EBOOK

Ransomware

cómo entender, prevenir y responder a una de las amenazas digitales más graves para la seguridad de su empresa

Sumário

Resumen Ejecutivo

Diversos relevamientos señalan al ransomware como una de las amenazas más graves o preocupantes. Un ejemplo de esto consta en el informe anual de 2021 del Centro de Ciberseguridad Nacional del Reino Unido (NSCS), que reconoció al ransomware como la mayor amenaza digital que enfrentó el país, debido, en especial, a los posibles daños en cuanto a la falta de servicios esenciales (electricidad, agua, red cloacal) o infraestructura.

La preocupación es legítima. Habitualmente, el impacto que causa un ataque de ransomware es dramático y visible, con períodos extensos de falta de servicios, suspensión de la actividad comercial e intentos de extorsión, con cifras millonarias.

No obstante, puede ser beneficioso entender el ransomware como una suma de amenazas, ya que, en definitiva, lo que lo hace tan insidioso es el hecho de que prácticamente cualquier descuido puede desencadenar un ataque. Gracias al ecosistema del ciberdelito y a otros softwares maliciosos conocidos hace mucho tiempo, como los que generan redes zombies, una única credencial filtrada, vulnerabilidad o un clic indebido en un link de un e-mail, es suficiente para exponer la red a un ransomware.

Este acceso inicial, gracias a la acción paciente (y especialización) de los delincuentes, será transformado en un incidente cuyo impacto se extenderá a toda la organización. De los servicios externos e internos al factor humano, el ransomware estresa a todas las capas de la infraestructura digital.

El desafío reside, por lo tanto, en priorizar las acciones con mayor potencial de efectividad. Al comprender el fraude, puede mapearse el flujo y las etapas en las cuales puede ser interrumpido, ya sea impidiendo el primer acceso o detectando uno de los demás ataques de los cuales el ransomware depende. Pensar sólo en la etapa más emblemática del ransomware (la criptografía, o el “rescate digital”) no nos ayudará a encontrar la respuesta.

Es por esto que realizaremos un perfil de la evolución del ecosistema del delito hasta nuestros días, mostrando cómo se benefician los operadores de ransomware. En este ecosistema existen las más amplias oportunidades de actuación de inteligencia, monitoreo y prevención.

Hacia el final, presentaremos una guía para responder a un ataque de ransomware, y observaremos cómo la preparación adecuada es la clave para mantener este proceso en orden.

Evolución del ransomware

Cómo llegamos al escenario actual

Directo al Punto — OEl ransomware no es una amenaza aislada. El ecosistema del crimen, que sustenta la operación de fraude de ransomware, depende de varios “servicios”, como por ejemplo, la capacidad de cobro, el lavado de dinero y la ocultación de rastros on-line. Explicamos aquí el modo en que el ransomware evolucionó de una estafa que bloqueaba la pantalla de la computadora y cobraba rescate por medio del SMS a un malware avanzado capaz de derribar la infraestructura digital de una empresa y pedir rescates de millones de dólares en criptomonedas.

El ‘primer’ ransomware

El ransomware no necesita presentación, habida cuenta de las veces en que se lo ha mencionado en los noticieros. Mientras algunas empresas pagan millones de dólares a los delincuentes a fin de poder retomar sus actividades, otras ni siquiera han tenido esta opción y sólo atinaron a declarar la quiebra o cerrar sus puertas. Pero ¿cómo es que esta amenaza ha logrado tanta envergadura en sólo una década de vida?

El primer código malicioso que puede considerarse un “ransomware” surgió en 1989. Creado por el biólogo Dr. Joseph Popp, este malware se distribuyó en disquetes que supuestamente contenían información sobre el SIDA, enfermedad que, una vez catalogada en 1981, ocupaba por aquella época la atención de los médicos. Luego de

instalado, este ransomware invadía el sistema y **pedía un rescate de US$ 189,00.**

Además de cobrar para restituir el sistema (con el mismo tipo de "mensaje de rescate" que existe en el **ransomware moderno**), el malware encriptaba el nombre de los archivos y carpetas y volvía imposible el uso de la computadora, lo que también se asocia a las técnicas más avanzadas que se usan hoy en día, con la **criptografía asimétrica.**

Ese código primitivo se llamó "AIDS Trojan" debido a las etiquetas de los disquetes que se distribuyeron para difundirlo, pero también se conoció como "PC Cyborg", ya que esta era la empresa que recibiría el rescate.

Las autoridades identificaron sin dificultades al autor de esta plaga digital. Sin embargo, Joseph Popp sufría de problemas mentales y la justicia lo declaró inimputable.

Ciberdelito moderno, criptomonedas y OPSEC

Aunque las similitudes sean evidentes, no es totalmente exacto que la explicación para el ransomware moderno se encuentre en programas maliciosos tan antiguos. La amenaza, tal como existe hoy en día, deriva de circunstancias que van **más allá de las capacidades técnicas y de software.**

Para quien asume el desafío de defender una red, conocer las condiciones necesarias de un ataque exitoso y **monitorear la actividad delictiva con el fin de anticiparse a las acciones y preparar respuestas** puede constituir la clave de una actuación asertiva capaz de desmantelar la potencialidad del delincuente para concretar la estafa.

El primer paso es detectar lo que el invasor busca y los medios y herramientas que tiene a su disposición. Desafortunadamente, la estructura delictiva actual, que es responsable por la existencia del ransomware, se construyó a lo largo de décadas de fraudes en internet.

En otras palabras, el ransomware es una amenaza desarrollada en el transcurso de, por lo menos, 15 años de perfeccionamiento de la actividad delictiva en el mundo digital.

Una de las demandas del delincuente profesional es la "OPSEC" (seguridad operativa), con el objetivo de reducir el riesgo de ser apresado y perder así el acceso a las ganancias ilícitas. Cuanto más fácil es recibir dinero ilícito o llevar a cabo delitos "tradicionales", como el lavado de dinero y la falsedad ideológica, más osado se vuelve el delito digital.

La transformación del ransomware en una amenaza personalizada, a través de la cual los delincuentes conocen a su víctima y saben cuánto pueden ganar con ella, se aceleró gracias al surgimiento de una modalidad de pago capaz de manejar transferencias millonarias: las criptomonedas.

El ransomware ya existía antes de las criptomonedas. En los países del ex bloque soviético, los primeros "bloqueadores" de sistemas habitualmente realizaban los cobros a través de SMS Premium: era necesario que la víctima enviara un SMS a un número informado previamente para recibir el código de desbloqueo. El monto del "rescate" aparecía en la cuenta del teléfono.

En otros casos, el cobro se hacía por medio de una plataforma llamada E-Gold, que fue interceptada en 2007

por el Departamento de Justicia de los Estados Unidos. En esa época, los montos exigidos para el “rescate” difícilmente superaban los US$ 300,00. En el caso de los SMSs, el valor, por lo general, era de US$ 10,00.

En otros países de Europa y América, donde el cobro por SMS no se permitía debido a las reglamentaciones en el sector de telecomunicaciones, **el “ransomware” podía ser enviado como un antivirus falso**. Bajo el pretexto de la venta del software, los delincuentes cobraban el rescate con tarjeta de crédito. El costo de estos “programas” era de aproximadamente US$ 50.

Fueron esos antivirus falsos que, en la segunda mitad de la década de 2000, dieron paso a los mensajes que alertaban sobre “problemas” en las computadoras, con técnicas como el cambio del fondo de pantalla, **algo que todavía hoy es utilizado por el ransomware**.

EPÍGRAFE: Fondo de pantalla usado por el ransomware LockBit.

Cuando se comunican con las empresas atacadas para "negociar" el rescate, no es extraño que las bandas de ransomware traten a las víctimas como "clientes" o "pacientes", lo que nos retrotrae a la época en que los delincuentes vendían programas de "seguridad". Algunos virus de rescate emblemáticos, como CryptoLocker y CryptoWall, usaban el mismo lenguaje visual (escudos y candados) que aparecía en los programas de seguridad falsos.

Evidentemente, no todos querían o lograban realizar los cobros por tarjetas de crédito, inclusive porque se comenzó a investigar a los compradores involucrados por el exceso de devoluciones de cargo (chargebacks). Había una "segunda línea" de bloqueadores que realizaba los cobros a través de tarjetas prepagas o tarjetas de regalo.

Un malware conocido de esta familia fue el Reveton. Considerado un "ransomware", no utilizaba criptografía sino que **aplicaba un ataque de tipo extorsión** alegando que la víctima había cometido un delito y debía pagar una multa. Para ello, usaba pantallas personalizadas, tomando el nombre y el distintivo de la autoridad policial del país asociado al sistema.

El cobro se llevaba a cabo a través de servicios que se especializaban en facilitar envíos internacionales, como Ukash, Paysafe y MoneyPak. Los montos eran de aproximadamente US$ 200,00.

Un nombre notorio en el rubro fue Liberty Reserve, fundada en 2001 y extinguida en 2013 por acción del FBI, luego de varias evidencias de que el servicio se utilizaba para realizar transacciones entre delincuentes.

Según el Departamento de Justicia de los Estados Unidos, Liberty Reserve habría sido empleada en un esquema de lavado de dinero en transacciones que ascendían a US$ 250 millones. El fundador del servicio se declaró culpable de las acusaciones y fue sentenciado, en 2016, a 20 años de prisión.

La caída, en 2013, de Liberty Reserve coincidió con el surgimiento del mercado de las criptomonedas. La empresa Mt. Gox todavía estaba en alza, con un repertorio de recursos y funciones que allanaba el camino a las futuras competidoras.

CryptoLocker: el malware que definió una categoría de estafa

En el mismo año 2013, los especialistas en seguridad detectaron el CryptoLocker. Principalmente distribuido por medio de otros códigos maliciosos ya existentes (como la botnet Gameover ZeuS) y plataformas de envío de spam, se cree que facturó cerca de US$ 27 millones, en bitcoins.

Las características y el funcionamiento del CryptoLocker lo pondrían a la altura de los códigos usados en 2022. Empleaba criptografía asimétrica y servidores de control, y fue catalogado como “crypto-ransomware”, para diferenciarlo de otros tipos de extorsión con rescate digital. Así, el éxito del CryptoLocker sirvió para **consolidar esta modalidad de fraude, que hoy conocemos simplemente como “ransomware”.**

Hasta hoy no existen herramientas de decodificación para recuperar archivos encriptados por el CryptoLocker. Quienes no pagaron el rescate y no tenían backup nunca recuperaron los datos perdidos.

Por otro lado, tres aspectos del CryptoLocker lo diferenciaban de las estafas de hoy: el monto del rescate, la forma de distribución y la ausencia de la "doble extorsión". Todos estos elementos están vinculados. Mientras hoy en día a algunas empresas víctimas de ransomware se les solicitan centenas de millares o hasta millones de dólares, el CryptoLocker cobraba cerca de US$ 500,00.

Los montos millonarios exigidos por un ransomware contemporáneo son la consecuencia de su modo de distribución y de la aplicación de la doble extorsión. Los operadores de ransomware dirigen de cerca cada invasión, introduciéndose en la red de la empresa de forma contundente y reduciendo las posibilidades de una recuperación por backup. La doble extorsión, a su vez, se realiza a través del robo de la información antes del ataque de criptografía, de modo que se pueda amenazar a la víctima con la filtración de los datos.

Nada de esto sucedía con el CryptoLocker. El malware era distribuido en masa a través de redes zombies y mediante el uso de los "exploit kits", que se servían de las fallas en los navegadores y plug-ins.

En otras palabras, era común que el usuario se infectara después de navegar en un sitio malicioso. Las visitas a estas páginas dependían de motores de búsqueda, anuncios fraudulentos e invasión a sitios legítimos vulnerables. Era un tipo de diseminación oportunista, sin dirección.

Tal vez el último ransomware emblemático distribuido de esta forma fue el WannaCry, en 2017. Programado para sacar provecho de una vulnerabilidad en Windows de forma automatizada, podía atacar cualquier sistema al que fuera capaz de acceder. De esta manera, era probable que los sistemas de backup salieran ilesos del ataque, facilitando la recuperación.

El WannaCry pedía un rescate de varias centenas de dólares (generalmente entre US$ 300,00 y US$ 600,00). Casi en paralelo, otro ransomware menos mediático, el Locky, empezaba a solicitar cifras de cuatro dígitos.

A partir de ese momento, de 2017 a 2020, sucedieron transformaciones importantes en el mundo del delito de ransomware:

1. 2017: El servicio de bitcoin BTC-e es desmantelado por el Departamento de Justicia de los Estados Unidos. Acusado de lavado de dinero (el monto sería de US$ 4 mil millones), era considerado uno de los preferidos de los operadores de ransomware. Como el principal acusado no pudo ser extraditado a los Estados Unidos debido a una disputa judicial que involucraba a Grecia, Rusia y Francia, el caso todavía no ha sido resuelto.

2. 2018: Surge el ransomware Ryuk, que concentra sus ataques en empresas y organizaciones. Los sistemas individuales, de consumidores y profesionales independientes, quedaban en segundo plano. Las estimaciones indican que, en 2018, hasta el 81% de todos los ataques de ransomware apuntaron a las empresas. Con objetivos más valiosos, los montos exigidos para los rescates explotaron: en 2019, el Ryuk llegó a intentar cobrar US$ 12,5 millones a una víctima.

3. 2019: Expansión de los servicios de “mixing” o “cryptocurrency tumblers”, que mezclan criptomonedas de diversos orígenes para ocultar ganancias ilícitas. Según un informe de BitFury, el volumen de bitcoins transferidos de mercados de las darknets, que era de sólo del 1% al inicio de 2019, subió de forma constante durante el año y alcanzó el 20% en el primer trimestre de 2020.

4. 2020: La estrategia de “doble extorsión” crece casi un 500% y los pagos se exigen en criptomoneda Monero. Comenzamos a observar la consolidación del ransomware también como vehículo de filtración de datos, en el cual la amenaza de exposición de la información corporativa es otra cara de la extorsión llevada adelante en el ataque. Paralelamente, los servicios de mixers se pusieron en la mira de las autoridades y los corredores de criptomoneda tuvieron que adoptar procesos de KYC (know your costumer) más robustos, que llevaron a algunos ransomwares emblemáticos (como REvil) a iniciar cobros en Monero (una moneda más difícil de rastrear), o cobrar hasta un 20% más caro a quienes sólo podían pagar en bitcoins. El resultado: en 2020 se atribuyó al ransomware la suma de US$ 692 millones en transacciones en criptomoneda.

A pesar de la evolución en los cobros de rescates (con cifras mayores y mecanismos más anónimos), el ransomware todavía presentaba una importante

dependencia de otros tipos de malware, como si el ransomware viajase como acompañante de otras infecciones. Sin embargo, cuando este modelo se mostró insuficiente, los operadores del delito apostaron por un modelo más especializado, compartimentando la actividad delictiva para ganar escala.

Línea de tiempo del ransomwaree

1989

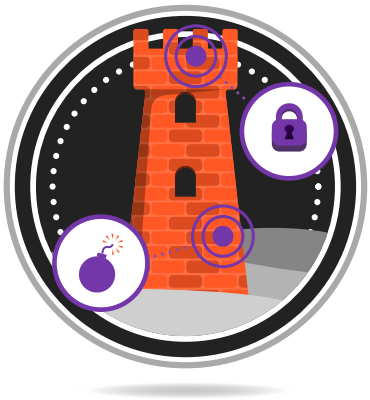
Lanzado el **malware AIDS**, el primer código malicioso que puede considerarse un "ransomware". Fue distribuido en disquetes que supuestamente tenían información sobre el SIDA, de ahí su nombre. Congelaba el sistema y pedía un rescate de US$ 189.

2004

Se detecta por primera vez el virus **GPCode**, que cifraba archivos para cobrar un rescate a través de un servicio de pago ruso.

2009

Se crea el primer bloque de **Bitcoin**, método de pago que sería adoptado para cobrar los rescates del ransomware en los años siguientes.

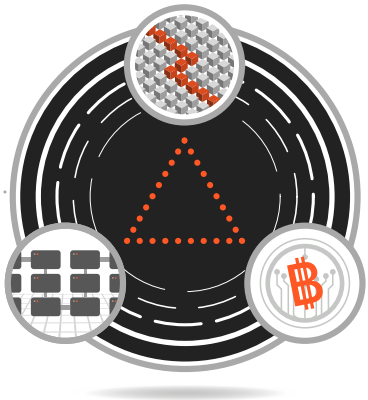


2012

Se crea el malware **Citadel**, un ladrón de credenciales que también instalaba el ransomware Reveton y producía informes de ingresos e instalación para el control de afiliados, consolidando el modelo "malware como servicio", en el que cada fase del ataque es realizada por individuos diferentes.

Primera detección del **CryptoLocker**, que combinaba cifrado asimétrico, servidores de control y opción de pago por Bitcoin, formando los pilares del golpe de ransomware para toda la década.

2013



2015

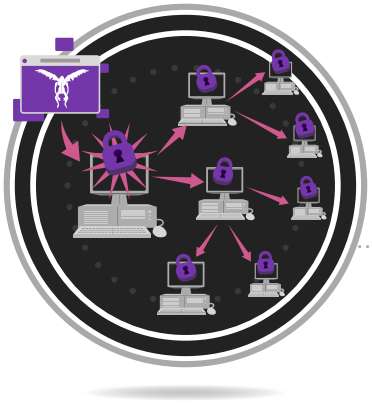
El modelo de **ransomware como servicio** abre las puertas a criminales sin habilidad técnica. El estafador ganaría una comisión por cada víctima que pagara el rescate a partir de la versión del malware generada en un sitio de la Deep Web.

Paralización de servicios y empresas debido al **WannaCry**, el último ransomware notorio que se distribuyó de forma indiscriminada, sin buscar objetivos específicos.

2017

2017 a 2020

grandes transformaciones en el delito de ransomware

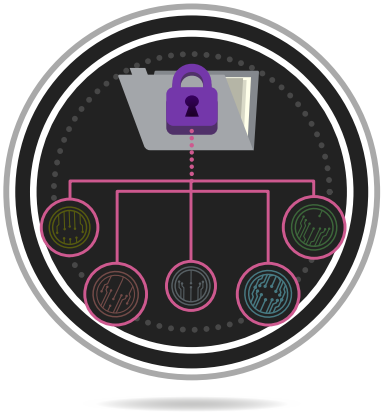


2018

Surge el ransomware **Ryuk,** que concentra los ataques en empresas y organizaciones.

Expansión de los servicios de **cryptocurrency tumblers**, que mezclan criptomonedas de diversas procedencias para ocultar ganancias ilícitas.

2019



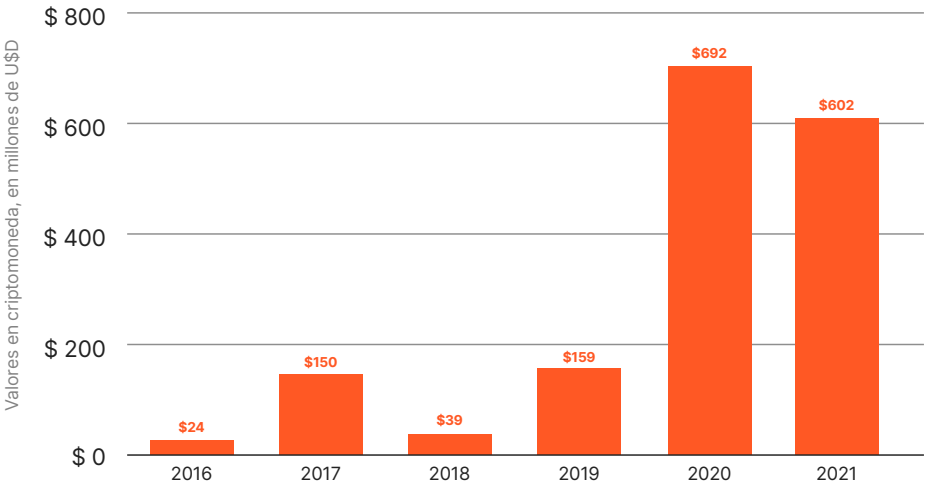
2020

Crece la estrategia de **extorsión doble**, que amenaza a las víctimas con la filtración de datos, y los pagos también se cobran en criptomoneda Monero.

Hoy

El ransomware sigue causando daños, pero la **prevención** a través de actividades de inteligencia y **monitoreo** tiene un potencial de eficacia altamente relevante, así como saber con quién contar en el momento más crítico de la recuperación.

Valores totales en criptomoneda recibidor por direcciones de Ransomware.



Las organizaciones delictivas detrás del ransomware

Así como una línea de producción, los delincuentes se especializaron

Directo al Punto — Las bandas que llevan a cabo estafas de ransomware enfrentan varios desafíos para expandir su escala sin comprometer la efectividad del ataque. Conocer el día a día de la actividad delictiva constituye el primer paso para definir una línea de actuación de los equipos de seguridad, especialmente en monitoreo y threat intelligence, con el objetivo de elaborar medidas preventivas y anticipar acciones futuras. Analizando grupos como Conti y DarkSide, entenderemos mejor el modo en que estos delincuentes se especializan, sus disputas internas y las frágiles relaciones de confianza que se construyen a partir de las ganancias y de la búsqueda de un aumento en el volumen de ataques.

DarkSide: el ransomware que desencadenó una emergencia

En mayo de 2021, Colonial Pipeline, un oleoducto de Estados Unidos, interrumpió la distribución de combustible luego de que su sistema de cobros **fuera derribado por um ataque de ransomware**. El rescate pedido (y pagado) fue de US$ 4,4 millones.

La investigación reveló que el ransomware no había llegado a la red corporativa a través de otro malware o por un phishing dirigido sino por una credencial antigua y expuesta que los delincuentes habían utilizado para iniciar la invasión, la cual proporcionaba el acceso al servicio de VPN de la compañía.

Fue el mismo presidente de la empresa, Joe Blount, que reveló el método usado por los invasores **en su declaración** para un comité del Senado norteamericano. Una cuestión técnica simplemente inadvertida por la alta dirección del oleoducto había causado un perjuicio millonario y el riesgo de falta de combustible en una región abastecida por la empresa.

La declaración del ejecutivo dejó dos impresiones.

1. La alta gestión debía prestar atención a la **amenaza representada por el ransomware.**

2. La **nueva modalidad** de ransomware, de ataques dirigidos y personalizados al entorno de destino, había madurado y podía generar consecuencias concretas inclusive para las personas en su desempeño cotidiano.

El ransomware que infectó a Colonial Pipeline se llamaba DarkSide. La exposición de este caso terminó echando luz sobre las operaciones de esa banda y presionando a las autoridades para que dieran una respuesta. La operación entera se realizó en el mes de mayo, teniendo su desenlace luego de que la infraestructura fuera confiscada por las autoridades y los líderes de DarkSide decidieran alejarse.

Sin embargo, este caso pudo ser un “ataque de un ataque”. El DarkSide funcionaba como “ransomware-as-a-service” (RaaS), un sistema que imita el modelo de “software como servicio” permitiendo que los creadores de un ransomware tomen distancia de la operación diaria y de los ataques a sus objetivos.

Con el RaaS, un ransomware posee diversos “afiliados” que realizan los ataques. Sin embargo, la negociación

de los montos que serán solicitados para el rescate quedan por cuenta del núcleo de la banda. Al “cerrar” sus actividades, DarkSide, en la práctica, podía defraudar a sus “afiliados”.

Cuando una operación delictiva obtiene esa escala y comienza a gestionar personas además de su propia infraestructura tecnológica, con el desafío adicional de que la confianza no es habitual en el mundo del delito, no es extraño que descuidos, infiltraciones y errores lleven a exponer la actividad que se está desarrollando.

Esta información ayuda a construir contramedidas y alertas activas sobre una posible actividad de ransomware en los entornos cubiertos por este monitoreo.

Algunos ejemplos de información que el monitoreo de las acciones delictivas puede ofrecer:

1. Tactics, techniques, and procedures (TTPs): cómo llega el ransomware a la red de destino, qué tipos de credenciales pueden estar siendo usadas (VPN, banco de datos, dominio, proveedores de nube), qué vulnerabilidades recientes exigen más precaución, entre otras.

2. Indicators of compromise (IoCs): archivos, direcciones de IP y comportamientos de sistema que pueden indicar la presencia de un ransomware antes de su activación.

3. Targets (objetivos): empresas y sectores que pueden estar en la mira de los delincuentes. Comunicados de grupos como LAPSUS (que no es estrictamente una banda de ransomware, aunque sus ataques sean similares) llegaron a nombrar empresas específicas que estaban en la mira del grupo y fueron interceptados por Axur.

4. Filtraciones y credenciales: para garantizar la máxima retribución por sus esfuerzos, los delincuentes anuncian los datos que tienen en venta, ofreciendo, inclusive, fragmentos de muestra. Especialmente cuando se trata de credenciales, estos datos funcionan como un indicio de vulnerabilidad o pronóstico de una futura violación de intereses.

5. Datos corporativos: además de las credenciales, el monitoreo de los delincuentes puede detectar la exposición indebida de otros datos de carácter corporativo (financieros o contables, datos personales de empleados y clientes, proyectos con socios etc.). Esta exposición indica la existencia de riesgos jurídicos y de reputación, y también puede servir para ayudar a rastrear un acceso ilegal ocurrido a partir de la naturaleza de los datos expuestos (por ejemplo, con una pericia en el sistema donde se almacena la información).

Luego de “cerrar” su actividad, DarkSide resurgió como un ransomware llamado BlackMatter. El establecimiento del vínculo entre familias aparentemente diferentes de ransomware permite prever ciertos aspectos del comportamiento del invasor, lo cual también ayuda en la respuesta a los incidentes.

Por qué el ransomware tiene empleados y proveedores

Un ataque de ransomware exitoso depende de una compleja cadena de eventos y herramientas.

Una filtración de las conversaciones de la banda de ransomware Conti, que sucedió en febrero de 2022, fue una de las fuentes de información más sólidas e interesantes sobre la actividad diaria de un ransomware. Los chats habrían sido divulgados por un investigador de seguridad ucraniano a modo de represalia contra el grupo luego de que este se manifestara a favor de Rusia en el conflicto militar con Ucrania.

A partir de los diálogos se pudo comprobar casi en su totalidad lo que se sospechaba sobre el cotidiano de una operación de ransomware, pero también se conoció que los líderes de las bandas frecuentemente pagan salarios a sus "empleados" (en el caso de Conti, eran al menos 100) y que existe una especie de "departamento de RRHH" para reclutar nuevos miembros y reemplazar a quien no cumple con el desempeño adecuado.

A pesar de ello, la desconfianza es una constante en este medio. Como sucedió en el caso de DarkSide, en el que los líderes podrían haber cometido una estafa a sus afiliados, los líderes de las bandas de ransomware deben enfrentar el temor de robos por parte de sus socios y colaboradores.

El modelo de afiliados y de "delito como servicio" empezó a crecer en la década de 2000, cuando los delincuentes vendían el acceso a los códigos maliciosos y a los

“Exploits Kits” (EKs), que son códigos preparados para aprovechar las vulnerabilidades en los navegadores, que se venden por suscripción o comisión y se controlan mediante estadísticas y métricas de éxito.

Los EKs y las redes de spam (que también comercializan su capacidad de envío de mensajes como servicio a otros delincuentes) formaron la base de las primeras infecciones de ransomware, además de distribuir ladrones de contraseñas y tarjetas, mineros de criptomonedas y otros fraudes.

La estafa del falso antivirus, que, con el pretexto de vender software, propiciaba fraudes, ya usaba el modelo de afiliados comisionados, una práctica legítima que existe en el mercado. De hecho, “culpar a los afiliados” por toda y cualquier práctica dudosa era una forma de blindaje para los delincuentes, que por aquella época debían evitar las represalias de Bancos y tarjetas de crédito.

Con las criptomonedas, este pretexto perdió utilidad. Sin embargo, el esquema de afiliados ayuda a garantizar una motivación clara y sostener la especialización de cada fase de la actividad delictiva.

Las especialidades del delito

El modelo “ransomware-as-a-service”, que aplica el método al ransomware, ya se diagramaba en 2012. En ese año, un malware llamado Winlocker, o “ Gimemo”, propuso un programa de afiliados con un panel de control que contabilizaba los rescates pagados y el porcentaje de comisión que recibía el afiliado.

El afiliado del ransomware sería el único responsable por infectar las computadoras. Por lo tanto, había dos figuras: el creador del ransomware, responsable de programar el software y mantener la infraestructura básica de control de la plaga para contabilizar estadísticas, y el propagador, responsable de que el malware llegara hasta la víctima.

El escenario en 2022 es más complejo. Tanto la tarea del creador del ransomware como la del propagador se dividieron en partes menores, cada una de ellas realizada por individuos dedicados a esa tarea.

Los cargos de empleados y afiliados del ransomware

También existen los auxiliares responsables por el estudio de los objetivos (estimando la facturación y la capacidad de pago) y la negociación con las víctimas.

Aun con toda esta serie de cargos y especializaciones, la actividad de un ransomware tiene otras demandas que deben ser atendidas por los proveedores.

En cualquier negocio, la ganancia de escala tiene sus pros y sus contras. En el caso del ransomware, por más que a partir de ella se aumenten las ganancias ilícitas mediante la sofisticación del fraude y la especialización de los involucrados, existe una demanda considerable por el acceso a nuevos objetivos.

Ciertamente algunos grupos son más organizados y especializados que otros. Asimismo, todos los delincuentes tienen a su disposición el mismo ecosistema, del cual pueden obtener información o contratar proveedores. Del mismo modo en que un programador de ransomware puede contratar un delincuente especializado en spam, otro puede comprar un malware preparado para ser propagado por las redes sociales o ingeniería social y ser cómplice del delito sin poseer ningún conocimiento técnico específico.

Para que todo esto sea posible, los delincuentes crearon espacios de negociación relativamente abiertos, habilitando la entrada de nuevos delincuentes capaces de sostener todo el esquema, independientemente de la actividad que cada uno sepa realizar.

Para quien cuenta con un monitoreo especializado, esas redes y espacios se vuelven una gran fuente de datos. Por su intermedio es posible prever o detectar ataques que aún están por suceder (por ejemplo, a través de la detección de una credencial filtrada).

Como el delincuente que roba la credencial no siempre es el mismo que la utiliza, interceptar estas tratativas puede resultar decisivo para bloquear un ataque antes de que suceda.

La prevención de un ataque de ransomware por medio de actividades de inteligencia y monitoreo tiene un potencial de eficacia altamente relevante en este escenario.

La doble extorsión provoca que las medidas de recuperación y restauración (como el backup) sean insuficientes para aliviar la presión de pago del rescate, pues la empresa todavía puede estar expuesta a una filtración de datos. Las filtraciones causan daños a la marca y a la reputación.

Hay registro de casos en que los estafadores usaron la base de clientes o de empleados de la víctima para avisarles del riesgo de exposición de su información personal si la empresa se negaba a pagar.

Esta es la gran apuesta del ransomware moderno: por más que una organización haya cumplido con los backups y tenga un plan de recuperación robusto, prácticamente es imposible evitar los daños que causa la exposición de los datos. Y peor aún: no existen garantías de que los delincuentes realmente los borren.

Os fornecedores do ransomware

SPAMMER

Delincuente especializado en comprar o crear una infraestructura capaz de enviar e-mails maliciosos, a demanda o de forma masiva. El criterio de éxito para un proveedor de este tipo es la capacidad de hacer llegar el correo electrónico a la bandeja de entrada eludiendo los mecanismos antispam.

INSIDER

Un empleado de la empresa atacada o un proveedor de servicios que ha sido contratado para proporcionar acceso a los operadores del ransomware.

ACCESS BROKER

Intermediario capaz de negociar un acceso (previamente obtenido) a una red corporativa. Puede especializarse en el uso de credential stealers o en la adquisición de credenciales obtenidas por otros delincuentes.

Prevención

Poniendo en práctica lo que sabemos sobre el adversario

Directo al Punto — Conociendo el ecosistema del delito y sus debilidades podemos actuar incisiva y abarcativamente en la recolección y procesamiento de los datos que los delincuentes exponen, haciendo un mapeo de los riesgos de la empresa y eliminando los puntos de ingreso que podrían utilizarse en los ataques. Como el ransomware depende de accesos externos, no siempre es necesario que estas medidas impacten en el equipo de seguridad, sino que este puede continuar centrándose en los activos internos.

Como la doble extorsión cambió el peso de la prevención

Si hasta 2020 una buena estrategia de recuperación era suficiente para mitigar el impacto del ransomware, la práctica de la doble extorsión (rescate de los datos con amenaza de filtración) estableció que la restauración de los sistemas no evitará otros perjuicios derivados del ataque, como los daños a la marca y las posibles consecuencias jurídicas previstas en legislaciones como la Ley General de Protección de Datos (LGPD, por sus siglas y denominación en Brasil).

Por esto, las medidas capaces de prevenir o interrumpir un ataque en marcha agregan mucho valor a la defensa contra la amenaza del ransomware. Al limitar y cortar el acceso del delincuente a la red antes de que se produzca el robo de los datos, la empresa protege sus secretos comerciales y su reputación, evitando a la vez tomar

decisiones sobre el pago de un rescate millonario.

La prevención de los ataques cibernéticos exige una buena madurez en seguridad de la información, con la aplicación de patches, políticas de seguridad y procesos adecuados. Asimismo, estos requisitos básicos no siempre resultan suficientes. Por otro lado, garantizar que no existan errores o no conformidades es un desafío de todos los días.

Por lo general, el ransomware se dirige a cada empresa en forma personalizada, con la intervención de un operador humano secundado por una banda interesada en derrotar mecanismos de seguridad tradicionales (como el antivirus). Por otro lado, los recursos de seguridad internos pueden ser escasos, inclusive por la brecha de profesionales que existe en el mercado de la seguridad.

Por esta razón, es necesario contar con equipos profesionales especializados en mitigar los riesgos, muchos de los cuales se visibilizan en el mundo externo gracias a las dificultades que los operadores de ransomware crearon para sí mismos al organizar operaciones delictivas sofisticadas en gran escala.

Filtración de credenciales: el presagio del ransomware

Como el ransomware contemporáneo depende de un verdadero ecosistema de ciberdelito, son varias las oportunidades para detectar la actividad sospechosa a través del monitoreo de ese ecosistema. Así, se recaba información que puede indicar el riesgo en que se encuentra una organización o, en el peor de los casos, si ya está en la mira de los delincuentes.

Con esta visión privilegiada de la actividad delictiva, una empresa puede actuar de forma proactiva para eliminar vulnerabilidades o canales de acceso que hayan sido comprometidos.

Los equipos de CTI (Cyber Threat Intelligence) y ART (Axur Research Team) de Axur lograron el acceso a los archivos de “log” de casi una decena de malwares dedicados al robo de credenciales (los credential stealers). Aunque no participen de la operación de un ransomware en sentido estricto, las credenciales obtenidas por el malware se reúnen en compilaciones (los ya mencionados “logs”) para ser vendidas en el submundo del delito. A partir de esta comercialización, se establece la conexión con todo tipo de actividad delictiva.

Los logs pueden ser vendidos a los access brokers o directamente a las bandas de ransomware, y estas, luego, encontrarán víctimas de su interés o credenciales de sistemas (infraestructuras de nube, dashboards, bancos de datos) que ya conocen y que saben que pueden asegurar un buen punto de acceso a la red de una empresa.

El trabajo de monitoreo de Axur ya identificó más de 170 millones de credenciales robadas por estos códigos maliciosos. Entre ellas, se pudieron vincular 18,2 millones a Brasil. Además, varias de estas contraseñas proporcionan acceso a servicios críticos o que claramente se utilizan como puerta de entrada para el ransomware.

Uno de los credential stealers más destacados que fue monitoreado por Axur es el RedLine. El análisis de los logs que Axur realizó tuvo como resultado la identificación de decenas de millones de credenciales robadas y, de ellas,

305,6 mil pudieron atribuirse directamente a empresas brasileras. Todo esto tuvo como origen la actividad de un único malware.

Este tipo de trabajo permite interrumpir una cadena de eventos que podría llevar a un ataque de ransomware. Cuando se llama la atención a la organización sobre contraseñas robadas o canales vulnerables a este tipo de acceso, esta tiene la oportunidad de reaccionar, y lo hace a través de la cancelación de la credencial, con lo que se interrumpe la escalada de las acciones maliciosas.

En el caso de Colonial Pipeline, por ejemplo, el acceso inicial se dio por medio de una credencial de VPN. De haber habido un aviso previo sobre la filtración de esta credencial, el incidente habría tenido otro desenlace.
Y los riesgos no existen sólo en la teoría: de todas las credenciales expuestas en los logs de los credential stealers monitoreados por Axur, se pudo atribuir 374 mil a los sistemas de VPN.

Un credential stealer se puede distribuir por e-mail (con ingeniería social y phishing), pero también es común su propagación en redes sociales. La capacidad de estos malwares para robar sesiones de login almacenadas en el navegador (muchas veces derrotando a la autenticación multifactor) los vuelve interesantes si la intención es robar cuentas de creadores de contenido, inclusive de los que utilizan todos los recursos de seguridad ofrecidos por los grandes prestadores de servicios de internet.

Un empleado puede poner en riesgo a su empresa aunque el ladrón de credenciales esté instalado a partir de un link de las redes sociales en su computadora personal. Todas las contraseñas robadas, inclusive las que no

poseen vínculo aparente con los sistemas corporativos, pueden usarse en los ataques de credential stuffing, en los cuales se llevan a cabo intentos de acceso a un objetivo a partir del uso de credenciales adquiridas para otro sistema.

Dicho de otro modo, una contraseña robada para cualquier servicio se puede revalidar y comprobar en un sistema corporativo, más valioso para las bandas de ransomware. Por medio de los “access brokers” (intermediarios que comercializan canales de acceso), la credencial llegará a los operadores más aptos, habilitando así el inicio del ataque de ransomware.

Las credenciales también se pueden exponer a partir del acceso no autorizado a los bancos de datos, ya sea de empresas o proveedores. Para facilitar la identificación precoz de una filtración y bloquear el ataque mediante la cancelación de la credencial o la baja en el acceso de los proveedores potencialmente comprometidos, se implementan los tokens de rastreo.

El trabajo de monitoreo se puede integrar a las operaciones de seguridad de la empresa. Contando con un mecanismo para detectar las violaciones a la política de seguridad y otras reglas de conformidad, inclusive de empleados que repiten contraseñas o de proveedores, la organización optimiza su protección contra ransomware a la vez que eleva su nivel de madurez en la seguridad de toda la cadena de operaciones.

Monitoreo de la superficie externa de ataque

Antes de obtener credenciales o datos corporativos, los delincuentes pueden realizar escaneos de los sistemas de la empresa que están expuestos en internet (servidores web, e-mails, VPN, canales de API, entre otros). Si encuentran en estos sistemas una vulnerabilidad, error de configuración o dato expuesto, es posible que también encuentren el camino para dar sus primeros pasos dentro del objetivo elegido.

En el complejo ecosistema digital corporativo, no resulta extraño que dashboards, servicios web, almacenamiento en la nube y otros recursos se adopten en forma “ad-hoc”, es decir, con el fin de atender a una necesidad específica o momentánea sin que tengan una conexión definida con los demás procesos y sistemas. Estos recursos no siempre cuentan con una documentación clara y, en ocasiones, el departamento de IT no está al tanto de su existencia, lo que genera el fenómeno conocido como “shadow IT”.

Por esta razón, no es suficiente que la empresa preste atención a la superficie de ataque interna y a los recursos administrados por el departamento de IT.

En la mayoría de los casos, el invasor está del lado de afuera y su primer contacto con el entorno de la empresa sucede justamente por medio de esta superficie externa, muchas veces a través de recursos que no son los oficialmente administrados por los equipos de IT.

La síntesis de este escenario es que, en muchos casos el invasor termina por conocer mejor esta superficie externa que la propia empresa, en especial si no existió un esfuerzo coordinado para monitorearla, mapearla y

protegerla. La aplicación de un patch de seguridad se hace imposible cuando el propio equipo de IT no conoce el uso del sistema.

Monitorear, mapear y buscar la conformidad en todos los sistemas externos es fundamental para evitar que los invasores encuentren “atajos” que los conduzcan dentro del entorno corporativo.

Inteligencia en ciberseguridad

Hacer un seguimiento de los movimientos de las bandas de ransomware permite mapear las vulnerabilidades y técnicas utilizadas. En la práctica, existe la posibilidad de priorizar las acciones que serán más eficaces para proteger la organización.

- Dar prioridad a la aplicación de patches de vulnerabilidades que usan las bandas de ransomware
- Reforzar la seguridad de los canales de servicios (como un cloud provider específico) que estén relacionados con ataques recientes
- Perfeccionar los sistemas de seguridad preexistentes (como antivirus y firewalls) con información relevante de IoCs, como direcciones IP y archivos maliciosos
- Conocer los riesgos específicos para cada sector de actuación
- Tomar medidas contra el reclutamiento de insiders que colaboren con los delincuentes

- Implementar sistemas de gestión de contraseñas (cajas fuertes) y autenticación multifactor (MFA) para reforzar la seguridad de las credenciales y de los canales de acceso. Estas medidas pueden evitar la exposición de una credencial o reducir la utilidad de una credencial robada.

Cómo el monitoreo de filtraciones rompe la cadena del ransomware desde el primer eslabón

1. Los operadores de ransomware adquieren las credenciales y los medios de acceso a los sistemas corporativos a otros delincuentes especializados en el acceso inicial o en el robo de logins y contraseñas (estos delincuentes suelen ser llamados “Access Brokers”)

2. A partir del monitoreo del flujo de esas transacciones y ofertas se puede identificar quién más está en riesgo y cómo los invasores logran el acceso a la red corporativa

3. Si se detecta la filtración de una credencial, la organización puede bloquearla

4. El operador de ransomware no obtendrá el acceso inicial a la organización

5. Sin este acceso inicial, el ataque se obstaculiza y no podrá continuar.

Recuperación y respuesta

Cómo reaccionar a un ataque de ransomware

Directo al Punto — Como la empresa muchas veces depende de su infraestructura tecnológica, un ataque de ransomware puede comprometer todo el negocio. La suspensión de las actividades exige una postura proactiva, que muestre la solidez esperada por los inversores, consumidores y otros stakeholders. Esto exige planificación, canales de comunicación y un buen checklist capaz de conducir la acción de los equipos que deben actuar en el momento más crítico (como es el caso del checklist de la CISA, una agencia del gobierno norteamericano, que citamos como referencia).

La visión ejecutiva de la respuesta al ransomware

En una estafa de doble extorsión (criptografía de archivos acompañada de amenazas de filtración de datos), común en los ataques de ransomware que están en evidencia, la organización enfrenta dos desafíos principales:

1. Restaurar la infraestructura de IT para retomar las operaciones y minimizar el daño derivado de la interrupción generada por la criptografía de los archivos

2. Proteger la reputación y la marca de la empresa de cara a los consumidores, empleados y demás stakeholders

Aunque la protección de la marca no sea una preocupación directa del equipo que actuará en la recuperación del sistema, es importante definir un canal de comunicación adecuado para los equipos encargados de esta responsabilidad.

Los equipos de IT también pueden dar prioridad a manifestaciones concretas que muestren la preocupación por los consumidores, como proteger las credenciales que hayan caído en manos de los delincuentes. La organización puede llevar a cabo esta acción invalidando las contraseñas anteriores y exigiendo el cambio en el próximo login, sin alarmar a los consumidores con un cambio obligatorio de contraseñas.

No obstante, es importante destacar que la legislación prevé responsabilidades específicas para las organizaciones. En Brasil, la Ley General de Protección de Datos (LGPD) obliga a las empresas a comunicar las filtraciones de datos personales a sus respectivos titulares en determinadas situaciones. Otras reglamentaciones similares también existen en varios estados norteamericanos y en Europa (el GDPR).

La planificación es fundamental

La respuesta a un incidente de ransomware será más eficaz si existe anteriormente una serie de preparativos.

Entrenar al equipo de IT para dar una respuesta inicial a los incidentes de seguridad. Es común que, ante las dificultades habituales, los administradores de redes y los analistas de IT tomen actitudes como reiniciar o apagar el sistema. Esto elimina las evidencias que en el futuro ayudarían a dilucidar el incidente. Los administradores y analistas, en la mayoría de los casos, serán los que

tengan el primer contacto con el síntoma provocado por la invasión, y una buena respuesta inicial puede facilitar muchas de las etapas posteriores.

Hacer el testeo de los backups y planear una recuperación. El backup está en el centro de las preocupaciones que derivan del ransomware. Sin embargo, no basta realizar un backup. Es necesario que los archivos estén protegidos y, preferentemente, desconectados (offline). Para los backups en la nube, se debe tener en cuenta el tiempo de restauración, que dependerá de la velocidad de la red y de otras limitaciones. También hay que considerar la dependencia del backup hacia un sistema conectado a la red y vulnerable al ransomware, lo cual dificultará el acceso a la información o, en el peor de los casos, permitirá que el ransomware también cifre el backup.

Determinar los canales de contacto para emergencias. Durante un incidente de ransomware, los canales de contacto de la empresa no serán totalmente confiables o no estarán plenamente disponibles. Es recomendable estar preparados para armar una sala de guerra y establecer contacto con consultores de seguridad, stakeholders y gerencias a través de canales que no dependan directamente de la infraestructura corporativa.

Elaborar un plan de recuperación y de Gestión de Continuidad del Negocio (GCN) y un Business Impact Analysis (BIA). Los planes de recuperación de desastre y GCN mapean los riesgos y la interdependencia de los procesos del negocio, facilitando la priorización de sistemas para su recuperación. Si no se cuenta con esto, un sistema considerado crítico en un análisis rápido

realizado durante el incidente puede ser restaurado y aun así continuar inoperante por alguna dependencia desconocida de otro sistema que no está en la fila de recuperación.

El Business Impact Analysis (BIA), por su lado, evalúa el impacto de la interrupción de los servicios para esbozar los requisitos operativos del negocio y recursos asociados. A partir de esto, colabora con el diseño de los modelos que debe alcanzar la recuperación y las estimaciones de los plazos en que esta puede ocurrir.

Cuanto menos preparada está la organización al depararse con un incidente de ransomware, más extenso tiende a ser el trabajo del equipo de respuesta, y así se prolonga el período en que el sistema permanece fuera de servicio, con las consecuentes pérdidas que esto ocasiona.

En contraposición, cuanto más rápida sea la respuesta y el retorno a la regularidad, menor tiende a ser el daño que sufre la imagen de la empresa, especialmente si se demuestra que no hubo pago de rescate.

Checklist: La respuesta a un incidente de ransomware

Una referencia recomendable para elaborar una estrategia de respuesta a un ataque de ransomware es la Ransomware Guide (Guía de Ransomware) elaborada por la CISA, agencia norteamericana encargada de la seguridad cibernética y de infraestructura.

El checklist cuenta con 19 ítems en 3 grandes etapas de respuesta. A continuación detallamos los 19 ítems con algunos comentarios adaptados:

Etapa 1: Detección y Análisis

1. Determinar los sistemas impactados y aislarlos inmediatamente

- Si hay posibilidad de que varias subnets hayan sido impactadas, desconectar todas del switch. Puede no ser viable desconectarlas individualmente durante el incidente.

- Si no es posible desconectar la red como un todo, desconectar los sistemas individuales desenchufando cables o retirándolos del Wi-Fi.

- Los sistemas también se pueden desconectar o aislar por medio de la segmentación en VLANs. En ciertos entornos o servicios (como la nube pública), esta puede ser la opción más viable.

- Los responsables del ataque pueden intentar monitorear la comunicación interna de la empresa. Se recomienda utilizar métodos alternativos de comunicación (como llamadas telefónicas) y continuar en forma coordinada para evitar el movimiento lateral de los delincuentes o el agravamiento del ataque.

2. Apagar los sistemas sólo en caso de que no sea posible desconectarlos de la red

- Los sistemas sólo deben apagarse en último caso, a fin de no eliminar las evidencias volátiles (como la memoria del sistema) y dificultar, así, la pericia.

3. Seleccionar los sistemas que deben ser restaurados y recuperados

- Identificar y priorizar los sistemas mapeando la naturaleza de los datos almacenados en cada uno y la función que desempeñan (seguridad, salud, generación de ingresos).

Etapa Intermedia: Comunicación, Documentación y Gestión

Aunque esta etapa no esté explicitada en la guía de la CISA, es en este momento cuando debe ser compilada que toda la información mapeada en la fase inicial. También es en este momento que se inicia un flujo de comunicación con gerencias y stakeholders, lo cual se deberá mantener durante todo el proceso de respuesta al incidente para resguardar de daños a la marca.

4. Reunirse con el equipo para desarrollar y documentar la comprensión inicial de lo ocurrido a partir del análisis inicial.

5. A partir de la información de contacto de autoridades y prestadores de servicios de la organización, dialogar con los equipos internos y externos y stakeholders, con el conocimiento de lo que ellos pueden aportar para ayudar a mitigar, responder y recuperar a la organización del incidente.

- Compartir la información disponible para que la ayuda sea sustancial. Mantener informados a gerentes y alta gestión sobre la marcha de los acontecimientos.

Etapa 2: Contención y erradicación

6. Guardar una imagen del sistema y copia de la memoria de una muestra de los dispositivos afectados (estaciones de trabajo y servidores, por ejemplo). Reunir logs relevantes y copias de archivos de malware precursores del ransomware y cualquier otro dato observable que pueda considerarse un IoC (direcciones IP de servidores de comando y control, entradas de registro sospechosas, entre otros archivos).

- Prestar atención a la preservación de la información altamente volátil, como logs y datos de memoria de sistema, para evitar pérdidas o modificaciones.

7. Consultar a las autoridades policiales sobre la posible existencia de herramientas de descifrado de las cuales se pueda disponer.

- Los especialistas de Axur están capacitados para ayudar a encontrar una herramienta de descifrado. Aun así, en la mayoría de los casos el descifrado no será posible.

8. Investigar fuentes confiables para obtener recomendaciones sobre la variante específica de ransomware y seguir los pasos indicados para detectar y aislar los sistemas o redes impactados.

9. Identificar credenciales y sistemas involucrados en la invasión inicial. La credencial puede ser una cuenta de e-mail.

10. Basándose en los datos de la invasión determinados en los pasos anteriores, aislar cualquier sistema asociado que se pueda utilizar para mantener un acceso no autorizado. Frecuentemente, las invasiones se acompañan con robos en masa de credenciales.

- Proteger la red y otras fuentes de información de nuevos accesos no autorizados podrá exigir desactivar servicios de VPN y de acceso remoto, servicios de login único (SSO) y otros activos de acceso público o de nube.

11. Acción adicional sugerida: pasos para identificar la criptografía de datos en servidores.

- Un ransomware instalado en el servidor puede cifrar los datos que se alojan en él. Pero también hay casos en que la criptografía se realiza a partir de un endpoint autorizado, sin que esto implique una infección del propio servidor.

- Por medio de las sesiones de acceso a carpetas compartidas abiertas, la información de propietario de archivos y los historiales de login en servicios de RDP, se puede descubrir si los datos almacenados en servidores están siendo encriptados a partir de un ransomware que se instaló en una estación de trabajo.

- El log de seguridad de Windows, logs de evento del servicio SMB y herramientas de análisis de tráfico (como Wireshark) pueden ayudar también a determinar la fuente del acceso indebido.

12. Examinar los sistemas existentes para detectar y prevenir ataques a la organización (antivirus, respuesta en endpoints, sistemas IDS e IPS etc.) y los logs. Esto puede revelar evidencia adicional sobre los sistemas o de malwares involucrados en las etapas iniciales del ataque.

- Buscar evidencia del malware de tipo “Dropper”, que actúa como precursor del ransomware. Como explicamos en la organización del ciberdelito, los operadores de ransomware frecuentemente compran el acceso a las redes corporativas, mientras los “Access

Brokers” se especializan en el acceso inicial con malwares de acceso remoto o de robo de credenciales.

13. Llevar adelante un extenso análisis para identificar mecanismos de persistencia de afuera hacia adentro y viceversa.

- “De afuera hacia adentro”: credenciales robadas o creadas por los propios invasores, vulnerabilidades, sistemas de perímetro infectados com malware de acceso remoto.

- “De adentro hacia afuera”: herramientas de acceso remoto instaladas en sistemas internos, que van desde Cobalt Strike, una suite profesional para este tipo de acciones, hasta herramientas típicas de soporte remoto, como AnyDesk.

14. Restaurar sistemas priorizando los servicios críticos (como los de salud y seguridad o generación de ingresos), y utilizando, preferentemente, imágenes preconfiguradas.

- Comprobar que se apliquen los patches apropiados y que esté presente el sistema de seguridad adecuado (antivirus o XDR).

15. Luego de que el entorno haya sido totalmente limpiado y restaurado (inclusive las credenciales impactadas y la remoción o erradicación de mecanismos de persistencia maliciosos), realizar una redefinición de contraseñas para todos los sistemas afectados y llevar a cabo el tratamiento de vulnerabilidades y brechas de seguridad o de visibilidad. Esto puede ser hecho mediante la aplicación de patches, la actualización de la seguridad y tomando otras precauciones de seguridad que todavía no hayan sido implementadas.

16. A partir de un criterio establecido, que puede incluir los pasos detallados antes o la búsqueda de asistencia externa, la autoridad de IT o de seguridad de IT declara la finalización del incidente de ransomware.

Etapa 3: Recuperación y actividad post-incidente

17. Reconectar los sistemas y restaurar datos a partir de backups offline y encriptados, priorizando los servicios críticos.

- Recuerde que: pagar el rescate no es garantía de que sus datos serán restituidos.

18. Documentar las lecciones aprendidas con el incidente y las actividades de respuesta para llevar a cabo actualizaciones y refinar las políticas de la organización, planes y procedimientos, y conducir ejercicios futuros a su respecto.

19. Considerar compartir las lecciones aprendidas e indicators of compromise con autoridades u organizaciones relevantes del sector para beneficiar a la comunidad.

Axur dispone de especialistas en el proceso de respuesta a incidentes que pueden integrar su sala de guerra (war room) y proveer una orientación efectiva de acuerdo con el ransomware involucrado y las especificidades de su negocio.

En cualquier incidente, como la propia guía de la CISA sugiere en el caso del ransomware, es importante saber con quién contamos para apoyar a la empresa.

Experiencias digitales más seguras

Protegemos la presencia digital de miles de empresas en todo el mundo

Agende una demo

Sobre Axur

Axur posibilita la escalabilidad y automatización del tratamiento de amenazas cibernéticas para apoyar a los equipos de seguridad de la información y proporcionar experiencias digitales más seguras. Nuestra plataforma de Threat Intelligence posee el tiempo de reacción más rápido del mercado, solicitando takedowns automáticos, 24x7.

Esto es posible porque la Plataforma Axur actúa en cuatro capas: la detección, las tecnologías de inspección, la automatización y la remoción, que disminuyen sustancialmente el promedio de tiempo de contención (MTTC) de los equipos de seguridad. Además, nuestros especialistas en Inteligencia Cibernética extienden la investigación tanto a la Surface como a la Deep & Dark Web, lo que hace de Axur la empresa líder en Cyber Threat Intelligence de Latinoamérica.

Contacto para prensa:
press@axur.com

Direcciones

EEUU
601 Brickell Key Drive, Suite 901
Miami, FL 33131

Singapur
109 North Bridge Road
Cityhall District, 179097

Brasil
Rua Mostardeiro, 322 15o andar
Porto Alegre, RS 90430000

axurbr Axur AxurBrasil AxurBrasil AxurBrasil Axur