INSTITUTO TECNOLÓGICO SUPERIOR DE XALAPA

“LOCKBIT RANSOMWARE: DETECCIÓN Y PREVENCIÓN”

INGENIERÍA EN SISTEMAS COMPUTACIONALES

Presentan:

GARCÍA GARCÍA URIEL
YAEL LANDA SANGABRIEL

DOCENTE:
VILLA REYES EDUARDO

Xalapa-Enríquez, Veracruz a 8 de noviembre 2025

Indice

INTRODUCCIÓN

La investigación sobre el ransomware LockBit es un estudio crucial que aborda un problema de creciente preocupación en el ámbito de la ciberseguridad. Con el avance constante de la tecnología y la digitalización de la información, las amenazas cibernéticas han evolucionado, destacándose entre ellas el ransomware, un tipo de malware empleado para el robo de datos y exige un rescate para su liberación. Este documento, se enfoca en la detección y prevención del ransomware LockBit, específicamente, analizando su funcionamiento, variantes y el impacto que ha tenido en diferentes sectores.

El problema planteado en el documento se centra en la necesidad de entender cómo operan las técnicas de detección de LockBit, así como las acciones que pueden llevar a cabo individuos y organizaciones para prevenir estos ataques. Para ello, se propone realizar un análisis forense digital que permita recolectar y analizar pruebas que nos ayuden a mantener la integridad de nuestros datos.

La investigación no solo tiene relevancia académica, sino también social, ya que pretende beneficiar a estudiantes, empresas tecnológicas y a cualquier persona que esté interesada en la seguridad digital. Al abordar la creciente sofisticación de los ataques de ransomware, el documento busca dar a conocer el tema y ofrecer herramientas prácticas para la detección y prevención de estos incidentes.

Con un enfoque en el análisis de las variantes de LockBit y sus métodos de propagación, este estudio contribuye a la comprensión de un fenómeno que representa un desafío para la ciberseguridad actual y que puede afectar a cualquier persona, por lo que se considera de gran importancia la propagación de la información presentada a continuación.

ANTECEDENTES

Diversos estudios y reportes han analizado el fenómeno del ransomware y su impacto en la seguridad informática. Organizaciones como INCIBE (Instituto Nacional de Ciberseguridad de España), empresas de ciberseguridad como Akamai, SentinelOne y Palo Alto Networks (Unit42), así como plataformas como MITRE ATT&CK y VirusTotal, han documentado la evolución de LockBit desde su aparición en 2019 hasta sus variantes más recientes (LockBit 2.0, LockBit Black y LockBit Green).

A nivel internacional, se ha observado que LockBit se posiciona como uno de los ransomware más utilizados, debido a su capacidad de autopropagación, evasión de defensas y doble extorsión. En México, aunque existen esfuerzos por aumentar la ciberseguridad, el número de ataques ha ido en aumento, generando pérdidas económicas y afectaciones a empresas privadas y organismos públicos.

Sin embargo, pese a los avances en la comprensión del ransomware, existen vacíos de conocimiento relacionados con la detección temprana de LockBit y la efectividad de las herramientas preventivas en entornos reales. Muchas investigaciones se centran en describir el comportamiento del malware, pero no profundizan en estrategias integrales para detenerlo antes de que cifre los archivos o exfiltre información confidencial.

Este estudio busca aportar un análisis actualizado que combine la revisión de la literatura técnica y casos documentados con propuestas prácticas de detección y prevención, contribuyendo así a cerrar parte de esos vacíos.

CAPÍTULO I. PLANTEAMIENTO DEL PROBLEMA

1.1 Selección del tema

Lockbit ransomware: detección y prevención

1.2 Problemática

El constante avance del internet ha beneficiado ampliamente a nuestra sociedad, pero también ha generado problemas de seguridad que han sido explotados por la ciberdelincuencia.

> "La ciberdelincuencia son todos aquellos delitos que se cometen mediante las TIC, ya sea contra individuos, empresas o gobiernos." (García, 2023).

Existen muchos tipos de ataques cibernéticos con el fin de causar daños al usuario, por lo cual constantemente se desarrollan métodos para llevarlos a cabo, uno de estos métodos es el secuestro de información almacenada en los dispositivos, como el celular o laptop, mejor conocido como Ransomware que es un:

> "tipo de software malintencionado o malware que amenaza a una víctima con destruir o bloquear el acceso a sistemas o datos críticos hasta que se pague un rescate." (Microsoft, s.f.).

Posterior a un ataque de Ransomware, es necesario conocer todos los detalles que puedan brindar información sobre lo que ocurrió; por esta razón, se debe realizar un análisis forense que permita determinar todas las causas y consecuencias de dicho ataque. Para comprender

> "El análisis forense digital es el proceso de recopilar y analizar pruebas digitales de forma que se mantenga su integridad y admisibilidad en los tribunales." (IBM, 2024).

De modo en el que objetivo final llega a ser la mayor búsqueda de información confiable y llevar a cabo su análisis.

Por otro lado, existen miles de ataques de Ransomware en todo el mundo, ocurriendo a todas horas. Se puede observar la gráfica de ataques ocurridos en todo México. En la parte izquierda se observa el gráfico, con los picos más altos situados el 13 y 14 de noviembre, donde ocurrieron 700 sucesos relacionados con el secuestro de información.

Es necesario conocer todos los daños que ha provocado el Ransomware durante y después del secuestro de información, ya que este se enfoca en perjudicar los datos críticos. de una empresa o persona en particular.

> El secuestro de información causa daños técnicos como el cifrado de archivos, pérdida de datos, interrupción del sistema e infecciones secundarias (los atacantes instalan malware adicional). Causa daños financieros como lo es el costo de rescate, costos de recuperación, multas regulatorias, y la pérdida de ingresos. (Goldstein, 2024).

1.2.1 Delimitación del tema

"ANÁLISIS Y PREVENCIÓN DEL RANSOMWARE LOCKBIT EN SISTEMAS COMPUTACIONALES EN XALAPA DE FEBRERO A JUNIO DE 2025".

1.3 *Objetivos*

1.3.1 OBJETIVO GENERAL

Analizar las características de operación del ransomware LockBit con el fin de establecer mecanismos de prevención y detección de este para evitar su respetiva contaminación.

1.3.2 OBJETIVOS ESPECÍFICOS

1. Identificar y recopilar información teórica acerca de las características del ransomware
2. LockBit.
3. Analizar los patrones comunes que presenta el ransomware LockBit a partir de casos documentados.
4. Medir las acciones del ransomware LockBit antes y después de afectar a un equipo.

1.4 Preguntas de investigación

¿Cuáles son las principales características que distinguen al ransomware de LockBit?

¿Qué patrones en común presentan los casos documentados de propagación de LockBit?

¿Qué acciones realiza LockBit una vez que infecta un sistema antes de cifrar los archivos y después de hacerlo?

1.5 *Hipótesis*

Ransomware LockBit presenta características técnicas avanzadas que lo diferencian de otros tipos de ransomware en cuanto a su estructura y comportamiento.
Los casos documentos de LockBit presentan patrones comunes en cuanto a vectores de ataque, así como el uso de correos electrónicos y vulnerabilidades de software.
Se asume que LockBit presenta acciones detectables antes de cifrar archivos de un sistema, tales como deshabilitar funciones de seguridad y eliminar copias de seguridad.

1.6 Justificación

A través de este documento de investigación se pretende el beneficio de distintos sectores de la población, entre los cuales se destacan a los estudiantes universitarios del área de

tecnología además de los egresados de estas, así como empresas tecnológicas que necesitan seguridad digital. Asimismo, se pretende que el documento sea útil para todas aquellas personas interesadas en su seguridad digital.

Esta investigación funciona como un marco de referencia sobre este ransomware, una amenaza actual y avanzada. En este sentido, se proponen herramientas de detección y prevención, es importante el conocimiento de estos puntos ante un ataque.

La investigación aborda un problema actual y real, según el Instituto Nacional de Seguridad:

> LockBit, a medida de su evolución ha aumentado su sofisticación y capacidad para evadir las medidas de detección y seguridad, lo que genera una mayor amenaza a las organizaciones, por lo tanto, esta investigación que analiza la forma de detectarlo y a su vez prevenirlo es de suma importancia para la mitigación de estos ataques.
> (INCIBE, LockBit: acciones de respuesta y recuperación, 2024).

CAPÍTULO II. MARCO TEÓRICO

2.1 LockBit Ransomware

2.1.1 Definición Ransomware

Se define un ataque de Ransomware como:

> intentar llevar a cabo un tipo de extorsión a una empresa, organización o institución, de forma en que esta no pueda tener acceso a sus datos, es una forma de código malicioso, comparable con los virus que afectan a los dispositivos electrónicos. (Kubovič, 2021)

2.1.2 Ransomware a través del correo electrónico

Una manera en la cual es posible obtener malware que acabe en ransomware es a través del correo electrónico, esto por medio del envió de descargadores que instalan el malware en el dispositivo que recibe los correos electrónicos, esto en búsqueda del robo de datos valiosos.

El correo electrónico funciona como un pilar importante de recepción de botnets en donde es posible el uso de documentos de Microsoft Office con macros maliciosas para realizar el adentramiento inicial. (Kubovič, 2021)

2.1.3 Ransomware a través de la cadena de suministro

Un pilar importante que funciona como vector de ataque para el ransomware es la cadena de suministro, haciendo referencia la inclusión de malware a través de los ciberdelincuentes manipulando las actualizaciones o los paquetes de software originalmente legítimo, convirtiéndolo en un vector de ataque del cual tomar en cuenta. (Kubovič, 2021)

2.1.4 Antecedentes Lockbit Ransomware

Lockbit corresponde a un tipo de Ransomware que fue desarrollado por el grupo Bitwise Spider, su primera aparición registrada fue dada en septiembre del año 2019, siendo LockBit un nombre asignado posteriormente ya que en un inicio era conocido como ABCD ransomware puesto que era el nombre de la extensión que era dada para el renombramiento de todos aquellos archivos cifrados, se buscaba un pago para descifrar los archivos afectados. (GRUPO SPRI)

2.1.5 Variantes del ransomware LockBit

“LockBit ha evolucionado continuamente en el transcurso del tiempo, siendo observado por primera vez en el año de 2019, su última versión conocida con actualizaciones data de abril de 2023”. (Akamai, 2024)

- Enero de 2020: Aparece una variante de ransomware conocida como “LockBit” como extensión fue identificada dentro de foros de ciberdelitos en idioma ruso.
- Junio de 2021: Aparece la segunda versión de LockBit (LockBit 2.0), incluye una herramienta de nombre “StealBit” diseñada con el propósito del robo de información.
- Octubre de 2021: El ransomware extendió sus capacidades para atacar sistemas Linux y VMware ESXi.
- Marzo de 2022: LockBit 3.0, o LockBit Black, surge, comparte múltiples características con Black Matter y ALPHV/BlackCat.
- Enero de 2023: La nueva variante LockBit Green incorpora el código fuente del ransomware Conti, agrega nuevas funcionalidades
- “Abril de 2023: Es detectado en VirusTotal cifradores de ransomware LockBit dirigidos al sistema operativo macOS.” (Akamai, 2024)

2.1.6 LockBit 2.0

LockBit 2.0, la nueva variante de LockBit que busca atacar a organizaciones a través de intermediarios buscando la maximización de ganancias.

Implementa una herramienta de nombre StealBit, la cual descarga datos de las víctimas, no depende de datos de la nube de terceros, clona carpetas de redes corporativas a gran velocidad.

A partir de inicios de 2022, se convierte en la variante de ransomware más impactante e implementada en las violaciones de seguridad en las organizaciones.. Firman haber exigido rescates de datos a una cantidad ascendente a 12,000 empresas, siendo los principales países victimarios Estados Unidos, Italia y Alemania.

LockBit 2.0 implementa la auto propagación, la eliminación de registros y la impresión de hojas de rescate en las impresoras de las zonas de red afectadas, esto hasta que se acabe el papel en ellas. (Elsad, Gumarin, & Barr, 2022)

2.1.7 LockBit Black

LockBit 3,0 es la nueva variante de LockBit, también conocida como LockBit Black observada por primera vez en junio 2022, incluye características de soporte para Zcash y capacidades de administración avanzadas además de herramientas para evitar su análisis, ataca a través de correos electrónicos de phishing y spear phishing, aplicaciones expuestas a las vulnerabilidades y a través de marco de terceros. (SentinelOne, 2024)

2.1.8 Tipos de amenazas de LockBit

2.1.8.1 Extensión .abcd

Primera versión de LockBit, en un inicio renombra a los archivos afectados, cambiando la extensión que le corresponde por. abcd y a su vez inserta en cada carpeta un archivo .txt con el contenido de la nota de rescate, con las instrucciones necesarias para llevar a cabo la restauración de los archivos dañados. (Kaspersky, s.f.)

2.1.8.2 Extensión .LockBit

Segunda versión de LockBit, cambia la extensión.abcd por .LockBit dándole su nombre actual al Ransomware, sin embargo a través de distintas revisiones en el backend es posible observar las mismas características conforme a la versión anterior. (Kaspersky, s.f.)

2.1.8.3 Extensión .LockBit segunda versión

Siguiente versión de LockBit, a diferencia de las anteriores ya no requiere de la instalación de Tor dentro de las instrucciones que adjuntas para la restauración de los archivos, envía a las víctimas a un sitio web a través de los navegadores tradicionales. (Kaspersky, s.f.)

2.1.9 Impacto LockBit Ransomware

Lockbit 3.0 ejecuta diferentes acciones asegurando la correcta eficacia del ransomware finalizando los servicios relacionados a la seguridad, como la copia de seguridad, la base de datos y cualquier aplicación que pueda interferir con el proceso, deshabilita servicios de seguridad como lo puede ser Windows defender, todas estas acciones en búsqueda de que LockBit pueda funcionar en el sistema sin ser bloqueado, elimina y altera registros en el sistema buscando ralentizar la investigación forense y el análisis, incluso vacía el contenido existente en la papelera de reciclaje. (EcuCert, 2024).

2.2 LockBit Ransomware: Detección

2.2.1 Funcionamiento de los ataques

Los ataques de LockBit cuentan con diferentes atapas, a partir de los diversos ataques que han presentado se pueden catalogar las siguientes para su estudio. Es importante conocer las distintas etapas de su acceso a los sistemas ya que a partir de ahí se hace posible su detección.

2.2.1.1 Infección

LockBit comienza accediendo a los sistemas posteriormente infectados a través de correos electrónicos de pishing, en búsqueda de las vulnerabilidades de las máquinas y sistemas, otra de las maneras en las que acceden a ellos es a través de credenciales robadas, accediendo a los sistemas con ayuda de herramientas de VPN, otra táctica común llega a

ser contactar con personas en la empresa para conseguir sus credenciales a cambio de una retribución económica. (Akamai, 2024).

2.2.1.2 Propagación

Una vez accedido a los sistemas de una organización, LockBit se encuentra en búsqueda de archivos de valor en las maquinas, este Ransomware tiene la habilidad de auto propagarse para encontrar los hosts adicionales a los que puede acceder de manera autónoma. (Akamai, 2024).

2.2.1.3 Preparación

LockBit utiliza diferentes herramientas con el objetivo de realizar diversas acciones previas al cifrado de los archivos; entre ellas se encuentran la obtención de privilegios de alguna cuenta, se desactivan programas y cualquier herramienta relacionada con la seguridad de las maquinas correspondientes buscando que la víctima no pueda recuperar todos los archivos cifrados por cuenta propia. (Akamai, 2024).

2.2.1.4 Exfiltración

“Buscan exfiltrar ciertos archivos a otro servidor, para que de esta forma sea más sencillo la extorción a la empresa que sufrió el ataque a través de diversas amenazas con datos confidenciales.” (Akamai, 2024).

2.2.1.5 Cifrado

Se comienza el cifrado de los archivos, la empresa ya no será capaz de acceder a ellos a menos que cuenten con una clave para ello.

De igual manera, el software deja notas de rescate en las diferentes carpetas existentes. (Akamai, 2024).

2.2.1.6 Doble extorsión

A través del proceso de exfiltración llevado a cabo en una de las etapas anteriores, los responsables del ataque del ransomware pueden llevar a cabo dos extorsiones a la víctima, una para recuperar los archivos cifrados y la otra para evitar la filtración de los datos confidenciales obtenidos. (Akamai, 2024). CVE-2021-34473 , CVE-2021-34523 , CVE**2021-31207**

2.2.2 Common Vulnerabilities and Exposures (CVE)

“Las vulnerabilidades y exposiciones comunes (CVE) generalmente se refieren a la lista CVE, un catálogo divulgado públicamente de vulnerabilidades de seguridad de la información establecido y mantenido por MITRE Corporation.” (Khan & Goodwin, 2024).

Entre los CVE más representativos se encuentran los siguientes:

2.2.2.1 ProxyShell

En esta sección podemos encontrar 3 diferentes

> "CVE-2021-34473 permite a los atacantes saltar la sección de la autentificación a aquellas unidades de software afectadas, genera vulnerabilidad y hace posible que el atacante pueda ejecutar código perjudicial." (INCIBE, 2024).
>
> "CVE-2021-34523 esta vulnerabilidad también trabaja con la autenticación de los sistemas afectados generando puntos accesibles en cuestión de los privilegios asignados. Es una vulnerabilidad identificada en Microsoft Exchange Server." (INCIBE, 2024)

CVE-2021-31207 se describe como:

> "Vulnerabilidad de omisión de funciones de seguridad de Microsoft Exchange Server" (INCIBE, 2024)

2.2.2.2 Papercut

> "La vulnerabilidad asociada a esta sección es CVE-2023-27350 con la cual los atacantes pueden pasar a través de las autenticaciones, este problema sucede por un uso inadecuado.
> Con esto se puede ejecutar código." (INCIBE, 2024).

2.2.2.3 BlueKeep

La vulnerabilidad asociada a esta sección es CVE-2019-0708 sucede:

> "cuando un atacante no autenticado se conecta al sistema de destino mediante RDP y envía solicitudes especialmente diseñadas, también conocida como "Vulnerabilidad de ejecución remota de código en los Servicios de Escritorio Remoto". (INCIBE, 2024).

2.2.2.4 Apache Log4j

> "La vulnerabilidad asociada a esta sección es CVE-2021-44228 con la cual el atacante tiene acceso a los mensajes de registro, logrando la ejecución de código a través de servidores externos." (INCIBE, 2024).

2.2.2.4 Citrix Bleed

"La vulnerabilidad asociada a esta sección es CVE-2023-4966 la cual se encarga de la divulgación de información confidencial cuando es configurado un servidor como virtual." (INCIBE, 2024).

2.2.3 Indicadores de Compromiso

Los indicadores de riesgo (IoC) son información que dejan los atacantes, esto es todo aquello que puede ayudar a los equipos de seguridad a determinar si se ha producido un ataque.

Entre algunos de los datos que se pueden incluir en los detalles del ataque, pueden ser el tipo de malware utilizado, las direcciones IP y algunos otros detalles técnicos.
(Cloudfare, s.f.)

2.2.3.1 Indicadores de Compromiso basados en la red

Son aquellos que:

"como direcciones IP, dominios o URL maliciosos, también pueden incluir patrones de tráfico de red, actividad inusual del puerto, conexiones de red a hosts maliciosos conocidos o patrones de exfiltración de datos." (Cloudfare, s.f.).

2.2.3.2 Indicadores de Compromiso basados en el servidor

"Están relacionados con la actividad en una estación de trabajo o servidor. Los nombres de archivo, las claves de registro o los procesos sospechosos que se ejecutan en el servidor son ejemplos de IoC basados en el servidor." (Cloudfare, s.f.).

2.2.3.3 Indicadores de Compromiso basados en archivos

"Los IoC basados en archivos incluyen archivos maliciosos, tales como malware o scripts." (Cloudfare, s.f.).

2.2.3.4 Indicadores de Compromiso de comportamiento.

"Cubren varios tipos de comportamiento sospechoso, como comportamientos extraños de los usuarios, patrones de inicio de sesión, patrones de tráfico de red e intentos de autenticación." (Cloudfare, s.f.).

2.2.3.5 Indicadores de metadatos

"Tienen que ver con los metadatos asociados a un archivo o documento, como el autor, la fecha de creación o los detalles de la versión." (Cloudfare, s.f.).

2.2.4 Técnicas para la detección

2.2.4.1 Sistemas de monitoreo de actividad inusual

Una de las formas de detección de algún tipo de ransomware es a través del monitoreo de los patrones de uso de datos, esto para verificar las actividades, buscando una inusual, una actividad fuera de lo común como cambiar las extensiones de los archivos o renombrar los mismos, además de transferencias de datos no permitidas, en caso de una de estas acciones se puede estar llevando a cabo un ataque.

No obstante, para que esta técnica sea efectiva, los expertos en seguridad deben establecer parámetros claros de normalidad. (Robb, 2022)

2.2.4.2 Detección de anomalías en copias de seguridad

Dado que el ransomware tiende a afectar primero a las copias de seguridad, las organizaciones deberían optar por una solución de copia de seguridad que incluya detección de anomalías que pueda identificar cambios en un entorno que requiera la atención del departamento. (Robb, 2022)

2.2.5 Herramientas para el rastreo de ransomware

Dicho esto, CISA mantiene una lista de vulnerabilidades y exposiciones comunes (CVE) conocidas y explotadas que pueden ser un buen recurso para monitorear el abuso. Si bien la inteligencia de amenazas no evitará un escenario de paciente cero, puede descubrir de manera retrospectiva síntomas de vulneración. (Robb, 2022).

2.2.5.1 Alertas de PowerShell

Una táctica de detección inteligente es prestar atención a la omisión de ejecución de PowerShell, una configuración que determina qué tipo de scripts de PowerShell (si los hay) se pueden ejecutar en los sistemas. Motivo: los atacantes y el software malintencionado pueden aprovechar la configuración de la política de ejecución de PowerShell para ejecutar código en sistemas sin acceso administrativo. (Robb, 2022).

2.2.5.2 Caza de amenazas

"Las herramientas de búsqueda de amenazas dinámicas que aprovechan la inteligencia artificial son fundamentales para la detección de ransomware, pero aún se necesita ese toque humano y la información que solo puede provenir de una persona." (Robb, 2022).

2.3 LockBit Ransomware: Prevención

2.3.1 Concepto de prevención en ciberseguridad

La prevención en el contexto de la ciberseguridad se refiere a la implementación de estrategias y tecnologías que permiten anticipar y mitigar posibles amenazas antes de que ocurran.

A través de algoritmos de aprendizaje automático y análisis predictivo, se pueden identificar patrones y comportamientos anómalos que indican posibles ataques.

Esto permite que las organizaciones tomen medidas proactivas para fortalecer sus defensas, minimizar riesgos y evitar que los ciberataques causen daño o comprometan la seguridad de los sistemas y datos. (Shah, 2021)

2.3.2 Importancia de la prevención

La prevención en ciberseguridad es esencial para minimizar los riesgos de ataques informáticos y proteger tanto los sistemas como los datos valiosos.

A través de un enfoque preventivo, se pueden identificar y corregir posibles vulnerabilidades antes de que sean explotadas por los atacantes.

Esto no solo ayuda a evitar pérdidas económicas y de reputación, sino que también promueve un entorno seguro en el que las organizaciones pueden anticiparse a las amenazas.

Implementar medidas de prevención robustas es una estrategia clave para fortalecer la seguridad y asegurar la continuidad de las operaciones en un entorno digital cada vez más complejo y vulnerable (Chalermpong, 2019).

2.3.3 Herramientas tecnológicas de prevención

La ciberseguridad moderna depende en gran medida de herramientas tecnológicas avanzadas que permiten a las organizaciones prevenir, detectar y mitigar los riesgos asociados con las amenazas cibernéticas, como el ransomware, malware y otros ataques maliciosos.

Las herramientas de prevención son esenciales para proteger los sistemas, redes y datos valiosos de las empresas. (Price, s.f.)

2.3.3.1 Copias de seguridad

Las copias de seguridad juegan un papel crucial en la defensa contra el ransomware, ya que permiten restaurar los sistemas y datos a un estado previo a la infección. Por esta razón, las copias de seguridad se convierten en una herramienta vital para mitigar los efectos de un ataque de ransomware, proporcionando una línea de defensa esencial. Al contar con copias de seguridad

bien gestionadas, las organizaciones pueden minimizar el impacto de los ataques, evitando la necesidad de pagar el rescate o reconstruir completamente sus sistemas, lo que puede ser costoso y prolongado.

> “Las copias de seguridad pueden usarse para restaurar datos y sistemas a un estado conocido y seguro antes de la infección por ransomware” (Thomas & Galligher, 2018, pág. 1).

2.3.3.2 Firewalls

Los firewalls son esenciales contra el ransomware, ya que controlan el acceso a la red, bloquean conexiones no autorizadas y previenen que el malware se comunique con sus servidores de control. Al implementar reglas de privilegios mínimos y monitorear intentos de acceso maliciosos, los firewalls ayudan a detectar y contener amenazas antes de que causen daños mayores, reforzando la seguridad de la red.

> Los firewalls son efectivos para prevenir ataques iniciados desde el exterior de la red de una organización, pero son vulnerables a ciertas amenazas externas.
>
> Por ejemplo, los ataques de ransomware pueden exponer datos sensibles del firewall a entidades maliciosas o deshabilitar la protección de la red proporcionada por el firewall. (Allami, & et. Al., 2024)

2.3.3.3 Actualización de software (Patch and Block)

En 2017, para Richardson & North:

> mantener el software actualizado es una estrategia clave para prevenir infecciones de ransomware.
>
> Esto implica asegurarse de que el sistema operativo, los navegadores, los programas de seguridad y los complementos de terceros, como Java y Flash, estén siempre actualizados con los últimos parches disponibles.
>
> Además, limitar los privilegios de los usuarios y utilizar listas blancas de aplicaciones en entornos empresariales ayuda a reducir significativamente el riesgo de ataques.
>
> Aunque estas medidas también protegen contra otros tipos de malware, es importante reconocer que el ransomware evoluciona constantemente para evadir los antivirus, por lo que el software por sí solo no garantiza una defensa completa.

CRONOGRAMA DE ACTIVIDADES

Semana	Actividad	Producto Esperado
1	Introducción y Antecedentes	Borrador de la introducción [1]y recopilación de antecedentes iniciales (antecedentes LockBit).
2	Problema y Justificación	Redacción final del planteamiento del problema y delimitación. Conclusión de la justificación.
3	Definición de Objetivos y Preguntas	Redacción y revisión final del Objetivo General, Específicos y las Preguntas de Investigación.
4	Hipótesis y Categorías de Análisis	Formulación de las Hipótesis y desarrollo de las Categorías de Análisis (incluyendo indicadores y fuentes).
5	Marco Teórico (Primer Borrador)	Desarrollo de las secciones 2.1 (Definición, Variantes) y 2.2.1 (Funcionamiento/Etapas del ataque).
6	Ampliación y Revisión del Marco Teórico	Desarrollo de las secciones 2.2 (Detección: CVE, IoC, Técnicas) y 2.3 (Prevención).
7	Metodología y Diseño de Instrumento	Desarrollo de la Metodología (Cap. III), incluyendo tipo de investigación, población/muestra e instrumentos (Matriz de Análisis Documental).
8	Cronograma Detallado y Recursos	Inclusión y revisión de este cronograma, listado de recursos, y el presupuesto.
9	Bibliografía y Referencias Formateadas	Compilación y revisión de todas las referencias citadas para asegurar el formato correcto.
10	Revisión General y Conclusiones	Revisión de coherencia global (Objetivos/Hipótesis/Metodología) y redacción de la Conclusión del Protocolo.
11		

CAPÍTULO III. ALCANCE DE LA INVESTIGACIÓN A REALIZAR

3.1 Tipo y diseño de la investigación

La investigación que se propone a realizar es de tipo descriptiva, transversal y analítica. Es descriptiva porque busca identificar las características de los ataques con ransomware Lockbit y las medidas implementadas para su detección y prevención, dichos aspectos de los cuales ya es conocido el problema, por lo que se trata de una recolección de datos existentes. Se considera transversal ya que los datos se recolectarán en un solo momento del tiempo, permitiendo analizar la situación actual, no se llevará a cabo un seguimiento posterior a la investigación como lo es la de tipo longitudinal. También se considera la investigación de tipo analítica, puesto que busca relacionar los métodos preventivos aplicados según los documentos analizados previos además de tomar en cuenta cada aspecto del ransomware para poder determinar ciertas reglas de detección y prevención.

3.1.1 Sistema de hipótesis y variables o de presupuestos y categorías de análisis

Hipótesis general

La identificación de las características operativas, los métodos de propagación y el comportamiento del ransomware Lockbit, basada en información teórica y casos documentados, permite establecer mecanismos de detección y prevención más eficaces para mitigar su impacto.

Basándose en los objetivos específicos del estudio, se establecen las siguientes categorías de análisis, sus respectivas definiciones, indicadores, reactivos sugeridos y tipo de fuente documental esperada:

Categoría de análisis	Definición conceptual	Indicador	Fuente esperada
características operativas de LockBit	Rasgos técnicos y funcionales que describen cómo actúa el ransomware desde su activación hasta el cifrado	Modo de ejecución, persistencia, evasión de detección, métodos de cifrado	Artículos científicos, Blogs técnicos
Métodos de propagación	Vías que utiliza Lockbit para expandirse dentro de sistemas o redes	Phishing, RDP, exploits, mals-pam	Reportes de incidentes
Comportamiento antes y después de la infección	Actividades detectadas en la fase de reconocimiento y ejecución	Comunicación con servidores, exfiltración de datos	Informes técnicos, bases de datos de ciberataques

Mecanismos de detección y prevención documentados	Medidas técnicas o estratégicas que se han documentado como efectivas para detener o mitigar ataques de Lockbit	Uso de firewalls, segmentación, capacitación, monitoreo de comportamiento	Guías de seguridad, artículos académicos.

Basándose en los objetivos específicos del estudio, se establecen las siguientes categorías de análisis, sus respectivas definiciones, indicadores, reactivos sugeridos y tipo de fuente documental esperada

3.2 Población, muestra y técnicas de recolección de información

En la presente investigación, enfocada en el análisis del ransomware Lockbit y sus mecanismos de detección y prevención, el universo de estudio no está constituido por personas o elementos humanos directamente, sino por una recopilación de fuentes documentales, información técnica, reportes de incidentes y estudios de caso, toda información disponible en línea sobre el comportamiento y funcionamiento de dicho ransomware.

Población

En este sentido, la población considerada está compuesta por:

- Reportes técnicos publicados por empresas de ciberseguridad
- Informes de análisis forense de ataques reales documentados por instituciones de ciberseguridad gubernamentales o privadas.
- Publicaciones científicas en revistas arbitradas que aborden el tema del ransomware Lockbit y el ransomware en general.
- Entradas en bases de datos de amenazas como MITRE ATT&CK, VirusTotal, y otras plataformas.
- Artículos académicos disponibles en bases de datos.

La extensión de esta población es de carácter global, dado que el ransomware Lockbit ha afectado sistemas en diferentes países e industrias a nivel mundial. Su contenido es variado, pero centrado en aspectos técnicos, prácticos y estratégicos que permiten un análisis profundo del funcionamiento y mitigación de este tipo de amenaza informática.

Muestra

Dado que no es viable analizar todos los documentos, casos y reportes existentes a nivel global sobre Lockbit, se procederá a una selección muestral hacia aquellos documentos y fuentes que cumplan con los siguientes criterios de inclusión:

Criterios de inclusión:

1. Documentos que traten específicamente sobre el ransomware Lockbit (versiones 1.0, 2.0, 3.0 o posterior).
2. Artículos o documentos con autoría reconocida o provenientes de fuentes institucionales oficiales.
3. Información publicada entre los años 2020 y 2025 para asegurar actualidad.

Criterios de exclusión:

1. Fuentes sin respaldo institucional, anónimas o que carezcan de verificabilidad.
2. Documentos que se enfoquen en ransomware genérico sin incluir a Lockbit.
3. Publicaciones repetidas o que no aporten información novedosa al estudio.

El tamaño estimado de la muestra incluirá entre 10 y 20 documentos seleccionados, incluyendo reportes, artículos, fichas técnicas y publicaciones académicas. Esta cantidad se considera adecuada para lograr una visión representativa de las distintas perspectivas del ransomware Lockbit sin perder profundidad analítica.

La selección se justifica en función del enfoque documental de la investigación. Al no trabajar directamente con personas ni con una población susceptible de medición estadística directa, se prioriza la calidad, relevancia, actualidad y profundidad de las fuentes por encima de la representatividad numérica.

3.2.1 Instrumentos

En esta investigación no se utilizarán cuestionarios, encuestas ni entrevistas como instrumentos de recolección de datos, ya que el enfoque del estudio es documental y exploratorio, orientado al análisis técnico y teórico del comportamiento del ransomware Lockbit. Dado que no se busca recolectar opiniones o experiencias directas de individuos, sino sistematizar y analizar información ya existente.

3.2.2 Equipos

Se emplearán únicamente computadoras personales con acceso a internet para la búsqueda y consulta de fuentes confiables. No se requiere equipo técnico especializado.

3.2.3 Instalaciones

Dado que la investigación es documental y en línea, se desarrollará sin necesidad de instalaciones especializadas.

3..3 Desarrollo

1. Búsqueda de fuentes documentales especializadas entre 2020 y 2025.
2. Selección y validación de fuentes confiables.
3. Registro de información clave.
4. Organización de las estrategias de detección y prevención encontradas.
5. Análisis comparativo entre enfoques recomendados y casos documentados.
6. Redacción de resultados y validación de hipótesis.

3.3.1 Técnica de análisis y procesamiento de la información

El análisis de la información en esta investigación se hará a partir de fuentes ya existentes, como artículos especializados, informes de empresas de ciberseguridad, noticias sobre ciberataques, y estudios académicos disponibles en internet. El enfoque será principalmente cualitativo, ya que no se trabajará con estadísticas o datos numéricos recolectados por medio de encuestas, sino con descripciones, explicaciones y casos reales documentados.

Lo primero será leer y seleccionar información confiable y actualizada, publicada por fuentes reconocidas y organizaciones que monitorean amenazas informáticas.

Posteriormente, se procederá a ordenar la información según los temas más relevantes. Por ejemplo, se clasificará el contenido en bloques como: características técnicas del ransomware, mecanismos de propagación, efectos antes y después del ataque, y métodos de prevención o detección utilizados en diferentes escenarios.

Una vez clasificada la información, se hará un análisis comparativo, revisando qué patrones se repiten entre los distintos documentos.

Además, se identificarán coincidencias o diferencias entre casos reales, lo que permitirá entender cómo ha cambiado el comportamiento de Lockbit con el tiempo, si ha evolucionado en sus técnicas, o si hay nuevas versiones más peligrosas.

CONCLUSIÓN

A partir del desarrollo de esta investigación acerca del ransomware lockbit ha sido posible obtener cierto conocimiento del mismo además de llegar a conclusiones gracias a la información que pudimos recuperar de las diferentes fuentes consultadas, todo esto a través de la adquisición de conocimientos acerca de las versiones de este malware, ciertas características del mismo y en principales elementos para su detección y prevención. Se obtuvo información acerca del nivel de peligrosidad que le corresponde a este malware además de una de las razones por las cuales es tan sofisticado o tan relevante su estudio puesto que tiene una gran capacidad de adaptación a diferentes entornos, un tema que pudimos ver ya que en sus diferentes versiones cada una mejoraba de forma en que fuera muy difícil o casi imposible de ser detectado por los sistemas, haciendo cada vez más dura la tarea de evitar ser infectados.

Sin embargo, aunque se logró obtener una cantidad considerable de información acerca del tema a partir de esta investigación, también surgieron diferentes obstáculos y dificultades durante su desarrollo, entre ellos la cantidad de fuentes disponibles, ya que en cuestión de artículos o libros al ser este tema un tanto reciente no existe una gran cantidad de fuentes suficientemente confiables a las cuales recurrir para llevar a cabo la investigación, Esto puede considerarse un obstáculo, ya que, al momento de recolectar la mayor cantidad posible de información, recurrimos a buscar fuentes adicionales más allá de artículos y libros, recurriendo a los sitios web, sin embargo al mismo tiempo cuidando que estos contuvieran información verídica y confiable para poder utilizarla en el documento.

¿Cómo funcionan las técnicas de detección de las variantes de LockBit Ransomware? ¿Qué acciones puede llevar a cabo una persona u organización para la prevención de estos ataques?

Respondiendo a las preguntas planteadas en un inicio a través de la investigación realizada, es posible proponer que las diferentes técnicas de detección que se manejan en el momento Bing tentar combatir este tipo de amenazas de manera principal lo que hacen es analizar comportamientos anormales en las máquinas o sistemas de una empresa, ya que esta es una de las principales maneras en las cual se puede detectar algún cambio en los archivos o algún tipo de actualización o cambio no autorizado, lo cual puede ser en realidad que se esté tratando de un ataque de malware, lo que hacen las herramientas de detección es principalmente un monitoreo y un análisis acerca de todos los comportamientos que existen, obviamente para poder realizar esto se tiene que tener en un principio un panorama de lo que vendría siendo un comportamiento normal en la empresa esto para tener un punto de referencia hacia los comportamientos anormales.

Por otro lado, algunas de las acciones que se pueden implementar principalmente en las organizaciones para prevenir estos ataques están relacionadas con la seguridad cibernética, esto es lo principal ya que una empresa con información delicada debería invertir en políticas de seguridad cibernética y en tener diferentes copias de seguridad para que los archivos no corran peligro ninguno de los casos, un punto claro es que, en el momento en que un ataque de este tipo

es detectado, puede que incluso ya sea tarde para generar una contramedida. Por lo tanto, lo más adecuado e ideal es intentar prevenirlos teniendo un buen manejo de los sistemas, máquinas y archivos de una empresa o de un usuario individual.

BIBLIOGRAFÍA

Akamai. (2024). *¿Qué es LockBit Ransomware?* Obtenido de https://www.akamai.com: https://www.akamai.com/glossary/what-is-lockbit-ransomware

Allami, A., Nicewarner, T., Goss, K., Kundu, A., Jiang, W., & Lin, D. (2024). Oblivious and distributed firewall policies for securing firewalls from. *Elsevier*, 13. Obtenido de https://www.sciencedirect.com/science/article/pii/S0167404824005066

Chalermpong, S. (2019). Port cybersecurity and threat: A structural model for prevention and.

Elsevier, 36. Obtenido de https://pdf.sciencedirectassets.com/282329/1-s2.0-

S2092521220X0006X/1-s2.0-S2092521220300389/main.pdf?X-Amz-Security-Token=IQoJb3JpZ2luX2VjEOD%2F%2F%2F%2F%2F%2F%2F%2F%2F%2FwEaCXVzLWVhc3QtMSJHMEUCIQDFomAcrU5j7TAwSfjPUh4ChEcJp2ZUGVBUI5jwNHCVWwIgQu2CljQcl6e%

Cloudfare. (s.f.). *¿Qué son los indicadores de compromiso (IoC)?* Obtenido de https://www.cloudflare.com: https://www.cloudflare.com/es-es/learning/security/whatare-indicators-of-compromise/

EcuCert. (10 de Mayo de 2024). *LockBit 3.0 Ransomware* . Obtenido de chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.ecucert.gob.ec/wpcontent/uploads/2024/05/AL-2024-007-LockBit-3.0-Ransomware.pdf

Elsad, A., Gumarin, J., & Barr, A. (9 de Junio de 2022). *LockBit 2.0: cómo funciona este RaaS y cómo protegerse contra él*. Obtenido de https://unit42.paloaltonetworks.co: https://unit42.paloaltonetworks.com/lockbit-2-ransomware/ franco, d. s. (2016). *LA PRIVACIDAD DE LA INFORMACIÓN GENERADA POR DISPOSITIVOS DE DOMÓTICA EN EL INTERNET DE LAS COSAS*. guatemala.

Goldstein, E. (16 de Septiembre de 2024). *Tendencias, estadísticas y datos sobre ransomware en 2024*. Obtenido de https://es.safetydetectives.com/blog/ransomware-statistics-es/

GRUPO SPRI. (s.f.). *LockBit Ransomware* . Obtenido de chrome-

extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.ciberseguridad.eus/sites/de fa ult/files/2022-08/bcsc-malware-lockbit-tlpwhite.pdf

IBM. (16 de Febrero de 2024). *¿Qué es el análisis forense digital?* Obtenido de https://www.ibm.com/es-es/topics/digital-forensics

INCIBE. (23 de Marzo de 2023). *Estudio de análisis de Lockbit.* Obtenido de https://www.incibe.es/incibe-cert/guias-y-estudios/estudios/estudio-de-analisis-de-lockbit

INCIBE. (25 de Julio de 2024). *CVE-2019-0708*. Obtenido de https://www.incibe.es: https://www.incibe.es/en/incibe-cert/early-warning/vulnerabilities/cve-2019-0708

INCIBE. (26 de Julio de 2024). *CVE-2021-31207*. Obtenido de https://www.incibe.es: https://www.incibe.es/en/incibe-cert/early-warning/vulnerabilities/cve-2021-31207

INCIBE. (2 de Febrero de 2024). *CVE-2021-34523*. Obtenido de https://www.incibe.es: https://www.incibe.es/en/incibe-cert/early-warning/vulnerabilities/cve-2021-34523

INCIBE. (24 de Julio de 2024). *CVE-2021-44228*. Obtenido de www.incibe.es: https://www.incibe.es/en/incibe-cert/early-warning/vulnerabilities/cve-2021-44228

INCIBE. (27 de Junio de 2024). *CVE-2023-27350*. Obtenido de https://www.incibe.es: https://www.incibe.es/en/incibe-cert/early-warning/vulnerabilities/cve-2023-27350

INCIBE. (27 de Junio de 2024). *CVE-2023-27350*. Obtenido de https://www.incibe.es: https://www.incibe.es/en/incibe-cert/early-warning/vulnerabilities/cve-2023-27350

INCIBE. (14 de Agosto de 2024). *CVE-2023-4966*. Obtenido de https://www.incibe.es: https://www.incibe.es/en/incibe-cert/early-warning/vulnerabilities/cve-2023-4966

INCIBE. (14 de Marzo de 2024). *LockBit: acciones de respuesta y recuperación*. Obtenido de https://www.incibe.es/incibe-cert/blog/lockbit-acciones-de-respuesta-y-recuperacion

Kaspersky. (s.f.). *Ransomware LockBit: lo que necesitas saber*. Obtenido de https://latam.kaspersky.com/resource-center/threats/lockbit-ransomware

Khan, T., & Goodwin, M. (22 de Julio de 2024). *¿Qué es Common Vulnerabilities and Exposures (CVE)?* Obtenido de https://www.ibm.com: https://www.ibm.com/mx-es/think/topics/cve

Kubovič, O. (Agosto de 2021). *RANSOMWARE: Un vistazo al arte criminal de los códigos maliciosos, la presión y la manipulación.* Obtenido de chromeextension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.eset.com/fileadmin/ESET/ES

/Landings/Whitepapers/RANSOMWARE_Un_vistazo_al_arte_criminal_de_los_c%C3%B3digos_maliciosos_20210922.pdf

Microsoft. (s.f.). *¿Qué es el ransomware?* Obtenido de https://www.microsoft.com/esmx/security/business/security-101/what-is-ransomware?msockid=3ed6e3c72e736fb418f4f7272f9d6e1a

Price, M. (s.f.). *Defensa contra ransomware: Mejores prácticas para la prevención de malware y ransomware*. Obtenido de Object First:

https://objectfirst.com/es/guides/ransomware/ransomware-defensestrategy/?utm_source=chatgpt.com

Richardson, R., & North, M. (2017). Ransomware: Evolution, Mitigation and Prevention. *International Management Review*, 13. Obtenido de

https://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=5312&context=facpubs

Robb, D. (24 de Marzo de 2022). *Técnicas para la detección de ransomware*. Obtenido de https://www.cioinsight.com: https://www.cioinsight.com/security/ransomware-detection/

SentinelOne. (2024). *LockBit 3.0 (LockBit negro)*. Obtenido de https://www.sentinelone.com: https://www.sentinelone.com/anthology/lockbit-3-0-lockbit-black/

Shah, V. (2021). Machine Learning Algorithms for Cybersecurity: Detecting and Preventing Threats. *CSIC*, 66. doi:10.5281

Thomas, J., & Galligher, G. (2018). Improving Backup System Evaluations in Information Security Risk. *Computer and Information Science*, 12. doi:10.5539/cis.v11n1p14