Universidad de Buenos Aires

Facultades de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática

Trabajo Final

Tema: Ransomware en Empresas con entornos Industriales.

Título

Ciberseguridad: Ransomware en entornos OT.

Autor: Ing. José Luis Mora Isaza

Tutores TFE: Patricia Prandini

Año de Presentación 2023

Cohorte 2019

DECLARACIÓN JURADA

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

FIRMADO

José Luis Mora Isaza

DNI 95.970.106

RESUMEN.

Este trabajo presenta a profesionales, entusiastas y todos los interesados en la **Ciberseguridad Industrial**, un análisis sobre la importancia de tomar acciones en instalaciones operativas de esta naturaleza, contra ataques de programas que actúan como secuestradores de datos, conocidos como “ransomware”. Este tipo de ataques ha disparado su capacidad de dispersión, variedad e impacto durante y luego de la pandemia de Covid-19.

La sofisticación en ataques de día cero, los nuevos indicadores de ataque y de compromiso (IOA e IOC, por sus siglas en idioma inglés), las nuevas mutaciones de malware o la escasez de centros de operaciones de ciberseguridad en empresas con entornos donde convergen redes IT/OT, traen consigo peligros o riesgos no gestionados, que afectan la gobernanza de la seguridad de la información en dichas organizaciones.

En síntesis, este resumen literario tiene como objetivo estudiar la criptografía y la criptovirología, así como identificar las diferentes familias de ransomware incluyendo su historia y evolución, además de detallar ciberataques en empresas de entornos OT con repercusiones relevantes en medios de comunicación para finalmente, proponer estrategias que apuntan a disminuir y/o minimizar el número de ataques exitosos y su impacto.

Palabras Claves

Ransomware, secuestro de datos, Ciberseguridad industrial, Convergencia IT/OT, Malware.

TABLA DE CONTENIDO

TABLA DE ILUSTRACIONES.

INTRODUCCIÓN.

El mundo se enfrentó recientemente a una pandemia que mostró su capacidad de paralizar casi completamente a la sociedad, generando cambios profundos conocidos como “nuevas normalidades”. El virus que la originó provocó la muerte de muchas personas, aumentó los niveles mundiales de pobreza y el cierre de empresas y le demandó a la humanidad la exigencia de adaptarse a nuevas formas de vida. Postpandemia del COVID-19, los entornos conectados a la internet han sido cada vez más vulnerables debido al aumento de tráfico y a los cambios de paradigmas entre lo presencial y lo virtual por lo que diversas organizaciones priorizaron la continuidad operativa en sus distintas actividades por encima de un factor determinante para la supervivencia de un sistema: la seguridad.

Indudablemente, los ataques están siendo cada vez más sofisticados y últimamente en mayor medida, adquieren la modalidad de secuestrar los datos, funcionando con un fin claro: escalar en privilegios dentro de un ecosistema para lograr vulnerar su seguridad y así propagarse por todo el entorno de una red e ir confiscando la información que encuentre a su paso. Entonces, se crea la necesidad de implementar herramientas para mitigar los efectos de este tipo de incidentes, haciendo necesaria la implantación de estrategias para protegerse de posibles ciberamenazas. Estas estrategias deben contemplar que quienes toman decisiones desde el gobierno de las organizaciones, tengan claro las distintas posturas a asumir sobre el manejo de riesgos.

En línea con lo anterior, el presente trabajo final de la Carrera de Especialización en Seguridad Informática de la Universidad de Buenos Aires busca analizar la historia, las diversas familias y la evolución de los programas secuestradores de datos, además de estudiar la repercusión que lograron diversos ciberataques exitosos en distintos medios de comunicación en organizaciones de entornos con tecnologías operativas. Concluye con una serie de estrategias para minimizar los efectos nocivos de estos tipos de software maliciosos.

CAPÍTULO 1. CRIPTOGRAFÍA MALICIOSA: HISTORIA Y EVOLUCIÓN.

1.1 Criptografía y criptovirología

A lo largo de la historia, la criptografía ha tenido como objetivo principal facilitar intercambios seguros de mensajes entre personas o grupos. En la actualidad, su aplicación se extiende al ámbito de las comunicaciones tecnológicas, donde se utiliza para brindar seguridad al proteger la información. Esto se logra mediante el uso de algoritmos de codificación, firmas digitales y funciones de hash, que garantizan que los datos sean ininteligibles e invulnerables a posibles amenazas. De esta manera, la criptografía desempeña un papel fundamental en la protección de la información.

Etimológicamente, la palabra criptografía [1] proviene del griego κρύπτος (kryptós), que significa "secreto", y γραφή (graphé), que significa "grafo" o "escritura". Literalmente significa "escritura secreta". A diferencia del pasado, el uso de la criptografía ya no es exclusivo para clanes, monarquías, altos mandos gubernamentales o milicias, sino que, con la masificación del uso de las computadoras interconectadas, se ha ampliado su aplicación a la seguridad de los datos en las comunicaciones en internet.

Dentro del ámbito de la seguridad de la información, es crucial garantizar la protección de los datos y recursos, asegurando que solo sean accesibles por entidades autorizadas, ya sean organizaciones o individuos. Además, se busca que los mensajes recibidos no hayan sufrido alteraciones no autorizadas, que el remitente sea auténtico y autorizado para enviar el mensaje, y que el destinatario no pueda negar haberlo recibido. Estos principios fundamentales se traducen en los requisitos de confidencialidad, integridad, autenticidad y no repudio. En el entorno digital, la criptografía se convierte en la columna vertebral de la ciberseguridad, ya que cumple con estos requisitos y desempeña un papel fundamental en la protección de la información y los sistemas.

Por otro lado, y en cuanto a la manera de proteger la información, su principal uso fue el de convertir un mensaje en uno que fuera inteligible, es decir, en un mensaje “cifrado” que no pudiera ser interpretado fácilmente al ojo humano. Sin embargo, ese mismo uso aplicado de las matemáticas en la comunicación de mensajes debe mantener la capacidad de poder recuperar el mensaje original con la plena seguridad de que sea fiel a la inicial, y que ningún tercero tenga la capacidad de ponerse en el medio y

descifrarlo. Para lograr estos objetivos, es imprescindible utilizar distintas técnicas, si bien no existen sistemas infalibles que garanticen la fiabilidad de esa información.

En cuanto a cómo se emplea, inicialmente se tenían métodos como el de la sustitución para la codificación de mensajes, como el reconocido cifrado César, en el cual las letras del mensaje original eran desplazadas un número determinado de veces. Este proceso convertía el mensaje en otro completamente diferente. Aunque esta técnica fue innovadora en su tiempo, con el paso del tiempo se descubrió que era fácilmente descifrable mediante el análisis lógico y estadístico basado en las frecuencias de uso de las letras en un determinado idioma.

Luego con la implementación de funciones matemáticas más complejas, se empezaron a generar claves de mayor longitud con números primos que técnicamente son casi imposible de quebrar con la tecnología actual de la que disponen las organizaciones. En consiguiente, es válido afirmar que son diversos los campos de acción de la criptografía, ya que se trata de una disciplina con una amplia variedad de aplicaciones, muchas de las cuales se utilizan en la vida cotidiana de la humanidad.

Por otro lado, un aspecto destacado de la criptografía es su importancia en la seguridad de las comunicaciones en las redes de computadoras. Permite establecer canales seguros en redes que no lo son inicialmente. Además, de desempeñar un papel fundamental en la identificación y autenticación de usuarios, utilizando firmas digitales y otras técnicas criptográficas. Esto proporciona niveles más elevados de seguridad en comparación con los sistemas de usuario y clave convencionales. En resumen, la criptografía juega un papel crucial en la protección de las comunicaciones en redes informáticas y en la garantía de la identificación y autenticación de los usuarios.

Otra aplicación importante es la de certificar origen, al permitir a agentes fiables validar la identidad de usuarios mediante el uso de algoritmos criptográficos a gran escala. Finalmente, también posibilita el comercio electrónico al habilitar el empleo de canales seguros y mecanismos de identificación, lo que reduce el riesgo de fraudes y robos para las empresas y los usuarios.

Por su parte la criptovirología [2] es la encargada de investigar el uso de criptografía

para la creación de piezas de software maliciosas potencialmente dañinas. Es notable su crecimiento reciente, motivado entre otras razones, en el acelerado crecimiento de las tecnologías de la información y las comunicaciones, el desarrollo de software y la necesidad de brindar seguridad a los datos.

1.2 Virus y sus tipologías

Los virus informáticos [3] son programas diseñados con la clara intención de infringir políticas o causar daños en redes y equipos. Se propagan ingresando a dispositivos a través de archivos infectados y permanecen inactivos hasta su activación. Con el avance de las técnicas, algunos virus pueden ser activados con un simple clic, pudiendo afectar archivos, programas y el sistema operativo del equipo infectado, resultando en fallos del sistema, pérdida de datos o robo de información.

A continuación, se presenta una categorización de los diferentes tipos de virus.

1.2.1 *Adware*

El *Adware* [4] se refiere al software con publicidad que se instala en un ordenador, cuya función principal es redirigir las solicitudes de búsqueda del usuario a sitios web de publicidad, así como también recopilar datos comerciales sobre sus hábitos de navegación, como los tipos de sitios que visita, con el objetivo de mostrar anuncios personalizados.

Hay dos maneras principales en que el adware puede entrar en un dispositivo:

- Freeware o shareware: Es una forma legítima del software de generar ingresos por publicidad para que ayuden a financiar el desarrollo y la distribución de estos programas.
- Sitios web infectados: A menudo se denominan secuestradores de navegador.

1.2.2 *Spyware*

Las piezas de softwares maliciosas de tipo espías suelen venir ocultos junto a otros softwares que se encargan de manera voluntaria y usualmente, son usados para recopilar

información de un dispositivo informático para luego transmitirla a una entidad externa sin la autorización del dueño. Al convivir con este tipo de software malicioso en un dispositivo se traduce en tiempos lentos de respuestas en las operaciones normales del equipo afectado.

Las funciones de este tipo especial de software son recopilar datos e información privada, hábitos de navegación y nombres de usuarios, mostrar anuncios no solicitados (pop-up), redirigir solicitudes de páginas e instalar marcadores de teléfono.

1.2.3 Gusanos

Un gusano [5] es un tipo de software con capacidad de propagación a través de redes informáticas y a sistemas conectados a Internet. No necesita infectar archivos legítimos o programas para propagarse. Suelen explotar vulnerabilidades en sistemas operativos y aplicaciones para infectar otros sistemas, a menudo de forma automática y sin la intervención del usuario.

Sus principales usos se llevan a cabo por medio de ataques masivos de denegación de servicio, robo de datos, espionaje y otras actividades maliciosas. Su objetivo principal, suele ser colapsar los ordenadores y las redes informáticas, impidiendo así el trabajo a los usuarios. A diferencia de los virus, los gusanos no infectan archivos.

Los gusanos se pueden dividir [6] principalmente según la forma en que se propagan:

- Gusanos de Internet.
- Gusanos de correo electrónico.
- Gusanos de mensajería instantánea.
- Gusanos para compartir archivos.

1.2.4 Redes Zombis o Botnets

También conocidas como la red de equipos zombis, las redes botnets [7] representan una de las formas más sofisticadas y frecuentes de ciberdelincuencia en la actualidad. Permiten que los piratas informáticos tomen el control de varias computadoras a la vez y las conviertan en computadoras "zombis" que actúan como parte de poderosas redes de robots que propagan virus, generan spam y se involucran en otros tipos de delitos y

fraudes.

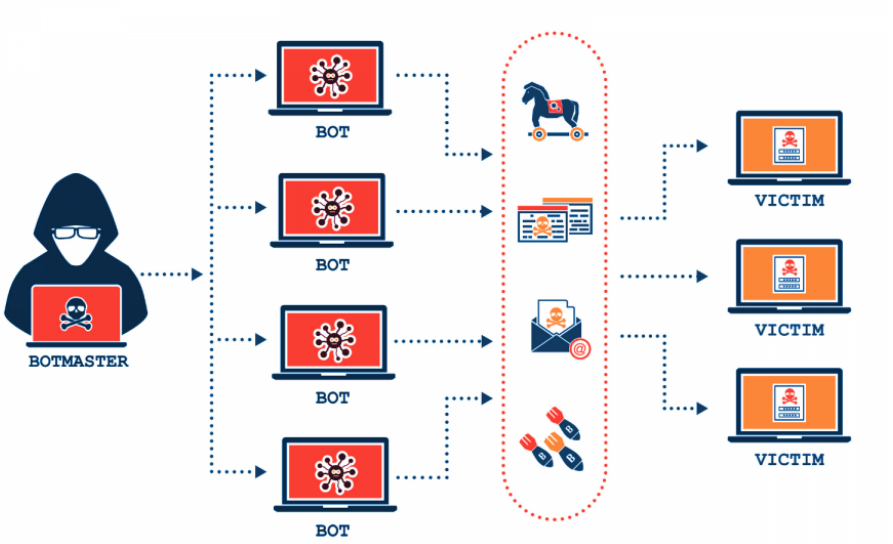

Ilustración 1. Esquema de funcionamiento de una botnet[1]

Estas redes de robots le permiten a un atacante tomar el control de un dispositivo infectado, distribuyendo virus, malwares, troyanos, etc., en sus diversos equipos y/u ordenadores conectados, y por toda la red para sacar cualquier tipo de rédito de sus víctimas. Estos equipos suelen formar parte de una red de máquinas infectadas que generalmente se encuentran distribuidas en todo el mundo. También, suelen ser utilizadas para minar criptomonedas con las capacidades de procesamiento y computo de sus víctimas.

1.2.5 Troyano

Este tipo de software debe su nombre al relato histórico sobre el caballo de la guerra en Troya. Se presenta como un software legítimo pero que, al ser ejecutado, le permite al malware leer contraseñas y pulsaciones de teclado, abrir puertas de acceso para la entrada de otros malwares y, en definitiva, deja que el atacante tome control del dispositivo infectado. Como consecuencia, los datos de la víctima pueden encontrarse en permanente riesgo y a merced del atacante, que puede para robar todo lo que quiera de los equipos infectados. A diferencia de los virus informáticos, los troyanos [8] no tienen la

[1] ¿Qué es una 'botnet' y cómo puedo prevenirla y evitarla? Tomado de: https://www.redseguridad.com/actualidad/cibercrimen/que-es-una-botnet-y-como-puedo-prevenirla-y-evitarla_20210630.html el 2/5/23 a las 18:25

capacidad de infectar a otros archivos por sí solos o de moverse dentro de la red o el equipo comprometido.

Estos son algunos de los más comunes:

- Troyano de puerta trasera: Dejan una puerta abierta en un equipo de un usuario, lo cual permite al atacante acceder al equipo a fin de controlarlo, cargar datos robados e incluso, descargar más software malicioso en el equipo.
- Troyano de descarga: Descargan contenido adicional en el equipo infectado, por ejemplo, más software malicioso.
- Troyano Infostealer: Roban información del equipo infectado.
- Troyano de acceso remoto: Buscan tomar control total sobre el equipo atacado.
- Troyano de ataque de denegación de servicio distribuido (DDoS): Saturan una red con tráfico para que deje de funcionar.

1.2.6 Apps maliciosas

Las aplicaciones maliciosas [9] son consideradas peligrosas porque infectan un dispositivo móvil con algún tipo de programa malicioso sin el conocimiento del usuario que la instala. Las más sofisticadas se camuflan como aplicaciones legítimas en el equipo y se mantienen operando en segundo plano.

1.2.7 Ransomware

En el siguiente capítulo se desarrollará más a detalle sobre este tipo de programa malicioso, siendo éste el objetivo central de este trabajo final de especialización

CAPÍTULO 2. RANSOMWARE.

2.1. ¿Qué es el ransomware y cómo ha evolucionado?

Una manera muy provechosa para un atacante y de potenciales consecuencias negativas sobre un dispositivo, red o una entidad, es el empleo de herramientas criptográficas a través de un software malicioso de tipo Ransomware [10]. Este tipo de malware actúa cobrando un rescate por la información cifrada que “secuestró” del usuario. Expertos indican que no existe garantía de recuperar los archivos, aun habiendo pagado.

Usualmente, los atacantes requieren obtener su paga en un plazo no superior a 3 días, y suele expandir su amenaza indicando que hará pública en la web la información secuestrada. La ingeniería social es la estrategia más explotada en la actualidad por los agentes que pretenden secuestrar datos de una organización o individuo a través del uso de ransomware.

Adicionalmente, el anonimato de las monedas criptográficas genera un panorama más amplio para lograr ejecutar sus cobros. La más conocida y usada para ese fin son los BTC o bitcoins depositados en billeteras virtuales con el plus del continuo aumento de la valorización de dicha moneda, aunque hoy se ha detectado un viraje hacia criptomonedas de menor conocimiento en el mercado, para dificultar las posibilidades de ser detectados.

2.2. Tipos de ransomware

Los ransomware existen bajo diferentes modalidades pensadas originalmente para proteger la información. Entre ellas, podemos encontrar a los siguientes:

2.2.1. Cifrador: (conocido como "*encryptor*" en inglés) es un tipo de software de seguridad que se utiliza para proteger la información mediante la encriptación de datos. En el proceso de cifrado es cuando convierten los datos en un formato ilegible utilizando un algoritmo de cifrado, de modo que sólo aquellos con la clave de descifrado correspondiente puedan leer la información.

Los cifradores se utilizan para proteger los datos almacenados en dispositivos y

redes, así como para asegurar la transmisión de datos a través de Internet. Existen diferentes tipos de cifradores, desde cifradores de archivos individuales hasta cifradores de discos completos y cifradores de correo electrónico.

Otro uso frecuente de estos programas es el de proteger información confidencial, como datos personales, información financiera y secreta comercial. La encriptación ayuda a prevenir el acceso no autorizado a la información, protegerla contra cualquier tipo de acceso que permita la modificación, eliminación o que directamente vulnere la privacidad de los usuarios.

2.2.2 Casilleros: Se utilizan desde el punto de vista de la actividad maliciosa, para bloquear el acceso a un sistema o archivo, y a menudo para pedir un rescate o extorsionar a la víctima. El término "*locker*" proviene del verbo en inglés "*to lock*", que significa "bloquear". Este tipo de código malicioso se instala en la computadora de la víctima para impedir el acceso al sistema operativo o a los archivos del usuario, cifrándolos con una clave de cifrado que sólo el atacante conoce.

La víctima entonces recibe una nota de rescate en la que se le exige el pago de una cantidad de dinero para desbloquear el sistema o los archivos. En algunos casos, los atacantes incluso amenazan con publicar los datos de la víctima en línea si no se paga el rescate.

2.2.3. Scareware: Es un tipo de software malicioso que utiliza técnicas de engaño y persuasión para convencer a los usuarios de computadoras para que descarguen o compren software falso o innecesario.

Por lo general, se presenta como una alerta o mensaje de seguridad que indica que el sistema está infectado con virus y que se necesita un programa de seguridad especial para eliminarlo. El objetivo principal del scareware es asustar al usuario para que haga clic en un enlace o compre o acceda a un programa que en realidad, no necesita y que puede dañar su computadora.

A menudo, los programas de scareware se distribuyen a través de publicidades engañosas o sitios web maliciosos y pueden ser difíciles de eliminar sin herramientas de

eliminación especializadas.

2.2.4. Doxware o software de filtración: Este tipo de programas usualmente amenazan con distribuir información confidencial personal o empresarial en línea. En muchos casos, los afectados entran en pánico y pagan el rescate para evitar que los datos privados caigan en las manos equivocadas o ingresen al dominio público.

Una variación es el ransomware de temática policial, que dice ser un agente de la ley y advierte que se ha detectado actividad ilegal en línea y que pagando una multa se pueden evitar sanciones como la prisión.

2.2.5. RaaS ó Ransomware como Servicio: Es un modelo de negocio en el que los ciberdelincuentes ofrecen herramientas y servicios de ransomware a otros delincuentes, a menudo en la dark web, a cambio de una parte de las ganancias obtenidas de las víctimas del ransomware. Los creadores de este servicio proporcionan a sus clientes potenciales todo lo que necesitan para llevar a cabo ataques de ransomware, como el software malicioso, el soporte técnico y el procesamiento de pagos.

A menudo, se comercializan con nombres de marca, características y precios diferenciados, lo que permite a los clientes elegir entre diferentes opciones para adaptarse a sus necesidades. Este modelo de negocio ha permitido a ciberdelincuentes con poca experiencia técnica llevar a cabo ataques de ransomware con mayor facilidad, lo que se refleja en un aumento en la cantidad de ataques en todo el mundo. Además, el modelo también permite a los creadores obtener beneficios financieros significativos sin tener que realizar los ataques ellos mismos, lo que aumenta la escala y el alcance potencial de estas amenazas.

2.3 Familias de ransomware

2.3.1 Matrix

El ransomware Matrix es una familia que ha estado activa desde al menos 2016 y ha evolucionado con el tiempo para ser más sofisticada y difícil de detectar. Una vez que infecta un sistema, comienza a cifrar los archivos importantes del usuario, como documentos, fotos y otros datos importantes.

Luego muestra un mensaje de rescate en el que se exige un pago en criptomonedas a cambio de la clave de descifrado necesaria para recuperar los archivos. A lo largo de los años ha evolucionado para incluir una amplia gama de tácticas de evasión y técnicas de cifrado más sofisticadas para eludir la detección y la eliminación. Lo que hace que Matrix sea particularmente peligroso es que también ataca a los sistemas de Backup y archivos de recuperación, lo que hace que sea casi imposible para las víctimas recuperar sus datos sin pagar el rescate.

La familia Matrix se ha utilizado en una variedad de ataques, habiendo registrado un serio impacto en casos de hospitales y organizaciones gubernamentales. Se cree que la mayoría de las variantes de este ransomware se originan en Rusia y se han propagado a través de kits de herramientas de ataque en línea, foros de piratería y sitios de descarga de software pirateado.

Ilustración 2. Mensaje de rescate de la familia Matrix[2]

2.3.2 Sodinokibi

Sodinokibi es una familia de ransomware que se descubrió por primera vez en abril de 2019 y que también se conoce como REvil y Sodin. Lo particular de esta familia es que se propaga principalmente a través de correos electrónicos de phishing y explota

[2]¿Qué es Matrix? Tomado de: https://www.pcrisk.es/guias-de-desinfeccion/8404-matrix-ransomware el 4/29/23 a las 22:53

vulnerabilidades en sistemas no parcheados.

Otra característica es la doble extorsión, lo que significa que los atacantes no solo cifran los archivos del usuario, sino que también exfiltran los datos confidenciales del sistema infectado. En otras palabras, los atacantes amenazan con publicar los datos robados si la víctima se niega a pagar el rescate. Además, Sodinokibi tiene una interfaz web integrada que permite a los atacantes interactuar con las víctimas y administrar la extorsión.

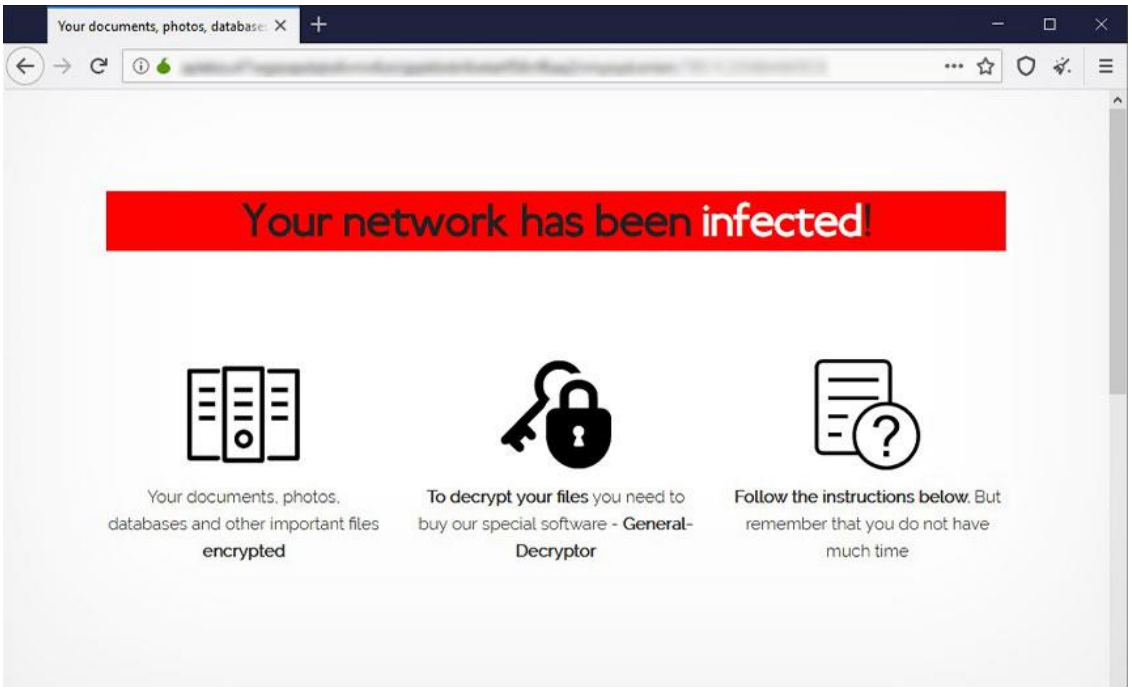

Ilustración 3. Mensaje de rescate de la familia Sodinokibi[3]

Este ha sido utilizado en varios ataques notables, incluido el ataque a la compañía de servicios de tecnología de la información estadounidense Kaseya, en julio de 2021, que afectó a cientos de empresas en todo el mundo.

2.3.3 SamSam

Samsam es una familia de ransomware que ha estado activa desde 2015. A

[3]Sodinokibi Ransomware Gang Targets POS Software Tomado de: https://www.bankinfosecurity.com/sodinokibi-ransomware-gang-targets-pos-software-a-14496 el 4/29/23 a las 22:53

diferencia de otros tipos de ransomware que se propagan a través de correos electrónicos de phishing o enlaces maliciosos, se propaga a través de la explotación de vulnerabilidades en servidores de Internet mal protegidos.

Una vez que el programa infecta un sistema, cifra los archivos y muestra una nota de rescate que exige un pago en Bitcoin a cambio de la clave de descifrado. Los atacantes detrás de Samsam han sido conocidos por apuntar a objetivos específicos, como hospitales, universidades y empresas de tecnología y han sido capaces de causar grandes daños y extorsiones.

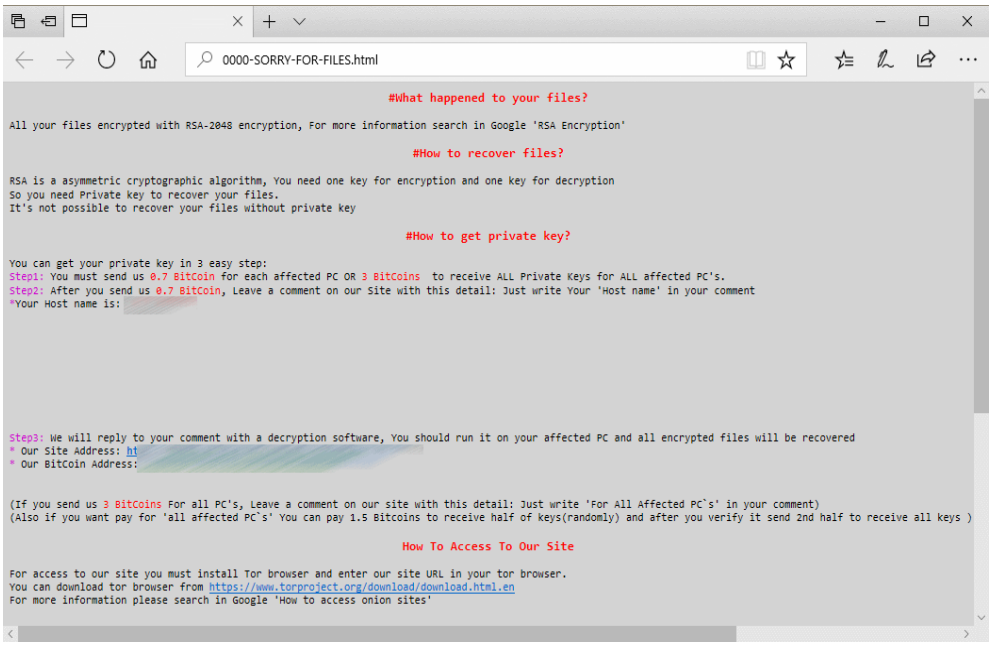

Ilustración 4. Mensaje de rescate de la familia SamSam[4]

Además, a diferencia de muchos otros tipos de ransomware, Samsam ha sido diseñado para eludir la detección y la eliminación, lo que hace que la recuperación de datos sea mucho más difícil. A lo largo de los años, ha evolucionado y agregado nuevas características, incluida la capacidad de propagarse a través de las redes, lo que permite a los atacantes infectar múltiples sistemas en un solo ataque. El impacto de esta actividad maliciosa ha sido muy costoso para las organizaciones afectadas. Efectivamente, algunos informes indican que las víctimas han pagado hasta varios cientos de miles de dólares en

[4]SamSam Ransomware Hits Hospitals, City Councils, ICS Firms Tomado de: https://www.bleepingcomputer.com/news/security/samsam-ransomware-hits-hospitals-city-councils-ics-firms/ el 03/05/2023 a las 15:07

rescates.

2.3.4 Dharma

Dharma es una familia de ransomware que se descubrió por primera vez en noviembre de 2016. Se propaga principalmente a través de correos electrónicos de phishing, kits de explotación y ataques de fuerza bruta en servidores de escritorio remoto (RDP). Una vez que infecta un sistema, cifra los archivos y muestra una nota de rescate que exige un pago en Bitcoin a cambio de la clave de descifrado.

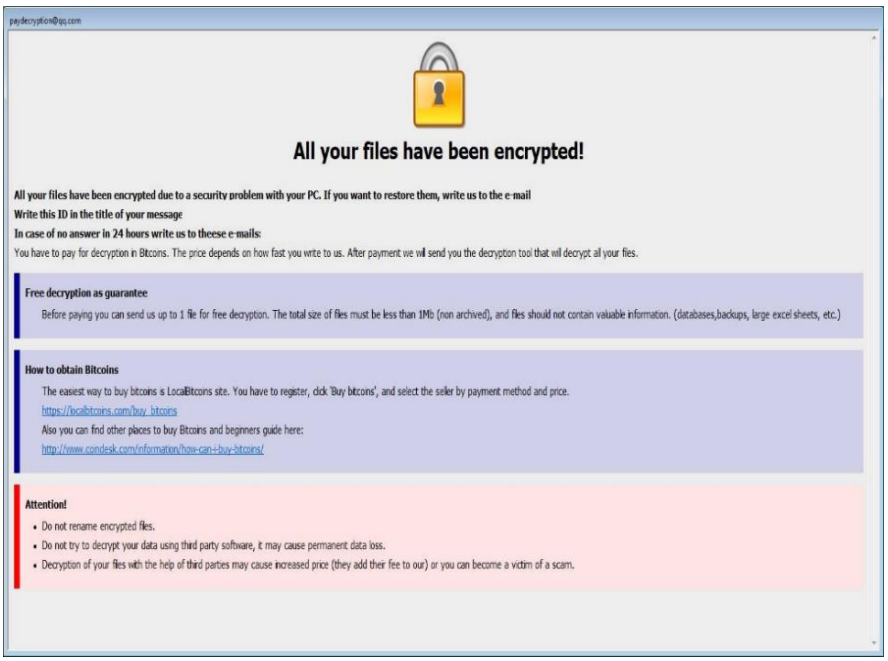

Ilustración 5. Mensaje de rescate de la familia Dharma[5]

Este es un ransomware muy activo y ha sido utilizado en muchos ataques en todo el mundo. A lo largo de los años, ha evolucionado y ha agregado nuevas características, incluida la capacidad de cifrar los archivos con una extensión personalizada y dejar notas de rescate en varios idiomas.

En contraste, comparándolo con otros tipos de ransomware, Dharma ha sido diseñado para eludir la detección y la eliminación, lo que hace que la recuperación de datos sea mucho más difícil. Los atacantes detrás de Dharma también han utilizado varias

[5]All your files have been encrypted. Tomado de: https://sensorstechforum.com/wp-content/uploads/2018/10/Dharma-ransomware-ransom-note-sensorstechforum-com.jpg 4/29/23 a las 23:23

tácticas para presionar a las víctimas a pagar, como amenazar con publicar los datos robados en línea y aumentar el monto del rescate si no se paga a tiempo.

2.3.5 BitPaymer

BitPaymer es una familia de ransomware que se utilizó por primera vez en 2017 y que se propaga principalmente a través de correos electrónicos de phishing y la explotación de vulnerabilidades en software desactualizado. Frecuentemente, al infectar a sus víctimas, cifra los archivos y muestra una nota de rescate que exige un pago en Bitcoin a cambio de la clave de descifrado.

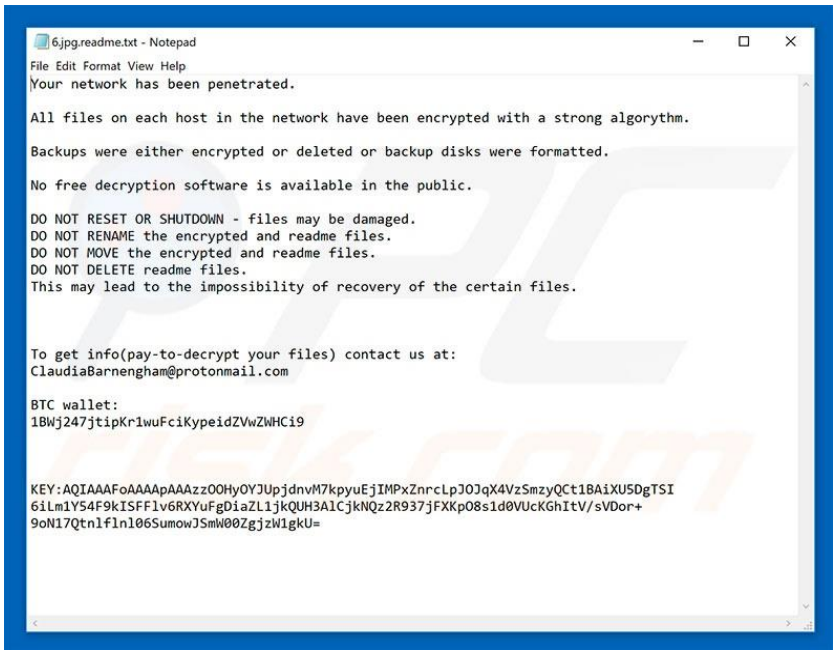

Ilustración 6. Mensaje de rescate de la familia BitPaymer[6]

Además, los atacantes detrás de esta familia han utilizado tácticas de doble extorsión, lo que significa que además del cifrado de archivos, amenazan con publicar datos robados en línea a menos que se pague el rescate. También han aumentado el monto del rescate a medida que pasa el tiempo, lo que hace que sea más costoso para las víctimas recuperar sus datos.

[6] Instrucciones para eliminar el virus criptográfico BitPaymer. Tomado de: https://www.pcrisk.es/guias-de-desinfeccion/8815-bitpaymer-ransomware el 24/29/23 a las 23:25

2.3.6 WannaCry

WannaCry es una familia de ransomware que se empleó por primera vez en mayo de 2017. Fue uno de los ataques más grandes y devastadores que se haya visto, y se propagó a través de una vulnerabilidad en el protocolo de comunicación SMB de Microsoft Windows. WannaCry infectó más de 200,000 sistemas en todo el mundo en cuestión de horas, cifrando los archivos de los usuarios y exigiendo un pago en Bitcoin a cambio de la clave de descifrado. También se propagó a través de las redes internas, lo que permitió que se distribuyera rápidamente internamente en las organizaciones.

Ilustración 7. Mensaje de rescate de la familia WannaCry[7]

Otra característica interesante de WannaCry es que fue uno de los primeros ataques de ransomware que utilizó la criptomoneda Bitcoin para recibir los pagos de rescate. El ransomware exigía un pago de 300 dólares en Bitcoin a cambio de la clave de descifrado para recuperar los archivos cifrados. Según datos conocidos públicamente, afectó a miles de empresas y organizaciones en todo el mundo, en diversos sectores y países.

El éxito de WannaCry se debió en gran parte a la explotación de una vulnerabilidad

[7] Microsoft culpa a la NSA y a los gobiernos del caos de WannaCry. Tomado de: https://computerhoy.com/noticias/software/microsoft-culpa-nsa-gobiernos-del-caos-wannacry-62310 el 4/29/23 a las 22:53

conocida en Windows que Microsoft había liberado meses antes del ataque, lo que le dio mayor relevancia al requerimiento de mantener actualizado el software del sistema y las aplicaciones. Aunque se tomaron medidas para detener la propagación de WannaCry, los ataques continuaron durante varios días, y los atacantes recaudaron cientos de miles de dólares en rescates.

Algunas de las empresas y organizaciones más destacadas que se vieron afectadas incluyen al Servicio Nacional de Salud (NHS)[8] del Reino Unido, la empresa de telecomunicaciones española Telefónica[9], la compañía de automóviles francesa Renault[10] y varias entidades del sistema bancario de Rusia[11], entre otras.

2.3.7 Ryuk

Ryuk es una familia de ransomware que se utilizó por primera vez en agosto de 2018. Se caracteriza por contar con técnicas avanzadas para evadir la detección, como la ofuscación del código y la eliminación de las copias de seguridad del sistema, lo que hace que sea más difícil para las víctimas recuperar sus datos sin pagar el rescate.

Quienes lo han explotado, también han involucrado tácticas de doble extorsión, lo que significa que además del cifrado de archivos, amenazan con publicar datos robados en línea a menos que se pague el rescate. Este secuestrador de datos es considerado uno de los ransomware más destructivos y rentables en la actualidad, y ha sido utilizado para recaudar millones de dólares en rescates.

[8] NHS ransomware attack spreads worldwide. Tomado de: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5461132/ el 15/04/23 a las 18:34

[9] El WannaCry y las 48 horas que el mundo miró a Telefónica Tomado de: https://www.eleconomista.com.mx/tecnologia/El-WannaCry-y-las-48-horas-que-el-mundo-miro-a-Telefonica-20170603-0008.html el 15/04/23 a las 19:32

[10] WannaCry: el ciberataque global paralizó la planta de Renault Tomado de: https://www.iprofesional.com/notas/249866-WannaCry-el-ciberataque-global-paraliz-la-planta-de-Renault el 3/11/22 a las 22:23

[11] Rusia denunció que el ciberataque también afectó a los bancos y ferrocarriles del país Tomado de: https://www.infobae.com/america/mundo/2017/05/13/rusia-denuncio-que-el-ciberataque-tambien-afecto-a-los-bancos-y-ferrocarriles-del-pais/ el 12/3/23 a las 12:21

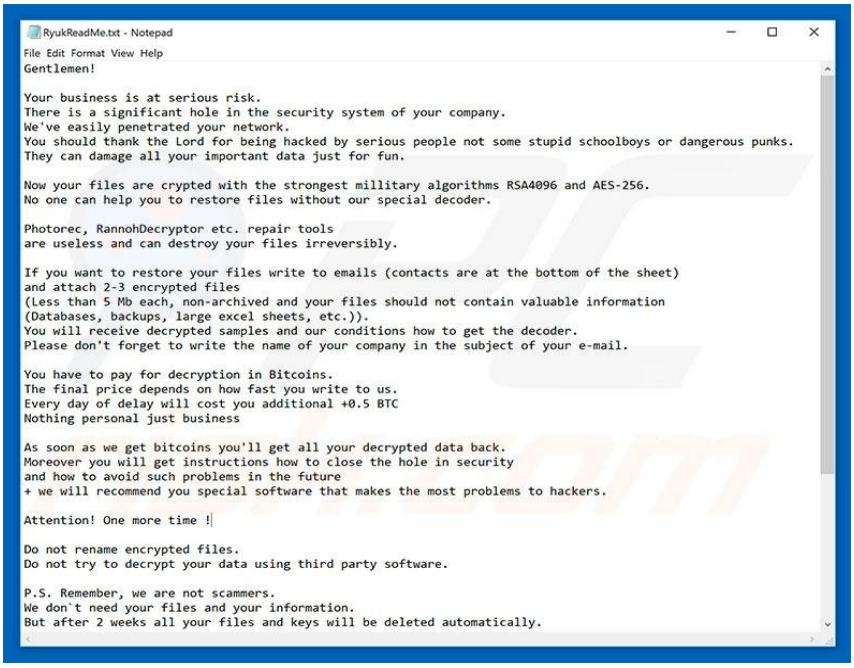

Ilustración 8. Mensaje de rescate de la familia Ryuk[12]

2.3.8 LockerGoga

LockerGoga es una familia de ransomware que se usó por primera vez en enero de 2019. Se propaga a través de correos electrónicos de phishing que contienen archivos adjuntos maliciosos y una vez que se instala en un sistema, cifra los archivos y muestra una nota de rescate que exige un pago en Bitcoin a cambio de la clave de descifrado.

Lo que hace que este código malicioso sea único es que una vez que infecta un sistema, utiliza técnicas avanzadas para evitar la detección, como el cifrado del propio malware y la eliminación de las copias de seguridad del sistema. Además, se ha demostrado que tiene la capacidad de propagarse lateralmente a través de la red de una organización, lo que significa que puede infectar múltiples sistemas en una única entidad.

Ha sido utilizado en varios ataques contra diversas organizaciones y se lo ha relacionado con varios grupos de ciberdelincuentes. Aunque no ha sido tan común como otras familias de ransomware como WannaCry y Ryuk, LockerGoga ha sido muy efectivo en las organizaciones que ha atacado, siendo responsable de la interrupción de las operaciones empresariales con costos financieros significativos.

[12] Cibersecuestro RYUK Tomado de: https://www.pcrisk.es/guias-de-desinfeccion/8879-ryuk-ransomware el 05/05/23 a las 19:20

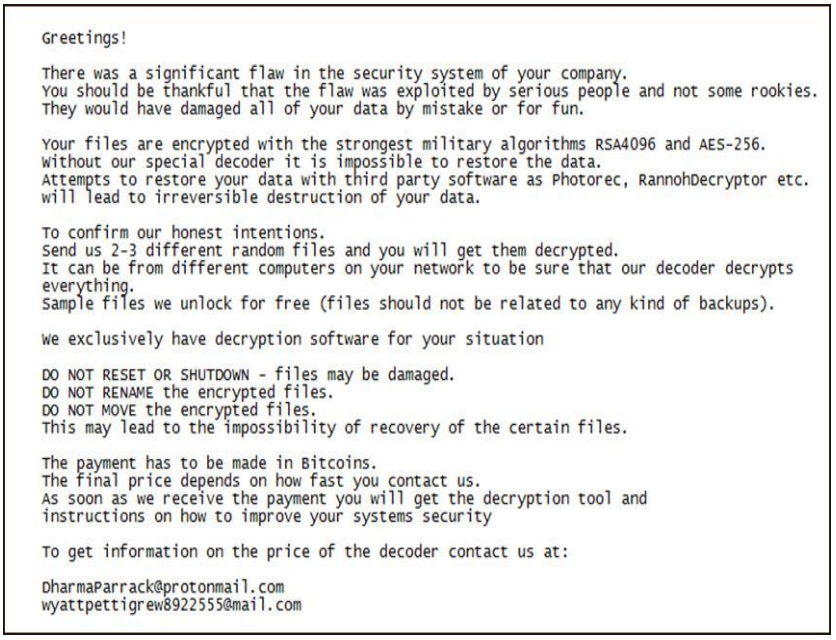

Ilustración 9. Mensaje de rescate de la familia LockerGoga[13]

2.3.9 TeslaCrypt

TeslaCrypt es una familia de ransomware que se empleó por primera vez en febrero de 2015. Se propaga a través de correos electrónicos de phishing y exploit de software desactualizado. Una vez que se instala en un sistema, cifra los archivos y muestra una nota de rescate que exige un pago en Bitcoin a cambio de la clave de descifrado. Su principal característica es que originalmente se centró en cifrar archivos relacionados con juegos de computadora, como archivos de guardado y perfiles de jugador. Sin embargo, a medida que evolucionó, comenzó a cifrar otro tipo de archivos, convirtiéndose en una amenaza más generalizada.

Este programa maligno fue utilizado en varios ataques contra empresas y organizaciones, así como contra individuos. En mayo de 2016, sus desarrolladores lanzaron una nota de disculpa y una clave maestra para desbloquear los archivos cifrados, lo que permitió a los usuarios afectados recuperar sus archivos sin pagar el rescate. Aunque ya no es una amenaza activa, es importante tomar medidas preventivas para protegerse contra las amenazas de ransomware similares.

[13]LockerGoga bug crashes ransomware before encrypting files. Tomado de: https://www.zdnet.com/article/lockergoga-bug-crashes-ransomware-before-encrypting-files/ el 02/05/23 a las 19:25

Ilustración 10. Mensaje de rescate de la familia TeslaCrypt[14]

Al igual que otros tipos de ransomware, TeslaCrypt afectó a diversas empresas en diferentes países del mundo. Aunque no se dispone de una lista exhaustiva de entidades afectadas, algunos de los casos más destacados incluyen:

1. Hollywood Presbyterian Medical Center (Estados Unidos)
2. Lansing Board of Water & Light (Estados Unidos)
3. University of Calgary (Canadá)
4. Trappe Borough Authority (Estados Unidos)
5. Lake City (Estados Unidos)

2.3.10 MegaCortex

MegaCortex es una familia de ransomware que se utilizó por primera vez en mayo de 2019. Se propaga a través de correos electrónicos de phishing y explota vulnerabilidades en el software del sistema. Una vez que se instala en un sistema, cifra los archivos y muestra una nota de rescate que exige un pago en Bitcoin a cambio de la clave de descifrado.

[14] Retire LockerGoga ransomware (extensión bloqueada) Tomado de: https://unaaldia.hispasec.com/2015/04/tesladecrypt-descifra-archivos-cifrados-por-ciertas-versiones-de-teslacrypt.html el 30/4/23 a las 13:33

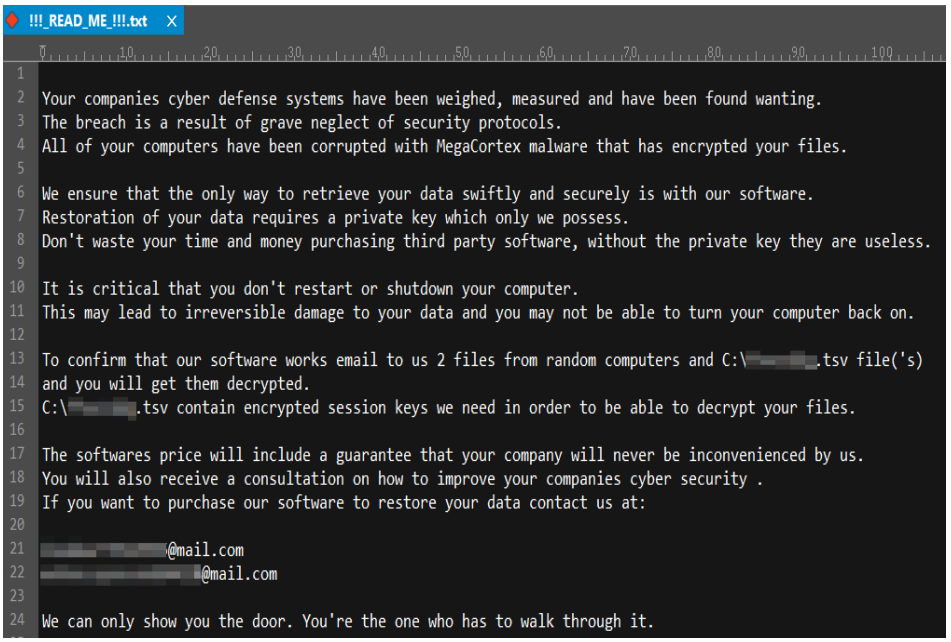

Ilustración 11. Mensaje de rescate de la familia MegaCortex[15]

Se caracteriza por su capacidad para propagarse a través de la red de una organización y afectar a múltiples sistemas. También cuenta con una función de "kill switch" que desactiva los servicios de seguridad y el antivirus en un sistema infectado, lo que lo hace más difícil de detectar y eliminar. Este programa ha sido utilizado en varios ataques dirigidos contra organizaciones de todo el mundo, por grupos de ciberdelincuentes que utilizan técnicas avanzadas para infiltrarse en redes corporativas y robar datos valiosos.

Algunas empresas que han sido víctimas de ataques de MegaCortex incluyen:

- EDP Renewables, una empresa portuguesa de energía renovable que sufrió un ataque en abril de 2020, lo que resultó en el cifrado de datos y la eliminación de sistemas.
- Allied Universal, una empresa de seguridad con sede en los Estados Unidos, que fue atacada en agosto de 2019. Los atacantes amenazaron con publicar datos robados si no se pagaba el rescate.
- Pemex, la compañía petrolera estatal de México, que fue atacada en noviembre de 2019. Los atacantes exigieron un rescate de $ 5 millones de dólares para desbloquear los archivos cifrados.
- Conduent, una empresa de servicios empresariales con sede en los Estados

[15]"MegaCortex" ransomware wants to be The OneTomado de: https://news.sophos.com/en-us/2019/05/03/megacortex-ransomware-wants-to-be-the-one/ el 29/04/23 a las 23:41

Unidos, que fue atacada en mayo de 2019. Los atacantes utilizaron MegaCortex para cifrar archivos en múltiples ubicaciones y exigieron un rescate para desbloquearlos.

2.3.11 RobbinHood

RobbinHood es una familia de ransomware que se empleó por primera vez en abril de 2019. Se propaga a través de ataques a servidores expuestos a Internet con servicios débilmente protegidos. Una de sus principales características es su capacidad para deshabilitar los servicios de seguridad y antivirus en un sistema infectado antes de comenzar a cifrar archivos, lo que lo hace más difícil de detectar y eliminar.

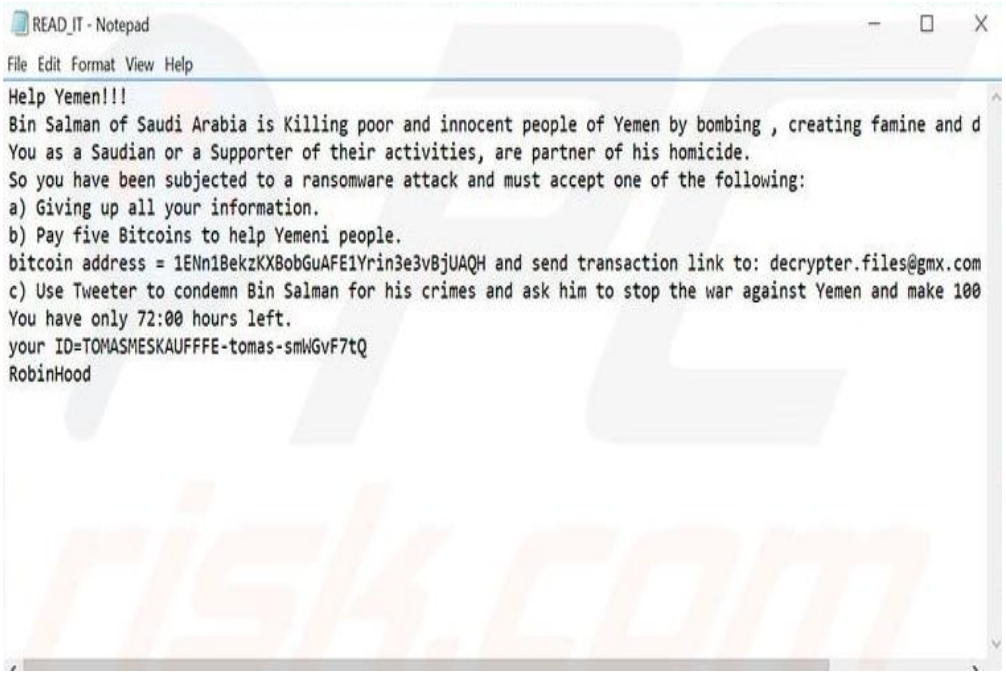

Ilustración 12. Mensaje de rescate de la familia Robbinhood[16]

También utiliza técnicas de cifrado avanzadas y una arquitectura modular que permite a los atacantes personalizar el malware para adaptarse a sus objetivos específicos. Esta familia ha sido utilizada en varios ataques contra empresas y organizaciones en todo el mundo y se lo ha relacionado con grupos de ciberdelincuentes que utilizan técnicas avanzadas de hacking para infiltrarse en redes corporativas y robar

[16] What is RobinHood? Tomado de: https://www.pcrisk.com/removal-guides/11546-robinhood-ransomware el 29/04/23 a las 23:41

datos valiosos.

2.3.12 GandCrab

GandCrab es una familia de ransomware que fue descubierta en enero de 2018 y se cree que ha sido desarrollada por un grupo de ciberdelincuentes rusos. Se propaga a través de correos electrónicos de phishing y kits de exploit, y una vez que se instala en un sistema, cifra los archivos y muestra una nota de rescate que exige un pago en Bitcoin o DASH a cambio de la clave de descifrado.

Lo que hace que sea particularmente peligroso es su capacidad para evadir la detección de los sistemas de seguridad. Además, sus desarrolladores han utilizado una variedad de técnicas para mejorar su capacidad de distribución y extorsión, incluyendo la creación de asociaciones con otros grupos de delincuencia organizada.

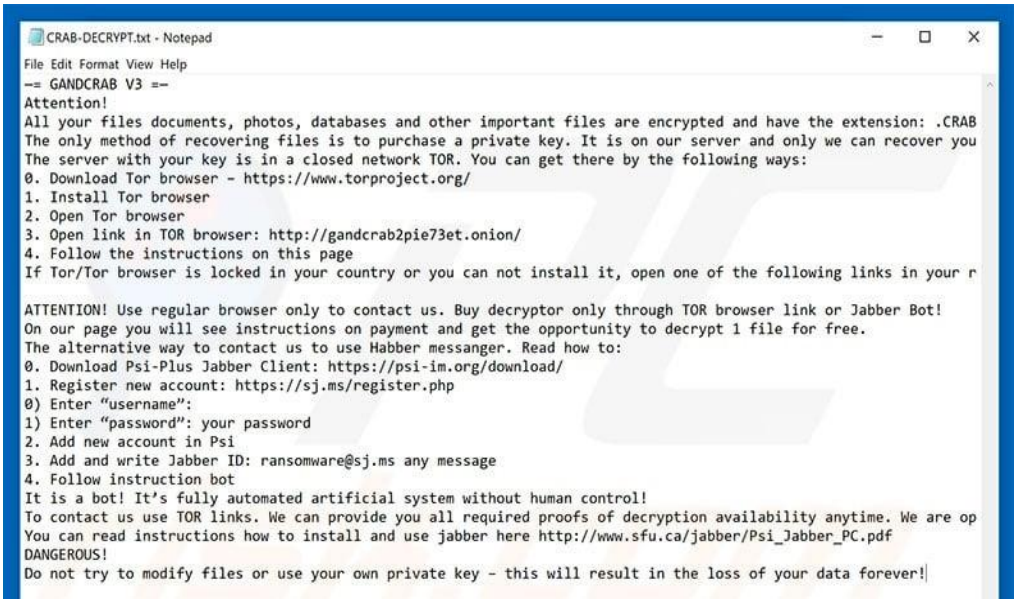

Ilustración 13. Mensaje de rescate de la familia GrandCrab[17]

A pesar de su éxito inicial, sus creadores anunciaron su cierre en junio de 2019, afirmando que habían ganado suficiente dinero y que era hora de retirarse. Sin embargo, han surgido informes de que el programa maligno sigue siendo utilizado por otros grupos de ciberdelincuentes.

[17]El FBI publica las claves maestras de descifrado del ransomware GandCrab. Tomado de: https://www.pcrisk.es/guias-de-desinfeccion/8759-gandcrab-3-ransomware el 29/04/23 a las 23:57

2.3.13 Jigsaw

Jigsaw es una familia de ransomware que se utilizó por primera vez en abril de 2016. Se propaga a través de correos electrónicos de phishing y sitios web maliciosos, y una vez que se instala en un sistema, cifra los archivos y muestra una nota de rescate que exige un pago en Bitcoin a cambio de la clave de descifrado. Se caracteriza por su alto grado de peligrosidad por su capacidad para eliminar gradualmente los archivos cifrados a menos que se realice el pago del rescate en un plazo determinado. Tiene la particularidad de borrar archivos del sistema y poner en peligro la privacidad de las víctimas al exponer su información personal en línea.

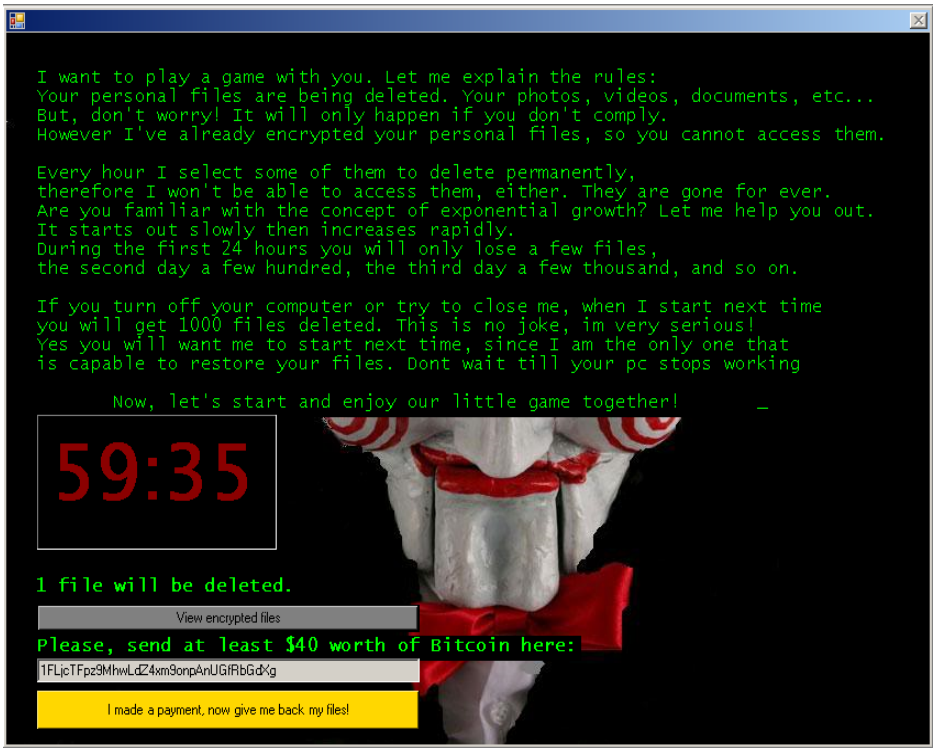

Ilustración 14. Mensaje de rescate de la familia Jigsaw[18]

Este software también utiliza tácticas de ingeniería social para asustar y presionar a las víctimas a que paguen el rescate. La nota de rescate incluye una cuenta regresiva que aumenta la cantidad de rescate a medida que el tiempo pasa, y también amenaza con eliminar archivos adicionales si el pago no se realiza de inmediato.

[18] Jigsaw y cómo el ransomware se vuelve más agresivo con nuevas capacidades. Tomado de: https://www.welivesecurity.com/la-es/2016/04/15/jigsaw-ransomware-mas-agresivo-nuevas-capacidades/ el 30/04/23 a las 00:12

2.4 ¿Qué hacer en caso de estar infectado?

En caso de haber sido infectado por ransomware, lo más importante es desconectar el dispositivo comprometido y otros dispositivos que pudieran estarlo, de la red de Internet para evitar que el programa se propague y proteger los datos y recursos no afectados aún. Además, es importante buscar asesoramiento de expertos en seguridad informática y evitar acciones tales como eliminar el ransomware o descifrar los archivos por sí mismo.

Es importante tener en cuenta que se debe evitar el pago del rescate exigido por los ciberdelincuentes, ya que esto no garantiza la recuperación de los datos y podría alentar a los atacantes a seguir realizando estas actividades maliciosas, inclusive contra la misma entidad. En su lugar, se debe intentar la recuperación de los datos afectados mediante copias de seguridad o herramientas específicas.

Adicionalmente, se deben tomar medidas para mejorar la seguridad de los dispositivos y evitar futuros ataques de ransomware, como mantener actualizado el software del sistema y las aplicaciones, hacer copias de seguridad regulares de los datos importantes, probando su restauración exitosa, implementar medidas de seguridad en servidores y redes, y capacitar a los usuarios para que estén atentos a los correos electrónicos de phishing y otras tácticas de ingeniería social.

2.4.1 Determinar el alcance

El alcance de un ataque de ransomware al ser descubierto puede ser difícil de determinar, ya que puede variar según el tipo y la magnitud del ataque, así como del tamaño de la organización afectada y la cantidad de sistemas y datos comprometidos. Sin embargo, algunos pasos que pueden resultar de utilidad son las siguientes:

- Identificar los sistemas y datos afectados: Esto implica realizar una evaluación completa de los sistemas y datos que están en riesgo, determinando cuáles han sido comprometidos por el ransomware.
- Medir el impacto del ataque: Determinar cuánto tiempo están inaccesibles los sistemas y datos afectados, cuánto tiempo llevará restaurar los sistemas y datos, y cuánto costará la recuperación.
- Evaluar la propagación del ransomware: Es importante determinar si el

ransomware se ha propagado a otros sistemas en la red e identificar esos sistemas.

- Determinar la fuente y el vector de ataque: Comprender cómo el ransomware se infiltró en la red y cómo se propagó ayudará a evitar futuros ataques y mejorar la seguridad de la red.
- Verificar si se ha perdido o expuesto información confidencial: Asegurarse de que no se hayan perdido o expuesto datos confidenciales o información de clientes o empleados durante el ataque y si fuera el caso, cuáles son esos datos afectados.

En general, es importante contar con un plan de respuesta a incidentes que entre otras cuestiones, se enfoque en ataques de ransomware y que incluya medidas para identificar el alcance del ataque y minimizar el impacto. Además, es crucial desarrollar medidas de seguridad proactivas, como copias de seguridad regulares, parches de seguridad, actualizaciones de software y una cultura de seguridad cibernética en toda la organización.

2.4.2 Determinar el riesgo en sistemas OT

Determinar el riesgo en ciberseguridad de entornos OT es sin dudas una tarea compleja, ya que involucra sistemas críticos que controlan procesos físicos y puede tener impactos graves en la seguridad y la salud de las personas y en el medio ambiente. Para evaluar el riesgo en este tipo de entornos, se deben tener en cuenta pasos como los siguientes:

- Identificar distintos escenarios de riesgo que podrían suceder.
- Identificar los sistemas OT críticos que se afectarían.
- Identificar las amenazas específicas de OT.
- Evaluar el impacto potencial de los ataques.
- Identificar las vulnerabilidades específicas de OT.
- Evaluar la probabilidad de que ocurra cada amenaza.
- Calcular el riesgo.
- Identificar medidas de tratamiento luego de una evaluación integral.

Es importante tener en cuenta que la evaluación de riesgos en entornos OT debe involucrar a expertos en ciberseguridad y a los propios operadores de los sistemas para garantizar que se tomen en cuenta todas las variables necesarias y se implementen medidas de mitigación adecuadas.

2.4.3 Evaluar las posibles respuestas

La evaluación de las posibles respuestas ante un incidente de seguridad en entornos industriales es una tarea importante para garantizar la continuidad de las operaciones críticas y minimizar los daños en caso de que ocurra un incidente. Algunos pasos que se pueden seguir para evaluar las posibles respuestas ante un incidente de seguridad en entornos industriales son:

- Caracterizar los escenarios de incidentes.
- Definir los objetivos de respuesta.
- Identificar las posibles respuestas.
- Evaluar la efectividad de las posibles respuestas.
- Definir el plan de respuesta.
- Probar y actualizar el plan de respuesta.

CAPÍTULO 3. ANÁLISIS DE ATAQUES CONOCIDOS POR RANSOMWARE EN ENTORNOS OT CON REPERCUSIÓN EN MEDIOS DE DIFUSIÓN.

Las empresas con redes OT son aquellas que utilizan tecnologías de control industrial y automatización para gestionar y controlar sus procesos y operaciones. Son empleadas en los entornos de producción para controlar y monitorear dispositivos y procesos físicos, como sistemas de control de procesos, robots industriales, sistemas de control de climatización y de seguridad, entre otros.

Las soluciones y servicios qué suelen ofrecer están encaminadas a la automatización y control de procesos industriales, conformadas en su mayoría como infraestructuras críticas. Por lo anterior, es importante mencionar que la ciberseguridad es esencial en estas organizaciones porque dependen en gran medida de sistemas de control y automatización para operar y gestionar sus procesos y operaciones, es decir para garantizar la continuidad de su actividad. Estos procesos incluyen generalmente dispositivos y equipos industriales, como sensores, actuadores, controladores lógicos programables (PLC) y sistemas de control distribuido (DCS), entre otros.

Además, suelen utilizar una red de comunicaciones que en muchos casos también está conectada a una red con acceso a internet, lo que los hace vulnerables a los ciberataques. La exposición en este tipo de sistemas a interferencias maliciosas externas o internas puede causar paralizaciones en las operaciones de la empresa, dañar equipos, afectar la calidad del producto final, poner en riesgo la seguridad de los trabajadores y en algunos casos, poner en peligro la seguridad pública (en empresas de agua, energía eléctrica, nucleoeléctricas, de aceite y gas, etcétera).

A continuación, se lista una serie de casos relacionados con los ataques conocidos de ransomware con repercusiones en medios de difusión registrados alrededor del mundo.

3.1. Caso AstraZeneca

AstraZeneca[19] es una empresa farmacéutica multinacional con sede en el Reino

[19] Un ataque de ransomware afectó los ensayos con la vacuna de coronavirus que se desarrolla en

Unido, que se dedica a la investigación, desarrollo y comercialización de productos farmacéuticos en todo el mundo. Produce una amplia gama de productos, incluyendo medicamentos para el cáncer, la diabetes y la enfermedad cardiovascular, así como vacunas y terapias biológicas. AstraZeneca es especialmente conocida por su vacuna COVID-19 y posiblemente por este motivo, durante la pandemia, sufrió un ataque de ransomware en julio de 2021. Según la compañía, el ataque fue realizado por un grupo de cibercriminales desconocido y tuvo como objetivo sus operaciones en Europa y Asia.

El ataque afectó principalmente los sistemas de TI de la empresa, pero también se informó que algunos sistemas de producción y control industrial se vieron afectados. La empresa aseguró que el ataque no tuvo ningún impacto en la seguridad o calidad de sus productos, y que no se había comprometido ninguna información personal de los pacientes o clientes.

La empresa respondió al ataque tomando medidas para asegurar sus sistemas y protegerse contra futuros ataques y también informó el incidente a las autoridades competentes y trabajó con expertos en seguridad para investigar y mitigar los efectos de incidente.

3.2. Caso Ataque a Norsk Hydro

En marzo de 2019, la compañía noruega de aluminio Norsk Hydro[20] fue víctima de un ataque de ransomware que afectó a sus operaciones en todo el mundo. El ataque comenzó con un correo electrónico de phishing que llevó a un empleado a abrir un archivo malicioso. A partir de ahí, el ataque se propagó rápidamente a través de la red OT de la empresa, cifrando los archivos y sistemas críticos.

El ciberataque utilizó un tipo de ransomware llamado LockerGoga, que se dirige a los sistemas de control industrial y puede causar interrupciones graves en las operaciones. La empresa tuvo que cerrar varias plantas de producción y cambiar a operaciones

Argentina Tomado de: https://www.clarin.com/tecnologia/ataque-ransomware-afecto-ensayos-vacuna-coronavirus-desarrolla-argentina_0_TxBdHHidW.html el 23/11/22 a las 14:34

[20]El ataque de ransomware cuesta Norsk Hydro $ 40 millones Tomado de: https://wiseplant.com/ransomware-attack-costs-norsk-hydro-40-million-so-far/ el 28/4/23 a las 20:23

manuales para evitar daños mayores.

Los delincuentes exigieron un rescate en criptomonedas para desbloquear los sistemas, pero Norsk Hydro optó por no pagar. En su lugar, la empresa colaboró con expertos en ciberseguridad para restaurar sus sistemas y datos afectados. Se estimó que el costo del ataque ascendió a aproximadamente 40 millones de dólares, incluyendo los gastos de recuperación y las pérdidas de ingresos. Adicionalmente, el costo del ataque incluyó los costos de restauración, las pérdidas en producción y ventas, así como los derivados de posibles implicaciones legales y consecuencias en las relaciones públicas.

3.3 Caso Colonial Pipeline

En mayo de 2021, la empresa de transporte de combustible Colonial Pipeline [11] sufrió un importante ciberataque de ransomware. El ataque tuvo lugar en el sistema de tecnología de la información de la empresa, que incluía sistemas de facturación y pagos. Los atacantes, un grupo de hackers conocido como DarkSide, lograron cifrar los sistemas de Colonial Pipeline y exigieron un rescate de 75 bitcoins, equivalentes a unos 4,4 millones de dólares en ese momento. A diferencia del caso anterior, la empresa decidió pagar el rescate para recuperar el acceso a sus sistemas, pero luego se informó que el FBI logró recuperar una parte del pago en criptomonedas.

Como resultado del ataque, Colonial Pipeline decidió cerrar temporalmente sus operaciones, lo que provocó una interrupción significativa en el suministro de combustible en varias regiones de Estados Unidos. El cierre de la empresa provocó una escasez de gasolina y un aumento de los precios del combustible en algunas partes del país.

Este caso de ataque es un ejemplo del impacto real de un ciberataque en la vida cotidiana de las personas y sobre la economía de un país. También se destacó la importancia de contar con medidas de seguridad adecuadas para proteger los sistemas críticos de infraestructuras pertenecientes a empresas de transporte y energía, que brindan servicios considerados esenciales para la sociedad.

Como respuesta a este evento de seguridad, fue el mismo presidente de los Estados Unidos, Joe Biden, qué emitió una serie de órdenes ejecutivas para fortalecer la

ciberseguridad nacional y proteger a las empresas consideradas como infraestructuras críticas. Estas órdenes incluyeron la creación de un estándar de seguridad para el software gubernamental y la revisión de los requisitos de divulgación de los ciberataques.

Además, el gobierno de los Estados Unidos tomó medidas para detener a los responsables del ataque. Se informó que el Departamento de Justicia incautó una gran parte del rescate pagado por Colonial Pipeline y rastreó y como se mencionó más arriba, se recuperó una parte de los fondos en criptomonedas pagados a los piratas informáticos.

También se ha informado que el gobierno de los Estados Unidos inicio un trabajo coordinado con aliados internacionales, incluyendo países europeos, para combatir el cibercrimen y mejorar la ciberseguridad global. En general, el ataque a Colonial Pipeline subrayó la importancia de la ciberseguridad en la infraestructura crítica que soporta servicios esenciales de un país y llevó a un mayor enfoque en la protección contra los ataques cibernéticos y a la colaboración internacional para abordar el problema.

3.4 Caso JBS (Jose Batista Sobrinho)

JBS es una organización de origen brasilero de la industria de alimentos y bebidas. Tiene una presencia significativa en el mercado mundial de carne y suministra productos a clientes de más de 100 países. El ataque de ransomware sufrido por esta empresa en 2021 tuvo un impacto significativo en la industria alimentaria en el mundo.

El ataque a JBS[21] afectó principalmente sus operaciones en América del Norte y Australia. La interrupción de sus sistemas de TI obligó a la empresa a detener la producción en varias plantas de procesamiento de carne en ambos continentes, lo que provocó escasez del producto en algunos mercados y aumentos en los precios.

Además, el ataque también afectó a las operaciones de logística de la empresa, lo que retrasó la entrega de productos a los clientes, por lo tuvo que trabajar con sus proveedores y clientes para minimizar el impacto del ataque en sus cadenas de suministro.

[21] Meat giant JBS pays $11m in ransom to resolve cyber-attack. Tomado de: https://www.bbc.com/news/business-57423008 el 3/05/2023 a las 16:37

JBS confirmó que pagó un rescate de 11 millones de dólares para recuperar el control de sus sistemas y evitar una mayor interrupción de sus operaciones. Si bien el pago del rescate le permitió recuperar el acceso a sus sistemas, a partir de este caso, se manifestó una mayor preocupación por el aumento del número de ataques de ransomware y el papel de los pagos de rescate en el fomento de este tipo de delitos cibernéticos.

3.5 Caso compañía de aguas ONWASA (Onslow water y sewer authority)

En octubre de 2018, el sistema de alcantarillado de la ciudad de Onslow, Carolina del Norte, manejado por ONWASA[22], fue comprometido por un ataque de ransomware. Los delincuentes cibernéticos bloquearon el acceso a los archivos y sistemas de la ciudad y exigieron un rescate para liberarlos.

La ciudad declaró el estado de emergencia y trabajó para recuperar el control de su sistema. Aunque no se pagó ningún rescate, el proceso de recuperación fue costoso y llevó varias semanas. Los servicios esenciales como el suministro de agua y la eliminación de residuos no se vieron afectados, pero el acceso a los registros de pagos y facturación se vio interrumpido, lo que afectó a la capacidad de la ciudad para procesar y enviar facturas a los clientes.

Este ataque destaca la importancia de la seguridad cibernética no solo para empresas y organizaciones gubernamentales, sino también para las ciudades y sus sistemas de infraestructura crítica. Además, también muestra cómo un ataque de ransomware puede afectar indirectamente a los ciudadanos y usuarios de los servicios públicos, lo que subraya la necesidad de medidas de seguridad más sólidas y planes de recuperación de desastres para hacer frente a estos tipos de situaciones.

3.6 Caso Kaseya VSA - Coopertus

El caso Kaseya VSA[23] se refiere a un ataque de ransomware que tuvo lugar en julio

[22] North Carolina water utility ONWASA taken down by ransomware Tomado de: https://www.scmagazine.com/news/critical-infrastructure/north-carolina-water-utility-onwasa-taken-down-by-ransomware el 29/04/23 a las 16:57

[23] Ataque de ransomware de la cadena de suministro de Kaseya VSA. Tomado de:

de 2021 y que afectó a la empresa, proveedor de software de gestión de servicios de TI; el software Kaseya VSA (Virtual System Administrator) es una herramienta de gestión remota que permite a los proveedores de servicios de TI administrar múltiples sistemas y redes de clientes desde una única consola.

En el ataque se afectó a varias empresas, incluyendo una empresa sueca de fabricación de paneles solares llamada Coopertus. La anterior, informó que su sistema de producción se vio afectado por el ataque y que se vio obligada a detener temporalmente sus operaciones.

Los atacantes explotaron una vulnerabilidad de día cero en el software para distribuir e implementar el ransomware REvil en los sistemas de los clientes de Kaseya. El ransomware cifró los datos de las víctimas y exigió un rescate a cambio de la clave. Se estima que al menos 1.500 empresas de todo el mundo fueron afectadas por el ataque, incluyendo empresas de Estados Unidos, Europa y América Latina.

El incidente fue especialmente preocupante al ser la organización atacada proveedora de servicios de TI de nivel empresarial que se utiliza en muchas grandes empresas y organizaciones gubernamentales, lo que significó que el impacto del ataque fue muy amplio y afectó a una gran cantidad de usuarios finales. Además, los atacantes exigieron un rescate de 70 millones de dólares en Bitcoin, lo que fue una de las mayores demandas de rescate jamás registradas.

Después del ataque, la empresa victima trabajó con el FBI y otras agencias de seguridad cibernética para investigar el incidente y desarrollar una solución de parcheo para la vulnerabilidad en su software. Además, los atacantes liberaron una clave de descifrado universal que permitió que muchas de las víctimas recuperaran sus datos sin tener que pagar el rescate. Este ciberataque es un ejemplo de la manera en que los atacantes pueden aprovechar las vulnerabilidades en los sistemas de terceros para llevar a cabo ataques de ransomware a gran escala.

---

https://news.sophos.com/es-419/2021/07/05/ataque-de-ransomware-de-la-cadena-de-suministro-de-kaseya-vsa/#:~:text=El%20viernes%202%20de%20julio,perimetrales%20en%20los%20%C3%BAltimos%20a%C3%B1os. el 28/4/23 a las 19:50

3.7 Caso Naval STX France

Naval STX France es una empresa francesa, perteneciente en parte al Estado francés, de construcción naval que se especializa en la construcción de grandes barcos de crucero y ferries. La empresa es conocida por haber construido algunos de los cruceros más grandes y lujosos del mundo, como el *Oasis of the Seas* y el *Harmony of the Seas* para la compañía de cruceros Royal Caribbean. En 2019, Naval STX France[24] fue víctima de un ataque de ransomware que afectó a su red informática y paralizó la producción en uno de sus astilleros. El ataque obligó a la empresa a cerrar temporalmente su astillero en Saint-Nazaire, lo que causó retrasos en la entrega de varios proyectos de construcción naval.

Los atacantes utilizaron un malware llamado DoppelPaymer para cifrar los archivos de la empresa y exigieron un rescate en bitcoin para liberar los sistemas. La empresa no hizo pública la cantidad exacta del rescate, pero se cree que fue de varios millones de dólares. El ataque a Naval STX France es un ejemplo más de cómo los ataques de ransomware pueden tener un impacto significativo en las empresas OT y en la cadena de suministro en general.

[24] Ransomware attack on chip supplier causes delays for semiconductor groups. Tomado de: https://www.ft.com/content/b8669140-8dde-493e-bb30-f5f1e9830804 el 03/05/23 a las 15:22

CAPÍTULO 4. ESTRATEGIAS PARA FORTALECER LA CIBERSEGURIDAD INDUSTRIAL FRENTE AL RANSOMWARE.

El ransomware ha estado en constante evolución, lo que hace que la protección de los sistemas y activos de información críticos sea un desafío para todos, ya que no solo afecta a las organizaciones sino a todos los usuarios conectados a redes con salida a internet. Por lo tanto, es crucial que las empresas industriales implementen medidas de ciberseguridad para proteger sus sistemas y procesos de los ciberataques.

Estas medidas incluyen la segmentación de redes, la implementación de políticas de acceso y autenticación, la monitorización continua de la red, la definición de procesos que faciliten la detección y respuesta a incidentes de seguridad, la capacitación de los empleados en ciberseguridad y la implementación de soluciones de seguridad específicas para OT, como firewalls industriales y sistemas de detección de intrusiones (IDS/IPS). De esta manera, las empresas pueden proteger sus activos críticos y garantizar la continuidad de sus operaciones en un entorno cada vez más peligroso en términos de ciberseguridad.

Por eso es necesario mencionar algunas estrategias que se pueden implementar para aumentar el nivel de seguridad contra ataques de ransomware, las cuales se listan a continuación:

- Realizar copias de seguridad de los datos críticos de forma regular, y asegurarse de que estas copias estén almacenadas de forma segura y que puedan ser recuperadas en caso de un ataque.
- Implementar medidas de seguridad en la red y en los dispositivos, como firewalls, antivirus, software de detección de intrusiones y parches de seguridad.
- Mantener actualizados los sistemas operativos y las aplicaciones.
- Limitar el acceso de los usuarios y empleados a los sistemas y datos críticos solo a quienes tienen “necesidad de saber”. Es decir, solo otorgar permisos de acceso necesarios para la función de cada usuario en un trabajo.
- Realizar pruebas de penetración y auditorías de seguridad regularmente para identificar posibles vulnerabilidades y anomalías en los sistemas y activos conectados a este.

- Utilizar herramientas de seguridad avanzadas, como sistemas de detección de anomalías y análisis de comportamiento para detectar actividades maliciosas en la red.
- Generar procesos y canales de comunicación que faciliten la emisión de alertas y el escalamiento de decisiones relacionadas por la ocurrencia potencial o real de incidentes de seguridad.
- Capacitar a los empleados en la detección de correos electrónicos sospechosos y mensajes de phishing. Deben elaborarse programas continuos de concientización que permitan una formación permanente y adaptada a las nuevas amenazas que puedan afectar los sistemas y activos de información de la empresa.

Si bien la concientización se indicó al final, resulta uno de los aspectos más relevantes a fortalecer por lo que a continuación se profundiza sobre esta temática.

4.1. Concientización.

En la actualidad, el entrenamiento de los usuarios de un sistema es un requisito mínimo para aumentar su seguridad y operar en el mundo digital. Los empleados son el recurso más preciado para el desarrollo de un negocio, pero también son la primera línea de defensa en términos de seguridad. Concientizar implica desarrollar un cambio en el comportamiento del usuario, generando en el un entendimiento de los riesgos y una modificación en su actitud. Implica también dar a conocer en un lenguaje sencillo y comprensible al tipo de destinatario, los indicios que señalarán una situación de peligro y las medidas a adoptar para evitarla.

Por lo tanto, se deben implementar prácticas de seguridad en todos los dispositivos y respecto a toda la información critica que se maneja en la empresa. Como ejemplos, cabe mencionar el uso de contraseñas sólidas, la conexión solo a redes Wi-Fi seguras y la vigilancia constante frente al riesgo de suplantación de identidad. Como se mencionó, su objetivo principal es cambiar comportamientos, hábitos y actitudes, utilizando recursos como seminarios, capacitación en línea, videos, correos electrónicos, carteles y juegos.

Un programa eficaz de concienciación sobre seguridad de la información permitirá a los usuarios comprender su importancia, su relevancia, la necesidad de estar siempre

alerta y cómo esto les ayudará a realizar sus tareas diarias de manera más efectiva. Es importante que el proceso sea continuo y a largo plazo, y que no se abrume al usuario con demasiada información a la vez.

4.2. Actualizaciones de software

Otro aspecto para tener en cuenta son los programas de parcheo o actualizaciones que son distintos tipos de software que se utilizan para corregir errores y vulnerabilidades y mejorar el rendimiento de un sistema o aplicación. Estos programas suelen ser proporcionados por el fabricante del software y se distribuyen como descargas en línea. Las actualizaciones pueden incluir nuevas características, correcciones de errores, parches de seguridad y mejoras de rendimiento.

Al instalar estas actualizaciones, se puede mejorar la estabilidad del sistema, reducir los riesgos de seguridad y mejorar la funcionalidad de las aplicaciones. Es importante mantener actualizado el software del sistema y las aplicaciones, ya que ayuda a proteger contra vulnerabilidades de seguridad conocidas y mejora la experiencia del usuario. Muchos sistemas operativos y aplicaciones tienen la opción de actualizar automáticamente, lo que permite que las actualizaciones se instalen sin necesidad de intervención del usuario.

4.3. Monitorear las redes y los sistemas de información

Se realiza un seguimiento continuo a las redes y sistemas de información para corroborar su normal funcionamiento, pero también por motivos diversos. A continuación, se enumeran algunos de ellos:

- Detectar fallos y errores: Al monitorear los sistemas, es posible detectar fallos y errores antes de que causen interrupciones graves en el servicio, lo que permite tomar medidas proactivas para resolverlos.
- Prevenir ataques cibernéticos: El monitoreo de los sistemas puede ayudar a detectar actividades maliciosas o sospechosas en la red, lo que permite tomar medidas para prevenir ataques cibernéticos y así proteger de manera eficiente los sistemas y datos.
- Optimizar el rendimiento: Si bien no se trata de un aspecto específicamente de

ciberseguridad, el monitoreo de los sistemas permite identificar cuellos de botella y otras áreas donde se puede mejorar el rendimiento de los sistemas y aplicaciones.

- Cumplimiento normativo: En muchos casos, el monitoreo de los sistemas es un requerimiento legal o regulatorio y de cumplimiento obligatorio para garantizar la seguridad de las personas y la privacidad de sus datos personales.

4.4. Inteligencia sobre amenazas

La inteligencia sobre amenazas es un proceso continuo de recopilación, análisis y distribución de información relevante para la seguridad cibernética con el objetivo de identificar, prevenir y mitigar riesgos y amenazas en la red. Este proceso implica la monitorización de fuentes abiertas y cerradas, la correlación de eventos de seguridad, la evaluación de vulnerabilidades y la identificación de patrones y comportamientos maliciosos en la red. La inteligencia sobre amenazas permite a las organizaciones estar al tanto de las últimas tendencias y tácticas utilizadas por los atacantes, a partir de lo cual pueden adoptar medidas proactivas para proteger sus sistemas y datos.

En resumen, la inteligencia sobre amenazas es una herramienta valiosa para cualquier organización que busque fortalecer su postura de seguridad cibernética y protegerse con la mayor antelación posible contra amenazas cada vez más sofisticadas.

CONCLUSIONES

La ciberseguridad en entornos industriales es un tema de vital importancia debido a la presencia de equipamiento y software con largos períodos de uso sin actualizaciones. Influye además la necesidad de continuidad en las operaciones, es decir, la imposibilidad de interrupciones en este tipo de instalaciones. Estas cuestiones aumentan significativamente el riesgo de vulnerabilidades y amenazas por posibles ataques cibernéticos. Por tanto, la protección y el fortalecimiento de estos sistemas se convierte en una prioridad crítica para garantizar su seguridad y continuidad operativa.

Las organizaciones con tecnologías operacionales son comúnmente vistas como objetivos atractivos para los ciberdelincuentes, ya que a menudo presentan niveles de madurez y robustez bajos en sus programas de seguridad. Lo anterior tiende a poner en riesgo la confidencialidad, integridad y disponibilidad de los sistemas y datos críticos, pero sobre todo, la continuidad del negocio. Por lo tanto, es crucial que estas organizaciones tomen medidas proactivas para mejorar sus prácticas de seguridad de su información y proteger sus activos.

El alarmante aumento de ataques de ransomware, que fue descripto a lo largo de este documento, así como su impacto al cifrar información valiosa y muchas veces, amenazar con la difusión del material sensible secuestrado, exigiendo rescates para su liberación, ha provocado graves consecuencias en empresas, entidades gubernamentales y usuarios individuales. Los daños resultantes son sustanciales e incluyen desde la pérdida de datos críticos, costos financieros considerables hasta los perjuicios de la reputación de sus víctimas.

La implementación de medidas adecuadas en todos los niveles de aseguramiento en entornos con tecnologías industriales, tal como lo plantean marcos de trabajos como el de la IEC 64443 que refiere al gobierno de la seguridad de la información en organizaciones con sistemas de gestión automatizados, necesitan cada día más decisiones imperiosas y requieren de una comprensión profunda de los distintos componentes que estos sistemas poseen, tales como PLC, SCADAS, tecnología de hardware y software asociada a sus procesos productivos, procesamientos de datos, entre otros, así como de los riesgos asociados a ellos y los que convergen con tecnologías informativas.

En el caso de estas empresas, es esencial desarrollar planes y medidas que, desde la perspectiva de la gobernanza de los entornos operativos, aseguren la continuidad de las operaciones de sus sistemas sin comprometer la seguridad de los diversos entornos presentes en ellos, incluyendo personas, procesos y tecnologías. Teniendo en cuenta que la “continuidad operativa” está tatuado en el ADN de estas organizaciones, es crucial poner en marcha programas de formación continua para los empleados en prácticas seguras de ciberseguridad, dado que ellos constituyen la primera barrera de defensa ante las posibles amenazas. Esta medida se convierte en un elemento fundamental para proteger los sistemas de la empresa y salvaguardar la información sensible contra potenciales ataques cibernéticos.

También, es cierto que existen múltiples fuentes que explican las diferencias en los requisitos entre la convergencia de las redes IT y OT, y comprender adecuadamente estas diferencias es el primer paso hacia una integración exitosa. El siguiente paso es llevar a cabo una evaluación minuciosa para asegurar que las redes operativas sean planificadas e implementadas de manera segura, para lograr una integración satisfactoria y sin contratiempos. Los lideres en los distintos niveles gerenciales son cada vez más conscientes de que disponer de una infraestructura segura es un requerimiento para hacer negocios en la actualidad y que los costes asociados a la recuperación de una brecha de seguridad suelen ser elevados y pueden apartar a los empleados de sus funciones principales para apoyar el esfuerzo de recuperación, haciendo que sea mucho más costosa la recuperación ante un incidente que la misma implementación de medidas para contrarrestarlos. Además, pueden aparecer posibles multas por violaciones a normativas y regulaciones que protegen datos e información de usuarios, clientes y proveedores.

Por estas razones, es importante aplicar medidas específicas de ciberseguridad en entornos industriales, como el control de acceso físico a los sistemas, la segmentación de la red para limitar el impacto de los ataques, la monitorización continua de los sistemas para detectar y prevenir amenazas y la formación y concientización del personal sobre las mejores prácticas de seguridad. En definitiva, hablar del "coste de no hacer nada" en materia de ciberseguridad es un riesgo muy alto para asumir. Aunque no existen redes absolutamente seguras, muchas alcanzan altos niveles de seguridad mediante la aplicación de las mejores prácticas de ciberseguridad que proponen los distintos marcos de trabajo como COBIT, el CyBok, el NIST o el mismo IEC 62443.

GLOSARIO.

• **0day:** Vulnerabilidad de la cual no se dispone de parche o forma para mitigarlo por parte del proveedor del servicio.

•**Alerta:** Evento que generalmente activa una notificación o alarma preconfigurada.

•**Algoritmo:** Conjunto de pasos lógicos para dar solución a un problema.

•**Algoritmo criptográfico:** Es un algoritmo que modifica los datos de un documento con el objetivo de alcanzar algunas características de seguridad como autenticación, integridad y confidencialidad.

•**Antimalware:** Solución que permite proteger dispositivos de programas malignos.

•**Astillero**: Lugar donde se construyen y reparan barcos y otras embarcaciones.

•**Backup:** Copia de seguridad, respaldo, copia de respaldo o copia de reserva.

•**Ciberseguridad Industrial:** Se refiere a la implementación de medidas o principios de seguridad a entornos con tecnologías de las operaciones.

•**Computadores zombi:** Es la denominación asignada a computadores personales que, tras haber sido infectados por algún tipo de programa maligno, pueden ser usados por una tercera persona para ejecutar actividades hostiles.

•**Criptografía:** Práctica de proteger información mediante el uso de algoritmos de cifrado.

•**Criptovirología:** Rama de la informática que se encarga del estudio del uso de la criptografía empleado en la creación de software malicioso.

•**Dashboard:** Tablero que permitirá visualizar fácilmente indicadores.

•**Doble Factor de Autenticación:** Mecanismo que mejora la seguridad al momento de identificar a un usuario dentro de una aplicación o sistema con algo que sé, algo que tengo o algo que soy.

•**Evento:** Log con un específico contexto que tiene un significado especial.

•**Firewalls:** diseñado para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

•**Hash:** Es un algoritmo matemático que transforma cualquier dato entrante en una serie de caracteres de salida, con una longitud fija o variable, dependiendo del algoritmo hash que estemos utilizando.

•**IAC:** Indicadores de ataques, se centran más en por qué y la intención de un actor. En simples palabras, se trata de una visión más estratégica de las TTP de un actor o grupo de amenazas.

•**IDPS:** Sistema de detección y prevención de intrusos.

•**Incidente:** Violación inminente de violación a las políticas de Seguridad Informática.

•**Informática Forense:** Aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.

•**Inteligencia de amenazas:** Información sobre amenazas y actores de amenazas que ayuda a mitigar eventos dañinos en el Internet.

•**IOC:** Indicadores de compromiso, se definen como evidencia que demuestran que se ha producido algún tipo de actividad maliciosa o sospechosa.

•**IT:** Tecnologías de la información.

•**Keylogger:** Software o un dispositivo hardware específico que se encarga de registrar las pulsaciones que se realizan en el teclado

•**Malware:** Software malicioso.

•**NIST:** National Institute of Standards and Technology (https://www.nist.gov/)

•**OT:** Tecnología de las operaciones sobre automatizaciones y sistemas distribuidos.

•**Ransomware:** Software maligno que pide rescate para recuperar el activo o la información secuestrada.

•**Software:** Programa informático que realiza una tarea especifica.

•**SOC:** Centro de operaciones de Ciberseguridad.

•**Recuperación en caso de peligro y continuidad de las operaciones:** Definen la forma en que una organización responde a un incidente de seguridad cibernética o a cualquier otro acontecimiento que cause la pérdida de operaciones o de datos y la continuidad de las actividades es el plan al que recurre la organización cuando intenta operar sin ciertos recursos.

•**SIEM:** gestión de eventos e incidentes de seguridad, este sistema se utiliza como correlacionador de eventos.

•**SLA:** acuerdo de nivel de servicio.

•**TICS:** Tecnologías de la información y de las telecomunicaciones.

•**Virus:** Software malicioso con capacidad de propagación.

BIBLIOGRAFÍA.

[1] S. Universidades, «Criptografía: el arte de cifrar mensajes,» Santander Universidades, 06 05 2022. [En línea]. Available: https://www.becas-santander.com/es/blog/criptografia.html#:~:text=En%20concreto%2C%20este%20t%C3%A9rmino%20proviene,transmitir%20mensajes%20de%20forma%20secreta. [Último acceso: 23 11 2022].

[2] S. H. D., QUÉ ES LA SEGURIDAD INFORMATICA, PAIDÓS, 2015.

[3] G. Global, «¿Que es un virus informático?,» GCF Global, [En línea]. Available: https://edu.gcfglobal.org/es/virus-informaticos-y-antivirus/que-es-un-virus-informatico/1/#. [Último acceso: 22 11 2022].

[4] M. d. J. y. D. H. d. Argentina, «¿Qué es un adware?,» Ministerio de Justicia y Derechos Humanos de Argentina, 12 2022. [En línea]. Available: https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-un-adware. [Último acceso: 14 15 2023].

[5] P. DOME, «Gusano,» Panda DOME, [En línea]. Available: https://www.pandasecurity.com/es/security-info/worm/. [Último acceso: 12 2 2023].

[6] HornetSecurity, «Gusanos informáticos,» HornetSecurity, [En línea]. Available: https://www.hornetsecurity.com/es/knowledge-base/gusanos-informaticos/. [Último acceso: 12 04 2023].

[7] K. Lab, «¿Qué es un botnet? - Definición,» Kaspersky Lab, [En línea]. Available: https://latam.kaspersky.com/resource-center/threats/botnet-attacks. [Último acceso: 15 03 2023].

[8] E. d. NortonLifeLock, «¿Qué es un troyano?,» NortonLifeLock, [En línea]. Available: https://lam.norton.com/blog/malware/what-is-a-trojan. [Último acceso: 16 04 2023].

[9] G. Atico34, «Aplicaciones maliciosas para Android: un peligro para tu seguridad,» Grupo Atico34 , [En línea]. Available: https://protecciondatos-lopd.com/empresas/aplicaciones-maliciosas/. [Último acceso: 17 04 2023].

[10] Malwarebytes, «Ransomware,» Malwarebytes, [En línea]. Available: https://es.malwarebytes.com/ransomware/. [Último acceso: 1 03 2023].

[11] J. Weiss, «The Colonial Pipeline cyberattack – Did IT/OT convergence contribute to the attack,» Control Global, 11 05 2021. [En línea]. Available: https://www.controlglobal.com/home/blog/11292226/information-technology. [Último acceso: 2022 12 20].

[12] F. M. Medina Carranza, *Seguridad Informática: virus ransomware, el Secuestro virtual de datos es Posible,* Buenos Aires, CABA: Universidad Siglo 21, 2017.

[13] Malwarebytes, «Ransomware,» Malwarebytes, 2022. [En línea]. Available: https://es.malwarebytes.com/ransomware/. [Último acceso: 15 12 2022].

[14] Acronis, «El ransomware: qué es y por qué es tan peligroso,» Acronis, 17 10 2018. [En línea]. Available: https://www.acronis.com/es-es/blog/posts/ransomware-protection/. [Último acceso: 2022 12 16].

[15] Portinos, «El 29% de las empresas en Argentina reconoció haber sido víctima de ciberataques,» Portinos, 10 02 2020. [En línea]. Available: https://blog.portinos.com/novedades/el-29-de-las-empresas-en-argentina-reconocio-haber-sido-victima-de-ciberataques. [Último acceso: 2023 04 16].

[16] J. M. Harán, «29 datos que deja el 2020 que hablan del estado actual de la ciberseguridad,» ESET Latinoamérica, 22 12 2020. [En línea]. Available: https://www.welivesecurity.com/la-es/2020/12/22/datos-2020-sobre-estado-actual-ciberseguridad/. [Último acceso: 2022 12 16].

[17] Fortinet, «Fortinet Threat Intelligence Insider Latin America» 08 08 2019. [En línea]. Available: https://www.fortinetthreatinsiderlat.com/es/Q4-2019/landing. [Último acceso: 08 08 2020].

[18] iPro UP, «iPro Up,» 03 03 2020. [En línea]. Available: https://www.iproup.com/innovacion/11963-seguridad-argentina-recibio-1-590-millones-de-ciberataques-en-2019. [Último acceso: 09 08 2022].

[19] Cisco, «Cisco Advanced Malware Protection» 2015. [En línea]. Available: https://www.cisco.com/c/dam/global/es_mx/assets/pdfs/cisco_advanced_malware_protection_breach_prevention_so_es_xl.pdf. [Último acceso: 07 08 2020].

[20] J. J. Cano, Ciberseguridad Empresarial, Bogotá: Lemoine Editores, 2021.

[21] T. N. C. S. Centre, The Cyber Security Body of Knowledege, UK, 2019.

[20] NIST, «Marco para la mejora de la seguridad cibernética en infraestructuras críticas,» 16 04 2018. [En línea]. Available: https://www.nist.gov/.