proofpoint.

LIBRO ELECTRÓNICO

Guía de supervivencia frente al ransomware 2022

Lo que todas las empresas necesitan saber antes, durante y después de un ataque

proofpoint.com/es

Índice

Resumen ejecutivo

El ransomware, o secuestro de datos, es una antigua amenaza que sigue siendo un problema moderno. Este tipo de malware, que recibe su nombre del rescate (*ransom* en inglés) exigido para devolver a las víctimas el acceso a sus archivos, es un problema grave para todas las empresas. En la actualidad constituye uno de los tipos de ciberataque más destructivos. En 2021, los principales incidentes de ransomware ocurridos en EE. UU. afectaron al suministro de combustible[1], la alimentación[2] y la infraestructura sanitaria[3], lo que demuestra que no hay objetivos intocables y que es más importante que nunca contar con un plan de mitigación de riesgos y de respuesta en caso de infección de los sistemas.

Por qué sigue habiendo ransomware

La persistencia del ransomware se justifica por cuatro motivos principales:

- Gracias a bitcoin y a otras monedas digitales, el pago de un rescate es más fácil de cobrar que con otros tipos de fraude.
- Los ciberdelincuentes disponen de muchos canales de distribución, incluidos los equipos comprometidos de un entorno, lo que incrementa sus posibilidades de éxito.
- Muchas empresas tienen ciberdefensas débiles u obsoletas y rutinas deficientes de copia de seguridad y recuperación, lo que las convierte en un gran grupo de objetivos potenciales.
- Los ciberdelincuentes afinan cada vez más a la hora de elegir sus objetivos y utilizan tácticas más sofisticadas.

Al igual que la mayoría de los ciberataques, el ransomware normalmente necesita que alguien actúe por el atacante, por ejemplo, abriendo un archivo adjunto o haciendo clic en una URL.

Sobrevivir al ransomware

El ransomware compromete sistemas y datos, pero los ataques que les llevan hasta ellos se dirigen contra personas. Al igual que la mayoría de los ciberataques, el ransomware normalmente necesita que alguien actúe por el atacante, por ejemplo, abriendo un archivo adjunto o haciendo clic en una URL. De ahí que la lucha contra el ransomware exija una estrategia centrada en las personas.

Considere esta guía como un punto de partida.

1 David Sanger, Clifford Krauss, Nicole Perlroth *(New York Times)* "Cyberattack Forces a Shutdown of a Top U.S. Pipeline" (Un ciberataque obliga a cerrar un importante oleoducto estadounidense). Mayo de 2021.
2 Julie Creswell, Nicole Perlroth, Noam Schreiber *(New York Times)* "Ransomware Disrupts Meat Plants in Latest Attack on Critical U.S. Business" (Un ransomware paraliza las plantas de procesamiento cárnico en el último ataque a empresas fundamentales de EE. UU.). Junio de 2021.
3 Nicole Perlroth, Adam Satariano *(New York Times)* "Irish Hospitals Are Latest to Be Hit by Ransomware Attacks" (Los hospitales irlandeses, últimos objetivos de los ataques de ransomware). Mayo de 2021.

Antes del ataque

La mejor estrategia de seguridad consiste en evitar el ransomware, pero eso es algo que requiere planificación y trabajo antes de que sobrevenga la crisis.

Utilice herramientas de copia de seguridad y restauración

Uno de los aspectos más importantes de cualquier estrategia de seguridad contra el ransomware es hacer copias de seguridad regularmente. Dado que numerosas variantes de ransomware están dirigidas contra las copias de seguridad conectadas a la red, mantenga las copias en una red independiente o en la nube. Y asegúrese de desactivar el acceso del sistema de archivos a esas copias de seguridad[4].

Sorprendentemente, pocas organizaciones realizan simulacros de copia de seguridad y restauración. Ambos procesos son importantes: los simulacros de restauración son la única manera de saber de antemano si el plan de copia de seguridad funciona.

Actualice y aplique parches

Asegúrese de aplicar los últimos parches y actualizaciones a los sistemas operativos, el software de seguridad, las aplicaciones y el hardware de red.

Invierta en soluciones robustas de seguridad centrada en las personas

Las soluciones avanzadas de seguridad del correo electrónico son capaces de proteger frente a las URL, los archivos adjuntos y los documentos maliciosos incluidos en mensajes de correo electrónico que permiten distribuir ransomware. Estas soluciones también protegen frente a otros tipos de malware que normalmente se distribuyen a través del correo electrónico y que pueden instalar ransomware con ataques de seguimiento dirigidos.

La formación y concienciación sobre seguridad de los empleados es fundamental. Deben saber lo que pueden y no puede hacer, cómo evitar los ataques de ransomware y cómo denunciarlos. Si un empleado recibe una petición de rescate, nunca debe intentar pagar por su cuenta y debe saber cómo alertar inmediatamente al equipo de seguridad.

Planifique la respuesta

No poder acceder a los sistemas críticos de la empresa es una situación estresante, que sin duda afecta a la toma de decisiones[5]. Sepa de antemano cómo va a responder para poder centrarse en la contención y la recuperación en caso de ataque.

No existe un plan de respuesta universal a los ataques de ransomware. Los hospitales y otras infraestructuras esenciales deben sopesar el coste de la interrupción de la actividad de forma muy diferente a las empresas de consumo. Una buena manera de planificar cada etapa de la respuesta es poner en marcha un ejercicio completo de simulación.

4 W. Curtis Preston *(Network World)*. "How to protect backups from ransomware" (Cómo proteger las copias de seguridad frente al ransomware). Febrero de 2021.
5 Kathleen M. Kowalski, Charles Vaught *(International Journal of Emergency Management)* "Judgement and Decision-Making Under Stress: An Overview for Emergency Managers" (Conclusiones y toma de decisiones bajo presión: panorámica para directivos de emergencias). Junio de 2003.

Durante el ataque

Aunque la mejor estrategia contra el ransomware es evitarlo, la creciente sofisticación de los ataques contra la cadena de suministro ha demostrado que hasta las empresas mejor preparadas pueden caer en la trampa[6]. Incluso es posible que la primera payload (carga maliciosa) en infectar un sistema no sea el ransomware. Ahora muchos grupos de ciberdelincuentes prefieren comprar el acceso a objetivos ya infectados con troyanos o malware cargador.

Durante un ataque hay problemas urgentes que resolver, como poner de nuevo en funcionamiento ordenadores, teléfonos y redes y afrontar la petición de rescate.

Denuncie ante las fuerzas de seguridad

El ransomware, igual que cualquier otra forma de robo y extorsión, es un delito. Denunciarlo ante las autoridades competentes es un primer paso necesario.

Si tiene un seguro antiransomware, también debe ponerse en contacto con la aseguradora.

Desconecte los sistemas de la red

En cuanto los empleados vean una petición de rescate o adviertan algo raro, deben desconectar el equipo infectado de la red y llevarlo al departamento de TI. Solo el equipo de seguridad de TI debe intentar reiniciarlo y esta medida solo funcionará si se trata de scareware falso o malware común y corriente.

Si el ransomware ya ha conseguido llegar a un servidor, el equipo de seguridad deberá aislarlo lo antes posible y organizar la respuesta.

No lo olvide: igual que en las plagas domésticas, un solo dispositivo infectado suele ser indicio de un problema mayor. Busque activamente otros sistemas infectados en su entorno.

Implemente la respuesta planificada

La respuesta planificada debe ser lo suficientemente flexible para adaptarse a una serie de factores:

- El tipo de ataque, específicamente la variante de ransomware utilizada y el ciberdelincuente que lo ha perpetrado
- La presencia previa de payloads de malware que puedan haberse utilizado para reconocimiento o para cargar el ransomware
- Quién se ha visto afectado en la empresa
- Qué permisos de red tienen las cuentas comprometidas

Las infecciones de ransomware suelen ser infecciones secundarias en redes ya comprometidas. Esto significa que cada uno de estos factores es crucial para evaluar el alcance del problema y prevenir más infecciones y pérdidas de datos.

Olvide las herramientas gratuitas de descifrado de ransomware

La mayoría de las herramientas gratuitas solo son eficaces para una variedad de ransomware o incluso para una sola campaña de ataque. Cuando los ciberdelincuentes actualizan su ransomware, las herramientas gratuitas quedan obsoletas y es probable que no funcionen con la variante utilizada contra su empresa.

Restaure a partir de las copias de seguridad

La única manera de recuperarse por completo de una infección de ransomware es restaurarlo todo a partir de las copias de seguridad. No obstante, aun teniendo copias de seguridad recientes, pagar el rescate puede ser más interesante desde el punto de vista económico y operativo.

6 Kellen Browning *(New York Times)* "Hundreds of Businesses, from Sweden to U.S., Affected by Cyberattack" (Cientos de empresas de Suecia a EE. UU. afectadas por un ciberataque). Julio de 2021.

Después del ataque

Aunque puede que la crisis inmediata haya terminado, todavía hay mucho trabajo por hacer.

Revise y refuerce

Le recomendamos que realice una evaluación completa de la seguridad para detectar si hay amenazas aún presentes en el entorno. Analice a fondo sus herramientas y procedimientos de seguridad y averigüe dónde han sido insuficientes.

Limpie los sistemas

Algunos tipos de ransomware se distribuyen a través de otras amenazas o de troyanos de puerta trasera que pueden dar lugar a futuros ataques. Con frecuencia, lo que abrió la puerta al ransomware fue la existencia de una infección anterior en el entorno de la víctima.

Busque a fondo amenazas ocultas que puedan haberse pasado por alto en medio del caos, especialmente si hay riesgo de que las copias de seguridad también se hayan visto comprometidas.

Lleve a cabo un examen retrospectivo

Revise su nivel de preparación frente a las amenazas, la cadena de acontecimientos que dieron lugar a la infección y su respuesta. Si no averigua cómo entró el ransomware, no tendrá manera de detener el próximo ataque.

Evalúe el nivel de concienciación de los usuarios

Un empleado bien informado constituye su última línea de defensa. Asegúrese de que sus empleados, personal administrativo e instructores están preparados. Las evaluaciones periódicas y las simulaciones de phishing pueden ayudar a identificar a las personas susceptibles de caer en determinados señuelos de correo electrónico y otras tácticas.

Formación

Elabore un programa de formación para abordar la vulnerabilidad de los empleados ante los ciberataques. El programa debe basarse en campañas de ataque y tácticas del mundo real. Cree un plan de comunicaciones de crisis para el caso de un futuro ataque y póngalo en práctica con simulaciones y pruebas de penetración.

Refuerce sus defensas tecnológicas

El panorama de amenazas actual cambia a toda velocidad y exige soluciones que puedan analizar, identificar y bloquear en tiempo real las URL y los archivos adjuntos maliciosos que sirven como punto de entrada inicial para el ransomware.

Busque soluciones de seguridad que puedan adaptarse a las amenazas nuevas y emergentes y que le ayuden a reaccionar ante ellas con mayor rapidez.

Introducción

El ransomware es una amenaza que está entre nosotros desde hace más de tres décadas y su evolución ha sido permanente durante todo este tiempo. La última vez que actualizamos este informe, las cifras de ransomware mostraban una tendencia a la baja porque las empresas y los proveedores de seguridad consiguieron neutralizar Locky, el ransomware responsable de la reaparición de esta amenaza en 2016.

300 %
DE INCREMENTO INTERANUAL
en ataques de ransomware a principios de 2021, según las cifras del gobierno de EE. UU.

Eso está cambiando. A principios de 2021, las cifras del gobierno estadounidense indicaban un nuevo repunte de los ataques de ransomware con un incremento interanual del 300 %[7].

Este cambio se ha debido a una transformación del ecosistema de la ciberdelincuencia. Los ciberdelincuentes ya no recurren a la distribución generalizada y a los rescates de pequeño importe. Ahora prefieren colaborar con otros distribuidores de malware que les venden el acceso a sistemas ya infectados con troyanos y cargadores para realizar la prospección, el reconocimiento y el ataque. Este enfoque les permite identificar objetivos de gran valor que tienen más que perder con la interrupción de su actividad y más capacidad para pagar.

Esta nueva táctica, junto con la creciente cotización de bitcoin y de otras criptomonedas, ha creado las condiciones para una epidemia de ransomware.

El ransomware es noticia

Durante los seis primeros meses de 2021, el ransomware pasó de ser un quebradero de cabeza para la ciberseguridad a convertirse en una crisis debatida en las más altas esferas gubernamentales. Los ataques dirigidos contra centros de enseñanza, departamentos de policía y autoridades de transporte demostraban una creciente disposición de las bandas de ransomware a atacar infraestructuras públicas.

Los ataques dirigidos contra centros de enseñanza, departamentos de policía y autoridades de transporte demostraban una creciente disposición de las bandas de ransomware a atacar infraestructuras públicas.

En mayo, un grupo de ciberdelincuentes asociado a la banda de ransomware DarkSide atacó Colonial Pipeline, cuyos sistemas abastecen de combustible a gran parte de la costa este estadounidense. Esta ofensiva generó escasez en varios estados cuando los consumidores entraron en pánico e intentaron acumular reservas. Al final, Colonial Pipeline decidió pagar un rescate de más de 4 millones de dólares en bitcoin para recuperar el acceso a sus sistemas[8].

Ese mismo mes, un grupo de atacantes relacionado con el ransomware REvil infectó JBS Foods, una empresa de elaboración de productos cárnicos presente en varios países, incluidos EE. UU., Brasil y Australia. El suministro de carne y otros productos cárnicos quedó interrumpido hasta que JBS accedió a pagar un rescate de 11 millones de dólares[9].

7 James Rundle y David Uberti *(The Wall Street Journal)*. "How Can Companies Cope with Ransomware?" (¿Cómo pueden las empresas hacer frente al ransomware?). Mayo de 2021.
8 Collin Eaton y Dustin Volz *(The Wall Street Journal)*. "Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom" (El CEO de Colonial Pipeline explica por qué pagó a los hackers un rescate de 4,4 millones de dólares). Mayo de 2021.
9 Jacob Bunge *(The Wall Street Journal)*. "JBS Paid $11 Million to Resolve Ransomware Attack" (JBS paga 11 millones de dólares para resolver un ataque de ransomware). Junio de 2021.

A principios de julio, REvil también se reveló como el grupo responsable de un ataque a la cadena de suministro de Kaseya, una firma de software[10]. Desde entonces, DarkSide y REvil han desaparecido de la red, pero constantemente surgen otros operadores de ransomware y, además, el cambio de nombre no es infrecuente entre los ciberdelincuentes que desean evitar ser centro de atención.

Con el creciente importe de los rescates y la posibilidad de que los agresores causen daños considerables a infraestructuras nacionales (de forma intencionada o no), los gobiernos de todo el mundo están empezando a darse cuenta de la gravedad de la situación. Después del incidente de Colonial Pipeline, el presidente estadounidense Joe Biden publicó una orden ejecutiva destinada a reforzar las ciberdefensas del país. Acusó al presidente ruso Vladimir Putin y a su gobierno de no perseguir a los grupos de ransomware que operan en territorio ruso.

Cómo funciona el ransomware

El ransomware funciona bloqueando el acceso a un sistema informático o a sus datos, normalmente cifrando archivos de extensiones determinadas (JPG, DOC, PPT, etc.). Los archivos quedan fuera del alcance hasta que la víctima paga al ciberdelincuente por el código de la clave de cifrado que desbloquea los archivos. En muchos casos, se establece un plazo para abonar el rescate. De no cumplirse, el rescate puede multiplicarse por dos o los datos perderse para siempre, divulgarse e incluso destruirse.

Y, en un número de casos cada vez mayor, las víctimas sufren varias extorsiones: primero por la clave de cifrado para desbloquear los datos y después para impedir que los atacantes publiquen o vendan copias en la web oscura.

Costes reales del ransomware

Casi el 80 % de las empresas estadounidenses sufrieron un ataque de ransomware en 2020 y un 68 % de ellas optó por pagar el rescate[11]. Las consecuencias económicas de un ataque pueden ser considerables y el importe del rescate se incrementa año tras año.

En la primera mitad de 2021, se confirmó el pago de 4,4 millones de dólares por parte de Colonial Pipeline[12], 11 millones por parte de JBS Foods[13] y un récord de 40 millones por parte de CNA Financial[14]. Y estos son solo los casos que se hicieron públicos. Es probable que el verdadero coste económico del ransomware sea mucho mayor de lo que revelan estas cifras, ya que inevitablemente algunas empresas intentan afrontar la intrusión en privado.

Pero el coste empresarial no se limita al gasto económico.

El 80 %
de las empresas estadounidenses sufrieron un ataque de ransomware en 2020.

El 68 %
decidieron pagar el rescate.

10 Jonathan Vanian *(Fortune)*. "Everything to know about REvil, the group behind a big ransomware spree" (Todo lo que hay que saber sobre REvil, el grupo responsable de una gran explosión de ransomware). Julio de 2021.
11 Proofpoint. "State of the Phish 2021". Febrero de 2021.
12 Collin Eaton y Dustin Volz (*The Wall Street Journal*). "Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom" (El CEO de Colonial Pipeline explica por qué pagó a los hackers un rescate de 4,4 millones de dólares). Mayo de 2021.
13 Jacob Bunge (*The Wall Street Journal*). "JBS Paid $11 Million to Resolve Ransomware Attack" (JBS paga 11 millones de dólares para resolver un ataque de ransomware). Junio de 2021.
14 Kartikay Mehrotra and William Turton (Bloomberg). "CNA Financial Paid $40 Million in Ransom After March Cyberattack" (CNA Financial paga 40 millones de dólares como rescate tras el ciberataque de marzo). Mayo de 2021.

Según Coveware, una consultora de respuesta a incidentes de ransomware, más de tres cuartos de los ataques de ransomware de la primera mitad de 2021 incluían la amenaza de divulgar los datos filtrados[15]. En 2020, la misma empresa informó de que el 65 % de las víctimas amenazadas con la divulgación de sus datos optó por pagar el rescate, lo que subraya el grave riesgo para la reputación que conlleva la filtración malintencionada de datos.

Quizá el coste más difícil de prever es el precio de la interrupción de la actividad, ya que las cadenas de suministro se paran, los equipos de ventas pierden acceso a las listas de clientes existentes y potenciales e incluso las herramientas de comunicación más básicas se vuelven impracticables. Las consecuencias pueden ser aún mayores en sectores críticos como la sanidad, tal como comprendió el sistema público de salud de Irlanda cuando un ataque del grupo del ransomware Conti demoró tratamientos y canceló servicios ambulatorios, entre ellos el diagnóstico radiológico[16].

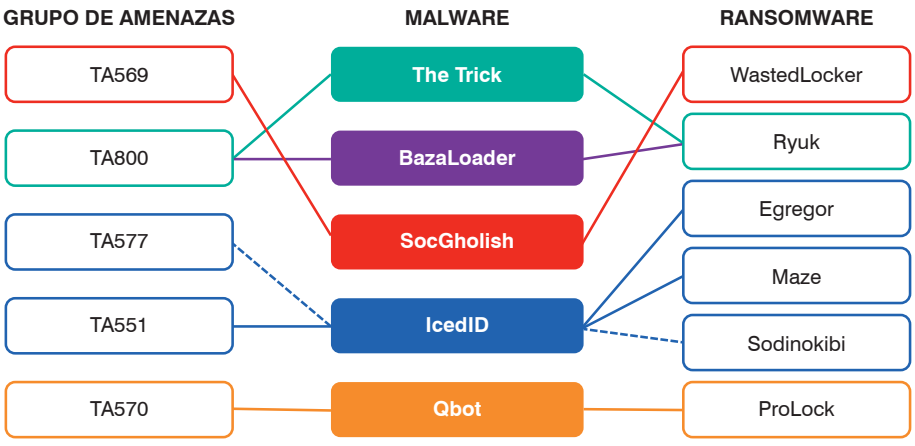
Ransomware y correo electrónico

Un elevado porcentaje de los ataques de ransomware empieza, directa o indirectamente, con un mensaje de phishing.

Un elevado porcentaje de los ataques de ransomware empieza, directa o indirectamente, con un mensaje de phishing. Estos mensajes incitan a los usuarios a abrir un adjunto malicioso o a hacer clic en una URL maliciosa.

Pero, en los cinco años transcurridos desde que Locky consiguió colarse en millones de bandejas de entrada, las cosas han cambiado. Últimamente, el ransomware se distribuye como infección secundaria una vez contaminado el sistema con un troyano o un cargador. A continuación, los grupos que distribuyen este tipo de malware venden el acceso a grupos de ransomware, que estudian las redes infectadas en busca de los objetivos más valiosos. Los agentes o facilitadores cobran una tarifa plana o un porcentaje del rescate a cambio de proporcionar un punto de entrada en la red.

No hay una mera relación 1:1 entre el malware de acceso inicial y la variante de ransomware que se distribuye a las víctimas, pero los investigadores de Proofpoint y de otras empresas del sector han encontrado asociaciones importantes.



15 Coveware. "Q2 Ransom Payment Amounts Decline as Ransomware becomes a National Security Priority" (El importe de los rescates pagados desciende en el segundo trimestre mientras el ransomware se convierte en prioridad de seguridad nacional).
16 Danny Palmer (ZDNet) "The human cost of ransomware: Disruption to Irish health service will continue for months" (El coste humano del ransomware: la interrupción del servicio de salud irlandés se prolonga durante meses). Junio de 2021.

Si bien la red de relaciones entre grupos de ciberdelincuentes es compleja, no lo es la secuencia de eventos del típico ataque de ransomware iniciado por correo electrónico: la infección por un troyano o un cargador deja la red en una posición de vulnerabilidad frente a las bandas que buscan objetivos de gran valor. Por lo tanto, para la mayor parte de las organizaciones la primera línea de defensa contra el ransomware es asegurarse de estar protegidas de otras clases de malware.

Es decir, si son capaces de bloquear el cargador, se habrán librado del ransomware.

Amenazas internas

En 2020, alguien ofreció 500 000 dólares a un empleado de Tesla por instalar ransomware en la red corporativa.

Además de los exploits tecnológicos y los señuelos que llegan por correo electrónico, los delincuentes han abierto otro frente en la guerra del ransomware: los colaboradores activos. En un pequeño aunque alarmante número de casos, los agresores intentan captar empleados de las empresas seleccionadas para que instalen ransomware en su lugar de trabajo a cambio de dinero.

En 2020, alguien ofreció 500 000 dólares a un empleado de Tesla por instalar ransomware en la red corporativa. El empleado denunció la tentativa y el acusado fue arrestado y declarado culpable, no sin antes alardear de haber tenido éxito con otras empresas.

En agosto de 2021, rastreamos una campaña de correo electrónico que ofrecía a los empleados un millón de dólares por instalar el ransomware DemonWare en la oficina. Más o menos en la misma época, LockBit modificó su nota de rescate con el ofrecimiento de pagar a los empleados millones de dólares a cambio de credenciales de cuentas válidas.

El agresor de DemonWare no intentó distribuir malware entre las direcciones de correo de los empleados reclutados. Algunos programas avanzados de seguridad del correo electrónico pueden detectar estas propuestas basándose en otras señales. Aun así, es buena idea enseñar a los empleados a reconocer estas amenazas y a denunciarlas inmediatamente.

Canales de distribución

El ransomware se distribuye a través de varios vectores de ataque básicos:

- Correo electrónico, incluidos los archivos adjuntos que contienen ransomware y las URL que conducen a archivos maliciosos
- Acceso a redes privadas virtuales (VPN) y protocolos de escritorio remoto (RDP) comprometidos
- Vulnerabilidades en equipos de red de la empresa
- Sitios web/enlaces infectados a través de redes sociales y publicidad infectada con malware (malvertising)
- Otro malware (como cargadores y ladrones) que pueden infectar con ransomware sistemas ya comprometidos

Aun cuando el ransomware provenga de otro malware, a menudo el correo electrónico es el vector inicial.

Son mensajes que parecen legítimos y pueden engañar a los empleados desprevenidos. Con frecuencia, los mensajes se disfrazan de actualizaciones oficiales de software, facturas impagadas o incluso una nota del jefe dirigida a un subordinado directo.

Por qué sigue aquí

El ransomware es un exploit con varias décadas de antigüedad, pero ha cobrado mayor importancia como amenaza por cuatro factores principales.

Más canales de distribución

Los ciberdelincuentes pueden atacar a miles de entidades a la vez utilizando distintos vehículos de ataque que abren la puerta a ataques de ransomware secundarios.

Las ciberdefensas convencionales se ven desbordadas con amenazas que llegan de todas partes:

- Campañas masivas de correo electrónico orquestadas con redes de bots
- Vulnerabilidades aprovechables del hardware y el software de red
- Malware polimórfico que supera la capacidad de los proveedores de seguridad para crear a tiempo nuevas firmas de malware
- Malvertising y sitios web comprometidos fuera del perímetro de la organización

Juntos, estos factores favorecen la intrusión inicial y dan al ransomware más oportunidades de infiltrarse en la red.

Objetivos más lucrativos

En lugar de utilizar ataques de amplio espectro, ahora los ciberdelincuentes tienden a elegir empresas con datos sensibles, departamentos de TI sobrecargados y fuertes motivaciones para liquidar la cuestión con rapidez.

Para añadir más leña al fuego, están los problemas de seguridad habituales en hospitales, departamentos de policía, colegios y otros organismos de la Administración estatal y local.

Para ellos, el tiempo de inactividad de la red no es una opción viable. No es de sorprender que muchos hagan rápidamente el cálculo y concluyan que desembolsar la cantidad exigida por el rescate es la mejor estrategia empresarial.

Mejor selección de objetivos y tácticas más avanzadas

El ransomware solía ser un juego de números: atacar a cientos de miles de destinatarios en campañas de correo electrónico de gran volumen y pedir un rescate reducido con la esperanza de que suficientes víctimas picaran el anzuelo.

Hoy, los agresores son más selectivos con sus objetivos. Para obtener sumas más elevadas, buscan sistemas y datos fundamentales para el negocio a los que las víctimas necesitan acceder desesperadamente.

Al mismo tiempo, los ataques de ransomware son cada vez más sofisticados. En lugar de utilizar ransomware en la primera etapa de un ataque, los ciberdelincuentes comprometen los sistemas con malware multifunción más robusto.

Una vez que consiguen infiltrarse, despliegan el ransomware en los dispositivos de interés.

Bitcoin y otras monedas digitales

Desde su aparición en 2009, el bitcoin ha sido una bendición tanto para los activistas de las libertades civiles como para los ciberdelincuentes. Los pagos no pueden rastrearse hasta el emisor ni el receptor, lo que proporciona una vía anónima y expedita para las transacciones privadas.

Al exigir el pago en esta moneda digital, los ciberdelincuentes obtienen una anonimidad que hace el cobro mucho más fácil que antes. Las primeras formas de ransomware a veces requerían el uso de tarjetas de débito prepago. Aunque este método podía sortear las medidas antifraude de los bancos, es mucho más complicada para las dos partes que intervienen en la transacción.

Todas las variantes principales del ransomware solicitan el pago en bitcoines (consulte **"La pista de los bitcoines" en la página 13**).

Una amenaza antigua pero más presente que nunca

Para entender lo insidiosos que son actualmente los ataques de ransomware (y cómo pueden afectar directamente a los consumidores), recuerde el ataque a Garmin Ltd., un servicio de red que distribuye datos a relojes inteligentes y controladores de la actividad física, entre otros dispositivos.

Garmin Ltd. utiliza tecnología GPS para compartir datos con controladores de la actividad física, como los de FitBit y Apple. Pero estos servicios se interrumpieron el 23 de julio de 2020 cuando Garmin fue víctima de un ciberataque que cifró sus sistemas online, entre ellos, "la atención al cliente, las aplicaciones para clientes y las comunicaciones de la compañía", según informó la empresa en una nota de prensa.

Garmin no pudo prestar muchos de sus servicios porque estos y los que suministraban sus centros de llamadas se cifraron, de forma que ni los usuarios finales ni la empresa podían acceder a ellos. Los servicios no pudieron descifrarse hasta que al parecer Garmin pagó un rescate de 10 millones de dólares a los agresores.

"Fuentes próximas a la respuesta al incidente de Garmin y un empleado de Garmin confirman […] que Garmin fue atacada por el ransomware WastedLocker", informaba el 1 de agosto el sitio de noticias tecnológicas BleepingComputer.

> "El departamento de TI de Garmin intentó cerrar a distancia todos los ordenadores de la red porque los ciberdelincuentes estaban cifrando los dispositivos, incluidos los ordenadores personales domésticos conectados por VPN", informaba BleepingComputer. "Al no lograrlo, indicaron a los empleados que apagaran cualquier ordenador de la red al que tuvieran acceso".

Garmin aseguraba que comenzó a reiniciar sus servicios online al cabo de cuatro días.

BleepingComputer añadía que el ransomware WastedLocker se ha relacionado con un grupo de ciberdelincuentes radicado en Rusia llamado Evil Corp. Aunque el nombre puede sonar como el malo de unos dibujos animados, Evil Corp. fue condenado por el Departamento de Justicia de los EE. UU. en diciembre de 2019 por su papel en el incidente del malware Dridex y por utilizar ransomware como parte de otros ataques, incluido el ransomware Locky y su propia variante, conocida como BitPaymer.

La pista de los bitcoines

En el secuestro tradicional por un rescate, la mayor dificultad siempre ha estado en recoger el dinero y huir. Por desgracia, los ciberdelincuentes del ransomware lo tienen mucho más fácil.

La forma más utilizada de pago es el uso de criptomonedas imposibles de rastrear, la más conocida de las cuales es el bitcoin. El bitcoin permite el pago de persona a persona a través de Internet sin la participación de bancos ni gobiernos.

Para entender las criptomonedas, basta con imaginarlas como el equivalente electrónico de las fichas de un casino. Las fichas no tienen valor intrínseco en el mundo real, pero los usuarios pueden comprarlas con su moneda local, utilizarlas en el establecimiento (en este caso, Internet) y después volver a canjearlas por su moneda al salir.

Igualmente, las criptomonedas pueden comprarse en Internet a fuentes legítimas con una tarjeta de crédito o una cuenta bancaria. En el caso del ransomware, una víctima puede convertir dinero local en bitcoines y después enviarlos a una dirección de criptomonedas anónima indicada por el ciberdelincuente.

Las monedas no siempre van directamente al atacante. En general, las monedas acaban en un "mezclador", un servicio electrónico que mezcla los bitcoines con otros y después los dispensa al ciberdelincuente (con otra numeración pero con el mismo valor, descontada la comisión).

Igual que ocurre con el blanqueo de dinero en el mundo físico, los delincuentes pueden conseguir pagos imposibles de rastrear que después convierten a la moneda física local cambiando los bitcoines por efectivo.

A diferencia de las monedas garantizadas por los gobiernos, las criptomonedas no están reconocidas ampliamente como dinero, más bien se consideran algo equivalente a las fichas de póker o de juego. Por lo tanto, el sistema de transmisión y los mezcladores no están regulados ni se definen como blanqueo de capitales, aunque sin duda su efecto es el mismo.

El atractivo del bitcoin es evidente. Facilita a los atacantes una cibermoneda difícil de rastrear y disponible en todo el mundo que se convierte directamente a divisa local: en otras palabras, son "billetes sin marcar".

Esta vía reúne claras ventajas sobre el uso de tarjetas de crédito robadas, pues su valor se desploma día a día porque las entidades financieras ya tienen práctica en cerrar con rapidez las cuentas de las víctimas.

Y el hecho de que el valor del bitcoin se haya incrementado en los últimos años y haya llegado a alcanzar casi 65 000 dólares por unidad añade un posible beneficio económico extra para los ciberdelincuentes.

Después del ataque a Colonial Pipeline, el FBI anunció que habían recuperado cerca de la mitad del rescate pagado en bitcoines. La agencia no ha revelado el modo y tampoco está claro si es posible repetir este tipo de recuperación[17].

17 Katie Brenner, Nicole Perlroth *(New York Times)* "U.S. Seizes Share of Ransom From Hackers in Colonial Pipeline Attack" (EE. UU. recupera parte del rescate de los hackers en el ataque a Colonial Pipeline). Junio de 2021.

Antes del ataque

La mejor estrategia de seguridad consiste en evitar la extorsión. Es algo que queda perfectamente al alcance de la mayoría de las empresas, pero que requiere planificación y trabajo antes de que sobrevenga la crisis.

Utilice herramientas de copia de seguridad y restauración

El aspecto más importante de cualquier estrategia de seguridad contra el ransomware es realizar regularmente copias de seguridad de sus datos. La mayoría de las empresas tiene esta práctica incorporada, pero sorprendentemente muy pocas realizan simulacros de copia de seguridad y restauración. Ambos procesos son importantes: los simulacros de restauración son la única manera de saber de antemano si el plan de copia de seguridad funciona.

Puede que tenga que resolver algún detalle antes de que se presente un problema. Si realiza pruebas periódicas de copia de seguridad y restauración, el impacto de una infección de ransomware no será devastador: su empresa dispondrá de un punto de restauración seguro y reciente.

Actualice y aplique parches

Mantenga totalmente actualizados los parches y las versiones de los sistemas operativos, el software de seguridad, las aplicaciones y el hardware de red. Parece bastante obvio, pero, según una encuesta reciente, más de la mitad de las organizaciones afirman que no es fácil saber si los parches corrigen las vulnerabilidades a tiempo y que las actualizaciones varían enormemente en complejidad y calendario de publicación[18].

Sin embargo, hay lugares a los que acudir para controlar la gestión de parches, como el Center for Internet Security (CIS), una organización no lucrativa que comparte y promueve buenas prácticas para la administración de seguridad de TI, incluida la amenaza del ransomware.

Para mantener un entorno seguro es imprescindible superar la "fatiga de los parches" y, para que los ciberdelincuentes no dispongan de puntos de acceso fácil desde los que lanzar sus ataques de ransomware, puede ser clave cerrar los protocolos de escritorio remoto y aplicar parches a las VPN.

Planifique la respuesta

Sepa de antemano cómo va a responder para, en caso de ataque, poder centrarse en la contención y la recuperación. En el momento, afrontar una intrusión de ransomware es una experiencia estresante y, mientras los agresores intentan adentrarse más en la red para hacer más daño, cada segundo cuenta.

18 Ponemon Institute. "Today's State of Vulnerability Response: Patch Work Demands Attention" (Estado actual de la respuesta a vulnerabilidades: hay que prestar atención a los parches). Abril de 2018.

En tiempo real es más difícil hallar la respuesta a preguntas fundamentales, entre ellas a quién hay que informar, cómo mantener las comunicaciones y cuánto está dispuesto a pagar (si es que está dispuesto a pagar). Esta presión crea cuellos de botella potenciales en la toma de decisiones y provoca costosas demoras. Si decide pagar el rescate, tendrá que elaborar un proceso adecuado que incluya a los directivos correspondientes, al personal operativo y a la asesoría jurídica.

No existe un plan de respuesta universal a los ataques de ransomware. Los hospitales y otras infraestructuras esenciales sopesan el coste de la interrupción de la actividad de forma muy diferente a las empresas de consumo. Una buena manera de planificar cada etapa de la respuesta es poner en marcha un ejercicio completo de simulación.

Invierta en soluciones de seguridad del correo electrónico, la web y la nube robustas y centradas en las personas

Actualmente, los mensajes de correo electrónico de phishing son sofisticados y altamente selectivos. Los delincuentes investigan meticulosamente sus objetivos para crear mensajes que parezcan legítimos y se aprovechan de la naturaleza humana para inducir a las víctimas a hacer clic.

Correo electrónico: el principal vector

En todas las redes deben ejecutarse y actualizarse gateways de correo electrónico, filtros web y software antivirus tradicionales. Sin embargo, por sí solas estas medidas no pueden hacer frente a la amenaza del ransomware. Para ser eficaz, una solución de seguridad del correo electrónico debe ir más allá.

El hecho de que el correo electrónico sea el punto de infección inicial que abre la puerta a la mayor parte del ransomware, obliga a disponer de soluciones avanzadas que protejan este vector crítico.

Esto significa analizar las URL incrustadas y los archivos adjuntos para asegurar que no entra contenido malicioso en el sistema. Los ciberdelincuentes siempre van un paso por delante y las configuraciones habituales de seguridad del correo electrónico se sustentan excesivamente en firmas obsoletas.

Las soluciones avanzadas de seguridad del correo electrónico son capaces de proteger frente a las URL, los archivos adjuntos y los documentos maliciosos incluidos en mensajes de correo electrónico que permiten distribuir ransomware. Y la autenticación del correo electrónico basada en la norma DMARC puede detener los ataques basados en la suplantación de dominios, es decir, los que fingen provenir del dominio de correo electrónico de la empresa para ganarse la confianza de los usuarios. La solución de seguridad del correo electrónico también debe proteger frente a otros tipos de usurpación de identidad, como la falsificación del "display name" (nombre mostrado) y los dominios similares.

Proteja sus cuentas cloud

Las cuentas de correo electrónico basadas en la nube son otro vector principal de propagación de malware. Los ciberdelincuentes pueden tomar el control de las cuentas cloud de los usuarios para atacar a otros usuarios de la organización. Las cuentas de correo electrónico pueden comprometerse de varias maneras, como:

- Ataques por fuerza bruta automatizados que prueban innumerables combinaciones de usuario/contraseña hasta que alguna funciona

- Robo de credenciales externas, porque saben que los usuarios a menudo reutilizan las contraseñas en otras cuentas
- Malware de robo de credenciales
- Controles cloud defectuosos

La protección de las cuentas cloud de los usuarios forma parte fundamental de su protección frente a los ataques de ransomware.

Por último, solicite a los usuarios remotos que se conecten a Internet a través de una VPN para que sus defensas de ciberseguridad los protejan estén donde estén.

Convierta a sus empleados en su última y sólida línea de defensa

La mayoría de las infecciones de malware empiezan por un solo empleado bienintencionado que abre lo que parece ser un mensaje de trabajo.

Por eso son cruciales la formación y la concienciación de los empleados. Deben saber lo que pueden y no puede hacer, cómo evitar los ataques de ransomware y cómo denunciarlos. Si el programa de formación puede mostrar ataques del mundo real y facilitar un sistema para denunciar mensajes sospechosos, los usuarios aprenderán mejor a detectar mensajes maliciosos y se reforzarán comportamientos positivos.

Si alguien recibe una petición de rescate, nunca debe intentar pagar por su cuenta y debe saber cómo alertar inmediatamente al equipo de seguridad. El pago puede acarrear graves consecuencias para la seguridad y la reputación de la marca y, en algunos casos, comportar importantes sanciones administrativas. Esta decisión debe sopesarla cuidadosamente la dirección con la asesoría jurídica.

Nuestras investigaciones demuestran que los ciberdelincuentes se aprovechan activamente de la curiosidad y los errores humanos. Forma parte de una tendencia más amplia: engañar a las personas para que se conviertan en cómplices involuntarios de su propósito de bloquear información y exigir rescate.

Estos ataques sacan partido de la ignorancia del usuario. En general, necesitan que alguien abra un archivo adjunto malicioso, que descargue, abra o ejecute un documento o un script, o que emprenda cualquier otra acción. Por ejemplo, en cuanto el usuario hace clic en el botón "Mostrar contenido" para activar las macros de un documento malicioso, este puede descargar ransomware e iniciar el proceso de ataque.

La formación más eficaz enseña a los usuarios las técnicas y las campañas de ataque del mundo real e incorpora lo último en inteligencia sobre amenazas para que conozcan las que tienen más probabilidades de afrontar. Las simulaciones de phishing pueden identificar a los usuarios especialmente susceptibles a dejarse engañar por el ransomware y otras tácticas de ataque.

Medidas técnicas que recomiendan las autoridades estadounidenses

Aparte de la estrategia de alto nivel propuesta en esta guía, el FBI también recomienda las siguientes medidas técnicas para atajar los ataques de ransomware.

Audite y gestione los privilegios de los usuarios

Aplique el principio de privilegios mínimos a la hora de otorgar permisos de acceso a recursos compartidos de archivos, directorios y red.

Por ejemplo, los usuarios que no necesitan modificar un archivo solo deben tener permiso de lectura para acceder a él. En muchos casos, no deben tener acceso en absoluto. A un cajero no le hace falta acceder a los registros financieros de la empresa. Y el CEO de un hospital no precisa consultar las historias clínicas de los pacientes.

Otorgue a los usuarios únicamente el nivel de acceso que requieren para hacer su trabajo.

Impida la ejecución de código en determinados lugares

Despliegue controles de software para impedir la ejecución de código en lugares habituales de ransomware. Entre ellos están las carpetas temporales que crean los navegadores web y los directorios de archivos comprimidos de la carpeta AppData/LocalAppData de Windows.

Limite el software desconocido

Considere la posibilidad de aplicar una política de listas seguras que permita a los sistemas ejecutar únicamente programas conocidos y autorizados. Esta política impediría la ejecución de gran parte del ransomware, aunque quizá no sea viable en todos los lugares de trabajo.

Utilice tecnología de máquinas virtuales

La tecnología de máquinas virtuales ejecuta aplicaciones e incluso sistemas operativos enteros en un entorno aislado.

Podría considerarse una "cámara de detonación" de software. Cuando se ejecuta código sensible o no autorizado en el entorno de una máquina o un contenedor virtual, todos los problemas de seguridad que surgen se circunscriben a ese entorno virtual y no afectan a otras partes del sistema.

Mantenga segmentados los sistemas y los datos

Mantenga aparte los datos y los sistemas de valor para que, si se produce un problema de seguridad en un sistema, no afecte a los demás. Por ejemplo, los datos confidenciales de una investigación o un negocio no deben residir en el mismo servidor y segmento de red que el entorno de correo electrónico de la organización.

Las recomendaciones completas del gobierno de EE. UU. están disponibles en **fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf.**

Durante el ataque

Acaba de sufrir un ataque de ransomware. ¿Y ahora qué?

Aunque la mejor estrategia contra el ransomware es evitarlo, la creciente sofisticación de los ataques contra la cadena de suministro ha demostrado que hasta las empresas mejor preparadas pueden ser víctimas. Incluso es posible que el ransomware no sea el primer malware en infectar el sistema, ya que ahora muchos grupos de ciberdelincuentes prefieren comprar el acceso a objetivos ya infectados con troyanos o malware cargador.

Durante un ataque, hay problemas que resolver a corto plazo, como poner de nuevo en funcionamiento ordenadores, teléfonos y redes y afrontar la petición de rescate.

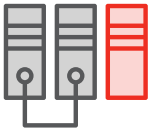
Pero las reacciones que dicta el miedo no son útiles y pueden empeorar las cosas.

Denuncie ante las fuerzas de seguridad

El ransomware, igual que cualquier otra forma de robo y extorsión, es un delito. Nadie tiene derecho a apoderarse de dispositivos, redes ni datos, y mucho menos a exigir un rescate a cambio de su devolución. Denunciarlo ante las autoridades competentes es un primer paso necesario.

Póngase inmediatamente en contacto con las fuerzas de seguridad locales o estatales. No tema coger directamente el teléfono y llamarles. Están para ayudarle.

Si tiene un seguro antiransomware, también debe ponerse en contacto con la aseguradora. Pueden ayudarle a coordinar la respuesta y la investigación del incidente.



Aísle los sistemas infectados

En cuanto los empleados vean una petición de rescate o adviertan algo raro, como que súbitamente han perdido acceso a sus propios archivos, deben desconectar el equipo infectado de la red y llevarlo al departamento de TI.

No aconsejamos indicar a los empleados que reinicien el sistema. Solo el equipo de seguridad de TI debe intentar reiniciarlo y esta medida solo funcionará si se trata de "scareware", es decir, ransomware falso.

En estos casos, lo que parece ser ransomware se describe mejor como "scareware". Aunque bloquee la pantalla del usuario con una petición de rescate e instrucciones de pago, en realidad no cifra los datos. En estas situaciones pueden ser útiles las herramientas antimalware estándar.

No siempre es fácil distinguirlos. Determine el alcance del problema sirviéndose de la inteligencia de amenazas. Aunque cualquier ransomware es malicioso, algunos ataques son peores que otros. Su respuesta (incluida la decisión de si pagar o no el rescate) debe basarse en diversos factores.

Hágase estas preguntas:

- **¿De qué tipo de ataque se trata?** ¿Se trata de una infección secundaria? ¿Procede de descargadores, troyanos de acceso remoto (RAT) u otro malware instalado en el equipo infectado o en otros equipos de la red?
- **¿Quién se ha visto afectado en la empresa?** ¿Qué grado de propagación ha alcanzado la infección? ¿Hay un ciberdelincuente explorando activamente la red, filtrando datos o a punto de distribuir ransomware a otros dispositivos?
- **¿Qué permisos de red tienen las cuentas o los dispositivos comprometidos?** Puede que el ransomware se haya instalado únicamente después de que los ciberdelincuentes se hayan desplazado lateralmente en la red o hayan robado credenciales y otros datos.

Las respuestas deben ayudar a los administradores de la red a averiguar la magnitud del problema, a diseñar un plan de acción y, posiblemente, a frenar la propagación.

Tenga en cuenta que el ransomware se extiende con rapidez y que, a menudo, es un producto secundario de otras amenazas. Si detecta una infección, probablemente hay otras que no ha visto. Busque proactivamente otros problemas en el entorno.

Despliegue su plan de respuesta

Dependiendo de la configuración de la red, quizá todavía sea posible contener la propagación a una sola estación de trabajo.

En el mejor de los casos, el equipo infectado puede sustituirse por un ordenador nuevo y los datos restaurarse a partir de la copia de seguridad. En el peor, se infectan todas las máquinas de la red. Tendrá que hacer un cálculo de costes y beneficios que compare el tiempo y los recursos necesarios para restaurar los datos con el pago del rescate.

Si el ransomware ya ha alcanzado sus servidores, aísle los sistemas infectados: es aquí donde la segmentación de la red puede ayudarle a contener la amenaza.

Buena parte de su respuesta consistirá en decidir si pagar el rescate. La decisión es compleja y quizá necesite consultar a las fuerzas de seguridad y a su asesoría jurídica. Para algunas víctimas, puede que pagar resulte inevitable (consulte **"Pagar o no pagar: el dilema moral y legal del ransomware" en la página 21**).

Olvide las herramientas gratuitas de descifrado de ransomware. Algunos proveedores de seguridad ofrecen programas gratuitos de descifrado de ransomware. En algunos casos, pueden ayudarle a recuperar sus datos sin pagar el rescate, pero la mayoría solo funcionan con una variedad de ransomware o incluso con una sola campaña de ataque. Cuando los ciberdelincuentes actualizan su ransomware, las herramientas gratuitas quedan obsoletas y es probable que no funcionen con la variante utilizada contra su empresa.

Quizá tenga suerte con una herramienta gratuita de descifrado, pero no la convierta en parte de su plan de respuesta a incidentes.

Restaure a partir de las copias de seguridad

La única manera de recuperarse por completo de una infección de ransomware es restaurarlo todo a partir de las copias de seguridad, y estas deben hacerse a diario. Quizá este sea el último paso que dar tras una infección, pero debe ser el primero en materia de prevención.

No obstante, aun teniendo copias de seguridad recientes, pagar el rescate puede ser más interesante desde el punto de vista económico y operativo. Restaurar las copias de seguridad lleva tiempo y esfuerzo y es posible que algunas empresas no puedan afrontar el tiempo de inactividad.

Pagar o no pagar: el dilema moral y legal del ransomware

El ransomware ya es de por sí suficientemente nocivo, pero uno de sus aspectos especialmente detestables es que obliga a las víctimas a hacer una elección necesaria pero moralmente problemática. Con la presión de una amenaza de ransomware, a nadie le sobra tiempo para calibrar cuidadosamente los matices morales del pago. El ataque se está produciendo aquí y ahora.

Pagar no es solo un mal aborrecible pero necesario: financia activamente al ciberdelincuente que acaba de introducirse en su red y robar sus datos, señala a su empresa como entidad cuya red es vulnerable y que tiene motivaciones para pagar y permite al ciberdelincuente sufragar futuros ataques.

Pero los últimos ataques han puesto de manifiesto una realidad incómoda: no siempre está claro si hay que pagar.

Ninguna organización quiere ser extorsionada y mucho menos financiar redes criminales, pero, a la vez, puede que muchas víctimas concluyan que no les queda más remedio. En cierto modo, es el precio que hay que pagar por haber asignado recursos insuficientes al departamento de TI y dejar que el software funcione sin parches o sin actualizar. En EE. UU., todavía hay hospitales que utilizan Microsoft Windows XP en ordenadores antiguos y el rescate suele ser un precio relativamente pequeño que pagar cuando hay vidas en juego.

A veces, hasta el FBI ha recomendado a las víctimas que paguen el rescate. Oficialmente, la agencia desaconseja pagar, pero hace poco ha prevenido al Congreso en contra de prohibir el pago[19]. Según la agencia, es posible que las empresas no recuperen sus datos ni siquiera pagando.

Sin embargo, en 2020 el Departamento del Tesoro estadounidense publicó una advertencia recordando a los ciudadanos y a las empresas estadounidenses que pagar un rescate puede considerarse infracción de reglas financieras y puede acarrear el pago de una sanción. Las repercusiones de este consejo para aseguradoras y negociadores de respuesta ante incidentes todavía son inciertas, pero los posibles riesgos jurídicos añaden otra capa de complejidad a la toma de decisiones.

Otra campaña para urgir a las personas a no pagar rescates procede de la Europol, el organismo policial de la Unión Europea. Su iniciativa "No More Ransom", lanzada hace cinco años, es una asociación público-privada cuyo fin es ayudar a las víctimas de ciberataques a reconstruir sus archivos de datos y descifrarlos sin pagar.

La iniciativa ha ayudado a seis millones de víctimas de ransomware a recuperar sus archivos y a evitar pagar casi 1000 millones de euros en rescates. (Las herramientas de "No More Ransom" están disponibles para todo el mundo, no solo para los ciudadanos de la Unión Europea).

Las organizaciones deben sopesar los pros y los contras a la hora de elegir la mejor forma de actuar. Estos factores pueden incluir:

- Tiempo y recursos para conectarse de nuevo a Internet.
- Las responsabilidades para con los accionistas de mantener la empresa en funcionamiento.
- La seguridad de los clientes y de los empleados.
- El tipo de actividad delictiva que el pago terminaría financiando.
- Las responsabilidades legales que puedan derivarse de proporcionar dinero a un particular o un Estado sancionado.

Tal y como sucede con la mayoría de las preguntas complejas, ninguna organización responderá como las demás.

Los últimos ataques han puesto de manifiesto una realidad incómoda: no siempre está claro si hay que pagar.

19 Maggie Miller *(The Hill)* "Top FBI Official Advises Congress Against Banning Ransomware Payments" (Alto cargo del FBI aconseja al Congreso en contra de prohibir los pagos de ransomware). Julio de 2021.

Después del ataque

Independientemente del daño que cause el ransomware, un ataque revela que un fallo de seguridad ha comprometido un dispositivo o una red. Ahora que las cosas han vuelto a la normalidad, tiene la oportunidad de aprender de esa violación de la seguridad para evitar futuros ataques.

Le recomendamos que realice una evaluación completa de la seguridad, quizá con la ayuda de una empresa de servicios externa, para detectar si hay amenazas aún presentes en el entorno. También es el momento de analizar a fondo sus herramientas y procedimientos de seguridad y averiguar dónde han sido insuficientes.

Limpie los sistemas

Algunos tipos de ransomware contienen otras amenazas o troyanos de puerta trasera que pueden dar lugar a futuros ataques. En otros casos, es una intrusión preexistente la que abre la puerta a la infección de ransomware. Por eso es imprescindible limpiar todos los dispositivos y restaurarlos a partir de una copia de seguridad limpia. Busque a fondo amenazas ocultas que puedan habérsele pasado por alto en medio del caos.

Lleve a cabo un examen retrospectivo

Revise su preparación y su respuesta frente a la amenaza. ¿Cómo se ha ejecutado el plan de crisis? ¿Puede mejorar la configuración de la red para contener futuros ataques? ¿Puede implementar una solución más robusta de seguridad del correo electrónico? ¿Debe aplicar una estrategia general de ciberseguridad completamente nueva?

Audite las medidas de seguridad actuales y pregúntese si son suficientes para combatir las amenazas de hoy. Convierta todo ello en una experiencia de aprendizaje, porque es muy fácil que vuelva a ocurrir.

Si no averigua cómo entró el ransomware, no tendrá manera de detener el próximo ataque.

Evalúe el nivel de concienciación de los usuarios

Muchas variantes de ransomware dependen de la interacción humana para desplegar su payload, ya sea una infección directa o una distribución posterior a través de otro tipo de malware. Si las medidas de seguridad actuales fallan y un mensaje falso de "factura impagada" consigue llegar al servidor de correo electrónico, son los usuarios bien informados los que constituirán la última línea de defensa para que la empresa, el hospital o el colegio siga en funcionamiento o se convierta en otra estadística más del ransomware. Asegúrese de que sus empleados, su personal administrativo y sus instructores están preparados.

Quizá también merezca la pena invertir en herramientas de simulación de phishing para concienciar a los empleados, identificar a los usuarios especialmente vulnerables y mejorar la seguridad en general. Al mostrar ataques reales, así como las últimas técnicas de ingeniería social y métodos de ataque, las simulaciones de phishing pueden contribuir a analizar e identificar las vulnerabilidades de seguridad relacionadas con las personas antes de un ataque real.

Formación

Una vez analizados los conocimientos de los empleados, elabore un plan de estudios para abordar su vulnerabilidad ante los ciberataques e incluya las lecciones aprendidas en anteriores enfrentamientos. Planifique cursos periódicos de seguimiento para las personas más vulnerables, las que reciben más ataques o las que tienen mayores privilegios de acceso a datos, sistemas y otros recursos sensibles.

E integre el programa de formación con sus otras ciberdefensas para ayudar a las personas no solo a identificar los ataques, sino también a notificarlos.

Invierta en defensas modernas

El objetivo de los ciberataques actuales son las personas, no las infraestructuras. Busque soluciones de seguridad que adopten una estrategia centrada en las personas para mantenerlas protegidas.

Los atacantes no ven el mundo como un diagrama de red. Despliegue una solución que permita ver a quién se dirige el ataque, cómo actúa y si la víctima ha hecho clic. Tenga en cuenta el riesgo individual que representa cada usuario, por ejemplo, qué tipo de ataques recibe, a qué datos tiene acceso y si suele ser presa de los ciberdelincuentes.

Al mismo tiempo, mantenga el contenido de los sitios web peligrosos fuera del entorno. La tecnología de aislamiento web puede mantener las páginas web de las URL sospechosas y no verificadas en un contenedor protegido dentro del navegador web habitual de los usuarios. El aislamiento web puede ser una protección esencial para las cuentas de correo electrónico compartidas, que son difíciles de proteger con autenticación multifactor. La misma tecnología puede aislar la navegación web personal y los servicios de correo web de los usuarios, lo que les da libertad y privacidad sin poner en riesgo a la empresa.

Los ataques focalizados y dirigidos exigen disponer de inteligencia sobre amenazas avanzada. Busque una solución que combine técnicas estáticas y dinámicas para detectar nuevas herramientas, tácticas y objetivos de ataque y que luego aprenda de ellas.

Pasos siguientes

El ransomware existirá de una forma u otra mientras los ciberdelincuentes puedan encontrar maneras de hacer dinero con él. Las recomendaciones de esta guía pueden iniciarle en el camino para afrontar el ransomware antes, durante y después de un ataque.

Por supuesto, la mejor manera de combatir el ransomware es detenerlo en el umbral. Para ello hacen falta ciberdefensas a la medida de las amenazas actuales.

Una ciberseguridad robusta es una ciberseguridad centrada en las personas que hace a los usuarios más resilientes mediante cursos de formación para concienciar en materia de seguridad basados en técnicas de ataque reales que identifica y elimina el ransomware dirigido a las personas de su organización, y que contiene las amenazas y le ayuda a reaccionar con rapidez y eficacia cuando algo va mal.

Para obtener más información sobre cómo puede detener los ataques de ransomware, visite **www.proofpoint.com/es**.

MÁS INFORMACIÓN

Para obtener más información, visite **proofpoint.com/es**.

ACERCA DE PROOFPOINT

Proofpoint, Inc. es una compañía líder en ciberseguridad y cumplimiento de normativas que protege el activo más importante y de mayor riesgo para las organizaciones: las personas. Gracias a una suite integrada de soluciones basadas en cloud, Proofpoint ayuda a empresas de todo el mundo a detener las amenazas dirigidas, a salvaguardar sus datos y a hacer a los usuarios más resilientes frente a ciberataques. Compañías líderes de todos los tamaños, entre las que se encuentran más de la mitad del Fortune 1000, confían en las soluciones de Proofpoint para su seguridad centrada en personas y su cumplimiento regulatorio, mitigando los riesgos más críticos en sus sistemas de correo electrónico, cloud, redes sociales y web. Encontrará más información en **www.proofpoint.com/es**.

proofpoint.

0501-006-01-01 11/21