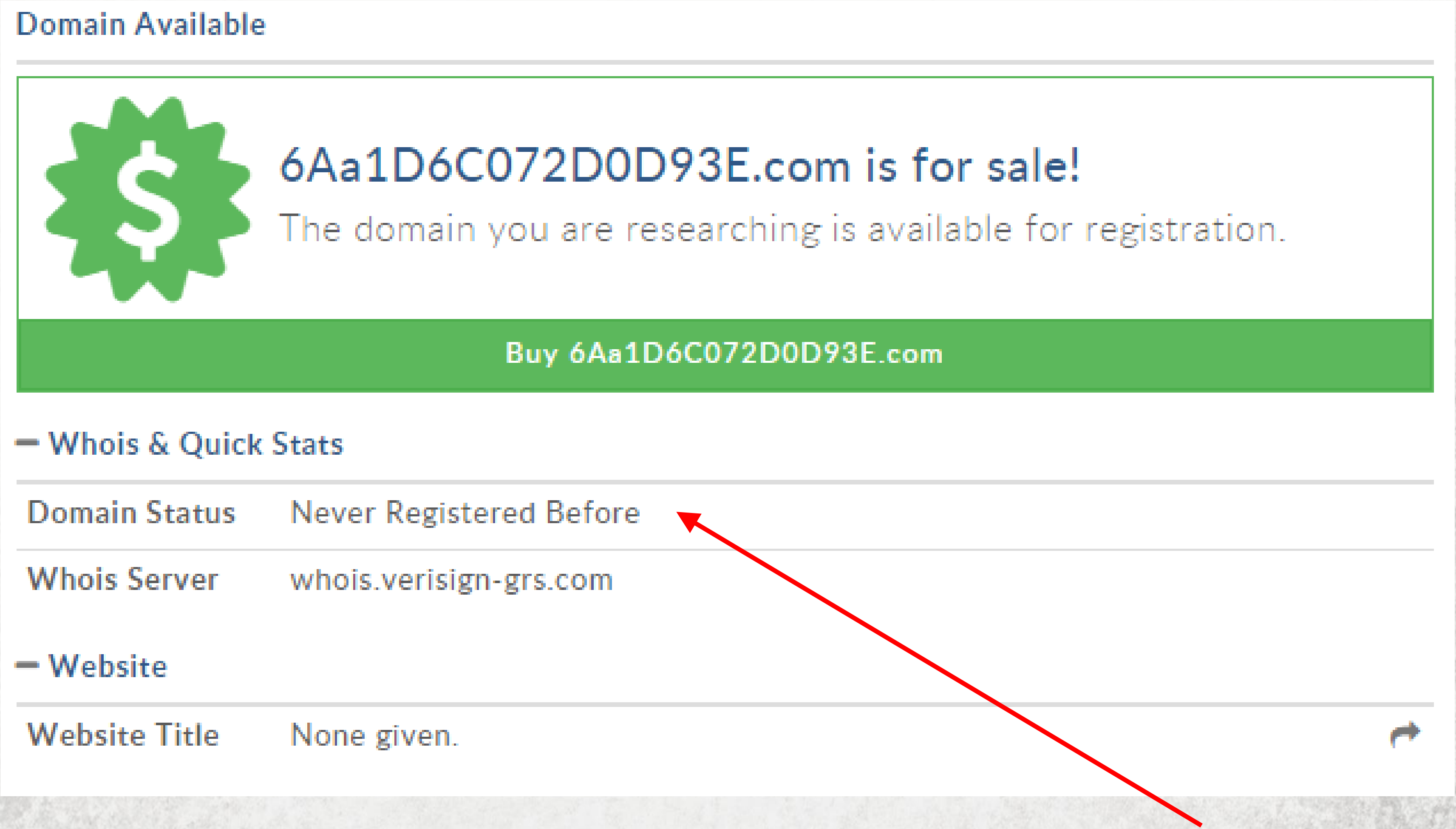
Surprenant…



```
No.   Time        Source        Destination   Protocol Length Info
  953 48.297701   192.168.1.22  8.8.8.8       DNS          80 Standard query 0x1fb3  A 6aa1d6c072d0d93e.com
  954 48.297718   192.168.1.22  8.8.8.8       DNS          80 Standard query 0x1fb3  A 6aa1d6c072d0d93e.com
  955 48.298343   192.168.1.22  8.8.8.8       DNS          80 Standard query 0x26db  A 6aa1d6c072d0d93e.com
  956 48.298353   192.168.1.22  8.8.8.8       DNS          80 Standard query 0x26db  A 6aa1d6c072d0d93e.com
  960 48.322990   8.8.8.8       192.168.1.22  DNS         153 Standard query response 0x1fb3 No such name
  961 48.323045   8.8.8.8       192.168.1.22  DNS         153 Standard query response 0x1fb3 No such name
  962 48.443439   8.8.8.8       192.168.1.22  DNS         153 Standard query response 0x26db No such name
  963 48.443489   8.8.8.8       192.168.1.22  DNS         153 Standard query response 0x26db No such name

▶Frame 960: 153 bytes on wire (1224 bits), 153 bytes captured (1224 bits)
▶Ethernet II, Src: Avm_72:1f:2d (08:96:d7:72:1f:2d), Dst: HonHaiPr_7c:c9:4b (f0:7b:cb:7c:c9:4b)
▶Internet Protocol Version 4, Src: 8.8.8.8 (8.8.8.8), Dst: 192.168.1.22 (192.168.1.22)
▶User Datagram Protocol, Src Port: domain (53), Dst Port: mxxrlogin (1035)
▼Domain Name System (response)
   [Request In: 954]
   [Time: 0.025272000 seconds]
   Transaction ID: 0x1fb3
  ▶Flags: 0x8183 Standard query response, No such name
   Questions: 1
   Answer RRs: 0
   Authority RRs: 1
   Additional RRs: 0
  ▶Queries
  ▶Authoritative nameservers
```

Ça s'explique…

ON VÉRIFIE L'HISTORIQUE…



Domain Available

6Aa1D6C072D0D93E.com is for sale!

The domain you are researching is available for registration.

Buy 6Aa1D6C072D0D93E.com

— Whois & Quick Stats

Domain Status	Never Registered Before
Whois Server	whois.verisign-grs.com

— Website

Website Title	None given.

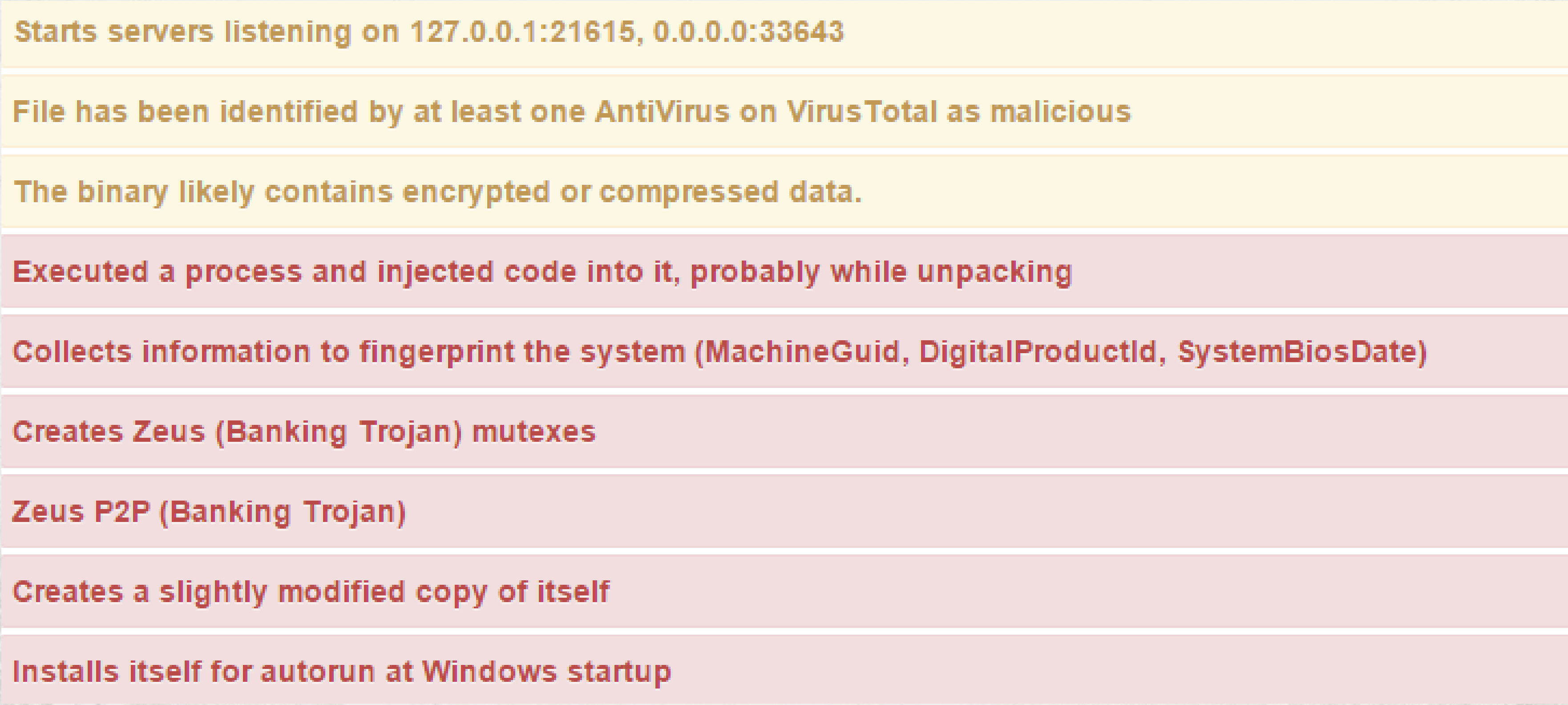
Encore plus surprenant…

RETWEAKING DE LA VM

- Désinstallation des VirtualBox guest tools.
- Nettoyage du registre (références à VirtualBox).
- Nettoyage des fichiers résiduels (références à VirtualBox).
- Modifications des drivers.

⇒ **Nouvelle analyse!**

NOUVELLES SIGNATURES



Starts servers listening on 127.0.0.1:21615, 0.0.0.0:33643

File has been identified by at least one AntiVirus on VirusTotal as malicious

The binary likely contains encrypted or compressed data.

Executed a process and injected code into it, probably while unpacking

Collects information to fingerprint the system (MachineGuid, DigitalProductId, SystemBiosDate)

Creates Zeus (Banking Trojan) mutexes

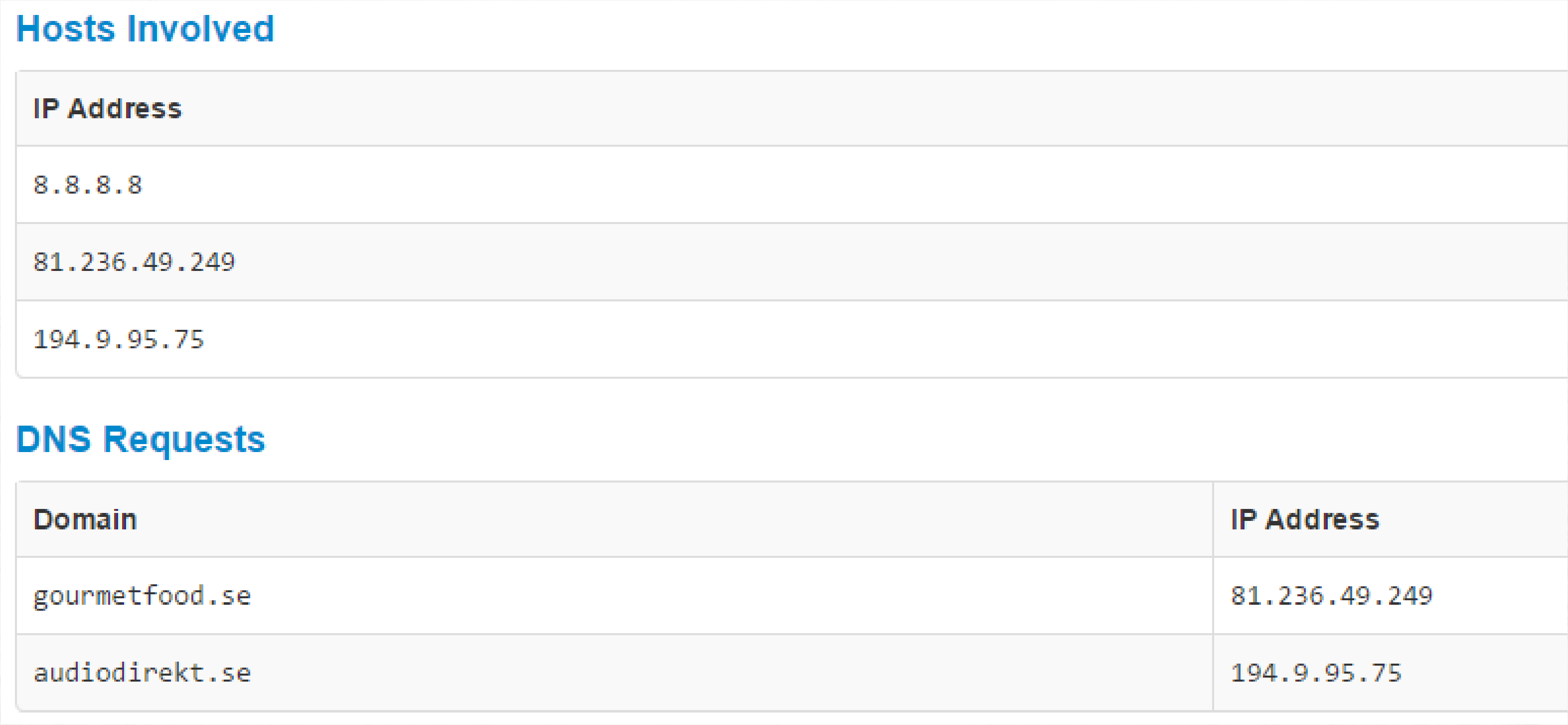
Zeus P2P (Banking Trojan)

Creates a slightly modified copy of itself

Installs itself for autorun at Windows startup

⇒ **Ne détecte plus VirtualBox.**

TOUT DE SUITE PLUS BAVARD…

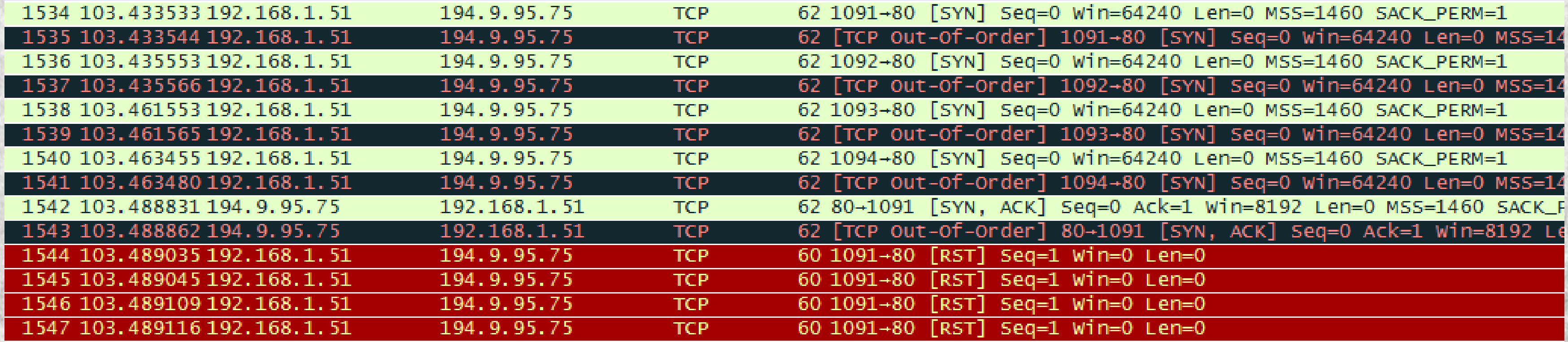


Hosts Involved

IP Address
8.8.8.8
81.236.49.249
194.9.95.75

DNS Requests

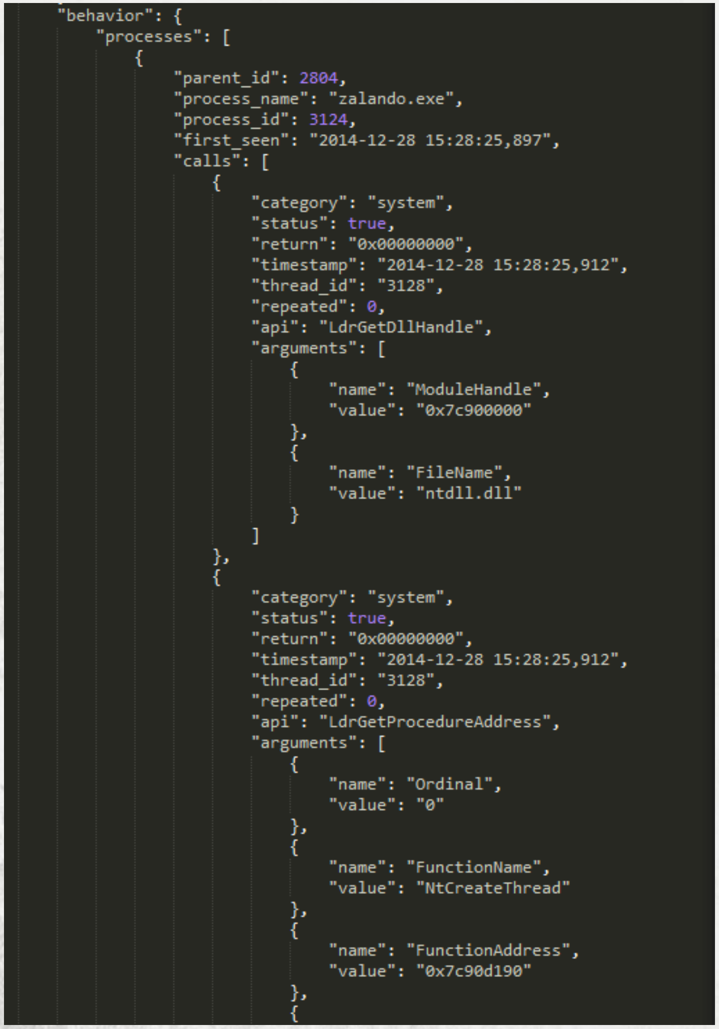
Domain	IP Address
gourmetfood.se	81.236.49.249
audiodirekt.se	194.9.95.75



```
1534 103.433533 192.168.1.51     194.9.95.75     TCP      62 1091→80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
1535 103.433544 192.168.1.51     194.9.95.75     TCP      62 [TCP Out-Of-Order] 1091→80 [SYN] Seq=0 Win=64240 Len=0 MSS=14
1536 103.435553 192.168.1.51     194.9.95.75     TCP      62 1092→80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
1537 103.435566 192.168.1.51     194.9.95.75     TCP      62 [TCP Out-Of-Order] 1092→80 [SYN] Seq=0 Win=64240 Len=0 MSS=14
1538 103.461553 192.168.1.51     194.9.95.75     TCP      62 1093→80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
1539 103.461565 192.168.1.51     194.9.95.75     TCP      62 [TCP Out-Of-Order] 1093→80 [SYN] Seq=0 Win=64240 Len=0 MSS=14
1540 103.463455 192.168.1.51     194.9.95.75     TCP      62 1094→80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
1541 103.463480 192.168.1.51     194.9.95.75     TCP      62 [TCP Out-Of-Order] 1094→80 [SYN] Seq=0 Win=64240 Len=0 MSS=14
1542 103.488831 194.9.95.75      192.168.1.51    TCP      62 80→1091 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 SACK_P
1543 103.488862 194.9.95.75      192.168.1.51    TCP      62 [TCP Out-Of-Order] 80→1091 [SYN, ACK] Seq=0 Ack=1 Win=8192 Le
1544 103.489035 192.168.1.51     194.9.95.75     TCP      60 1091→80 [RST] Seq=1 Win=0 Len=0
1545 103.489045 192.168.1.51     194.9.95.75     TCP      60 1091→80 [RST] Seq=1 Win=0 Len=0
1546 103.489109 192.168.1.51     194.9.95.75     TCP      60 1091→80 [RST] Seq=1 Win=0 Len=0
1547 103.489116 192.168.1.51     194.9.95.75     TCP      60 1091→80 [RST] Seq=1 Win=0 Len=0
```

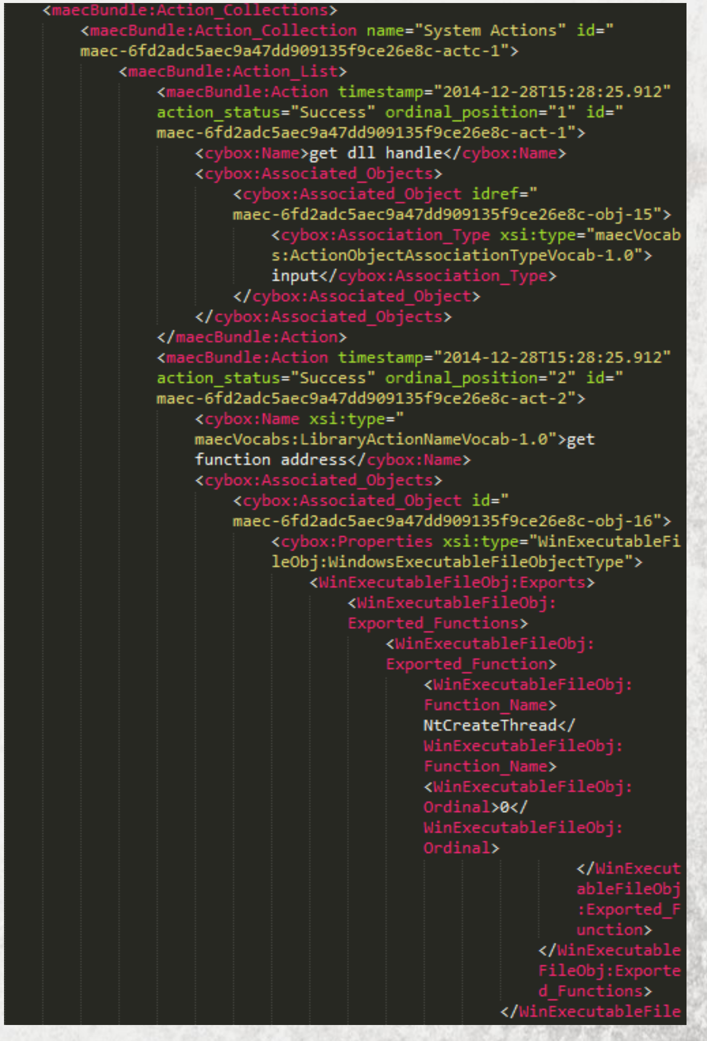
AUTRES FORMATS DE REPORTING

JSON



```
"behavior": {
    "processes": [
        {
            "parent_id": 2804,
            "process_name": "zalando.exe",
            "process_id": 3124,
            "first_seen": "2014-12-28 15:28:25,897",
            "calls": [
                {
                    "category": "system",
                    "status": true,
                    "return": "0x00000000",
                    "timestamp": "2014-12-28 15:28:25,912",
                    "thread_id": "3128",
                    "repeated": 0,
                    "api": "LdrGetDllHandle",
                    "arguments": [
                        {
                            "name": "ModuleHandle",
                            "value": "0x7c900000"
                        },
                        {
                            "name": "FileName",
                            "value": "ntdll.dll"
                        }
                    ]
                },
                {
                    "category": "system",
                    "status": true,
                    "return": "0x00000000",
                    "timestamp": "2014-12-28 15:28:25,912",
                    "thread_id": "3128",
                    "repeated": 0,
                    "api": "LdrGetProcedureAddress",
                    "arguments": [
                        {
                            "name": "Ordinal",
                            "value": "0"
                        },
                        {
                            "name": "FunctionName",
                            "value": "NtCreateThread"
                        },
                        {
                            "name": "FunctionAddress",
                            "value": "0x7c90d190"
                        },
                        {
```

MAEC XML



```
<maecBundle:Action_Collections>
    <maecBundle:Action_Collection name="System Actions" id="
    maec-6fd2adc5aec9a47dd909135f9ce26e8c-actc-1">
        <maecBundle:Action_List>
            <maecBundle:Action timestamp="2014-12-28T15:28:25.912"
            action_status="Success" ordinal_position="1" id="
            maec-6fd2adc5aec9a47dd909135f9ce26e8c-act-1">
                <cybox:Name>get dll handle</cybox:Name>
                <cybox:Associated_Objects>
                    <cybox:Associated_Object idref="
                    maec-6fd2adc5aec9a47dd909135f9ce26e8c-obj-15">
                        <cybox:Association_Type xsi:type="maecVocab
                        s:ActionObjectAssociationTypeVocab-1.0">
                        input</cybox:Association_Type>
                    </cybox:Associated_Object>
                </cybox:Associated_Objects>
            </maecBundle:Action>
            <maecBundle:Action timestamp="2014-12-28T15:28:25.912"
            action_status="Success" ordinal_position="2" id="
            maec-6fd2adc5aec9a47dd909135f9ce26e8c-act-2">
                <cybox:Name xsi:type="
                maecVocabs:LibraryActionNameVocab-1.0">get
                function address</cybox:Name>
                <cybox:Associated_Objects>
                    <cybox:Associated_Object id="
                    maec-6fd2adc5aec9a47dd909135f9ce26e8c-obj-16">
                        <cybox:Properties xsi:type="WinExecutableFi
                        leObj:WindowsExecutableFileObjectType">
                            <WinExecutableFileObj:Exports>
                                <WinExecutableFileObj:
                                Exported_Functions>
                                    <WinExecutableFileObj:
                                    Exported_Function>
                                        <WinExecutableFileObj:
                                        Function_Name>
                                        NtCreateThread</
                                        WinExecutableFileObj:
                                        Function_Name>
                                        <WinExecutableFileObj:
                                        Ordinal>0</
                                        WinExecutableFileObj:
                                        Ordinal>
                                                        </WinExecut
                                                        ableFileObj
                                                        :Exported_F
                                                        unction>
                                                    </WinExecutable
                                                    FileObj:Exporte
                                                    d_Functions>
                                                </WinExecutableFile
```

THREAT Toons™
by: Alex Savchuk
SO... DID YOU SOLVE OUR APT PROBLEM AT BLACKHAT?

CUCKOO SANDBOX, OÙ ET QUAND?

	PRÉVENTIF (LEVÉE DE DOUTE)	RÉACTIF (INCIDENT RESPONSE)	POST-MORTEM (ANALYSE FORENSIQUE)	THREAT INTELLIGENCE (IOC, SIGNATURES)
Equipe sécurité	◑	◑	◔	◔
SOC, intégration infra.	◑	◕	◔	◑
CERT / CSIRT	◑	◕	◕	●
Equipe forensique	○	●	●	◔
Prestataires externes	◔	●	●	◑
Autre…	?	?	?	?

Appréciations complètement subjectives…

CONCLUSION

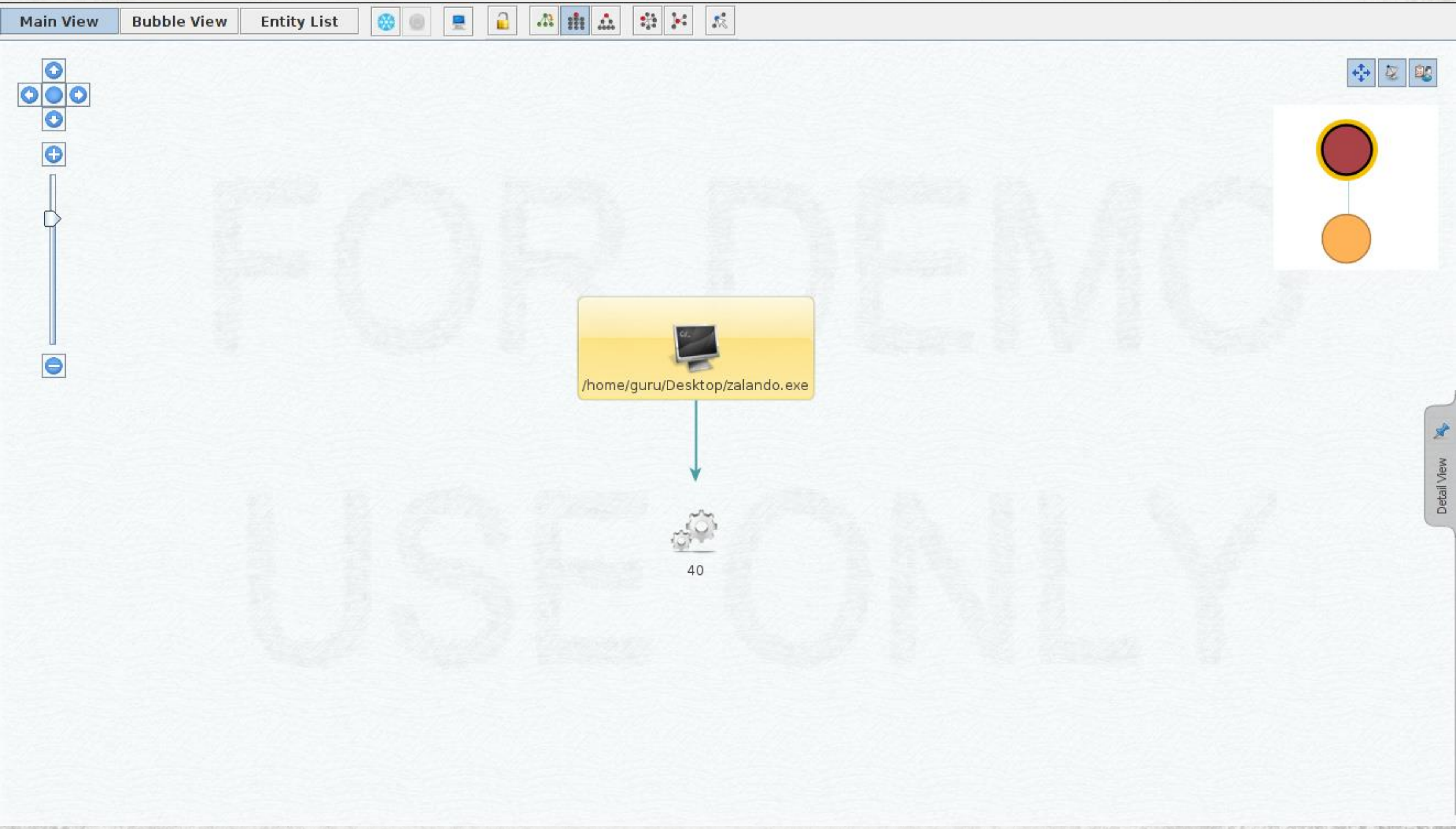
- Ne demande pas des connaissances aussi pointues que pour l'analyse manuelle.
- La qualité de l'analyse dépend fortement de la capacité d'interprétation des résultats.
- L'environnement Cuckoo + VM peut être détectable par certains malwares.
- La globalité du code du malware ne sera très probablement pas totalement exécutée.
- Comporte toujours un risque (débordement du sandboxing, LAN, etc.)…

- Très bonne documentation.
- Communauté très active autour du produit.
- Automatisable et intégrable au sein d'une architecture.

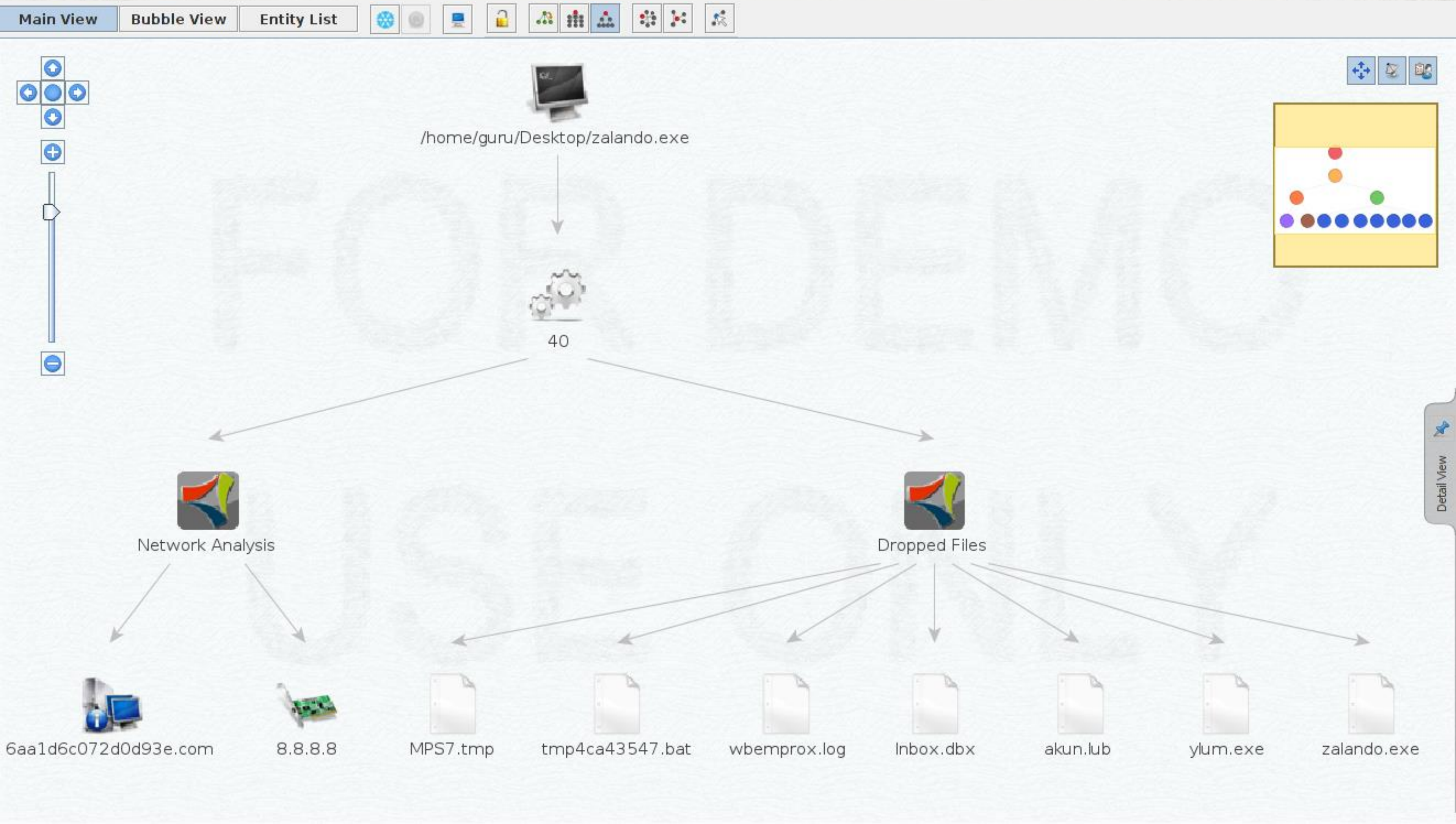
BONUS

Un peu de visualisation avec Maltego

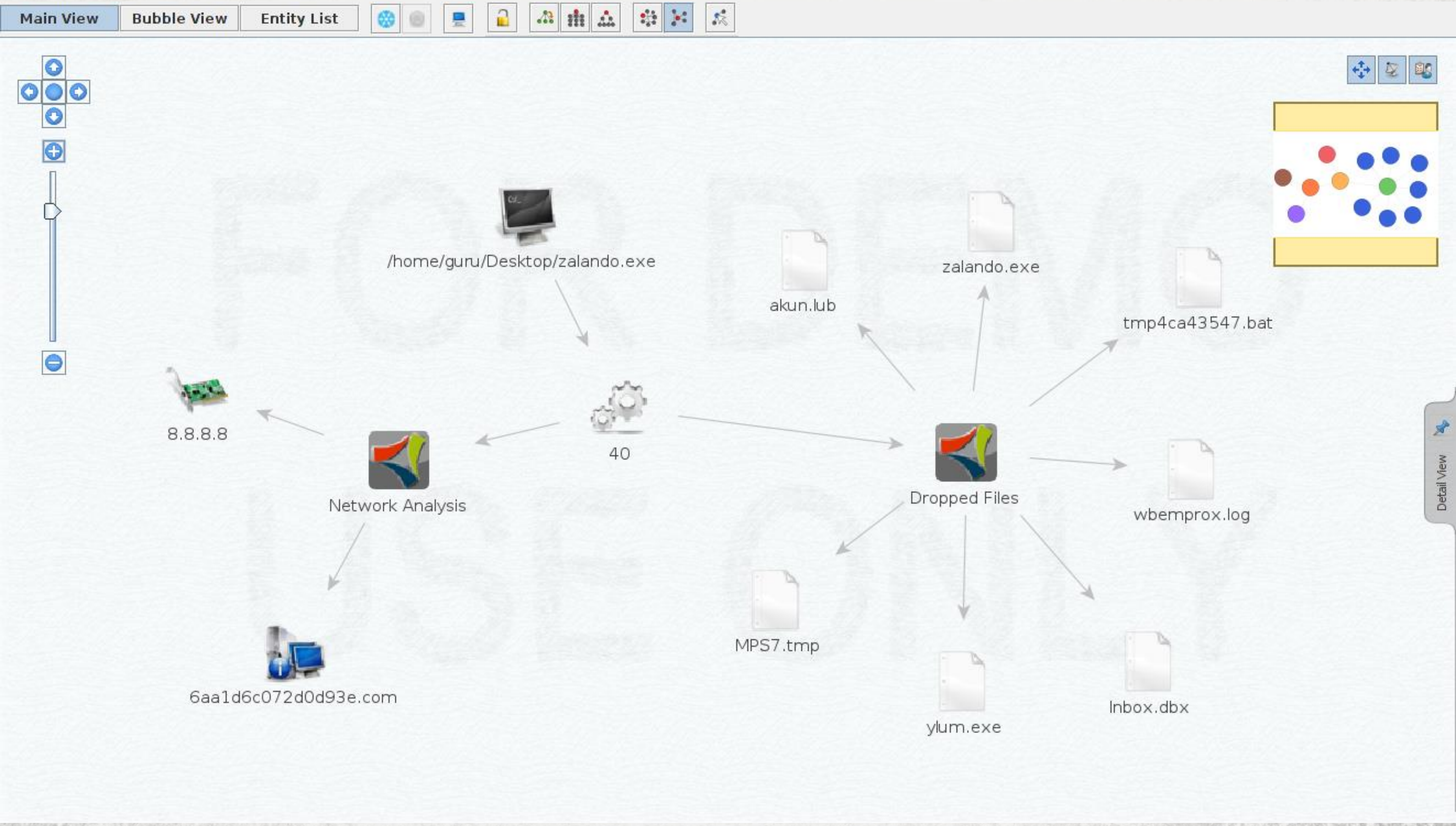
UN PEU DE VISUALISATION - MALTEGO



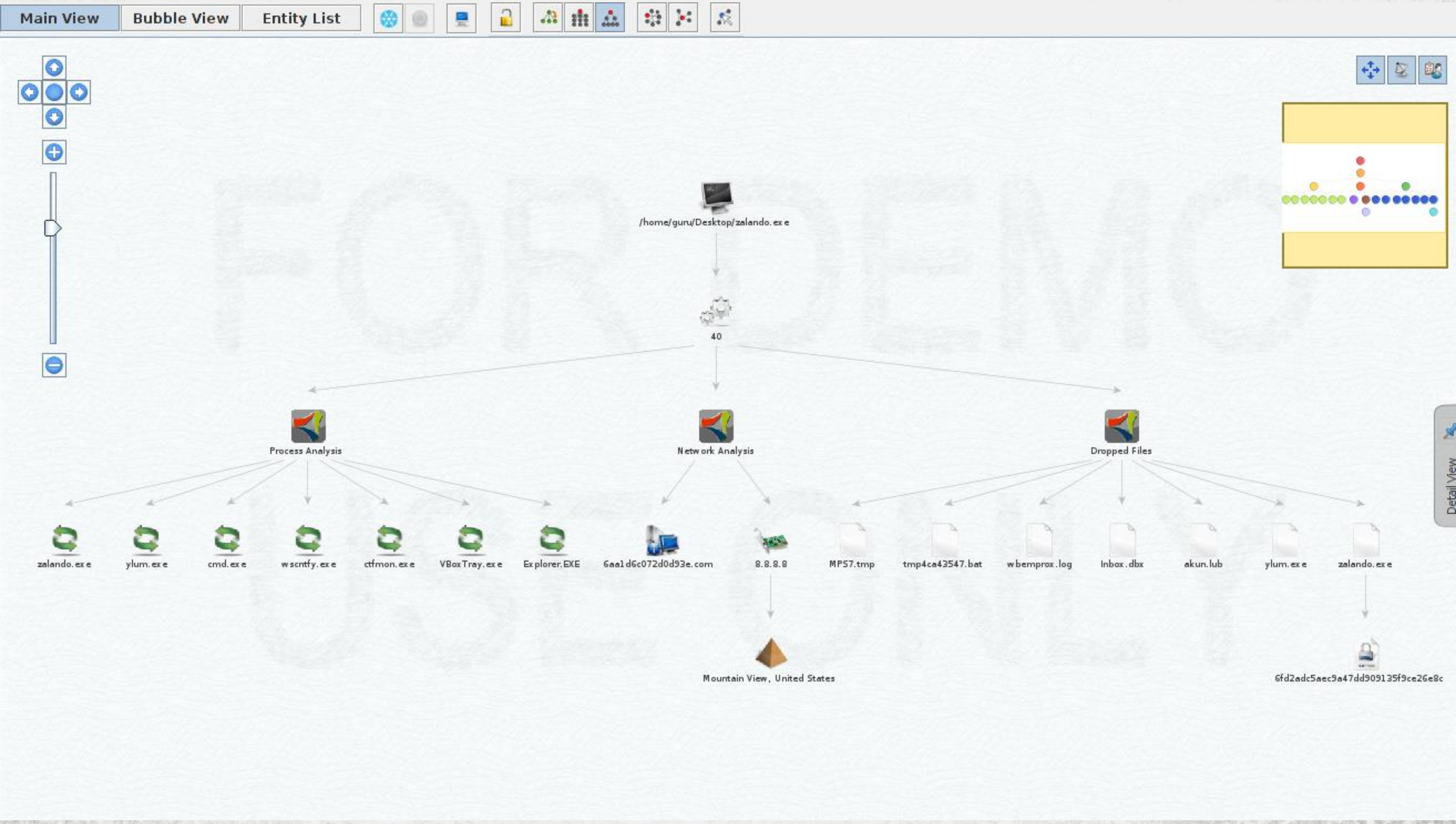
UN PEU DE VISUALISATION - MALTEGO



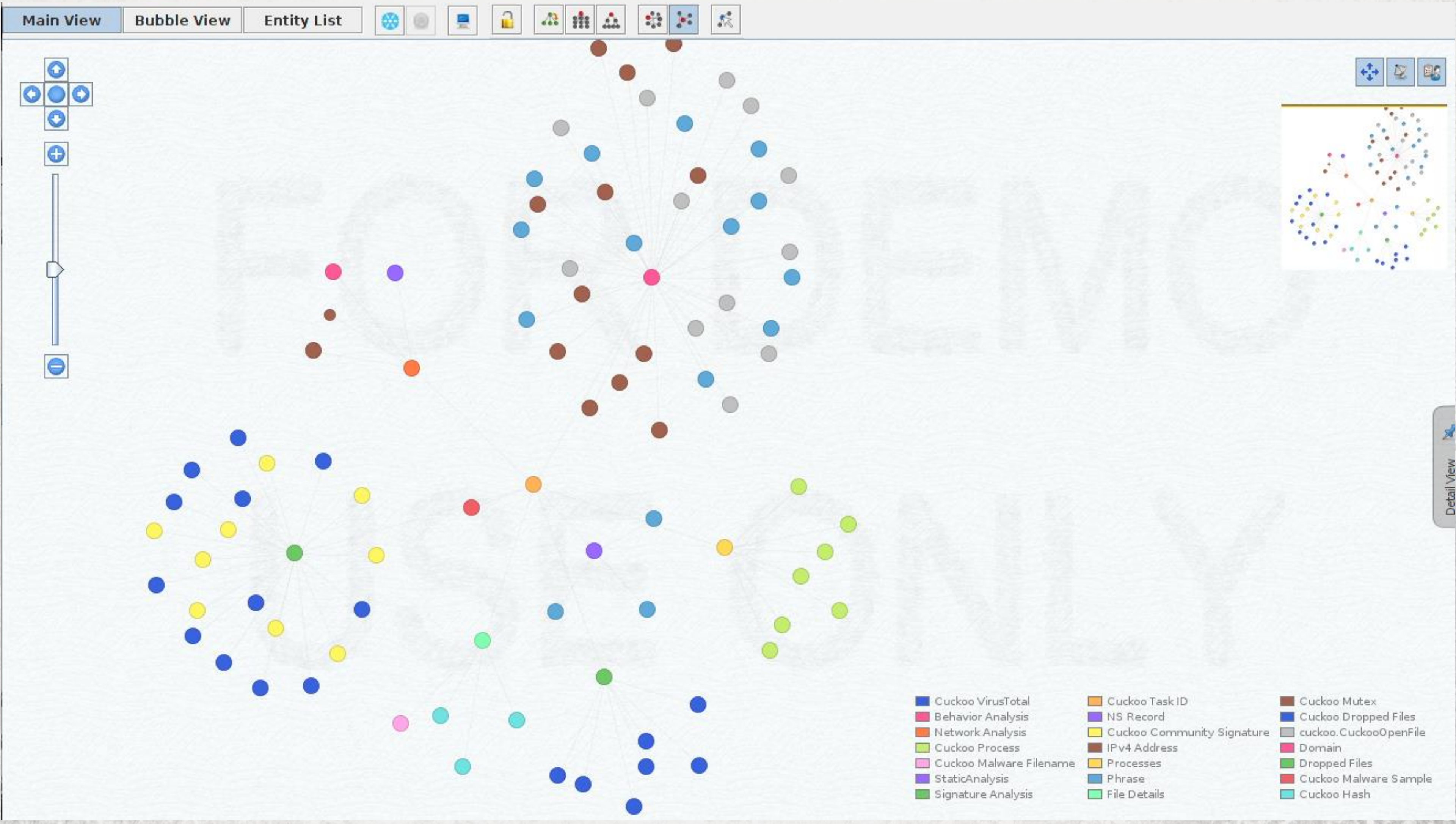
UN PEU DE VISUALISATION – MALTEGO



UN PEU DE VISUALISATION - MALTEGO



UN PEU DE VISUALISATION - MALTEGO



POUR ALLER PLUS LOIN…

Malwr:

- Version online gratuite de Cuckoo Sandbox.
- Parfait pour des tests de malwares «communs».
- Attention à la confidentialité!!!
- Pas de possibilité de récupérer les dumps mémoire et réseau.

Cuckoo Android Extension:

- Support de l'émulateur Android ARM pour exécuter des APK's et des URL.

Community.py:

- Utilitaire pour télécharger et installer les modules développés par la communauté.

El Jefe:

- Intégration avec l'outil El Jefe (détection, réponse et traçage des menaces).

QUESTIONS

MERCI!

Alain Sullam
alain.sullam [at] gmail.com
https://ch.linkedin.com/in/alainsullam
https://github.com/sysinsider

http://www.cuckoosandbox.org

Quelques références utiles:

- http://docs.cuckoosandbox.org/en/latest/
- https://www.packtpub.com/networking-and-servers/cuckoo-malware-analysis
- https://github.com/a0rtega/pafish
- https://github.com/conix-security/zer0m0n
- https://github.com/markedoe/cuckoo-sandbox
- http://www.inetsim.org/
- https://github.com/cuckoobox/community
- https://www.paterva.com/web6/products/maltego.php
- https://malwr.com/
- https://eljefe.immunityinc.com/
- https://github.com/idanr1986/cuckoo
- https://github.com/xme/cuckoomx