Ransomware en evolución

Cómo la amenaza dejó de limitarse al cifrado de datos, incorporó la extorsión basada en filtraciones, los ataques a la cadena de suministro y un ecosistema criminal cada vez más sofisticado.

AXUR

Resumen ejecutivo

A estas alturas, el ransomware es una amenaza que no necesita presentación. Ha llenado titulares en los medios, mantiene ocupadas a las fuerzas policiales e incluso preocupa a políticos y analistas de seguridad nacional que temen que un ataque pueda paralizar sistemas responsables de servicios críticos como energía y agua.

En la mayoría de las empresas, los analistas de ciberseguridad comparten preocupaciones similares. El ransomware puede detener por completo la operación, incluyendo los sistemas más críticos, dejando a la compañía a merced de los criminales y poniendo en riesgo la continuidad del negocio.

Aun así, cada organización es responsable de definir su propia estrategia de defensa y prevención contra el ransomware. Lo que funciona para una no siempre servirá para otra, considerando la diversidad de software y procesos internos.

Por esta razón, no siempre resulta sencillo convertir esas preocupaciones en un plan de acción efectivo.

Pensando en ello, hemos creado esta guía general y completa sobre la amenaza del ransomware, que reúne información actualizada sobre cómo operan estos delincuentes y datos históricos que ayudan a entender cómo se formó el escenario actual.

Desde la descripción de los principales grupos de ransomware hasta las recomendaciones para prevención y recuperación, hemos reunido lo que consideramos esencial para que cada organización diseñe su estrategia según sus prioridades de gestión de riesgos, recursos disponibles y nivel de exposición a esta amenaza.

Dicho esto, es clave comprender desde ahora que el ransomware no es una amenaza estática. Los atacantes buscan constantemente nuevas formas de llegar a sus objetivos, tanto en la fase técnica inicial como en la etapa final de extorsión.

La mejora continua y la capacidad de adaptación deben formar parte de la estrategia defensiva, ya que las protecciones que funcionaban ayer no siempre serán eficaces para prevenir o mitigar los ataques de hoy.

El ransomware no es solo una amenaza más. En los últimos años ha absorbido casi cualquier actividad de ciberdelito que no involucre fraude comercial o financiero. Hoy vemos intentos de extorsión incluso sin cifrado de datos, presionando a las empresas con posibles daños reputacionales y obligaciones legales relacionadas con la protección de la información.

Proteger una organización contra el ransomware no es difícil únicamente porque sea una amenaza compleja, sino porque gran parte de los riesgos asociados a vulnerabilidades de la infraestructura de TI convergen en este tipo de ataque.

Las cifras del ransomware

Los rescates pagados por empresas a bandas de ransomware sumaron **813 millones de dólares** en 2024 y **1,25 mil millones** en 2023.
(Chainalysis, 2025)

El rescate promedio exigido en un ataque de ransomware es de **1,3 millones de dólares.**
(Coalition)

6% de los ataques de extorsión amenazan a las víctimas con filtración de datos y ya no usan cifrado.
(Sophos, 2025)

25% de las empresas pagan el rescate exigido.
(Veeam, Q4 2024)

Considerando solo los ataques que emplean filtración de datos sin cifrado, 41% de las víctimas paga la extorsión.
(Veeam, Q4 2024)

Qué hay de nuevo

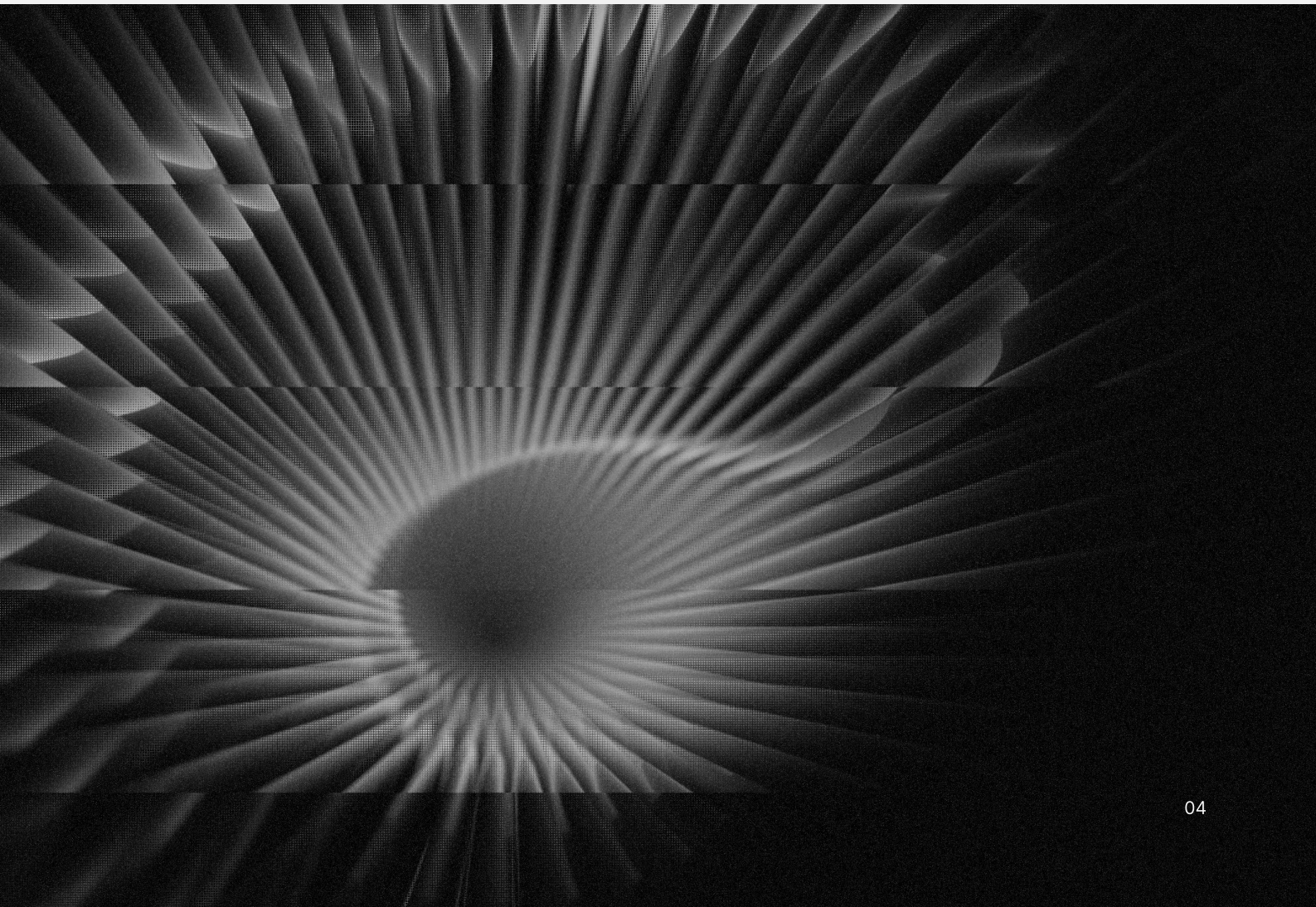
Esta es una versión revisada y actualizada de un documento que publicamos en 2022. Si leíste la versión original, las principales actualizaciones se encuentran en los capítulos sobre los grupos de ransomware y las medidas de prevención.

Aunque el ransomware se ha consolidado como una de las principales amenazas cibernéticas durante los últimos 15 años, las bandas que atacan a las empresas no son organizaciones estables. Acciones policiales, problemas operativos y conflictos internos llevan a muchas de estas pandillas a cesar sus actividades —o al menos a declararlo públicamente para despistar a las autoridades o a antiguos cómplices. Por eso, los nombres y actores relevantes en el mundo del ransomware ya no son los mismos.

Las prioridades de prevención también han cambiado. Los grupos de ransomware apuestan cada vez más por la presión de las repercusiones legales y el daño reputacional que conlleva la exposición de datos robados.

Una estrategia de prevención y recuperación que solo contemple copias de seguridad y reinstalación de sistemas comprometidos no basta para evitar que la empresa sea presionada por los delincuentes.

Creemos que los capítulos dedicados a estos temas merecen ser revisados. Algunas secciones son completamente nuevas (como la que aborda los ataques a la cadena de suministro), mientras que otras se reescribieron o complementaron con datos actualizados.



Evolución del ransomware

Cómo llegamos al escenario actual

Directo al punto — El ransomware no es una amenaza aislada. El ecosistema criminal que sostiene este tipo de fraude depende de varios "servicios": cobro, lavado de dinero y ocultación de rastros digitales son algunos de los más relevantes. Aquí explicamos cómo el ransomware pasó de ser un malware rudimentario que bloqueaba la pantalla y exigía rescate vía SMS a convertirse en una herramienta capaz de paralizar la infraestructura digital de una empresa y exigir millones de dólares en criptomonedas.

El "primer" ransomware

Tras tantas menciones en los titulares, el ransomware casi no necesita presentación. Mientras algunas empresas han pagado millones de dólares a criminales para retomar operaciones, otras ni siquiera han tenido la opción y se han visto forzadas a cerrar. Pero ¿cómo logró esta amenaza fortalecerse tanto en apenas una década?

El primer código malicioso que puede considerarse "ransomware" apareció en 1989. Creado por el biólogo Joseph Popp, se distribuía en disquetes que supuestamente contenían información sobre el VIH/SIDA, de gran interés médico en esa época. Una vez instalado, bloqueaba el sistema y pedía un rescate de **189 dólares.**

Además de exigir pago para recuperar el sistema, el mismo tipo de "**mensaje de rescate**" que existe hoy, el malware cifraba nombres de archivos y carpetas, impidiendo usar el ordenador. Era un anticipo de técnicas actuales, como la **criptografía asimétrica.**

Este código primitivo se conoce como "AIDS Trojan" por la etiqueta de los disquetes utilizados para propagarlo, aunque también se lo llama "PC Cyborg", pues era la empresa que supuestamente recibiría el pago del rescate.

Las autoridades no tuvieron problemas para identificar al autor. Sin embargo, Joseph Popp presentaba problemas mentales y fue declarado inimputable por los tribunales.

Ciberdelito moderno, criptomonedas y OPSEC

Aunque las similitudes saltan a la vista, no es del todo correcto buscar explicaciones para el ransomware moderno observando programas maliciosos tan antiguos. Esta amenaza, tal como existe hoy, es **producto de circunstancias que van más allá de las capacidades técnicas y del software.** De hecho, las circunstancias legales y las obligaciones que enfrentan las víctimas de las bandas de ransomware han surgido como una de las principales cartas de negociación de los delincuentes.

Para quienes tienen el desafío de defender una red, conocer las condiciones necesarias para un ataque exitoso y **monitorear la actividad criminal para anticipar movimientos** y preparar una respuesta puede ser clave para actuar con firmeza y desmantelar la capacidad del atacante de concretar el fraude.

El primer paso es analizar qué busca el intruso y qué medios y herramientas tiene a su alcance. Lamentablemente, la estructura criminal que existe hoy, y que sostiene al ransomware, se ha construido a lo largo de décadas de fraudes en internet.

En otras palabras, el ransomware es una amenaza que se ha desarrollado durante al menos 15 años de perfeccionamiento de la actividad delictiva en el entorno digital.

Una de las principales preocupaciones del criminal profesional es la OPSEC (seguridad operacional), cuyo objetivo es reducir el riesgo de ser arrestado y perder acceso a las ganancias ilícitas. Cuanto más fácil resulte recibir dinero ilegal o realizar delitos “tradicionales” como el lavado de activos y la falsificación de identidad, más audaz tiende a ser el crimen digital.

La transformación del ransomware en una amenaza personalizada, en la que los delincuentes saben exactamente a quién atacan y cuánto pueden exigir a la víctima, fue impulsada por la aparición de un medio de pago capaz de viabilizar transferencias millonarias: las criptomonedas.

La relación entre el ransomware y las criptomonedas es realmente profunda. En 2017, las autoridades estadounidenses desmantelaron la casa de cambio de criptomonedas BTC-e, acusándola de ayudar a los criminales. En 2025, un investigador que se identifica solo como GangExposed afirmó que un evento de blockchain no era más que una fachada para lavar dinero proveniente de fraudes.

Aunque ninguna acción oficial confirmó esa denuncia, las criptomonedas y la tecnología blockchain aparecen con frecuencia en estos delitos, incluso mediante servicios para ocultar el origen de los fondos y lavar activos, conocidos como tumblers.

A pesar de esta relación tan estrecha hoy en día, **el ransomware existía antes de las criptomonedas.** En los países del antiguo bloque soviético, los primeros “bloqueadores” de sistemas cobraban mediante servicios de SMS Premium: la víctima solo debía enviar un mensaje al número indicado para recibir el código de desbloqueo, y el cobro aparecía luego en la factura telefónica.

En otros casos, el pago se hacía a través de una plataforma llamada E-Gold, que fue cerrada por el Departamento de Justicia de Estados Unidos en 2007. En aquella época, los montos exigidos por el “rescate” difícilmente superaban los 300 dólares. En el caso de los SMS, el costo solía ser de apenas 10 dólares.

En el resto de Europa y en América, donde las regulaciones más estrictas en el sector de telecomunicaciones impedían este tipo de cobro por SMS, el "ransomware" solía presentarse **disfrazado de un antivirus falso**. El pretexto de vender software permitía a los criminales cobrar el "rescate" con tarjeta de crédito. El costo de estos "programas" rondaba los 50 dólares.

Fueron estos falsos antivirus los que, en la segunda mitad de la década de 2000, introdujeron mensajes que alertaban sobre supuestos "problemas" en el ordenador, con tácticas como cambiar el fondo de pantalla, una técnica que los ransomwares siguen utilizando.

Cuando se comunican con las empresas atacadas para "negociar" el rescate, no es raro que las bandas de ransomware aún traten a las víctimas como "clientes" o "pacientes", un eco de aquella época en que los delincuentes vendían programas de "seguridad". Para reforzar la presión, algunos incluso llegaron a ofrecer supuesta "asesoría legal" a los propios criminales involucrados en la negociación, con el fin de intimidar a la víctima con riesgos jurídicos.

Algunos virus de rescate icónicos, como CryptoLocker y CryptoWall, usaban la misma estética visual (escudos y candados) que caracterizaba a los falsos programas de seguridad.

Por supuesto, no todos querían o podían cobrar con tarjeta de crédito, sobre todo porque las entidades procesadoras empezaron a ser investigadas debido al alto volumen de devoluciones (chargebacks). Así surgió una "segunda línea" de bloqueadores que cobraban mediante tarjetas prepago y vales de regalo.

Un malware destacado de esta familia fue Reveton. Ya considerado un verdadero "ransomware", no empleaba cifrado. En su lugar, realizaba **una estafa de extorsión** alegando que la víctima había cometido un delito y debía pagar una multa.

Ejemplo: fondo de pantalla usado por el ransomware LockBit.

Para ello, mostraba pantallas personalizadas con el nombre y la imagen de la autoridad policial correspondiente al país del usuario.

El cobro se hacía a través de servicios especializados en facilitar transferencias internacionales, como Ukash, Paysafe y MoneyPak. Los montos exigidos rondaban los 200 dólares.

Un nombre especialmente notorio en este ámbito fue Liberty Reserve, fundada en 2001 y desmantelada en 2013 por una operación del FBI después de que salieran a la luz múltiples pruebas de que la plataforma se utilizaba para transacciones entre delincuentes.

Según el Departamento de Justicia de Estados Unidos, Liberty Reserve habría servido para lavar alrededor de 250 millones de dólares. Su fundador se declaró culpable y fue condenado a 20 años de prisión en 2016.

La caída de Liberty Reserve en 2013 coincidió con la maduración del mercado de criptomonedas. En ese momento, la casa de cambio Mt. Gox seguía en auge, con un conjunto de funciones y características que marcarían el camino para futuras plataformas competidoras.

CryptoLocker: el malware que definió una categoría de extorsión

Fue también en 2013 cuando especialistas en seguridad detectaron CryptoLocker. Distribuido principalmente a través de otros códigos maliciosos ya existentes (como la botnet Gameover ZeuS) y plataformas de envío masivo de spam, se estima que recaudó cerca de 27 millones de dólares en bitcoin.

Las características y el funcionamiento de CryptoLocker lo colocan a la par de códigos modernos. Utilizaba criptografía asimétrica y servidores de control, siendo clasificado como crypto-ransomware para diferenciarlo de otras formas de extorsión digital. Sin embargo, el éxito de CryptoLocker ayudó a consolidar esta modalidad de fraude, **que hoy conocemos simplemente como "ransomware".**

A diferencia de otros malwares de la época, el sistema criptográfico de CryptoLocker no fue quebrado. Solo fue posible desarrollar una herramienta de descifrado después de una operación policial que permitió obtener las claves utilizadas en la estafa.

Por otro lado, tres aspectos diferenciaban a CryptoLocker de las extorsiones actuales: el monto exigido, la forma de distribución y la ausencia de "doble extorsión". Todos están conectados. Mientras que hoy las víctimas corporativas pueden recibir demandas de cientos de miles o incluso millones de dólares, CryptoLocker pedía alrededor de 500 dólares.

Las cifras millonarias que vemos hoy son consecuencia del modo de distribución y de la práctica de la doble extorsión. En la actualidad, los operadores controlan cada invasión de manera directa, penetrando profundamente en la red corporativa y reduciendo las posibilidades de recuperación a partir de copias de seguridad. La doble extorsión consiste en robar la información antes de cifrarla, para amenazar a la víctima con filtrarla públicamente.

Nada de esto ocurría con CryptoLocker. El malware se distribuía masivamente a través de redes zombi y con el uso de exploit kits, que aprovechaban fallas en navegadores y complementos.

En otras palabras, era común que el usuario se infectara simplemente por visitar un sitio web malicioso. Estas visitas dependían de motores de búsqueda, anuncios fraudulentos y la intrusión en páginas legítimas pero vulnerables. Era un modelo de propagación oportunista y no dirigido. **Quizá el último ransomware relevante distribuido de esta manera fue WannaCry en 2017.**

Programado para explotar una vulnerabilidad de Windows de forma automática, WannaCry atacaba cualquier sistema accesible. Esto aumentaba la probabilidad de que los sistemas de copia de seguridad quedaran intactos, facilitando la recuperación.

El rescate exigido por WannaCry seguía siendo relativamente bajo —entre 300 y 600 dólares. Casi en paralelo, otro ransomware menos mediático, Locky, comenzaba a escalar y a cobrar cantidades de cuatro dígitos.

A partir de 2017, se producen transformaciones importantes en el mundo del crimen de ransomware:

2017

La casa de cambio de bitcoin BTC-e es desmantelada por el Departamento de Justicia de Estados Unidos. Acusada de lavado de dinero (el monto estimado sería de 4 mil millones de dólares), era considerada una de las plataformas favoritas de los operadores de ransomware. Como el principal acusado no pudo ser extraditado a EE. UU. por una disputa judicial entre Grecia, Rusia y Francia, el caso aún no tiene resolución definitiva.

2018

Aparece el ransomware Ryuk, que concentra sus ataques en empresas y organizaciones. Los sistemas individuales de consumidores y profesionales independientes quedan en segundo plano. Se estima que hasta el 81% de todos los ataques de ransomware en 2018 tuvieron como víctimas a empresas. Con objetivos más valiosos, el monto exigido por los rescates se disparó: en 2019, Ryuk llegó a intentar cobrar 12,5 millones de dólares a una sola víctima.

2019

Expansión de los servicios de mixing o cryptocurrency tumblers, que mezclan criptomonedas de distintos orígenes para ocultar ganancias ilícitas. Según un informe de BitFury, el volumen de bitcoins transferidos desde mercados de la darknet, que era de solo 1% a inicios de 2019, creció de forma constante durante el año y alcanzó el 20% en el primer trimestre de 2020.

2020

La estrategia de doble extorsión crece casi 500%, y los pagos empiezan a cobrarse en la criptomoneda Monero. El ransomware se consolida también como mecanismo de filtración de datos, donde la amenaza de divulgar información corporativa se convierte en la segunda cara de la extorsión. En paralelo, los servicios de mixers comienzan a ser perseguidos por autoridades y las casas de cambio de criptomonedas se ven obligadas a implementar procesos más estrictos de KYC (Know Your Customer). Esto lleva a que ransomwares notorios, como REvil, empiecen a exigir pagos en Monero —más difícil de rastrear— o a cobrar hasta 20% más caro a quienes solo pueden pagar en bitcoin. El resultado: en 2020 se atribuyeron al ransomware 692 millones de dólares en transacciones con criptomonedas.

2023

Los grupos de ransomware comienzan a enfocarse en proveedores y a apostar por la filtración de datos. El éxito de la doble extorsión llevó a que algunas bandas experimentaran ataques basados únicamente en el robo de información, sin cifrado. Ataques dirigidos a proveedores de software o servicios de TI, ya sea explotando vulnerabilidades o credenciales filtradas, provocaron incidentes que afectaron a cientos de empresas al mismo tiempo, sin necesidad de penetrar directamente sus redes corporativas.

A pesar de la evolución en los mecanismos de cobro (rescates más altos y pagos más anónimos), el ransomware seguía dependiendo en gran medida de otros tipos de malware, como si "viajara" aprovechando infecciones previas. Cuando este modelo se mostró limitado, los operadores criminales apostaron por una estructura más especializada, dividiendo y compartimentando la actividad delictiva para lograr mayor escala.

Al empezar a buscar objetivos específicos y de alto valor, los grupos de ransomware lograron justificar demandas cada vez más altas, alcanzando millones de dólares en algunas víctimas.

Esta estrategia culminó con ataques a empresas de sectores críticos. El grupo DarkSide golpeó a Colonial Pipeline en 2021, exigiendo un rescate de 4,4 millones de dólares, marcando un hito histórico en los ciberataques. Ese y otros incidentes similares demostraron que el ransomware podía impactar operaciones de infraestructura, salud y energía, consolidándose como la mayor amenaza digital moderna.

TOTAL ROBADO POR RANSOMWARE 2020–2024:

US$ 4,8 mil millones

COSTO PROMEDIO DE UN ATAQUE DE RANSOMWARE EN 2024:

US$ 5,13 millones

Las organizaciones criminales detrás del ransomware

Como en una línea de producción, los delincuentes se han especializado

Directo al punto — Las bandas que ejecutan ataques de ransomware enfrentan múltiples desafíos para escalar sus operaciones sin perder efectividad. Conocer el funcionamiento diario de estas redes criminales es el primer paso para que los equipos de seguridad, especialmente los de monitoreo e inteligencia de amenazas, puedan diseñar medidas preventivas e incluso anticipar acciones futuras. Analizando grupos como BlackCat, Clop y DragonForce, entenderemos cómo se especializan, sus disputas internas y las frágiles relaciones de confianza que se construyen a partir de la ambición y el afán de aumentar el volumen de ataques.

Clop y Scattered Spider: extorsión a través de servicios de TI

Las bandas responsables de ransomwares no son estructuras estables. Por diversas razones — peleas internas, reestructuraciones, estafas entre criminales (calotes) y operaciones policiales— es común que se disuelvan, incluso con anuncios públicos de "retiro" de actividades. Sin embargo, los individuos que las integran y las herramientas empleadas suelen permanecer en la escena, ya sea mediante la venta del código utilizado o formando nuevas alianzas y grupos.

Clop es un ejemplo claro. Surgió como sucesor de un ransomware conocido como CryptoMix y opera desde 2019. Se ha vuelto relevante por llevar a cabo una serie de ataques y extorsiones que se apartan significativamente del patrón tradicional de un ransomware.

Una de sus características más notorias son los ataques masivos a través de servicios de TI o software empleados por múltiples empresas. Desde finales de 2020, Clop ejecutó cuatro grandes ataques contra plataformas de transferencia de datos, robando información de miles de compañías. Una estimación sugiere que una sola campaña masiva contra MOVEit Transfer le habría generado más de 75 millones de dólares a la banda.

Clop también se destacó por realizar ataques sin depender del cifrado de archivos, apoyándose exclusivamente en la presión que ejerce la amenaza de filtrar datos corporativos para obligar a sus víctimas a pagar.

En un escenario de ransomware más tradicional, una empresa atacada se preocuparía principalmente por sus propios datos, por la recuperación de sistemas y por la continuidad del negocio. En cambio, en un fraude centrado en la filtración de información, las mayores inquietudes son las consecuencias legales y comerciales, como la pérdida de clientes y la exposición de proyectos sensibles.

Las copias de seguridad ya no impactan directamente la capacidad de respuesta de la empresa. De hecho, un backup sin protección puede convertirse en una brecha a explotar, pues los delincuentes solo necesitan acceder a una copia de los archivos, sin importar dónde esté almacenada. Esto contrasta con el ransomware tradicional, donde el malware debía comprometer todos los respaldos para ser efectivo.

Al no cifrar archivos, Clop logra mayor escala y rapidez en sus ataques masivos. Además, no requiere acceso completo a los sistemas corporativos ni permisos de escritura sobre los datos; la lectura basta para copiar la información y comenzar la extorsión.

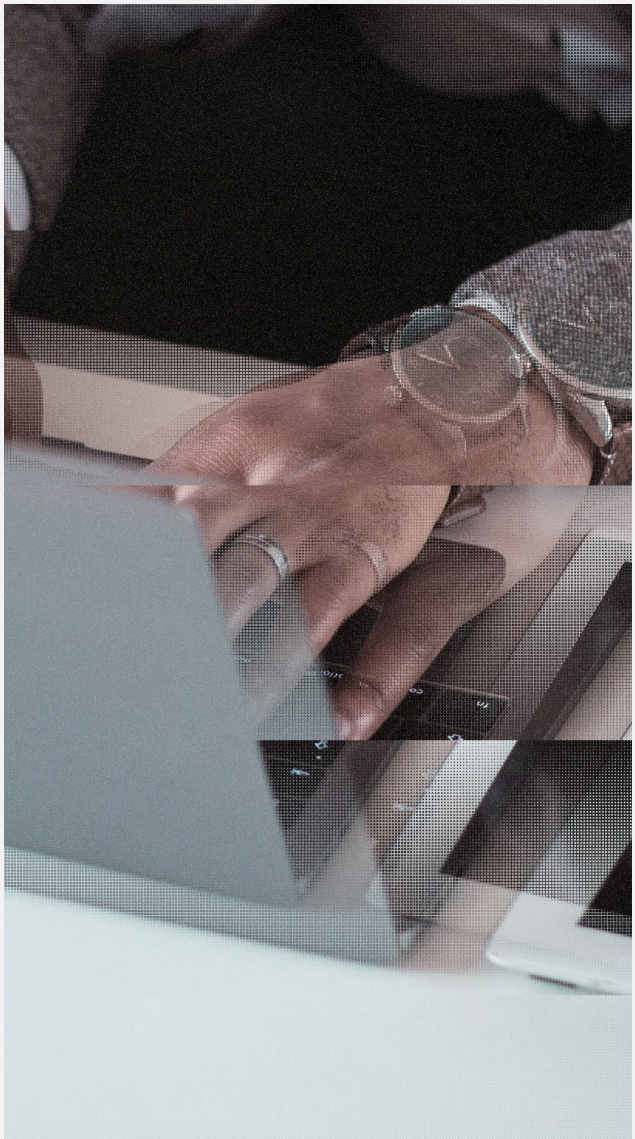
Evidentemente, la ausencia de cifrado también significa que la extorsión suele ser menos contundente que la doble extorsión (que combina cifrado con amenaza de filtración). Sin embargo, Clop ha demostrado que no es necesario cifrar datos para que la operación sea rentable.

Se estima que Clop ya ha recaudado alrededor de 500 millones de dólares en pagos de rescate desde su creación.

Por su parte, Scattered Spider, conocido por varios alias en la comunidad de ciberseguridad y vinculado a un colectivo llamado “The Com”, es célebre por sus tácticas de ingeniería social. Se cree que el grupo cuenta con numerosos cómplices en países occidentales, dado que estos ataques de ingeniería social también se realizan por teléfono.

Los objetivos de ingeniería social de Scattered Spider son casi siempre proveedores de servicios que trabajan en helpdesks o funciones de soporte similares. En general, el grupo es conocido por explotar debilidades en sistemas y procesos de autenticación, recurriendo a phishing, SIM swapping y otras técnicas.

Al igual que Clop, individuos vinculados a esta banda han llevado a cabo extorsiones sin usar ransomware tradicional para cifrar archivos. Tanto por la forma de obtener acceso a las redes corporativas como por su método de extorsión, Scattered Spider plantea nuevas preocupaciones para las empresas.



Dragonforce

Aunque hay indicios de que la banda DragonForce se organizó en 2023 como un grupo de hacktivismo en defensa de Palestina, sus acciones recientes tienen una motivación claramente financiera.

DragonForce ha crecido estableciendo alianzas bajo un modelo de ransomware as a service (RaaS, "ransomware como servicio"), ganando notoriedad por su capacidad de absorber afiliados descontentos con otras operaciones criminales.

El RaaS imita el modelo de software como servicio (SaaS) para permitir que los desarrolladores de un ransomware se distancien de la operación diaria y de los ataques directos a las víctimas.

Este modelo no es nuevo. Antes de la existencia de DragonForce, el grupo Conti lo perfeccionó con una estructura altamente segmentada, dejando a los "afiliados" la tarea de comprometer a los objetivos. Sin embargo, Conti cesó sus operaciones en 2022 tras una serie de filtraciones de comunicaciones internas que expusieron conflictos y desconfianza dentro de la banda.

Un rasgo particular de DragonForce es la posibilidad para los afiliados de crear sitios propios donde publican los ataques y gestionan las negociaciones. Esto ayuda a ocultar la relación entre el afiliado y DragonForce, permitiendo que cada uno opere con su propia "marca" mientras se aloja en la infraestructura del grupo. DragonForce llama a este modelo "cártel", ya que otorga mayor autonomía a cada afiliado.

A mediados de 2025, surgieron indicios de que individuos vinculados a Scattered Spider estaban desplegando el ransomware de DragonForce en sus ataques, consolidando una nueva alianza criminal.

Este tipo de movimientos demuestra que los vínculos en el mundo del cibercrimen son altamente flexibles y suelen adaptarse a la conveniencia del momento, aunque los delincuentes intenten agruparse en torno a organizaciones con cierta estabilidad y reputación

Aunque DragonForce sea un nombre relativamente nuevo, su estructura, así como las tácticas y herramientas que utiliza (por ejemplo, Mimikatz y Cobalt Strike), ya han sido empleadas previamente por otros actores delictivos.

Ransomware como servicio: un pilar del ransomware

Con el modelo RaaS (Ransomware as a Service), un ransomware cuenta con múltiples afiliados encargados de realizar las intrusiones, mientras que la negociación de los pagos queda en manos del núcleo central de la banda. Cuando una operación criminal alcanza este nivel de escala y debe gestionar personas e infraestructura tecnológica propia, con el desafío añadido de que la confianza es un recurso escaso en el mundo del delito, no es raro que descuidos, infiltraciones y errores expongan detalles valiosos sobre cómo operan.

Esta información permite construir contramedidas y emitir alertas tempranas frente a posibles actividades de ransomware en los entornos vigilados.

Algunos ejemplos de información que el monitoreo de la actividad criminal puede proporcionar:

1. Tactics, techniques, and procedures (TTPs): cómo llega el ransomware a la red objetivo, qué tipos de credenciales pueden estar en uso (VPN, bases de datos, dominios, proveedores de nube), qué vulnerabilidades recientes requieren más atención, entre otros factores.

2. Indicators of compromise (IoCs): archivos, direcciones IP y comportamientos de sistemas que pueden señalar la presencia de ransomware antes de que se active.

3. Targets (objetivos): empresas y sectores que podrían estar bajo la mira de los delincuentes. Por ejemplo, comunicados de grupos como LAPSUS (que no es estrictamente una banda de ransomware, aunque sus ataques son similares) llegaron a identificar públicamente compañías específicas; varias de estas fueron detectadas e interceptadas por Axur.

4. Filtraciones y credenciales: para maximizar ganancias, los criminales anuncian los datos que poseen para venderlos, ofreciendo incluso muestras de información. En especial cuando incluyen credenciales, estos datos son un fuerte indicador de una violación ya ocurrida o inminente.

5. Datos corporativos: además de credenciales, el monitoreo puede revelar exposición de información empresarial sensible (finanzas y contabilidad, datos personales de empleados y clientes, proyectos con socios, etc.). Esto indica riesgos legales y de reputación y puede servir para rastrear una intrusión a partir del tipo de información expuesta (por ejemplo, mediante un análisis forense del sistema donde se almacenaba).

Por qué el ransomware tiene empleados y proveedores

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

Una de las fuentes más sólidas y reveladoras sobre la operación diaria de un ransomware fue la filtración de conversaciones internas de la banda Conti, ocurrida en febrero de 2022. Estos chats habrían sido divulgados por un investigador de seguridad ucraniano como represalia, después de que el grupo manifestara apoyo a Rusia en el conflicto con Ucrania.

Los diálogos confirmaron muchas sospechas sobre el funcionamiento cotidiano de estas organizaciones, pero también mostraron que los líderes de las bandas pagan salarios a sus "empleados" (en el caso de Conti, eran al menos 100 personas) y que existe una especie de "departamento de recursos humanos" para reclutar nuevos miembros y reemplazar a quienes no cumplen las expectativas de desempeño.

Aun así, la desconfianza es una constante. Un caso notorio fue el de la banda **BlackCat**, que cerró sus operaciones en mayo de 2024 dejando a varios afiliados reclamando comisiones impagas.

El riesgo de estafas internas y traiciones mantiene tensiones permanentes en el ecosistema del cibercrimen.

El modelo de afiliados y de "crimen como servicio" comenzó a consolidarse ya en la década de 2000, cuando delincuentes vendían acceso a códigos maliciosos y a los Exploit Kits (EKs), herramientas diseñadas para explotar vulnerabilidades en navegadores, mediante suscripciones o comisiones, y con estadísticas de éxito integradas.

Fueron precisamente los EKs y las redes de spam (que también alquilan su capacidad de envío masivo de correos a otros criminales) los que sentaron la base para las primeras infecciones de ransomware. Además, distribuían ladrones de credenciales, datos de tarjetas de crédito, mineros de criptomonedas y otras formas de fraude digital.

La estafa de los antivirus falsos, que vendían supuestos programas de seguridad, también usaba este esquema de afiliados comisionados, una práctica legítima en el mercado formal, pero explotada aquí para encubrir responsabilidades. De hecho, "culpar a los afiliados" de las prácticas dudosas servía como mecanismo de protección para los delincuentes, que en esa época temían la represalia de bancos y emisores de tarjetas de crédito.

Con la llegada de las criptomonedas, este pretexto perdió relevancia. Sin embargo, el modelo de afiliados sigue siendo clave para mantener la motivación económica y sostener la especialización en cada fase de la operación criminal.

Las especialidades del delito

El modelo “ransomware como servicio”, que llevó este método al ransomware, ya se estaba esquematizando en 2012. 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 el afiliado recibiría.

El afiliado del ransomware sería el único responsable de la infección de las computadoras. Había, por lo tanto, dos figuras: el autor del ransomware, responsable de programar el software y mantener la infraestructura básica de control de la amenaza para recopilar estadísticas, y el distribuidor, responsable de encargarse de toda la entrega del malware hasta la víctima.

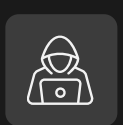
El escenario actual es más complejo. Tanto la tarea del autor del ransomware como la del distribuidor se han dividido en partes más pequeñas, cada una realizada por individuos dedicados a la tarea.

Cargos de empleados y afiliados de ransomware

Programadores, o “coders”: son los responsables de crear el software necesario para la operación. Ellos desarrollan el ransomware, aplican los algoritmos de cifrado en el código e integran herramientas.

Probadores: el “control de calidad” de un ransomware depende principalmente de su capacidad para evitar herramientas antivirus. Las pruebas, en este caso, se realizan mediante el análisis del malware frente a soluciones de seguridad y la modificación de su código para eludir protecciones.

Administradores de red: son responsables de la infraestructura, servidores de control y distribución. Muchos ransomwares utilizan archivos de configuración dinámicos, lo que les permite cambiar a una nueva infraestructura si la anterior es desmantelada. Para aprovechar esta funcionalidad, la infraestructura debe reconstruirse periódicamente.



Cazadores de vulnerabilidades: realizan ingeniería inversa en software y sistemas para encontrar fallas de seguridad que puedan explotarse en ataques.

Hackers: utilizan la infraestructura, los programas y las vulnerabilidades preparados por el resto del equipo para ejecutar ataques contra los objetivos planificados. Son responsables del movimiento lateral dentro de las organizaciones, empleando herramientas de robo de contraseñas y de escaneo de red (como Nmap y Mimikatz) para que la ejecución final del ransomware afecte la mayor cantidad posible de sistemas, incluso en diferentes sistemas operativos.

Negociadores y "abogados": individuos responsables de dialogar con las víctimas del ransomware para obtener el pago. Los "abogados" pueden ayudar en la negociación reforzando los riesgos legales derivados de la filtración de los datos robados por la banda.

Especialistas en criptomonedas: son los encargados de diseñar los mecanismos de lavado de dinero que se usarán para transferir las sumas pagadas por las víctimas al sistema bancario.

Aun con toda esta gama de roles y especializaciones, la operación de un ransomware sigue teniendo otras demandas que necesitan ser cubiertas por proveedores externos.

En cualquier negocio, el crecimiento a gran escala tiene pros y contras. En el caso del ransomware, aunque el aumento de escala incrementó las ganancias ilícitas mediante la sofisticación del fraude y la especialización de los involucrados, también generó una demanda considerable de acceso a nuevos objetivos.

Es evidente que algunos grupos son más organizados y especializados que otros. Sin embargo, todos los delincuentes tienen acceso al mismo ecosistema, del cual pueden adquirir información o contratar servicios. Así como un programador de ransomware puede contratar a un criminal especializado en spam, otro puede comprar un malware ya preparado para distribuirlo a través de redes sociales o técnicas de ingeniería social y convertirse en cómplice del delito sin necesidad de conocimientos técnicos profundos.

Para que todo esto sea posible, los criminales crearon espacios de negociación relativamente abiertos, facilitando la entrada de nuevos actores capaces de sostener todo el esquema, sin importar cuál sea su habilidad principal.

Para quienes cuentan con un monitoreo especializado de esas redes y espacios, estos entornos se convierten en una fuente valiosa de datos. A través de ellos es posible anticipar o detectar ataques antes de que ocurran, por ejemplo, mediante la identificación temprana de credenciales filtradas.

Como el criminal que roba una credencial no siempre es el mismo que la usa, interceptar estas transacciones puede ser decisivo para frenar un ataque antes de que se ejecute.

La prevención de un ataque de ransomware mediante actividades de inteligencia y monitoreo tiene un potencial de eficacia sumamente relevante en este escenario.

La extorsión basada en la filtración de datos hace que las medidas de recuperación y restauración (como las copias de seguridad) resulten insuficientes para aliviar la presión del pago del rescate, ya que la empresa puede seguir expuesta a una filtración de datos. Estas filtraciones provocan daños a la marca y a la reputación.

Se han registrado casos en los que los delincuentes usaron la base de clientes o de empleados de la víctima para advertirles sobre el riesgo de exposición de su información personal en caso de que la empresa se negara a pagar.

Esta es la gran apuesta del ransomware moderno: aunque una organización haya hecho su tarea con copias de seguridad y cuente con un plan de recuperación sólido, prácticamente no hay cómo evitar el daño provocado por la exposición de datos. Para empeorar la situación, no existe garantía alguna de que los datos realmente serán eliminados por los criminales.

Proveedores del ransomware

Spammer: un delincuente especializado en comprar o montar una infraestructura capaz de enviar correos electrónicos maliciosos. Estos correos pueden enviarse de forma masiva o diseñarse a medida para alcanzar un objetivo específico. El criterio de éxito para este proveedor es lograr que el mensaje llegue a la bandeja de entrada superando los filtros anti-spam.

Access Broker: un intermediario que negocia accesos previamente obtenidos a una red corporativa. Puede estar especializado en el uso de ladrones de credenciales o en la compra de credenciales robadas por otros criminales. Las negociaciones y ofertas de accesos suelen realizarse abiertamente en los darknet markets y otros espacios frecuentados por delincuentes.

Insider: un empleado dentro de la empresa atacada o de un proveedor de servicios (como una operadora de telecomunicaciones) reclutado para ofrecer acceso a los operadores de ransomware. Las ofertas para contratar insiders suelen ser descaradas, con publicaciones en redes sociales o incluso en el fondo de pantalla configurado por el ransomware (táctica utilizada por LockBit).

Prevención

Llevando a la práctica lo que sabemos sobre el adversario

Directo al punto — Conociendo el ecosistema del crimen y sus debilidades, es posible actuar de manera incisiva y amplia en la recolección y el análisis de los datos expuestos por los delincuentes, mapeando el riesgo de la empresa y eliminando los puntos de entrada que podrían ser utilizados en los ataques. Como el ransomware depende de accesos externos, estas medidas no siempre necesitan involucrar únicamente al equipo interno de seguridad y deben considerar una acción más amplia que incluya la ciberseguridad externa.

Endurecimiento contra Ransomware

Guía Rápida

Evalúe las protecciones existentes frente a los vectores de ataque del ransomware

Credenciales robadas

- Use un servicio de monitoreo de credenciales
- Implemente autenticación multifactor (MFA) resistente al phishing
- Adopte un sistema de gestión de identidad
- Capacite y concientice a los usuarios sobre el uso seguro de credenciales
- Aplique una arquitectura *zero trust*

Malware

- Utilice una solución de EDR/XDR
- Conecte sus soluciones de seguridad a plataformas de inteligencia
- Implemente soluciones IDS o restrinja el uso de aplicaciones no autorizadas

Ingeniería social

- Incluya la concienciación de los colaboradores en su política de seguridad
- Añada protecciones a los navegadores, como sandbox o restricciones de acceso externo

Vulnerabilidades

- Utilice una solución de External Attack Surface Management (EASM) para detectar sistemas expuestos a la red y vulnerabilidades
- Aplique actualizaciones con parches de seguridad
- No exponga sistemas de acceso remoto (RDP) a la red
- Mantenga habilitadas las funciones de seguridad
- Proteja los recursos de la red corporativa utilizando autenticación Kerberos y funciones de seguridad en los controladores de dominio

Proveedores y terceros

- Supervise las prácticas de seguridad de proveedores y terceros para que estén alineadas con las políticas aplicadas a todo el negocio
- Cree mecanismos de aislamiento con privilegios reducidos y controles de acceso a recursos en la nube

Cómo la amenaza de filtraciones cambió el peso de la prevención

Hasta 2020, una buena estrategia de recuperación era suficiente para mitigar el impacto del ransomware, pero la práctica de la doble extorsión (rescate de datos acompañado de amenaza de filtración) cambió este escenario. Incluso con la restauración de los sistemas, el riesgo de exposición de datos dificulta evitar otros perjuicios derivados del ataque, como el daño a la marca y las posibles consecuencias legales previstas en leyes de privacidad y protección de datos.

Con la amenaza de la doble extorsión ya consolidada, algunos grupos comenzaron a explorar un nuevo enfoque basado exclusivamente en la filtración de datos. Estos ataques liberan al atacante de la necesidad de obtener accesos de escritura a la información, abriendo un abanico mucho más amplio de posibilidades para llevar a cabo extorsiones.

Ya hay quienes prefieren utilizar el término "extorsión de datos" para referirse a todas las modalidades de chantaje, abandonando el concepto tradicional de ransomware.

El Clop, que ya hemos mencionado, Hunters International y criminales vinculados a The Com (Scattered Spider) son algunos de los actores que han tenido éxito con este tipo de amenaza. De acuerdo con el informe State of Ransomware 2025 de Sophos, la cantidad de ataques de extorsión sin cifrado, basados únicamente en la amenaza de filtrar datos, se duplicó en un año.

En ese estudio, este tipo de ataques representa el 6 % de todos los incidentes de extorsión y el 13 % de los incidentes de esta categoría en empresas con menos de 250 empleados.

Ya sea en un contexto de doble extorsión o como extorsión única, el robo de datos seguido de la amenaza de exponer información corporativa provoca un cambio en las prioridades a la hora de combatir el ransomware.

En este escenario, las medidas capaces de prevenir o interrumpir un ataque en curso agregan un gran valor a la estrategia de defensa.

Al limitar y cortar el acceso del delincuente a la red de la empresa antes de la sustracción de datos, la organización protege sus secretos comerciales y su reputación, y evita tener que tomar una decisión sobre pagar o no un rescate millonario.

La prevención de cualquier ataque cibernético requiere una madurez sólida en seguridad de la información, con la aplicación de parches, políticas y procesos adecuados. Sin embargo, estos pasos básicos no siempre son suficientes. Además, garantizar que no haya errores o incumplimientos es un desafío constante.

El ransomware suele dirigirse a cada empresa de forma personalizada, con un operador humano respaldado por una banda interesada en superar mecanismos de seguridad tradicionales (como el antivirus). Por otro lado, los recursos de seguridad internos pueden ser limitados, en especial debido a la escasez de profesionales que enfrenta el mercado de ciberseguridad.

Por esta razón, es necesario contar con equipos especializados en mitigar riesgos específicos, muchos de ellos visibles desde el exterior, precisamente por las dificultades que los propios operadores de ransomware se han creado al organizar operaciones delictivas sofisticadas y a gran escala.

Filtraciones de credenciales: el preludio del ransomware

Según la edición 2025 del Data Breach Investigations Report (DBIR) de Verizon, el 22 % de las intrusiones comienzan con una credencial robada. Este conjunto incluye ataques de extorsión, ya sea mediante ransomware tradicional o amenazas de exponer información corporativa.

A pesar de que el robo de credenciales representa un riesgo importante, existen formas de enfrentar este desafío.

Como el ransomware contemporáneo depende de un verdadero ecosistema de ciberdelincuencia, hay múltiples oportunidades para detectar actividades sospechosas mediante el monitoreo de ese ecosistema. Se trata de información que puede indicar que una organización está en riesgo o, en el peor de los casos, que ya está bajo la mira de criminales.

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

Además de contraseñas filtradas de bases de datos comprometidas, los equipos de CTI (Cyber Threat Intelligence) y ART (Axur Research Team) de Axur siguen de cerca filtraciones derivadas del uso de malware dedicado al robo de credenciales (credential stealers). Aunque no sean parte directa de la operación de un ransomware, las credenciales obtenidas por este tipo de malware se agrupan en colecciones destinadas a ser vendidas en el mercado negro digital. A través de esta comercialización, se conectan con todo tipo de actividades delictivas.

Las credenciales pueden venderse a access brokers o directamente a bandas de ransomware, que luego encontrarán víctimas de su interés o credenciales de sistemas (infraestructuras en la nube, paneles de control, bases de datos) que ya conocen y saben que pueden servir como un buen punto de entrada a la red de una empresa.

El monitoreo de Axur ya ha identificado más de 17 mil millones de credenciales robadas, y cada mes se detectan cerca de 700 mil nuevas, representando un riesgo para miles de personas y para las empresas donde trabajan.

Este tipo de trabajo permite interrumpir una cadena de eventos que podría terminar en un ataque de ransomware. Al ser alertada sobre contraseñas robadas o canales vulnerables a este tipo de acceso, la organización puede reaccionar: al cancelar la credencial comprometida, la escalada de acciones maliciosas se detiene.

Tanto en el caso de Colonial Pipeline en 2021 como en el ataque a Change Healthcare en 2024, el acceso inicial ocurrió a través de credenciales robadas. Según lo que se sabe, la serie de ataques que afectó a empresas usuarias del sistema de almacenamiento Snowflake, también en 2024, se originó igualmente en credenciales comprometidas.

Una alerta previa sobre la filtración de esas credenciales podría haber cambiado el rumbo de estos incidentes.

Un credential stealer puede ser distribuido por correo electrónico mediante ingeniería social y phishing, pero también es muy común su propagación a través de redes sociales. La capacidad de este tipo de malware para robar sesiones de inicio de sesión almacenadas en el navegador (muchas veces derrotando la autenticación multifactor) los hace especialmente atractivos para secuestrar cuentas de creadores de contenido, incluso de aquellos que utilizan todos los mecanismos de seguridad que ofrecen los grandes proveedores de servicios de internet.

Un empleado puede poner en riesgo a la empresa aun cuando el credential stealer se haya instalado en su computadora personal a partir de un enlace compartido en redes sociales. Todas las contraseñas robadas, incluso las que aparentemente no guardan relación con sistemas corporativos, pueden ser usadas en ataques de credential stuffing, donde se prueban credenciales obtenidas en otro servicio para intentar acceder a un sistema más valioso.

En otras palabras, una contraseña robada de cualquier cuenta puede ser validada y probada contra sistemas corporativos de mayor interés para bandas de ransomware. A través de los access brokers, intermediarios que comercializan canales de acceso, esas credenciales llegan a operadores mejor capacitados, dando inicio al ataque de ransomware.

Las credenciales también pueden quedar expuestas debido a accesos no autorizados a bases de datos, ya sea de la propia empresa o de un proveedor externo. Implementar tokens de rastreo puede facilitar la detección temprana de una filtración y detener el ataque mediante la revocación de credenciales comprometidas o la eliminación del acceso de proveedores que hayan sido afectados.

Este trabajo de monitoreo puede integrarse directamente en la operación de seguridad de la organización. Al contar con mecanismos para detectar violaciones a las políticas de seguridad y otras normas de cumplimiento, incluso de empleados que reutilizan contraseñas o de proveedores que no siguen buenas prácticas, la empresa fortalece su protección contra ransomware y eleva su nivel de madurez en ciberseguridad a lo largo de toda la cadena de operación.

Monitoreo de la superficie de ataque externa

Antes incluso de obtener credenciales o datos corporativos, los atacantes pueden realizar exploraciones (scans) en los sistemas que la empresa expone a internet, como servidores web, correos electrónicos, VPN y canales de API. Al encontrar una vulnerabilidad, un error de configuración o datos expuestos, pueden descubrir el camino inicial para infiltrarse en el entorno de la víctima.

En el complejo ecosistema digital corporativo no es raro que dashboards, servicios web, almacenamiento en la nube y otros recursos se adopten de forma improvisada para cubrir una necesidad específica o temporal, sin integrarse claramente a los procesos y sistemas oficiales. Muchas veces estos recursos carecen de documentación y su existencia no se comunica al departamento de TI, generando el fenómeno conocido como shadow IT.

Por esta razón, no basta con que la empresa vigile únicamente su superficie de ataque interna y los recursos administrados por el departamento de TI.

En la mayoría de los casos, el atacante está fuera y, por lo tanto, el primer contacto con el entorno corporativo ocurre precisamente a través de esta superficie externa, incluso con aquellos recursos que no son administrados oficialmente por el equipo de TI.

En resumen, el atacante puede llegar a conocer mejor esta superficie externa que la propia empresa, especialmente si no ha existido un esfuerzo coordinado para monitorearla, mapearla y protegerla. No es posible aplicar un parche de seguridad a un sistema cuyo uso el propio equipo de TI desconoce.

Las soluciones de External Attack Surface Management (EASM) ayudan a las organizaciones a visualizar su infraestructura desde fuera, tal como lo haría un atacante. El EASM apoya la gestión de vulnerabilidades, detecta errores de configuración e identifica software y dispositivos indebidamente expuestos a la red.

Monitorear, mapear y garantizar la conformidad de todos estos sistemas externos es esencial para impedir que los atacantes encuentren accesos ocultos al entorno corporativo.

El riesgo de ataques a terceros y la seguridad de la cadena de suministro (supply chain)

En lugar de atacar directamente a sus objetivos finales, algunos grupos de ransomware buscan puntos de falla comunes en los proveedores de las empresas. Estos ataques se conocen como supply chain attacks, ya que alcanzan a la organización a través de otras entidades de las que depende.

Como muchas compañías permiten conexiones directas o indirectas de terceros a su infraestructura de TI, el riesgo involucrado en este tipo de campañas no difiere mucho del de un ataque directo contra la propia organización.

Para el atacante, encontrar una vulnerabilidad o falla en un proveedor puede permitirle impactar a decenas o cientos de empresas con una sola acción. De esta manera, un único ataque cibernético se convierte en múltiples intentos de extorsión, dirigidos individualmente a cada víctima.

Tipos de ataques a terceros

No existe una categorización formal para todos los ataques dirigidos a proveedores, pero muchas de estas acciones pueden agruparse según el tipo de tercero explotado.

Ataques a infraestructura tercerizada

Estos ataques aprovechan características, fallas o puntos comunes en un servicio digital utilizado por varias empresas.

El ejemplo más emblemático es el caso de Snowflake, un servicio de almacenamiento en la nube. Aunque los responsables del ataque no explotaron vulnerabilidades en la propia plataforma, la falta de autenticación multifactor (MFA) en numerosas cuentas de clientes permitió un robo masivo de datos, afectando a 165 organizaciones sin necesidad de comprometer directamente su infraestructura interna.

En otros casos, los delincuentes intentaron explotar debilidades en proveedores de identidad y otros servicios de TI.

Esta estrategia también ha sido utilizada por actores fuera del ámbito del ransomware. Un caso particularmente preocupante se reportó en 2023, cuando hackers chinos obtuvieron una clave criptográfica de la infraestructura en la nube de Microsoft para atacar a clientes de la empresa en el gobierno de Estados Unidos. Este incidente motivó una investigación de la recién creada Cyber Safety Review Board.

Ataques a servicios de apoyo

Los criminales han empleado ingeniería social para engañar a centros de atención o helpdesk tercerizados y así obtener acceso a la infraestructura corporativa.

Dado que estos equipos suelen tener permisos para restablecer contraseñas de usuarios, se convierten en un punto débil del proceso de autenticación. El atacante puede hacerse pasar por un empleado de la empresa y solicitar el restablecimiento de la contraseña, e incluso la desactivación de factores adicionales de autenticación.

También existen reportes de amenazas de violencia física contra empleados tercerizados que prestan estos servicios. Si la empresa contratante no cuenta con mecanismos para registrar y monitorear estos incidentes, puede enterarse de un intento de ataque únicamente después de que la intrusión ya se haya concretado.

Ataques a softwares

Los ataques que explotan vulnerabilidades en software no son nuevos. Sin embargo, el tipo de vulnerabilidad utilizada y el propósito de la explotación crean un escenario particular que debe entenderse dentro del contexto general de ataques a proveedores.

El elemento clave a considerar es la finalidad de explotar la falla: si se usará para un esquema de extorsión de datos. Los programas que cumplen funciones críticas dentro de las redes corporativas, como servicios de transferencia de datos y herramientas de administración remota, suelen ser los objetivos preferidos de este tipo de acción.

No siempre es necesario que el ataque se base en una vulnerabilidad del propio software. Los delincuentes también pueden intentar comprometer directamente a la empresa desarrolladora para manipular el producto y, desde allí, llegar a las víctimas. El caso de SolarWinds, en 2020, es el ejemplo más conocido de este tipo de ataque, aunque no involucró ransomware.

Esto no significa que el ransomware no adopte la misma táctica. En 2017, el software de contabilidad M.E. Doc fue alterado para propagar el malware conocido como NotPetya. Hoy NotPetya se clasifica como un wiper, ya que carecía de una función real para descifrar y recuperar archivos.

Aun así, el impacto sobre las víctimas fue muy similar al de un ataque de ransomware de la época, y es poco probable que los operadores de ransomware no estén buscando software que pueda servir como puerta de entrada a redes corporativas.

Los casos más recientes y notorios de ataques de extorsión explotando software fueron liderados por el grupo Clop, que aprovechó vulnerabilidades en servicios como GoAnywhere y MOVEit Transfer, amenazando a cientos de organizaciones con divulgar la información sustraída a través de esas plataformas.

Con herramientas de ciberseguridad externa, las empresas pueden ganar visibilidad sobre los problemas presentes en sus conexiones con terceros. Por ejemplo, el monitoreo de credenciales puede ampliarse para incluir a proveedores o socios que tengan acceso a sistemas corporativos.

Paralelamente, el seguimiento de información de inteligencia mantiene a los equipos de seguridad al tanto de las tácticas más recientes utilizadas por los grupos de ransomware y de qué programas o servicios están siendo explotados en campañas activas, lo que permite una respuesta más rápida y precisa para prevenir o minimizar el impacto de los ataques.

Inteligencia en ciberseguridad

Seguir de cerca los movimientos de las bandas de ransomware permite mapear las vulnerabilidades y técnicas que utilizan. En la práctica, esto hace posible priorizar las acciones con mayor impacto para proteger la organización.

- Priorizar la aplicación de parches para vulnerabilidades que están siendo explotadas activamente por bandas de ransomware.
- Reforzar la seguridad de canales y servicios (como un proveedor de nube específico) que estén implicados en ataques recientes.
- Mejorar los sistemas de seguridad ya implementados (antivirus, firewalls, XDR) con información relevante de IoCs, como direcciones IP y archivos maliciosos.
- Conocer los riesgos específicos para el sector de actividad de la empresa.
- Actuar para impedir el reclutamiento de insiders que puedan colaborar con ciberdelincuentes.
- Adoptar sistemas de gestión de contraseñas (bóvedas) y autenticación multifactor (MFA) para fortalecer la seguridad de credenciales y canales de acceso. Estas medidas pueden evitar que una credencial se filtre o disminuir su utilidad en caso de ser robada.

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

1. Los operadores de ransomware adquieren credenciales y medios de acceso a sistemas corporativos de otros delincuentes especializados en la intrusión inicial o en el robo de inicios de sesión y contraseñas (estos actores a veces son llamados Access Brokers).

2. Monitorear el flujo de estas transacciones y ofertas permite identificar quién más puede estar en riesgo y cómo los atacantes podrían obtener acceso a la red corporativa.

3. Al detectar una credencial filtrada, la organización puede bloquearla de inmediato.

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

5. Sin ese acceso inicial, el ataque se vuelve mucho más difícil y no puede continuar.

Recuperación y respuesta

Cómo reaccionar ante un ataque de ransomware

Directo al Punto — Dado que una empresa suele depender en gran medida de su infraestructura tecnológica, un ataque de ransomware puede comprometer todo el negocio. La paralización de las actividades exige una postura proactiva que proyecte la solidez esperada por inversionistas, clientes y otros stakeholders. Esto requiere preparación, canales de comunicación claros y un buen checklist que oriente la actuación de los equipos involucrados en el momento más crítico. El checklist de la Agencia de Ciberseguridad de los Estados Unidos (CISA) es nuestra referencia para esta guía.

La visión ejecutiva de la respuesta al ransomware

En un fraude de doble extorsión (cifrado de archivos acompañado de la amenaza de filtración de datos), como ocurre en la mayoría de los ataques de ransomware actuales, la organización enfrenta dos desafíos principales:

1. Restaurar la infraestructura de TI para reanudar las operaciones y minimizar el perjuicio derivado de la interrupción causada por el cifrado de archivos.
2. Proteger la reputación y la marca de la empresa ante clientes, empleados y demás stakeholders.

Aunque la protección de la marca no sea una preocupación directa del equipo encargado de recuperar los sistemas, es importante definir un canal de comunicación adecuado para quienes asumirán esa responsabilidad.

El equipo de TI también puede priorizar acciones concretas que demuestren preocupación por los clientes, como proteger las credenciales que puedan haber caído en manos de los atacantes. La organización puede lograrlo invalidando las contraseñas antiguas y exigiendo un cambio en el próximo inicio de sesión, sin alarmar a los usuarios con una notificación de cambio masivo.

No obstante, es importante señalar que la organización puede tener obligaciones legales específicas. En Estados Unidos, por ejemplo, diversas leyes de notificación de filtraciones de datos exigen a las empresas comunicar a los titulares afectados cuando su información personal ha sido comprometida. Reglas semejantes existen en otras jurisdicciones, como la normativa europea de protección de datos (GDPR).

Si el ataque no cifró datos, la extorsión suele basarse principalmente en repercusiones legales y reputacionales. Los delincuentes incluso pueden chantajear a la empresa amenazando con divulgar el incidente a clientes y socios cuyas informaciones fueron obtenidas durante la intrusión.

Para estos escenarios, es recomendable preparar una estrategia de comunicación sólida que oriente a clientes y socios sobre la situación y evite que los criminales tomen el protagonismo al divulgar el incidente. La comunicación será más efectiva si la empresa cuenta con controles de seguridad o procesos capaces de determinar con precisión qué datos fueron comprometidos y qué acciones deben tomar todas las partes afectadas por la filtración.

La preparación es esencial

La respuesta a un incidente de ransomware puede ser mucho más efectiva si se han tomado ciertas medidas previas.

Capacite al equipo de TI para la respuesta inicial a incidentes de seguridad.

No es raro que, frente a problemas cotidianos, administradores de redes y analistas de TI opten por reiniciar o apagar sistemas. Estas acciones pueden eliminar evidencias que después serían útiles para esclarecer el incidente. Dado que suelen ser ellos quienes detectan primero los síntomas de una intrusión, una respuesta inicial adecuada puede facilitar las etapas siguientes.

Pruebe las copias de seguridad y planifique la recuperación.

El backup es un elemento central frente al ransomware. Sin embargo, no basta con realizar copias de seguridad: es fundamental que los archivos estén protegidos y, preferiblemente, desconectados (offline).

Considere los riesgos específicos de los respaldos en la nube.

En backups alojados en la nube, es necesario evaluar el tiempo de restauración (dependiente de la velocidad de red y otras limitaciones) y la posible dependencia de sistemas conectados y vulnerables al ransomware. Usar múltiples proveedores de nube y soluciones de almacenamiento inmutable puede ayudar a evitar que los atacantes comprometan todos los respaldos. Dado que los backups en la nube pueden ser accedidos de manera remota, también deben cifrarse para impedir que sean usados para chantajear a la empresa con amenazas de divulgación de datos.

Determine canales de contacto de emergencia.

Los canales de comunicación habituales de la empresa pueden no ser confiables o incluso quedar fuera de servicio durante un incidente de ransomware. Es fundamental estar preparado para montar una sala de guerra y establecer contacto con consultoras de ciberseguridad, partes interesadas y directivos mediante medios que no dependan directamente de la infraestructura corporativa.

Estructure procesos de control de datos y privacidad.

En muchos países, la legislación vigente exige que las empresas protejan los datos personales y notifiquen a las personas afectadas por una filtración. Determinar si un atacante obtuvo o no acceso a información personal puede ser clave para evitar que la organización sea chantajeada con amenazas de exposición de datos.

Elabore un plan de recuperación y un programa de Gestión de Continuidad de Negocio (GCN) junto con un Business Impact Analysis (BIA).

Os planos de recuperação de desastre e GCN mapeiam riscos e a interdependência de processos do negócio, facilitando a priorização de sistemas para a recuperação. Sem isso, um sistema considLos planes de recuperación ante desastres y de continuidad de negocio ayudan a mapear riesgos y la interdependencia de procesos críticos, facilitando la priorización de sistemas a restaurar. Sin esta preparación, un sistema considerado crítico durante un análisis apresurado puede ser recuperado y seguir inoperante debido a dependencias no identificadas con otros sistemas fuera de la lista de restauración.

El Business Impact Analysis (BIA), por su parte, evalúa el impacto de la interrupción de servicios para definir los requisitos operativos y recursos necesarios. Con ello, contribuye a establecer hitos claros para la recuperación y estimar los plazos de restablecimiento. Cuanto menos preparada esté la organización al enfrentar un incidente de ransomware, mayor será el esfuerzo requerido del equipo de respuesta, prolongando la indisponibilidad de sistemas y aumentando las pérdidas.

Además, mientras más rápida sea la reacción y la reanudación de operaciones normales, menor será el daño a la reputación de la empresa, especialmente si puede demostrarse que no se pagó el rescate.

Checklist: respondiendo a un incidente de ransomware

Una buena referencia para elaborar una estrategia de respuesta ante un ataque de ransomware es el Ransomware Guide elaborado por la CISA, la agencia estadounidense responsable de la ciberseguridad y la infraestructura.

El checklist contiene 19 ítems divididos en 3 grandes etapas de respuesta. A continuación, se presentan los 19 puntos con algunos comentarios adaptados:

Etapa 1: Detección y Análisis

1. Determine los sistemas impactados y aíslelos de inmediato

- Si varias subredes pueden haber sido afectadas, desconéctelas todas desde el switch. Puede que no sea viable desconectar equipo por equipo durante el incidente.
- Si no es posible desconectar toda la red, desconecte sistemas individuales quitando cables o eliminando la conexión Wi-Fi.
- Los sistemas también pueden aislarse mediante segmentación en VLANs. En algunos entornos o servicios (como la nube pública), esta puede ser la opción más adecuada.
- Si la intrusión comenzó a través de un tercero o socio, revoque todas las credenciales o canales de acceso vinculados a él.
- Los atacantes pueden intentar monitorear la comunicación interna de la empresa. Utilice preferiblemente métodos alternativos de comunicación (como llamadas telefónicas) y actúe de manera coordinada para evitar el movimiento lateral de los delincuentes o el agravamiento del ataque.

2. Solo apague sistemas si no es posible desconectarlos de la red

- El apagado debe ser el último recurso, ya que elimina evidencia volátil (como la memoria del sistema) y dificulta el análisis forense.

3. Clasifique los sistemas que deben ser restaurados y recuperados

- Identifique y priorice los sistemas evaluando la naturaleza de los datos almacenados en cada uno y la función que cumplen (seguridad, salud, generación de ingresos, etc.).

Etapa 1: Detección y Análisis

4. Inicie un esfuerzo de Threat Hunting para comprender cómo ocurrió el ataque.

- Busque nuevas cuentas creadas en el directorio de usuarios o cuentas cuyas propiedades de autenticación hayan sido modificadas.
- Revise los inicios de sesión en sistemas de acceso remoto y VPN.
- Analice los endpoints en busca de herramientas que puedan haber comprometido copias de seguridad y credenciales (como Mimikatz) o que se hayan usado para exfiltrar datos (herramientas como Rclone y clientes de almacenamiento en la nube que no son utilizados por la organización).
- Verifique registros de actividad relacionados con el envío de datos hacia el exterior de la red, en cualquier puerto.

Etapa Intermedia: Comunicación, Documentación y Gestión

Aunque esta etapa no está explícitamente definida en la guía de la CISA, es en este momento cuando deben consolidarse todas las informaciones recopiladas durante la fase inicial. También aquí se inicia un flujo de comunicación con directivos y stakeholders, **que debe mantenerse durante todo el proceso de respuesta para proteger la reputación de la empresa.**

5. Reúnase con su equipo para desarrollar y documentar la comprensión inicial de lo ocurrido a partir del análisis preliminar.

6. Utilizando la información de contacto de autoridades y proveedores de servicios de la organización, comuníquese con equipos internos y externos, así como con stakeholders, teniendo claro qué puede aportar cada uno para ayudar a mitigar, responder y recuperarse del incidente.
   - Comparta la información que tenga para que el apoyo recibido sea relevante y efectivo. Mantenga informados a los responsables y a la alta dirección con actualizaciones regulares sobre el progreso de la situación.

Etapa 2: Contención y Erradicación

7. Guarde una imagen del sistema y una copia de la memoria de una muestra de los dispositivos afectados (por ejemplo, estaciones de trabajo y servidores). Recoja registros relevantes y copias de archivos de malware que actúen como precursores del ransomware, así como cualquier otro dato observable que pueda considerarse un IoC (direcciones IP de servidores de comando y control, entradas sospechosas en el registro del sistema, entre otros archivos).
   - Preste especial atención a preservar información altamente volátil, como registros y datos en memoria del sistema, para evitar su pérdida o alteración.

8. Consulte a las autoridades policiales sobre la posible existencia de herramientas de descifrado disponibles.
   - Los especialistas de Axur pueden ayudar a encontrar herramientas de descifrado; sin embargo, en la mayoría de los casos el descifrado no será posible.

9. Investigue fuentes confiables para obtener recomendaciones específicas sobre la variante de ransomware identificada y siga los pasos sugeridos para detectar e aislar los sistemas o redes comprometidos.

10. Identifique las credenciales y sistemas involucrados en la intrusión inicial. Una credencial comprometida puede ser, por ejemplo, una cuenta de correo electrónico.

11. Con base en los datos de la intrusión obtenidos en las fases anteriores, aísle cualquier sistema que pueda ser usado para mantener acceso no autorizado. Estas invasiones suelen ir acompañadas de un robo masivo de credenciales.
    - Para proteger la red y otras fuentes de información frente a nuevos accesos no autorizados, puede ser necesario desactivar servicios de VPN y acceso remoto, inhabilitar el inicio de sesión único (SSO) y restringir activos de acceso público o en la nube.

12. Acción adicional sugerida: identificación de cifrado de datos en servidores
    - Los datos en servidores pueden ser cifrados por un ransomware instalado directamente en ellos. Sin embargo, también existen casos en los que el cifrado se realiza desde un endpoint autorizado sin que esto signifique que el propio servidor esté infectado.
    - Sesiones de acceso abiertas a carpetas compartidas, la información de propietario de los archivos y los historiales de inicio de sesión en servicios de RDP pueden ayudar a descubrir si los datos almacenados en servidores están siendo cifrados desde una estación de trabajo comprometida.
    - El registro de seguridad de Windows, los registros de eventos del servicio SMB y herramientas de análisis de tráfico (como Wireshark) también pueden ayudar a identificar el origen del acceso no autorizado.

Etapa 2: Contención y Erradicación

13. Examine los sistemas existentes de detección y prevención de ataques a la organización (antivirus, respuesta en endpoints, sistemas IDS e IPS, etc.) y sus registros. Esto puede revelar evidencias adicionales sobre sistemas comprometidos o malware involucrado en las etapas iniciales del ataque.
    - Busque señales de malware del tipo Dropper, que actúa como precursor del ransomware. Como explicamos al abordar la estructura del cibercrimen, el acceso a redes corporativas suele ser comprado por los operadores de ransomware, mientras que los Access Brokers se especializan en obtener el acceso inicial mediante malware de acceso remoto o de robo de credenciales.

14. Realice un análisis exhaustivo para identificar mecanismos de persistencia de afuera hacia adentro y de adentro hacia afuera.
    - De afuera hacia adentro: credenciales robadas o creadas por los atacantes, vulnerabilidades, sistemas perimetrales comprometidos con malware de acceso remoto.
    - De adentro hacia afuera: herramientas de acceso remoto instaladas en sistemas internos que van desde suites ofensivas profesionales como Cobalt Strike hasta utilidades de soporte remoto como AnyDesk.

15. Restaure los sistemas priorizando los servicios críticos (como los de salud, seguridad o generación de ingresos), preferiblemente utilizando imágenes preconfiguradas.
    - Asegúrese de que se apliquen los parches adecuados y que el sistema de seguridad correspondiente (antivirus o XDR) esté presente y activo.

16. Una vez que el entorno haya sido completamente limpiado y restaurado (incluyendo la eliminación de mecanismos de persistencia y la rotación de credenciales comprometidas), realice un restablecimiento de contraseñas en todos los sistemas afectados y atienda las vulnerabilidades y brechas de seguridad o visibilidad mediante parches, actualizaciones y otras medidas de protección que aún no se hubiesen adoptado.

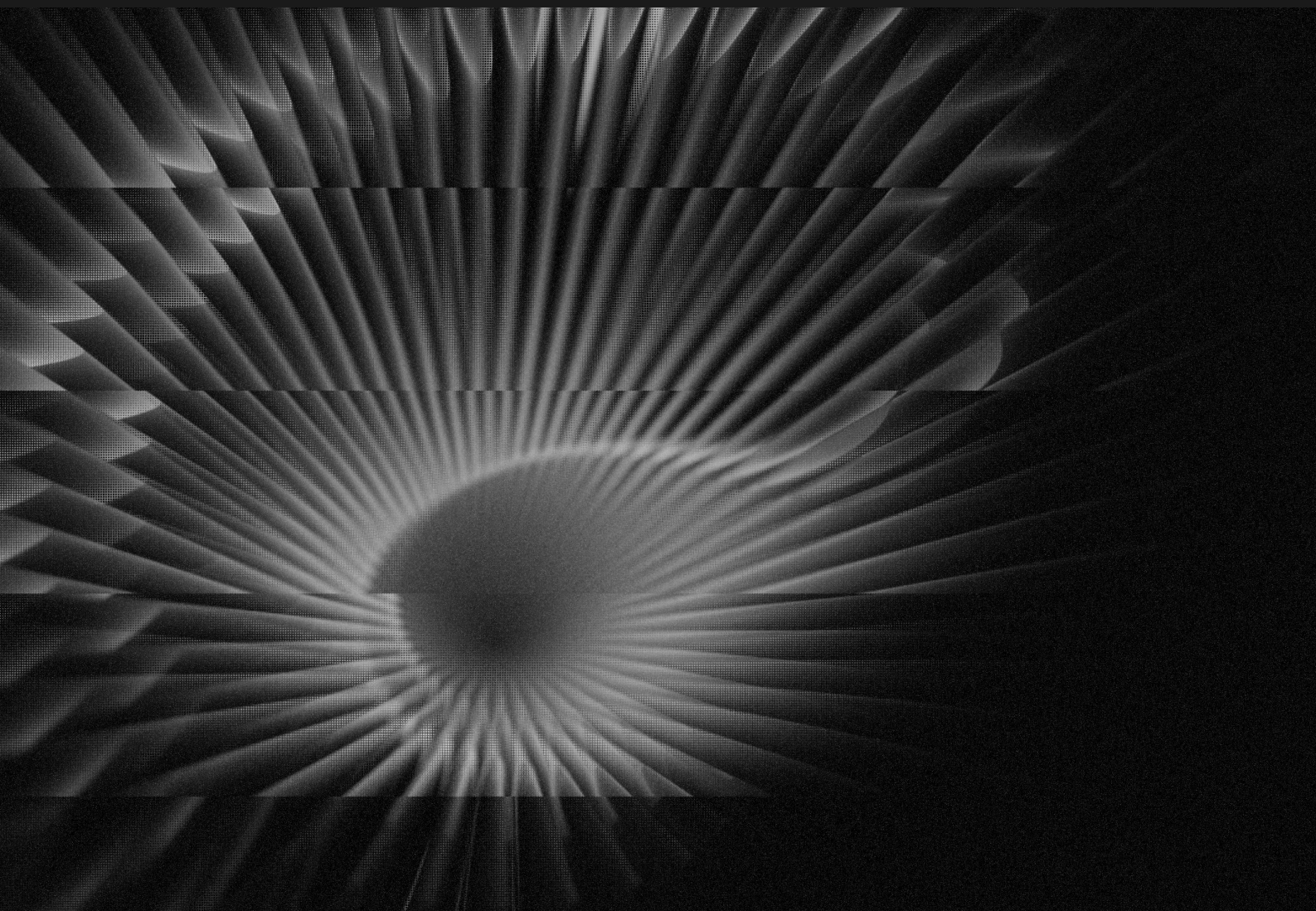
17. Con base en criterios previamente definidos —que pueden incluir todos los pasos anteriores o la búsqueda de asistencia externa—, la autoridad responsable de TI o ciberseguridad puede declarar el fin del incidente de ransomware.

Etapa 3: Recuperación y Actividad Post-Incidente

18. Reconecte los sistemas y restaure los datos a partir de backups fuera de línea y cifrados, priorizando los servicios críticos.
    - Recuerde: pagar el rescate no garantiza que sus datos serán devueltos ni que no se divulgarán.

19. Documente las lecciones aprendidas del incidente y todas las actividades de respuesta para respaldar la actualización y el perfeccionamiento de las políticas, planes y procedimientos de la organización, además de orientar futuros ejercicios y simulacros relacionados.

20. Considere compartir las lecciones aprendidas y los indicators of compromise (IoC) con autoridades u organizaciones relevantes del sector para contribuir a la mejora colectiva de la ciberseguridad.



Cuente con inteligencia externa para anticipar ataques

Axur refuerza la defensa contra el ransomware actuando donde los delincuentes inician todo: fuera del perímetro corporativo. Nuestra plataforma monitorea de manera continua credenciales filtradas, datos sensibles y puntos de exposición en la superficie externa de su organización y de sus proveedores, interceptando accesos que podrían ser vendidos a operadores de ransomware.

Con esta visibilidad anticipada, los equipos de seguridad pueden bloquear credenciales comprometidas, corregir vulnerabilidades críticas y reducir drásticamente las posibilidades de intrusión antes de que ocurra el ataque.

Además de la prevención, Axur acelera la respuesta a incidentes. Nuestra inteligencia sobre tácticas, técnicas y procedimientos (TTPs) de los grupos de ransomware alimenta los mecanismos de detección e investigación, facilitando la identificación de accesos no autorizados y la contención rápida de movimientos laterales.

Con la automatización de análisis, datos procesables y dashboards inteligentes, su equipo obtiene ventaja frente a un ecosistema criminal dinámico y puede mantener la continuidad operativa y la reputación incluso en escenarios de alta presión.

Refuerce su defensa contra el ransomware

AGENDE UNA DEMO

bsi ISO/IEC 27001 Information Security Management CERTIFIED

CleanDNS Trusted Reporter

Descubra todas nuestras soluciones en **axur.com**

///AXUR