Ciberataques: análisis de Ransomware y métodos de protección.

John Edisson Romero Rubiano

Máster Universitario en Ciberseguridad y Privacidad

Seguridad empresarial

Nombre Tutor/a de TF
Angela María García Valdés
Profesor/a responsable de la asignatura
Víctor García Font

PEC4, 12 junio 2023

Universitat Oberta de Catalunya

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Ciberataques: análisis de Ransomware y métodos de protección.*
Nombre del autor:	*John Edisson Romero Rubiano*
Nombre del consultor/a:	*Angela María García Valdés*
Nombre del PRA:	*Víctor García Font*
Fecha de entrega (mm/aaaa):	*06/2023 PEC4*
Titulación o programa:	Máster Universitario en Ciberseguridad y Privacidad
Área del Trabajo Final:	*Seguridad empresarial*
Idioma del trabajo:	*Castellano*
Palabras clave	*Ransomware, Cibercrimen, Protección*

Resumen del Trabajo

Es este TFM se describe el problema del Ransomware en la sociedad actual, cada vez los ataques son más recurrentes y sofisticados donde afecta diversos sectores como salud, gobierno y banca. Se establece una metodología con un enfoque investigativo para analizar este tipo de malware, por tal razón inicia el estudio del estado de arte para el Ransomware, su historia, detallar las etapas de un ataque y características como velocidad de cifrado.

Luego se hace un análisis del impacto de este tipo de malware y una reflexión si se debe pagar por este tipo de extorsiones. Como funcionan estas campañas, cuál es su modelo de negocio y como realizan el blanqueo de dinero.

Se procede a revisar los vectores de ataques conocidos, las tácticas y herramientas usadas por los adversarios. Así como las recomendaciones de entidades expertas en seguridad como ENISA y un análisis de la legislación aplicable para estos casos.

A continuación, se realiza una simulación en ambiente controlado del ataque Ransomware LockBit, iniciando por un análisis estático y dinámico, así como la toma de evidencias de los procesos y mecanismos usados por este malware.

Para finalizar los resultados se plasman en un mapa de descripción del ataque y una matriz con tácticas de MITRE ATT&CK que permitan describir el modo de operación de LockBit, luego se exponen una serie de recomendaciones a nivel empresarial que ayuden a prevenir y mitigar el impacto de este tipo de malware.

Abstract

The TFM describes the Ransomware problem in actual society, every time the attacks are more recurrent and sophisticated and affects multiple sectors such as health, government and banking. Established a investigative methodology to analyze this type of malware, for this reason the investigation of the state of the art for Ransomware begins, its history, detailing the stages of an attack, characteristics such as encryption speed.

Then an analysis of the impact of this type of malware and reflection on paying for this type of extortion. How do these campaigns work, what is their business model and how do they legalize money.

We proceed to review the known attack vectors, the tactics and tools used by the adversaries. Some recommendations of expert security entities (ENISA), and an analysis of the applicable legislation for these cases.

Next, a simulation of the LockBit attack in Sandbox, starting with a static and dynamic analysis, as well as taking evidence of the processes and mechanisms used by this malware.

Finally, the results are reflected in a map describing the attack and a matrix with MITRE ATT&CK tactics that allow Lockbit's mode of operation to be described, some recommendations are presented at the business level that help prevent and mitigate the impact of attacks this type of malware.

Índice

Lista de figuras

Lista de tablas

1. Introducción

1.1. Contexto y justificación del trabajo

Cada vez son más frecuentes los ataques de ciberdelincuentes a distintos sectores económicos como salud, gobierno, banca, energético entre otros. Actividades que hacen uso de la globalización y tecnología para ser cada vez más sofisticadas, convirtiéndose en una de las preocupaciones a nivel mundial. Estas acciones delictivas son realizadas normalmente con ánimo de lucro, activistas e incluso con intereses políticos.

Los ciberataques pueden catalogarse como un problema en la sociedad actual en donde se pone en riesgo la información y privacidad de naciones enteras, personas jurídicas y naturales. De este modo surge la necesidad de protección frente al cibercrimen, una carrera constante para garantizar la disponibilidad, integridad y confidencialidad de la información.

Con el paso del tiempo son más diversos y variados los tipos de malware usados para estas acciones delictivas, uno de estos es el Ransomware o software de secuestro de información que principalmente van dirigidos a empresas, el cual impide el acceso a sistemas informáticos y datos, donde el atacante solicita una compensación monetaria o pago de rescate para que la víctima recupere el acceso a su información. Aunque el origen del Ransomware data del año 1989 [1] en la actualidad sigue estando muy vigente, pues los ciberdelincuentes evolucionan constantemente y cada día aparecen nuevos tipos de fraude, formas de ataque y cobros como la exigencia de pago en bitcoins para dificultar el seguimiento de estas transacciones.

En este trabajo final de máster se busca investigar los diferentes tipos de Ransomware, analizar las tecnologías y medios usados, estudiar las formas en que operan con el fin de aportar a la sociedad al definir mecanismos para prevenir y mitigar el impacto. Como objeto de estudio en este TFM se realizará el análisis detallado de LockBit [2] una campaña de Ransomware como servicio (RaaS), el cual ha afectado a diversos sectores y empresas a nivel global con un alto impacto económico y social.

1.2. Objetivos del trabajo

Para este TFM los objetivos principales abordados desde una perspectiva técnica son:

- Investigar tipos de Ransomware e impacto en la sociedad.
- Analizar vectores de infección y describir en forma detallada su modo de operación.
- Simular en ambiente controlado un ataque de Ransomware, exponer su anatomía y funcionamiento.
- Definir mecanismos de prevención y buenas prácticas de seguridad ante el Ransomware.

1.3. Impacto en sostenibilidad, ético-social y de diversidad

Los profesionales en ciberseguridad en su deber ético y de responsabilidad social deben velar por el bienestar de la comunidad, por esto uno de los objetivos al realizar este TFM es definir mecanismos de prevención y buenas prácticas de seguridad ante el Ransomware. Aportar a la sociedad en cuanto a las acciones que pueden mejorar la seguridad en el entorno empresarial que ayuden a garantizar la privacidad de la información.

Tomando como referencia los objetivos de desarrollo sostenible de Naciones Unidas [3] y el impacto de la ciberseguridad en la sociedad. La tecnología y seguridad juegan un papel importante en el alcance los objetivos de la ODS en cuanto a los siguientes factores:

Figura 1: ODS y TFM, Elaboración propia a partir de [3]

1.4. Enfoque y método seguido

Como base inicial de este TFM se realizará investigación documental acerca de los tipos de Ransomware y modos de operación, observar y analizar información disponible de entes expertos en seguridad e indagar acerca de la legislación aplicable en estos ciberdelitos, que permitan sentar un marco de referencia.

La segunda etapa comprende el análisis para detallar los mecanismos y tecnologías usadas en los vectores de infección, poder explicar al lector de una forma clara cómo no caer en el engaño de los ciberdelincuentes. Posteriormente haciendo uso de una simulación en ambiente controlado, se realizará el análisis de una campaña de Ransomware, desglosando su arquitectura y explicando su modo de operación.

Como etapa final se busca definir los controles y políticas que ayuden a prevenir y mitigar el impacto de estas acciones. Documentar una guía de buenas prácticas que faciliten la gestión de seguridad en un entorno empresarial.

El método seguido debe ajustarse al contexto y debido a que el Ransomware es una actividad en constante evolución, se requiere observar e investigar los últimos ataques o campañas de este malware, seguido de un desglose de su modo de actuar y vectores

que permitan definir la mejor manera de prevenir y mitigar su afectación, estos pasos se resumen en la siguiente figura:

Figura 2: Metodología

1.5. Planificación del trabajo

El progreso de este proyecto se alinea con las entregas del aula de Seguridad Empresarial y la metodología propuesta, como actividades principales se contemplan:

- Planificación TFM.
- Investigación tipos de Ransomware, modos de operación.
- Estudio de marco legal y legislación aplicable a los ciberdelitos.
- Análisis de vectores - detallar mecanismos, tecnologías aplicadas.
- Definir acciones de prevención y mitigación.
- Memoria TFM.

Mediante el siguiente cronograma se planifican las tareas, dando relevancia a los hitos que corresponde a cada entrega de las PEC.

ID	Actividad	Inicio	Fin	Días
1	Planificación	3/3/2023	13/3/2023	11
1.1	Definir contexto y justificación	2/3/2023	5/3/2023	4
1.2	Establecer objetivos	4/3/2023	12/3/2023	9
1.3	Definir metodología	7/3/2023	10/3/2023	4
1.4	Planificación actividades	9/3/2023	11/3/2023	3
1.5	Implantar cronograma de trabajo	11/3/2023	12/3/2023	2
1.6	Entrega PEC1 TFM - Plan de Trabajo	12/3/2023	**13/3/2023**	2
2	Investigar Ransomware	14/3/2023	10/4/2023	28
2.1	Estado de arte	14/3/2023	17/3/2023	4
2.2	Consultar tipos de Ransomware	17/3/2023	24/3/2023	8
2.3	Describir modos de operación	20/3/2023	3/4/2023	15
2.4	Consultar legislación aplicable	27/3/2023	3/4/2023	8
2.5	Entrega PEC2 TFM - Entrega Seguimiento	1/4/2023	**10/4/2023**	10
3	Análisis Vectores Infección	11/4/2023	25/4/2023	15
3.1	Detallar mecanismos	11/4/2023	18/4/2023	8
3.2	Tecnologías aplicadas	18/4/2023	25/4/2023	8
4	Prevenir y Mitigar	26/4/2023	8/5/2023	13
4.1	Definir controles y políticas de seguridad	26/4/2023	4/5/2023	9
4.2	Entrega PEC3 TFM - Entrega Seguimiento	5/5/2023	**8/5/2023**	4
5	Memoria TFM y Presentación Final	9/5/2023	29/6/2023	52
5.1	Entrega PEC 4 TFM - Memoria final	9/5/2023	**12/6/2023**	35
5.2	Presentación en vídeo	12/6/2023	**19/6/2023**	8
5.3	Defensa del TFM	20/6/2023	**29/6/2023**	10

Tabla 1: Cronograma

Al plasmar el anterior listado de actividades en un diagrama de Gantt, obtenemos una línea visual que ayuda en la gestión y seguimiento. Ver Anexo 1.

1.6. Breve sumario de productos obtenidos

- Planificación de trabajo: Proponer objetivos, metodología y planificación para el desarrollo del TFM.
- Marco conceptual Ransomware.
- Análisis de modelo de operación y vectores de ataque.
- Controles y políticas de seguridad para prevención.

1.7. Breve descripción de los otros capítulos de la memoria

En base a la metodología y cronograma propuesto en los siguientes apartados se encuentra la siguiente información:

- Estado del arte: Definición y cronología del Ransomware, impacto social, modelo de negocio, vectores de ataques y medidas de defensa.
- Análisis de Ransomware: Identificar los mecanismos y tecnologías usadas en los vectores de infección, mediante practica em ambiente controlado detallar el modo de operación de uno de estos ataques.
- Definición de políticas y mecanismos de prevención y buenas prácticas de seguridad ante el Ransomware.
- Resultados y conclusiones generales, de acuerdo a la metodología planteada se describe el alcance de los objetivos.

2. Estado del arte

2.1 Ransomware

El software de secuestro es un tipo de malware que impide el acceso a información o sistema informático, luego solicita a la víctima un pago de rescate para retirar la restricción, bloqueo o cifrado. Amenazando con destruir la información, divulgarla públicamente o incluso venderla al mejor postor.

Este tipo de malware puede atacar de dos maneras, una de ellas consiste en el bloqueo de dispositivo o sistema informático, en donde se restringe el acceso al equipo generalmente por ataques a su sistema operativo. Un segundo grupo son los ataques contra la información almacenada, en donde se cifran los ficheros de los usuarios y se impide el acceso.

La Agencia de Ciberseguridad de la Unión Europea (ENISA) [4] identifica 5 etapas en un ataque de Ransomware:

Figura 3: Etapas ataque Ransomware, elaboración propia a partir de ENISA

- Acceso inicial: Utiliza técnicas similares a otros malware como son explotación de vulnerabilidades, uso de credenciales robadas, phishing, entre otros.

- Ejecución: Luego de tener el acceso al sistema o información, el atacante analiza el objetivo, tratando de encontrar más activos para afectar o realizar movimiento lateral.

- Acción sobre objetivos: En este punto el Ransomware despliega su ataque con acciones como bloquear, encriptar, borrar y robar. Afectando la disponibilidad, integridad y confidencialidad de la información.

- Extorsión: Luego de asegurar de que se llevó a cabo el ataque proceden con el chantaje, solicitando el pago de una compensación económica, lo hacen en tres etapas iniciando con informar al afectado del ataque, seguido de la amenaza si no se realiza el pago y finaliza con la demanda o indicación del monto a pagar. En la actualidad estas demandas se realizan de manera pública en portales donde se exponen las empresas o entidades afectadas, los activos o información comprometida con el ánimo de desacreditar y generar daño reputacional.

- Negociación: Comunicación privada entre atacante y víctima, para negociar o acordar el pago de la extorsión, ENISA [4] recomienda abstenerse de participar en esta etapa y en general no realizar el pago ya que no hay garantía de recuperarse totalmente del incidente y afectación.

2.2 Historia del Ransomware

Se estima el origen del Ransomware en el año de 1989[1], el avance y nuevas tácticas de ataque son cada vez más sofisticadas. Acciones iniciales de este malware son cifrar información, bloqueo de pantalla del PC, modificaciones al Master Boot Record (MBR), avanzando hacia cifrado de servidores web, o ataques dirigidos a dispositivos móviles y sistemas operativos específicos.

En la siguiente figura podemos observar la cronología de este tipo del malware y su evolución:

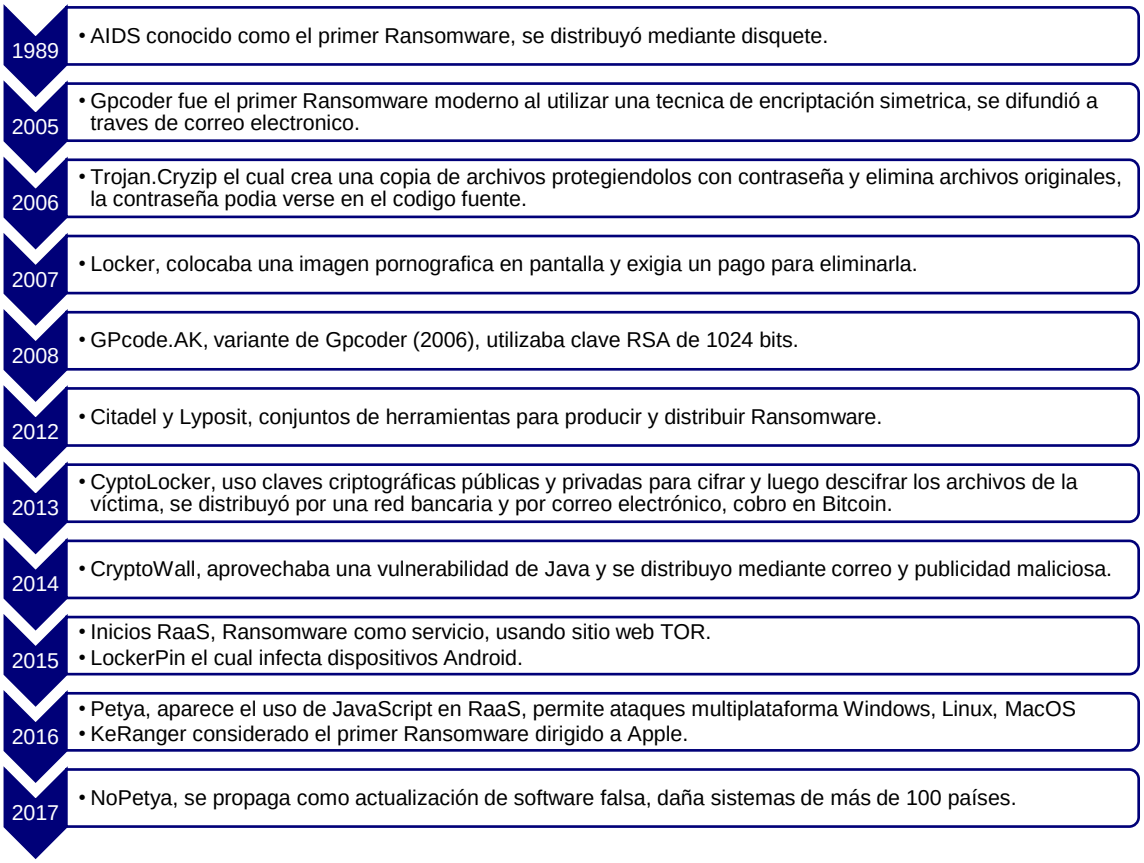


Figura 4: Cronología y evolución Ransomware, elaboración a partir de [5] [6]

2.3 Ransomware - velocidad de cifrado

En cuanto al riesgo de ser atacado por un Ransomware es importante conocer el tiempo que tenemos desde que se inicia el ataque y el momento en donde todos los archivos comprometidos han sido cifrados. La herramienta Splunk [7] realizo un estudio para medir la velocidad de cifrados de las diferentes campañas de Ransomware, encontrando que LockBit es uno de los más rápidos en cifrar los datos debido a que tardo menos de 5 minutos en cifrar 53GB de información.

Family	Median Duration
LockBit	00:05:50
Babuk	00:06:34
Avaddon	00:13:15
Ryuk	00:14:30
Revil	00:24:16
BlackMatter	00:43:03
Darkside	00:44:52
Conti	00:59:34
Maze	01:54:33
Mespinoza (PYSA)	01:54:54
Average of the median	**00:42:52**

Figura 5: Top 10 Velocidad de cifrado, tomado de [7]

En los últimos años el Ransomware usa técnicas de cifrado intermitente o parcial para aumentar la velocidad, pues solo necesita encriptar una parte de los bits de un archivo para dejarlo inutilizable, debido a esta característica las operaciones de escritura en disco son variables lo cual dificulta el análisis y detección [8].

En base a estos tiempos podemos decir que, si el adversario realizo el ataque la probabilidad de ser detectados disminuye y es muy complejo que la organización responda de manera eficiente y deba recurrir a copias de seguridad y respaldos para recuperar sus sistemas y servicios.

2.4 Evolución LockBit

LockBit: septiembre de 2019 [9] originalmente conocido como virus ".abcd" debido a que cifraba los archivos con esta extensión, campaña que funciona en modo RaaS es dirigida especialmente a empresas y organizaciones, amenaza con interrumpir operaciones, extorsión, exfiltración y publicación. Con capacidad de auto propagación, luego de infectar un host ejecuta scripts para afectar más host en la red.

LockBit 2.0: febrero 2022 [10], de acuerdo a IC3 usa herramientas como Mimikatz para aumentar privilegios. Agrega cifrado automático en dispositivos mediante abuso de políticas de directorio activo, omite archivos de funciones principales del sistema. Para la exfiltración usa el malware Stealbit.

LockBit 3.0: marzo 2023 [11], también conocido como LockBit Black es más modular y comparte similitudes con otras campañas de Ransomware como Blackmatter y Blackcat, esta versión de LockBit acepta configuraciones específicas para realizar movimiento lateral y puede reiniciar el equipo en modo seguro. Encripta su código mediante una clave que solo conocen los afiliados de esta campaña lo cual dificulta la detección de este malware. Como la clave cambia también lo hace su hash y de esta manera elude las detecciones basadas en firmas.

2.5 Impacto social del Ransomware

De acuerdo a la intención principalmente con ánimo de lucro con que se desarrollan las campañas de Ransomware es preciso revisar en números y cuantificar las pérdidas que generan estos ataques en la sociedad. Solo en 2021 de acuerdo a un informe de Internet Crime Complaint Center (IC3) del FBI [12], se recibieron 3729 denuncias y se calculan pérdidas de más de 49 millones de dólares. Estos cálculos corresponden únicamente a las perdidas reportadas por empresas, sin embargo, en muchas ocasiones estos ataques no son denunciados ni reportados. Cabe destacar del mismo informe la tasa de crecimiento en las pérdidas financieras pues aumento un 69% respeto al año 2020, lo cual demuestra que los ataques de Ransomware continúan muy vigentes y en crecimiento consolidándose como un problema en la sociedad actual.

IC3 contempla 16 sectores con infraestructura critica e informó que de 649 denuncias en 2021 el sector más atacado fue el de salud, seguidos del sector financiero y SI/TI como se observa en el siguiente gráfico.

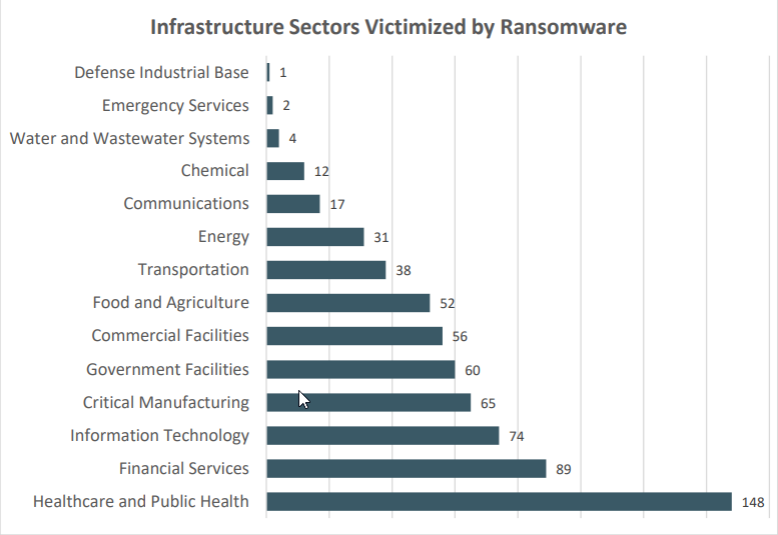


Figura 6: IC3, sectores con más ataques en 2021 [12]

Para comprender porque este sector es el más atacado, debemos analizar su modo de operación, debido a que en la actualidad los servicios de salud poseen sistemas de información conectados a internet, que facilitan la gestión de sus servicios y dan mayor alcance y facilidades a todos sus usuarios, estos sistemas albergan gran cantidad de información sensible como números de identificación, dirección, historia clínica, datos familiares entre otros. Tal concentración de información convierte este sector en un blanco perfecto para los ciberdelincuentes, donde cada año se evidencian ataques que afectan el servicio, genera pérdidas económicas e incluso el cierre de operaciones. Otro estudio realizado por Verizon en el año 2020 [13] indico que el sector salud reportó 798 incidentes de los cuales 521 divulgaron información.

De acuerdo al Estudio sobre el impacto de los ataques de Ransomware en el Sector de la Salud [14] se resumen los siguientes impactos:

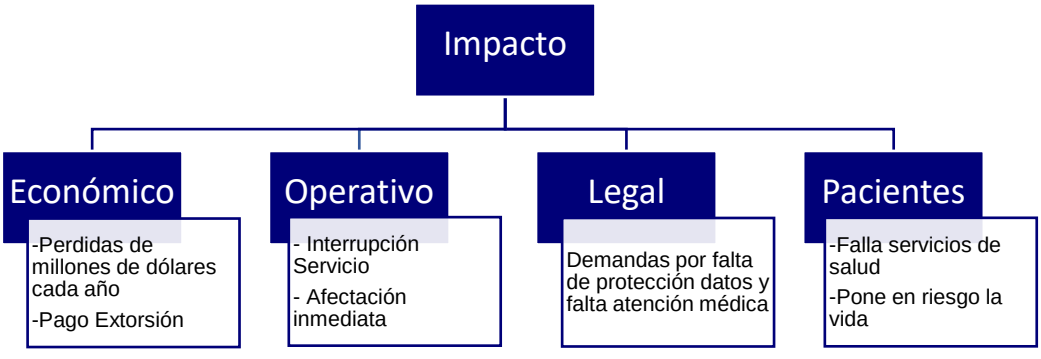


Figura 7: Impactos Ransomware en sector salud, elaboración a partir de [14]

Los ataques de Ransomware causan un daño y pérdidas económicas de gran magnitud, cada año las empresas y entidades afectadas pagan estas extorsiones y tienen pérdidas de ingresos. Estas acciones delictivas también ocasionan un impacto operativo pues genera interrupciones de servicio en ocasiones de forma inmediata pues se deben bajar servicios, apagar o aislar infraestructura.

Aún más grave es el impacto a los usuarios, al presentarse fallas de los servicios de salud se está colocando en riesgo la vida de los pacientes, un ejemplo de ello es la telemedicina y cirugía a distancia que ante la eventualidad de un ataque falle y ocasione el deceso de una persona.

En cuanto a lo legal las víctimas también deben responder por múltiples denuncias ocasionadas por la protección de datos de sus usuarios y debido al daño operativo responder por la falta de atención médica a sus usuarios.

2.6 Modelo negocio del Ransomware

El Ransomware está diseñado para realizar extorsión a sus víctimas, mediante la amenaza de destruir información o sistemas informáticos, desde el 2015 RaaS se postula como uno de los modelos de negocio principales, donde se facilita que atacantes sin experiencia creen y difundan este malware, también abre la posibilidad de tener afiliados en estas actividades donde se reparten las utilidades generadas ilícitamente.

Según expone ENISA [4] los atacantes se están moviendo a un modelo de negocio llamado “Data Brokerage”, donde los datos robados y accesos obtenidos se venden al mejor postor, para ataques adicionales. Este tipo de exfiltración de datos vulnera la privacidad de la información en especial datos confidenciales del sector salud y educación usando técnicas como automatización, fragmentación, protocolos alternativos, servicios web y en nube [15].

Factores adicionales en el modelo de negocio es la forma de cobro de los ciberdelincuentes, desde el 2013 con el uso indebido de criptomonedas como el bitcoin donde no se tiene una entidad de control centralizada, se garantiza cierto grado de anonimato. Adicional el uso de redes TOR que preservan la privacidad, ocultan el emisor y dificultan su seguimiento. Las anteriores se convierten en herramientas que facilitan el crecimiento de estas actividades fraudulentas. En la siguiente figura se tiene una línea de tiempo entre los años 2013 y 2017 [16] con las campañas de Ransomware que realizaron sus cobros mediante bitcoin.

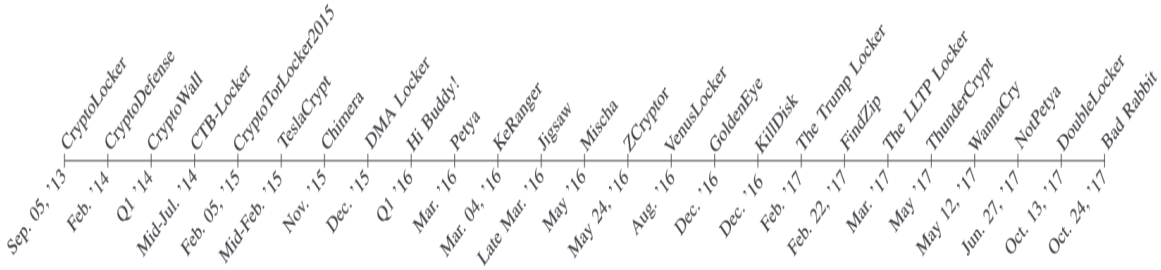


Figura 8: Ransomware y cobros mediante bitcoin, fuente [16]

2.7 Pagar o no pagar ante un ataque

Una de las discusiones entre proveedores, organizaciones de seguridad de la información y víctimas es si pagar o no pagar por este tipo de extorsión, el portal web nomoreransom.org [1] recomienda no realizar el pago a este tipo de chantajes por las siguientes razones:

- No se garantiza solución del problema.
- Perdida de datos en el proceso de cifrado y descifrado.
- Se incentiva esta actividad ilícita.

De acuerdo al informe de ENISA [4] de las empresas que pagaron por el rescate, el 18% se filtró su información afectando la confidencialidad y el 35% no lograron recuperar sus datos.

Realizar el pago a estas acciones delictivas envalentona y anima a los adversarios a realizar más ataques, dedicando mayor esfuerzo en el desarrollo de nuevas estrategias y campañas de Ransomware. Es recomendable dirigir estos recursos para fortalecer la infraestructura y seguridad en el entorno empresarial, formar una cultura de prevención y tener claras las acciones para mitigar el impacto y recuperación. En caso de un ataque la mejor opción es denunciar y contactar a las entidades pertinentes.

2.8 Blanqueo de dinero

De acuerdo al artículo 1 de la ley 10/2010 de 28 de abril [17], se considera blanqueo de dinero la conversión o trasferencia de activos con pleno conocimiento de su origen y carácter ilícito. También lo es ocultar el origen y localización del propietario real de estos dineros. Esta figura corresponde al modelo fraudulento en que los atacantes usan las criptomonedas.

De esta manera puede considerarse al bitcoin con habilitador para el blanqueo de dinero, pues no se tiene una entidad central o reguladora, cada transferencia se realiza únicamente entre dos partes, sin regulación, no se tienen restricciones geográficas, es rápido y anónimo.

Luego de que el atacante tiene en su poder los bitcoins que obtuvo ilícitamente debe buscar la forma de lavar ese dinero, existen páginas en la Darkweb que ofrecen estos servicios y otras estrategias para poner estos recursos en el mundo real como desviar estos fondos a múltiples cuentas y realizar retiro en cajero automático, o compra de activos o mercancías en línea [18].

Aunque se tiene anonimato en las transacciones realizadas con bitcoin, de acuerdo a una noticia en la web de KPMG [19] el FBI logro recuperar parte del pago de un rescate,

por un ataque sobre la empresa energética Colonia Pipeline Co. Este tipo de acciones sumado a la desvalorización de la moneda de Bitcoin pueden ser un factor que desaliente a los criminales a realizar estos ataques.

En parte debido a los problemas de privacidad del Bitcoin surge una nueva criptomoneda que los atacantes han incorporado como opción de pago en sus actividades ilícitas, se trata de Zcash que introduce una capa adiciona de cifrado, que oculta los datos que identifica la transacción como emisor, monto de dinero y destinatario [20]. Inclusive la campaña de Ransomware LockBit 3.0 ha lanzado un programa de recompensas haciendo uso de Zcash, para aquellos que reporten errores e indiquen nuevas tácticas de ataque, algo completamente ilegal pero que demuestra la capacidad financiera que tiene este tipo de organizaciones delictivas [21].

2.9 Vectores de ataque

El Instituto Nacional De Ciberseguridad INCIBE describe los 10 vectores de ataque más usados por los ciberdelincuentes [22]:

Vectores de ataque	1. Correo Electrónico: phishing, se intenta robar credenciales o que la víctima descargue archivos maliciosos.
	2. Navegación web: visitar paginas fraudulentas, vulnerabilidad por falta de actualización o plugins maliciosos.
	3. Endpoints vulnerables: terminales o equipos que no tienen configuraciones de seguridad adecuadas.
	4. Aplicaciones web, portal corporativo: configuraciones defectuosas que permitan el ingreso de un atacante.
	5. Redes mal configuradas: software desactualizado, configuraciones por defecto o mal realizadas.
	6. Credenciales de usuario comprometidas: por fuga de datos, ingeniería social, keyloggers.
	7. Contraseñas por defecto: falta u omisión de configuración de credenciales por defecto.
	8. Insiders: personas con acceso que filtran información de la compañía.
	9. Carencia Cifrado: uso de algoritmos y claves de cifrado débiles.
	10. Debilidades de cadena de suministro: falla en resguardo de información de proveedores causado por incidentes.

Figura 9: Vectores de ataque, elaboración propia a partir de [22]

Las tácticas de los atacantes están en constante evolución, IC3 [12] indica en su informe de 2021 que los 3 principales vectores de ataque son phishing, exploits de acceso a escritorio remoto RDP y explotación de vulnerabilidades de software. Con un aumento drástico a partir del 2020 en parte impulsado por el trabajo remoto y conexiones en nube a causa de la pandemia COVID19.

2.10 Técnicas y modos de operación

2.10.1 Descubrimiento de red:

Cuando un malware alcanza una red corporativa y compromete un host puede realizar un escaneo de la red para propagar la infección, existen varios mecanismos que se ubican en capas del modelo OSI. Inicialmente es posible realizar un escaneo ARP en capa 2 y encontrar equipos que se encuentren en el mismo segmento de red. A nivel de capa 3 podemos usar el protocolo ICMP para hacer un ping masivo en la red y descubrir equipos, este mecanismo tiene el inconveniente de que necesita ser enrutado y posiblemente pase por un firewall lo cual limitaría el resultado. Otra alternativa es enviar paquetes TCP y UDP en la capa de transporte y esperar respuesta de algún host [23].

2.10.2 Wake on LAN:

Otra técnica usada por Ransomware es usar la función Wake on LAN para encender ordenadores de manera remota en la red LAN, esto se realiza mediante paquetes UDP hacia todas las direcciones de la tabla ARP, acto seguido envía paquetes ICMP para conocer las IP de los nuevos equipos a atacar [24].

Después de conocer los equipos que hacen parte de la red un atacante tiene la capacidad de moverse lateralmente y afectar otras computadoras y servidores con la intención de alcanzar y afectar la mayor cantidad de información posible.

2.10.3 Directorio activo y políticas de grupo:

Cuando se compromete e infecta un servidor de directorio activo LockBit puede automatizar la propagación en una red LAN, usa el protocolo LDAP para tener un listado de equipos y crea políticas de grupo que se envían a cada máquina del dominio [25], en un principio se intentara deshabilitar la seguridad en los ordenadores al bajar servicios de Windows defender o antivirus, para luego crear tareas programadas y ejecutar el malware en cada dispositivo.

2.10.4 Distribución de carga útil:

Los atacantes cada vez intentan buscar nuevas formas de ataque y de ocultar sus acciones y movimientos, de esta manera evadir ser detectados por los sistemas de seguridad. En este punto la intención es distribuir y ocultar el malware hasta que llegue a la víctima para luego ser ejecutado. El correo electrónico es uno de los principales vectores para distribuir malware y en los últimos años los atacantes han optado por realizar macros o códigos e incrustarlos en documentos legítimos como por ejemplo en Microsoft Office (Word, Power Point, Excel), PDF entre otros, cuando la víctima abre este tipo de adjuntos el macro se ejecuta y el malware se inicia en la máquina. Este tipo de ataques hicieron que Microsoft optara por deshabilitar la ejecución automática de macros [26].

2.10.5 Malware sin Archivos:

Una de las últimas técnicas de los atacantes es el malware en donde no se requiere un archivo en el host para su ejecución, estos se ejecutan en aplicaciones en memoria RAM y para lograr persistencia pueden enconder el código malicioso en el registro de Windows y carpeta de inicio, usan el WMI para instalar crear puertas traseras en donde el atacante pueda tener acceso al equipo [27].

2.10.6 Herramientas de hacking:

Existen diversas herramientas como Cobalt Strike, Mimikatz y Metasploit que el personal de seguridad de la información usa para pruebas de pentesting, simular ataques de amenazas persistentes APT, descubrir vulnerabilidades, explorar puertos, movimiento lateral, recuperación de contraseñas, entre otras. Estos programas son usados para probar los sistemas de seguridad empresariales y a nivel educativo en el entrenamiento y análisis defensivo. Aunque su concepción y políticas de uso apuntan a la legalidad, desafortunadamente estas herramientas son de doble filo y su uso ilegal es muy frecuente. La agencia de seguridad cibernética del gobierno de Estados Unidos (CISA) en un informe de marzo de 2023 [28] indica que la campaña de Ransomware LockBit 3.0 usa herramientas como Cobalt Strike y Metasploit para reconocimiento de red, acceso remoto y creación de túneles y exfiltración de información. Señala también que los afiliados de esta campaña de Ransomware usan herramientas legitimas y gratuitas como se muestra en la siguiente figura.

Tool	Description	MITRE ATT&CK ID
Chocolatey	Command-line package manager for Windows.	T1072
FileZilla	Cross-platform File Transfer Protocol (FTP) application.	T1071.002
Impacket	Collection of Python classes for working with network protocols.	S0357
MEGA Ltd MegaSync	Cloud-based synchronization tool.	T1567.002
Microsoft Sysinternals ProcDump	Generates crash dumps. Commonly used to dump the contents of Local Security Authority Subsystem Service, LSASS.exe.	T1003.001
Microsoft Sysinternals PsExec	Execute a command-line process on a remote machine.	S0029
Mimikatz	Extracts credentials from system.	S0002
Ngrok	Legitimate remote-access tool abused to bypass victim network protections.	S0508
PuTTY Link (Plink)	Can be used to automate Secure Shell (SSH) actions on Windows.	T1572
Rclone	Command-line program to manage cloud storage files.	S1040
SoftPerfect Network Scanner	Performs network scans.	T1046
Splashtop	Remote-desktop software.	T1021.001
WinSCP	SSH File Transfer Protocol client for Windows.	T1048

Figura 10: Herramientas gratuitas usadas por LockBit3.0, fuente [28]

2.11 Medidas de defensa

ENISA [4] recomienda las siguientes acciones para prevenir ataques de Ransomware y mitigar el impacto:

Recomendaciones ENISA	Copias de seguridad de todos los datos, actualizadas y aisladas de la red.
	Regla de respaldo 3-2-1. 3 copias, 2 medios de almacenamiento diferentes, 1 copia fuera del sitio o nube.
	Mantener datos personales encriptados.
	Ejecutar Software de seguridad para detectar Ransomware.
	Mantener políticas de seguridad, segmentación de redes, sistemas actualizados, gestión de usuarios, uso de MFA.
	Realizar evaluación de riesgos.
	Restringir privilegios administrativos, usar el principio de privilegio mínimo.
	Familiarizarse con entes gubernamentales de seguridad que brindan asistencia y definen protocolos.

Figura 11: Recomendaciones ENISA, elaboración propia a partir de [4]

Un factor adicional es la necesidad de que en el entorno empresarial todos los empleados tengan conocimiento de las políticas de seguridad, explicar los riesgos a los que se exponen con tareas sencillas como abrir un correo desconocido o compartir datos en portales web.

2.12 Uso de inteligencia artificial para combatir el Ransomware

En los últimos años los proveedores de servicios de seguridad de sistemas de TI como IDS, EDR, Firewall, antivirus han optado por incluir motores de inteligencia artificial para prevenir y detectar de una manera más eficiente y oportuna el ataque de este tipo de malware.

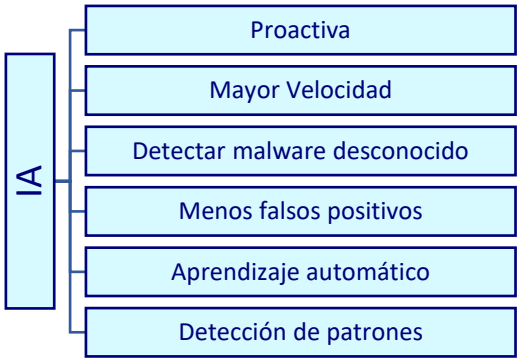


Figura 12: Ventajas Inteligencia Artificial, elaboración propia a partir de [29] y [30]

En resumen, la IA puede monitorear patrones de uso de los dispositivos y grandes cantidades de datos para luego detectar actividades inusuales y finalmente desplegar de manera oportuna respuestas automatizadas. Estas notables capacidades vienen a apoyar la función del personal de seguridad de la información, impulsando la mejora continua y la prevención de ataques.

2.13 Legislación aplicable

Diversos países en su lucha contra al actual problema de los ciberdelitos, continuamente crean y actualizan su legislación con el ánimo de dar respuesta efectiva. Un factor reciente fue la aparición de la pandemia COVID19 y el aumento de los ciberdelitos donde surge como reacción el Real Decreto 1150/2021, de 28 de diciembre, por el que se aprueba y actualiza la Estrategia de Seguridad Nacional 2021, en el tercer capítulo se reconocen algunos riesgos para la seguridad, donde el Ransomware se distingue como una tipología de amenaza en el ciberespacio, que actúa sobre elementos tecnológicos y puede secuestrar información y denegar el servicio [31].

Continuando con la legislación en España abordamos el Real Decreto 43/2021, de 26 de enero [32], que tiene como objeto desarrollar el Real Decreto-ley 12/2018 de 7 de septiembre, decretos relativos a la directiva NIS (Security of Network and Information Systems) 2016/1148 de la Unión Europea. Parte de este texto denota la importancia en la notificación de incidentes, en los artículos 8 al 11 expresa la obligación de los operadores esenciales de reportar estos eventos que alteran el funcionamiento de redes y sistemas de información, enuncia un procedimiento para estas notificaciones en la Plataforma Nacional de Notificación y Seguimiento de Ciber incidentes con el ánimo de intercambiar información entre CSIRT, autorizadas competentes y gubernamentales. Esta información servirá de insumo para generar un reporte anual con el tipo y cantidad de incidentes y su efecto [32]. En el transcurso de este TFM se ha referenciado el impacto que tienen los ciberdelitos en la sociedad, sin embargo, es importante resaltar que la mayor cantidad de incidentes nunca se reportan lo cual en cierta medida favorece estos delitos, debido a que no se cuantifica el daño total, no compartir y divulgar esta información impide que se desarrollen e implantes mecanismos de defensa.

En cuanto a las sanciones y penas para este tipo de delitos aún se mantiene vigente la Ley Orgánica 10/1995, de 23 de noviembre [33], en el artículo 264 del Código Penal se describen acciones delictivas típicas que se desarrollan en el delito de Ransomware *"El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a tres años"* [33], existen algunos agravantes como si esta actividad de desarrollo en conjunto de una organización criminal, la gravedad del daño, afectar servicios públicos, de primera necesidad o sistemas críticos.

Es imperativo que la legislación mantenga una actualización constante para clasificar y enmarcar los delitos causados por el malware, ajustar las penas y sanciones que faciliten el principio de proporcionalidad, pues este tipo de ciberdelitos pueden generar

perdidas de millones de dólares y causar afectación de servicios esenciales como en el sector salud.

3. Simulación en ambiente controlado

Para el análisis del modo de ejecución y mecanismos usados por el Ransomware LockBit se llevó a cabo el siguiente proceso:

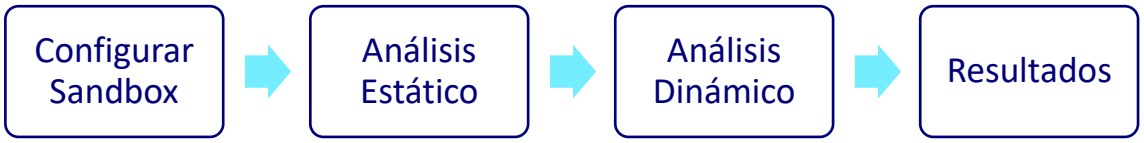


Figura 13: Proceso de simulación y análisis

3.1 Configurar Sandbox

En una computadora sin ningún tipo de información personal se instaló la aplicación de virtualización Virtual Box y una máquina Windows 10.

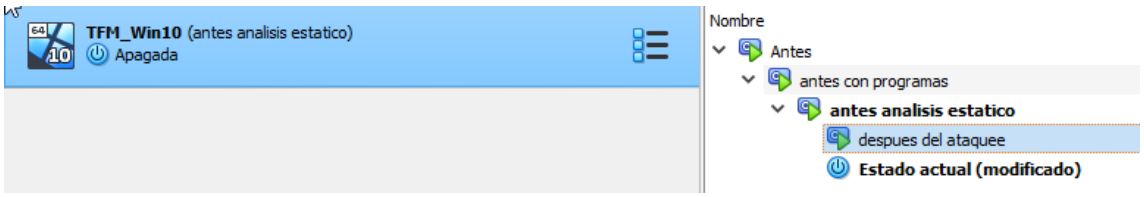


Figura 14: Sandbox

En esta máquina se instalaron algunos programas para el análisis como, Ghidra, Pestudio, Process Monitor, Regshot, Wireshark y x64dbg.

En este entorno controlado ya es posible ejecutar pruebas de una forma aislada y sin afectar datos o usuarios. El paso siguiente fue descargar una muestra del Ransomware LockBit https://github.com/Ucodedev/lockbit-3.0-files, y extraer todos los ficheros identificando el archivo de ejecución principal LB3.exe.

3.2 Análisis estático

En este punto se analiza el ejecutable LB3.exe, mediante herramientas para examinar el código fuente y obtener información, sin llegar en ningún momento a ejecutar el código malicioso.

En uno de los archivos de configuración de este malware es posible realizar una parametrización del ataque, escoger los medios a atacar, finalizar servicios de sistema, establecer fondo de pantalla, iconos, excluir carpetas, archivos o extensiones, asignar usuarios y contraseñas para un ataque dirigido.


```
"config": {
    "settings": {
      "encrypt_mode": "auto",
      "encrypt_filename": false,
      "impersonation": true,
      "skip_hidden_folders": false,
      "language_check": false,
      "local_disks": true,
      "network_shares": true,
      "kill_processes": true,
      "kill_services": true,
      "running_one": true,
      "print_note": true,
      "set_wallpaper": true,
      "set_icons": true,
      "send_report": false,
      "self_destruct": true,
      "kill_defender": true,
      "wipe_freespace": false,
      "psexec_netspread": false,
      "gpo_netspread": true,
      "gpo_ps_update": true,
      "shutdown_system": false,
      "delete_eventlogs": true,
      "delete_gpo_delay": 1
```


Figura 15: Opciones de configuración LB3.exe

Con la herramienta Pestudio se identifican las librerías que emplea el ejecutable:

library (3)	duplicate (0)	flag (0)	bound (0)	first-thunk-original (INT)	first-thunk (IAT)	type (1)	imports (24)
gdi32.dll	-	-	-	0x0001A2D0	0x0001A050	implicit	6
USER32.dll	-	-	-	0x0001A2A0	0x0001A020	implicit	11
KERNEL32.dll	-	-	-	0x0001A280	0x0001A000	implicit	7

Figura 16: Librerías usadas por LB3.exe

Con el uso de gdi32.dll el Ransomware puede realizar operaciones con los gráficos del sistema operativo, desplegar mensajes, manipular imágenes o elementos visuales para disuadir a la víctima.

La librería user32.dll del sistema operativo Windows es usada para funciones con la interfaz gráfica de usuario permite la manipulación de ventanas o menús, creación, modificar propiedades, desplegar mensajes. El Ransomware puede hacer uso de esta librería para:

- Crear ventanas emergentes para indicar algún error al usuario o solicitar una entrada o aceptación, desplegar mensajes falsos.

- Ocultar o cerrar ventanas, impidiendo al usuario el uso normal de la computadora, también se puede cambiar la apariencia de las ventanas y engañar al usuario.

- USER32.dll también puede usarse para interceptar eventos con el teclado y mouse, capturar lo que el usuario escribe y monitorear la actividad.

Otra de las librerías usadas por LockBit y quizás la más importante es kernel32.dll, originalmente es usada por el sistema operativo como modulo central que contiene el núcleo de procesos, se encarga de controlar las operaciones, tareas y programas en ejecución. Algunas de las formas en que es usada esta librería por el Ransomware son:

- Manipular carpetas y ficheros: Es posible buscar, abrir, modificar, eliminar archivos. Este es el punto central pues permite al malware de forma masiva encontrar y cifrar la información del usuario para luego eliminarla.

- Procesos y tareas: Permite usar procesos legítimos del sistema operativo, crear nuevos procesos, ejecución en segundo plano del código malicioso.

- Alterar registro de Windows: Permite leer y escribir el registro de Windows, con esto el Ransomware puede realizar modificaciones al sistema, otorgarse permisos, deshabilitar controles y tener persistencia.

- Manipulación de memoria: Esta librería permite la gestión de la memoria RAM del equipo, esto puede ser usado para inyectar código malicioso en procesos legítimos y evadir los sistemas de detección.

Funciones que se encontraron en el análisis estático del ejecutable, donde algunas se vinculan con técnicas descritas en Mitre Att&ck.

imports (24)	flag (2)	hint	group (5)	technique (3)	type (1)	library (3)
GetTickCount	-	758 (0x02F6)	reconnaissance	T1124 | System Time Discovery	implicit	KERNEL32.dll
LoadLibraryW	-	943 (0x03AF)	dynamic-library	T1106 | Execution through API	implicit	KERNEL32.dll
GetWindowTextW	x	419 (0x01A3)	windowing	T1010 | Window Discovery	implicit	USER32.dll
DefWindowProcW	-	156 (0x009C)	windowing	-	implicit	USER32.dll
GetMessageW	-	349 (0x015D)	windowing	-	implicit	USER32.dll
GetKeyNameTextW	x	316 (0x013C)	input-output	-	implicit	USER32.dll
GetCommandLineW	-	458 (0x01CA)	execution	-	implicit	KERNEL32.dll
GetCommandLineA	-	457 (0x01C9)	execution	-	implicit	KERNEL32.dll
FreeLibrary	-	414 (0x019E)	dynamic-library	-	implicit	KERNEL32.dll

Figura 17: Funciones usadas por LB3.exe

GetTikCount: El adversario intenta averiguar la zona horaria y hora del sistema, esto puede ser útil para ejecutar tareas programadas y descubrir la localización de la víctima.

LoadLibraryW: Usada para interactuar con el sistema operativo y solicitar servicios, un llamado a esta función permite eludir herramientas defensivas, desconectar o cerrar funciones de seguridad como Windows Defender.

GetWindowsTextW: Un adversario puede obtener una lista de las aplicaciones abiertas en la máquina del usuario, conocer el uso del sistema, si se tienen sistemas de seguridad en ejecución.

Siguiendo con la herramienta Pestudio se encontraron diversos strings o comandos, que nos dan una idea global de lo que puede realizar el ejecutable LB3.exe, como desplegar mensajes, obtener información del sistema, procesos en ejecución, ventanas abiertas, cargar librerías, imágenes, archivos.

size (bytes)	flag (2)	label (42)	group (5)	technique (3)	value (4441)
13	-	import	windowing	-	DefWindowProc
10	-	import	windowing	-	GetMessage
13	x	import	windowing	T1010 | Window Discovery	GetWindowText
12	-	import	reconnaissance	T1124 | System Time Discovery	GetTickCount
14	x	import	input-output	-	GetKeyNameText
14	-	import	execution	-	GetCommandLine
14	-	import	execution	-	GetCommandLine
11	-	import	dynamic-library	-	FreeLibrary
11	-	import	dynamic-library	T1106 | Execution through API	LoadLibrary
16	-	import	-	-	CreateSolidBrush
13	-	import	-	-	GetDeviceCaps
12	-	import	-	-	GetTextColor
13	-	import	-	-	SelectPalette
15	-	import	-	-	SetDCBrushColor
8	-	import	-	-	SetPixel
10	-	import	-	-	CreateMenu
14	-	import	-	-	DialogBoxParam
9	-	import	-	-	EndDialog
10	-	import	-	-	GetDlgItem
18	-	import	-	-	IsDlgButtonChecked
9	-	import	-	-	LoadImage
8	-	import	-	-	LoadMenu
12	-	import	-	-	GetLastError

Figura 18: Strings usados por LB3.exe

Para continuar con el análisis estático, mediante la herramienta Ghidra desarrollada por la Agencia de Seguridad Nacional de los Estados Unidos (NSA), podemos observar en detalle las librerías del sistema operativo que el Ransomware usa “Imports” y en “Exports” las librerías que se usaran para atacar el sistema.

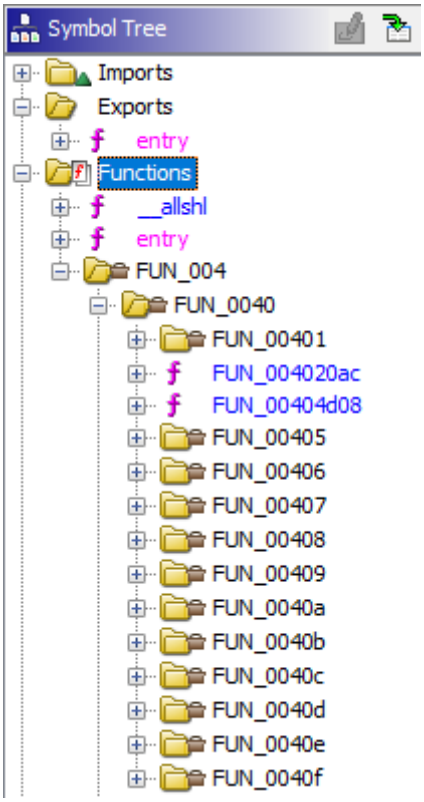


Figura 19: Funciones Export LB3.exe

Como se observa en Exports tenemos una función llamada “entry” la cual está compuesta por decenas de funciones con una estructura bastante compleja, a continuación de muestran algunas fracciones de código:

ProcessEnvironmentBlock es una estructura de datos que contiene información acerca de los procesos de Windows, se observa que este Malware intenta descubrir, manejar y controlar los procesos del sistema.

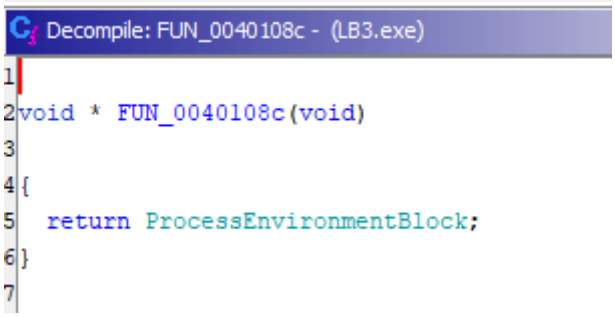


Figura 20: Función ProcessEnvironmentBlock

Definición de múltiples variables y usos de funciones random para alterar la estructura de información de la máquina.

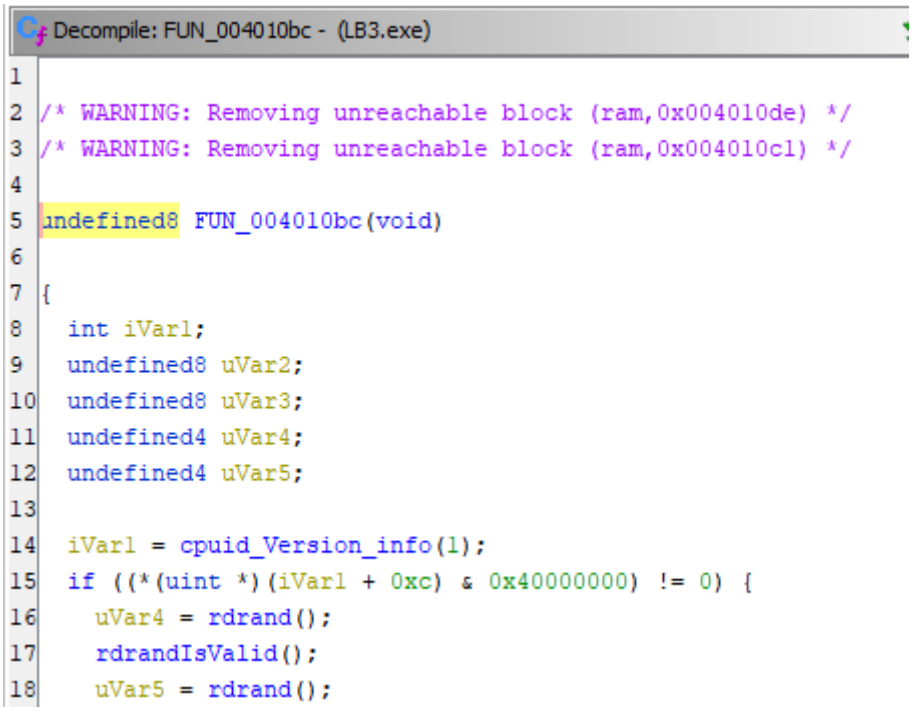


Figura 21: Función definir variables

Realiza cálculos matemáticos para afectar la estructura de archivos, es las siguientes imágenes podemos observar cómo realiza operaciones entre variables posiblemente para el cifrado de datos.

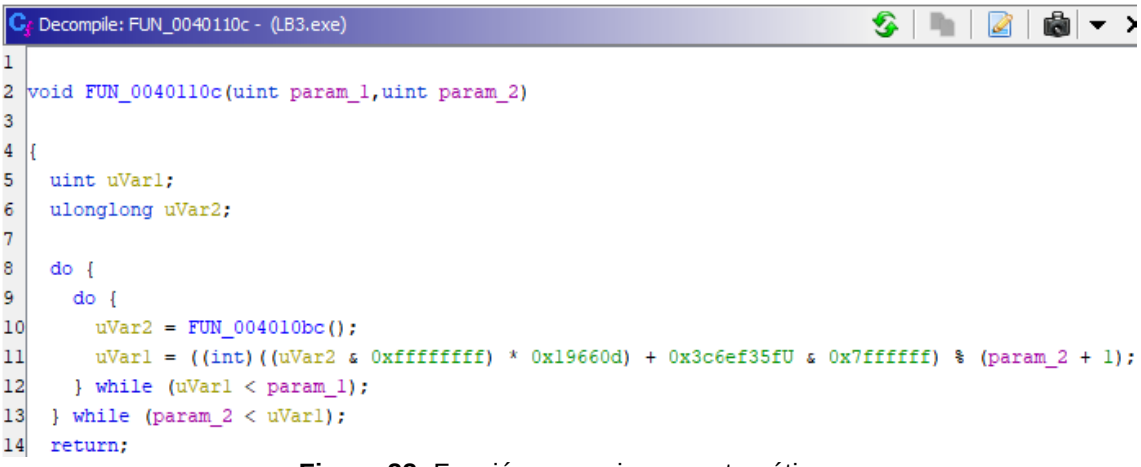


Figura 22: Función operaciones matemáticas

Se tienen diversas funciones en las figuras 23 y 24, la gran mayoría con procesos y cálculos numéricos para múltiples variables.

Figura 23: Función operaciones matemáticas 2

```
*(undefined4 *)(*(int *)((int)this + 0x10) + iVar2 * 4) =
     *(undefined4 *)
      (*(int *)((int)this + (uint)**(byte **)((int)this + 0x418) * 4 + 0x14) +
      (uint)(*(byte **)((int)this + 0x418))[1] * 4);
*(undefined4 *)
 (*(int *)((int)this + (uint)**(byte **)((int)this + 0x418) * 4 + 0x14) +
 (uint)(*(byte **)((int)this + 0x418))[1] * 4) = *(undefined4 *)((int)this + 0x4]
*(int *)((int)this + 0x414) = *(int *)((int)this + 0x414) + 1;
*(int *)((int)this + 0x418) = *(int *)((int)this + 0x418) + 1;
if (0x16800 < (uint)(*(int *)((int)this + 0x414) - *(int *)((int)this + 0x41c)))
  *(int *)((int)this + 0x41c) = *(int *)((int)this + 0x414) + -1;
}
```

Figura 24. Función operaciones matemáticas 3

3.2.1 Análisis MD5

Para el análisis de esta variante de LockBit se tomó el hash MD5 9b9d47110c131ee17bf08df6b3787f43

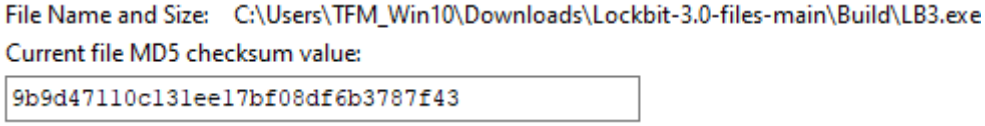


Figura 25. Análisis MD5

El cual corresponde a uno de los ejecutables distribuidos por el grupo de amenazas de LockBit. Al ser analizado en VirusTotal fue identificado como malicioso por 54 de 70 proveedores.

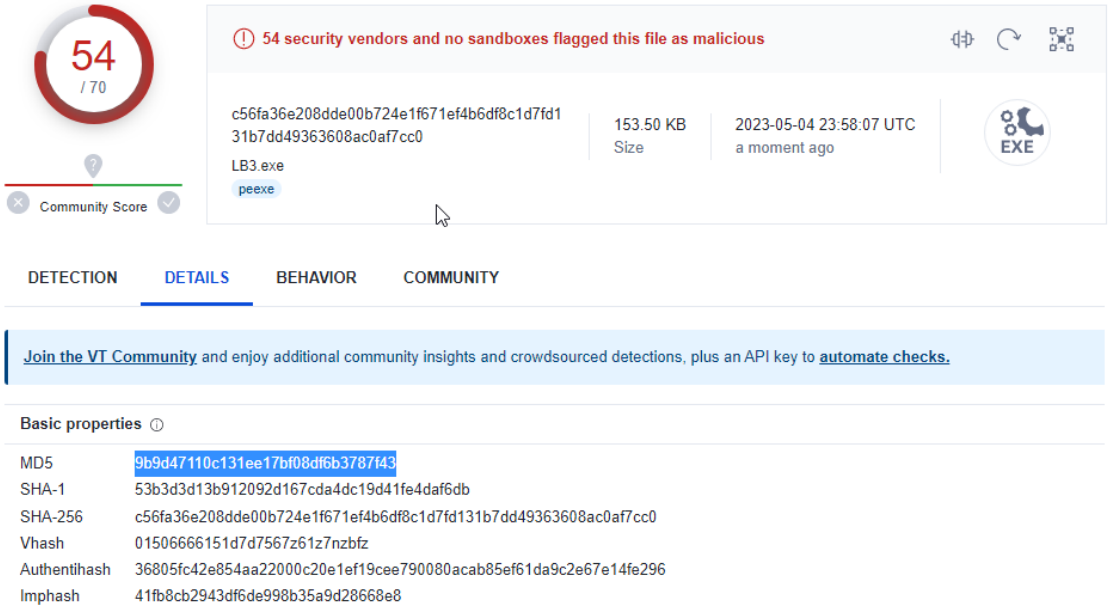


Figura 26. VirusTotal análisis LB3.exe

Proveedores que reportaron este ejecutable como un código malicioso:

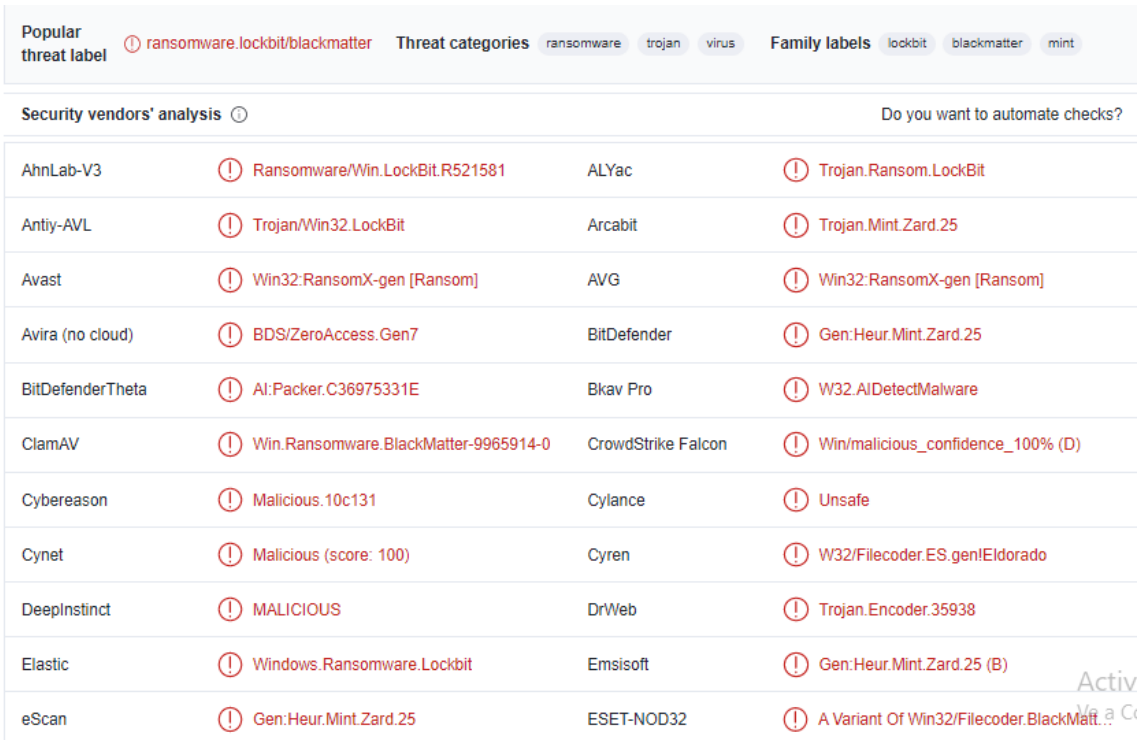


Figura 27: VirusTotal reporte vendors 1

F-Secure	Backdoor.BDS/ZeroAccess.Gen7	Fortinet	W32/Lockbit.K!tr.ransom
GData	Gen:Heur.Mint.Zard.25	Google	Detected
Gridinsoft (no cloud)	Ransom.Win32.Qadars.oa!s1	Ikarus	Trojan-Ransom.BlackMatter
Jiangmin	Trojan.Crypmodng.cd	Kaspersky	HEUR:Trojan-Ransom.Win32.Generic
Malwarebytes	Qadars.Trojan.Banking.DDS	MAX	Malware (ai Score=89)
MaxSecure	Trojan.Malware.300983.susgen	McAfee	BlackMatter!9B9D47110C13
McAfee-GW-Edition	BehavesLike.Win32.BlackMatter.cc	Microsoft	Ransom:Win32/Lockbit.HA!MTB
NANO-Antivirus	Virus.Win32.Gen.ccmw	Panda	Trj/Genetic.gen
QuickHeal	Ransom.Lockbit.S28885638	Rising	Ransom.LockBit!1.DFDC (CLASSIC)
Sangfor Engine Zero	Ransom.Win32.Save.LockBit30	SecureAge	Malicious
SentinelOne (Static ML)	Static AI - Suspicious PE	Sophos	ML/PE-A
TACHYON	Ransom/W32.Agent.157184	Tencent	Virus.Win32.BlackMatter.b
Trapmine	Malicious.high.ml.score	Trellix (FireEye)	Generic.mg.9b9d47110c131ee1
TrendMicro	Ransom.Win32.LOCKBIT.SMYXCGU	VBA32	TrojanRansom.Crypmodng

Figura 28: VirusTotal reporte vendors 2

Continuando con el análisis estático, se usó el sitio de VirusTotal para cargar el archivo LB3.exe y realizar un mapa de relaciones de este malware.

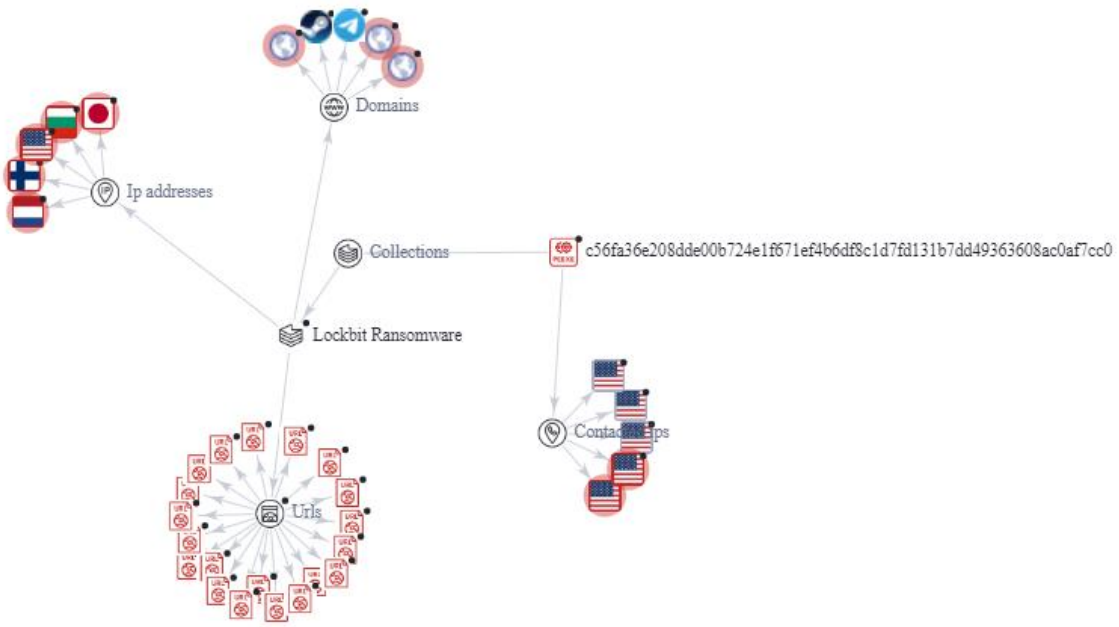


Figura 29: VirusTotal mapa relaciones

Encontrando algunos de los proveedores que han reportado este mismo ejecutable, las URL y dominios implicados en la ejecución del malware, IP detectadas como maliciosas.

Este tipo de mapas ayudan a comprender las relaciones entre diferentes indicadores de compromiso, entender cómo se propagan y las conexiones usadas. De tener nuevas versiones de este malware es posible revisar conexiones en común, si existe algún tipo de patrón.

De acuerdo a lo expuesto en este TFM el Ransomware está en constante evolución y las diferentes campañas de Ransomware en ocasiones comparten funcionalidades, código, e indicadores de compromiso, con esta herramienta es posible visualizar si comparten infraestructura y son comandadas desde el mismo sitio.

3.3 Análisis dinámico

En este punto se ejecuta el código fuente de LockBit y registra el comportamiento, procedemos a tomar evidencias y capturas de los procesos en ejecución, conexiones de red, archivos de confirmación de ataque y solicitud de pago.

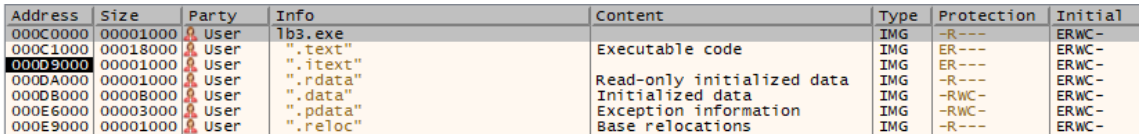
Iniciamos con la herramienta open source x64dbg donde analizamos el llamado de funciones del ejecutable y la información en memoria del sistema.

Address	Disassembly	Destination
000D94B0	call <JMP.&GetTickCount>	<kernel32.GetTickCount> (754823A0)
000D94B5	call <JMP.&GetCommandLineW>	<kernel32.GetCommandLineW> (75481D70)
000D94BA	call <JMP.&FreeLibrary>	<kernel32.FreeLibrary> (75480AE0)
000D94BF	call <JMP.&GetLastError>	<kernel32.GetLastError> (7547E010)
000D94C4	call <JMP.&FreeLibrary>	<kernel32.FreeLibrary> (75480AE0)
000D94C9	call <JMP.&FreeLibrary>	<kernel32.FreeLibrary> (75480AE0)
000D94CE	call <JMP.&GetCommandLineA>	<kernel32.GetCommandLineA> (75481EE0)
000D94D3	call <JMP.&SetLastError>	<kernel32.SetLastError> (7547DFA0)
000D94D8	call <JMP.&LoadLibraryW>	<kernel32.LoadLibraryW> (754816C0)
000D94DD	call <JMP.&IsDlgButtonChecked>	<user32.IsDlgButtonChecked> (7680B660)
000D94E2	call <JMP.&EndDialog>	<user32.EndDialog> (7680A650)
000D94E7	call <JMP.&GetMessageW>	<user32.GetMessageW> (7681B390)
000D94EC	call <JMP.&GetDlgItem>	<user32.GetDlgItem> (76818FB0)
000D94F1	call <JMP.&LoadImageW>	<user32.LoadImageW> (76811320)
000D94F6	call <JMP.&LoadMenuW>	<user32.LoadMenuW> (76810450)
000D94FB	call <JMP.&GetWindowTextW>	<user32.GetWindowTextW> (76819D50)
000D9500	call <JMP.&GetKeyNameTextW>	<user32.GetKeyNameTextW> (768739A0)
000D9505	call <JMP.&NtdllDefWindowProc_W>	<ntdll.NtdllDefWindowProc_W> (77337FA0)
000D950A	call <JMP.&NtdllDefWindowProc_W>	<ntdll.NtdllDefWindowProc_W> (77337FA0)
000D950F	call <JMP.&GetWindowTextW>	<user32.GetWindowTextW> (76819D50)
000D9514	call <JMP.&EndDialog>	<user32.EndDialog> (7680A650)
000D9519	call <JMP.&CreateMenu>	<user32.CreateMenu> (7680BAA0)
000D951E	call <JMP.&DialogBoxParamW>	<user32.DialogBoxParamW> (7683E3F0)
000D9523	call <JMP.&SelectPalette>	<gdi32.SelectPalette> (76294290)
000D9528	call <JMP.&SetPixel>	<gdi32.SetPixel> (76295200)
000D952D	call <JMP.&CreateSolidBrush>	<gdi32.CreateSolidBrush> (76297340)
000D9532	call <JMP.&GetTextColor>	<gdi32.GetTextColor> (762941A0)
000D9537	call <JMP.&SetPixel>	<gdi32.SetPixel> (76295200)
000D953C	call <JMP.&GetDeviceCaps>	<gdi32.GetDeviceCaps> (76295EC0)
000D9541	call <JMP.&SetDCBrushColor>	<gdi32.SetDCBrushColor> (76297F50)

Figura 30: Librerías y strings usados por LB3.exe

Al igual que en el análisis estático se observa el llamado de las funciones kernel32, gdi32 y user32, pero al correr el ejecutable observamos el llamado de la librería ntdll usada administración de procesos en el sistema operativo, gestión de memoria y más importante aún la manipulación de archivos como apertura y escritura.

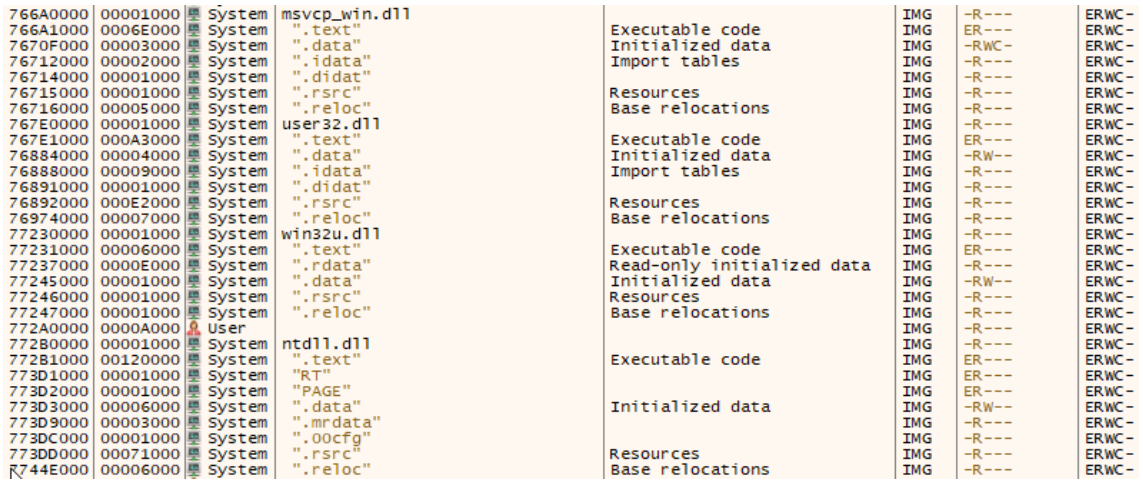
En memoria se observa que el ejecutable LB3.exe carga las secciones “.text” donde se almacena el código del ejecutable, “itext” y “rdata” para almacenar datos de lectura accesibles para el código fuente.



Address	Size	Party	Info	Content	Type	Protection	Initial
000C0000	00001000	User	lb3.exe		IMG	-R---	ERWC-
000C1000	00018000	User	".text"	Executable code	IMG	ER---	ERWC-
000D9000	00001000	User	".itext"		IMG	ER---	ERWC-
000DA000	00001000	User	".rdata"	Read-only initialized data	IMG	-R---	ERWC-
000DB000	0000B000	User	".data"	Initialized data	IMG	-RWC-	ERWC-
000E6000	00003000	User	".pdata"	Exception information	IMG	-RWC-	ERWC-
000E9000	00001000	User	".reloc"	Base relocations	IMG	-R---	ERWC-

Figura 31: Ejecución en memoria de LB3.exe

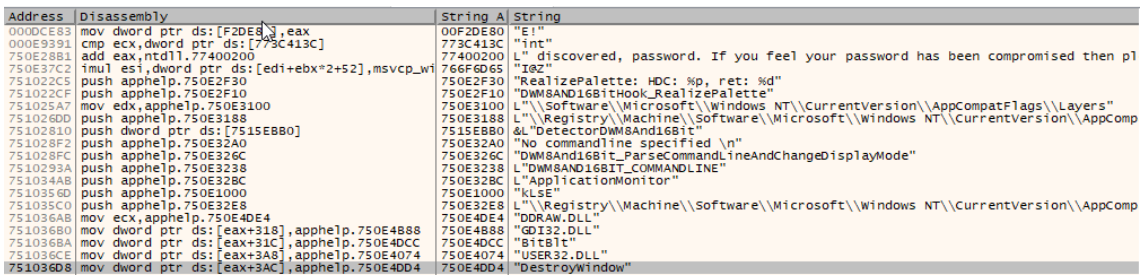
En cuanto a la información en memoria encontramos la ejecución de algunas librerías adicionales como “msvcp_win.dll” que nos indica que posiblemente el ejecutable fue desarrollado en Visual Studio y “win32u.dll” librería del sistema operativo para el control y gestión de ventanas e interfaz.



766A0000	00001000	System	msvcp_win.dll		IMG	-R---	ERWC-
766A1000	0006E000	System	".text"	Executable code	IMG	ER---	ERWC-
7670F000	00003000	System	".data"	Initialized data	IMG	-RWC-	ERWC-
76712000	00002000	System	".idata"	Import tables	IMG	-R---	ERWC-
76714000	00001000	System	".didat"		IMG	-R---	ERWC-
76715000	00001000	System	".rsrc"	Resources	IMG	-R---	ERWC-
76716000	00005000	System	".reloc"	Base relocations	IMG	-R---	ERWC-
767E0000	00001000	System	user32.dll		IMG	-R---	ERWC-
767E1000	000A3000	System	".text"	Executable code	IMG	ER---	ERWC-
76884000	00004000	System	".data"	Initialized data	IMG	-RW--	ERWC-
76888000	00009000	System	".idata"	Import tables	IMG	-R---	ERWC-
76891000	00001000	System	".didat"		IMG	-R---	ERWC-
76892000	000E2000	System	".rsrc"	Resources	IMG	-R---	ERWC-
76974000	00007000	System	".reloc"	Base relocations	IMG	-R---	ERWC-
77230000	00001000	System	win32u.dll		IMG	-R---	ERWC-
77231000	00006000	System	".text"	Executable code	IMG	ER---	ERWC-
77237000	0000E000	System	".rdata"	Read-only initialized data	IMG	-R---	ERWC-
77245000	00001000	System	".data"	Initialized data	IMG	-RW--	ERWC-
77246000	00001000	System	".rsrc"	Resources	IMG	-R---	ERWC-
77247000	00001000	System	".reloc"	Base relocations	IMG	-R---	ERWC-
772A0000	0000A000	User			IMG	-R---	ERWC-
772B0000	00001000	System	ntdll.dll		IMG	-R---	ERWC-
772B1000	00120000	System	".text"	Executable code	IMG	ER---	ERWC-
773D1000	00001000	System	"RT"		IMG	ER---	ERWC-
773D2000	00001000	System	"PAGE"		IMG	ER---	ERWC-
773D3000	00006000	System	".data"	Initialized data	IMG	-RW--	ERWC-
773D9000	00003000	System	".mrdata"		IMG	-R---	ERWC-
773DC000	00001000	System	".00cfg"		IMG	-R---	ERWC-
773DD000	00071000	System	".rsrc"	Resources	IMG	-R---	ERWC-
7744E000	00006000	System	".reloc"	Base relocations	IMG	-R---	ERWC-

Figura 32: Librerías adicionales usadas por LockBit

Este malware automáticamente cierra algunas ventanas del sistema operativo, mediante la función “DestroyWindows” e inicia modificaciones sobre el registro de Windows.



Address	Disassembly	String A	String
000DCE83	mov dword ptr ds:[F2DE8],eax	00F2DE80	"E!"
000E9391	cmp ecx,dword ptr ds:[773C413C]	773C413C	"int"
750E28B1	add eax,ntdll.77400200	77400200	L" discovered, password. If you feel your password has been compromised then pl
750E37C2	imul esi,dword ptr ds:[edi+ebx*2+52],msvcp_wi	766F6D65	"I@Z"
751022C5	push apphelp.750E2F30	750E2F30	"RealizePalette: HDC: %p, ret: %d"
751022CF	push apphelp.750E2F10	750E2F10	"DWM8AND16BitHook_RealizePalette"
751025A7	mov edx,apphelp.750E3100	750E3100	L"\\Software\\Microsoft\\Windows NT\\CurrentVersion\\AppCompatFlags\\Layers"
751026DD	push apphelp.750E3188	750E3188	L"\\Registry\\Machine\\Software\\Microsoft\\Windows NT\\CurrentVersion\\AppComp
75102810	push dword ptr ds:[7515EBB0]	7515EBB0	&L"DetectorDWM8And16Bit"
751028F2	push apphelp.750E32A0	750E32A0	"No commandline specified \n"
751028FC	push apphelp.750E326C	750E326C	"DWM8And16Bit_ParseCommandLineAndChangeDisplayMode"
7510293A	push apphelp.750E3238	750E3238	L"DWM8AND16BIT_COMMANDLINE"
751034AB	push apphelp.750E32BC	750E32BC	L"ApplicationMonitor"
7510356D	push apphelp.750E1000	750E1000	"kLsE"
751035C0	push apphelp.750E32E8	750E32E8	L"\\Registry\\Machine\\Software\\Microsoft\\Windows NT\\CurrentVersion\\AppComp
751036AB	mov ecx,apphelp.750E4DE4	750E4DE4	"DDRAW.DLL"
751036B0	mov dword ptr ds:[eax+318],apphelp.750E4B88	750E4B88	"GDI32.DLL"
751036BA	mov dword ptr ds:[eax+31C],apphelp.750E4DCC	750E4DCC	"BitBlt"
751036CE	mov dword ptr ds:[eax+3A8],apphelp.750E4074	750E4074	"USER32.DLL"
751036D8	mov dword ptr ds:[eax+3AC],apphelp.750E4DD4	750E4DD4	"DestroyWindow"

Figura 33: Función DestroyWindows

El Ransomware crea y asigna valores en el registro de Windows.

Address	Disassembly	String A	String
7514FE92	mov dword ptr ds:[eax+4],apphelp.750FC6F8	750FC6F8	"AccessCheck"
7514FEB2	mov dword ptr ds:[eax+1C],apphelp.750FC728	750FC728	"CheckTokenMembership"
7514FED2	mov dword ptr ds:[eax+34],apphelp.750FC540	750FC540	"RegCreateKeyA"
7514FEF2	mov dword ptr ds:[eax+4C],apphelp.750FC550	750FC550	"RegCreateKeyW"
7514FF12	mov dword ptr ds:[eax+64],apphelp.750FC560	750FC560	"RegCreateKeyExA"
7514FF32	mov dword ptr ds:[eax+7C],apphelp.750FC570	750FC570	"RegCreateKeyExW"
7514FF58	mov dword ptr ds:[eax+94],apphelp.750FC580	750FC580	"RegOpenKeyA"
7514FF81	mov dword ptr ds:[eax+AC],apphelp.750FC58C	750FC58C	"RegOpenKeyW"
7514FFAA	mov dword ptr ds:[eax+C4],apphelp.750FC598	750FC598	"RegOpenKeyExA"
7514FFD3	mov dword ptr ds:[eax+DC],apphelp.750FC5A8	750FC5A8	"RegOpenKeyExW"
7514FFFC	mov dword ptr ds:[eax+F4],apphelp.750FC5B8	750FC5B8	"RegSetValueA"
75150025	mov dword ptr ds:[eax+10C],apphelp.750FC5C8	750FC5C8	"RegSetValueW"
7515004E	mov dword ptr ds:[eax+124],apphelp.750FC5D8	750FC5D8	"RegSetValueExA"
75150077	mov dword ptr ds:[eax+13C],apphelp.750FC5E8	750FC5E8	"RegSetValueExW"
751500A0	mov dword ptr ds:[eax+154],apphelp.750FC5F8	750FC5F8	"RegSetKeyValueA"
751500C9	mov dword ptr ds:[eax+16C],apphelp.750FC608	750FC608	"RegSetKeyValueW"
751500F2	mov dword ptr ds:[eax+184],apphelp.750FC740	750FC740	"GetTokenInformation"
75150110	mov dword ptr ds:[eax+198],apphelp.750FC7A8	750FC7A8	"SHELL32.DLL"
7515011F	mov dword ptr ds:[eax+19C],apphelp.750FC754	750FC754	"IsUserAnAdmin"
7515013D	mov dword ptr ds:[eax+1B0],apphelp.750FC7B4	750FC7B4	"NETAPI32.DLL"
7515014C	mov dword ptr ds:[eax+1B4],apphelp.750FC764	750FC764	"NetUserGetInfo"

Figura 34: Modificaciones registro de Windows

Ahora al abrir el ejecutable “LB3.exe” el Ransomware LockBit inmediatamente cierra algunos servicios de Windows para desplegar su ataque como:

Centro de seguridad de Windows: Es una característica integrada del sistema operativo, el objetivo principal es proporcionar seguridad mediante servicios de antivirus, firewall, actualizaciones.

Figura 35: Mensaje desactivación servicio

Service VSS: Servicio de instantáneas de volumen que permite que las copias de seguridad se realicen mientras las aplicaciones se ejecutan.

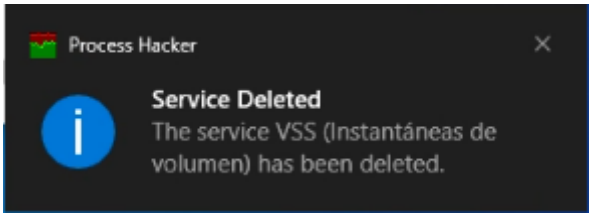


Figura 36: Mensaje eliminación servicio VSS

Servicio vmicvss: Se refiere específicamente al servicio VSS para copia de seguridad de máquinas virtuales completas.

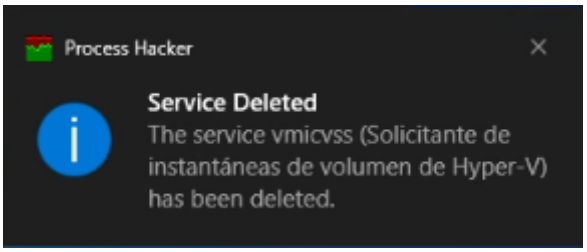


Figura 37: Mensaje eliminación servicio vmicvss

Servicios de Protección contra amenazas avanzada: Es una capa adicional de seguridad de Windows Defender, usa técnicas de análisis y detección avanzadas, como análisis de comportamiento, aprendizaje automático, protección en tiempo real.

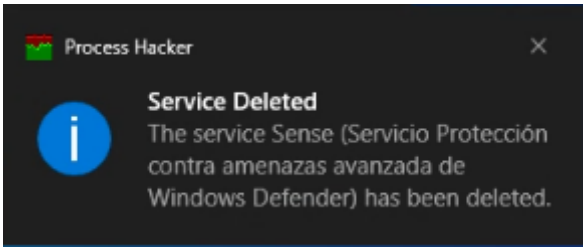


Figura 38: Mensaje eliminación Servicio de Protección contra amenazas avanzada

Al verificar los procesos en ejecución incluso después de reiniciar el equipo afectado, se encuentra TrustedInstaller el cual es usado para detener servicios legítimos de Windows [34].

Mediante un volcado de memoria y análisis con la herramienta Volatility y el comando ”pslist” observamos el proceso en ejecución.

```
Volatility Foundation Volatility Framework 2.6.1
0xffffa20e24561080 TrustedInstall         5456    632
```

Figura 39: TrustedInstaller usado para detener servicios

Durante la ejecución del malware se evidencia un alto uso del disco duro, por las actividades de lectura y escritura del Ransomware mientras realiza el cifrado de datos en la máquina afectada.

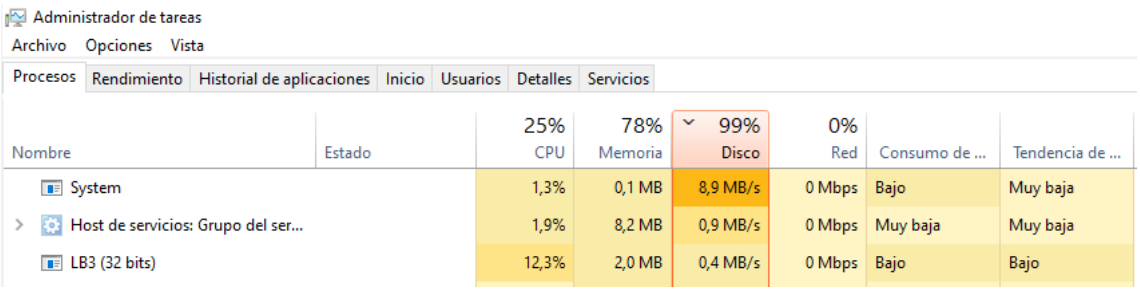


Figura 40: Proceso LB3.exe en ejecución

Encriptar los archivos del sistema operativo tarda unos pocos minutos, y al cabo de ese tiempo se despliega en el escritorio la nota de que los archivos han sido cifrados, tanto en el escritorio como en todas las carpetas del sistema se incluye el archivo de texto README.txt con las instrucciones, vínculos y opciones para contactar a los atacantes.

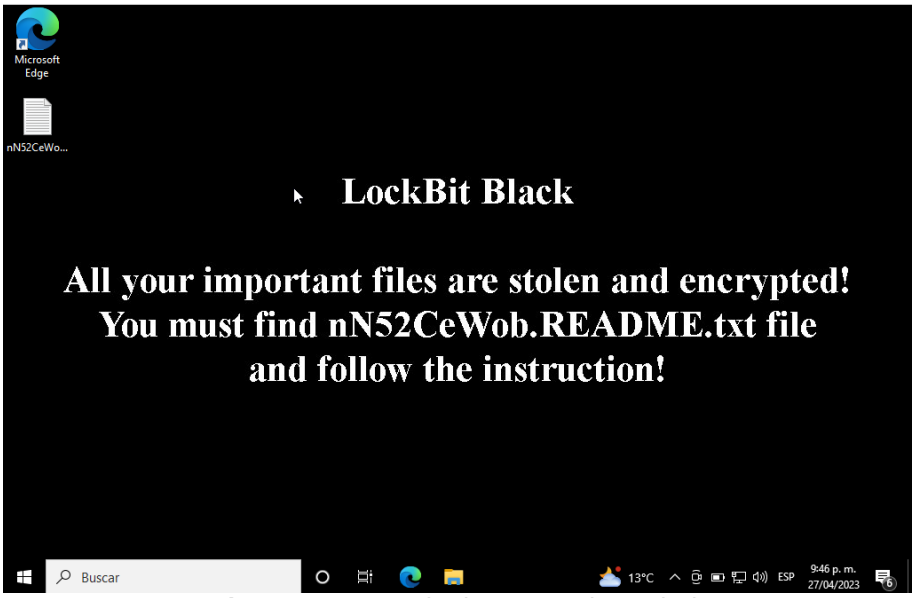


Figura 41: Mensaje de ataque de LockBit

Después del ataque no se puede acceder a características del sistema, como el administrador de tareas.

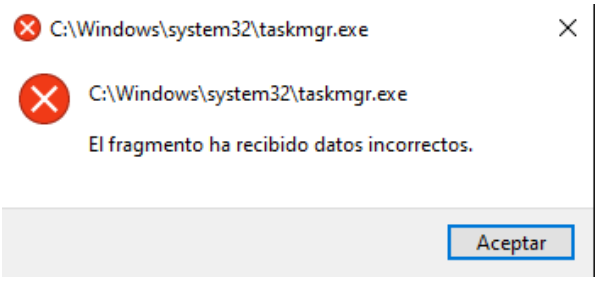


Figura 42: Mensaje error luego de ataque

En diversas carpetas se encuentra el archivo con la información del ataque y la solicitud de pago.

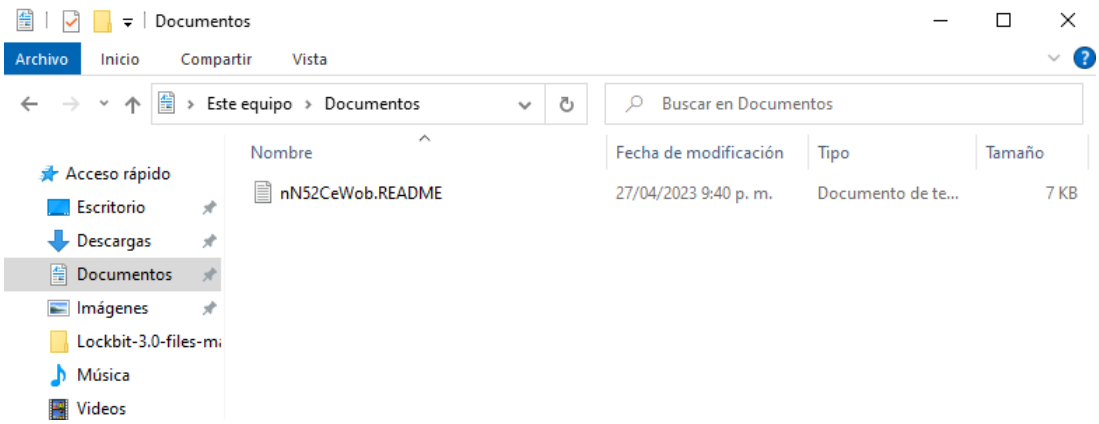


Figura 43: Archivo nota de rescate

Los archivos de la máquina se reemplazan por la nota de rescate, impidiendo el acceso del usuario a su información.

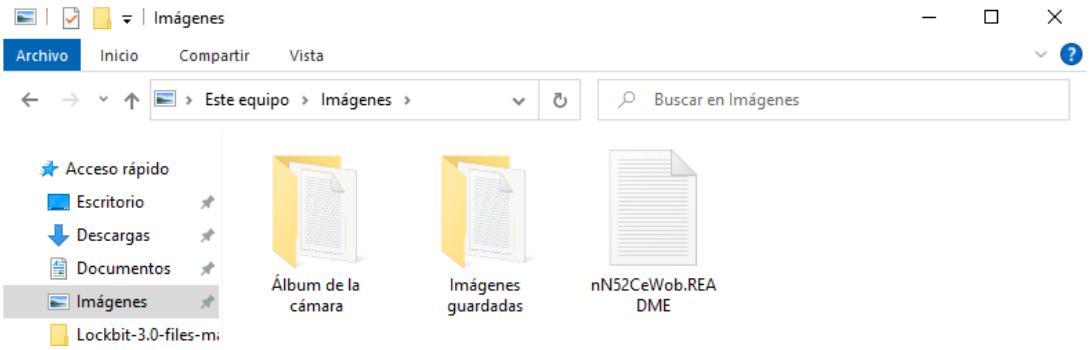


Figura 44: Archivos cifrados

El archivo de texto contiene el recordatorio de que el sistema ha sido atacado y despliegan links de contacto para el navegador TOR o navegadores tradicionales.

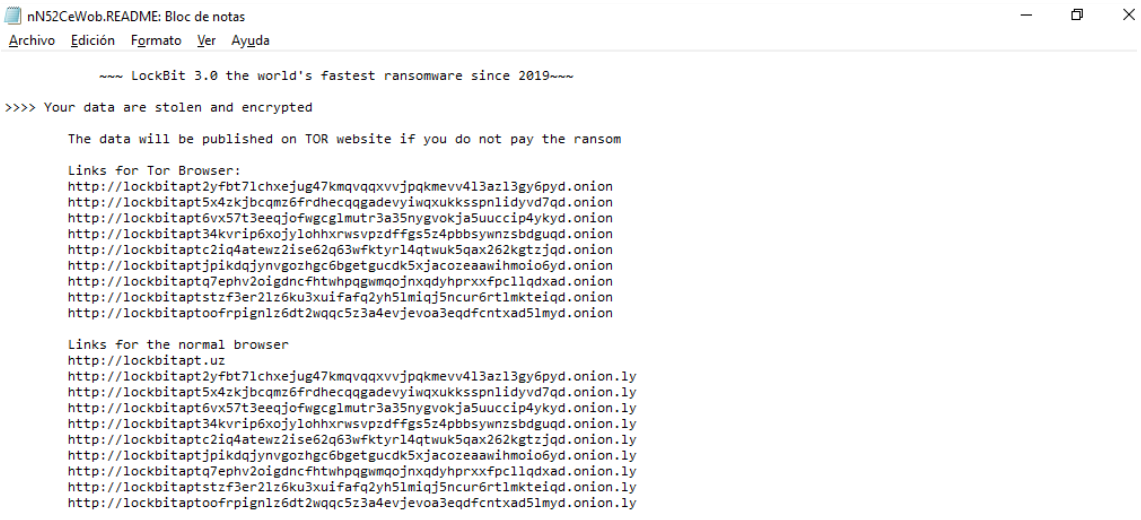
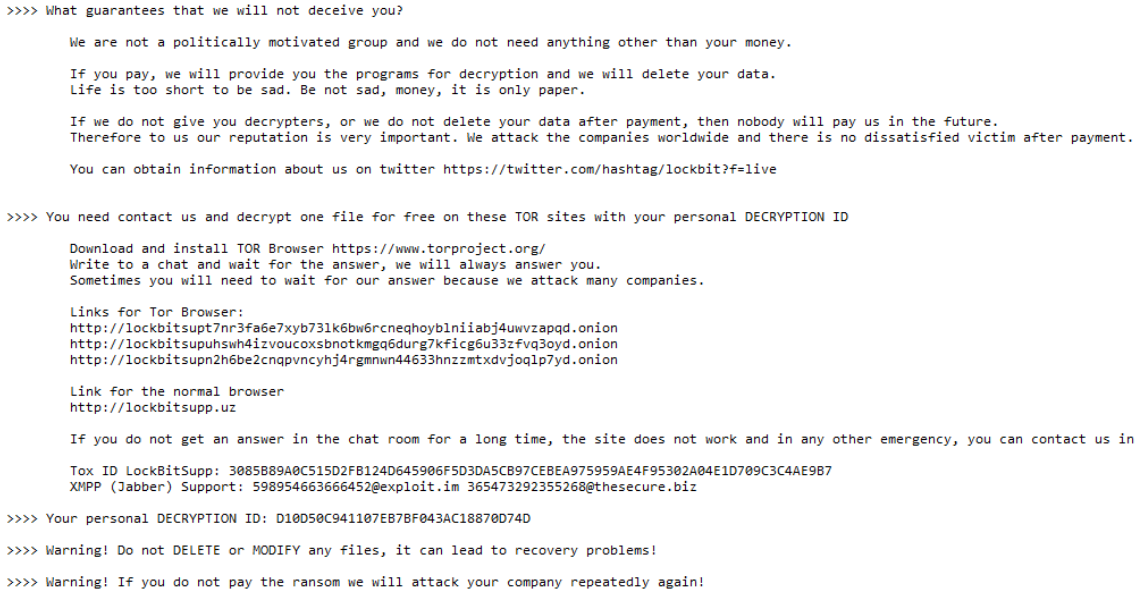


Figura 45: Nota rescate, URL

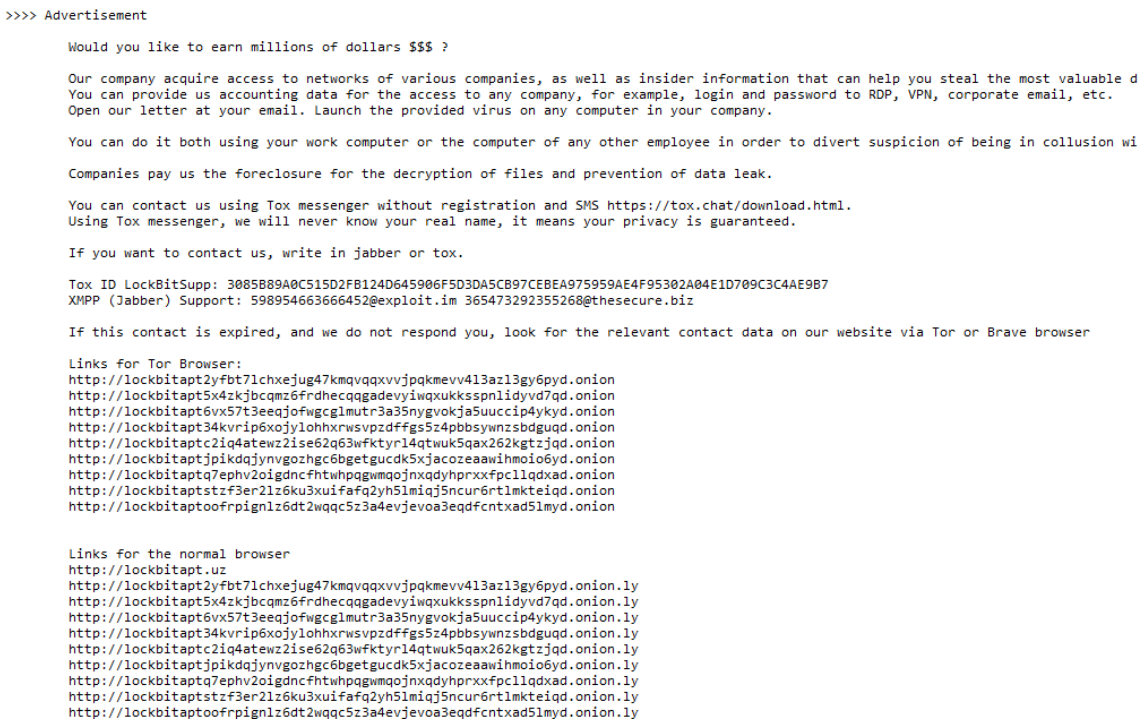
En la nota de mensaje se trata de disuadir a la víctima para que realice el pago y confié en que no a va ser engañado.



```
>>>> What guarantees that we will not deceive you?

        We are not a politically motivated group and we do not need anything other than your money.

        If you pay, we will provide you the programs for decryption and we will delete your data.
        Life is too short to be sad. Be not sad, money, it is only paper.

        If we do not give you decrypters, or we do not delete your data after payment, then nobody will pay us in the future.
        Therefore to us our reputation is very important. We attack the companies worldwide and there is no dissatisfied victim after payment.

        You can obtain information about us on twitter https://twitter.com/hashtag/lockbit?f=live


>>>> You need contact us and decrypt one file for free on these TOR sites with your personal DECRYPTION ID

        Download and install TOR Browser https://www.torproject.org/
        Write to a chat and wait for the answer, we will always answer you.
        Sometimes you will need to wait for our answer because we attack many companies.

        Links for Tor Browser:
        http://lockbitsupt7nr3fa6e7xyb73lk6bw6rcneqhoyblniiabj4uwvzapqd.onion
        http://lockbitsupuhswh4izvoucoxsbnotkmgq6durg7kficg6u33zfvq3oyd.onion
        http://lockbitsupn2h6be2cnqpvncyhj4rgmnwn44633hnzzmtxdvjoqlp7yd.onion

        Link for the normal browser
        http://lockbitsupp.uz

        If you do not get an answer in the chat room for a long time, the site does not work and in any other emergency, you can contact us in

        Tox ID LockBitSupp: 3085B89A0C515D2FB124D645906F5D3DA5CB97CEBEA975959AE4F95302A04E1D709C3C4AE9B7
        XMPP (Jabber) Support: 598954663666452@exploit.im 365473292355268@thesecure.biz

>>>> Your personal DECRYPTION ID: D10D50C941107EB7BF043AC18870D74D

>>>> Warning! Do not DELETE or MODIFY any files, it can lead to recovery problems!

>>>> Warning! If you do not pay the ransom we will attack your company repeatedly again!
```

Figura 46: Nota rescate, disuadir víctima

También exponen la idea de que se puede ganar dinero al compartir datos o cuentas de acceso RDP o VPN.



```
>>>> Advertisement

        Would you like to earn millions of dollars $$$ ?

        Our company acquire access to networks of various companies, as well as insider information that can help you steal the most valuable d
        You can provide us accounting data for the access to any company, for example, login and password to RDP, VPN, corporate email, etc.
        Open our letter at your email. Launch the provided virus on any computer in your company.

        You can do it both using your work computer or the computer of any other employee in order to divert suspicion of being in collusion wi

        Companies pay us the foreclosure for the decryption of files and prevention of data leak.

        You can contact us using Tox messenger without registration and SMS https://tox.chat/download.html.
        Using Tox messenger, we will never know your real name, it means your privacy is guaranteed.

        If you want to contact us, write in jabber or tox.

        Tox ID LockBitSupp: 3085B89A0C515D2FB124D645906F5D3DA5CB97CEBEA975959AE4F95302A04E1D709C3C4AE9B7
        XMPP (Jabber) Support: 598954663666452@exploit.im 365473292355268@thesecure.biz

        If this contact is expired, and we do not respond you, look for the relevant contact data on our website via Tor or Brave browser

        Links for Tor Browser:
        http://lockbitapt2yfbt71chxejug47kmqvqqxvvjpqkmevv4l3az13gy6pyd.onion
        http://lockbitapt5x4zkjbcqmz6frdhecqqgadevyiwqxukksspnlidyvd7qd.onion
        http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion
        http://lockbitapt34kvrip6xojylohhxrwsvpzdffgs5z4pbbsywnzsbdguqd.onion
        http://lockbitaptc2iq4atewz2ise62q63wfktyrl4qtwuk5qax262kgtzjqd.onion
        http://lockbitaptjpikdqjynvgozhgc6bgetgucdk5xjacozeaawihmoio6yd.onion
        http://lockbitaptq7ephv2oigdncfhtwhpqgwmqojnxqdyhprxxfpcllqdxad.onion
        http://lockbitaptstzf3er2lz6ku3xuifafq2yh5lmiqj5ncur6rtlmkteiqd.onion
        http://lockbitaptoofrpignlz6dt2wqqc5z3a4evjevoa3eqdfcntxad5lmyd.onion


        Links for the normal browser
        http://lockbitapt.uz
        http://lockbitapt2yfbt71chxejug47kmqvqqxvvjpqkmevv4l3az13gy6pyd.onion.ly
        http://lockbitapt5x4zkjbcqmz6frdhecqqgadevyiwqxukksspnlidyvd7qd.onion.ly
        http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion.ly
        http://lockbitapt34kvrip6xojylohhxrwsvpzdffgs5z4pbbsywnzsbdguqd.onion.ly
        http://lockbitaptc2iq4atewz2ise62q63wfktyrl4qtwuk5qax262kgtzjqd.onion.ly
        http://lockbitaptjpikdqjynvgozhgc6bgetgucdk5xjacozeaawihmoio6yd.onion.ly
        http://lockbitaptq7ephv2oigdncfhtwhpqgwmqojnxqdyhprxxfpcllqdxad.onion.ly
        http://lockbitaptstzf3er2lz6ku3xuifafq2yh5lmiqj5ncur6rtlmkteiqd.onion.ly
        http://lockbitaptoofrpignlz6dt2wqqc5z3a4evjevoa3eqdfcntxad5lmyd.onion.ly
```

Figura 47: Nota rescate, invitación a participar de actividad delictiva

3.3.1 Análisis Registro de Windows

Con la herramienta Regshot se tomo captura de la configuración del registro de Windows antes y despues del ataque, luego de la comparación se observa que se eliminaron 1059 claves, entre ellas configuraciones de eventlog con el ánimo de ocultar las acciones realizadas, claves de seguridad y auditoría.

```
Regshot 1.9.0 x64 ANSI
Comentarios:
Fecha y hora:2023/5/2 20:03:55  ,  2023/5/2 20:34:58
Computador:DESKTOP-08UBLH4 , DESKTOP-08UBLH4
Usuario:TFM_Win10 , TFM_Win10

----------------------------------
Claves borradas:1059
----------------------------------
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\NetworkServiceTriggers\Triggers\bc90d167-9470-4139-a9ba-be0bbbf5b74d\9435cc56-
HKLM\SYSTEM\ControlSet001\Services\CDPUserSvc_3a490
HKLM\SYSTEM\ControlSet001\Services\CDPUserSvc_3a490\Security
HKLM\SYSTEM\ControlSet001\Services\EventLog
HKLM\SYSTEM\ControlSet001\Services\EventLog\Application
HKLM\SYSTEM\ControlSet001\Services\EventLog\Application\.NET Runtime
HKLM\SYSTEM\ControlSet001\Services\EventLog\Application\.NET Runtime Optimization Service
HKLM\SYSTEM\ControlSet001\Services\EventLog\Application\Application
HKLM\SYSTEM\ControlSet001\Services\EventLog\Application\Application Error
HKLM\SYSTEM\ControlSet001\Services\EventLog\Application\Application Hang
HKLM\SYSTEM\ControlSet001\Services\EventLog\Application\Application Management
HKLM\SYSTEM\ControlSet001\Services\EventLog\Application\Application-Addon-Event-Provider
HKLM\SYSTEM\ControlSet001\Services\EventLog\Application\AutoEnrollment
HKLM\SYSTEM\ControlSet001\Services\EventLog\Application\CardSpace 4.0.0.0
HKLM\SYSTEM\ControlSet001\Services\EventLog\Application\CertCa
HKLM\SYSTEM\ControlSet001\Services\EventLog\Application\CertCli
HKLM\SYSTEM\ControlSet001\Services\EventLog\Application\CertEnroll
HKLM\SYSTEM\ControlSet001\Services\EventLog\Application\Chkdsk
HKLM\SYSTEM\ControlSet001\Services\EventLog\Application\COM
HKLM\SYSTEM\ControlSet001\Services\EventLog\Application\COM+
HKLM\SYSTEM\ControlSet001\Services\EventLog\Application\DeliveryOptimization
HKLM\SYSTEM\ControlSet001\Services\EventLog\Application\Desktop Window Manager
HKLM\SYSTEM\ControlSet001\Services\EventLog\Application\DiskQuota
```

Figura 48: Registro de Windows claves borradas

Se añadieron 105 claves en el registro de Windows, con lo cual realizacion asociaciones de sus procesos dentro de la estructura del sistema operativo, tambien puede contener información sobre las acciones o procesos a realizar. Se observa que crean llaves de registro para modificar los certificados de confianza los cuales se usan para verificar la autenticidad y generar confianza.

```
Claves añadidas:105
----------------------------------
HKLM\SOFTWARE\Classes\.VnJT3T87f
HKLM\SOFTWARE\Classes\VnJT3T87f
HKLM\SOFTWARE\Classes\VnJT3T87f\DefaultIcon
HKLM\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\F81F111D0E5AB58D396F7BF525577FD30FDC95AA
HKLM\SOFTWARE\Microsoft\SystemCertificates\TrustedPublisher\Certificates\F81F111D0E5AB58D396F7BF525577FD30FDC95AA
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Mrt\_Merged\Windows.UI.ShellCommon
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1312
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1628
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1884
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\3300
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\3388
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\4376
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\5252
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\6164
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\7532
HKLM\SOFTWARE\Policies\Microsoft\Windows\IPSec\Policy\Local
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\CurrentVersion
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\CurrentVersion\Software Protection Platform
HKLM\SOFTWARE\WOW6432Node\Microsoft\SystemCertificates\ROOT\Certificates\F81F111D0E5AB58D396F7BF525577FD30FDC95AA
HKLM\SOFTWARE\WOW6432Node\Microsoft\SystemCertificates\TrustedPublisher\Certificates\F81F111D0E5AB58D396F7BF525577FD30FDC95AA
HKLM\SOFTWARE\WOW6432Node\Policies\Microsoft\Windows\IPSec\Policy\Local
HKLM\SOFTWARE\WOW6432Node\Policies\Microsoft\Windows NT\CurrentVersion
HKLM\SOFTWARE\WOW6432Node\Policies\Microsoft\Windows NT\CurrentVersion\Software Protection Platform
HKLM\SYSTEM\ControlSet001\Control\Nsi\{eb004a00-9b1a-11d4-9123-0050047759bc}\16
HKLM\SYSTEM\WPA\8DEC0AF1-0341-4b93-85CD-72606C2DF94C-7P-22
HKLM\SYSTEM\WPA\8DEC0AF1-0341-4b93-85CD-72606C2DF94C-7P-23
HKLM\SYSTEM\WPA\8DEC0AF1-0341-4b93-85CD-72606C2DF94C-7P-24
HKLM\SYSTEM\CurrentControlSet\Control\Nsi\{eb004a00-9b1a-11d4-9123-0050047759bc}\16
```

Figura 49: Registro de Windows claves añadidas

También de identificó que se borraron 2461 valores en el registro de Windows, para eliminar restricciones y ganar privilegios.

```
----------------------------------
Valores borrados:2461
----------------------------------
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\VolatileNotifications\41C64E6DA3FBF855:  01 00 04 80 44 00 00 00 50 00 00 0
HKLM\SYSTEM\ControlSet001\Control\hivelist\\REGISTRY\WC\Silo1c869c66-c801-fc2f-29c3-d69571fe371bsoftware:  5C 44 65 76 69 63
HKLM\SYSTEM\ControlSet001\Control\hivelist\\REGISTRY\WC\Silo1c869c66-c801-fc2f-29c3-d69571fe371buser_sid:  5C 44 65 76 69 63
HKLM\SYSTEM\ControlSet001\Control\hivelist\\REGISTRY\WC\Silo1c869c66-c801-fc2f-29c3-d69571fe371buser_classes:  5C 44 65 76 69
HKLM\SYSTEM\ControlSet001\Control\hivelist\\REGISTRY\WC\Silo95d6c329-fe71-1b37-669c-861c01c82ffccom:  5C 44 65 76 69 63 65 5C
HKLM\SYSTEM\ControlSet001\Control\hivelist\\REGISTRY\WC\Silo1c869c66-c801-fc2f-29c3-d69571fe371bcom:  5C 44 65 76 69 63 65 5C
HKLM\SYSTEM\ControlSet001\Services\CDPUserSvc_3a490\Type: 0x000000E0
HKLM\SYSTEM\ControlSet001\Services\CDPUserSvc_3a490\Start: 0x00000002
HKLM\SYSTEM\ControlSet001\Services\CDPUserSvc_3a490\ErrorControl: 0x00000001
HKLM\SYSTEM\ControlSet001\Services\CDPUserSvc_3a490\ImagePath: "C:\Windows\system32\svchost.exe -k UnistackSvcGroup"
HKLM\SYSTEM\ControlSet001\Services\CDPUserSvc_3a490\DisplayName: "Servicio de usuario de plataforma de dispositivos conectado
HKLM\SYSTEM\ControlSet001\Services\CDPUserSvc_3a490\FailureActions:  80 51 01 00 00 00 00 00 00 00 00 03 00 00 00 14 00 00
HKLM\SYSTEM\ControlSet001\Services\CDPUserSvc_3a490\Description: "@%SystemRoot%\system32\cdpusersvc.dll,-101"
HKLM\SYSTEM\ControlSet001\Services\CDPUserSvc_3a490\Security\Security:  01 00 14 80 A0 00 00 00 AC 00 00 00 14 00 00 00 30 00
HKLM\SYSTEM\ControlSet001\Services\EventLog\Description: "@%SystemRoot%\system32\wevtsvc.dll,-201"
HKLM\SYSTEM\ControlSet001\Services\EventLog\DisplayName: "@%SystemRoot%\system32\wevtsvc.dll,-200"
HKLM\SYSTEM\ControlSet001\Services\EventLog\ErrorControl: 0x00000001
HKLM\SYSTEM\ControlSet001\Services\EventLog\FailureActions:  80 51 01 00 00 00 00 00 00 00 00 03 00 00 00 14 00 00 00 01 0
HKLM\SYSTEM\ControlSet001\Services\EventLog\FailureActionsOnNonCrashFailures: 0x00000001
HKLM\SYSTEM\ControlSet001\Services\EventLog\Group: "Event Log"
HKLM\SYSTEM\ControlSet001\Services\EventLog\ImagePath: "%SystemRoot%\System32\svchost.exe -k LocalServiceNetworkRestricted -p
HKLM\SYSTEM\ControlSet001\Services\EventLog\ObjectName: "NT AUTHORITY\LocalService"
HKLM\SYSTEM\ControlSet001\Services\EventLog\PlugPlayServiceType: 0x00000003
HKLM\SYSTEM\ControlSet001\Services\EventLog\RequiredPrivileges:  53 65 43 68 61 6E 67 65 4E 6F 74 69 66 79 50 72 69 76 69 6C
HKLM\SYSTEM\ControlSet001\Services\EventLog\ServiceSidType: 0x00000001
HKLM\SYSTEM\ControlSet001\Services\EventLog\Start: 0x00000002
HKLM\SYSTEM\ControlSet001\Services\EventLog\SvcMemHardLimitInMB: 0x00000014
HKLM\SYSTEM\ControlSet001\Services\EventLog\SvcMemMidLimitInMB: 0x0000000F
HKLM\SYSTEM\ControlSet001\Services\EventLog\SvcMemSoftLimitInMB: 0x0000000B
```

Figura 50: Registro de Windows valores borrados

Dentro de los valores borrados se encuentran configuraciones para Software Protection Platform Service.

```
HKLM\SYSTEM\ControlSet001\Services\EventLog\Application\Software Protection Platform Service\EventMessageFile: "%SystemRoot%\system32\
HKLM\SYSTEM\ControlSet001\Services\EventLog\Application\Software Protection Platform Service\ProviderGuid: "{E23B33B0-C8C9-472C-A5F9-F
HKLM\SYSTEM\ControlSet001\Services\EventLog\Application\Software Protection Platform Service\TypesSupported: 0x00000007
```

Figura 51: Registro de Windows valores de seguridad borrados

Se agregan registros de seguridad y demás valores para alterar completamente el funcionamiento del sistema operativo.

```
-----------------------------------
Valores añadidos:351
-----------------------------------
HKLM\HARDWARE\DEVICEMAP\PointerClass\\Device\PointerClass3: "\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\mouclass"
HKLM\SOFTWARE\Classes\.VnJT3T87f\: "VnJT3T87f"
HKLM\SOFTWARE\Classes\VnJT3T87f\DefaultIcon\: "C:\ProgramData\VnJT3T87f.ico"
HKLM\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\F81F111D0E5AB58D396F7BF525577FD30FDC95AA\Blob:  19 00 00 00 01 0
B1 C2 21 C3 67 97 70 C4 01 DE 98 69 5E 88 CA D6 21 B3 19 73 0D CA BE DF 4C 47 09 EE BE 81 26 DD 56 7A 9A B3 87 DA B7 EA 13 B3
HKLM\SOFTWARE\Microsoft\SystemCertificates\TrustedPublisher\Certificates\F81F111D0E5AB58D396F7BF525577FD30FDC95AA\Blob:  03 0
48 B0 39 8B E6 F9 D3 4F 84 C6 0E 69 4C 47 2C 72 F9 B7 02 03 01 00 01 A3 43 30 41 30 3F 06 03 55 1D 01 04 38 30 36 80 10 E4 E1
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Mrt\_Merged\Windows.UI.ShellCommon\: "C:\Windows\rescache\_merged\314483308\66
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1312\Terminator: "HAM"
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1312\Reason: 0x00000004
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1312\CreationTime:  42 68 DE 47 5A 80 D9 01
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1628\Terminator: "HAM"
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1628\Reason: 0x00000004
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1628\CreationTime:  85 AE 84 64 58 80 D9 01
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1884\Terminator: "HAM"
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1884\Reason: 0x00000004
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1884\CreationTime:  27 13 E4 93 59 80 D9 01
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\3300\Terminator: "HAM"
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\3300\Reason: 0x00000004
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\3300\CreationTime:  B4 6B 57 EB 58 80 D9 01
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\3388\Terminator: "HAM"
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\3388\Reason: 0x00000004
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\3388\CreationTime:  A2 24 2D AA 59 80 D9 01
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\4376\Terminator: "HAM"
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\4376\Reason: 0x00000004
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\4376\CreationTime:  5E F7 6F D6 56 80 D9 01
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\5252\Terminator: "HAM"
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\5252\Reason: 0x00000004
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\5252\CreationTime:  F7 20 C0 D5 56 80 D9 01
```

Figura 52: Registro de Windows valores añadidos

```
-----------------------------------
Valores modificados:1730
-----------------------------------
HKLM\SOFTWARE\Microsoft\IdentityCRL\ClockSkew: 0xFFFFE870
HKLM\SOFTWARE\Microsoft\IdentityCRL\ClockSkew: 0xFFFFDFBD
HKLM\SOFTWARE\Microsoft\IdentityCRL\ClockData\ClockTimeSeconds:  94 9C 56 64 00 00 00 00
HKLM\SOFTWARE\Microsoft\IdentityCRL\ClockData\ClockTimeSeconds:  A3 B9 56 64 00 00 00 00
HKLM\SOFTWARE\Microsoft\IdentityCRL\ClockData\TickCount:  F8 92 70 00 00 00 00 00
HKLM\SOFTWARE\Microsoft\IdentityCRL\ClockData\TickCount:  BA 37 E6 00 00 00 00 00
HKLM\SOFTWARE\Microsoft\Internet Explorer\Registration\ProductId: "00330-80000-00000-AA364"
HKLM\SOFTWARE\Microsoft\Internet Explorer\Registration\ProductId: "00331-10000-00001-AA198"
HKLM\SOFTWARE\Microsoft\Internet Explorer\Registration\DigitalProductId:  A4 00 00 00 03 00 00 00 30 30 33 33 30 2D 38 30 30
HKLM\SOFTWARE\Microsoft\Internet Explorer\Registration\DigitalProductId:  A4 00 00 00 03 00 00 00 30 30 33 33 31 2D 31 30 30
HKLM\SOFTWARE\Microsoft\Internet Explorer\Registration\DigitalProductId4:  F8 04 00 00 04 00 00 00 30 00 33 00 36 00 31 00 32
0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 52
HKLM\SOFTWARE\Microsoft\Internet Explorer\Registration\DigitalProductId4:  F8 04 00 00 04 00 00 00 30 00 33 00 36 00 31 00 32
0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 56
HKLM\SOFTWARE\Microsoft\Multimedia\Audio\Journal\Render:  53 00 57 00 44 00 5C 00 4D 00 4D 00 44 00 45 00 56 00 41 00 50 00 4
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
HKLM\SOFTWARE\Microsoft\Multimedia\Audio\Journal\Render:  53 00 57 00 44 00 5C 00 4D 00 4D 00 44 00 45 00 56 00 41 00 50 00 4
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
HKLM\SOFTWARE\Microsoft\Security Center\cval: 0x00000001
HKLM\SOFTWARE\Microsoft\Security Center\cval: 0x00000000
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Diagnostics\DiagTrack\LastFreeNetworkLossTime:  B7 91 E1 30 42 80 D9 01
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Diagnostics\DiagTrack\LastFreeNetworkLossTime:  0E CD E0 A9 56 80 D9 01
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Diagnostics\DiagTrack\LastConnectivityHeartBeatTime:  82 73 23 33 42 80 D9 01
```

Figura 53: Registro de Windows modificados

En total LockBit realiza 5706 cambio de configuración en el registro de Windows.

```
HKU\S-1-5-18\Software\Microsoft\IdentityCRL\Immersive\production\Token\{2B379600-B42B-4FE9-A59C-A312FB934935}\DeviceTicket:
 55 40 83 9E 66 74 2D 61 4D A9 53 89 53 8B B2 5E 4D 3C BB 61 7C BB 8A F7 9E 27 51 E2 66 44 00 34 36 D7 CC CE F6 83 6D EB F2 9
EC 06 A7 60 56 B2 03 2C 39 B3 DA AF 57 36 93 C8 90 9C 19 1B 1D EE 03 3A 83 49 CD 91 5C 6F 7D 77 56 46 D3 FB F7 AB EE 30 0A 1E
2 9F A8 6E 68 7D 9A DB CF 4F E6 6D 4E E4 F0 34 C1 64 27 FD 1C 30 3A C1 1C A4 53 32 9C 77 B8 CE 36 1E 16 03 B8 7E 87 00 17 49
 A9 26 9B 8D 56 A6 E8 0A 2B 20 C6 E6 A4 E7 BB 11 C3 6D 36 BB 1E ED 1E 7E 50 A1 F9 0D 8D 0C 0F 0E A5 4B E1 56 1E 79 86 0C 90 5
B6 9A EA 6E DE 5E 76 0C 84 0E 7F 40 7B D1 14 8B B8 79 13 43 2B 2C B2 2D BE 6B 26 73 BF D5 BB E0 F0 40 9C F8 0E B1 1E DC E3 8D
B 7E 2D F2 B0 3B 06 06 3D 2F 4F 5E 59 F4 DA A3 34 86 D6 9C 23 69 0B 2D CB A0 06 AF 9F 21 FF 63 8D 67 80 91 D9 6F 81 60 CE C4

-----------------------------------
Total de cambios:5706
-----------------------------------
```

Figura 54: Registro de Windows total ajustes realizados por LB3.exe

Esto nos demuestra que LockBit aparte de cifrar los archivos, ataca el registro de Windows por las siguientes razones:

- Ganar persistencia y asegurar que el Ransomware mantiene el control de la máquina aun si se reinicia.

- Ocultarse de los sistemas de seguridad y otras herramientas que monitorean el sistema.

- Bloquear y alterar sistemas de seguridad como el Centro de Seguridad de Windows, Windows Defender, así como el bloqueo de sistemas de copias de seguridad y respaldo. Una de las modificaciones en la máquina es deshabilitar AMSI (Antimalware Scan Interface), se genera error al intentar abrir el antivirus de la máquina y desde Powershell la herramienta AMSIUtils no se encuentra disponible.

```
PS C:\Windows\system32> amsiultils
amsiultils : El término 'amsiultils' no se reconoce como nombre de un cmdlet, función, archivo de script o programa
ejecutable. Compruebe si escribió correctamente el nombre o, si incluyó una ruta de acceso, compruebe que dicha ruta
es correcta e inténtelo de nuevo.
En línea: 1 Carácter: 1
+ amsiultils
+ ~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (amsiultils:String) [], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException
```

Figura 55: AMSI deshabilitado

3.3.2 Escaneo ARP

Este Ransomware antes de encriptar los archivos de la víctima evalúa el entorno de red donde es ejecutado, se identificó múltiples validaciones a la red interna 192.168.1.0/24 mediante el protocolo ARP, esto es con el fin de validar que equipos hay activos en la red y proceder a su listado para próximas afectaciones.

arp

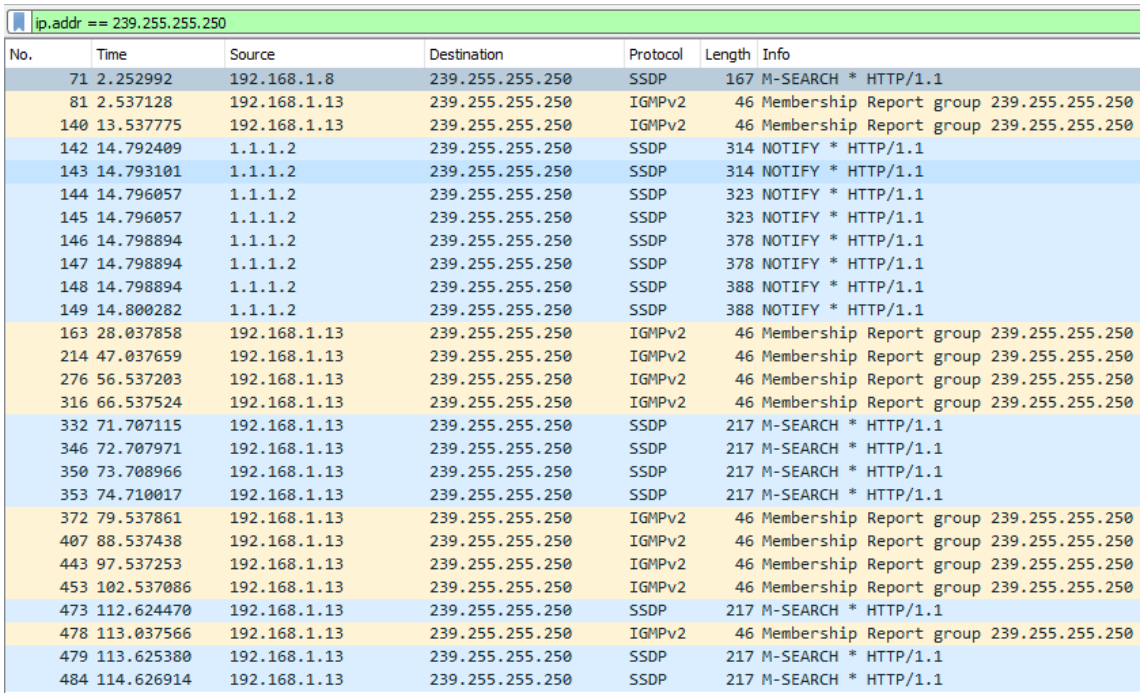
No.	Time	Source	Destination	Protocol	Length	Info
29	6.999006	MitraSta_f9:f6:e0	Broadcast	ARP	60	Who has 192.168.1.7? Tell 192.168.1.1
30	7.654153	MitraSta_f9:f6:e0	Broadcast	ARP	60	Who has 192.168.1.13? Tell 192.168.1.1
34	7.987893	MitraSta_f9:f6:e0	Broadcast	ARP	60	Who has 192.168.1.7? Tell 192.168.1.1
44	8.49574	MitraSta_f9:f6:e0	Broadcast	ARP	60	Who has 192.168.1.23? Tell 192.168.1.1

Figura 56: Escaneo ARP

3.3.3 Análisis de conexiones de red

Desde el equipo anfitrión y mediante la herramienta Wireshark se detectaron conexiones hacia IP catalogadas como maliciosas.

IP 239.255.255.250

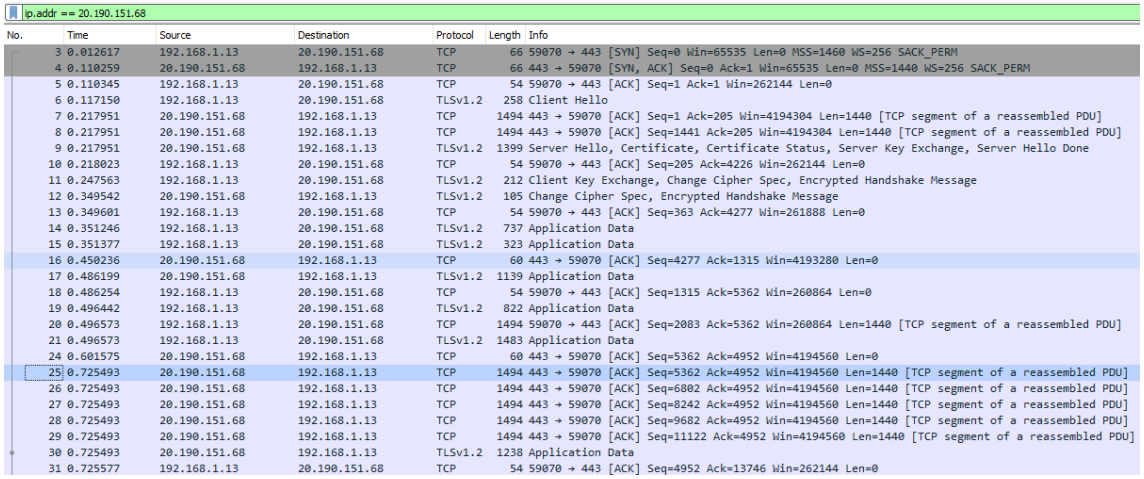


ip.addr == 239.255.255.250

No.	Time	Source	Destination	Protocol	Length	Info
71	2.252992	192.168.1.8	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
81	2.537128	192.168.1.13	239.255.255.250	IGMPv2	46	Membership Report group 239.255.255.250
140	13.537775	192.168.1.13	239.255.255.250	IGMPv2	46	Membership Report group 239.255.255.250
142	14.792409	1.1.1.2	239.255.255.250	SSDP	314	NOTIFY * HTTP/1.1
143	14.793101	1.1.1.2	239.255.255.250	SSDP	314	NOTIFY * HTTP/1.1
144	14.796057	1.1.1.2	239.255.255.250	SSDP	323	NOTIFY * HTTP/1.1
145	14.796057	1.1.1.2	239.255.255.250	SSDP	323	NOTIFY * HTTP/1.1
146	14.798894	1.1.1.2	239.255.255.250	SSDP	378	NOTIFY * HTTP/1.1
147	14.798894	1.1.1.2	239.255.255.250	SSDP	378	NOTIFY * HTTP/1.1
148	14.798894	1.1.1.2	239.255.255.250	SSDP	388	NOTIFY * HTTP/1.1
149	14.800282	1.1.1.2	239.255.255.250	SSDP	388	NOTIFY * HTTP/1.1
163	28.037858	192.168.1.13	239.255.255.250	IGMPv2	46	Membership Report group 239.255.255.250
214	47.037659	192.168.1.13	239.255.255.250	IGMPv2	46	Membership Report group 239.255.255.250
276	56.537203	192.168.1.13	239.255.255.250	IGMPv2	46	Membership Report group 239.255.255.250
316	66.537524	192.168.1.13	239.255.255.250	IGMPv2	46	Membership Report group 239.255.255.250
332	71.707115	192.168.1.13	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
346	72.707971	192.168.1.13	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
350	73.708966	192.168.1.13	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
353	74.710017	192.168.1.13	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
372	79.537861	192.168.1.13	239.255.255.250	IGMPv2	46	Membership Report group 239.255.255.250
407	88.537438	192.168.1.13	239.255.255.250	IGMPv2	46	Membership Report group 239.255.255.250
443	97.537253	192.168.1.13	239.255.255.250	IGMPv2	46	Membership Report group 239.255.255.250
453	102.537086	192.168.1.13	239.255.255.250	IGMPv2	46	Membership Report group 239.255.255.250
473	112.624470	192.168.1.13	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
478	113.037566	192.168.1.13	239.255.255.250	IGMPv2	46	Membership Report group 239.255.255.250
479	113.625380	192.168.1.13	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
484	114.626914	192.168.1.13	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1

Figura 57: Análisis conexiones de red 1

IP 20.190.151.68



ip.addr == 20.190.151.68

No.	Time	Source	Destination	Protocol	Length	Info
3	0.012617	192.168.1.13	20.190.151.68	TCP	66	59070 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
4	0.110259	20.190.151.68	192.168.1.13	TCP	66	443 → 59070 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
5	0.110345	192.168.1.13	20.190.151.68	TCP	54	59070 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
6	0.117150	192.168.1.13	20.190.151.68	TLSv1.2	258	Client Hello
7	0.217951	20.190.151.68	192.168.1.13	TCP	1494	443 → 59070 [ACK] Seq=1 Ack=205 Win=4194304 Len=1440 [TCP segment of a reassembled PDU]
8	0.217951	20.190.151.68	192.168.1.13	TCP	1494	443 → 59070 [ACK] Seq=1441 Ack=205 Win=4194304 Len=1440 [TCP segment of a reassembled PDU]
9	0.217951	20.190.151.68	192.168.1.13	TLSv1.2	1399	Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
10	0.218023	192.168.1.13	20.190.151.68	TCP	54	59070 → 443 [ACK] Seq=205 Ack=4226 Win=262144 Len=0
11	0.247563	192.168.1.13	20.190.151.68	TLSv1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
12	0.349542	20.190.151.68	192.168.1.13	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
13	0.349601	192.168.1.13	20.190.151.68	TCP	54	59070 → 443 [ACK] Seq=363 Ack=4277 Win=261888 Len=0
14	0.351246	192.168.1.13	20.190.151.68	TLSv1.2	737	Application Data
15	0.351377	192.168.1.13	20.190.151.68	TLSv1.2	323	Application Data
16	0.450236	20.190.151.68	192.168.1.13	TCP	60	443 → 59070 [ACK] Seq=4277 Ack=1315 Win=4193280 Len=0
17	0.486199	20.190.151.68	192.168.1.13	TLSv1.2	1139	Application Data
18	0.486254	192.168.1.13	20.190.151.68	TCP	54	59070 → 443 [ACK] Seq=1315 Ack=5362 Win=260864 Len=0
19	0.496442	192.168.1.13	20.190.151.68	TLSv1.2	822	Application Data
20	0.496573	192.168.1.13	20.190.151.68	TCP	1494	59070 → 443 [ACK] Seq=2083 Ack=5362 Win=260864 Len=1440 [TCP segment of a reassembled PDU]
21	0.496573	192.168.1.13	20.190.151.68	TLSv1.2	1483	Application Data
24	0.601575	20.190.151.68	192.168.1.13	TCP	60	443 → 59070 [ACK] Seq=5362 Ack=4952 Win=4194560 Len=0
25	0.725493	20.190.151.68	192.168.1.13	TCP	1494	443 → 59070 [ACK] Seq=5362 Ack=4952 Win=4194560 Len=1440 [TCP segment of a reassembled PDU]
26	0.725493	20.190.151.68	192.168.1.13	TCP	1494	443 → 59070 [ACK] Seq=6802 Ack=4952 Win=4194560 Len=1440 [TCP segment of a reassembled PDU]
27	0.725493	20.190.151.68	192.168.1.13	TCP	1494	443 → 59070 [ACK] Seq=8242 Ack=4952 Win=4194560 Len=1440 [TCP segment of a reassembled PDU]
28	0.725493	20.190.151.68	192.168.1.13	TCP	1494	443 → 59070 [ACK] Seq=9682 Ack=4952 Win=4194560 Len=1440 [TCP segment of a reassembled PDU]
29	0.725493	20.190.151.68	192.168.1.13	TCP	1494	443 → 59070 [ACK] Seq=11122 Ack=4952 Win=4194560 Len=1440 [TCP segment of a reassembled PDU]
30	0.725493	20.190.151.68	192.168.1.13	TLSv1.2	1238	Application Data
31	0.725577	192.168.1.13	20.190.151.68	TCP	54	59070 → 443 [ACK] Seq=4952 Ack=13746 Win=262144 Len=0

Figura 58: Análisis conexiones de red 2

IP 204.79.197.200

ip.addr == 204.79.197.200

No.	Time	Source	Destination	Protocol	Length	Info
233	55.927953	192.168.1.13	204.79.197.200	TCP	66	59077 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
242	55.957278	204.79.197.200	192.168.1.13	TCP	66	443 → 59077 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
243	55.957351	192.168.1.13	204.79.197.200	TCP	54	59077 → 443 [ACK] Seq=1 Ack=1 Win=132352 Len=0
245	55.964965	192.168.1.13	204.79.197.200	TLSv1.2	251	Client Hello
246	55.992882	204.79.197.200	192.168.1.13	TCP	60	443 → 59077 [ACK] Seq=1 Ack=198 Win=4194304 Len=0
247	55.994523	204.79.197.200	192.168.1.13	TCP	1494	443 → 59077 [ACK] Seq=1 Ack=198 Win=4194304 Len=1440 [TCP segment of a reassembled PDU]
248	55.994523	204.79.197.200	192.168.1.13	TCP	1494	443 → 59077 [ACK] Seq=1441 Ack=198 Win=4194304 Len=1440 [TCP segment of a reassembled PDU]
249	55.994523	204.79.197.200	192.168.1.13	TCP	1494	443 → 59077 [ACK] Seq=2881 Ack=198 Win=4194304 Len=1440 [TCP segment of a reassembled PDU]
250	55.994523	204.79.197.200	192.168.1.13	TCP	1494	443 → 59077 [ACK] Seq=4321 Ack=198 Win=4194304 Len=1440 [TCP segment of a reassembled PDU]
251	55.994523	204.79.197.200	192.168.1.13	TLSv1.2	1330	Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
252	55.994597	192.168.1.13	204.79.197.200	TCP	54	59077 → 443 [ACK] Seq=198 Ack=7037 Win=132352 Len=0
262	56.283363	192.168.1.13	204.79.197.200	TLSv1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
263	56.283803	192.168.1.13	204.79.197.200	TLSv1.2	141	Application Data
266	56.309828	204.79.197.200	192.168.1.13	TCP	60	443 → 59077 [ACK] Seq=7037 Ack=356 Win=4194304 Len=0
267	56.309828	204.79.197.200	192.168.1.13	TCP	60	443 → 59077 [ACK] Seq=7037 Ack=443 Win=4194048 Len=0
268	56.309828	204.79.197.200	192.168.1.13	TLSv1.2	396	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
269	56.309828	204.79.197.200	192.168.1.13	TLSv1.2	123	Application Data
270	56.309904	192.168.1.13	204.79.197.200	TCP	54	59077 → 443 [ACK] Seq=443 Ack=7448 Win=131840 Len=0
271	56.312824	192.168.1.13	204.79.197.200	TLSv1.2	92	Application Data
272	56.336204	204.79.197.200	192.168.1.13	TLSv1.2	92	Application Data
273	56.338603	204.79.197.200	192.168.1.13	TCP	60	443 → 59077 [ACK] Seq=7486 Ack=481 Win=4194048 Len=0
274	56.376386	192.168.1.13	204.79.197.200	TCP	54	59077 → 443 [ACK] Seq=481 Ack=7486 Win=131840 Len=0
277	58.914203	192.168.1.13	204.79.197.200	TLSv1.2	725	Application Data
278	59.045683	204.79.197.200	192.168.1.13	TCP	60	443 → 59077 [ACK] Seq=7486 Ack=1152 Win=4193536 Len=0
279	59.045683	204.79.197.200	192.168.1.13	TCP	1494	443 → 59077 [ACK] Seq=7486 Ack=1152 Win=4193536 Len=1440 [TCP segment of a reassembled PDU]
280	59.045683	204.79.197.200	192.168.1.13	TLSv1.2	1130	Application Data
281	59.045683	204.79.197.200	192.168.1.13	TLSv1.2	92	Application Data
282	59.045741	192.168.1.13	204.79.197.200	TCP	54	59077 → 443 [ACK] Seq=1152 Ack=10040 Win=132352 Len=0

Figura 59: Análisis conexiones de red 3

Estas IP se revisaron en la herramienta VirusTotal y se encuentran reportadas como maliciosas.

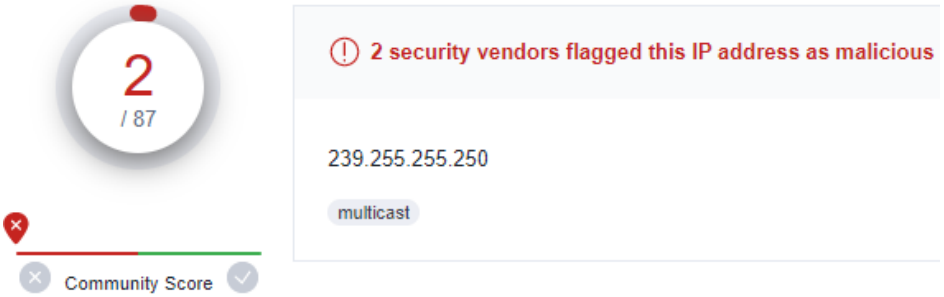


Figura 60: IP maliciosa 239.255.255.250

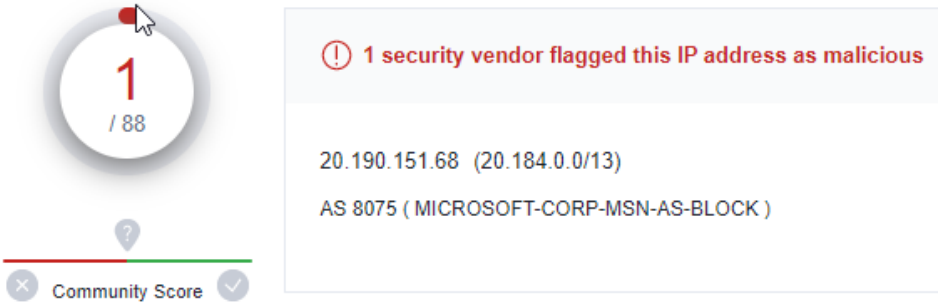


Figura 61: IP maliciosa 20.190.151.68

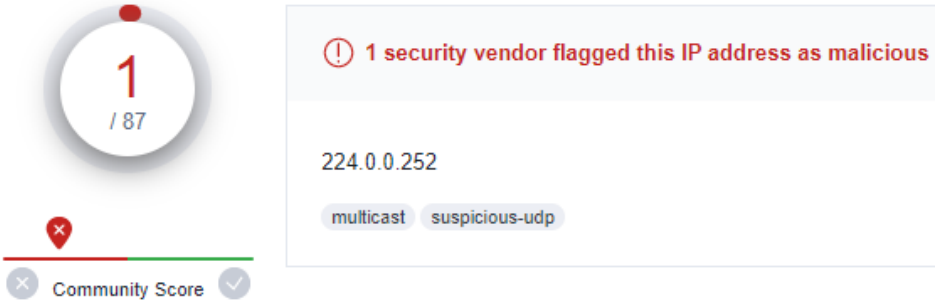


Figura 62: IP maliciosa 224.0.0.252

Es importante realizar un control y seguimiento de todos estos indicadores de compromiso, son múltiples las IP, dominios y hash que deben bloquearse y actualizarse contantemente en los sistemas de seguridad de las empresas.

3.4 Resultados

El esquema de afectación de LockBit se basa en un modelo RaaS, por esta razón muchas de sus fases dependen de sus afiliados y vectores de acceso a las redes corporativas. En el siguiente mapa desglosa el modelo de operación de este Ransomware:

Figura 63: Esquema de afectación LockBit

De acuerdo al modelo Cyber Kill Chain podemos hablar de las etapas con que los ciberdelincuentes llevan a cabo sus ataques:

Reconocimiento: El adversario o comunidad de afiliados recopilan información de su objetivo, para el modelo RaaS se tienen mercados con información de usuarios o cuentas de acceso, así como mecanismos de entrada o vulnerabilidades conocidas que se venden al mejor postor.

Preparación e intrusión: El modelo de Ransomware LockBit permite configurar algunos parámetros para el ataque, en este punto el adversario puede tener un primer acercamiento con la empresa mediante Phishing o verificar los accesos comprados.

Expansión: Una vez el adversario logra entrar a la red corporativa, busca ampliar sus privilegios y alcance, como se ha descrito una de las formas es escanear la red y

hacerse con el control de otras máquinas o directorio activo, el objetivo de este paso es moverse lateralmente y aumentar la superficie de ataque.

Explotación: En este punto se aprovechan los accesos y vulnerabilidades del sistema para y realizar la ejecución remota del código, desplegar el ataque. Se intentará escalar privilegios, de acuerdo a lo observado en el análisis dinámico se realizan configuraciones sobre la máquina y cifran los datos.

Persistencia: El atacante intentara deshabilitar sistemas de seguridad de los equipos o redes afectadas. Como por ejemplo deshabilitar y eliminar servicios de Windows como el antivirus o el centro de seguridad, modificar configuraciones de registro y demás configuraciones de seguridad que limiten su funcionamiento, todas estas configuraciones pensadas para persistir luego del reinicio de la máquina.

Exfiltración: Para las campañas de Ransomware este punto es donde culmina su ataque, se extraen los datos y se almacenan en sus servidores de comando y control para llevar a cabo una doble extorsión primero exigir el pago para desencriptar la información y segundo amenazar a la víctima en publicar la información en caso de no recibir el pago.

Con la herramienta JoeSandbox y la información del fichero ejecutable como el hash md5 9b9d47110c131ee17bf08df6b3787f43 a continuación se tiene una caracterización de las funcionalidades asociadas a LockBit. Como se observa la tendencia de esta amenaza está asociada a espiar, evadir y el secuestro de la información.

Figura 64: Caracterización LockBit por JoeSandbox, fuente [35]

3.4.1 Análisis MITRE ATT&CK

Como parte de los resultados y mediante las tácticas descritas para Windows en MITRE ATT&CK se conformó la siguiente matriz que puede dar una aproximación acerca del modo de operación de LockBit.

TA0001: Initial Access	TA0002: Execution	TA0003: Persistence	TA0004: Privilege Escalation	TA0005: Defense Evasion	TA0006: Credential Access	TA0007: Discovery	TA0008: Lateral Movement	TA0009: Collection	TA0011: Command and Control	TA0010: Exfiltration	TA0040: Impact
T1566: Phishing	T1053: Scheduled Task/Job	T1037: Boot or Logon Initialization Scripts	T1055: Process Injection	T1036: Masquerading	T1003: OS Credential Dumping	T1083: File and Directory Discovery	T1021: Remote Services	T1560: Archive Collected Data	T1105: Ingress Tool Transfer	T1020: Automated Exfiltration	T1485: Data Destruction
T1078: Valid Accounts	T1047: Windows Management Instrumentation		T1543: Create or Modify System Process	T1055: Process Injection		T1057: Process Discovery		T1005: Data from Local System		T1011: Exfiltration Over Other Network Medium	T1486: Data Encrypted for Impact
			T1548: Abuse Elevation Control Mechanism	T1070: Indicator Removal		T1082: System Information Discovery		T1039: Data from Network Shared Drive		T1029: Scheduled Transfer	T1489: Service Stop
				T1027: Obfuscated Files or Information				T1119: Automated Collection			T1490: Inhibit System Recovery
				T1218: System Binary Proxy Execution							

Figura 65: Matriz Mitre Att&ck

El acceso inicial puede darse a través de Phishing donde se entregue la carga útil, o tener el acceso inicial como cuentas de usuario privilegiadas compradas o compartidas por los afiliados.

La ejecución puede ser programada o recurrente esto para pasar desapercibidos o evadir sistemas de seguridad, también pueden usar procesos o mecanismos de Windows para ejecutar código malicioso.

Para ganar persistencia este malware modifica archivos de registro de sistema operativo, con el fin de mantener el control de la máquina inclusos entre reinicios.

En cuanto a la escalada de privilegios LockBit puede hacer uso de librerías y procesos legítimos de Windows, de esta manera evadir defensas y tener acceso a la memoria, recursos de red y datos de la máquina afectada. También puede crear y ejecutar procesos como por ejemplo LB3.exe el cual de encarga de realizar configuraciones sobre la máquina y realizar el proceso de cifrado de los datos.

Este tipo de malware puede evadir las defensas de su víctima como por ejemplo enmascarando o cambiando nombres de archivos o presentación de sus ejecutables, usar librerías y funciones legitimas para desplegar su ataque. También vimos que es

capaz de eliminar configuraciones de registros de eventos para dificultar su observación y seguimiento.

Una de las características principales del Ransomware LockBit es la capacidad de descubrir la información de la víctima, mediante el uso de procesos legítimos de Windows buscar en ubicaciones específicas del disco o carpetas de red, seleccionar de manera rápida los archivos a cifrar y realizar el proceso evadiendo los sistemas de defensa.

Movimiento lateral como se ha visto este malware siempre busca descubrir los equipos en la red, usar los accesos o cuentas privilegiadas para aumentar sus objetivos, incluso propagándose por entornos empresariales a través del directorio activo y políticas de grupo.

La recopilación de información se da principalmente de los archivos y datos del usuario, sus carpetas personales y locales, así como las carpetas compartidas en red, realizando el cifrado y comprimiendo la información a extraer.

El comando y control de estas campañas de Ransomware suelen hacer uso de infraestructura en nube o compartida a través de redes TOR, para transferir cargas hacia los equipos comprometidos y realizar nuevos ataques.

Estos mismos sistemas puede usarse para desplegar sus páginas web donde publican listados de sus víctimas y cuando no se recibe el pago exponen la información.

En cuanto al impacto de este tipo de malware va directamente contra la información o datos de las compañías, cifrar la información puede ser vista como destruirla pues así se realice el pago se genera afectación en la integridad de los datos, dependiendo del tipo de información pueden detenerse por completo los servicios que presta una compañía.

4. Recomendaciones

Para prevenir ataques de Ransomware son múltiples las recomendaciones que a nivel de entidades y expertos en seguridad se promueven para luchar contra este problema social. En este TFM se definen algunas sugerencias desde un punto de vista empresarial y se dividen en grupos.

Recomendaciones respecto a los usuarios, políticas y controles:

- Revisar y actualizar las cuentas de usuario actuales y eliminar las cuentas de funcionarios retirados, con el fin de evitar compromisos con cuentas antiguas y/o no utilizadas.

- Tener una política de contraseñas fuertes, con extensión mínima y complejidad.

- Implementar sistemas de segundo factor de autenticación, para conexiones remotas, servicios de nube y administración de infraestructura.

- Llevar y gestionar matrices de usuarios y permisos, publicar esta información entre los responsables de la información y área de auditoría.

- Otorgar permisos con el mínimo privilegio de acceso, permisos adicionales deben ser autorizados por los responsables de la información.

- En cuanto a los recursos de red y carpetas compartidas otorgar permisos de lectura, y de escritura con la debida aprobación de los responsables de la información.

- Restringir permisos de instalación de aplicaciones en los equipos.

- Limitar el uso de Terminal de Windows y PowerShell.

- Restringir que los usuarios puedan deshabilitar sistemas de seguridad como antivirus y EDR.

- Solo el personal de soporte podrá usar el usuario “Administrador” en las máquinas y en casos absolutamente necesarios.

Recomendaciones en la gestión de infraestructura, vulnerabilidades e incidentes:

- Tener un plan de auditoria con revisiones periódicas de los controles y procesos de la compañía, en especial con aquellos que manejen información sensible o de Core del negocio.

- Realizar escaneos periódicos de vulnerabilidades sobre la infraestructura.

- Una vez al año realizar pruebas de penetración preferiblemente con empresas externas y dedicadas a esta función.

- Realizar planes para remediación de vulnerabilidades en especial sobre la infraestructura critica de la compañía.

- Mantener actualizadas las aplicaciones y servicios de la compañía, como el antivirus y sistemas operativos.

- Usar sistemas EDR para análisis inteligente y detección de amenazas.

- Conformar o afiliarse a un CSIRT que ayude en la gestión de vulnerabilidades e incidentes, involucrarse y participar activamente en estos grupos especializados ayuda a mejorar la seguridad de la compañía.

- Bloquear indicadores de compromiso en sistemas como firewall, antivirus, antispam.

- Bloquear la ejecución de archivos .exe y demás extensiones.

- Deshabilitar las versiones antiguas del protocolo SMB.

- Usar sistemas de cifrado en las comunicaciones, como VPN para los accesos RDP y SMB.

- Segmentar la red LAN de la compañía, por ejemplo, tener una VLAN dedicada para cada área de la empresa, compras, tecnología, recursos humanos, etc. Esto limita la superficie de ataque del Ransomware.

- Tener una política de respaldos de información y copias de seguridad, que permitan restaurar a información en caso de un ataque.

- Contar con equipo de respuesta a crisis e incidentes CSIRT, que controlen y gestionen los sistemas de detección, ayuden en la respuesta y recuperación, promuevan una cultura de seguridad en la organización.

- Contar con un plan de plan de recuperación de desastres (DRP) y continuidad del negocio, medir la eficacia de estos planes con simulaciones al menos una vez a año.

- Usar mecanismos de encriptación de la información en nube tanto on- premises, ayuda a mantener la privacidad de los datos incluso si somo víctimas de un malware que exfiltre la información de la compañía.

Recomendaciones para la comunidad empresarial, usuarios, empleados, clientes:

- Realizar capacitaciones para socializar y sensibilizar la importancia de la seguridad en entornos empresariales.

- Educar al personal sobre cómo proteger la información empresarial y personal, explicar los conceptos de información confidencial, restringida y publica.

- Capacitaciones sobre phishing, no hacer clic en enlaces sospechosos o enviar información confidencial. Uso de herramientas de cifrado.

- Realizar campañas de concientización sobre ingeniería social a los colaboradores.

- No descargar software de sitios no oficiales.

5. Conclusiones

Este trabajo final de Master sobre el Ransomware es una oportunidad para contribuir en la compresión de esto tipo de malware, los efectos que acarrea en la sociedad y descubrir sus modos de operación.

En cuanto al alcance de los objetivos e interpretación de los resultados podemos concluir que:

- El Ransomware LockBit está en constante evolución, se adapta a nuevos modelos de negocio, es altamente personalizable y usa vectores de ataque diseñados para el entorno corporativo. Estos tipos de malware se convierten en una problemática global que se debe investigar continuamente para descubrir sus modos de operación y apoyar en la lucha contra este flagelo que le cuesta miles de millones a la sociedad cada año.

- En el entorno corporativo el Ransomware es una amenaza latente que tiene grandes consecuencias económicas y sociales, a pesar de que entidades expertas y proveedores mantienen un trabajo continuo en la prevención, al igual que las compañías despliegan infraestructura de punta, en ocasiones tiene mayor importancia el factor social, la capacitación de todos los empleados y mantener una cultura en base a la seguridad concebida en todas las etapas y procesos de una compañía.

- En este TFM se describieron y analizaron los mecanismos y vectores usados en un ataque de LockBit, con técnicas cada vez más sofisticadas y métodos más efectivos. Se observo como estos ataques son cada vez más rápidos, pues en unos pocos minutos es capaz de cifrar grandes cantidades de datos. Todo esto crea la necesidad de que las organizaciones este preparadas para gestionar este tipo de incidentes y dar respuesta oportuna en caso de un ataque.

- Se exploraron algunas de las mejores prácticas para responder y mitigar el impacto a estos ataques, uno de los factores primordiales es reforzar el factor social, pues no basta con tener infraestructura de punta y aplicaciones de seguridad, si por otro lado no se gestiona y usa adecuadamente. Es necesario formar una cultura entorno a la seguridad de la información por parte de toda la comunidad empresarial como empleados, usuarios y clientes.

- Una futura investigación sobre el Ransomware requiere abordar técnicas avanzadas de detección, el uso de inteligencia artificial y desarrollar nuevas

herramientas y aplicaciones para prevenir este tipo de ataques de doble extorsión.

- A nivel tecnológico una posible alternativa para mitigar el impacto de un ataque consistiría en tener una fuerte gestión de respaldo de información y copias de seguridad periódicas, combinado con el cifrado de datos sensibles. Esto ayudara a mantener la confidencialidad y recuperación de los datos de una compañía incluso al ser víctima del Ransomware.

- Cualquier usuario corporativo por desconocimiento, confianza excesiva, represarías o engaño está expuesto a ser usado y participar en un vector de ingreso de un ataque, de allí la importancia de la capacitación y la formación de conciencia y cultura en cuanto a la importancia de la seguridad en la actualidad.

- Invertir en infraestructura, aplicaciones y capacitación en seguridad, aunque no se llegue a materializar un incidente y sea difícil calcular un retorno de inversión, garantiza la continuidad de operación de la compañía, privacidad de la información y trae grandes beneficios en cuanto a confianza, reputación y solidez.

6. Glosario

Bitcoin: Criptomoneda o moneda virtual, medio de intercambio electrónico.

Darkweb: internet oscura es el contenido de internet no indexado y oculto.

ENISA: Agencia de Ciberseguridad de la Unión Europea.

Exploit: Programa informático que se aprovecha de un error o vulnerabilidad.

FBI: Buró Federal de Investigaciones.

IC3: Internet Crime Complaint Center.

LAN: Red de área local o interna.

LockBit: Campaña de Ransomware basada en RaaS.

ODS: Objetivos Desarrollo Sostenible, Naciones Unidas.

RaaS: Ransomware como servicio.

VLAN: Red de área local virtual, permite segmentar el tráfico en una LAN.

Zcash: Criptomoneda que se centra en la privacidad.

7. Bibliografía

[1] La Historia del Ransomware [Internet]. The No More Ransom Project. [citado 12 de marzo de 2023]. Disponible en: https://www.nomoreransom.org/es/ransomware-qa.html

[2] kcarten. LockBit 3.0 Ransomware | Health Cyber: Ransomware Resource Center [Internet]. [citado 12 de marzo de 2023]. Disponible en: https://healthcyber.mitre.org/blog/lockbit-3-0-ransomware/

[3] Gamez MJ. Objetivos y metas de desarrollo sostenible [Internet]. Desarrollo Sostenible. [citado 12 de marzo de 2023]. Disponible en: https://www.un.org/sustainabledevelopment/es/objetivos-de-desarrollo-sostenible/

[4] 1. ENISA Threat Landscape for Ransomware Attacks [Internet]. ENISA. [citado 12 de marzo de 2023]. Disponible en: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks

[5] Richardson R. Ransomware: Evolution, Mitigation and Prevention. 2017;13(1).

[6] Maurya AK, Kumar N, Agrawal A, Khan ProfR. Ransomware Evolution, Target and Safety Measures. International Journal of Computer Sciences and Engineering. 31 de enero de 2018;6:80-5.

[7] An Empirically Comparative Analysis of Ransomware Binaries [Internet]. Splunk. [citado 2 de abril de 2023]. Disponible en: https://www.splunk.com/en_us/form/an-empirically-comparative-analysis-of-ransomware-binaries/thanks.html

[8] 1. Milenkoski A. Crimeware Trends | Ransomware Developers Turn to Intermittent Encryption to Evade Detection [Internet]. SentinelOne. 2022 [citado 3 de abril de 2023]. Disponible en: https://www.sentinelone.com/labs/crimeware-trends-ransomware-developers-turn-to-intermittent-encryption-to-evade-detection/

[9] LockBit ransomware — What You Need to Know [Internet]. www.kaspersky.com. 2022 [citado 3 de abril de 2023]. Disponible en: https://www.kaspersky.com/resource-center/threats/lockbit-ransomware

[10] Internet Creme Complaint Center(IC3) | Industry Alerts [Internet]. [citado 3 de abril de 2023]. Disponible en: https://www.ic3.gov/Home/IndustryAlerts?pressReleasesYear=_2022

[11] Internet Creme Complaint Center(IC3) | Industry Alerts [Internet]. [citado 3 de abril de 2023]. Disponible en: https://www.ic3.gov/Home/IndustryAlerts?pressReleasesYear=_2023

[12] Internet Crime Complaint Center(IC3) | Annual Reports [Internet]. [citado 12 de marzo de 2023]. Disponible en: https://www.ic3.gov/Home/AnnualReports

[13] Langlois P. 2020 Data Breach Investigations Report.

[14] Istacuy, C. (2020). Estudio sobre el impacto de los ataques de Ransomware en el Sector de la Salud. Recuperado 12 de marzo de 2023, de https://incibe.gt/wp-content/uploads/2021/09/Revista-Digital-Cybersecurity-Vol4.pdf#page=29

[15] Exfiltration, Tactic TA0010 - Enterprise | MITRE ATT&CK® [Internet]. [citado 3 de abril de 2023]. Disponible en: https://attack.mitre.org/tactics/TA0010/

[16] Conti M, Gangwal A, Ruj S. On the economic significance of ransomware campaigns: A Bitcoin transactions perspective. Computers & Security. 1 de noviembre de 2018;79:162-89.

[17] Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.

[18] Fernández ÁC. Las criptomonedas frente al delito de blanqueo de capitales y la complejidad de la prueba pericial en el ámbito ciberdelincuente. Anuario de Derecho Penal y Ciencias Penales [Internet]. 2022 [citado 12 de marzo de 2023];(1). Disponible en: https://revistas.mjusticia.gob.es/index.php/ADPCP/article/view/9697

[19] Chopra GA Paul Black,Priyank Baveja,Saahil. Uso de blockchain para rastrear el dinero en ransomware - KPMG Panamá [Internet]. KPMG. 2022 [citado 12 de marzo de 2023]. Disponible en: https://kpmg.com/pa/es/home/insights/2021/08/blockchain-analytics-tools-follow-money-in-ransomware-cases.html

[20] The Crazy Security Behind the Birth of Zcash, the Inside Story - IEEE Spectrum [Internet]. [citado 4 de abril de 2023]. Disponible en: https://spectrum.ieee.org/the-crazy-security-behind-the-birth-of-zcash

[21] Abrams L. LockBit 3.0 introduces the first ransomware bug bounty program.

[22] Los 10 vectores de ataque más utilizados por los ciberdelincuentes [Internet]. INCIBE. 2022 [citado 13 de marzo de 2023]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/los-10-vectores-ataque-mas-utilizados-los-ciberdelincuentes

[23] Zhang Z, Esaki H, Ochiai H. Unveiling Malicious Activities in LAN with Honeypot. En: 2019 4th International Conference on Information Technology (InCIT). 2019. p. 179-83.

[24] Santanaría Claro H. Análisis del ransomware Ryuk, impacto en los sistemas afectados y técnicas API Hooking y de aprendizaje automático como medidas de mitigación ante el ransomware. 5 de octubre de 2022 [citado 4 de abril de 2023]; Disponible en: http://e-spacio.uned.es/fez/view/bibliuned:master-ETSInformatica-CBS-Hsantamaria

[25] LockBit 2.0 uses group policies to spread [Internet]. 2021 [citado 4 de abril de 2023]. Disponible en: https://www.kaspersky.com/blog/ransomware-group-policies/40877/

[26] Ramaswami SS, Swain G. Detecting Macro less and Anti-evasive Malware in Malspam Word Attachments Using Anergy Scoring Methodology. En: 2023 International Conference on Advances in Intelligent Computing and Applications (AICAPS). 2023. p. 1-8.

[27]. Kara I. Fileless malware threats: Recent advances, analysis approach through memory forensics and research challenges. Expert Systems with Applications. 15 de marzo de 2023;214:119133.

[28] #StopRansomware: LockBit 3.0 | CISA [Internet]. 2023 [citado 5 de abril de 2023]. Disponible en: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-075a

[29] Seguridad con Deep Learning e IA [Internet]. SOPHOS. [citado 6 de abril de 2023]. Disponible en: https://www.sophos.com/es-es/content/deep-learning-cybersecurity

[30] IA y aprendizaje automático | Tecnología | Avast [Internet]. [citado 6 de abril de 2023]. Disponible en: https://www.avast.com/es-co/technology/ai-and-machine-learning

[31]. Presidencia del Gobierno. Real Decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021 [Internet]. Sec. 1, Real Decreto 1150/2021 dic 31, 2021 p. 167795-830. Disponible en: https://www.boe.es/eli/es/rd/2021/12/28/1150

[32] Ministerio de la Presidencia, Relaciones con las Cortes y Memoria Democrática. Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información [Internet]. Sec. 1, Real Decreto 43/2021 ene 28, 2021 p. 8187-214. Disponible en: https://www.boe.es/eli/es/rd/2021/01/26/43

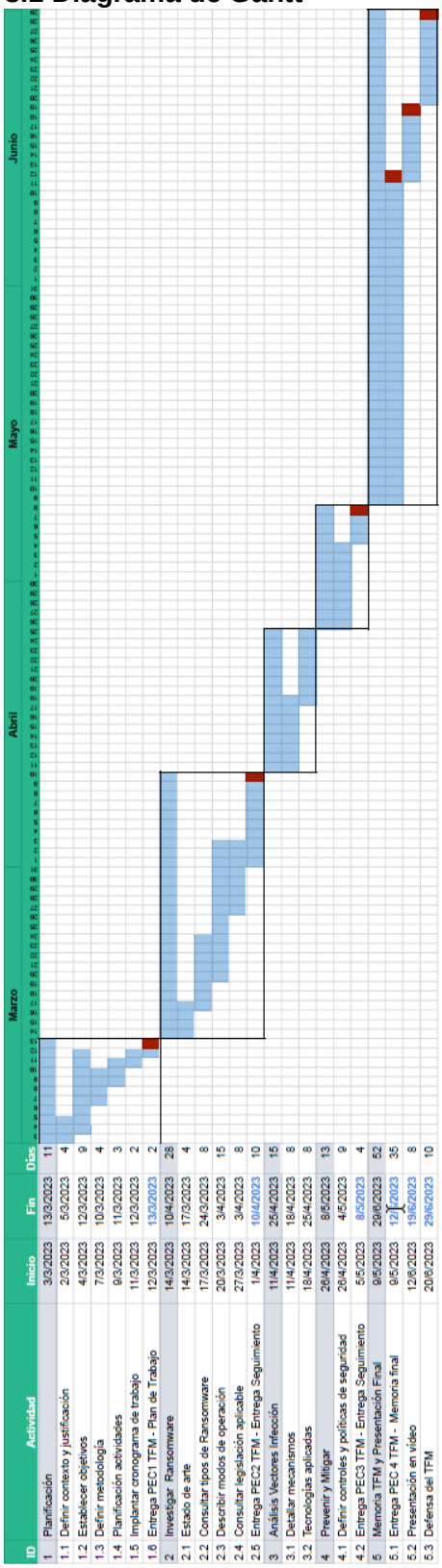
[33] BOE-A-1995-25444 Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. [Internet]. [citado 9 de abril de 2023]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444

[34] Estudio De Analisis De Lockbit | INCIBE-CERT | INCIBE [Internet]. [citado 1 de junio de 2023]. Disponible en: https://www.incibe.es/incibe-cert/guias-y-estudios/estudios/estudio-de-analisis-de-lockbit

[35] Automated Malware Analysis Report for vtTJ7BGJ3i.exe - Generated by Joe Sandbox [Internet]. [citado 1 de junio de 2023]. Disponible en: https://www.joesandbox.com/analysis/860399/0/html

8. Anexos

8.1 Diagrama de Gantt



ID	Actividad	Inicio	Fin	Días
1	Planificación	3/3/2023	13/3/2023	11
1.1	Definir contexto y justificación	2/3/2023	5/3/2023	4
1.2	Establecer objetivos	4/3/2023	12/3/2023	9
1.3	Definir metodología	7/3/2023	10/3/2023	4
1.4	Planificación actividades	9/3/2023	11/3/2023	3
1.5	Implantar cronograma de trabajo	11/3/2023	12/3/2023	2
1.6	Entrega PEC1 TFM - Plan de Trabajo	12/3/2023	13/3/2023	2
2	Investigar Ransomware	14/3/2023	10/4/2023	28
2.1	Estado de arte	14/3/2023	17/3/2023	4
2.2	Consultar tipos de Ransomware	17/3/2023	24/3/2023	8
2.3	Describir modos de operación	20/3/2023	3/4/2023	15
2.4	Consultar legislación aplicable	27/3/2023	3/4/2023	8
2.5	Entrega PEC2 TFM - Entrega Seguimiento	1/4/2023	10/4/2023	10
3	Análisis Vectores infección	11/4/2023	25/4/2023	15
3.1	Detallar mecanismos	11/4/2023	18/4/2023	8
3.2	Tecnologías aplicadas	18/4/2023	25/4/2023	8
4	Prevenir y Mitigar	26/4/2023	8/5/2023	13
4.1	Definir controles y políticas de seguridad	26/4/2023	4/5/2023	9
4.2	Entrega PEC3 TFM - Entrega Seguimiento	5/5/2023	8/5/2023	4
5	Memoria TFM y Presentación Final	9/5/2023	20/6/2023	52
5.1	Entrega PEC 4 TFM - Memoria final	9/5/2023	12/6/2023	35
5.2	Presentación en vídeo	12/6/2023	19/6/2023	8
5.3	Defensa del TFM	20/6/2023	29/6/2023	10