

INFORME DE MALWARE

Análisis Estático de Ramsonware.Hive

Contenido

1	Resumen Ejecutivo	3
2	Palabras clave	3
3	INTRODUCCION	4
3.1	Objeto y Objetivos de estudio.....	4
3.2	Objetivo General	4
3.3	Objetivos específicos.....	4
3.4	Metodología	4
3.5	Herramientas Utilizadas	5
3.6	Información general de la muestra utilizada para el estudio de Ransomware.Hive	6
4	ANALISIS ESTATICO.....	7
5	CONCLUSIONES	30

1 Resumen Ejecutivo

El grupo encargado del desarrollo del ransomware Hive, al igual que la gran mayoría de los nuevos grupos que se dedican a lo mismo en la actualidad, han elegido distribuir Hive en forma de Ransomware as a Service (RaaS).

Su primera aparición data de junio de 2021 y, a diferencia con otros grupos detrás de la distribución de RaaS, éstos no tienen consideraciones con el tipo de sector al que afectan y solo tres semanas después de su aparición, un hospital se vio afectado por un ataque con Hive. Tras ese incidente el FBI realizó un aviso y pusieron al grupo bajo el punto de mira. Aun así, el grupo continúa manteniendo sus objetivos y los sectores más afectados por el ransomware Hive son las industrias energéticas y de la salud.

Hive ha ido recibiendo diferentes actualizaciones desde su fecha de salida, mejorando algunos aspectos o incluyendo nuevas funcionalidades, pero la actualización más importante surge en marzo de 2022 cuando el grupo encargado del desarrollo traspasó el código fuente del lenguaje GOlang a RUST. No es el primer grupo importante de ransomware en desarrollar en lenguaje RUST: recientemente el grupo encargado del desarrollo de BlackCat han decidido desarrollar su ransomware en ese mismo lenguaje. Este lenguaje es de gran utilidad para los desarrolladores pues mantiene una sintaxis similar al lenguaje C/C++ pero incluye muchas librerías de criptografía, además de ofrecer grandes facilidades para parallelizar tareas y un gran control de excepciones.

También cabe añadir que el grupo de Hive tiene un portal web montado sobre un nodo Tor donde las víctimas de los ataques pueden acceder con las credenciales facilitadas en las notas que dejan tras los ataques y comunicarse con los atacantes para negociar el rescate de sus ficheros. Este portal solo es accesible para aquellas personas que dispongan de las credenciales de acceso.

2 Palabras clave

- Malware
- Análisis estático
- Ransomware.hive
- Ransomware
- Ransomware as a Service (RaaS)

3 INTRODUCCION

3.1 Objeto y Objetivos de estudio

En el presente trabajo se aborda el estudio del malware HIVE, desde una perspectiva estatica, con el fin de conocer a detalle este ransomware, su funcionalidad, contenido y comprender su impacto desde una visión general a partir de su disección.

Para realizar lo mencionado en el párrafo anterior, se utilizaran una serie de herramientas que arrojan un análisis estatico del malware a partir de su contenido y su funcionalidad, esto se llevara a cabo en un laboratorio de Virtualbox en una maquina virtual Windows 7 professional. Cabe resaltar que este informe no incluye el análisis dinamico del ransoware Hive.

3.2 Objetivo General

Analizar de forma estatica el malware Hive, conocer su funcionalidad y la diseccion de este para su mejor comprensión y estudio.

3.3 Objetivos específicos.

- Conocer la historia del malware Hive
- Explorar de forma superficial el malware Hive a través de herramientas profesionales.
- Comprender el contenido del ransomware Hive a través de herramientas de diseccion de su contenido.
- Analizar de forma profunda el malware Hive de manera que se pueda determinar su funcionalidad e impacto en los sistemas de información.

3.4 Metodología

El método a través del cual se realiza realizar el análisis del malware es el Análisis estático.

El análisis estático de *malwares* es un conjunto de técnicas que permiten estudiar, prever y observar el funcionamiento de este tipo de *softwares* sin necesidad de ejecutarlos. El análisis se hace por medio de la revisión del código fuente del archivo y la identificación de elementos maliciosos en el mismo. De este modo, un analista puede hacerse una idea de las tareas que ejecuta el *malware* en un sistema sin correr el riesgo de infectar el ordenador con este.

El análisis estático comprende diferentes protocolos, técnicas y herramientas que permiten realizar este tipo de estudio. Este análisis se ubica en la primera fase del proceso descrito en la introducción, ya que les indica a los investigadores qué aspectos del *malware* observar a la hora de ejecutarlo en un entorno virtual controlado.

3.5 Herramientas Utilizadas

- Virustotal
- pafish
- Portex analyzer
- Strings
- GMER
- dependency Walker
- PE BEAR
- Proteccion ID
- Detect it easy
- Cerbero Profiler advanced

3.6 Información general de la muestra utilizada para el estudio de Ransomware.Hive



Teniendo en cuenta la forma en que se han realizado los ataques con este malware, el flujo de infección que termina derivando en que la detonación del ransomware puede variar de unos casos a otros.

Dado que el ransomware no posee altas capacidades para propagarse a través de Internet, el proceso de compromiso inicial es llevado a cabo por operadores humanos. De esta forma, el operador debe encargarse de desplegarlo a través de la red interna. Deben tenerse en cuenta todas las opciones que puedan terminar derivando en una ejecución de código malicioso, como la explotación de vulnerabilidades, el envío de correos con adjuntos maliciosos o el uso de exploit kits.

Una vez comprometido el sistema, los atacantes recopilan credenciales e información sobre la víctima hasta que deciden ejecutar el ransomware que cifrará toda la información y con el cual habrá concluido el ataque.

Al igual que otros operadores de ransomware, el grupo detrás de Hive estaría tratando de llevar a cabo un modelo de doble extorsión. Siguiendo este modelo, además de reclamar una suma de dinero en criptomonedas a cambio de descifrar la información, amenazan con filtrar los datos que han robado, venderlos al mejor postor si las víctimas se niegan a pagar o sencillamente haciéndolos accesibles al público y devaluando la marca.

Para realizar el estudio estatico del malware Hive, se procede a descargarlo del repositorio de github

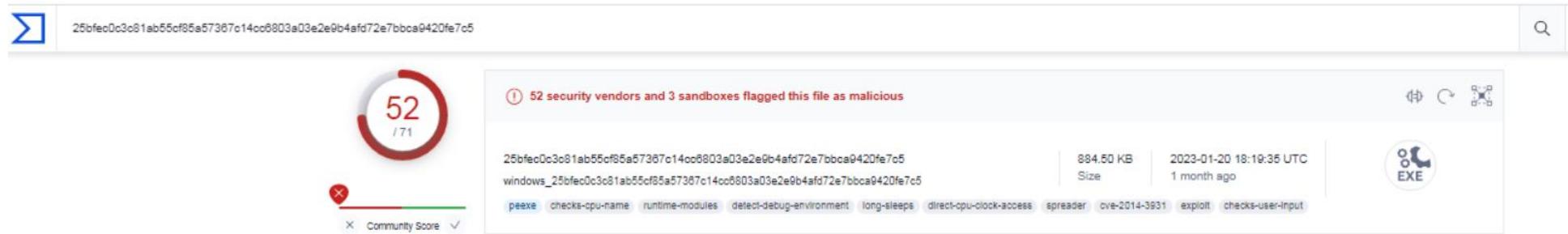
<https://github.com/ytisf/theZoo/tree/master/malware/Binaries/Ransomware.Hive>

Se descarga un zip del malware en la máquina virtual Windows 7 y se procede a realizar la descompresión del zip.

4 ANALISIS ESTATICO

En un primer acercamiento al malware subimos el malware a **virustotal** para ver que datos arroja acerca del malware.

Cabe destacar que el SHA256 es 25bfec0c3c81ab55cf85a57367c14cc6803a03e2e9b4af72e7bbca9420fe7c5



La puntuación del archivo de infección es de 52/71 y como era de esperarse virustotal anuncia que el fichero es malicioso, teniendo en cuenta estos 52 indicadores.

Abajo se pueden ver las ilustraciones de los resultados arrojados por virustotal, todos los antivirus detectan este archivo como malicioso, entre ellos AVAST, Ikarus, Kaspersky, Mcfee, yandex, Sophos, k7 antivirus, Google, fitdefender.

Por ende desde un primer reconocimiento se puede decir que el archivo es malicioso, con las herramientas que utilizaremos a partir de este momento se podrá ver mejor el contenido de este ransomware.

[Join the VT Community](#) and enjoy additional community insights and crowdsourced detections.

Security vendors' analysis ⓘ

Do you want to automate checks?

Alibaba	ⓘ Ransom:Win32/FileCryptor.d52c04d1	ALYac	ⓘ Trojan.Ransom.Filecoder
Antiy-AVL	ⓘ GrayWare/Win32.Kryptik.ffd	Arcabit	ⓘ Trojan.Generic.D23C97DE
Avast	ⓘ Win32:Malware-gen	AVG	ⓘ Win32:Malware-gen
Avira (no cloud)	ⓘ TR/Redcap.ealww	BitDefender	ⓘ Trojan.GenericKD.37525470
BitDefenderTheta	ⓘ Gen>NN.ZexaCO.36212.3mGfaGsSREb	CrowdStrike Falcon	ⓘ Win/malicious_confidence_100% (W)
Cylance	ⓘ Unsafe	Cynet	ⓘ Malicious (score: 100)
Cyren	ⓘ W32/ABRisk.WQTP-6647	DrWeb	ⓘ Trojan.MulDrop18.37605
Elastic	ⓘ Malicious (moderate Confidence)	Emsisoft	ⓘ Trojan.GenericKD.37525470 (B)
eScan	ⓘ Trojan.GenericKD.37525470	ESET-NOD32	ⓘ A Variant Of WinGo/Agent.CC
F-Secure	ⓘ Trojan.TR/Redcap.ealww	Fortinet	ⓘ W32/Agentb.AG!tr
GData	ⓘ Trojan.GenericKD.37525470	Google	ⓘ Detected
Gridinsoft (no cloud)	ⓘ Ransom:Win32.Wecstao.oels2	Ikarus	ⓘ Trojan.WinGo.Agent
Jiangmin	ⓘ Trojan.Agentb.kco	K7AntiVirus	ⓘ Riskware (0040eff71)
K7GW	ⓘ Riskware (0040eff71)	Kaspersky	ⓘ Trojan-Ransom.Win32.Hive.ai

Lionic	① Trojan.Win32.Hive.jlc	Malwarebytes	① Trojan.MalPack.UPX
MAX	① Malware (ai Score=83)	MaxSecure	① Trojan.Malware.1728101.susgen
McAfee	① RDN/Ransom	McAfee-GW-Edition	① BehavesLike.Win32.Generic.co
Microsoft	① Trojan:Win32/Sabsik.FL.B!rfn	Panda	① Trj/CI.A
Rising	① Ransom.Agentb!8.1139A (CLOUD)	Sangfor Engine Zero	① Ransom.Win32.Agent.V181
SecureAge	① Malicious	Sophos	① Mal/Genérico-S
Symantec	① Downloader	Tencent	① Win32.Trojan.Hive.Htgl
Trapmine	① Malicious.moderate.ml.score	Trellix (FireEye)	① Trojan.GenericKD.37525470
TrendMicro	① Ransom_Hive.R002C0DJ622	TrendMicro-HouseCall	① Ransom_Hive.R002C0DJ622
VBA32	① TrojanRansom.Agentb	VIPRE	① Trojan.GenericKD.37525470
Webroot	① W32.AGentb	Yandex	① Trojan.Agentb!nSN7QfQlps4
Zillya	① Trojan.Agent.Win32.2417589	ZoneAlarm by Check Point	① Trojan-Ransom.Win32.Hive.ai

Se ejecuta la herramienta **Pafish**, para verificar como de detectable es la maquina virtual, esta aplicación no sólo detecta si se encuentra en una máquina virtual, además detecta si está siendo depurado, si se está ejecutando en una sandbox, etc. Cuantos más OK en verde se vea, mejor. Si detectan la maquina, aparecerá el mensaje de traced en rojo.

En la ilustración de abajo se puede ver que la herramienta ha detectado que se encuentra en un entorno de virtualización.

```
C:\Users\master\Desktop\pafish64.exe
[*] Checking the difference between CPU timestamp counters <rdtsc> ... OK
[*] Checking the difference between CPU timestamp counters <rdtsc> forcing VM execution ... traced!
[*] Checking hypervisor bit in cpuid feature bits ... traced!
[*] Checking cpuid hypervisor vendor for known VM vendors ... traced!

[-] Generic reverse turing tests
[*] Checking mouse presence ... OK
[*] Checking mouse movement ... traced!
[*] Checking mouse speed ... OK
[*] Checking mouse click activity ... traced!
[*] Checking mouse double click activity ... traced!
[*] Checking dialog confirmation ... OK
[*] Checking plausible dialog confirmation ... OK

[-] Generic sandbox detection
[*] Checking username ... OK
[*] Checking file path ... OK
[*] Checking common sample names in drives root ... OK
[*] Checking if disk size <= 60GB via DeviceIoControl() ... traced!
[*] Checking if disk size <= 60GB via GetDiskFreeSpaceExA() ... traced!
[*] Checking if Sleep() is patched using GetTickCount() ... OK
[*] Checking if NumberOfProcessors is < 2 via PEB access ... OK
[*] Checking if NumberOfProcessors is < 2 via GetSystemInfo() ... OK
[*] Checking if physical memory is < 1Gb ... OK
[*] Checking operating system uptime using GetTickCount() ... OK
[*] Checking if operating system IsNativeUhdBoot() ... OK

[-] Sandboxie detection
[*] Using GetModuleHandle<sbiedll.dll> ... OK

[-] Wine detection
[*] Using GetProcAddress<wine_get_unix_file_name> from kernel32.dll ... OK
[*] Reg key <HKCU\SOFTWARE\Wine> ... OK

[-] VirtualBox detection
[*] Scsi port->bus->target id->logical unit id-> 0 identifier ... traced!
[*] Reg key <HKLM\HARDWARE\Description\System "SystemBiosVersion"> ... traced!
[*] Reg key <HKLM\SOFTWARE\Oracle\VirtualBox Guest Additions> ... traced!
[*] Reg key <HKLM\HARDWARE\Description\System "VideoBiosVersion"> ... traced!
[*] Reg key <HKLM\HARDWARE\ACPI\NDSDT\UBOX__> ... traced!
[*] Reg key <HKLM\HARDWARE\ACPI\FADT\UBOX__> ... traced!
[*] Reg key <HKLM\HARDWARE\ACPI\RSDT\UBOX__> ... traced!
[*] Reg key <HKLM\SYSTEM\ControlSet001\Services\VBox*> ... traced!
[*] Reg key <HKLM\HARDWARE\DESCRIPTION\System "SystemBiosDate"> ... traced!
[*] Driver files in C:\WINDOWS\system32\drivers\VBox* ... traced!
[*] Additional system files ... traced!
[*] Looking for a MAC address starting with 08:00:27 ... traced!
[*] Looking for pseudo devices ... traced!
[*] Looking for VBoxTray windows ... traced!
[*] Looking for VBox network share ... traced!
[*] Looking for VBox processes <vboxservice.exe, vboxtray.exe> ... traced!
[*] Looking for VBox devices using WMI ... traced!
```

Para un primer reconocimiento del Malware se utiliza la herramienta **Portex Analyzer** de manera que se pueda obtener una radiografia sintetica del malware con información general e importante para empezar a realizar el análisis de este.

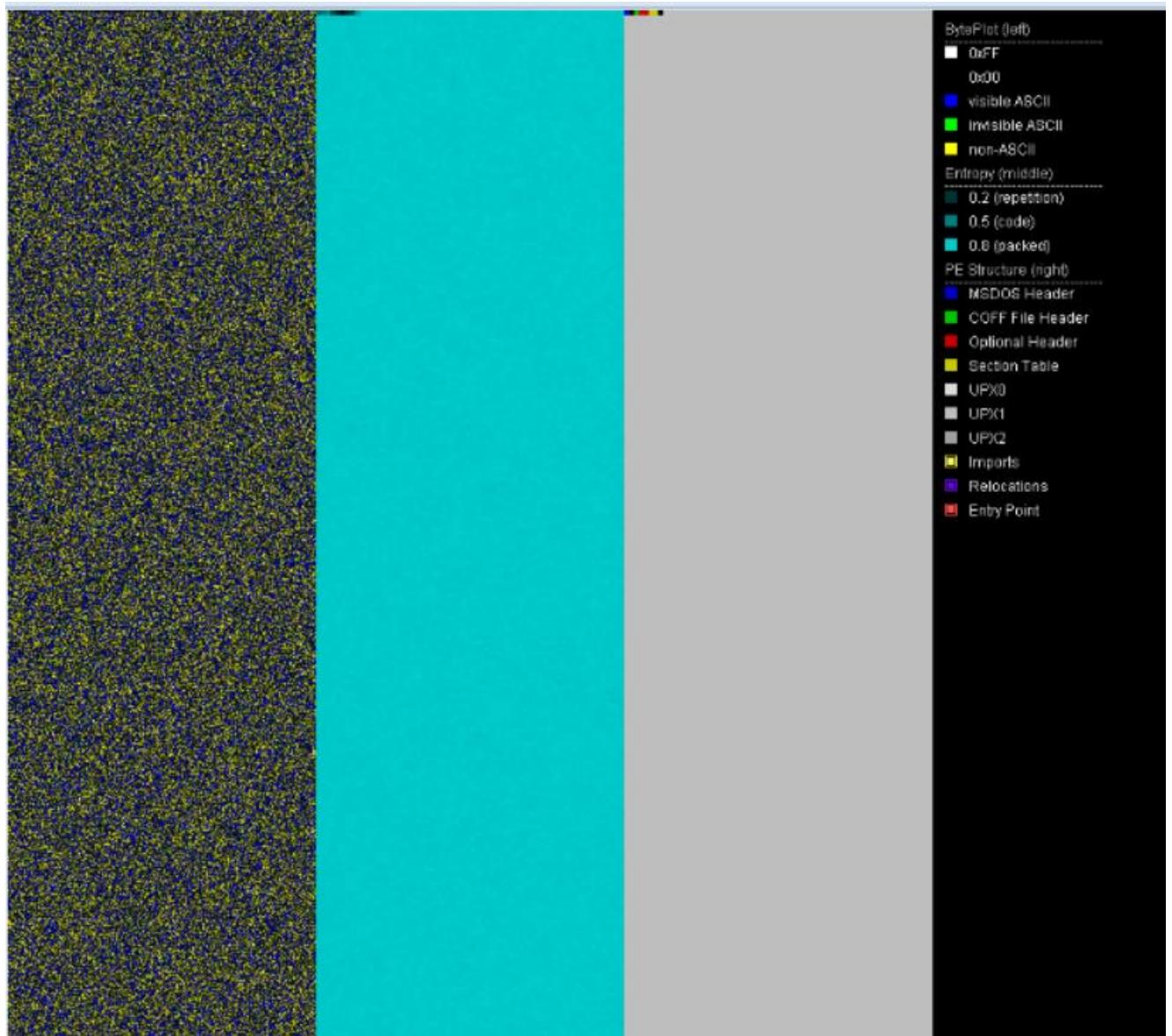
```

Administrator: C:\Windows\System32\cmd.exe
01/03/2023 23:11          0 hi_sandbox_rtt_mouse_double_click
01/03/2023 23:11          0 hi_sandbox_rtt_mouse_movement
01/03/2023 23:11          0 hi_virtualbox
01/03/2023 23:11          0 hi_vmware
01/03/2023 23:11          3.992 pafish.log
07/05/2022 22:20          121.344 pafish64.exe
17/03/2021 03:00 <DIR>          PE Bear
03/11/2008 13:49          219.136 PEiD.exe
07/01/2021 21:03 <DIR>          pestudio
08/01/2021 00:26          11.548.450 PortexAnalyzer.jar
07/05/2022 22:54 <DIR>          Programas Análisis Malware
07/01/2021 23:21 <DIR>          Protection_ID
20/11/2020 09:27          5.680.128 ResourceHacker.exe
06/01/2021 21:38          347.016 strings.exe
17/03/2021 01:26 <DIR>          Systernals
14/05/2020 05:27 <DIR>          UBoxHardenedLoader-2.0.1
06/08/2022 12:25          905.728 windows_25bfec0c3c81ab55cf85a57367c14cc6803a
03e2e9b4afd72e7bbca9420fe7c5
23 archivos   20.809.064 bytes
9 dirs    24.642.908.160 bytes libres

C:\Users\master\Desktop>clear
"clear" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.

C:\Users\master\Desktop>PortexAnalyzer.jar -p radiohive.png windows_25bfec0c3c81
ab55cf85a57367c14cc6803a03e2e9b4afd72e7bbca9420fe7c5
C:\Users\master\Desktop>_

```



La ilustración anterior muestra una radiografía del malware, en la parte derecha se pueden ver los primeros datos del ransomware.hive, la información sobre la entropía, teniendo en cuenta los resultados arrojados es de 0.8 packed, lo cual indica que el malware ha sido comprimido o empaquetado.

UPX es un compresor de archivos ejecutable avanzado. UPX normalmente reducirá el tamaño de archivo de los programas y DLL entre un 50 % y un 70 %, lo que reducirá el espacio en disco, los tiempos de carga de la red, los tiempos de descarga y otros costos de distribución y almacenamiento. En este caso se ve que se utiliza este compresor UPX0, UPX1 y UPX2.

Una vez realizado un primer análisis superficial del malware hive, se procede a analizar el archivo con la herramienta **PESTUDIO**, este software permite a los analistas de malware examinar y analizar ficheros .exe y sus librerías dinámicas.

La herramienta muestra varios ficheros que se pueden investigar para saber qué acciones realiza cuando lo ejecutamos. De este modo, se puede saber si se trata de un malware, y en caso de que así sea, observar qué acciones es capaz de llevar a cabo la amenaza.

La primera grafica de abajo muestra la información general del archivo estos son los hashes según tipo, la entropía que es casi 8.00 y que desde un primer acercamiento aparentemente el archivo es malicioso, también enumera que es un fichero ejecutable de 32-bit.

En la ilustración siguiente se muestra el apartado de indicadores del malware, los indicadores dan información acerca de porque el archivo puede ser sospechoso y su nivel de severidad, en este caso en particular, se ven 33 indicadores que hacen que el fichero pueda ser sospechoso, estas diferenciadas según el nivel de criticidad, los del nivel 1 son aquellos que indican que el archivo es malicioso, entre estos ítems se encuentran las referencias que posee se encuentran en la lista negra, también la puntuación de virustotal, las librerías utilizadas por este ransomware son sospechosas, los archivos contienen una section de la lista negra, la localización del punto de entrada es sospechosa, por otro lado, las catalogadas en el nivel 2 configuran el hecho de que el archivo es modifiable y ejecutable UPX0, UPX1 y UPX2, lo cual lo hace sospechoso también y las del nivel 3 engloban a que el archivo referencia un grupo de API y hint.

pestudio 9.09 - Malware Initial Assessment - www.winitor.com [c:\users\master\Desktop\windows_25bfec0c3c81ab55cf85a57367c14cc6803a03e2e9b4afd72e7bbca9420fe7c5]	
file	settings
c:\users\master\Desktop\windows_25bfec0c3c81ab55cf85a57367c14cc6803a03e2e9b4afd72e7bbca9420fe7c5	
indicators (33)	
virustotal (52/71)	
dos-header (64 bytes)	
dos-stub (64 bytes)	
rich-header (n/a)	
file-header (compiler-stamp)	
optional-header (console)	
directories (2)	
sections (entry-point)	
libraries (count)	
imports (count)	
exports (n/a)	
exceptions (n/a)	
tls-callbacks (n/a)	
relocations (4)	
resources (n/a)	
strings (10841)	
debug (n/a)	
manifest (n/a)	
version (n/a)	
certificate (n/a)	
overlay (n/a)	

pestudio 9.09 - Malware Initial Assessment - www.winitor.com [c:\users\master\Desktop\windows_25bfec0c3c81ab55cf85a57367c14cc6803a03e2e9b4afd72e7bbca9420fe7c5]																																																																																																			
file	settings	about																																																																																																	
c:\users\master\Desktop\windows_25bfec0c3c81 .id indicators (33) virustotal (52/71) dos-header (64 bytes) dos-stub (64 bytes) rich-header (n/a) file-header (compiler-stamp) optional-header (console) directories (2) sections (entry-point) libraries (count) imports (count) exports (n/a) exceptions (n/a) tls-callbacks (n/a) relocations (4) resources (n/a) abc strings (10841) debug (n/a) manifest (n/a) version (n/a) certificate (n/a) overlay (n/a)	<table border="1"> <thead> <tr> <th>xml-id</th> <th>indicator (33)</th> <th>detail</th> <th>level</th> </tr> </thead> <tbody> <tr><td>1430</td><td>The file references string(s) tagged as blacklist</td><td>count: 4</td><td>1</td></tr> <tr><td>1120</td><td>The file is scored by virustotal</td><td>score: 52/71</td><td>1</td></tr> <tr><td>1485</td><td>The count of libraries is suspicious</td><td>count: 1</td><td>1</td></tr> <tr><td>1266</td><td>The file imports symbol(s) tagged as blacklist</td><td>count: 1</td><td>1</td></tr> <tr><td>1265</td><td>The count of imports is suspicious</td><td>count: 4</td><td>1</td></tr> <tr><td>1245</td><td>The file contains a blacklist section</td><td>section: UPX0</td><td>1</td></tr> <tr><td>1245</td><td>The file contains a blacklist section</td><td>section: UPX1</td><td>1</td></tr> <tr><td>1245</td><td>The file contains a blacklist section</td><td>section: UPX2</td><td>1</td></tr> <tr><td>1223</td><td>The first section is writable</td><td>section: UPX0</td><td>1</td></tr> <tr><td>1225</td><td>The location of the entry-point is suspicious</td><td>section: UPX1:0x003100E0</td><td>1</td></tr> <tr><td>1631</td><td>The file contains self-modifying executable section(s)</td><td>status: yes</td><td>1</td></tr> <tr><td>2215</td><td>The file contains writable and executable section(s)</td><td>count: 2</td><td>1</td></tr> <tr><td>1321</td><td>The time-stamp of the compiler is suspicious</td><td>year: 0</td><td>2</td></tr> <tr><td>1200</td><td>The value of 'pointer-symbol-table' is suspicious</td><td>value: 0x002DCA00</td><td>2</td></tr> <tr><td>1153</td><td>The file contains a virtualized section</td><td>section: UPX0</td><td>2</td></tr> <tr><td>1036</td><td>The file checksum is invalid</td><td>checksum: 0x00000000</td><td>3</td></tr> <tr><td>1634</td><td>The file references a group of API</td><td>api: execution, count: 1</td><td>3</td></tr> <tr><td>1634</td><td>The file references a group of API</td><td>api: dynamic-library, count: 2</td><td>3</td></tr> <tr><td>1634</td><td>The file references a group of API</td><td>api: memory, count: 1</td><td>3</td></tr> <tr><td>1633</td><td>The file references a group of hint</td><td>hint: dos-message, count: 1</td><td>3</td></tr> <tr><td>1633</td><td>The file references a group of hint</td><td>hint: utility, count: 2</td><td>3</td></tr> <tr><td>1633</td><td>The file references a group of hint</td><td>hint: file, count: 12</td><td>3</td></tr> <tr><td>1633</td><td>The file references a group of hint</td><td>hint: base64, count: 2</td><td>3</td></tr> </tbody> </table>	xml-id	indicator (33)	detail	level	1430	The file references string(s) tagged as blacklist	count: 4	1	1120	The file is scored by virustotal	score: 52/71	1	1485	The count of libraries is suspicious	count: 1	1	1266	The file imports symbol(s) tagged as blacklist	count: 1	1	1265	The count of imports is suspicious	count: 4	1	1245	The file contains a blacklist section	section: UPX0	1	1245	The file contains a blacklist section	section: UPX1	1	1245	The file contains a blacklist section	section: UPX2	1	1223	The first section is writable	section: UPX0	1	1225	The location of the entry-point is suspicious	section: UPX1:0x003100E0	1	1631	The file contains self-modifying executable section(s)	status: yes	1	2215	The file contains writable and executable section(s)	count: 2	1	1321	The time-stamp of the compiler is suspicious	year: 0	2	1200	The value of 'pointer-symbol-table' is suspicious	value: 0x002DCA00	2	1153	The file contains a virtualized section	section: UPX0	2	1036	The file checksum is invalid	checksum: 0x00000000	3	1634	The file references a group of API	api: execution, count: 1	3	1634	The file references a group of API	api: dynamic-library, count: 2	3	1634	The file references a group of API	api: memory, count: 1	3	1633	The file references a group of hint	hint: dos-message, count: 1	3	1633	The file references a group of hint	hint: utility, count: 2	3	1633	The file references a group of hint	hint: file, count: 12	3	1633	The file references a group of hint	hint: base64, count: 2	3		
xml-id	indicator (33)	detail	level																																																																																																
1430	The file references string(s) tagged as blacklist	count: 4	1																																																																																																
1120	The file is scored by virustotal	score: 52/71	1																																																																																																
1485	The count of libraries is suspicious	count: 1	1																																																																																																
1266	The file imports symbol(s) tagged as blacklist	count: 1	1																																																																																																
1265	The count of imports is suspicious	count: 4	1																																																																																																
1245	The file contains a blacklist section	section: UPX0	1																																																																																																
1245	The file contains a blacklist section	section: UPX1	1																																																																																																
1245	The file contains a blacklist section	section: UPX2	1																																																																																																
1223	The first section is writable	section: UPX0	1																																																																																																
1225	The location of the entry-point is suspicious	section: UPX1:0x003100E0	1																																																																																																
1631	The file contains self-modifying executable section(s)	status: yes	1																																																																																																
2215	The file contains writable and executable section(s)	count: 2	1																																																																																																
1321	The time-stamp of the compiler is suspicious	year: 0	2																																																																																																
1200	The value of 'pointer-symbol-table' is suspicious	value: 0x002DCA00	2																																																																																																
1153	The file contains a virtualized section	section: UPX0	2																																																																																																
1036	The file checksum is invalid	checksum: 0x00000000	3																																																																																																
1634	The file references a group of API	api: execution, count: 1	3																																																																																																
1634	The file references a group of API	api: dynamic-library, count: 2	3																																																																																																
1634	The file references a group of API	api: memory, count: 1	3																																																																																																
1633	The file references a group of hint	hint: dos-message, count: 1	3																																																																																																
1633	The file references a group of hint	hint: utility, count: 2	3																																																																																																
1633	The file references a group of hint	hint: file, count: 12	3																																																																																																
1633	The file references a group of hint	hint: base64, count: 2	3																																																																																																

Los resultados arrojados en el item de Virustotal son exactamente iguales a los ya analizados en la misma herramienta anteriormente por lo que si se desea ahondar mas se puede referir al análisis realizado con Virustotal , el score arrojado es de 52/71, lo cual significa que el archivo es altamente sospechoso.

pestudio 9.09 - Malware Initial Assessment - www.winitor.com [c:\users\master\Desktop\windows_25bfec0c3c81]

property	value
md5	5A5821E97DAFC1A33214AA2FFD66D413
sha1	0242BE4F6DA0542BAD5CB0403F6DF671534FF28
sha256	030401206EA093C9FCB13369C19D7D2E4B6C8497B37972E6E5CF0440D58129F5
size	0x40 (64 bytes)
entropy	3.685
file-ratio	0.00 %
file-header-offset	0x00000000

El encabezado Dos posee entropía de 3.685

pestudio 9.09 - Malware Initial Assessment - www.winitor.com [c:\users\master\Desktop\windows_25bfec0c3c81]

property	value
md5	ADEA9A7C7548BD31136524773DEF37F
sha1	9B9309B58CB37542A8F83D6123E88D1F38AABFCC
sha256	7764E7022DCAC1B5779D1F96FC05AF5C1FEE394AFF8A3A7E9A881E1A1B163A3
size	0x40 (64 bytes)
entropy	4.794
file-ratio	0.01 %
message	This program cannot be run in DOS mode.

El dos -stub posee una entropía de 4.794 y anuncia que el programa no se puede correr en el modo DOS.

Abajo se muestran los directorios.

pestudio 9.09 - Malware Initial Assessment - www.winitor.com [c:\users\master\Desktop\windows_25bfec0c3c81]

name (15/15)	size (bytes)	location (address)	location (section)	time-stamp	invalid (0)	missing (0)	empty (13)
export-table	0x00000000 (0)	0x00000000	n/a	n/a	-	-	x
import-name	0x00000088 (136)	0x00311000	UPX2	empty	-	-	-
resource	0x00000000 (0)	0x00000000	n/a	n/a	-	-	x
exception	0x00000000 (0)	0x00000000	n/a	n/a	-	-	x
security	0x00000000 (0)	0x00000000	n/a	n/a	-	-	x
relocation	0x0000000C (12)	0x00311088	UPX2	empty	-	-	-
debug	0x00000000 (0)	0x00000000	n/a	n/a	-	-	x
architecture	0x00000000 (0)	0x00000000	n/a	n/a	-	-	x
global-pointer	0x00000000 (0)	0x00000000	n/a	n/a	-	-	x
thread-storage	0x00000000 (0)	0x00000000	n/a	n/a	-	-	x
load-configuration	0x00000000 (0)	0x00000000	n/a	n/a	-	-	x
bound-import	0x00000000 (0)	0x00000000	n/a	n/a	-	-	x
import-address	0x00000000 (0)	0x00000000	n/a	n/a	-	-	x
delay-loaded	0x00000000 (0)	0x00000000	n/a	n/a	-	-	x
com-runtime	0x00000000 (0)	0x00000000	n/a	n/a	-	-	x
strings (10841)							

En el screen siguiente se puede visualizar de manera detallada el porque se dice que el archivo es sospechoso.

The screenshot shows the PEStudio interface with the following details:

File Path: c:\users\master\Desktop\windows_25bfec0c3c81

Analysis Results:

property	value	value	value
name	UPX0	UPX1	UPX2
md5	n/a	1C6BA787BE2AB42C18D588...	C363A0A8619C9CA2E98C99...
entropy	n/a	8.000	1.513
file-ratio (99.94 %)	n/a	99.89 %	0.06 %
raw-address	0x00000200	0x00000200	0x000DD000
raw-size (905216 bytes)	0x00000000 (0 bytes)	0x000DCE00 (904704 bytes)	0x00000200 (512 bytes)
virtual-address	0x00401000	0x00634000	0x00711000
virtual-size (3215360 bytes)	0x00233000 (2306048 bytes)	0x000DD000 (905216 bytes)	0x00001000 (4096 bytes)
entry-point	-	0x003100E0	-
characteristics	0xE0000080	0xE0000040	0xC0000040
writable	x	x	x
executable	x	x	-
shareable	-	-	-
discardable	-	-	-
initialized-data	-	x	x
uninitialized-data	x	-	-
unreadable	-	-	-
self-modifying	x	x	-
virtualized	x	-	-
file	n/a	n/a	n/a

Diseccionado por el valor de punto de entrada UPX, se puede ver que el fichero es modificable, ejecutable y automodificable, lo cual es un signo claro de que se trata de un archivo malicioso.

En cuanto a las librerías la herramienta hallo la librería kernel32.dll lo cual es normal en un archivo Windows.

The screenshot shows the pestudio 9.09 interface. On the left, there is a tree view of file contents under the path c:\users\master\Desktop\windows_25bfec0c3c81. The 'libraries' node is expanded, showing 'kernel32.dll' as the only entry. On the right, a table provides details about this library:

library (1)	blacklist (0)	type (1)	imports (4)	description
kernel32.dll	-	implicit	4	Windows NT BASE API Client DLL

En cuanto a los archivos importados se hallaron 4, uno de ellos virtualprotect esta dentro de la lista negra, esto se puede ver en la columna de blacklist lo cual es una señal de que el archivo podría ser sospechoso, todos estos archivos son soportados por la librería kernel32.dll

The screenshot shows the pestudio 9.09 interface. On the left, there is a tree view of file contents under the path c:\users\master\Desktop\windows_25bfec0c3c81. The 'imports' node is selected. On the right, a table lists the imported functions:

name (4)	group (3)	type (1)	ordinal (0)	blacklist (1)	anti-debug (0)	undocumented (0)	deprecated (0)	library (1)
VirtualProtect	memory	implicit	-	x	-	-	-	kernel32.dll
LoadLibraryA	dynamic-library	implicit	-	-	-	-	-	kernel32.dll
GetProcAddress	dynamic-library	implicit	-	-	-	-	-	kernel32.dll
ExitProcess	execution	implicit	-	-	-	-	-	kernel32.dll

Las reloaciones son muy comunes en los malwares y este caso se hallaron cuatro ítems.

item (4)	address	type (2)
0x30E2	0x000010E2	high-low
0x0000	0x00001000	absolute
0x30E2	0x000020E2	high-low
0x0000	0x00002000	absolute

pestudio 9.09 - Malware Initial Assessment - www.winitor.com [c:\users\master\Desktop\windows_25bfec0c3c81ab55cf85a57367c14cc6803a03e2e9b4af72e7bbca9420fe7c5]

file settings about

c:\users\master\Desktop\windows_25bfec0c3c81

type (1)	size (bytes)	file-offset	blacklist (4)	hint (17)	group (3)	value (10841)
ascii	4	0x00000178	x	utility	-	UPX0
ascii	4	0x000001A0	x	utility	-	UPX1
ascii	14	0x0000DD078	x	-	memory	VirtualProtect
ascii	4	0x000001C8	x	-	-	UPX2
ascii	4	0x00002E35	-	file	-	Op.H
ascii	4	0x00008CBB	-	file	-	p.C
ascii	6	0x0018108	-	file	-	HO.lwd
ascii	4	0x002F00D	-	file	-	o.RM
ascii	5	0x00044402	-	file	-	E.e.C
ascii	4	0x0006A3B9	-	file	-	z).H
ascii	4	0x0006B58F	-	file	-	:l.C
ascii	4	0x0006DC48	-	file	-	os.c
ascii	10	0x00079004	-	file	-	nAg\$d3Ya.c
ascii	4	0x000C4537	-	file	-	:DB
ascii	4	0x000CC25A	-	file	-	:l.Z
ascii	12	0x000DD03C	-	file	-	KERNEL32.DLL
ascii	40	0x0000004D	-	dos-message	-	This program cannot be run in DOS mode.
ascii	14	0x000A71B	-	base64	-	5a3:y9&_H8wn=
ascii	8	0x0009B08B	-	base64	-	FX!&s%=_
ascii	11	0x000DD04C	-	-	execution	ExitProcess
ascii	14	0x000DD05A	-	-	dynamic-library	GetProcAddress
ascii	11	0x000DD06B	-	-	dynamic-library	LoadLibrary
ascii	4	0x000001F0	-	-	-	3.95
ascii	4	0x000001F5	-	-	-	UPX!
ascii	5	0x00000224	-	-	-	<7 =
ascii	4	0x00000247	-	-	-	k.SS
ascii	4	0x00000290	-	-	-	8&Pr
ascii	4	0x000002CD	-	-	-	aiY?
ascii	4	0x000002DE	-	-	-	x&v
ascii	4	0x000002EA	-	-	-	mb:n

Con relación a los strings, se puede ver que se hallaron 10.841 ítems de tipo ascii, 4 de ellas se encuentran en la blacklist, ya lo hemos visto y comentado antes, UPX0, UPX1, UPX2 y virtualprotect. También se encontraron librerías dinámicas como GetProcAddress, load library y un ejecutable Exit process, estos tres ítems engloban un proceso, exitprocess termina un proceso, los procesos que vinculan explícitamente a un archivo DLL llaman a GetProcAddress para obtener la dirección de una función exportada en el archivo DLL y la función LoadLibrary proyecta el módulo ejecutable especificado en el espacio de direcciones del proceso desde el que se invoca.

Para hallar strings también se usa la herramienta **strings** ejecutada desde un cmd y hallo varios datos que podrían ser importantes y está ligada al fichero, esta herramienta como se ve, hallo menos ítems que PEStudio, el cual arroja resultados más completos.

```
C:\Users\master\Desktop>strings.exe -n 10 windows_25bfec0c3c81ab55cf85a57367c14c6803a03e2e9b4af72e7bbca9420fe7c5

Strings v2.53 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

!This program cannot be run in DOS mode.
v&Ei3zgOrJ
5a3;y<9&,H8wn=
d\Jz+PEfR6
bUbz,zo}lZ
>\U4GdY~l<~
>W8OK/'ePu
;0~O_vRhX
q5lagY;r5K"j
3bMHYMGc=/:_
=Xmp5a"><.
q?Jp;_EC>v
56a7hL82s0
E!6>*Zx"U:
&Z!_nX1'U
;Qh6<E?D~6!
nAg$3Ya.c
?c[&TMsU_#
+e/ ]!ILi
Dy8i!6~i:<
U0! 'USW!N<RT&
Jr[?P1_,>q
"-^,^=f<H
;>EJNc3>&d1
G2Z91glaOP
KERNEL32.DLL
ExitProcess
GetProcAddress
LoadLibraryA
VirtualProtect

C:\Users\master\Desktop>
```

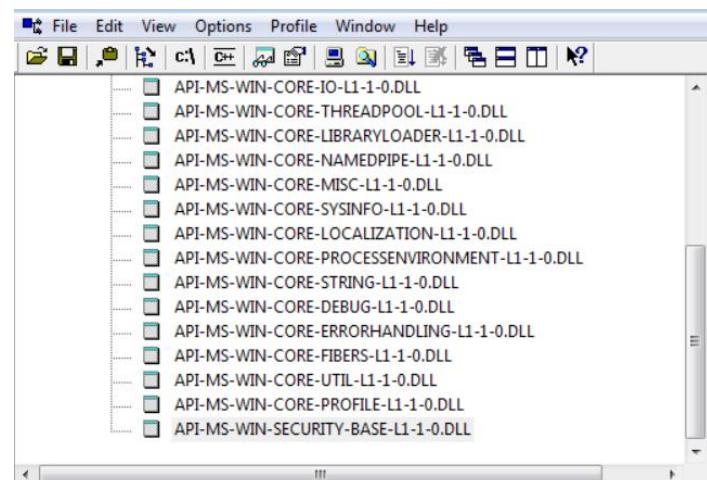
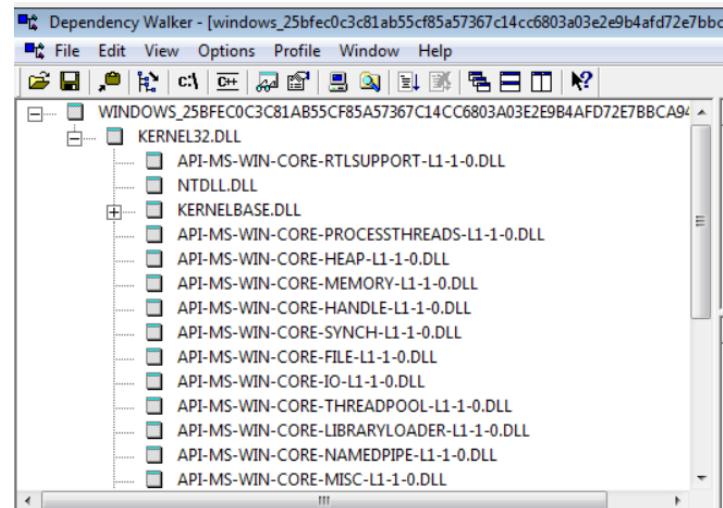
Procedemos a ahondar el análisis con la herramienta **GMER**, que es una aplicación que detecta y elimina rootkits, en el pantallazo siguiente se muestran los procesos que se están ejecutando, teniendo en cuenta que se trata de un análisis estatico y el malware no esta siendo ejecutado.

GMER 2.2.19882 - WINDOWS 6.1.7601 Service Pack 1 x64 AntiVirus: http://www.avast.com											
Processes	Modules	Services	Files	Registry	Rootkit/Malware	CMD	Autostart				
Process	Parameters	PID	Memory	Thr...	Handles	User time	Kernel time				
System Idle		0	24 K	2	0	0,000	299,406				
System		4	1080 K	89	522	0,000	10,406				
\SystemRoot\System32\smss.exe		260	1272 K	2	30	0,000	0,015				
C:\Windows\system32\csrss.exe		340	6144 K	9	473	0,015	0,156				
C:\Windows\system32\wininit.exe		392	8600 K	3	80	0,000	0,046				
C:\Windows\system32\csrss.exe		400	7140 K	10	196	0,062	0,687				
C:\Windows\system32\winlogon.exe		456	1198...	4	112	0,046	0,062				
C:\Windows\system32\services.exe		492	1296...	11	201	0,046	0,203				
C:\Windows\system32\lsass.exe		516	1859...	9	626	0,390	0,156				
C:\Windows\system32\lsm.exe		524	1153...	12	208	0,000	0,015				
C:\Windows\system32\svchost.exe		628	1875...	12	358	0,093	0,171				
C:\Windows\System32\VBoxService.e...		692	9260 K	14	128	0,015	0,062				
C:\Windows\system32\svchost.exe		760	1256...	8	284	0,015	0,046				
C:\Windows\System32\svchost.exe		848	2541...	21	435	0,078	0,187				
C:\Windows\System32\svchost.exe		912	2861...	18	377	0,015	0,046				
C:\Windows\system32\svchost.exe		936	2070...	18	359	0,093	0,078				
C:\Windows\system32\svchost.exe		964	5866...	45	1144	0,375	0,296				
C:\Windows\system32\svchost.exe		384	2676...	26	551	0,031	0,125				
C:\Windows\system32\svchost.exe		224	1511...	19	249	0,000	0,015				
C:\Windows\System32\spoolsv.exe		1184	2463...	14	284	0,015	0,031				
C:\Windows\system32\svchost.exe		1212	2438...	20	326	0,234	0,093				
C:\Windows\System32\svchost.exe		1308	1378...	11	143	0,000	0,000				
C:\Program Files (x86)\free FTPd\freeF...		1336	1808...	5	116	0,015	0,031				
C:\Windows\System32\svchost.exe		2040	1003...	15	371	2,015	0,484				
C:\Windows\system32\taskhost.exe		1876	2400...	13	215	0,015	0,046				
C:\Windows\system32\taskeng.exe		1964	1082...	7	87	0,000	0,000				
C:\Windows\system32\sppsvc.exe		1304	1603...	5	149	0,140	0,203				
Libraries Threads											
<table border="1"> <thead> <tr> <th>Name</th> <th>Size</th> <th>Address</th> </tr> </thead> </table>									Name	Size	Address
Name	Size	Address									

La grafica abajo muestra los rootkit/malware hallados por esta herramienta y el tipo de archivo de estos rootkits.

GMER 2.2.19882 - WINDOWS 6.1.7601 Service Pack 1 x64 AntiVirus: http://www.avast.com		
Processes	Modules	Services
Type	Name	Value
.text	C:\Windows\system32\ntoskrnl.exe!KiCpul + 978	fffff80002cab372 1 byte [21]
.text	C:\Program Files\CCleaner\CCleaner64.exe[2440] C:\Windows\system32\kernel32.dll!SetUnhandledExceptionFilter + 1	0000000077608d61 7 bytes [31, C0, C3, 90, 90, 90, 90]
Reg	HKLMSYSTEM\CurrentControlSet\services\BTHPORT\Parameters\Keys\b8e856301701	
Reg	HKLMSYSTEM\ControlSet002\services\BTHPORT\Parameters\Keys\b8e856301701 (not active ControlSet)	

La herramienta **Dependency Walker**, ayuda a ver a detalle el contenido y como esta confirmado el fichero, esta herramienta trae mucha información diseccionada por lo que se tomara solo pantallazos de lo mas importante.



Dependency Walker - [windows_25bfec0c3c81ab55cf85a57367c14cc6803a03e2e9b4af72e7bbca9420fe7c5]

File Edit View Options Profile Window Help

API-MS-WIN-CORE-IO-L1-1-0.DLL
 API-MS-WIN-CORE-THREADPOOL-L1-1-0.DLL
 API-MS-WIN-CORE-LIBRARYLOADER-L1-1-0.DLL
 API-MS-WIN-CORE-NAMEDPIPE-L1-1-0.DLL
 API-MS-WIN-CORE-MISC-L1-1-0.DLL
 API-MS-WIN-CORE-SYSINFO-L1-1-0.DLL
 API-MS-WIN-CORE-LOCALIZATION-L1-1-0.DLL
 API-MS-WIN-CORE-PROCESSENVIRONMENT-L1-1-0.DLL
 API-MS-WIN-CORE-STRING-L1-1-0.DLL
 API-MS-WIN-CORE-DEBUG-L1-1-0.DLL
 API-MS-WIN-CORE-ERRORHANDLING-L1-1-0.DLL
 API-MS-WIN-CORE-FIBERS-L1-1-0.DLL
API-MS-WIN-CORE-UTIL-L1-1-0.DLL
 API-MS-WIN-CORE-PROFILE-L1-1-0.DLL
 API-MS-WIN-SECURITY-BASE-L1-1-0.DLL

PI	Ordinal ^	Hint	Function	Entry Point
E	N/A	0 (0x000)	Beep	Not Bound

E	Ordinal ^	Hint	Function	Entry Point
E	1 (0x001)	0 (0x000)	Beep	0x00001059
E	2 (0x002)	1 (0x001)	DecodePointer	0x00001063
E	3 (0x003)	2 (0x002)	DecodeSystemPointer	0x00001063
E	4 (0x004)	3 (0x003)	EncodePointer	0x00001063
E	5 (0x005)	4 (0x004)	EncodeSystemPointer	0x00001063

Dependency Walker - [windows_25bfec0c3c81ab55cf85a57367c14cc6803a03e2e9b4af72e7bbca9420fe7c5]

File Edit View Options Profile Window Help

API-MS-WIN-CORE-IO-L1-1-0.DLL
 API-MS-WIN-CORE-THREADPOOL-L1-1-0.DLL
 API-MS-WIN-CORE-LIBRARYLOADER-L1-1-0.DLL
 API-MS-WIN-CORE-NAMEDPIPE-L1-1-0.DLL
 API-MS-WIN-CORE-MISC-L1-1-0.DLL
 API-MS-WIN-CORE-SYSINFO-L1-1-0.DLL
 API-MS-WIN-CORE-LOCALIZATION-L1-1-0.DLL
 API-MS-WIN-CORE-PROCESSENVIRONMENT-L1-1-0.DLL
 API-MS-WIN-CORE-STRING-L1-1-0.DLL
 API-MS-WIN-CORE-DEBUG-L1-1-0.DLL
API-MS-WIN-CORE-ERRORHANDLING-L1-1-0.DLL
 API-MS-WIN-CORE-FIBERS-L1-1-0.DLL
 API-MS-WIN-CORE-UTIL-L1-1-0.DLL
 API-MS-WIN-CORE-PROFILE-L1-1-0.DLL
 API-MS-WIN-SECURITY-BASE-L1-1-0.DLL

PI	Ordinal ^	Hint	Function	Entry Point
E	N/A	0 (0x000)	GetErrorMode	Not Bound
E	N/A	1 (0x001)	GetLastError	Not Bound
E	N/A	2 (0x002)	RaiseException	Not Bound
E	N/A	3 (0x003)	SetErrorMode	Not Bound
E	N/A	4 (0x004)	SetLastError	Not Bound

E	Ordinal ^	Hint	Function	Entry Point
E	1 (0x001)	0 (0x000)	GetErrorMode	0x00001062
E	2 (0x002)	1 (0x001)	GetLastError	0x00001062
E	3 (0x003)	2 (0x002)	RaiseException	0x0000106A
E	4 (0x004)	3 (0x003)	SetErrorMode	0x0000107A
E	5 (0x005)	4 (0x004)	SetLastError	0x00001072
E	6 (0x006)	5 (0x005)	SetUnhandledExceptionFilter	0x0000107A
E	7 (0x007)	6 (0x006)	UnhandledExceptionFilter	0x0000107A

Dependency Walker - [windows_25bfec0c3c81ab55cf85a57367c14cc6803a03e2e9b4af72e7bbc9420fe7c5]

PI	Ordinal ^	Hint	Function	Entry Point
E	N/A	0 (0x0000)	ExpandEnvironmentStringsA	Not Bound
E	N/A	1 (0x0001)	ExpandEnvironmentStringsW	Not Bound
E	N/A	2 (0x0002)	FreeEnvironmentStringsA	Not Bound
E	N/A	3 (0x0003)	FreeEnvironmentStringsW	Not Bound
E	N/A	4 (0x0004)	GetCommandLineA	Not Bound
E	N/A	5 (0x0005)	GetCommandLineW	Not Bound
E	N/A	6 (0x0006)	GetCurrentDirectoryA	Not Bound
E	N/A	7 (0x0007)	GetCurrentDirectoryW	Not Bound
E	1 (0x0001)	0 (0x0000)	ExpandEnvironmentStringsA	0x0000108D
E	2 (0x0002)	1 (0x0001)	ExpandEnvironmentStringsW	0x0000108D
E	3 (0x0003)	2 (0x0002)	FreeEnvironmentStringsA	0x0000106F
E	4 (0x0004)	3 (0x0003)	FreeEnvironmentStringsW	0x0000106F
E	5 (0x0005)	4 (0x0004)	GetCommandLineA	0x00001067
E	6 (0x0006)	5 (0x0005)	GetCommandLineW	0x00001067
E	7 (0x0007)	6 (0x0006)	GetCurrentDirectoryA	0x00001083
E	8 (0x0008)	7 (0x0007)	GetCurrentDirectoryW	0x00001083

Dependency Walker - [windows_25bfec0c3c81ab55cf85a57367c14cc6803a03e2e9b4af72e7bbc9420fe7c5]

PI	Ordinal ^	Hint	Function	Entry Point
E	N/A	0 (0x0000)	GetComputerNameExA	Not Bound
E	N/A	1 (0x0001)	GetComputerNameExW	Not Bound
E	N/A	2 (0x0002)	GetDynamicTimeZoneInformation	Not Bound
E	N/A	3 (0x0003)	GetLocalTime	Not Bound
E	N/A	4 (0x0004)	GetLogicalProcessorInformation	Not Bound
E	N/A	5 (0x0005)	GetLogicalProcessorInformationEx	Not Bound
E	N/A	8 (0x0008)	GetSystemInfo	Not Bound
E	N/A	9 (0x0009)	GetSystemTime	Not Bound
E	1 (0x0001)	0 (0x0000)	GetComputerNameExA	0x0000105C
E	2 (0x0002)	1 (0x0001)	GetComputerNameExW	0x0000105C
E	3 (0x0003)	2 (0x0002)	GetDynamicTimeZoneInformation	0x00001082
E	4 (0x0004)	3 (0x0003)	GetLocalTime	0x00001066
E	5 (0x0005)	4 (0x0004)	GetLogicalProcessorInformation	0x0000106E
E	6 (0x0006)	5 (0x0005)	GetLogicalProcessorInformationEx	0x0000105C
E	7 (0x0007)	6 (0x0006)	GetSystemDirectoryA	0x0000106E
E	8 (0x0008)	7 (0x0007)	GetSystemDirectoryW	0x0000106F

Estos son algunos de las dependencias interesantes halladas con la herramienta Dependency Walker.

Otra herramienta de análisis que se puede utilizar es **PEBEAR**, permite de un vistazo rápido conocer información sobre el malware. También muestra la información que hemos visto anteriormente como Dos header y Dos stub, y un árbol que ya vimos con otra herramienta.

Información general del malware que ya se vio, como los hashes, en el segundo gráfico de este apartado e puede ver que el archivo es ejecutable.

File Settings View Compare Info

Disasm: Headers to [UPX1] General DOS Hdr File Hdr Optional Hdr Section Hdrs Imports BaseReloc.

Path	C:/Users/master/Desktop/windows_25bfec0c3c81ab55cf85a57367c14cc6803a03e2e9b4af72e7bbca9420fe7c5
Is Truncated?	No
File size	905728
Loaded size	905728
File Alignment Units	1769
Checksum	ead1a
MDS	da13022097518d123a91a3958be326da
SHA1	24a71ab462594d5a159bbf176588af951aba1381
SHA256	25bfec0c3c81ab55cf85a57367c14cc6803a03e2e9b4af72e7bbca9420fe7c5

Disasm: Headers to [UPX1] General DOS Hdr File Hdr Optional Hdr Section Hdrs Imports BaseReloc.

Offset	Name	Value	Meaning
84	Machine	14c	Intel 386
86	Sections Count	3	3
88	Time Date Stamp	0	jueves, 01.01.1970 00:00:00 UTC
8C	Ptr to Symbol Table	2dca00	3000832
90	Num. of Symbols	0	0
94	Size of OptionalHeader	e0	224
96	Characteristics	302	
		2	File is executable (i.e. no unresolved external references).
		100	32 bit word machine.
		200	Debugging info stripped from file in .DBG file

Lo que se rescata de esta herramienta es el desmembramiento y el nivel de detalle del malware como se muestra en la grafica de abajo como los datos de directorio y la diferenciación según el comprresor.

Data Directory		Address	Size
F8	Export Directory	0	0
100	Import Directory	311000	88
108	Resource Directory	0	0
110	Exception Directory	0	0
118	Security Directory	0	0
120	Base Relocation Table	311088	C
128	Debug Directory	0	0
130	Architecture Specific Data	0	0
138	RVA of GlobalPtr	0	0
140	TLS Directory	0	0
148	Load Configuration Directory	0	0
150	Bound Import Directory in headers	0	0
158	Import Address Table	0	0
160	Delay Load Import Descriptors	0	0
168	.NET header	0	0

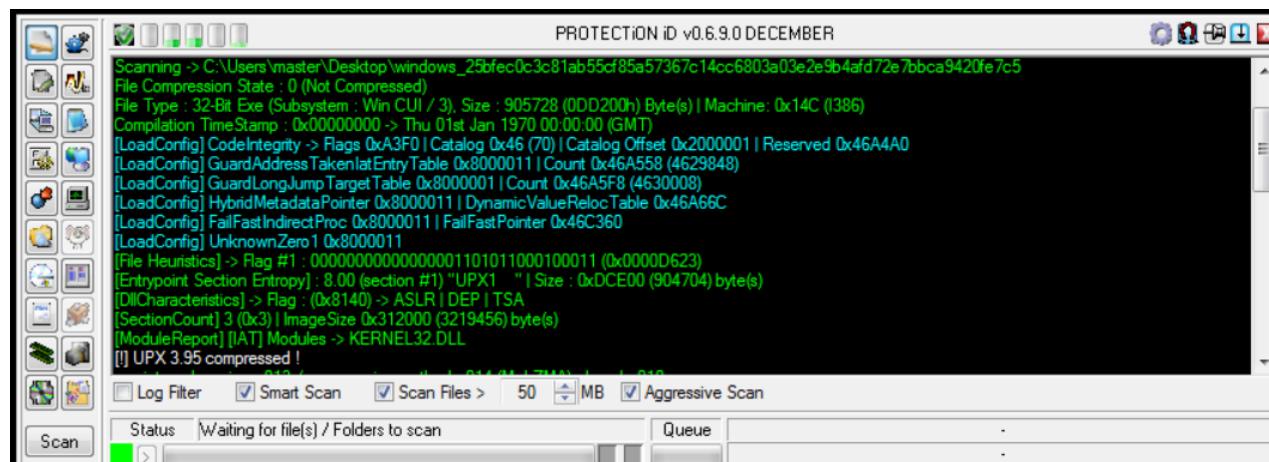
Disasm: Headers to [UPX1]									
	General	DOS Hdr	File Hdr	Optional Hdr	Section Hdrs	Imports	BaseReloc.		
+	+								
Name	Raw Addr.	Raw size	Virtual Addr.	Virtual Size	Characteristics	Ptr to Reloc.	Num. of Reloc.	Num. of Linenum.	
▷ UPX0 200	0	1000	233000	E0000080	0	0	0	0	
▷ UPX1 200	DCE00	234000	DD000	E0000040	0	0	0	0	
▷ UPX2 DD000	200	311000	1000	C0000040	0	0	0	0	

Tambien lo ya visto en otra herramienta de otra forma, la librería y sus dependencias.

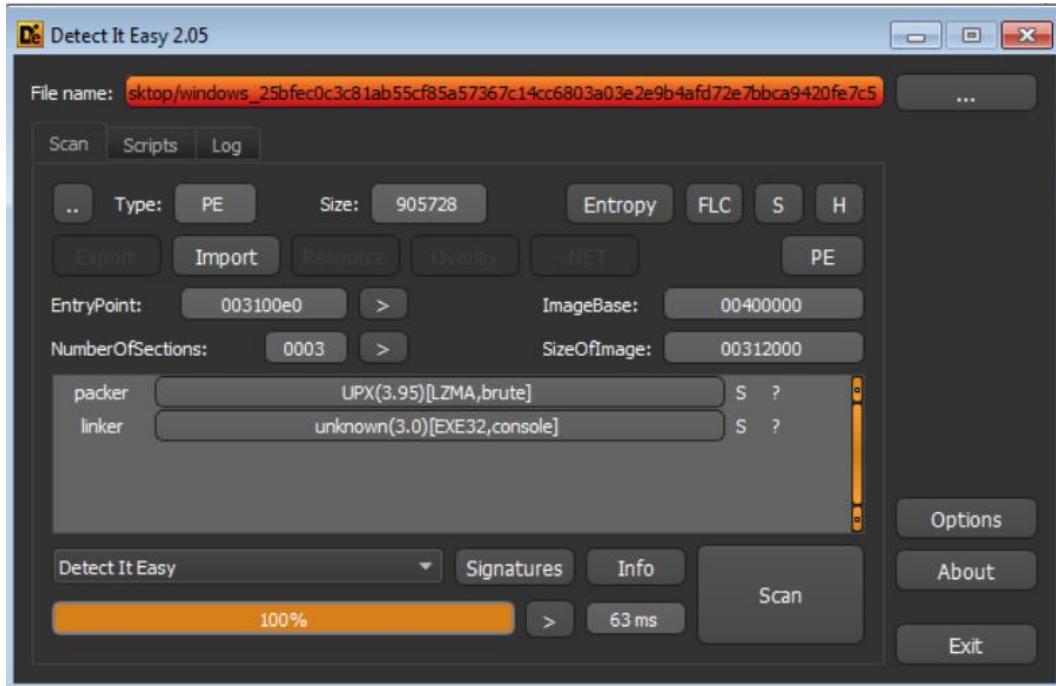
Disasm: Headers to [UPX1]		General	DOS Hdr	File Hdr	Optional Hdr	Section Hdrs	<input checked="" type="checkbox"/> Imports	<input checked="" type="checkbox"/> BaseReloc.
Offset	Name	Func. Count	Bound?	OriginalFirstThun	TimeDateStamp	Forwarder	NameRVA	FirstThunk
DD000	KERNEL32.DLL	4	FALSE	0	0	0	31103C	311028

KERNEL32.DLL [4 entries]						
Call via	Name	Ordinal	Original Thunk	Thunk	Forwarder	Hint
311028	LoadLibraryA	-	-	311068	-	0
31102C	ExitProcess	-	-	31104A	-	0
311030	GetProcAddress	-	-	311058	-	0
311034	VirtualProtect	-	-	311076	-	0

Por otro lado, la herramienta **protección ID**, detecta si el archivo esta comprimido o no, se ha pasado a la herramienta primero el archivo que se ha estado analizando denominado Windows, y detecto la compresión



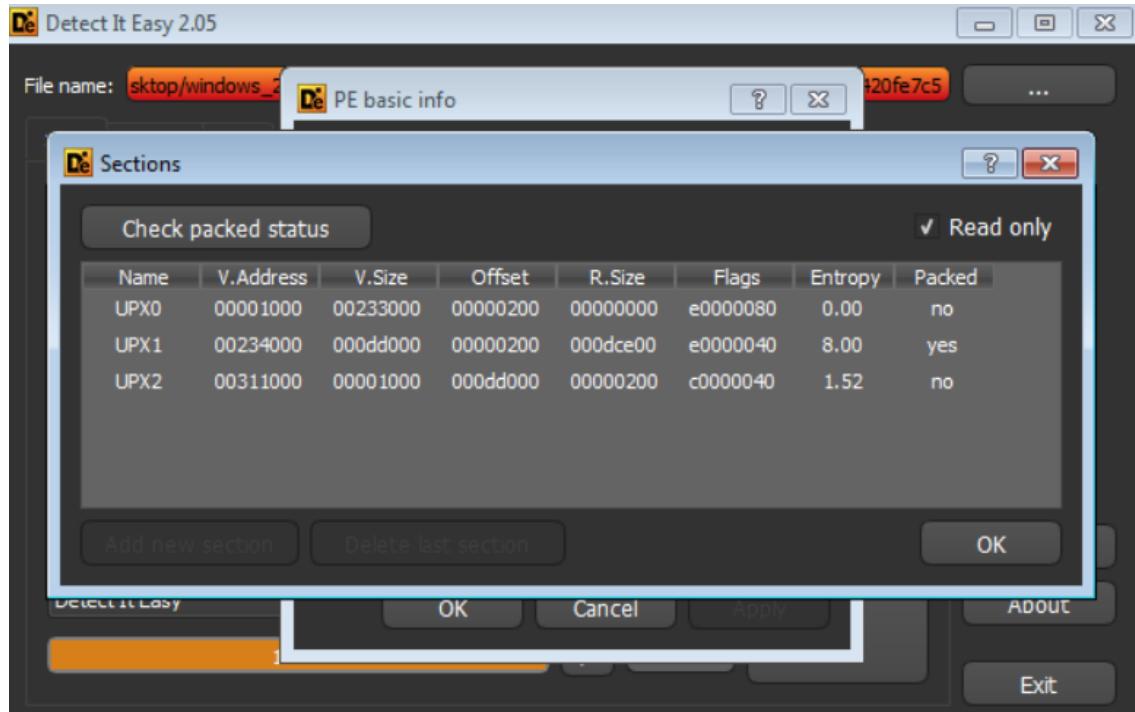
La herramienta Detect it easy es otra herramienta que disecciona el archivo sospechoso,



En el pantallazo anterior se puede ver el tamaño del archivo y en el siguiente la entropía que es lo que determina si el archivo es malicioso, y con la puntuación cerca de 8 se determina que se trata de un malware



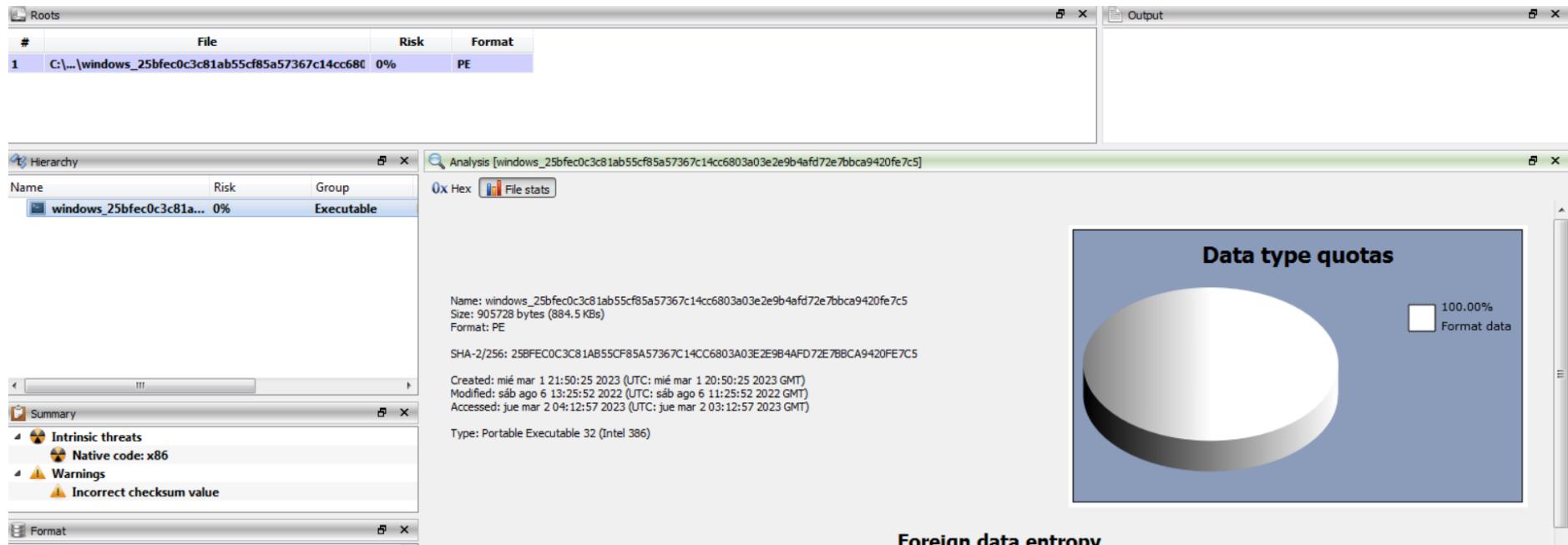
Con la herramienta PEBEAR hemos visto el mismo dato pero con esta herramienta se puede ver mejor



The screenshot shows the main interface of Detect It Easy 2.05. The title bar shows the file path 'C:/Users/master/Desktop/windows_25bfec0c381ab55cf85a57367c14cc6803a03e2e9b4af72e7bbca9420fe7c5'. The toolbar includes 'New', '525', 'Read only', 'Save', 'Debug', 'Run', 'Show type', 'Show version', 'Show options', and 'Highlight'. The left sidebar lists various file names under the 'PE' category, with 'ABC_Cryptor.2.sg' selected. The right pane contains a code editor with the following C-like pseudocode:

```
1 // DIE's signature file
2
3 init("protector","ABC Cryptor");
4
5 function detect(bShowType,bShowVersion,bShowOptions)
6 {
7     if(PE.compareEP("68FF6424F06858585890FFD4508840F205B095F6950F850181BBFF"))
8     {
9         sVersion="1.0";
10        bDetected=1;
11    }
12
13    return result(bShowType,bShowVersion,bShowOptions);
14}
15
```

La última herramienta de análisis utilizada es **Cerbero** que si bien no arroja mucha información confirma todo lo ya visto anteriormente, como el SHA256 y menciona que el archivo es ejecutable.



5 CONCLUSIONES

Concluido este estudio, y luego de una exploración del contenido del archivo se concluye que se trata de un archivo malicioso, que una vez ejecutado puede robar información de un sistema, esto teniendo en cuenta el análisis estático realizado y que mostró algunos patrones, librerías, strings que se encuentran en lista negra que podrían actuar de manera amenazante al ser ejecutado el archivo. Se comprobó con diversas herramientas que arrojaron resultados similares que el archivo puede ser malicioso.

Se recomienda la realización de un análisis dinámico y un análisis de código para conocer más a fondo la funcionalidad del malware y su impacto real de manera que se tomen las medidas necesarias y preventivas para evitar ataques con este tipo de ransomware que se puede ser transmitido a través de correos como phishing o ataques man in the middle mediante el acceso a una máquina objetivo.

