

# **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.....	8
5	ANALISIS DINAMICO.....	31
6	CONCLUSIONES Y RECOMENDACIONES.....	52
7	BIBLIOGRAFIA .....	54
8	ANEXOS .....	55

## 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 paralelizar 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
- Analisis estatico
- 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 integral del malware HIVE, desde una perspectiva estática y dinámica, con el fin de conocer a detalle este ransomware, su funcionalidad, contenido y comprender procesos y su impacto desde una visión general a partir de su disección y estudio dinámico.

Para realizar lo mencionado en el párrafo anterior, se utilizarán una serie de herramientas que arrojan un análisis estático y dinámico del malware a partir de su contenido, su funcionalidad y sus procesos, esto se llevará a cabo en un laboratorio de Virtualbox en una máquina virtual Windows 7 professional.

#### 3.2 Objetivo General

Analizar de forma estatica Y dinamica 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 disección 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.

El análisis dinámico de malwares es la segunda etapa de un proceso de estudio acerca de un programa malicioso en ciberseguridad. Los análisis dinámicos consisten en ejecutar malwares en máquinas virtuales, que son entornos preparados especialmente para hacerlo sin dañar el hardware o el software de la máquina real en el que se hace el estudio.

### 3.5 Herramientas Utilizadas

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

### 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

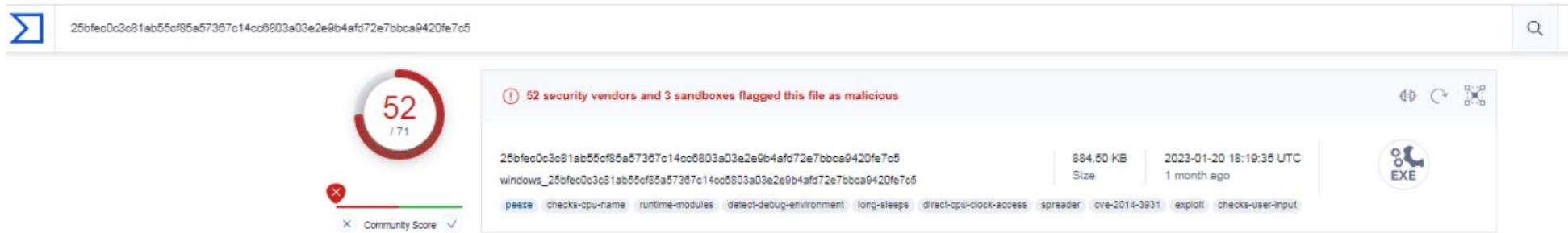
<https://github.com/ytisf/theZoo/tree/master/malware/Binaries/Ransomware.Hive>

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 exit ... 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\NSDT\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.

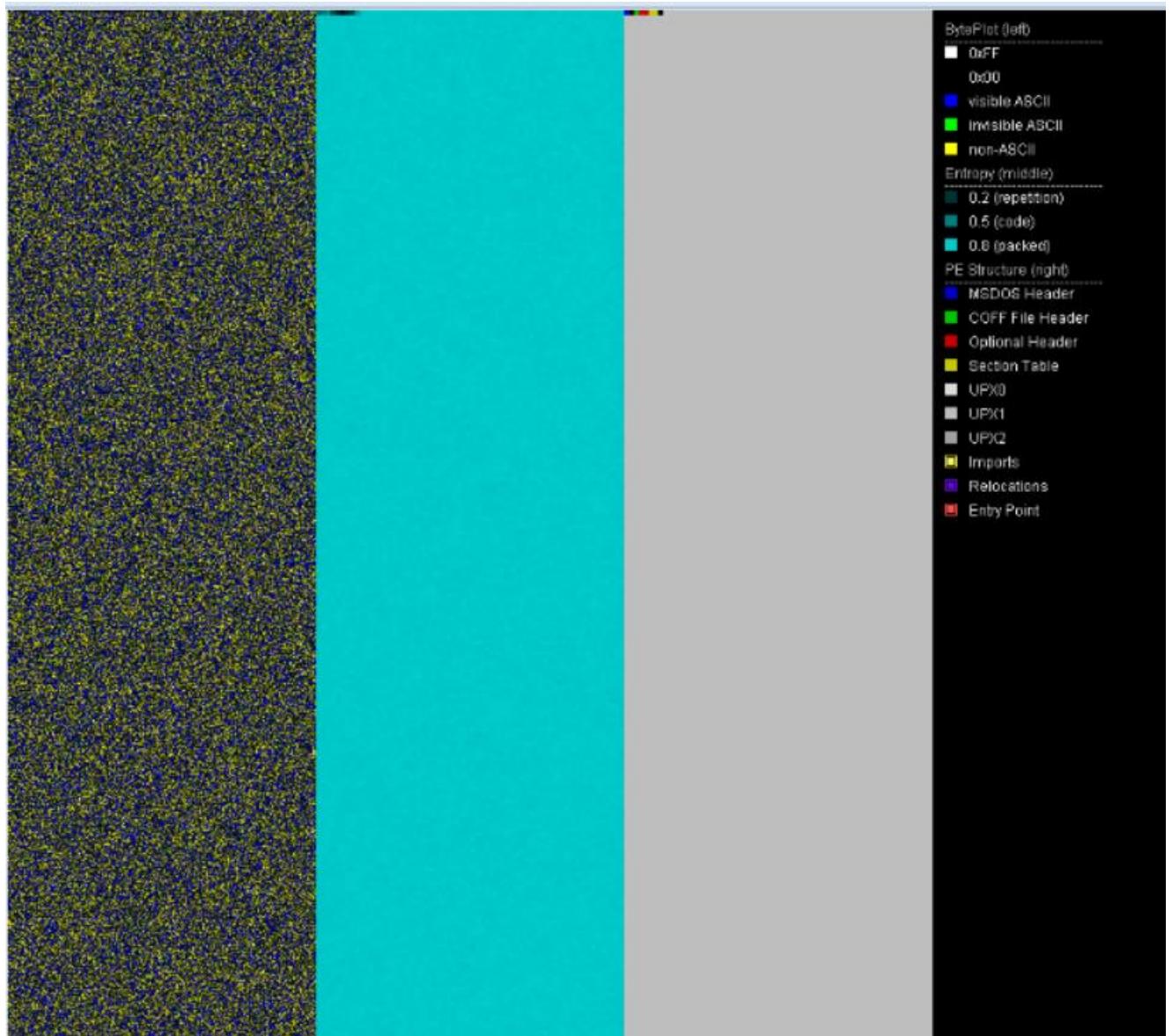
```

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 about

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:**

- Indicators:** UPX0, UPX1, UPX2
- MD5:** n/a, 1C6BA787BE2AB42C18D588...
- Entropy:** n/a, 8.000, 1.513
- File Ratio:** 99.94%, 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 for the file '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 for the file '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\_25bfec0c3c81]

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	<a href="#">VirtualProtect</a>
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	<a href="#">ExitProcess</a>
ascii	14	0x000DD05A	-	-	dynamic-library	<a href="#">GetProcAddress</a>
ascii	11	0x000DD06B	-	-	dynamic-library	<a href="#">LoadLibrary</a>
ascii	4	0x000001F0	-	-	-	3.95
ascii	4	0x000001F5	-	-	-	UPX!
ascii	5	0x00000224	-	-	-	< ? =
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 items 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?7Jp;_EC>v
56a7hL82s0
E!6>*Zx"U:
&Z!_nX1'U
;Qh6<E?D~6!
nAg$3Ya.c
?c[&TMsU_#
+e/ !I Li
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>
```

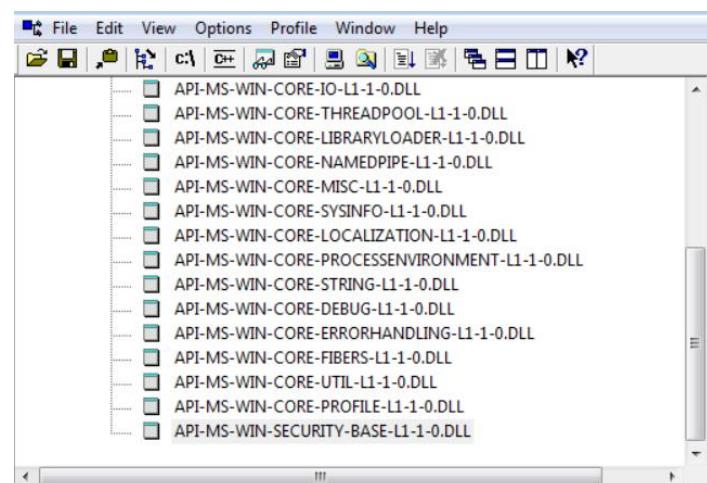
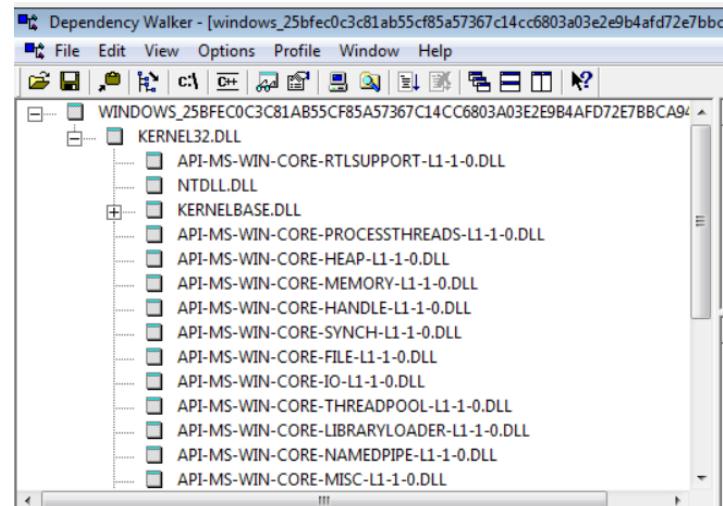
Procedemos a ahondar el análisis con la herramienta **GMER**, que es una aplicación que detecta y elimina rootkits, en el pantallazo siguiente se muestran los procesos que se están ejecutando, teniendo en cuenta que se trata de un análisis estatico y el malware no esta siendo ejecutado.

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				
<a href="#">Libraries</a>   <a href="#">Threads</a>											
<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]**

**Dependency Walker - [windows\_25bfec0c3c81ab55cf85a57367c14cc6803a03e2e9b4af72e7bbc9420fe7c5]**

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

E	Ordinal ^	Hint	Function	Entry Point
[C]	1 (0x0001)	0 (0x0000)	GetComputerNameExA	0x0000105C
[C]	2 (0x0002)	1 (0x0001)	GetComputerNameExW	0x0000105C
[C]	3 (0x0003)	2 (0x0002)	GetDynamicTimeZoneInformation	0x00001082
[C]	4 (0x0004)	3 (0x0003)	GetLocalTime	0x00001066
[C]	5 (0x0005)	4 (0x0004)	GetLogicalProcessorInformation	0x0000106E
[C]	6 (0x0006)	5 (0x0005)	GetLogicalProcessorInformationEx	0x0000105C
[C]	7 (0x0007)	6 (0x0006)	GetSystemDirectoryA	0x0000106E
[C]	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

**File**

- Windows\_25bfec0c3c81ab55cf...
- DOS Header
- DOS stub
- NT Headers
  - Signature
  - File Header
  - Optional Header
- Section Headers
- Sections
  - UPX0
  - UPX1
  - EP = DC2E0
  - UPX2

**Disasm: Headers to [UPX1]**

0	1	2	3	4	5	6	7	8	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8
1FF	B8	B0	D0	3C	A9	E7	86	EE	30	00	C2	C0	0D	00	00	CC	* * B < @ q . , 0						
20F	2D	00	24	1A	00	54	1A	03	00	45	B1	00	67	D4	E5	35	- - \$ . . T . . .						
21F	38	18	79	EA	T3	3C	5D	37	7B	3D	B6	20	D4	93	CD	C9	8 . y & < ] 7 {						
22F	03	4D	39	EE	F9	A6	D6	C0	05	9F	3A	18	09	2C	BC	5D	. M 9 i u ; O & .						
23F	C9	B9	FF	FD	42	94	91	9F	6B	20	35	24	AA	6F	A7	3C	é i y y B . . . k						
24F	EB	CC	C4	15	B1	7A	BB	F3	F3	B6	D7	91	24	2C	FF	74	8 i Ä . . . z . ó ó						
25F	CF	EA	EE	FO	A0	C4	3C	33	A0	D9	A6	4C	97	37	79	5B	I ö i ä . Ä < 3 .						
26F	CR	D1	F9	6C	9E	5E	54	F5	B1	CC	34	FC	CR	41	2F	00	¶ n a i . o t d .						

**File info**

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]			
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

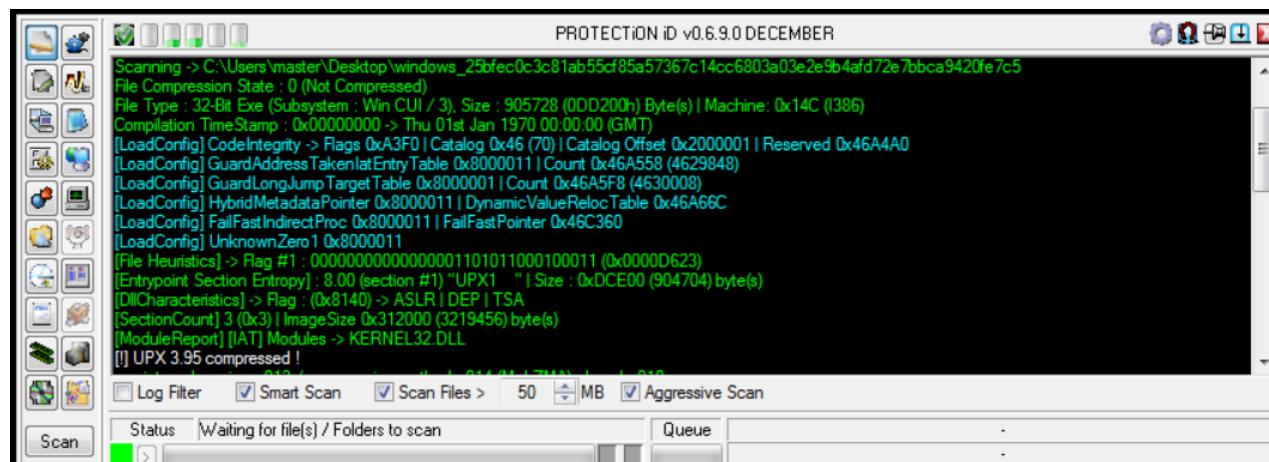
Disasm: Headers to [UPX1]									
	General	DOS Hdr	File Hdr	Optional Hdr	Section Hdrs	Imports	BaseReloc.		
+	00								
Name	Raw Addr.	Raw size	Virtual Addr.	Virtual Size	Characteristics	Ptr to Reloc.	Num. of Reloc.	Num. of Linenum.	
▷ UPX0	200	0	1000	233000	E0000080	0	0	0	
▷ UPX1	200	DCE00	234000	DD000	E0000040	0	0	0	
▷ UPX2	DD000	200	311000	1000	C0000040	0	0	0	

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

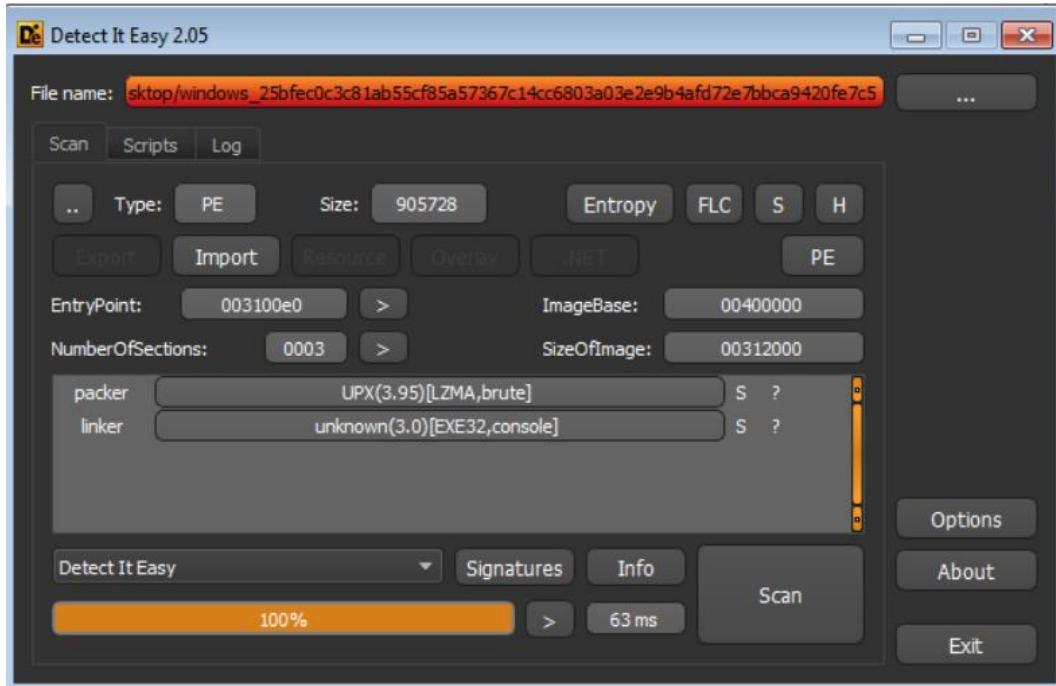
Disasm: Headers to [UPX1]		General	DOS Hdr	File Hdr	Optional Hdr	Section Hdrs	<input checked="" type="checkbox"/> Imports	<input checked="" type="checkbox"/> BaseReloc.
Offset	Name	Func. Count	Bound?	OriginalFirstThunk	TimeDateStamp	Forwarder	NameRVA	FirstThunk
DD000	KERNEL32.DLL	4	FALSE	0	0	0	31103C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



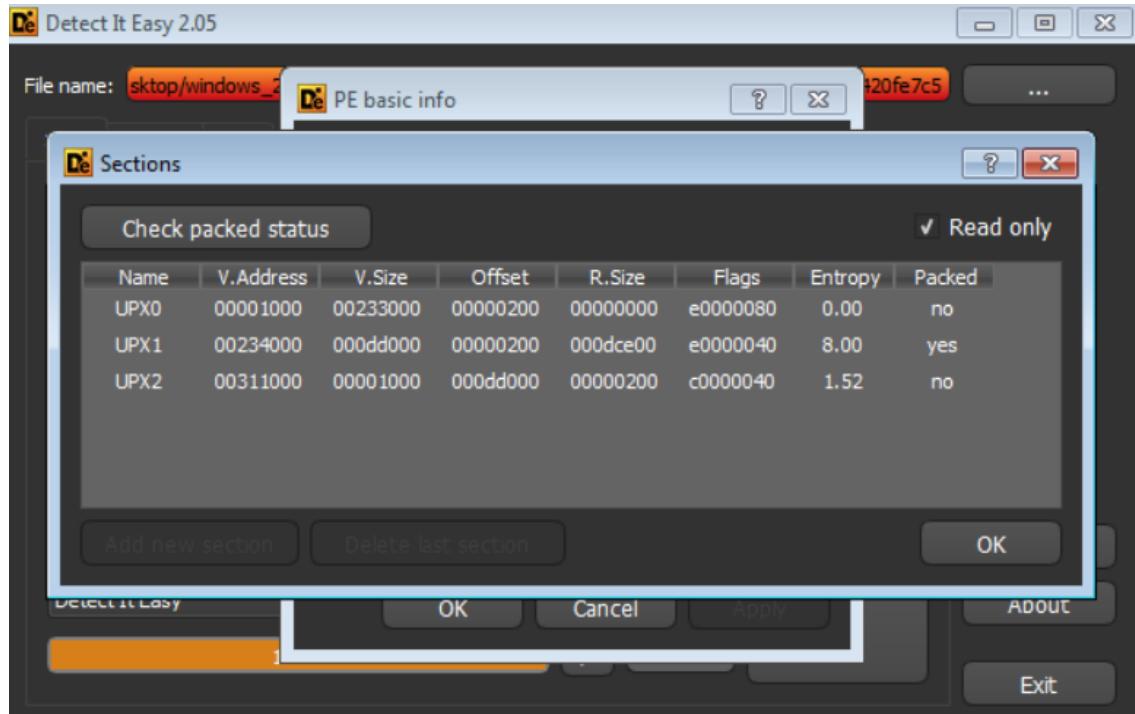
La herramienta Detect it easy es otra herramienta que disecciona el archivo sospechoso,



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

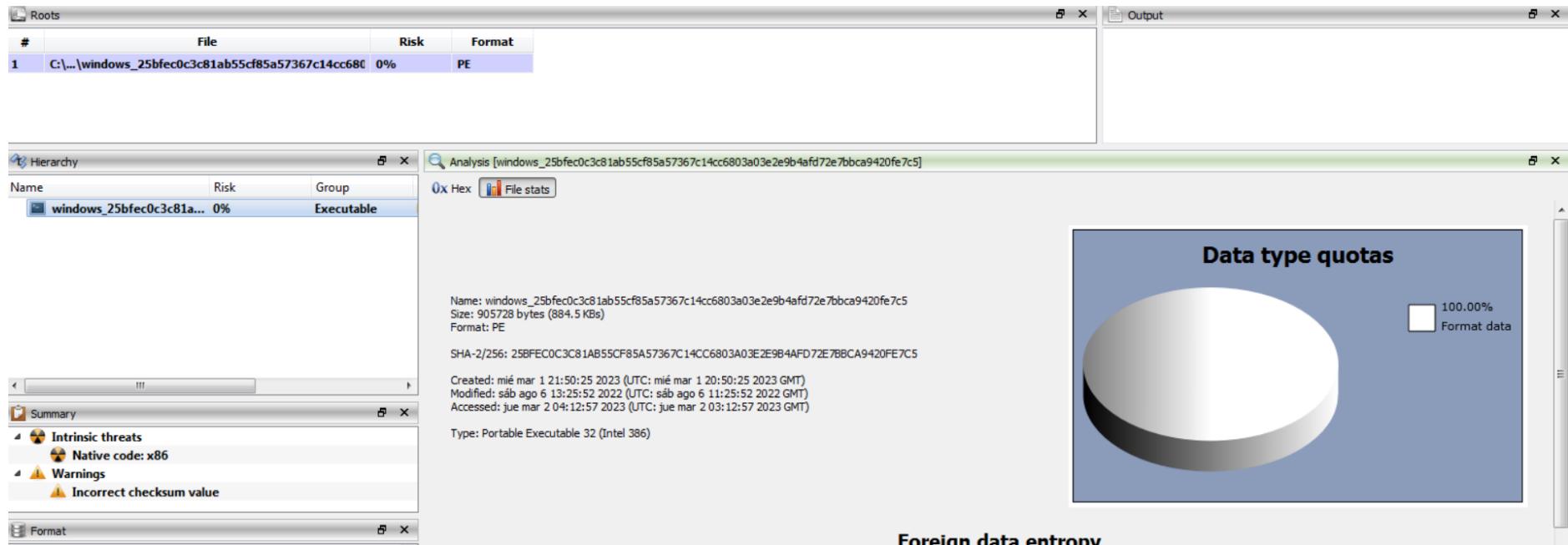


The screenshot shows the 'Detect It Easy 2.05' application window with the 'Signature' tab selected. The title bar shows the file path 'C:/Users/master/Desktop/windows\_25bfec0c381ab55cf85a57367c14cc6803a03e2e9b4af72e7bbca9420fe7c5'. The main interface includes a toolbar with 'New', 'Save', 'Debug', and 'Run' buttons, and a checkbox for 'Read only'. Below the toolbar is a list of file types: PE, 12Ghosts Zip2.1.sg, 32Lite.2.sg, 7z.1.sg, 7z.6.sg, \_BJFnt.2.sg, \_denuvoComplete.2.sg, \_NET Reactor.2.sg, \_NET Spider.2.sg, \_NET-3.sg, \_netshrink.2.sg, \_NETZ.2.sg, Aase Crypter.2.sg, Abbyy Lingvo.1.sg, ABC\_Cryptor.2.sg, ACCAStore.1.sg, ACE.6.sg, AcidCrypt.2.sg, ACProtect.2.sg, Acronis installer.1.sg, Active Delivery.1.sg, ActiveMark.2.sg, Actual Installer.1.sg, Adept Protector.2.sg, Adobe Flash Player installer.1.sg, Adobe FlashPlayer downloader.1.sg, Adobe installers.1.sg, ADS Self Extractor.1.sg, Advanced BAT to EXE converter.2.sg, Advanced installer.1.sg, Adveractive.1.sg. The 'ABC\_Cryptor.2.sg' entry is highlighted. To the right of the list is a code editor window displaying 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
```

At the bottom of the code editor are 'Clear' and 'Highlight' buttons.

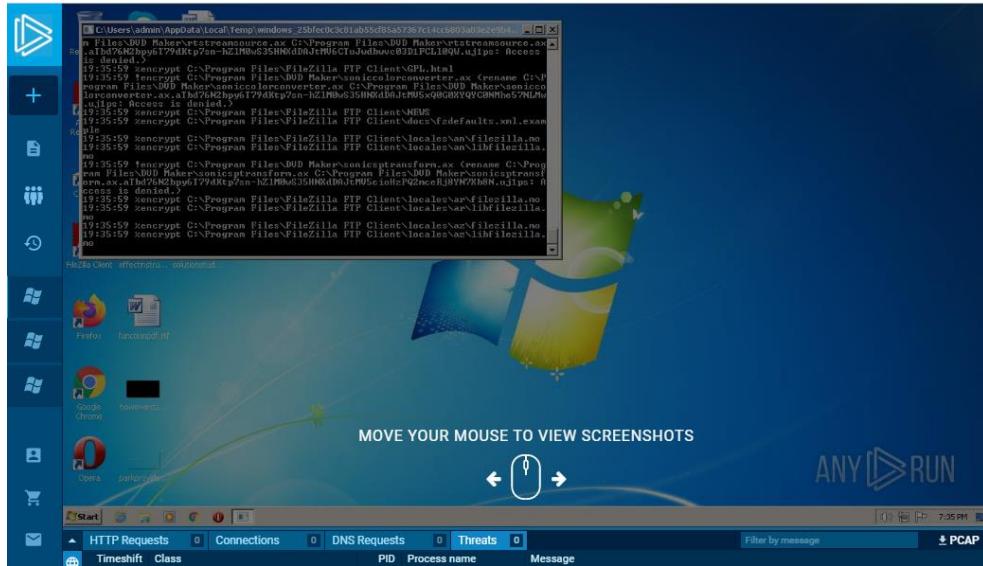
La última herramienta de análisis utilizada es **Cerbero** que si bien no arroja mucha información confirma todo lo ya visto anteriormente, como el SHA256 y menciona que el archivo es ejecutable.



## 5 ANALISIS DINAMICO

Antes de la realización del análisis dinamico se realiza una condensación de información general acerca del malware Ransomware.hive. Los datos expuestos en este apartado son resultado del análisis del malware con la herramienta de any.run.

La primera ilustración es una visión general de la maquina y los llamados a servicios como HTTP, DNS y conexiones, en el caso particular de este ransomware se visualiza que no hay llamados a los servicios mencionados ni conexiones.



En un primer acercamiento a datos generales de funcionamiento de este malware en la grafica siguiente se puede ver información como el nombre del ransomware hive para Windows, porque cabe destacar que este virus puede infectar no solamente maquinas Windows sino también linux y MAC os.

Se verifica el reporte de texto arrojado por la herramienta,

ANY RUN  
INTERACTIVE MALWARE ANALYSIS

General Behavior MalConf Static information Screenshots System events Network  Add for printing

### General Info

File name: windows\_25bfec0c3c81ab55cf85a57367c14cc6803a03e2e9b4af72e7bbca9420fe7c5  
Full analysis: <https://app.any.run/tasks/34a62f13-e5c6-4239-a186-b4144b20f5a1>  
Verdict: **Malicious activity**  
Analysis date: March 02, 2023, 20:35:04  
OS: Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)  
Indicators:   
MIME: application/x-dosexec  
File info: PE32 executable (console) Intel 80386 (stripped to external PDB), for MS Windows, UPX compressed  
MD5: DA13022097518D123A91A3958BE326DA  
SHA1: 24A71AB462594D5A159BBF176588AF951ABA1381  
SHA256: 25BFEC0C3C81AB55CF85A57367C14CC6803A03E2E9B4AFD72E7BBCA9420FE7C5  
SSDeep: 12288:Sv41dVzVThPCsM18GLHe7wlDdkPAQEtxr0ffvRmhEBWtdUJIAUP/T/kAfMvgVt:od1HDmIDdkZ4YXPpaTTXMw

ANY.RUN is an interactive service which provides full access to the guest system. Information in this report could be distorted by user actions and is provided for user acknowledgement as it is. ANY.RUN does not guarantee maliciousness or safety of the content.

La información de la ilustración anterior, denota que la actividad del archivo analizado es definitivamente malicioso, se parte desde esta afirmación para seguir realizando el análisis del malware, ahora que se sabe certamente que se trata de un archivo malicioso se procede a descifrar el funcionamiento y el impacto de este malware en la seguridad de la información y en los equipos.

Los demás datos ya fueron analizados en el apartado de análisis estático, se tratan los hashes del malware y que se trata de un archivo ejecutable.

Para referencia se dejan pantallazos de la información estática del malware.

#### TRID

```
.exe | Win32 Executable (generic) (52.9)
.exe | Generic Win/DOS Executable (23.5)
.exe | DOS Executable Generic (23.5)
```

#### EXIF

EXE	
MachineType:	Intel 386 or later, and compatibles
TimeStamp:	0000:00:00 00:00:00
ImageFileCharacteristics:	Executable, 32-bit, No debug
PEType:	PE32
LinkerVersion:	3
CodeSize:	905216
InitializedDataSize:	4096
UninitializedDataSize:	2306048
EntryPoint:	0x3100e0
OSVersion:	6.1
ImageVersion:	1
SubsystemVersion:	6.1
Subsystem:	Windows command line

#### Summary

Architecture:	IMAGE_FILE_MACHINE_I386
Subsystem:	IMAGE_SUBSYSTEM_WINDOWS_CUI
Compilation Date:	01-Jan-1970 00:00:00

#### DOS Header

Magic number:	MZ
Bytes on last page of file:	0x0090
Pages in file:	0x0003
Relocations:	0x0004
Size of header:	0x0000
Min extra paragraphs:	0x0000
Max extra paragraphs:	0xFFFF
Initial SS value:	0x0000
Initial SP value:	0x008B
Checksum:	0x0000
Initial IP value:	0x0000
Initial CS value:	0x0000
Overlay number:	0x0000
OEM identifier:	0x0000
OEM information:	0x0000
Address of NE header:	0x00000080

#### PE Headers

Signature:	PE
Machine:	IMAGE_FILE_MACHINE_I386
Number of sections:	3
Time date stamp:	01-Jan-1970 00:00:00
Pointer to Symbol Table:	0x002DCA00
Number of symbols:	0
Size of Optional Header:	0x00E0
Characteristics:	IMAGE_FILE_32BIT_MACHINE IMAGE_FILE_DEBUG_STRIPPED IMAGE_FILE_EXECUTABLE_IMAGE

## Sections

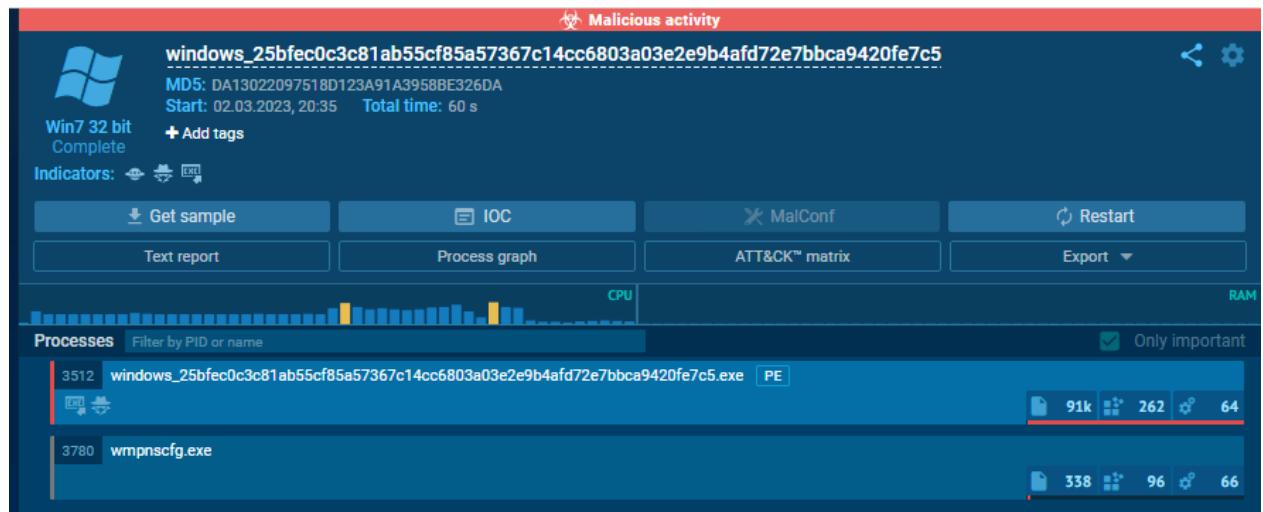
Name	Virtual Address	Virtual Size	Raw Size	Characteristics	Entropy
UPX0	0x00001000	0x00233000	0x00000000	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	0
UPX1	0x00234000	0x000DD000	0x000DCE00	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	7.99968
UPX2	0x00311000	0x00001000	0x00000200	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	1.51293

## Imports

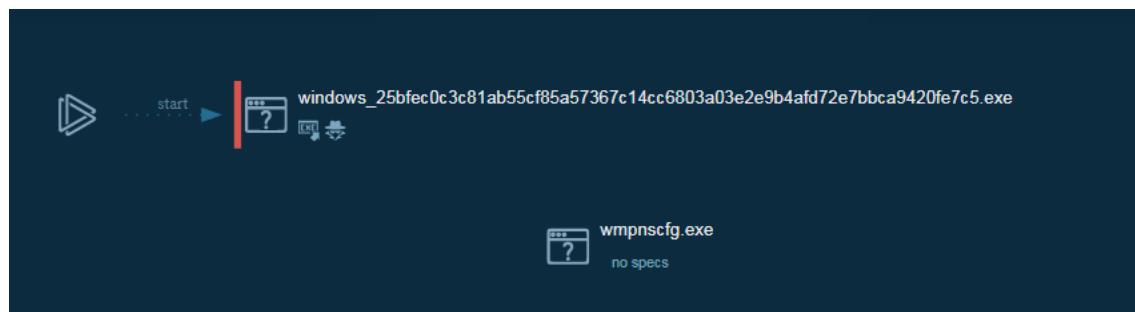
KERNEL32.DLL

Los datos detallados anteriormente corresponden a la disección y análisis del contenido del malware antes de ser ejecutado, es decir, de manera estática.

Para iniciar el análisis dinámico, en un primer momento, se analiza los datos de proceso del virus, esto es, como es que funciona el malware dentro del equipo y su comportamiento.



Como se puede notar, se detectan dos procesos monitorizados, el primero, la ejecución del archivo que se esta analizando ID 3512, y posterior a esto, la ejecución del archivo exe de ID 3780. Abajo el grafico de proceso del malware.



Se analiza cada proceso a detalle para comprender donde se aloja y que hace cada uno.

En el apartado anterior se comentó el flujo de infección del ransomware hive, este virus se propaga a través de ingeniería social como ser phishing, es decir, correos maliciosos, entre otros tipos de ataques.

Abajo el comportamiento de la actividad visto de una manera general, este se divide es actividad maliciosa, actividad sospechosa y actividad informativa, el comportamiento de cada proceso se analizara a detalle en paginas siguientes, por el momento la figura abajo muestra como se da la actividad de ejecución y propagación del malware.

El proceso se inicia con la actividad maliciosa de soltar el archivo malicioso en el equipo, seguida de la actividad sospechosa de ejecutar o sobreescribir el archivo, luego la actividad informativa configura la lectura del GUID desde el registro, la ejecución manual del ejecutable, la lectura del equipo, chequeo de la protección LSA, el lenguaje, creación de carpetas y archivos en el directorio del usuario y por ultimo soltar el archivo compilado en modo debug y a partir de allí se produce el robo de información y cifrado de archivos.

Behavior activities		
<input checked="" type="checkbox"/> Add for printing		
<b>MALICIOUS</b>	<b>SUSPICIOUS</b>	<b>INFO</b>
Drops the executable file immediately after the start • windows_25bfec0c3c81ab55cf85a57367c14cc6803a03e2e9b 4afd72e7bbca9420fe7c5.exe (PID: 3512)	Executable content was dropped or overwritten • windows_25bfec0c3c81ab55cf85a57367c14cc6803a03e2e9b 4afd72e7bbca9420fe7c5.exe (PID: 3512)	Reads the machine GUID from the registry • wmpnscfg.exe (PID: 3780)  Manual execution by a user • wmpnscfg.exe (PID: 3780)  Reads the computer name • windows_25bfec0c3c81ab55cf85a57367c14cc6803a03e2e9b 4afd72e7bbca9420fe7c5.exe (PID: 3512) • wmpnscfg.exe (PID: 3780)  The process checks LSA protection • wmpnscfg.exe (PID: 3780)  Checks supported languages • windows_25bfec0c3c81ab55cf85a57367c14cc6803a03e2e9b 4afd72e7bbca9420fe7c5.exe (PID: 3512) • wmpnscfg.exe (PID: 3780)  Creates files or folders in the user directory • windows_25bfec0c3c81ab55cf85a57367c14cc6803a03e2e9b 4afd72e7bbca9420fe7c5.exe (PID: 3512)  Drops a file that was compiled in debug mode • windows_25bfec0c3c81ab55cf85a57367c14cc6803a03e2e9b 4afd72e7bbca9420fe7c5.exe (PID: 3512)

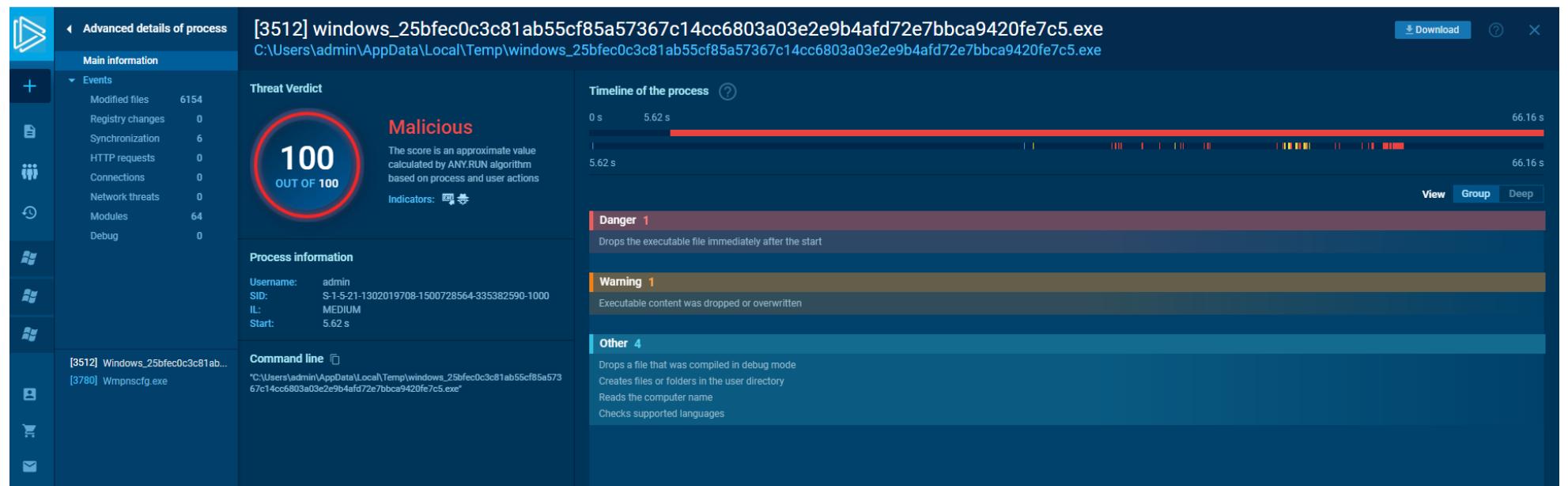
 Find more information about signature artifacts and mapping to MITRE ATT&CK™ MATRIX at the [full report](#) 

El primer archivo de proceso con el cual inicia todo el ataque es el de ID 3512, detectado como malicioso por la herramienta con un score de 100/100, es decir, es certamente malicioso el archivo, en la grafica de abajo se puede notar los eventos que crea este archivo, modifica 6154 archivos y 64 módulos (ver mas detalle en el apartado de ANEXOS).

El proceso ocurre en 66.16 segundos, desde soltar el archivo en la ruta C:/Users/AppData/Local/Temp/windows\_25bfec0c3c81ab55cf85a57367c14cc6803a03e2e9b4af72e7bbca9420fe7c5.exe

Esto es muy lógico ya que una ruta preferida para soltar archivos es la carpeta de archivos temporales, obviamente luego de chequear permisos.

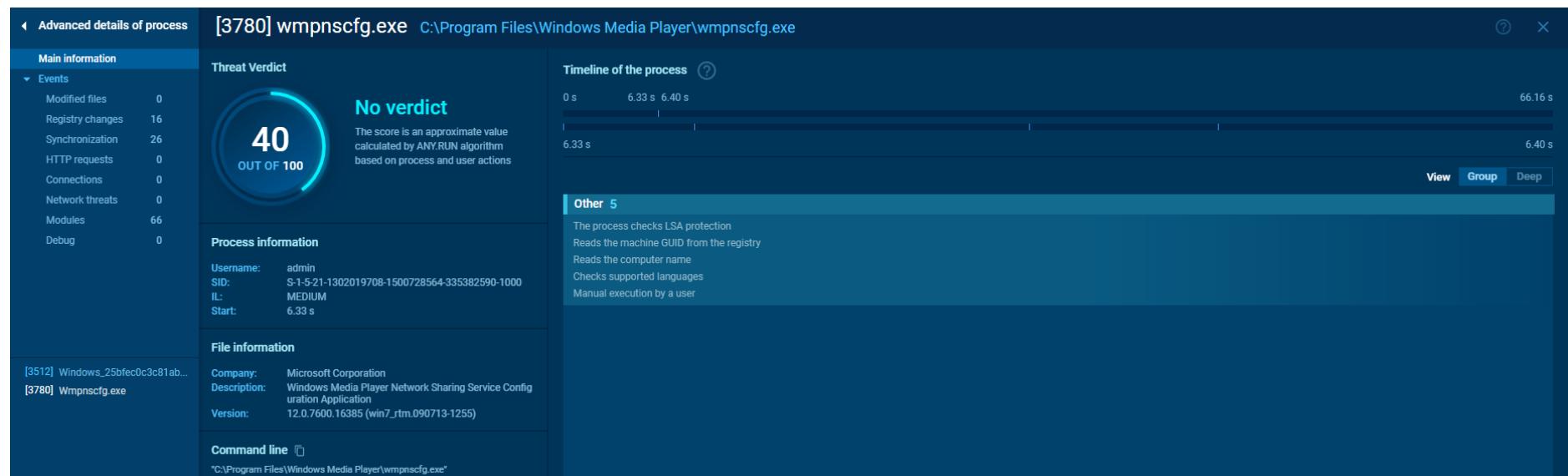
Como también se puede notar hay actividad peligrosa, como soltar el archivo ejecutable en una ruta, actividad sospechosa de sobrescribir el archivo, soltar el archivo compilado en una ruta, crear archivos y carpetas en el directorio de usuario, lectura del nombre de la computadora y chequear el lenguaje.



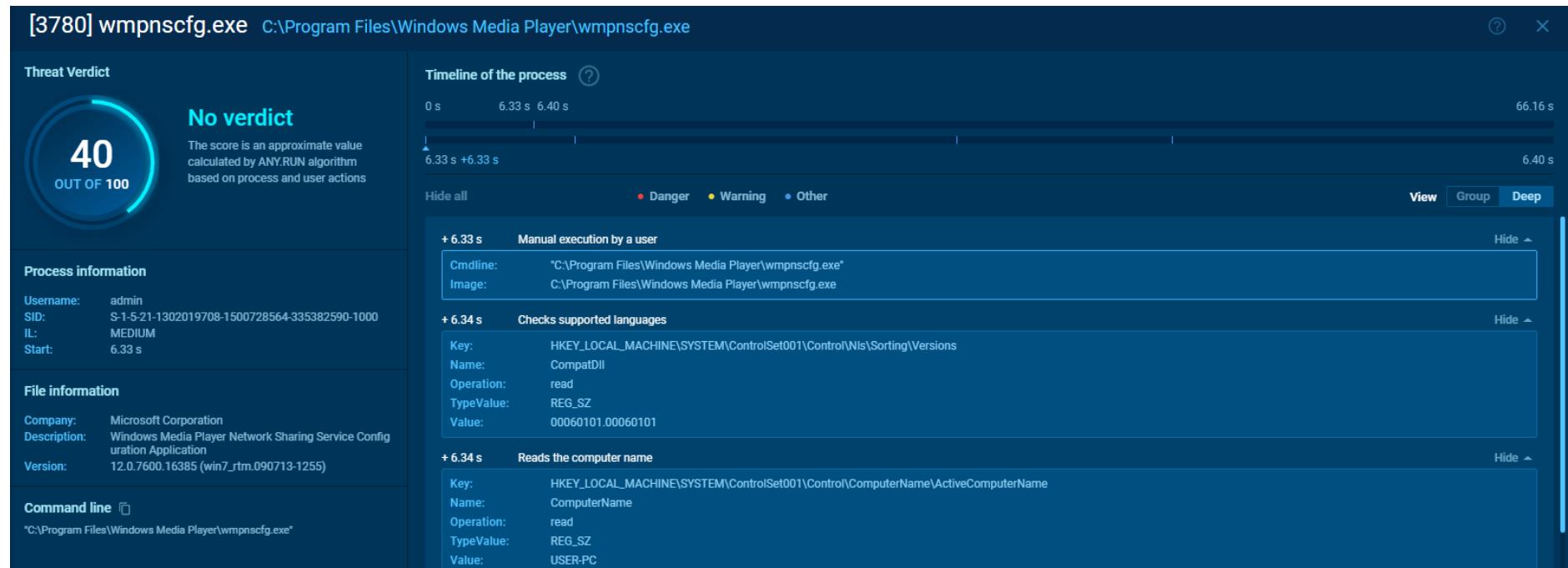
Para ver la información detallada de las actividades peligrosos, sospechosas e informáticas, como y en que ruta se llevan a cabo, debido a su extensión referirse al enlace siguiente:

<https://app.any.run/tasks/34a62f13-e5c6-4239-a186-b4144b20f5a1#>

En cuanto al siguiente proceso realizado con el archivo wmpnscfg.exe, no posee veredicto y su puntuación es de 40/100 relativamente bajo para ser un archivo malicioso, este fichero se aloja en la ruta C:\Program Files\Windows Media Player\wmpnscfg.exe y realiza cambios de registro, sincronización y modulos.



En la ilustración siguiente se puede ver las actividades con el timeline de cada uno, es decir, cuanto dura cada proceso, en primer lugar se ejecuta manualmente el archivo, se chequea el lenguaje, se lee el nombre de la computadora, desde el registro se lee el GUID,



Y por ultimo se verifica si la protección LSA se encuentra activada, la protección LSA denominada Autoridad de seguridad local en español, si esta activa evita la inyección de códigos que puede poner en peligro las credenciales de un equipo, si no esta activa se hace mas fácil para los atacantes realizar alteraciones de credenciales, en las graficas tanto anterior como siguiente se puede ver la llave, el nombre, la operación y los valores de las actividades que realiza este archivo.

**Threat Verdict**



**No verdict**  
The score is an approximate value calculated by ANY.RUN algorithm based on process and user actions

**Timeline of the process** ⓘ

0 s      6.33 s      6.40 s      66.16 s

6.33 s      +6.34 s      6.40 s

Hide all      • Danger      • Warning      • Other

Value: 00060101.00060101

+ 6.34 s      Reads the computer name      Hide ▲

Key: HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Control\ComputerName\ActiveComputerName  
Name: ComputerName  
Operation: read  
TypeValue: REG\_SZ  
Value: USER-PC

+ 6.37 s      Reads the machine GUID from the registry      Hide ▲

Key: HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Cryptography  
Name: MachineGuid  
Operation: read  
TypeValue: REG\_SZ  
Value: 90059c37-1320-41a4-b58d-2b75a9850d2f

+ 6.38 s      The process checks LSA protection      Hide ▲

Key: HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Control\Lsa\AccessProviders  
Name: MartaExtension  
Operation: read  
TypeValue: REG\_SZ  
Value: ntmlarta.dll

**Process information**

Username: admin  
SID: S-1-5-21-1302019708-1500728564-335382590-1000  
IL: MEDIUM  
Start: 6.33 s

**File information**

Company: Microsoft Corporation  
Description: Windows Media Player Network Sharing Service Configuration Application  
Version: 12.0.7600.16385 (win7\_rtm.090713-1255)

**Command line** ⓘ  
"C:\Program Files\Windows Media Player\wmpnscfg.exe"

Una vez analizados los dos procesos se muestran la cantidad total de procesos que se llevan a cabo, que son 38 de los cuales 2 son monitorizados, y uno se considera malicioso, que ya se vio anteriormente.

Processes			
Total processes	Monitored processes	Malicious processes	Suspicious processes
38	2	1	0

Otro dato interesante, es conocer la cantidad de eventos de registro que se producen en la maquina objetivo, todos ellos llevados a cabo por los dos archivos monitorizados con ID 3512 e ID 3780, del total de eventos 336 fueron de lectura, 16 de escritura y 6 eliminados.

Registry activity			
Total events	Read events	Write events	Delete events
358	336	16	6

Por otro lado, también se registran actividades de archivo, se hallan 76 archivos ejecutables, 2988 archivos sospechosos, 2908 archivos de texto y 162 archivos desconocidos, en cuanto a tipo y función.

Files activity			
Executable files	Suspicious files	Text files	Unknown types
76	2 988	2 908	162
Dropped files			

Para ver información detallada acerca de las actividades de registro y actividades de archivo debido a su extensión, referirse al siguiente enlace:

[https://any.run/report/25bfec0c3c81ab55cf85a57367c14cc6803a03e2e9b4af72e7bbca9420fe7c5/34a62f13-e5c6-4239-a186-b4144b20f5a1?gl=1\\*f186rw\\*ga\\*MTcyNTc1NjUwNy4xNjc3Nzg1NTk0\\*ga\\_53KB74YDZR\\*MTY3Nzc4NTU5NS4xLjEuMTY3Nzc4NjAzNi4xNi4wLjA.&ga=2.125915021.1689493847.1677785594-1725756507.1677785594](https://any.run/report/25bfec0c3c81ab55cf85a57367c14cc6803a03e2e9b4af72e7bbca9420fe7c5/34a62f13-e5c6-4239-a186-b4144b20f5a1?gl=1*f186rw*ga*MTcyNTc1NjUwNy4xNjc3Nzg1NTk0*ga_53KB74YDZR*MTY3Nzc4NTU5NS4xLjEuMTY3Nzc4NjAzNi4xNi4wLjA.&ga=2.125915021.1689493847.1677785594-1725756507.1677785594)

En el enlace proporcionado también se encuentran otros tipos de datos importantes tanto de análisis dinámico como estático.

Otro reporte importante generado son los Indicadores de compromiso, que es toda aquella información relevante que describe cualquier incidente de ciberseguridad, actividad y/o artefacto malicioso, mediante el análisis de sus patrones de comportamiento. En este caso se hallaron 41 indicadores de compromiso de los cuales 38 son archivos ejecutables.

Mediante la información que se visualiza abajo se muestran los datos de cada uno de los hashes y los archivos ejecutables y donde estos se encuentran alojados y de qué tipo de archivo se trata, estos 38 archivos son parte de los 38 procesos ejecutados.

windows\_25bfec0c3c81ab55cf85a57367c14cc6803a03e2e9b4af72e7bbca9420fe7c5

sha256 25bfec0c3c81ab55cf85a57367c14cc6803a03e2e9b4af72e7bbca9420fe7c5

sha1 24a71ab462594d5a159bbf176588af951aba1381

md5 da13022097518d123a91a3958be326da

Dropped executable file

La estructura es la siguiente, la ruta del ejecutable y su hash de tipo SHA256

sha256

C:\Program Files\Adobe\Acrobat Reader

DC\Reader\Locale\en\_US\stopwords.ENU.aTbd76N2bpy6T79dKtp7sn-hZIM0wS35HNXdDAJtMV6XNGzHuntZeg3EjjY67bUH.uj1ps

df0d131b17301c570aeb4d155e7c32a1bafde79118c7d58652b16ddb5d26a4db

sha256

C:\Users\admin\AppData\Local\VirtualStore\Program Files\Adobe\Acrobat Reader

DC\Reader\WebResources\Resource0\static\js\plugins\on-boarding\images\themeless\Localized\_images\tr-tr\PlayStore\_icon.svg

19a4a1bdec5b53d8d925988719c745e55a3f7962562de04c81d3eee168619dae

sha256

C:\Program Files\Adobe\Acrobat Reader

DC\Reader\plug\_ins\Accessibility.api.aTbd76N2bpy6T79dKtp7sn-hZIM0wS35HNXdDAJtMV4wWAoa1yYaGaS3RAEosPlz.uj1ps

6d400d992f5b09dac8edf493725a15beb1528876295aaeb855ff49a1d2cfbb4f

**sha256**

C:\Program Files\Adobe\Acrobat Reader  
DC\Reader\plug\_ins\AcroForm\PMP\AdobePDF417.pmp.aTbd76N2bpy6T79dKtp7sn-  
hZlM0wS35HNXdDAJtMV57seWjXrvdvrsSQh\_wAsk.uj1ps  
  
713157fe860ab0d02735eebcc41cd540089214ceca934a9ffd67c53ec9bed861

**sha256**

C:\Program Files\Adobe\Acrobat Reader  
DC\Reader\plug\_ins\AcroForm\PMP\DataMatrix.pmp.aTbd76N2bpy6T79dKtp7sn-  
hZlM0wS35HNXdDAJtMV4yzCRWle2tOM5s4kM1CWB\_.uj1ps  
  
f00662ffe9952a03ea6e0a99294a136e81c26950b518b7e57bf697e21e0debb2

**sha256**

C:\Program Files\Adobe\Acrobat Reader  
DC\Reader\plug\_ins\AcroForm\PMP\QRCode.pmp.aTbd76N2bpy6T79dKtp7sn-  
hZlM0wS35HNXdDAJtMV4U4Hljoq5bH2zKeLCh4iE7.uj1ps  
  
067b16594d1ae22262e9ea9d081c36f5cd8557b5b8f09979533bb7ae4985dd15

**sha256**

C:\Program Files\Adobe\Acrobat Reader  
DC\Reader\plug\_ins\AcroForm.api.aTbd76N2bpy6T79dKtp7sn-  
hZlM0wS35HNXdDAJtMV44\_HH-GZtyG6i0RFPah0Nx.uj1ps  
  
e821fc30201bd2a6d53410316ae9373e481066a9199e112e9cf66fbbaeef105

**sha256**

C:\Program Files\Adobe\Acrobat Reader  
DC\Reader\plug\_ins\Annots.api.aTbd76N2bpy6T79dKtp7sn-  
hZlM0wS35HNXdDAJtMV4jE-ry9z2LQWSlc1oEr31Q.uj1ps  
  
3087bd7404a53b3ff73e57daa0336a80a9aba240018253129e9f10983f2018eb

**sha256**

C:\Program Files\Adobe\Acrobat Reader  
DC\Reader\plug\_ins\Checkers.api.aTbd76N2bpy6T79dKtp7sn-  
hZIM0wS35HNXdDAJtMV5R-jDNvDhrW5fHHdQjvB4o.uj1ps  
  
44e0b386824e086e702fc74496c7f7545af34e370a3e5e41fa5e871f5105372d

**sha256**

C:\Program Files\Adobe\Acrobat Reader  
DC\Reader\plug\_ins\DigSig.api.aTbd76N2bpy6T79dKtp7sn-  
hZIM0wS35HNXdDAJtMV62LhVntVwmYiVoPMbqRe9J.uj1ps  
  
102c9d258898d0ec86177d590ad036025230ffb13b2690f0800fa135d5027c8e

**sha256**

C:\Program Files\Adobe\Acrobat Reader  
DC\Reader\plug\_ins\DV.API.aTbd76N2bpy6T79dKtp7sn-  
hZIM0wS35HNXdDAJtMV55UknN8cGoCEWb7fJbr8sh.uj1ps  
  
356276bcf224681dd44a839294732f71192fe2c265d872fa2e7ffdc7a000f782

**sha256**

C:\Program Files\Adobe\Acrobat Reader  
DC\Reader\plug\_ins\DropboxStorage.api.aTbd76N2bpy6T79dKtp7sn-  
hZIM0wS35HNXdDAJtMV4AkE-i0mFZZsJrdI9y4yxL.uj1ps  
  
79d4bd596eadb645b8a1f2b1a478f0c5cc46657869bbdf1c7cb2078e86005a06

**sha256**

C:\Program Files\Adobe\Acrobat Reader  
DC\Reader\plug\_ins\Multimedia\MPP\WindowsMedia.mpp.aTbd76N2bpy6T79dKtp7s  
n-hZIM0wS35HNXdDAJtMV6HZW7HGnDENxz5pdNgPVoU.uj1ps  
  
b0120f08b76ca24addb524960050dea2c20a46bafefd12bff48d2d40053135c8

**sha256**

C:\Program Files\Adobe\Acrobat Reader  
DC\Reader\plug\_ins\Multimedia\MPP\MCIMPP.mpp.aTbd76N2 bpy6T79dKtp7sn-  
hZIM0wS35HNXdDAJtMV4KqNObhsBEOfHxAwRqG4dp.uj1ps  
75e63d3faf2a43d59c73f83e2ea5b283ad1fd683dc085b41e8f77c8e47988ac0

**sha256**

C:\Program Files\Adobe\Acrobat Reader  
DC\Reader\plug\_ins\IA32.api.aTbd76N2 bpy6T79dKtp7sn-  
hZIM0wS35HNXdDAJtMV51yKn1N04cMkljOygU\_JZt.uj1ps  
f90080109ff74c573b5f7ae0ce43f5884df035139f8b6940fb296ba5649fd80f

**sha256**

C:\Program Files\Adobe\Acrobat Reader  
DC\Reader\plug\_ins\Multimedia\MPP\QuickTime.mpp.aTbd76N2 bpy6T79dKtp7sn-  
hZIM0wS35HNXdDAJtMV5QCSy5tYD2cZGhJjp9qYoH.uj1ps  
0418d1083f1b3f3475b7d6feb411172d58525801912703ebf9aab61e863d117

**sha256**

C:\Program Files\Adobe\Acrobat Reader  
DC\Reader\plug\_ins\PDDom.api.aTbd76N2 bpy6T79dKtp7sn-  
hZIM0wS35HNXdDAJtMV6pzkMiDTFqLJsOzBYj27py.uj1ps  
f48bfff6e62701667b8413a517aee5b1d5ba8439db417c3860d2a4fa8f0c1161

**sha256**

C:\Program Files\Adobe\Acrobat Reader  
DC\Reader\plug\_ins\Multimedia\MPP\Flash.mpp.aTbd76N2 bpy6T79dKtp7sn-  
hZIM0wS35HNXdDAJtMV5EAC0pD8NtMIuj9X9LA6wd.uj1ps  
a604ef1008bc75db748a6cb93dbf3ded65ea028065f45f953b84fb39a6bc3c1b

**sha256**

C:\Program Files\Adobe\Acrobat Reader  
DC\Reader\plug\_ins\Multimedia.api.aTbd76N2 bpy6T79dKtp7sn-  
hZIM0wS35HNXdDAJtMV7egHd8Z7SHI3h39VuMHwd7.uj1ps  
3d57616b1eb46ec7681386914252edf3dfdcf796cc8db65c4e74cc237cba28a4

**sha256**

C:\Program Files\Adobe\Acrobat Reader  
DC\Reader\plug\_ins\EScript.api.aTbd76N2 bpy6T79dKtp7sn-  
hZIM0wS35HNXdDAJtMV7THdniq71mdMcAgu6muvNv.uj1ps  
4a2626fdaf81411f79db63956e2886078fa9ae20c1865d902475a27a3a0ffc20

**sha256**

C:\Program Files\Adobe\Acrobat Reader  
DC\Reader\plug\_ins\MakeAccessible.api.aTbd76N2 bpy6T79dKtp7sn-  
hZIM0wS35HNXdDAJtMV4WMQHOQpcEaoB-BjVeChRW.uj1ps  
bf7054715a58385abd4ba73f0b809af8bd6ded950baedee0f2c577cbd3af79a7

**sha256**

C:\Program Files\Adobe\Acrobat Reader  
DC\Reader\plug\_ins\PPKLite.api.aTbd76N2 bpy6T79dKtp7sn-  
hZIM0wS35HNXdDAJtMV5KIAMwnxZolsN08CJ\_XCM1.uj1ps  
de557b37ab7ea6b2d0b2206aab38100d43fc7d7f9de4219739805112e9e173c1

**sha256**

C:\Program Files\Adobe\Acrobat Reader  
DC\Reader\plug\_ins\ReadOutLoud.api.aTbd76N2 bpy6T79dKtp7sn-  
hZIM0wS35HNXdDAJtMV73UkheKPuXKiuRuvioQR4.uj1ps  
cb9cd8986b9a88abb5c1cc31ebcd500af0bf0e5def62d91eb7af8ad004749b39

**sha256**

C:\Program Files\Adobe\Acrobat Reader  
DC\Reader\plug\_ins\SaveAsRTF.api.aTbd76N2bpy6T79dKtp7sn-  
hZIM0wS35HNXdDAJtMV6nSVEQfXUeB41J6eKUV8gk.uj1ps  
ebd5d7b7cde387e5774698bcbfe7d96f64a7242164c2264e0264ccb5e870c293

**sha256**

C:\Program Files\Adobe\Acrobat Reader  
DC\Reader\plug\_ins\Search.api.aTbd76N2bpy6T79dKtp7sn-  
hZIM0wS35HNXdDAJtMV5Otmjl20fpF5KWTSi0LgJ0.uj1ps  
e5021f9d3d48d22177bd81b0ffd7661036486d1f454ab7ff7aca5353d61e783a

**sha256**

C:\Program Files\Adobe\Acrobat Reader  
DC\Reader\plug\_ins\SendMail.api.aTbd76N2bpy6T79dKtp7sn-  
hZIM0wS35HNXdDAJtMV7uTfAxMNpLHMHLLwHch-9g.uj1ps  
0940241ada97863199842693570140d21d60a137f8afc5745c7a44bc2be85b34

**sha256**

C:\Program Files\Adobe\Acrobat Reader  
DC\Reader\plug\_ins\StorageConnectors.api.aTbd76N2bpy6T79dKtp7sn-  
hZIM0wS35HNXdDAJtMV5jRzIp\_O20NZGfFPBV3PlV.uj1ps  
fcf185e861acdbf0f6dd55a0fd5cdea0a58c9d18259a3b412dfd188a90f5c101

**sha256**

C:\Program Files\Adobe\Acrobat Reader  
DC\Reader\plug\_ins\reflow.api.aTbd76N2bpy6T79dKtp7sn-  
hZIM0wS35HNXdDAJtMV7cpqWn4ceoICi\_SJ-YpWdZ.uj1ps  
4c5d40e0d9e945626ab28e06b8ff9c277e7185afd090e20d98f3d31e65fd6e22

**sha256**

C:\Program Files\Adobe\Acrobat Reader  
DC\Reader\plug\_ins\Spelling.api.aTbd76N2bpy6T79dKtp7sn-  
hZIM0wS35HNXdDAJtMV7\_HUpwPXA5bEE51UOmrXIg.uj1ps  
41c2ac6f6577f43e1f19589a790d51211d9124074d7fd02d8b7f77df9111e5d6

**sha256**

C:\Program Files\Adobe\Acrobat Reader  
DC\Reader\plug\_ins\Updater.api.aTbd76N2bpy6T79dKtp7sn-  
hZIM0wS35HNXdDAJtMV7BtNoWuSODLr--CTBaUl9I.uj1ps  
1e6424977f6fe99fddb8eddc3a20e25f97bda6b9180819535833fa0d60b498e0

**sha256**

C:\Program Files\Adobe\Acrobat Reader  
DC\Reader\plug\_ins\eBook.api.aTbd76N2bpy6T79dKtp7sn-  
hZIM0wS35HNXdDAJtMV5q1tTAq-u\_WvbzbDBiCvtO.uj1ps  
b9e7a702f2c652fb84be00ede677485ca102633177ffc2c42173071ef45f9e48

**sha256**

C:\Program Files\Adobe\Acrobat Reader  
DC\Reader\plug\_ins3d\2d.x3d.aTbd76N2bpy6T79dKtp7sn-  
hZIM0wS35HNXdDAJtMV4A\_yWsBwbDUM9yNCiJQZBr.uj1ps  
d028d209dbbbd9c4bacc2c4ad0bc5ff6385108e63523c6d05fb7668b1262daf

**sha256**

C:\Program Files\Adobe\Acrobat Reader  
DC\Reader\plug\_ins\weblink.api.aTbd76N2bpy6T79dKtp7sn-  
hZIM0wS35HNXdDAJtMV4V2u7aX8u6ZFBjYarZw0l\_.uj1ps  
c57c29b471aa18c2cbdf78f207e1a2287814a51956621180394ac29087eb192e

**sha256**

C:\Program Files\Adobe\Acrobat Reader  
DC\Reader\plug\_ins3d\3difr.x3d.aTbd76N2bpy6T79dKtp7sn-  
hZIM0wS35HNXdDAJtMV7e5d411m3WPLzXQA5b9htL.uj1ps  
6335a5d53e544bd05314a586c229023b70f173ad56e130422f5767c61c219dd5

**sha256**

C:\Program Files\Adobe\Acrobat Reader  
DC\Reader\plug\_ins3d\drvDX9.x3d.aTbd76N2bpy6T79dKtp7sn-  
hZIM0wS35HNXdDAJtMV4Yye\_OgbSCSARWVIWDm-tR.uj1ps  
705250a41fc3e2e5f1a822d23279f3a4269e08d2199b2c0f8e75b94b695d644f

**sha256**

C:\Program Files\Adobe\Acrobat Reader  
DC\Reader\plug\_ins3d\drvSOFT.x3d.aTbd76N2bpy6T79dKtp7sn-  
hZIM0wS35HNXdDAJtMV6REkRW96dfTjgoBRF5EtNP.uj1ps  
66d72e7a8aaa37923e0b28ce10b1cdf2041652777acfbed7d54691130eb4a43b

**sha256**

C:\Program Files\Adobe\Acrobat Reader  
DC\Reader\plug\_ins3d\prcr.x3d.aTbd76N2bpy6T79dKtp7sn-  
hZIM0wS35HNXdDAJtMV4yr30jaVLqb-LME9cmZY1p.uj1ps  
a3193826a5d0d6d95762b0bd6806395e8904c5d1cb1cc47fd21bb1f7fa7018f9

**sha256**

C:\Program Files\Adobe\Acrobat Reader  
DC\Reader\plug\_ins3d\tesselate.x3d.aTbd76N2bpy6T79dKtp7sn-  
hZIM0wS35HNXdDAJtMV7n\_ujqdJsXLYBwwlhG1UEo.uj1ps  
ed553b4de044d203306afee0c43c7652604359d2959dbef806476d75f7857ca9

El ultimo reporte a analizar es la matriz de ataque MITRE, esta matriz esta diseccionada según los eventos que realiza el malware.



El primer evento es la ejecución que ya se ha visto antes , un usuario debe ejecutar el archivo malicioso de forma manual, esto no requiere permisos , los recursos de datos configuran Container: Container Creation, Network Traffic: Network Connection Creation, Container: Container Start, Instance: Instance Creation, Instance: Instance Start, Image: Image Creation, Process: Process Creation, Network Traffic: Network Traffic Content, Command: Command Execution, Application Log: Application Log Content, File: File Creation. Un adversario puede basarse en acciones específicas de un usuario para lograr la ejecución. Los usuarios pueden estar sujetos a ingeniería social para que ejecuten código malicioso, por ejemplo, abriendo un archivo o enlace de documento malicioso. Estas acciones del usuario generalmente se observarán como un comportamiento de seguimiento de las formas de phishing. Si bien la ejecución del usuario ocurre con frecuencia poco después del acceso inicial, puede ocurrir en otras fases de una intrusión, como cuando un adversario coloca un archivo en un directorio compartido o en el escritorio de un usuario con la esperanza de que haga clic en él. Esta actividad también se puede ver poco después de Internal Spearphishing.

Los adversarios también pueden engañar a los usuarios para que realicen acciones como habilitar el software de acceso remoto, permitir el control directo del sistema al adversario o descargar y ejecutar malware para la ejecución del usuario. Por ejemplo, las estafas de soporte técnico se pueden facilitar a través de phishing, vishing o varias formas de interacción con el usuario. Los adversarios pueden utilizar una combinación de estos métodos, como la suplantación de identidad y la promoción de números gratuitos o centros de llamadas que se utilizan para dirigir a las víctimas a sitios web maliciosos, para entregar y ejecutar cargas útiles que contienen malware o software de acceso remoto. (Cita: entrega de ataque telefónico)

**Techniques details**

Get to know what this threat is about

Image: Image Creation, Process: Process Creation, Network Traffic: Network Traffic Content, Command: Command Execution, Application Log: Application Log Content, File: File Creation

An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behavior from forms of [Phishing](#). While [User Execution](#) frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared

Malicious File ▾

- Manual execution by a user (1)  
3780 wmpnscfg.exe (1)

Image: C:\Program Files\Windows Media Player\wmpnscfg.exe  
Cmdline: "C:\Program Files\Windows Media Player\wmpnscfg.exe"

1 of 1

El segundo evento de este ransomware se encuentra en la columna Discovery, se denomina query registry o consultas al query, esto requiere permisos de usuario administración y sistema y los recursos de datos pueden ser Process: OS API Execution, Process: Process Creation, Command: Command Execution, Windows Registry: Windows Registry Key Access.

**Techniques details**

Get to know what this threat is about

**T1012**

**«Query Registry»**

Permissions required: User, Administrator, SYSTEM

Data sources: Process: OS API Execution, Process: Process Creation, Command: Command Execution, Windows Registry: Windows Registry Key Access

Adversaries may interact with the Windows Registry to gather information about the system, configuration, and installed software. The Registry contains a significant amount of information about the operating system, configuration, software, and security.(Citation: Wikipedia Windows Registry)

● Reads the computer name (2)  
3512 windows\_25bfec0c3c81ab55cf85a57367c14cc6803a03e2e9b4af72e  
7bbc9420fe7c5.exe (1)  
3780 wmpnscfg.exe (1)

● Checks supported languages (2)  
3512 windows\_25bfec0c3c81ab55cf85a57367c14cc6803a03e2e9b4af72e  
7bbc9420fe7c5.exe (1)  
3780 wmpnscfg.exe (1)

● Reads the machine GUID from the registry (1)

Operation: READ  
Name: COMPUTERNAME  
Value: USER-PC  
Key: HKEY\_LOCAL\_MACHINE\SYSTEM\CONTROLSET001\CONTROL\COMPUTERNAME\ACTIVECOMPUTERNAME  
TypeValue: REG\_SZ

1 of 1

Normalmente estas consultas se hacen ya que el registro contiene una cantidad significativa de información acerca de la máquina objetivo, operación, configuración, software y seguridad. La información se puede consultar fácilmente utilizando la utilidad Reg, aunque existen otros medios para acceder al Registro. Parte de la información puede ayudar a los adversarios a promover su operación dentro de una red. Los adversarios pueden usar la información de Query Registry durante el

descubrimiento automatizado para dar forma a comportamientos de seguimiento, incluso si el adversario infecta o no completamente al objetivo y/o intenta acciones específicas.

Las operaciones en este punto son de lectura y verificación, de información del equipo, el lenguaje de soporte y por supuesto la lectura de GUID de la maquina objetivo, abajo los detalles.

### Lectura del nombre de la computadora,

- Reads the computer name (2)  
3512 windows\_25bfec0c3c81ab55cf85a57367c14cc6803a03e2e9b4af72e  
7bbca9420fe7c5.exe (1)  
3780 wmpnscfg.exe (1)
  - Checks supported languages (2)  
3512 windows\_25bfec0c3c81ab55cf85a57367c14cc6803a03e2e9b4af72e  
7bbca9420fe7c5.exe (1)  
3780 wmpnscfg.exe (1)
  - Reads the machine GUID from the registry (1)
- Operation: READ  
Name: COMPUTERNAME  
Value: USER-PC  
Key: HKEY\_LOCAL\_MACHINE\SYSTEM\CONTROLSET001\CONTROL\COMPUTERNAME\ACTIVECOMPUTERNAME  
TypeValue: REG\_SZ

◀ 1 of 1 ▶

### Verificación del soporte del lenguaje

- Reads the computer name (2)  
3512 windows\_25bfec0c3c81ab55cf85a57367c14cc6803a03e2e9b4af72e  
7bbca9420fe7c5.exe (1)  
3780 wmpnscfg.exe (1)
  - Checks supported languages (2)  
3512 windows\_25bfec0c3c81ab55cf85a57367c14cc6803a03e2e9b4af72e  
7bbca9420fe7c5.exe (1)  
3780 wmpnscfg.exe (1)
  - Reads the machine GUID from the registry (1)
- Operation: READ  
Name: COMPATDLL  
Value: 00060101.00060101  
Key: HKEY\_LOCAL\_MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\SORTING\VERSIONS  
TypeValue: REG\_SZ

◀ 1 of 1 ▶

### Lectura de GUID de la maquina haciendo una consulta al registro.

The screenshot shows a Windows Event Log entry. The event details are as follows:

- Process:** 3512 windows\_25bfec0c3c81ab55cf85a57367c14cc6803a03e2e9b4af72e  
7bbc9420fe7c5.exe (1)
- Event ID:** 3780 wmpnscfg.exe (1)
- Action:** Checks supported languages (2)
- Action:** Reads the machine GUID from the registry (1)
- Value:** 3780 wmpnscfg.exe (1)

Below the event details, the registry key information is listed:

- Operation:** READ
- Name:** MACHINEGUID
- Value:** 90059C37-1320-41A4-B58D-2B75A9850D2F
- Key:** HKEY\_LOCAL\_MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY
- TypeValue:** REG\_SZ

At the bottom right of the screenshot, there is a navigation bar with arrows and the text "1 of 1".

El ultimo evento configura el descubrimiento de informacion del sistema, no requiere permisos y los recursos de datos son: Process: OS API Execution, Process: Process Creation, Command: Command Execution.

Se pueden utilizar herramientas como Systeminfo para recopilar información detallada del sistema. Si se ejecuta con acceso privilegiado, se puede recopilar un desglose de los datos del sistema a través de la herramienta de configuración systemsetup en macOS. Como ejemplo, los adversarios con acceso a nivel de usuario pueden ejecutar el comando df -aH para obtener los discos montados actualmente y el espacio libre disponible asociado. Los adversarios también pueden aprovechar una CLI de dispositivo de red en dispositivos de red para recopilar información detallada del sistema (por ejemplo, mostrar la versión). desarrollo y ocultación. (Cita: OSX.FairyTale) (Cita: 20 Herramientas y técnicas comunes de macOS)

Los proveedores de nube de infraestructura como servicio (IaaS) como AWS, GCP y Azure permiten el acceso a la información de instancias y máquinas virtuales a través de API. Las llamadas API autenticadas exitosas pueden devolver datos como la plataforma del sistema operativo y el estado de una instancia en particular o la vista del modelo de una máquina virtual. (Cita: Amazon Describe Instance) (Cita: Google Instances Resource) (Cita: Microsoft Virutal Machine API).

Este item realiza las mismas actividades detalladas en las 3 graficas anteriores.

En total la matriz de ataque configura 3 tacticas, 3 tecnicas y 11 eventos.

## 6 CONCLUSIONES Y RECOMENDACIONES

Teniendo en cuenta el análisis estático realizado al malware ransomware.hive y luego de realizar una exploración superficial y luego profunda del contenido del virus en este apartado, por sus características y funcionalidades se concluye que podría tratarse de un archivo malicioso y una amenaza para la seguridad de la información de las empresas. Esto teniendo en cuenta que luego de haber diseccionado el archivo que infecta maquinas Windows se constato que el fichero contenía algunas características propias de un malware, como la entropía de puntuación 8.00, los tipos de archivos UPX, y las librerías importadas, además de que algunos de sus contenidos, en total 4 son parte de la lista negra.

Luego de una exploración al contenido del archivo malware, se sometió a este a un análisis dinámico con la herramienta ANY.RUN, esta herramienta arrojo resultados tanto de análisis estático como dinámico, pero centrando la atención en el análisis dinámico desde un principio esta herramienta dio al archivo 100/100 de puntuación como archivo malicioso, se realizó un exhaustivo análisis de los procesos que sigue este ransomware al realizar una infección a una maquina objetivo, se encontraron 2 procesos monitorizados de 38 procesos. También se obtuvieron datos acerca del comportamiento del malware incluso según el timeline de cada proceso y cada evento que realizan los archivos maliciosos, se obtuvo una matriz de ataque, un esquema de comportamiento del malware, los indicadores de compromiso IOC, y muchos otros datos relevantes que denotan que definitivamente se trata de un archivo malicioso que actúa como ransomware como servicio (RaaS), uno de los actores de amenazas financiera mas activos de este periodo, que adopta un modelo de doble extorsion, utiliza la ingeniería social para tener acceso a las maquinas objetivo, las estudian cuidadosamente y una vez ejecutado el archivo se procede al secuestro de datos median el cifrado de archivos.

Se recomienda que las organizaciones prohíban o, al menos, monitoricen la ejecución de binarios no conocidos previamente dentro de sus máquinas o aquellos no provenientes de fuentes confiables. Aunque imperfecto, por la forma en la que se crea y distribuye el software legítimo, esta medida puede servir como una alarma inicial para impulsar una mayor investigación y, posiblemente, limitar su propagación. Con el objetivo de disminuir el tiempo de reacción frente a este tipo de amenazas se recomienda mantener vigilado el endpoint con soluciones de monitorización y de antivirus/EDR así como disponer de una política de actualizaciones que mantenga el endpoint con las últimas vulnerabilidades.

Si se dispone de los mecanismos para inspeccionar el tráfico que ocurre dentro de la red, se debería identificar la transferencia de binarios desconocidos dentro de ella. Por otro lado, es altamente recomendable mantener una segmentación adecuada de la red para evitar desplazamientos laterales y que finalmente se alcancen los sistemas críticos de la organización.

Para evitar en mayor medida los ataques de tipo ransomware es recomendable seguir una correcta política de copias de seguridad. Para ello es necesario realizar copias periódicas de los servicios (datos, software, licencias, configuraciones, etcétera) y almacenarlas en sistemas externos los cuales se puedan desconectar de la máquina y así evitar que se puedan cifrar.

Se debe monitorizar y deshabilitar las técnicas habituales utilizadas por los atacantes para eliminar las copias de seguridad internas del propio sistema operativo o que quieran para la generación de copias de seguridad. Se debe mantener un control de las

cuentas de usuario siguiente una política de privilegios mínimos, de esta forma se pueda evitar que un usuario cualquiera pueda modificar ficheros del sistema, parar procesos o incluso servicios.

Se deben aplicar políticas de seguridad que prohíban la enumeración de recursos y servicios compartidos en red. De esta forma se puede evitar que pueda infectar toda la red desde un mismo equipo.

Se deben enviar todos los eventos del sistema, o al menos los más importantes, a un sistema externo que reúna todos los eventos de todos los equipos de la red. De esta forma se puede evitar la pérdida de trazabilidad. Además, esta mitigación podría ayudar a crear alertas tempranas que avisen de una posible intrusión en el sistema y de esta forma evitar el ataque. Se debe mantener una política de actualizaciones.

Es de suma importancia que todos los sistemas se encuentren totalmente actualizados para evitar posibles vulnerabilidades de seguridad que los atacantes puedan explotar para hacerse con el control de una máquina, obtener credenciales o realizar una escalada de privilegios.

Se debe eliminar cualquier contraseña por defecto establecida en cualquier sistema o aplicación, además de generar una política de contraseñas que obligue al uso de contraseñas seguras y que cambien de forma periódica. Aplicar sistemas de autenticación en dos pasos en todos aquellos sistemas que lo permitan.

Se debe mantener al equipo de seguridad actualizado de todas las nuevas vulnerabilidades conocidas, que tengan conocimiento de todos los sistemas utilizados en el parque tecnológico y que decidan si es necesario aplicar medidas de mitigación adicionales antes situaciones específicas.

En caso de incidente con este malware, se debe de reportar a las autoridades pertinentes lo más rápido posible

## 7 BIBLIOGRAFIA

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

<https://malpedia.caad.fkie.fraunhofer.de/details/win.hive>

<https://yoroi.company/research/on-the-footsteps-of-hive-ransomware/>

<https://www.microsoft.com/en-us/security/blog/2022/07/05/hive-ransomware-gets-upgrades-in-rust/>

<https://www.connectwise.com/resources/hive-profile>

<https://app.any.run/tasks/34a62f13-e5c6-4239-a186-b4144b20f5a1/>

[https://any.run/report/25bfec0c3c81ab55cf85a57367c14cc6803a03e2e9b4afd72e7bbca9420fe7c5/34a62f13-e5c6-4239-a186-b4144b20f5a1?gl=1\\*x8d5q6\\*ga\\*MTcyNTc1NjUwNy4xNjc3Nzg1NTk0\\*ga\\_53KB74YDZR\\*MTY3NzgxMTU1My40LjEuMTY3NzgxMTU3OS4zNC4wLjA.&ga=2.140133427.1689493847.1677785594-1725756507.1677785594](https://any.run/report/25bfec0c3c81ab55cf85a57367c14cc6803a03e2e9b4afd72e7bbca9420fe7c5/34a62f13-e5c6-4239-a186-b4144b20f5a1?gl=1*x8d5q6*ga*MTcyNTc1NjUwNy4xNjc3Nzg1NTk0*ga_53KB74YDZR*MTY3NzgxMTU1My40LjEuMTY3NzgxMTU3OS4zNC4wLjA.&ga=2.140133427.1689493847.1677785594-1725756507.1677785594)

<https://www.virustotal.com/gui/file/25bfec0c3c81ab55cf85a57367c14cc6803a03e2e9b4afd72e7bbca9420fe7c5>

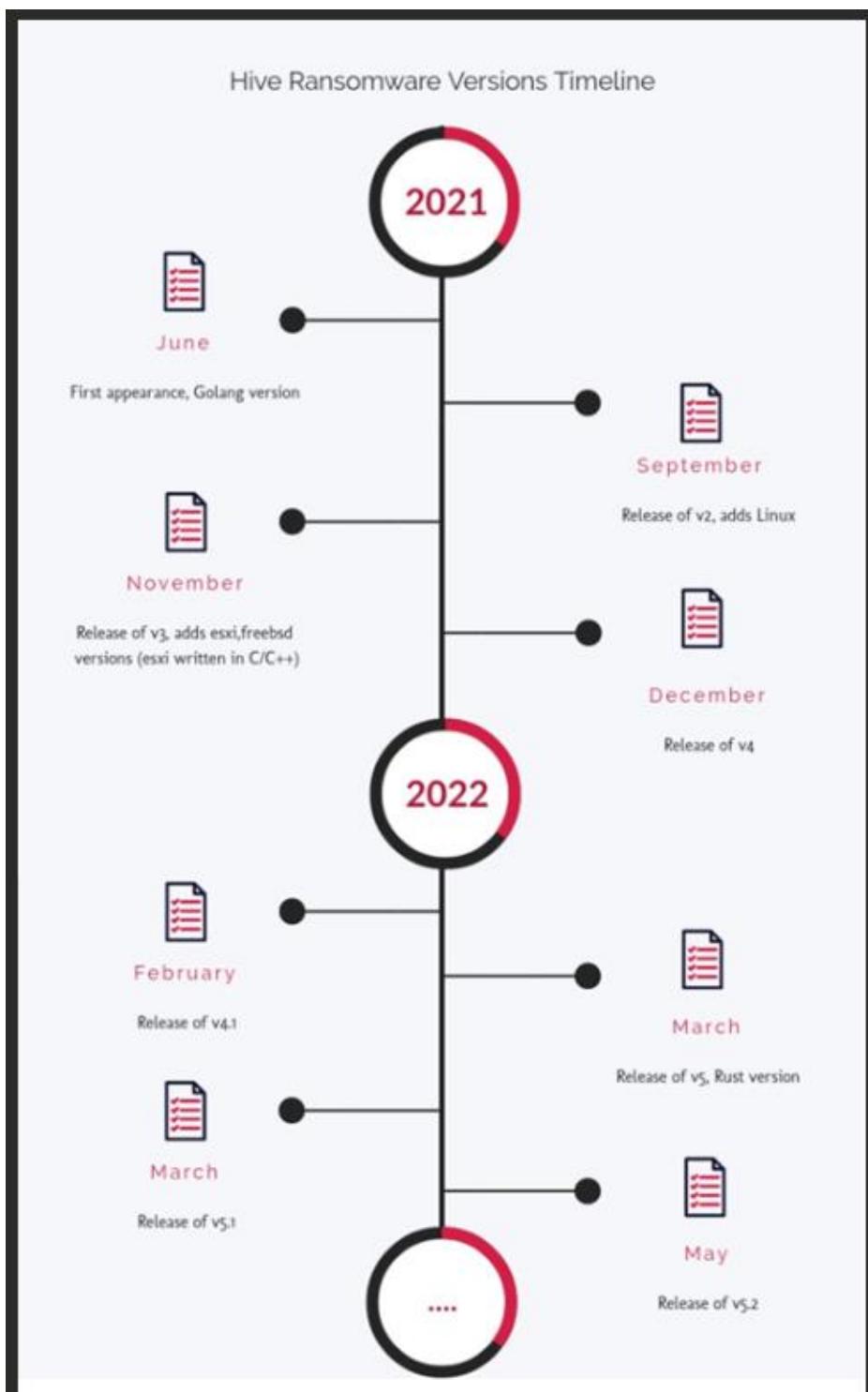
## 8 ANEXOS

Modelo de negocio Doble-extorsión, ransomware as a service

Hive (TH-313)		
Targets	Companies	
Objectives	Double extortion	
Payload Delivery	Initial access through vulnerabilities/VPN credentials/Malicious attachments	
TTPs	T1078 Valid Accounts T1003 OS Credential Dumping T1486 Data Encrypted for Impact T1567 Exfiltration over web service T1068 Exploitation for Privilege Escalation T1135 Network Share Discovery	T1140 Deobfuscate/Decode Files T1021 Remote Services T1071.001 Web Protocols T1022 Data Encrypted T1021.001 Remote Desktop Protocol T1083 File and directory discovery

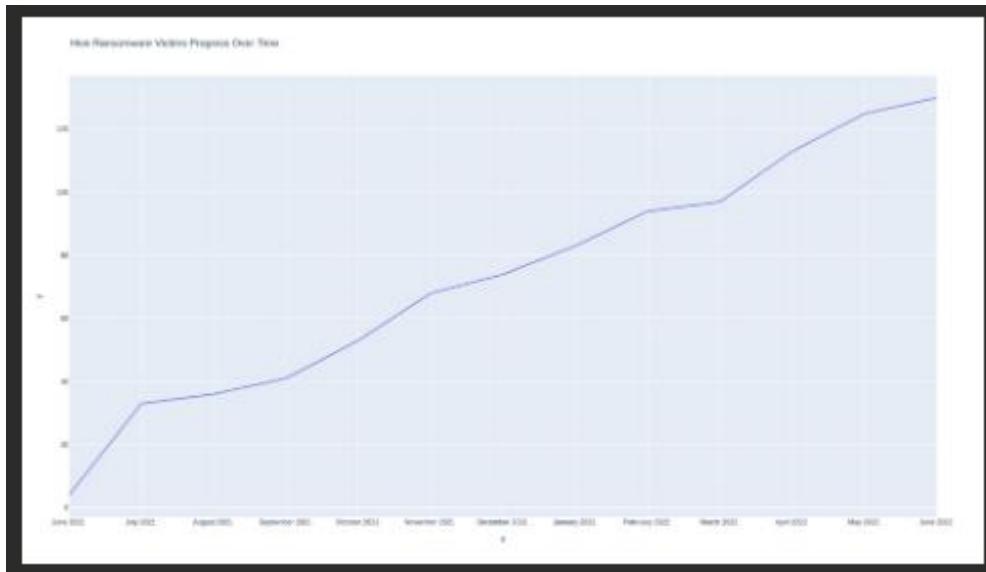
Figura 1: la Colmena

## Cronología de las versiones del ransomware Hive.



**Figura 2: Cronología de la colmena.**

Progreso de numero de victimas del Ransomware hive desde junio 2021.



**Figura 3: Cronología de ataques del ransomware hive.**

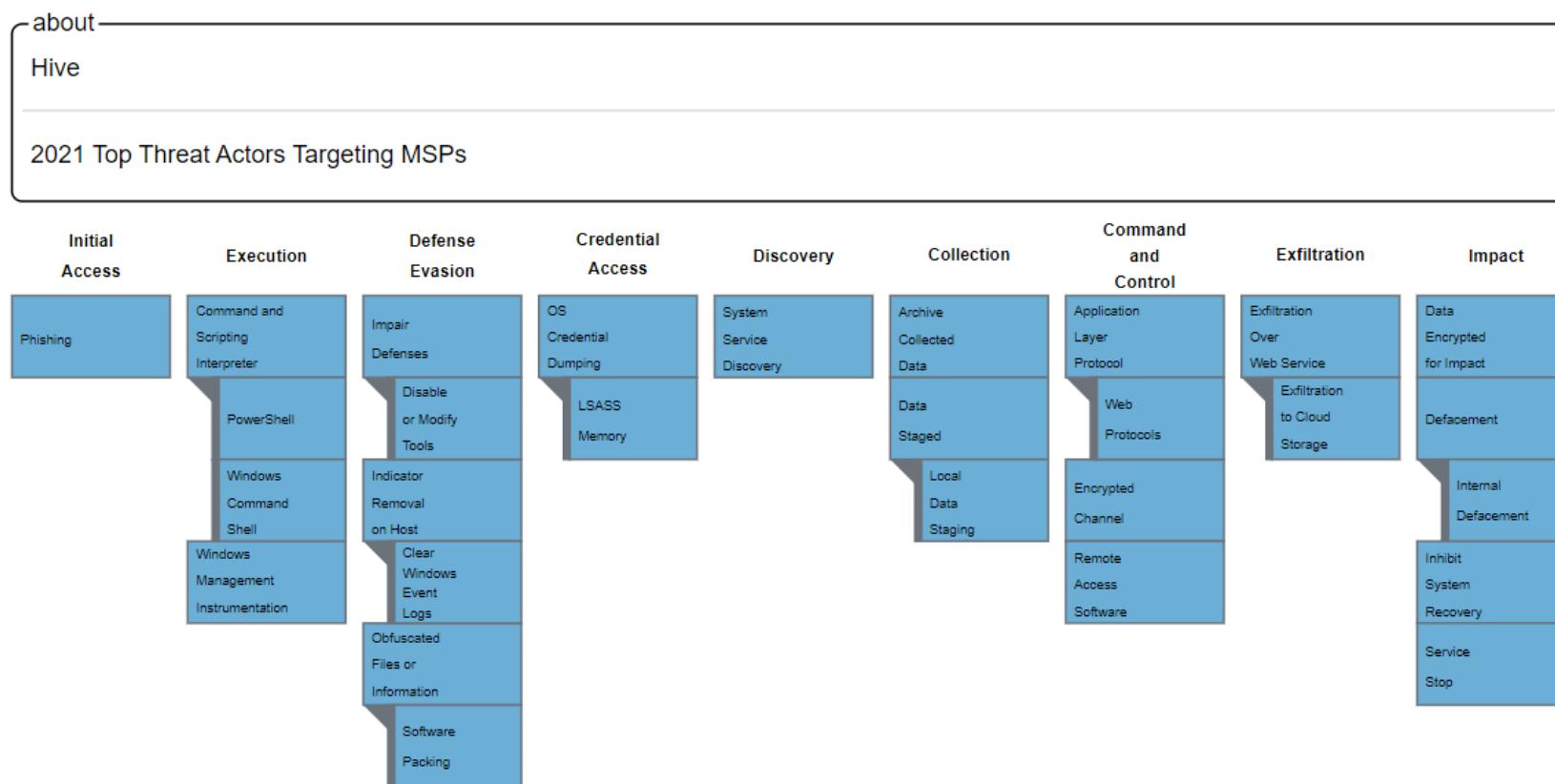
Al igual que la mayoría de los ransomware modernos, Hive introduce parámetros de línea de comandos, que permiten a los atacantes flexibilidad al ejecutar la carga útil agregando o eliminando funciones. Por ejemplo, un atacante puede elegir cifrar archivos en recursos compartidos remotos o solo archivos locales o seleccionar el tamaño mínimo de archivo para el cifrado. En la nueva variante de Hive, encontramos los siguientes parámetros en diferentes muestras:

Parámetro	Funcionalidad
-no-local	No cifra archivos locales
-sin montar	No cifra archivos en recursos compartidos de red montados
-no-descubrimiento	No descubrir recursos compartidos de red
-solo locales	Cifra solo archivos locales
-solo red	Cifra solo archivos en recursos compartidos de red
-solo explícito	Cifra carpetas específicas. Por ejemplo, ' <i>-explicit-only c:\mydocs c:\myphotos</i> '
-min-tamaño	Tamaño mínimo de archivo, en bytes, para cifrar. Por ejemplo, ' <i>-min-size 102400</i> ' cifrará archivos con un tamaño igual o superior a 100 kb
-da	[Se está analizando el uso.]
-F	[Se está analizando el uso.]
-fuerza	[Se está analizando el uso.]
-wmi	[Se está analizando el uso.]

**Figura 4: Parámetros de línea de comandos**

Se ha analizado la matriz de ataque mitre arrojado por la herramienta ANY.RUN, no obstante, se ha hallado otra matriz de ataque que podría ser más completa y se incluye para referencia. **Figura 5: Matriz de ataque Mitre.**

# Mapeo MITRE ATT&CK®



## HIVE Y MITIGACIONES POSIBLES SEGÚN TECNICAS DE ATAQUE.

**Figura 6: Mitigaciones según técnicas de ataque del ramsonware hive.**

Táctica ATT&CK	Técnica ATT&CK	Mitigaciones
Acceso inicial	<p><b>T1566 - Suplantación de identidad:</b> Los adversarios pueden enviar mensajes de phishing para obtener acceso a los sistemas de las víctimas. Todas las formas de phishing son ingeniería social entregada electrónicamente.</p>	<p><b>M1049 - Antivirus/Antimalware:</b> el antivirus puede poner en cuarentena automáticamente los archivos sospechosos.</p> <p><b>M1031 - Prevención de intrusiones en la red:</b> Los sistemas de prevención de intrusiones en la red y los sistemas diseñados para escanear y eliminar archivos adjuntos o enlaces de correo electrónico maliciosos se pueden usar para bloquear la actividad.</p> <p><b>M1021 - Restringir contenido basado en la web:</b> Determine si ciertos sitios web o tipos de archivos adjuntos (p. ej., .scr, .exe, .pif, .cpl, etc.) que se pueden usar para el phishing son necesarios para las operaciones comerciales y considere bloquear el acceso si la actividad no se puede monitorear bien o si plantea un riesgo significativo.</p> <p><b>M1054 - Configuración del software:</b> Utilice mecanismos de autenticación de correo electrónico y contra la suplantación de identidad para filtrar los mensajes en función de las comprobaciones de validez del dominio del remitente (mediante SPF) y la integridad de los mensajes (mediante DKIM). Habilitar estos mecanismos dentro de una organización (a través de políticas como DMARC) puede permitir que los destinatarios (dentro de la organización y entre dominios) realicen un filtrado y validación de mensajes similares.[3][4]</p> <p><b>M1017 - Capacitación de usuarios:</b> Los usuarios pueden recibir capacitación para identificar técnicas de ingeniería social y correos electrónicos de phishing.</p>

		<p><b>M1049 - Antivirus/antimalware:</b> El antivirus se puede utilizar para poner en cuarentena automáticamente los archivos sospechosos.</p> <p><b>M1045 - Firma de código:</b> Establezca la política de ejecución de PowerShell para ejecutar solo scripts firmados.</p> <p><b>M1042 - Desactivar o eliminar función o programa:</b> es posible eliminar PowerShell de los sistemas cuando no se necesita, pero se debe realizar una revisión para evaluar el impacto en un entorno, ya que podría estar en uso para muchos fines legítimos y funciones administrativas.</p> <p><b>Deshabilite o restrinja el servicio WinRM para ayudar a evitar el uso de PowerShell para la ejecución remota.</b></p> <p><b>M1038 - Prevención de ejecución:</b> utilice el control de aplicaciones cuando corresponda.</p> <p><b>M1026 - Administración de cuentas con privilegios:</b> cuando sea necesario PowerShell, restrinja la política de ejecución de PowerShell a los administradores. Tenga en cuenta que existen métodos para omitir la política de ejecución de PowerShell, según la configuración del entorno.</p>
Ejecución	<p><b>T1059.001 - Intérprete de comandos y secuencias de comandos – PowerShell:</b> los adversarios pueden abusar de los comandos y secuencias de comandos de PowerShell para su ejecución. PowerShell es una potente interfaz de línea de comandos interactiva y un entorno de secuencias de comandos incluido en el sistema operativo Windows.</p> <p><b>T1059.003 - Consola de comandos de Windows:</b> Los adversarios pueden abusar del shell de comandos de Windows para su ejecución. El shell de comandos de Windows (cmd) es el símbolo del sistema principal en los sistemas Windows.</p>	<p><b>M1038 - Prevención de ejecución:</b> Utilice el control de aplicaciones cuando corresponda.</p>

	<p><b>T1047 - Instrumentación de gestión de Windows:</b> Los adversarios pueden abusar del Instrumental de administración de Windows (WMI) para ejecutar cargas y comandos maliciosos. WMI es una función de administración que proporciona un entorno uniforme para acceder a los componentes del sistema de Windows.</p>	<p><b>M1040 - Prevención de comportamiento en el punto final:</b> en Windows 10, habilite las reglas de reducción de superficie de ataque (ASR) para bloquear la ejecución de procesos creados por comandos WMI. Nota: muchas herramientas y aplicaciones legítimas utilizan WMI para la ejecución de comandos.</p> <p><b>M1038 - Prevención de ejecución:</b> Use el control de aplicaciones configurado para bloquear la ejecución de wmic.exe si no es necesario para un sistema o red determinado para evitar un posible uso indebido por parte de los adversarios. Por ejemplo, en Windows 10 y Windows Server 2016 y versiones posteriores, se pueden aplicar reglas de política de control de aplicaciones de Windows Defender (WDAC) para bloquear la aplicación wmic.exe y evitar abusos.</p> <p><b>M1026 - Gestión de cuenta privilegiada:</b> Evite la superposición de credenciales entre sistemas de administrador y cuentas privilegiadas.</p> <p><b>M1018 - Gestión de cuentas de usuario:</b> De forma predeterminada, solo los administradores pueden conectarse de forma remota mediante WMI. Restrinja a otros usuarios que pueden conectarse o no permita que todos los usuarios se conecten de forma remota a WMI.</p>
--	--	---

	<p><b>T1070.001</b> – Eliminación del indicador en el host: Borrar registros de eventos de Windows:</p> <p>Los adversarios pueden borrar los registros de eventos de Windows para ocultar la actividad de una intrusión. Los registros de eventos de Windows son un registro de las alertas y notificaciones de una computadora. Hay tres orígenes de eventos definidos por el sistema: Sistema, Aplicación y Seguridad, con cinco tipos de eventos: Error, Advertencia, Información, Auditoría de éxito y Auditoría de falla.</p>	<p><b>M1041</b> - Cifrar información confidencial:</p> <p>Ofusque/cifre los archivos de eventos localmente y en tránsito para evitar dar retroalimentación a un adversario.</p> <p><b>M1029</b> - Almacenamiento de datos remoto:</p> <p>Reenvíe eventos automáticamente a un servidor de registro o depósito de datos para evitar condiciones en las que el adversario pueda ubicar y manipular datos en el sistema local. Cuando sea posible, minimice el tiempo de demora en el informe de eventos para evitar un almacenamiento prolongado en el sistema local.</p> <p><b>M1022</b> - Restringir permisos de archivos y directorios:</p> <p>Proteja los archivos de eventos generados que se almacenan localmente con los permisos y la autenticación adecuados y limite las oportunidades para que los adversarios aumenten los privilegios al evitar oportunidades de escalamiento de privilegios.</p>
Evasión de defensa	<p><b>T1027.002</b> – Información o archivos ofuscados: Paquete de software:</p> <p>Los adversarios pueden realizar paquetes de software o protección de software de máquinas virtuales para ocultar su código. El paquete de software es un método para comprimir o cifrar un ejecutable. Empaquetar un ejecutable cambia la firma del archivo en un intento de evitar la detección basada en firmas. La mayoría de las técnicas de descompresión descomprimen el código ejecutable en la memoria.</p>	<p><b>M1049</b> - Antivirus/antimalware:</p> <p>Emplee la detección de malware basada en heurística. Garantice definiciones de virus actualizadas y cree firmas personalizadas para el malware observado.</p>

	<p><b>T1562.001</b> – Deterioro de defensas: deshabilitar o modificar herramientas:</p> <p>Los adversarios pueden modificar y/o deshabilitar las herramientas de seguridad para evitar la posible detección de su malware/herramientas y actividades. Esto puede tomar muchas formas, como eliminar procesos o servicios de software de seguridad, modificar/eliminar claves de registro o archivos de configuración para que las herramientas no funcionen correctamente, u otros métodos para interferir con las herramientas de seguridad que escanean o informan información.</p>	<p><b>M1022</b> - Restringir permisos de archivos y directorios:</p> <p>Asegúrese de que existan los permisos de archivos y procesos adecuados para evitar que los adversarios deshabiliten o interfieran con los servicios de seguridad.</p> <p><b>M1024</b> - Restringir permisos de registro:</p> <p>Asegúrese de contar con los permisos de registro adecuados para evitar que los adversarios deshabiliten o interfieran con los servicios de seguridad.</p> <p><b>M1018</b> - Gestión de cuentas de usuario:</p> <p>Asegúrese de contar con los permisos de usuario adecuados para evitar que los adversarios deshabiliten o interfieran con los servicios de seguridad.</p>
--	---	--

		<p><a href="#">M1040</a> - Prevención del comportamiento en el punto final:</p> <p>En Windows 10, habilite las reglas de reducción de superficie de ataque (ASR) para proteger LSASS y evitar el robo de credenciales.</p> <p><a href="#">M1043</a> - Protección de acceso de credenciales:</p> <p>Con Windows 10, Microsoft implementó nuevas protecciones llamadas Credential Guard para proteger los secretos de LSA que se pueden usar para obtener credenciales a través de formas de volcado de credenciales. No está configurado de forma predeterminada y tiene requisitos de sistema de hardware y firmware. Tampoco protege contra todas las formas de dumping de credenciales.</p> <p><a href="#">M1028</a> - Configuración del sistema operativo:</p> <p>Considere deshabilitar o restringir NTLM. Considere deshabilitar la autenticación WDigest.</p> <p><a href="#">M1027</a> - Políticas de contraseña:</p> <p>Asegúrese de que las cuentas de administrador local tengan contraseñas únicas y complejas en todos los sistemas de la red.</p> <p><a href="#">M1026</a> - Gestión de cuenta privilegiada:</p> <p>No coloque cuentas de dominio de usuario o administrador en los grupos de administradores locales en todos los sistemas a menos que estén estrictamente controlados, ya que esto suele ser equivalente a tener una cuenta de administrador local con la misma contraseña en todos los sistemas. Siga las mejores prácticas para el diseño y la administración de una red empresarial para limitar el uso de cuentas con privilegios en todos los niveles administrativos.</p> <p><a href="#">M1025</a> - Integridad del proceso privilegiado:</p> <p>En Windows 8.1 y Windows Server 2012 R2, habilite Protected Process Light para LSA.</p> <p><a href="#">M1017</a> - Capacitación de usuarios:</p> <p>Límite la superposición de credenciales entre cuentas y sistemas capacitando a los usuarios y administradores para que no usen la misma contraseña para varias cuentas.</p>
Acceso a Credenciales	<p><a href="#">T1003.001</a> : volcado de credenciales del sistema operativo: memoria LSASS:</p> <p>Los adversarios pueden intentar acceder al material de credenciales almacenado en la memoria de proceso del Servicio del Subsistema de la Autoridad de Seguridad Local (LSASS). Después de que un usuario inicia sesión, el sistema genera y almacena una variedad de materiales de credenciales en la memoria del proceso LSASS. Estos materiales de credenciales pueden ser recopilados por un usuario administrativo o SISTEMA y utilizados para realizar un movimiento lateral mediante el uso de material de autenticación alternativo.</p>	

Descubrimiento	<p><a href="#">T1007</a> - Detección de servicios del sistema:</p> <p>Los adversarios pueden intentar obtener información sobre los servicios registrados. Los comandos que pueden obtener información sobre los servicios usando las utilidades del sistema operativo son "sc", "tasklist /svc" usando Tasklist y "net start" usando Net, pero los adversarios también pueden usar otras herramientas. Los adversarios pueden usar la información de System Service Discovery durante el descubrimiento automatizado para dar forma a comportamientos de seguimiento, incluso si el adversario infecta o no completamente al objetivo y/o intenta acciones específicas.</p>	<p>Este tipo de técnica de ataque no se puede mitigar fácilmente con controles preventivos ya que se basa en el abuso de las funciones del sistema.</p>
----------------	--	---

	<p><b>T1074.001</b> - Datos por etapas: Datos locales por etapas:</p> <p>Los adversarios pueden organizar los datos recopilados en una ubicación central o directorio en el sistema local antes de la Exfiltración. Los datos pueden guardarse en archivos separados o combinarse en un solo archivo a través de técnicas como Archivar datos recopilados. Se pueden usar shells de comandos interactivos, y se puede usar la funcionalidad común dentro de cmd y bash para copiar datos en una ubicación de preparación.</p> <p><b>T1560</b> - Archivar datos recopilados:</p> <p>Un adversario puede comprimir y/o cifrar los datos que se recopilan antes de la exfiltración. Comprimir los datos puede ayudar a ocultar los datos recopilados y minimizar la cantidad de datos enviados a través de la red. El cifrado se puede utilizar para ocultar la información que se extrae de la detección o hacer que la exfiltración sea menos notoria tras la inspección por parte de un defensor.</p>	<p>Este tipo de técnica de ataque no se puede mitigar fácilmente con controles preventivos ya que se basa en el abuso de las funciones del sistema.</p>
--	---	---

	<p><b>T1071.001</b> - Protocolo de capa de aplicación: Protocolos web:</p> <p>Los adversarios pueden comunicarse utilizando protocolos de capa de aplicación asociados con el tráfico web para evitar la detección/filtrado de la red mezclándose con el tráfico existente. Los comandos al sistema remoto y, a menudo, los resultados de esos comandos, se integrarán en el tráfico de protocolo entre el cliente y el servidor.</p> <p>Los protocolos como HTTP y HTTPS que transportan tráfico web pueden ser muy comunes en los entornos. Los paquetes HTTP/S tienen muchos campos y encabezados en los que se pueden ocultar datos. Un adversario puede abusar de estos protocolos para comunicarse con los sistemas bajo su control dentro de la red de una víctima mientras imita el tráfico esperado normal.</p> <p><b>T1573</b> - Canal encriptado:</p> <p>Los adversarios pueden emplear un algoritmo de cifrado conocido para ocultar el tráfico de comando y control en lugar de confiar en las protecciones inherentes proporcionadas por un protocolo de comunicación. A pesar del uso de un algoritmo seguro, estas implementaciones pueden ser vulnerables a la ingeniería inversa si las claves secretas se codifican o generan dentro de muestras/archivos de configuración de malware.</p>	<p><b>M1031</b> - Prevención de intrusiones en la red:</p> <p>Los sistemas de detección y prevención de intrusiones en la red que usan firmas de red para identificar el tráfico de malware adversario específico se pueden usar para mitigar la actividad a nivel de red.</p> <p><b>M1031</b> - Prevención de intrusiones en la red:</p> <p>Los sistemas de detección y prevención de intrusiones en la red que usan firmas de red para identificar el tráfico de malware adversario específico se pueden usar para mitigar la actividad a nivel de red.</p> <p><b>M1020</b> - Inspección SSL/TLS:</p> <p>La inspección SSL/TLS se puede utilizar para ver el contenido de las sesiones cifradas para buscar indicadores basados en la red de protocolos de comunicación de malware.</p>
--	---	---

	<p><b>T1219</b> – Software de Acceso Remoto:</p> <p>Un adversario puede usar soporte de escritorio legítimo y software de acceso remoto, como Team Viewer, Go2Assist, LogMeIn, AmmyyAdmin, etc., para establecer un canal de comando y control interactivo para atacar sistemas dentro de las redes. Estos servicios se usan comúnmente como software de soporte técnico legítimo y pueden estar permitidos por el control de la aplicación dentro de un entorno de destino.</p>	<p><b>M1038</b> - Prevención de ejecución:</p> <p>Utilice el control de aplicaciones para mitigar la instalación y el uso de software no aprobado que se puede utilizar para el acceso remoto.</p> <p><b>M1037</b> - Filtrar tráfico de red:</p> <p>Configure adecuadamente los firewalls, los firewalls de aplicaciones y los proxies para limitar el tráfico saliente a los sitios y servicios utilizados por las herramientas de acceso remoto.</p> <p><b>M1031</b> - Prevención de intrusiones en la red:</p> <p>Los sistemas de detección y prevención de intrusiones en la red que utilizan firmas de red pueden evitar el tráfico a los servicios de acceso remoto.</p>
exfiltración	<p><b>T1567.002</b> – Exfiltración a través del servicio web: Exfiltración al almacenamiento en la nube:</p> <p>Los adversarios pueden filtrar datos a un servicio de almacenamiento en la nube en lugar de a través de su canal principal de comando y control. Los servicios de almacenamiento en la nube permiten el almacenamiento, la edición y la recuperación de datos desde un servidor remoto de almacenamiento en la nube a través de Internet.</p>	<p><b>M1021</b> - Restringir contenido basado en la web:</p> <p>Los proxies web se pueden usar para hacer cumplir una política de comunicación de red externa que evita el uso de servicios externos no autorizados.</p>
	<p><b>T1486</b> - Datos cifrados para impacto:</p> <p>Los adversarios pueden cifrar los datos en los sistemas de destino o en una gran cantidad de sistemas en una red para interrumpir la disponibilidad de los recursos del sistema y de la red. Pueden intentar hacer que los datos almacenados sean inaccesibles cifrando archivos o datos en unidades locales y remotas y reteniendo el acceso a una clave de descifrado.</p>	<p><b>M1040</b> - Prevención del comportamiento en el punto final: en Windows 10, habilite la protección proporcionada por la nube y las reglas de reducción de la superficie de ataque (ASR) para bloquear la ejecución de archivos que se asemejan al ransomware.</p> <p><b>M1053</b> - Respaldo de datos: considere implementar planes de recuperación de desastres de TI que contengan procedimientos para realizar y probar respaldos de datos con regularidad que se puedan usar para restaurar datos de la organización. Asegúrese de que las copias de seguridad se almacenen fuera del sistema y estén protegidas de los métodos comunes que los adversarios pueden usar para obtener acceso y destruir las copias de seguridad para evitar la recuperación. Considere habilitar el control de versiones en entornos de nube para mantener copias de seguridad de los objetos de almacenamiento.</p>
	<p><b>T1490</b> - Recuperación del sistema Habitante:</p> <p>Los adversarios pueden eliminar o eliminar los datos del sistema operativo integrado y desactivar los servicios diseñados para ayudar en la recuperación de un sistema dañado para evitar la recuperación. Los sistemas operativos pueden contener funciones que pueden ayudar a reparar sistemas corruptos, como un catálogo de respaldo, instantáneas de volumen y funciones de reparación automática. Los adversarios pueden deshabilitar o eliminar las funciones de recuperación del sistema para aumentar los efectos de la destrucción de datos y el cifrado de datos para impacto.</p>	<p><b>M1053</b> - Respaldo de datos: considere implementar planes de recuperación de desastres de TI que contengan procedimientos para realizar respaldos de datos regulares que se puedan usar para restaurar datos organizacionales. Asegúrese de que las copias de seguridad se almacenen fuera del sistema y estén protegidas de los métodos comunes que los adversarios pueden usar para obtener acceso y destruir las copias de seguridad para evitar la recuperación.</p> <p><b>M1028</b> - Configuración del sistema operativo: considerar controles técnicos para evitar la desactivación de servicios o la eliminación de archivos involucrados en la recuperación del sistema.</p>

Impacto	<p><b>T1489 - Parada de servicio:</b></p> <p>Los adversarios pueden detener o deshabilitar los servicios en un sistema para que esos servicios no estén disponibles para los usuarios legítimos. Detener servicios o procesos críticos puede inhibir o detener la respuesta a un incidente o ayudar en los objetivos generales del adversario para causar daño al medio ambiente.</p>	<p><b>M1030 - Segmentación de red:</b> Opere sistemas de detección, análisis y respuesta de intrusos en una red separada del entorno de producción para disminuir las posibilidades de que un adversario pueda ver e interferir con las funciones de respuesta críticas.</p>
	<p><b>T1491.001 - Desfiguración interna:</b></p> <p>Un adversario puede desfigurar los sistemas internos de una organización en un intento de intimidar o engañar a los usuarios. Esto puede tomar la forma de modificaciones en los sitios web internos o directamente en los sistemas de los usuarios con el reemplazo del fondo de pantalla del escritorio. Se pueden usar imágenes perturbadoras u ofensivas como parte de la desfiguración interna para incomodar al usuario o para presionar el cumplimiento de los mensajes adjuntos. Dado que la desfiguración interna de los sistemas expone la presencia de un adversario, a menudo se lleva a cabo después de que se hayan logrado otros objetivos de intrusión.</p>	<p><b>M1022 - Restringir permisos de archivos y directorios:</b> asegúrese de que se implementen los permisos de archivos y procesos adecuados para evitar que los adversarios deshabiliten o interfieran con los servicios críticos.</p> <p><b>M1024 - Restringir permisos de registro:</b> asegúrese de que se cuente con los permisos de registro adecuados para evitar que los adversarios deshabiliten o interfieran con los servicios críticos.</p> <p><b>M1018 - Administración de cuentas de usuario:</b> limite los privilegios de cuentas y grupos de usuarios para que solo los administradores autorizados puedan interactuar con los cambios y las configuraciones del servicio.</p> <p><b>M1053 - Copia de seguridad de datos:</b></p> <p>Considere implementar planes de recuperación ante desastres de TI que contengan procedimientos para realizar copias de seguridad de datos periódicas que se puedan usar para restaurar datos de la organización. Asegúrese de que las copias de seguridad se almacenen fuera del sistema y estén protegidas de los métodos comunes que los adversarios pueden usar para obtener acceso y destruir las copias de seguridad para evitar la recuperación.</p>

