



universidad
de león

Escuela de Ingenierías I.I.



Industrial, Informática y Aeroespacial

**MÁSTER UNIVERSITARIO EN
INVESTIGACIÓN EN CIBERSEGURIDAD**

Trabajo de Fin de Máster

ANÁLISIS DE RANSOMWARE COINLOCKER

ANALYSIS OF RANSOMWARE COINLOCKER

Autor: Javier del Amo Mateos

Tutor: Angel Manuel Guerrero Higueras

Cotutor: Alberto Miguel Diez

(Julio, 2025)

UNIVERSIDAD DE LEÓN

Escuela de Ingenierías I.I.

MÁSTER UNIVERSITARIO EN INVESTIGACIÓN EN CIBERSEGURIDAD

Trabajo de Fin de Máster

ALUMNO: Javier del Amo Mateos

TUTOR: Angel Manuel Guerrero Higueras

CO-TUTOR: Alberto Miguel Diez

TÍTULO: Análisis del Ransomware CoinLocker

CONVOCATORIA: Julio, 2025

RESUMEN:

Durante el pasado 2024 el número de ataques relacionados con el ransomware ha ido en aumento. Esta dinámica se lleva produciendo muchos años de manera consecutiva. Nuevos grupos de ransomware en constante aparición, engaños más sofisticados que, junto con la aparición de la inteligencia artificial, conforman un escenario perfecto para que el ransomware mantenga su rentabilidad, eficacia y persistencia en el tiempo. El mero hecho de sufrir un ataque de ransomware genera un elevado impacto tanto a nivel económico como reputacional, pudiendo comprometer gravemente la continuidad del negocio. Adicionalmente, las acciones que llevan a cabo estos grupos suelen incluir exfiltración de información sensible antes del proceso de cifrado, lo que permite incrementar la presión sobre la víctima junto con la amenaza explícita de divulgación pública de los datos sustraídos.

En el presente informe se realiza un análisis del ransomware CoinLocker, firma de la que no se cuenta con demasiada información y que comenzó a operar en el año 2015, tanto en entornos empresariales como en la nube.

Su objetivo principal es el mismo que expresa el propio concepto de ransomware, exigir una cantidad de 100BTC a cambio del descifrado de los archivos afectados. A pesar de no haber registros con casos públicos conocidos, ha demostrado contar con una capacidad de cifrado agresiva en diferentes entornos, aunque principalmente dirige sus esfuerzos a entornos Windows.

ABSTRACT:

During the past 2024 the number of ransomware-related attacks has been on the rise. This dynamic has been occurring consecutively for many years. New ransomware groups are constantly appearing, more sophisticated deceptions, and the emergence of artificial intelligence provide a perfect scenario for ransomware to maintain its profitability, effec-

tiveness and persistence over time. The mere fact of suffering a ransomware attack generates a high economic and reputational impact, and can seriously compromise business continuity. In addition, the actions carried out by these groups usually include the exfiltration of sensitive information before the encryption process, which increases the pressure on the victim together with the explicit threat of public disclosure of the stolen data.

This report provides an analysis of the CoinLocker ransomware, a firm about which not much information is available and which began operating in 2015, both in enterprise environments and in the cloud.

Its main objective is the same as the concept of ransomware itself, to demand 100BTC in exchange for decryption of the affected files. Although there are no known public cases on record, it has proven to have aggressive encryption capabilities in different environments, although it mainly targets Windows environments.

Palabras clave: Ransomware, CoinLocker, análisis forense, RaaS

Firma del alumno:	VºBº Tutor:	VºBº Co-Tutora:
		

Índice general

Índice de figuras	v
Índice de tablas	vii
Glosario de términos	viii
Introducción	1
1. Estudio del problema	7
1.1. El contexto del problema	7
1.2. El estado de la cuestión	9
1.2.1. Malware, el origen de todo	10
1.2.2. El Ransomware: orígenes, evolución y funcionamiento	14
1.2.3. La red TOR	23
1.2.4. TOR y los <i>Hidden Sites</i> relacionados con RaaS	25
1.2.5. TOR y el RaaS	28
1.2.6. Algoritmos criptográficos	33
1.2.7. Herramientas de descifrado	35
1.3. La definición del problema	35
2. Gestión de proyecto software	37
2.1. Alcance del proyecto	37
2.1.1. Definición del proyecto	37
2.1.2. Estimación de tareas y recursos	38
2.1.3. Presupuesto	39
2.2. Plan de trabajo	41
2.2.1. Identificación de tareas	41
2.2.2. Estimación de tareas	42
2.2.3. Planificación de tareas	44

2.3.	Gestión de recursos	45
2.3.1.	Especificación de recursos	46
2.3.2.	Asignación de recursos	46
2.4.	Gestión de riesgos	46
2.4.1.	Identificación de riesgos	46
2.4.2.	Análisis de riesgos	47
2.4.3.	Legislación y normativa	50
3.	Solución	52
3.1.	Descripción de la solución	52
3.2.	El proceso de desarrollo	53
3.2.1.	Análisis estático	53
3.2.2.	Análisis dinámico	62
3.2.3.	Herramientas utilizadas	72
4.	Evaluación	74
4.1.	Proceso de evaluación	74
4.1.1.	Forma de evaluación	74
4.1.2.	Casos de prueba	74
4.2.	Ánalisis de resultados	76
Conclusión		79
Lista de referencias		81
A. Seguimiento de proyecto fin de máster		90
A.1.	Forma de seguimiento	90
A.2.	Planificación inicial	91
A.3.	Planificación final	92
B. Control de versiones		93

Índice de figuras

1.1.	Usuarios atacados por ransomware, de noviembre de 2023 a octubre de 2024	9
1.2.	Disquete de 5½" de distribución de AIDS	15
1.3.	Mensaje de extorsión de AIDS Information	16
1.4.	Informe del CIAC sobre el denominado PC CYBORG AIDS del 19 de diciembre de 1989.	16
1.5.	Funcionamiento de la criptovirología	17
1.6.	The 2024 State of Malware & Ransomware Defense Report.	19
1.7.	Porcentaje de víctimas por países – 2024. Fuente: LAB52	20
1.8.	Cyber Security Report 2025 - Ransomware double-extortion groups, by percentage of total published victims in 2024.	21
1.9.	Datos mundiales de víctimas en 2024 desglosados por grupo de ransomware y trimestre.	22
1.10.	Lockbit 3.0 Leaked Data	26
1.11.	Publicación en la red TOR de empresa comprometida por ransomware Hive	26
1.12.	Grupo Akira en la red TOR	27
1.13.	Nota de rescata Blackcat con dirección de TOR	28
1.14.	LockBit Blog en su dirección TOR	30
1.15.	Ranion RaaS en su dirección TOR	31
1.16.	Condiciones de LockBit en su dirección TOR	32
2.1.	Diagrama de Gantt con la planificación de las tareas	38
2.2.	Diagrama de Gantt con la planificación de las tareas	44
3.1.	Resultados del programa ExeInfo PE relacionados con la muestra . .	54
3.2.	Resultados del programa ExeInfo PE relacionados con las secciones .	55
3.3.	Resultados del programa HxD con las cabeceras del archivo	56
3.4.	Resultados del programa HxD donde muestra la nota de rescate . .	57

3.5. Resultados del programa PEview donde muestra la fecha de compilación	58
3.6. Resultados del programa PEStudio donde muestra los strings	58
3.7. Resultados del programa Ghidra donde muestra la función AES <i>Encrypt</i>	59
3.8. Resultados del programa Ghidra donde muestra la nota de rescate . .	59
3.9. Resultados del programa Ghidra donde muestran las extensiones de ficheros a cifrar	60
3.10. Resultados de los motores de VT que han detectado la muestra como maliciosa	60
3.11. Resultado de detonar el fichero que contiene el ransomware	62
3.12. Resultados de la herramienta Process Explorer en cuanto a informa- ción del sistema	63
3.13. Resultados de la herramienta Process Explorer en cuanto a informa- ción de consumo de la CPU	64
3.14. Resultados de Any Run donde muestra la nota de rescate y la familia de ransomware (coinlocker)	65
3.15. Resultados de Any Run donde muestran las ejecuciones de la consola de Windows	66
3.16. Resultados de Any Run donde la ejecución de borrado puntos de restauración	67
3.17. Resultados de Any Run donde la ejecución de borrado de copias de seguridad utilizando WMIC	67
3.18. Resultados de Any Run donde la ejecución de borrado de copias de seguridad utilizando VSS Admin	68
3.19. Resultados de Any Run donde se muestran tácticas y técnicas rela- cionadas con MITRE ATTACK	68
3.20. Resultados de Joe Sandbox donde se muestra la creación del fichero con la nota de rescate	69
3.21. Resultados de Joe Sandbox donde se muestra el árbol de procesos que ejecuta el ransomware	70
3.22. Listado de archivos de prueba antes y después del cifrado	71
3.23. Extensión .tiff inexistente en código para cifrar	72
3.24. Fichero de texto antes y después del cifrado	72
4.1. Resultado del análisis de la muestra en ID Ransomware	78
A.1. Planificación incial	91
A.2. Planificación incial	92

Índice de tablas

2.1. Presupuesto de personal	40
2.2. Presupuesto de Hardware	40
2.3. Beneficio industrial	41
2.4. Presupuesto total	41
3.1. Principales Hashes de la muestra a analizar	53
3.2. Valores de los campos correspondientes al <i>Header</i>	61
3.3. Valores de la IP detectada por <i>Xcitium Verdict Cloud</i> como maliciosa	61
4.1. Porcentaje de detección de plataformas	74
4.2. Porcentaje de detección de plataformas	75
4.3. Datos mostrados en la nota de rescate	75
4.4. Consumos de diferentes detonaciones de la muestra	76

Glosario de términos

Catálogo de términos específicos del contexto del trabajo.

AES : Advanced Encryption Standard. Se trata de un estándar cifrado simétrico, el cual usa la misma clave tanto para cifrar como para descifrar.

ARPANET : *Advanced Research Projects Agency Network*. En español Red de Agencias de Proyectos de Investigación Avanzada, construida en 1969, era una red de computadoras cuyo objetivo era enviar datos militares y conectar a los principales grupos de investigación e instituciones académicas de los Estados Unidos.

CCN-CERT : Centro de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional y Centro Nacional de Inteligencia. Creado en el año 2006 como CERT Gubernamental Nacional español, sus funciones quedan recogidas en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia, el RD 421/2004 de regulación del CCN y en el RD 311/2022, de 3 de mayo, que regula el Esquema Nacional de Seguridad.

Ciberseguridad : Protección de los sistemas informáticos y de sus redes de comunicaciones, con el objetivo de mantener segura la información que procesan.

DDoS : *Distributed Denial-of-Service*. En español, ataque de denegación de servicio distribuido, es un tipo de ataque con fines maliciosos en los que el atacante sobrecarga un servidor con mucho tráfico de Internet para evitar el acceso de los usuarios del servicio.

DES : *Data Encryption Standard*. Es un algoritmo criptográfico, de tipo cifrado por bloque.

ENISA : *European Union Agency for Cybersecurity*. En español Agencia de la Unión Europea para la Ciberseguridad, es la encargada de garantizar la ciber-

seguridad de las comunicaciones y servicios de la administración comunitaria y nacional, y de los ciudadanos de la Unión Europea.

IA : Inteligencia artificial. Disciplina científica que se ocupa de crear programas informáticos que ejecutan operaciones comparables a las que realiza la mente humana, como el aprendizaje o el razonamiento lógico.

INCIBE : Instituto Nacional de Ciberseguridad, anteriormente Instituto de Tecnologías de la Comunicación (INTECO), es una sociedad que, actualmente, depende del Ministerio para la Transformación Digital y de la Función Pública a través de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, red académica y de investigación, profesionales, empresas y especialmente, para sectores estratégicos.

IoT : Abreviación del término en inglés *Internet of Things*. En español Internet de las Cosas, es un concepto que se refiere a la interconexión digital de objetos cotidianos, como relojes, cámaras de grabación, electrodomésticos, etc. mediante Internet.

MaaS : *Malware as a Service*. Malware como servicio, es un negocio ilegal que implica el alquiler de software malicioso cuyo fin es la ejecución de ataques cibernéticos.

NIST : *National Institute of Standards and Technology*. En español Instituto Nacional de Estándares y Tecnología, fue conocido como Oficina Nacional de Normas (NBS, por sus siglas en inglés *National Bureau of Standards*) entre los años 1901 y 1988. Se trata de una agencia de la Administración de Tecnología del Departamento de Comercio de los EEUU.

Phishing : se trata de una técnica mediante la cual un atacante suplanta a una entidad o servicio con el fin de robar las credenciales de acceso o datos bancarios de un usuario. Para perpetrar el engaño, se suele utilizar el correo electrónico o la mensajería instantánea los cuales contendrán un enlace malicioso y preparado para el robo de las credenciales.

RaaS : *Ransomware as a Service*. Conocido como Ransomware como Servicio, se trata de un modelo de negocio en el que los cibercriminales venden el código del ransomware a terceros, llamados afiliados, los cuales posteriormente lo utilizarán para realizar sus propios ataques.

RSA : debe su nombre a las iniciales de sus creadores Rivest–Shamir–Adleman. Es un estándar de cifrado asimétrico que usa un par de claves (pública y privada), para el intercambio seguro de claves y firmas digitales.

Spam : cualquier forma de comunicación no solicitada enviada de forma masiva. Normalmente se asocia al correo electrónico y se produce cuando se realizan envíos indiscriminadamente correos con fines publicitarios o maliciosos. También puede estar asociado a la mensajería instatánea, redes sociales o mensajes de voz (llamadas telefónicas).

Introducción

Pasado un cuarto del presente siglo XXI, nos hemos acostumbrado tanto a los avances tecnológicos que prácticamente los damos por supuestos. El elevado número de transacciones digitales de todo tipo que se acometen por segundo hace imperativo tratar con la ciberseguridad o con la protección de la información.

De una evolución digital presente a principios de siglo, hemos pasado a vernos inmersos en un proceso de grandes cambios protagonizados por una era tecnológica en la que la Inteligencia Artificial (en adelante IA), es protagonista del presente más cercano y, de manera más que probable, del futuro más próximo. De la adaptación a este constante proceso de cambio continuo dependerá la capacidad de defensa frente a las amenazas, las cuales evolucionan al mismo ritmo que este desarrollo tecnológico.

Hablar de ciberataques en lenguaje coloquial es algo comúnmente relacionado con acciones maliciosas únicamente orientadas hacia grandes corporaciones o relacionadas con actos de espionaje gubernamental. Pero hackear una gran multinacional o acceder a los servidores centrales del FBI es algo que dejaremos para las películas. Sin embargo, si existen situaciones relacionadas con las brechas de seguridad que se producen en multitud de ámbitos que pueden abarcar desde el mundo industrial, la administración pública, las pymes o incluso, los particulares. El desarrollo tecnológico está directamente relacionado con el crecimiento, distribución y sofisticación de las amenazas.

La aparición y uso de diferentes sistemas operativos, entornos industriales con dispositivos del conocido como Internet de las Cosas (en adelante IoT por sus siglas en inglés de *Internet of the Things*), el desarrollo de la IA o la interconectividad global existente a través de un smartphone, han llevado a los ciberdelincuentes a desarrollar un amplio elenco de código malicioso conocido como Malware y orientado a comprometer los diferentes sistemas para la obtención ilegítima de información. Esto hace aun más necesaria la creación de estrategias de defensa orientadas a

proteger la integridad, disponibilidad o confidencialidad de la información, principal activo tanto de empresas como de individuos.

El presente Trabajo de Fin de Máster (TFM), pretende analizar la situación actual tanto a nivel de amenazas como de análisis de las mismas, ya sea en entornos del ámbito empresarial o doméstico, comprendiendo y entendiendo las técnicas o tácticas utilizadas por los atacantes de cara a desarrollar estrategias de defensa útiles y efectivas. Bajo esta premisa, se presenta un análisis estático y dinámico del ransomware CoinLocker orientado a reunir toda la información necesaria que identifique las características propias y comportamiento de su código.

Planteamiento del problema

“Conoce a tu enemigo” es un dicho que proviene del libro *El arte de la guerra* [72] de Sun Tzu (también conocido como Maestro Sun), famoso estratega militar chino. Si hacemos propias estas palabras y las encajamos en el contexto que queremos desarrollar, podríamos decir que "para poder combatir y prevenir el Ransomware, primero hay que conocerlo".

Según un informe de Rapid 7 Labs [57], solo en el primer semestre de 2024 se identificaron más de 2.570 incidentes de ransomware, lo que equivale a una media de 14 incidentes diarios, esto, sin tener en cuenta aquellos que no han sido denunciados, lo que a buen seguro incrementaría estas cifras de manera considerable. Por otro lado, la plataforma Wired [?] publica datos aportados por Allan Liska, analista de *threat intelligence* de la compañía Recorded Future, en donde se estima que el número de ataques en todo 2024 fue de 4634, frente a 4400 de 2023.

Este volumen de ataques supone un problema cuantioso para todo tipo de empresas u organizaciones, ya sean del ámbito público o privado. Hacerse con la información que albergan se ha convertido el principal objetivo de este tipo de ciberdelincuentes.

Además, todos los tipos de malwares evolucionan y el ransomware no es una excepción. Tratan de ir mutando para evitar ser detectado por los sistemas antivirus por lo que conocer muy a fondo a nuestro enemigo, hará que podamos combatirlo con mayor eficacia. No en vano, Security Brief [63] publica que 80 grupos de ransomware estaban activos en el primer trimestre de 2025, de los cuales 16 son nuevos desde el 1 de enero.

En esta línea, la principal motivación de este trabajo es estudiar un tipo de amenaza de cara a poder desarrollar estrategias de protección de la información más efectivas y actuales.

Objetivos

El objetivo de este TFM será estudiar el Ransomware CoinLocker, obteniendo toda la información posible en base a las siguientes metas:

1. Estudio general del problema y desarrollo de la situación actual, en base a diferentes desarrollos del Ransomware as a Service (RaaS). En este sentido, para poder establecer un contexto genérico, se seguirán las siguientes líneas de investigación:
 - Origen y evolución y funcionamiento del Malware y de su variante Ransonware.
 - Análisis de las principales técnicas de engaño utilizadas y vectores de entrada a sistemas.
 - Análisis de los principales grupos de ransomware, cómo operan o dónde publican la información (red TOR).
 - Análisis de algoritmos de cifrado utilizados por este tipo de amenazas y herramientas de descifrado.
2. Análisis del marco normativo relacionado con el actual proyecto.
3. Análisis estático de la muestra de cara a extraer del binario toda la información posible sin que sea necesaria su ejecución.
4. Análisis dinámico de la muestra empleando entornos virtualizados y técnicas de *sandboxing* (uso de entornos controlados), de cara a poder determinar su comportamiento, establecer cómo cifra los archivos o el tiempo de ejecución, e identificar cualquier otro tipo de información adicional que pueda ser relevante.
5. Identificar los posibles Indicadores de Compromiso (en adelante IoC, por sus siglas en inglés "Indicators of Compromise").
6. Posibles líneas de investigación futura y desarrollo de medidas de defensa efectivas contra el ransomware, basadas en el análisis realizado de la muestra.

Metodología

La metodología utilizada para el desarrollo del actual proyecto será Scrum, método de gestión de proyectos ágil orientada a estructurar y gestionar el trabajo de manera colaborativa, centrándose ciclos de vida iterativos (*sprints*) e incrementales, realizando entregas del trabajo periódicas para conseguir una versión estable y mejorada del proyecto.

Esta metodología permitirá que el proyecto sea más fácil de gestionar ya que, la recolección de trabajo se realizará con más frecuencia y proporcionará una gran adaptación ante cualquier cambio que pudiera derivarse del proceso de investigación o del análisis de la muestra de ransomware.

Para la aplicación de esta metodología en el presente proyecto se han establecido 4 roles principales:

- *Product Owner*: representante del cliente y responsable de velar por los intereses del negocio. Definirá los requisitos del producto y los objetivos para su obtención. En este caso será Javier del Amo Mateos.
- *Scrum Master*: será el encargado de ofrecer ayuda, dar soporte y resolver los problemas que pueda tener el equipo de desarrollo (*Scrum Team*) para lograr las metas y objetivos que se hayan propuesto. En este caso será D. Ángel Manuel Guerrero Higueras.
- Equipo de desarrollo (*Scrum Team*): equipo encargado del desarrollo y entrega tanto de cada sprint, como del producto final al cliente. Para lograr esta labor, únicamente se contará con Javier del Amo Mateos.
- *Stakeholders*: entidad que encarga el proyecto. Su participación se reduce únicamente a las reuniones previas, ya sean telemáticas o presenciales, que servirán para establecer y definir los estándares necesarios tanto para el desarrollo del proyecto como para la presentación final. En este caso, será la Universidad de León.

Teniendo en cuenta cómo se organizan los proyectos bajo la metodología Scrum, hay que definir y establecer los eventos tanto de entrega como de evaluación, los cuales serán:

- Sprint: medida de tiempo determinado en la que se desarrolla el trabajo establecida (entregable).

- Reunión de planificación de cada Sprint (*Sprint Planning Meeting*): reunión que se llevará a cabo al inicio de cada sprint. En ella se acordarán las tareas a acometer y cómo se organizarán de cara a contar con una ejecución eficiente.
- Daily (reunión diaria): breve reunión diaria en la que se describe el trabajo realizado en la jornada previa y la previsión de trabajo a ejecutar en la actual. En esta reunión se ponen de manifiesto los problemas que hubieran podido surgir de cara a su resolución conjunta.
- Weekly (reunión semanal): reunión semanal de corta duración donde se expone con el equipo el trabajo realizado en la semana en curso (se realiza cada viernes), de cara a poner en común los posibles problemas que hubieran podido surgir en su desarrollo.
- Revisión del Sprint (*Sprint review*): reunión que se realiza al finalizar cada sprint, en la que el Product Owner revisará si el trabajo está correcto o si este se ha completado. Retrospectiva del Sprint (*Sprint Retrospective*): al igual que la anterior, se realiza al finalizar cada sprint para poner en manifiesto las posibles mejoras de cara a los futuros sprints.

Adicionalmente, Scrum también cuenta con una serie de bloques que forman parte de su ciclo de vida y que incluyen las funcionalidades necesarias para el desarrollo del proyecto que se está planificando. En este caso serán las siguientes:

- *Product Backlog* o Pila del Producto: necesidades del cliente representadas en el alcance general y las prioridades del producto.
- *Sprint Backlog* o Pila de Sprint: trabajo que el equipo deberá completar en cada Sprint. Destacar que esta división en entregables será inamovible una vez iniciado la sesión de trabajo.

En definitiva, se utiliza la metodología Scrum ya que está orientada al desarrollo de proyectos cambiantes y de continua evolución o mejora, que requieren de una gran capacidad de adaptación a los cambios del ciclo de vida del proyecto.

Las sprints han tenido lugar cada 2 semanas con su correspondiente reunión, cuyo objetivo fue exponer posibles mejoras, resolver dudas de cara a solventar algún problema y planificar el siguiente.. Adicionalmente también se realizó una reunión de planificación inicial y una final, de revisión general. Concluida esta, se realizaron una serie de mejoras que no formaban parte de la planificación ni de los sprints.

Estructura del trabajo

Este apartado está dedicado a definir cada una de las secciones del proyecto de cara a facilitar la lectura del presente documento, detallando el contenido de cada apartado. En esta línea, la división se ha realizado en base a los siguientes capítulos:

- Introducción: exposición del planteamiento que ha llevado al desarrollo del proyecto, a la estructura de los objetivos planteados y la metodología bajo la cual se ha llevado a cabo.
- Capítulo 1. Estudio del problema: en este capítulo se detalla el contexto general de la cuestión planteada, estudio del Malware como precursor del Ransomware, origen, evolución y funcionamiento del Ransomware, técnicas de engaño, grupos o familias de ransomware, RAAS, algoritmos criptográficos y herramientas de descifrado.
- Capítulo 2. Gestión del proyecto. En este capítulo se desarrolla la estimación de tareas y recursos, el presupuesto y plan de trabajo a realizar. También cuenta con una identificación y análisis de riesgos asociados al mismo.
- Capítulo 3. Solución. En este capítulo se describe la solución y el proceso de desarrollo que incluye el análisis estático y dinámico de las muestras así como una descripción de las herramientas utilizadas.
- Capítulo 4. Evaluación. Apartado donde se expone una evaluación y una comparativa de los resultados obtenidos en los análisis del apartado anterior.
- Capítulo 5. Conclusiones. Exposición de ideas resultantes de los resultados de la investigación, principales problemas que han surgido y previsiones y futuras líneas de investigación.

Capítulo 1

Estudio del problema

Para poder ahondar en la problemática que rodea al planteamiento que se pretende desarrollar, en primer lugar, se debe conocer cuáles son los aspectos genéricos sobre los que se basa el ransomware. Esto implica ser conscientes de cómo afecta al funcionamiento diario de una compañía, cuáles son los principales tipos que operan en la actualidad, qué grupos están detrás de su desarrollo y explotación, cómo se lleva a cabo la extorsión o qué vectores de ataque son los más utilizados para perpetrar el robo de información.

1.1. El contexto del problema

El ransomware ha pasado de ser una amenaza esporádica a convertirse en un adversario implacable. En el año 2025 se puede asegurar que los ataques de ransomware no son incidentes aislados, sino que se trata de un tipo de ataque que está a la vanguardia y que ocurre constantemente. Los grupos de cibercriminales que están detrás de estos ataques son capaces de orquestarlos de manera múltiple y sucesiva, explotando todo tipo de vulnerabilidades en cualquier organización, con independencia del sector en el que operen o el tamaño: sanidad (ciberataque al Hospital Clinic de Barcelona¹) [16], educación (Un presunto hacker amenaza con tener miles de

¹<https://www.clinicbarcelona.org/prensa/ultima-hora/ciberataque-al-hospital-clinic-de-barcelona>

datos de estudiantes y familiares de la web de Educacyl²) [12], servicios (El Grupo Santillana sufre un ataque de 'ransomware'³) [47], por poner algunos ejemplos.

Además, en los últimos años, han aparecido grupos que utilizan el ransomware como herramienta de doble funcionalidad: por un lado, con fines económicos (la obtención del pago por el rescate de los archivos cifrados), y por otro, con fines estratégicos y geopolíticos. Prueba de ello es que, según publica el informe elaborado por el equipo de LAB52 de S2GRUPO [61] "Panorama del Ransomware 2025", el grupo ruso APT44 habría utilizado el ransomware no solo para la obtención de rescates, sino también para destruir datos en ataques dirigidos contra infraestructuras críticas en Ucrania y Polonia. En Corea del Norte, grupos como Moonstone Sleet han utilizado ransomware personalizado (FakePenny) para robar información confidencial y generar ingresos ilícitos para financiar actividades estatales. Grupos como ChamelGang, alineados con China, han utilizado el ransomware para encubrir operaciones de ciberespionaje.

Por otro lado, según se revela en el informe de Semperis [65] "2024 Ransomware Risk Report", el 74 % de las víctimas de las víctimas de ransomware fueron atacadas varias veces. Si bien es cierto que hubo países e industrias más propensos a sufrir ataques posteriores, no quita para que, en general, más de la mitad de las empresas encuestadas fueron vulneradas con éxito dos o más veces, incluso, en ocasiones, en el mismo día.

Otro de los datos que revela dicho informe, es que el 78 % de las empresas que sufrieron un ataque de ransomware pagaron el rescate. En los últimos 12 meses, el 32 % realizó 4 o más pagos (en Alemania, esta cifra ascendió casi el 50 %). Cerca del 10 % pagaron más de 600.000 dólares solo en concepto de rescate. Esto conduce a pensar que los costes del ransomware, se están disparando.

Hay que tener en cuenta que el 35 % de las organizaciones que pagaron el rescate, no recibieron las claves de descifrado o no pudieron recuperar sus activos o información secuestrada. Además, muchas empresas sufrieron otro tipo de daños a largo plazo aunque pagaran. Según el informe de Veam "Ransomware Trends 2024" [73], el 54 % de los datos cifrados derivados de un ataque de ransomware, fueron recuperables. Esta estadística implica que hay un 46 % que no se pudo recuperar. Este

²<https://cadenaser.com/castillayleon/2025/05/31/un-presunto-hacker-amenaza-con-tener-miles-de-datos-de-estudiantes-y-familiares-de-la-web-de-educacyl-radio-valladolid/>

³<https://www.lavanguardia.com/sociedad/20250325/10518060/grupo-santillana-sufre-ataque-ransomware-agenciaslv20250325.html>

estudio señala que ni el tamaño ni la ubicación de las empresas encuestadas tuvo especial relevancia en la recuperabilidad de los datos.

Según los datos emitidos en el informe "Kaspersky Security Bulletin 2024. Statistics" [41], desde noviembre de 2023 hasta el pasado octubre de 2024, se identificaron 26 nuevas familias de ransomware y 16.035 variantes diferentes. Además, tal y como se muestra en la Figura 1.1, durante dicho periodo se detectaron 303.298 ataques de ransomware a usuarios únicos. De ellos, 98.208 eran usuarios corporativos y 14.517 estaban asociados a pequeñas y medianas empresas.

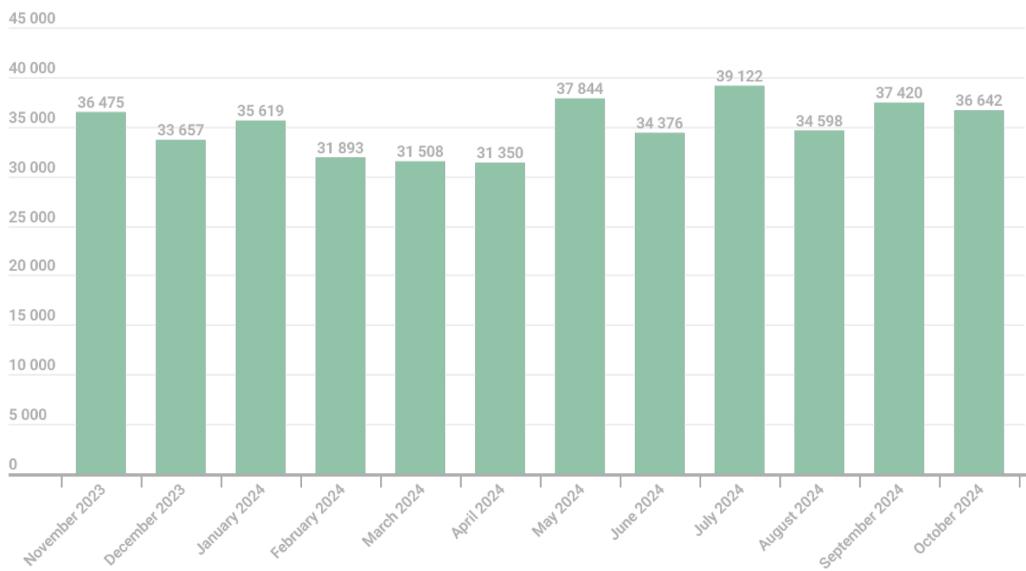


Figura 1.1: Usuarios atacados por ransomware, de noviembre de 2023 a octubre de 2024

Fuente: <https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2024/12/03153220/KSB-statistics-of-the-year-EN-final.pdf>

Teniendo en cuenta todos estos datos, es visible que sufrir un ataque de ransomware conlleva unos costes, tanto económicos como reputacionales, para cualquier compañía que se pueda ver afectada, con independencia de su tamaño o ubicación. Esta situación se agrava teniendo en cuenta lo que supone un éxito de un ataque de este tipo, la pérdida de información confidencial (especialmente preocupante si se trata del sector sanitario o de la administración pública).

1.2. El estado de la cuestión

Según el informe de la Agencia de la Unión Europea para la Ciberseguridad (ENISA), "Threat Landscape Report 2024" [23], de nuevo, se ha vuelto a detectar un incremento sustancial de los incidentes relacionados con el ransomware. Esto

reafirma que se trata de un tipo de ataque con un crecimiento continuo (ya en el informe de 2023 [22] se reflejaba un aumento significativo de este tipo de ataque), así como una amenaza constante.

Para poder obtener una visual completa de la cuestión que se plantea, es preciso comprender una serie de conceptos sobre el malware, sus variedades (ransomware), tipologías o cómo opera y quién está detrás. Para conseguirlo se realiza una exposición de términos y estadísticas necesarias para el desarrollo del estado de la cuestión.

1.2.1. Malware, el origen de todo

El malware es un término genérico que se utiliza para tipificar cualquier tipo de software malicioso, cuyo objetivo es dañar a la víctima, ya sea aprovechando cualquier tipo de vulnerabilidad de redes, dispositivos, servicios o simplemente, de su desconocimiento [49]. Su misión principal es la obtención de información (financiera, registros médicos, información personal, etc.).

En términos históricos, el primer virus informático que se conoce como tal fue desarrollado en el año 1971 por Bob Thomas [51] (programador de BBN Technologies). El elemento diferencial con respecto a la concepción actual que se tiene de la definición de malware, es que este desarrollo no se realizó con intenciones maliciosas ya que, su único objetivo, estaba relacionado con la capacidad de autorreplicación y movilidad del software en redes (por aquel entonces, la infraestructura que se utilizaba era ARPANET), por lo que sería un virus de tipo gusano. Su nombre fue Creeper y se consideraba código inofensivo ya que su único objetivo era dejar el siguiente mensaje en aquellas computadoras que conseguía infectar: "*I'm the creeper, catch me if you can!*" (Soy Creeper, ¡atrápame si puedes!).

Creeper era considerado más bien de una prueba de seguridad la cual, intentaba eliminarse a sí mismo del equipo anfitrión anterior al que había accedido por lo que, más que replicarse, su capacidad se basaba en saltar de una máquina a otra. Una de las principales consecuencias de la creación de este virus fue el desarrollo de Reaper [30], el primer antivirus, creado por Ray Tomlinson en 1972.

Siguiendo la línea temporal, en el año 1974 se creó el virus Wabbit. En este caso, sí tenía una intención maliciosa ya que se trataba de un programa de autoreplicación que realizaba múltiples copias de sí mismo en una misma computadora, reduciendo el rendimiento del sistema hasta que conseguía finalmente colapsarlo. El nombre de este virus obedece a su alta velocidad en la capacidad de replicación.

En el año 1975, el programador informático John Walker creó el que muchos consideran el primer troyano llamado Animal [27] escrito para un UNIVAC 1108 (si bien es cierto que, actualmente, existe un desacuerdo sobre si se trataba de un virus o un troyano). Se trataba de un juego en el que, a través de 20 preguntas, intentaba adivinar en qué animal estaba pensando el usuario. Adicionalmente, Walker, creó Prevade, que se instalaba junto a Animal el cual, examinaba los directorios disponibles realizando una copia de Animal en aquellos en los que no estuviera replicado. El motivo de considerarse troyano es que, dentro de un programa (Animal), coexistía otro cuya ejecución y acciones se perpetraban sin la aprobación del usuario.

En 1982, un joven estudiante de 15 años llamado Richard Skrenta (Rich), con el objetivo de gastar una broma a sus compañeros de instituto, desarrolló un sencillo programa al que llamó Elk Cloner [46], el cual, a través de un disquete, era capaz de dañar el sistema de arranque de los dispositivos Apple II. Es considerado como el primer virus informático de expansión real y descontrolada.

En el año 1986, los hermanos Basit y Amjad Farooq Alvi, gerentes de una tienda informática en Pakistán, crearon el primer virus compatible para IBM PC, denominado Brain [43]. En un intento por evitar la generación de copias ilegales de disquetes con software, Brain reemplazaba el sector de arranque de un disquete por el virus el cual, no provocaba daños ya que, únicamente, mostraba el siguiente mensaje relacionado con derechos de autor:

*Welcome to the Dungeon © 1986 Basit * Amjad (pvt) Ltd. BRAIN COMPUTER SERVICES 730 NIZAM BLOCK ALLAMA IQBAL TOWN LAHORE-PAKISTAN PHONE: 430791,443248,280530. Beware of this VIRUS.... Contact us for vaccination...*

Posteriormente, hubo más desarrollos de código malicioso: Gusano Morris (1988), Ghostball (1989), AIDS Trojan (1989), Chamaleon (1990), Staog (1996), CIH (1998), LOVEYOU (2000), etc. A partir de entonces el código malicioso ha ido en constante y continua evolución. Sirvan como ejemplo Conficker (2008), Zeus (2007-2011), Cryptolocker (2013), WannaCry (2017), Emotet (2018-2020) o Ryuk (2018-2020).

Este pequeño repaso histórico muestra que, en función de su funcionamiento, existen varios conceptos o tipologías de código malicioso, las cuales se exponen a continuación:

- **Gusanos:** se trata de uno de los tipos de malware más comunes cuya principal característica es que se replica sin requerir acción alguna por parte de nadie. Un ejemplo de este tipo sería el SQL Slammer. Su funcionamiento se basaba

en la generación aleatoria de direcciones IP a las que enviarse en busca de objetivos desprotegidos e sistemas antivirus. Su virulencia fue tal que, en el año 2003 fue capaz de infectar más de 75.000 equipos en tan solo 10 minutos aprovechándose de la vulnerabilidad de Microsoft MS02-039 [50].

- **Troyanos:** también conocidos como Caballos de Troya, es un software que intenta hacerse pasar como legítimo para provocar su ejecución. Suele utilizarse como puerta de entrada para que, posterior a su ejecución, el actor malicioso pueda acceder a datos del dispositivo infectado o como parte de una botnet. Un ejemplo de este tipo sería Qakbot (también conocido como Qbot o Pinkslipbot), se trata de un troyano bancario activo desde el año 2008 cuyo principal objetivo era el hurto de credenciales bancarias. La evolución inherente a su naturaleza, ha provocado que se combine con otros tipos de malware, provocando pérdidas económicas cuantitativas [35].
- **Adware:** debe su nombre a la contracción derivada de *Advertising-Supported Software* (software con publicidad), utiliza anuncios no deseados con el objetivo de recopilar información sobre los gustos de la víctima para venderlos a terceros anunciantes sin su consentimiento o personalizar la aparición de publicidad. Un ejemplo sería Fireball, aparecido en 2017, que afectó a más de 250 millones de equipos y a una quinta parte de las redes corporativas mundiales [40]. Su funcionamiento se basaba en hacerse con el navegador (impidiendo modificar su configuración), cambiando la página de inicio por una falsa e insertando anuncios molestos en las páginas web visitadas.
- **Spyware:** se trata de un tipo de malware que se oculta en el dispositivo para robar datos e información confidencial o monitorizar la actividad de quien lo sufre. Un ejemplo de este tipo sería CoolWebSearch, cuya primera aparición data del año 2003. Este spyware se aprovechaba de vulnerabilidades de Internet Explorer provocando cambios en su configuración del navegador y recolectando datos de navegación del usuario.
- **Ransomware:** también conocido como malware de rescate, se utiliza para bloquear o denegar el acceso al sistema o a los datos que se contienen en el mismo hasta que se realice el pago de un rescate solicitado por el atacante. Para llevar a cabo este bloque se utilizan mecanismos de cifrado y se solicita una contrapartida económica (normalmente en criptomonedas), para su descifrado, antes de una fecha concreta. Ejemplos de este tipo hay muchos ya que se trata de una amenaza persistente. Uno de ellos podría ser CryptoLocker, muy

presentes en los años 2013 y 2014, que se instalaba en el directorio Documentos, cifrando cierto tipo de archivos allí contenidos [2].

- **Virus:** se trata de un fragmento de código que se ejecuta cuando la aplicación en la que se encuentra, se abre. A partir de este momento, puede extraer datos o ejecutar otros ataques (por ejemplo DDoS o ransomware). Los virus permanecen inactivos hasta que son ejecutados y a partir de ese momento, puede propagarse o replicarse. Un ejemplo de este tipo de malware sería Stuxnet. Este virus apareció en el año 2010 provocando un fallo de las centrifugadoras de la planta nuclear iraní de Natanz [5].
- **Keyloggers:** debe su nombre a la abreviatura de *keystroke logging*, es una variedad de spyware que se utiliza para el robo de contraseñas, información bancaria o confidencial a través del registro de las pulsaciones de teclas que se realicen en la máquina infectada. Un ejemplo del uso de este tipo de malware lo protagonizó un joven estudiante de la Universidad de Iowa en el año 2017, tras ser arrestado y sentenciado a cuatro meses de prisión por utilizar keyloggers con el fin de robar credenciales para modificar sus calificaciones [71].
- **Botnets:** compuestas por bots (equipos zombies), que son máquinas infectadas por un malware que se puede controlar de forma remota. Estos dispositivos, una vez infectados, pasan a formar parte de una colección llamada botnet, la cual, pueden estar compuestas por millones de dispositivos infectados. SueLEN utilizarse para realizar ataques DDoS o enviar de forma masiva mensajes de spam o phishing. Un ejemplo sería Andrómeda, botnet que afecta a equipos windows que llegó a infectar a un millón de máquinas al mes. La acción conjunta de varias agencias internacionales desmantelaron esta operación en 2017 [26].
- **Rootkit:** se trata de un tipo de malware diseñado para tomar el control sobre un dispositivo, normalmente consiguiendo permisos de administrador en la máquina infectada. Un ejemplo de este tipo sería Flame, programa utilizado para recopilar información que se utilizó por primera vez en 2012 en ataques contra organizaciones y estados nacionales en Oriente Medio [74].
- **Bombas lógicas:** son un tipo de malware que solo tienen actividad cuando son activadas en función de una fecha y hora específicas o cuando se cumple una determinada condición. En 2016, un programador logró que en la sucursal de Siemens Corporation, no funcionaran correctamente las hojas de cálculo cada cierto tiempo, provocando que le contrataran para su solución [11].

La existencia de tal cantidad de variantes y combinaciones de malware se basa, en gran medida, a la evolución que ha sufrido a lo largo de los años y que se ha evidenciado en el presente apartado. Pero además, la existencia de servicios como el Malware as a Service (MaaS), implican la posibilidad de alquilar código malicioso utilizado para la realización de ataques dirigidos contra objetivos concretos, permitiendo que personas con bajos conocimientos sobre el tema puedan realizarlos sin mayor dificultad. Según el estudio publicado por Kaspersky "Understanding Malware-as-a-Service" [42], el ransomware supondría el 58 % de todo el MaaS distribuido entre los años 2015 a 2022. Con estas cifras, se hace imprescindible analizar qué es el ransomware y cuáles son las cuestiones que en las que se basa su funcionamiento.

1.2.2. El Ransomware: orígenes, evolución y funcionamiento

En el informe de ENISA (Agencia de la Unión Europea para la Ciberseguridad) "Threat Landscape 2024" [23], el ransomware se define como un tipo de ataque en el que los atacantes toman el control de los activos de un objetivo y exigen a cambio un rescate para recuperar la disponibilidad de esos activos. Esta definición contempla los tres elementos clave presentes en todo tipo de ransomware, que son: activos, acciones y chantaje.

Por el contrario, si se atiende a la definición de la NIST [56], el ransomware es un tipo de ataque malicioso en el que un atacante cifra los datos de una organización y exige a cambio un pago para restaurar el acceso. En algunas ocasiones, los atacantes también podrían exigir un pago adicional a cambio de no revelar información confidencial a autoridades, competidores o simplemente, para no hacerla pública.

Considerando este concepto, habría que remontarse a 1989 para identificar el que podría considerarse primer ransomware y que se muestra en la Figura 1.2, con nombre AIDS Information, el cual afectaba a los sistemas operativos MS-DOS 2.0 (o superior), creado por el Dr. Joseph L. Popp Jr.. Su distribución se realizó a través de discos de $5\frac{1}{4}$ cuyo envío, se producía mediante correo postal:

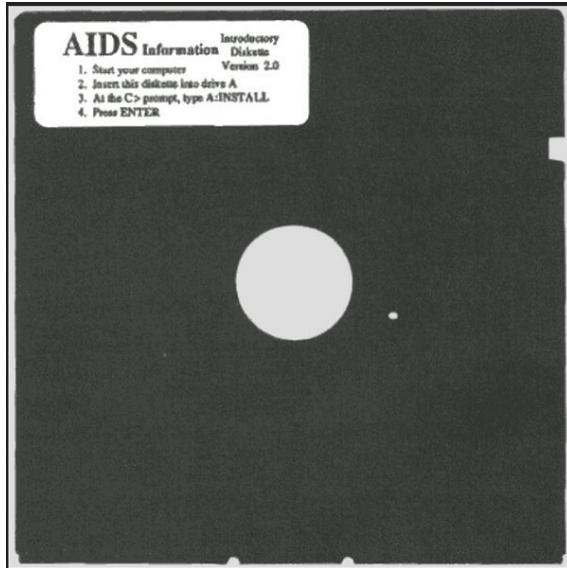


Figura 1.2: Disquete de 5 $\frac{1}{4}$ " de distribución de AIDS

Fuente: <https://www.linkedin.com/pulse/ransomware-o-paciente-zero-adriano-cansian/>

AIDS era un programa escrito en QuickBASIC 3.0, con apariencia educativa cuya temática versaba sobre el riesgo de contraer el SIDA. Su funcionamiento se basaba en sustituir el AUTOEXEC.BAT (fichero donde se ejecutan órdenes DOS de carga al iniciar el uso del ordenador), por instrucciones maliciosas, de tal manera que, tras arrancar el ordenador de la víctima en varias ocasiones, se mostraba una pantalla con una nota de rescate aderezada con lenguaje legal tal cual muestra la Figura 1.3. Esto provocaba que los directorios y archivos (aunque parece ser que no su contenido), se cifraran mediante un algoritmo propio [1], con el objetivo de impedir el acceso a los mismos a menos que se realizara el pago de 189 US\$ a entregar en Panamá a nombre de PC CYBORG CORPORATION:

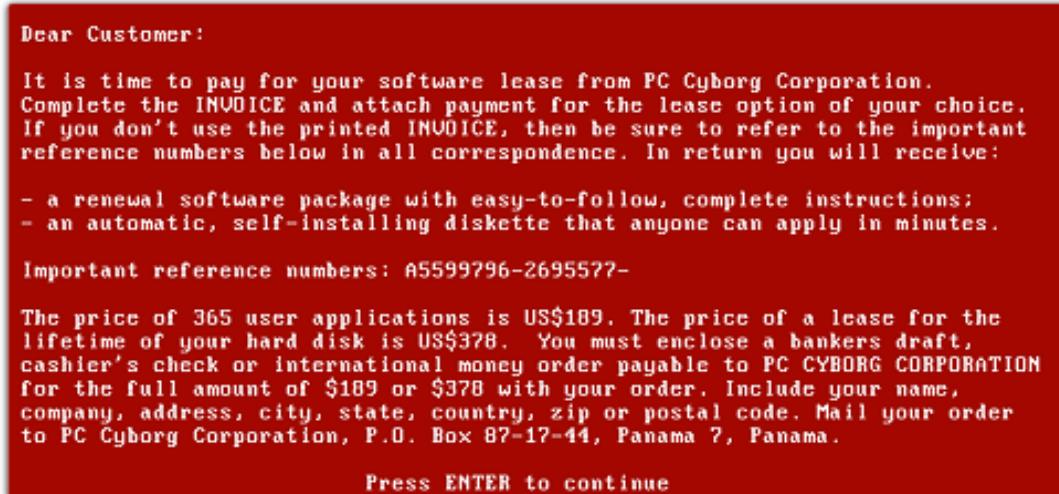


Figura 1.3: Mensaje de extorsión de AIDS Information.

Fuente: <https://www.linkedin.com/pulse/ransomware-o-paciente-zero-adriano-cansian/>

Tras la puesta en circulación del malware, la primera entidad en emitir una alerta fue el *Computer Incident Advisory Capability*, perteneciente al Departamento de Energía de EEUU tal y como muestra la Figura 1.4:

THE COMPUTER INCIDENT ADVISORY CAPABILITY
CIAC
INFORMATION BULLETIN

Information about the PC CYBORG (AIDS) trojan horse
December 19, 1989, 1600 PST Number A-10

There recently has been considerable attention in the news media about a new trojan horse which advertises that it provides information on the AIDS virus to users of IBM PC computers and PC clones. Once it enters a system, the trojan horse replaces AUTOEXEC.BAT, and may count the number of times the infected system has booted until a criterion number (90) is reached. At this point PC CYBORG hides directories, and scrambles (encrypts) the names of all files on drive C: There exists more than one version of this trojan horse, and at least one version does not wait to damage drive C:, but will hide directories and scramble file names upon the first boot after the trojan horse is installed.

Figura 1.4: Informe del CIAC sobre el denominado PC CYBORG AIDS del 19 de diciembre de 1989.

Fuente: <https://www.linkedin.com/pulse/ransomware-o-paciente-zero-adriano-cansian/>

Si se atiende a la evolución del ransomware, la expansión de Internet y nos centramos en el siglo actual, en el 2004 encontramos GPCode [67] el cual se centraba en cifrar ciertas extensiones de Office como .xls o .doc, otras de compresión de archivos como .zip o .rar y otras de uso común como .html, .jpg, .txt, .db, etc., haciendo uso de algoritmos de cifrado robustos como RSA-1024 [48] y AES-256 [54]. Poco después, en el año 2006 apareció Cryzip, parecido al anterior. El elemento diferencial se basaba en que Cryzip utilizaba una librería Zip comercial para cifrar archivos y comprimirlos con contraseña. Esto implica una evolución en los métodos de cifrado ya que pasó a externalizarse este proceso abriéndose a opciones más complejas y robustas.

Para focalizar la evolución del concepto de ransomware, hay que remontarse a la publicación realizada en IEEE en 1966 por Adam Young y Moti Yung llamada Simposio sobre Seguridad y Privacidad [75], en la que se propuso el término criptovirología para acuñar este tipo de ataque. En esta exposición se utiliza un tipo de malware que, una vez infecta la víctima, cifra sus archivos con una clave simétrica aleatoria local y, a su vez, cifra también esa clave simétrica generada de forma asimétrica, utilizando para este fin una clave pública. El siguiente paso es generar la nota de rescate y exponer el medio de contacto con el ciberdelincuente. Posteriormente, la víctima envía el pago y la clave simétrica cifrada asimétricamente, la cual es descifrada por el ciberdelincuente con su clave privada y enviada a la víctima para que pueda descifrar los archivos o ficheros, tal y como muestra el diagrama representando en la Figura 1.5:



Figura 1.5: Funcionamiento de la criptovirología

A partir de aquí comienza una evolución imparable de este tipo de malware, que, combinado con herramientas como la Inteligencia Artificial no solo optimizan la creación y mejora del código malicioso, sino que conforman un escenario per-

fector para que el ransomware mantenga su rentabilidad, eficacia y persistencia en el tiempo, haciendo uso de campañas de engaño y manipulación digital cada vez más sofisticadas y creíbles que están estrechamente relacionadas con los siguientes métodos utilizados por los ciberdelincuentes para perpetrar el engaño:

- **Phishing:** definido por el CCN-CERT [13] como método de ataque cuyo objetivo es obtener información confidencial a través del engaño y la picardía, mediante la suplantación de identidad de una entidad de confianza. Es decir, que se intenta imitar un correo o un mensaje de un servicio legítimo, en el que se incluirá un fichero adjunto que, una vez abierto, cifre el contenido del equipo donde se ha ejecutado o, en su defecto, un enlace a una dirección web de descarga de un fichero de ransomware con idéntica finalidad.
- **Ingeniería Social:** abarca una amplia gama de actividades orientadas a explotar el error humano con el objetivo de obtener acceso a servicios, información confidencial o, mediante la manipulación, engañar a la víctima para abrir documentos (que podrían contener ransomware), o visitar URLs de descarga de malware.
- **Vulnerabilidades:** explotar vulnerabilidades conocidas puede ser otra forma de entrar en el sistema objetivo e instalar software no deseado para posteriormente extorsionar y obtener rédito económico.
- **Ataques contra máquinas remotas:** pueden ser tipo RDPs (por sus siglas en inglés *Remote Desktop Protocol*, en español, protocolo de escritorio remoto), es un estándar utilizado para acceder de manera remota a un escritorio o máquina. Si un atacante se hiciera con credenciales de acceso de este tipo, o la máquina no estuviera debidamente bastionada, podría instalar un ransomware en el objetivo, cifrar el contenido y tomar el control sobre la misma. Esto también podría ocurrir mediante protocolos FTP (por sus siglas en inglés *File Transfer Protocol*), utilizado para el intercambio de archivos, o SSH (por sus siglas en inglés *Secure Shell*), que es un protocolo de administración remota, entre otros.

Además, a todo esto se une que los objetivos principales de los grupos de ciberdelincuentes han pasado a ser empresas de todo tipo, las cuales pueden ser estudiadas minuciosamente e investigar qué tipo de datos podrían comprometer y si pueden obtener o no el pago solicitado. Otro actor muy importante relacionado con los pagos y el ransomware es la criptomonedas, basada en transacciones irrastreables y anónimas. En el artículo *On the Economic Significance of Ransomware Campaigns: A Bitcoin*

Transactions Perspective publicado en 2028 por Mauro Conti, Ankit Gangwal y Sushmita Ruj [19] se analiza cómo los ciberdelincuentes aprovechan la criptomonedra Bitcoin para dificultar el rastreo por parte de las autoridades competentes, de sus transacciones ilícitas.

El informe publicado por Sophos titulado "El estado del ransomware 2024" [68], indica que, en promedio, el 49 % de los dispositivos de una organización fueron afectados por un ataque de ransomware. De este porcentaje, el 4 % afirmó haber sufrido un cifrado del 91 % o más de sus dispositivos, lo que implica casi su totalidad. En esta línea, el informe de SpyCloud "The 2024 State of Malware & Ransomware Defense Report" [69], publica que el 92 % de las organizaciones se vieron afectadas por el ransomware al menos una vez. Esto supone un aumento del 81 % con respecto al año 2023. A su vez, esto significa que solo el 8 % de las organizaciones no recibieron ningún impacto, tal y como muestra la Figura 1.6, frente al 19 % de 2023.

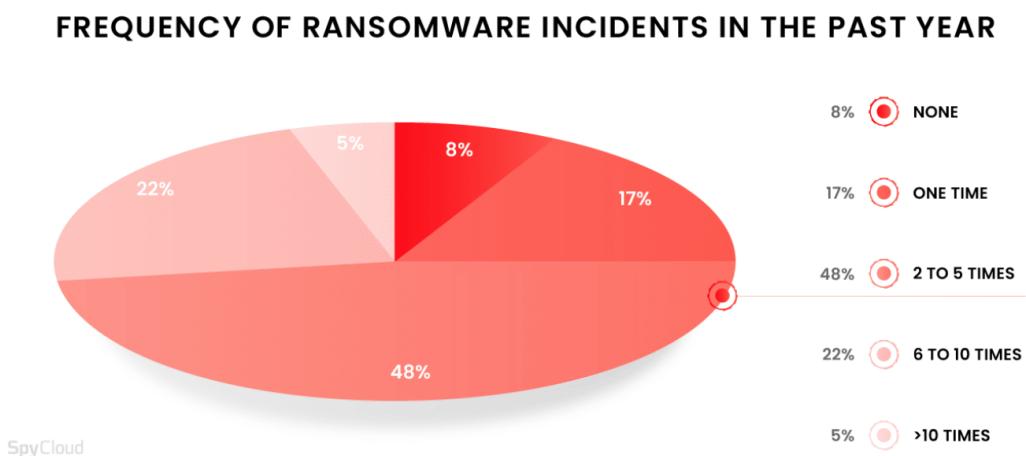


Figura 1.6: The 2024 State of Malware & Ransomware Defense Report.

Fuente: <https://spycloud.com/resource/2024-malware-ransomware-defense-report/>

En gran medida, este aumento es debido a una continua proliferación del conocido como RaaS (*Ransomware as a Service*). Este tipo de infraestructura permite a desarrolladores de ransomware poner al servicio de ciberdelincuentes sin conocimientos profundos en la materia, ataques sofisticados a cambio de una pequeña contrapartida económica. Atendiendo a los resultados publicados en el informe de Thales S21sec llamado *Threat Landscape Report 2024* [60], en la segunda mitad de 2024, se registraron un total de 2.909 incidentes relacionados con el ransomware frente a los 2.175 que se registraron en la primera parte del año. Si tenemos en cuenta los totales, hablaríamos de 5.084 ataques, que en comparación con los 4.618 registrados en 2023, supone un aumento del 10,1 %. Atendiendo a la geografía, en

este informe de refleja que EEUU es el país que más se ve afectado por incidentes de ransomware, pero España ocuparía el octavo puesto con 49 ataques recibidos en el segundo demestre de 2024. Estos datos son corroborados por el informe de LAB52 para S2GRUPO [61] "Panorama del Ransomware 2025", donde se indica que, en términos de víctimas a nivel mundial durante el año 2024, Estados Unidos seguiría ocupando la primera posición con un 53 % de ataques recibidos, ocupando España el noveno puesto, tal y como muestra la figura 1.7:

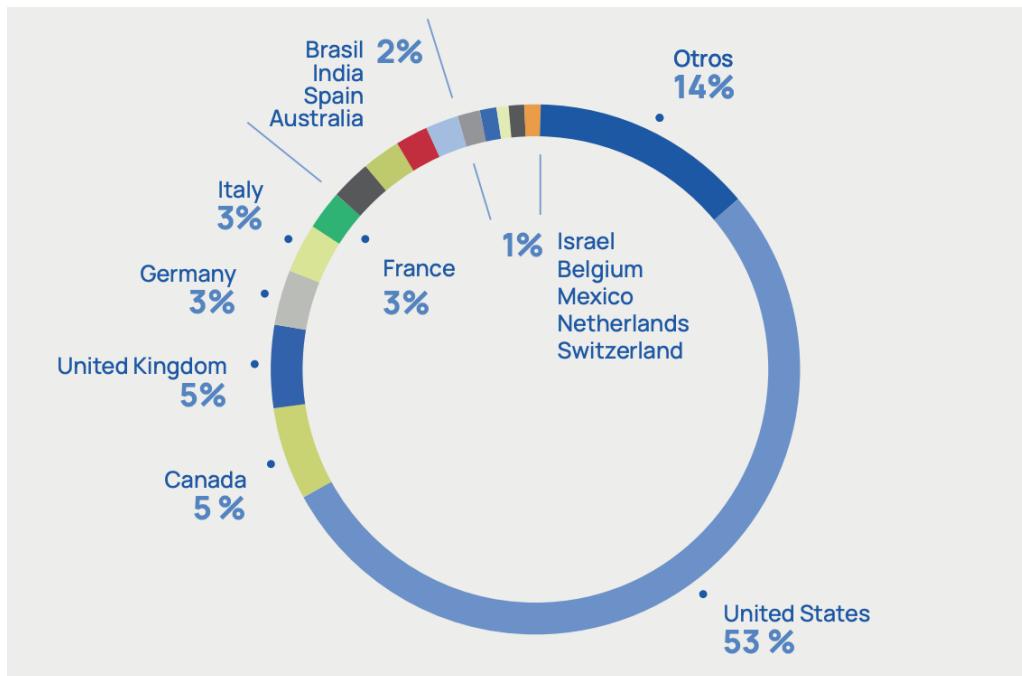


Figura 1.7: Porcentaje de víctimas por países – 2024. Fuente: LAB52

Fuente: <https://5529275.fs1.hubspotusercontent-na1.net/hubfs/5529275/Panorama%20del%20Ransomware%202025%20-%20S2GRUPO.pdf>

Esta demanda de este tipo de servicios ha provocado un amuento considerable y sustancial del número de grupos de cibadelincuentes que se esconden detrás de estos desarrollos maliciosos. Según se indica en el informe de Searchlight Cyber titulado *Ransomware in H1 2024: Trends from the Dark Web* [62], el incremento del número de grupos de ransomware activos es del 56 % con respecto a 2023. Concretamente, se identificaron 73 solo en la primera mitad de 2024. Además, incluso habiéndose desmantelado en este pasado 2024 grupos como Lockbit⁴, han surjido actores que trabajan en varios grupos de ransomware y han consolidado lo que se ha denominado como democratización del ransomware. Un ejemplo lo muestra Talos (división de

⁴<https://www.xataka.com/seguridad/adios-lockbit-banda-ransomware-peligrosa-mundo-ha-sido-desmantelada-operacion-internacional>

inteligencia de Cisco), en su informe de Revisión del Año de 2023 [70], donde se indica que, tras haberse conseguido interrumpir la infraestructura de Hive⁵, muchos de sus miembros se unieron a otros grupos de ransomware en los días que duró dicha interrupción. Por otro lado, si tenemos en cuenta los datos publicados por Security Brief [63], serían 80 los grupos de ransomware activos en el primer trimestre de 2025, 16 de los cuales de nueva creación a fecha 1 de enero.

En cuanto a los grupos de ransomware más activos de 2024, según el informe *The State of Cyber Security 2025* publicado por Check Point [15], RansomHub se ha convertido en el grupo más activo de 2024, por encima de Akira, Play o el propio Lockbit, tal y como se muestra en la Figura 1.8, extraída de dicho informe.

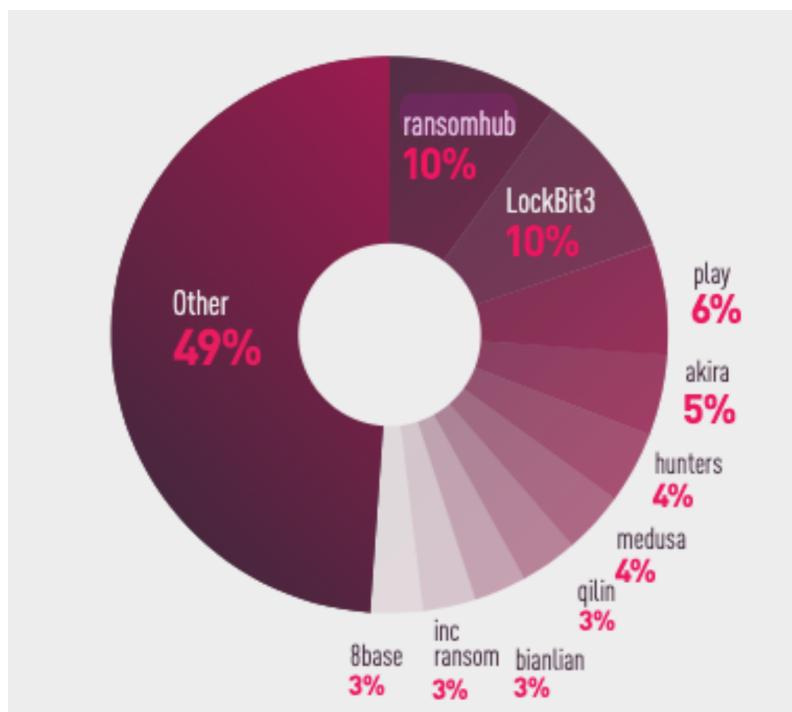


Figura 1.8: Cyber Security Report 2025 - Ransomware double-extortion groups, by percentage of total published victims in 2024.

Fuente: <https://www.checkpoint.com/security-report/?flz-category=items&flz-item=report-cyber-security-report-2025>

Si nos atenemos a los datos publicados por LAB52 para S2GRUPO [61], RansomHub, LockBit, Play, Akira y Hunters International ocuparían los primeros puestos de este listado tal y como muestra la Figura 1.9:

⁵<https://www.justice.gov/archives/opa/pr/us-department-justice-disrupts-hive-ransomware-variant>

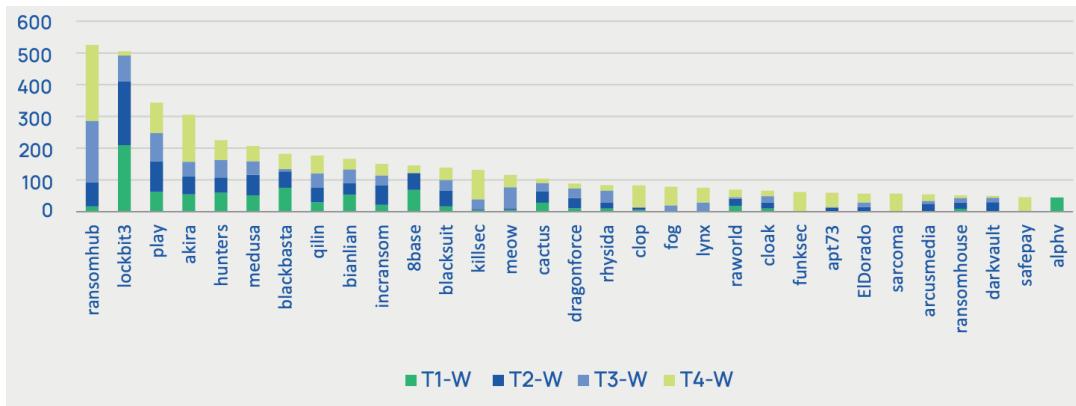


Figura 1.9: Datos mundiales de víctimas en 2024 desglosados por grupo de ransomware y trimestre.

Fuente: <https://5529275.fs1.hubspotusercontent-na1.net/hubfs/5529275/Panorama%20del%20Ransomware%202025%20-%20S2GRUPO.pdf>

En España, según datos publicados por S21sec en el informe *Threat Landscape Report 2024* [60], se registraron un total de 165 ataques en 2024, siendo 58 en el primer semestre y 107 en el segundo. Algunos ejemplos en la administración pública serían los siguientes:

- Agencia Tributaria: en diciembre de 2024 el grupo de ransomware Trinity afirmó haber sustraído 560 GB de datos⁶, algo que fue negado por la propia Agencia.
- Instituto Nacional de Investigación y Tecnología Agraria y Alimentaria (INIA-CSIC): En noviembre de 2024, este centro del CSIC sufrió un ataque de ransomware que paralizó el acceso a sus ordenadores (y a los datos almacenados en los mismos), junto a Internet, afectando a más de 600 empleados⁷.
- Comisión Nacional de los Mercados y la Competencia (CNMC): En diciembre de 2024, la CNMC reconoció haber sufrido un ataque provocando la filtración de más de 240 GB de datos personales (2.000 millones de registros con datos de titulares de telefonía móvil)⁸.

Además, en el ámbito de la empresa privada, también se dieron casos con mucha repercusión, algunos de los cuales se muestran a continuación:

⁶<https://elpais.com/tecnologia/2024-12-01/unos-piratas-dicen-haber-robado-datos-a-la-agencia-tributaria-y-esta-responde-que-no-ha-detectado-brecha-alguna.html>

⁷<https://elpais.com/ciencia/2024-11-26/el-mayor-centro-del-csic-paralizado-por-los-hackers.html>

⁸<https://elpais.com/economia/2024-12-09/la-audiencia-nacional-investigara-un-ciberataque-masivo-a-la-cnmc-que-afecto-a-datos-de-titulares-de-telefonia-movil.html>

- Infortisa: en noviembre de 2024, en plena campaña de Black Friday, este mayorista informático valenciano sufrió un ataque de ransomware que le obligó a desconectar servidores y equipos informáticos. Se vieron comprometidos datos personales e información bancaria y fiscal ⁹.
- Ibermutua: el pasado 23 de septiembre de 2024 esta entidad publicó un comunicado donde se indicaba que habían sufrido un acceso no autorizado a sus sistemas. En dicho comunicado no se hablaba expresamente de ransomware pero posteriormente, en su boletín número 326, página 2, afirmaron manifiestamente que, el 27 de agosto de 2024, sufrieron un ataque de ransomware provocando dicho acceso no autorizado ¹⁰.

En lo que de año, también se han registrado ataques que han afectado a entidades españolas, algunos ejemplos son los siguientes:

- Hospital Los Madroños: el pasado mes de marzo, fue el propio hospital quien hizo pública una violación de sus sistemas provocada por un ataque de ransomware atribuido al grupo Qilin, el cual logró cifrar sus sistemas y extraer opciones no autorizadas de datos almacenados ¹¹.
- Fundación Universidad de Valladolid: el 12 de febrero del presente año, la fundación emitió un comunicado en el que informaba haber detectado un ataque de ransomware ¹².

1.2.3. La red TOR

Con el objetivo de ampararse en el anonimato mediante el cifrado de las comunicaciones, haciéndolas irrastreables se crea una parte de Internet conocida como Dark Web.

El proyecto TOR, tiene sus orígenes en 2006, aunque la idea de desarrollar un enrutamiento en capas (como si de una cebolla se tratase, de ahí la etimología TOR como "*The Onion Route*"), data de la década de los noventa. Esta idea fue desarrollada por el matemático Paul Syverson y los científicos informáticos Michael G. Reed y David Goldschlag. Es en el año 1998 cuando estos tres publicaron el

⁹<https://www.channelpartner.es/seguridad/principales-ciberataques-en-espana-en-2024>

¹⁰<https://www.ibermutua.es/wp-content/uploads/2024/10/BOLETIN-326.pdf>

¹¹<https://hospitalosmadronos.es/aviso-de-ciberseguridad/>

¹²<https://comunicacion.uva.es/es/detalle/Comunicado-de-la-Fundacion-Universidad-de-Valladolid>

artículo *Anonymous Connections and Onion Routing* [59] presentando este concepto que se puede resumir en los siguientes puntos clave:

- **Objetivo:** el principal objetivo del enrutamiento cebolla es el desarrollo de una infraestructura que permita la creación de conexiones anónimas resistentes al análisis de tráfico (lo que desemboca en una protección de la identidad y fomenta el anonimato).
- **Funcionamiento:** se basa principalmente en dos aspectos fundamentales. El primero es que las conexiones son bidireccionales y operan en tiempo real. El segundo es que se emplean capas (*onions*) para establecer conexiones anónimas. A su vez, cada *onion* contiene capas de cifrado que se descifran en cada nodo de la red, revelando la siguiente dirección destino e impidiendo que un nodo conozca el origen o el destino final de la comunicación.
- **Implementación:** este sistema fue implementado en Sun Solaris 2.X, con proxies desarrollados para aplicaciones como navegadores web, inicios de sesión remotos y correo electrónico.
- **Vulnerabilidades y rendimiento:** en el artículo se presentan análisis de posibles vulnerabilidades del sistema así como resultados de rendimiento y eficiencia.

Este trabajo, sentó las bases para desarrollos posteriores como Tor Project, Inc., organización sin ánimo de lucro fundada en 2006 cuyo objetivo era mantener el desarrollo de TOR, el cual comenzó a ganar adeptos y cuyo mayor interés era el mantenimiento de la privacidad. Fruto de estas investigaciones, en el año 2008, nació el Navegador TOR, proporcionando tanto protección de la identidad de las personas en línea como el acceso a recursos o sitios bloqueados en Internet.

No obstante, aunque relacionados, hay que diferenciar la red TOR de la Deep Web y la Dark Web:

- Red Tor: infraestructura que permite una navegación anónima por la Red. Funciona mediante tráfico redirigido por una serie de servidores que cifran los datos en múltiples capas (enrutamiento cebolla), dificultando el rastreo o la ubicación de quien la usa. Se utiliza como método de acceso a la dark web.
- Deep Web: se compone de aquellas partes de Internet que no están indexadas por motores de búsqueda tradicionales (como por ejemplo, Google). Es accesible mediante navegadores estandar en tanto se cuente con credenciales adecuados.

- Dark Web: es un subconjunto de la Deep Web que requiere de software específico como por ejemplo, el navegador TOR [58]. Las direcciones suelen tener la terminación ".onion". También está diseñada para el anonimato pero la gran diferencia radica en que también es utilizada para actividades ilícitas como el mercado de armas, drogas, falsificaciones de todo tipo o, en el caso de que nos ocupa, alojar sitios de grupos de Ransomware donde publicar los resultados de los ataques a sus víctimas potenciales.

Cabe destacar que los servicios ".onion", se generan automáticamente (al contrario que en la navegación normal en la que es necesario usar o comprar un dominio), y se componen de una cadena de 56 letras y números generados de manera aleatoria en base a un hash procedente de la generación de una clave pública RSA de 1024 bits que se utilizará posteriormente para firmar peticiones junto con los nodos que harán como puntos de introducción y encuentro [21].

1.2.4. TOR y los *Hidden Sites* relacionados con RaaS

Son varios los grupos de ransomware que utilizan la red TOR para realizar publicaciones y así filtrar cuáles han sido sus víctimas. Algunos ejemplos serían los siguientes:

- **LockBit**: se trata de un grupo que opera desde 2019, de origen ruso, y que para operar, utiliza el modelo de ransomware como servicio (RaaS). Denominado originalmente como "ABCD", ha evolucionado en varias ocasiones, siendo la versión 3.0 la última conocida [36]. Un ejemplo de estas publicaciones es el que se muestra en la Figura 1.10:

The screenshot shows a grid of 10 website entries from the Lockbit 3.0 Leaked Data page. Each entry includes the website URL, a 'PUBLISHED' status indicator, a short description of the company and its industry, and a timestamp of when the data was uploaded. The websites listed are:

- essenzamovies.com.br**: Greetings! Today we are posting here the new company, "ESSENZA DESING INDUSTRIA DE MOVIES LTDA". Company Description: Essenza was founded in 2001 in the Serra Gaúcha region.
- unila.edu.mx**: Greetings! Today we are posting here the new company, "UNILA SA DE CV". Company Description: Universidad Latina is constantly advancing towards excellence and institutional
- ossc.mx**: Greetings! Today we are posting here the new company, "OSSC Mexico". Company Description: In 2008, OSSC was created with a base of experts who already had more than ten years of experience in the field of high-quality meat and by-products.
- bioclimaservice.it**: Greetings! Today we are posting here the new company, "BIO - CLIMA SERVICE S.R.L.". Company Description: Bio-Clima Service SRL is a company founded in 2002 and specialized in
- fepasa.com.ar**: Greetings! Today we are posting here the new company, "F.E.P.A.S.A.". Company Description: FEPASA – Argentine poultry company operating in the field of high-quality meat and by-products.
- 51talk.com**: A lot of interesting info: 1G - 51TalkActivity_backup_2025_01_25_030001_1281 1G - 51TalkNewStaff backup 2025 01 25 030001 12
- gruppocogesi.org**: CO.GE.S.I. si è specializzata nel supporto tecnico – amministrativo finalizzato alla definizione delle istanze di condono edilizio e delle istanze edilizie presentate ai sensi del d.o.r. n. 380/2001.
- ahn.org**: Greetings! Today we are posting here the new company, "West Penn Allegheny Health System Inc.". Company Description: West Penn Hospital, centrally located in Pittsburgh's Bloomfield
- jtu.com.br**: Greetings! Today we are posting here the new company, "JACAREÍ TRANSPORTE URBANO LTDA". Company Description: JACAREÍ TRANSPORTE URBANO was founded with the
- viacaojacarei.com.br**: Greetings! Today we are posting here the new company, "JACAREÍ TRANSPORTE URBANO LTDA". Company Description: JACAREÍ TRANSPORTE URBANO was founded with the
- gelco-sa.com.br**: Greetings! Today we are posting here the new company, "Gelco Gelatinas do Brasil Ltda". Company Description: Gelco Gelatinas do Brasil Ltda. is an enterprise in Brazil, with the main office
- fordcountrymotors.mx**: Greetings! Today we are posting here the new company, "CMAMERICAS S.A. DE C.V.". Company Description: COUNTRY MOTORS specializes in the retail sale of new passenger cars and trucks.

Figura 1.10: Lockbit 3.0 Leaked DataFuente: <http://lockbit7ouvrsgtjoeoj5hvubljqtghitekwpdy3b6y62ixtsu5jqd.onion/>

- **Hive**: más orientado hacia sectores de ámbito industrial así como organizaciones del sector salud, agrícola o de la energía. Detectado por primera vez en junio de 2021, puso en jaque a más de 1.300 empresas en 80 países¹³. En la Figura 1.11 se puede ver una publicación en TOR que afirma haber comprometido una empresa en cuestión.

The screenshot shows a leak page for the company **SANDO**. The page includes the following information:

- Encrypted at:** 17 June 2022 00:13:30
- Disclosed at:** 13 July 2022 16:08:00
- Website:** sando.com
- Revenue:** \$668M
- Employees:** 2 951
- Disclosure Links:** 1 link

Figura 1.11: Publicación en la red TOR de empresa comprometida por ransomware HiveFuente: <http://hiveleakdbtp76ulyhi52eag6c6tyc3xw7ez7iqy6wc34gd2nekazyd.onion/>

- **Akira**: más reciente, del año 2023, emergió como una división del ransomware Conti. Según se publica en Statista¹⁴, en el tercer trimestre de 2024, fue responsable del 13 % de los ataques de ransomware en EEUU. En la Figura 1.12 se muestra cómo son sus publicaciones en la red TOR:

¹³<https://www.scientificamerican.com/article/fbi-takes-down-hive-criminal-ransomware-group1/>

¹⁴<https://www.statista.com/statistics/1411163/ransomware-variants-detected-usby-market-share/>

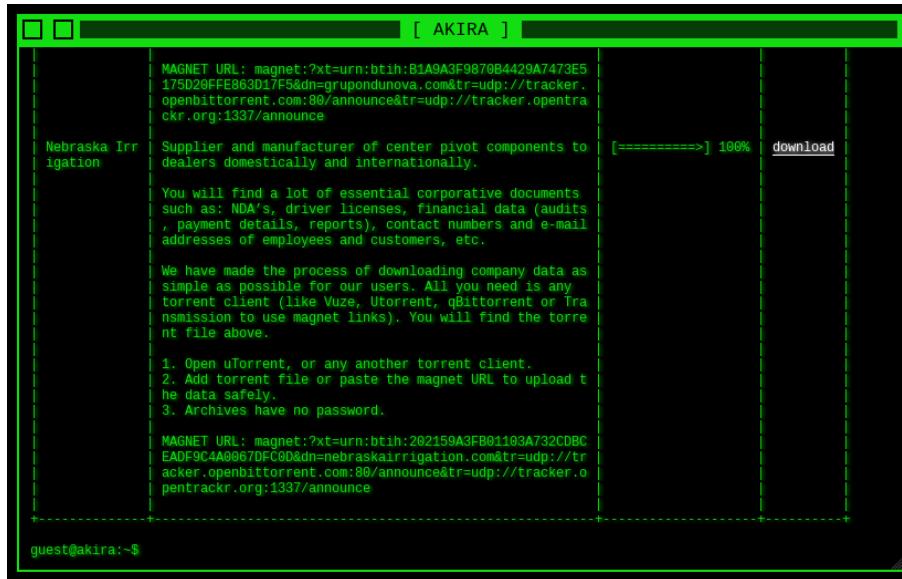


Figura 1.12: Grupo Akira en la red TOR

Fuente: <https://akirral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad.onion/>

- **Blackcat:** también conocido como ALPHV o Noberus, es un grupo surgido a mediados de noviembre de 2021 que opera bajo el modelo de ransomware como servicio (RaaS), caracterizado por reclutar afiliados para llevar a cabo ataques y para, posteriormente, compartir con ellos un porcentaje significativo (entre el 80-90 %), de los rescates obtenidos. De entre la multitud de ataques realizados por este grupo en los últimos años, caben destacar los realizados a Roblox, Twitch o Tipalti. Blackcat, una vez ha cifrado los archivos de su víctima, deja una dirección .onion en su nota de rescate con una clave de acceso específica, tal y como se muestra en la Figura 1.13:

```
->> Introduction

Important files on your system was ENCRYPTED and now they have have "wpzlbji"
extension.
In order to recover your files you need to follow instructions below.

->> Sensitive Data

Sensitive data on your system was DOWNLOADED and it will be PUBLISHED if you refuse to
cooperate.

Data includes:
- Employees personal data, CVs, DL, SSN.
- Complete network map including credentials for local and remote services.
- Financial information including clients data, bills, budgets, annual reports, bank
statements.
- Complete datagrams/schemas/drawings for manufacturing in solidworks format
- And more...

->> CAUTION

DO NOT MODIFY FILES YOURSELF.
DO NOT USE THIRD PARTY SOFTWARE TO RESTORE YOUR DATA.
YOU MAY DAMAGE YOUR FILES, IT WILL RESULT IN PERMANENT DATA LOSS.
YOUR DATA IS STRONGLY ENCRYPTED, YOU CAN NOT DECRYPT IT WITHOUT CIPHER KEY.

->> Recovery procedure

Follow these simple steps to get in touch and recover your data:
1) Download and install Tor Browser from: https://torproject.org/
2) Navigate to:
http://2cuqgeerjdba2rhdviezodpu3lc4qz2sjf4qin6f7std2evleqlzjid.onion/?\(ACCESS\_KEY\)
```

Figura 1.13: Nota de rescata Blackcat con dirección de TOR

Fuente: <https://unit42.paloaltonetworks.com/blackcat-ransomware>

En definitiva, los grupos de ransomware harán uso de la red TOR para ampararse en el anonimato, ocultando IPs de usuario o ubicaciones de servidores, para la gestión de los pagos, mediante direcciones .onion donde se puede pagar el rescate en criptomonedas, o para extorsionar y ejercer presión pública, a través de "leak sites" o sitios de filtración donde poder publicar muestras de datos robados y así forzar a la víctima a que realice el pago solicitado.

1.2.5. TOR y el RaaS

Además de todo lo expuesto en los apartados anteriores, donde se explica el propio funcionamiento de TOR o la relación que guarda con los *Hidden Sites* de los grupos dedicados al ransomware, a continuación, se desarrollará que relación hay entre TOR y el funcionamiento del ransomware como servicio o RaaS.

Según señala IBM [31], el RaaS es un modelo de negocio en el que los desarrolladores de ransomware crean y mantienen el software malicioso para luego alquilarlo o venderlo a otros cibercriminales, conocidos como "afiliados", que serán quienes utilicen dicho código para perpetrar los ataques posteriores.

Es decir, que este modelo permite a cualquier usuario de la red TOR comprar un paquete o kit ofertado y convertirse en un potencial atacante. Todo esto sin la necesidad de contar con habilidades técnicas sofisticadas, tal y como se evidencia en el artículo publicado en ScienceDirect *The Ransomware-as-a-Service economy within the darknet* [66]. Esto implica que, detrás del modelo RaaS, existe una infraestructura completa y gestionada que reduce o elimina la barrera de entrada para nuevos atacantes alentando la profesionalización de la cibodelincuencia y que podría resumirse en los siguientes puntos:

- **Panel de control** (Dashboard RaaS): accesible mediante URL .onion. Permite a los afiliados la generación de binarios, realizar seguimientos de las víctimas, visualización de pagos u otro tipo de estadísticas más personalizadas. Además, estos paneles permiten seleccionar el tipo de cifrado (AES, RSA, etc.), editar el texto de la nota de rescate, establecer la dirección del monedero de criptomonedas para el pago o configurar el tiempo en el que este expiraría.
- **Constructor de payloads**: herramientas que permiten la generación de archivos ejecutables que cuentan con un empaquetado propio orientado a evitar ser detectados por antivirus. Además, en muchas ocasiones permiten establecer configuraciones personalizadas (dirección de un servidor C2).
- **Sorporte**: algunos paneles incluyen sistemas automatizados como chatbots o foros internos para afiliados donde exponer sus dudas. También suelen contar con FAQs, instrucciones paso a paso o vídeo tutoriales para usuarios juniors.
- **Infraestructura backend**: esto incluiría servidores proxy o VPN para anonimizar el tráfico, alojamiento seguro para páginas de pago con criptomonedas entre otras funcionalidades orientadas a la monitorización o recepción de claves de cifrado.
- **Servicios adicionales**: tales como actualizaciones del malware o del ransomware orientadas a evitar firmas de antivirus o sistemas de detección, asistencia técnica que, en algunos casos, podría ser 24/7, herramientas auxiliares como por ejemplo un kit para phishing o exploits de vulnerabilidades comunes conocidas, garantías de funcionamiento para casos en los que el payload fuera detectado antes de provocar la infección o incluso un *marketplace* de víctimas que no hubieran realizado el pago.

Pero, además de este tipo de *Group Sites* orientados a la administración de campañas (RaaS panels / dashboards), existen otros tipos [28] como los que se describen a continuación:

- Leak sites (sitios de filtración), orientados a la extorsión. Son *sites* en los que se publican los datos de las víctimas que no han realizado el pago. También pueden utilizarse para publicaciones de muestras de datos de una víctima en concreto, con el objetivo de demostrar la posesión del total de los mismos o, para realizar anuncios de víctimas futuras. Algunos ejemplos serían Conti News, LockBit Blog (Figura 1.14), o BlackCat ALPHV leaks site:

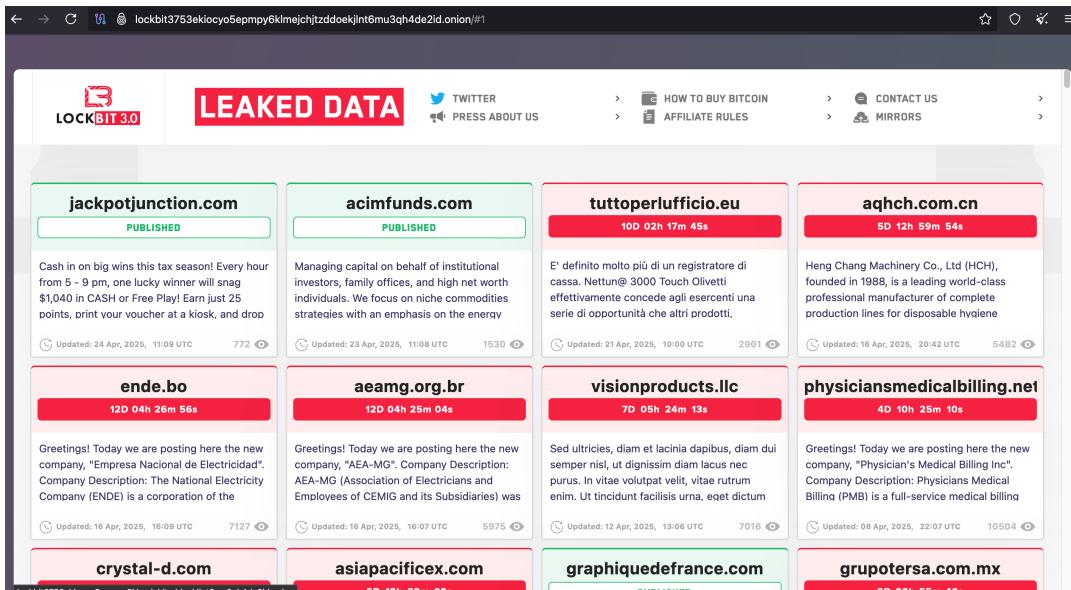


Figura 1.14: LockBit Blog en su dirección TOR

Fuente: <http://lockbit3753ekiocyo5epmpy6klmejchjtzddoekjlnt6mu3qh4de2id.onion/#1>

- Sitios de reclutamiento de afiliados. Suelen ser secciones de foros donde se realiza el reclutamiento de esta figura y en los que se suelen publicar las condiciones, los porcentajes de pago de cada cobro obtenido por la extorsión o los requerimientos técnicos necesarios.
- *Marketplaces* internos. Son *sites* en los que se pueden encontrar, a cambio de una contraprestación económica, accesos tipo RDP de empresas, cuentas comprometidas, malware tipo *rootkit* o *keylogger*, exploits, etc.
- Soporte y documentación. Se trata de foros cerrados o paneles privados de los RaaS donde se ofrece documentación técnica, tutoriales y guías para la configuración del ransomware así como soluciones a dudas o problemas técnicos.
- Portales para que las víctimas realicen los pagos. En este caso, no están dirigidos a afiliados pero son gestionados por el grupo malicioso. En este tipo de *sites* las víctimas introducen su ID de infección para recibir las instrucciones

de pago, probar a descifrar algún archivo o incluso con canales de chat para negociar.

Además de ofrecer infraestructura técnica, los *sites* de afiliados que operan bajo RaaS también ofertan modelos comerciales perfectamente estructurados, como si de páginas legítimas de software se tratase. Dependiendo del grupo, los sitios de afiliación presentan distintos tipos de suscripciones, tarifas o esquemas de reparto de ganancias:

- RaaS con modelo de suscripción mensual, donde se establece una couta fija para acceder al panel y utilizar el código malicioso. Suelen tener varios niveles (básico, medio, avanzado, etc.), en función de los cuales podrán o no acceder a ciertas funciones premium. Un ejemplo lo muestra la Figura 1.15, con dos modelos de diferente coste y funcionalidad:

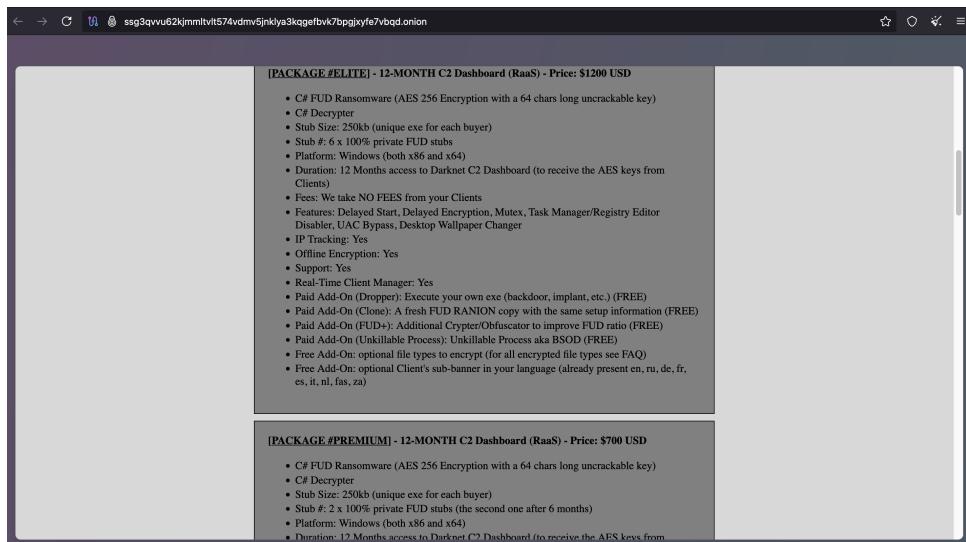


Figura 1.15: Ranion RaaS en su dirección TOR

Fuente: <http://ssg3qvvu62kjmmllvt574vdmv5jnkiya3kqgefbyk7bpgjxyfe7vbqd.onion/>

- RaaS por comisión sobre rescate, donde se ofrecen las herramientas de forma gratuita a cambio de una comisión por cada caso de éxito. Son *sites* más controlados, donde los afiliados son aceptados manualmente por operadores del propio grupo. Un ejemplo es el que se muestra en la figura 1.16, donde LockBit se queda con un 20 % del rescate:

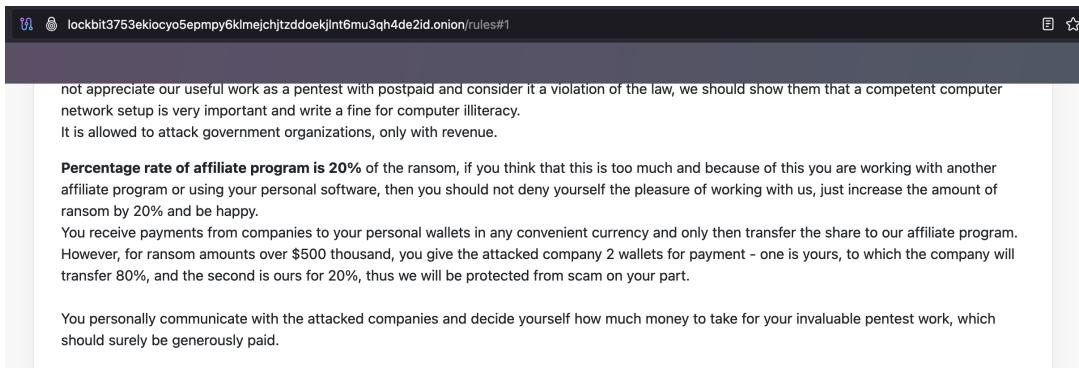


Figura 1.16: Condiciones de LockBit en su dirección TOR

Fuente: <http://lockbit3753ekiocy05epmpy6klmejchjtddoekjlnt6mu3qh4de2id.onion/rules#1>

- RaaS basado en campañas, también denominados *Pay-per-campaign*, donde el *site* cobra una tarifa por cada campaña lanzada la cual varía en función del número de binarios generados, de cuál sea la región objetivo, o de la persistencia del malware e integración con exploits.
- RaaS tipo *Marketplace Premium*”, cerrados y que funcionan solo por invitación donde los afiliados pueden comprar accesos a infraestructuras, kits a la carta, como por ejemplo un servicio combinado de phishing + ransomware donde se paga por item y no existen tarifas fijas.
- RaaS con tarifas por resultados, orientados a afiliados novatos que ofertan cobrar únicamente si se consigue el resultado exitoso. Este porcentaje de cobro suele ser mayor que los RasS por comisión de rescate, oscilando entre el 30-50 %.

Estos portales que operan bajo esquemas de suscripción y tarificación resultan esenciales para impulsar el crecimiento del ransomware como una industria global, adoptando estructuras más sofisticadas y automatizadas, y, por lo tanto, estableciendo modelos económicos más definidos y organizados.

En cuanto a los principales grupos de ransomware que operan bajo el modelo RaaS, caben destacar:

- **LockBit.** Se trata de un grupo de gran actividad desde el año 2019, ofrece un panel avanzado y un *site* donde publica los datos de aquellas víctimas que no hayan realizado el pago una vez transcurrido un tiempo de margen estipulado.
- **BlackCat / ALPHV.** Ofrece un esquema RaaS basado en Rust (compatible con Windows, Linux y ESXi), y cuenta con uno de los *Leaks sites* más avanzados e importantes donde no duda en amenazar públicamente a sus víctimas.

- **Cl0p.** Enfocado hacia grandes corporaciones (MOVEit [37]) y especializado en extorsionar por los datos sensibles sustraídos ilícitamente, utiliza las vulnerabilidades en software conocidas para comprometer a sus víctimas.
- **Royal.** Grupo semi-privado formado por exmiembros de Conti (disuelto en 2022 [20]). Opera con afiliados seleccionados y técnicas de ingeniería social y distribución avanzadas.
- **REvil/Sodinokibi.** Su primera aparición fue en 2019 y fue un grupo muy activo hasta 2021. Responsable del ataque a Kaseya [34], ofrece un modelo altamente profesionalizado basado en la doble extorsión (robo de datos y cifrado), que llegó a pedir hasta el 40 % de las ganancias obtenidas tras el pago del rescate.
- **DarkSide/BlackMatter.** Precursor de ALPHV, su actividad se enfocó principalmente en grandes infraestructuras de sectores críticos (como la energía). Tras el ataque a Colonial Pipeline [52] reaparecieron como BlackMatter y, posteriormente, evolucionaron a ALPHV.
- Otros ejemplos de grupos emergentes podrían ser **NoEscape** (modelo RaaS privado que suele amenazar de publicaciones inmediatas si no se realizan los pagos solicitados), **Play** (modelo de afiliados limitados caracterizado por el mensaje “PLAY” como firma), **Black Basta** (formado por exmiembros de Conti, utiliza accesos RDP para cifrar en entornos corporativos), **8Base** (que no deja claro si cuenta con afiliados y mezcla extorsión y cifrado), o **BianLian** (centrado en negociar todas sus exfiltraciones).

1.2.6. Algoritmos criptográficos

El algoritmo criptográfico es definido por el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés), como un procedimiento computacional bien definido que toma entradas variables, incluida una clave criptográfica, y produce una salida [53]. Asimismo, dicha entidad define el proceso de encriptación o cifrado como aquel proceso que transfiere texto plano en texto cifrado, utilizando para tal efecto un algoritmo criptográfico y una clave.

Según la publicación especial del NIST 800-175B Rev.1, titulada *Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms* [55], los algoritmos criptográficos se agrupan en las siguientes categorías:

- **Algoritmos de clave simétrica:** utilizan la misma clave de cifrado y descifrado. Esta circunstancia lo convierte en un método vulnerable debido a la existencia de procedimientos de descifrado. Es utilizado para cifrar grandes volúmenes de datos y su consumo de recursos es bajo. Dentro de este tipo podemos encontrar diferentes modalidades:
 - Cifrado por bloques (*Block Chipher*), donde el mensaje a cifrar se divide en varios bloques del mismo tamaño cifrándose independientemente con una clave la cual será necesaria para su posterior descifrado. Algunos de los ejemplos de algoritmos de este tipo son AES (con longitudes de bloque de 128 bits), DES (con longitudes de bloque de 64 bits, inseguros ante ataques de fuerza bruta), Triple DES (también conocido como TDES, y llamado así por utilizar DES tres veces aunque su nombre es TDEA por sus siglas en inglés *Triple Data Encryption Algorithm*), IDEA (por sus siglas en inglés *International Data Encryption Algorithm* con bloques de 64 bits), entre otros muchos.
 - Cifrados basados en Hash (Hash-based Symmetric-key Algorithms), que, además de la clave de cifrado, utilizan funciones hash garantizando que el mensaje viene de fuentes legítimas junto con su integridad (mensaje sin alterar). Para esta tipología se podría destacar HMAC (por sus siglas en inglés *Hash-based Message Authentication Code*).
 - Cifrado de flujos (*Stream Chiper*) [44], en este caso, el cifrado del texto se produce bit a bit. Un ejemplo de este tipo sería Rivest 4 (RC4), utilizado en cifrados WEB y WPA para Wi-Fi.
- **Algoritmos de clave asimétrica:** en este caso, se utilizan un par de claves. Una pública, conocida por todos, y una privada que solo es conocedora por quien descifrará el mensaje. Con este tipo de cifrado NIST contempla diferentes tipos de algoritmos, algunos de los cuales son los siguientes:
 - RSA (*Rivest–Shamir–Adleman*): utilizado en protocolos como SSL, certificados digitales, cifrado de aplicaciones, firma digital entre otros. Su fortaleza radica en la factorización de grandes números enteros.
 - DSA (*Digital Signature Algorithm*): permiten la firma digital de mensajes con una clave pública, lo cual es verificable por cualquier haciendo uso de la misma clave pública del firmante.

- ECDSA (*Elliptic Curve Digital Signature Algorithm*): basado en la criptografía de curva elíptica y utilizado preferentemente en sistemas con recursos limitados, como dispositivos móviles o de IoT.
- Algoritmos de Diffie-Hellman (DH). Aunque no se trata de un mecanismo de cifrado como tal, este algoritmo fue enunciado por primera vez en 1976 por W. Diffie y M. Hellman, y está basado en la dificultad de calcular logaritmos discretos. Por este motivo se utiliza para el intercambio de claves.

1.2.7. Herramientas de descifrado

Teniendo en cuenta que el principal objetivo de conocer a fondo al ransomware es intentar descifrar lo que de manera maliciosa se ha cifrado, se harán uso de algunas herramientas publicadas como la herramienta de *ID Ransomware* [33] donde con una muestra de ficheros cifrados y la nota de rescate puede identificar algunos tipos de cifrados y la firma que realizó el ataque. También existen otras herramientas gratuitas para descifrar archivos afectados por variantes específicas de ransomware, como las ofrecidas por Avast o AVG [3] para ransomware como Apocalypse, BadBlock, Bart, Crypt888, Legion, SZFLocker o TeslaCrypt. También el FBI, tras desmantelar en 2023 al grupo BlackCat ofreció una herramienta para el descifrado de archivos. No obstante, estudios publicados en la revista Computers & Security [29] indican que casi la mitad de las herramientas existentes no logran recuperar los datos comprometidos lo que hace necesario mejorar la eficacia y eficiencia de estas soluciones.

1.3. La definición del problema

Tal y como se ha dejado patente en los apartados anteriores, los ataques de ransomware han sido de los más utilizados en el pasado 2024. La publicación de CM-Alliance titulada *Top 10 Biggest Cyber Attacks of 2024 & 25 Other Attacks to Know About* [17] indica que entre los ataques más destacados se encuentra el sufrido por Change Healthcare [32], empresa del sector de la salud.

En España, según publica Channel Partner, el ransomware ha estado presente en los principales ataques ocurridos durante el 2024 [14]. Adicionalmente, no dejan de aparecer nuevos grupos de ransomware de los que apenas se cuenta con información.

Por todo esto, el presente estudio pretende analizar el ransomware CryptoLocker para conocer sus principales características, métodos de cifrado, o IoCs que pudieran

determinarse de cara a componer medidas de seguridad que puedan ser partícipes en la prevención de este tipo de ataques.

Capítulo 2

Gestión de proyecto software

El presente capítulo trata de exponer los criterios metodológicos y estratégicos considerados en la fase de definición y planificación del proyecto. Con base en la identificación de las actividades clave y los hitos asociados al alcance definido, se lleva a cabo una estimación sistemática de los recursos requeridos para su implementación y desarrollo.

2.1. Alcance del proyecto

En este apartado se delimita el conjunto de entregables, funcionalidades y resultados necesarios para la realización del proyecto dentro del marco metodológico Scrum. Esto contempla la estructuración del trabajo, la planificación de tareas de cada sprint, la asignación de recursos, la previsión del presupuesto y la identificación de potenciales riesgos que podrían afectar el desarrollo del mismo.

2.1.1. Definición del proyecto

El presente proyecto realiza un estudio de una muestra de ransomware de la familia CoinLocker. Para contextualizar el trabajo se realiza una investigación sobre el ransomware, con datos estadísticos relacionados con la cuestión planteada, como pueden ser infecciones, países con más casos, principales grupos o técnicas de engaño. También se realiza un recorrido por la red TOR para exponer los sitios donde los grupos operan o publican los resultados de sus ataques.

El segundo paso será realizar un análisis estático de la muestra seleccionada, sin ejecutarlo, para obtener toda la información posible y poder establecer una serie de IoCs. Posteriormente se realizará un análisis dinámico en diferentes entornos

controlados para estudiar el modo en el que se cifran los ficheros, ver la nota de rescate y cómo se daña el equipo de cara a obtener la mayor información posible.

Por último, se analizará toda la información extraída de ambos análisis para la exposición de las conclusiones.

2.1.2. Estimación de tareas y recursos

Tareas

Como se ha indicado anteriormente, al utilizar metodología Scrum para el desarrollo del proyecto, se ha elaborado un diagrama de Gantt que se muestra en la Figura 2.1 con los tiempos previstos para la realización de cada tarea. La planificación incial es de 3 meses dedicando 5 horas de trabajo diario. El comienzo es en marzo y la finalización en mayo.

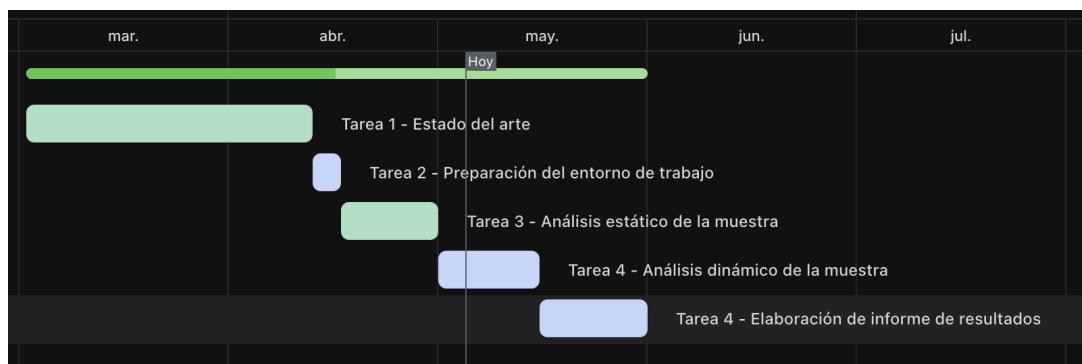


Figura 2.1: Diagrama de Gantt con la planificación de las tareas

Recursos

A continuación se muestran los recursos necesarios para el desarrollo del proyecto, tanto físicos como humanos:

- **Recursos humanos:**

- **Scrum Master:** supervisor del trabajo y encargado de organizar las actividades programadas. Hará las labores de guía para ofrecer ayuda en la resolución de cualquier tipo de obstáculo que pudiera presentarse. Este papel lo llevará a cabo el cotutor del proyecto.
- **Scrum Team:** formado por un analista de seguridad informática que será el encargado del desarrollo del proyecto. Realizará el estudio del estado del arte en referencia a la temática a desarrollar y analizará la muestra.

de ransomware seleccionada. El integrante de este equipo será el autor del presente documento.

■ **Recursos físicos:**

- Oficina para el desarrollo del proyecto.
- Gastos de luz asociados.
- Ordenador personal con las siguientes características:
 - MacBook Pro, Retina, 15 pulgadas.
 - Procesador 2,5 GHz Intel Core i7 de 4 núcleos.
 - Memoria de 16 GB 1600 MHz DDR3.
 - Gráficos Intel Iris Pro 1536 MB.
 - Software: las aplicaciones serán *opensource*.

2.1.3. Presupuesto

A continuación se detalla un presupuesto estimado y aproximado para el coste total de este proyecto en función de los recursos establecidos previamente.

Coste de personal

El presupuesto relacionado con los recursos humanos está calculado en función del coste de cada miembro del equipo, el cual, dependerá de los gastos asociados a su perfil, quedando reflejados en la tabla 2.1

- Scrum Master: en España, según datos publicados en "Indeed" [39], el salario medio de relacionado con este perfil sería de 39.160€ anuales (actualizado a 10 de abril de 2025). Teniendo en cuenta que las jorandas son de 40 horas y que el número total de horas anuales trabajadas sería de 1.826, nos dejaría un coste final de aproximadamente 21,5€ la hora.
- Analista de seguridad informática: en España, según datos publicados en "Indeed", el salario medio relacionado con este perfil está entorno a los 50.000€ [38], dependiendo de la experiencia y perfil del puesto a desarrollar. En base al mismo número de horas anuales trabajadas que en el anterior caso, el coste por hora sería de 27€. En la Tabla 2.1 se desglosa el coste total del personal:

Perfil	Horas	Euros/Hora	Total
Scrum Master	20	21,5	430 €
Analista de seguridad informática	300	25	7500 €
Total	320	-	7930 €

Tabla 2.1: Presupuesto de personal

Adicionalmente, hay que incluir todos aquellos gastos derivados de los recursos físicos como el alquiler de la oficina donde se desarrollará el proyecto, luz, Internet, limpieza del local o el material de oficina.

Coste del hardware

Para la realización de este proyecto se ha utilizado un ordenador portátil personal con las siguientes características:

1. Ordenador MacBook Pro 11.2:

- Procesador: 2,5 GHz Intel Core i7 de 4 núcleos
- Velocidad del procesador: 2,5 GHz
- RAM: 16 GB 1600 MHz DDR3
- Disco duro: 250 GB.
- Tarjeta gráfica: Intel Iris Pro 1536 MB
- Monitor: Retina, 15"

Se trata de un equipo que rondaría un coste de 1.399€ en total. El tiempo de amortización sería de 3 años, repercutiendo en el proyecto los 2 meses de duración, lo que supondría un coste de 77,72€ tal y como se muestra en la Tabla 2.2

Modelo	Coste (Euros)	Amortización	Proyecto	Total
MacBook Pro 11.2	1.399,00 €	3 años (38,86 €/mes)	2 meses	77,72 €

Tabla 2.2: Presupuesto de Hardware

Beneficio Industrial

Se trata del porcentaje de beneficio que se obtiene de los resultados generados, que en este caso será del 11 % de los gasto de personal de la Tabla 2.1 y de hardware de la Tabla 2.2 y que se representa en la Tabla 2.3:

Concepto	Coste (Euros)
Costes de personal	7.930,00 €
Costes de hardware	77,72 €
Subtotal	8.007,72 €
Beneficio industrial (11 %)	880,75 €

Tabla 2.3: Beneficio industrial

Coste total

A continuación se muestran los datos correspondientes al coste total representados en la Tabla 2.4:

Concepto	Coste (Euros)
Costes de personal	7.930,00 €
Costes de hardware	77,72 €
Beneficio industrial (11 %)	880,75 €
Subtotal	8.888,47 €
IVA (21 %)	1.866,58 €
Total Proyecto	10.755,05 €

Tabla 2.4: Presupuesto total

2.2. Plan de trabajo

Esta sección se corresponde con las tareas e hitos que se han llevado a cabo e identificado para la consecución del proyecto. Cada tarea irá acompañada de la estimación de tiempo necesaria para darla por concluida.

2.2.1. Identificación de tareas

A continuación se muestra el listado de tareas que se han definido en relación a los sprints planificados:

- **Sprint 1:** se corresponde con la fase de estudio e investigación del estado del arte en donde se define el contexto y las bases del trabajo a realizar:

2 de marzo de 2025 - 13 de abril de 2025

- Definición de objetivos y requisitos técnicos para llevar a cabo la propuesta.

- Análisis histórico del ransomware y su estado actual.
 - Relación del ransomware con la red TOR y los sitios de publicación de leaks.
 - Análisis del modelo de negocio RaaS y la relación con los principales grupos de ransomware que operan en la actualidad.
- **Sprint 2:** planificación y preparación del entorno de trabajo.

13 de abril de 2025 - 16 de abril de 2025

- Instalación de máquina virtual.
- Pruebas de concepto de herramientas destinadas al análisis estático.
- Pruebas de concepto de herramientas destinadas al análisis dinámico.

- **Sprint 3:** Análisis estático de la muestra.

17 de abril de 2025 - 30 de abril de 2025

- Obtención de hashes. Información de composición del binario.
- Análisis de la cabecera del binario.
- Análisis de librerías y strings.
- Análisis de código ensamblador.

- **Sprint 4:** Análisis dinámico de la muestra.

1 de mayo de 2025 - 15 de mayo de 2025

- Análisis de ejecución del fichero: monitorización de CPU, memoria e I/O.
- Análisis post ejecución: archivos cifrados.
- Análisis de la nota de rescate.

- **Sprint 5:** Elaboración del informe de resultados.

16 de mayo de 2025 - 31 de mayo de 2025

2.2.2. Estimación de tareas

El presente proyecto se basa en el análisis de una potencial amenaza como es el ransomware. Por este motivo, una de las principales tareas desarrolladas ha sido profundizar en este concepto, conocer su entorno, dónde opera, cuáles son los sitios

utilizados para publicar los datos sustraídos o los principales grupos que hacen uso de este tipo de malware para perpetrar sus ataques. Adicionalmente, tal y como se ha indicado en apartados anteriores, se ha realizado haciendo uso de la metodología *scrum*.

Esto implica la planificación de tareas independientes con una evolución y desarrollo continuo denominadas *Sprints*. En el transcurso de estas fases, se realizan reuniones de planificación y revisión.

El presente proyecto de análisis de una muestra de ransomware tipo CriptoLocker se ha dividido en 5 fases las cuales se detallan a continuación:

1. Fase de aprendizaje e investigación

Esta fase se ha basado en el estudio del estado del arte del tipo de malware conocido como ransomware. Para comprenderlo mejor, se estudian los diferentes tipos y grupos más relevantes. Con el objetivo de no incidir en grupos bastante conocidos de los se cuenta con bastante conocimiento y publicaciones, se ha elegido un tipo de ransomware del que no existe demasiada información, llamado CriptoLocker.

Para poder conocer cómo opera se han tenido que consultar y analizar diferentes publicaciones y artículos científicos relevantes, permitiendo obtener una visión actual de las técnicas más utilizadas para su propagación y detección cuyo resultante es forjar una base sólida de conocimiento en este campo de la ciberseguridad.

2. Preparación del entorno de trabajo

Esta fase engloba el *sprint 2* y ha consistido en la preparación y configuración de un entorno adaptado y securizado, de tal manera que la detonación de una muestra de ransomware no provoque daños locales irreparables. En este entorno virtualizado se realizará tanto el análisis estático como el dinámico. Por último se selecciona una muestra para poder llevar a cabo el estudio.

3. Análisis estático de la muestra

Se corresponde con el *sprint 3* en la que se analiza la estructura del archivo malicioso sin llevar a cabo su ejecución. Esto implica obtener sus hashes, investigar de qué secciones está compuesto el binario, obtener información de la cabecera del archivo malicioso y llevar a cabo un análisis de librerías, strings y código en lenguaje ensamblador.

4. Análisis dinámico de la muestra

Esta fase, que se corresponde con el *sprint* 4, se basa en la detonación de la muestra en un entorno completamente controlado lo cual permitirá conocer datos como los consumos de memoria o CPU, así como la resultante del cifrado de archivos o la nota de rescate generada.

5. Análisis de resultados y elaboración del informe

Correspondiente al *sprint* 5, en esta fase se recopilará toda la información obtenida, se evaluarán los resultados analizados y se procederá con la redacción del informe que acumule la información resultante. de todo lo establecido anteriormente.

Investigación (*Sprint* 1):

2.2.3. Planificación de tareas

Para facilitar la planificación de las tareas, se ha elaborado el siguiente diagrama de Gantt que se corresponde con la Figura 2.2, donde se pueden observar los tiempos planificados. El tiempo total para el desarrollo del proyecto ha sido estimado en 3 meses, dedicando 5 horas de trabajo diarias, siendo marzo el mes de comienzo, y mayo el de final.



Figura 2.2: Diagrama de Gantt con la planificación de las tareas

Especificando tiempos y fases, la resultante sería la siguiente:

- Investigación (*Sprint* 1): 2 de marzo de 2025 - 13 de abril de 2025

Los participantes en esta fase han sido el *Scrum Master* y el analista de seguridad informática participando en la reunión de planificación de tareas a realizar en el presente *sprint* y planteamiento de objetivos y requerimientos técnicos, que se corresponden con el análisis del estado del arte del ransom-

ware, la relación del ransomware con la red TOR y el análisis del modelo de negocio RaaS.

- Preparación del entorno de trabajo: 13 de abril de 2025 - 16 de abril de 2025

Los participantes en esta fase han sido el *Scrum Master* y el analista de seguridad informática de cara a determinar la muestra a analizar y los pormenores relacionados con el entorno controlado en el que se realizarán las pruebas tanto estáticas como dinámicas incluyendo la instalación del entorno virtual y las pruebas de concepto necesarias de las herramientas.

- Análisis estático de la muestra: 17 de abril de 2025 - 30 de abril de 2025

Los participantes en esta fase han sido el *Scrum Master* y el analista de seguridad informática que determinaron conjuntamente cuáles son las tareas relacionadas con el análisis estático de la muestra de ransomware, que incluirán la obtención de hashes, el análisis del binario que comprenderá cabecera, librerías strings y código en lenguaje ensamblador.

- Análisis dinámico de la muestra: 1 de mayo de 2025 - 15 de mayo de 2025

Los participantes en esta fase han sido el *Scrum Master* y el analista de seguridad informática que determinaron conjuntamente cuáles serían las tareas relacionadas con un análisis dinámico de la muestra de ransomware, siendo las principales el análisis de memoria y CPU, análisis y extensión de ficheros cifrados o el análisis de la nota de rescate.

- Elaboración del informe de resultados: 16 de mayo de 2025 - 31 de mayo de 2025

En este caso la participación de esta fase se basa únicamente en el analista de seguridad informática, que será el encargado de desarrollar el informe que aglutine todos los datos y conclusiones que se hayan podido detectar y determinar una vez hayan concluido todos los análisis y estudios.

2.3. Gestión de recursos

Esta sección alberga el detalle de los recursos utilizados para la elaboración y desarrollo de este proyecto, incluyendo tanto los humanos como los físicos:

2.3.1. Especificación de recursos

Recursos humanos:

- *Scrum Master.*
- Analista de seguridad informática.

Recursos materiales

- Oficina para el desarrollo del proyecto (junto con la luz, línea de Internet y limpieza del local).
- Ordenador personal.

2.3.2. Asignación de recursos

Asignación de un ordenador personal a cada miembro del equipo junto con material de oficina que fuere necesario, luz e Internet. Con este material, el equipo puede realizar el análisis y estudio del ransomware.

2.4. Gestión de riesgos

2.4.1. Identificación de riesgos

Se trata de un apartado fundamental a la hora de planificar un proyecto ya que el objetivo y fin del mismo podría verse afectado. Con este análisis se trataron de identificar los principales riesgos asociados para plantear acciones de reducción o mitigación asociadas a cada uno.

Con independencia de que existen numerosos tratamientos y guías para la gestión de riesgos, en esta caso, se ha tenido a bien utilizar como referencia el modelo de calidad CMMI (por sus siglas en inglés *Capability Maturity Model Integration*) [18], que tanto en su versión de desarrollo (CMMI-DEV) como en la de servicios (CMMI-SVC), recoge un proceso para la gestión de riesgos conocido como RSKM (*Risk Management*), el cual, a pesar de estar indicado a partir del nivel 3 de madurez, define las claves para la gestión de riesgos de un proyecto como parte del proceso de mejora continua en gestión de la calidad.

Junto con esta matriz, se clasificarán los riesgos en base a tres categorías:

- Riesgos externos, relacionados con factores externos como pueden ser la legislación, el acceso a muestras o factores vinculados a proveedores.

- Riesgos técnicos, que en este caso estarían relacionados con fallos provocados por las tecnologías utilizadas, complejidad del análisis de la muestra o con el rendimiento.
- Riesgos de la organización y dirección (en la matriz de riesgos Org.) de proyecto, relacionados con la disponibilidad de los recursos, financiación, gestión de las tareas, incumplimiento de objetivos o pérdida de datos.

2.4.2. Análisis de riesgos

Para analizar los riesgos identificados que podrían tener impacto en el desarrollo del presente proyecto, se ha utilizado la matriz de Registro y Evaluación de Riesgos conforme al modelo *CMMI for Development* (CMMI-DEV). Esta matriz identifica riesgos, los categoriza, establece un impacto y una probabilidad, que determinarán el nivel de riesgo, una estrategia de mitigación o contingencia y un responsable de la misma.

La descripción de cada columna sería la siguiente:

- **ID.** Identificador único de cada riesgo.
- **Riesgo.** Breve descripción del riesgo identificado. Debe ser clara y concisa.
- **Categoría (Cat.).** Categorización de riesgos establecida para el actual proyecto.
- **Probabilidad (Prob.).** Define la probabilidad de que el riesgo ocurra. Esta podrá ser Alta/Media/Baja.
- **Impacto (Imp.).** Define el nivel de afectación al proyecto en caso de que llegara a ocurrir. Podrá ser Alto/Medio/Bajo
- **Nivel.** Será la resultante de combinar probabilidad e impacto (Alto, Medio, Bajo, Crítico).
- **Estrategia de mitigación (Estr.).** Acciones a llevar a cabo de cara a reducir la probabilidad o el impacto el riesgo (y por lo tanto, el nivel).
- **Responsable (Resp.).** Persona (o rol), responsable de monitorizar o ejecutar acciones sobre el riesgo identificado.

La Matriz sería la siguiente:

ID	Riesgo	Cat.	Prob.	Imp.	Nivel	Estr.	Resp.
01	Acceso a las muestras de RW	Externo	Medio	Alta	Alto	Tener identificadas varias fuentes de acceso.	Analista
02	Falta de información sobre CoinsLocker	Externo	Medio	Medio	Medio	Búsquedas activas incluyendo red TOR.	Analista
03	Fallo en herramientas aplicadas	Técnico	Baja	Medio	Bajo	Disponer de herramientas alternativas.	Analista
04	Complejidad de la muestra	Técnico	Alta	Alto	Alto	Adquirir conocimientos de lenguaje ensamblador.	Analista
05	Retraso de entregables	Org.	Media	Bajo	Bajo	Adaptarse a nuevas planificaciones.	Analista
06	Pérdida del documento	Org.	Baja	Alto	Alto	Realización de <i>backups</i> y uso de herramientas <i>cloud</i> .	Analista
07	Desajustes presupuestarios	Org.	Baja	Medio	Medio	Realizar modificaciones en base a la nueva situación.	Analista

Riesgo 01: Acceso a las muestras de RW. Este riesgo está asociado a la dificultad de encontrar una muestra de la familia que se pretende analizar para el estudio o bien, que la muestra identificada en un momento de la línea temporal del desarrollo del análisis desaparezca. Como solución se propone tener identificadas varias fuentes de descarga de muestras así como la identificación de foros donde se puedan encontrar hashes para la facilitación de búsquedas.

Riesgo 02: Falta de información sobre CoinLocker. A pesar de tipificarse como medio, es uno de los riesgos que puee llegar a producirse ya que, hasta que no se realice una búsqueda exahustiva de información sobre esta familia de ransomware, no se sabrá si el riesgo se produce, ni cuál podrá ser su impacto. En aras de prevenir un nivel alto de afectación, se acumulará información sobre el desarrollo histórico que pueda abarcar un amplio periodo temporal de cara a proponer una evolución histórica de esta familia o sus relaciones con otros grupos.

Riesgo 03: Fallo en herramientas aplicadas. Esto podría producirse por errores en la compatibilidad de dispositivos y herramientas, modificaciones de software o cambios en las políticas de uso de las mismas. Como solucio se propone contar con herramientas alternativas de tal forma que si fallara una, se tuviera otra de similares características y resultados.

Riesgo 04: Complejidad de la muestra. Al tratarse de una muestra asociada a un grupo del que no se tiene demasiada información, unido a la rápida evulución del ransomware, podría dificultarse el análisis de la muestra seleccionada. Conocer el lenguaje ensamblador o los diferentes algoritmos de cifrado serán tareas a realizar como medidas de contingencia de este riesgo.

Riesgo 05: Retraso en entregables. Se trataría de incumplir los objetivos marcados en la planificación de las tareas o *sprints*. Estos retrasos podrían estar asociados a la falta de experiencia en el análisis de ransomware o a factores externos relacionados con la actividad laboral y familiar. Como contramedida se propone una replanificaciòn consensuada con el *Scrum Master* para que, en caso de que se llegara a producir, se pudiara adaptar la nueva planificación a las nuevas situaciones identificadas.

Riesgo 06: Pérdida del documento. Este riesgo hace alusión al presente documento de análisis. Para evitar que se produzcan estos riesgos de alto nivel, se recomienda la realización de copias de seguridad (*backups*) así como el uso de herramientas cloud que puedan garantizar la integridad y disponibilidad de la información almacenada.

Riesgo 07: Desajustes presupuestarios. Desajustes que pudieran provocar dificultades en el desarrollo del proyecto. Para evitarlo, el presupuesto deberá contar con una horquilla económica suficiente y adaptarse a eventualidades que pudieran surgir.

2.4.3. Legislación y normativa

Este apartado trata de identificar las leyes y normas que aplican al actual proyecto.

En primer lugar y, dado que una de las particularidades del ransomware es el robo de información confidencial (datos personales, sensibles, credenciales, etc.), es de obligado cumplimiento mencionar el *Reglamento General de Protección de Datos* [25]. En dicho reglamento se estipulan qué acciones se deben tomar ante una violación de la seguridad de datos protegidos, debiéndose realizar en un período de 72h desde su conocimiento. Adicionalmente contempla los principios de confidencialidad e integridad de la información. Esto englobaría los datos personales que sean tratados en cualquier organización de tal forma que se asegure su tratamiento y se garantice protección frente a terceros no autorizados, accesos ilícitos o contra su pérdida, destrucción o daño.

Si hablamos de sectores de alto riesgo (energía, salud, agua, servicios financieros, TIC o la misma Administración Pública), donde se podrían incluir todo tipo de infraestructuras críticas, las medidas en materia de ciberseguridad a nivel del territorio de la UE se recogen en la conocida como NIST2 (UE 2022/2555) [24], que viene a reemplazar a la NIS 2016/1148 ampliando su alcance. Esta directiva viene a garantizar y elevar el nivel de ciberseguridad de toda la UE aumentando la resiliencia de todo tipo de organizaciones frente a las amenazas, notificando en un plazo de 24 horas a la autoridad nacional competente cualquier tipo de incidente significativo.

A nivel nacional también existen normativas y leyes orientadas a garantizar la seguridad de la información. En esta línea contamos con la *Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD)* [8], antiguamente conocida como Ley Orgánica de Protección de Datos (LOPD), que es la que se encargó de adaptar la legislación española al RGPD.

El Real Decreto 311/2022 conocido como *Esquema Nacional de Seguridad* [9], de obligado cumplimiento para todas las administraciones públicas y empresas que

presten servicios a las mismas, establece los requisitos mínimos y medidas de seguridad para proteger la información tratada electrónicamente en las mismas.

En cuanto al Código Penal, el artículo 197 [6] regula los delitos de descubrimiento y revelación de secretos que incluye accesos no autorizados a sistemas, la interceptación de comunicaciones, la difusión de datos o contenidos obtenidos ilícitamente o la distribución de herramientas diseñadas para acometer el delito. El artículo 264 [7] se recogen los delitos relacionados con la destrucción, deterioro, alteración de datos o sistemas (esto incluye accesos no autorizados a sistemas y posterior cifrado de su contenido, tal y como hace el ransomware).

Como se puede comprobar, el marco normativo vigente en materia de ciberseguridad, tanto a nivel europeo como nacional, está orientado en la protección frente a amenazas como el ransomware. Normas como el RGPD, la NIS2 o el ENS obligan a empresas y administraciones a garantizar la protección de sus sistemas y datos, fomentando una cultura de prevención y respuesta frente a ciberataques. Además, herramientas como la *Guía Nacional de Notificación y Gestión de Ciberincidentes* [10] aprobada por el Consejo Nacional de Ciberseguridad ofrecen pautas prácticas para actuar con rapidez y eficacia ante este tipo de amenazas, fortaleciendo la capacidad de respuesta ante las mismas.

Capítulo 3

Solución

Una vez recopilados y expuestos todos los datos relacionados con el estudio que representa el presente documento, planificadas las tareas, estimados los costes, en el presente apartado, se propone la solución a la cuestión planteada que incluye los análisis realizados sobre la muestra seleccionada.

3.1. Descripción de la solución

El presente documento se ha basado en el análisis de una muestra de ransomware de la familia CoinLocker. Cabe destacar que no existe información sobre este variante, incluso podría tratarse de una designación genérica o interna utilizada por ciertos motores antivirus para referirse a una variante de ransomware que comparte características con otras familias conocidas, como CryptoLocker.

La primera aparición de CryptoLocker data de entre septiembre de 2013 y finales de mayo de 2014. Se trata de un virus tipo Troyano orientado a sistemas Windows que utilizaba como vector de entrada a los sistemas falsos correos electrónicos suplantando a empresas como FedEx o UPS y, especialmente diseñados para engañar a usuarios.

Una vez se desplegaba el código malicioso, este cifraba archivos ubicados en unidades de red, USBs, discos duros externos o archivos compartidos, tanto en red y en algunas unidades, hasta en la nube. Se estima que, en noviembre de 2013, CryptoLocker pudo haber infectado unos 34.000 equipos, de las cuales más de 10.000 se habrían producido en EEUU [64].

Al no tratarse de un virus o gusano con capacidad de replicarse, los desarrolladores de CryptoLocker, con el fin de propagar la infección de este ransomware, hicieron uso de una botnet conocida como Gameover ZeuS, que fue desmantelada en el año 2014 por una gran operación internacional llamada **Operación Tovar** [45].

En ese mismo año, *Fox-IT* y *FireEye* publicaron un portal denominado *Decrypt Cryptolocker*, que permitió el descifrado de archivos. A pesar de esto, se considera que aproximadamente el 1,3 % de infectados pagaron el rescate, cuyo montante total se cree que rondó los 300 millones de dólares [4].

CriptoLocker hacía uso del cifrado asimétrico, de tal forma que utilizaba un par de claves, una pública para el cifrado (RSA de 2048 bits), y otra privada únicamente conocida por sus creadores que permitiría el descifrado. Una vez que infectaba a la víctima mostraba una pantalla de advertencia indicando que los datos serían destruidos en tanto no se pagara un rescate para obtener la clave privada.

El primer paso para plantear la solución ha sido conocer el contexto general en el que se desarrolla el Ransomware, sus características, tipos así como cualquier información relevante relacionada. Posteriormente y, una vez conocidas algunas de las características de este tipo de ransomware, se ha procedido con un análisis estático y dinámico de una muestra de CryptoLocyer.

3.2. El proceso de desarrollo

El estudio del ransomware CoinLocker se ha realizado sobre una muestra que contiene las siguientes características representadas en la Tabla 3.1:

Hash	Valor
MD5	a88a0aa62a9e29cc30948b721e9e8b52
SHA-1	45b71da84aca13b69dd9c8cb21b815260c23a215
SHA-256	9d70b9e0df50aedb0a5864fc53b4c738b5725e4fec5286f723b52eef0c709211

Tabla 3.1: Principales Hashes de la muestra a analizar

3.2.1. Análisis estático

El objetivo de realizar un análisis estático es la obtención de información del fichero que detona el ransomware sin necesidad de ejecutarlo de tal forma que pueda entenderse su funcionamiento y extraer información como por ejemplo *strings*, en

qué lenguaje está programado, enlaces (que podrían ser hacia la red TOR), etc. Adicionalmente se puede bajar al código más básico haciendo uso de un desensamblador que traduzca este tipo de código en instrucciones.

Herramienta ExeInfo PE

Para comenzar el análisis del binario, se ha analizado en primer lugar la compilación del malware. Para este análisis se ha utilizado la herramienta ExeInfo PE, cuyo resultado se muestra en la Figura 3.1:

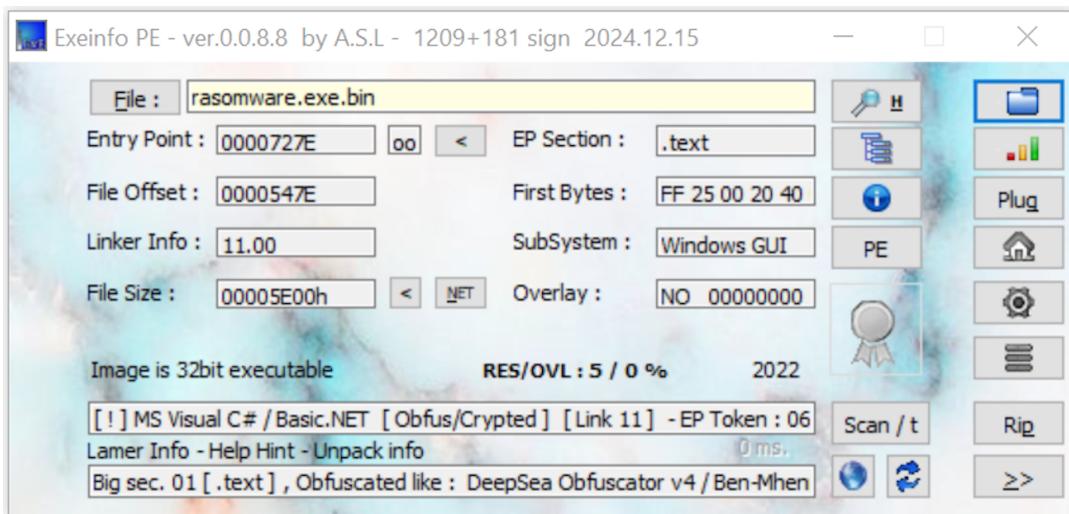


Figura 3.1: Resultados del programa ExeInfo PE relacionados con la muestra

Como se puede ver en la figura 3.1, se trata de un ejecutable orientado a sistemas Windows, en el que el *main* del código fuente (campo Entry Point), está en la dirección de memoria 0x0727E (en caso de que llegara a ejecutarse). El tamaño del archivo sería de 24 KB (el que sea un archivo tan pequeño podría dar a entender que está altamente ofuscado). Se trata de una aplicación orientada a sistemas de 32 bits (muy común en los ransomwares), cuyo más que probable año de compilación fuera el 2022.

También se puede comprobar que es una aplicación .NET y que, además, está ofuscada o cifrada, también muy común en los ransomware para evitar ser detectados, siendo el patrón utilizado para tal efecto muy similar al que genera la herramienta DeepSea Obfuscator, normalmente utilizada para proteger código (o, como en este caso, para ocultar malware).

La Figura 3.2 muestra información relacionada con las distintas secciones del binario, las cuales están relacionadas con las direcciones de memoria en las que se cargan en el momento de ejecutarse:

Figura 3.2: Resultados del programa ExeInfo PE relacionados con las secciones

Como se puede comprobar, son 3 las secciones que han sido identificadas, las cuales se explican a continuación:

- Sección *.text* (código del ejecutable). Se trata de la sección que alberga el código y por lo tanto, donde comienza la ejecución. El campo *Virtual Offset* indica la dirección de memoria donde comenzará la carga (0x2000), los campos *Virtual Size* y *RAW Size* que marcan los tamaños en memoria al ejecutarse (21.156 bytes) y en disco (21.504 bytes) respectivamente. Esta sección de por sí no ofrece información que pueda considerarse como sospechosa, ya que únicamente muestra valores de un binario que podría ser legítimo.
 - Sección *.rsrc* (recursos del ejecutable). Esta sección contiene recursos embebidos como podrían ser imágenes, iconos, mensajes, etc. En este caso el *Virtual Size* (1256 bytes) y el *RAW Size* (1536 bytes) confieren a esta sección un tamaño pequeño. Cabe destacar que un ransomware complejo podría hacer uso de recursos de varios KB o incluso MB. Esto podría ser un indicativo de que los recursos de este ransomware o bien están muy limitados, o bien podrían estar cifrados o empaquetados en otra ubicación.
 - Sección *.reloc* (relocation table). Esta sección contiene una serie de entradas que indican al sistema cómo modificar direcciones si el binario no puede cargarse en su dirección original. El tamaño de 12 bytes correspondiente al *Virtual*

Size implica que serán muy pocas las direcciones que puedan requerir de reubicación

En resumen, del análisis de las secciones se puede concluir que el binario presenta características técnicamente válidas pero que sugieren modificaciones o un posible empaquetamiento.

Herramienta HxD

Se trata de un editor en hexadecimal que permite ver otro tipo de características del binario, tal y como se muestra en la Figura 3.3:

Offset(h)	Hex	ASCII	Texto decodificado
00000000	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00	MZ.....ÿÿ..	
00000010	B8 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00@.....	
00000020	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00000030	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00e....	
00000040	0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68	...!..Í!.L!Th	
00000050	69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F	is program canno	
00000060	74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20	t be run in DOS	
00000070	6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00	mode....S.....	
00000080	50 45 00 00 4C 01 03 00 38 8D 51 63 00 00 00 00	PE.L...8.Qc....	

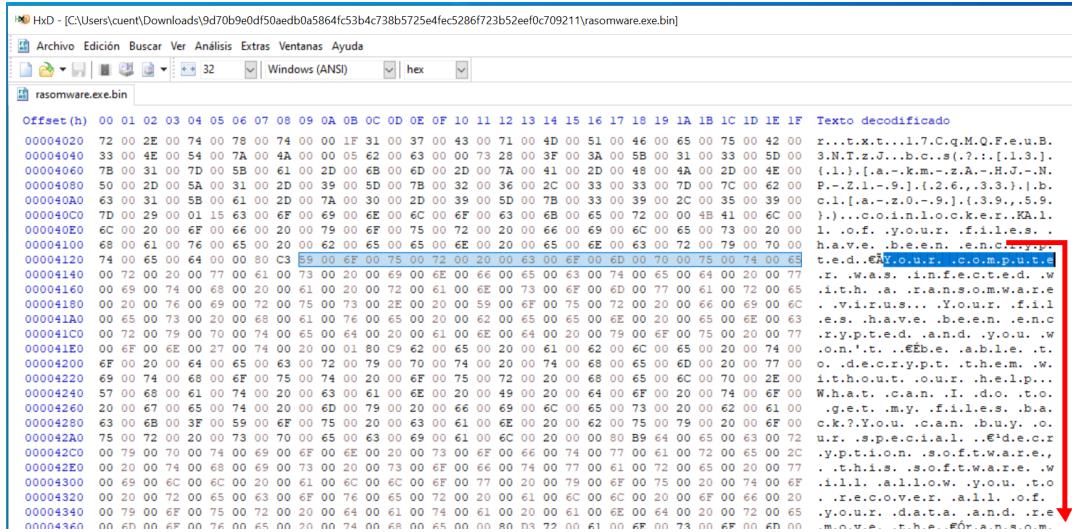
Figura 3.3: Resultados del programa HxD con las cabeceras del archivo

Las partes que se muestran en la figura 3.3 son las siguientes:

- **Magic Number.** Se trata de una firma numérica del archivo y que sirve para identificar su tipo y su formato. Este valor se encuentra en los primeros 2 bytes, siendo en este caso 4D 5A, lo que indica que se trataría de un archivo ejecutable. Estos valores en ASCII se representan con las letras MZ, visibles en el recuadro en rojo ubicado en la columna *Texto decodificado* (letras que deben su valor a las iniciales de Mark Zbikowski, uno de los desarrolladores del formato DOS).
- **This program cannot be run in DOS mode.** Se trata de una cadena estándar que forma parte de los archivos ejecutables de Windows, la cual, únicamente se mostraría si se intentara detonar un archivo ejecutable (por ejemplo, un .exe), en un entorno DOS.
- **PE Header.** Este tercer valor destacado de la figura 3.3, indica que se trata de un archivo tipo *Portable Executable*, es decir, ejecutable de Windows (.exe, .dll, etc.), lo que definirá cómo debe cargarse y ejecutarse en memoria. Esta

estructura comienza con la firma PE\0\0 (50 45 00 00 en hexadecimal), y contiene información esencial para el sistema, como la organización del archivo, secciones, direcciones y tamaños, etc.

Otro de la información que se ha extraído con HxD es la nota de rescate, tal y como se muestra en la Figura 3.4:



```

HxD - [C:\Users\cuent\Downloads\9d70b9e0df50aedb0a5864fc53b4c738b5725e4fe5286f723b52ee0c709211\rasomware.exe.bin]
Archivo Edición Buscar Ver Análisis Extras Ventanas Ayuda
hex Windows (ANSI) 32
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F Texto decodificado
00004020 72 00 2E 00 74 00 78 00 74 00 00 1F 31 00 37 00 43 00 71 00 4D 00 51 00 46 00 65 00 75 00 42 00 r...t.x.t...1.7.C.q.M.Q.F.e.u.B.
00004040 33 00 4E 00 54 00 7A 00 4A 00 00 05 62 00 63 00 00 73 28 00 3F 00 3A 00 5B 00 31 00 33 00 5D 00 3.N.T.z.J...b.c.s(.?.:.[1.3].N.
00004060 7B 00 31 00 7D 00 5B 00 61 00 2D 00 6B 00 6B 00 2D 00 7A 00 41 00 2D 00 48 00 4A 00 2D 00 4E 00 {.1.].[a.-k.m.-z.A.-H.J.-N.
00004080 50 00 2D 00 5A 00 31 00 2D 00 39 00 5D 00 7B 00 32 00 36 00 2C 00 33 00 33 00 7D 00 7C 00 62 00 P.-Z.l.-[9].).[2.6.,3.3.).|.b.
000040A0 63 00 31 00 5B 00 61 00 2D 00 7A 00 30 00 2B 00 39 00 5D 00 7B 00 33 00 39 00 2C 00 35 00 39 00 c.l.[a.-z.0.-[9].)(3.9.,5.9.
000040C0 7D 00 29 00 01 15 63 00 6F 00 69 00 6E 00 6F 00 63 00 6B 00 65 00 72 00 00 4B 41 00 6C 00 )...c.o.i.n.l.o.c.k.e.r..K.A.l.
000040E0 6C 00 20 00 6F 00 66 00 20 00 79 00 6F 00 75 00 72 00 20 00 66 00 69 00 6C 00 65 00 73 00 20 00 l...o.F. .y.o.u.r. .f.i.l.l.e.s. .
00004100 68 00 61 00 76 00 65 00 20 00 62 00 65 00 65 00 6E 00 20 00 65 00 6E 00 63 00 72 00 79 00 70 00 h.a.v.e. .b.e.e.n. .e.n.c.r.y.p.
00004120 74 00 65 00 64 00 80 C3 00 6F 00 75 00 72 00 20 00 63 00 6D 00 6D 00 70 00 75 00 74 00 63 t.e.d..@T.y.o.u.r. .c.o.m.p.u.t.s.
00004140 00 72 00 20 00 77 00 61 00 73 00 20 00 69 00 6E 00 66 00 65 00 63 00 74 00 65 00 64 00 20 00 77 .r.w.a.s. .i.n.f.e.c.t.e.d. .W.
00004160 00 69 00 74 00 68 00 20 00 62 00 20 00 72 00 61 00 6E 00 73 00 6F 00 6D 00 77 00 61 00 72 00 65 i.t.h..a..r.a.n.s.o.m.w.a.r.e
00004180 00 20 00 76 00 69 00 72 00 75 00 73 00 2E 00 20 00 59 00 67 00 75 00 72 00 20 00 66 00 69 00 6C .v.i.r.u.s... .Y.o.u.r. .f.i.l.l
000041A0 00 65 00 73 00 20 00 68 00 63 00 73 00 65 00 20 00 62 00 65 00 66 00 6E 00 20 00 65 00 6E 00 63 e.s..h.a.v.e..b.e.e.n..e.n.c
000041C0 00 72 00 79 00 70 00 74 00 65 00 64 00 20 00 61 00 6E 00 64 00 20 00 79 00 6F 00 75 00 20 00 77 r.y.p.t.e.d..a.n.d..y.o.u..w
000041E0 00 6F 00 6E 00 27 00 74 00 20 00 01 80 C9 62 00 65 00 20 00 61 00 62 00 6C 00 65 00 20 00 74 00 o.n.'t..@E.b.e..a.b.l.e..t
00004200 6F 00 20 00 64 00 65 00 63 00 72 00 79 00 70 00 74 00 20 00 74 00 68 00 65 00 6D 00 20 00 77 00 o..d.e.c.r.y.p.t..t.h.e.m..w
00004220 69 00 74 00 68 00 6F 00 75 00 74 00 20 00 6F 00 75 00 72 00 20 00 68 00 65 00 6D 00 20 00 70 00 i.t.h.o.u.t..o.u.r..h.e.l.p...
00004240 57 00 68 00 63 00 74 00 20 00 63 00 61 00 6F 00 20 00 49 00 20 00 64 00 6F 00 20 00 74 00 6F 00 W.h.a.t..c.a.n..I..d.o..t.o.
00004260 20 00 67 00 65 00 74 00 20 00 6D 00 79 00 20 00 66 00 69 00 6C 00 65 00 73 00 20 00 62 00 61 00 .g.e.t..m.y..f.i.l.l.e.s..b.a.
00004280 63 00 6B 00 3F 00 59 00 6F 00 75 00 20 00 63 00 61 00 6E 00 20 00 62 00 75 00 79 00 20 00 6F 00 c.k.7.Y.o.u..c.a.n..b.u.y..o.
000042A0 75 00 72 00 20 00 73 00 70 00 65 00 63 00 69 00 61 00 6C 00 20 00 08 B9 64 00 65 00 63 00 72 u.r..s.p.e.c.i.a.l..@d.e.c.e.r
000042C0 00 79 00 70 00 74 00 69 00 6F 00 6E 00 20 00 73 00 67 00 66 00 74 00 77 00 61 00 72 00 65 00 2C .y.p.t.i.o.n..s.o.f.t.w.a.r.e.,
000042E0 00 20 00 74 00 68 00 69 00 73 00 20 00 73 00 6F 00 66 00 74 00 77 00 61 00 72 00 65 00 20 00 77 .t.h.i.s..s.o.f.t.w.a.r.e..W
00004300 00 69 00 6C 00 6C 00 20 00 61 00 6C 00 6C 00 6F 00 67 00 77 00 20 00 79 00 6F 00 75 00 20 00 74 00 6F i.l.l..a.l.l.o.w..y.o.u..t.o
00004320 00 20 00 72 00 65 00 63 00 66 00 76 00 65 00 72 00 20 00 61 00 6C 00 6C 00 20 00 6F 00 66 00 20 .r.e.c.o.v.e.r..a.l.l..o.f.e
00004340 00 79 00 6F 00 75 00 72 00 20 00 64 00 61 00 74 00 61 00 20 00 61 00 6E 00 64 00 20 00 72 00 65 y.o.u.r..d.i.a.t.a..a.n.d..r.e
00004360 00 6D 00 6F 00 76 00 65 00 20 00 74 00 6A 00 65 00 6D 00 6A 00 61 00 6F 00 6D 00 20 00 73 00 6D 00 m.o.v.e..t.h.e.s..f.o.r.a.n.s.o.m.

```

Figura 3.4: Resultados del programa HxD donde muestra la nota de rescate

Herramienta PEview

Se trata de otra herramienta orientada al análisis de ejecutables de Windows para poder conocer su estructura interna. En este caso, se ha podido verificar que la fecha de compilación coincide con la que se refleja en Virus Total, tal y como muestra la Figura 3.5:

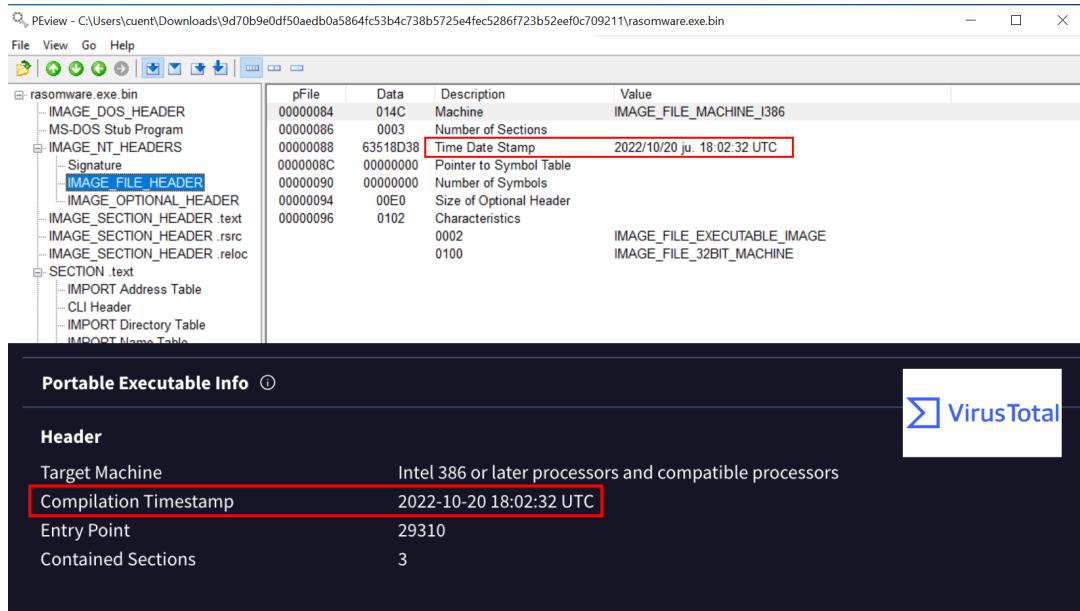


Figura 3.5: Resultados del programa PEview donde muestra la fecha de compilación

Herramienta PEStudio

Mediante el uso de esta herramienta se han podido visualizar de forma muy estructurada los strings que componen el ejecutable, como por ejemplo la nota de rescate, que se muestra en la Figura 3.6:

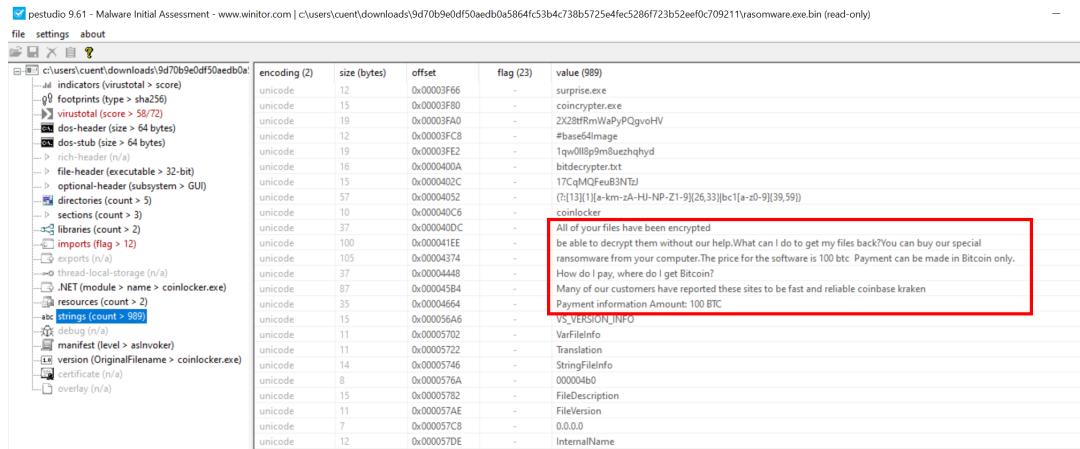


Figura 3.6: Resultados del programa PEStudio donde muestra los strings

Herramienta Ghidra

Se trata de una herramienta de ingeniería inversa desarrollada por la NSA (siglas de *National Security Agency*), agencia de inteligencia de los Estados Unidos que se

utiliza para el análisis de ejecutables y, al igual que las anteriores, para ayudar a entender el funcionamiento interno de binarios sin necesidad de ejecutarlos.

Una de las funciones que se ha podido detectar es la de cifrado de datos, denominada *AES_Encrypt*(*byte* BytesToBeEncrypted, byte* passwordBytes*).

Esta función cifra un bloque de datos (`BytesToBeEncrypted`) utilizando una contraseña (`passwordBytes`) presumiblemente, bajo el tipo de cifrado AES, tal y como se puede ver en la Figura 3.7:

```
00 00 0a ...  
*****  
* FUNCTION ...  
*****  
byte * AES_Encrypt(byte * bytesToBeEncrypted, byte * p...  
byte * EAX:4 <RETURN>  
byte * Stack[0x4]:4 bytesToBeEncrypted  
byte * Stack[0x8]:4 passwordBytes  
.NET CLR Managed Code  
AES_Encrypt  
00402604 14 0a 1e db[198]  
8d 19 00  
00 01 25 ...  
00402604 [0] 14h, Ah, 1Eh, 8Dh,  
00402608 [4] 19h, 0h, 0h, 1h,  
0040260c [8] 25h, D0h, 22h, 0h,  
00402610 [12] C0h, 00h, 00h, 00h
```

Figura 3.7: Resultados del programa Ghidra donde muestra la función AES_{Encrypt}

Si se realiza un visionado de los strings, también se puede identificar la nota de rescate, donde es visible la cantidad a pagar (100BTC), el monedero, tal y como muestra la imagen correspondiente a la Figura 3.8:

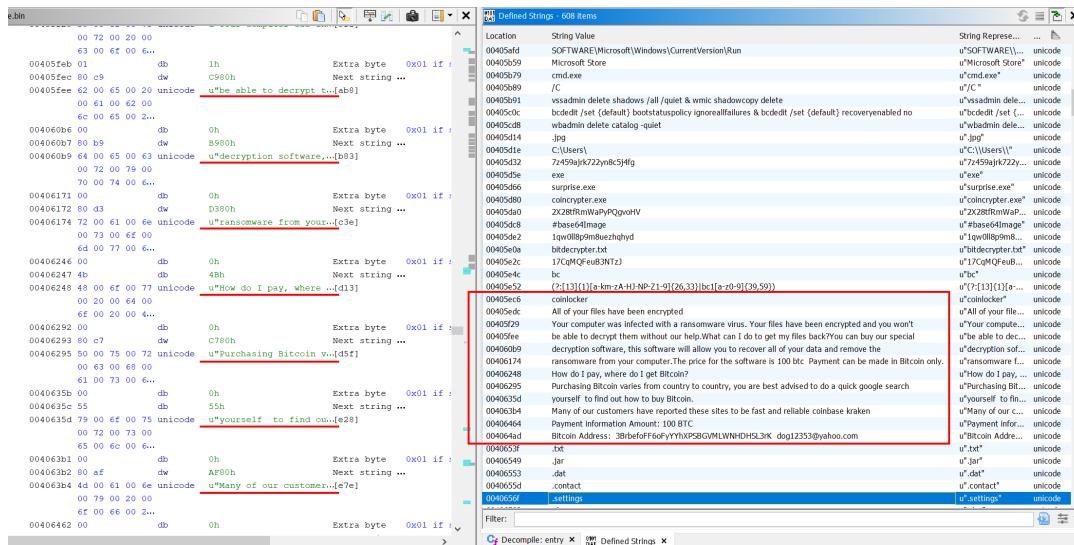


Figura 3.8: Resultados del programa Ghidra donde muestra la nota de rescate

Posteriormente, aparece un listado de extensiones que se incluirán en el cifrado, tal y como muestra la Figura 3.9:

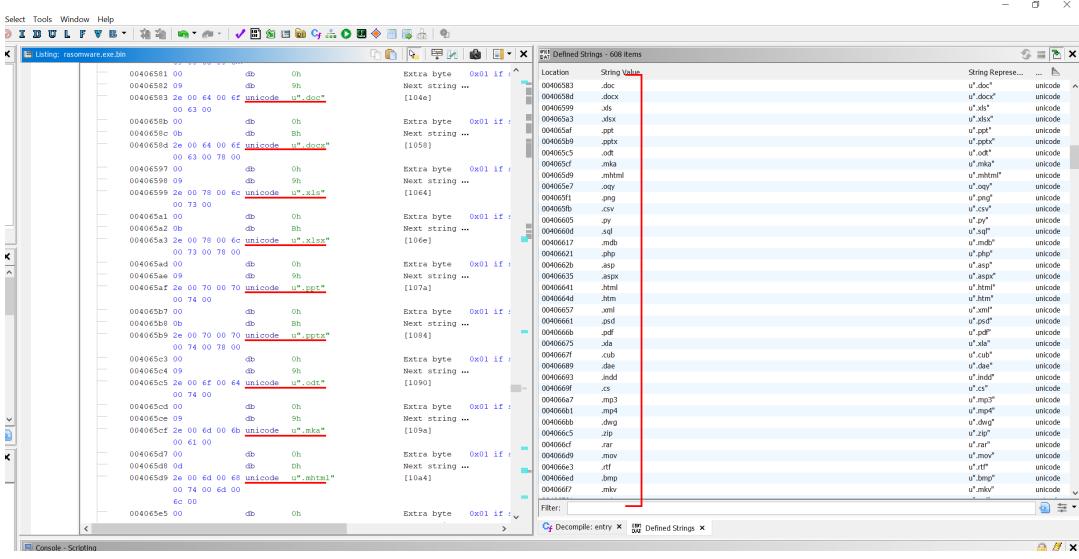


Figura 3.9: Resultados del programa Ghidra donde muestran las extensiones de ficheros a cifrar

Virus Total

Virus Total es una plataforma online destinada al análisis de archivos, URLs o Hashes cuyo principal objetivo es la búsqueda de malware para lo cual hace uso de múltiples motores antivirus o herramientas de seguridad.

Una vez subida la muestra en cuestión, se puede comprobar que 59 de 72 motores han identificado la muestra como maliciosa, tal y como muestra la Figura 3.10:



Figura 3.10: Resultados de los motores de VT que han detectado la muestra como maliciosa

Adicionalmente, dentro de la pestaña *Details* se puede encontrar información relacionada con el fichero, como pueden ser los diferentes tipos de hashes, cuyos principales valores (MD5, SHA-1 y SHA-256) se encuentran reflejados en la Tabla 3.1.

Otra información que muestra es el *Header*, cuyos valores se muestran en la Tabla 3.2:

Header	Valor
Target Machine	Intel 386 or later processors and compatible processors
Compilation Timestamp	2022-10-20 18:02:32 UTC
Entry Point	29310
Contained Sections	3

Tabla 3.2: Valores de los campos correspondientes al *Header*

Los datos aportados indican que hay 3 secciones en el *Header* que se corresponden con las mostradas anteriormente en la Figura 3.2 (".*text*", ".*rsrc*" y ".*reloc*") obtenidas con la herramienta ExeInfo PE.

En cuanto al apartado *Relations*, Virus Total muestra una serie de IPs con las que se contactaría, una de las cuales (mostrada en la Tabla 3.3), es detectada por un motor como maliciosa:

IP	Detections	Country
192.229.211.108	1/94	US

Tabla 3.3: Valores de la IP detectada por *Xcitium Verdict Cloud* como maliciosa

Otro de los aspectos a destacar son los comandos que se ejecutan en terminal (*Shell commands*), todos orientados a impedir que el sistema pueda recuperarse y a eliminar las *shadow copies*:

```

- "%ComSpec%" /C bcdeedit /set {default} bootstatuspolicy
ignoreallfailures & bcdeedit /set {default} recoveryenabled no
- "%ComSpec%" /C vssadmin delete shadows /all /quiet & wmic
shadowcopy delete
- "%ComSpec%" /C wbadmin delete catalog -quiet
- %SAMPLEPATH%
- bcdeedit /set {default} bootstatuspolicy ignoreallfailures
- bcdeedit /set {default} recoveryenabled no
- vssadmin delete shadows /all /quiet
- wbadmin delete catalog -quiet
- wmic shadowcopy delete
- "C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe" /svc

```

3.2.2. Análisis dinámico

El análisis dinámico de un malware y, más en concreto, de un ransomware es el proceso de analizar su comportamiento al ejecutarlo en un entorno controlado (por ejemplo, una sandbox o una máquina virtual) que permita ver qué hace realmente el malware al ejecutarse. De esta forma, se puede observar qué archivos modifica (en este caso, cifra), si hay o no conexiones de red, borrado de logs, elevación de privilegios, modificaciones del registro, etc.

Entorno controlado de ejecución

Para el desarrollo del actual proyecto se ha utilizado una máquina virtual Windows 10 (64-bit) junto con la herramienta de Microsoft Process Explorer, visor de procesos para Windows. Para poder detonar la muestra, ha habido que cambiar la extensión del fichero a ".exe", haciendo del fichero un ejecutable.

Una vez ejecutado el ransomware, el aspecto que presenta el equipo es el que se muestra en la Figura 3.11, donde se visibiliza la nota de rescate y los iconos figuran todos con extensión ".exe", incluyendo la barra de tareas:

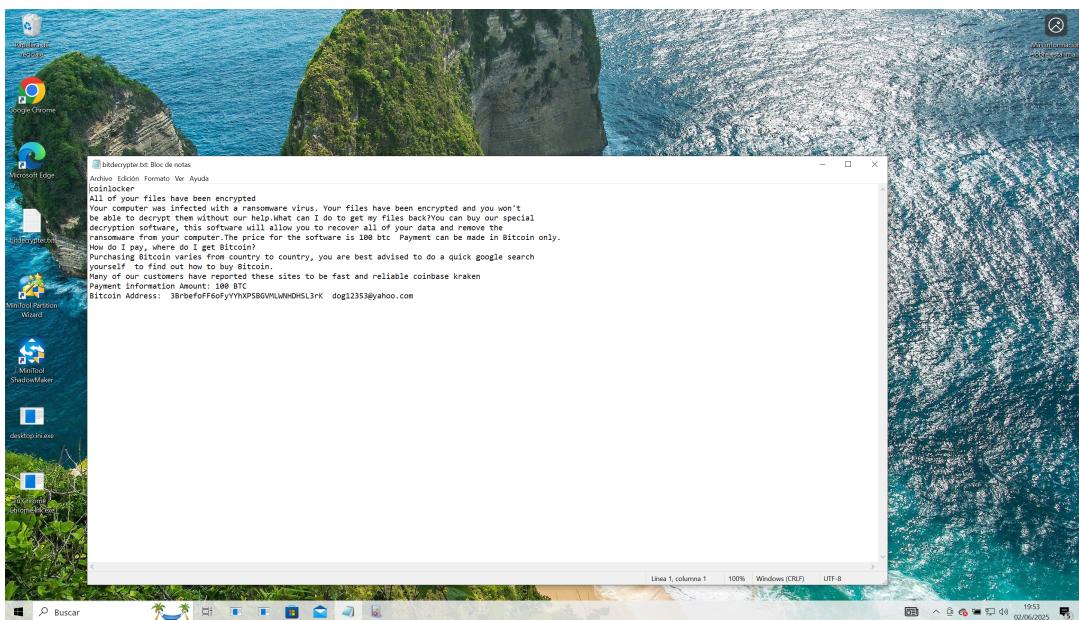


Figura 3.11: Resultado de detonar el fichero que contiene el ransomware

Atendiendo a la información del sistema obtenida en Process Explorer, se puede observar que en el momento de detonar la muestra se exigen una alta cantidad de recursos, tal y como se muestra en la Figura 3.12:

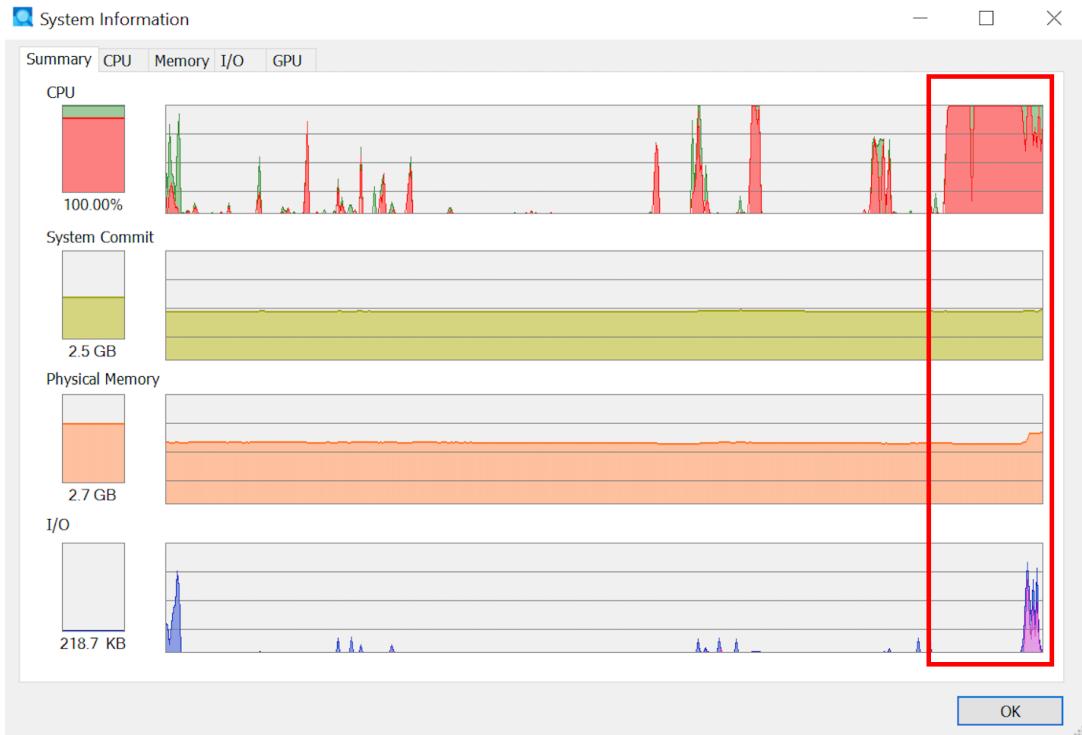


Figura 3.12: Resultados de la herramienta Process Explorer en cuanto a información del sistema

Teniendo en cuenta que todas las operaciones que el ransomware realiza sobre el disco, el consumo de CPU es el que más afectado se ve, ya que estas implican cambios en lectura y escritura de ficheros, provocados por el cifrado de los mismos, tal y como se muestra en la Figura 3.13:

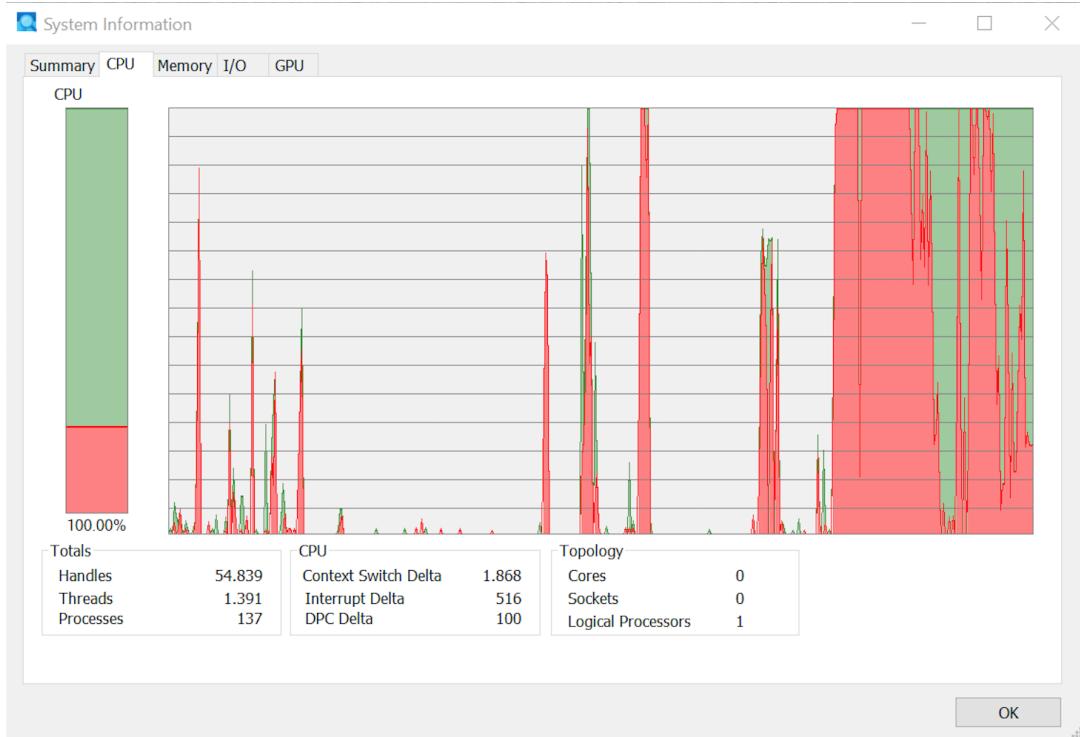


Figura 3.13: Resultados de la herramienta Process Explorer en cuanto a información de consumo de la CPU

Ejecución del ransomware en SandBox virtual

Para el desarrollo de este apartado se ha utilizado la SandBox virtual **Any Run** y **Joe Sandbox**. Se trata de herramientas a la que se accede a través del navegador web.

Para el caso de Any Run, el sistema utilizado para esta ejecución ha sido Windows Windows 10 Professional (build 19044 , 64 bit). Cabe destacar que la versión gratuita, la cual es la que se ha utilizado, únicamente permite una ejecución de 60 segundos, tiempo suficiente para comprobar que los archivos del sistema se han cifrado y ver la nota de rescate, tal y como muestra la Figura 3.14:

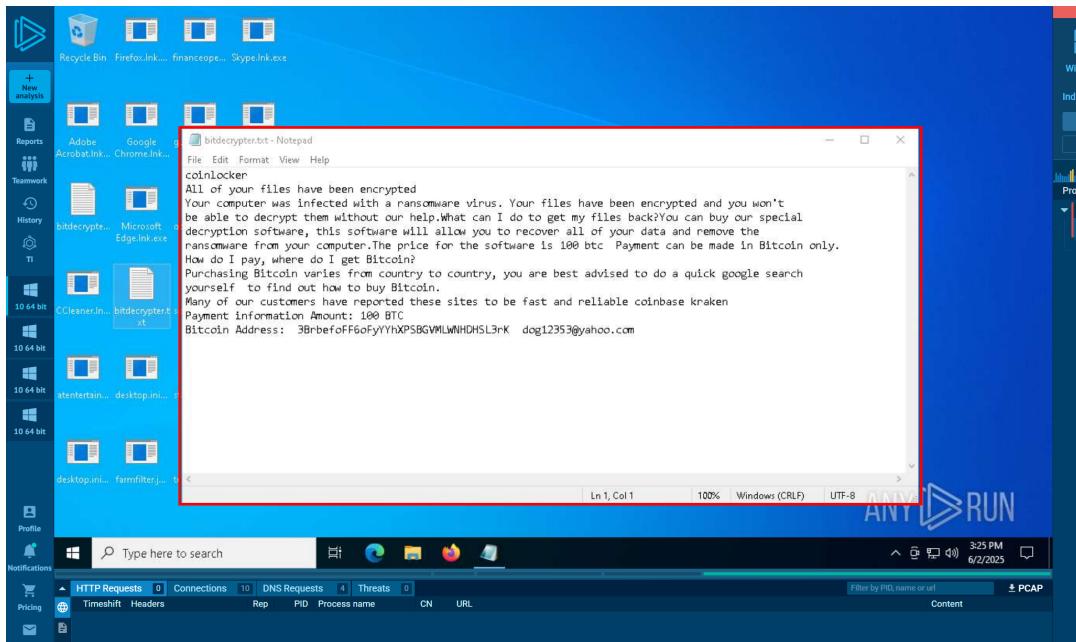


Figura 3.14: Resultados de Any Run donde muestra la nota de rescate y la familia de ransomware (coinlocker)

De los datos que se pueden consultar se destaca el gráfico que muestra la Figura 3.15, donde se pueden ver las ejecuciones que se han realizado desde la consola de Windows (cmd.exe):



Figura 3.15: Resultados de Any Run donde muestran las ejecuciones de la consola de Windows

Como se puede observar, existen una serie de ejecuciones cuyo principal objetivo es eliminar cualquier forma de recuperación del sistema, antes de que los archivos sean cifrados. El primer comando es *delete shadows /all /quiet* el cual, borra todas las copias de seguridad de volumen (shadow copies). Se trata de un tipo de copias que se utilizan para restaurar el sistema o para establecer puntos de restauración. Los parámetros que se han utilizado se pueden ver en la Figura 3.16, y son los siguientes:

- **/All:** elimina todas las copias de seguridad.
- **/quiet:** utilizado para evitar mostrar confirmación al usuario.

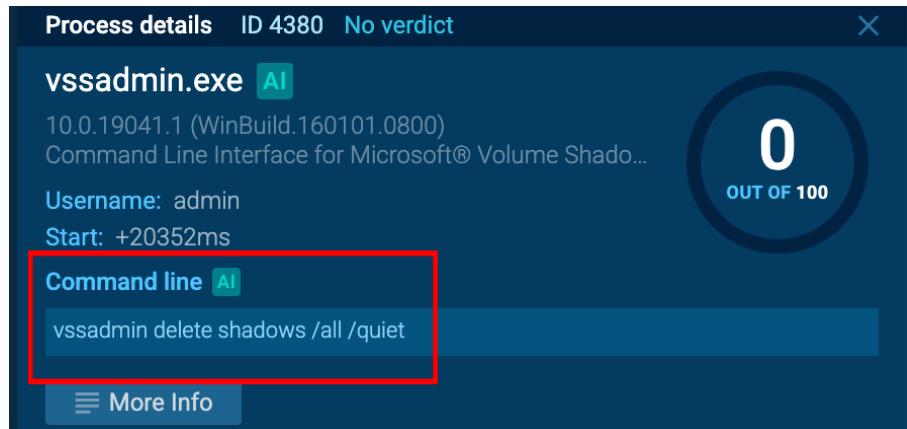


Figura 3.16: Resultados de Any Run donde la ejecución de borrado puntos de restauración

Seguidamente ejecuta el comando *wmic shadowcopy delete*, para eliminar copias de seguridad del sistema. En este caso utiliza WMIC (Windows Management Instrumentation Command-line) tal y como muestra la Figura 3.17:



Figura 3.17: Resultados de Any Run donde la ejecución de borrado de copias de seguridad utilizando WMIC

Otra de las ejecuciones orientadas al mismo fin sería "wbadmin delete catalog -quiet", mostrada en la Figura 3.18, que también tiene el objetivo de evitar una recuperación del sistema, eliminando el catálogo de copias de seguridad en este caso, utilizando VSS Admin:

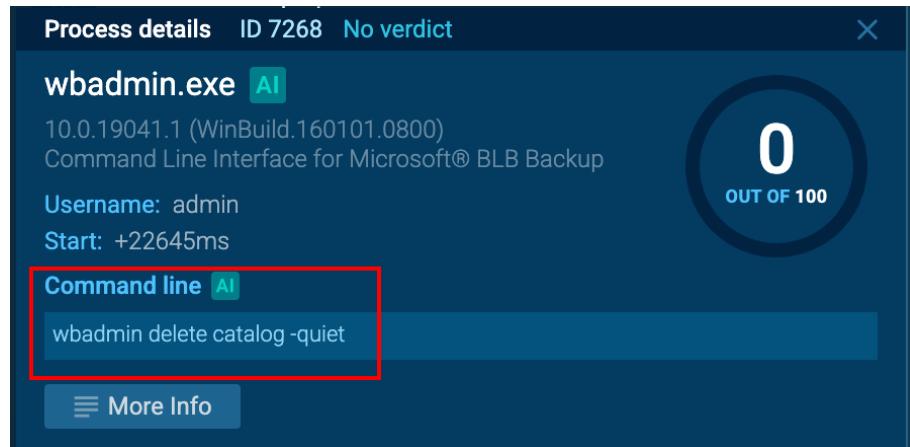


Figura 3.18: Resultados de Any Run donde la ejecución de borrado de copias de seguridad utilizando VSS Admin

Any Run también muestra qué tácticas y técnicas de ataque se han detectado durante el análisis del ransomware, organizados según el marco de referencia del MITRE ATT&CK tal y como muestra la Figura 3.19:

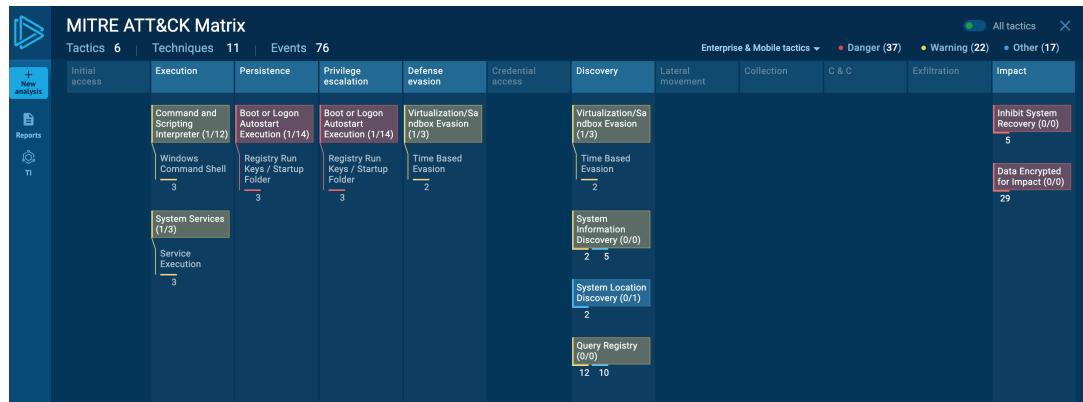


Figura 3.19: Resultados de Any Run donde se muestran tácticas y técnicas relacionadas con MITRE ATT&CK

En cuanto a información que se podido extraer de la detonación de la muestra en Joe Sandbox, destacar la creación del fichero bitdecrypter.txt que contiene la nota de rescate, tal y como se muestra en la Figura 3.20:

C:\Users\Public\Documents\bitdecryter.txt	
Process:	C:\Users\user\AppData\Roaming\coincrypter.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	841
Entropy (8bit):	4.698660703940251
Encrypted:	false
SSDEEP:	12:AMXHnJ8AiGQnGtgMZAEWtaNrO41jHUAG81oEjrPljg+c/B7Sm3v/oUfa:RXnBmMZANlmhVkr++c53JS
MD5:	F85C68FE12158C0EFB2879128BAEE80B
SHA1:	6891E95A79B09AE5FD6FF51EB88E9C53269DC3D
SHA-256:	E14340F08EE0417848D9E652E53C8A8CA34EF932CD5D4DB442514A6EB0388785
SHA-512:	B16A22CD06A871E0E00D766254628EEFEDD606B6AB70E61AB52435E03F6337C709C42BD6CE162F95900318A27ED4B533E588AFB2DAE6B27699E5EE29A6F6B3751
Malicious:	true
Preview:	coinlocker..All of your files have been encrypted..Your computer was infected with a ransomware virus. Your files have been encrypted and you won't .. be able to decrypt them without our help.What can I do to get my files back?You can buy our special ..decryption software, this software will allow yo u to recover all of your data and remove the..ransomware from your computer.The price for the software is 100 btc Payment can be made in Bitcoin only ...How do I pay, where do I get Bitcoin?.Purchasing Bitcoin varies from country to country, you are best advised to do a quick google search..yourself f to find out how to buy Bitcoin. ..Many of our customers have reported these sites to be fast and reliable coinbase kraken..Payment information Amou nt: 100 BTC..Bitcoin Address: 3BrbefoFF6ofyYhXPSBGVMLWHDHSL3rk dog1235@yahoo.com.....

Figura 3.20: Resultados de Joe Sandbox donde se muestra la creación del fichero con la nota de rescate

Adicionalmente, este análisis identifica la muestra como una amenaza tipo **Chaos**. Se trata de una familia de ransomware que fue lanzada en junio de 2021 por un actor desconocido. Aunque inicialmente fue atribuido a un trabajador de Ryuk, actualmente es una amenaza que carece características propias del ransomware, como la exfiltración de datos.

En cuanto al conjunto de procesos que se llevan a cabo en la ejecución del ransomware, Joe Sanbox traza su comportamiento de la siguiente forma que representa la Figura 3.21, donde caben destacar acciones típicas de este tipo de malware, como son duplicarse para tener persistencia, eliminar cualquier posibilidad de recuperación del sistema o mostrar una nota de rescate:



Figura 3.21: Resultados de Joe Sandbox donde se muestra el árbol de procesos que ejecuta el ransomware

Por último, otra de las comprobaciones que se realizó fue comprobar el comportamiento de diferentes tipos de ficheros una vez ejecutado el ransomware. Para ello, se creó un directorio de prueba que contenía un conjunto de ficheros. En la Figura 3.22 se muestra una comparativa del estado del mismo antes y después de ejecutar el malware:

Nombre	Fecha de modificación	Tipo	Tamaño
EJEMPLO_JPG.jpg	02/06/2025 22:27	Archivo JPG	8.589 KB
EJEMPLO_BMP.bmp	04/06/2025 17:59	Archivo BMP	0 KB
EJEMPLO_documentoPDF.pdf	04/06/2025 17:42	Microsoft Edge PDF ...	1.629 KB
EJEMPLO_DOCX.docx	04/06/2025 18:00	Documento XML abi...	0 KB
EJEMPLO_JSON.json	04/06/2025 17:58	Archivo JSON	1 KB
EJEMPLO_MP3.mp3	04/06/2025 17:53	Archivo MP3	427 KB
EJEMPLO_MP4.mp4	04/06/2025 17:39	Archivo MP4	6.051 KB
EJEMPLO_PNG.png	04/06/2025 18:04	Archivo PNG	5 KB
EJEMPLO_textoplano - abierto.txt	04/06/2025 17:46	Documento de texto	3 KB
EJEMPLO_TIFF.tif	04/06/2025 18:06	Archivo TIFF	2 KB
EJEMPLO_TXT.txt	04/06/2025 17:45	Documento de texto	0 KB
EJEMPLO_XML.xml	04/06/2025 18:01	Microsoft Edge HTM...	1 KB
EJEMPLO_ZIP.zip	04/06/2025 17:48	Carpeta comprimida ...	1 KB

Nombre	Fecha de modificación	Tipo	Tamaño
bitdecrypter.txt	09/06/2025 13:16	Documento de texto	1 KB
EJEMPLO_JPG.jpg.exe	09/06/2025 13:16	Aplicación	5.174 KB
EJEMPLO_BMP.bmp.exe	09/06/2025 13:16	Aplicación	1 KB
EJEMPLO_documentoPDF.pdf.exe	09/06/2025 13:16	Aplicación	2.172 KB
EJEMPLO_DOCX.docx.exe	09/06/2025 13:16	Aplicación	1 KB
EJEMPLO_JSON.json.exe	09/06/2025 13:16	Aplicación	1 KB
EJEMPLO_MP3.mp3.exe	09/06/2025 13:16	Aplicación	569 KB
EJEMPLO_MP4.mp4.exe	09/06/2025 13:16	Aplicación	3.646 KB
EJEMPLO_PNG.png.exe	09/06/2025 13:16	Aplicación	7 KB
EJEMPLO_textoplano - abierto.txt.exe	09/06/2025 13:16	Aplicación	4 KB
EJEMPLO_TIFF.tif	04/06/2025 18:06	Archivo TIFF	2 KB
EJEMPLO_TXT.txt.exe	09/06/2025 13:16	Aplicación	1 KB
EJEMPLO_XML.xml.exe	09/06/2025 13:16	Aplicación	2 KB
EJEMPLO_ZIP.zip.exe	09/06/2025 13:16	Aplicación	1 KB

Figura 3.22: Listado de archivos de prueba antes y después del cifrado

Como se puede observar, una vez se ha ejecutado el ransomware, en el directorio de prueba aparece la nota de rescate (también figura en el escritorio), y los archivos han pasado a tener extensión ".exe" a excepción del fichero de prueba con extensión ".tiff" que no ha sufrido daño alguno. Esto se debe a que su extensión no figura en el rango de extensiones de archivos a cifrar, tal y como muestra una búsqueda realizada en la función *validExtensions* cuyo código se ha obtenido utilizando el programa dnSpy y se muestra en la Figura 3.23:

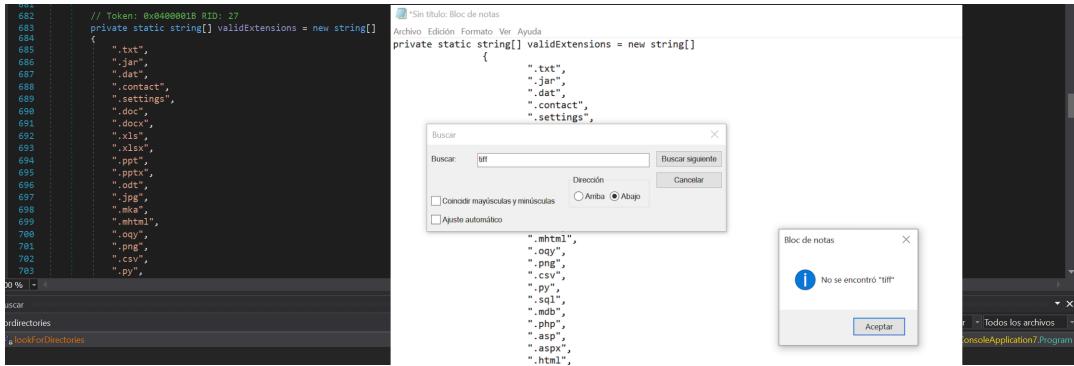


Figura 3.23: Extensión .tiff inexistente en código para cifrar

También se probó a cambiar la extensión de un fichero de texto cifrado, quitando ".exe" y dejando la extensión original. A pesar de abrirse el archivo, el contenido se mostraba cifrado. En la Figura 3.24 se muestra el contenido antes y después de ejecutar el malware:

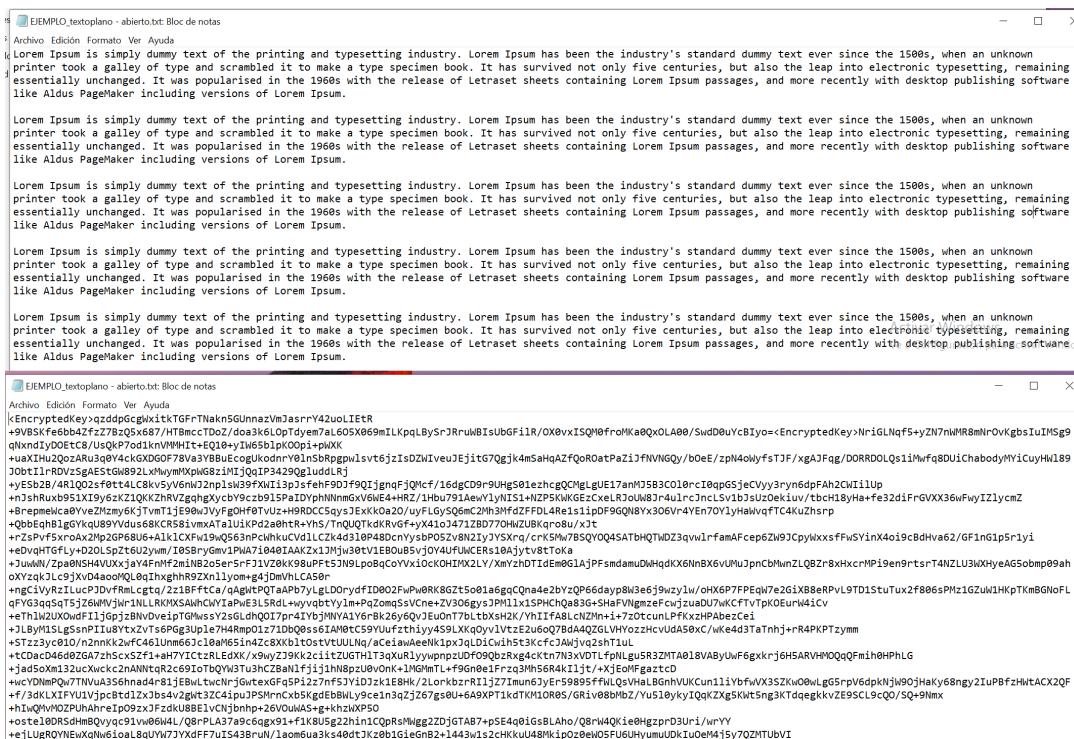


Figura 3.24: Fichero de texto antes y después del cifrado

3.2.3. Herramientas utilizadas

- ExeInfo PE:** programa que permite analizar ejecutables ".exe" utilizado en el análisis estático que identifica, entre otras cosas, el lenguaje de programación en el que está desarrollado.

- **HxD**: editor hexadecimal que permite visualizar el binario y sus strings ya que muestra el contenido tanto en formato hexadecimal como en ASCII.
- **PEview**: utilizada para analizar la estructura interna del ejecutable (cabezas, secciones, fecha de compilación, etc).
- **PEStudio**: utilizada para obtener información de amenazas como los strings en el análisis estático del ejecutable.
- **Ghidra**: utilizada para descompilar el código de un ejecutable tipo ".exe" o ".dll" y poder analizar funciones, strings o extensiones.
- **Process Explorer**: herramienta utilizada en el análisis dinámico para poder obtener información detallada de procesos Windows como el consumo de CPU o memoria en el momento de detonar el fichero malicioso.
- **Any Run**: herramienta tipo sandbox para el análisis dinámico en la nube. Permite la ejecución del fichero malicioso sin que exista afectación en el equipo pudiendo obtener información sobre procesos, conexiones o cambios en el sistema en el que se ejecuta.
- **Joe SandBox**: herramienta utilizada en el análisis dinámico ya que permite la ejecución de archivos maliciosos en un entorno controlado para analizar el comportamiento del archivo detonado y así determinar cuáles han sido las acciones catalogadas como sospechosas o directamente maliciosas las cuales quedan reflejadas en un informe junto con todos los IoCs.
- **Virtual Box**: herramienta de virtualización de sistemas operativos utilizada para contar con un entorno seguro para el estudio y posterior detonación del malware.
- **Virus Total**: herramienta online para el análisis de IoCs tales como archivos, URLs, hashes, IPS..., cuyo principal objetivo es compartir el resultado de dicho análisis para la detección de amenazas.
- **dnSpy**: herramienta de ingeniería inversa que se utiliza para el análisis y depuración de aplicaciones ".net", permitiendo la descompilación de ejecutables (.exe, .dll) y así ver su código fuente.
- **Navegador TOR**: navegador web que permite el acceso a direcciones de la *dark web*, utilizada con el objetivo de intentar acceder a sitios de grupos de ransomware y comprobar si existen filtraciones de datos provocadas por los mismos.

Capítulo 4

Evaluación

4.1. Proceso de evaluación

4.1.1. Forma de evaluación

Para evaluar este ransomware, se ha utilizado una muestra con fecha de compilación 2022-10-20 18:02:32 UTC, de la que se ha obtenido información sobre su funcionamiento, despliegue y acciones que realiza tras su detonación.

4.1.2. Casos de prueba

En la Tabla 4.1 se muestra una relación de plataformas en las que se ha analizado la muestra junto con el porcentaje de detección asociado al tal análisis:

Plataforma	Detecciones
Virus Total	81 %
Kaspersky	100 %
Hybrid Analysis	90 %
ReversingLabs	96 %
Avira	100 %
Joe Sandbox ML	100 %
Any Run	100 %

Tabla 4.1: Porcentaje de detección de plataformas

En el presente estudio, al detonarse una única muestra y, de cara a comprobar el cifrado de distintos tipos de archivos para verificar si existen varias extensiones

utilizadas por el malware, se crea un listado de diferentes archivos para tal fin. El resultado se muestra en la Tabla 4.2 donde se pudo comprobar que todos los ficheros creados se cifraron con extensión ".exe". Esto es debido a que todos estos tipos de archivos se encontraban en el propio código, el cual se pudo visualizar en el análisis estático de la muestra. En el caso de ejemplo, la extensión ".tiff\"", al no encontrarse en dicho código, no se cifró.

Fichero sin cifrar	Fichero cifrado
EJEMPLO_JPG.jpg	EJEMPLO_JPG.jpg.exe
EJEMPLO_BMP.bmp	EJEMPLO_BMP.bmp.exe
EJEMPLO_documentoPDF.pdf	EJEMPLO_documentoPDF.pdf.exe
EJEMPLO_DOCX.docx	EJEMPLO_DOCX.docx.exe
EJEMPLO_JSON.json	EJEMPLO_JSON.json.exe
EJEMPLO_MP3.mp3	EJEMPLO_MP3.mp3.exe
EJEMPLO_MP4.mp4	EJEMPLO_MP4.mp4.exe
EJEMPLO_PNG.png	EJEMPLO_PNG.png.exe
EJEMPLO_textoplano-aberto.txt	EJEMPLO_textoplano-aberto.txt.exe
EJEMPLO_TIFF.tiff	EJEMPLO_TIFF.tiff
EJEMPLO_TXT.txt	EJEMPLO_TXT.txt.exe
EJEMPLO_XML.xml	EJEMPLO_XML.xml.exe
EJEMPLO_ZIP.zip	EJEMPLO_ZIP.zip.exe

Tabla 4.2: Porcentaje de detección de plataformas

En cuanto a información mostrada por la nota de rescate tras detonar el ransomware, en la Tabla 4.3 se pueden comprobar los datos que se muestran, basados en una cartera de bitcoin, la cantidad (100 BTC), y un correo electrónico:

Tipo	Información nota de rescate
Cartera de bitcoin	3BrbefoFF6oFyYYhXPSBGVMLWNHDHSL3rk
Correo electrónico	dog12353@yahoo.com
Cantidad	100 BTC

Tabla 4.3: Datos mostrados en la nota de rescate

Con respecto a los consumos, se realizaron varias detonaciones de la muestra para verificar el consumo de CPU en cada una de ellas, no llegando en ningún caso al 100% y siendo la primera detonación la que más recursos consumió, tal y como se puede ver en la Tabla 4.4:

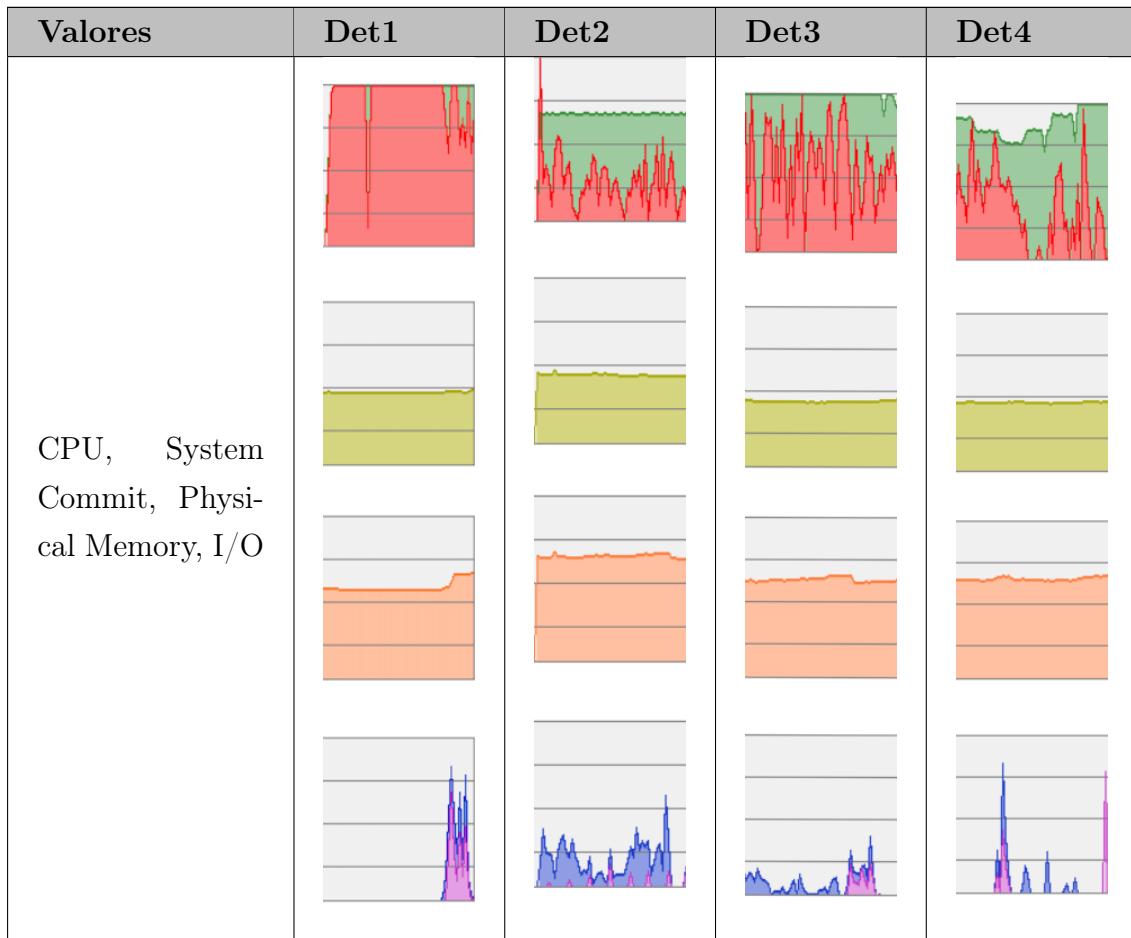


Tabla 4.4: Consumos de diferentes detonaciones de la muestra

4.2. Análisis de resultados

De la muestra analizada, se han obtenido una serie de resultados que nos ayudarán a establecer una evaluación final de este tipo de ransomware.

De la tabla 4.1, se pueden extraer las diferentes plataformas en las que se encuentra la muestra analizada. En el caso de Virus Total, 58 de 72 motores identificaron la muestra como maliciosa. Hybrid Analysis cuenta además con resultados provenientes de CrowdStrike Falcon (Static Analysis and ML), que identifica a la muestra como 100 % maliciosa y de MetaDefender, con 21 de 26 motores que la identifican como tal.

En cuanto a los informes emitidos por Joe Sandbox y Any Run, en ambos casos, se indica que la muestra analizada sería de un ransomware de la familia "Chaos". Además, estos informes muestran el uso de *bcdedit.exe* para inutilizar acciones de recuperación.

En cuanto al consumo de recursos, tal y como se muestra en la tabla 4.4, el consumo de CPU una vez se detonó la muestra se elevó considerablemente, aunque no llegó a realizar un consumo del 100 %. Posteriormente se realizaron varias ejecuciones previa restauración de la máquina virtual para comprobar los consumos, siendo muy dispares y en ningún caso colapsando la máquina.

Por otro lado, para comprobar el comportamiento del ransomware con diferentes tipos de archivos, se creó una carpeta con diferentes tipos, tal y como se muestra en la tabla 4.2. Todos fueron cifrados con extensión ".exe" salvo el fichero con extensión ".tiff". Esto es comprobable en el análisis estático del binario ya que se pueden comprobar las extensiones a las que afectará la ejecución del ransomware.

En la tabla 4.3 muestra los datos que son visibles en la nota de rescate que comprenden la cartera de bitcoins donde realizar el pago, un correo electrónico y la cantidad a abonar.

Por último, mediante las diferentes herramientas utilizadas en el análisis estático se han podido visualizar diferentes componentes del binario, como son los strings o funciones, cuyo resultado final podría ser la conformación de IoCs, como podrían ser los siguientes:

- "encryptionAesRsa"
- "encryptedFileExtension"
- "checkAdminPrivilage"
- "encryptDirectory"
- "rsaKey"
- "AES_Encrypt"
- "AESEncrypt"
- "EncryptFile"
- "deleteShadowCopies"
- "disableRecoveryMode"
- "deleteBackupCatalog"
- "TextToEncrypt"
- "coinlocker"

- "CreateEncryptor"
- "CryptoStream"
- "</RSAParameters"
- "<EncryptedKey"
- "coincrypter.exe"
- "bitdecrypter.txt"
- "All of your files have been encrypted"
- "<requestedPrivileges"
- "a88a0aa62a9e29cc30948b721e9e8b52"
- "45b71da84aca13b69dd9c8cb21b815260c23a215"
- "9d70b9e0df50aedb0a5864fc53b4c738b5725e4fec5286f723b52eef0c709211"
- "3BrbefoFF6oFyYYhXPSBGMMLWNHDHSL3rk"

Una de las principales funciones detectadas es el borrado de copias de seguridad y que deshabilita el modo de recuperación del sistema. También es detectable el uso de algoritmos de cifrado AES y RSA.

En caso de haber sido infectado por este tipo de ransomware se pueden utilizar herramientas como ID Ransomware que nos indicará, además del tipo de malware del que se trata, si existen actualmente herramientas de descifrado. Para el caso que se analiza en el presente documento, no existen, tal y como muestra la Figura 4.1:

1 Result

Chaos

⚠ Este ransomware no tiene ninguna forma conocida para descifrar los datos en este momento.

Se recomienda hacer una copia de seguridad de sus archivos cifrados, con la esperanza de una solución a futuro.

Identificado por

- sample_bytes: [0x00 - 0x0E] 0x3C456E637279707465644B65793E

Haga clic aquí para obtener más información acerca de Chaos

🔔 Would you like to be notified if there is any development regarding this ransomware? [Click here.](#)

Figura 4.1: Resultado del análisis de la muestra en ID Ransomware

Conclusión

En el presente trabajo se ha realizado un estudio de una muestra de ransomware de tipo CoinLocker (identificado como Chaos en diferentes plataformas y motores), cuyo estudio ha cumplido con los objetivos marcados:

- Análisis del contexto general del ransomware, exponiendo la situación y problemática actual, conceptos, tipos y grupos de ransomware, técnicas y algoritmos utilizados y operativa en la Deep Web.
- Análisis estático de la muestras seleccionada cuyo principal objetivo es recabar todo tipo de información relevante acerca de su funcionamiento sin haberlo detonado.
- Análisis dinámico en entornos seguros y controlados, tanto en máquinas virtuales como en sandbox en la nube.
- Análisis de la información obtenida y planteamiento de propuestas futuras para seguir esta investigación.

El ransomware CoinLocker data del año 2015 y está principalmente dirigido a sistemas Windows. En este caso, los archivos han sido cifrados con extensiones ".exe" generando una nota de rescate para realizar un pago de 100BTC en una cartera de bitcoinins. Cabe destacar que motores antivirus y sandbox han identificado la muestra como Chaos, aunque este es posterior a CoinLocker ya que data del año 2021. Comparte características comunes como es el uso de algoritmos híbridos (AES y RSA), o el uso de herramientas destinadas a la eliminación de las copias de seguridad (shadow copies). Es posible que este tipo de IoCs sean los motivo por los cuales ha sido identificado como tal.

Aportaciones realizadas

Finalizado el estudio se concluye que se ha cumplido con el principal objetivo, estudiar el comportamiento de una muestra de ransomware tipo CoinLocker. Mediante

los diferentes análisis realizados se ha recopilado de información sobre el comportamiento de este ransomware o cómo se enmarca dentro de la operativa general de este tipo de ataques que cada vez afectan a un mayor número de empresas organizaciones y particulares.

Trabajos futuros

Como propuestas de mejora o trabajos futuros se exponen las siguientes:

- Buscar y analizar un mayor número de muestras de este tipo y realizar comparativas para poder profundizar más en su comportamiento y evolución.
- Análisis más exhaustivo del código ensamblador.
- Creación de reglas Yara o Snort para que pueda ser detectado.
- Ejecutar muestras de este ransomware en otros sistemas operativos y analizar su comportamiento.

Problemas encontrados

El principal problema para el desarrollo del actual trabajo es la escasa información que existe sobre CoinLocker. Asimismo, la falta de acceso a plataformas de pago limitó la posibilidad de consultar ciertos análisis técnicos especializados, como el informe de Kaspersky, que podría haber proporcionado información adicional sobre la muestra.

Opiniones personales

El desarrollo del presente trabajo me ha permitido adquirir conocimientos sobre el funcionamiento del ransomware, sobre todo en cuanto el proceso de investigación del estado de la cuestión y de ambos análisis, estático y dinámico.

Por otro lado, también he podido comprobar las dificultades asociadas a llevar a cabo un proceso de investigación relacionado con un caso del que existe muy poca información y del cual, el que suscribe cuenta con escaso conocimiento.

Lista de referencias

- [1] A.Solomon, Nielson, B., Meldrum, S.: "Information about the AIDS diskette trojan",. [En línea] (1989)
- [2] Avast: ¿Qué es el ransomware Cryptolocker y de dónde procede? [En línea] (2020), <https://www.avast.com/es-es/c-cryptolocker>, [Último acceso: 2025-03-19]
- [3] AVG: Herramientas gratuitas para deshacer el cifrado por ransomware. [En línea] <https://www.avg.com/es-mx/ransomware-decryption-tools>, [Último acceso: 2025-05-01]
- [4] BBC: Cryptolocker victims to get files back for free. [En línea] (August 2014), <https://www.bbc.com/news/technology-28661463>, [Último acceso: 2025-05-20]
- [5] BBCNews: El virus que tomó control de mil máquinas y les ordenó autodestruirse. [En línea] (2015), https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet, [Último acceso: 2025-03-19]
- [6] BOE: Código Penal, artículo 197. [En línea] (1995), <https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444#a197>, [Último acceso: 2025-05-15]
- [7] BOE: Código Penal, artículo 264. [En línea] (1995), <https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444#a264>, [Último acceso: 2025-05-15]
- [8] BOE: Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales. [En línea] (12 2018), <https://www.boe.es/eli/es/lo/2018/12/05/3/con>, [Último acceso: 2025-05-15]
- [9] BOE: Real Decreto 311/2022, por el que se regula el Esquema Nacional de Seguridad. [En línea] (12 2018), <https://www.boe.es/eli/es/lo/2018/12/05/3/con>, [Último acceso: 2025-05-15]

- [10] BOE: Guía Nacional de Notificación y Gestión de Ciberincidentes. [En línea] (2020), https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf, [Último acceso: 2025-05-15]
- [11] BusinessInsider: A contract programmer faces 10 years in jail for inserting a 'logic bomb' into a spreadsheet that caused the company to keep rehiring him. [En línea] (2019), <https://www.businessinsider.in/a-contract-programmer-faces-10-years-in-jail-for-inserting-a-logic-bomb-into-a-articleshow/70354739.cms>, [Último acceso: 2025-03-19]
- [12] CadenaSer: Un presunto hacker amenaza con tener miles de datos de estudiantes y familiares de la web de Educacyl. [En línea] (May 2025), <https://cadenaser.com/castillayleon/2025/05/31/un-presunto-hacker-amenaza-con-tener-miles-de-datos-de-estudiantes-y-familiares.html>, [Último acceso: 2025-07-01]
- [13] CCN-CERT: ESQUEMA NACIONAL DE SEGURIDAD GLOSARIO DE TÉRMINOS Y ABREVIATURAS. [En línea] (febrero 2016), <https://www.ccn-cert.cni.es/es/800-guia-esquema-nacional-de-seguridad/499-ccn-stic-800-glosario-de-terminos-y-abreviaturas-del-ens/file.html>, [Último acceso: 2025-03-20]
- [14] Channel Partner: Principales ciberataques en España en 2024. [En línea] (2024), <https://www.channelpartner.es/seguridad/principales-ciberataques-en-espana-en-2024/>, [Último acceso: 2025-05-01]
- [15] CheckPoint: The State of Cyber Security 2025. En línea (2025), <https://www.checkpoint.com/security-report/?flz-category=items&flz-item=report--cyber-security-report-2025>, [Último acceso: 2025-03-31]
- [16] ClínicBarcelona: Ciberataque al hospital Clínic de Barcelona. [En línea] (July 2023), <https://www.clinicbarcelona.org/prensa/ultima-hora/ciberataque-al-hospital-clinic-de-barcelona>, [Último acceso: 2025-07-01]
- [17] CM-Alliance: Top 10 Biggest Cyber Attacks of 2024 25 Other Attacks to Know About! [En línea] (January 2025), <https://www.cm-alliance.com/cybersecurity-blog/>

- top-10-biggest-cyber-attacks-of-2024-25-other-attacks-to-know-about, [Último acceso: 2025-05-01]
- [18] CMMI: CMMI. [En línea] (2025), <https://cmmiinstitute.com/cmmi/v2-0>, [Último acceso: 2025-05-10]
- [19] Conti, M., Gangwal, A., Ruj, S.: On the Economic Significance of Ransomware Campaigns: A Bitcoin Transactions Perspective. Computers & Security **79**, 162–189 (2018). <https://doi.org/10.1016/j.cose.2018.08.008>, <https://www.sciencedirect.com/science/article/pii/S0167404818304334>
- [20] CronUp: El grupo criminal Cl0p responsable de la oleada de ciberataques a MOVEit. [En línea] (May 2022), <https://www.cronup.com/la-banda-de-conti-ransomware-finaliza-sus-operaciones-pero-mantiene-el-sitio-d> [Último acceso: 2025-04-25]
- [21] Dingledine, R., Mathewson, N., Syverson, P.: Tor: The Second-Generation Onion Router. [En línea] pp. 303–320 (2004), <https://www.usenix.org/conference/13th-usenix-security-symposium/tor-second-generation-onion-router>
- [22] ENISA: ENISA Threats Landscape 2023. [En línea] (2024), <https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf>, [Último acceso: 2025-03-17]
- [23] ENISA: ENISA Threats Landscape 2024. [En línea] (2024), https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf, [Último acceso: 2025-03-17]
- [24] EUR-Lex: Directive (EU) 2022/2555. [En línea] (2022), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555>, [Último acceso: 2025-05-15]
- [25] EUR-Lex: Reglamento General de Protección de Datos (RGPD). [En línea] (2022), <https://eur-lex.europa.eu/ES/legal-content/summary/general-data-protection-regulation-gdpr.html>, [Último acceso: 2025-05-15]
- [26] Europol: Andromeda botnet dismantled in international cyber operation. [En línea] (2017), <https://www.europol.europa.eu/media-press/newsroom/news/>

- andromeda-botnet-dismantled-in-international-cyber-operation,
[Último acceso: 2025-03-19]
- [27] Fourmilab: The Animal Episode. [En línea] (2017), <https://www.fourmilab.ch/documents/univac/animal.html>, [Último acceso: 2025-03-19]
- [28] Griffith, Virgil and Balakrishnan, Mahesh and others: A Broad Evaluation of the Tor English Content Ecosystem. [En línea] (2019), <https://doi.org/10.48550/arXiv.1902.06680>, [Último acceso: 2025-07-07]
- [29] Gómez-Hernández, J.A., Álvarez González, L.: Ransomware and its impact on cybersecurity: A comprehensive analysis of decryption tools. Computers & Security **105**, 102236 (2021). <https://doi.org/10.1016/j.cose.2021.102236>, <https://www.sciencedirect.com/science/article/abs/pii/S0167404821002935>, [Último acceso: 2025-05-01]
- [30] Hiruni, C.: From Creeper to Ransomware: The Evolution of Malware. ResearchGate (11 2024). <https://doi.org/10.13140/RG.2.2.17919.83369>
- [31] Holdsworth, J., Kosinski, M.: "¿Qué es el ransomware como servicio (RaaS)? [En línea] (September 2024), <https://www.ibm.com/es-es/topics/ransomware-as-a-service>
- [32] IBM: Change Healthcare discloses USD 22M ransomware payment. [En línea] (May 2024), <https://www.ibm.com/think/news/change-healthcare-22-million-ransomware-payment>, [Último acceso: 2025-05-01]
- [33] IDRansomware: ID Ransomware. [En línea] https://id-ransomware.malwarehunterteam.com/index.php?lang=es_ES, [Último acceso: 2025-07-01]
- [34] INCIBE: Ciberataque de cadena de suministro contra el software VSA de Kaseya. [En línea] (July 2021), <https://www.incibe.es/incibe-cert/publicaciones/bitacora-de-seguridad/ciberataque-cadena-suministro-el-software-vsa-kaseya>, [Último acceso: 2025-04-25]
- [35] INCIBE: Estados Unidos desmantela el malware Qakbot en un ciberataque internacional. [En línea] (2023), <https://www.incibe.es/incibe-cert/publicaciones/bitacora-de-seguridad/estados-unidos-desmantela-el-malware-qakbot-en-un-ciberataque>, [Último acceso: 2025-03-19]

- [36] INCIBE: Estudio del análisis de LockBit. [En línea] (March 2023), https://www.incibe.es/sites/default/files/contenidos/estudios/doc/incibe-cert_estudio_analisis_lockbit_2023_v1.pdf, [Último acceso: 2025-04-02]
- [37] INCIBE: La banda de Conti Ransomware finaliza sus operaciones, pero mantiene el sitio de filtraciones. [En línea] (2023), <https://www.cronup.com/la-banda-de-conti-ransomware-finaliza-sus-operaciones-pero-mantiene-el-sitio-d>, [Último acceso: 2025-04-25]
- [38] Indeed: Sueldo de Analista de seguridad informática en España. [En línea] (2025), <https://es.indeed.com/career/analista-de-seguridad-inform%C3%A1tica/salaries>, [Último acceso: 2025-05-02]
- [39] Indeed: Sueldo de Scrum master/a en España. [En línea] (2025), <https://es.indeed.com/career/scrum-master/salaries>, [Último acceso: 2025-05-02]
- [40] Kaspersky: Fireball: un adware con posibles consecuencias mundiales. [En línea] (2017), <https://www.kaspersky.es/blog/fireball-adware/13086/?srltid=AfmB0or4EydWZ5fgMJPZS15ZWaq5cfaxf3RIlay1NRsT7AvkPVinAquH>, [Último acceso: 2025-03-19]
- [41] Kaspersky: Kaspersky Security Bulletin 2024. Statistics. [En línea] (2024), <https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2024/12/03153220/KSB-statistics-of-the-year-EN-final.pdf>, [Último acceso: 2025-03-17]
- [42] Kaspersky: Understanding Malware-as-a-Service. [En línea] (2024), https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2023/06/06114408/Understanding_Malware-as-a-Service.pdf, [Último acceso: 2025-03-17]
- [43] KeepCoding: ¿Qué hace el virus Brain? [En línea] (2024), <https://keepcoding.io/blog/que-hace-el-virus-brain/>, [Último acceso: 2025-03-19]
- [44] Keyfactor: Tipos de algoritmos de cifrado + ventajas e inconvenientes de cada uno. [En línea] <https://www.keyfactor.com/es/education-center/types-of-encryption-algorithms/>, [Último acceso: 2025-05-01]

- [45] KrebsonSecurity: Operation Tovar Targets Gameover Zeus Botnet, Cryptolocker Scourge. [En línea] (June 2014), <https://krebsonsecurity.com/2014/06/operation-tovar-targets-gameover-zeus-botnet-cryptolocker-scourge/>, [Último acceso: 2025-05-20]
- [46] LaSexta-TecnoXplora: Elk Cloner: 35 años del primer virus informático. [En línea] (2017), https://www.lasexta.com/tecnologia-tecnoxplora/ciencia/divulgacion/elk-cloner-anos-primer-virus-informatico_2017040758ec8a110cf2f2c8756479de.html, [Último acceso: 2025-03-19]
- [47] LaVanguardia: El Grupo Santillana sufre un ataque de 'ransomware'. [En línea] (March 2025), <https://www.lavanguardia.com/sociedad/20250325/10518060/grupo-santillana-sufre-ataque-ransomware-agenciaslv20250325.html>, [Último acceso: 2025-07-01]
- [48] Lenstra, A.K., Tromer, E., Shamir, A., Kortsmit, W., Dodson, B., Hughes, J., Leyland, P.: Factoring Estimates for a 1024-Bit RSA Modulus. [En línea] (2003), <https://cs-people.bu.edu/tromer/papers/factorest.pdf>
- [49] McAfee: ¿qué es el malware? [En línea] (2024), <https://www.mcafee.com/es-es/antivirus/malware.html>, [Último acceso: 2025-03-17]
- [50] Microsoft: Boletín de seguridad de Microsoft Ms02-039: Crítico. [En línea] (2023), <https://learn.microsoft.com/es-es/security-updates/securitybulletins/2002/ms02-039>, [Último acceso: 2025-03-19]
- [51] MuyInteresante: Creeper virus, así fue el primer virus de la historia. [En línea] (2023), <https://www.muyinteresante.com/tecnologia/62784.html>, [Actualizado en 2025][Último acceso: 2025-03-19]
- [52] NewYorkTimes: Ciberataque al oleoducto Colonial Pipeline: esto sabemos. [En línea] (May 2021), <https://www.nytimes.com/es/2021/05/11/espanol/colonial-pipeline-ransomware.html>, [Último acceso: 2025-04-25]
- [53] NIST: Cryptographic algorithm. [En línea] https://csrc.nist.gov/glossary/term/cryptographic_algorithm, [Último acceso: 2025-04-25]
- [54] NIST: Advanced Encryption Standard (AES). [En línea] (FIPS PUB 197) (November 2001), <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197-upd1.pdf>

- [55] NIST: Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms. [En línea] (March 2020), <https://doi.org/10.6028/NIST.SP.800-175Br1>, [Último acceso: 2025-04-25]
- [56] NIST: Gestión de riesgo de ransomware: un perfil de marco de ciberseguridad. [En línea] (Febrero 2022), <https://doi.org/10.6028/NIST.IR.8374.spa>
- [57] "Rapid7Labs": Ransomware Radar Report. [En línea] (2024), https://www.rapid7.com/globalassets/_pdfs/2024-rapid7-ransomware-radar-report-final.pdf, [Último acceso: 2025-03-07]
- [58] RedesZone: Red Tor vs navegador Tor Browser: qué es cada término. En línea (February 2023), <https://www.redeszone.net/tutoriales/internet/diferencias-red-tor-navegador-tor/>, [Último acceso: 2025-04-03]
- [59] Reed, M., Syverson, P., Goldschlag, D.: Anonymous Connections and Onion Routing. IEEE Journal on Selected Areas in Communications **16**(4), 482–494 (1998). <https://doi.org/10.1109/49.668972>
- [60] S21SEC: Threat Landscape Report 2024. En línea (2024), https://www.s21sec.com/wp-content/uploads/2025/02/TLR_2024_H2_EN.pdf, [Último acceso: 2025-03-31]
- [61] S2GRUPO: Panorama del RANSOMWARE 2025. [En línea] (Junio 2025), <https://5529275.fs1.hubspotusercontent-na1.net/hubfs/5529275/Panorama%20del%20Ransomware%202025%20-%20S2GRUPO.pdf>, [Último acceso: 2025-06-26]
- [62] SearchLightCyber: Ransomware in H1 2024: Trends from the Dark Web. En línea (2024), <https://slcyber.io/whitepapers-reports/ransomware-in-h1-2024-trends-from-the-dark-web>, [Último acceso: 2025-03-27]
- [63] SecurityBrief: 2025 Ransomware: Business as Usual, Business is Booming. [En línea] (April 2025), <https://securitybrief.com.au/story/2025-ransomware-business-as-usual-business-is-booming>, [Último acceso: 2025-06-26]
- [64] SecurityWeek: Cryptolocker Infections on the Rise; US-CERT Issues Warning. [En línea] (2013), <https://www.securityweek.com/>

- cryptolocker-infections-rise-us-cert-issues-warning/, [Último acceso: 2025-05-19]
- [65] Semperis: 2024 Ransomware Risk Report. [En línea] (2024), <https://www.semperis.com/wp-content/uploads/resources-pdfs/ransomware-report-2024.pdf>, [Último acceso: 2025-03-12]
- [66] Shidlovski, Y., Abendroth, J., Häggerli, B.M.: The Ransomware-as-a-Service economy within the darknet. Computers & Security **92**, 101748 (2020). <https://doi.org/10.1016/j.cose.2020.101748>, <https://www.sciencedirect.com/science/article/pii/S0167404820300468>
- [67] SonicWall: GPcode ransomware leaves victims stranded. [En línea] (2023), <https://www.sonicwall.com/blog/gpcode-ransomware-leaves-victims-stranded>, [Último acceso: 2025-03-20]
- [68] Sophos: El estado del ransomware 2024. En línea (2024), <https://www.sophos.com/es-es/whitepaper/state-of-ransomware>, [Último acceso: 2025-03-26]
- [69] SpyCloud: The 2024 Malware and Ransomware Defense Report. En línea (2024), <https://spycloud.com/resource/2024-malware-ransomware-defense-report/>, [Último acceso: 2025-03-26]
- [70] Talos: Revisión del año 2023. En línea (2023), https://www.cisco.com/c/dam/global/es_mx/products/pdfs/talos-2023-report.pdf, [Último acceso: 2025-03-27]
- [71] TheGazzete: Former UI student sentenced to 4 months in federal prison for changing grades, copying exams. [En línea] (2018), <https://www.thegazette.com/education/former-ui-student-sentenced-to-4-months-in-federal-prison-for-changing-grades-> [Último acceso: 2025-03-19]
- [72] Tzu, S.: El arte de la guerra. Ediciones Urano, Barcelona (2002), edición comentada
- [73] Veeam: Ransomware Trends 2024. [En línea] (2024), https://www.veeam.com/analyst-reports/2024-ransomware-trends-executive-summary-emea_wpp.pdf, [Último acceso: 2025-03-12]

- [74] Wired: Meet Flame, the massive spy malware infiltrating iranian computers. [En línea] (2012), <https://www.wired.com/2012/05/flame/>, [Último acceso: 2025-03-19]
- [75] Young, A., Yung, M.: Cryptovirology: extortion-based security threats and countermeasures. Proceedings 1996 IEEE Symposium on Security and Privacy pp. 129–140 (1996). <https://doi.org/10.1109/SECPRI.1996.502676>

Anexo A

Seguimiento de proyecto fin de máster

A.1. Forma de seguimiento

En el presente anexo se incluyen las imágenes que muestran tanto la planificación inicial del proyecto, como al resultante final. En ellas se muestran las tareas y subtareas que lo conforman.

A.2. Planificación inicial

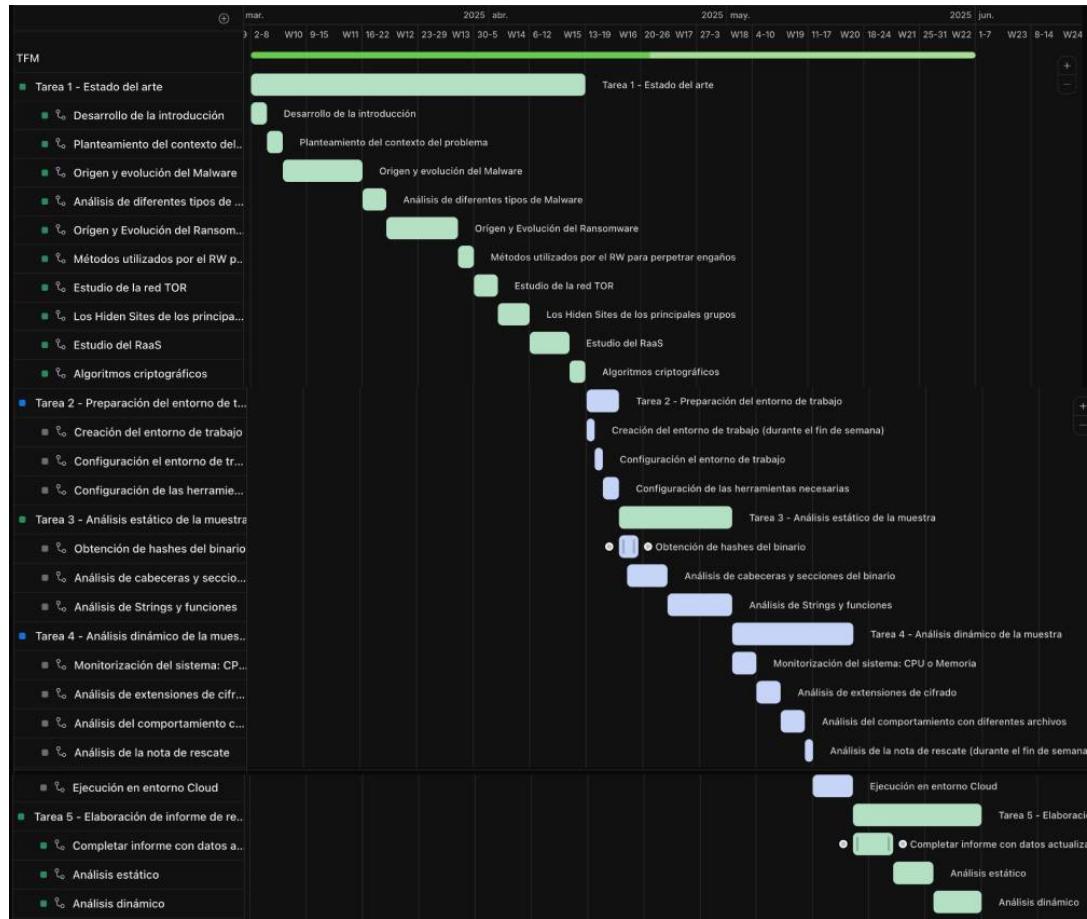


Figura A.1: Planificación incial.

A.3. Planificación final

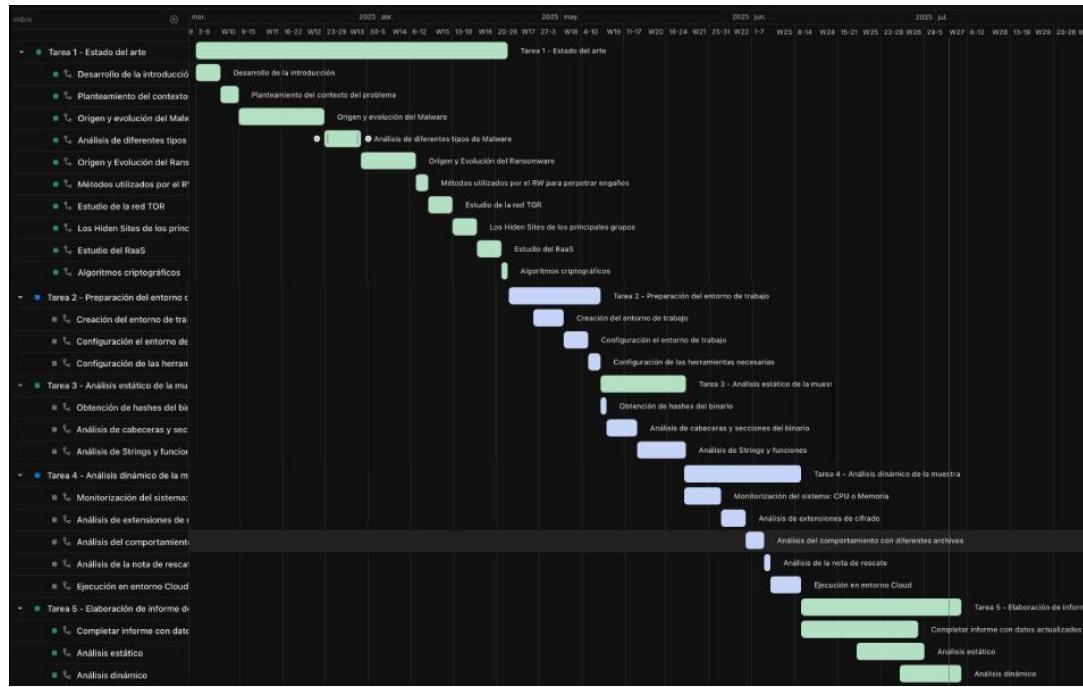


Figura A.2: Planificación incial.

Anexo B

Control de versiones

La herramienta utilizada para llevar a cabo un control de las versiones a desarrollar ha sido GitHub. La dirección donde se pueden encontrar es la siguiente: <https://github.com/cuentadecurrele/TFM-RW-CoinLocker.git>

Cabe destacar que únicamente se ha utilizado una sola rama ya que las modificaciones del proyecto son ejecutadas por un único usuario.

Adicionalmente, se pueden encontrar los siguientes directorios archivos:

- **HERRAMIENTAS.** Herramientas utilizadas para el desarrollo del proyecto, a excepción de Ghidra cuyo tamaño no permite la subida a GitHub.
- **MUESTRA.** Contiene la muestra utilizada para el análisis realizado en el presente trabajo.
- **Documentos:** versiones del documento de entrega del trabajo de fin de máster.