UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS “ESPOG”

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Resolución: **RPC-SO-02-No.053-2021**

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGÍSTER

Título del proyecto:
Descripción del ataque del Ransomware EXX bajo un entorno controlado en máquinas virtuales
Línea de Investigación:
Seguridad Informática
Campo amplio de conocimiento:
Tecnologías de la Información y Comunicación
Autora:
Páez Padilla Mónica Elizabeth
Tutor:
Recalde Varela Pablo Marcelo

Quito – Ecuador

2023

APROBACIÓN DEL TUTOR

Yo, Pablo Marcelo Recalde Varela con C.I: 171168505-5 en mi calidad de Tutor del proyecto de investigación titulado: Descripción del ataque del Ransomware EXX bajo un entorno controlado en máquinas virtuales.

Elaborado por: Páez Padilla Mónica Elizabeth de C.I:171473018-9 estudiante de la Maestría: Seguridad Informática, mención: de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., marzo de 2023

Firmado electrónicamente por:
PABLO MARCEL
RECALDE VARELA

Firma

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, Mónica Elizabeth Páez Padilla con C.I: 171473018-9, autora del proyecto de titulación denominado: Descripción del ataque del Ransomware EXX bajo un entorno controlado en máquinas virtuales; previo a la obtención del título de Magister en Seguridad Informática.

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autora del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M.,marzo de 2023

Firma

ORCID: 0009-0006-1030-1394

Tabla de contenidos

Índice de tablas

Índice de figuras

INFORMACIÓN GENERAL

Contextualización del tema

El recurso más valioso para las organizaciones hoy en día, ya sean de carácter económico, político o social es la información que a través de Internet, computadoras y redes de datos convergen en un solo elemento, la mayoría de las actividades diarias, incluidos los pagos por servicios simples, transacciones bancarias y otras actividades, se han digitalizado, a los nuevos sistemas tecnológicos y la población se ha ajustado a estos cambios. (Vargas, 2020).

Algunas empresas de telecomunicaciones se han visto expuestas a otro tipo de ataques dirigidos a nivel de red o a través de una conexión remota, ataques que antes no se consideraban significativos, pero que ahora suponen una amenaza importante para el sector público y privado, cuando se consigue vulnerar la seguridad informática de cualquier empresa, se ven comprometidos datos confidenciales, personales e incluso íntimos, la ciberseguridad ahora ayuda a prevenir o reducir el riesgo de ataques cibernéticos a las redes de datos e información que manejan, y que son esenciales para sus actividades. (INCIBE, 2019)

Los avances tecnológicos y la creciente dependencia de los medios digitales crean un entorno extremadamente frágil que interfiere con el funcionamiento adecuado de varias funciones organizacionales y plantea posibles amenazas a la seguridad, para evitar un aumento de los ataques cibernéticos y de las infraestructuras de telecomunicaciones existentes, se debe establecer un proceso de seguridad de forma técnica y jurídica que comprenda los recursos intangibles de toda empresa que necesitan ser protegidos, y la ciberseguridad son áreas clave de investigación estratégica para proteger el ciberespacio. (Freire, 2017)

Con referencia a los acontecimientos, se realizan diversos estudios para determinar qué vulnerabilidades se han producido, patrones de ataque y su impacto en las organizaciones afectadas, y desarrollar políticas de seguridad robustas y fiables permitiendo prevenir la pérdida de información. (Castro, 2015).

A continuación, podemos mencionar algunas estadísticas sobre seguridad informática:

- En más de 90% de todas las organizaciones de salud se ha reportado la existencia de brechas en los últimos tres años, la ciberseguridad. (Frost & Sullivan)
- El 62,7% de las empresas reportan un aumento en los ataques cibernéticos como resultado de la pandemia de COVID 19. (Prey, 2021)
- Las pequeñas empresas son el objetivo del 43% de los ciberataques. (Trends, 2022)
- A partir de 2019, el 93 % de las muestras de malware son polimórficas, lo que significa que pueden cambiar su programación para evadir la detección. (Webroot, 2022)

Problema de investigación

A través de la investigación del comportamiento de Ransomware *Ransonexx* es posible establecer mecanismos para la recuperación de la información.

Se debe hacer una pausa para considerar qué sucedería si fuéramos víctimas de robo o daño a nuestra información porque la mayoría de las actividades diarias que realizamos involucran un alto nivel de transaccionalidad de datos.

El activo más valioso, ya sea personal o relacionado con el negocio, debe protegerse y preservarse, por lo que debemos tomar las medidas adecuadas.

Es una responsabilidad ser conscientes de que la seguridad informática es una necesidad en nuestro día a día porque somos susceptibles a cualquier tipo de ataque informático que ponga en peligro la accesibilidad, privacidad y exactitud de los datos, si bien la conveniencia y la comodidad que nos brinda la tecnología captan constantemente nuestra atención, es mejor que nos concentremos en la seguridad informática a medida que la tecnología continúa avanzando.

Según un Informe de Interpol (2020) los ciberataques a los sistemas de información y servidores que alojan datos confidenciales aumentaron más del 51% en 2020, resultado de un ataque reciente que se está volviendo más frecuente, como el malware de la variedad Ransomware, que utiliza un programa para cifrar datos y exige un rescate para descifrarlos.

Información recopilada por el equipo de investigación de ciberataques señalan que en 2016 surgieron sesenta y dos nuevas familias de ransomware. Además, muestran que desde que se realizaron dos mil novecientas modificaciones en el primer trimestre de 2016, la cantidad de nuevas variaciones de ransomware se ha multiplicado por once del tercer trimestre, 32.091 modificaciones y adiciones. Además, una de cada cinco pymes pagó el rescate. Su información nunca fue devuelta. Esto sugiere que el ransomware está en desarrollo y que a pesar de los pagos no se pueden restaurar los archivos cifrados.

¿Por medio de una descripción detallada del ransomware se puede entender y tener una mejor óptica para la protección empresarial contra ataques de ransomware?

Objetivo general

Realizar una descripción del ataque del «Ransomware Ransonexx» con la finalidad de identificar los patrones y vectores de ataque que utiliza por medio de una simulación en ambiente controlado, usando máquinas virtuales.

Objetivos específicos

1. Revisar la evolución de los ataques de Ransomware desde su aparición hasta la actualidad desde una revisión documental que incorpore casos de estudio.

2. Identificar brechas de seguridad que permiten el ataque del Ransomware Ransonexx desde la simulación en escenarios controlados.
3. Proponer medidas preventivas ante los ataques por Ransomware Ransonexx, considerando las principales debilidades o brechas de seguridad.

Vinculación con la sociedad y beneficiarios directos:

Esta investigación busca ayudar a la sociedad en general a entender el comportamiento y las posibles soluciones contra el ataque de Ransomware Ransonexx, y así evitar el secuestro de información a las empresas o personas. Acorde al Objetivo de Desarrollo sostenible (ODS) nueve de las Naciones Unidas que indica «Construir infraestructuras resilientes, promover la industrialización sostenible y fomentar la innovación»

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

En este capítulo se presenta la situación de estudio de la problemática de ataques Ransomware.

1.1 Contextualización general del estado del arte

Según Moncayo (2019), el malware a menudo se equipará con los virus informáticos, pero los virus son solo una de las muchas subcategorías de malware. El malware asociado a menudo se basa en códigos cifrados recibidos al descargar productos digitales o abrir páginas, este código se propaga a través de varias fuentes y al descargarlo, se activa en el dispositivo afectado.

Las consecuencias no siempre son obvias a primera vista: No todo el malware se activa en un corto período de tiempo, y los programas más pequeños pueden infiltrarse en los datos escaneados, analizan flujos de datos, recuperan contraseñas y a la larga, hacen más que daños significativos. Por lo tanto, la precaución es la mejor solución para prevenir eficazmente los ataques desde Internet, por eso es aún más importante que las empresas con redes internas hagan todo lo posible para evitar las intrusiones de malware.

Con los diferentes tipos de malware hay numerosos factores de riesgo para los equipos. El Ransomware es la forma más directa de malware en este momento y aparece a los pocos segundos de la instalación. Otros programas maliciosos sólo muestran su efecto en un momento posterior y permanecen discretos al principio, así pues, sólo conducen al daño real más adelante, mientras tanto, por ejemplo, se recogen datos e información sobre los usuarios del dispositivo, por regla general, el malware está programado para causar daños concretos, sirven como medio para un fin y obtener los datos necesarios para el hacker, el resultado puede ser robo de información financiera o el robo de identidades que luego pueden utilizarse con fines delictivos.

Por esta razón, es importante identificar el malware a tiempo y luego eliminarlo,sin embargo, con la ayuda de un escáner de malware, es posible detectar las amenazas antes de que surtan efecto y eliminar el software de los dispositivos afectados.

Clasificación del Malware

Según Moncayo (2019)**,** el malware se logra categorizar de muchas maneras diferentes, por lo que se crearon tres grupos para comprender de mejor forma los tipos de malware que existen, que se mostrarán en las Tablas 1, 2 y 3 en ese orden:

Tabla 1.
Clasificación de Malware por cómo actúan

Por su manera de cómo actúan
Virus: Es un código malicioso que consigue infectar a los computadores al modificarlos, depende de otros programas y, por lo general, requiere la intervención humana para propagarse. Los virus informáticos se pueden diseñar para que sean rápidos y pequeños utilizando las mismas herramientas que otro software.
Gusanos: Este es un programa de computadora que no se autorreplica parasitariamente. Es decir, pueden funcionar de forma independiente. Los gusanos normalmente toman el control de una computadora y la usan como punto de partida para comprobar otros sistemas vulnerables.

.

Nota: El malware se puede categorizar de varias maneras, por lo que se han creado tres grupos para una mejor comprensión. Adaptado de: (Moncayo P,2019).

Tabla 2.
Clasificación de Malware por la manera de lucrar

Por su manera de lucrar
Bot: Derivado de la palabra robot y conocido como auto ataque. El propósito de un bot suele ser infectar una computadora para conectarse a un servidor central que lleva a cabo las instrucciones para que el Bot lance ataque global a un objetivo específico.
Adware: Generar automáticamente informes dentro de nuestros servicios o aplicaciones que se presentan a los usuarios. Puedes obtener dos tipos de ingresos. Uno es mostrar anuncios y el otro es que los usuarios hagan clic en anuncios destacados.

Nota: El malware se puede categorizar de varias maneras, por lo que se han creado tres grupos para una mejor comprensión. Adaptado de: (Moncayo P, 2019).

Ransomware

El malware conocido como ransomware engaña a las víctimas para que paguen un rescate para restaurar los archivos modificados. (Proofpoint, 2021)

- Cifrar la información de la víctima y evitar que la víctima acceda a su información personal.
- Restringir el acceso a la computadora de la víctima.

RansomEXX

Según Bestuzhev (2021), RansomEXX no es malware; muchas personas todavía creen que el ransomware es un programa malicioso, por lo que abordan el problema desde el ángulo equivocado. Ransomware ha podido ganar algunas batallas, pero no la guerra, debido a esta grave falla.

Ransomware Exx es una nueva amenaza que se dirige a las computadoras vulnerables, la amenaza puede afectar a diferentes tipos de archivos, asegurándose de causar el mayor daño posible al equipo infectado. Las víctimas del ransomware Exx no podrán acceder ni utilizar ninguno de sus archivos personales. El archivo de destino se cifrará utilizando un algoritmo de cifrado fuerte y se agregará '. exx' a su nombre original, después decodificar, Ransomware Exx envía una nota de rescate.

Sin embargo, llevan a cabo cada acción por su cuenta, directamente cada víctima se selecciona a mano y el patrón utilizado para atacar a la víctima incluye el nombre de la empresa en un código "cifrado". En este sentido, recordamos el famoso atentado ocurrido en Brasil hace unos meses, en este ataque, el sistema cifrado fue un entorno virtualizado.

Historia de RansomExx

Defray era el nombre original de RansomExx cuando apareció por primera vez en 2018. Luego de una serie de ataques a instituciones destacadas, incluido el Departamento de Transporte de Texas, el grupo permaneció en gran parte desconocido durante algunos años antes de volverse conocido a mediados de 2020. Alrededor de este tiempo, la operación de ransomware cambió su nombre a RansomExx. (Sertecompsa, 2023).

Solo los sistemas Windows fueron los objetivos iniciales de RansomExx. Pero en julio de 2020 se identificó una nueva variante de RansomExx Linux. Aunque la versión de Linux compartía muchas características con el primer sistema operativo Windows, estaba rezagada con respecto a su predecesor al tener fallos en la transmisión de datos concernientes al comando y control, estrategias y la habilidad de bloquear los procesos en ejecución. En diciembre de 2020, RansomExx lanzó un sitio web de filtraciones en la web oscura donde la empresa pública los datos robados de las víctimas que se niegan a pagar el rescate. (GlobalSuites, 2022).

Desde que se descubrió RansomExx por primera vez, se han recibido trescientos cuarenta y seis envíos a ID Ransomware, una herramienta en línea que ayuda a las víctimas a identificar el ransomware que ha cifrado sus archivos. Si nuestra estimación de la tasa de envío de víctimas, que es solo del 25 %, es correcta, es posible que haya habido un total de mil trescientos ochenta y cuatro incidentes de RansomExx desde la creación del ransomware. (Kaspersky, 2023).

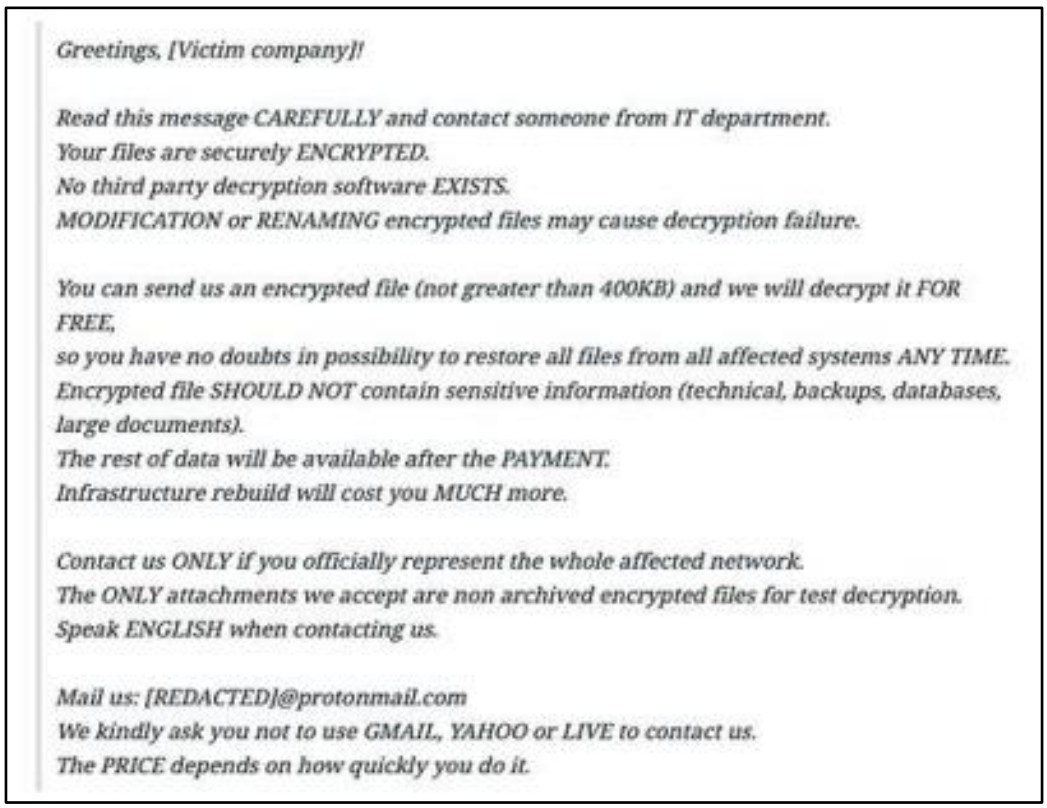
Nota de rescate de RansomExx.

Una vez que finaliza el proceso de cifrado, RansomExx envía una "nota de rescate" a cada directorio infectado. La nota informa al lector cómo ponerse en contacto con los atacantes y que los archivos de la víctima han sido encriptados. La nota también proporciona un descifrado gratuito de un archivo cifrado para demostrar la confiabilidad del descifrador proporcionado por el atacante. (Sertecompsa, 2023).

Un ejemplo de una nota de rescate de Ransonexx se muestra en la Figura 1:

Figura 1.

Nota de Rescate de RansomExx



Greetings, [Victim company]!

Read this message CAREFULLY and contact someone from IT department.
Your files are securely ENCRYPTED.
No third party decryption software EXISTS.
MODIFICATION or RENAMING encrypted files may cause decryption failure.

You can send us an encrypted file (not greater than 400KB) and we will decrypt it FOR FREE,
so you have no doubts in possibility to restore all files from all affected systems ANY TIME.
Encrypted file SHOULD NOT contain sensitive information (technical, backups, databases, large documents).
The rest of data will be available after the PAYMENT.
Infrastructure rebuild will cost you MUCH more.

Contact us ONLY if you officially represent the whole affected network.
The ONLY attachments we accept are non archived encrypted files for test decryption.
Speak ENGLISH when contacting us.

Mail us: [REDACTED]@protonmail.com
We kindly ask you not to use GMAIL, YAHOO or LIVE to contact us.
The PRICE depends on how quickly you do it.

Nota: En esta figura se muestra un ejemplo de un mensaje de rescate de Ransomexx.

A quién se dirige RansomExx

Según Price Waterhouse and Coopers, PWC (2022), el RansomExx se dirige a grandes organizaciones, como empresas y agencias gubernamentales que tienen los medios y el deseo de satisfacer una demanda de rescate considerable a cambio del descifrado de sus datos. Uno de los pocos programas de ransomware que ataca los sistemas basados en Linux y Windows se llama RansomExx. Las organizaciones en las Américas, Asia, Europa y Oceanía se han visto afectadas por RansomExx dejándolas varadas a nivel corporativo.

Propagación de RansomExx

Por lo general, los ataques de RansomExx comienzan infiltrándose en los sistemas de destino utilizando protocolos de escritorio remoto comprometidos, trucos de phishing, explotando vulnerabilidades conocidas o usando credenciales que han sido robadas, antes de que se publique el ejecutable del ransomware, los datos se extraen y se envían a un servidor que está bajo el control del atacante. (Samaniego, 2021).

Ransonexx por lo general, viene en forma de malware sin archivos. Debido a que se carga en la memoria automáticamente y se ejecuta sin tocar el disco, puede ser un desafío para las soluciones de seguridad detectarlo. Debido a que el ataque Ransonexx es tan meticuloso y manual, el plan de ataque específico de cada incidente puede diferir. (Malwarebytes, 2022).

Principales ataques de RansomExx.

La tabla 3, incluye una lista de algunas de las empresas a las que RansomExx ha perjudicado a nivel mundial, junto con el impacto en sus sistemas.

Tabla 3.

Principales Ataques de RansomExx

Nombre	Empresa	Ataque	Fecha
RasomEXX	Departamento de Transporte de Texas	Esta empresa se vio afectada por RansomExx, lo que provocó la interrupción del sitio web de la agencia y una serie de servicios. La organización emitió un comunicado anunciando que el incidente había sido aislado de inmediato y que el FBI lo estaba investigando.	Mayo 2020
RasomEXX	Konika Minolta	Una infección por RansomExx provocó que Konica Minolta, una empresa japonesa de fabricación de tecnología con más de 40 000 empleados, experimenta interrupciones en el servicio durante casi una semana. Los clientes no pudieron	Julio 2020

		durante este tiempo. Se puede acceder a algunas impresoras Konica Minolta, así como al sitio web de soporte de la empresa "Error de notificación de servicio" se mostró como mensaje de error.	
RasomEXX	Gigabyte	Un ataque de Ransonexx ocurrió al fabricante de hardware informático taiwanés Gigabyte. El incidente provocó la caída de parte del sitio web de Gigabyte, sin embargo, los sistemas de producción de la empresa no se vieron afectados. A menos que la empresa pagara el rescate exigido por los atacantes, amenazaron con publicar 112 GB de los datos robados.	Julio 2022
RasomEXX	CNT	Una forma de malware o virus conocida como ataques ransomwarexx en CNT restringe el acceso de los usuarios a sus sistemas o archivos y requiere que soliciten recuperar el acceso. Sin embargo, Maino afirmó que, en el caso de CNT, el ataque afectó directamente a los sistemas de TI internos, incluida la facturación, la activación y los cobros.	Julio 2020

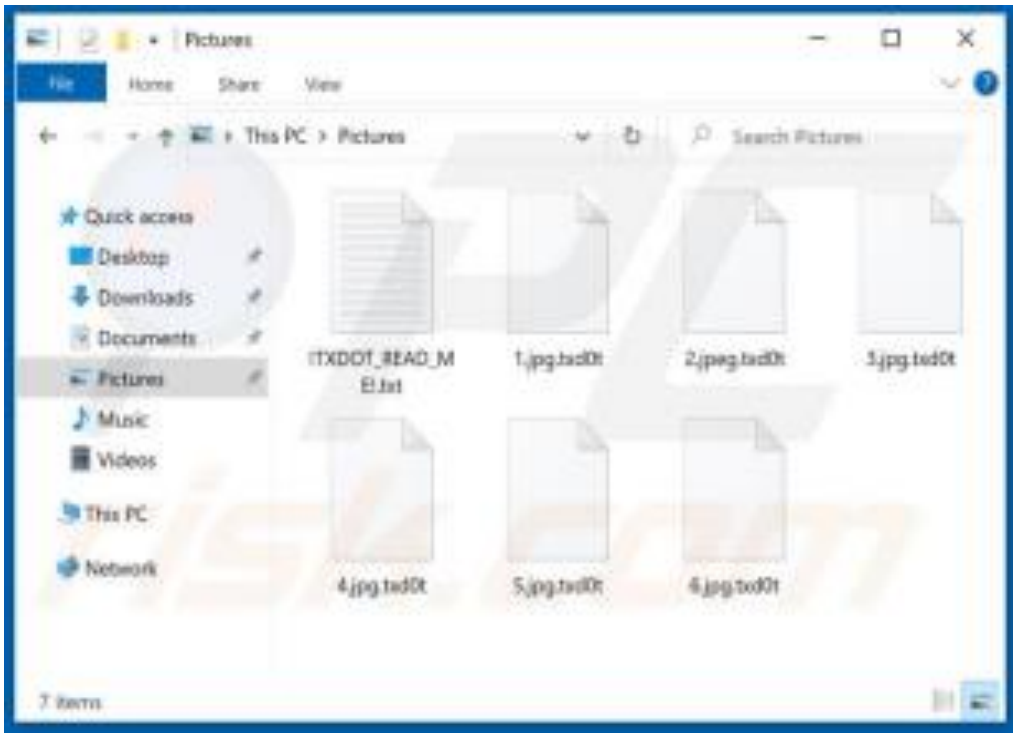
Nota: El malware se puede categorizar de varias maneras, por lo que se han creado tres grupos para una mejor comprensión. Adaptado de: Emsisoft (2022).

Cómo eliminar RansomExx

RansomExx actualmente utiliza un método de cifrado que hace que sea imposible descifrar datos sin pagar las herramientas de descifrado proporcionadas por los atacantes. (Puodzius, 2021).

Figura 2.

Ransomware RansomExx - Desencriptado, eliminación y recuperación



Nota: El gráfico representa como se desencripta la información, así como también se elimina y se recupera en un ataque de Ransomexx.

Para restaurar sus sistemas a partir de copias de seguridad, las víctimas de RansomExx deberían estar listas para hacerlo. Estos procedimientos deben describirse en el plan de respuesta a incidentes de la empresa. (Microsoft, 2020).

Se recomiendan las siguientes acciones:

- Tome medidas para contener la amenaza.
- Determinar la extensión de la infección.
- Identificar la fuente de la infección.
- Recolectar evidencia.
- Restaurar el sistema desde la copia de seguridad.
- Identificar, fortalecer las vulnerabilidades y reducir el riesgo de incidentes recurrentes.

¿Quiénes son las víctimas del RansomEXX?

Según Bestuzhev (2021), en Estados Unidos, Brasil, Francia, Ecuador, Indonesia y los gobiernos de otras naciones, la aviación civil, las instituciones educativas y la industria pesada son solo algunas de las víctimas.

Detección y protección

Los ataques de ransomware dirigidos y el grupo RansomEXX son complicados y no deben tratarse sólo como un problema de malware como mencionamos en el artículo, los atacantes con frecuencia se basan en componentes de red que están inaccesibles de protección por las defensas convencionales.

Sin embargo, para detectar las operaciones de Ransomware dirigidas, se pueden encontrar desde el principio con la ayuda de una serie de herramientas y técnicas, es decir antes de la fuga de datos de la red y antes del cifrado de datos.

Según Sharma (2022), estas son algunas de las recomendaciones a implementar, para hacer frente a estos ataques:

- Enrutadores que están parcheados, así como otro hardware de red como puertas de enlace VPN.
- Instale un sistema EDR en la red, revise las alertas recibidas y tome las medidas necesarias. Luego puede concentrarse en detectar el movimiento lateral dentro de la red.
- En los servidores conectados a Internet, deshabilite el protocolo RDP.
- Habilite la autenticación ssh usando certificados en lugar de solo contraseñas para servidores Linux que están conectados a Internet.
- Actualizar responsable y permanentemente todos los sistemas, dando prioridad a aquellos que están expuestos a Internet.
- Habilite Sysmon en las máquinas para enviar los eventos a un correlacionador de eventos y procesar los eventos con las reglas Sigma.
- Escanee los sistemas utilizando las reglas de Yara de forma regular para buscar anomalías y acciones de actores que ya conoce.
- Vuelca las imágenes de la memoria RAM para que las examinen los sistemas de análisis de similitud de código. Por ejemplo, KTAE de Kaspersky.
- Ser capaz de ver el DNS y los proxies de la empresa para detectar conexiones a centros de comando y control y exfiltración de datos.
- Si la empresa utiliza un proxy, aplicarle las reglas de Suricata dentro del tráfico de la red, detectar los patrones de los actores de ataque.

- Para controlar las solicitudes de DNS de la red interna a Internet, use fuentes de inteligencia sobre IP y reputación de dominio.
- Utilice un administrador de tráfico de red con una interfaz visual que le permita darse cuenta fácilmente cuando aumenta la cantidad de tráfico saliente. Bueno, la relación natural entre el tráfico entrante y el tráfico saliente cambia inmediatamente cuando se filtra la información. Estas anomalías actúan como una señal de advertencia para continuar con una Caza de Amenazas.
- Realizar trabajos de Threat Hunting 3 o 4 veces al año le permitirá detectar a los atacantes antes de que lleguen a su punto de finalización.
- Exx es el nombre que recibe otro criptovirus. Exx acaba de unirse a la escena del ransomware. Es un programa malicioso que daña la configuración de seguridad principal del sistema y deja al PC extremadamente vulnerable a nuevos ataques de malware, otro objetivo de la corrupción de la seguridad del sistema es el cifrado de datos importantes.

Se recomienda a las víctimas del ransomware Exx que no se pongan en contacto con delincuentes en línea; no confíe en ellos porque solo empeorarán su mala situación al robarle su dinero y no brindarle una solución de descifrado.

Los kits de explotación, los ataques multicapa, el malware o las campañas de phishing son las formas más comunes en que se propaga el ransomware cuando se lanza un ransomware, normalmente reconoce los archivos y datos de los usuarios y los encripta utilizando una lista integrada de extensiones de archivo.

Además, está programado para evitar ciertas carpetas del sistema (como la carpeta del sistema Linux y algunas carpetas de archivos de programa) para mantener la estabilidad del sistema y pagar el rescate una vez que finaliza la descarga. Se cifran los archivos de la ubicación especificada que coincidan con cualquiera de las extensiones de archivo enumeradas, de lo contrario, el archivo no se modificará; después de cifrar los archivos, el ransomware exige con frecuencia el pago en forma de nota de rescate. (Ivanova, 2021)

Cómo proteger la red de RansomExx

Acorde a Emsisoft (2022), las organizaciones pueden disminuir su riesgo de incidentes de Ransomexx implementando los siguientes procedimientos:

- Capacitación de concientización sobre seguridad cibernética: las organizaciones deben implementar programas de capacitación destinados a educar a los usuarios finales sobre los fundamentos de la seguridad cibernética porque la mayoría de las infecciones de ransomware son causadas por acciones iniciadas por el usuario. Para garantizar que los usuarios finales estén preparados para las amenazas actuales, la capacitación debe

ser un proceso continuo. El ransomware y sus técnicas de distribución cambian constantemente.

- Autenticación multifactor (MFA): MFA agrega una capa adicional de seguridad para ayudar a evitar el acceso no autorizado a cuentas, herramientas, sistemas y repositorios de datos. Cuando sea práctico, las organizaciones deberían pensar en habilitar MFA.
- Parches de seguridad: para reducir la ventana de oportunidad de un ataque, las organizaciones de todos los tamaños deben tener una sólida estrategia de administración de parches que garantice que las actualizaciones de seguridad se apliquen lo antes posible a todos los puntos finales, servidores y dispositivos.
- Dado que muchas cepas de ransomware pueden propagarse lateralmente a través de la red y cifrar las copias de seguridad almacenadas localmente, las organizaciones deben usar una combinación de copia de seguridad de almacenamiento de medios y copias de seguridad tanto dentro como fuera del sitio. Las copias de seguridad son una de las formas más efectivas de reducir el impacto de un incidente de ransomware.
- Fortalecimiento del sistema: para minimizar el área de superficie expuesta a vulnerabilidades y administrar posibles vulnerabilidades de seguridad, es esencial fortalecer las redes, los servidores, los sistemas operativos y las aplicaciones. Deshabilitar servicios como PowerShell, RDP, Windows Script Host, macros de Microsoft Office y otros innecesarios y potencialmente explotables. reduce el riesgo de infección inicial, mientras que la aplicación del principio de privilegio mínimo puede ayudar a prevenir el movimiento lateral.
- Deshabilitar macros: muchas familias de ransomware se distribuyen a través de documentos de Microsoft Office o PDF que tienen macros incrustados. Las empresas deben evaluar cómo usan las macros, pensar en bloquearlas todas de Internet y solo permitir que las macros examinadas y aprobadas se ejecuten desde fuentes confiables.
- Autenticación de correo electrónico: las empresas pueden utilizar una variedad de métodos de autenticación de correo electrónico, incluidos marcos de políticas de remitentes, autenticación de mensajes basada en dominio, detección de suplantación de identidad de correo electrónico y correos electrónicos que han sido identificados como compatibles.
- La segregación eficaz de la red ayuda a contener los incidentes, detiene la propagación del malware y reduce la interrupción general del negocio.
- Los sistemas de monitoreo de red deben estar implementados para empresas de todos los tamaños a fin de vigilar los posibles canales de salida de datos y reaccionar rápidamente ante cualquier actividad sospechosa.
- Las pruebas de penetración pueden ser útiles para identificar debilidades en la infraestructura de TI y la susceptibilidad de los empleados al ransomware.

- Plan de respuesta a incidentes: las organizaciones deben tener un plan completo de respuesta a incidentes que especifique en cada situación con precisión qué hacer en caso de una infección. Una respuesta rápida puede reducir la interrupción, detener la propagación de malware, y garantizar que el incidente sea manejado de la manera más efectiva posible.

Según Emsisoft (2022), la tabla 4 muestra las etapas típicas de un ataque de Ransomware.

Tabla 4.

Fases típicas en un Ataque de Ransomware

Número	Fase
1	Contagio. Cuando el Ransomware se entrega a un sistema a través de un archivo adjunto de correo electrónico (generalmente phishing, aplicaciones infectadas o algún otro método), el Ransomware se propaga a la computadora de la víctima y a todos los dispositivos de red a los que no tiene acceso
2	Intercambio seguro de claves. El Ransomware se conecta a los servidores de comando y control operados por los ciberdelincuentes detrás de los ataques para generar claves de cifrado para usar en los sistemas locales.
3	Cifrado. También encontrará que el Ransomware comenzará a cifrar todos los archivos que encuentre en su computadora y redes locales
4	Extorsión. Una vez cifrado, el Ransomware muestra instrucciones para pagar un rescate por el sistema o los datos afectados y advierte al usuario que los datos se eliminarán si el pago no se realiza dentro del tiempo especificado destruido.
5	Desbloqueo Las organizaciones y los usuarios pagan el rescate, eliminan los archivos y sistemas infectados de sus redes y restauran los datos a partir de copias de seguridad limpias con la esperanza de que los ciberdelincuentes puedan descifrar o restaurar los archivos infectados

Nota: Esta tabla muestra las fases típicas en un ataque de ransomware. Tomado de: Emsisoft (2022)

¿Qué es una máquina virtual?

Acorde a Ramírez (2016), una máquina virtual (VM) es un entorno virtual que simula un sistema informático virtual y tiene su propia CPU, memoria, interfaces de red y almacenamiento, pero se basa en hardware físico interno o externo. Los recursos de la máquina se separan del

sistema de hardware y se hacen accesibles a las máquinas virtuales mediante un sistema de software conocido como hipervisor.

Las máquinas host, las computadoras host, los sistemas operativos host o simplemente hosts son máquinas físicas que tienen hipervisores, como máquinas virtuales basadas en kernel (KVM) y otras máquinas virtuales. Las computadoras invitadas, los sistemas operativos invitados o simplemente invitados se encuentran entre las diversas máquinas virtuales que hacen uso de ese recurso. El hipervisor utiliza recursos informáticos como CPU, memoria y almacenamiento como grupos de medios para que las nuevas máquinas virtuales o los invitados existentes puedan compartir fácilmente estos recursos. Una sola pieza de hardware puede admitir varias máquinas virtuales, pero la máquina virtual está aislada del resto del sistema.

La experiencia del usuario final simulado dentro de una máquina virtual es casi idéntica al sistema operativo en tiempo real que se ejecuta en la máquina física porque las máquinas virtuales le permiten ejecutar varios sistemas operativos diferentes en la misma computadora a la vez.

Virtual box

Para garantizar que sea compatible con todos los sistemas operativos físicos, incluidos Windows, Mac OS y Linux, es una aplicación de servidor y cliente multiplataforma. También es compatible con las tecnologías de virtualización VT-x y AMD-v, lo que le permite definir y cambiar los dispositivos de hardware necesarios para la máquina virtual. Red, disco duro, número de núcleos y procesadores dedicados, tamaño de RAM, dispositivos de entrada y salida de audio.

Sandbox

El sandbox está pensado como un duplicado del área operativa de los ordenadores de sobremesa, portátiles y otros equipos informáticos. El sandboxing se encarga de apartar un programa en un entorno diferente cuando se utiliza un programa o una aplicación en un entorno distinto. Cuando surge un problema de seguridad, el sandbox funciona realmente de forma independiente, simulando un sistema operativo y defendiendo las estaciones de trabajo y la red. La única distinción es que el servicio sandbox no tiene acceso a la red completa (Romero, 2021).

Mediante el uso de las siguientes características, todas las aplicaciones que se ejecutan en un sandbox lo hacen de forma regulada:

- Reciben una asignación de espacio en disco. Cualquier espacio de disco que no haya sido asignado a estos programas será inaccesible para ellos.

- Para mantener nuestros programas separados del resto del sistema operativo, podemos hacer que operen en un sistema de archivos temporal.
- También se les asigna un espacio de memoria. Otras regiones de memoria que no han sido asignadas a los programas no serán accesibles para ellos.
- Podemos concederles acceso y control sobre las consultas en el almacenamiento externo, o podemos restringirlo.
- Limitamos su acceso a la máquina anfitriona para su inspección.

Utilidad de Sandbox

Se puede deducir que su propósito principal es permitir a los usuarios ejecutar programas sin riesgo y sin poner en peligro el resto del sistema operativo. (Carles, 2017)

Se puede utilizar un sandbox en las siguientes situaciones, como ejemplo:

- Instalar y utilizar de forma segura aplicaciones que no son fiables o pueden estar contaminadas con malware.
- Utilizar aplicaciones como un navegador web, Skype, un lector de PDF, un keygen descargado de internet, etc. que tienen la capacidad de poner en peligro la seguridad del sistema operativo.

1.2. Proceso investigativo metodológico

El proceso metodológico a emplear es exploratorio, bibliográfico, experimental.

Se utiliza el método exploratorio para encontrar una visión general del problema este tipo de investigación al ser poco estudiada, por lo que no se puede obtener una hipótesis exacta de este tema.

Se utiliza investigación bibliográfica histórica de acontecimientos o hechos suscitados en otros lugares, de tal forma se pueda extraer la mayor cantidad de información posible.

La investigación experimental se lleva a cabo en este proceso ya que se realizará pruebas y se comparará variables a fin de determinar las causas y efectos de este Ransomware exx.

CAPÍTULO II ARTÍCULO PROFESIONAL

2.1. Resumen

Esta propuesta tecnológica se plantea con el objetivo de realizar una descripción del ataque del Ransomware EXX ya que es una de las nuevas amenazas a las que están expuestos los sistemas de información sean estos empresariales o personales. El Ransomware EXX se infiltra en el sistema de la víctima con métodos inteligentemente diseñados y encripta los archivos que se encuentran en el sistema después del proceso de encriptación, el atacante deja un mensaje exigiendo un rescate en moneda virtual para abrir el acceso a los archivos cifrados y advierte que de lo contrario los archivos no podrán ser accesibles.

El escritorio de Linux, los dispositivos móviles, y las microcomputadoras se exponen de la misma manera a la fuga de información y apropiación indebida de datos, poniendo en peligro la seguridad personal o de las empresas. El Ransomware Ransonexx ha ido evolucionando y su principal método de propagación es la ingeniería social.

Este estudio presenta un caso de infección con ransomware exx en un ambiente controlado, utilizando sandbox y Ubuntu con el fin de establecer cuáles son los mecanismos de infiltración, propagación, encriptación de datos hasta llegar a la nota de rescate para la entrega de la clave de descifrado, para luego de esto establecer medidas de seguridad para salvaguardar la información.

Palabras clave: ransomware, seguridad, datos, empresa, pérdida.

2.2. Abstract

This technological proposal is proposed with the objective of making a description of the EXX Ransomware attack since it is one of the new threats to which information systems are exposed, whether business or personal. EXX Ransomware infiltrates victim's system with cleverly designed methods and encrypts files on system after encryption process, attacker leaves message demanding ransom in virtual currency to open access to recorded files and I warn that otherwise the files may not be accessible.

Linux desktops, devices, and microcomputers are just as exposed to mobile information leakage and data misappropriation, endangering personal or business security. Ransonexx Ransomware has been evolving and its main spread method is social engineering.

This study presents a case of infection with exx ransomware in a controlled environment, using sandbox and Ubuntu in order to establish competent are the mechanisms of infiltration, propagation, data encryption until reaching the ransom note for the delivery of the key decryption, and after that establish security measures to save the information.

Keywords: ransomware, seguridad, datos, empresa, pérdida.

2.3. Introducción

El avance del mundo digital y de la información hace de los datos el activo más valioso en este momento; la protección de datos y seguridad se vuelven necesarios a partir de varias amenazas tales como daños, desastres naturales y delitos cibernéticos. Los ataques de ciberdelincuentes han utilizado virus Ransomware y para este caso Ransonexx en los últimos años para obtener beneficios, usa criptografía para cifrar archivos en la computadora comprometida, evitando que los usuarios accedan a ellos (Romero et al., 2018).

Es el ransomware más común, moderno y efectivo, y aunque se puede eliminar fácilmente de una computadora, la información que se ha visto comprometida es muy difícil de volver a recuperar y en su mayor parte, imposible de restablecer. Por lo general, intenta atacar las extensiones de archivo que son de interés para el usuario, como archivos de oficina, archivos multimedia, bases de datos, etc.

La gran cantidad de información que ahora manejan los medios informáticos y el gran alcance de conectividad que vivimos en estos momentos, han hecho que gente inescrupulosa con propósitos ilegítimos se especialicen en estas actividades vayan en busca de información confidencial, con el propósito de quebrantar el derecho a la privacidad y cobrar un rescate por la información comprometida (CEPAL, 2018).

Este contexto ha dado lugar a la exigencia de establecer procedimientos y herramientas que nos permitan protegernos de este tipo de amenazas, que nos permitan reducir y mitigar el riesgo de estos ataques, de esta premisa nace la necesidad de comprender cómo actúan los ransomware y lograr establecer todas las posibles acciones, para evitar sus efectos, es por esto que este trabajo está orientado a estimar el impacto real que tiene de forma cuantitativa y cualitativa, se realizaron algunos estudios, de análisis de Ransomware Ransonexx a través del tiempo de ejecución y métodos para identificar características detalladas de análisis de actividad y patrones de red contra el virus usando análisis a través del tráfico características de las redes móviles Android.

Este estudio utiliza ambiente de simulación para el Ransomware Ransonexx, que puede propagar infecciones y encriptar datos simultáneamente. Las características son destructivas al propagarse rápidamente a través de las redes informáticas después de la ejecución, apuntando a todos los datos encriptados y habilitando el proceso, basados en estas características, los ataques pueden propagarse en la computadora las redes se convierten en una grave amenaza, este estudio utiliza un entorno virtual para llevar a cabo el ataque, escenarios, y redes de monitoreo contra Ransomware Ransonexx. El proceso de construcción de un entorno controlado que utiliza el software VirtualBox permite la virtualización de

computadoras y es la forma más sencilla de analizar un archivo malicioso y ejecutarlo en un entorno controlado para observar los resultados, la utilización de entornos virtuales se hace vital importancia, ya que permite la recuperación casi instantánea del estado inicial de la máquina.

2.4. Metodología

El proceso metodológico a emplear exploratorio, bibliográfico, experimental.

Se utiliza el método exploratorio para encontrar una visión general del problema este tipo de investigación al ser poco estudiada, por lo que no se puede obtener una hipótesis exacta de este tema, se utiliza investigación bibliográfica histórica de acontecimientos o hechos suscitados en otros lugares, de tal forma se pueda extraer la mayor cantidad de información posible, la investigación experimental se lleva a cabo en este proceso ya que se realizará pruebas y se comparará variables a fin de determinar las causas y efectos de este Ransomwarexx.

En cuanto a la metodología de desarrollo planteada a lo largo de este artículo científico se detalla los siguientes puntos:

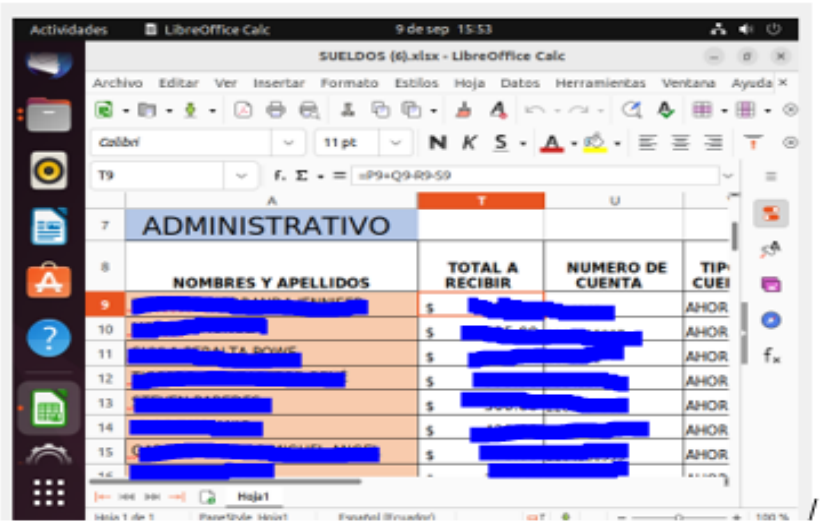
Identificación de Evidencias.

Para el desarrollo de la propuesta se planteó un escenario en dónde un servidor principal aloja información relevante, en este caso se incluye nómina de pagos y otros archivos.

Como primera instancia se puede observar que en el servidor FTP se puede acceder sin problemas a la información detallada, tal como se lo muestra en la Figura 3.

Figura 3.

Nómina de pago

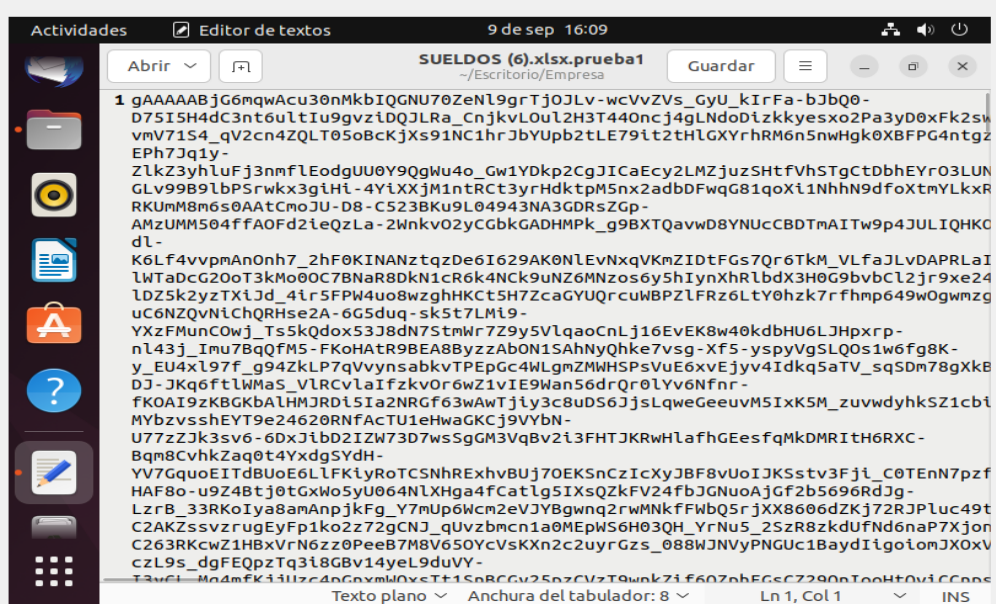


Nota: Nómina de pago, elaborado por autor

Y como parte del laboratorio se diseñó un script de Ransomware exx, el cual al ejecutarse encriptará la información de los archivos, secuestrando la data y posteando una nota de rescate tal como se lo muestra en la Figura 4 y 5

Figura 4.

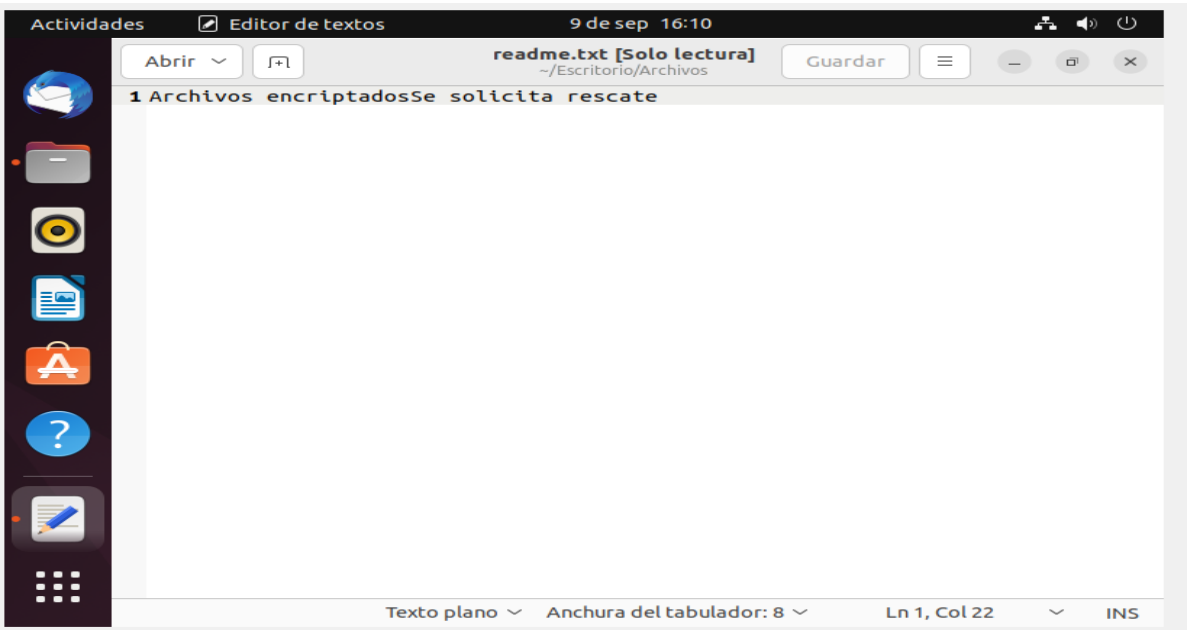
Archivos encriptados



Nota: Nómina, elaborado por autor.

Figura 5.

Nota de Rescate

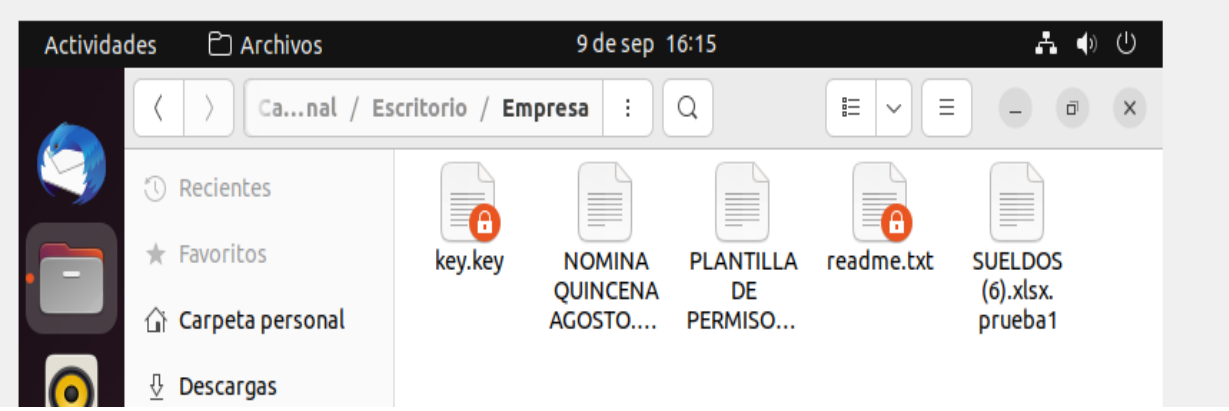


Nota: Aviso de rescate, elaborado por autor

Asimismo, se muestra la modificación de la extensión de los archivos atacados, en este caso se le agregó como extensión. prueba*1*, lo que nos demuestra el accionar de este incidente el cual de acuerdo a su teorización se basa no solo en la encriptación de la información sino también en el cambio de las extensiones de los archivos como se lo refleja en la Figura 6, acción que provoca una confusión al usuario.

Figura 6.

Modificación de la extensión



Nota: Modificación de extensión, elaborado por autor

Adquisición y preservación de las evidencias.

A través de la cadena de custodia, se da un registro detallado de la evidencia, en esta se detallan todos los vinculantes en el proceso: personal responsable, actividades que se realizan, y sobre todo el estado en el que se encuentra la evidencia, se sobreentiende que el registro no altera ni vulnera la evidencia, sino que ayuda a conocer el escenario en que se dieron los hechos y quienes tuvieron la responsabilidad en ese momento.

La finalidad del documento es que la evidencia sea segura, se pueda mostrar la identidad, fidelidad y registro que ayude con la continuidad de la prueba, la cual se da inicio en el momento de la obtención de la información hasta que finalice la etapa probatoria.

Para que la cadena de custodia cumpla con todos los parámetros requeridos, el documento emitido debe presentar todos los datos incluyendo nombre de personas, fecha de la evidencia, situaciones y actividades presentadas, y los requerimientos que el caso suscitado requiera.

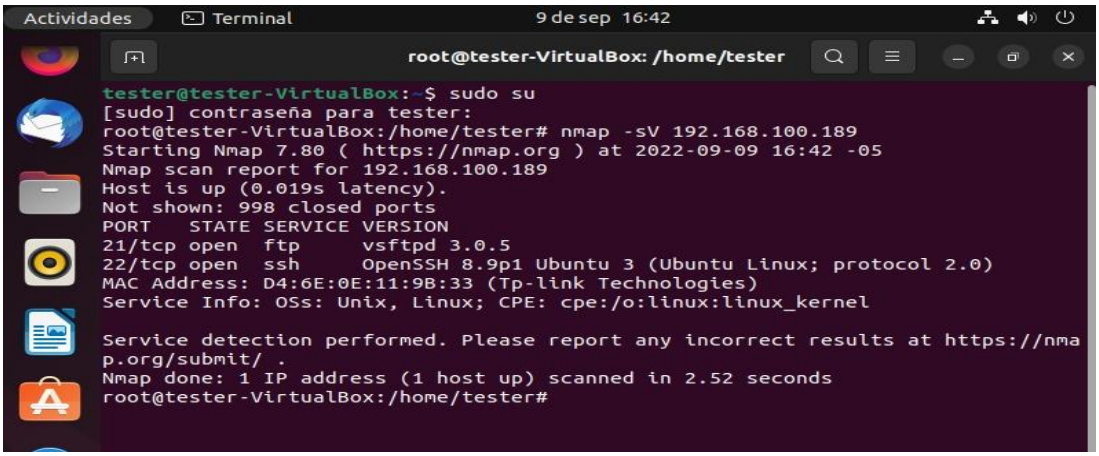
Análisis de evidencias.

Con todos los pasos previamente ingresados y basados en la conceptualización del ataque es irrefutable que la integridad de la información del servidor se vio comprometido debido a un Rasomware y por ende, el enfoque del análisis se centrará en la detección de cómo se realizó el ataque, para esto se realizará como prueba principal un escaneo de puertos al

servidor FTP, para esto se utilizó un servidor de tipo tester y mediante un escaneo de puertos se buscará la manera en la que el virus se filtró, tal como se lo muestra a continuación en la figura 7.

Figura 7.

Escaneo de puertos del servidor

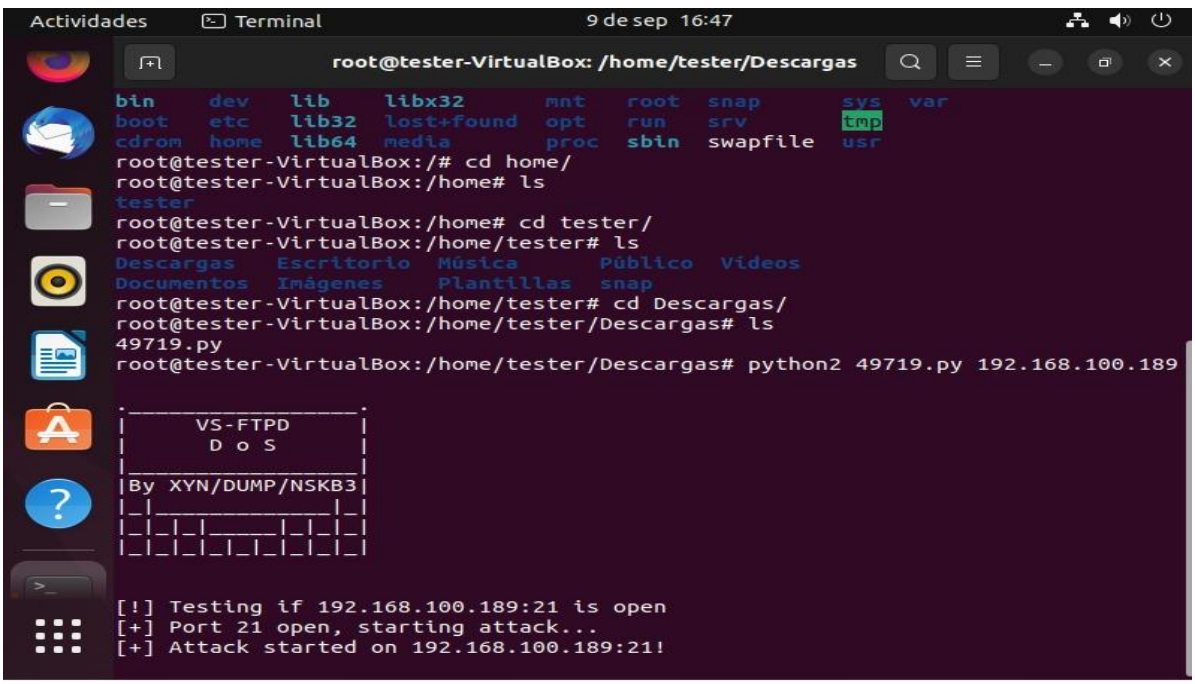


Nota: Escaneo de puerto, elaborado por autor

Y para comprobar las vulnerabilidades se realizaron pruebas y para esto se utilizaron metasploits, tal como se lo muestra en la Figura 8.

Figura 8.

Comprobación de la vulnerabilidad del servidor



Nota: Escaneo de puerto, elaborado por autor

Y ya, partiendo del análisis obtenido por el escaneo de puertos, lo que muestra que este servidor presenta una gran brecha de seguridad tanto en los puertos 21 y 22 lo que implica que ataques de tipo Backdoor pueda comprometer la integridad del equipo, y lo que finalmente conlleva al análisis del problema sumamente delicado, el cual se basó en la corrupción y secuestro de información privada. Entre los patrones identificados podemos observar que los archivos se encuentran corrompidos ya que estaban cifrados y la extensión de los archivos no es el original que es xlsx, al querer acceder a la nómina tuvo inconvenientes para manejar tal información, los archivos se encontraban comprometidos y además se encontraba una notificación de rescate, fuimos víctima de un Rasomware y al realizar el levantamiento de información respectivo, se comprobó que el servidor presenta grandes vulnerabilidades tanto en los puertos SSH y FTP, por lo que la PC se vio infectada a través de un backdoor, por lo que esto concuerda que el ataque haya pasado desapercibido.

2.5. Resultados – Discusión

Dentro de los resultados obtenidos en la presente investigación, el objetivo uno abarcaba la revisión documental de la evolución de los ataques Ransomware desde su aparición hasta la actualidad desde una revisión documental que incorpore casos de estudio. En este sentido, los principales hitos sobre la aparición de este evento, el ransomware ha establecido su capacidad para interrumpir cualquier empresa o comunidad, independientemente de su tamaño o nivel de seguridad, y se ha convertido en una de las herramientas más conocidas utilizadas por los ciberdelincuentes.

1989 PC Cyborg: Troyano que reemplazaba el archivo AUTOEXEC.BAT, luego ocultaba los directorios y cifraba los nombres de todos los archivos de la unidad C, haciendo inutilizable el sistema. Por último, le solicitaba al usuario “renovar su licencia” con un pago de 189 dólares a una casilla de correo a nombre de PC Cyborg Corporation.

2005 GPCoder: Cifraba archivos con extensiones específicas, cómo documentos e información del usuario (xls, doc, txt, rtf, zip, rar, dbf, htm, html, jpg, db, etc.). Luego dejaba un archivo de texto en el escritorio con las instrucciones al usuario para el pago del rescate a cambio del programa y la clave para descifrar los archivos.

2010 WinLock: Bloqueaba el equipo y desplegaba un mensaje en la pantalla, donde solicitaba al usuario enviar una cantidad de SMS Premium para desbloquearlo.

2012 Reveton: También conocido como el “virus de la policía”, que también bloqueaba el acceso al equipo, pero esta vez desplegando una pantalla con un falso mensaje de la policía nacional, o incluso del FBI. En esta pantalla le indicaba al usuario que el equipo había sido bloqueado por contener material ilegal, como pornografía infantil, software pirata o contenido con derechos de autor, por lo que debía pagar una “multa” para restaurar el acceso normal.

2013 CryptoLocker y CryptoWall: Ransomware criptográfico que se caracterizó por utilizar cifrados asimétricos con clave pública RSA de 2048 bits; cifrar únicamente extensiones específicas de archivos de documentos, fotos e información del usuario; utilizar conexiones anónimas con el controlador del atacante a través de TOR; y ser uno de los primeros en solicitar el pago del rescate en bitcoins.

2015 CTB Locker: Con un comportamiento similar a Cryptolocker, se propagaba a través de un troyano que al ser ejecutado descargaba el código malicioso que cifraba los archivos del usuario. Asimismo, supo manejar muy bien su credibilidad, ofrecía al usuario la posibilidad de descifrar de manera gratuita hasta cinco archivos para demostrar que podían ser recuperados.

2017 WannaCryptor: Se volvió popular bajo el nombre de WannaCry (en español “quieres llorar”), cifra los archivos del equipo infectado utilizando una combinación de los algoritmos AES-128 y RSA-2048, lo cual hace imposible su recuperación mediante técnicas de análisis. Sin embargo, lo que convirtió al ataque en algo realmente escandaloso fue su capacidad de propagarse por sí mismo, de manera similar a un gusano, a través de las redes de los equipos infectados, utilizando una vulnerabilidad en el protocolo de archivos compartidos de Windows.

2019 JSWorm: Fue descubierto en 2019, y a lo largo de su historia sus diversas subespecies han ganado notoriedad bajo varios nombres como Nemty, Nephilim y Offwhite, dentro de cada variante "renombrada", se lanzaron otras versiones con diversos grados de cambios de código, diferentes nombres de extensión de archivo, diferentes esquemas de cifrado y diferentes claves de cifrado.

JSWorm 4.0.3 esta es una versión mejorada y actualizada de JSWorm que intenta corregir errores encontrados en variantes anteriores, esta muestra contiene un escaneo de idioma de la computadora infectada. RU (ruso), BE (bielorruso), UZ (uzbeko), KY (kirguís), TG (tayiko), TK (turcomano), KK (kazajo), UK (ucraniano), el cual pude ser para evitar el cifrado de datos en los sistemas que usan este tipo de idiomas.

Nemty 1.4 Los cambios de código entre JSWorm y Nemty son significativos lo que sugiere que el autor del malware pudo haber reescrito el troyano desde cero. Esto puede ser para contrarrestar los intentos de descifrado anteriores que permitieron a las víctimas de varias variantes de JSWorm recuperar sus datos sin pagar una tarifa.

Este ejemplo también se desarrolló en C++ y se compiló con MS Visual Studio. Implementa un pequeño truco anti-análisis que consiste en un algoritmo de ofuscación de cadenas. Las cadenas (por ejemplo, el nombre y el contenido de la nota de rescate, la clave pública RSA, la URL de pago, etc.) se cifran mediante la clave codificada 'fuckav' y el método

de flujo RC4 codificado en Base 64.

2020 Nefilim: En de marzo de 2020, los desarrolladores cambiaron el nombre del troyano a Nephilim. Cuando aparecieron las primeras variantes de Nephilim, el modelo de distribución de la familia ya había cambiado. Los desarrolladores han cambiado del esquema RaaS público utilizado por las variantes de JSWorm y Nemty a colaboraciones privadas con afiliados con el propósito de "cazar mayor". Los actores de amenazas han comenzado a apuntar a víctimas de alto perfil y a manipular manualmente sus redes para extraer datos confidenciales y amenazar con exponerlos a la intimidación.

Todas las funciones auxiliares, como la finalización del proceso, la eliminación de instantáneas, la comunicación C&C, etc., se han eliminado del código troyano. El troyano se transforma en un binario de un solo propósito que se usa solo para el cifrado de archivos y, si se desea, todos realizan la acción.

Nefilim, como Nemty, fue desarrollado en C++ y compilado con MS Visual Studio. La duplicación de código entre Nemty (2+) y las versiones más nuevas de Nefilim es tan significativa que probablemente se desarrollaron a partir del mismo código fuente.

Fusion: Esta variante de troyano está escrita en el lenguaje de programación Go. Como se mencionó anteriormente, se desarrollaron en C++. Esto significa que ha sido completamente reescrito desde cero, posiblemente por otro desarrollador.

Sin embargo, las similitudes en el modus operandi general del malware, el esquema de cifrado, la nota de rescate coincide con sus predecesores y el hecho de que el binario está firmado sugieren que esta muestra es una nueva variante de la familia JSWorm.

Además, las direcciones por donde se produjo la fuga de datos cifrados en el cuerpo del troyano son las mismas que las utilizadas anteriormente por estos actores

2021 Milihpen: En las variantes de Milihpen, los actores detrás de la familia JSWorm reescribieron completamente el código del malware o contrataron a otro desarrollador para implementarlo desde cero. Nuevamente,esta versión se desarrolló en C++ (como Nephilim y sus variantes anteriores) y no en Golang (como Fusion).

Sin embargo, la funcionalidad principal, el flujo de ejecución, el esquema de cifrado y la dirección de la página de salida de datos permanecen intactos. El nombre del troyano también indica una conexión con una de las primeras variantes del malware, ya que la palabra "Nephilim" se escribe al revés.

El troyano ahora registra todas las acciones en la consola. Esto facilita que los operadores de malware controlen el proceso de infección**.**

2021 Gangbang: La cepa Gangbang es idéntica a Milihpen y actualmente es la última cepa encontrada en esta familia de ransomware. La diferencia más significativa es el hecho de que la composición de la configuración se almacena en cifrado AES con clave codificada e IV, y no en su forma pura, como en Milihpen. Además, a diferencia de las similares anteriores, la firma digital de esta muestra no es válida.

Las plataformas de ransomware como servicio (RaaS) han experimentado una de las revoluciones más recientes en los métodos de operación de los ciberdelincuentes, debido a esto, los grupos de atacantes menos calificados tienen la oportunidad de obtener acceso a una infraestructura completa y aprovechar las campañas de ransomware que ya están listas para funcionar, las plataformas también pueden cobrar a las víctimas una parte del rescate además de alquilar sus soluciones maliciosas. Según Pierre-Olivier Kaplan, el crecimiento de la sofisticación del malware también es el resultado de la popularidad de las plataformas de ransomware como servicio, a fines de 2010, el ransomware estaba en declive porque los pagos de rescate no eran seguros y podrían estar vinculados a redes criminales, las transferencias de dinero se han vuelto esencialmente "seguras" para los grupos atacantes gracias a la proliferación y el advenimiento de las criptomonedas, que permiten cierto anonimato en los pagos de rescate

La lista de ransomware ya es bastante larga, hasta el punto de que las autoridades francesas actualmente realizan un seguimiento de no menos de 120 familias de ransomware diferentes Ransomware parece ser una historia interminable. También se pueden anticipar nuevos tipos de amenazas cibernéticas con la aparición de nuevas tecnologías (Web3, NFT, movilidad autónoma), así como el resurgimiento de conflictos geopolíticos, por lo que desafortunadamente, la historia del ransomware está lejos de terminar.

Brechas de Seguridad

El ambiente de simulación evidencio las brechas de seguridad e incorporó la corrupción y secuestro de información privada, como es el caso de los roles de y otros archivos, entre los patrones identificados se encuentran que los archivos se encuentran corruptos ya que estaban cifrados y la extensión de los archivos no es el original que es xlsx.

Cabe destacar que ningún sistema de alerta dio aviso de este ataque lo que demuestra que no se cuenta con medidas de seguridad informática activas ya sea a nivel de firewalls, IDS (Sistema de detección de Intrusos) o IPS (Sistema de Protección de Intrusos). Adicionalmente, revisando los informes de trabajo se identifica que al querer acceder a la nómina el día anterior a la prueba, no tuvo inconvenientes para manejar tal información. Sin embargo, al aprobar los pagos se encontró con la novedad que los archivos se encontraban comprometidos y además una notificación de rescate.

Para este caso particular los ataques a los sistemas Linux, suelen implicar ataques de

fuerza bruta para obtener credenciales de acceso remoto (SSH) y la manipulación de aplicaciones web, otro tipo de ataque puedo haberse dado por phishing.

En los ataques de fuerza bruta, los piratas utilizan múltiples combinaciones de nombre de usuario y contraseña para obtener acceso a una cuenta de usuario o entorno informático. Casi todos los ataques de fuerza bruta de hoy en día para descifrar contraseñas son llevados a cabo por programas llamados bots, que pueden realizar tareas específicas de forma continua sin ayuda o intervención humana. La mayoría de estos ataques de descifrado de contraseñas son llevados a cabo por botnets, redes de bots que consisten en cientos o miles de computadoras infectadas con malware, que pueden ser controladas por un atacante.

Los mensajes de correo electrónico son la forma más fácil de transmitir Rasomware es a través de archivos adjuntos a los mensajes, y si el destinatario comete el error de ejecutarlo, se instala sobre el servidor y el intruso toma control sobre la computadora infectada, los servicios de Internet (HTTP, FTP, ICQ, chat, mensajería instantánea) son una vulnerabilidad crítica que puede descargar e infectar automáticamente los sistemas con troyanos de puerta trasera similares a los servidores FTP. El uso de servicios de mensajería instantánea como MSN Messenger, Yahoo Messenger, etc. pueden propagar infecciones entre usuarios conectados a la misma sesión.

Tomando en consideración los servicios necesarios para el desarrollo de las actividades, podemos detectar muchos posibles escenarios por donde se puede desplegarse un ataque por los siguientes puertos:

- Puerto 21: es utilizado por el protocolo de transferencia de archivos FTP.
- Puerto 22: lo usa el protocolo SSH para administrar computadoras remotas
- Puerto 23: lo usa el protocolo Telnet para administrar computadoras remotas (no seguras)
- Puertos 80, 8080, 8088, 8888 y 443: todos los puertos están orientados a la web que necesitamos para cerrarlos si no tenemos un servidor web y, de ser así, debemos monitorearlo adecuadamente para mitigar los ataques web que pueden ocurrir como inyección SQL, XSS y otros ataques.
- Puerto 4444: Protocolo simple de Network Pagging, este puerto suele ser utilizado por troyanos y malware en general, siempre se debe bloquear este puerto.
- Puertos 6660-6669: estos puertos son comúnmente utilizados por IRC, si no los usamos, no los abriremos.
- Puerto 161 UDP: lo utiliza el protocolo SNMP para ver configuraciones y administrar varios dispositivos, como enrutadores, conmutadores y servidores. Debe estar cerrado si no lo está utilizando.

- Puerto UDP 53: puerto utilizado por el protocolo DNS, este puerto se puede utilizar para auto filtrar información en consultas DNS.

Brechas internas

Vulnerabilidad física: una brecha de seguridad física es el control de acceso, muchas veces se tiene acceso a infraestructura crítica y no se tiene las credenciales correctas, cualquiera puede ingresar al Data Center y eso es un gran riesgo para la organización porque cualquier usuario puede entrar con un USB y copiar la información, también puede infectar la misma infraestructura.

Denegación de servicio distribuida (DDoS): los atacantes toman el control de una gran cantidad de dispositivos para formar una botnet y los utilizan para inundar un sistema de destino con tráfico, abrumando su ancho de banda y recursos del sistema. DDoS no es un medio directo para violar los sistemas organizacionales, pero puede usarse como una distracción mientras los atacantes cometen la violación real.

Protección de firewall fallida: los firewalls están diseñados para restringir el acceso a los recursos corporativos, pero también pueden ser objeto de ataques. Si aún tiene acceso a puertos y servicios de gestión de riesgos, los ciberdelincuentes pueden acceder a su red corporativa.

Uso no autorizado de la información: Muchos problemas de seguridad de datos se derivan de la falta de sistemas de control y políticas de acceso adecuadas. Esto significa que los empleados pueden, de forma intencionada o no, acceder a datos que no están autorizados a ver.

Vulnerabilidad de Configuración: Puede ser la configuración del sistema operativo por defecto o incluso de algunas aplicaciones de servidor abiertas, también puede ser la configuración de algunos cortafuegos que no están bien gestionados y la infraestructura perimetral, afecta directamente la infraestructura y el desarrollo de las operaciones.

Falla de Actualización de Sistema: El software obsoleto es un área de vulnerabilidad de la que pueden aprovecharse los piratas informáticos. Las actualizaciones y mejoras del sistema se realizan para optimizar la usabilidad o el diseño de un programa y para añadir nuevas funciones de seguridad.

Falta de capacitación del personal: La formación de los empleados es fundamental para evitar brechas de seguridad. Esta formación es necesaria tanto para los nuevos empleados como para los antiguos empleados. Esto es parte del proceso de reclutamiento de empleados para la empresa para evitar que los errores de los empleados se conviertan en un problema grave.

- **Brechas externas**

Ataques de ingeniería social: los atacantes manipulan a los usuarios o empleados para engañarlos y revelar datos confidenciales. Un sistema de ataque común es el phishing, donde los atacantes envían correos electrónicos o mensajes falsos para engañar a los usuarios para que respondan con información personal, hagan clic en enlaces a sitios web maliciosos o envíen archivos adjuntos maliciosos.

Password Craking: Este proceso de descifrado de contraseñas, utiliza un software especializado y un potente hardware informático, permite a los atacantes probar muchas combinaciones diferentes de contraseñas en un corto período de tiempo hasta que encuentran la adecuada para acceder a información confidencial**.**

Data Exfiltración (Filtración Externa de datos): Se refiere a una copia o transferencia no autorizada de datos fuera del dominio. Esto se puede llevarse a cabo manualmente como mediante código malicioso en la red.

Seguridad en la Red: El enfoque principal está en la protección, seguridad y confiabilidad de la red de transmisión de datos, como es de nuestro conocimiento la mayoría de las amenazas cibernéticas penetran a través de Internet y varias redes a las que están conectadas las computadoras de una organización. Es en este entorno donde se realizan la mayoría de los intentos de 'atrapar'.

Medidas preventivas ante los ataques por Ransomware.

Entre las principales medidas que se propone para prevenir los ataques de Ransomware, se identificaron las siguientes:

A nivel de Infraestructura y Software

Seguridad de la Red: Por el lado de la red, es posible implementar medidas de segmentación de red, proxis de comunicación, firewalls, sistemas de detección y prevención de intrusos, etc., pero esto ya conduciría a la formación de más capas externas en términos de servidores y estaciones de trabajo. Es muy arriesgo confiar toda la protección de los equipos a la protección perimetral, ya que, si se supera, nada protegerá al equipo, es decir, siempre se debe proteger a diferentes niveles de profundidad, una protección por capas de la red se basa en los siguientes puntos:

• Segmentación de redes

• Proxies

• Firewalls

• IDS e IPS.

Implementación de IDS y IPS: IDS (Sistema de detección de Intrusos) o IPS (Sistema de Protección de Intrusos). son cada vez más comunes y, en algunos casos, pueden denominarse sistemas antimalware cliente-servidor, lo que significa que pueden informar a un servidor central, que es lo que permite al Administrador del sistema tener una visión general del estado de seguridad de su infraestructura y recibir advertencias sin tener que informar al usuario de la computadora cuando aparece una ventana emergente de advertencia.

A nivel de recurso humano

Concienciación de usuarios: Los usuarios pueden actuar voluntariamente o sin saberlo para causar daño, con o sin intención de causar daño, pero la verdad es que pueden hacerlo y también están sujetos a la ingeniería social, por lo que la conciencia de seguridad del usuario es un trabajo sumamente importante. Esto puede determinar en gran medida el éxito de un plan de seguridad.

Evitar hacer clic en enlaces de mensajes de spam o en sitios web desconocidos o de dudosa procedencia. Esto podría ocasionar una descarga automática con algún archivo infectado.

En caso de recepción de llamadas, un mensaje de texto o un correo electrónico de una fuente que no sea de confianza en donde se le solicita información personal, no debe responder ya que los ciberdelincuentes pueden recopilar información personal para personalizar suplantación de identidades o extorsión.

No debe abrirse archivos adjuntos de correos electrónicos sospechosos, primero debe verificar que el correo electrónico sea de confianza, preste especial atención al remitente y compruebe que la dirección sea correcta.

Actualización del software con regularidad: El software obsoleto es un área de vulnerabilidad de la que pueden aprovecharse los piratas informáticos. Las actualizaciones y mejoras del sistema se realizan para optimizar la usabilidad o el diseño de un programa y para añadir nuevas funciones de seguridad.

CONCLUSIONES

Para lograr la identificación de brechas de seguridad que permiten el ataque del *Ransomware Ransonexx*, se llevó adelante una simulación en escenarios controlados, sugiriendo diversos escenarios para conocer el comportamiento del sistema en base a premisas como corrupción y secuestro de archivos o información, poniendo como muestra, aquellos archivos críticos de la organización, que son los preferidos por este tipo de Ransomware, tales como: datos de clientes, contables y financieros.

El ambiente de simulación incorporó la corrupción y secuestro de información privada de los roles de pago tanto para el sector administrativo como para el sector operativo. Entre los patrones identificados se encuentran que los archivos se encuentran corrompidos ya que estaban cifrados y la extensión de los archivos no es el original que es xlsx. Considerando que no hubo alertas dando cuenta de este inusual caso, se evidencia que no se contaba con medidas de seguridad perimetral informática activa, ni a nivel de hardware (firewalls) ni a nivel de software (IDS o IPS). IDS (Sistema de detección de Intrusos) IPS (Sistema de Protección de Intrusos).

La revisión de los informes de trabajo da cuenta de que al querer acceder a la nómina el día anterior a la prueba, sin inconvenientes para manejar tal información. Sin embargo, se asume que el archivo infeccioso fue alojado en el proceso de aprobación de pagos que se encontraban comprometidos y además se encontraba una notificación de rescate que es una característica de este tipo de ataques (extorsivos).

El análisis en ambientes controlados de Ransomware, permite determinar cuan catastrófica puede llegar a ser una infección con Ransomware exx, determinar cuáles son los archivos con mayor vulnerabilidad y encontrar posibles fallos de seguridad nos conllevan a entender el comportamiento y accionar de este código malicioso. Establecer políticas de seguridad empresariales en donde se considere distintos escenarios desde una posible intrusión hasta el secuestro de información por gente inescrupulosa, cada escenario debe tener un plan de seguridad.

El ataque de tipo Ransomware causa un daño significativo a los recursos del computador, incluyendo el uso de la CPU, la memoria y el ancho de banda. El ataque Ransomware, aunque no consume recursos del ordenador, es el más peligroso porque no permite al usuario entrar en el ordenador. Este tipo de ataque secuestra todo el disco duro inmediatamente y, por tanto, no consume recursos, pero esto no implica que afecte directamente, ya que compromete la información interna de la misma, para este caso específico el daño se dio en los archivos de la nómina

Finalmente, luego de identificar y conocer la magnitud de los daños que pueden ocasionar los Ransonware, se propuso medidas preventivas ante los ataques por Ransomware Ransonexx, considerando las principales debilidades o brechas de seguridad, además de reconocer que los datos informáticos son vulnerables a este tipo de amenazas, por lo cual es necesario mantener respaldos de información de forma periódica o a su vez realizar entornos virtuales donde si llegara a suceder algún tipo de intrusión se restablezca el sistema o los datos a su forma inicial. Las principales medidas de seguridad están en las manos del consumidor final y del navegante de internet.

Entre las principales medidas preventivas se encuentran el uso de redes seguras no públicas, el uso de memorias extraíbles o USB que sean de origen seguro, evitar la apertura de mensajería por correo electrónico de fuentes no confiables o desconocidas, revisar o validar que el correo que recibió sea del destinatario que llega, además de no dar ningún tipo de información personal cuando lo llaman o le piden por correo electrónico.

RECOMENDACIONES

Para detectar ataques de Ransomwarexx ejecutándose en algún sistema de información lo antes posible y mitigar sus efectos, se recomienda mantener un sistema de monitoreo activo.

Mantener activa la seguridad mediante software de protección antivirus que permitan la detección y bloqueo de ransomware.

Realizar pruebas en laboratorios virtuales con el propósito de estudiar a fondo el comportamiento y consecuencias de una infección con ransomware.

Mantener políticas definidas para evitar ser víctima de un ransomware, desde el uso del antivirus, la topología de red y lo más importante capacitación de los usuarios.

No se recomienda el pago de la recompensa exigida por los ciberdelincuentes, esto fomenta que ellos generen códigos cada vez más sofisticados y complejos que a futuro podrían comprometer mucho más la información confidencial.

BIBLIOGRAFÍA

Acurio, S. (2020). *Manual de Manejo de Evidencias Digitales.* Obtenido de https://www.oas.org/juridico/english/cyb_pan_manual.pdf

Ambit. (2020). *Tipos de Vulnerabilidades y Amenazas informáticas.* Obtenido de https://www.ambit-bst.com/blog/tipos-de-vulnerabilidades-y-amenazas-inform%C3%A1ticas

Bestuzhev, D. (2021). *"RansomEXX y sus operaciones en Latinoamérica. Capítulo Ecuador" .* Obtenido de https://gmsseguridad.com/ransomexx-y-sus-operaciones-en-latinoamerica/

CEPAL. (2018). *Una mirada regional al acceso y tenencia de tecnologías de la información y comunicaciones – TIC, a partir de los censos.* Obtenido de https://www.cepal.org/es/enfoques/mirada-regional-al-acceso-tenencia-tecnologias-la-informacion-comunicaciones-tic-partir

Fernandez, Y. (2019). *Qué es el Ransomware y cómo te puedes proteger de él.* Obtenido de https://www.xataka.com/basics/que-ransomware-como-te-puedes-proteger

GlobalSuites. (2022). *Las siete filtraciones de datos de 2020.* Obtenido de https://www.globalsuitesolutions.com/es/filtraciones-de-datos-de-2020/

Interpol. (2020). *Un informe de INTERPOL muestra un aumento alarmante de los ciberataques durante la epidemia de COVID-19.* Obtenido de https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19

Interpol. (2022). *Análisis forense digital.* Obtenido de https://www.interpol.int/es/Como-trabajamos/Innovacion/Analisis-forense-digital#:~:text=El%20an%C3%A1lisis%20forense%20digital%20es,datos%20almacenados%20por%20medios%20electr%C3%B3nicos.

Karpesky. (2023). *Identificación de ransomware: en qué se diferencian los troyanos de cifrado.* Obtenido de https://latam.kaspersky.com/resource-center/threats/ransomware-attacks-and-types

Malwarebytes. (2022). *Ransomware.* Obtenido de https://es.malwarebytes.com/ransomware/

Microsoft. (2020). *Prepararse para un ataque por ransomware.* Obtenido de https://learn.microsoft.com/es-es/azure/security/fundamentals/ransomware-prepare

Proofpoint. (2021). *Definición de ransomware.* Obtenido de https://www.proofpoint.com/es/threat-reference/ransomware#:~:text=Preguntas%20frecuentes-,Definici%C3%B3n%20de%20ransomware,viene%20con%20una%20fecha%20l%C3%ADmite.

Puodzius, C. (2021). *Cómo y por qué el cifrado moldeó al ransomware criptográfico.* Obtenido de https://www.uv.mx/infosegura/general/conocimientos_ransomware-5/

Pwc. (2022). Ciberriesgos 2021:Un año en retrospectiva. *PWC*.

Romero, M., Figueroa, G., Vera , D., & Alava, J. (2018). *INTRODUCCIÓN A LA SEGURIDAD.* Obtenido de https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

Samaniego, R. (2021). *Ransomware.* Obtenido de https://zerodayschool.net/2021/10/28/ransomware/

Sertecompsa. (2023). *La historia de RansomExx.* Obtenido de https://www.sertecomsa.com/post/perfil-de-ransomware-ransomexx#:~:text=RansomExx%20surgi%C3%B3%20por%20primera%20vez,Departamento%20de%20Transporte%20de%20Texas.

Sharma, L. (2022). *13 herramientas EDR para detectar y responder a ataques cibernéticos rápidamente.* Obtenido de https://geekflare.com/es/edr-tools/

Castro, E. (2015). *Estudio Prospectivo de la ciberdefensa en las fuerzas armadas del Ecuador* . Obtenido de http://repositorio.espe.edu.ec/jspui/bitstream/21000/11583/1/T ESPE-049543.pdf.

Freire, K. (2017).). *Estudio y análisis de ciberataques en América Latina*. Obtenido de http://192.188.52.94:8080/bitstream/3317/9203/1/T-UCSG-PRE-TEC-ITEL-245.pdf

Frost, & Sullivan. (s.f.). US Healthcare Cybersecurity Market, 2020 - Frost Radar Report.

INCIBE. (5 de septiembre de 2019). Obtenido de: Ingeniería social: técnicas utilizadas por los ciberdelincuentes y cómo protegerse. (2019, septiembre 5). INCIBE. https://www.incibe.es/protege-tu-empresa/blog/ingenieria-social-tecnicas-utilizadas-los-ciberdelincuentes-y-protegerse.

Cisco Systems. (2017). WannaCry: La Industria 4.0 bajo amenaza. Recuperado el 26 de abril de 2022, a partir de https://gblogs.cisco.com/la/sg-silcarlos-wannacry-la-industria-4-0-bajo amenaza/?doing_wp_cron=1502225974.3392050266265869140625.

Consejo de Seguridad Nacional. 2013. “Estrategia de Ciberseguridad Nacional de 2013”, https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies ncsss/ES_NCSS.pdf

Deming, E. (05 de 06 de 2021). Vista de Análisis y técnicas de prevención ante ataques ransomware. [online] Revista-edwardsdeming.com. Obtenido de http://revista edwardsdeming.com/index.php/es/article/view/73/124

Emsisoft. (2022, abril 17). Perfil de Ransomware: RansomExx. *Sertecomsa.com*. https://www.sertecomsa.com/post/perfil-de-ransomware-ransomexx.

IEEE (Instituto Español de Estudios Estratégicos). 2010. “Ciberseguridad: Retos y amenazas a la seguridad nacional en el ciberespacio”, http://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf.

Ivanova, G. (2021, junio 15). *Quitar Exx Ransomware Virus*. Cómo, Foro de Tecnología y Seguridad PC | Sensorstechforum.com; SensorsTechForum. https://sensorstechforum.com/es/remove-exx-ransomware/

John Wiley & Sons, I. (1999). Obtenido de https://ietresearch.onlinelibrary.wiley.com/doi/full/10.1049/iet-net.2017.0207

Jurisprudencia, Ciencias Políticas y Sociales, Quito: Ecuador. Disponible en: http://www.dspace.uce.edu.ec/bitstream/25000/19494/1/T-UCE-0013-JUR-216.pdf.

Llangarí A. (2016). Análisis de los delitos informáticos y de telecomunicaciones en el Ecuador bajo las nuevas normas jurídicas. Carrera de Ingeniería Electrónica, Redes y Comunicación de datos, Sangolquí: Ecuador. Disponible en: http://repositorio.espe.edu.ec/jspui/bitstream/21000/11654/1/T ESPE-053079.pdf.

Meskauskas, T. (2021, enero 22). *Ransomware RansomExx*. Pcrisk.es; PCrisk. https://www.pcrisk.es/guias-de-desinfeccion/10315-ransomexx-ransomware

Moncayo P. (2019). Herramientas jurídicas para garantizar la ciberseguridad del Estado. Análisis comparado de Colombia, Chile y Ecuador. Universidad Central del Ecuador.

Moran C. (2017). Seguridad informática y realidad jurídica del ciberespacio en el Ecuador. Facultad de Derecho y Ciencias Sociales. Disponible en: http://dspace.udla.edu.ec/bitstream/33000/7974/3/udla-ec tab-2017-70.pdf.

Ramírez, I. (2016, julio 25). *Máquinas virtuales: qué son, cómo funcionan y cómo utilizarlas*. Xataka.com; Xataka. https://www.xataka.com/especiales/maquinas-virtuales-que-son-como-funcionan-y-como-utilizarlas

Ransomware – Qué es y cómo protegerse. (2021, diciembre 27). Proofpoint. https://www.proofpoint.com/es/threat-reference/ransomware

RansomEXX y sus operaciones en Latinoamérica. Capítulo Ecuador” - Dmitry Bestuzhev - GMS Seguridad de la Información. (2021, agosto 3). GMS Seguridad de la Información. https://gmsseguridad.com/ransomexx-y-sus-operaciones-en-latinoamerica/

Ruiz Díaz, Joaquín. 2016. “Ciberamenazas: ¿el terrorismo del futuro?”,

http://www.ieee.es/Galerias/fichero/docs_opinion/2016/DIEEEO86.

Technologies, W. (2022). Libro electrónico - Ransomware. Obtenido de https://www.watchguard.com/es/wgrd-resource-center/ebook/ransomware-es-419TEC-ITEL-245.pdf.

Umbrella, Cisco. (s.f.). Obtenido de https://learn-umbrella.cisco.com/i/829449-defensa-contra-el ransomware/0.

Urueña Centeno, Francisco Javier. 2015. “Ciberataques, la mayor amenaza actual”, http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO09.

Vargas, R. y. (05 de 2020). ANÁLISIS DE ATAQUES CIBERNÉTICOS HACIA EL ECUADOR. Obtenido de https://revistacientificaistjba.edu.ec/images/home/documentos/Mayo_2020/2.pdf.