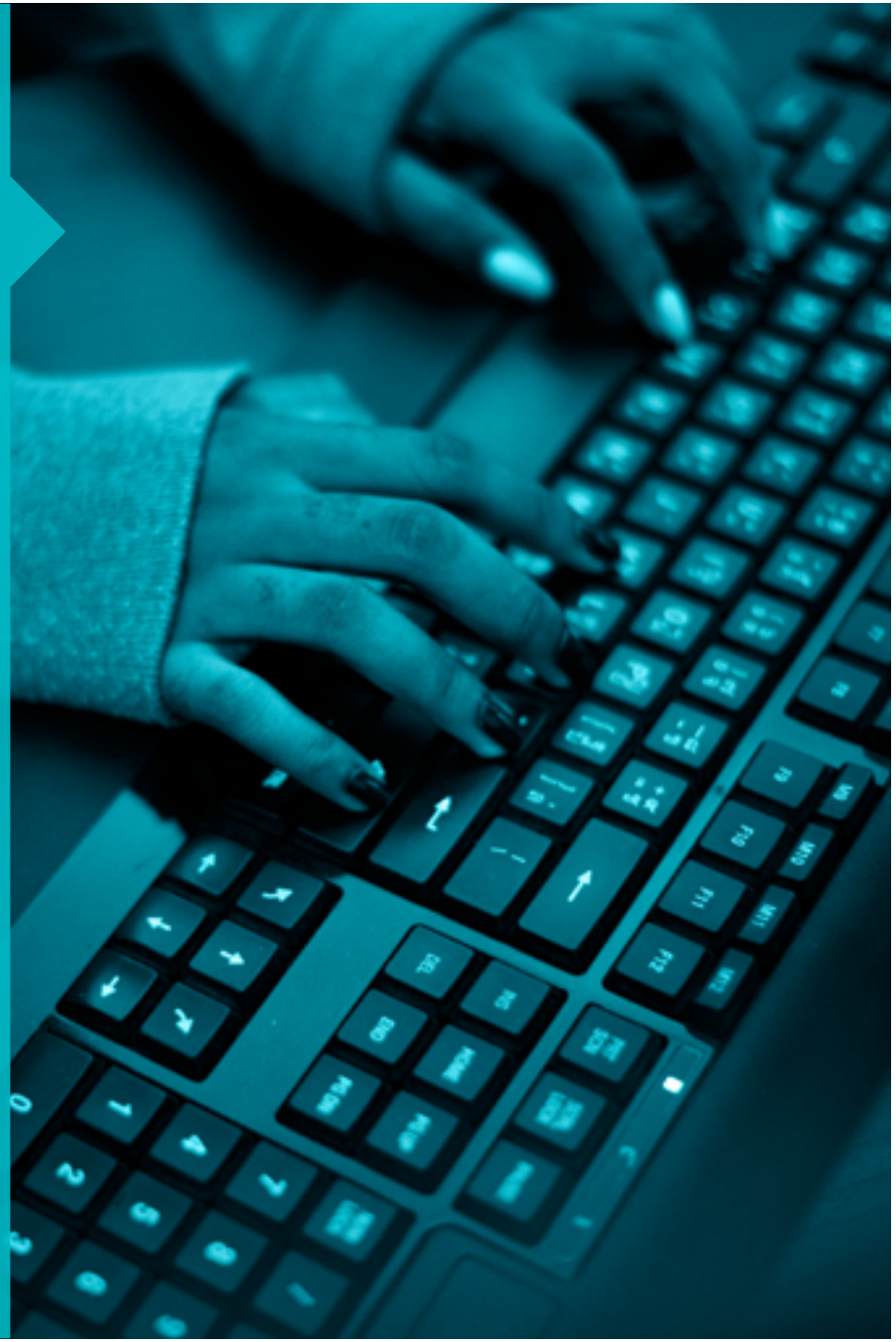
GUÍA DE

Ransomware

Índice



¿Qué es el ransomware?

Ransomware es una categoría que corresponde a todo tipo de código malicioso que le exige al usuario el pago de un rescate para recuperar información y también como veremos más adelante en el caso de las organizaciones, para evitar la divulgación de información robada y el consecuente daño a la reputación y confianza de los usuarios o clientes. Una vez que infectó el equipo, este malware utiliza diferentes mecanismos para dejar los datos inaccesibles para el usuario, con el objetivo de extorsionarlo y exigirle el pago de una cantidad de dinero a cambio de recuperar el acceso a la información. Es importante entender que el ransomware en general no roba ni accede al contenido de la información, sino que bloquea el acceso a ella.

Las primeras variantes de ransomware bloqueaban la pantalla del usuario y utilizaban diferentes engaños para hacerle creer que tenía un problema o había cometido algún delito y debía pagar para solucionarlo. En la actualidad, existen nuevas variantes que utilizan algoritmos complejos de cifrado para bloquear la información y solicitar dinero a cambio de recuperarla.

A diferencia de otros códigos maliciosos, el ransomware no busca pasar inadvertido, por el contrario: quiere llamar la atención de los usuarios infectados. Quizá muchas empresas se hayan infectado con códigos malicioso de los que jamás se han enterado, o hayan pasado varios días hasta que detectaron la infección. Lejos de esto, una vez que es liberado el ransomware se detecta en el momento, ya que el mismo código despliega un mensaje dando aviso al usuario que su información es inaccesible y que debe pagar.

Variantes y tipos de ransomware

Existen dos variantes principales de código malicioso usado para extorsionar a sus víctimas. Por un lado, el ransomware de bloqueo de pantalla, más conocido como "lockscreen", que impide el acceso al equipo.

Por otro lado, están los ransomware criptográficos, llamados "cryptolockers", que son aquellos que cifran la información dentro del equipo, impidiendo el acceso a los archivos.

Cryptolockers

El ransomware de tipo criptográfico utiliza diversos algoritmos de cifrado para bloquear el acceso a los archivos del usuario. Una vez que se apodera de un sistema, se inicia el cambio en la estructura de los archivos y documentos, de manera tal que solo se podrán volver a leer o utilizar tras restaurarlos a su estado original, lo cual requiere del uso de una clave conocida únicamente por los ciberdelincuentes. En la mayoría de los casos, el ataque afecta solo a ciertos archivos, siendo los de ofimática los más comúnmente perjudicados.

Una vez finalizada la infección, se despliega una pantalla que indica que los archivos han sido cifrados y explicando al usuario el proceso de pago de una cantidad de dinero a cambio de la clave para descifrar la información.

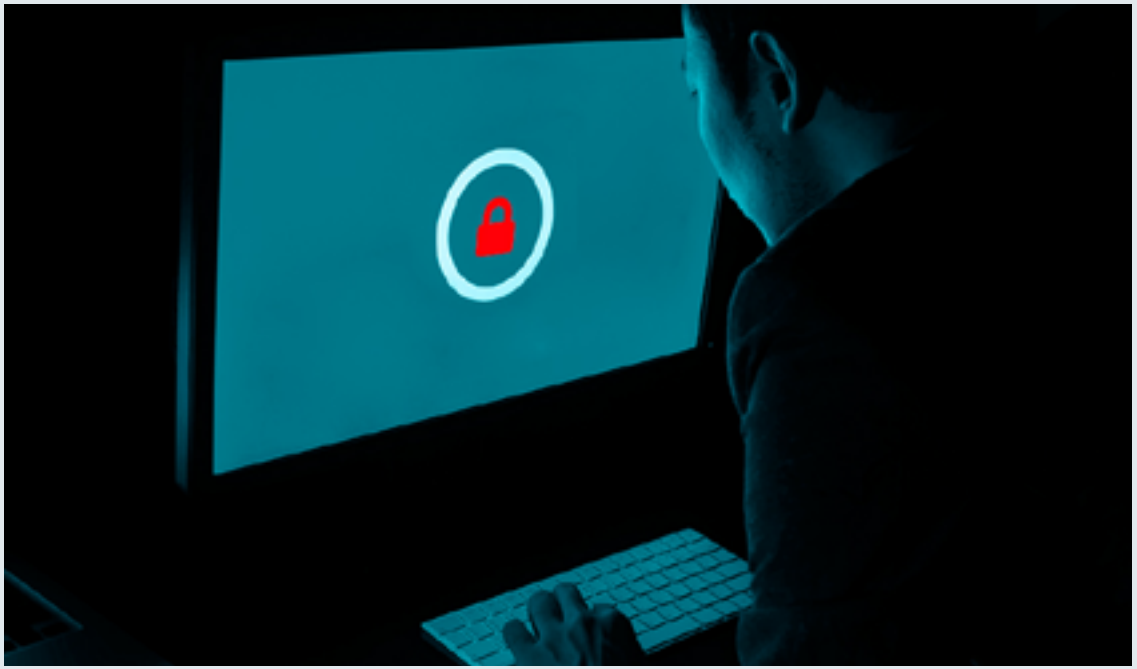
Esto no significa que el cifrado sea intrínsecamente malicioso. De hecho, es una herramienta poderosa y legítima empleada por individuos particulares, empresas y gobiernos para proteger los datos ante el acceso no autorizado. Sin embargo, al igual que cualquier otra herramienta poderosa, el cifrado se puede usar indebidamente con fines maliciosos, y esto es exactamente lo que hace el ransomware criptográfico.

Variantes y tipos de Ransomware

Lockscreen

El ransomware de tipo lockscreen, no tan frecuente en la actualidad, se caracteriza por impedir el acceso y el uso del equipo mediante una pantalla de bloqueo, imposibilitando cualquier acción para cerrarla, abrir el administrador de tareas, los navegadores web o cualquier otra parte del sistema. En esta pantalla típicamente se muestra un mensaje donde se explica lo ocurrido y se solicita el pago de un rescate.

Dado que esta variante no cifra los archivos, en estos casos la información podría recuperarse, ya que se puede extraer el disco rígido y luego limpiar el equipo de la infección. Por esta misma razón, este malware suele utilizar engaños y trucos de ingeniería social para persuadir al usuario a que pague el rescate.



¿Se pueden recuperar los archivos?

Esta es una de las primeras preguntas, si no la primera, que se hace una víctima del ransomware; y la respuesta es: depende. Naturalmente, si se cuenta con la clave maestra se van a poder descifrar todos los documentos, no obstante, conseguir la clave sin ceder ante el pago de los cibercriminales es lo complejo.

Si bien existen variantes de *cryptolockers* para las cuales es posible descifrar y recuperar los archivos afectados, en la mayoría de las ocasiones esto resulta casi imposible, sobre todo si el algoritmo es fuerte; la clave no puede ser obtenida a partir del código del malware; y las claves maestras son únicas para cada víctima y funciona solo para un equipo.

Ataques de ransomware dirigidos

Un cambio importante en la escena del malware que comenzó en 2018 después de lo que fue el fenómeno de WannaCry, es el enfoque hacia los ataques dirigidos en lugar de los ataques masivos. Los operadores detrás de los distintos grupos de ransomware dejaron de concentrarse en buscar la mayor cantidad de víctimas posibles y comenzaron a lanzar ataques personalizados a blancos específicos y elegidos previamente para maximizar las ganancias.

El objetivo de esta estrategia es afectar a organizaciones y compañías del sector público y privado (incluidas las pequeñas y medianas empresas) de diversas industrias o sectores que tengan recursos suficientes para hacer frente al pago de un rescate y por montos más elevados, y que podrían verse más afectados por los daños a la reputación. Además, que la sensibilidad de la información afectada presione a las víctimas a tener que pagar. De esta manera, los cibercriminales pueden recaudar más dinero y con una menor cantidad de víctimas.

Este enfoque hacia los ataques dirigidos modificó los mecanismos de distribución o propagación más comunes, apuntando sobre todo a servidores de empresas y organismos priorizando las fuentes de datos que tengan potencial de comprometer la continuidad y la imagen de la empresa u organización afectada.

Por otra parte, esta direccionalidad llevó a los cibercriminales a evolucionar hacia una mayor sofisticación y planificación. Ahora necesitan estudiar en profundidad a los blancos a los que apuntan, lo que implica en muchos casos un período en el que los atacantes, luego del compromiso inicial, exploran la red con el objetivo de recopilar información de interés y conocer los recursos de la víctima para luego en un momento liberar el ransomware en el sistema. Esto les permite, entre otras cosas, determinar el monto máximo que una víctima podría pagar por el rescate.

Nuevas modalidades extorsivas

Otro cambio que comenzó a observarse en el comportamiento de algunas familias de ransomware a fines de 2019 y que se consolidó en 2020 con muchos grupos que lo adoptaron, es la estrategia del doxing; es decir, el robo de información previo al cifrado de los archivos que los atacantes utilizarán para extorsionar a sus víctimas para que paguen. El ransomware Maze fue el primero en adoptar esta estrategia que incluyó la creación de un sitio en el que publican el nombre de la víctima y muestras de la información robada, amenazando a víctima con publicarla en caso de no llegar a un acuerdo en un plazo de tiempo establecido. Después de Maze, varios grupos adoptaron esta misma estrategia, como Dopplepaymer, REvil o Netwalker, y también crearon con un sitio para filtrar la información.

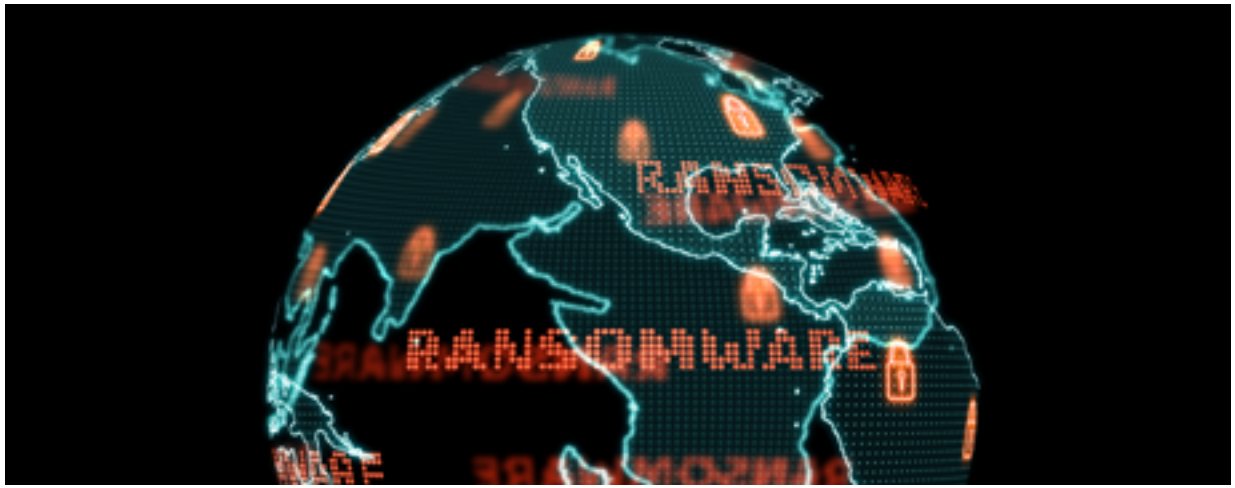
Además del doxing, otros grupos comenzaron también a implementar los ataques de DDoS a los sitios de sus víctimas para convencerlos de la necesidad de pagar. Si esto no era suficiente, otra de las estrategias que se ha visto ejecutar a algunos grupos son las llamadas en frío, en las cuales los atacantes llaman telefónicamente a sus víctimas en caso de utilizar las copias de seguridad o backup.

El modelo del Ransomware-as-a-Service

El Ransomware-as-a-Service (RaaS, por sus siglas en inglés) no es algo nuevo, pero entre 2019 y 2020 se registró un importante incremento de grupos operando bajo este modelo que consiste en crear un programa de afiliados compuesto por diferentes actores con roles bien definidos que se llevan porcentajes diferentes de las ganancias. Por ejemplo, quienes desarrollan la amenaza y ofrecen acceso a terceros para su distribución, quienes promocionan el grupo dentro de la dark web, o los que contactan con las víctimas luego de la infección. Este esquema resulta atractivo para cibercriminales sin conocimientos técnicos que pueden acceder a formas lucrativas de hacer dinero.

En 2020 había más de 20 grupos de ransomware luchando por lograr su espacio —en una escena cada vez más saturada y en crecimiento— intentando mejorar su reputación a partir demostrar sus cualidades técnicas y de mantenerse en actividad por un largo período de tiempo. REvil, Ryuk, Netwalker, Maze o DopplePaymer, fueron algunos de los grupos de ransomware más activos entre 2020 y 2021, pero fueron surgiendo otros.

El modelo colaborativo del RaaS permite la construcción de un servicio de creación de amenazas a medida en el que los distintos ransomware puedan adaptar los mecanismos de infección según características del blanco elegido. Esto implica variaciones en los métodos utilizados para acceder al sistema, el monto que se solicita a la víctima para el pago del rescate, o modificar para cada ataque el código malicioso para evitar ser detectados por soluciones de seguridad que sepan de la existencia de ataques previos de la misma amenaza.



Vectores de propagación

Las formas de propagación del ransomware son diversas, como correos electrónicos falsos (phishing), explotación de vulnerabilidades o ataques al Protocolo de Escritorio Remoto (RDP, por sus siglas en inglés). A continuación, los vectores de infección más comunes.

Mensajes engañosos de correo electrónico

Un método típico de infección de ransomware es a través de un **correo electrónico falso,** que habitualmente asegura provenir de una empresa conocida, una entidad bancaria o una agencia gubernamental. Estos correos engañan al usuario para lograr que descargue un archivo, ya sea adjunto en el correo o a través de un link a la web. Estos archivos maliciosos suelen ser troyanos que aparentan ser documentos de texto o imágenes inofensivas, pero al abrirlos descargan el ransomware que finalmente bloquea el equipo o los archivos del usuario. Por esta razón, siempre se recomienda no abrir archivos adjuntos ni ingresar a links de correos electrónicos desconocidos o no esperados.

Ataques al protocolo de escritorio remoto (RDP)

El Protocolo de Escritorio Remoto, más conocido como RDP, permite a una computadora acceder a otra de manera remota e interactuar con la misma igual que lo haría si estuviese sentado frente al máquina. A través del RDP es posible conectarse a otro equipo o a un servidor. En el caso de los ataques de ransomware, el RDP es uno de los vectores de ataque más utilizados para comprometer a las empresas con ransomware.

Para lograr acceder a través del RDP a un equipo o servidor los atacantes suelen recurrir a los ataques de fuerza bruta aprovechando la existencia de contraseñas débiles, así como también a los mercados clandestinos en los que se ofrecen credenciales de inicio de sesión al RDP robadas. Una vez que tienen las credenciales intentarán acceder al servidor como administrador para realizar distintos tipos de acciones maliciosas, como borrar archivos, deshabilitar las copias de seguridad y la solución de seguridad, o descargar e instalar malware.

Si bien los ataques al RDP no son nuevos, desde 2020 que los intentos de ataque a este protocolo han tenido un crecimiento muy importante.

Vectores de propagación

Descargas de archivos en redes p2p o sitios de software pirata.

En el caso de los ataques masivos, si bien han disminuido considerablemente, esto no implica que hayan desaparecido. Teniendo esto en cuenta, otro vector de propagación son las **descargas de archivos mediante redes p2p o sitios de software pirata**. Muchos de estos sitios o archivos prometen software gratuito o cracks para evadir verificaciones de licenciamiento. Sin embargo, lejos de ser gratuitos, pueden infectar el equipo del usuario para obtener algún tipo de rédito económico, por ejemplo, mediante el pago de un rescate. Asimismo, este tipo de programas suele solicitar que se deshabilite la protección antivirus, por lo que les resulta aún más sencillo infectar el equipo.

En ambos casos, ya sea a través de un correo electrónico falso o una página maliciosa, el atacante requiere de la intervención del usuario para descargar y ejecutar el archivo malicioso, y para lograr engañarlos se vale de la ingeniería social. Por lo tanto, la precaución y educación en seguridad informática es clave ante estos casos.

¿Sí o sí se propagan a través de un engaño al usuario?

Más allá de los correos de phishing y los ataques intentando abusar del RDP, muchos códigos maliciosos aprovechan vulnerabilidades de los sistemas o aplicativos que no se encuentran actualizados, como soluciones VPN o tecnologías utilizadas para el acceso remoto a redes de Windows. Algunos malware tienen incluso la capacidad de propagarse por sí mismos explotando estas vulnerabilidades, como fue el caso de WannaCry. Muchas variedades de ransomware traen consigo un exploit que aprovecha dichas vulnerabilidades sin parchear para poder ejecutar el código en el equipo, copiar así el ransomware y ejecutarlo.

Otros mecanismos de distribución utilizados son mediante botnets o la descarga de un troyano que logra la infección inicial, como fue en su momento con Emotet, o como se ha visto con los troyanos QakBot y Trickbot, que han sido utilizados para distribuir los ransomware Ryuk y Conti .

¿Qué pasa con los dispositivos móviles?

A principios de 2014 surgieron diversas familias de ransomware para dispositivos Android que utilizaban el mismo engaño que el denominado Virus de la policía o Reveton; es decir, afirmando que el equipo había sido bloqueado por infringir una ley y demandando el pago de una multa. Estos ransomware de bloqueo de pantalla, detectados por ESET como Android/Koler o Android/Locker, utilizaban técnicas de ingeniería social, incluyendo asegurar que el usuario era espiado por la cámara, para conseguir mayor credibilidad y aumentar así las posibilidades de cobro.

Pero no fue hasta mediados de 2014 que se detectó el primer ransomware de cifrado para archivos en dispositivos Android; una evolución esperada en ese entonces debido a la gran extensión de este tipo de códigos maliciosos en dispositivos Windows.
Llamado Simplocker, este troyano escanea la tarjeta SD del dispositivo y luego cifra los archivos utilizando el algoritmo AES. Dado que se trata de un algoritmo simétrico, la clave de cifrado queda codificada dentro del equipo y es posible recuperar los archivos infectados sin pagar los 20 dólares que solicita el rescate.
Sin embargo, en un segundo brote, se encontraron nuevas variantes de Simplocker que incorporaban la utilización de claves únicas generadas y enviadas a través de conexiones anónimas con la consola del atacante por medio de la red Tor, por lo que ya no fue posible descifrar la información.

¿Qué pasa con los dispositivos móviles?

Ya en 2015, hizo su aparición un nuevo ransomware de bloqueo de pantalla: Lockerpin. Este código malicioso accede al equipo con permisos de administrador y cambia el PIN de desbloqueo del equipo. La particularidad de Lockerpin radica en los diferentes engaños que utiliza para conseguir permisos de administrador, desde simplemente solicitárselos al usuario, hasta hacerse pasar por una supuesta actualización del sistema. Además, ante cualquier intento por revocar estos permisos o intentar recuperar la información, el ransomware arroja un error y cambia aleatoriamente el PIN. El usuario, entonces, debe reestablecer su equipo a la configuración de fábrica para eliminar el malware, junto con todos los datos y archivos del dispositivo.

En Android

En el caso de las variantes para dispositivos móviles, la propagación suele darse a través de aplicaciones maliciosas en tiendas no oficiales y foros. Muchas veces estas aplicaciones se hacen pasar por versiones gratuitas o modificadas de aplicaciones o juegos populares, guías o trucos para estos juegos, o aplicativos que dicen agregar funciones extras al dispositivo. Además, mediante el uso de la ingeniería social, los atacantes manipulan a las víctimas para que hagan clic en un enlace malicioso y dirigirlos a un paquete de aplicaciones Android (APK) infectado. En muchos casos, estos enlaces maliciosos llegan a través de correos electrónicos, SMS o incluso mensajes en foros y comentarios.

Por otro lado, a partir de 2016 comenzaron a aparecer casos donde los cibercriminales incorporaron otros métodos más sofisticados a sus técnicas de propagación. Los atacantes intentan esconder los payloads (la parte maliciosa del código) lo más profundo posible dentro de las aplicaciones, con el objetivo de que sean indetectables ante los controles de las tiendas oficiales y algunos foros. Para ello, una técnica es cifrar el código y luego trasladar el archivo a la carpeta de activos, que se suele utilizar para guardar imágenes u otros contenidos necesarios de la aplicación móvil. Por lo tanto, la app parece no tener ninguna funcionalidad maliciosa en el exterior, pero lleva oculta en el interior una herramienta capaz de descifrar y ejecutar el ransomware.

Es por eso que a la hora de utilizar el dispositivo móvil lo más importante es no descargar aplicaciones de foros o repositorios no oficiales, además de mantener el equipo actualizado y sobre todo tener instalado un software de seguridad.

¿Cuál es el riesgo del ransomware para una empresa?

La información es un activo muy valioso para la organización. Por lo tanto, si se compromete la disponibilidad de la información o se amenaza son la divulgación de información sensible de usuarios o clientes, cualquiera de estos casos puede implicar grandes consecuencias, quizá hasta devastadoras. Esta es la principal razón por la cual muchos ataques de ransomware están orientados a infectar archivos e información corporativa.

Asimismo, la mayoría de las empresas trabajan con redes compartidas de información, lo que hace que una infección pueda propagarse rápidamente a través de la red, infectando no solo las estaciones de trabajo de los empleados, sino también los servidores y bases de datos de la compañía, donde muchas veces se aloja la información crítica y sensible.

A continuación, detallaremos algunos riesgos específicos a tener en cuenta:

En primer lugar, tenemos que mencionar las pérdidas financieras, particularmente en casos donde la información que se pierde está compuesta de datos privados de clientes a quienes se debe resarcir y/o indemnizar de alguna manera. En el mismo sentido, si los archivos afectados son patentes o fórmulas de ciertos productos, esto podría derivar en la interrupción completa o parcial del negocio.

¿Cuál es el riesgo del ransomware para una empresa?

En esta misma línea, hay compañías que concentran su trabajo en servidores en la nube, por ende, si estos resultan infectados y no se cuenta con un plan de continuidad para seguir trabajando fuera de línea, entonces el correcto funcionamiento del negocio también se verá interrumpido.

Seguidamente, tenemos que mencionar un tema muy importante: el daño a la marca. Este es un riesgo que compromete directamente el prestigio, la solidez y hasta credibilidad de una compañía; y si bien resulta difícil de medir en cuanto al dinero neto que podría perderse, sí puede verse en la percepción de los usuarios o clientes, quienes pierden la confianza en un segundo, y recuperarla se torna una tarea muy compleja.

Finalmente, destacamos el tema de la responsabilidad legal, es decir, las obligaciones que tiene una compañía de acuerdo con las leyes de protección de datos en los países donde opera. Nuevamente, en caso de perder información, se deben pagar multas e indemnizaciones a quienes resulten víctimas del ataque.

Si bien no es recomendable pagar el rescate, muchas veces resulta más perjudicial la pérdida de la información que ceder ante al atacante. Es que en el caso de las empresas, no solo deben considerar el valor en sí de la información que se perdió o ya no está disponible, sino también los costos indirectos (muchas veces mayores, tal como destacamos en los puntos anteriores) que implican detener la operatoria, no brindar un servicio, demorar las actividades o cualquier otra consecuencia que afecte la continuidad del negocio.

Medidas de protección

El ransomware atenta principalmente sobre la disponibilidad de la información, por lo que su éxito será determinado por la capacidad de bloquear los archivos o el sistema de la víctima, y que ésta, de hecho, no tenga un plan de recuperación de datos, como puede ser un backup. Por lo tanto, al igual que con cualquier amenaza que ponga en riesgo el acceso a la información, la principal herramienta para recuperarla es tener una copia de respaldo.

La importancia del backup

Contar con una copia de los archivos críticos es muy importante en el caso de una pérdida de la información, especialmente porque existen múltiples causas por las cuales un usuario podría experimentar este problema. Por ejemplo, la limitada vida útil de los discos duros, los robos o extravíos de los dispositivos y, por supuesto, los ya conocidos códigos maliciosos.

Dado que el objetivo de un backup es poder recuperar la información en caso de que ocurra alguno de estos incidentes, no es recomendable que las unidades de respaldo estén conectadas a la red todo el tiempo, ya que, en caso de una infección en la red, también podrían verse afectadas. Siempre es mejor que el backup sea realizado en un disco o dispositivo externo, que se almacene en un lugar diferente al equipo, de forma tal que no sea robado, extraviado ni afectado por un incidente.

Medidas de protección

¿Qué debe incluir una política de backup empresarial?

No toda la información posee el mismo valor, por ende, antes de comenzar con el proceso de backup, es fundamental determinar qué información será respaldada. Esto se puede lograr valorando los datos y estableciendo cuáles tienen mayor relevancia según las preferencias personales, el tipo de trabajo que se haga con dichos datos, o incluso el objetivo o utilidad que tengan. Existen tres aspectos que deben ser analizados a la hora de clasificar la información y establecer una política de **backup:**

Criticidad:
Determinar qué información es importante respaldar. Tener en cuenta toda la información que utiliza la empresa diariamente para funcionar, así como también aquella que debe conservar para futuras consultas. Es importante entender que realizar un backup requiere costo y esfuerzo, por lo que es importante determinar cuál es la información que realmente vale la pena resguardar.

Periodicidad:
No se puede perder de vista la frecuencia con la cual se modifican los datos. Existe información dinámica e histórica y es importante entender la diferencia entre cada una para determinar cada cuanto tiempo se realizará el resguardo de información. Existen diferentes tipos de backup: Completo, Diferencial o Incremental. Cada uno tiene sus beneficios en cuanto a costo, esfuerzo y periodicidad, por lo que es recomendable saber cada cuanto se requiere resguardar la información para elegir el que mejor se ajuste a las necesidades.

Medio:
El tipo de soporte que se elija para resguardar la información (disco rígido, cintas, medios ópticos, la nube, etc.), dependerá de la cantidad de información que deba guardar, la periodicidad con la que se haga el backup y de la accesibilidad que se requiera. Además, se debe considerar que el espacio físico en donde se guarde el soporte de respaldo también debe estar protegido.

Por último, es recomendable no pensar únicamente en los archivos o datos a resguardar, sino también en las configuraciones y documentación necesaria para poner en funcionamiento un equipo o sistema. En muchos casos, ante una infección de ransomware es probable que los técnicos deban reestablecer los sistemas, lo cual implica invertir muchas horas en configuraciones. Tener un respaldo de estas configuraciones seguramente ahorrará varias horas de trabajo.

Educación y concientización

Los usuarios vulnerables son los que están desinformados, aquellos que no están alertas si reciben un correo falso, que creen que el ransomware es un tema de películas o que los incidentes de seguridad ocurren únicamente en gobiernos y grandes corporaciones multinacionales.

La mayoría de las infecciones de ransomware requieren, en cierto momento, de la intervención del usuario: ya sea para descargar un archivo, ingresar a un link malicioso, abrir un documento o realizar el pago creyendo algún engaño. Tarde o temprano el factor de ingeniería social será clave para el éxito de la infección. Por lo tanto, otro punto importante en la prevención es la educación y concientización de los usuarios.

Estar informado sobre cómo actúan las amenazas, cuáles son los engaños que utilizan para infectar a los usuarios, de qué forma se propagan y cómo prevenirlas son algunos de los conocimientos que evitarán que un empleado sea infectado.

Una buena campaña de concientización no se logra con acciones esporádicas, por el contrario, es **necesario una educación periódica y constante.** La clave es no centrarse en un solo recurso, sino aprovechar cualquier oportunidad para educar. No solo se logra la concientización mediante charlas y cursos explicando los riesgos y las medidas de seguridad, además, se puede complementar con recordatorios periódicos de buenas prácticas, un boletín de noticias de actualidad, guías y manuales de configuraciones de privacidad y seguridad, o incluso videos y posters con consejos prácticos.

Otras medidas de protección

Sin lugar a dudas, el uso de la ingeniería social es uno de los principales mecanismos utilizados por los atacantes para propagar sus amenazas, sin embargo, no es el único, ya que hay técnicas que no requieren que un usuario interactúe con la amenaza para que esta se instale. Por ejemplo, la inyección de un iframe en un sitio web vulnerable puede llevar a que un atacante instale algo en el dispositivo del usuario sin que este se percate de lo que está pasando. Es por esto que también es importante contar con una solución de seguridad que detecte este comportamiento malicioso.

En cuanto a los ataques que buscan acceder a través del RDP, se recomienda deshabilitar los servicios RDP expuestos a Internet, deshabilitar conexiones externas a máquinas locales en el puerto 3389 (TCP/UDP) en el firewall perimetral, y habilitar la Autenticación a nivel de red. Para las cuentas que puedan iniciar sesión a través del RDP, utilizar contraseñas complejas (más de 15 caracteres) para protegerse contra ataques de fuerza bruta; implementar el doble factor de autenticación al menos en todas las cuentas que puedan iniciar sesión a través del RDP; utilizar una VPN para gestionar todas las conexiones RDP fuera de la red local, y aislar cualquier computadora insegura a la que deba accederse desde Internet utilizando RDP.

Si bien el ransomware pareciera ser la amenaza "de moda" en los últimos tiempos, son muchos los tipos de amenazas que se están propagando y afectando a los usuarios. Ya sea que se trate de un troyano, un gusano, un bot o el mismísimo ransomware, una buena herramienta integral de seguridad va a ser capaz de prevenir la infección.

Si bien el término "antivirus" quedó acuñado en el subconsciente colectivo, este tipo de herramientas han evolucionado y pasaron de detectar solamente virus informáticos hasta convertirse en soluciones de seguridad completas, que proveen muchas otras funcionalidades como firewall, filtros de email y antispam, antiphishing o escaneo de memoria, entre otras, que dan una protección integral al sistema y te permiten navegar seguro en el contexto actual de amenazas.

Por último, es importante actualizar regularmente los sistemas y aplicaciones, ya que muchas amenazas aprovechan vulnerabilidades no corregidas para propagarse por la red. Si bien esta tarea parece tediosa y rutinaria, existen herramientas de gestión de parches y actualizaciones que simplifican notablemente el trabajo.

Qué hacer si ocurre una infección

Es importante destacar que, ante una infección, la posibilidad de recuperar la información y la forma de hacerlo dependerá del tipo de amenaza específica.

En general, en los casos del tipo lockscreen es posible recuperar el acceso al sistema limpiando la infección o restaurando el equipo. Además, en estos casos, si los archivos no son cifrados es posible recuperarlos del disco afectado. Sin embargo, en algunas variantes, especialmente aquellas que afectan dispositivos móviles, el bloqueo no permite la recuperación del equipo, por lo que la única solución terminará siendo un reseteo de fábrica, borrando toda la información.

En el caso de los filecoders la recuperación puede ser más complicada. Sí bien, en la mayoría de los casos, un buen software de seguridad tendría que ser capaz de quitar el ransomware del equipo, los archivos seguirán cifrados y dada la evolución de la amenaza algunos archivos podrían ser publicados. En algunas familias de ransomware, especialmente las que utilizan el cifrado simétrico y guardan la clave dentro del código malicioso, es posible recuperar los archivos utilizando la herramienta específica de descifrado; aunque cada vez son menos las amenazas que utilizan este tipo de modelos. La gran mayoría de familias de ransomware que utilizan mecanismos de cifrado más sofisticados, como Ryuk, son imposibles de descifrar sin la clave correcta.

En cualquier caso, si ocurre una infección es recomendable limpiar el equipo de la infección, ya sea utilizando una herramienta de seguridad o reinstalando el sistema, y luego recuperar la información y los archivos mediante un respaldo limpio.

¿Pagar o no pagar?

Hoy en día el ransomware es un negocio rentable para los cibercriminales, ya que muchas personas y empresas deciden acceder a las demandas y pagar el rescate a cambio de recuperar su información. En 2020 se registró un importante crecimiento de las ganancias de los grupos de ransomware producto de la cantidad de nuevos grupos y también debido al crecimiento de los montos demandados para el pago de los rescates. En 2018, atacantes comprometían con ransomware a la ciudad de Atlanta en Estados Unidos y solicitaban el pago de 51.000 dólares para recuperar la información, mientras que en 2020 se registraron varios ataques en los cuales los criminales solicitaron varios millones de dólares para recuperar los archivos y evitar la filtración de la información.

En general, al hacer el pago, se recupera la clave para descifrar la información, ya que si se corriera la voz de que los atacantes no mantienen su lado del acuerdo, nadie pagaría. Sin embargo, desde el laboratorio de ESET recomendamos **no pagar** el rescate ni acceder a las demandas, por dos razones concretas.

Si bien en muchos casos al pagar el rescate se restaura el acceso a los datos, la realidad es que se está negociando con un cibercriminal del otro lado, del cual no sabemos su identidad ni tenemos forma de encontrarlo. Por lo tanto, no existe ninguna garantía de que realmente enviará las claves de descifrado. De hecho, ha habido casos en los que no se ha recuperado la información, el delincuente jamás respondió luego del pago del rescate, o incluso solicitó el pago tres veces antes de realmente devolver el acceso a los datos.

Por otro lado, acceder ante estas demandas contribuye a que el negocio del ransomware sea cada vez más rentable para los atacantes, y por lo tanto, estos irán perfeccionando sus técnicas y adaptándose a nuevos escenarios. Si las víctimas tienen resguardo de sus datos y están prevenidas, no será necesario que paguen el rescate, por lo que el negocio irá decayendo.

Por último, el pago del rescate no significa que el usuario va a estar fuera de peligro. Los criminales pueden dejar malware en el equipo, además de que ahora saben que está dispuesto a pagar dinero para recuperar el acceso al equipo o a los datos. En resumen, podría volver a ser el objetivo de otro ataque futuro.

Conclusión

El ransomware es una amenaza que ha ido evolucionando a lo largo de los años, utilizando métodos y algoritmos de cifrado cada vez más complejos y sumando nuevas modalidades extorsivas para el pago del rescate. Lamentablemente, mientras esta amenaza continúe siendo una de las actividades más rentables los criminales continuarán perfeccionando sus técnicas y adaptándose a nuevos escenarios. De todas formas, las mismas técnicas de propagación seguirán vigentes: archivos adjuntos en correos electrónicos, ataques al RDP y explotación de vulnerabilidades, principalmente.

Está claro que las cosas se están poniendo cada vez más sofisticadas en el mundo de la tecnología y las amenazas acompañan esta evolución. Con la aparición de los dispositivos móviles no tardaron en aparecer las variantes de ransomware y otras amenazas que afectan dispositivos Android, y con el auge del Internet de las Cosas se vieron ataques de ransomware apuntando a estos equipos. Por otra parte, la adopción de nuevos mecanismos de extorsión deja en evidencia que el objetivo es el dinero, y que los cibercriminales harán los cambios y ajustes necesarios que garanticen mayores probabilidades de que las víctimas paguen.

Por lo tanto, con el ransomware cada vez más evolucionado y las nuevas tecnologías en auge, resulta de vital importancia la educación de los usuarios, tanto en su vida personal como en sus actividades dentro de la empresa. Así como también es indispensable para las organizaciones combatir este tipo de amenazas con una correcta gestión de la seguridad y, en caso de resultar víctimas, no realizar ningún pago para terminar con esta conducta criminal.

www.eset.com/latam

/esetla

@esetla

/company/eset-latinoamerica