El ransomware, el software malicioso usado para atacar a las organizaciones

primero la gente

Secretaría de Innovación Tecnológica del Sector Público

Jefatura de Gabinete de Ministros Argentina

El ransomware, el software malicioso usado para atacar a las organizaciones

El presente informe contiene información sobre el ransomware. Al igual que el resto de los textos publicados en esta página web, fue elaborado por la **Dirección Nacional de Ciberseguridad** para ser comprendido por todo tipo de lectores. Por tal motivo, se evitaron agregar contenidos y términos técnicos complejos.

Qué es el ransomware

El ransomware es un tipo de software utilizado generalmente por los cibercriminales para cifrar archivos o sistemas informáticos. El término incluye a todas las formas de código malicioso, como virus y gusanos informáticos. Su finalidad es *"secuestrar información"* y, de esta manera, impedir a una persona u organización el acceso a sus datos o dispositivos hasta que se haya pagado un dinero como rescate, que frecuentemente suele ser en criptomonedas para permitir al ciberdelincuente ocultar su rastro.

Si observamos estos ataques, notaremos que las víctimas pertenecen a diversas industrias, tanto del sector público como del privado. Debido a que nadie está exento de convertirse en víctima del ransomware, su propagación lo ha convertido en un gran negocio para los atacantes, provocando pérdidas anuales de cientos de millones de dólares.

El ransomware se propaga, como otros tipos de malware, por múltiples vías. Algunas de ellas son a través de campañas de spam, vulnerabilidades o malas configuraciones de software, actualizaciones de software falsas, canales de descarga de software no confiables y herramientas de activación de programas no oficiales.

Los ciberdelincuentes tratan de que el usuario abra un archivo adjunto infectado o haga clic en un vínculo que lo lleve al sitio web del atacante, donde será infectado. De este modo, los atacantes utilizan cada vez más tácticas, como eliminar las copias de seguridad del sistema, que hacen que la restauración y la recuperación sean más difíciles o inviables para las organizaciones afectadas (o en forma local).

La evidencia demuestra que aparecen nuevas y mejoradas versiones que necesitan de la asistencia de técnicas de ataques, como ingeniería social y otros malware, para ingresar en un sistema. Frente a estas vulnerabilidades, debemos trabajar en la creación de una Internet segura y prepararnos para enfrentar los desafíos de una realidad hiperconectada, creando conciencia y diseñando estrategias de seguridad de la red que sean robustas y actualizadas.

Como se puede observar, el ransomware es una de las amenazas más peligrosas para las organizaciones, pero la naturaleza y el alcance de sus ataques a menudo se malinterpretan, lo que lleva a precauciones inadecuadas, respuestas incorrectas y a ataques exitosos.

La realidad es que esta clase de código malicioso, a menudo, se implementa como parte de un ataque más grande que puede implicar penetración de la red, robo de credenciales para cuentas críticas del sistema, ataques a la consola de administración de copias de seguridad y robo de datos.

Este proceso puede tardar semanas o incluso meses en lograrse, y a menudo deja al malware profundamente integrado en los sistemas de toda la organización. Cuando se completa este trabajo, el ransomware se implementa para cifrar datos críticos, incluido el almacén de copias de seguridad, si es accesible en la red.
Los ataques devastadores de esta naturaleza se están volviendo cada vez más frecuentes, tardando días o incluso semanas en recuperarse, y se estima que la recuperación total no siempre sea posible.

El ransomware es probablemente una de las amenazas cibernéticas más graves a las que se enfrentan personas usuarias y, sobre todo, organizaciones privadas y gubernamentales. ¿Por qué? Porque, en los últimos años, las bandas criminales -que crean este tipo de malware y lo ofrecen como servicio- han estado perfeccionando un enfoque diferente con objetivos más específicos, y las métricas de estos ataques son mucho más difíciles de obtener.

Además, los ciberdelincuentes están constantemente ideando nuevos métodos para asegurarse el pago del rescate, como por ejemplo aumentando la presión sobre la víctima.

En los últimos años se ha visto una transición en los ataques de ransomware porque pasaron de ser ataques masivos (que apuntaban a un gran número de personas y solicitaban sumas modestas de rescates) a ser ataques dirigidos a sectores específicos, exigiendo montos mucho mayores a grupos de víctimas más pequeños. Estas víctimas elegidas tienen bolsillos más grandes y miembros que no pueden permitirse perder el acceso o el control de sus datos.

Cómo opera el ransomware

Una vez que el ciberdelincuente cifró los datos, es habitual que incluya un límite de tiempo para pagar, antes de que se produzca la destrucción total de los archivos secuestrados, su publicación o un incremento del valor del rescate, si no se paga a tiempo.

Los datos, ya sean considerados de propiedad personal, profesional o intelectual son, en todo caso, confidenciales y valiosos. La presión se incrementa cuando las personas u organizaciones pueden llegar a sufrir daños a la reputación, interrupciones comerciales o incluso sanciones legales y financieras.

Las víctimas a menudo ven afectadas múltiples facetas de sus puntos de contacto digitales, desde ataques de denegación de servicios en sus sitios web hasta molestas demostraciones de la presencia de los cibercriminales en la red. Algunas de estas provocan una conmoción, como es el caso del print bombing, que consiste en utilizar las impresoras disponibles en la red de la víctima para imprimir el mensaje que exigen los ciberdelincuentes para el rescate. Esta situación impide que la gerencia pueda controlar la comunicación interna y externa sobre el incidente.

En resumen, el ransomware puede convertirse de un incidente de malware desafortunado en una guerra psicológica, cuyo objetivo es obligar a las víctimas a actuar contra su propia voluntad y sus intereses.

Al hacer un paralelismo entre los secuestradores que actúan en el espacio físico y el virtual, podemos ver las ventajas que tienen los ciberdelincuentes. Los delincuentes involucrados en secuestros físicos suelen comenzar sus "campañas de presión'' con una ventaja, pero pueden quedarse sin opciones más adelante. En cambio, los ciberdelincuentes cuentan con una variedad aún más amplia de métodos a los que recurrir, para ganar influencia y desestimar cualquier esperanza de recuperación sin problemas, resguardándose detrás del anonimato.

Para lograr sus objetivos maliciosos, los atacantes utilizan una gran cantidad de enfoques que les permiten obtener acceso remoto, monitorear las actividades de sus víctimas y luego aplicar una presión extremadamente precisa. Esto demuestra el poder que tienen sobre los datos, las redes, la continuidad del negocio y la reputación de sus víctimas. De hecho, estos ataques no provienen necesariamente de malware personalizado, exploits 0-day[1] ni campañas persistentes a largo plazo.

Pueden ser tan solo el resultado de malas prácticas de seguridad por parte de los empleados, una mala configuración del Protocolo de escritorio remoto (RDP) u otras herramientas de acceso remoto, o prácticas y procesos defectuosos, tanto dentro de su propia organización como de sus proveedores de servicios u otros eslabones de su cadena de suministro.

En qué consiste el cifrado de información

Cuando hablamos del cifrado criptográfico de información, nos referimos a una operación matemática que toma un dato y una clave, y modifica el dato en base a esta última. Para que el dato vuelva a su forma original, se debe aplicar una función de descifrado. En otras palabras, el cifrado consiste en ocultar la información con técnicas de codificación para evitar que los datos sean legibles por quien no tenga la clave de decodificación.

Existen dos esquemas de criptografía:

• **Criptografía simétrica:** se utiliza una sola clave, tanto para la función de cifrado como para la del descifrado.

• **Criptografía asimétrica:** se utilizan dos claves vinculadas entre sí, llamadas usualmente clave pública y clave privada. Todo lo que se cifra con una de las claves sólo puede ser descifrado con la otra. Es decir, si se utiliza para cifrar la clave pública sólo podrá descifrarse con la clave privada o viceversa.

En general, los ransomware aplican un esquema de criptografía simétrica sobre la información que afectan, generando claves de cifrado aleatorias. Estas claves se transmiten por Internet a

[1] Es un ataque contra una aplicación o sistema que tiene como objetivo la ejecución de código malicioso gracias al conocimiento de vulnerabilidades que son desconocidas para los usuarios y para el fabricante del producto.

los servidores de los atacantes, de modo que puedan ser enviadas a la víctima luego de pagado el rescate.

En algunos casos, también utilizan un esquema asimétrico para almacenar, junto con los archivos de la víctima, las claves utilizadas para cifrar la información. De esta forma, no necesitan contar con conexión a Internet al momento de cifrar los archivos. Simplemente cifran con la clave pública las claves de cifrado de los archivos y, al recibir el pago, enviarán un software de descifrado que conoce la clave privada necesaria para recuperar las claves.

Niveles de extorsión que utilizan los atacantes

En 2019, los ciberdelincuentes que utilizan el ransomware implementaron una doble extorsión, que combina el cifrado de datos habitual con la extracción de datos para su divulgación. De esta manera, no sólo le impiden a la víctima el acceso a sus archivos valiosos, críticos o confidenciales, sino que también amenazan con exponerlos públicamente o venderlos a otros actores maliciosos.

Actualmente, existen diferentes niveles o marcos de extorsión:

• Primera extorsión: consiste en el cifrado de la información, y la exigencia de un pago para recuperarla.

• Doble extorsión: además del cifrado, se amenaza con filtrar públicamente la información secuestrada.

• Triple extorsión: se añaden ataques de denegación de servicio, afectando aún más la disponibilidad de los servicios afectados por el cifrado de la información.

• Cuádruple extorsión: los atacantes se comunican con clientes y proveedores de la víctima para exponer la situación y, eventualmente, filtrar información. En algunos casos, exigen el pago directamente a los proveedores y/ o clientes de la víctima.

Cada uno de estos niveles o marcos de extorsión contiene a los anteriores. Así, el último contiene a los tres anteriores, el tercero a los dos anteriores y el segundo al primero.

La seguridad de la información, la clave para prevenir el ransomware

Es necesario que se implementen procesos y políticas para garantizar la seguridad de las instalaciones y de los sistemas. Un escenario bastante común es que una organización sea

atacada a través de un activo conectado a Internet, que el personal de seguridad de la organización no sabía que existía hasta después del ataque.

Sin embargo, por más que se hayan implementado las políticas y protocolos de seguridad o se esté trabajando para implementarlos, las reglas por sí solas no garantizarán la seguridad total de los accesos.

Aún será necesario que la organización se asegure de que todo el personal cumpla con las instrucciones y, que al mismo tiempo, estén preparados para manejar un ataque, es decir, para saber qué hacer ante un incidente, cómo resolverlo y volver a estar operativos.

Cabe destacar que cualquier organización que tenga un programa de seguridad de la información maduro detectará y bloqueará un ransomware embebido en un archivo adjunto de un correo electrónico entrante y que, en muchos casos, el atacante logrará igual su cometido a pesar de la existencia de medidas preventivas.

Asimismo, la organización deberá contar con políticas para abordar la seguridad del acceso remoto. Las recomendaciones se sustentan en diferentes estrategias y técnicas:

A. Documentar el problema: asegurarse de que todos los activos conectados a Internet de su organización sean conocidos por las personas a las que se les ha asignado la tarea de protegerlos. Disponer de un proceso para garantizar que se incluyan todos los dispositivos nuevos.

B. Limitar los activos expuestos: asegurarse de que ningún activo digital sea accesible de manera remota directamente desde Internet, a menos que haya sido aprobado para usarse de esa manera y esté configurado adecuadamente.

C. Proteger los activos expuestos: si definitivamente se debe usar el Protocolo de escritorio remoto (RDP) sin una red privada virtual (VPN), se deben tener en consideración las siguientes sugerencias:

a. Cambiar la contraseña de la cuenta de usuario a la que se está conectando en la máquina remota con regularidad. Asegurarse de cambiar la contraseña predeterminada que a veces se genera automáticamente para las instancias en la nube.

b. Hacer cumplir la complejidad de la contraseña. Es obligatorio que sea una frase de contraseña larga que contenga más de 15 caracteres, sin frases relacionadas con la organización, con los nombres de productos o con los usuarios.

c. Establecer un límite de bloqueo de cuenta para bloquear el acceso remoto después de cierta cantidad de intentos fallidos consecutivos de inicio de sesión. Al configurar la computadora para que bloquee una cuenta durante un período de tiempo tras una serie de conjeturas incorrectas, obstaculizará a los atacantes que utilizan herramientas automáticas de adivinación de contraseñas (ataque por fuerza bruta).

d. Probar e instalar los parches para todas las vulnerabilidades conocidas y asegurarse de que las más conocidas y obvias se encuentren entre los defectos corregidos. Si los parches no se pueden instalar en una computadora determinada, planificar su reemplazo oportuno.

e. Utilizar más de un factor de autenticación. Hay tres factores posibles: algo que uno sabe, como el nombre de usuario y la contraseña; algo que uno es, como la huella dactilar o de voz; y algo que uno tiene, como el teléfono, que puede recibir un código de acceso de un solo uso o ejecutar una aplicación de autenticación que generará el código cuando lo necesite. Sin embargo, si usa como segundo factor un código enviado a un teléfono, evitar los códigos por SMS, porque los delincuentes ya se las ingeniaron para interceptar este tipo de mensajes de autenticación.

f. Restringir los derechos de acceso al servidor para un grupo limitado de usuarios. Esto reduce la superficie de ataque de los servidores, ya que limita la cantidad de usuarios que pueden acceder a ellos.

g. Aislar las computadoras no seguras a las que se deba acceder desde Internet usando el Protocolo de acceso remoto (RDP).

Algunas modalidades de ataques de ransomware

El uso de software legítimo o "living off the land "

Algunos atacantes intentan introducir un fragmento de código malicioso lo más pequeño posible para minimizar la detección. A continuación, el malware emplea la estrategia conocida en inglés como *"living off the land"* (LotL), es decir, hace uso de software legítimo para extender su penetración en la red.

Como existen razones válidas para que se estén ejecutando estos programas, detectar su uso indebido por parte de un atacante puede ser difícil, aunque no imposible.
Uno de los ejemplos más arquetípicos, en donde los atacantes se aprovecharon de vulnerabilidades no corregidas en un software legítimo del sistema, fue el reconocido ransomware WannaCryptor, que se propagó usando indebidamente una vulnerabilidad de alta severidad.

A pesar de que los parches estaban disponibles al público desde hacía dos meses antes de la campaña de WannaCryptor, que comenzó el 12 de mayo de 2017, los atacantes lograron encontrar e infectar más de 200.000 máquinas vulnerables. Incluso en las últimas etapas de este brote, los dispositivos infectados continuaron siendo una amenaza, por ejemplo, cuando los usuarios llevaban, sin saberlo, computadoras portátiles infectadas a lo que los administradores consideraban un perímetro seguro.

Naturalmente, en algunos casos existe la posibilidad de que el primer punto de contacto entre el atacante y la organización sea un servidor que aloja una base de datos crítica. Un delincuente oportunista podría decidir que prefiere ahorrar algo de tiempo y esfuerzo y buscará una victoria rápida simplemente robando datos, cifrándolos y pidiendo un rescate por los archivos de ese único servidor.

Sin embargo, se puede ganar mucho más mediante la persistencia, por lo que es probable que en la mayoría de los casos los operadores de ransomware continúen llevando a cabo un

proceso de reconocimiento, incluso después de haber robado los datos y antes de cifrarlos, solo para asegurarse de que tienen suficiente influencia.

Cómo evitar los ataques LotL

Los ciberataques *Living off the Land* pueden suponer graves consecuencias para las organizaciones que los sufran, como ya pasó a nivel global con los ataques NotPetya en 2017, de modo que se deben arbitrar las medidas necesarias para prevenirlos.

A. Será clave ejercer un acto de monitorización y seguimiento del sistema informático, atendiendo a todos los procesos que esté albergando para encontrar acciones sospechosas y accionar a tiempo.

B. Contar con una solución de ciberseguridad avanzada capaz de monitorizar todos los procesos del sistema en busca de comportamientos anómalos o posibles amenazas para acabar con ellas antes de que se manifiesten, entre otras.

Movimiento Lateral

El término movimiento lateral se utiliza para describir la estrategia de afianzarse en un sistema y utilizarlo para infectar otros dispositivos a los que se puede llegar desde allí. Por ejemplo, los atacantes pueden utilizar credenciales comprometidas para infectar un servidor que ni siquiera está presente en la organización objetivo, y luego usar su conexión a la infraestructura principal para entregar el ransomware.

Cómo prevenir los ataques de movimiento lateral en la red

A. Detectar en tiempo real y analizar las amenazas dentro de la red, captando el robo de credenciales, el esparcimiento lateral de programas maliciosos, ransomware y de ataques dirigidos dentro de redes de usuarios, centros de datos, nube, entornos IOT[2] y SCADA[3].

B. Establecer alertas fundamentadas, evaluación de vulnerabilidades de las rutas de ataque, análisis detallado e informes y reproducción de ataques transcurridos en el tiempo para fortalecer las defensas generales.

C. Realizar pruebas de penetración puede ayudar a las organizaciones a cerrar las partes vulnerables de la red que podrían permitir un movimiento lateral. En las pruebas de penetración, una organización contrata a un hacker ético para que ponga a prueba su seguridad intentando penetrar lo más profundamente que sea posible en la red sin ser detectado. El hacker explica entonces a la organización lo que ha encontrado, y esta puede utilizar esta información para arreglar los agujeros de seguridad que haya utilizado el hacker.

D. La seguridad Zero Trust es una filosofía de seguridad de red que no confía por defecto en ningún usuario, dispositivo o conexión. Una red Zero Trust asume que todos los usuarios y

[2] Internet de las cosas (IoT) describe la red de objetos físicos ("cosas") que llevan incorporados sensores, software y otras tecnologías con el fin de conectarse e intercambiar datos con otros dispositivos y sistemas a través de Internet. Los entornos o plataformas IoT son el software que permite conectar dispositivos, sensores, actuadores y equipos industriales en un entorno digital, generando una red para que éstos puedan comunicarse y crear información valiosa.

[3] SCADA es el acrónimo de Supervisory Control And Data Acquisition, que es un concepto que se emplea para realizar un software para ordenadores que permite controlar y supervisar procesos industriales a distancia. Facilita retroalimentación en tiempo real con los dispositivos de campo, y controla el proceso automáticamente.

dispositivos representan una amenaza y reautentica continuamente tanto a los usuarios como a los dispositivos. Zero Trust también utiliza un enfoque de mínimos privilegios para el control de acceso y divide las redes en pequeños segmentos. Estas estrategias hacen que la escalada de privilegios sea mucho más difícil para los atacantes, y facilita a los administradores de seguridad la detección y puesta en cuarentena de la infección inicial.

E. La seguridad en los puntos de conexión implica escanear con regularidad los dispositivos de los puntos de conexión (ordenadores de escritorio, portátiles, teléfonos inteligentes, etc.) con software antimalware, entre otras tecnologías de seguridad.

F. Gestión de acceso e identidad correcta (IAM) es un componente fundamental para evitar el movimiento lateral. Los privilegios de los usuarios se tienen que gestionar de forma estricta: si los usuarios tienen más privilegios de los que realmente necesitan, las consecuencias de una toma de posesión de la cuenta son todavía más graves.

G. Además, el uso de la autenticación en dos fases (2FA), que significa exigir a un usuario que demuestre su identidad de dos maneras diferentes antes de concederle acceso, lo cual puede ayudar a detener el movimiento lateral. En un sistema que utiliza 2FA, obtener las credenciales del usuario no es suficiente para que un atacante ponga en riesgo una cuenta; el atacante también tiene que robar el token de autenticación secundario, lo cual es mucho más difícil.

Amenazas dirigidas al Protocolo SMB

El protocolo Bloque de Mensajes del Servidor (SMB), que se utiliza sobre todo para compartir archivos e impresoras en redes corporativas, también se puede usar indebidamente como un servicio remoto para introducir el ransomware.

En el primer cuatrimestre de 2021, las tecnologías de una empresa privada bloquearon 335 millones de ataques por fuerza bruta a servicios SMB orientados al público. Aunque esa cifra representa una disminución del 50% en comparación con la de los últimos cuatro meses del 2020, los ataques a través de SMB siguen siendo una amenaza importante. Además, el WannaCryptor, que abarcó el 41% de las detecciones de ransomware en este mismo primer cuatrimestre de 2021, se propaga mediante el aprovechamiento de vulnerabilidades en el protocolo SMBv1.

Recomendaciones para protegerse contra las amenazas dirigidas al protocolo SMB:

A. Deshabilitar SMBv1 y SMBv2. Tener en cuenta que se deberá gestionar cualquier dependencia existente en estas versiones obsoletas.

B. Actualizar a la última versión del protocolo SMB, que actualmente es SMBv3.

C. Utilizar la configuración de la directiva de grupo para asegurar que se requiera la firma de SMB entre los hosts y los controladores de dominio para evitar ataques de reproducción en su red, entre otras.

Ataques de ransomware por correo electrónico

Algunos atacantes todavía siguen usando archivos adjuntos en correos electrónicos para instalar malware como etapa inicial de una infección que termina con ransomware. Los ciberdelincuentes pueden usar este vector para instalar malware en la máquina del destinatario del correo electrónico o para lograr afianzarse en una máquina que está dentro de la red de una organización. Esta presencia les sirve de base para luego intentar robar los datos valiosos y cifrar los archivos de toda la organización, para más tarde hacer un pedido de rescate.

En enero de 2021, se produjo un aumento en los correos electrónicos que entregaban documentos maliciosos. En octubre de 2020, una botnet[4] popular, Trickbot, sufrió la interrupción de una parte de su infraestructura. Sin embargo, parece haber sido solo un revés temporal, ya que sus operadores no tardaron mucho en lanzar una nueva campaña de phishing en enero de 2021 dirigida a empresas de seguros y servicios jurídicos en América del Norte.

Recomendaciones para proteger a la organización contra ataques de ransomware provenientes del correo electrónico:

La primera línea de defensa es filtrar todo el correo entrante en busca de spam y mensajes de phishing.

Es posible ir un paso más lejos mediante la implementación del bloqueo de todos los tipos de archivos adjuntos que la organización normalmente no espera recibir por correo electrónico. Sin embargo, esta estrategia sólo será adecuada para ciertos tipos de sectores y probablemente requerirá cambiar algunos hábitos de trabajo.

Por ejemplo, si los empleados acostumbran a enviarse hojas de cálculo y documentos de textos por correo electrónico es posible que la organización deba adoptar primero una solución o un marco de colaboración seguro para compartir archivos, y hacer que el personal comience a utilizar la nueva modalidad antes de bloquear rigurosamente los archivos adjuntos al correo electrónico con un filtrado más estricto.

Verificar que todos los endpoints (dispositivos informáticos remotos que se comunican a una red a la que están conectados, como por ejemplo ordenadores de escritorio o portátiles, tablets, servidores y estaciones de trabajo) estén ejecutando un software de protección de alta calidad. De esa manera, se espera evitar que los empleados accedan a páginas web, donde se sabe que se alojan malware. También se puede utilizar el filtrado de contenido web como capa adicional de protección.

Además de bloquear sitios web maliciosos, un filtro de contenido web puede impedir que los empleados visiten sitios web que se consideran inapropiados en el ámbito laboral.

Asimismo, será necesario verificar que todos los dispositivos estén ejecutando la última versión del producto de seguridad y que estén recibiendo correctamente las actualizaciones. Si un proveedor tiene un componente en la nube, es recomendable asegurarse de que esté activado, ya que permite una reacción aún más rápida a las nuevas amenazas.

[4] Es un término que hace referencia a un conjunto o red de robots informáticos o bots, que se ejecutan de manera autónoma y automática. El creador de la botnet puede controlar todos los ordenadores/servidores infectados de forma remota.

La instalación rápida y completa de los parches para sistemas operativos y aplicaciones ayudará a evitar que el ransomware ingrese a través de archivos adjuntos de correo electrónico o descargas no autorizadas. La configuración segura también puede resultar útil.

Otra medida, será mantener actualizada la capacitación en ciberseguridad de los empleados para que refleje las últimas tendencias en el panorama de amenazas. Ello logrará reducir la cantidad de incidentes de malware con los que tiene que lidiar la organización si se les informa a los empleados qué buscar y qué evitar en relación con el phishing y otros contenidos maliciosos. Las advertencias tempranas ayudan a la organización a ajustar sus filtros de contenido y correo no deseado, así como a reforzar sus firewalls y otras defensas.

Ataques de ransomware por cadena de suministro

Un vector de ataque de ransomware que merece especial atención en la actualidad es la cadena de suministro de software[5]. Así como el ransomware se remonta al siglo pasado, los riesgos en la cadena de suministro de software también. Cuando el vector de ataque principal para los virus informáticos eran los discos de computadora, y estos eran la forma principal en que las personas adquirían software, el malware a veces terminaba en discos de producción o en los discos de software de prueba que solían distribuirse con revistas de informática.

Recomendaciones para protegerse de ataques de ransomware por cadena de suministro.

A. La primera línea de defensa contra este tipo de ataques es tener un buen producto de protección para endpoints que incluya herramientas de EDR[6]. De esta forma, debido al impacto que pueden provocar estos ataques y a las mitigaciones que luego pueden requerir, los investigadores y administradores de seguridad deben mantenerse atentos.

B. Defenderse contra este tipo de ataque implica mantenerse al día con los parches, usar software de protección para endpoints, utilizar soluciones EDR y educar a los usuarios sobre los correos electrónicos no solicitados que los persuaden para que visiten sitios web desconocidos.

Ataques por vulnerabilidades

Si bien los ciberdelincuentes pueden beneficiarse tanto de las vulnerabilidades conocidas como de las desconocidas, el uso de vulnerabilidades 0-day[7] por lo general pertenece al mundo de los grupos de Amenaza Persistente Avanzada (APT)-un conjunto de amenazas sofisticadas que evaden las herramientas de seguridad tradicionales- y los actores maliciosos patrocinados por Estados.

Un ejemplo es el hecho de que casi todos los fabricantes de seguridad cibernética todavía siguen detectando el exploit EternalBlue (de 2017) y sus muchas variantes, como así también

[5] Es la herramienta de software que se utiliza para ejecutar transacciones de la cadena de suministro, administrar las relaciones con los proveedores y controlar los procesos empresariales asociados.

[6] Endpoint Detection and Response (conocida por sus siglas en inglés EDR) es una herramienta que proporciona monitorización y análisis continuo del endpoint y la red. La finalidad es identificar, detectar y prevenir amenazas avanzadas (APT) con mayor facilidad.

[7] Una vulnerabilidad de día cero es un fallo de seguridad de software descubierto recientemente para el que aún no existe un parche porque los desarrolladores de software desconocían su existencia.

el aprovechamiento continuo de vulnerabilidades en el protocolo SMBv1 para el intercambio de archivos.

Antes de avanzar, cabe aclarar que un exploit es un ataque que aprovecha las vulnerabilidades de las aplicaciones, las redes, los sistemas operativos y/o el hardware. Generalmente, toman la forma de un programa de software o de una secuencia de código previsto para tomar el control de los ordenadores o robar datos de la red.

La larga vida útil de las vulnerabilidades y amenazas, como WannaCryptor, generalmente se debe a la falta de instalación de actualizaciones y parches en empresas e instituciones.

Paralelamente, la creciente complejidad del panorama de amenazas ha producido nuevas herramientas para combatir tipos de ataques más modernos, pero estas herramientas también implican una carga técnica adicional: estar atento a las vulnerabilidades de los productos y llevar a cabo una administración cuidadosa de los parches.

El uso de las redes privadas virtuales (VPN) en grandes instituciones y empresas, si bien es altamente efectivo, añade una responsabilidad adicional con respecto a la actualización del producto cuando sea necesario. Este enfoque en las actualizaciones oportunas debe acompañarse por la implementación de la autenticación en varias fases para iniciar sesión en sus respectivos servicios VPN. Si surge la sospecha de un abuso de credenciales, las organizaciones deben restablecer las cuentas por completo. Estos desafíos también se reflejan en el aumento global en el uso de grandes plataformas de productividad y colaboración.

Otras medidas preventivas

Segmentación de la red

Independientemente del vector de ataque empleado por el ransomware, si ingresa a la organización, es muy probable que intente propagarse a tantas máquinas como pueda, lo que posiblemente afectará todas las operaciones de la organización. Está claro que limitar la cantidad de máquinas a las que un atacante puede llegar desde un único punto de entrada tiene importantes beneficios como estrategias defensivas.

Existen varios enfoques para implementar una estrategia de ese tipo y el más importante es la segmentación de la red, que consiste en una técnica de seguridad que divide una red en distintas subredes más pequeñas, que permiten a los equipos de red compartimentar las subredes y otorgar controles y servicios de seguridad únicos a cada subred. El análisis de los detalles de la arquitectura de red está fuera del alcance del presente informe. No obstante, toda organización necesita comprender las fortalezas y debilidades de seguridad de la arquitectura de red actual. Una auditoría simple basada en preguntas y respuestas puede mejorar esa comprensión. Será recomendable preguntarse, por ejemplo: “¿Puedo ir de acá hasta allá?” o “¿Qué impide que alguien pueda llegar desde allá hasta acá?”.

Seguridad en la nube

Una estrategia de arquitectura de sistemas popular en los últimos años ha sido mover datos a la nube, pero esta no proporciona inmunidad automática contra los ataques de ransomware (a pesar de los esfuerzos de proveedores poco escrupulosos para crear la impresión de que la nube es sinónimo de seguridad).

De hecho, el bajo costo y la relativa facilidad con la que se pueden aprovisionar nuevos servidores en la nube y conectarlos al resto de la infraestructura digital de la organización han convertido a ésta en un terreno de caza fértil para los delincuentes. Sin duda, cualquier uso de la nube por cualquier parte de la organización debe estar debidamente autorizado y configurado de manera segura. Además, como todos los otros sistemas, los que están en la nube deben tener programado un régimen apropiado de creación de backups y recuperación.

La instalación de parches (que consiste en una pieza de software para hacer mejoras, actualizaciones, reparar errores o añadir una nueva funcionalidad) y la creación de backups son dos aspectos del funcionamiento y la administración de sistemas que desempeñan un papel fundamental en la defensa contra un ataque de ransomware. Al mantener un sistema con los parches al día, se cierran las posibles vías de ataque y puede evitar que el ransomware ingrese a la organización o, si lo hace, reducir el daño que pueda causar.

Por supuesto, como sabe todo administrador de sistemas, la aplicación de parches puede ser mucho más complicada de lo que parece. Los parches y las actualizaciones deben probarse antes de su implementación.

Algunos de los sistemas de tu organización pueden depender de software que deja de funcionar cuando actualiza a la última versión de una aplicación o sistema operativo. Sin embargo, el elevado costo de un ataque de ransomware dentro de su red justifica el esfuerzo de abordar esos desafíos y mantener un régimen de instalación de parches rápido y completo para que el ransomware se quede afuera.

Creación de backups

Se suele decir que si el ransomware ingresa a la organización, un programa de backup y recuperación completa, adecuadamente administrado, es un mecanismo de defensa vital y constituye un elemento crucial para la recuperación posterior. Hay mucha verdad en esta afirmación y son varias las buenas razones para tener un programa de este tipo, pero hay que recordar que algunos ataques de ransomware se ejecutan en un período de tiempo prolongado, durante el que también puede haber hecho un backup del ransomware, comprometiendo así la posibilidad de lograr una restauración sin problemas.

Es por eso que el backup no es una defensa para configurar y olvidarse, debe ser monitoreado y administrado, y el proceso de recuperación debe probarse con regularidad. En estos días, existen más opciones que nunca para hacer backups y recuperar los datos, en especial gracias al almacenamiento en la nube, ya sea de manera remota, local o híbrida.

Sin embargo, también hay más datos para respaldar desde más ubicaciones. A menos que tenga una estrategia de backup completa, siempre existe la posibilidad de que los actores que suministran el ransomware encuentren aquel dispositivo que olvidó incluir en el último backup.

Un backup completo incluye los datos y el estado del sistema en todas los endpoints, servidores, buzones de correo, unidades de red, dispositivos móviles y máquinas virtuales. El análisis detallado de la estrategia de backup y recuperación para grandes corporaciones está fuera del alcance del presente white paper, pero debe quedar claro que contar con una estrategia de este tipo es más crítico que nunca.

El ransomware simplemente se suma a la larga lista de razones por las que la organización no debe escatimar en esta parte del programa de TI[8]. Sin embargo, existen algunas advertencias específicas para el ransomware. Por ejemplo, cuando el almacenamiento está "siempre activo", su contenido puede ser vulnerable al ransomware de la misma manera que lo es el almacenamiento local u otro conectado a la red.

Para evitar que lo intercepte el ransomware, se deberá optar por un almacenamiento externo que:

• No esté online en forma rutinaria y permanente;

• Proteja los datos respaldados de modificaciones o sobreescrituras automáticas y silenciosas por malware cuando la instalación remota esté online;

• Proteja las generaciones anteriores de datos respaldados contra las infecciones, de modo que incluso si ocurre un desastre en los últimos backups, al menos se puedan recuperar algunos datos, incluyendo las versiones anteriores de los datos actuales;

• Proteja al cliente detallando las responsabilidades legales o contractuales del proveedor, por ejemplo, que indique qué sucede si el proveedor cierra, etc.

Por supuesto, existen muchas otras razones por las que la organización necesita implementar un programa de backup y recuperación, por ejemplo, en caso de incendios, inundaciones, daños por tormentas, etc.

Casos resonantes de ataques de ransomware

- **El WannaCry**

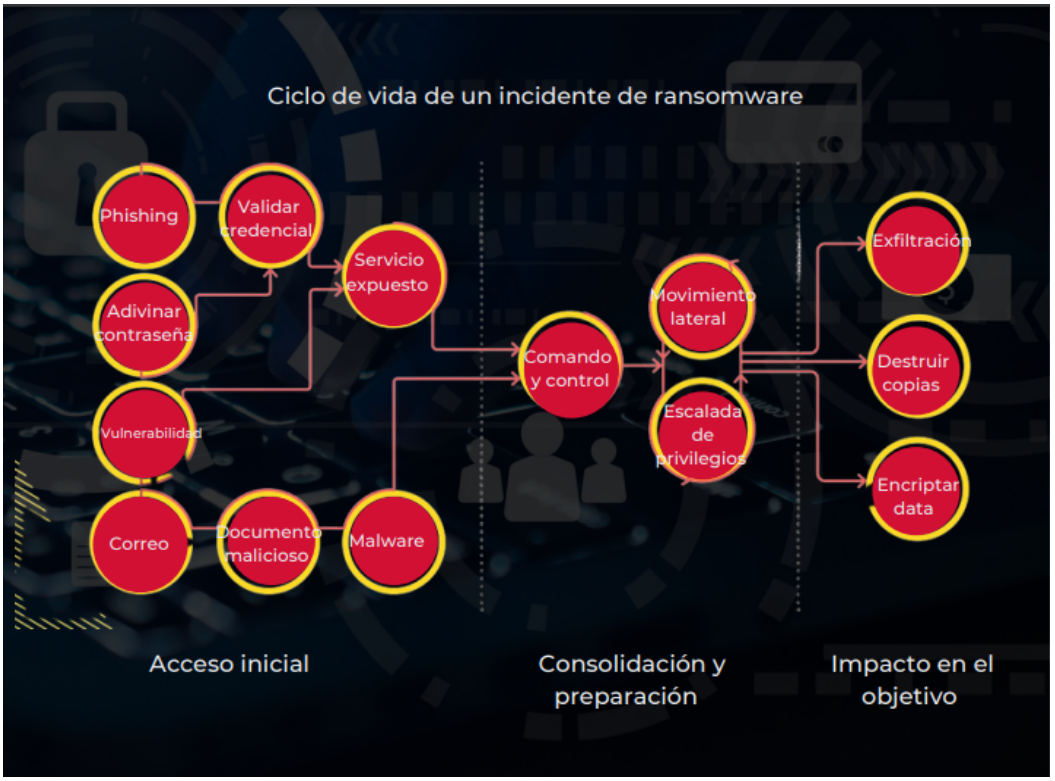
El WannaCry o WannaCryptor es un tipo de ransomware que comenzó a propagarse en mayo de 1017, con el objetivo de cifrar los archivos de los equipos infectados, para pedir luego un rescate en BitCoins. Se viraliza a partir de un archivo aparentemente inofensivo que la

[8] Se basa en el estudio y desarrollo de sistemas de información como aplicaciones software y hardware de computadoras, que se encarga de garantizar que las computadoras funcionen correctamente para los usuarios.

persona usuaria abre bajo un engaño y, que al ser ejecutado, encripta el contenido de la computadora.

Un ejemplo de esa situación puede ser la de un e-mail que urge a la víctima, mediante algún pretexto alarmante, a abrir el adjunto o hacer click en un link. Casi de inmediato aparece un cuadro que anuncia que los archivos del equipo han sido cifrados, así como las instrucciones para pagar el rescate y recibir la contraseña para descifrarlos. Para generar presión, le dice a la víctima que si no abona lo exigido, hará pública la información encriptada.

El programa se comporta como un gusano informático, es decir, que se propaga a través de las redes, porque no fue detectado por la mayoría de los antivirus. Atacó a las redes usando SMBv1, un protocolo de uso compartido de archivos que permite a las computadoras comunicarse con las impresoras y otros dispositivos conectados a la misma red.
El WannaCry, que traducido al castellano quiere decir "Quiero llorar", afectó a más de 170 países, donde los blancos fueron personas y muchas empresas.



- **Cryptolocker**

En informática, la forma más usual de infección de equipos es a través de la apertura de archivos adjuntos recibidos en correos electrónicos no solicitados o al hacer clic en vínculos que aseguran provenir de entidades bancarias o de empresas de mensajería. Sin embargo,

también se encontraron ataques de ransomware a través de redes peer to-peer (P2P)[9], utilizadas para compartir archivos de computadoras.

Uno de ellos fue el llamado Cryptolocker que simulaba ser claves de activación para programas populares de software como el famoso editor de fotografías o el paquete de oficina. Una vez que el equipo se infecta, Cryptolocker busca una amplia gama de archivos para cifrar y, al finalizar el ataque, muestra un mensaje que exige una transferencia electrónica para descifrar la información.

En algunos casos, la pantalla de bloqueo también incluye la transmisión en vivo de lo que la cámara web del equipo está viendo en ese momento. Esta maniobra se utiliza para que las personas usuarias con menos conocimientos técnicos piensen que realmente están siendo observados por las autoridades.

En el año 2013, esta clase de ransomware dejó medio millón de afectados, y fue distribuido originalmente a través de la botnet Zeus y, también, a través de correos electrónicos. En sus primeros meses, logró que los afectados pagasen rescates que, en total, sumaron 2,7 millones de euros. A diferencia de otros ransomwares, no bloqueaba todo el ordenador, sólo archivos personales como fotos, documentos e imágenes que guardaban en un servidor externo.

- **Ransomware del tipo LockScreen**

El ransomware de tipo lockscreen se caracteriza por bloquear el equipo e impedir que se lo utilice hasta que se realice el pago del rescate. Este malware utiliza a veces trucos psicológicos para engañar a la víctima y, así, apresurar el pago. Por ejemplo, en algunas ocasiones, en el mensaje de la pantalla de bloqueo se hacen pasar por un aviso de la policía. Se indica que las autoridades demandan el pago de una multa porque se encontraron en el equipo de la víctima imágenes de abuso contra personas menores de edad o de zoofilia, situación que, supuestamente, evidenciaría haber visitado sitios web ilegales o software pirata.

- **Gpcoder**

El ransomware Gpcoder se detectó en mayo de 2005 y, en un principio, usaba técnicas de cifrado débiles que eran fáciles de superar. Utilizaba algoritmos simétricos, es decir, que la clave para cifrar era la misma que para descifrar. Zippo y Archiveus fueron otros de los ransomwares primigenios.

- **Krotten**

En el año 2010, Krotten era un ransomware ucraniano que pedía el pago de 30 grivnas ucranianas (equivalente a 3 euros) a un operador de telefonía móvil de este país para recibir una clave de desbloqueo. Este código malicioso bloqueaba el sistema operativo de diversas formas, cambiaba varias claves de registro y añadía mensajes en ruso en el menú de inicio del famoso sistema operativo de ventanas.

- **Dorkbot**

[9] Una red peer-to-peer, red de pares, red entre iguales o red entre pares es una red de ordenadores en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre sí.

Dorkbot, una nueva variante de gusano bancario, fue utilizada en 2012 por los hackers para atacar cuentas de la plataforma de videollamadas Skype, así como de las redes sociales Facebook y Twitter.

La mecánica era la siguiente: se reproducía un mensaje seguido de un enlace malicioso, que llevó a que miles de usuarios de Skype descargaran un archivo. Al clickear ese archivo, empezaba a funcionar un software malicioso que bloqueaba el programa durante 48 horas. Para obtener el desbloqueo, los cibercriminales exigían un pago de 177 euros en ese plazo de tiempo o, de lo contrario, indicaban que todos los archivos iban a ser eliminados.

- **Cryptowall**

Cryptowall nació como un clon de Cryptolocker pero, a principios de 2014, ya había adoptado entidad propia. Entre marzo y agosto de ese año, ya tenía en su haber más de 600.000 sistemas infectados y 5.250 millones de archivos encriptados. Los usuarios resultaban atacados a través de anuncios con malware ubicados en dominios de distintas empresas y redes sociales. La versión 4.0 no sólo encripta los archivos sino que también les cambia los nombres aleatoriamente.

- **CTB-Locker**

Los creadores de CTB-Locker tenían una forma particular de operar ya que daban la posibilidad de desencriptar cinco documentos al azar antes de pagar el rescate, como una señal de "buena voluntad". Una vez recuperados esos archivos, el virus guiaba a la víctima para que supiera cómo comprar 8 bitcoins –unos 1.500 euros en 2015-, y dónde hacer la transacción, etc. El mensaje estaba en distintos idiomas, como inglés, alemán, holandés e italiano.

- **Vaultcrypt**

En el caso Vaultcrypt, cuando un usuario trata de acceder a un archivo afectado por este virus, le aparece un mensaje con una dirección a la que sólo se puede acceder desde el navegador Tor, utilizado en la Internet profunda, es decir, en la parte de "la red de redes" que no está indexada a los clásicos buscadores conocidos. El cibercriminal utiliza Tor para asegurase su anonimato, ya que su acceso le permite no ser detectado fácilmente por el tipo de diseño que contiene.

Una vez que la víctima llegó a la página de la dirección indicada y se registró, la contraseña viene en un archivo almacenado en el ordenador, se muestran los documentos encriptados y la cantidad a pagar. Vaultcrypt no sólo encripta sino que también introduce un software malicioso del tipo troyano, que roba las contraseñas almacenadas en el sistema.

- **Sodinokibi y REvil**

En enero del 2020, la empresa de cambios de divisa Travelex sufrió un ciberataque y se vio obligada a apagar todos sus sistemas y regresar a la modalidad clásica del lápiz y el papel. Además, el incidente forzó a la organización a desactivar su sitio web en treinta países.

Los responsables del ataque -un grupo conocido como "Sodinokibi" y "REvil"- le exigieron el pago de 6 millones de dólares. Decían tener acceso a la red de la compañía desde hacía seis

meses y aseguraban que, en ese período, habían robado mucha información confidencial (5 GB) sobre sus clientes. Aseguraban tener sus fechas de nacimiento y los números de sus tarjetas de crédito.

Si Travelex pagaba el rescate, los hackers decían que eliminarían esa información, de lo contrario, duplicarían el monto del rescate. Sus exigencias volverían a duplicarse cada dos días hasta llegar al séptimo, es decir, al límite máximo para vender la información a otros delincuentes.

Según trascendió, Travelex pagó 2.3 millones de dólares en bitcoins al grupo y logró reactivar sus sistemas tras dos semanas de inactividad. En agosto de 2020, la empresa se declaró insolvente.

- **Ragnar Locker**

En abril del 2020, se supo que el gigante de la electricidad Energías de Portugal (EDP) había sido víctima de un ataque. Un grupo de delincuentes logró cifrar los sistemas de la empresa utilizando el ransomware Ragnar Locker y exigió el pago de casi 10 millones de dólares.

Los atacantes aseguraban tener mucha información confidencial (más de 10 TB) y amenazaban con divulgarla si la empresa no pagaba el rescate. Para demostrar que contaban con esos datos, publicaron capturas de algunos de los archivos comprometidos en un sitio web dedicado a las filtraciones de datos. Entre la información robada, había supuestamente detalles privados vinculados a facturación, contratos, clientes y asociados de la empresa.

- **Ataque al Tribunal Superior de Justicia de Brasil**

En noviembre de 2020, el Tribunal Superior de Justicia de Brasil sufrió un serio ataque de ransomware que afectó su infraestructura de tecnología de la información, y dejó fuera de servicio su sitio web.
Los atacantes le aseguraron al Tribunal que habían cifrado la totalidad de su base de datos y que todo intento de descifrarla sería en vano. En la nota de rescate dejada, los hackers ofrecieron una dirección de correo electrónico para estar en contacto.

El Tribunal denunció el caso en la policía para que se investigue, y la Secretaría de Tecnología de la Información y Comunicación se hizo cargo del tema para restaurar todos los sistemas.
Asimismo, se dio a conocer que los responsables de este incidente también intentaron atacar otros sitios web relacionados con el gobierno de Brasil.

- **Ataque a la Universidad de Utah**

En agosto del 2020, la Universidad de Utah pagó un rescate de 457.000 dólares a un grupo de ciberdelincuentes para evitar la publicación de una serie de archivos confidenciales, sustraídos a raíz de un ataque de ransomware. El ataque afectó a algunos servidores de la Facultad de Ciencias Sociales y Ciencias del Comportamiento de la universidad. Los delincuentes cifraron el contenido de estos servidores. Antes de ello, hicieron copias de los archivos en su formato original.

El robo constaba de información perteneciente a los alumnos y empleados de la universidad. Finalmente, el rescate se pagó para evitar que los datos se filtraran. Luego, a modo de prevención, se les recomendó a los alumnos y empleados de la facultad afectada que cambiaran las contraseñas de sus servicios en línea, y que se mantuvieran en alerta para detectar movimientos sospechosos en sus historiales crediticios.

Bibliografía de referencia

https://www.nextgov.com/cybersecurity/2018/09/ransomware-strikes-launched-cyber-cleansing-program-transportation/151092/

https://thehackernews.com/2019/11/financial-cyberattacks.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Cyber+Security+Blog%29&_m=3n.009a.2114.po0ao0di5a.1bgs

https://www.ccn-cert.cni.es/seguridad-al-dia/alertas-ccn-cert/9403-ccn-cert-al-02-20-repunte-de-la-campana-de-emotet.html

https://www.cisa.gov/stopransomware

https://www.ibm.com/security/data-breach/threat-intelligence/

https://www-genbeta-com.cdn.ampproject.org/c/s/www.genbeta.com/seguridad/hospital-moises-broggi-barcelona-sufre-ciberataque-se-apunta-a-hackers-rusos-como-responsables-ransomware/amp

https://latam.kaspersky.com/blog/ransomware-telecommuting/18987/?mkt_tok=eyJpIjoiWXpOaE5qTTVaVEkxT0RZNSIsInQiOiJIZ2ZMc1hlRWpZeWpHNm5maVNscXJqMEZNcnB0QmFKWFZUK2pcLzNqM1NDWmI0ZzJYVzEwN05DR0lLRmZ2enB0cTkxTlJyU3FLMWtBQ3F0NW1cL3pWNDFPVVdiTHF3cXFMVW5VVGZiU0xacTNURFdPQW5CNVpvc0tjY2RVTFl3dVYzV0Fvd1NSWWlPckpCakFtdjQzZ0c2QT09In0%3D

https://www.cisa.gov/uscert/ncas/alerts/aa20-345a

https://unaaldia.hispasec.com/2021/03/el-hacker-del-ransomware-de-tesla-se-declara-culpable-y-un-hacktivista-suizo-es-acusado-de-fraude.html

https://revistabyte.es/ciberseguridad/ataq-sistemas-de-control-industrial/

https://thehackernews.com/2021/08/lockfile-ransomware-bypasses-protection.html

https://news.sophos.com/en-us/2021/08/27/lockfile-ransomwares-box-of-tricks-intermittent-encryption-and-evasion/

https://www.gartner.com/technology/media-products/reprints/Veeam/1-258L9XRD-ESL.html

https://revistabyte.es/ciberseguridad/un-34-un-ataque-de-ransomware/

Gestión de incidentes de ransomware:

https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/5867-ccn-cert-bp-21-gestion-de-incidentes-de-ransomware-1/file.html

https://revistabyte.es/ciberseguridad/ataq-sistemas-de-control-industrial/

Ransomware – Sistema de control Industrial

https://thehackernews.com/2021/08/lockfile-ransomware-bypasses-protection.html

Ransomware – Cifrado Inminente

https://news.sophos.com/en-us/2021/08/27/lockfile-ransomwares-box-of-tricks-intermittent-encryption-and-evasion/

https://www.cisa.gov/uscert/sites/default/files/2019-08/CISA_Insights-Ransomware_Outbreak_S508C.pdf