ANÁLISIS FORENSE INFORMÁTICO

INFORME PERICIAL

ANÁLISIS DE RED Y MALWARE

TRABAJO REALIZADO POR

ILIAN LUBENOV

CONTENIDO

1. Identificación del perito 1

2. Objeto de la pericia 2

3. Alcance y limitaciones 3
   3.1 Alcance del trabajo 3

   3.2 Limitaciones 3

4. Antecedentes 5

5. Resumen ejecutivo 7

6. Elementos recibidos y verificación de integridad 9
   6.1 Descripción de los indicios entregados 9

   6.2 Control de Integridad y Validación Criptográfica 9

7. Entorno metodológico y herramientas utilizadas 11

8. Análisis detallado de artefactos 12
   8.1 Identificación del equipo infectado 12

   8.2 Análisis del tráfico malicioso y exfiltración de datos 13

   8.3 Identificación de la infraestructura de mando y control (C2) 17

   8.4 Análisis estadístico del tráfico y confirmación de la amenaza 20

9. Conclusiones periciales 25
   9.1 Cronología 27

10. Anexo 28
   10.1 Identificación del caso 28

   10.2 Descripción de los indicios 28

   10.3 Verificación criptográfica (Hashes) 28

   10.4 Registro de traspaso (Transfer logs) 30

1

Identificación del perito

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

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

Nombre completo: Ilian Lubenov.

Documento Nacional de Identidad: 123456789K.

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

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

Empresa/s: Digitechfp.

2

Objeto de la pericia

El objeto de este informe es realizar el análisis forense digital del volcado de tráfico de red EVID-NET-01.pcap, capturado en el segmento 10.1.21.0/24 del dominio win11office[.]com, tras la activación de una regla del IDS que detectó tráfico saliente desde el segmento interno con destino a la IP externa **153[.]92[.]1[.]49**, consistente con la actividad del malware Lumma Stealer, el 27 de enero de 2026.

Para responder a este incidente, el análisis se centra en cumplir los siguientes objetivos técnicos:

- **Identificación del activo:**

  Determinar de forma inequívoca el equipo afectado, extrayendo su dirección IP, MAC, nombre de host y la cuenta de usuario de Windows activa durante el compromiso.

- **Trazabilidad de la descarga:**

  Verificar si el usuario descargó archivos maliciosos, identificándolos y contrastando su peligrosidad mediante fuentes de inteligencia de amenazas.

- **Alcance e infraestructura C2:**

  Localizar todos los dominios y servidores de Comando y Control (C2) con los que interactuó el equipo para coordinar su bloqueo perimetral.

- **Extracción de IoCs:**

  Recopilar todos los Indicadores de Compromiso presentes en la captura para facilitar el aislamiento del equipo y la contención del incidente.

- **Fundamento técnico:**

  Aportar la evidencia digital documentada que sirva de base para las medidas legales, disciplinarias o de respuesta que la autoridad competente o la corporación estime oportuno adoptar.

3

Alcance y limitaciones

3.1 Alcance del trabajo

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

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

- **Volcado de tráfico de red (EVID-NET-01.pcap):**

  Captura íntegra del tráfico de red del segmento LAN 10.1.21.0/24 del dominio win11office[.]com, obtenida mediante puerto espejo (*SPAN Port*) en el nodo perimetral durante la ventana temporal del incidente del 27 de enero de 2026, sobre la cual se han realizado todos los análisis descritos en el presente informe, sin alteración alguna del material original.

Queda expresamente fuera del alcance de esta pericia cualquier análisis sobre los dispositivos finales del segmento afectado, la infraestructura del potencial atacante, otros segmentos de red corporativa no incluidos en la captura, o cualquier otro activo no referenciado en la cadena de custodia.

3.2 Limitaciones

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

- **Imposibilidad de extracción del archivo malicioso:** La descarga del archivo malicioso que originó la infección se realizó mediante el protocolo HTTPS, cuyo contenido viaja cifrado entre el cliente y el servidor. Al no disponer de las claves de sesión TLS correspondientes, el contenido de dicha transferencia no es accesible desde el análisis del PCAP, lo que impide identificar el archivo descargado, obtener su nombre, su hash criptográfico o someterlo a análisis de malware. Esta limitación afecta directamente a la acreditación inequívoca del archivo

malicioso requerida en el objeto de la pericia, si bien el dominio de distribución media[.]megafilehub4[.]lat ha sido identificado e independientemente acreditado como sitio de distribución de malware mediante inteligencia de amenazas.

- **Acotación temporal de la evidencia:** El análisis se limita estrictamente al tráfico registrado durante la ventana de captura de 621 segundos. Comunicaciones anteriores al inicio del PCAP incluyendo posiblemente fases previas de la cadena de ataque no son recuperables a partir de esta evidencia.
- **Exclusión del análisis del dispositivo final:** Queda fuera del alcance de esta pericia cualquier análisis forense del equipo DESKTOP-ES9F3ML, incluyendo su memoria volátil, disco persistente, registros del sistema operativo o artefactos de aplicación. El análisis se ha realizado exclusivamente sobre los artefactos de red disponibles en la captura.
- **Exclusión de la infraestructura del atacante:** Queda igualmente fuera del alcance cualquier análisis de los servidores de mando y control identificados (whitepepper[.]su, communicationfirewall-security[.]cc, whooptm[.]cyou, holiday-forever[.]cc y media[.]megafilehub4[.]lat), así como de cualquier otra infraestructura externa no incluida en la cadena de custodia.
- **Imposibilidad de determinar el alcance exacto de la exfiltración:** Aunque el análisis confirma que se produjeron transmisiones de datos hacia el servidor C2 en el momento de la captura, no es posible determinar desde el análisis de red qué credenciales concretas fueron comprometidas ni si los datos exfiltrados llegaron a ser utilizados con fines fraudulentos con anterioridad a la captura.

4

Antecedentes

El presente informe responde a la solicitud del Departamento de Seguridad Corporativa, a raíz de la detección de un incidente de seguridad activo en el segmento de red 10.1.21.0/24 del dominio win11office[.]com, registrado con fecha **27 de enero de 2026 a las 23:05 horas (UTC)**. Los hechos que motivan la presente pericial se desarrollaron bajo la siguiente secuencia técnica:

- **Detección inicial:**

  Durante la revisión del histórico de alertas por parte del equipo del Centro de Operaciones de Seguridad (SOC), se identificó la activación de una regla del Sistema de Detección de Intrusiones (IDS) sobre el tráfico del segmento interno. La firma registrada fue ET MALWARE Lumma Stealer Victim Fingerprinting Activity, una regla de detección específica asociada al malware **Lumma Stealer**, una amenaza de tipo *infostealer* cuya finalidad es la recopilación sistemática y exfiltración de credenciales almacenadas, datos del sistema y otra información sensible del equipo comprometido.

- **Análisis del tráfico malicioso:**

  El análisis del evento detonante permitió constatar que un dispositivo perteneciente al segmento interno 10.1.21.0/24, dentro del dominio corporativo win11office[.]com, había establecido comunicación hacia la dirección IP externa **153[.]92[.]1[.]49** a través del puerto **TCP 80**. El patrón de tráfico observado es consistente con la fase de *fingerprinting* característica de Lumma Stealer, esto es, la fase de reconocimiento inicial en la que el malware recopila información del sistema víctima con carácter previo a la exfiltración de los datos robados hacia la infraestructura de mando y control (C2) del atacante.

- **Preservación de la evidencia:**

  Con el fin de asegurar la integridad de las evidencias digitales y dar cumplimiento a los principios de la prueba electrónica, el **31 de enero de 2026 a las 09:15 horas (UTC)** se procedió a la exportación lógica de los registros de tráfico desde el repositorio centralizado del SIEM, en modo de solo lectura, generando el volcado de tráfico de red continuo **EVID-NET-01.pcap**. De forma inmediata a la adquisición, se calculó el valor hash criptográfico del fichero obtenido a fin de garantizar el principio de

mismidad de la evidencia, verificando que el material no había sido alterado desde su origen. La evidencia fue almacenada en una unidad de almacenamiento forense cifrada y el proceso completo quedó debidamente documentado en el Registro Estricto de Cadena de Custodia adjunto al presente informe.

5

Resumen Ejecutivo

El presente informe documenta el análisis forense digital realizado sobre el tráfico de red del equipo DESKTOP-ES9F3ML, asignado al usuario gwyatt dentro de la red corporativa del dominio win11office[.]com, tras detectarse el 27 de enero de 2026 actividad maliciosa en el segmento interno de la empresa.

La investigación confirma de forma concluyente que el equipo fue comprometido por el malware conocido como **Lumma Stealer**, un programa malicioso especializado en el robo automatizado de contraseñas almacenadas en navegadores web, credenciales de acceso a plataformas digitales y otra información sensible del sistema. El análisis de la captura de red evidencia que el usuario descargó el archivo malicioso desde un servidor externo de distribución de malware, momento a partir del cual el programa se instaló de forma silenciosa en el equipo sin que el usuario fuera consciente de ello.

Una vez activo, el malware estableció comunicaciones regulares y automatizadas con cinco servidores maliciosos en Internet denominados en el ámbito de la ciberseguridad como infraestructura de *mando y control* a los cuales remitió de forma cifrada las credenciales robadas del equipo comprometido. El análisis forense acredita que la transmisión de datos robados hacia el servidor principal whitepepper[.]su se encontraba activa y en curso en el momento en que fue detectada la actividad maliciosa, habiéndose confirmado el envío de al menos dos paquetes de datos con credenciales comprimidas de un tamaño total superior a 15.000 bytes.

Impacto y estado actual: El análisis del tráfico de red confirma que el malware estuvo activo y realizó transmisiones de datos hacia la infraestructura maliciosa. No es posible determinar desde el análisis de la captura de red qué credenciales concretas fueron comprometidas ni si los datos transmitidos llegaron a ser utilizados con fines fraudulentos, por lo que se recomienda el cambio inmediato de todas las contraseñas del usuario afectado y la revisión de los accesos corporativos asociados a la cuenta gwyatt.

6

Elementos recibidos y verificación de integridad

6.1 Descripción de los indicios entregados

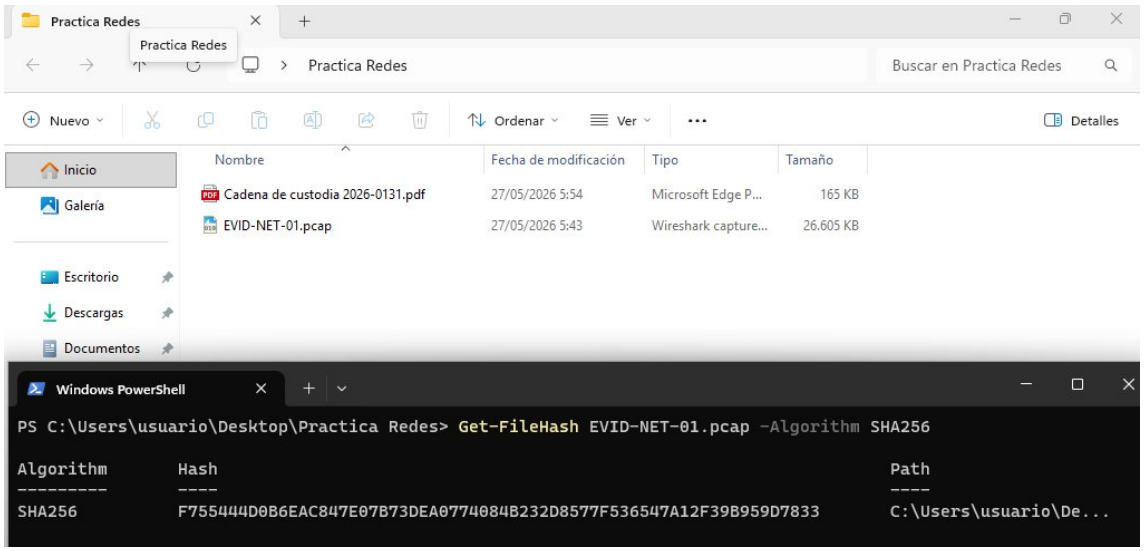
El laboratorio forense ha recibido en fecha **31 de enero de 2026** los siguientes indicios digitales, debidamente precintados y referenciados en el registro estricto de la cadena de custodia:

- **Elemento 1 (Imagen Pericial):**

  Un archivo EVID-NET-01 con extensión .pcap que contiene el volcado de tráfico de red continuo del segmento LAN 10.1.21.0/24 del dominio win11office[.]com, adquirido el **27 de enero de 2026 a las 23:05h (UTC)** mediante captura pasiva por puerto espejo (*SPAN Port*) en el nodo perimetral, exportado del repositorio centralizado del SIEM con permisos de solo lectura. El tamaño del archivo es de **25,9 MB** en formato estándar libpcap.

6.2 Control de Integridad y Validación Criptográfica

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



(Imagen 1; Cálculo del hash del tráfico de red PCAP para verificar su vericidad con la cadena de custodia).

Elemento / Evidencia.	Algoritmo.	Hash Original (Cadena Custodia).	Hash Calculado (Laboratorio).	Resultado de Validación.
Volcado de tráfico de red EVID-NET-01.pcap	SHA-256	F755444D0B6EAC847E07B73DEA0774084B232D8577F536547A12F39B959D7833	F755444D0B6EAC847E07B73DEA0774084B232D8577F536547A12F39B959D7833	Coincidente (OK)

7

Entorno metodológico y herramientas utilizadas

Herramienta forense	Versión	Fabricante	Finalidad
sha256sum	GNU coreutils	GNU Project	Verificación criptográfica (SHA-256) del volcado de tráfico de red
Wireshark	4.4.6	Gerald Combs	Análisis de tráfico
VirusTotal	N/A	Bernardo Quintero, equipo de Hispasec	Geolocalizar IP's Consultar si un archivo es malware dado su hash

8

Análisis de tráfico de red

8.1 Identificación del equipo infectado

Para determinar la identidad del equipo comprometido dentro del segmento 10.1.21.0/24, se aplicó el filtro bootp sobre la evidencia EVID-NET-01.pcap, aislando el intercambio DHCP registrado al inicio de la captura. El análisis del paquete DHCP Request (frame 3) permitió extraer los identificadores únicos del equipo, al contener en sus opciones de protocolo la dirección física del adaptador de red, el nombre de host del sistema y la dirección IP solicitada al servidor DHCP 10.1.21.1.

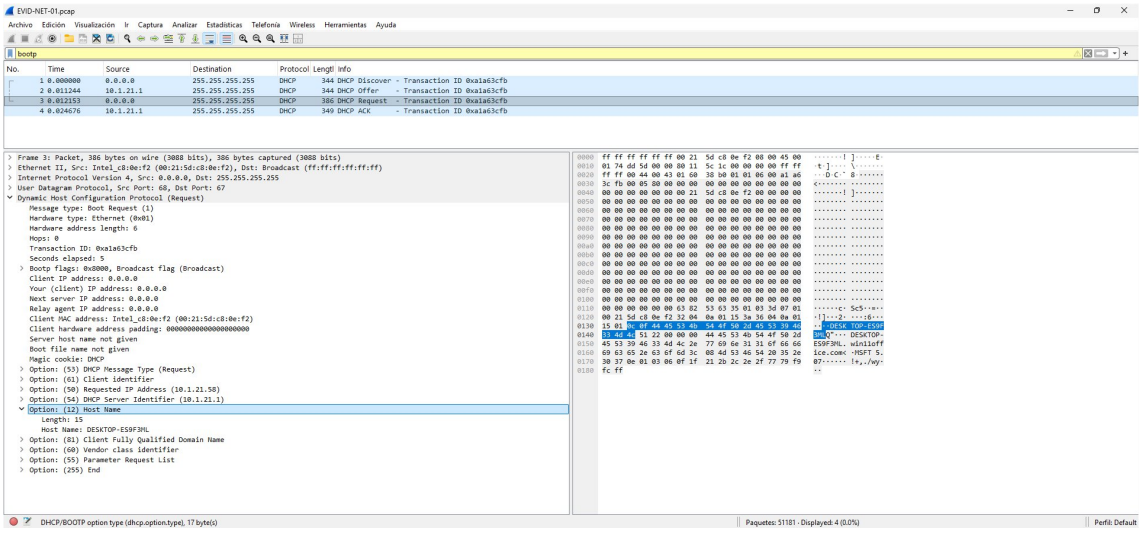


Figura 1: Paquete DHCP Request (frame 3) en Wireshark con filtro bootp sobre EVID-NET-01.pcap, con las opciones DHCP desplegadas: Client MAC Address (00:21:5d:c8:0e:f2), Requested IP Address (Option 50: 10.1.21.58) y Host Name (Option 12: DESKTOP-ES9F3ML).

Con el fin de identificar la cuenta de usuario de Windows activa durante el incidente, se aplicó el filtro kerberos sobre la captura, localizando el paquete AS-REQ (frame 214), que contiene la solicitud de autenticación enviada por el equipo víctima al Controlador de Dominio 10.1.21.2 (WIN-LU4L24X3UB7). El campo cname-string del bloque req-body de dicha solicitud contiene el nombre de usuario en texto claro, confiriendo plena identificación del titular de la sesión activa durante el incidente.

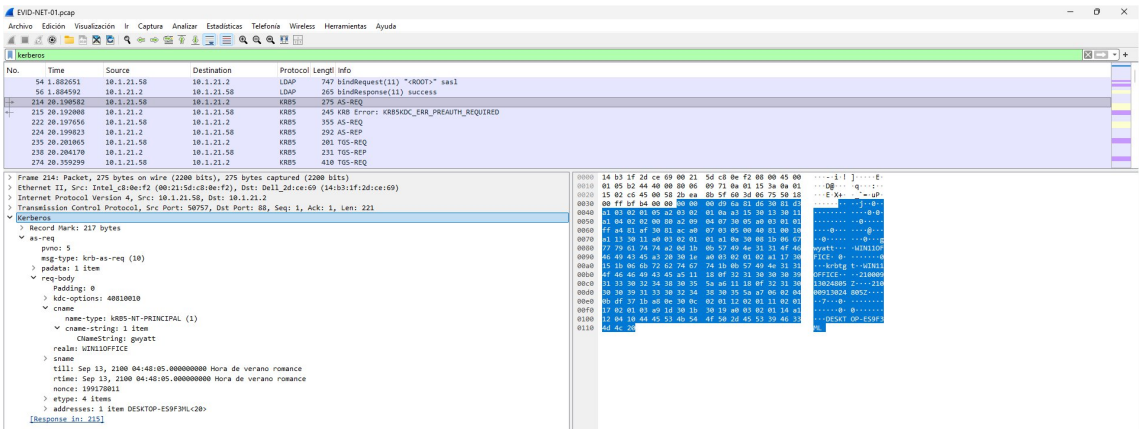


Figura 2: Paquete AS-REQ Kerberos (frame 214) en Wireshark con filtro kerberos, mostrando el bloque req-body de la solicitud de autenticación del equipo 10.1.21.58 al Domain Controller 10.1.21.2 con el campo cname-string: gwyatt y el campo addresses: DESKTOP-ES9F3ML.

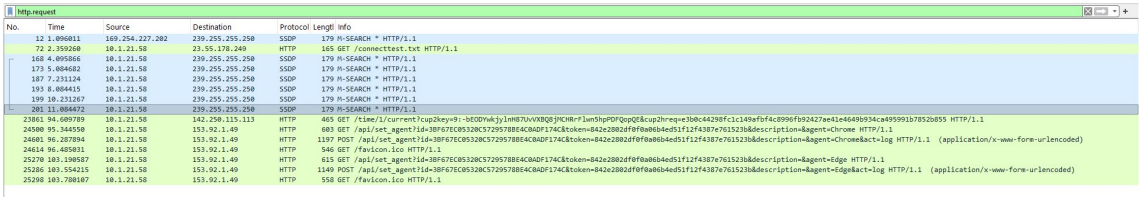
Del análisis de ambos artefactos de red se extraen los siguientes datos identificativos del equipo comprometido:

CAMPO	VALOR
Dirección IP	10.1.21.58
Dirección MAC	00:21:5d:c8:0e:f2
Hostname	DESKTOP-ES9F3ML
Usuario Windows	gwyatt

La coincidencia entre el campo addresses: DESKTOP-ES9F3ML<20> del paquete Kerberos y el campo Option 12: Host Name del paquete DHCP confirma la consistencia de los datos identificativos obtenidos a partir de dos fuentes independientes de la captura.

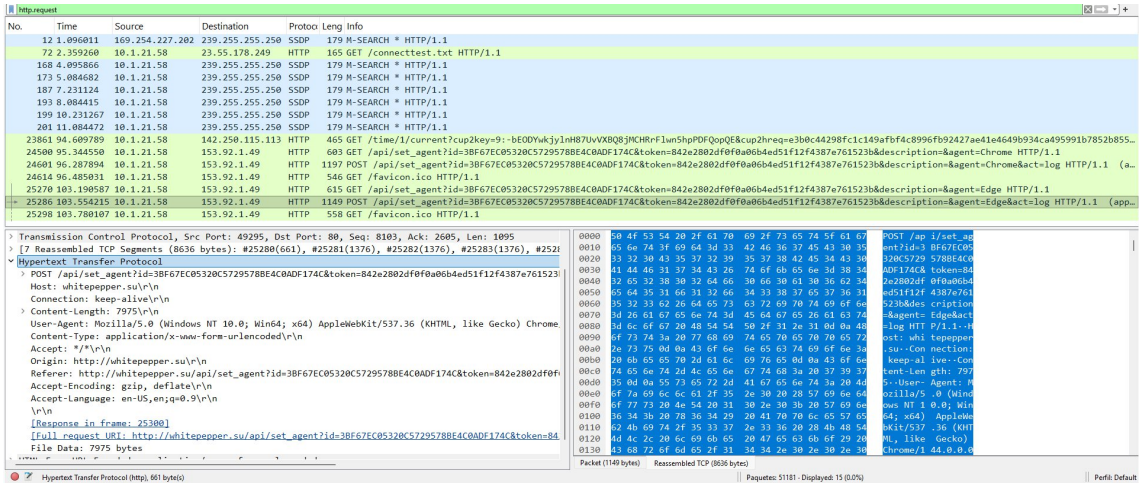
8.2 Análisis del tráfico malicioso y exfiltración de datos

Con el fin de identificar las comunicaciones maliciosas presentes en la captura, se aplicó el filtro http.request sobre la evidencia EVID-NET-01.pcap, aislando la totalidad de las peticiones HTTP realizadas desde el segmento interno. Del análisis del tráfico resultante se distinguen dos categorías: tráfico HTTP legítimo de sistema la comprobación NCSI hacia www.msftconnecttest.com y la actualización del navegador hacia clients2.google.com y tráfico HTTP malicioso de mando y control dirigido íntegramente hacia la dirección IP 153[.]92[.]1[.]49.



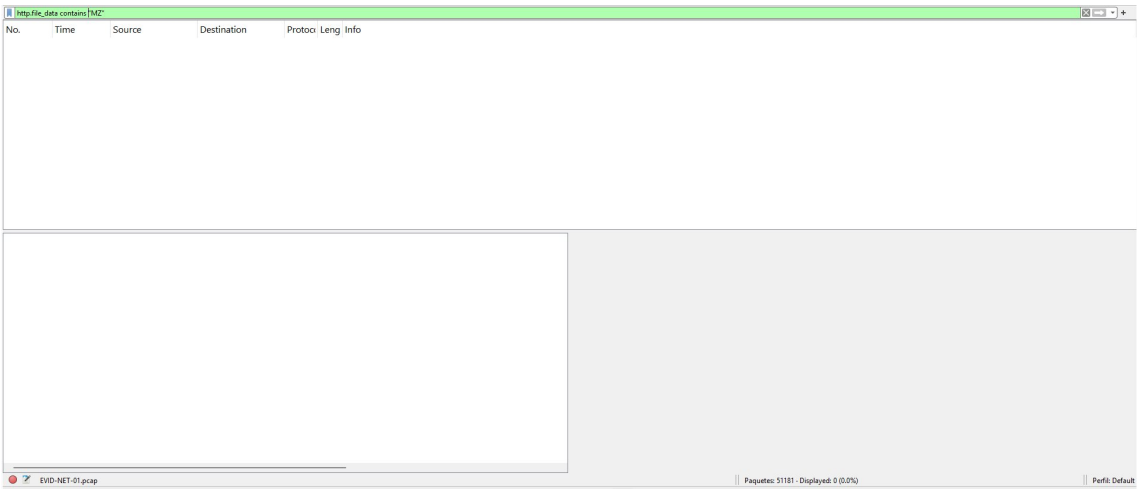
(Figura 3: Resultado del filtro http.request sobre EVID-NET-01.pcap en Wireshark, mostrando las peticiones HTTP del equipo víctima. Se aprecian comunicaciones legítimas de sistema y tráfico malicioso de C2 hacia 153[.]92[.]1[.]49 con el endpoint /api/set_agent.)

El análisis detallado de las peticiones POST dirigidas al servidor C2 reveló el endpoint /api/set_agent, patrón característico de la infraestructura de Lumma Stealer para el registro de víctimas y la exfiltración de credenciales. La cabecera Host del paquete 25286 confirma el dominio whitepepper[.]su como servidor receptor, el parámetro act=log indica la fase activa de envío de datos robados, y el campo Content-Length evidencia la transferencia de una carga de datos sustancial. Los bytes PK identificados en el cuerpo del formulario confirman que el malware comprime en formato ZIP las credenciales robadas antes de exfiltrarlas.

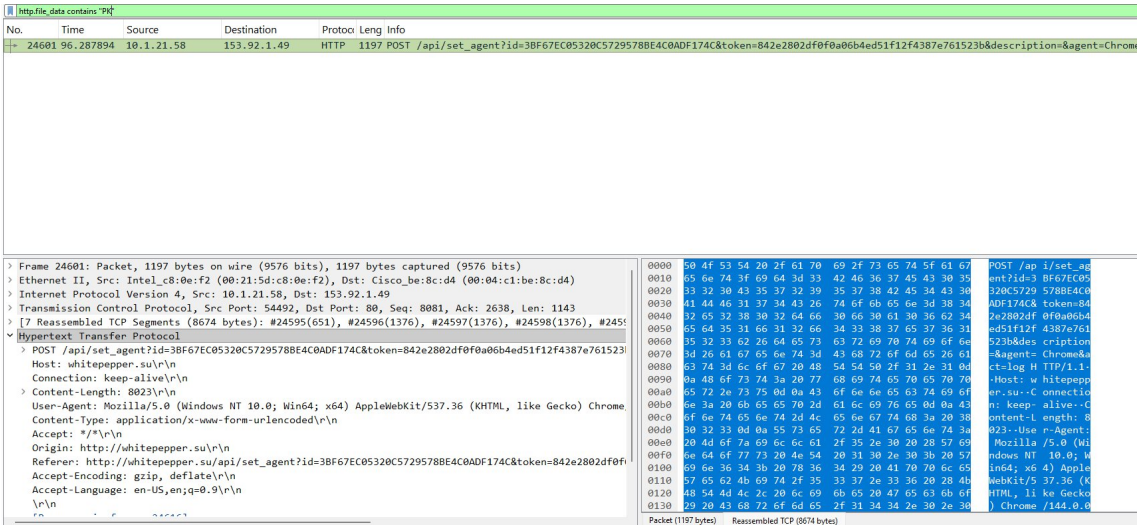


(Figura 4: Detalle del paquete POST 25286 en Wireshark, mostrando la cabecera HTTP con el campo Host: whitepepper[.]su, el endpoint /api/set_agent con parámetro act=log y el tipo de contenido application/x-www-form-urlencoded con los datos exfiltrados.)

Siguiendo el procedimiento de file carving, se aplicó el filtro http.file_data contains "MZ" con el fin de localizar transferencias de archivos ejecutables Windows (formato PE) por HTTP. El resultado fue nulo: ningún ejecutable fue descargado mediante HTTP durante la ventana de captura.

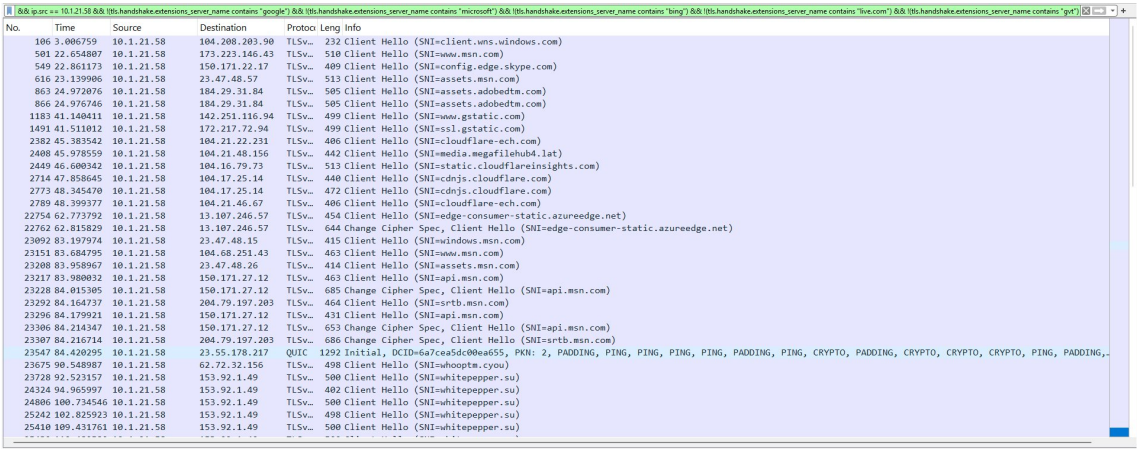


(Figura 5: Resultado del filtro http.file_data contains "MZ" sobre EVID-NET-01.pcap en Wireshark. La ausencia de resultados confirma que ningún archivo ejecutable fue descargado mediante HTTP sin cifrar durante el incidente.)



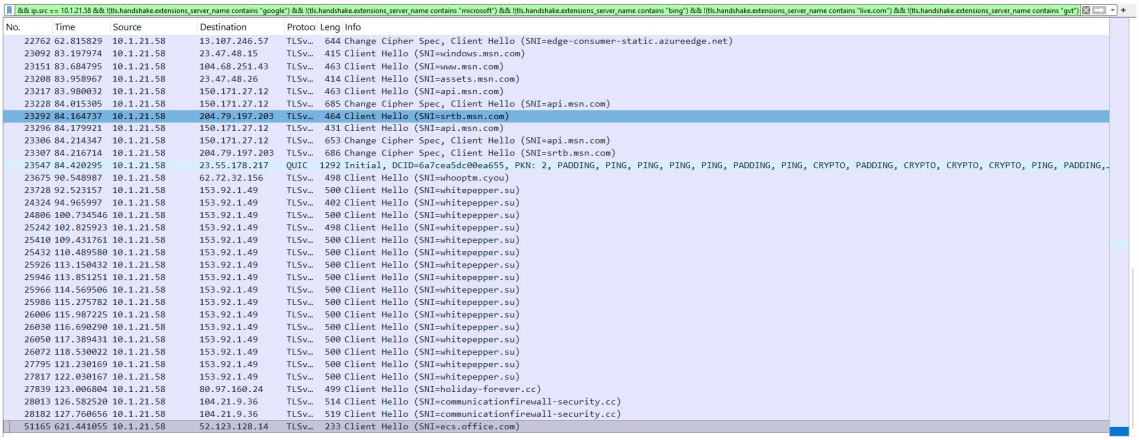
(Figura 6: Resultado del filtro http.file_data contains "PK" sobre EVID-NET-01.pcap. Los bytes PK (magic bytes del formato ZIP) fueron localizados en el cuerpo de una petición POST a whitepepper[.]su, correspondientes a los datos de credenciales comprimidos antes de su exfiltración al C2.)

Al no haberse localizado el archivo malicioso mediante HTTP, se procedió al análisis del tráfico HTTPS cifrado mediante el filtro tls.handshake.type == 1 && ip.src == 10.1.21.58, que aísla los paquetes TLS Client Hello originados por el equipo infectado. Este filtro expone el campo SNI (Server Name Indication), que revela el nombre del servidor destino en texto claro pese al cifrado del contenido. Eliminando los dominios legítimos conocidos de Microsoft, Google y Cloudflare, se identificaron los siguientes dominios de carácter sospechoso.



No.	Time	Source	Destination	Protoc	Leng	Info
106	3.006759	10.1.21.58	104.208.203.90	TLSv…	232	Client Hello (SNI=client.wns.windows.com)
501	22.654807	10.1.21.58	173.223.146.43	TLSv…	510	Client Hello (SNI=www.msn.com)
549	22.861173	10.1.21.58	150.171.22.17	TLSv…	409	Client Hello (SNI=config.edge.skype.com)
616	23.139906	10.1.21.58	23.47.48.57	TLSv…	513	Client Hello (SNI=assets.msn.com)
863	24.972076	10.1.21.58	184.29.31.84	TLSv…	505	Client Hello (SNI=assets.adobedtm.com)
866	24.976746	10.1.21.58	184.29.31.84	TLSv…	505	Client Hello (SNI=assets.adobedtm.com)
1183	41.140411	10.1.21.58	142.251.116.94	TLSv…	499	Client Hello (SNI=www.gstatic.com)
1491	41.511012	10.1.21.58	172.217.72.94	TLSv…	499	Client Hello (SNI=ssl.gstatic.com)
2382	45.383542	10.1.21.58	104.21.22.231	TLSv…	406	Client Hello (SNI=cloudflare-ech.com)
2408	45.978559	10.1.21.58	104.21.48.156	TLSv…	442	Client Hello (SNI=media.megafilehub4.lat)
2449	46.600342	10.1.21.58	104.16.79.73	TLSv…	513	Client Hello (SNI=static.cloudflareinsights.com)
2714	47.858645	10.1.21.58	104.17.25.14	TLSv…	440	Client Hello (SNI=cdnjs.cloudflare.com)
2773	48.345470	10.1.21.58	104.17.25.14	TLSv…	472	Client Hello (SNI=cdnjs.cloudflare.com)
2789	48.399377	10.1.21.58	104.21.46.67	TLSv…	406	Client Hello (SNI=cloudflare-ech.com)
22754	62.773792	10.1.21.58	13.107.246.57	TLSv…	454	Client Hello (SNI=edge-consumer-static.azureedge.net)
22762	62.815829	10.1.21.58	13.107.246.57	TLSv…	644	Change Cipher Spec, Client Hello (SNI=edge-consumer-static.azureedge.net)
23092	83.197974	10.1.21.58	23.47.48.15	TLSv…	415	Client Hello (SNI=windows.msn.com)
23151	83.684795	10.1.21.58	104.68.251.43	TLSv…	463	Client Hello (SNI=www.msn.com)
23208	83.958967	10.1.21.58	23.47.48.26	TLSv…	414	Client Hello (SNI=assets.msn.com)
23217	83.980032	10.1.21.58	150.171.27.12	TLSv…	463	Client Hello (SNI=api.msn.com)
23228	84.015305	10.1.21.58	150.171.27.12	TLSv…	685	Change Cipher Spec, Client Hello (SNI=api.msn.com)
23292	84.164737	10.1.21.58	204.79.197.203	TLSv…	464	Client Hello (SNI=srtb.msn.com)
23296	84.179921	10.1.21.58	150.171.27.12	TLSv…	431	Client Hello (SNI=api.msn.com)
23306	84.214347	10.1.21.58	150.171.27.12	TLSv…	653	Change Cipher Spec, Client Hello (SNI=api.msn.com)
23307	84.216714	10.1.21.58	204.79.197.203	TLSv…	686	Change Cipher Spec, Client Hello (SNI=srtb.msn.com)
23547	84.420295	10.1.21.58	23.55.178.217	QUIC	1292	Initial, DCID=6a7cea5dc00ea655, PKN: 2, PADDING, PING, PING, PING, PING, PADDING, PING, CRYPTO, PADDING, CRYPTO, CRYPTO, CRYPTO, PING, PADDING,
23675	90.548987	10.1.21.58	62.72.32.156	TLSv…	498	Client Hello (SNI=whooptm.cyou)
23728	92.523157	10.1.21.58	153.92.1.49	TLSv…	500	Client Hello (SNI=whitepepper.su)
24324	94.965997	10.1.21.58	153.92.1.49	TLSv…	402	Client Hello (SNI=whitepepper.su)
24806	100.734546	10.1.21.58	153.92.1.49	TLSv…	500	Client Hello (SNI=whitepepper.su)
25242	102.825923	10.1.21.58	153.92.1.49	TLSv…	498	Client Hello (SNI=whitepepper.su)
25410	109.431761	10.1.21.58	153.92.1.49	TLSv…	500	Client Hello (SNI=whitepepper.su)

(Figura 7: Primera parte del resultado del filtro tls.handshake.type == 1 con exclusión de dominios legítimos sobre EVID-NET-01.pcap, mostrando los dominios sospechosos identificados en los campos SNI de los paquetes TLS Client Hello.)

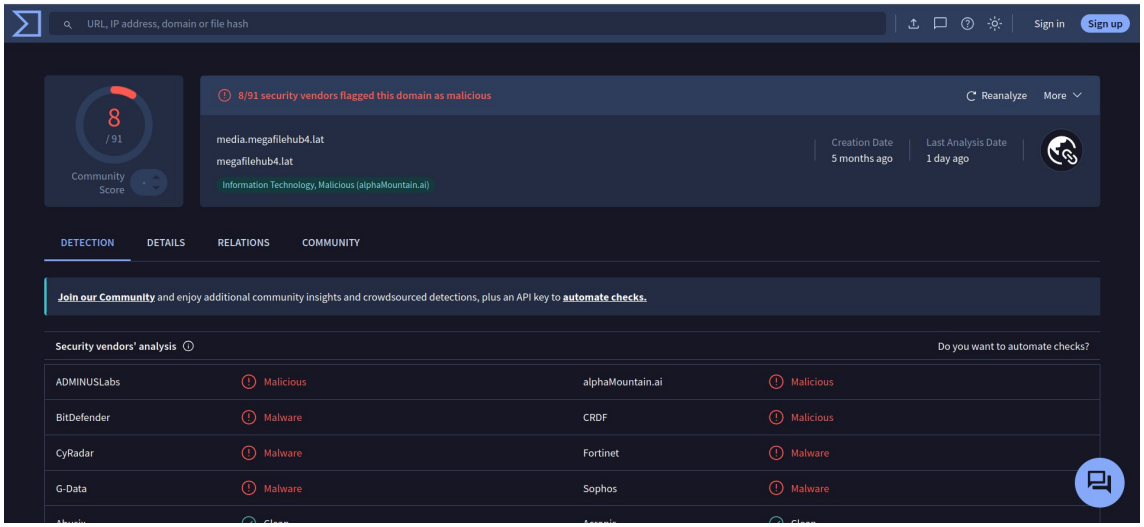


No.	Time	Source	Destination	Protoc	Leng	Info
22762	62.815829	10.1.21.58	13.107.246.57	TLSv…	644	Change Cipher Spec, Client Hello (SNI=edge-consumer-static.azureedge.net)
23092	83.197974	10.1.21.58	23.47.48.15	TLSv…	415	Client Hello (SNI=windows.msn.com)
23151	83.684795	10.1.21.58	104.68.251.43	TLSv…	463	Client Hello (SNI=www.msn.com)
23208	83.958967	10.1.21.58	23.47.48.26	TLSv…	414	Client Hello (SNI=assets.msn.com)
23217	83.980032	10.1.21.58	150.171.27.12	TLSv…	463	Client Hello (SNI=api.msn.com)
23228	84.015305	10.1.21.58	150.171.27.12	TLSv…	685	Change Cipher Spec, Client Hello (SNI=api.msn.com)
23292	84.164737	10.1.21.58	204.79.197.203	TLSv…	464	Client Hello (SNI=srtb.msn.com)
23296	84.179921	10.1.21.58	150.171.27.12	TLSv…	431	Client Hello (SNI=api.msn.com)
23306	84.214347	10.1.21.58	150.171.27.12	TLSv…	653	Change Cipher Spec, Client Hello (SNI=api.msn.com)
23307	84.216714	10.1.21.58	204.79.197.203	TLSv…	686	Change Cipher Spec, Client Hello (SNI=srtb.msn.com)
23547	84.420295	10.1.21.58	23.55.178.217	QUIC	1292	Initial, DCID=6a7cea5dc00ea655, PKN: 2, PADDING, PING, PING, PING, PING, PADDING, PING, CRYPTO, PADDING, CRYPTO, CRYPTO, CRYPTO, PING, PADDING,
23675	90.548987	10.1.21.58	62.72.32.156	TLSv…	498	Client Hello (SNI=whooptm.cyou)
23728	92.523157	10.1.21.58	153.92.1.49	TLSv…	500	Client Hello (SNI=whitepepper.su)
24324	94.965997	10.1.21.58	153.92.1.49	TLSv…	402	Client Hello (SNI=whitepepper.su)
24806	100.734546	10.1.21.58	153.92.1.49	TLSv…	500	Client Hello (SNI=whitepepper.su)
25242	102.825923	10.1.21.58	153.92.1.49	TLSv…	498	Client Hello (SNI=whitepepper.su)
25410	109.431761	10.1.21.58	153.92.1.49	TLSv…	500	Client Hello (SNI=whitepepper.su)
25432	110.489580	10.1.21.58	153.92.1.49	TLSv…	500	Client Hello (SNI=whitepepper.su)
25926	113.150432	10.1.21.58	153.92.1.49	TLSv…	500	Client Hello (SNI=whitepepper.su)
25946	113.851251	10.1.21.58	153.92.1.49	TLSv…	500	Client Hello (SNI=whitepepper.su)
25966	114.569506	10.1.21.58	153.92.1.49	TLSv…	500	Client Hello (SNI=whitepepper.su)
25986	115.275782	10.1.21.58	153.92.1.49	TLSv…	500	Client Hello (SNI=whitepepper.su)
26006	115.987225	10.1.21.58	153.92.1.49	TLSv…	500	Client Hello (SNI=whitepepper.su)
26030	116.690290	10.1.21.58	153.92.1.49	TLSv…	500	Client Hello (SNI=whitepepper.su)
26050	117.389431	10.1.21.58	153.92.1.49	TLSv…	500	Client Hello (SNI=whitepepper.su)
26072	118.530022	10.1.21.58	153.92.1.49	TLSv…	500	Client Hello (SNI=whitepepper.su)
27795	121.230169	10.1.21.58	153.92.1.49	TLSv…	500	Client Hello (SNI=whitepepper.su)
27817	122.030167	10.1.21.58	153.92.1.49	TLSv…	500	Client Hello (SNI=whitepepper.su)
27839	123.006804	10.1.21.58	80.97.160.24	TLSv…	499	Client Hello (SNI=holiday-forever.cc)
28013	126.582520	10.1.21.58	104.21.9.36	TLSv…	514	Client Hello (SNI=communicationfirewall-security.cc)
28182	127.760656	10.1.21.58	104.21.9.36	TLSv…	519	Client Hello (SNI=communicationfirewall-security.cc)
51165	621.441055	10.1.21.58	52.123.128.14	TLSv…	233	Client Hello (SNI=ecs.office.com)

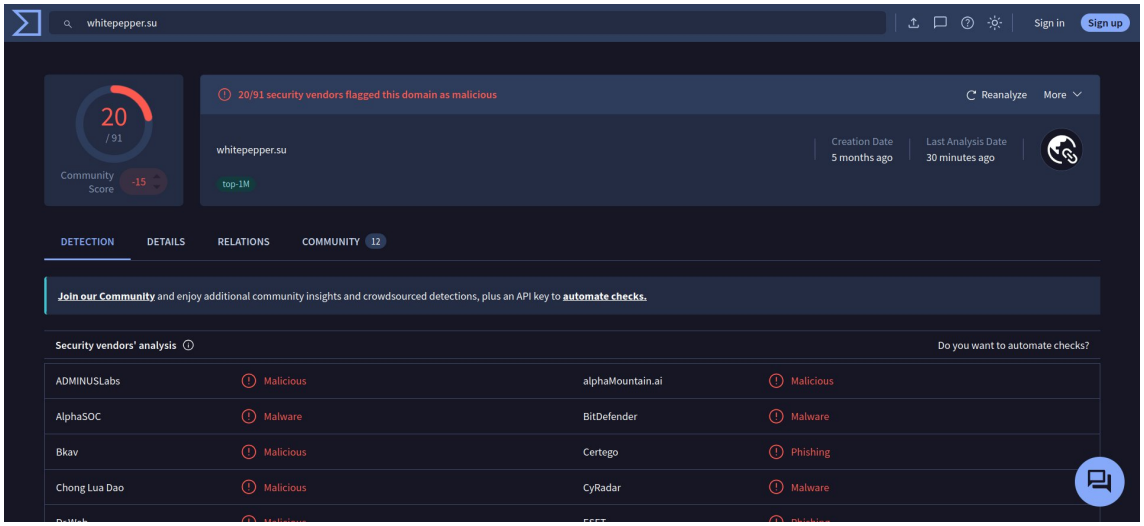
(Figura 8: Segunda parte del resultado del filtro TLS Client Hello, mostrando el dominio whitepepper[.]su con patrón de beaconing masivo múltiples conexiones regulares cada 1-2 segundos junto con los dominios holiday-forever[.]cc y communicationfirewall-security[.]cc.)

8.3 Identificación de la infraestructura de mando y control (C2)

Los dominios identificados en el apartado anterior fueron sometidos a verificación en la plataforma de inteligencia de amenazas VirusTotal con el fin de acreditar su naturaleza maliciosa y determinar su rol dentro de la infraestructura del atacante. El dominio media[.]megafilehub4[.]lat, contactado por el equipo víctima a los 45 segundos del inicio de la captura con carácter previo al inicio del beaconing C2, fue el primero en ser verificado por su posible papel como vector de descarga del malware.

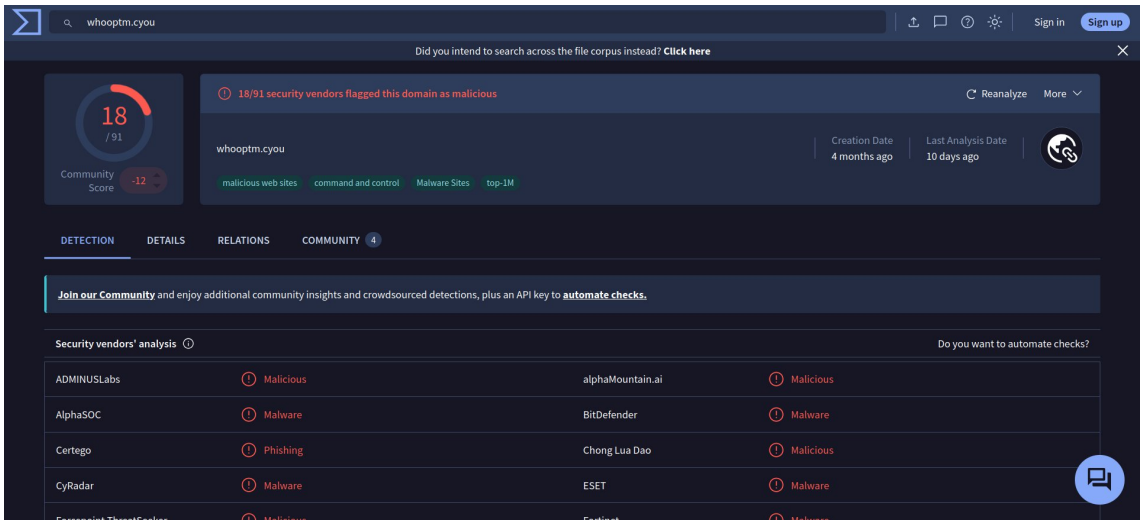


(Figura 9: Análisis del dominio media[.]megafilehub4[.]lat en VirusTotal. 8 de 91 motores de seguridad lo clasifican como malicioso, con categoría "Information Technology, Malicious". Dominio creado 5 meses antes del incidente.)

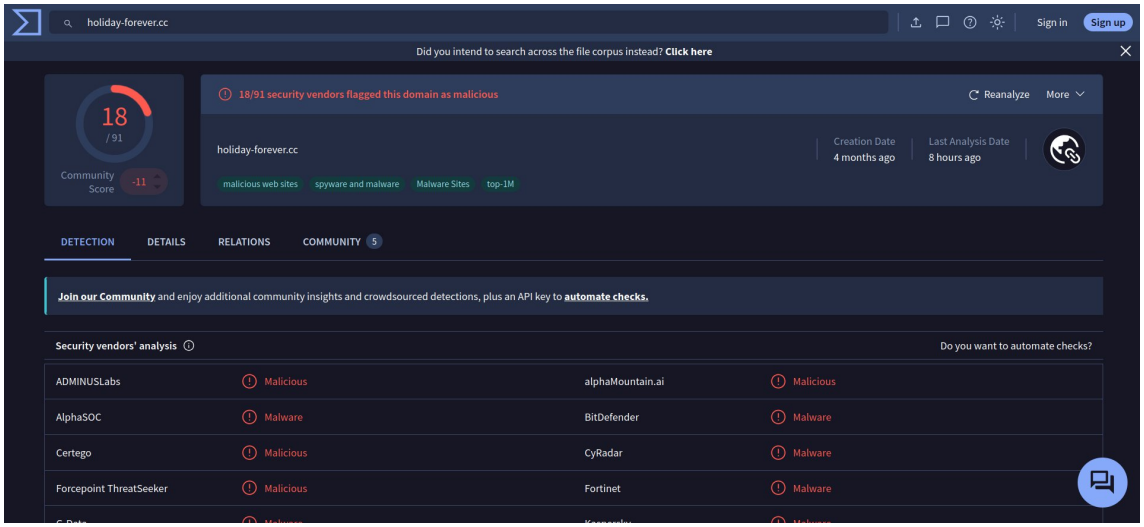


(Figura 10: Análisis del dominio whitepepper[.]su en VirusTotal. 20 de 91 motores lo clasifican como malicioso con una puntuación comunitaria de -15. Dominio creado 5 meses antes del incidente.)

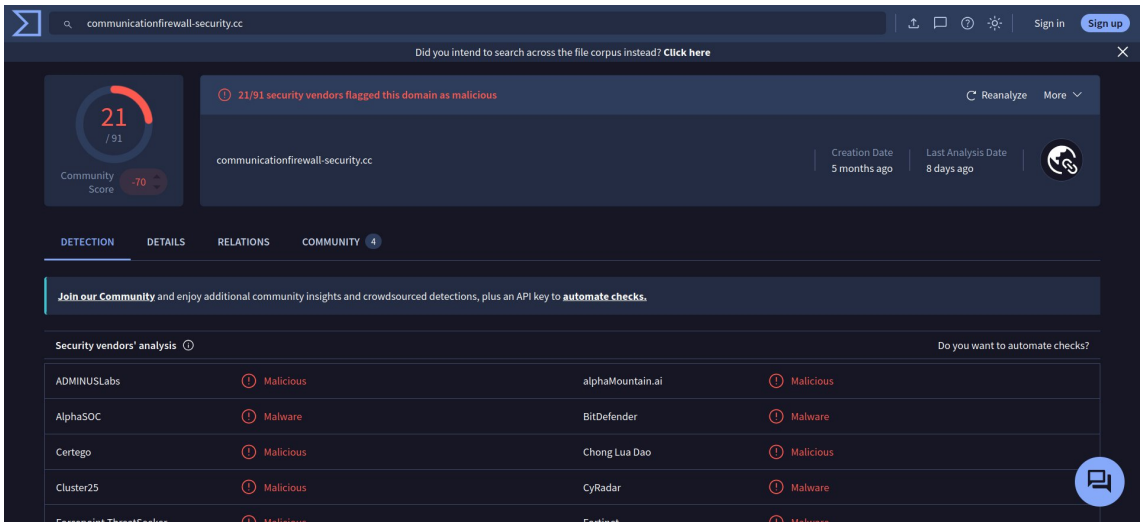
La verificación de los dominios adicionales detectados en el tráfico TLS confirmó la naturaleza maliciosa de la totalidad de los dominios sospechosos identificados en la captura.



(Figura 11: Análisis del dominio whooptm[.]cyou en VirusTotal. 18 de 91 motores lo clasifican como malicioso, con las categorías explícitas "command and control" y "Malware Sites". Puntuación comunitaria de -12.)



(Figura 12: Análisis del dominio holiday-forever[.]cc en VirusTotal. 18 de 91 motores lo clasifican como malicioso, con las categorías "spyware and malware" y "Malware Sites". Puntuación comunitaria de -11.)



(Figura 13: Análisis del dominio communicationfirewall-security[.]cc en VirusTotal. 21 de 91 motores lo clasifican como malicioso, con una puntuación comunitaria de -70, la más negativa de toda la infraestructura identificada.)

El siguiente cuadro resume la infraestructura maliciosa completa identificada en la captura:

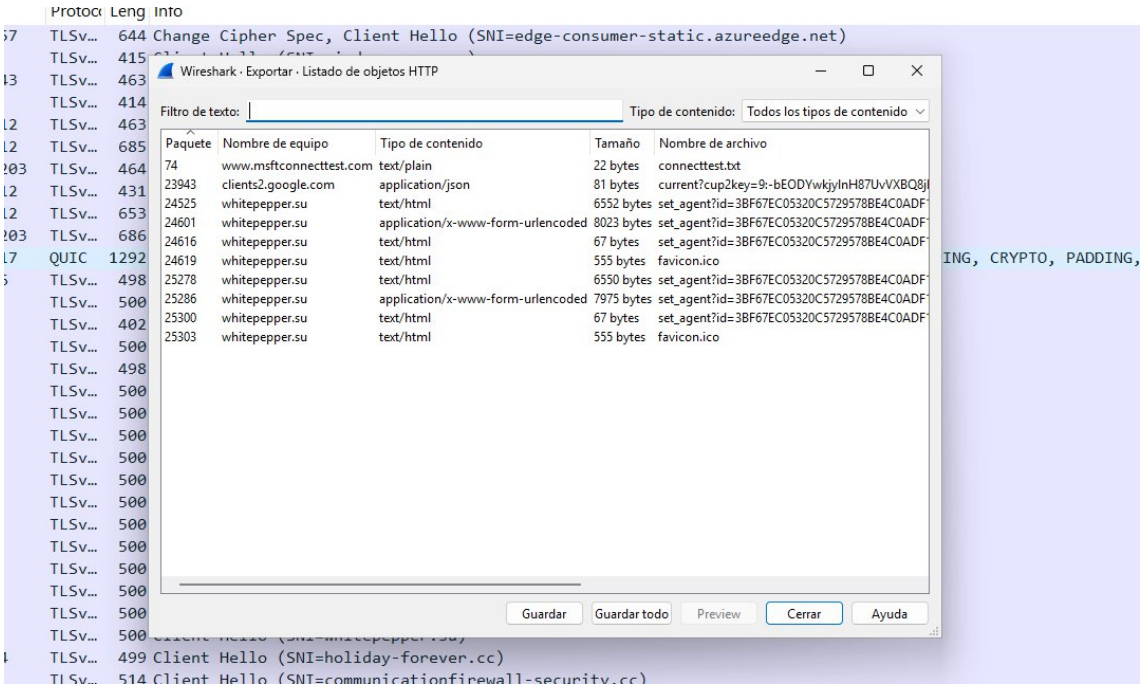
Dominio	IP
whitepepper[.]su	153[.]92[.]1[.]49
communicationfirewall-security[.]cc	104[.]21[.]9[.]36
whooptm[.]cyou	62[.]72[.]32[.]156
holiday-forever[.]cc	80[.]97[.]160[.]24
media[.]megafilehub4[.]lat	104[.]21[.]48[.]156

El análisis cronológico de las conexiones TLS revela el patrón de infección:

- A los 45 segundos del inicio de la captura se produce la primera conexión al dominio media[.]megafilehub4[.]lat, vector probable de la descarga del malware por HTTPS
- A los 90 segundos se conecta con whooptm[.]cyou
- A los 92 segundos se inicia la comunicación HTTPS con whitepepper[.]su
- Y a los 95 segundos comienza el beaconing HTTP activo con el servidor C2, que se mantiene de forma regular cada 1-2 segundos durante todo el resto de la captura.

8.4 Análisis estadístico del tráfico y confirmación de la amenaza

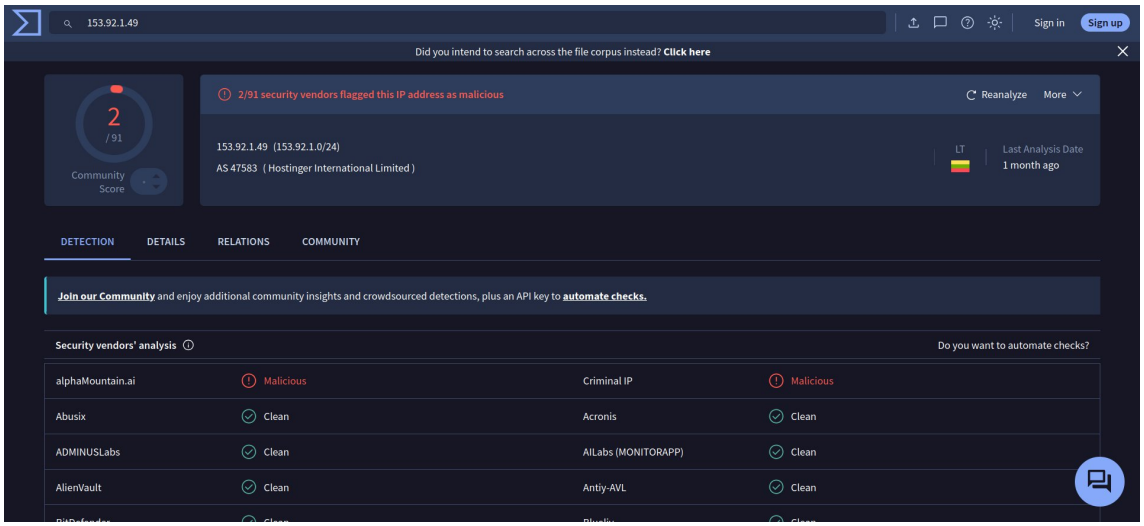
Con el fin de verificar exhaustivamente la ausencia de archivos maliciosos descargados por HTTP, se utilizó la función Exportar objetos → HTTP de Wireshark, que reconstruye y lista la totalidad de los objetos HTTP ensamblados a partir del tráfico capturado. El inventario resultante confirma que los únicos objetos HTTP presentes son: la comprobación de conectividad NCSI (22 bytes), la respuesta de actualización de Google (81 bytes) y los objetos generados por la comunicación C2 con whitepepper[.]su, entre los cuales destacan dos cuerpos de petición POST de 8.023 bytes y 7.975 bytes respectivamente, correspondientes a los datos de credenciales exfiltrados.



(Figura 14: Listado de objetos HTTP reconstruidos por Wireshark mediante Exportar objetos → HTTP sobre EVID-NET-01.pcap. Se confirma la ausencia de ejecutables descargados por HTTP y se evidencian los cuerpos POST con datos exfiltrados al C2.)

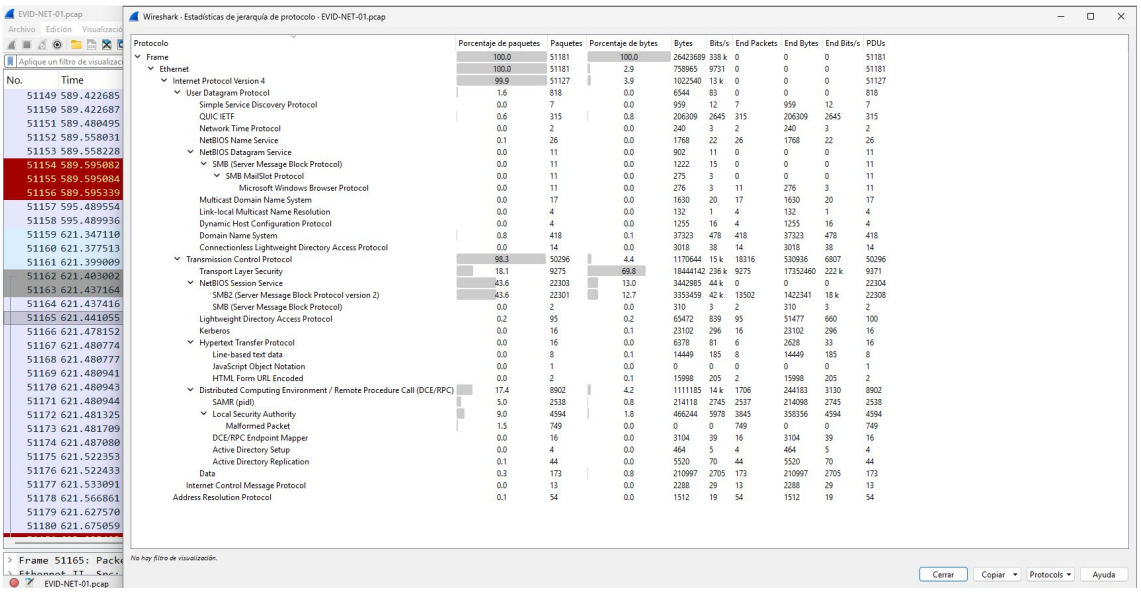
La dirección IP 153[.]92[.]1[.]49, correspondiente al servidor C2 principal, fue verificada directamente en VirusTotal. La menor tasa de detección de la IP en comparación con el dominio whitepepper[.]su es característica de los proveedores de alojamiento legítimos empleados de forma abusiva por actores maliciosos: los motores de reputación son más lentos en penalizar IPs

compartidas. El servidor pertenece al sistema autónomo AS47583 (Hostinger International Limited), con localización en Lituania.



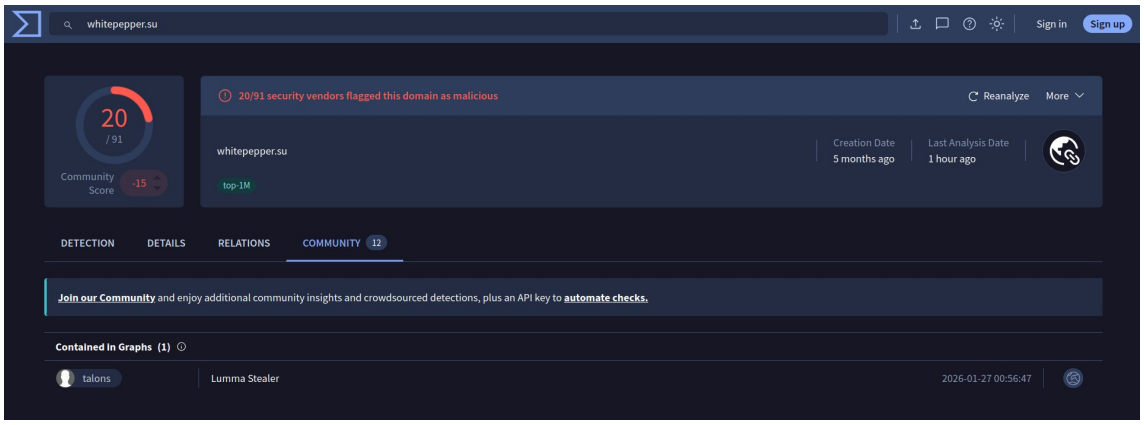
(Figura 15: Análisis de la dirección IP 153[.]92[.]1[.]49 en VirusTotal. 2 de 91 motores la clasifican como maliciosa. La IP pertenece al AS47583 (Hostinger International Limited), con geolocalización en Lituania.)

El análisis estadístico del tráfico mediante la función Estadísticas → Jerarquía de protocolos de Wireshark ofrece una visión global de la composición del PCAP y contextualiza los hallazgos del análisis. Los 51.181 paquetes capturados (26,4 MB) presentan una distribución característica: el protocolo TLS representa el 69,8% del volumen de bytes con tan solo el 18,1% de los paquetes, lo que refleja el alto volumen de tráfico HTTPS cifrado en el que se enmarca tanto la descarga del malware como las comunicaciones adicionales de C2. El protocolo HTTP, en contraste, apenas representa 16 paquetes (0,0%), confirmando que la actividad HTTP visible en el PCAP se limitaba exclusivamente a la comunicación C2 con whitepepper[.]su. El tráfico SMB2 (43,6% de los paquetes) y el DCE/RPC (17,4%) corresponden a las operaciones legítimas del equipo con el Controlador de Dominio.



(Figura 16: Estadísticas de jerarquía de protocolo de EVID-NET-01.pcap generadas por Wireshark. Se observa el dominio del protocolo TLS (69,8% del volumen de bytes) y la presencia mínima de HTTP (16 paquetes), junto con tráfico legítimo de dominio Windows (SMB2, DCE/RPC, Kerberos, LDAP).)

La atribución definitiva a la familia de malware Lumma Stealer se obtuvo mediante la consulta de la pestaña Community de VirusTotal para el dominio whitepepper[.]su. En dicha pestaña consta que el dominio fue incluido en un grafo de amenazas etiquetado explícitamente como "Lumma Stealer" por el usuario "talons", con fecha 2026-01-27 a las 00:56:47 UTC: el mismo día del incidente registrado en la captura. Este hallazgo cierra el círculo entre la firma IDS que detonalizó el caso (ET MALWARE Lumma Stealer Victim Fingerprinting Activity), la infraestructura C2 identificada en el PCAP (whitepepper[.]su, 153[.]92[.]1[.]49) y la familia de malware confirmada por inteligencia comunitaria.



(Figura 17: Pestaña Community del dominio whitepepper[.]su en VirusTotal, mostrando su inclusión en un grafo de amenazas clasificado como "Lumma Stealer" con fecha 2026-01-27, coincidente con el día del incidente analizado.)

9

Conclusiones periciales

Del análisis forense digital realizado sobre el volcado de tráfico de red (EVID-NET-01.pcap) del segmento 10.1.21.0/24 del dominio win11office[.]com, se establecen las siguientes conclusiones:

Primera.

El equipo infectado ha sido identificado de forma inequívoca a partir de los artefactos de red presentes en la captura. Mediante el análisis del intercambio DHCP (frame 3) y de la solicitud de autenticación Kerberos AS-REQ (frame 214), se determinó que el equipo comprometido presenta la dirección IP 10.1.21.58, la dirección MAC 00:21:5d:c8:0e:f2 (fabricante Intel), el nombre de host DESKTOP-ES9F3ML y la cuenta de usuario de Windows gwyatt, perteneciente al dominio WIN11OFFICE.

Segunda.

El análisis del tráfico HTTP confirma que el equipo infectado estableció comunicaciones activas con el servidor de mando y control whitepepper[.]su (IP 153[.]92[.]1[.]49) mediante peticiones al endpoint /api/set_agent. La presencia de peticiones POST con el parámetro act=log y cargas útiles de 8.023 y 7.975 bytes respectivamente, cuyos bytes iniciales PK evidencian compresión en formato ZIP, acredita que la exfiltración de datos robados hacia el servidor C2 se encontraba activa y en curso en el momento de la captura.

Tercera.

No se ha podido recuperar el archivo malicioso descargado por el usuario a partir de la captura de red, al haberse producido la descarga mediante el protocolo HTTPS, cuyo contenido se transmite cifrado y no es accesible en el PCAP. El análisis del tráfico TLS Client Hello identifica el dominio media[.]megafilehub4[.]lat (IP 104[.]21[.]48[.]156) como el origen más probable de la descarga, al ser el primer dominio externo sospechoso contactado por el equipo víctima, con carácter previo al inicio de las comunicaciones C2, y al estar catalogado por 8 de 91 motores de VirusTotal como sitio de distribución de malware.

Cuarta.

Se han identificado y acreditado cinco dominios maliciosos que constituyen la infraestructura de mando y control de la amenaza. El dominio principal whitepepper[.]su actúa como servidor C2 activo con patrón de beaconing regular confirmado, con 20 de 91 detecciones en VirusTotal y puntuación comunitaria de -15. Los dominios communicationfirewall-security[.]cc (21/91, comunidad -70), whooptm[.]cyou (18/91, comunidad -12, categoría explícita *command and control*), holiday-forever[.]cc (18/91, comunidad -11) y media[.]megafilehub4[.]lat (8/91) conforman la infraestructura complementaria de la campaña. Todos los dominios fueron registrados en los cuatro o cinco meses previos al incidente.

Quinta.

La atribución de la amenaza a la familia de malware **Lumma Stealer** queda acreditada por la convergencia de tres fuentes independientes: la firma del Sistema de Detección de Intrusiones que detonó el caso (ET MALWARE Lumma Stealer Victim Fingerprinting Activity), el patrón de tráfico observado en el PCAP registro de víctima mediante /api/set_agent y exfiltración de credenciales de navegadores web y la clasificación explícita del dominio C2 principal whitepepper[.]su dentro de un grafo de amenazas etiquetado como *Lumma Stealer* por la comunidad de VirusTotal con fecha 27 de enero de 2026, coincidente con el día del incidente.

9.1 Cronología

Suceso	Tiempo en captura	Hora aproximada (UTC)
El equipo DESKTOP-ES9F3ML (usuario gwyatt) completa el intercambio DHCP y obtiene la dirección IP 10.1.21.58 del servidor 10.1.21.1.	t = 0 s	27/01/2026 23:05h
El equipo establece sesión Kerberos con el Controlador de Dominio 10.1.21.2, confirmando la autenticación del usuario gwyatt en el dominio WIN11OFFICE.	t ≈ 2 s	27/01/2026 23:05h
Primera conexión TLS hacia media[.]megafilehub4[.]lat (IP 104[.]21[.]48[.]156), dominio catalogado como sitio de distribución de malware. Vector probable de descarga del archivo malicioso mediante HTTPS.	t ≈ 45 s	27/01/2026 23:05h
Primera conexión TLS hacia whooptm[.]cyou (IP 62[.]72[.]32[.]156), dominio catalogado como *command and control* por VirusTotal.	t ≈ 90 s	27/01/2026 23:06h
Primera conexión TLS hacia whitepepper[.]su (IP 153[.]92[.]1[.]49), servidor C2 principal de la campaña	t ≈ 92 s	27/01/2026 23:06h

Lumma Stealer.		
Inicio del beaconing HTTP activo hacia whitepepper[.]su. El malware comienza a registrar la víctima mediante peticiones GET al endpoint /api/set_agent con parámetros id, token y agent (Chrome, Edge).	t ≈ 95 s	27/01/2026 23:06h
El malware ejecuta peticiones POST al endpoint /api/set_agent?act=log sobre whitepepper[.]su, exfiltrando las credenciales robadas comprimidas en formato ZIP (cargas de 8.023 y 7.975 bytes). La exfiltración de datos queda confirmada.	t ≈ 103 s	27/01/2026 23:07h
El equipo contacta con holiday-forever[.]cc (IP 80.97.160.24) y communicationfirewall-security[.]cc (IP 104.21.9.36), dominios adicionales de la infraestructura maliciosa.	t ≈ 123-127 s	27/01/2026 23:07h
El beaconing hacia whitepepper[.]su continúa de forma regular cada 1-2 segundos hasta el final de la captura. Último paquete registrado.	t = 621 s	27/01/2026 23:15h

10

Anexo

10.1 Identificación del caso

Nº Expediente o Atestado	CASO2026-0131
Juzgado o autoridad solicitante	Departamento de Seguridad Corporativa
Fecha y hora de la intervención y análisis	31 de enero de 2026 - adquisición a las 09:15h (UTC)
Lugar de intervención	Centro de Operaciones de Seguridad (SOC) - Extracción lógica remota sobre el segmento LAN 10.1.21.0/24
Persona a la que se le interviene	Usuario gwyatt, equipo DESKTOP-ES9F3ML, segmento 10.1.21.0/24, dominio win11office[.]com
Perito interviniente	Ilian Lubenov

10.2 Descripción de los indicios

ID de la evidencia	EVID-NET-01
Tipo de dispositivo	Volcado de tráfico de red (Packet Capture)
Marca y modelo	N/A - Appliance de red (Sensor IDS / Switch Core)
Capacidad Nominal	25,9 MB
Número de serie	N/A
Conexión o Interfaz	Captura pasiva mediante puerto espejo (SPAN Port) en el nodo perimetral
Descripción	Volcado de tráfico de red continuo del segmento LAN 10.1.21.0/24 del dominio win11office[.]com, adquirido mediante exportación lógica del repositorio centralizado del SIEM el 31/01/2026 a las 09:15h (UTC), en modo de solo lectura
Notas:	N/A

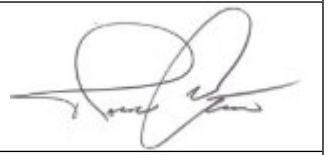
10.3 Verificación criptográfica (Hashes)

Dispositivo	SHA-256
Volcado de tráfico de red "EVID-NET-	F755444D0B6EAC847E07B73DEA0774084B232D8577F536547A12F39B959D7833

01.pcap"	

Resultado de la verificación: Coincidente (Verification OK)

10.4 Registro de traspaso (Transfer logs)

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